Edivaldo João dos Santos

dicasetruquesdopc.blogspot.com

Segurança de informação

Como estar seguro utilizando a Internet?

Revisão técnica
Sérgio David Maziano
Higino D. A. João

Editora
MVDA

DEDICATÓRIA

Eu dedico este livro a Josimar dos Santos Fernandes e João Dias dos Santos.
Eles impulsionaram a minha vida de maneira profunda, pelo que eu sou mui grato.
Eles estarão para sempre no meu coração.

Também dedico este livro aos meus pais, Cosme de Abreu e Maria Antónia, por terem estado sempre ao meu lado.

Mais importante, eu dedico este livro a Deus, pelo talento e dom da vida que Ele me concedeu e por permitir-me contribuir desta forma por um mundo melhor. Glória a Ele, pois este livro não teria sido possível sem Ele.

Autor: EJ. Santos
Blog: https://dicasetruquesdopc.blogspot.com

Índice

Prefácio

Segurança de informação significa proteger a informação e o sistema de informação de acesso não autorizado, utilização, modificação, vistoria, gravação ou destruição.

Os termos segurança de informação, segurança computacional e asseguramento da informação são frequentemente utilizados de forma incorrecta. São campos muitas vezes relacionados e partilham objectivos comuns de proteger a confidencialidade, integridade e disponibilidade da informação; porém, existem algumas diferenças entre os mesmos.

Essas diferenças referem-se fundamentalmente a abordagem do tema, metodologias utilizadas e as áreas de concentração. A segurança de informação focaliza-se na confidencialidade, integridade e disponibilidade dos dados indiferentemente da forma que os dados tenham (electrónica, imprensa ou outras formas).

Segurança computacional pode focar-se em assegurar a disponibilidade e correcta operação do sistema computacional sem se preocupar com a informação armazenada ou processada pelo computador.

Acessos a informação armazenada em base de dados computacionais aumentaram em demasia. Cada vez mais as empresas estão a armazenar informações individuais e de negócio em computadores. Muita dessa informação armazenada é altamente confidencial e não é de domínio público.

Muitos negócios apenas funcionam com informações guardadas em computadores. Dados pessoais de funcionários, lista de clientes, salários, contas bancárias, informações de venda e marketing estão armazenadas numa base de dados. Sem esta informação seria muito difícil para certas organizações funcionar. A segurança de sistemas de informação precisa de ser implementada para proteger essa informação.

Um sistema de segurança de informação eficiente incorpora uma variedade de políticas, produtos de segurança, tecnologias e procedimentos. Softwares que forneçam um firewall e antivírus não são suficientes por si só para proteger a informação. Um conjunto de procedimentos e sistemas precisam de ser aplicados para impedir de forma eficiente o acesso não autorizado á informação.

Existem pessoas que vivem de hackear ou invadir o sistema de segurança de sistemas de informação. Eles usam os seus conhecimentos técnicos para invadirem sistemas informáticos e aceder informação privada. Firewalls, que servem para prevenir o acesso a redes de computadores, podem ser penetradas por um hacker com o hardware apropriado. Isso pode resultar na perda de

informação vital, ou um vírus pode ser instalado para apagar toda informação. Um hacker pode ter acesso á uma rede se um firewall for desligado por um minuto apenas.

Uma das maiores ameaças á segurança da informação é a pessoa que lida com o computador. Uma empresa pode ter um excelente sistema de segurança de informação a sua disposição, mas a segurança pode ser facilmente comprometida. Se um helpdesk receber um pedido de reset de senha por telefone, e assim proceder sem antes verificar para quem é esta informação, em seguida qualquer pessoa poderá facilmente ter acesso ao sistema. Os utilizadors de computador devem ser advertidos sobre a importância da segurança.

Algumas medidas simples de segurança podem ser tomadas por todos para manter os dados seguros. Mudar as senhas do seu computador periodicamente e utilizar combinação de letras e números caracteres maiúsculos e minúsculos e caracteres especiais, torna difícil os hackers terem acesso. Não mantenha uma nota no seu computador com as suas palavras-chave (isto é o mesmo que não guardar o teu multicaixa e o código pin juntos). Tu não gostarias que qualquer pessoa tivesse acesso a sua informação ou dinheiro disponível na sua conta bancária, e é o mesmo com o seu computador.

Nunca existirá um sistema totalmente seguro. Os hackers tentarão sempre encontrar formas sofisticadas de ganhar acesso. Porém, com a tecnologia implementando níveis cada vez mais altos de segurança de informação, tal como um sistema de reconhecimento por íris, os sistemas de segurança poderão mantê-los afastados por enquanto.

Este livro aborda a segurança do computador em varias vertentes, não se restringido apenas em explicar ao leitor como se defender, mas fazendo um a abordagem mais ampla. Falando das ameaças a segurança, como são feitas as invasões, como funcionam os antivírus, como os mesmos actuam, como identificar uma ameaça, o que fazer em caso do seu computador ser infectado ou invadido. Pode-se considerar este livro como uma inovação na abordagem do problema de segurança de sistemas de informação por tratar-se de vários livros em um só.

Como é organizado este livro

Breve descrição dos capítulos

Quem deveria ler este livro?

Os profissionais que devem se beneficiar mais com este livro são:

- Profissionais graduados em informática, formados há muitos ou poucos anos e que estejam preocupados com segurança;
- Programadores/Analistas/Desenvolvedores de Software e Engenheiros/Progra-madores/ de Testes e Gestores de Projectos;
- Profissionais de MIS e US&T (Information Systems and Tecnology – Sistemas de Informação e Tecnologia);
- Profissionais envolvidos com a configuração, implementação e gestão de intranets e da Intranet;
- Webmasters;
- Profissionais iniciantes (em termos de estudo de computação) que desejam entender como a internet funciona, ao invés do uso da Internet;
- Pessoas com formação avançada em Informática que queiram utilizar este livro como guia rápido;
- Pessoas que queiram aprender um pouco mais sobre segurança na Internet;
- Pessoas preocupadas com segurança de informação;
- Estudantes de TIC (Tecnologias de Informação e Comunicação).

Agradecimentos

Muitos são os amigos e profissionais que contribuíram, directa ou indirectamente, para a publicação deste livro. Os nomes de todos eles seria praticamente impossível recordar nesse momento, por serem tantos. Mas eu gostaria de agradecer àqueles que se superaram em me ajudar a tornar esse livro possível, começando com os grandes profissionais que estão a fazer a diferença na área de tecnologias de informação em Angola e não só, e aqueles que me ajudaram com dicas, sugestões, conhecimento técnico e apoio. Eles são Sergio Maziano da Alng, Higino João do BES, Yactiro Loureiro da ServiStar, Aires Tomás da Key IT, Hélder Cangula da PWC, Alberto Cardoso da TAAG, Gerson Santos do MCS, Mara António, Arnaldo Chitangueleca e Manuel Miguel do Minju, Boiki Pitlo e Daniel Mokgalapa da Botswana Telcom Corporation, Adam Smith da Cisco Systems, Johan Snyman da Torque IT, Craig Smith da ITSA Adam W. Smith da Microsoft, Robert Richardson da Computer Security Institute (CSI), Juan Brown da E-Council, Hélio Campos e José Gomes da Valleysoft, SA, Seydú Guimarães, Wilson dos Santos Albino, Jussie António, João Ndala da Indispensável, Lda.

O meu agradecimento especial áquelas pessoas ou instituições que tornaram possível a publicação dessa obra, são eles:

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.

Agradeço ao meu editor XXXXXXXXXXXXXXXX, pela ajuda que me concedeu com este livro e a Sérgio David Maziano e Higino D. A. João, pelo seu árduo trabalho de revisão técnica deste livro.

Gostaria também de agradecer aos meus pais, irmãos e primos e em especial a minha noiva pela compreensão quando tive que alterar a minha rotina e horários para que este livro fosse terminado! Serei eternamente grato a Deus, por todos aqueles acima e por permitir-me chegar às pessoas desta forma. Agradeço a Ele por ter-me dado a força necessária para a conclusão desta obra.

Edivaldo João dos Santos – edivaldo.santos@mss-ao.com

Parte I

Aprendendo como é feito o ataque

Capitulo I

Noções básicas de segurança

Noção de segurança

Sabemos que no mundo real não existem sistemas totalmente seguros e o mundo virtual segue o mesmo preceito. Por maior que seja a protecção adoptada, estaremos sempre sujeitos a invasões, roubos e ataques. Então é importante que conheçamos o perigo e saibamos como proteger-nos.

Actualmente já utilizamos a Internet para realizar diversos serviços comuns, como compras, serviços bancários, investimentos, além de negócios ou troca de informações confidenciais via e-mail.

Grande parte dos problemas ocorre por puro desconhecimento dos procedimentos básicos de segurança por parte dos utilizadors. Saber como agir em caso de problemas, também poderá ajudar, e muito, nas investigações policiais dos crimes virtuais. Mas, como tudo isso pode ser feito de maneira segura? Para fornecer informações de como utilizar de maneira segura os serviços da Internet e rede é que este livro foi elaborado.

Antes de aprofundarmos sobre o tema central do livro, farei uma breve abordagem sobre o conceito de segurança de informação.

O que é a segurança de informação?

Segurança da Informação está relacionada com protecção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São características básicas da segurança da informação os atributos de confidencialidade, integridade, disponibilidade e autenticidade, não estando esta segurança restrita somente a sistemas computacionais, informações electrónicas ou sistemas de armazenamento. O conceito aplica-se a todos os aspectos de protecção de informações e dados. O conceito de *Segurança Informática* ou *Segurança de Computadores* está intimamente relacionado com o de Segurança da Informação, incluindo não apenas a segurança dos dados/informação, mas também a dos sistemas em si.

Actualmente o conceito de Segurança da Informação está padronizado pela norma ISO/IEC 17799:2005, influenciada pelo padrão inglês (British Standard) BS 7799. A série de normas ISO/IEC 27000 foram reservadas para tratar de padrões de Segurança da Informação, incluindo a complementação ao trabalho original do padrão inglês. A ISO/IEC 27002:2005 continua a ser considerada formalmente como 17799:2005 para fins históricos.

Conceitos de segurança

A Segurança da Informação refere-se à protecção existente sobre as informações de uma determinada empresa ou pessoa, isto é, aplica-se tanto as informações corporativas quanto às pessoais. Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma

organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.

Podem ser estabelecidas métricas (com o uso ou não de ferramentas) para a definição do nível de segurança existente e, com isto, serem estabelecidas as bases para análise da melhoria ou deterioração da situação de segurança existente. A segurança de uma determinada informação pode ser afectada por factores comportamentais e de uso de quem usufrui dela, pelo ambiente ou infra-estrutura que a cerca ou por pessoas mal intencionadas que têm o objectivo de furtar, destruir ou modificar tal informação.

A tríade CIA (Confidentiality, Integrity and Availability) -- Confidencialidade, Integridade e Disponibilidade -- representa os principais atributos que, actualmente, orientam a análise, o planeamento e a implementação da segurança para um determinado grupo de informações que se deseja proteger. Outros atributos importantes são a irretratabilidade e a autenticidade. Com o evoluir do comércio electrónico e da sociedade da informação, a privacidade é também uma grande preocupação.

Portanto os atributos básicos, segundo os padrões internacionais (ISO/IEC 17799:2005) são os seguintes:

- ***Confidencialidade*** - propriedade que limita o acesso a informação tão-somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação.
- ***Integridade*** - propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controlo de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição).
- ***Disponibilidade*** - propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles utilizadors autorizados pelo proprietário da informação.

Para a montagem desta política, deve-se levar em conta:

- Riscos associados à falta de segurança;
- Benefícios;
- Custos de implementação dos mecanismos.

Mecanismos de segurança

O suporte para as recomendações de segurança pode ser encontrado em:

- *Controlos físicos*: são barreiras que limitam o contacto ou acesso directo a informação ou a infra-estrutura (que garante a existência da informação) que a suporta.

Existem mecanismos de segurança que apoiam os controlos físicos:

Portas / trancas / paredes / blindagem / guardas / etc...

- *Controlos lógicos*: são barreiras que impedem ou limitam o acesso a informação, que está em ambiente controlado, geralmente electrónico, e que, de outro modo, ficaria exposta a alteração não autorizada por elemento mal intencionado.

Existem mecanismos de segurança que apoiam os controlos lógicos:

- ***Mecanismos de criptografia***. Permitem a transformação reversível da informação de forma a torná-la ininteligível a terceiros. Utiliza-se para tal, algoritmos determinados e uma chave secreta para, a partir de um conjunto de dados não criptografados, produzir uma sequência de dados criptografados. A operação inversa é a decifração.
- ***Assinatura digital*.** Um conjunto de dados criptografados, associados a um documento do qual são função, garantindo a integridade e autenticidade do documento associado, mas não a sua confidencialidade.
- ***Mecanismos de garantia da integridade da informação*.** Usando funções de "Hashing" ou de verificação, consistindo na adição.
- ***Mecanismos de controlo de acesso*.** Palavras-chave, sistemas biométricos, firewalls, cartões inteligentes.
- ***Mecanismos de certificação*.** Certifica a validade de um documento.
- ***Integridade*.** Medida em que um serviço/informação é genuíno, isto é, está protegido contra a personificação por intrusos.
- ***Honeypot*:** É o nome dado a um software, cuja função é detectar ou de impedir a acção de um cracker, de um spammer, ou de qualquer agente externo estranho ao sistema, enganando-o, fazendo-o pensar que esteja de facto a explorar uma vulnerabilidade daquele sistema.
- ***Protocolos seguros*:** uso de protocolos que garantem um grau de segurança e usam alguns dos mecanismos citados aqui

Existe hoje em dia um elevado número de ferramentas e sistemas que pretendem fornecer segurança. Alguns exemplos são os detectores de intrusões, os anti-vírus, firewalls, firewalls locais, filtros anti-spam, fuzzers, analisadores de código, etc.

Ameaças à segurança

As ameaças à segurança da informação são relacionadas directamente à perda de uma de suas 3 características principais, quais sejam:

- ***Perda de Confidencialidade*:** seria quando há uma quebra de sigilo de uma determinada informação (ex: a senha de um utilizador ou administrador de sistema) permitindo que sejam expostas informações restritas as quais seriam acessíveis apenas por um determinado grupo de utilizadors.
- ***Perda de Integridade*:** acontece quando uma determinada informação fica exposta a manuseio por uma pessoa não autorizada, que efectua alterações que não foram aprovadas e não estão sob o controlo do proprietário (corporativo ou privado) da informação.
- ***Perda de Disponibilidade*:** acontece quando a informação deixa de estar acessível por quem necessita dela. Seria o caso da perda de comunicação com um sistema importante para a empresa, que aconteceu com a queda de um servidor ou de uma aplicação crítica de negócio, que apresentou uma falha devido a um erro causado por motivo interno ou externo ao equipamento ou por acção não autorizada de pessoas com ou sem má intenção.

No caso de ameaças à rede de computadores ou a um sistema, estas podem vir de agentes maliciosos, muitas vezes conhecidos como crackers, (hackers não são agentes maliciosos, pois tentam ajudar a encontrar possíveis falhas). Estas pessoas são motivadas para fazer esta ilegalidade por vários motivos. Os principais são: notoriedade, auto-estima, vingança e o dinheiro. De acordo com pesquisa elaborada pelo Computer Security Institute (http://gocsi.com/), mais de 70% dos ataques partem de utilizadors legítimos de sistemas de informação (Insiders) -- o que motiva corporações a investir largamente em controlos de segurança para seus ambientes corporativos (intranet).

Invasões na Internet

Todo sistema de computação necessita de um sistema para protecção de ficheiros. Este sistema é um conjunto de regras que garantem que a informação não seja lida, ou modificada por quem não tem permissão. A segurança é usada especificamente para referência do problema genérico do assunto, já os mecanismos de protecção são utilizados para salvar as informações a serem protegidas. A segurança é analisada de várias formas, sendo os principais problemas causados com a falta dela a perda de dados e as invasões de intrusos. A perda de dados na maioria das vezes é causada por algumas razões: factores naturais: incêndios, cheias, terramotos, e vários outros problemas de causas naturais; Erros de hardware ou de software: falhas no processamento, erros de comunicação, ou bugs em programas; Erros humanos: entrada de dados incorrecta, montagem errada de disco ou perda de um disco. Para evitar a perda destes dados é necessário manter uma cópia de segurança (backup) confiável, guardado longe destes dados originais.

Exemplos de Invasões

O maior acontecimento causado por uma invasão foi em 1988, quando um estudante colocou na Internet um programa maldoso (worm), afectando milhares de computadores pelo mundo. Sendo identificado e removido logo após. Mas até hoje há controvérsias de que ele não foi completamente removido da rede. Esse programa era feito em linguagem C, e não se sabe até hoje qual era o objectivo, o que se sabe é que ele tentava descobrir todas as senhas que o utilizador digitava. Mas esse programa auto-copiava-se em todos os computadores em que o estudante invadia. Essa "brincadeira" não durou muito, pois o estudante foi descoberto pouco tempo depois, processado e condenado a liberdade condicional, e teve que pagar uma multa alta.

Um dos casos mais recentes de invasão por meio de vírus foi o do Vírus Conficker (ou Downup, Downadup e Kido) que tinha como objectivo afectar computadores dotados do sistema operacional Microsoft Windows, e que foi primeiramente detectado em Outubro de 2008. Uma versão anterior do vírus propagou-se pela internet através de uma vulnerabilidade de um sistema de rede do Windows 2000, Windows XP, Windows Vista, Windows Server 2003, Windows Server 2008, Windows 7 Beta e do Windows Server 2008 R2 Beta, que tinha sido lançado anteriormente naquele mês. O vírus bloqueia o acesso a websites destinados à venda, protegidos com sistemas de segurança e, portanto, é possível a qualquer utilizador de internet verificar se um computador está infectado ou não, simplesmente por meio do acesso a websites destinados a venda de produtos dotados de sistemas de segurança. Em Janeiro de 2009, o número estimado de computadores infectados variou entre 9 e 15 milhões. Em 13 de Fevereiro de 2009, a Microsoft estava ofereceu 250.000 dólares americanos em recompensa para qualquer informação que levasse à condenação e à prisão de pessoas por trás da criação e/ou distribuição do Conficker. Em 15 de Outubro de 2008, a Microsoft disponibilizou um patch de emergência para corrigir a vulnerabilidade MS08-067, através da qual o vírus prevalece-se para poder espalhar-se. As aplicações da actualização automática aplicam-se somente para o Windows XP SP2, SP3, Windows 2000 SP4 e Windows Vista; o Windows XP SP1 e versões mais antigas não são mais suportados. Os softwares antivírus não-ligados a Microsoft, tais como a BitDefender, Enigma Software, Eset, F-Secure, Symantec, Sophos, e o Kaspersky Lab disponibilizaram actualizações com programas de detecção nos seus produtos e são capazes de remover o vírus. A McAfee e o AVG também são capazes de remover o vírus através de análise de discos duros e médias removíveis.

Através desses dados vemos que os anti-vírus devem estar cada vez mais actualizados, estão sempre a surgir novos vírus rapidamente, e com a mesma velocidade deve ser lançado actualizações para as base de dados dos anti-vírus para que os mesmos sejam identificados e excluídos. Com a criação da internet essa propagação de vírus é muito rápida e muito perigosa, pois se não houver a actualização

dos anti-virus o computador e utilizador ficam vulneráveis, pois com a criação da Internet várias empresas começaram a utilizar Internet, como exemplo dessas empresas temos os bancos, mas como é muito vulnerável esse sistema, pois existem vírus que tem a capacidade de ler o teclado (in/out), instruções privilegiadas como os keyloggers. Com esses vírus é possível ler a senha do utilizador que acede a sua conta no banco, com isso é mais indicado ir directamente ao banco e não aceder a sua conta pela Internet quando pretenderes realizar transacções.

Nível de segurança

Depois de identificado o potencial de ataque, as organizações têm que decidir o nível de segurança a estabelecer para uma rede ou sistema os recursos físicos e lógicos a necessitar de protecção. No nível de segurança devem ser quantificados os custos associados aos ataques e os associados à implementação de mecanismos de protecção para minimizar a probabilidade de ocorrência de um ataque.

Segurança física

Considera as ameaças físicas como incêndios, desabamentos, relâmpagos, cheias, acesso indevido de pessoas, forma inadequada de tratamento e manuseio do material.

Segurança lógica

Atenta contra ameaças ocasionadas por vírus, acessos remotos à rede, *backup* desactualizados, violação de senhas, etc.

Segurança lógica é a forma como um sistema é protegido no nível de sistema operacional e de aplicação. Normalmente é considerada como protecção contra ataques, mas também significa protecção de sistemas contra erros não intencionais, como remoção acidental de importantes ficheiros do sistema ou aplicação.

Políticas de segurança

De acordo com o RFC 2196 (http://tools.ietf.org/html/rfc2196 *The Site Security Handbook*), uma política de segurança consiste num conjunto formal de regras que devem ser seguidas pelos utilizadores dos recursos de uma organização.

As políticas de segurança devem ter implementação realista, e definir claramente as áreas de responsabilidade dos utilizadores, do pessoal de gestão de sistemas e redes e da direcção. Deve também adaptar-se a alterações na organização. As políticas de segurança fornecem um enquadramento para a implementação de mecanismos de segurança, definem procedimentos de segurança adequados, processos de auditoria à segurança e estabelecem uma base para procedimentos legais na sequência de ataques.

O documento que define a política de segurança deve excluir todos os aspectos técnicos de implementação dos mecanismos de segurança, pois essa implementação pode variar ao longo do tempo. Deve ser também um documento de fácil leitura e compreensão, além de resumido.

Algumas normas definem aspectos que devem ser levados em consideração ao elaborar políticas de segurança. Entre essas normas estão a BS 7799 (elaborada pela British Standards Institution). A ISO começou a publicar a série de normas 27000, em substituição à ISO 17799 (e por conseguinte à BS 7799), das quais a primeira, ISO 27001, foi publicada em 2005.

Existem duas filosofias por trás de qualquer política de segurança: a proibitiva (tudo que não é expressamente permitido é proibido) e a permissiva (tudo que não é proibido é permitido).

Os elementos da política de segurança devem ser considerados:

- A Disponibilidade: o sistema deve estar disponível de forma que quando o utilizador necessitar, possa usar. Dados críticos devem estar disponíveis ininterruptamente.
- A Utilização: o sistema deve ser utilizado apenas para os determinados objectivos.
- A Integridade: o sistema deve estar sempre íntegro e em condições de ser usado.
- A Autenticidade: o sistema deve ter condições de verificar a identidade dos utilizadors, e este ter condições de analisar a identidade do sistema.
- A Confidencialidade: dados privados devem ser apresentados somente aos donos dos dados ou ao grupo por ele autorizado.

Senhas

Uma senha ou password na Internet, ou em qualquer sistema computacional, serve para autenticar o utilizador, ou seja, a senha garante que determinado indivíduo que utiliza um serviço é ele mesmo. Se você fornecer a sua senha para uma outra pessoa, esta poderá utilizar a senha para se passar por você na Internet e, dependendo do caso, o estrago poderá ser grande. Portanto, a senha merece consideração especial, afinal, ela é de sua inteira responsabilidade.

Políticas de Senhas

Dentre as políticas utilizadas pelas grandes corporações a composição da senha ou password é a mais controversa. Por um lado profissionais com dificuldade de memorizar varias senhas de acesso, por outros funcionários displicentes que anotam a senha sob o teclado no fundo das gavetas, em casos mais graves o colaborador anota a senha no monitor do computador.

Recomenda-se a adopção das seguintes regras para minimizar o problema, mas a regra fundamental é a consciencialização dos colaboradores quanto ao uso e manutenção das senhas.

- **Senha com data para expiração**

  Adopta-se um padrão definido onde a senha possui prazo de validade com 30 ou 45 dias, obrigando o colaborador ou utilizador a renovar a sua senha.

- **Inibir a repetição**

  Adopta-se através de regras predefinidas que uma senha uma vez utilizada não poderá ter mais que 60% dos caracteres repetidos, p. ex: senha anterior “123senha” nova senha deve ter 60% dos caracteres diferentes como “456seuse”, neste caso foram repetidos somente os caracteres “s” “e” os demais diferentes.

- **Obrigar a composição com número mínimo de caracteres numéricos e alfabéticos**

  Define-se obrigatoriedade de 4 caracteres alfabéticos e 4 caracteres numéricos, por exemplo: 1s4e3u2s ou posicionais os 4 primeiros caracteres devem ser numéricos e os 4 subsequentes alfabéticos por exemplo: 1432seus.

- **Criar um conjunto com possíveis senhas que não podem ser utilizadas**

  Monta-se uma base de dados com formatos conhecidos de senhas e proíbir o seu uso, como por exemplo o utilizador chama-se Jose da Silva, logo sua senha não deve conter partes do nome como 1221jose ou 1212silv etc, os formatos DDMMAAAA ou 19XX, 1883emc ou I2B3M4

- **Recomenda-se ainda utilizar senhas com Case Sensitive e utilização de caracteres especiais como:** @ # $ % & *

Como escolher uma boa senha?
Uma boa senha deve ter pelo menos oito caracteres (letras maiúsculas e minúsculas, números e símbolos), deve ser simples de digitar e, o mais importante, deve ser fácil de recordar. Normalmente os sistemas diferenciam letras maiúsculas das minúsculas o que já ajuda na composição da senha. Claro que o seu apelido, números de documentos, matrículas de carros, números de telefones e datas deverão estar fora da sua lista de senhas. Pois esses dados são muito fáceis de obter-se e qualquer criminoso tentaria utilizar este tipo de informação para se autenticar como você. Existem várias regras de criação de senhas que você pode utilizar, uma regra de ouro para a escolha de uma boa senha é: jamais utilize como senha palavras que façam parte de dicionários (de qualquer língua, deste ou de outros planetas).

O que fazer então? Fácil perceber, quanto mais confusa a senha melhor, pois mais difícil será descobri-la. Assim tente misturar letras maiúsculas, minúsculas, números e sinais de pontuação. Uma regra realmente prática e que gera boas senhas difíceis de serem descobertas é utilizar uma frase qualquer e pegar a primeira, segunda ou a última letra de cada palavra.

Por exemplo: usando a frase “batata quando nasce espalha-se pelo chão” podemos gerar a seguinte senha “BqnsepC”. Mas só tem 7 caracteres! Precisamos de pelo menos mais um para completar o mínimo de 8 caracteres. Assim a senha gerada fica: “!BqnespC”. Note que a senha gerada é demasiada confusa, tem 8 caracteres com letras minúsculas e maiúsculas e um sinal de pontuação colocado num lugar pouco convencional. Senhas geradas desta maneira são fáceis de lembrar e são normalmente difíceis de serem descobertas. Utilizando a última letra de cada palavra da frase da senha anterior, por exemplo, não gera uma senha muito elegante (aoeaeoo) e há repetição de caracteres.

Com que frequência devo mudar minha senha?
A regra básica é trocá-la pelo menos a cada dois ou três meses. Existem páginas nos provedores que facilitam a troca da senha, e estão lá para serem utilizadas. Trocando-a regularmente você garante a integridade da mesma. Caso não encontre o serviço de troca de senha no site do seu provedor, entre em contacto com o serviço de suporte, mas não aceite que a mudança da senha seja feita por funcionários. A alteração da senha sempre deve ser feita pelo próprio dono! Lembrando: a senha é importante e mantê-la em segredo é a sua segurança!

Devo utilizar quantas senhas diferentes?
Várias, uma para cada site de e-mail gratuito, uma para o seu provedor, uma para o banco, etc. Imagine os danos que uma pessoa pode fazer se descobrir uma das suas senhas, e se esta senha que

você usa for igual para todos os sites e serviços que você utiliza, com certeza o estrago vai ser muito maior. Não se esqueça das senhas de partilha na rede, pastas e impressoras, elas também são importantes e devem seguir as mesmas regras. Lembre-se, a partilha deve durar somente o tempo necessário.

Problemas usuais de segurança

Engenharia Social

Em Segurança da informação, chama-se **Engenharia Social** as práticas utilizadas para obter acesso a informações importantes ou sigilosas em organizações ou sistemas por meio do engano ou exploração da confiança das pessoas. Para isso, o burlão pode passar-se por outra pessoa, assumir outra personalidade, fingir que é um profissional de determinada área, etc. É uma forma de entrar em organizações que não necessita da força bruta ou de erros em máquinas. Explora as falhas de segurança das próprias pessoas que, quando não treinadas para esses ataques, podem ser facilmente manipuladas.

O termo é utilizado para os métodos de obtenção de informações importantes do utilizador, através da sua ingenuidade ou da confiança. Quem está mal intencionado geralmente utiliza telefone, e-mails ou salas de chat para obter as informações que necessita.

Por exemplo: Algum desconhecido liga para a sua casa e se diz do suporte técnico do seu provedor. Nesta ligação ele te convence de que a sua conexão com a Internet está problemática e pede a sua senha para corrigir o problema.

Como sempre, o bom senso nestes casos é tudo. Duvide desse tipo de abordagem e contacte o provedor/administrador de rede caso algum técnico ligue para sua casa pedindo dados confidenciais a seu respeito (senhas, nome do computador, rede, número de IP, números de cartões etc.) avisando-o do ocorrido.

Outro caso típico são sites desconhecidos que prometem horas grátis no seu provedor caso você passe o seu nome de utilizador e a sua senha para eles. É claro que eles utilizarão estes dados para conseguir horas grátis, não para você mas para eles.

Compreendendo a Engenharia Social

Engenharia social compreende a inaptidão dos indivíduos manterem-se actualizados com diversas questões pertinentes a tecnologia da informação, além de não estarem conscientes do valor da informação que eles possuem e, portanto, não terem preocupação em proteger essa informação conscientemente. É importante salientar que, a engenharia social é aplicada em diversos sectores da segurança da informação independente de sistemas computacionais, software e ou plataforma utilizada, o elemento mais vulnerável de qualquer sistema de segurança da informação é o **ser humano**, o qual possui traços comportamentais e psicológicos que o torna susceptível a ataques de engenharia social. Dentre essas características, pode-se destacar:

- **Vaidade pessoal e/ou profissional:** O ser humano costuma a ser mais receptivo a avaliação positiva e favorável aos seus objectivos, aceitando basicamente argumentos favoráveis a sua avaliação pessoal ou profissional ligada directamente ao benefício próprio ou colectivo de forma demonstrativa.

- **Autoconfiança:** O ser humano procura transmitir em diálogos individuais ou colectivos o acto de fazer algo bem, colectivamente ou individualmente, procurando transmitir segurança, conhecimento, saber e eficiência, de formas a criar uma estrutura base para o início de uma comunicação ou acção favorável a uma organização ou indivíduo.

- **Formação profissional:** O ser humano procura valorizar a sua formação e suas habilidades adquiridas nesta faculdade, procurando o controlo numa comunicação, execução ou apresentação seja ela profissional ou pessoal procurando o reconhecimento pessoal inconscientemente em primeiro plano.

- **Vontade de ser útil :** O ser humano, comummente, procura agir com cortesia, bem como ajudar os outros quando necessário.

- **Procura por novas amizades :** O ser humano costuma a agradar-se e a sentir-se bem quando elogiado, ficando mais vulnerável e aberto a dar informações.

- **Propagação de responsabilidade :** Trata-se da situação na qual o ser humano considera que ele não é o único responsável por um conjunto de actividades.

- **Persuasão :** Compreende quase uma arte a capacidade de persuadir pessoas, onde se procura obter respostas específicas. Isto é possível porque as pessoas possuem características comportamentais que as tornam vulneráveis a manipulação.

A engenharia social não é exclusivamente utilizada em informática, a engenharia social é uma ferramenta onde exploram-se falhas humanas em organizações físicas ou jurídicas onde operadores do sistema de segurança da informação possuem poder de decisão parcial ou total ao sistema de segurança da informação seja ele físico ou virtual, porém devemos considerar que as informações pessoais, não documentadas, conhecimentos, saber, não são informações físicas ou virtuais, elas fazem parte de um sistema em que possuem características comportamentais e psicológicas na qual a engenharia social passa a ser auxiliada por outras técnicas como: leitura fria, linguagem corporal, leitura quente, termos usados no auxílio da engenharia social para obter informações que não são físicas ou virtuais mas sim comportamentais e psicológicas.

A engenharia social é praticada em diversas profissões beneficamente ou não, visando proteger um sistema da segurança da informação ou atacar um sistema da segurança da informação.

Um engenheiro social não é um profissional na engenharia social (a engenharia social não é uma faculdade e sim técnicas), mas trata-se de uma pessoa que possui conhecimentos em diversas áreas profundamente ou não, 99% das pessoas que praticam a engenharia social, de forma benéfica ou não, trabalham em grandes empresas ou em empresas de médio porte, visando procurar falhas num sistema de segurança da informação para aperfeiçoar ou explorar falhas.

A engenharia social muito confundida com a arte de enganar em termos técnicos por estar relacionada em casos de violação da segurança da informação virtualmente e fisicamente, porém devemos lembrar que a engenharia social é utilizada para a protecção da informação também, estes casos são frequentes e não são divulgados por motivos de segurança da informação de uma pessoa jurídica ou pessoa física, uma falha descoberta por uma pessoa com habilidades na engenharia social ela pode ser explorada de duas formas, beneficamente ou maleficamente, a sua actuação como pessoa com habilidades na engenharia social contratado para solucionar falhas e não amplia-las, está é a forma benéfica de usar a engenharia social, a forma maléfica de utilizar a engenharia social está ligada a 99% dos casos por pessoas que procuram violar, obter a informação de forma desonesta, procurando o lucro pessoais ou empresariais, lembramos que a engenharia social não é

uma faculdade e sim uma habilidade pessoal de um profissional ou não numa determinada área, profissão, dedicação, hobby, entre outros.

A engenharia social é utilizada no dia-a-dia de pessoas comuns ou não de forma involuntária, o que difere o uso involuntário da engenharia social do julgamento prévio ou dedução é a vaidade pessoal ligada ao objectivo pessoal que induz a engenharia social involuntária, frequentes em lugares comuns como:

Exemplos de locais:

- **Feiras livres:** A engenharia social involuntária é frequente nas feiras livres em desconfiamos da qualidade, da validade, do preço, usamos a engelharia social involuntária para obtermos informações que nos favoreça directamente, esta forma de praticar a engenharia social involuntária é avaliada como traço comportamental.

- **Bares:** A engenharia social involuntária é frequente em bares, procurando informações que possam nos favorecer, na sua grande maioria esta prática está ligada à conquista, romantismo, de uma forma geral visando a conquista afectiva ou amorosa de uma segunda pessoa seja organizadamente ou não.

A engenharia social lida com varias formas e técnicas em situações diversas, pessoas com habilidades na engenharia social que actuam nesta área por muitos anos definem a engenharia social como uma das ferramentas mais utilizadas no mundo em comunicação humana, visando proteger a informação ou não, divulgar a informação ou não, uma arma ou uma flor nas suas mãos com uma imagem desfocada ou focada, porém muito perigosa ao coração.

Técnicas

A maioria das técnicas de engenharia social consiste em obter informações privilegiadas enganando os utilizadores de um determinado sistema através de identificações falsas, aquisição de carisma e confiança da vítima. Um ataque de engenharia social pode dar-se através de qualquer meio de comunicação. Tendo-se destaque para telefonemas, conversas directas com a vítima, e-mail e WWW. Algumas dessas técnicas são:

- **Vírus que se espalham por e-mail**

Criadores de vírus geralmente usam e-mail para propagar as suas criações. Na maioria dos casos, é necessário que o utilizador ao receber o e-mail execute o ficheiro em anexo para que o seu computador seja contaminado. O criador do vírus pensa então numa maneira de fazer com que o utilizador clique no anexo. Um dos métodos mais utilizados é colocar um texto que desperte a curiosidade do utilizador. O texto pode tratar de sexo, de amor, de notícias actuais ou até mesmo de um assunto particular do internauta. Um dos exemplos mais clássicos é o vírus I Love You, que chegava ao e-mail das pessoas utilizando este mesmo nome. Ao receber a mensagem, muitos pensavam que tinham um(a) admirador(a) secreto(a) e na expectativa de descobrir quem era, clicavam no anexo e contaminam o computador. Repare que neste caso, o autor explorou um assunto que desperta qualquer pessoa. Alguns vírus possuem a característica de se espalhar muito facilmente e por isso recebem o nome de worms. Aqui, a engenharia social também pode ser aplicada. Imagine, por exemplo, que um worm se espalha por e-mail usando como tema cartões virtuais de amizade. O internauta que acreditar na mensagem vai contaminar o seu computador e o worm, para se propagar, envia cópias da mesma mensagem para a lista de contactos da vítima e coloca o endereço de e-mail dela como remetente. Quando alguém da lista receber a mensagem, vai

pensar que foi um conhecido que enviou aquele e-mail e como o assunto é amizade, pode acreditar que está mesmo a receber um cartão virtual do seu amigo. A táctica de engenharia social para este caso, explora um assunto que diz repeito a qualquer pessoa: a amizade.

- **E-mails falsos (spam)**

Este é um dos tipos de ataque de engenharia social mais comuns e é usado principalmente para obter informações financeiras da pessoa, como número de conta bancárias e senha. Neste caso, o aspecto explorado é a confiança. A maior parte dos criadores desses e-mails são criminosos que desejam roubar o dinheiro presente em contas bancárias. Porém, os sistemas dos bancos são muito bem protegidos e quase que invioláveis! Como é inviável tentar burlar a seguranças dos sistemas bancários, é mais fácil ao criminoso tentar enganar as pessoas para que elas forneçam as suas informações bancárias. A táctica utilizada é a seguinte: o criminoso adquire uma lista de e-mails utilizados para SPAM que contém milhões de endereços, depois vai a um site de um banco muito conhecido, copia o layout da página e o salva num site provisório, que tem a url semelhante ao site do banco. Por exemplo, imagine que o nome do banco seja 'Banco Dinheiro' e o site seja www.bancodinheiro.com. O criminoso cria um site semelhante: 'www.bancodinhero.com' ou 'www.bancodinheiro.co.ao' ou 'www.bancodinheiro.org', enfim. Neste site, ele faz uma cópia **idêntica** a do banco e disponibiliza campos específicos para o utilizador digitar os seus dados confidenciais. O passo seguinte é enviar um e-mail à lista adquirida usando um layout semelhante ao do site. Esse e-mail é acompanhado por um link que leva ao site falso. Para fazer com que o internauta clique no link, o texto da mensagem pode, por exemplo, sugerir um prémio: "Você acaba de ser premiado com 10 mil dólares. Clique no link para actualizar o seu registo e receber o prémio".

Como a instituição bancária escolhida geralmente é muito conhecida, as hipóteses de que o internauta que recebeu o e-mail seja cliente do banco são grandes. Assim, ele pode pensar que de facto foi o banco que enviou aquela mensagem, afinal, o e-mail e o site do link tem o layout da instituição. Como consequência, a vítima ingenuamente digita os seus dados e dias depois percebe que todo o dinheiro da sua conta desapareceu! Repare que em casos assim, o burlador usa a imagem de confiabilidade que o banco tem para enganar as pessoas. Mensagens falsas que dizem que o internauta recebeu um cartão virtual ou ganhou um prémio de uma empresa grande são comuns. Independente do assunto tratado em e-mails desse tipo, todos tentam convencer o internauta a clicar num link ou no anexo. A forma utilizada para convencer o utilizador a fazer isso é uma táctica de engenharia social.

Cavalos de Tróia (Trojan Horses)

Conta a mitologia grega, que há muito tempo atrás, houve uma guerra entre as cidades de Atenas e de Tróia. Como Tróia era extremamente fortificada, os militares gregos a consideravam invencível. Para dominá-la os gregos construíram uma enorme estátua de madeira na forma de um cavalo e deram de presente para os troianos que a aceitaram de bom grado. O problema é que o cavalo foi preenchido com centenas de soldados que, durante a noite, abriram os portões da cidade possibilitando a entrada dos soldados gregos e a dominação de Tróia. Daí surgiram os termos Presente de Grego e Cavalo de Tróia.

Em tempos modernos o cavalo virou um programa e a cidade o seu computador. Conhecidos como Cavalos de Tróia ou Trojan Horses estes programas são construídos de tal maneira que, uma vez instalados nos computadores, abrem portas no seu computador, tornando possível o roubo de informações (ficheiros, senhas etc.).

Como o meu computador pode ser infectado por um Cavalo de Tróia?
Normalmente você receberá o Cavalo de Tróia como presente (de grego). Ele pode ser dado de várias maneiras, mas na maioria das vezes ele vem anexado a algum e-mail. Estes e-mails vêm acompanhados de mensagens bonitas que prometem mil maravilhas se o ficheiro anexado for aberto. Não se deixe enganar. A melhor política é nunca abrir um ficheiro anexado, principalmente se o remetente for desconhecido.

Programas piratas, adquiridos pela rede, poderão conter Cavalos de Tróia, assim, evite a instalação de programas de procedência desconhecida ou duvidosa

O que um Cavalo de Tróia pode fazer no meu computador?
O Cavalo de Tróia, na maioria das vezes, vai possibilitar aos hackers o controlo total da sua máquina. Ele poderá ver e copiar todos os seus ficheiros, descobrir todas as senhas que você digitar, formatar o seu disco duro, ver o seu ecrã e até mesmo ouvir a sua voz se o computador tiver um microfone instalado. Este processo é chamado de **invasão**.

O hacker poderá me invadir se o computador não estiver conectado à Internet?
Não, o Cavalo de Tróia somente poderá ser utilizado se o computador estiver conectado à Internet. Os hackers somente invadem computadores quando eles estão conectados.

O computador pode ser infectado por um Cavalo de Tróia sem que se perceba?
Sim, com certeza! Essa é a ideia do Cavalo de Tróia, entrar em silêncio para que você não perceba e quando você descobrir ser tarde demais.

Como posso saber se o computador está infectado?
Os programas anti-vírus normalmente detectam os programas Cavalos de Tróia e tratam de eliminá-los como se fossem Vírus. As actualizações dos Anti-Vírus possibilitam a detecção dos Cavalos de Tróia mais recentes.

Como proteger o computador dos Cavalos de Tróia?
A maioria dos bons programas de anti-vírus são capazes de detectar e eliminar estes programas. Mesmo assim a protecção é parcial, uma vez que os Cavalos de Tróia mais novos poderão passar despercebidos. O ideal é nunca abrir documentos anexados aos e-mails, vindos de desconhecidos. Existem ainda programas de Firewall pessoais que podem ser utilizados para bloquear as conexões dos hackers com os Cavalos de Tróia que possam estar instalados no seu computador. Tais programas não eliminam os Cavalos de Tróia, mas bloqueiam o seu funcionamento.

Backdoors

Existe uma confusão entre o que é um Backdoor e um Cavalo de Tróia, principalmente porque o estrago provocado por ambos é semelhante. Para deixar claro, um Cavalo de Tróia é um programa que cria deliberadamente um Backdoor no seu computador. Programas que usam a Internet e que são de uso comum, como Browsers (navegadores web), programas de e-mail, ICQ ou IRC podem possuir Backdoors.

Os Backdoors são abertos devido a defeitos de fabricação ou falhas no projecto dos programas, isto pode acontecer tanto acidentalmente ou ser introduzido ao programa propositadamente. Como exemplo: versões antigas do ICQ possuem defeito que abre um Backdoor que permite ao hacker deixar cair a conexão do programa com o servidor, fazendo que ele pare de funcionar.

Como se prevenir dos Backdoors?
A maneira mais correcta é sempre actualizar as versões dos programas instalados no seu computador. É de responsabilidade do fabricante do software avisar aos utilizadors e prover uma nova versão corrigida do programa quando é descoberto um Backdoor no mesmo.

A dica é sempre visitar os sites dos fabricantes de software e verificar a existência de novas versões do software ou de pacotes que eliminem os Backdoors (esses pacotes de correcção são conhecidos como patches ou service packs.).

Os programas Anti-Vírus não são capazes de descobrir Backdoors, somente a actualização dos programas é que podem eliminar em definitivo este problema. Programas de Firewall pessoais, no entanto, podem ser úteis para amenizar (mas não eliminar) este tipo de problema.

Vírus

Vírus é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e tornando-se parte de outros programas e ficheiros de um computador. O vírus **depende** da execução do programa ou ficheiro hospedeiro para que possa se tornar activo e dar continuidade ao processo de infecção.

Entende-se por computador qualquer dispositivo computacional passível de infecção por vírus. Computadores domésticos, *notebooks*, telefones celulares e PDAs são exemplos de dispositivos computacionais passíveis de infecção.

Como um vírus pode afectar um computador?

Normalmente o vírus tem controlo total sobre o computador, podendo fazer de tudo, desde mostrar uma mensagem de "feliz aniversário", até alterar ou destruir programas e ficheiros do disco.

Como o computador é infectado por um vírus?

Para que um computador seja infectado por um vírus, é preciso que um programa previamente infectado seja executado. Isto pode ocorrer de diversas maneiras, tais como:

- abrir ficheiros anexados aos *e-mails*;
- abrir ficheiros do Word, Excel, etc;
- abrir ficheiros armazenados noutros computadores, através da partilha de recursos;
- instalar programas de procedência duvidosa ou desconhecida, obtidos pela Internet, de disquetes, *pen drives*, CDs, DVDs, etc;
- ter alguma media removível (infectada) conectada ou inserida no computador, quando ele é ligado.

Novas formas de infecção por vírus podem surgir. Portanto, é importante manter-se informado através de jornais, revistas e dos *sites* dos fabricantes de antivírus.

Um computador pode ser infectado por um vírus sem que se perceba?

Sim. Existem vírus que procuram permanecer ocultos, infectando ficheiros do disco e executando uma série de actividades sem o conhecimento do utilizador. Ainda existem outros tipos que permanecem inactivos durante certos períodos, entrando em actividade em datas específicas.

O que é um vírus propagado por *e-mail*?

Um vírus propagado por *e-mail* (*e-mail borne virus*) normalmente é recebido como um ficheiro anexado à uma mensagem de correio electrónico. O conteúdo dessa mensagem procura induzir o utilizador a clicar sobre o ficheiro anexado, fazendo com que o vírus seja executado. Quando este tipo de vírus entra em acção, ele infecta ficheiros e programas e envia cópias de si mesmo para os contactos encontrados nas listas de endereços de *e-mail* armazenadas no computador do utilizador.

É importante ressaltar que este tipo específico de vírus não é capaz de se propagar automaticamente. O utilizador precisa executar o ficheiro anexado que contém o vírus, ou o programa leitor de *e-mails* precisa estar configurado para auto-executar ficheiros anexados.

O que é um vírus de macro?

Uma macro é um conjunto de comandos que são armazenados em alguns aplicactivos e utilizados para automatizar algumas tarefas redundantes. Um exemplo seria, num editor de textos, definir uma macro que contenha a sequência de passos necessários para imprimir um documento com a orientação de retrato e utilizando a escala de cores em tons cinzentos.

Um vírus de macro é escrito de forma a explorar esta facilidade de automatização e é parte de um ficheiro que normalmente é manipulado por algum aplicactivo que utiliza macros. Para que o vírus possa ser executado, o ficheiro que o contém precisa ser aberto e, a partir daí, o vírus pode executar uma série de comandos automaticamente e infectar outros ficheiros no computador.

Existem alguns aplicativos que possuem ficheiros base (modelos) que são abertos sempre que o aplicativo é executado. Caso este ficheiro base seja infectado pelo vírus de macro, toda vez que o aplicativo for executado, o vírus também será.

Ficheiros nos formatos gerados por programas da Microsoft, como o Word, Excel, Powerpoint e Access, são os mais susceptíveis a este tipo de vírus. Ficheiros nos formatos RTF, PDF e *PostScript* são menos susceptíveis, mas isso não significa que não possam conter vírus.

Como posso saber se um computador está infectado?

A melhor maneira de descobrir se um computador está infectado é através dos programas antivírus.

É importante ressaltar que o antivírus e suas assinaturas devem estar **sempre actualizados**, caso contrário poderá **não** detectar os vírus mais recentes.

Existe alguma maneira de proteger um computador de vírus?

Sim. Algumas das medidas de prevenção contra a infecção por vírus são:

- instalar e manter actualizados um bom programa antivírus e suas assinaturas;

- desabilitar no seu programa leitor de *e-mails* a auto-execução de ficheiros anexados às mensagens;
- não executar ou abrir ficheiros recebidos por *e-mail* ou por outras fontes, mesmo que venham de pessoas conhecidas. Caso seja necessário abrir o ficheiro, certifique-se que ele foi verificado pelo programa antivírus;
- procurar utilizar na elaboração de documentos formatos menos susceptíveis à propagação de vírus, tais como RTF, PDF ou *PostScript*;
- procurar não utilizar, no caso de ficheiros comprimidos, o formato executável. Utilize o próprio formato compactado, como por exemplo Zip ou Gzip.

O que é um vírus de telefone celular?

Um vírus de celular se propaga de telefone para telefone através da tecnologia *bluetooth* ou da tecnologia MMS (*Multimedia Message Service*). A infecção dá-se da seguinte forma:

1. O utilizador recebe uma mensagem que diz que o seu telefone está prestes a receber um ficheiro.
2. O utilizador permite que o ficheiro infectado seja recebido, instalado e executado no seu aparelho.
3. O vírus, então, continua o processo de propagação para outros telefones, através de uma das tecnologias mencionadas anteriormente.

Os vírus de celular diferem-se dos vírus tradicionais, pois normalmente não inserem cópias de si mesmos em outros ficheiros armazenados no telefone móvel, mas podem ser especificamente projectados para sobrescrever ficheiros de aplicativos ou do sistema operacional instalado no aparelho.

Depois de infectar um telefone móvel, o vírus pode realizar diversas actividades, tais como: destruir/sobrescrever ficheiros, remover contactos da agenda, efectuar ligações telefônicas, acabar a carga da bateria, além de tentar propagar-se para outros telefones.

Como posso proteger um telemóvel de vírus?

Algumas das medidas de prevenção contra a infecção por vírus em telemóveis são:

- mantenha o *bluetooth* do seu aparelho desabilitado e somente habilite-o quando for necessário. Caso isto não seja possível, consulte o manual do seu aparelho e configure-o para que não seja identificado (ou "descoberto") por outros aparelhos (em muitos aparelhos esta opção aparece como "Oculto" ou "Invisível");
- não permita a recepção de ficheiros enviados por terceiros, mesmo que venham de pessoas conhecidas, salvo quando você estiver a espera de receber um ficheiro específico;
- fique atento às notícias veiculadas no *site* do fabricante do seu aparelho, principalmente àquelas sobre segurança;
- aplique todas as correcções de segurança (*patches*) que forem disponibilizadas pelo fabricante do seu aparelho, para evitar que possua vulnerabilidades;
- caso você tenha comprado uma aparelho usado, restaure as opções de fábrica (em muitos aparelhos esta opção aparece como "Restaurar Configuração de Fábrica" ou "Restaurar Configuração Original") e configure-o como descrito no primeiro item, antes de inserir quaisquer dados.

Os fabricantes de antivírus têm disponibilizado versões para diversos modelos de telemóveis. Caso você opte por instalar um antivírus no seu telefone, consulte o fabricante e verifique a viabilidade e disponibilidade de instalação para o modelo do seu aparelho. Lembre-se de manter o antivírus sempre actualizado.

Spyware e Adware

Spyware

Spyware consiste num programa automático de computador, que recolhe informações sobre o utilizador, sobre os seus costumes na Internet e transmite essa informação a uma entidade externa na Internet, sem o seu conhecimento nem o seu consentimento.

Diferem dos cavalos de Tróia por não terem como objectivo que o sistema do utilizador seja dominado, seja manipulado, por uma entidade externa, por um cracker.

Os spywares podem ser desenvolvidos por empresas comerciais, que desejam monitorar o hábito dos utilizadores para avaliar os seus costumes e vender estes dados pela internet. Desta forma, estas empresas costumam a produzir inúmeras variantes dos seus programas-espiões, aperfeiçoando-o, dificultando em muito a sua remoção.

Por outro lado, muitos vírus transportam spywares, que visam roubar certos **dados confidenciais** dos utilizadores. Roubam dados bancários, montam e enviam registos das actividades do utilizador, roubam determinados ficheiros ou outros documentos pessoais.

Com frequência, os spywares costumavam a vir legalmente embutidos em algum programa que fosse shareware ou freeware. A sua remoção era por vezes, feita a quando da compra do software ou de uma versão mais completa e paga.

Numa tradução ao pé da letra, Spyware significa "aplicativo ou programa espião".

Adwares

Muitas vezes usa-se de forma genérica o termo spyware para os malware e adwares, que são programas indesejáveis. Costuma-se incluir os **adwares** no estudo dos spywares, pois assemelham-se na sua forma de infecção e na sua forma de desinstalação. Seriam como se fossem um sub-grupo dos spywares.

Os adwares são conhecidos por trazerem para o ecrã do utilizador algum tipo de **propaganda**.

Como geralmente são **empresas comerciais** que os desenvolvem, é comuns os adwares virem embutidos em diversos programas de livre download (freeware), com a autorização dos seus autores.

O Kazaa oficial é um programa de partilha de ficheiros, sendo um exemplo do casamento de um software gratuito com adwares, pois estes lhe proporcionam uma fonte de renda.

Inicialmente os adwares procuravam exibir propagandas em janelas, chamadas de banners, pequenas janelas de propagandas, embutidas em softwares de terceiros. Caso o utilizador gostasse deste software, poderia adquirir uma versão mais avançada, paga, livre destas propagandas.

Posteriormente os adwares passaram a monitorar a actividade do utilizador na internet, podendo desta forma mostrar propagandas personalizadas, além de enviar dados sobre hábitos do utilizador a certos sites, tendo então funções de spyware e adware, de forma simultânea.

Mais adiante certos adwares passaram a exibir janela do tipo pop-up, pequena janela de propaganda solta pelo ecrã, em vez de banners.

Um pouco mais a frente os adwares passaram a instalar-se no navegador do utilizador, acrescentando certas funcionalidades duvidosas, principalmente no **Internet Explorer**. Avanços (ou upgrades) no Internet Explorer, passaram a exigir o consentimento do utilizador para a sua instalação.

Porém com o passar do tempo, os adwares sofisticaram-se, incluindo propagandas persistentes, com inúmeras variantes, onde a sua desinstalação passou a ser um tarefa bastante penosa ou mesmo impossível, sem uma ajuda externa. A insistência no aparecimento das propagandas e sua difícil desinstalação, levaram os utilizadores a classificá-los como pragas ou spywares e não mais como simples adwares.

Certos adwares passaram a ser instalados no Internet Explorer, quando o utilizador navegava em sites maliciosos.

Os adwares se sofisticaram, tornaram-se pragas. Produzem alterações no registo do Windows e depois somem ou se escondem para garantir que as alterações não sejam desfeitas, exigindo então não mais a acção de um antivírus ou de um simples anti-spyware, mas sim de um programa específico que repara o registo.

Por vezes os adwares exibem propagandas pornográficas, falsas propagandas de infecção do sistema por vírus, falsa propaganda de venda de produtos e passaram também a causar instabilidade no sistema, principalmente no navegador.

Suspeita-se que possam tornar o sistema do utilizador aberto a acção de hackers, devido a falta de maiores cuidados na elaboração dos adwares.

Ransomware

Os **Ransomwares** são softwares maliciosos que, ao infectarem um computador, criptografam todo ou parte do conteúdo do disco duro. Os responsáveis pelo software exigem da vítima, um pagamento pelo "resgate" dos dados. Ransonwares são ferramentas para crimes de extorsão e são extremamente ilegais. O PC Cyborg Trojan, foi o primeiro código de um ransomware conhecido. Nomes de alguns Ransomwares conhecidos: **Gpcode-B** e **PGPCoder.**

Contaminação

Eventualmente anexos de e-mails ou mensagens vindas de mensageiros como o MSN e o ICQ, também podem conter spywares. Empresas comerciais exploram maldosamente a curiosidade dos utilizadores e desenvolvem novas formas de transmissão e de instalação de spywares.

Recentemente uma grande parte dos spywares são assimilados pelo navegador, como plug-ins. O utilizador deve ser cuidadoso ao instalar os diversos plug-ins disponíveis na internet.

Prevenção e Remoção

Os softwares anti-espião, também denominados antispywares, são feitos para removê-los.

Antes de mais nada, verifique se a "praga" adicionou uma entrada em **Adicionar ou remover programas**, o que facilita a sua desinstalação. Certas "pragas" como alguns redirecionadores do Internet Explorer, disponibilizam ferramentas de remoção, no item suporte ou help na página redireccionada.

Actualmente recomenda-se a instalação de algum programa **anti-espião** (ou **antispyware** em inglês), pois como já foi comentado, certos softwares trazem consigo spywares ou adwares, ou mesmo o Internet Explorer pode ser contaminado por algum spywares, pois ainda não há certeza absoluta que ele possa ficar imune, das variadas formas de adwares desenvolvidos por empresas comerciais.

Backdoors

Normalmente um atacante procura garantir uma forma de retornar a um computador comprometido, sem precisar recorrer aos métodos utilizados na realização da invasão. Na maioria dos casos, também é intenção do atacante poder retornar ao computador comprometido sem ser notado.

A esses programas que permitem o retorno de um invasor a um computador comprometido, utilizando serviços criados ou modificados para este fim, dá-se o nome de *backdoor*.

Como é feita a inclusão de um *backdoor* em um computador?

A forma usual de inclusão de um *backdoor* consiste na disponibilização de um novo serviço ou substituição de um determinado serviço por uma versão alterada, normalmente possuindo recursos que permitam acesso remoto (através da Internet). Pode ser incluído por um invasor ou através de um cavalo de tróia.

Uma outra forma é a instalação de pacotes de *software*, tais como o *BackOrifice* e *NetBus*, da plataforma Windows, utilizados para administração remota. Se mal configurados ou utilizados sem o consentimento do utilizador, podem ser classificados como *backdoors*.

A existência de um *backdoor* depende necessariamente de uma invasão?

Não. Alguns dos casos onde a existência de um *backdoor* não está associada a uma invasão são:

- instalação através de um cavalo de tróia.
- inclusão como consequência da instalação e má configuração de um programa de administração remota;

Alguns fabricantes incluem/incluíam *backdoors* nos seus produtos (*softwares*, sistemas operacionais), alegando necessidades administrativas. É importante ressaltar que estes casos constituem uma séria ameaça à segurança de um computador que contenha um destes produtos instalados, mesmo que *backdoors* sejam incluídos por fabricantes conhecidos.

Backdoors são restritos a um sistema operacional específico?

Não. *Backdoors* podem ser incluídos em computadores executando diversos sistemas operacionais, tais como Windows (por exemplo, 95/98, NT, 2000, XP, 2003, Vista, 2008 ou Seven), Unix (por exemplo, Linux, Solaris, FreeBSD, OpenBSD, AIX), Mac OS, entre outros.

Existe alguma forma de proteger um computador de *backdoors*?

Embora os programas antivírus não sejam capazes de descobrir *backdoors* num computador, as medidas preventivas contra a infecção por vírus (secção sobre vírus) são válidas para se evitar algumas formas de instalação de *backdoors*.

A idéia é que você **não** execute programas de procedência duvidosa ou desconhecida, sejam eles recebidos por *e-mail*, sejam obtidos na Internet. A execução de tais programas pode resultar na instalação de um *backdoor*.

Caso você utilize algum programa de administração remota, certifique-se de que ele esteja bem configurado, de modo a evitar que seja utilizado como um *backdoor*.

Uma outra medida preventiva consiste na utilização de um *firewall* pessoal. Apesar de não eliminarem os *backdoors*, se bem configurados, podem ser úteis para amenizar o problema, pois podem bloquear as conexões entre os invasores e os *backdoors* instalados num computador.

Também é importante visitar constantemente os *sites* dos fabricantes de *softwares* e verificar a existência de novas versões ou *patches* para o sistema operacional ou *softwares* instalados no seu computador.

Existem casos onde a disponibilização de uma nova versão ou de um *patch* está associada à descoberta de uma vulnerabilidade num *software*, que permite a um atacante ter acesso remoto a um computador, de maneira similar ao acesso aos *backdoors*.

Keyloggers

Keylogger é um programa capaz de capturar e armazenar as teclas digitadas pelo utilizador no teclado de um computador.

Que informações um *keylogger* pode obter se for instalado num computador?

Um *keylogger* pode capturar e armazenar as teclas digitadas pelo utilizador. Dentre as informações capturadas podem estar o texto de um *e-mail*, dados digitados ao registar-se e outras informações sensíveis, como senhas bancárias e números de cartões de crédito.

Em muitos casos, a activação do *keylogger* é condicionada a uma acção prévia do utilizador, como por exemplo, após o acesso a um *site* específico de comércio electrónico ou *Internet Banking*. Normalmente, o *keylogger* contém mecanismos que permitem o envio automático das informações capturadas para terceiros (por exemplo, através de *e-mails*).

Diversos *sites* de instituições financeiras utilizam teclados virtuais. Neste caso eu estou protegido dos *keyloggers*?

As instituições financeiras desenvolveram os teclados virtuais para evitar que os *keyloggers* pudessem capturar informações sensíveis de utilizadores. Então, foram desenvolvidas formas mais avançadas de *keyloggers*, também conhecidas como *screenloggers*, capazes de:

- armazenar a posição do cursor e o ecrã apresentado no monitor, nos momentos em que o *mouse* é clicado, ou
- armazenar a região que circunda a posição onde o *mouse* é clicado.

Na posse destas informações um atacante pode, por exemplo, descobrir a senha de acesso ao banco utilizada por um utilizador.

Como é feita a inclusão de um *keylogger* num computador?

Normalmente, o *keylogger* vem como parte de um programa *spyware* (veja a secção spyware) ou cavalo de tróia (veja a cavalo de tróia). Desta forma, é necessário que este programa seja executado para que o *keylogger* se instale num computador. Geralmente, tais programas vêm anexados a *e-mails* ou estão disponíveis em *sites* na Internet.

Lembre-se que existem programas leitores de *e-mails* que podem estar configurados para executar automaticamente ficheiros anexados às mensagens. Neste caso, o simples facto de ler uma mensagem é suficiente para que qualquer ficheiro anexado seja executado.

Como posso proteger um computador dos *keyloggers*?

Para se evitar a instalação de um *keylogger*, as medidas são similares àquelas discutidas nas secções sobre vírus, cavalo de tróia, *worm* ou *bots.*

Worms

Worm é um programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador.

Diferente do vírus, o *worm* **não** embute cópias de si mesmo em outros programas ou ficheiros e **não** necessita ser explicitamente executado para se propagar. A sua propagação dá-se através da exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em computadores.

Como um *worm* pode afectar um computador?

Geralmente o *worm* não tem como consequência os mesmos danos gerados por um vírus, como por exemplo a infecção de programas e ficheiros ou a destruição de informações. Isto não quer dizer que não represente uma ameaça à segurança de um computador, ou que não cause qualquer tipo de dano.

Worms são notadamente responsáveis por consumir muitos recursos. Degradam sensivelmente o desempenho de redes e podem lotar o disco duro de computadores, devido à grande quantidade de

cópias de si mesmo que costumam propagar. Além disso, podem gerar grandes transtornos para aqueles que estão recebendo tais cópias.

Como posso saber se o meu computador está a ser utilizado para propagar um *worm*?

Detectar a presença de um *worm* num computador não é uma tarefa fácil. Muitas vezes os *worms* realizam uma série de actividades, incluindo a sua propagação, sem que o utilizador tenha conhecimento.

Embora alguns programas antivírus permitam detectar a presença de *worms* e até mesmo evitar que eles se propaguem, isto nem sempre é possível.

Portanto, o melhor é evitar que o seu computador seja utilizado para propagá-los.

Como posso proteger um computador de *worms*?

Além de utilizar um bom antivírus, que permita detectar e até mesmo evitar a propagação de um *worm*, é importante que o sistema operacional e os *softwares* instalados no seu computador não possuam vulnerabilidades.

Normalmente um *worm* procura explorar alguma vulnerabilidade disponível num computador, para que possa se propagar. Portanto, as medidas preventivas mais importantes são aquelas que procuram evitar a existência de vulnerabilidades.

Uma outra medida preventiva é ter instalado no seu computador um *firewall* pessoal. Se bem configurado, o *firewall* pessoal pode evitar que um *worm* explore uma possível vulnerabilidade em algum serviço disponível no seu computador ou, em alguns casos, mesmo que o *worm* já esteja instalado no seu computador, pode evitar que explore vulnerabilidades em outros computadores.

Bots e Botnets

De modo similar ao *worm*, o *bot* é um programa capaz de propagar-se automaticamente, explorando vulnerabilidades existentes ou falhas na configuração de *softwares* instalados num computador. Adicionalmente ao *worm*, dispõe de mecanismos de comunicação com o invasor, permitindo que o *bot* seja controlado remotamente.

Como o invasor se comunica com o *bot*?

Normalmente, o *bot* conecta-se a um servidor de IRC (*Internet Relay Chat*) e entra num canal (sala) determinado. Então, ele aguarda por instruções do invasor, monitorando as mensagens que estão a ser enviadas para este canal. O invasor, ao conectar-se ao mesmo servidor de IRC e entrar no mesmo canal, envia mensagens compostas por sequências especiais de caracteres, que são interpretadas pelo *bot*. Estas sequências de caracteres correspondem a instruções que devem ser executadas pelo *bot*.

O que o invasor pode fazer quando estiver no controlo de um *bot*?

Um invasor, ao comunicar-se com um *bot*, pode enviar instruções para que ele realize diversas actividades, tais como:

- desferir ataques na Internet;
- executar um ataque de recusa de serviço;
- furtar dados do computador onde está a ser executado, como por exemplo números de cartões de crédito, senhas;
- enviar *e-mails* de *phishing*;
- enviar *spam*.

O que são *botnets*?

Botnets são redes formadas por computadores infectados com *bots*. Estas redes podem ser compostas por centenas ou milhares de computadores. Um invasor que tenha controlo sobre uma *botnet* pode utilizá-la para aumentar a potência dos seus ataques, por exemplo, para enviar centenas de milhares de *e-mails* de *phishing* ou *spam*, desferir ataques de negação de serviço, etc.

Como posso saber se um *bot* foi instalado num computador?

Identificar a presença de um *bot* num computador não é uma tarefa simples. Normalmente, o *bot* é projectado para realizar as instruções passadas pelo invasor sem que o utilizador tenha conhecimento.

Embora alguns programas antivírus permitam detectar a presença de *bots*, isto nem sempre é possível. Portanto, o melhor é procurar evitar que um *bot* seja instalado no seu computador.

Como posso proteger um computador dos *bots*?

Da mesma forma que o *worm*, o *bot* é capaz de propagar-se automaticamente, através da exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados num computador.

Portanto, a melhor forma de proteger-se dos *bots* é manter o sistema operacional e os *softwares* instalados no seu computador sempre actualizados e com todas as correcções de segurança (*patches*) disponíveis aplicadas, para evitar que possuam vulnerabilidades.

A utilização de um bom antivírus, mantendo-o sempre actualizado, também é importante, pois em muitos casos permite detectar e até mesmo evitar a propagação de um *bot*. De recordar que o antivírus só será capaz de detectar *bots* conhecidos.

Outra medida preventiva consiste em utilizar um *firewall* pessoal. Normalmente, os *firewalls* pessoais não eliminam os *bots*, mas, se bem configurados, podem ser úteis para amenizar o problema, pois podem bloquear a comunicação entre o invasor e o *bot* instalado num computador.

Podem existir outras formas de propagação e instalação de *bots* num computador, como por exemplo, através da execução de ficheiros anexados a *e-mails*.

Rootkits

O que é um rootkit?

Um rootkit é um cavalo de tróia que procura se esconder de softwares de segurança e do utilizador utilizando diversas técnicas avançadas de programação.

Rootkits escondem a sua presença no sistema, escondendo as suas chaves no registo (para que você não possa vê-las) e escondendo os seus processos no Gestor de Tarefas, além de retornar sempre erros de "ficheiro inexistente" ao tentar aceder os ficheiros do trojan.

Diversos trojans utilizam essas tecnologias com o objectivo de dificultar a sua remoção e o fazem com sucesso: os rootkits mais avançados são bem difíceis de serem removidos.

Origem do nome rootkit

Os rootkits possuem esse nome por terem sido, inicialmente, "kits" de programas para a plataforma Linux/Unix para manter o acesso total ao sistema previamente comprometido, agindo como backdoor. Como "root" é o utilizador com o controlo total do computador nas plataformas Unix, originou-se o nome "rootkit" para denominar estes conjuntos de aplicativos.

Funcionamento

Os rootkits para Linux/Unix geralmente substituem os programas mais comuns, como os programas que listam ficheiros, de modo que o administrador do sistema, ao listar os ficheiros, não veja a presença dos ficheiros do trojan.

No Windows, eles 'infectam' os processos na memória, de modo que toda vez que um processo requisite alguma informação sobre os ficheiros do trojan, esta informação seja anulada antes de ser retornada ao programa, o que fará com que os softwares acreditem que estes ficheiros não estejam lá.

Um invasor, ao realizar uma invasão, pode utilizar mecanismos para esconder e assegurar a sua presença no computador comprometido. O conjunto de programas que fornece estes mecanismos é conhecido como *rootkit*.

É muito importante ficar claro que o nome *rootkit* **não** indica que as ferramentas que o compõem são usadas para obter acesso privilegiado (*root* ou *Administrator*) num computador, mas sim para mantê-lo. Isto significa que o invasor, após instalar o *rootkit*, terá acesso privilegiado ao computador previamente comprometido, sem precisar recorrer novamente aos métodos utilizados na realização da invasão, e as suas actividades serão escondidas do responsável e/ou dos utilizadores do computador.

Que funcionalidades um *rootkit* pode conter?

Um *rootkit* pode fornecer programas com as mais diversas funcionalidades. Dentre eles, podem ser citados:

- programas para esconder actividades e informações deixadas pelo invasor (normalmente presentes em todos os *rootkits*), tais como ficheiros, directórios, processos, conexões de rede, etc;

- *backdoors* (vide backdoors), para assegurar o acesso futuro do invasor ao computador comprometido (presentes na maioria dos *rootkits*);
- programas para remoção de evidências em ficheiros de *logs*;
- *sniffers*, para capturar informações na rede onde o computador está localizado, como por exemplo senhas que estejam trafegando em formato de texto, ou seja, sem qualquer método de criptografia;
- *scanners*, para mapear potenciais vulnerabilidades em outros computadores;
- outros tipos de *malware*, como cavalos de tróia, *keyloggers*, ferramentas de ataque de recusa de serviço, etc.

Como posso saber se um *rootkit* foi instalado num computador?

Existem programas capazes de detectar a presença de um grande número de *rootkits*, mas isto não quer dizer que são capazes de detectar todos os disponíveis (principalmente os mais recentes). Alguns destes programas são gratuitos e podem ser obtidos pela Internet (antes de obter um programa para a detecção de *rootkits* pela Internet, verifique a sua procedência e certifique-se que o fabricante é confiável).

Como os *rootkits* são projectados para ficarem ocultos, ou seja, não serem detectados pelo responsável ou pelos utilizadores de um computador, a sua identificação é, na maioria das vezes, uma tarefa bem difícil. Deste modo, o melhor é procurar evitar que um *rootkit* seja instalado no seu computador.

Como posso proteger um computador dos *rootkits*?

Apesar de existirem programas específicos para a detecção de *rootkits*, a melhor forma de se proteger é manter o sistema operacional e os *softwares* instalados em seu computador sempre actualizados e com todas as correcções de segurança (*patches*) disponíveis aplicadas, para evitar que possuam vulnerabilidades.

Desta forma, você pode evitar que um atacante consiga invadir o seu computador, através da exploração de alguma vulnerabilidade, e instalar um *rootkit* após o comprometimento.

O Hacker Defender é um dos rootkits mais avançados para Windows actualmente.

Programas de E-Mail

Medidas Preventivas no uso dos programas de E-Mail

Existem no entanto medidas preventivas que minimizam os problemas trazidos com os e-mails:

1. Desligue a opção de auto-execução dos programas anexados ao e-mail;

2. Desligue a opção de auto-abertura dos ficheiros anexados aos e-mails;

3. Desligue as opções de execução de programas Java e do JavaScript.

Todos estes itens evitam a propagação automática dos Vírus e Cavalos de Tróia. Alguns programas de e-mail não possuem estas opções, neste caso estas funções não estão implementadas, ou seja, o programa de e-mail não realizará estas tarefas porque não foi programado para isto.

É claro que se o utilizador desligar as opções 1 e 2, mas ainda assim abrir os ficheiros ou executar manualmente os programas que vêm anexados aos e-mails, será infectado pelo Vírus (ou Cavalo de Tróia).

Portanto, a regra de ouro é: Não abra ficheiros ou programas anexados aos e-mails enviados por desconhecidos.

Browsers

Browser ou navegador é todo e qualquer programa que procura páginas na Internet e as apresentam no ecrã. Os mais utilizados são o Netscape Navigator e o Internet Explorer.

Como um Browser pode ser perigoso?
De várias maneiras:

- Através de programas Java;
- Através de programas JavaScript;
- Através de programas ou controlos ActiveX;
- Através de downloads de programas hostis em sites não confiáveis.

Nos três primeiros casos o seu browser executa os programas sozinhos sem interferência do utilizador, no último caso você tem que descarregar o programa da Internet numa pasta e executar ou instalar o mesmo.

O que é Java?
Java é um jeito de fazer programas, desenvolvido pela empresa Sun Microsystems de modo que o programa feito possa ser utilizado em diversos tipos diferentes de computadores e aparelhos.

Na verdade quem executa os programas Java é um outro programa chamado Máquina Virtual Java. Praticamente todos os browsers possuem uma máquina virtual dessas embutidas e como não existe diferença entre uma máquina virtual de um browser para outro, basta fazer uma única versão do programa em Java.

Estes programas aparecem dentro das páginas da Internet e podem ser desde simples programas de efeitos especiais como pacotes de escritórios completos, com editor de texto, folha de cálculo etc. Claro que quanto mais complexo for o programa em Java, maior é seu tamanho e mais tempo leva para descarregá-lo da rede.

Um programa Java é seguro?
Normalmente sim. As máquinas virtuais dos browsers são isoladas do resto do computador, assim um programa Java não tem como afecta-lo directamente. Mas defeitos nestas máquinas virtuais podem fazer com que determinados programas em Java (só os hostis) possam causar algum estrago ao computador.

Como me protejo de um programa Java hostil?
Normalmente as páginas não têm muitos programas em Java ou estes não comprometem a sua visualização. Assim sendo, pode-se desligar o Java no seu browser evitando-se assim maiores dores de cabeça. Claro que se for absolutamente necessário o Java estar ligado para que as páginas de um site possam ser vistas (no caso dos sites de Home-Banking, por exemplo), basta ligá-lo novamente e entrar no site. Se você mantiver seu browser sempre actualizado não terá grandes dores de cabeça

com o Java e alguns dos anti-vírus mais actuais possuem a capacidade de detectar os programas Java hostis enquanto o browser está a descarregar pela Internet.

O que é javascript?
Lembra do Java? Agora imagine que você quer só colocar um programa na página para mudar a cor de um desenho quando a seta do rato passar por cima dele. Pensando nisso, foi criado o JavaScript. Curiosidade: o JavaScript acompanha a página, ou seja, ele está misturado com os códigos da página e pode ser visto se você pedir para o browser mostrar os códigos. Assim, para usar o mesmo programa JavaScript em outras páginas o profissional que faz as páginas tem que reescrever o programa em cada uma delas (se usasse Java, neste caso, só teria que escrever uma única vez).

Um programa javascript é seguro?
Como o JavaScript é uma versão bem enxuta do Java ele normalmente não é capaz de realizar grandes estragos em seu computador, mas valem para ele as mesmas dicas do Java.

Como me protejo de um programa javascript?
JavaScript é muito mais utilizado em páginas do que o Java, assim caso você desligue esta opção muitas páginas deixarão de funcionar. Assim, o conselho é desligar o JavaScript quando visitar uma página desconhecida e religá-lo depois, caso seja necessário

O que é activex?
Os programas (ou controlos) feitos em ActiveX funcionam de maneira similar aos programas feitos em Java, mas só podem ser rodados em máquinas com Windows. Basicamente estes programas fazem a mesma coisa que os programas Java fazem.

O activex é seguro?
Diferente dos programas Java, os programas ActiveX podem fazer de tudo no seu computador, desde enviar um ficheiro qualquer pela Internet, até instalar programas na sua máquina. Antes de descarregar um programa ActiveX o seu browser verifica a procedência do mesmo através de um esquema de certificados digitais. Se você aceitar a certificação o programa será rodado na sua máquina. Se os programas vierem de um site idóneo e você aceitar o certificado do site não haverá grandes problemas.

Como me protejo de um programa activex?
Você pode não aceitá-los quando entra num site ou somente aceitá-los de sites conhecidos e de boa reputação. Alguns programas de anti-vírus são capazes de identificar e bloquear programas ActiveX maliciosos.

Webchats

WebChats são conhecidos por vários nomes, você já deve ter visitado alguns ou pelo menos já ouviu falar deles. WebChats são as famosas salas de chat (bate-papo), onde as pessoas entram para conversar uns com os outros ou em grupos.

Há perigo em webchats?
Alguns WebChats usam Java ou JavaScript nas suas páginas, assim, valem as dicas do Java e do JavaScript. Normalmente o perigo nas salas de bate-papo são as conversas mesmo. Você pode transmitir o seu e-mail, endereço, telefone, etc, etc, numa conversa amigável e descobrir depois que a pessoa do outro lado é um burlador. Lembre-se que você não vê nem ouve as pessoas que estão

nas salas. Portanto, tente não se arriscar muito nos chats, evitando passar informações que podem ser utilizadas contra você.

Programas de Troca Instantânea de Mensagens

São programas que possibilitam descobrir se uma pessoa está ligada na Internet e, ao mesmo tempo, trocar mensagens, endereços de sites e ficheiros com ela. Alguns programas de troca criam salas de bate-papo com diversos tópicos, ou canais, como normalmente são chamados. Os mais conhecidos são: ICQ, IRC, AIM, MSN Messenger, Yahoo Messenger, Google Talk, etc. Praticamente cada provedor tem o seu próprio programa para troca de mensagens.

Como funciona os programas de Troca Instantânea de Mensagens?

Basicamente o programa utiliza a Internet para se conectar a um servidor específico. Quando o mesmo se conecta ao servidor ele regista o utilizador no banco de dados e verifica quais dos seus amigos estão no ar. A partir daí este programa estará apto a trocar as mensagens. Caso a outra pessoa esteja fora do ar, a mensagem será guardada no servidor e enviada tão logo esta pessoa se conecte. Normalmente a troca de mensagens e ficheiros não passa pelo servidor. Toda vez que a conexão é feita o servidor passa a conhecer o endereço na Internet (endereço IP) do seu computador. Este IP é enviado para os programas de troca de mensagem de seus amigos, assim, como cada um conhece o endereço do outro, as trocas de mensagem ou ficheiros não mais necessitarão do servidor.

Os programas de Troca Instantânea de Mensagens são seguros?

Programas de troca de mensagens ficam sempre conectados a um servidor (senão não teriam como saber quem está no ar) e, como estão conectados, podem ser atacados por hackers. Não se esqueça que os programas que utilizam a Internet para prestar algum serviço (neste caso troca de mensagens) podem possuir Backdoors e ficarem sujeitos a ataques externos.

Quais são os riscos associados ao uso de salas de chat e de programas como o MSN Messenger, Gtalk, ICQ ou IRC?

Os maiores riscos associados ao uso destes programas estão no conteúdo dos próprios diálogos. Alguém pode utilizar técnicas de engenharia social para obter informações (muitas vezes sensíveis) dos utilizadores destes programas.

Você pode ser persuadido a fornecer numa conversa "amigável" seu *e-mail*, telefone, endereço, senhas (como a de acesso ao seu provedor), número do seu cartão de crédito, etc. As consequências podem ser desde o recebimento de mensagens com conteúdo falso/alarmante ou mensagens não solicitadas contendo propagandas, até a utilização da conta no seu provedor para realizar actividades ilícitas ou a utilização do seu número de cartão de crédito para fazer compras em seu nome.

Além disso, estes programas podem fornecer o seu endereço na Internet (endereço IP). Um atacante pode usar esta informação para, por exemplo, tentar explorar uma possível vulnerabilidade no seu computador.

Como me proteger nos programas de Troca Instantânea de Mensagens?

Valem sempre as mesmas regras básicas. Não aceite ficheiros de pessoas desconhecidas, principalmente programas de computadores. Tente evitar fornecer muita informação a pessoas que você acabou de conhecer, como nos WebChats e, principalmente, esconda o seu endereço da

Internet (endereço IP) quando estiver a utilizar este tipo de programa. Os programas de troca de mensagens possuem esta opção na sua configuração e quando accionada a troca das mensagens passa ao executar somente pelo servidor (a troca de ficheiros normalmente deixa de funcionar neste caso). Os fornecedores destes programas geralmente mantêm páginas na Internet com considerações a respeito de segurança e o que fazer para se proteger melhor. Vale a pena gastar uns minutozitos do seu tempo para ler estas páginas ou ler dicas de utilização nas revistas especializadas em informática. A cada nova versão destes programas, mais recursos são introduzidos, mudando os aspectos de segurança, assim, o negócio é ficar sempre atento nestes sites, nas revistas especializadas e nos cadernos de informática dos jornais para verificar se as opções de segurança dos programas foram alteradas, assim como dicas de utilização.

O caso do IRC é mais complicado, como o programa é mais complexo, possui um grande número de comandos e tem várias salas de bate-papo (no IRC são chamados de canais), fica difícil pensar em segurança. Por exemplo: existe a possibilidade de o utilizador do IRC, sem querer, tornar disponível o acesso ao disco rígido (drive C:) do seu computador, possibilitando aos outros utilizadores do IRC roubarem a sua senha do provedor ou outros dados importantes. O IRC é um programa muito utilizado por hackers para troca de informações e ficheiros, por isso, todo cuidado é pouco.

Programas de distribuição de ficheiros

Ficheiros podem ser enviados (upload) ou recebidos (download) por uma infinidade de maneiras diferentes: através do e-mail, através dos programas de mensagem instantânea e mesmo através dos browsers. Mas, diferente destes, existem os programas construídos com a única finalidade de facilitar a troca de determinados tipos de ficheiros entre os utilizadores, como foi o caso do Napster (que trocava ficheiros de música do tipo MP3) e\ou o Gnutella (que troca todo e qualquer tipo de ficheiro).

Como funcionam os programas de distribuição de ficheiros?

Estes programas funcionam da seguinte forma: quando o programa é conectado ao servidor ele envia uma lista dos ficheiros que estão numa pasta específica (já pré-configurada na instalação do programa) do seu computador e esta lista fica disponível para os demais utilizadores do programa no mundo todo. Quando você procura por um ficheiro (música por exemplo) o programa pergunta ao servidor quais computadores possuem aquele ficheiro, quando você escolhe um dos ficheiros o programa que está em execução no seu computador se conectará ao programa da outra pessoa e baixará o ficheiro escolhido para alguma pasta do seu computador (já pré-configurada e, normalmente, diferente da pasta anterior). Assim o único trabalho do servidor é manter uma lista de quais computadores estão no ar (conectados à Internet e a executar o programa de distribuição de ficheiros) e a lista dos ficheiros disponíveis. O trabalho de baixar e enviar os ficheiros é do seu computador.

Os programas de distribuição de ficheiros são seguros?

Imagine a seguinte situação, se você sem querer altera a configuração de um programa desses e coloca como pasta de distribuição (aquela onde você coloca os ficheiros para distribuição) uma pasta com informações confidenciais a seu respeito ou na pasta C:\Windows onde ficam guardadas as suas senhas, no caso do Gnutella, automaticamente todos os ficheiros estarão disponíveis. Dificilmente ficheiros de música, foto ou vídeo apresentarão problemas, a dificuldade maior será

com os ficheiros de programas que poderão conter Vírus ou Cavalo de Tróia embutidos. Vale a mesma regra dos casos anteriores, evite baixar da rede programas de desconhecidos.

Quais são os riscos associados ao uso de programas de distribuição de ficheiros?

Existem diversos riscos envolvidos na utilização de programas de distribuição de ficheiros, tais como o Bearshare, Kazaa, Morpheus, Edonkey, Gnutella e BitTorrent. Dentre estes riscos, podem-se citar:

> **Acesso não autorizado:** o programa de distribuição de ficheiros pode permitir o acesso não autorizado ao seu computador, caso esteja mal configurado ou possua alguma vulnerabilidade;
>
> ***Softwares* ou ficheiros maliciosos:** os *softwares* ou ficheiros distribuídos podem ter finalidades maliciosas. Podem, por exemplo, conter vírus, ser um *bot* ou cavalo de tróia, ou instalar *backdoors* num computador;
>
> **Violação de direitos autorais (*Copyright*):** a distribuição não autorizada de ficheiros de música, filmes, textos ou programas protegidos pela lei de direitos autorais constitui a violação desta lei.

Como me proteger usando programas de distribuição de ficheiros?
Valem sempre as mesmas regras: sempre desconfie de programas ou ficheiros de desconhecidos, pois eles podem conter Vírus ou Cavalos-de-Tróia. Tenha um bom anti-vírus no seu computador e mantenha-o actualizado sempre.

Que medidas preventivas devo adoptar no uso de programas de distribuição de ficheiros?

Algumas medidas preventivas para o uso de programas de distribuição de ficheiros são:

- manter o seu programa de distribuição de ficheiros sempre actualizado e bem configurado;
- ter um bom antivírus instalado no seu computador, mantê-lo actualizado e utilizá-lo para verificar qualquer ficheiro obtido, pois eles podem conter vírus, cavalos de tróia, entre outros tipos de *malware*;
- certificar-se que os ficheiros obtidos ou distribuídos são **livres**, ou seja, não violam as leis de direitos autorais.

Privacidade

Privacidade nas visitas aos sites
Você já deve ter percebido que quando entra em determinados sites aparecem na página dados do seu computador que às vezes até assustam. Parecem adivinhar até a cor do papel-de-parede que você está a utilizar no seu computador. Isto ocorre porque existe uma "conversa" entre o seu browser e o site que você está a visitar. Entre as informações que o seu browser entrega de bandeja para o servidor do site visitado estão:

- O endereço na Internet de seu computador (endereço IP);
- Nome e versão do sistema operacional;
- Nome e versão do browser;
- Última página visitada;

- Resolução do monitor.

Com estas informações os sites conseguem fazer as estatísticas de visita, adequar à página do site ao browser do utilizador etc. O seu browser sempre passará estas informações aos sites visitados.

Se você quer realmente se esconder (ficar anónimo) e não passar nenhuma informação ao site visitado deverá se utilizar de serviços como o do Anonymizer (http://www.anonymizer.com).

O que são Cookies?
Cookies são pequenas informações, deixadas pelos sites que você visita, no seu browser. Os Cookies são utilizados pelos sites de diversas formas, eis algumas:

- Para guardar a sua identificação e senha quando você pula de uma página para outra;
- Para manter uma lista de compras em sites de comércio electrónico;
- Personalização de sites pessoais ou de notícias, quando você escolhe o que quer que seja mostrado nas páginas destes sites;
- Manter alvos de marketing, como quando você entra num site de CDs e pede somente CDs de hip hop, rock e Semba, e depois de um tempo você percebe que as promoções que aparecem são sempre de CDs de hip hop, rock e Semba (as que você mais gosta);
- Manter a lista das páginas vistas em um site, para estatística ou para retirar as páginas que você não tem interesse dos links.

O problema com relação aos Cookies é que eles são utilizados por empresas que vasculham as suas preferências de compras e espalham estas informações para outros sites de comércio electrónico. Assim você sempre terá páginas de promoções ou publicidade, nos sites de comércio electrónico, dos produtos de seu interesse. Na verdade não se trata de um problema de segurança, mas alguns utilizadores podem considerar este tipo de atitude uma **invasão de privacidade**.

Os browsers possuem opções que desligam totalmente o recebimento de Cookies, limitam o trânsito dos mesmos entre o seu browser e os sites visitados ou opções que fazem com que o seu browser peça uma confirmação ao utilizador toda vez que recebe um cookie. Alguns browsers possibilitam ver o conteúdo dos Cookies.

Privacidade dos E-Mails
Todos os provedores são capazes de ler as correspondências electrónicas dos seus utilizadores, sempre. Esta notícia geralmente cai como uma bomba. Por mais que os provedores possam negar, os e-mails ficam a disposição do administrador dos servidores. Existe, no entanto, um consenso ético de o provedor nunca olhar o conteúdo das caixas de correio dos utilizadores sem o consentimento dos mesmos.

O sistema de envio e recebimento de e-mails foi criado, na década de 70, visando a troca de mensagens simples e curtas entre duas pessoas. A partir daí este serviço cresceu assustadoramente, mas manteve a simplicidade original. O problema desse sistema é que foi comparado com o correio terrestre normal (se bem que um carteiro qualquer poderia ler os seus cartões-postais), dando a falsa ideia de que os e-mails são confidenciais.

As mensagens que chegam na sua caixa postal ficam armazenadas num ficheiro no servidor até você conectar-se na Internet e descarregar os e-mails através do seu programa de e-mails. Portanto,

enquanto os e-mails estiverem no servidor ou em trânsito eles poderão ser lidos pelos administradores dos servidores do provedor.

Se a informação que se deseja enviar por e-mail for confidencial a solução é a utilização de programas de criptografia que codificam o e-mail através de chaves (senhas ou frases) e que só podem ser descodificados por quem possuir a chave certa para isso. Alguns programas de criptografia já podem estar embutidos nos programas de e-mails ou podem ser adquiridos separadamente e serem anexados aos programas de e-mails. Prefira no caso os programas de criptografia que trabalham com pares de chaves, ver criptografia.

SPAM

Muitos de nós já devem ter recebido pelo menos um SPAM. Estas são as famosas mensagens de e-mails não solicitadas e que inundam as nossas caixas de correio de baboseiras. O SPAM não é oficialmente proibido, mas considera-se, na Internet, uma falta de ética. Existem organizações não governamentais que mantêm listas de domínios neste contexto (domínios são os nomes que aparecem depois do @ no endereço de e-mail) que sempre são origem de SPAM. O seu provedor pode, ou não, dependendo da política adoptada, configurar o sistema de recebimento de e-mails para bloquear os e-mails vindos dos domínios destas listas.

Blogs e Redes sociais

Que cuidados devo ter ao disponibilizar uma página na Internet, como por exemplo um *blog*?

Um utilizador, ao disponibilizar uma página na Internet, precisa ter alguns cuidados, visando proteger os dados contidos em sua página.

Um tipo específico de página *Web* que vem sendo muito utilizado por utilizadores de Internet é o *blog* e as paginas pessoais nos sites de relacionamentos. Estes serviços são usados para manter um registo frequente de informações, e tem como principal vantagem permitir que o utilizador publique o seu conteúdo sem necessitar de conhecimento técnico sobre a construção de páginas na Internet.

Apesar de terem diversas finalidades, os *blogs* têm sido muito utilizados como diários pessoais. Em no *blog*, um utilizador poderia disponibilizar informações, tais como:

- seus dados pessoais (*e-mail*, telefone, endereço, etc);
- informações sobre seus familiares e amigos (como árvores genealógicas, datas de aniversário, telefones, etc);
- dados sobre o seu computador (dizendo, por exemplo, "...comprei um computador da marca X e instalei o sistema operacional Y...");
- dados sobre os *softwares* que utiliza (dizendo, por exemplo, "...instalei o programa Z, que acabei de obter do *site* W...");
- informações sobre o seu quotidiano (como, por exemplo, hora que saiu e voltou para casa, data de uma viagem programada, horário que foi ao multicaixa, etc);

É extremamente importante estar atento e avaliar com cuidado que informações serão disponibilizadas numa página *Web*. Estas informações podem não só ser utilizadas por alguém mal-intencionado, por exemplo, num ataque de engenharia social, mas também para atentar contra a segurança de um computador, ou até mesmo contra a segurança física do próprio utilizador.

Cuidados a ter-se em *sites* de redes sociais

Os *sites* de redes sociais, como o facebook, twitter, badoo ou orkut, tiveram uma ampla aceitação e inserção de utilizadores da Internet, por proporcionarem o encontro de pessoas (amigos) e permitirem a criação e participação em comunidades com interesses em comum.

Um *site* de redes sociais normalmente permite que o utilizador registe informações pessoais (como nome, endereços residencial e comercial, telefones, endereços de *e-mail*, data de nascimento, etc), além de outros dados que irão compor o seu perfil. Se o utilizador não limitar o acesso aos seus dados para apenas aqueles de interesse, todas as suas informações poderão ser visualizadas por qualquer um que utilize este *site*. Além disso, é recomendável que o utilizador evite fornecer muita informação a seu respeito, pois nenhum *site* está isento do risco de ser invadido e de ter as suas informações furtadas por um invasor.

A participação de um utilizador em determinados tipos de comunidades também pode fornecer muita informação para terceiros. Por exemplo, a comunidade de donos de um determinado veículo, ou dos frequentadores do estabelecimento X, pode dizer qual é a classe social de um utilizador, que locais ele gosta de frequentar, etc.

Desta forma, é extremamente importante estar atento e avaliar com cuidado que informações você disponibilizará nos *sites* de redes de relacionamentos, principalmente aquelas que poderão ser vistas por todos, e em que comunidades você participará. Estas informações podem não só ser utilizadas por alguém mal-intencionado, por exemplo, num ataque de engenharia social, mas também para atentar contra a segurança física do próprio utilizador.

HOAX

Hoaxes são comuns na Internet e são e-mails que possuem conteúdos alarmantes ou falsos, geralmente apontando como remetentes empresas importantes ou órgãos governamentais. Em geral se você ler atentamente estes e-mails notará que os seus conteúdos são absurdos e sem sentido. Essas mensagens podem estar acompanhadas de vírus. Dentre os hoaxes típicos temos as correntes ou pirâmides, pessoas ou crianças que estão prestes a morrer de câncer, etc. Histórias deste tipo são criadas para espalhar desinformação pela Internet. Este tipo de e-mail foi inventado para entupir as caixas postais dos grandes provedores. Outro objectivo de quem escreve este tipo de mensagem é verificar o quanto ela se espalha pelo mundo e por quanto tempo ela continua a ser espalhada, mais ou menos os objectivos de quem programa Vírus. Estas mensagens se propagam tanto pela boa vontade e solidariedade de quem as recebe e, por isso, é praticamente impossível eliminá-las da Internet.

Quem repassa este tipo de mensagem para os amigos ou conhecidos acaba aderindo ou avalizando indirectamente o que está escrito, e as pessoas que recebem os seus -mails acabam confiando em ti e não verificam a procedência nem a veracidade da história.

Neste endereço, http://HoaxBusters.ciac.org/ você encontra uma lista de hoaxes que estão a circular pela Internet com seus respectivos textos.

Os seus dados pessoais!

Jamais entregue os seus dados pessoais (nome, e-mail, endereço, números de documentos e, principalmente, número de cartão de crédito) em qualquer site que você visita. Não se esqueça que estas informações são guardadas em alguma base de dados do site e podem ser vendidas (o que

seria anti-ético) para outras empresas. O seu e-mail pode ser utilizado em alguma lista de distribuição de SPAMs.

Formulários, Comércio Electrónico e Home-Banking

Sempre que utilizar a Internet para transacções comerciais envolvendo o seu dinheiro, verifique dois itens importantíssimos.

Se o site visitado pertence a uma instituição de confiança e tem bom nome no mercado;

Se o site utiliza algum esquema de conexão segura.

O primeiro item deve ser óbvio ao utilizador, sites desconhecidos podem causar mais aborrecimentos do que soluções. O segundo item é o mais importante no caso, pois garante que os dados digitados nos formulários (ou na realização das transacções bancárias, por exemplo) estejam protegidos dos olhares curiosos dos hackers. Como verificar, então, se a conexão é segura? Existem duas maneiras diferentes, primeiro através do endereço do site que deve começar com https:// (diferente de http://das conexões normais), o s antes do sinal de dois-pontos indica que o endereço em questão é de um site com conexão segura e, portanto, os dados do formulário serão criptográfados (ver criptografia) antes de serem enviados.

Outra indicação, e a mais importante, é que o seu browser irá indicar se a conexão está segura através de algum sinal. O sinal mais adoptado nos browsers é o de um desenho de um cadeado fechado (se o cadeado estiver aberto, a conexão não é segura). Se você clicar em cima deste cadeado você obterá informações sobre o método de criptografia utilizado para cifrar os dados do formulário (ou da transacção), verifique sempre o tamanho da chave utilizada, chaves menores que 40 bits, que são utilizadas em browsers mais antigos, são consideradas inseguras, o ideal é utilizar browsers que usem chaves de pelo menos 128 bits de tamanho (as versões mais actuais dos browsers já utilizam chaves deste tamanho).

As transacções comerciais via Internet são tão seguras quanto as realizadas no balcão, somente verifique se a conexão está segura antes enviar qualquer dado ao site.

Programas para a protecção do utilizador

Anti-Vírus

Os anti-vírus são programas que detectam, anulam e eliminam os Vírus de computador. Actualmente os programas anti-vírus foram ganhando novas funcionalidades e conseguem eliminar Cavalos de Tróia, impedem programas Java e ActiveX hostis e verificam e-mails.

Um bom anti-vírus deve possuir as seguintes funcionalidades:

Identificar e eliminar uma boa quantidade de Vírus;

Analisar os ficheiros que estão a ser descarregados pela Internet;

Verificar continuamente os discos duros e flexíveis de forma transparente ao utilizador;

Procurar vírus e cavalos de tróia em ficheiros anexados aos e-mails;

Criar uma disquete de verificação (disquete de boot) que pode ser utilizado caso o vírus seja mais esperto e anule o anti-vírus que está instalado no computador;

Actualizar as bases de dados de vírus pela rede.

Alguns anti-vírus, além das funcionalidades acima, ainda verificam o funcionamento dos programas do seu computador, avisando ao utilizador; caso algum programa comece a apresentar algum comportamento suspeito (como por exemplo, o programa de e-mail começar a mandar e-mails sozinho).

Algumas versões de anti-vírus são gratuitas para uso pessoal e podem ser descarregadas pela Internet.

Firewalls

Os Firewalls são sistemas ou programas que bloqueiam conexões indesejadas na Internet. Assim, se algum hacker ou programa suspeito tenta fazer uma conexão ao seu computador o Firewall irá bloquear. Com um Firewall instalado no seu computador, grande parte dos cavalos de tróia serão bloqueados mesmo se já estiverem instalados no seu computador. Alguns programas de Firewall chegam ao requinte de analisar continuamente o conteúdo das conexões, filtrando os Cavalos de tróia e os vírus de e-mail antes mesmo que os anti-vírus entrem em acção. Esta análise do conteúdo da conexão serve, ainda, para os utilizadores bloquearem o acesso a sites com conteúdo erótico ou ofensivo, por exemplo. Existem, ainda, pacotes de Firewall que funcionam em conjunto com os anti-vírus possibilitando ainda um nível maior de segurança nos computadores que são utilizados em conexões com a Internet. Assim como certos anti-vírus, alguns fabricantes de Firewalls oferecem versões gratuitas dos seus produtos para uso pessoal. Existem programas e sistemas de Firewall extremamente complexos que fazem uma análise mais detalhada das conexões entre os computadores e que são utilizados em redes de maior dimensão e que são muito caros para o utilizador doméstico. A versão doméstica deste programa geralmente é chamada de Firewall pessoal. Normalmente estes programas de Firewall criam ficheiros especiais no seu computador denominados de ficheiros de log. Nestes ficheiros serão armazenadas as tentativas de invasão que o Firewall conseguiu detectar e que são avisadas ao utilizador. Caso necessário envie este ficheiro de log para o seu provedor, assim o pessoal do provedor poderá comparar os seus logs com os do provedor, verificando se a invasão ocorreu de facto ou foi um alarme falso

Criptografia e Assinatura Electrónica de Documentos

Criptografia é a arte e a ciência de criar mensagens que possuem combinações das seguintes características: ser privada, somente quem enviou e quem recebeu a mensagem poderá lê-la; ser assinada, a pessoa que recebe a mensagem pode verificar se o remetente é mesmo a pessoa que diz ser e ter a capacidade de repudiar qualquer mensagem que possa ter sido modificada. Os programas de criptografia disponíveis no mercado, para criptografia de mensagem de e-mails, normalmente possuem todas estas características. Um método de criptografia de texto utilizado por Júlio César para comunicar-se com as suas tropas é conhecido actualmente por Rot13, que consistia em trocar as letras das palavras por outras (13 letras distantes), assim A seria trocado por O, B por P e assim por diante (Z seria trocado por M). Para obter o texto original basta destrocar as letras.

É claro que actualmente existem “receitas” de criptografia muito mais complicadas e poderosas do que esta. As “receitas” de criptografia actuais utilizam o que chamamos de chave para cifrar e decifrar uma mensagem. Esta chave é uma sequência de caracteres, como a sua senha, que são

convertidos num número. Este número é utilizado pelos programas de criptografia para cifrar a sua mensagem e é medido em bits, quanto maior o tamanho da chave, mais caracteres (letras, números e sinais) devem ser utilizados para cria-las.

Criptografia de Chave Única

Quando um sistema de criptografia utiliza chave única quer dizer que a mesma chave que cifra a mensagem serve para decifrá-la. Isto quer dizer que para você e os seus amigos poderem trocar mensagens cifradas todos deverão utilizar a mesma chave. É claro que se você se corresponder (trocar e-mails) com um grande número de pessoas a sua chave perderá a utilidade pois todos a conhecerão, portanto, estes métodos são mais úteis para cifrar documentos que estejam no seu computador do que para enviar mensagens para amigos. Os métodos de criptografia por chave simples são rápidos e difíceis de decifrar. As chaves consideradas seguras para este tipo de método de criptografia devem ter pelo menos 128 bits de comprimento.

Criptografia de chave pública e privada e assinatura electrónica de documentos

Este tipo de método de criptografia utiliza duas chaves diferentes para cifrar e decifrar as suas mensagens. Eis como funciona: com uma chave você consegue cifrar e com a outra você consegue decifrar a mensagem. Qual a utilidade de se ter duas chaves então? Ora, se você distribuir uma delas (a chave pública) para seus amigos eles poderão cifrar as mensagens com ela, e como somente a sua outra chave (a chave privada) consegue decifrar, somente você poderá ler a mensagem. Este método funciona ao contrário também, se você usa a sua chave privada para cifrar a mensagem, a chave pública consegue decifrá-la. Parece inútil mas serve para implementar um outro tipo de serviço nas suas mensagens (ou documentos): a Assinatura Electrónica.

A assinatura electrónica funciona da seguinte forma: o texto da sua mensagem é verificado e nesta verificação é gerado um número (este número é calculado de tal forma que se apenas uma letra do texto for mudada, pelo menos 50% dos dígitos do número mudam também), este número será enviado junto com a sua mensagem mas será cifrado com a sua chave privada. Quem receber a mensagem e possuir a sua chave pública vai verificar o texto da mensagem novamente e gerar um outro número.

Se este número for igual ao que acompanha a mensagem, então a pessoa que enviou o e-mail será mesmo quem diz ser. Ainda, se alguém mudar algo na mensagem os números não serão mais iguais mostrando que a mensagem foi modificada por alguém. Lembre-se que as suas mensagens de e-mail poderão ser somente cifradas, somente assinadas ou cifradas e assinadas ao mesmo tempo. As duas operações são independentes. Estes métodos de criptografia, no entanto, apresentam dois problemas. São muito mais lentos que os métodos de chave única e as chaves públicas e privadas têm que ser muito maiores. Uma chave segura neste caso deve medir pelo menos 512 bits. O método de chave pública e privada mais conhecida é o PGP (existem versões gratuitas na Internet) que adiciona estas funcionalidades ao seu programa de e-mail. Só por curiosidade, a Casa Branca utiliza este tipo de programa para a troca de mensagens entre o presidente e os seus assessores.

Quão segura é a "receita" de criptografia?

Sabemos que por mais poderosa que seja a receita de criptografia ainda assim ela pode ser decifrada. O importante é saber em quanto tempo isto pode ocorrer, por exemplo, no caso de métodos de chave única, se utilizarmos chaves de 40 bits em alguns dias a mensagem pode ser decifrada (testando dois elevado a quarenta chaves possíveis). Se utilizarmos chaves de 128 bits

(dois elevado a cento e vinte e oito chaves possíveis) um super-computador demoraria alguns milhões de anos. Este é o caso de se testar todas as chaves possíveis, é claro que podem ter falhas na receita da criptografia, mas as receitas que estão no mercado foram bem testadas e a complexidade de algumas delas garantem a segurança do método. Normalmente as quebras das chaves são realizadas por força-bruta (brute force) mesmo, testando uma por uma até descobrir a chave utilizada.

Fui atacado! E agora?

Toda vez que te sentires lesado, seja por ataques, seja por e-mail não solicitado, entre em contacto com o seu provedor de acesso a Internet ou de E-mail. Todos os bons provedores possuem uma equipe para cuidar da segurança dos seus utilizadores e do próprio provedor. Segundo normas da Internet (RFC2142), todos os provedores ou domínios devem possuir os seguintes endereços de e-mails:

abuse@(o seu provedor).co.ao - Usado para informar a respeito dos SPAMs ou emails de conteúdo abusivo ou ofensivo;

noc@(seu provedor).co.ao - Utilizado para relatar problemas com a rede;

security@(seu provedor).co.ao - Utilizado para relatar problemas envolvendo segurança, como invasões, ataques etc.

Todos os bons provedores costumam auxiliar o utilizador quando este é atacado ou invadido por hackers.

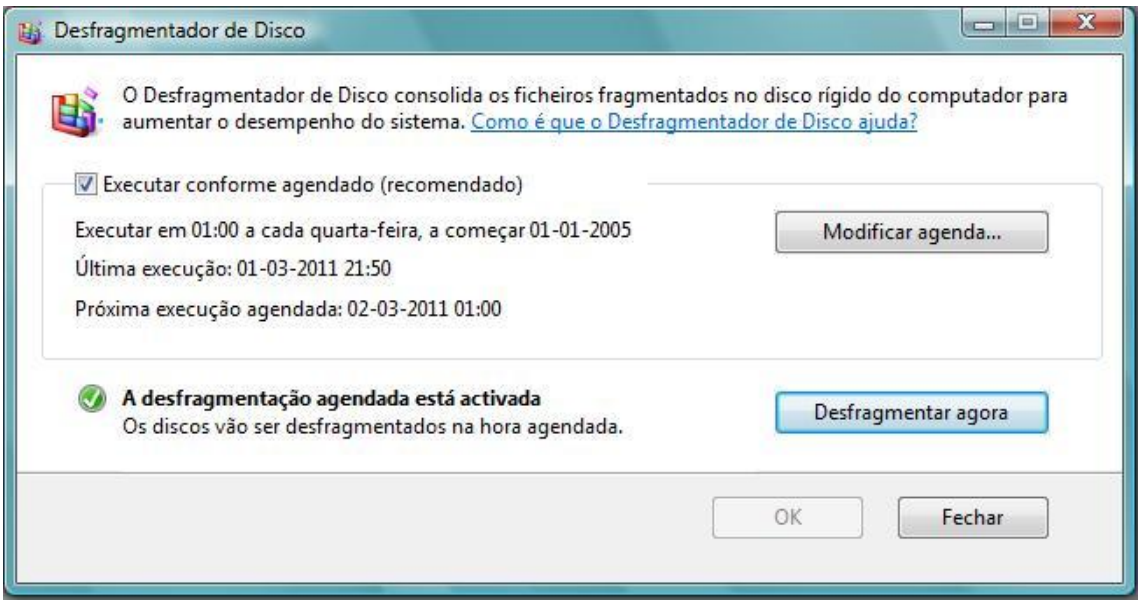
Práticas recomendáveis

Windows update

Manter o computador com patches actualizados é muito importante. Portanto, visitas ao site do Windows Update e do Office devem ser uma prática regular. As actualizações corrigem os problemas encontrados em versões anteriores dos softwares (programas).

Desfragmentador de disco

Para entender o que o Desfragmentador de Disco faz, é necessário ter uma visão geral de como funciona o disco duro. O disco rígido grava as informações em blocos de dados na sua área de armazenamento. Esses blocos de informações são ficheiros do Windows, dos programas e ficheiros de trabalhos. Nem sempre o disco duro grava esses blocos em sequência, o que não significa que os ficheiros são perdidos. O disco duro possui um índice de ficheiros (a FAT - File Alocation Table, ou Tabela de Alocação de Ficheiros) que indica aonde estão esses blocos.



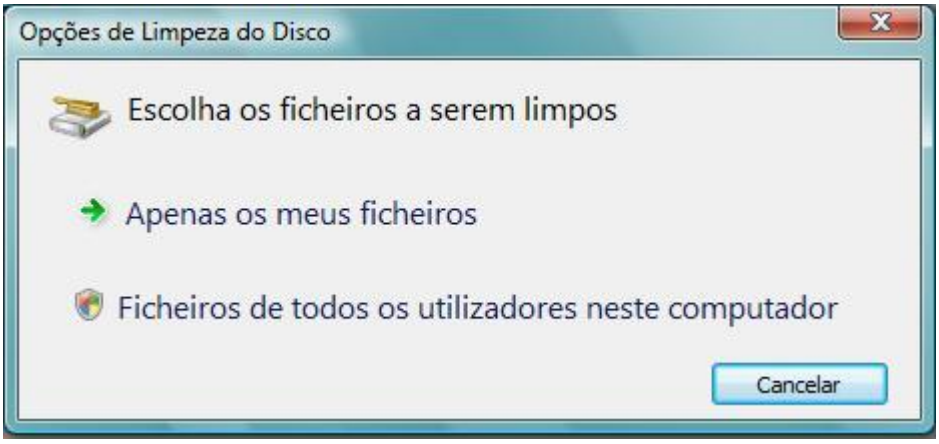
A ferramenta Desfragmentador de Disco re-aloca os blocos de informação no disco de forma que eles fiquem em sequência, para que o disco duro não tenha tanto trabalho para ler a informação. Assim, quando o computador lê o disco duro, ele lê na FAT aonde estão esses blocos de informação e faz uma ida só até o local.

Scandisk

O disco rígido é a unidade principal de armazenamento de dados do computador. Então ele tem que ser verificado com alguma regularidade. Esta ferramenta existe para isso. Ela verifica o disco duro a procura de sectores com defeitos e que podem causar perda de dados. Quando isso existe ou quando esta ferramenta encontra erros em ficheiros (chamados de ficheiros corrompidos), um ficheiro do tipo CHK é gerado com a informação recuperada. Este ficheiro é utilizado pelos técnicos de informática para recuperar os ficheiros, mas em geral nem todos os dados são recuperáveis. Por isso estes ficheiros podem ser apagados. Mas, a partir do momento que foram apagados, não podem mais ser recuperados.

Limpeza de disco

Esta ferramenta existe para que o utilizador não tenha problemas de espaço do disco rígido ocupado por ficheiros que podem ser eliminados. O ideal é que a limpeza de disco seja feita antes de executar o Desfragmentador de disco e até mesmo antes do Scandisk.

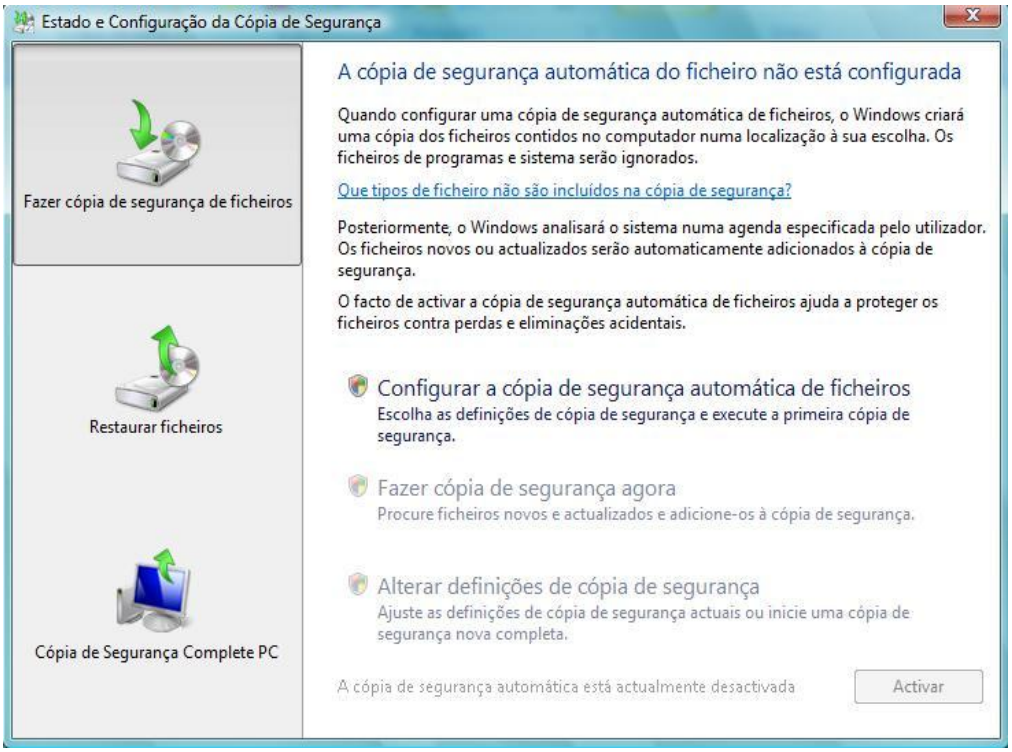


Quando os programas gravam os dados no computador, ou quando a Internet é acedida, são gerados ficheiros temporários para o Windows trabalhar mais rapidamente. Mas nem todos os ficheiros gerados são apagados, alocando assim um espaço do disco duro que poderia ser utilizado por ficheiros mais úteis ao utilizador. A Lixeira também armazena ficheiros que podem ser apagados.

Todos esses ficheiros podem ser apagados do disco duro com a ferramenta de Limpeza de disco, que encontra e apaga esses ficheiros. Isso geralmente libera muito espaço para quem trabalha com ficheiros grandes e para quem aceda a Internet com regularidade.

Backup (Copia de Segurança)

O backup é uma ferramenta que permite a cópia de mais de um directório ou todo o conteúdo do computador para unidades externas de armazenamento.



Capitulo II

Invasões e ataques: como são feitas e como se proteger?

Segurança em informática

Estamos seguros?

A fragilidade dos sistemas informatizados não é nenhuma novidade. Há décadas, "celebridades" como Robert Morris Jr, Capitão Crunch, Kevin Poulsen e Kevin Mitnick, esses últimos dois mais recentes, fazem com que as pessoas se preocupem e tenham um medo maior do computador. Esse medo virou pânico em pleno século XXI. Piratas novamente existem, mas a sua arma não é mais a espada, é o fax-modem. Graças à essa maravilha do mundo moderno, dados podem navegar por linhas telefónicas, cabos e satélites, diminuindo as distâncias entre os povos e iniciando a nova era digital. Ladrões assaltam bancos confortavelmente no Havaí enquanto desviam o dinheiro para a Suíça. A espionagem industrial é um dos problemas agravados. Ela sempre existiu, mas com a facilidade de acesso à Internet, qualquer pessoa pode conseguir dados confidenciais e vendê-los para concorrentes.

Diariamente, páginas e páginas são tiradas do ar por piratas digitais. Grupos de hackers e crackers, como Prime Suspectz e Inferno.br (esse último já extinto), junto a outras centenas pelo mundo realizam façanhas extraordinárias, como invadir vários sites da Microsoft, Nasa, FBI, Interpol e muitos outros. Os grupos brasileiros actualmente são os que mais invadem homepages em todo o mundo, fazendo com que a própria Nasa restrinja acesso ao Brasil em algumas das suas páginas. Mas nem todos são ruins. Existem grupos que se especializam em criar ferramentas e ajudar utilizadores comuns. Isso demonstra a fragilidade da situação. Respondendo à perguntado tópico: estamos seguros? Com certeza que não.

Vulnerabilidades

Como posso saber se os *softwares* instalados no meu computador possuem alguma vulnerabilidade?

Existem *sites* na Internet que mantêm listas actualizadas de vulnerabilidades em *softwares* e sistemas operacionais. Alguns destes *sites* são http://www.cert.org/, http://cve.mitre.org/ e http://www.us-cert.gov/cas/alerts/.

Além disso, fabricantes também costumam a manter páginas na Internet com considerações a respeito de possíveis vulnerabilidades nos seus *softwares*.

Portanto, a idéia é estar sempre atento aos *sites* especializados em acompanhar vulnerabilidades, aos *sites* dos fabricantes, às revistas especializadas e as newsletters de segurança de informação, para verificar a existência de vulnerabilidades no sistema operacional e nos *softwares* instalados no seu computador.

Como posso corrigir as vulnerabilidades dos *softwares* em meu computador?

A melhor forma de evitar que o sistema operacional e os *softwares* instalados num computador possuam vulnerabilidades é mantê-los **sempre actualizados**.

Entretanto, fabricantes em muitos casos não disponibilizam novas versões dos seus *softwares* quando é descoberta alguma vulnerabilidade, mas sim correcções específicas (*patches*). Estes *patches*, em alguns casos também chamados de *hot fixes* ou *service packs*, têm por finalidade corrigir os problemas de segurança referentes às vulnerabilidades descobertas.

Portanto, é **extremamente importante** que você, além de manter o sistema operacional e os *softwares* sempre actualizados, instale os *patches* sempre que forem disponibilizados.

Características de um sistema inseguro

A segurança de sistemas existe por um conjunto de factores. Engana-se quem pensa que somente por utilizar uma plataforma Unix ao invés de Windows está seguro. Ou que é só colocar um anti-vírus e um firewall na sua empresa que está tudo bem. A proporção do problema é bem maior. Geralmente os sistemas mais vulneráveis da rede possuem dois pontos em comum:

Administrador

O ponto-chave e essencial para qualquer sistema de computador é o administrador. Ele é responsável por fazer com que tudo corra perfeitamente. Verifica os dados, administra utilizadores, controla servidores, verifica logs, tudo todos os dias. Acontece que a grande maioria dos administradores hoje não se preocupa com a segurança como deve. Logo terá problemas com o seu sistema, não importa qual seja. É como se fosse mãe e filho. Se uma mãe alimenta o seu filho, cuida dos seus deveres de casa, compra roupas novas, dá brinquedos mas não é capaz de comprar um seguro de vida, ou pior, zela tão pouco pela segurança dele que ao sair de casa deixa as portas ou janelas abertas. Essa não pode ser uma boa mãe.

Mesmo que uma rede utilize um sistema operacional que contenha muitas falhas, os bons administradores têm que pesquisar diáriamente por falhas descobertas e corrigindo-as. Já os outros provavelmente ficarão entretidos com algum chat ou rede social.

Sistemas operacionais

Como eu disse anteriormente, não há realmente um sistema que seja melhor que o outro. Existem vantagens e desvantagens de cada um. Tudo bem que alguns possuem erros muitos grandes, mas podem facilmente ser corrigidos. A intenção do sistema também importa. Não adianta ter uma rede e utilizar Windows 98 ou ME. Os recursos de segurança deles são muito escassos, pois foram feitos para o utilizador comum e não para o ambiente empresarial. Não adianta também instalar o Digital Unix, FreeBSD ou AIX se o seu administrador não possuir experiência nesses sistemas. O sistema também vai depender do tipo de rede que você possuir. Se você tiver um servidor Web ou algum tipo de acesso externo, seria melhor utilizar o Linux ou o Windows Server (2003 ou 2008). Se for uma rede interna somente, utilize Novell Netware, que não é tão bom quanto ao Linux ou Windows Server no que a Internet diz respeito, mas ainda é excelente para redes locais.

A segurança ao longo da história

Anos atrás, os operadores de um computador ENIAC depararam-se com uma coisa curiosa. Um insecto havia ficado preso dentro da máquina e estava a dificultar o funcionamento da mesma. Daí surgiu o termo bug (insecto) que virou sinónimo de falha. Hoje quando se descobre um erro em algum programa, diz-se: "novo bug descoberto". De lá para cá, as coisas evoluíram muito, mas os bugs continuam a existir. Muitos deles são frutos da história do próprio programa ou sistema. O Windows por exemplo. O Windows NT foi construído a partir do zero, mas o Windows ME não. Desde o início da criação da sua primeira interface gráfica, a Microsoft vêm tendo problemas com erros graves no seu sistema operacional. Já o sistema Unix, foi criado pelos desenvolvedores da linguagem C, para ser um sistema versátil e poderoso. Para conhecer melhor sobre a história de cada sistema, leia a secção sistemas operacionais. A Internet também tem os seus problemas ligados à história da sua origem. Desde que se chamava Arpanet e foi criada pelo exército americano para resistir à guerra fria, a rede evoluiu muito e foram criados novos serviços como E-mail, WorldWideWeb, Gopher, Whois e outros. Milhões de computadores juntaram-se a ela e os seus recursos são cada vez mais sofisticados. Mas alguns problemas bem antigos ainda prejudicam hoje. Uma falha na implementação do TCP/IP (conjunto de protocolos em que a Internet se baseia) por exemplo, possibilita que o ataque de Spoof aconteça.

Invasores digitais

Todos os dias surgem notícias sobre piratas digitais na televisão ou na Internet. Um pirata invadiu o computador de um sistema de comércio electrónico, roubou os números de cartão, comprou Viagra e mandou entregar na casa do Bill Gates. Outro conseguiu pôr em baixo sites famosos como YAHOO, CNN, AMAZON e ZDNET. Mais recentemente um grupo estrangeiro conseguiu tirar mais de 650 sites do ar num minuto. Para entender como se organiza a hierarquia virtual da Internet, vamos estudar os seus principais integrantes:

Hackers

Na verdade, os hackers são os "bons rapazes". Ele possui os mesmos poderes que o seu "irmão" do lado negro da força (cracker) mas os utiliza para protecção. É um curioso por natureza, uma pessoa que tem em aprender e se desenvolver um hobby, assim como ajudar os "menos prevalecidos". Um bom exemplo real foi quando o cracker Kevin Mitnick invadiu o computador do analista de sistemas Shimomura. Mitnick destruiu dados e roubou informações vitais. Shimomura é chamado de hacker pois usa a sua inteligência para o bem, e possui muitos mais conhecimentos que o seu inimigo digital. Assim facilmente montou um honeypot (armadilha que consiste em criar uma falsa rede para pegar o invasor) e pegou Kevin. Infelizmente a imprensa confundiu os termos e toda notícia referente a anarquistas digitais se refere à hacker.

Crackers

Esses sim são os maldosos. Com um alto grau de conhecimento e nenhum respeito, invadem sistemas e podem apenas deixar a sua "marca" ou destruí-los completamente. Geralmente são hackers que querem se vingar de algum operador, adolescentes que querem ser aceitos por grupos de crackers (ou script kiddies) e saem apagando tudo que vêem ou mestres da programação que são pagos por empresas ou governos para fazerem espionagem industrial. Hackers e crackers costumam entrar muito em conflito. Guerras entre grupos é comum, e isso pode ser visto em muitos fóruns de discussão e em grandes empresas, as quais contratam hackers para proteger os seus sistemas.

Os hackers e crackers são eternos inimigos. Um não gosta do outro e sempre estão em confronto pelos seus ideais. Resumindo, Hackers e Crackers são pessoas com poderes iguais mas de ideologias opostas. Os nossos invasores digitais são assim: "O artista e o rei dos bandidos em confronto".

Phreakers

Maníacos por telefonia. Essa é a maneira ideal de descrever os phreakers. Utilizam programas e equipamentos que fazem com que possam utilizar telefones gratuitamente. O primeiro phreaker foi o Capitão Crunch, que descobriu que um pequeno apito encontrado em pacotes de salgados possuía mesma frequência das cabines de telefones públicos da AT&T, fazendo com que discassem de graça. Um programa comum utilizado é o bluebox, que gera tons de 2600 pela placa de som, fazendo com que a companhia telefónica não reconheça a chamada. Também tem o Black Box que faz com que você possa ligar de borla do seu telefone doméstico e o Red Box que possibilita que se ligue de telefones públicos. Se quiser saber mais sobre o assunto, consulte o site www.txt.org.

Outra técnica muito utilizada é a de utilizar um diodo e um resistor em telefones públicos. Ou descobrir o cartão telefónico de papel alumínio para que os créditos não acabem (nunca testei, mas me disseram que funciona). Técnicas como essas são utilizadas no mundo inteiro. O phreaker é uma categoria à parte, podem ser hackers, crackers ou nenhum dos dois. Alguns phreakers são tão avançados que têm acesso directo à centrais de telefonia, podendo desligar ou ligar telefones, assim como apagar contas. Um dos programas muito utilizados para isso é o ozterm, software de terminal que funciona em modo Dos. Por sinal, muito difícil de encontrar na internet.

Funcionários

Outro problema grave. 60% das invasões hoje acontecem de dentro da própria empresa, por funcionários insatisfeitos ou ex-funcionários que querem vingança. Utilizam-se do conhecimento adquirido e arrasam com dados do sistema. Copiam coisas do seu interesse (como a base de dados que possui o telefone de alguém muito importante) ou instalam jogos em rede que podem comprometer a segurança, pois com certeza não se preocupam em passar anti-vírus. Utilizam trojans, scanners e sniffers para capturar o que lhes interessa. Firewall é ineficaz contra eles. Afinal, do que adianta a grande muralha da china se algum soldado é o traidor?

Mitos e fantasias

O maior mito existente na Internet é que o cracker pode invadir qualquer computador na hora que quiser. Não é bem assim. Invasões por ICQ por exemplo, pura mentiram. Só era possível em versões antigas e mesmo assim se o servidor Web que vêm com o programa estivesse activo. Isso porquê para conseguir acesso a o interpretador de comandos do sistema por alguma porta, têm de existir um serviço próprio para isso. Para se invadir um computador pessoal, só existem duas maneiras: trojans e netbios. A não ser que seja um computador que rode muitos serviços (FTP,Web,Telnet), o perigo é mínimo. Outro mito é o que o hacker e o cracker são vistos como génios da informática. Bom, os de antigamente realmente eram e ainda existem alguns poucos, mas a grande maioria que se diz "hacker" hoje em dia aproveita-se de ferramentas encontradas na Internet. Nem programar sabem. São os famosos Script Kiddies, subcategoria de crackers. Não têm um alvo certo, tentam invadir tudo que vêm na frente. Pior que eles só os Lamers, aqueles que chegam nos chats anunciando "vou te invadir, sou o melhor" mas acaba desistindo pois não consegue descompactar nem um ficheiro *.rar.

Como conseguir uma política eficiente de protecção?

Leia muito sobre as novidades do mundo da segurança. Veja se o seu administrador realmente preocupa-se com a protecção do sistema ou contrate alguém somente com essa função. Faça sempre backup dos logs e varredura do sistema por falhas. Verifique o computador dos funcionários a procura de programas escondidos e passe um bom anti-vírus neles. Se for usar algum programa de segurança, como firewalls, detectores de invasão e outros, dê preferência para aqueles mais conhecidos e confiáveis.

Tenha certeza de que quando despedir alguém, mudar as senhas de acesso ao sistema. Nunca discuta com um cracker (para o seu próprio bem). E o mais importante: saiba que apesar de tudo isso, nunca vai estar totalmente seguro. Nenhum sistema é 100% à prova de falhas. Mas pelo menos você pode diminuir muito o risco.

Analisando o nível de perigo

A influência do sistema operacional

Como vimos no capítulo anterior, o sistema operacional não influi tanto na segurança quanto algumas pessoas pensavam. Citei anteriormente que se alguém precisasse de um servidor externo seria melhor que utilizasse o Linux ou o Windows Server se fosse apenas uma rede local. E o Netware? A Novell passou a apostar na Internet mais tarde, as suas antigas versões não possuiam o suporte devido à rede. E os seus servidores Web ainda não são tão utilizados em larga escala quanto o Apache e o IIS. Por isso não nos aprofundaremos muito nele, pois o nosso principal foco é os ataques remotos. Leia um pouco mais sobre cada um.

Unix versus Windows

Por serem os dois sistemas mais usados quando se utiliza servidores externos (servidores de e-mail, abordaremos uma breve explicação sobre as suas diferenças. Para mais detalhes ver a secção sistemas operacionais. O Unix é multi-tarefa e o Windows também. Ambos são largamente usados hoje em dia, sendo distribuídos em várias variantes (Linux, Xenix, Windows ME, Windows 2000, Windows 2000 Server, Windows XP, Windows 2003 Server, Vista, Windows 2008 Server e 7). O Windows possui algumas vantagens sobre o Unix. Mais simples de se usar, é fácil de se instalar programas e drivers, e possui mais programas no mercado. Apenas isso. O Unix em comparação, possui inúmeras vantagens sobre o Windows. Vamos listar algumas.

-Têm distribuições gratuitas (como é o caso do Linux)

-Criptografia inquebrável de senhas. Só se descobre no método da tentativa e erro.

-Melhores ferramentas de rede

-Melhor gerenciamento de permissões

-Código-fonte aberto

Vantagens do open source

As vantagens do código-fonte aberto (ou open-source) são muito grandes. Esse termo significa que os programas criados (ou o próximo sistema operacional) vêm junto com o seu código fonte, ou seja, você pode ver exactamente o que está a executar. Para começar, qualquer um pode fazer a sua própria versão de Unix ou Linux (como foram os casos das versões Angolanas do Linux, AngolanOS e Angolinux). É só pegar o código fonte de algum sistema já existente e alterá-lo. Como o sistema operacional foi feito de programadores para programadores, ainda possuem alguns recursos que o utilizador comum não consegue entender. Mas até isso o open-source está a mudar.Novas ferramentas gráficas foram criadas para facilitar o uso do Unix. Podem torná-lo mais fácil de utilizar quanto o Windows. E o melhor são melhoradas rapidamente pelos seus próprios utilizadores e distribuídas gratuitamente. Alguns bons exemplos são o GNOME e o KDE, os ambientes gráficos mais usados na actualidade.

Configurações malfeitas

A configuração malfeita é a perdição de um bom sistema. Contas padrões, serviços desnecessários activos e erros em permissões de ficheiros são falhas muito grandes. As contas padrões são perigosas pois todo mundo conhece sobre elas. O caso do Unix por exemplo. Contas como Bin e admin vêm com senhas padrões de acesso ao sistema. Desabilite-as ou mude as senhas. Quanto aos serviços, se você possui um servidor telnet, ou mesmo ftp, que estiver usando pouco, desabilite-os. Ou pelo menos configure para esse servidor as relações desconfiança dizendo qual endereço IP poderá ter acesso a ele e qual o acesso será restrito. As permissões de ficheiro também são importantes. Elas impedem que alguém execute algum programa malicioso ou aceda o ficheiro de senhas.

Ataques restritos a um tipo de sistema

Todo sistema sofre ataques de maneiras diferentes. E alguns desses ataques afectam o sistema ou não causam absolutamente nada. Um bom exemplo é o caso dos vírus e trojans. Para Unix, eles praticamente não existem. Mas para Windows há milhões deles. O Unix possui falhas em alguns servidores que o Windows não, como o sendmail. O melhor arma para invadir algum sistema é ele mesmo. Por exemplo, se quero conseguir acesso a um servidor Linux, dificilmente conseguirei utilizando Windows NT.

Ataques universais intra-sistemas

São ataques em que não importa o tipo do SO (Sistema Operacional) de origem ou de destino. Funciona em todos os sistemas. Como é o caso do IPSpoof. Ele trabalha a nível de protocolo, utilizando-o você consegue acesso a qualquer máquina, seja Windows, Unix, Novell, DEC-10,VMS,Novell o que for.

Recusa de Serviço (DoS – Denial of Service) e Invasão

Existem apenas dois tipos de ataques que um sistema pode sofrer. O primeiro é o Denial of Service (DoS) ou Recusa de serviço. Esse ataque consiste em inundar a máquina-alvo com dezenas de pacotes de informação, fazendo com que ela não consiga processar a todos e consuma toda a sua memória, paralisando-a. Esse ataque apenas causa danos temporários, como tirar o servidor do ar,

mas não fornece acesso aos ficheiros. É como se um ladrão, vendo que não vai conseguir roubar um carro, fure os quatro pneus. É chato, demora para trocar os pneus, mas pelo menos o reprodutor e os documentos do carro não foram levados. Já a invasão é diferente. Consiste em procurar e utilizar alguma falha do sistema contra ele próprio. Ou então instalar programas residentes na memória (trojans ou sniffers) para que monitorem todo o tráfego de senhas e forneçam acesso a ficheiros importantes.

Protocolos, ferramentas de rede e footprinting

Protocolos

Esse capítulo foi feito para quem quer entender um pouco mais sobre protocolos de rede e como eles funcionam. Se você não tem nenhum interesse em dados teóricos, pule o capítulo. Protocolos são programas e devem ser instalados em componentes de rede que precisam deles. Computadores só podem comunicar-se entre si se utilizarem o mesmo protocolo. Se o protocolo usado por um computador não for compatível pelo usado em outro, eles não podem trocar informações. Uma variedade de protocolos está disponível para uso em sistemas de rede fechados (como Novell Netware).

Tipos de protocolos

Dois tipos de protocolos existem hoje: abertos e específicos.

Protocolos Abertos

Protocolos abertos são protocolos feitos para o padrão da indústria. Eles se comunicam com outros protocolos que utilizam o mesmo padrão. Um protocolo aberto não possui dono e todos os sistemas podem fazer implementações livremente. Um óptimo exemplo do que é um protocolo aberto é o TCP/IP (Transfer Control Protocol/Internet Protocol). Ele é composto por muitos outros protocolos e está implementado em muitos sistemas (como Macintosh, Windows, Linux, Unix, etc...). O TCP/IP é o protocolo padrão da Internet.

Protocolos Específicos

Protocolos específicos são feitos para ambientes de redes fechados e possuem donos. Como é o caso do IPX/SPX que foi desenvolvido especificamente para a estrutura Novell Netware.

Tipos de transmissão de dados

Protocolos roteáveis, permitem a transmissão de dados entre diversos segmentos de uma rede. O problema é que o grande volume de certo tipo de tráfego (como executar uma aplicação multimédia pesada) deixa a velocidade de conexão muito lenta. A quantidade de tráfego gerada em uma rede, pode ser de três tipos: Unicast, Broadcast e Multicast.

Unicast

Numa transmissão unicast, uma cópia separada dos dados são enviados de sua origem para cada computador cliente que os requeste. Nenhum outro computador na rede precisa processar o tráfego gerado. No entanto, numa rede com muitos computadores o unicast não é muito eficiente pois o computador de origem terá que transmitir múltiplas cópias dos dados (resultado, ficará lento). O unicast é bom de ser usado apenas em pequenas redes.

Broadcast

Esse é o tipo de transmissão preferido de quem gosta de um Denial of Service. Nesse tipo de transmissão, os dados são enviados apenas uma vez mas para toda a rede. Esse processo não é muito eficiente pois faz a velocidade cair bastante já que todos os computadores irão receber os dados. Mesmo os hosts que não fizeram o pedido receberão os dados. Somente não irão processá-los. Esse método é utilizado no ataque de smurf, em que é enviado um broadcast para diversos endereços IP e o endereço de origem (que deveria ser o IP de quem enviou) é modificado para o da vítima. Resultado: centenas de máquinas mandarão milhares de unicasts para um pobre coitado.

Multicast
É uma mistura dos dois. É enviada apenas uma cópia dos dados e somente os computadores que fizeram o pedido os recebem, assim evitando de se causar um tráfego muito intenso e consequentemente um congestionamento na rede. Muitos serviços de Internet usam multicast para se comunicar com computadores clientes (quando se diz cliente, é o computador que faz o pedido, que espera uma resposta). Inclusive é nesse tipo de comunicação que se baseia o protocolo IGMP.

NetBios

A interface NetBIOS (NetBEUI) foi um dos primeiros protocolos disponíveis para uso em redes compostas de computadores pessoais. Como o próprio nome diz, o NETwork Basic Input Output System, foi designado para ser um protocolo eficiente e pequeno para uso em redes caseiras não roteadas de cerca de no máximo 200 computadores.

Actualmente o NetBIOS é usado mais exclusivamente em pequenas redes não roteadas podendo ou não estar rodando em vários sistemas operacionais. A implementação NetBIOS do Windows é chamada de NetBEUI. As suas vantagens incluem:

- Grande velocidade de transferência
- Nenhuma necessidade de configuração
- Compatibilidade com praticamente todos os sistemas operacionais, inclusive o Linux (ustilizando o Debian).

A única desvantagem é que o NetBIOS não suporta roteamento. Trocando em miúdos: o máximo que se consegue invadir utilizando esse protocolo é o computador do seu primo ou da sua namorada que utilizam o mesmo provedor que você. Se for um provedor diferente, esqueça, como foi explicado anteriormente). Outro problema: a estrutura de segurança do Net BIOS é extremamente pobre. Facilmente podemos quebrar as senhas utilizadas (usando brute force). Além do Shadow Scan já citado anteriormente, o NAT (NetBIOS Auditing Tool) também é uma óptima ferramenta para fazê-lo.

Alguns bugs também são facilmente encontrados, como a má configuração do IPC$ do Windows NT. Aliás, pense um pouco nesta pergunta: porquê o NetBIOS do WindowsNT possui a partilha IPC$ padrão, o Windows9x possui o $printer (que possibilita cair no Windows\System utilizando partilha de uma impressora) e o Linux não possui nenhum desses? Qual o objectivo dessas partilhas? Fiz essa pergunta a um formando de Ciências da Computação e ele não soube me responder. Existem duas respostas, uma longa e uma curta. A longa deixarei para a análise pessoal de cada um. Já a curta é simples: o Linux é bem mais seguro.

Para se resolver nomes NetBIOS, podem ser utilizadas três maneiras:

1. Ficheiro LMHOSTS
2. Broadcast
3. WINS

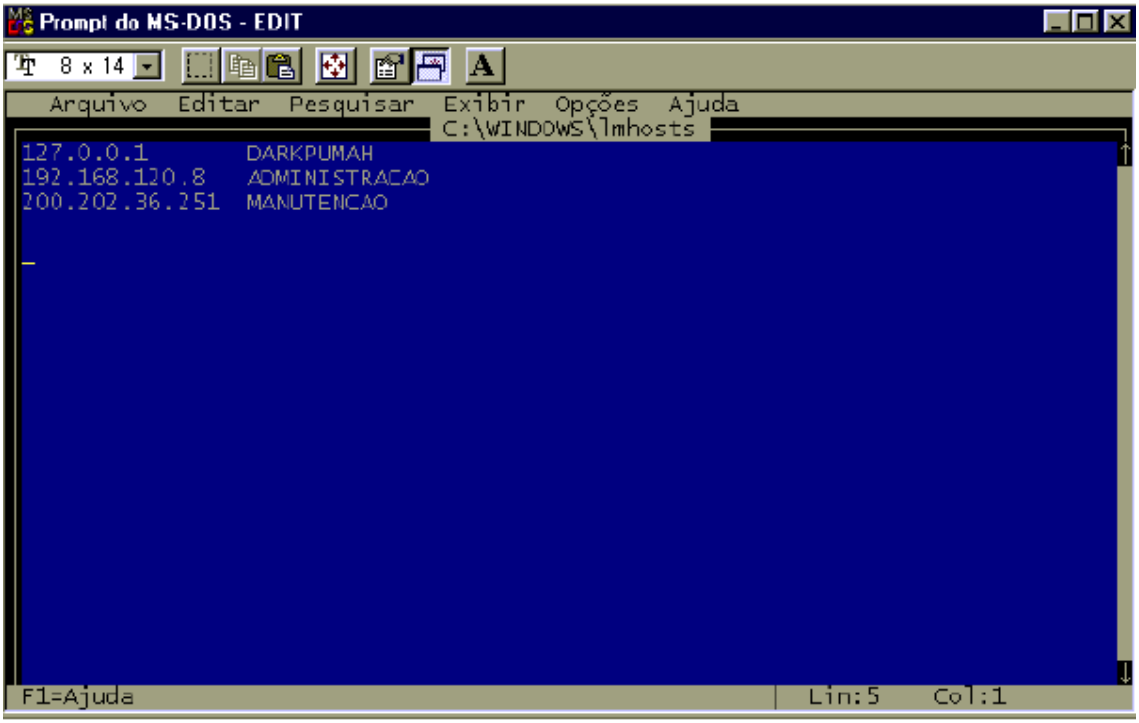
Vamos analisar o método do LMHOSTS que creio ser o mais simples de todos. Ele consiste na tradução de endereços NetBIOS em endereços IP, somente configurando o ficheiro lmhosts. O ficheiro não possui extensão e pode ser encontrado nos directórios dos seguintes sistemas:
UNIX ./etc

Mac OS X System Folder
Windows 9X c:\windows (ou onde o Windows foi instalado)
Windows NT c:\winnt\System32\Drivers\Etc

O ficheiro deve ser criado utilizando a seguinte sintaxe:
<endereçoIP> espaço <nomeNetBIOS>

Esse é o modo mais simples de criação do ficheiro. Podem-se adicionar comentários utilizando o carácter #. Atenção: não confundir ficheiro LMHOSTS com HOSTS (visto em TCP/IP).

Um exemplo de ficheiro LMHOSTS:



Nesse exemplo criamos um ficheiro simples, ligando três endereços IP a nomes NetBIOS. Observe que o primeiro é o endereço de local (o chamado loopback). Leia mais sobre endereço na secção sobre TCP/IP.

Há dois tipos de ambiente NetBIOS: Único e grupo. Um nome único deve ser único através da rede (um utilizador por exemplo). Um nome de grupo não precisa ser único e processa informações de todo um grupo de trabalho. Cada nó NetBIOS mantém uma tabela de todos os nomes possuídos por ele. A convenção do nome NetBIOS possibilita que se crie nomes com 16 caracteres. A Microsoft, entretanto, limita esses nomes para 15 caracteres e usa o 16º carácter como um sufixo NetBIOS. Um sufixo NetBIOS é usado pelo software de rede da Microsoft para identificar o serviço que está a ser executado.

Nota: SMB e NBT (NetBIOS sobre o TCP/IP, alguns o chamam apenas de SMB por TCP/IP) funcionam de modo muito parecido e ambos usam as portas 137, 138, 139. A porta 137 é o nome

NetBIOS por UDP. A porta 138 é o datagrama NetBIOS por UDP. E a porta 139 é a sessão NetBIOS por TCP. Mas o NBT costuma usar a porta 445 também.

IPX/SPX

Internetwork Packet Exchange / Sequenced Packet Exchange (IPX/SPX) é um protocolo desenvolvido especificamente para a estrutura Novell NetWare. O IPX define o endereçamento da rede NetWare e o SPX fornece segurança e confiabilidade ao IPX. (O SPX é como aqueles homens que só se sentem seguros ao lado da esposa). Para comparação, o IPX é como se fosse o IP do protocolo TCP/IP (que será abordado mais adiante). O IPX/SPX possui as seguintes características:

- São usados com servidores NetWare
- São roteavéis, permitem que os computadores e num ambiente de rede trocam informações através de segmentos.

Apple Talk

Protocolo criado pela Apple para utilização em redes Macintosh para a partilha de ficheiros e impressoras. É componente específico, ou seja não é um padrão do mercado. As duas principais características do Apple Talk são:

1. Possibilita clientes Macintosh acederem servidores WindowsNT

2. É roteável. (pode se comunicar com redes externas, tal como o IPX/SPX e o TCP/IP)

TCP/IP

Sem dúvida o melhor dos protocolos. Quando alguém chega a mim e diz que se converteu ao TCP/IP, creio que sinto o mesmo prazer de um crente que consegue levar o amigo à sua igreja. Diferente dos outros protocolos vistos aqui, o TCP/IP na verdade é um conjunto de muitos protocolos. Usando uma arquitectura cliente-servidor quase perfeita, esse conjunto de protocolos possibilita praticamente todo tipo de sistema operacional e rede de se comunicarem entre si, possibilitando até a criação da Internet. Ora, como seria possível um monte de computadores utilizando Macintosh, Unix, Linux e Windows comunicarem-se sem maiores problemas? Não, não é um filme de Hollywood e muito menos um sonho distante. É a tecnologia a nosso serviço. E o melhor de tudo, é um protocolo aberto. Para começarmos o nosso estudo sobre os protocolos que compõem o TCP/IP, analisemos um a um os mais importantes deles. Ou em outras palavras, os que mais iremos utilizar. Não dá para vermos todos pois além de serem muitos, têm de ser estudados a fundo. Apenas darei uma noção.

IP

O IP (Internet Protocol) é o responsável por rotear e entregar os pacotes contendo as informações que serão enviadas. O endereço IP contém um cabeçalho aonde estão indicados os endereços de redes e de hosts. Esse endereço é representado por quatro bytes separados por pontos. Por exemplo:

200.202.36.251

As três primeiras partes (200.202.36) indicam o endereço da rede. Ou seja, provavelmente todos os hosts dessa rede começam com esse endereço. O que vai mudar de host para host é a parte final do endereço (251). Claro que isso não é uma regra, existem redes gigantescas em que essas

propriedades podem mudar. Para saber se qual o endereço de rede e o endereço de host de uma rede, verifique a **máscara de sub-rede.**

A máscara de sub-rede (subnet mask) nos informa quais áreas do ip são mutáveis (usadas por hosts) e quais não mudam. Exemplo: **255.255.255.0**

O que isso significa? Quando uma área da máscara de sub-rede tiver o número 255, significa que aquela área é imutável e quando for 0 a área pode mudar. Achou difícil? Não é. Preste atenção: observando o endereço acima, dá para notarmos o quê? Que somente a última partedo endereço IP está com o zero. Supondo que o endereço IP de uma máquina da rede seja 200.131.16.1. Provavelmente existirão hosts com esses endereços:

200.131.16.2

200.131.16.3

200.131.16.4

200.131.16.5

Mas não existirão máquinas com esses endereços:

200.131.63.1

200.131.65.6

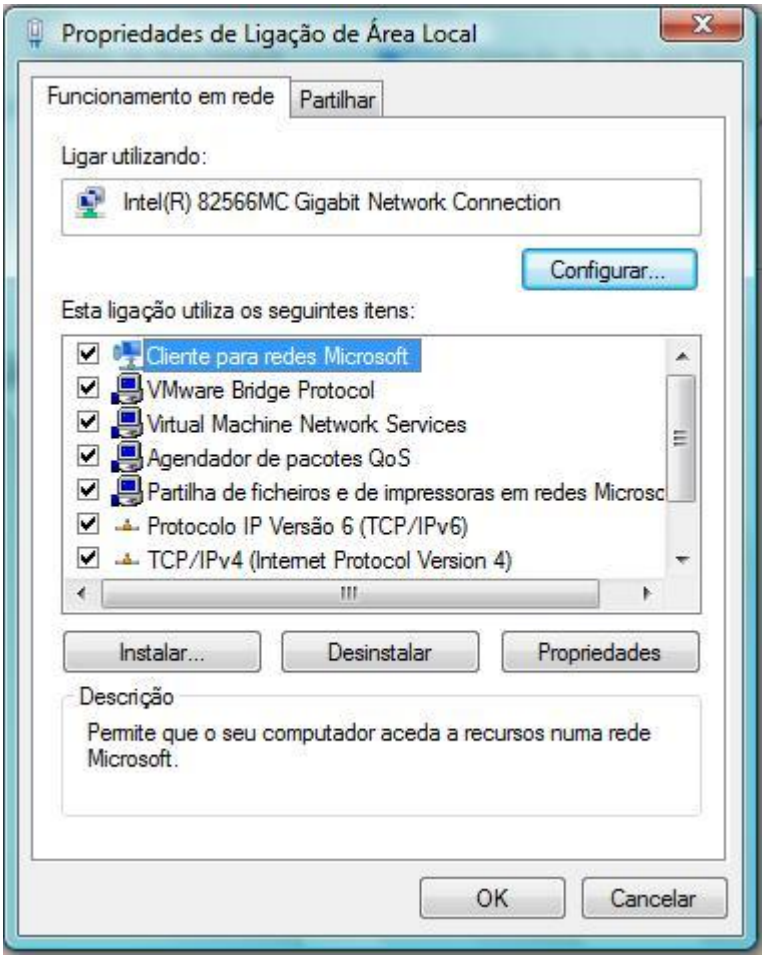
200.131.19.4

200.131.33.66

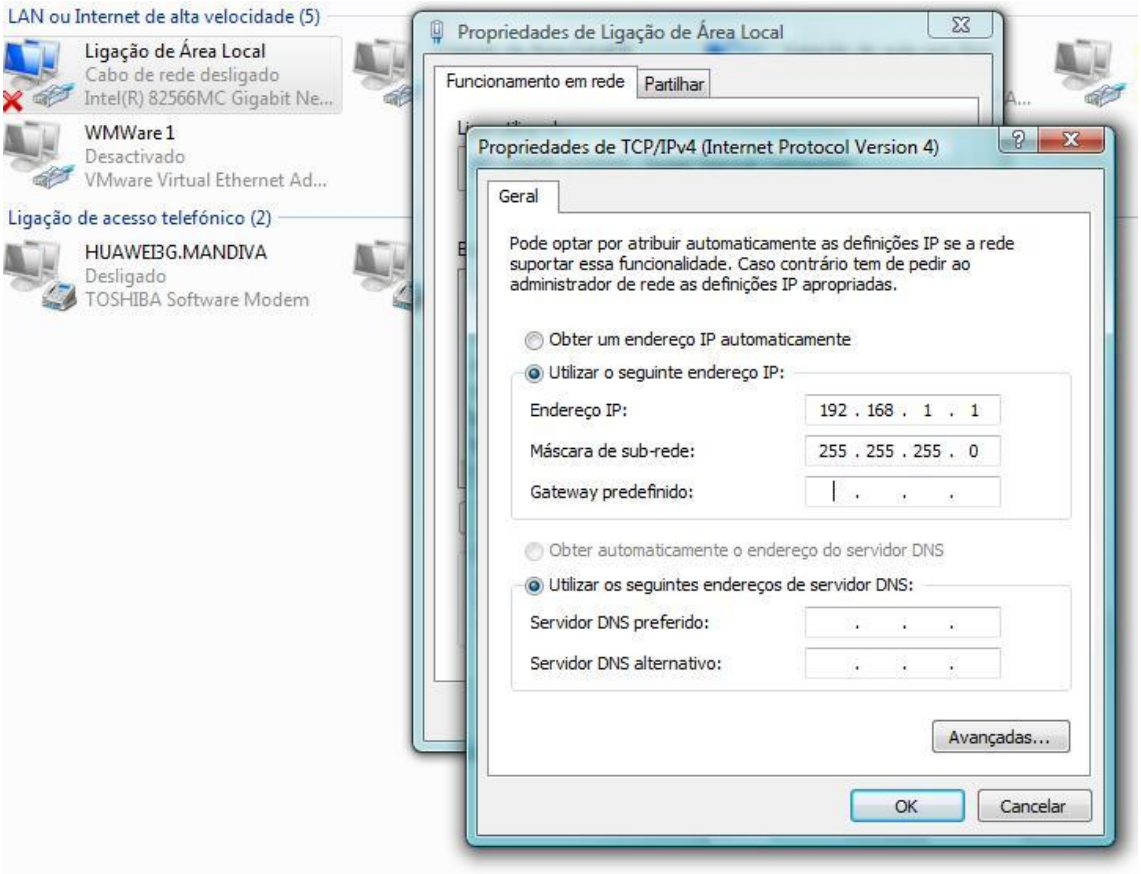
Porquê? Porque como a máscara de sub-rede foi configurada para 255.255.255.0, somente o último byte do ip pode ser alterado. Agora, se a máscara for mudada para 255.255.0.0, os endereços ip acima seriam aceitos pois os últimos dois bytes (as duas últimas áreas separadas por pontos) podem ser mudados. Nas propriedades de TCP/IP (que variam de um sistema operacional para o outro) você encontra a máscara de sub-rede.

No Windows Vista, siga os seguintes passos:

1. Clique em Iniciar e vá em Painel de Controlo;
2. Clique em centro de rede e partilha;
3. Clique em gerir ligações de rede;
4. Seleccione a ligação de rede que pretende verificar a mascara de sub-rede;
5. Clique no menu de atalho do rato (botão direito) e seleccione propriedades;



6. Seleccione a versão do protocolo TCP/IP (IPv4 neste caso) e clique em propriedades;



7. Agora seleccione “utilizar o seguinte endereço IP” e coloque como teste o endereço 192.168.1.1;
8. Escreva a máscara de sub-rede desejada abaixo;
9. Não se esqueça depois de que se anteriormente a opção de “obter um endereço IP automaticamente” estava habilitada, habilite-a antes de sair.

Propriedades do protocolo TCP/IP

No endereço IP os números podem variar de 0 a 255, mas geralmente em hosts são utilizados apenas de 1 a 254. O 0 e o 255 são usados apenas para a máscara de sub-rede.

Portas

Se você quisesse colocar um servidor web e um servidor de jogos num host tendo um só endereço IP seria impossível. Como o cliente saberia identificar qual dos servidores precisa se conectar? Para isso criaram as portas. Elas identificam conexões utilizando números de 0 a 65536. Alguns serviços já possuem até suas portas padrões, como é o caso do Telnet (porta 23) e do FTP (porta 21). Para saber quais serviços existem em um servidor, leia a secção sobre scanners para saber como scannear portas.

DNS

Nosso próximo passo no estudo do TCP/IP é o Domain Name Server (DNS) ou Servidor de Nome de Domínio, em português. A função dessa maravilha é extremamente útil. Já imaginou se você tivesse que decorar o endereço IP de todas as páginas que visita na Internet? No máximo uns 10 você decoraria, mas e o resto? Para acabar com esse problema surgiu o DNS. A sua função é procurar numa base de dados um nome que corresponda a um IP. Quando digitamos www.yahoo.com por exemplo, não precisamos saber o endereço IP.O DNS do nosso provedor de acesso vai verificar esse nome em seu banco de dados e se encarregar de nos direccionar ao IP encontrado.

Nós mesmo podemos configurar e ligar alguns nomes a endereços IP. O método mais fácil de se fazê-lo é utilizar o ficheiro HOSTS. O processo é o mesmo do LMHOSTS do NetBIOS, e o ficheiro é encontrado no mesmo local. O interessante do HOSTS é que você pode gozar com os seus amigos, direccionando endereços como www.fbi.gov para o IP de alguma página da web hackeada ou até seu endereço IP local e gabar-se de que invadiu o FBI.

SMTP

O Simple Mail Transfer Protocol é o protocolo responsável por entregar mensagens de e-mail a um destinatário. Toda vez que seus e-mails são enviados, um servidor smtp se encarrega de levá-los ao seu destino. Esse servidor geralmente se aloja na porta 25. O interessante do SMTP é que ao contrário do POP3 (que será a seguir), não é necessária senha para enviar um e-mail. Eu posso abrir o Microsoft Outlook e mandar e-mails como se fosse Barack Obama ou Tom Cruise. A falta de segurança no envio de mensagens é o ponto de partida para a facilidade de se enviar e-mails

anónimos (como visto em anonimidade). O SMTP ainda permite anexar à uma mensagem de texto conteúdos binários (programas por exemplo), utilizando o MIME.

POP3

Outro protocolo de mensagens, só que agora é o responsável por o recebimento dessas mensagens. O POP3 já necessita de senhas para poder habilitar o acesso dos utilizadores às suas caixas postais, além de saber "re-montar" os ficheiros enviados em formato MIME como SMTP. O POP3 geralmente se localiza na porta 113. Uma grande desvantagem dele é que fica muito fácil fazer um ataque de brute force para tentar descobrir as senhas, já que a maioria dos servidores possui falhas que possibilitam softwares maliciosos de serem executados.

TELNET

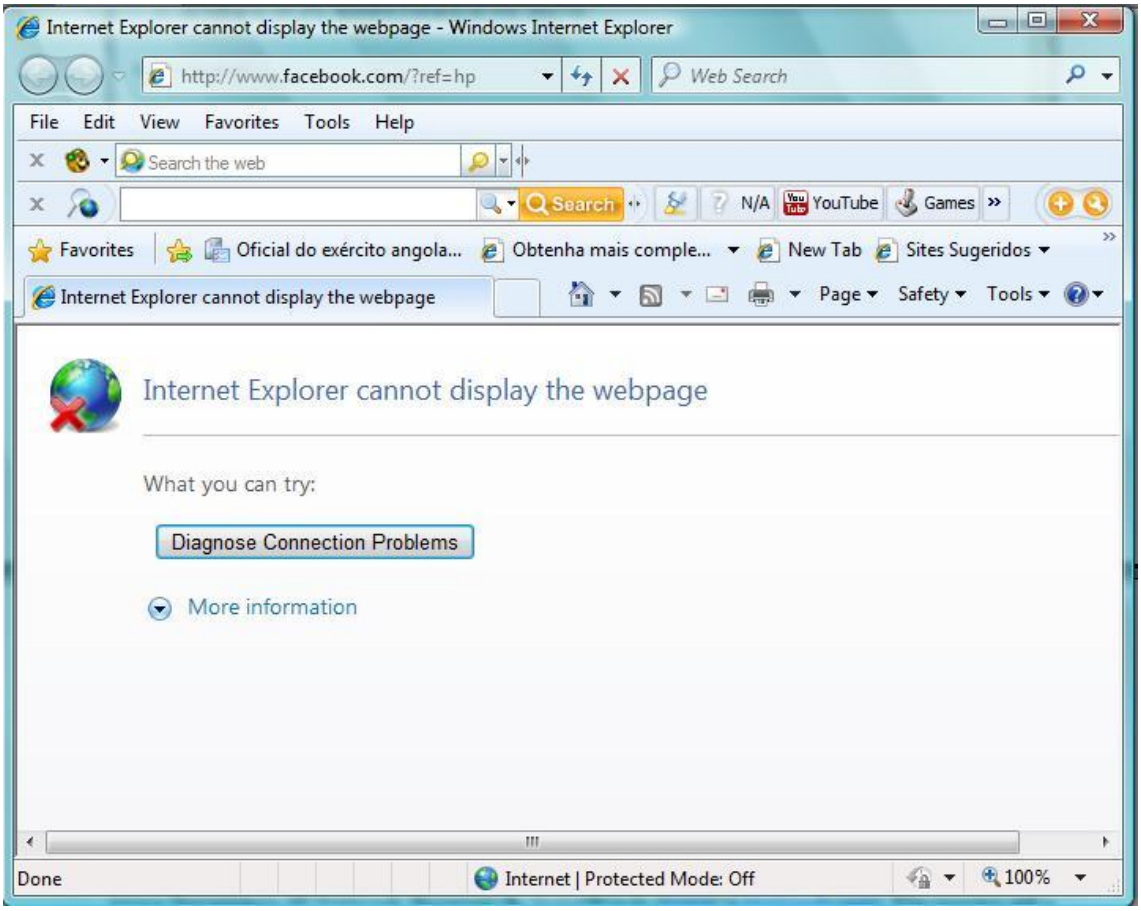
Telnet, ou terminal remoto é um modo de se aceder remotamente sistemas como se você os estivesse operando localmente. Por exemplo: utilizando o telnet (e um trojan instalado) podemos ter acesso ao MS-DOS de qualquer um. Do mesmo modo que poderíamos digitar comandos para listar, copiar e apagar dados, conectados a outro computador também podemos. Na verdade, todos os trojans são clientes telnet. Apenas são disfarçados com botõezinhos bonitos pois geralmente quem precisa de trojans para invadir sistemas são pessoas que não possuem um bom conhecimento de segurança. Se você encontrar alguma porta activa em algum sistema (qualquer uma, seja de trojan, SMTP, POP3, etc...), pode se conectar a ela por telnet. Resumindo, se você souber usar bem telnet não precisa mais de outros programas no computador. Ele acede servidores utilizados pelos browsers (como Netscape e Internet Explorer), clientes de E-mail, IRC, absolutamente tudo. Leia sobre o cliente telnet do Windows no capítulo seguinte.

FTP

File Transfer Protocol é o seu nome real. O protocolo de transferência de ficheiros serve única e exclusivamente para ser um banco de software. Não se pode executar programas remotamente como no caso do telnet, apenas pegar e colocar ficheiros. Desde a criação da Internet, o ftp é largamente usado. Uma das suas vantagens é, como ele é usado somente para transferências de ficheiros, a sua velocidade pode chegar a ser muito maior do que apanhar ficheiros em http (será visto mais adiante). No próximo capítulo você aprenderá os comandos básicos de um cliente FTP e como manipular os ficheiros dentro deste.

HTTP

Esse sem dúvida é conhecido por muitos. Afinal, quem nunca viu na frente do endereço de uma homepage esse nome? http://www.altavista.com/. O Hyper Text Transfer Protocol é o protocolo responsável de transmitir textos, imagens e multimédia na Internet. Sempre que você abre um website (mesmo que ele só contenha textos), você está usando esse protocolo. Achei interessante comentar sobre ele para que se entenda melhor como a Internet não funciona isolada com um só protocolo. HTTP, FTP, TELNET e os outros muitas vezes trabalham em conjunto e nem percebemos. Quando você for baixar um ficheiro, preste atenção no link. É muito provável que de uma página navegada por HTTP, se envie a um servidor FTP.



SNMP

Simple Network Management Protocol. Algo como protocolo simples para gerir a rede. E é exactamente isso o que ele faz. Usando o SNMP você pode obter informações detalhadas sobre contas de utilizador, equipamentos de rede, portas e serviços abertos e muito mais. A má configuração desse protocolo (deixando o seu status como público principalmente). Use a óptima ferramenta IP Network Browser da SolarWinds (**www.solarwinds.net**). É recomendado a correcta configuração do SNMP ou a desactivação desse serviço.

Screenshot do IP Network Browser

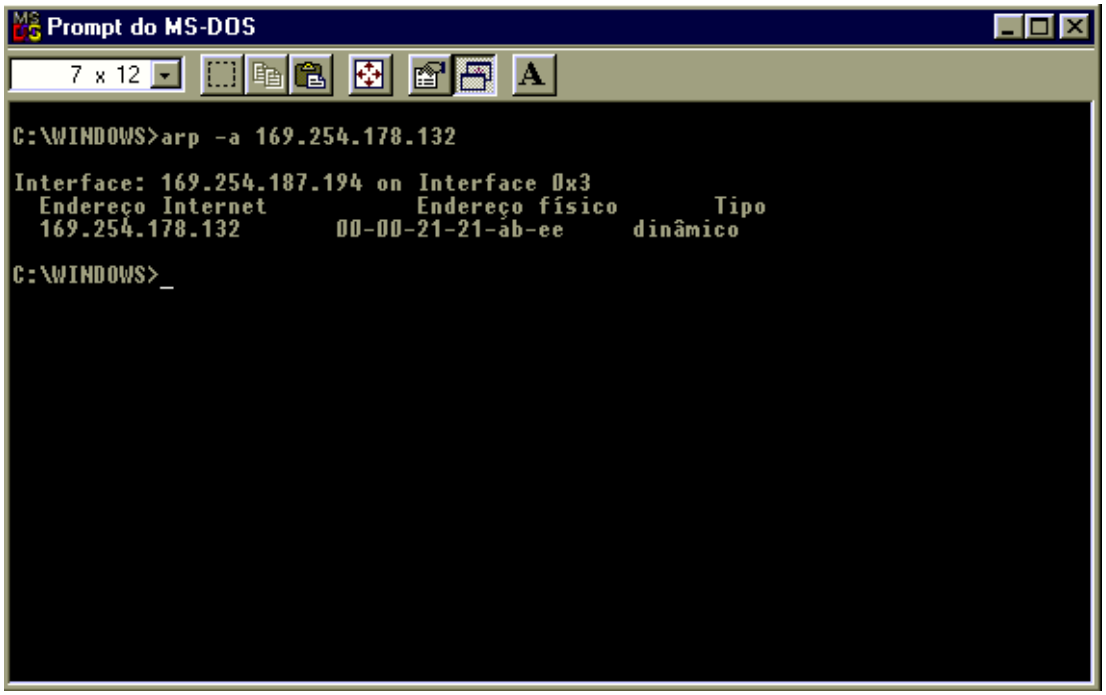
Ferramentas TCP/IP

Utilitários úteis

Existem muitos programas que vêm com o Windows e que possuem grande utilidade. A grande maioria deles também funciona em Linux e Unix (o que muda um pouco é apenas a sintaxe). Agora que já passei uma noção do que é o TCP/IP e como funcionam muitos de seus protocolos, ficará mais fácil de aprendermos sobre as ferramentas essenciais de rede. Será apresentada a ferramenta, uma tela de ilustração e sua sintaxe de uso. Como as ferramentas existentes são muitos, veremos apenas as mais importantes para nós.

Arp

Permite realizar consultas e alterações na tabela de mapeamento entre endereços IP e endereços MAC do cache ARP.



arp -a [*endereçoIP*] [**-N** *IPInterface*]
arp -s *endereçoIP endereçoMAC* [*IPInterface*]
arp -d *endereçoIP* [*IPInterface*]

Parâmetro	**Descrição**
Endereço IP	Especifica o endereço IP a resolver ou alterar.
Endereço MAC	Especifica o endereço MAC a acrescentar ao cache do ARP. O endereço MAC é composto por 6 bytes (expressos em notação hexadecimal) separados por hífen.
IPInterface	Especifica o endereço IP da placa de rede cuja tabela ARP deverá ser alterada. Por default, a primeira interface disponível será utilizada.

-a: Exibe as entradas de cache do ARP. Se o *endereço IP* tiver sido especificado, mostra somente a entrada referente a esse endereço.

-g: O mesmo que **–a**.

-d: Exclui do cache do ARP o host especificado por *endereço IP* . Se *IPInterface* for especificado, exclui o host do cache da placa de rede indicada por *IPInterface.*

-s: Acrescenta ao cache do ARP uma associação entre *o endereço MAC* e *endereço IP* . Se *IPInterface* tiver sido especificado, acrescenta a associação no cache do ARP da placa de rede indicada por *IPInterface.*

-N: Especifica o endereço IP da placa de rede à qual o comando se aplica.

FTP

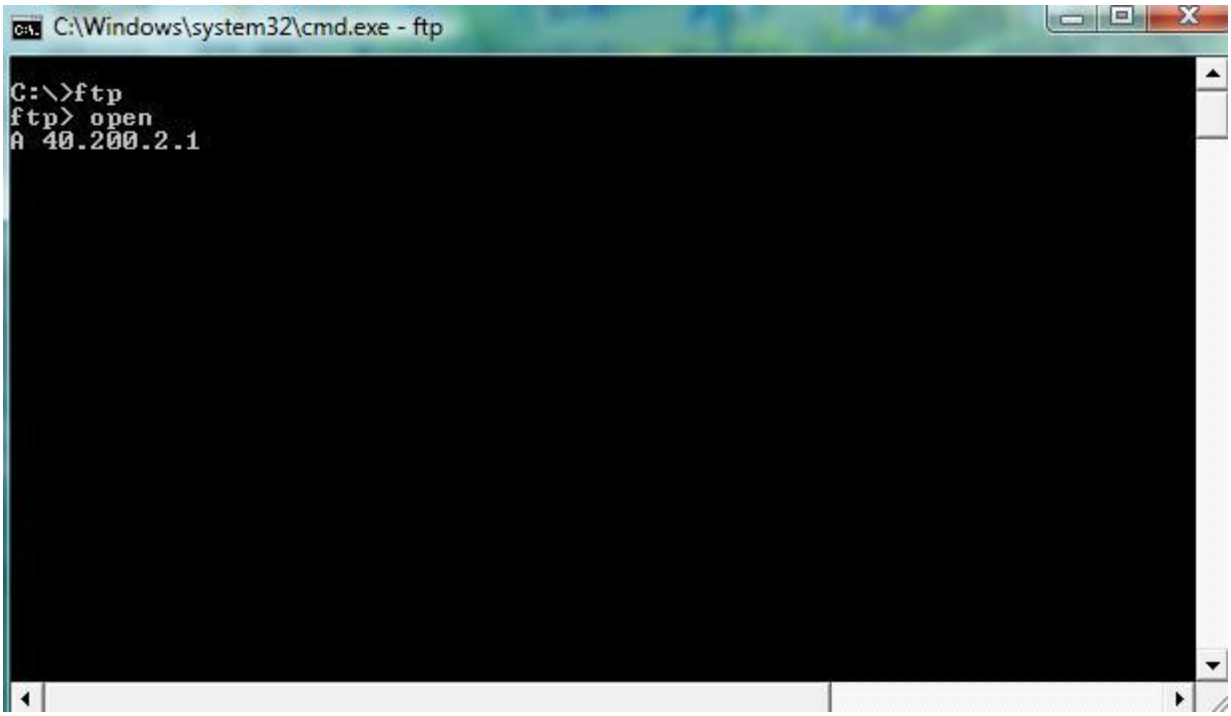


Figura: Screenshot de uma sessão ftp.

Transfere ficheiros de ou para um computador remoto.

ftp [**-v**] [**-d**] [**-i**] [**-n**] [**-g**] [**-s** : *nomearq*] [**-a**] [**-w** : *tamanho*] [*computador*]

O servidor ftp solicitará um utilizador e a senha correspondente.
A maioria dos servidores FTP pode ser acedida por utilizadors não cadastrados, utilizando o utilizador *Anonymous.*
Esse utilizador não requer senha, mas muitos servidores solicitam como senha um endereço de e-mail.

Opção **Descrição**

-v	Elimina as mensagens de resposta do servidor.
-d	Activa o modo de depuração, exibindo os comandos FTP enviados e recebidos.
-i	Desactiva a confirmação para a transferência de cada ficheiro em operações com múltiplos ficheiros.
-n	Elimina o login automático na conexão inicial.
-g	Desactiva o *globbing* , que permite o uso de caracteres de máscara (*, ?) em nomes de ficheiros.
-s	Especifica um ficheiro de texto contendo os comandos FTP a serem executados automaticamente.
-a	Utiliza qualquer placa de rede para estabelecer a conexão com o servidor FTP.
-w	Define o tamanho do buffer de transferência (o default é de 4 KBytes).
	Computador Nome do servidor FTP ou endereço IP. Deve ser o último parâmetro da linha de comando.
	A seguir está a sintaxe dos comandos interactivos do protocolo FTP. Esses comandos são utilizados de acordo com cada sistema e geralmente já com a conexão online.

Comando Descrição

***append*:** Acrescenta informações a um ficheiro.

***ascii*:** Indica que a transferência de ficheiros será feita no modo de texto (ficheiros apenas de texto, como TXT ou HTML).

***bell*:** Emite aviso sonoro ao término do comando.

binary: Indica que a transferência de ficheiros será feita no modo binário. (utilizado para ficheiros não-texto, como fotos, programas e vídeos).

bye: Fecha a sessão FTP e sai do programa FTP.

***cd*:** Selecciona um novo directório de trabalho no computador remoto.

close: Fecha a sessão com um servidor FTP.

debug: Activa/desactiva o modo de depuração.

delete: Elimina ficheiros no computador remoto.

***dir*:** Lista o conteúdo de um directório remoto.

***disconnect*:** Fecha a sessão com um servidor FTP.

***get*:** Copia um ficheiro de um computador remoto para o computador local

***glob*:** Activa/desactiva o uso de caracteres de máscara (*,?) em nomes de ficheiros.

***hash*:** Activa/desactiva a impressão de "#" par a cada buffer transferido.

***help*:** Exibe help on-line de um comando FTP. Se o comando não for especificado, exibe a lista dos comandos disponíveis.

***Lcd*:** Selecciona um novo directório de trabalho no computador local.

***literal*:** Envia uma linha de comando directamente ao servidor FTP.

***ls*:** Lista o conteúdo de um directório remoto.

***mdelete*:** Elimina múltiplos ficheiros no computador remoto.

***mdir*:** Lista o conteúdo de múltiplos directórios no servidor remoto

***mget*:** Copia múltiplos ficheiros do computador remoto para o computador local.

***mkdir*:** Cria um directório no computador remoto.

***mls*:** Lista o conteúdo de múltiplos directórios no servidor remoto

***mput*:** Copia múltiplos ficheiros do computador local para o computador remoto.

***open*:** Estabelece uma conexão com um servidor FTP.

***prompt*:** Activa/desactiva a confirmação para a transferência com muitos ficheiros

put: Copia um ficheiro do computador local para um computador remoto (*upload*).

***pwd*:** Exibe o directório corrente no computador remoto.

***quit*:** Fecha a sessão FTP e sai do programa FTP.

***quote*:** Envia uma linha de comando directamente ao servidor FTP.

***recv*:** Copia um ficheiro de um computador remoto para o computador local

***remotehelp*:** Exibe help on-line para comandos directos do servidor FTP.

***rename*:** Renomeia um ficheiro.

***rmdir*:** Remove um directório no computador remoto.

***send*:** Copia um ficheiro do computador local para um computador remoto (*upload*).

***status*:** Exibe informações sobre a configuração do cliente FTP.

***trace*:** Activa/desactiva o modo trace (exibição de todas as acções executadas).

***type*:** Define ou exibe o tipo de transferência de ficheiro (ASCII ou binary).

user: Especifica um novo utilizador para o computador remoto.

IPCONFIG

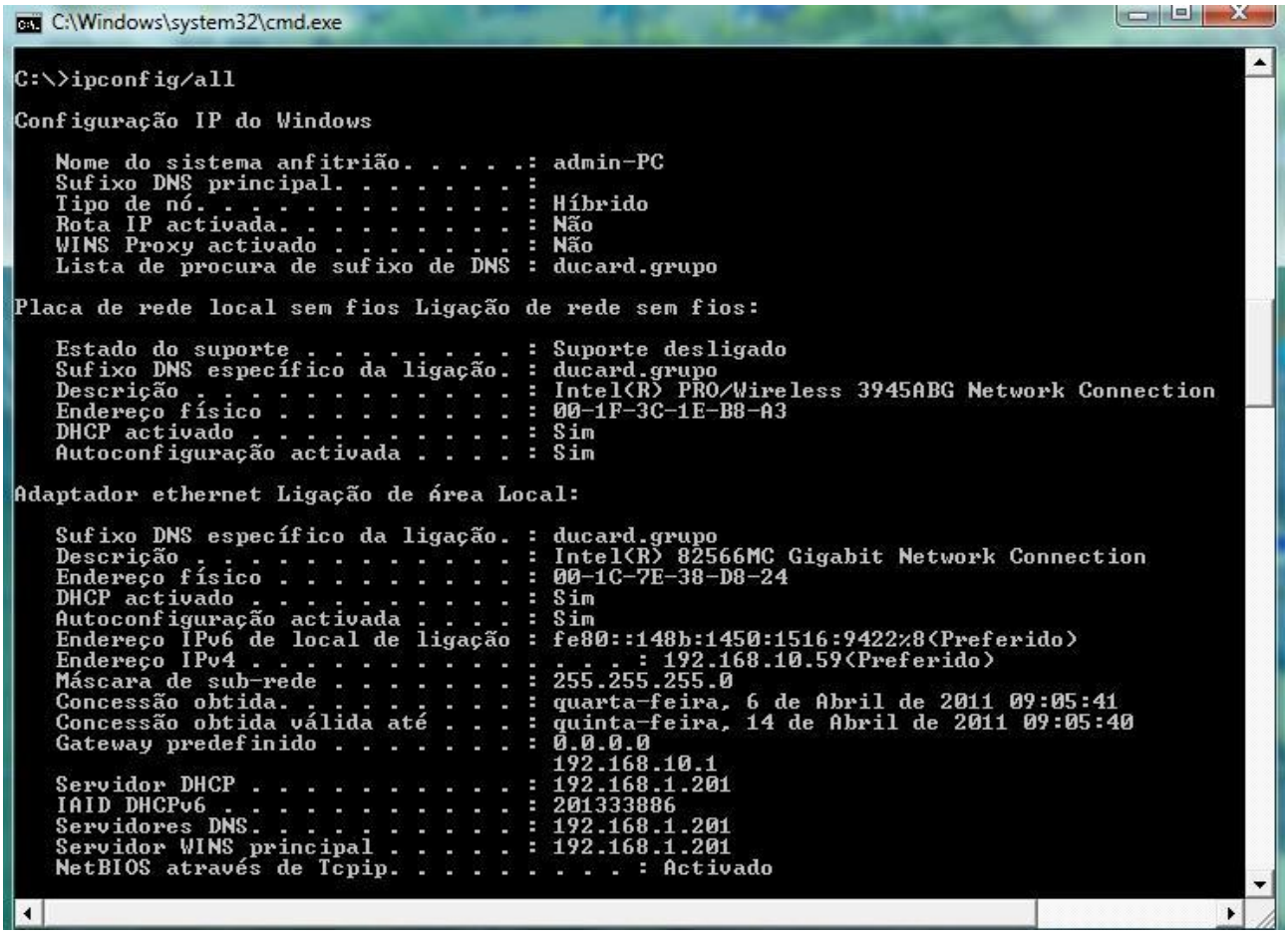


Figura: Screenshot usando o ipconfig

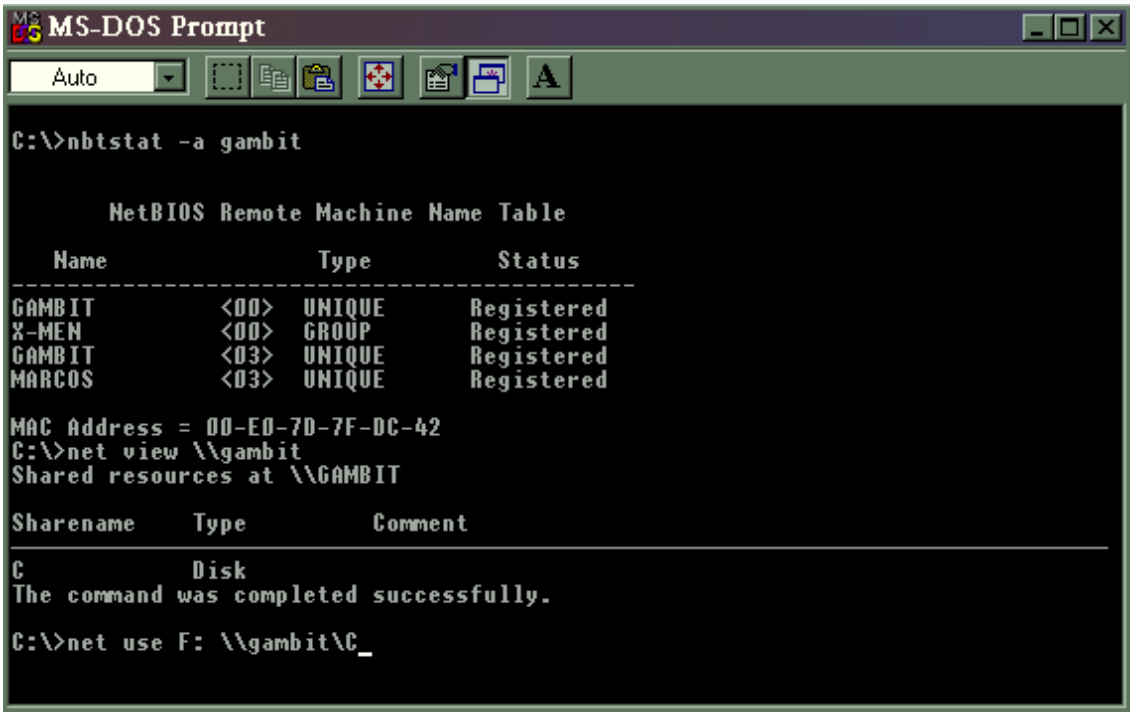
Exibe a configuração do protocolo TCP/IP. Sem nenhum parâmetro, exibe os valores do endereço IP, máscara de sub-rede e *default gateway* para cada placa de rede instalada.

ipconfig [/? | /all | /release [*adaptador*] | /renew [*adaptador*]]

Opção	Descrição
/all	Exibe informações detalhadas de IP para as placas de rede instaladas. Além do endereço IP, da máscara de sub-rede e do *default gateway*, são exibidos também os endereços dos servidores DHCP, WINS e DNS para cada placa de rede instalada.
/release	Liberta o endereço IP obtido para uma placa de rede através de um servidor DHCP. Se a placa de rede não for especificada, liberta os endereços IP obtidos para todas as placas de rede do computador.
/renew	Renova um endereço IP obtido para uma placa de através de um servidor DHCP. Se a placa de rede não for especificada, renova os endereços IP obtidos para todas as placas de rede instaladas no computador.
adaptador	Específica uma placa de rede na renovação ou libertação de um endereço

IP obtido através de um servidor DHCP. Para saber os nomes associados às placas de rede, utilize o comando Ipconfig sem parâmetros.

Nbstat



Exibe estatísticas de protocolos e conexões TCP/IP usando NetBIOS sobre TCP/IP.

nbtstat [**-a** *hostname*] [**-A** *endereço IP*] [**-c**] [**-n**] [**-R**] [**-r**] [- **RR**] [**-S**] [**-s**] [*intervalo*] [-?]

Opção	Descrição
-a	Exibe a tabela de nomes NetBIOS registrados num computador (determinado pelo *hostname*).
-A	Exibe a tabela de nomes NetBIOS registrados num computador remoto (determinado pelo endereço IP).
-c	Exibe a lista de nomes NetBIOS (e endereços IP) do cache NetBIOS do computador.
-C	Exibe a lista de nomes NetBIOS (e endereços IP) do cache NetBIOS do computador para cada placa de rede.
-n	Exibe os nomes NetBIOS e os serviços registados no computador local.
-r	Exibe os nomes NetBIOS resolvidos através de WINS ou mensagens *broadcast* .

-R Recarrega o cache de nomes NetBIOS utilizando as entradas no ficheiro LMHOSTS com o parâmetro #PRE.

-RR Envia pacotes de liberação de nomes ao WINS e actualiza a lista de nomes.

-s Exibe as sessões TCP/IP estabelecidas no computador (usando nomes de host do ficheiro HOSTS).

-S Exibe as sessões TCP/IP estabelecidas no computador (usando endereços IP).

intervalo Especifica o tempo (em segundos) de pausa intermediária para re-exibir as informações seleccionadas. Pressione Ctrl+C para interromper a exibição.

Ping

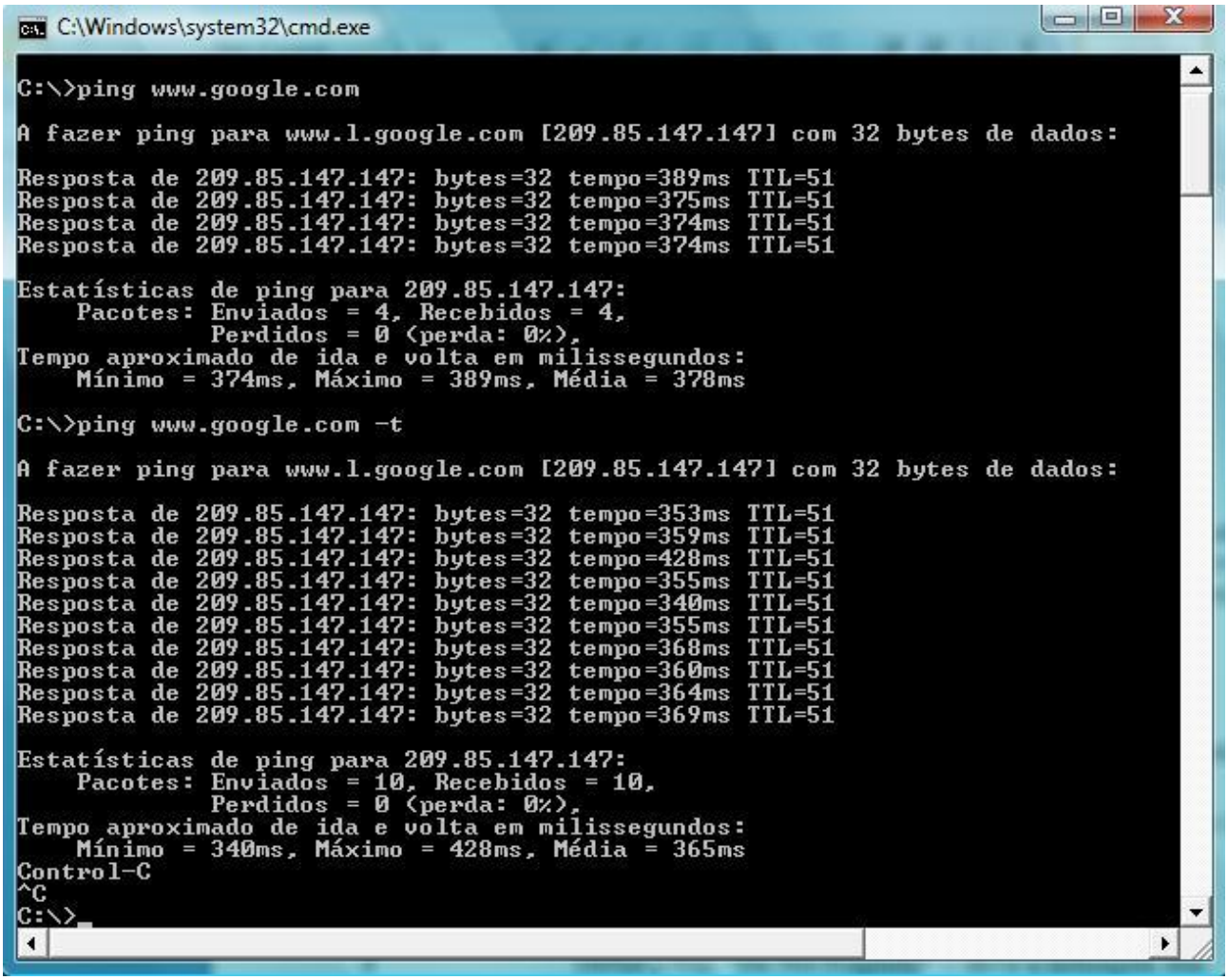


Figura: Screenshot do utilitário Ping

Utilizado para testar a conexão com outro host (trata-se do melhor amigo dos administradores de rede). O Ping envia uma mensagem ao host remoto e aguarda uma resposta contendo a mesma mensagem (*echo*). Se essa resposta chegar, presume-se que o host esteja vivo (literalmente).

ping *endereçoIP* | *hostname* [*chaves*]

Opção	**Descrição**
endereçoIP	Endereço IP (ou hostname) do host com o qual se está testando a conexão.
-a	Realiza a resolução DNS reversa, informando o hostname do host.
-n número	Define o número de comandos Ping que serão executados.
-l tamanho	Define o tamanho da mensagem utilizada no comando Ping (default=32 bytes).
-f	Define a flag; "Do Not Fragment" – envia a mensagem sem fragmentá-la.
-i *ttl*	*Time To Live* – Define o máximo número de *hops* pelos quais os pacotes podem passar (1-255).
-j *hosts*	Rota de origem livre usando as entradas em *hosts* .
-k *hosts*	Rota de origem restrita usando as entradas em *hosts* .
-r *número*	Regista a rota dos pacotes. Define quantos *hops* serão armazenados (máximo=9).
-s *número*	*Timestamp* do número de *hops* especificado.
-v TOS	Especifica o tipo de serviço a ser utilizado.
-t	Emite comandos Ping continuamente até ser interrompido. Normalmente "Ctrl+C" é utilizado para interromper.
-w	Define o tempo máximo que o comando aguardará por uma resposta (*timeout*).

Alguns roteadores, por questões de segurança, não encaminham pacotes enviados através do protocolo ICMP (utilizado pelo Ping). O comando Ping pode não obter sucesso devido a essa política de segurança.

Telnet

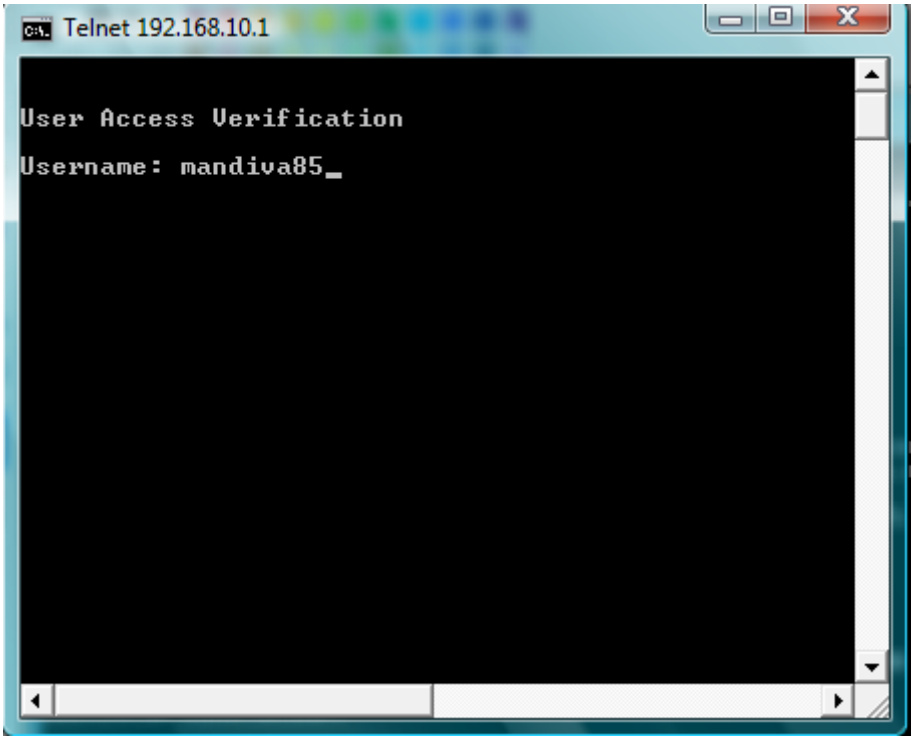


Figura: Screenshot de uma sessão telnet

Conecta-se a uma máquina remota, utilizando os seus recursos disponíveis.

telnet [*host* [*porta*]]

Opção	**Descrição**
Host	Nome de host ou endereço IP do endereço remoto.
Porta	Endereço da porta remota.

Comandos Interactivos do Telnet

close	Fecha uma conexão.
display	Exibe opções de conexão.
environ	Define variáveis de ambiente.
logout	Encerra uma conexão.
mode	Alterna entre o modo de transferência ASCII e binário.
open	Efectua a conexão com um computador remoto.
quit	Sai do Telnet.
Send	Envia sequências de protocolo Telnet especiais para um computador remoto.
set	Define opções de conexão.
unset	Desactiva parâmetros de conexão.

Tracert

O Tracert (“trace route” - traçar rota) serve para verificarmos quantos e quais computadores os nossos dados passam até chegar a um destino especificado. No exemplo acima, levou apenas umcomputador para alcançar o destino pedido.

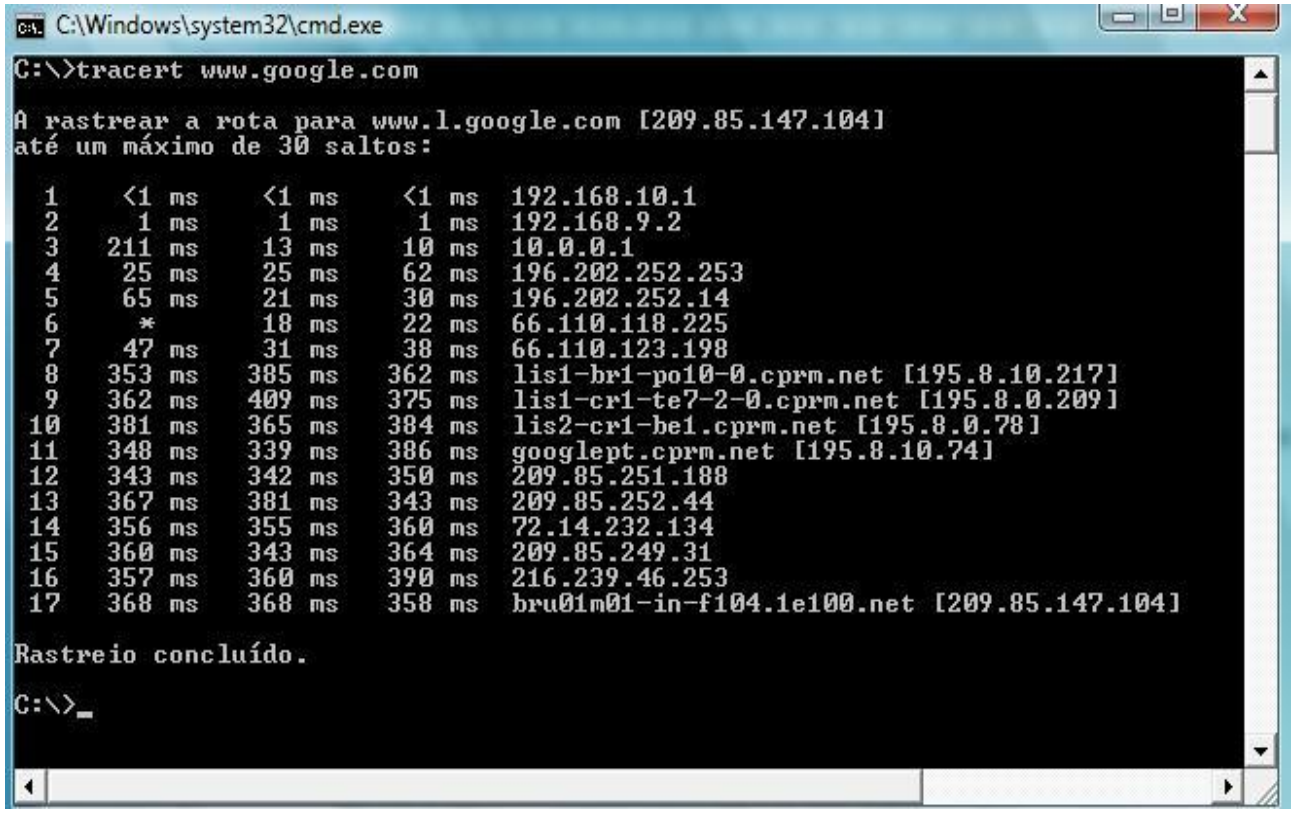


Figura: Utilitário Tracert

tracert [**-d**] [**h-** *hopsmáx*] [**-j** *listahops*] [**-w** *timeout*] *destino*

Opção	**Descrição**
-d	Não converte os endereços em nomes de host.
-h	Número máximo de *hops* (TTL) para encontrar o destino.
-j	Rota de origem livre com a *listahops* .
-w	*Timeou* t, ou tempo máximo para resposta (em milissegundos).
destino	Nome do host de destino (ou endereço IP).

Winipcfg

O Winipcfg é uma excelente ferramenta no que se trata de mostrar informações sobre o protocolo IP. Podemos dizer que ele é o IPCONFIG com interface GUI (interface gráfica).

Mostra seu IP local, IP da rede, máscara da sub-rede e muito mais. Para aceder, vá em iniciar / executar e digite winipcfg (utilizando o Windows Milenium, 98, 2000 e XP).

Serviços de Internet de Banda Larga

Os serviços de banda larga são aqueles que permitem ao utilizador conectar os seus computadores à Internet com velocidades maiores do que as normalmente utilizadas em linhas discadas. Exemplos desse tipo de serviço são ADSL, *cable modem* e acesso via satélite.

Além da maior velocidade, outra característica desse tipo de serviço é a possibilidade do utilizador deixar o seu computador conectado à Internet por longos períodos de tempo, normalmente sem limite de uso ou custos adicionais.

Porquê que um atacante teria maior interesse por um computador com banda larga e quais são os riscos associados?

Geralmente um computador conectado através de banda larga possui uma boa velocidade de conexão, muda o endereço IP com pouca freqüência e fica por longos períodos ligado à Internet, mas não possui os mesmos mecanismos de segurança que servidores. Isto torna-os alvos mais fáceis para os atacantes.

Por estas características, estes computadores podem ser utilizados pelos atacantes para diversos propósitos, como por exemplo:

- realizar ataques de recusa de serviço, aproveitando-se da maior velocidade disponível. Diversas máquinas comprometidas podem também ser combinadas de modo a criar um ataque de recusa de serviço distribuído.
- usar a máquina comprometida como ponto de partida para atacar outras redes, dificultando o rastreio (tracking) da real origem do ataque;
- furtar informações, tais como números de cartões de crédito, senhas, etc;
- usar recursos do computador. Por exemplo, o invasor pode usar o espaço disponível no seu disco duro para armazenar programas copiados ilegalmente, música, imagens, etc. O invasor também pode usar a CPU disponível para, por exemplo, decifrar senhas de sistemas comprometidos;
- enviar *spam* ou navegar na Internet de maneira anônima, a partir de certos programas que podem estar instalados no seu computador, tais como AnalogX e WinGate, e que podem estar mal configurados.

Vale ressaltar que todas essas actividades podem ser realizadas de maneira automatizada, caso o computador seja infectado por um *bot*.

O que fazer para proteger um computador conectado por banda larga?

Os utilizadoes de serviços de banda larga devem tomar os seguintes cuidados com o seu computador:

- instalar um *firewall* pessoal e ficar atento aos registos de eventos (*logs*) gerados por este programa;
- instalar e manter actualizado um bom programa antivírus;
- actualizar as assinaturas do antivírus diariamente;
- manter os seus *softwares* (sistema operacional, programas que utiliza, etc) sempre actualizados e com as últimas correcções de segurança aplicadas (*patches*);

- desligar a partilha de disco, impressora, etc;
- mudar a senha padrão do seu equipamento de banda larga (*modem* ADSL, por exemplo) pois as senhas destes equipamentos podem ser facilmente encontradas na Internet com uma simples busca (ver senhas padrão). Esse facto é de conhecimento dos atacantes e bastante abusado. A escolha de uma boa senha é discutida na Parte I: Noções de Segurança.

O que fazer para proteger uma rede conectada por banda larga?

Muitos utilizadores de banda larga optam por montar uma pequena rede (doméstica ou mesmo em pequenas empresas), com vários computadores a utilizarem o mesmo acesso a Internet. Nesses casos, alguns cuidados importantes, além dos citados anteriormente, são:

- instalar um *firewall* separando a rede interna da Internet;
- caso seja instalado algum tipo de *proxy* (como AnalogX, WinGate, WinProxy, etc), configurá-lo para que apenas aceite requisições partindo da rede interna;
- caso seja necessário partilhar recursos como disco ou impressora entre máquinas da rede interna, devem-se tomar os devidos cuidados para que o *firewall* não permita que esta partilha seja visível pela Internet.

É muito importante notar que apenas instalar um *firewall* **não** é suficiente -- todos os computadores da rede devem estar configurados de acordo com as medidas preventivas mencionadas neste livro.

Muitos equipamentos de banda larga, como roteadores ADSL, estão a incluir outras funcionalidades, como por exemplo concentradores de acesso (*Access Points*) para redes *wireless.*

Redes Sem Fio (*Wireless*)

As redes sem fio (*wireless*), também conhecidas como IEEE 802.11, Wi-Fi ou WLANs, são redes que utilizam sinais de rádio para a sua comunicação.

Este tipo de rede define duas formas de comunicação:

> **modo infraestrutura:** normalmente o mais encontrado, utiliza um concentrador de acesso (*Access Point* ou AP);
>
> **modo ponto a ponto (*ad-hoc*):** permite que um pequeno grupo de máquinas se comunique directamente, sem a necessidade de um AP.

Estas redes ganharam grande popularidade pela mobilidade que oferecem aos seus utilizadores e pela facilidade de instalação e uso em ambientes domésticos e empresariais, hotéis, conferências, aeroportos, etc.

Quais são os riscos do uso de redes sem fio?

Embora esse tipo de rede seja muito conveniente, existem alguns problemas de segurança que devem ser levados em consideração pelos seus utilizadores:

- estas redes utilizam sinais de rádio para a comunicação e qualquer pessoa com um mínimo de equipamento poderá interceptar os dados transmitidos por um cliente da rede sem fio (como *laptops*, PDAs, computadores pessoais, etc);

- por serem bastante simples de instalar, muitas pessoas utilizam redes desse tipo em casa, sem nenhum cuidado adicional, e até mesmo em empresas, sem o conhecimento dos administradores de rede.

Que cuidados devo ter com um cliente de uma rede sem fio?

Vários cuidados devem ser observados quando se pretende conectar à uma rede sem fio como cliente, seja com *laptops*, PDAs, computadores pessoais, etc. Dentre eles, podem-se citar:

- considerar que, ao conectar a uma WLAN, você estará conectando-se a uma rede pública e, portanto, o seu computador estará exposto a ameaças. É muito importante que você tome os seguintes cuidados com o seu computador:
    - instalar um *firewall* pessoal;
    - instalar e manter actualizado um bom programa antivírus;
    - actualizar as assinaturas do antivírus diariamente;
    - aplicar as últimas correcções nos seus *softwares* (sistema operacional, programas que utiliza, etc);
    - desligar a partilha de disco, impressora, etc.

- desabilitar o modo *ad-hoc*. Utilize esse modo apenas se for absolutamente necessário e desligue-o assim que não necessitar mais;
- sempre que possível usar WEP (*Wired Equivalent Privacy*), que permite criptografar o tráfego entre o cliente e o AP. Fale com o seu administrador de rede para verificar se o WEP está habilitado e se a chave é diferente daquelas que acompanham a configuração padrão do equipamento. O protocolo WEP possui diversas fragilidades e deve ser visto como uma camada adicional para evitar a escuta não autorizada;
- verificar com o seu provedor de rede sem fio sobre a possibilidade de utilizar WPA (Wi-Fi *Protected Access*) em substituição ao WEP, uma vez que este padrão pode aumentar significativamente a segurança da rede. Esta tecnologia inclui duas melhorias em relação ao protocolo WEP que envolvem melhor criptografia para transmissão de dados e autenticação de utilizador. Mesmo que o seu equipamento seja mais antigo, é possível que exista uma actualização para permitir o uso de WPA;
- considerar o uso de criptografia nas aplicações, como por exemplo, o uso de PGP para o envio de *e-mails*, SSH para conexões remotas ou ainda o uso de VPNs;
- evitar o acesso a serviços que não utilizem conexão segura, ao usar uma rede sem fio em local público. Por exemplo, se for necessário ler *e-mails* ou aceder a Intranet da sua empresa, dê preferência a serviços que usem criptografia;
- habilitar a rede sem fio somente quando for usá-la e desabilitá-la após o uso. Alguns computadores pessoais e *laptops* permitem habilitar e desabilitar o uso de redes sem fio através de comandos ou botões específicos. No caso de *laptops* com cartões PCMCIA, insira o cartão apenas quando for utilizar a rede e retire-o ao terminar de utilizar.

Que cuidados devo ter ao montar uma rede sem fio doméstica?

Pela conveniência e facilidade de configuração das redes sem fio, muitas pessoas têm instalado estas redes nas suas casas. Nestes casos, além das preocupações com os clientes da rede, também são necessários alguns cuidados na configuração do AP. Algumas recomendações são:

- ter em mente que, dependendo da potência da antena do seu AP, a sua rede doméstica pode abranger uma área muito maior que apenas a da sua casa. Com isto a sua rede pode ser

utilizada sem o seu conhecimento ou ter o seu tráfego capturado por vizinhos ou pessoas que estejam nas proximidades da sua casa;

- mudar configurações padrão que acompanham o seu AP. Alguns exemplos são:
    - alterar as senhas. Dicas para a escolha de uma boa senha podem ser obtidas na Parte I: Noções de Segurança;
    - alterar o SSID (*Server Set ID*);
    - desabilitar o *broadcast* de SSID;
    - permitir que um computador se conecte ao AP para alterar as configurações apenas através da rede cabeada, se esta opção estiver disponível. Desta maneira um possível atacante externo (via rede sem fio) não poderá acessar o AP directamente para promover mudanças na configuração.Verifique a documentação do seu AP sobre como efectuar estas mudanças, caso estejam disponíveis;

- verificar se os seus equipamentos já suportam WPA (Wi-Fi *Protected Access*) e utilizá-lo sempre que possível. Esta tecnologia é mais recente e inclui melhorias em relação ao protocolo WEP para fornecer uma segurança adicional contra acesso e escuta de tráfego não autorizada. Lembre-se que actualizações para WPA estão disponíveis para a maior parte dos equipamentos mais antigos;
- caso o WPA não esteja disponível, usar sempre que possível WEP (*Wired Equivalent Privacy*), para criptografar o tráfego entre os clientes e o AP. Vale a pena recordar que o protocolo WEP possui diversas fragilidades e deve ser visto como uma camada adicional para evitar a escuta não autorizada;
- se for utilizar WEP, trocar as chaves que acompanham a configuração padrão do equipamento. Procure utilizar o maior tamanho de chave possível (128 bits);
- desligar o seu AP quando não estiver a utilizar a sua rede.

Existem configurações de segurança mais avançadas para redes sem fio, que requerem conhecimentos de administração de redes.

Footprinting

Footprinting é a arte de obter informações sobre um sistema alvo utilizando tácticas "seguras", sem perigo de detecção, e que pode dar muitas informações sobre ele. Tais como visitar o site da empresa em que se quer invadir e ler as seções para ver se encontra algo de interessante.

Whois

O Whois é excelente para obtermos informações sobre sites. Base de dados como o Internic (www.internic.org) mantêm informações preciosas sobre os domínios, tais como nome do dono, endereço e telefone. Em Angola, o órgão responsável por essa tarefa é a UAN (Universidade Agostinho Neto) em colaboração com a fundação para a computação científica nacional de Portugal (FCCN).

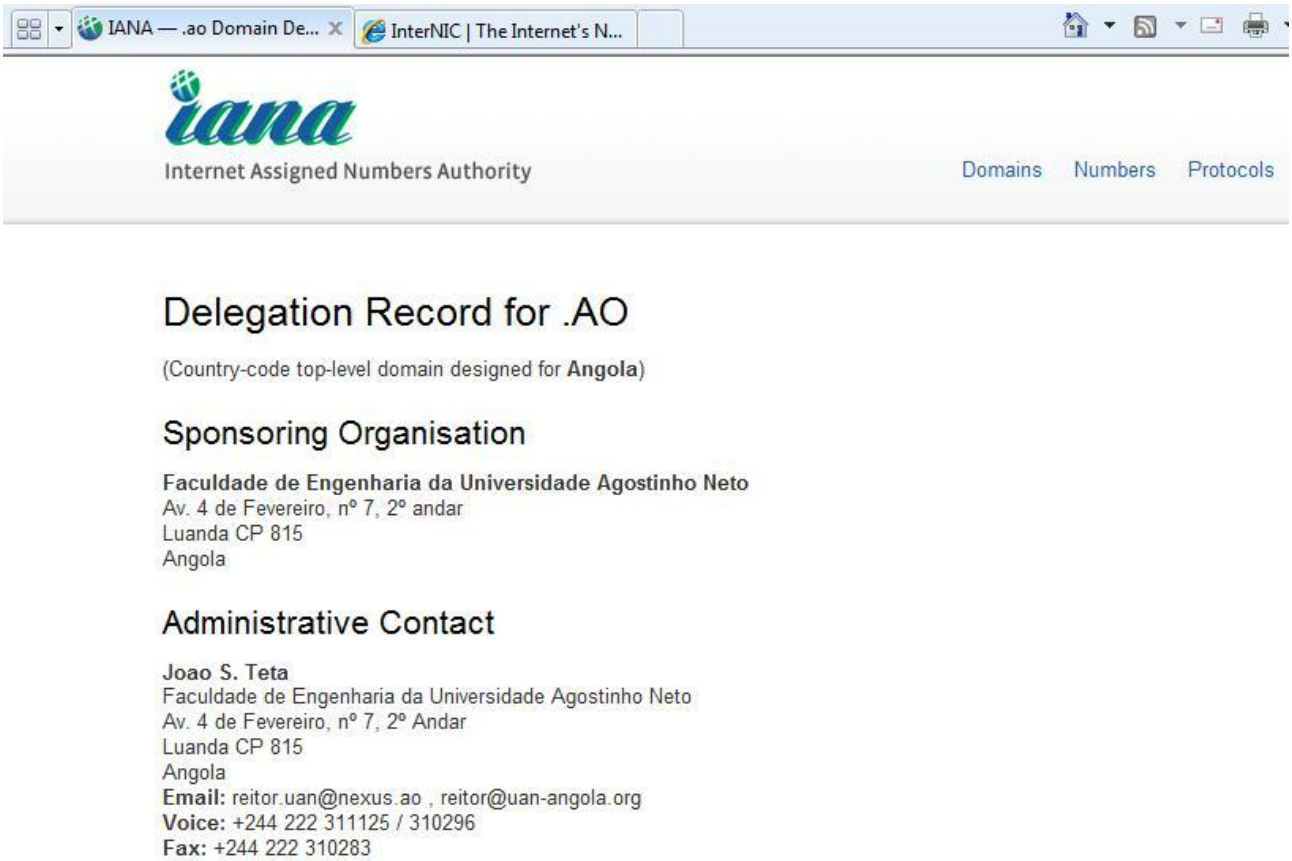


Figura: Screenshot do delegation record para o top-level domínio .AO

Análise de websites

Consiste em entrar no site, ler tudo quanto é página, websites pessoais de funcionários (se for uma empresa), absolutamente tudo. Parece incrível mas muitos lugares mostram até configurações da rede nas suas páginas. O código em html também deve ser analisado a procura de comentários. Muitos deles podem ser extremamente úteis. Verifique todos os links, observe os endereços em que as páginas se posicionam. Já dá para começarmos o montar um mapa da rede (antes do invasor fazer um ataque directo scanneando mais tarde).

Pesquisa geral

O invasor utiliza ferramentas de procura como o Google para descobrir outras páginas com o nome do domínio atacado. Pesquisa em jornais notícias e revistas sobre o "alvo", tais como se ele já foi atacado, se já sofreu algum tipo de invasão, etc. Tenta conhecer pessoas que trabalham lá, ter uma noção de quantos empregados existem a cuidar daquele servidor. Enfim, quanto mais eles puderem descobrir na pesquisa geral, mas fácil o trabalho ficará depois. Daí, a importância de ensinar os funcionários ou colaboradores de uma instituição ou empresa, sobre a importância da segurança da informação, sobre a confidencialidade das informações e alertá-los sobre a engenharia social e como proteger-se dela.

Trojans

Definição de Trojan

O nome trojan é uma alusão à história do antigo cavalo de tróia, em que o governante da cidade de Tróia na antiga Grécia foi presenteado com um cavalo de madeira no qual havia escondido soldados inimigos. Possui muitas características similares aos vírus, tais como: perda de ficheiros, falhas na memória, erros em periféricos, etc... A grande diferença é que o trojan pode ser considerado um vírus inteligente, pois é controlado à distância pela pessoa que o instalou. Esse indivíduo então, consegue "ver" o seu computador, podendo realizar desde as mais simples tarefas como mexer o rato à utilização do seu IP como ponte para outros ataques. Conseguem ficar escondidos em ficheiros de inicialização do sistema operacional e iniciam toda vez que a máquina é ligada.

Na informática, um cavalo de tróia (*trojan horse*) é um programa, normalmente recebido como um "presente" (por exemplo, cartão virtual, álbum de fotos, protector de ecrã, jogo, etc), que além de executar funções para as quais foi aparentemente projectado, também executa outras funções normalmente malignas e sem o conhecimento do utilizador.

Algumas das funções maliciosas que podem ser executadas por um cavalo de tróia são:

- instalação de *keyloggers* ou *screenloggers* ;
- furto de senhas e outras informações sensíveis, como números de cartões de crédito;
- inclusão de *backdoors*, para permitir que um atacante tenha total controlo sobre o computador;
- alteração ou destruição de ficheiros.

Perigo real

A popularização da Internet e a facilidade de se criar um programa cavalo de tróia fazem com que esse método de invasão seja actualmente o mais perigoso de todos. Ele não depende de falhas no seu sistema, é quase indetectável e pela sua facilidade de uso pode ser operado por crianças de 6 anos. Pode-se esconder um trojan em fotos, ficheiros de música, aplicativos e jogos. Sendo assim, nunca abra ficheiros executáveis enviados por estranhos ou adquiridos em sites duvidosos. Existem muitas técnicas para se instalar um trojan numa máquina. Um bom exemplo no Windows 98/ME 2000 é mapeando a unidade desse computador (netbios), copiar o programa e alterar o ficheiro win.ini Assim toda vez que você for jogar paciência ou mesmo abrir o bloco de notas, tome cuidado com o tamanho do ficheiro executável. Se estiver muito grande, desconfie.

Como um cavalo de tróia pode ser diferenciado de um vírus ou *worm*?

Por definição, o cavalo de tróia distingue-se de um vírus ou de um *worm* por não infectar outros ficheiros, nem propagar cópias de si mesmo automaticamente.

Normalmente um cavalo de tróia consiste num único ficheiro que necessita ser explicitamente executado.

Podem existir casos onde um cavalo de tróia contenha um vírus ou *worm*. Mas mesmo nestes casos é possível distinguir as acções realizadas como consequência da execução do cavalo de tróia propriamente dito, daquelas relacionadas ao comportamento de um vírus ou *worm*.

Como um cavalo de tróia se instala num computador?

É necessário que o cavalo de tróia seja executado para que ele se instale num computador. Geralmente um cavalo de tróia vem anexado a um *e-mail* ou está disponível em algum *site* na Internet.

É importante ressaltar que existem programas leitores de *e-mails* que podem estar configurados para executar automaticamente ficheiros anexados às mensagens. Neste caso, o simples facto de ler uma mensagem é suficiente para que um ficheiro anexado seja executado.

Que exemplos podem ser citados sobre programas contendo cavalos de tróia?

Exemplos comuns de cavalos de tróia são programas que você recebe ou obtém de algum *site* e que **parecem ser** apenas cartões virtuais animados, álbuns de fotos de alguma celebridade, jogos, protetores de tela, entre outros.

Enquanto estão a ser executados, estes programas podem ao mesmo tempo enviar dados confidenciais para outro computador, instalar *backdoors*, alterar informações, apagar ficheiros ou formatar o disco duro.

Existem também cavalos de tróia, utilizados normalmente em esquemas fraudulentos, que, ao serem instalados com sucesso, apenas exibem uma mensagem de erro.

O que um cavalo de tróia pode fazer num computador?

O cavalo de tróia, na maioria das vezes, instalará programas para possibilitar que um invasor tenha controlo total sobre um computador. Estes programas podem permitir que o invasor:

- tenha acesso e copie todos os ficheiros armazenados no computador;
- descubra todas as senhas digitadas pelo utilizador;
- formate o disco duro do computador, etc.

Um cavalo de tróia pode instalar programas sem o conhecimento do utilizador?

Sim. Normalmente o cavalo de tróia procura instalar, sem que o utilizador perceba, programas que realizam uma série de actividades maliciosas.

É possível saber se um cavalo de tróia instalou algo num computador?

A utilização de um bom programa antivírus (desde que seja actualizado frequentemente) normalmente possibilita a detecção de programas instalados pelos cavalos de tróia.

É importante lembrar que nem sempre o antivírus será capaz de detectar ou remover os programas deixados por um cavalo de tróia, principalmente se estes programas forem mais recentes do que as assinaturas do seu antivírus.

Existe alguma forma de proteger um computador dos cavalos de tróia?

Sim. As principais medidas preventivas contra a instalação de cavalos de tróia são semelhantes às medidas contra a infecção por vírus e estão listadas na secção sobre vírus.

Uma outra medida preventiva é utilizar um *firewall* pessoal. Alguns *firewalls* podem bloquear a recepção de cavalos de tróia.

Tipos de cavalo de tróia

Invasão por portas TCP e UDP

Esse é o trojan mais comum existente na Internet hoje. Netbus, Back Orifice, SubSeven, Hack'a'tack, Girlfriend, Netsphere e muitos outros são facilmente encontrados pela rede. Possuem na sua maioria dois ficheiros: um servidor para ser instalado no computador da vítima e um cliente com interface gráfica para manipular o servidor remotamente. As portas de um sistema variam entre 0 e 65535 e servem para identificar serviços em execução no sistema (como o servidor web que utiliza a porta 80). O servidor torna-se mais um serviço ao escolher alguma porta para "escutar" as chamadas do cliente. O cavalo de tróia que utiliza portas TCP, estabelece uma conexão com o servidor, actuando directamente de dentro do sistema. Já o que utiliza portas UDP, comunica-se via pacotes de dados enviados ao host alvo. Não tão confiável como o TCP, não garante a entrega dos pacotes e o recebimento da resposta. Quase todos os trojans actuais são para a arquitectura Windows. Os poucos existentes em outros sistemas, tais como: Unix, Linux, Novell e Macintosh são chamados de *backdoors* . A diferença entre o cavalo de tróia comum e o backdoor é que o último é muito mais difícil de se instalar. Em sistemas Unix por exemplo, para conseguir instalar-se um backdoor é preciso possuir privilégios de super utilizador (root).

Trojans de informação

Não é tão utilizado quanto o de portas mas igualmente (ou até mais) perigoso. Enquanto a maioria das funções dos cavalos de tróia comuns é apenas para aborrecer (desaparecer com a barra de tarefas, apagar o monitor, desligar o Windows, etc...), o cavalo de tróia de informação concentra-se em ficar residente detectando todos os tipos de dados vitais do sistema. Ele consegue toda senha digitada no servidor junto ao endereço ip das máquinas e envia a informação para uma conta de e-mail configurada pelo invasor. Existem alguns programas mais sofisticados que além de enviar por e-mail, pode enviar a informação por icq, msn Messenger, yahoo messenger ou qualquer outro tipo de messenger. Geralmente o programa envia a informação num prazo de cada 5 a 10 minutos. Ao contrário do cavalo de tróia de portas, possui apenas o ficheiro servidor e um tamanho bem menor. Exemplo: o servidor do cavalo de tróia de portas Netbus possui cerca de 490 kb de tamanho. Já o cavalo de tróia de informações k2ps possui cerca de 17 kb.

Trojans de ponte

É um tipo não muito conhecido mas largamente utilizado por hackers e crackers do mundo inteiro. Consiste em instalar um servidor no seu computador que possibilite que através dele (e do seu endereço ip) o invasor possa realizar ataques de invasão e de recusa de serviço. Então, se um grande site for invadido e baterem na sua casa, procure pois deve haver algum desses no seu

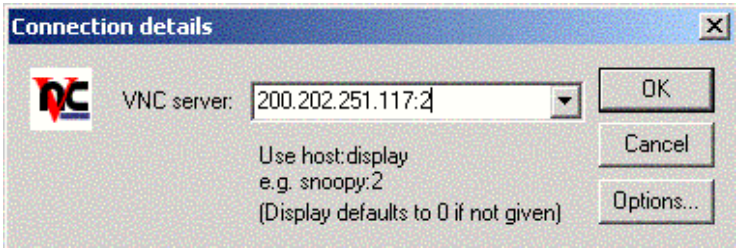
sistema. Um programa comum é o WinProxy, que pode ser instalado facilmente e não levanta nenhum tipo de suspeitas. Conheço alguém que o possui na sua máquina e jura que é um firewall. Leia mais sobre os trojans de ponte na secção *anonimidade.*

Rootkits

Esse tipo especial de backdoor é utilizado no Unix e Linux. Ao ser executado pelo operador do sistema ele substitui ficheiros executáveis importantes (como o ps por exemplo) por versões "infectadas". Essas versões podem ser tanto trojans de portas quanto de informação. Vão fornecer acesso irrestrito ao invasor com poderes de super-utilizador, e o mais importante: os acessos não ficam registados nos logs. Para conhecer alguns dos rootkits mais usados e o tipo de alteração causada por eles, visite o website: www.rootshell.com.

Trojans comerciais

Alguém já ouviu falar do PcAnywhere? Ou do terminal remoto do Windows 2000 e XP? Esses programas (além de muitos outros) possibilitam que você controla completamente a máquina de alguém, como se estivesse sentado ali. Quer jogar Solitário no computador invadido? Clique no botão iniciar dele e faça tudo como se estivesse no seu próprio computador. A vantagem desses programas (já que são comerciais), é que o anti-vírus não detecta. Tente também o excelente VNC (o seu download pode ser feito em: www.thepiratebay.org), que é gratuito.



Cliente para conexões do programa comercial VNC, criado pela AT&T

Escondendo o cavalo de tróia em ficheiros confiáveis

Existem muitos programas na Internet que escondem os servidores em ficheiros executáveis. Um deles é o **The Joiner** , que possibilita você juntar o cavalo de tróia com algum outro executável e criar um terceiro contendo os dois. Além de possibilitar que o coloque em fotos. Um método engraçado muito utilizado hoje pelos que se dizem "hackers", é renomear algum executável para foto e deixar um largo espaço. Por exemplo: supondo que o nosso servidor é o ficheiro **server.exe.** Então iríamos renomeá-lo para **pornografia.jpg .exe.**

Assim muitos utilizadores inexperientes caem no truque. Todos os métodos citados anteriormente têm somente uma falha: se você criar um executável pelo The Joiner ou renomear o servidor, qualquer programa anti-vírus logo detectará o ficheiro. Para que o anti-vírus não o detecte, usa-se a imaginação. Cria-se um programa em alguma linguagem e coloque o servidor no meio dos ficheiros. Faça com que o programa quando executado renomeie o servidor e o execute. Assim, se o servidor estiver como **voodoo.dll** passe-o para **sysconf.exe** e execute. Esse método não é infalível mas engana

a grande maioria dos programas de detecção. Mas não todos. Anti-vírus geralmente o detecta.

The Joiner: esconde o servidor noutro ficheiro utilizando compressores de executáveis

Como vimos no item anterior, vários métodos podem ser usados para esconder um cavalo de tróia. Depende mais da imaginação do invasor. Só que ainda assim podem ser facilmente detectados. Esse é o primeiro livro a citar o método do compressor de executáveis Windows 32 bits, apesar de essa técnica já vir a ser utilizada em larga escala. Consiste em utilizar um programa compressor de ficheiros EXE, que apenas diminua o seu tamanho retirando espaços vazios desnecessários. Um programa comum é o **Petite** que diminui cerca de 30% ou mais do ficheiro original. Um cavalo de tróia (ou mesmo um vírus) comprimido é absolutamente indetectável por anti-vírus e scanners. Isso porque esses programas baseiam-se na estrutura do ficheiro a identificá-lo. É como se tivesse fotos na memória e as comparasse. Como não encontrou nenhuma igual, não mostra nenhum tipo de aviso. Um operador de sistemas tem que conhecer muito bem seus ficheiros e conferir sempre novas alterações (como datas e horas de novos ficheiros) para evitar que um cavalo de tróia comprimido seja instalado no seu sistema. Não dependa só de anti-vírus. Mas atenção: os compressores de executáveis não comprimem ficheiros que já foram comprimidos (como o server do cavalo de tróia subseven).

Vamos verificar passo a passo o processo de esconder um cavalo de tróia de um anti-vírus.

1. Passaremos o Norton para que encontre o ficheiro infectado:

Screenshot do Norton fazendo a varredura de um trojan

2. Agora, abriremos o programa PETITE para comprimir o ficheiro EXE do servidor do Netbus.

Screenshot do petite (joiner) escondendo o trojan

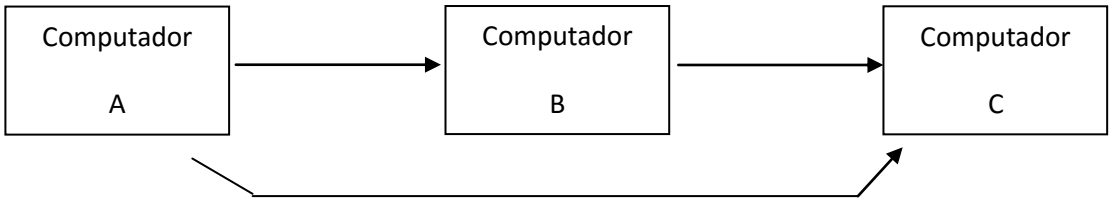
3. Com o ficheiro já comprimido, novamente testamos o anti-vírus

Screenshot do antivírus fazendo o scan sem sucesso do trojan mascarado

Spoofing

É muito raro a utilização do spoof em trojans. Isso porquê se a pessoa envia um pedido de conexão a um servidor, ela precisa usar o seu endereço IP real para receber a resposta. Apenas com o protocolo UDP, que envia comandos sem estabelecimento de conexão, isso é possível. Em quase

todos os casos, o endereço IP capturado por um programa anti-trojans é realmente o do invasor. A única excepção é quando se utiliza um cavalo de tróia de ponte para se conectar a outro (geralmente TCP). Exemplo:



O **computador A** tem duas opções. Pode conectar-se ao cavalo de tróia existente no **computador C**. Mas o invasor não quer correr nenhum risco pois não está usando nenhum tipo de recursos de anonimidade. Então ele conecta-se ao **computador B** que está na mesma rede que o **computador C** mas não possui nenhum tipo de segurança. Se utilizando da confiança entre as duas máquinas, ele conecta-se ao **computador C** que vai responder tudo o que invasor quiser, pois pensa que o **computador B**. Essa técnica, chamada de IP Spoof, foi utilizado pelo hacker Kevin Mitnick para conseguir acesso ao computador do analista de sistemas Shimomura. O processo será descrito em detalhes na secção anonimidade.

Métodos eficazes e os não tão eficazes de se retirar o programa

Basicamente existem quatro métodos de se retirar um cavalo de tróia. Cada um possui as suas vantagens e falhas. O ideal seria usar um pouco de todos.

Detecção por portas

Esse é um método utilizado por programas como o Xôbobus, um bom Anti-Trojans e muitos outros. Funciona do seguinte modo: os programadores estudam as portas TCP e UDP utilizadas pelos trojans e criam um programa que abre essas portas. Assim, quando um invasor vir a porta aberta e pensar que é um cavalo de tróia que está instalado ali, cairá numa armadilha tendo o seu endereço IP detectado. Esse método não é muito eficiente pois facilmente podemos mudar as portas que os trojans utilizam. Mas ainda é um método muito utilizado pois muitas pessoas não se lembram de trocar as portas.

Detecção pelo ficheiro

Esse é o método usado pelos anti-vírus e o programa The Cleaner. Ele detecta o cavalo de tróia verificando a sua estrutura. Se o ficheiro estiver renomeado (sem ser para executável) ou estiver comprimido, esse método torna-se inútil. Para ser realmente eficaz, deve ser utilizado junto à detecção de portas. Assim, mesmo que o seu anti-vírus não encontrou um cavalo de tróia, o Anti-Trojans pode encontrar.

Detecção por string

Na minha opinião, o melhor método de todos. Pouco divulgado publicamente, torna-se a melhor garantia para detectar-se um cavalo de tróia sem falhas. Isso porquê mesmo que o programa for comprimido ou mude as suas portas, ele ainda estará utilizando uma das 65535 portas do sistema e se comunicará com o cliente. A comunicação entre cliente e servidor dá-se por uma string (texto) enviada. Por exemplo: O Netbus envia uma string assim "Netbus" quando alguma conexão é estabelecida. Se for o cliente, ele responderá com outra string. Então para analisar todas as portas do seu sistema e saber quais estão abertas e possuem strings, utilize um programa como o Chaoscan ou algum outro scanner de porta que lhe dê essas informações.

Detecção manual

Muito eficaz também, a verificação manual do sistema pelo operador pode facilitar muito a vida. Olhando registo, ficheiros de inicialização, verificando os programas carregados na memória, o tamanho dos ficheiros, etc... Todas essas precauções evitam dores de cabeça. Essa política adoptada junto aos outros tipos de detecção faz com que você exclua em 100% a possibilidade de uma invasão por cavalos de tróia.

Passo-a-passo: cavalos de tróia

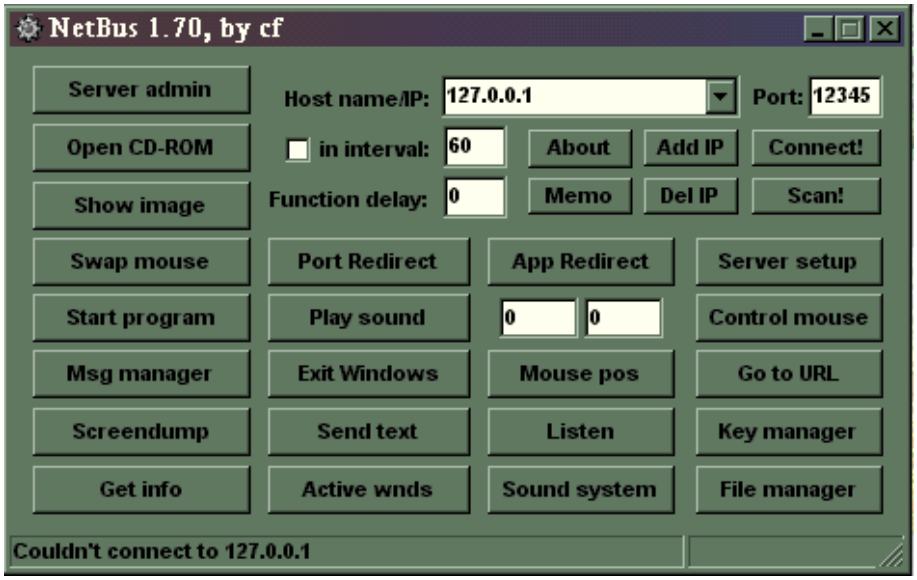
Utilizando um cavalo de tróia

Vamos utilizar um cavalo de tróia para nos conectarmos a algum computador infectado. Antes de tudo, verifique se o computador alvo está com o servidor instalado (o ficheiro que comprimimos anteriormente). Agora seguiremos os seguintes passos com o cavalo de tróia Netbus:

1. Abra o programa Netbus (se o anti-vírus acusar vírus, passe o petite nele também);

2. Em hostname / IP, coloque o IP da máquina a ser invadida (se for o seu próprio computador, utilize 127.0.0.1). Se a porta no servidor for diferente de 12345 (o padrão do Netbus), coloque-a em port;

3. Clique em connect!



Ao aparecer a mensagem " **Connected** " na barra de status, significa que a invasão foi bem sucedida. Vamos agora realizar algumas acções:

1. Clique em Open CD-ROM para abrir o drive de cd da vítima.
2. Vá em Start Program e coloque **c:\windows\calc.exe** para abrir a calculadora.
3. Clique em Go to URL e mande a pessoa par a algum site.
4. Use Listen para pegar os caracteres digitados pela pessoa e intervir no meio (como se você estivesse escrevendo no Word e de repente as palavras se formam sozinhas).
5. A Port Redirect cria uma ponte. Coloque uma porta (geralmente use a 80) e um site. Assim quando for ao Internet Explorer e digitar o IP do computador invadido, você cairá nesse site configurado. Por exemplo: ao digitar **127.0.0.1** no browser fui enviado para **www.whitehouse.gov**.
6. Dá para fuçar bem nas opções, mas a mais interessante é a App Redirect. Abra-a, coloque uma porta qualquer (100 por exemplo) e mande executar um shell nessa porta (no caso do Windows 95, 98 e ME, use **c:\command.com** , no NT, 2000 e XP use cmd.exe). Agora utilize o **telnet** (vá em iniciar/ executar e digite: telnet 127.0.0.1 100, trocando o endereço ip padrão pelo da vítima) e pronto. Você está no prompt do MS-DOS da pessoa. Têm o controla total da máquina.
7. Para desconectar, apenas clique em disconnect.
8. A opção server admin retira o servidor.

Utilizando o Anti-Trojans

Vamos utilizar como exemplo de detecção por portas, o programa **Anti-Trojans** Se quiser tentar algum programa, tente o Nod32 Anti-Trojan ou algum outro (procure no thepiratebay.org). É claro que um firewall (como veremos depois) é mais potente. Mas é mais complicado para utilizadores comuns. Veremos passo a passo.

1. Abra o programa
2. Clique na pasta Configuração, e coloque a mensagem para a pessoa que tentar lhe invadir. Se quiser, configure um e-mail para que a tentativa de invasão seja reportada.

3. Clique na pasta Monitorar.
4. Clique no botão Monitorar. Agora clique com o botão direito no ícone do superman na barra de tarefas e seleccione esconder.
5. Simule uma tentativa de invasão indo em Iniciar / Executar e digitando:

   telnet 127.0.0.1 12345

O programa irá detectar a tentativa de invasão e mostrará uma mensagem com o horário, o endereço IP do invasor, o seu host e o tipo de invasão tentada.

NB: Para terminar o capítulo de trojans, uma pequena dica: tenha muito cuidado com os ficheiros autorun.inf de algum cd/dvd (aquele que faz o cd/dvd executar automaticamente quando no drive), pois muitos deles fazem executar cavalos de Tróia, disfarçados através das técnicas que verificamos anteriormente.

Denial of Service (DoS)

Definição

A diferença entre um cracker e um script kiddie pode ser vista aqui. Um invasor decente estuda em detalhes o sistema alvo, às vezes por meses, conhecendo todo o seu processo de autenticação, utilizadores e falhas que podem levá-lo a ter acesso a ficheiros vitais. Já o script kiddie faz o download de uma ferramenta "hacker" num website duvidoso de fundo preto e imagens de caveiras animadas, tenta usá-lo no primeiro sistema que vê na frente e se não consegue invadi-lo, o torna indisponível para mostrar que é "bom". Isso é absolutamente inútil, afinal se o sistema travar e cair devido ao Denial of Service, provavelmente ele volta a funcionar com questão de poucos minutos. Ou o administrador competente rapidamente percebe. Alguns programas bons para essa tarefa são o Agressor, o IGMP Nuker e o Divine Intervention (para Windows). Para Linux e Unix, sem dúvida o melhor é o excelente Tribal Flood Network.

Danos sem invasões

Por ser um ataque apenas voltado para o consumo de memória ou do processamento, o DoS não é usado para invasão. Ao contrário de alguns programas que causam uma sobrecarga de memória já sabendo que esse problema lhe dará acesso ao sistema (programas que causam buffer overflow), a intenção do DoS é só chatear. Mesmo assim em grandes empresas o prejuízo pode ser grande. Quando a *Amazon.com* foi tirada do ar por exemplo, chegou a ficar apenas poucos minutos desligada, mas nesse tempo perdeu muito dinheiro em compras. O mesmo aconteceu com o Yahoo e até com o UOL, que já foi tirado do ar.

Utilizando o broadcast como arma

Realizar um ataque de DoS é muito simples. Pode-se utilizar vários tipos de programas e **softwares fantasmas** para fazê-lo. Às vezes nem é preciso um programa adicional. Sites como Yahoo e Altavista utilizam webspiders (programa utilizado para procurar informações indo de link em link) para verificar o conteúdo de **websites. Muitos webspiders verificando o mesmo servidor ao mesmo tempo podem** levá-lo ao colapso. Causar um DoS em algum servidor de e-mail é ainda mais fácil. Utiliza-se um programa de e-mail bomba (software que envia milhares de e-mails p**ara o mesmo endereço) ou regist**ando o e-mail alvo em serviços de spam (como mensagens de anjos, piadas, notícias e outros) pode encher a sua caixa postal e travar todo o sistema. Ou mande um e-mail para alguém que tenha serviço de **resposta automática**, utilizando o próprio endereço da pessoa. É assim: mande uma mensagem para **fulano@provedor.co.ao** utilizando esse e-mail (como se fosse o seu, já que para mandar e-mails não se precisa de senha). A resposta automática da caixa postal do Fulano mandará mensagens para ele mesmo, travando a sua caixa postal. O endereço de broadcast de redes geralmente é o com final 255 (exemplo: 200.202.243.255). A solução para o problema do e-mail é mais simples. Apenas use um bom filtro ou algum programa que impossibilite que se receba mais de três e-mails enviados da mesma origem (endereço IP) durante um certo intervalo de tempo.

Um ecrã de um programa de e-mail bomba

Syn-flood

O tipo de ataque usado para gerar o ip spoof. A autenticação por Syn é feita em três vias.
O ataque consiste em não completar essas três vias. Mais ou menos assim. No caso do ping, ele é em duas vias, apenas envia o pacote e recebe a resposta. Para o Syn-flood, primeiro é enviado o pacote Syn e logo depois teria que ser enviado o Ack para a conexão se estabelecer, mas ele não é enviado, fazendo com que a máquina alvo consuma os seus recursos ao receber muitos Syns e esperar muitos

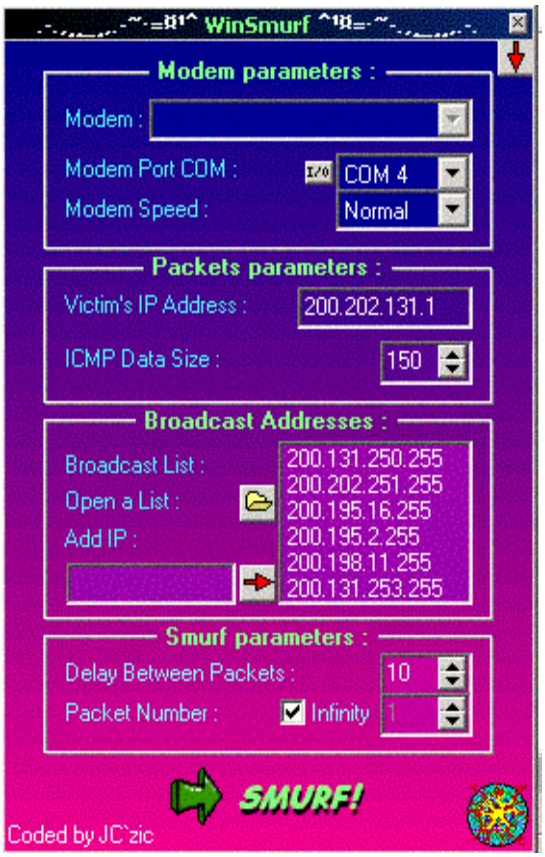
Acks. O ataque por ping é parecido, é enviado vários pings com grandes pacotes fazendo com que um sistema trave. Mas é mais difícil de ocorrer o travamento do que o ataque por syn.

OOB

Ataque Out-of-Band ou popularmente conhecido como WinNuke. Consiste em mandar pacotes mal formados para uma porta Netbios do Windows. Geralmente utilizado nas portas 135, 137 e 139, essa última sendo a mais usada. O sistema não consegue lidar com os pacotes, trava e mostra a famosa tela azul de erro. Nos Windows 95, Millenium e 98 esse ataque era mais eficaz, agora está tornar-se obsoleto.

Smurf

Na minha opinião o mais devastador de todos os ataques. Envia pacotes ICMP (protocolo que informa condições de erro) spoofados para centenas, talvez milhares de sites. Envia-se os pacotes com o endereço IP da vítima, assim fazendo com que ela receba muitos pacotes ping de resposta ao mesmo tempo, causando uma indisponibilidade total. Ainda não existe uma protecção eficaz contra esse tipo de ataque. Um programa bom (para Windows) que realiza o smurf é o WinSmurf.



Ecrã do winsmurf

Softwares fantasmas

Programas que automatizam o processo de causar um DoS em alguma máquina. São instalados em computadores estratégicos (como universidades, centros de pesquisa e outros) que possuem conexão rápida à Internet e configurados para atacar ao mesmo tempo. Se eu instalar o programa em vinte máquinas de diferentes endereços e configurá-las para enviar 10.000 pacotes cada uma, com certeza derruba qualquer host. Um programa muito utilizado para isso é o **Tribal Flood Network**. Trojans

também são largamente usados para esse fim.

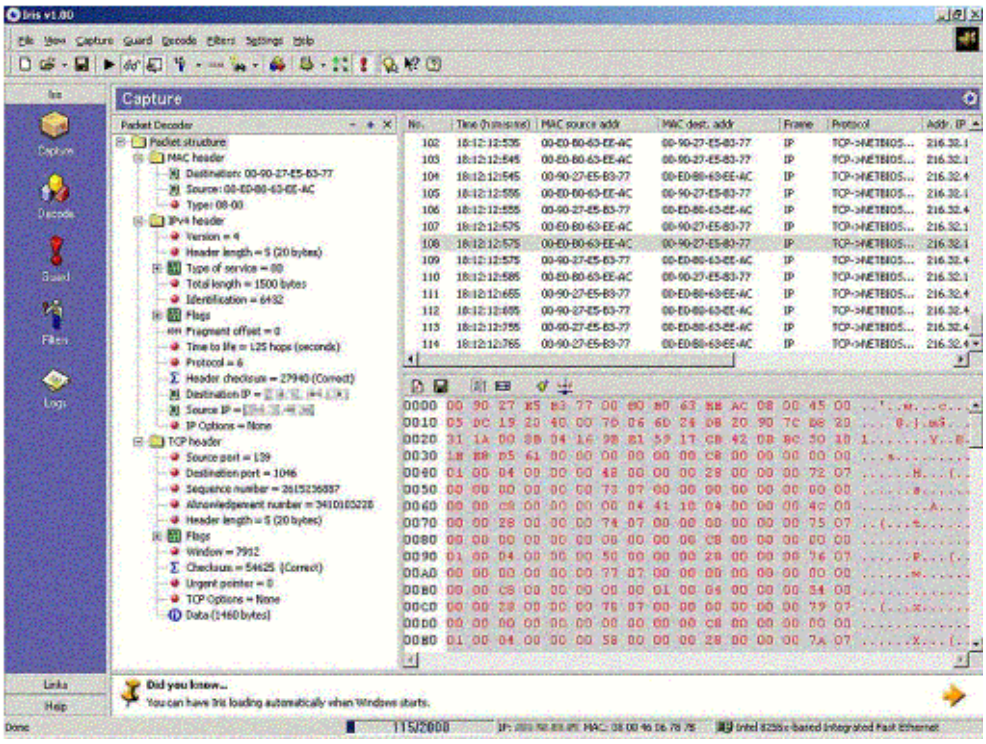
Diminuindo o impacto causado pelos ataques

O melhor procedimento para se adoptar é procurar os sites do fabricante do sistema operacional e descarregar as actualizações para as falhas. Como foi o caso do OOB (Winnuke). A Microsoft colocou um patch de correcção no seu website. Evitar o máximo de uso desnecessário da memória, assim dificultando um pouco os ataques. E sempre que puder, aumentar a capacidade de processamento e a memória RAM do sistema. Isso não vai impedir os ataques pois alguns não têm solução, mas só funcionam mesmo quando utilizados em larga escala. O Smurf por exemplo, para tornar indisponível um computador pessoal é fácil, mas um grande host para cair seria preciso muitas pessoas realizando o ataque ao mesmo tempo. Ou a utilização do software fantasma.

Sniffers

Definição

Os sniffers ou farejadores são o tipo de programas mais usados para conseguir senhas numa rede. Eles ficam residentes na memória como um cavalo de Tróia, analisando todo o tráfego que ali passa. Qualquer entrada ou saída de dados é capturada, seja num servidor FTP, uma página de chat ou um e-mail digitado. O sniffer captura os pacotes recebidos no seu estado bruto e os transforma em texto puro para serem lidos. Sempre foram mais usados em sistemas Unix, mas ultimamente todos os outros sistemas contam com poderosos sniffers. Desde sniffers comercias como o excelente Íris até sniffers mais simples, como o tcpdump e sniffers de trojans. Vamos fazer uma análise de como programas perigosos funcionam.



Ecrã de um programa de sniffer (Programa Iris) filtrando pacotes na rede.

Muitas pessoas pensam que o sniffer pode ser usado no seu computador para capturar pacotes do seu provedor. Não é bem assim. O programa tem de estar instalado no computador central de uma rede em que se quer capturar pacotes. Utilizando o exemplo do provedor, todos os seus utilizadores realizam o processo de autenticação num servidor antes de conectarem-se à rede. Assim, primeiro é necessário conseguir invadir o servidor e depois colocar o sniffer. Ele irá monitorar absolutamente tudo, às vezes até informações pessoais dos utilizadores, como endereço e telefone. Como são muitos os pacotes numa rede, o farejador é configurado para obter somente o essencial e importante: as senhas.

Capturando senhas

A principal preocupação de um operador é , ou pelo menos deveria ser, as senhas. Afinal, por mais seguro que o sistema seja, uma senha adquirida maliciosamente é sempre perigosa. O único interesse dos crackers é capturar logins e senhas. Nem se encontrar um e-mail da sua namorada para o amante o cracker deixará de se concentrar na sua tarefa. Existem algumas opções que ainda possibilitam filtrar os tipos de pacotes recebidos. Vamos supor que eu quero descobrir todas as senhas que comecem com "C". Após configurar o sniffer e esperar, ele começa a me enviar os pacotes recebidos já "seleccionados" com o que desejo.

Sniffers em trojans

Alguns trojans como o **Back Orifice** possuem sniffers como plug-ins (partes extras que podem ser anexadas ao programa). O **Buttsniffer**, um dos melhores plug-ins para o BO monitora absolutamente tudo no sistema Windows. Além de ter um ficheiro executável à parte, podendo funcionar sem depender do Back Orifice. Alguns outros trojans mais novos já possuem o sniffer embutido. A tendência do sniffer e do cavalo de tróia é de se tornarem uma ferramenta apenas, já que ambos têm características parecidas. O cavalo de tróia de e-mail **k2ps** é um bom exemplo disso. Ele monitora e envia todo tipo de senha importante por e-mail (na verdade, alguns o consideram um keylogger que é um programa que grava tudo que se escreve no teclado, eu não o considero assim pois ele é selectivo: só envia coisas importantes).

Roteadores

Alguns sniffers conseguem obter dados directo do roteador. Mesmo que seja instalada uma protecção eficaz no sistema operacional, como um anti-sniffer, não adiantaria de nada se o programa estiver a apanhar os dados directamente roteados. A correcção tem de ser feita actualizando-se o próprio roteador. O ideal seria procurar a página do fabricante e verificar se existe alguma dica ou informação sobre o assunto. Afinal, o seguro morreu de velho.

Anti-Sniffers

Como o próprio nome diz, são programas que detectam tentativas de sniffing. Ficam residentes na memória como um anti-trojans, aguardando o invasor tentar algo. Há vários tipos de anti-sniffers, alguns são péssimos e outros muito bons. Uma boa opção do software são fingir o envio de dados, para que o cracker engane-se e pense que realmente está conseguindo as senhas. Se você tem sofrido muitas invasões, comprovou-se de não ser por falhas ou trojans, monte um **honeypot** com um anti-sniffer. Com certeza deve apanhar algum intruso. Experimente o programa Anti-sniff que o seu download pode ser feito no Piratebay ou no Superdowloads (www.thepiratebay.org ou

www.superdownloads.com.br).

Scanners

Definição

Todos sabemos que nenhum sistema é perfeito. Falhas em programas e sistemas existem sim e são uma ameaça à segurança. Geralmente ocorre do seguinte modo: um administrador acidentalmente descobre que algum recurso do seu sistema gera um erro em resposta a algum tipo de pedido. Para exemplificar, suponhamos que a rede em que o administrador trabalha só se comunica gerando mensagens de "olá". Um dia ele escreve "alô" sem querer e descobre que ao enviar a mensagem para outra máquina, ela fica confusa e trava. Bem, a resposta deveria dizer "Desculpe, só olá aceito". Foi descoberto um **bug**. Agora imagine que centenas de bugs são descobertas a cada dia e que o seu sistema "confiável" de hoje, pode ser destruído amanhã. Existem algumas saídas para fazer uma análise mais garantida. A primeira é que você se torne um completo *nerd* e conheça desde o primeiro ao último bug existente. Se você trabalha com mais de um tipo de sistema operacional então, boa sorte. Uma outra saída, infinitamente mais eficaz, é a utilização de **scanners**. São programas que analisam um sistema ou rede a procura de falhas de qualquer tipo. Existem dezenas de scanners diferentes, cada um com as suas vantagens. Aprendendo melhor sobre eles, poderá proteger-se melhor e evitar que algum invasor malicioso dê um passo à sua frente.

Descobrindo falhas num host

Para entender qual a parte do seu sistema é mais vulnerável, você terá que pensar com malícia. Ora, se você usa um firewall e desabilita o acesso externo aos servidores de FTP e Telnet, com certeza eles não serão a sua maior preocupação. Em alguns hosts, deixa-se habilitada apenas a porta 80 (www) para acesso externo. Muitos sentem-se seguros desse modo. Mas enganam-se. Actualmente, a quantidade de falhas existentes em servidores World Wide Web é espantosa. Tanto Internet Information Server (IIS), quanto Apache ou qualquer outro, possuem erros. Alguns deles tão perigosas que possibilitam acesso ao interpretador de comandos do sistema, podendo gerar uma "entrada" para o invasor na rede. Outros podem fazer com que se consuma toda a memória existente, causando um *Buffer Overflow* (nome dado ao "congelamento" do sistema devido a falhas de memória). Vamos dividir o nosso estudo sobre scanners em partes: os scanners de portas, scanners de host, scanners netbios e scanners de vulnerabilidade.

Portas abertas com serviços activos

Ao contrário do que popularmente se pensa, não é tão fácil assim invadir um computador pessoal. Nós já sabemos que o sistema é composto de 65535 portas TCP e UDP. Em servidores, muitas delas possuem serviços em execução, tais como:

21 - FTP (File Transfer Protocol)
23 - TELNET
25 - SMTP (Simple Mail Transf er Protocol)
79 - FINGER
80 – WWW

Esses são apenas alguns dos muitos serviços que são executados em computadores de empresas que precisam estabelecer contacto com filiais e clientes. Realmente, um sistema que possua os seguintes serviços acima activos, pode ganhar sérios problemas com segurança. Mas imagine o seu computador na sua casa, em cima da mesa da sala, cheio de jogos dos seus filhos e que você só utiliza para ler e-mails e navegar pelas páginas web. As portas do seu computador estão totalmente inactivas. Às vezes, uma ou outra abre para estabelecer conexão com um site, ou mandar uma mensagem pelo ICQ. Mas essas são **aleatórias**, ou seja, a cada vez que uma conexão for feita, a porta mudará. Isso impede que algum invasor fique à espreita e tente conectar-se a portas padrões. Dificulta, mas não impede. Algum cavalo de tróia instalado sem você saber pode abr ir uma porta qualquer e permitir a conexão de qualquer pessoa. Para saber quais portas estão abertas em um sistema remoto, utilizamos o **scan de portas**. Existem muitos e muitos programas desse tipo. Alguns exemplos são o Cha0scan, o Shadow Scan e o Haktek.

Funcionam da seguinte maneira: tentarão conectar-se a todas as portas de um endereço ip fornecido, mostrando todas as portas encontradas “activas” e o seu conteúdo. É uma boa táctica para encontrar cavalos de tróia sem depender de **anti-vírus** , já que todos usam portas. Exemplo: eu quero analisar o meu próprio computador para saber se existe alguma porta aberta.

Para isso, vou usar o HakTek. Então mando o programa tentar scannear portas no endereço **127.0.0.1** (o chamado endereço de *loopback* . Serve para quando você não está conectado na Internet e precisa utilizar algum programa de análise que precise de endereço IP). Encontrei as seguintes portas activas:

80
1256
21554
31337

Ora, a primeira porta eu sei que é o servidor de páginas que executo no meu computador. Mas e as outras três? A porta 1256 era a que o icq havia aberto na hora. As outras duas são portas de trojans que usei como teste. A porta 21554 é do cavalo de tróia Girlfriend e a porta 31337 é do Back Orifice.

O único problema desse scan é que como ele foi feito nas três vias do tcp (syn, syn-ack, ack) pode ser facilmente detectado por sistemas IDS (detecção de intrusos). Uma boa saída é usar o **NMAP**, disponível tanto em Windows quanto em Linux. Utilizando-o, você pode scannear portas de maneira furtiva, sem realizar as três vias do tcp. Ele possui muitas opções diferentes para scan de portas, experimente-as.

Máquinas activas da subnet

O segundo tipo de scanner estudado, é o mais usado quando o objectivo do invasor é determinar todos os hosts activos da subnet e saber os seus nomes (DNS). Assim, vamos supor que o endereço principal de um provedor é www.mandiva.co.ao. Utilizamos um ping qualquer, ou o próprio scanner, e descobrimos que o endereço ip é 200.205.215.37. Agora vou utilizar o scanner de hosts para saber quais outras máquinas dessa rede estão activas.

200.205.215.9 - direccao.mandiva.co.ao

200.205.215.34 - lab.mandiva.co.ao

200.205.215.35 - milho.mandiva.co.ao

200.205.215.36 - cranico.mandiva.co.ao

200.205.215.37 - server.mandiva.co.ao

200.205.215.65 - route.mandiva.co.ao

Com isso conseguimos informações importantes do sistema. Sabemos por exemplo qual é o endereço do roteador, e onde deve ficar informações importantes. Se fosse um site de comércio electrónico por exemplo, as hipóteses de conseguir os dados era enorme, pois mesmo que o invasor não conseguisse acesso directamente ao computador **200.205.215.37** (que pode inclusive ser um firewall) ele poderia conectar-se a um outro IP da subnet e conseguir os dados a partir dele. Às vezes poderia haver algum backup perdido por aí. Alguns bons scanners de hosts são o **Shadow Scan**, o **Haktek** e o **Projecto r3x,** entre outros. Claro que para Unix e Linux existem outros muito melhores. No site www.securityfocus.com existem excelentes códigos fonte para essa tarefa.

Scanneando o netbios

Netbios é uma espécie de protocolo que facilita a comunicação de uma pequena rede, porém não é roteável. Isso significa que: você pode conseguir invadir o computador e mapear drives de todas as pessoas que estão conectadas no mesmo provedor que você, pois estão na mesma subnet. Agora, se você estiver num provedor e tentar alguma invasão em outro, ela não será possível com o SMB, apenas com o Netbios por TCP/IP (o que acaba dando quase na mesma, coloquei as diferenças por uma questão didáctica). Alguns cuidados devem ser tomados. Que hacker iniciante nunca ouviu falar de "invasão por ip", um texto que roda na internet há anos?. Pois é, ele corresponde à invasão por netbios. Para que você esteja protegido quanto a ataques, tome algumas providências:

- Se você não pertencer a nenhuma rede ou não precisar de partilhar ficheiros pela Internet, desabilite as opções "Partilhar ficheiros e impressoras" no assistente de rede do painel de

controlo do Windows. Assim você não será detectado por netbios.

- Caso você precise do protocolo, ao menos quando for partilhar algum disco, coloque uma senha. Assim dificulta o acesso não autorizado.

- Corrija os bugs do seu sistema. Especialmente se utiliza a versão Brasileira do Linux (Samba) para partilhar uma conexão netbios entre o Linux e o Windows. O Windows 98, ME, NT e 2000 também possuem alguns erros graves. Alguns deles possibilita que você possa mapear algum recurso da rede sabendo apenas o primeiro carácter e da senha do netbios.

- Utilize algum bom scanner para netbios. Um excelente é o **NAT** (Netbios Auditing Tool). Ele utiliza um dicionário de senhas para tentar conseguir acesso ao sistema, e ainda verifica se o mesmo possui falhas que possibilitem a conexão anónima. Para os que têm preguiça de usar programas em linhas de comando, sugiro o **Legion,** o **Shadow Scan** e o **Projecto r3x** . Uma outra maneira rápida de verificar se o netbios está activo é usando o comando **nbtstat** do Windows. Geralmente a sintaxe é: **nbtstat –a<endereço ip>** . Existe um modo mais fácil de se tentar invadir um computador que esteja com o netbios activo. É só ir em iniciar / executar e digitar **\\endereço ip.** Mas vamos fazer do modo convencional:

1º passo: utilizar o nbtstat.
2º passo: encontrado um computador activo (é sempre o que possui os números 00 e 03, além de ser UNIQUE no Type), vamos explorar os seus recursos.

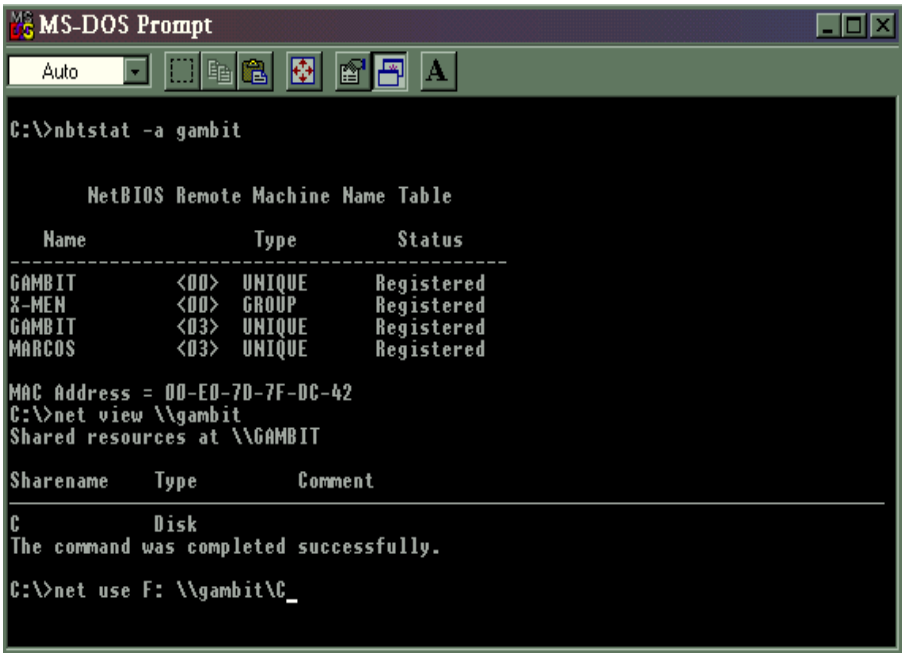
3º passo: Encontrado algum recurso disponível (no caso do exemplo, o disco C), vamos mapeá-lo (mapear significa adicionar o recurso como se fosse do seu próprio computador, como é o caso dos discos e impressoras em rede). Para mapear, utilizamos o comando:

net use F: \\gambit\C

Pronto. Mapeamos o disco C da máquina encontrada para o nosso disco F. É só ir ao Windows Explorer para aceder o disco ou simplesmente acede-lo pelo DOS (o que é muito mais rápido). Para desconectar a unidade mapeada, usaremos o seguinte comando:

net use F: /DELETE

Para uma explicação melhor sobre a sintaxe do comando NET ou para conhecer outros recursos do Windows, verifique a secção de sistemas operacionais.



NB: Se o seu computador não tiver os comandos net (net use, net view), tente instalar no painel de controlo (em rede) o protocolo netbeui e o cliente para redes Microsoft. Também verifique na sua conexão dial-up se o netbios está activo.

Verificando as vulnerabilidades em servidores HTTP e FTP

Tranquilamente o mais perigoso de todos. Os scanners de servidores HTTP e FTP, chamados de scanners de vulnerabilidade, podem encontrar erros em sistemas em segundos e ainda indicar como explorar esses erros. Essa é a principal ferramenta do "Script Kiddie", típica criança que quer ser hacker, consegue um software destes e sai fazendo varreduras em diversos sistemas. Mesmo que você não tenha inimigos, pode ser alvo de algum desses indivíduos algum dia, pois ele diverte-se em tirar páginas do ar, colocar mensagens estúpidas e rir das pessoas que o acham um mestre. Não têm interesses de espionagem, é apenas uma criança. Chegamos num problema: essas ferramentas não deviam ter a sua distribuição controlada? Se são tão perigosas, algumas até encontram-se facilmente na Internet, deviam possuir algum tipo de restrição. Todos têm direito à informação, se souberem usá-la da maneira certa.

Alguns scanners são tão poderosos que possuem funções de scanneamento de portas, hosts e vulnerabilidades num só host. Ou seja: descobre os hosts activos, analisa as portas e analisa as vulnerabilidades encontradas nas portas. E meu amigo, se não tiver uma boa política de segurança, tudo vai abaixo.

Bons scanners de vulnerabilidades para Windows: Security Shadow Scan, Retina, TWWWScan, Simpsons CGI Scanner, Stealth Scan, Lan guard, Nettools, entre outros. Para Unix, temos o Nmap, o Nessus, o ISS e uma infinidade de programas. Não importa qual sistema seja executado, geralmente esses programas podem scannear servidores em todo tipo de sistema. Do Windows ao Macintosh.

Retomando o exemplo do provedor fictício **www.mandiva.co.ao**, vamos realizar uma análise. Passamos um scanner qualquer e veremos os resultados.

Buffer overflow

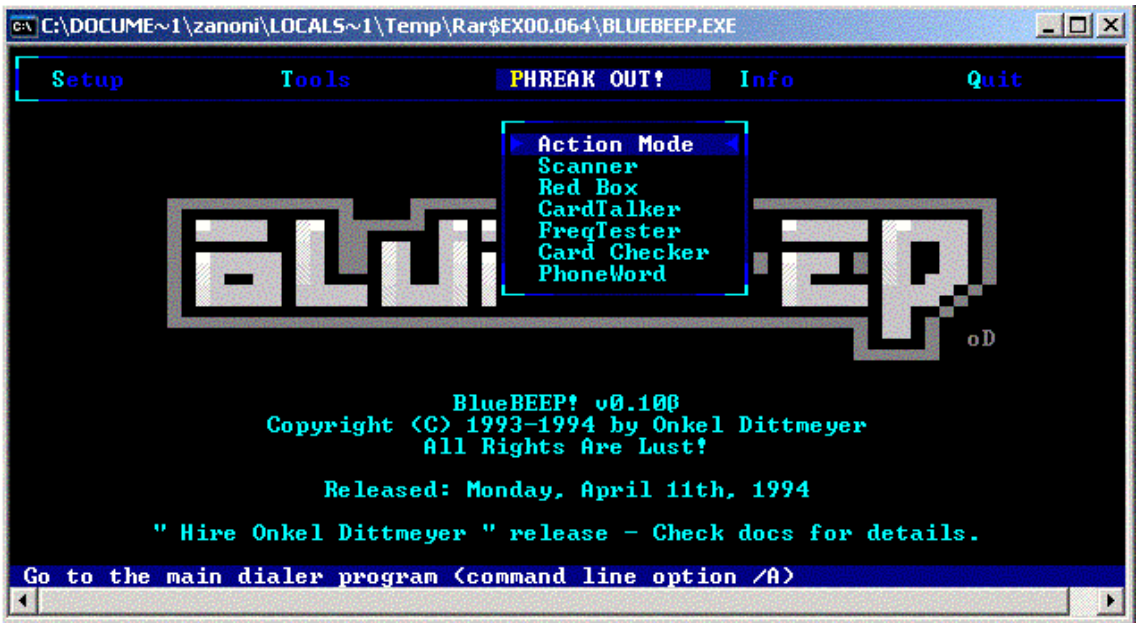
Descobrimos muita coisa. O sistema operacional usado, o servidor http e erros. Se fosse o programa real fazendo a análise, ele daria um link ou exemplos de como explorar os erros para conseguir acesso ao servidor. E para colocar um pouco mais de medo nos administradores, esses softwares têm uma opção de auto-upgrade, ou seja, actualizam-se semanalmente com novas falhas descobertas.

Analisando partes físicas

O firewall e o roteador, por também conter falhas, são muito analisados pelos scanners. Alguns deles (firewalls) são tão sofisticados que enviam vários tipos de pacotes de informação somente para "deduzir" quais deles o firewall barra e quais não, assim descobrindo erros na sua implementação e para onde redireccionam os dados. O **Shadow Scan** por exemplo, consegue descobrir o endereço real de um servidor através da grande maioria dos firewalls. Portanto não adianta apenas instalar a sua barreira. Precisa actualizá-la sempre. Para saber mais sobre o assunto e conhecer alguns problemas exclusivos que elas sofrem, consulte a secção Firewall.

Wardialers

Os wardialers ou "discadores de guerra", são programas que analisam uma lista de telefones procurando por telefones conectáveis. Por exemplo, supondo que o telefone comercial de uma empresa seja **222-323100**. Mande algum programa (como Toneloc) tentar se conectar a telefones do número **222-323000** á **222-323200**. Pode ficar um pouco caro a conta telefónica, mas a hipótese de você conseguir algum número de modem externo é grande. E geralmente utilizando sistemas com senhas ridículas (ou até sem senhas).



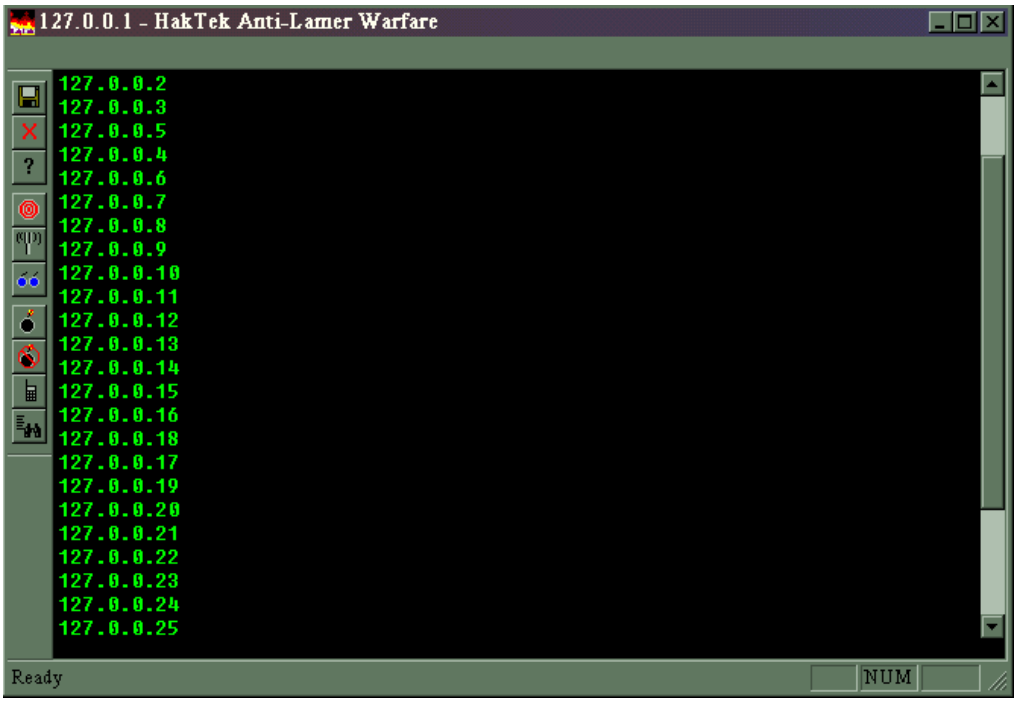
O Wardialer e o gerador de tons BlueBEEP

Instalando protecções

Para proteger-se, você precisa seguir a seguinte política: esteja sempre passando scanners no seu sistema, actualizando o seu firewall e instalando protecções extras (como detectores para scanners de porta. Quando alguém tentar varrer o seu sistema analisando os serviços activos, ele impede e lhe fornece o ip da pessoa). Mas e se você descobrir alguma falha? Na informação fornecida pelo scanner de vulnerabilidade está aonde você pode conseguir o **patch** (actualização) para essa falha. Então visite o site do fabricante (no caso do nosso exemplo do provedor Mandiva, seria a Microsoft), descarregue o patch e leia com atenção para saber como aplicá-lo no seu sistema. Se encontrar tempo para fazer tudo isso, garanto que pode lhe render algumas boas noites de sono.

Passo-a-passo: Scanneando

Scanneando hosts conhecidos de uma rede



Para esse exercício pode ser usado qualquer scanner. Usaremos o haktek.

1. Abra o programa
2. Clique no botão que parece um controlo remoto e coloque em range os ips que deseja procurar. Por exemplo: 200.187.138.1 a 200.187.138.250 (endereço fictício).

O programa mostrará todos os hosts encontrados (que estão activos) e mostrar seus respectivos nomes (se tiverem).

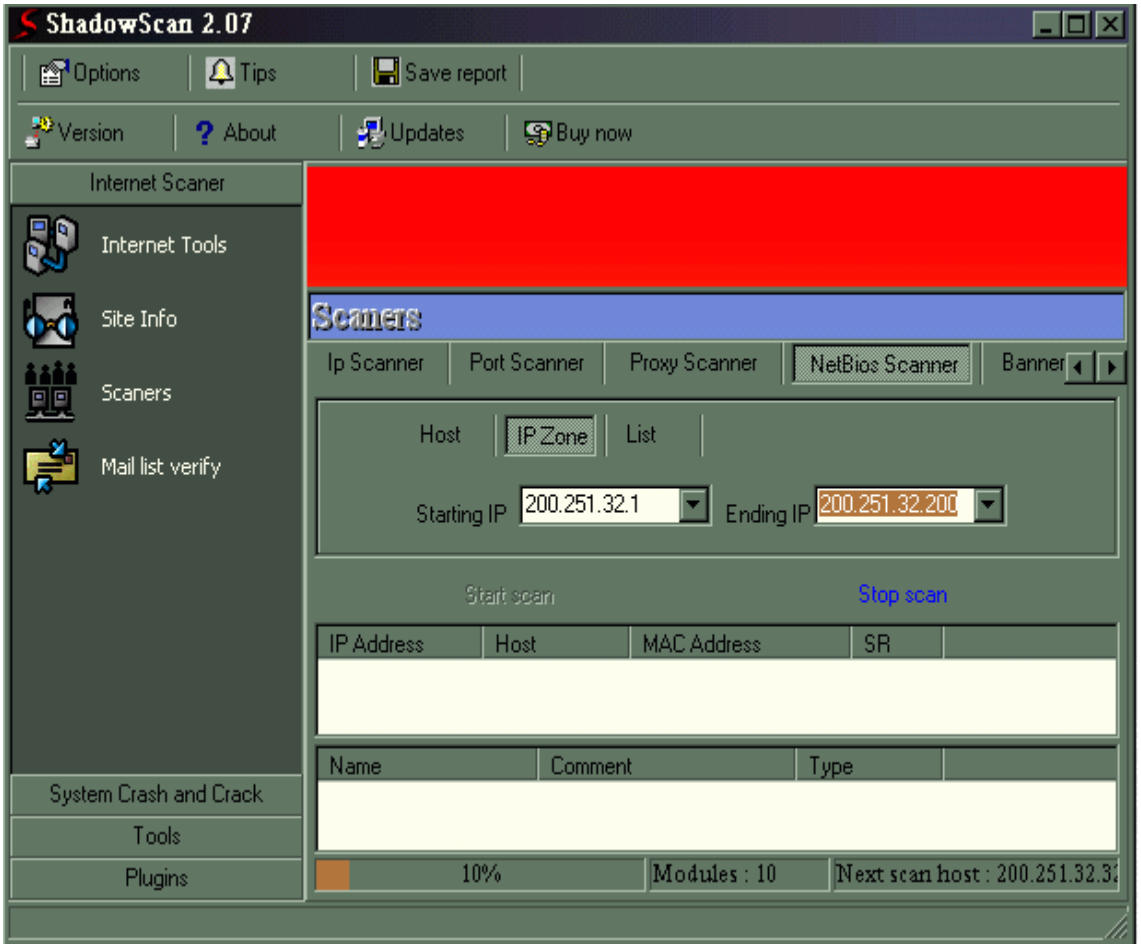
Scanneando o NetBIOS

Para realizarmos uma análise de máquinas com NetBIOS activas, utilizaremos primeiramente o programa **Shadow Scan**.

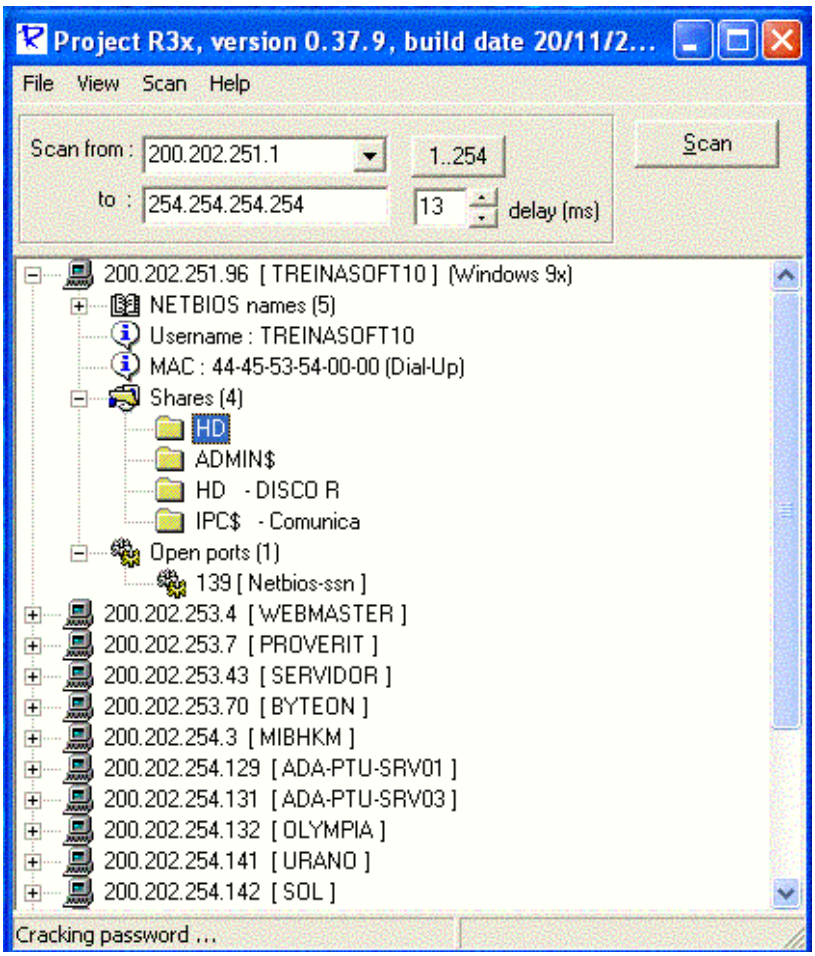
Abra o programa.

1. Clique em Internet Scanner depois em Scanners.
2. Seleccione NetBios Scanner.
3. Clique em IP Zone e coloque a subnet que você irá procurar (de qual a qual endereço ip). Não se esqueça que como o NetBIOS não é roteável você só pode fazê-lo no seu provedor ou rede local.

O ShadowScan é um dos melhores programas de segurança para Windows. Possui praticamente de tudo.



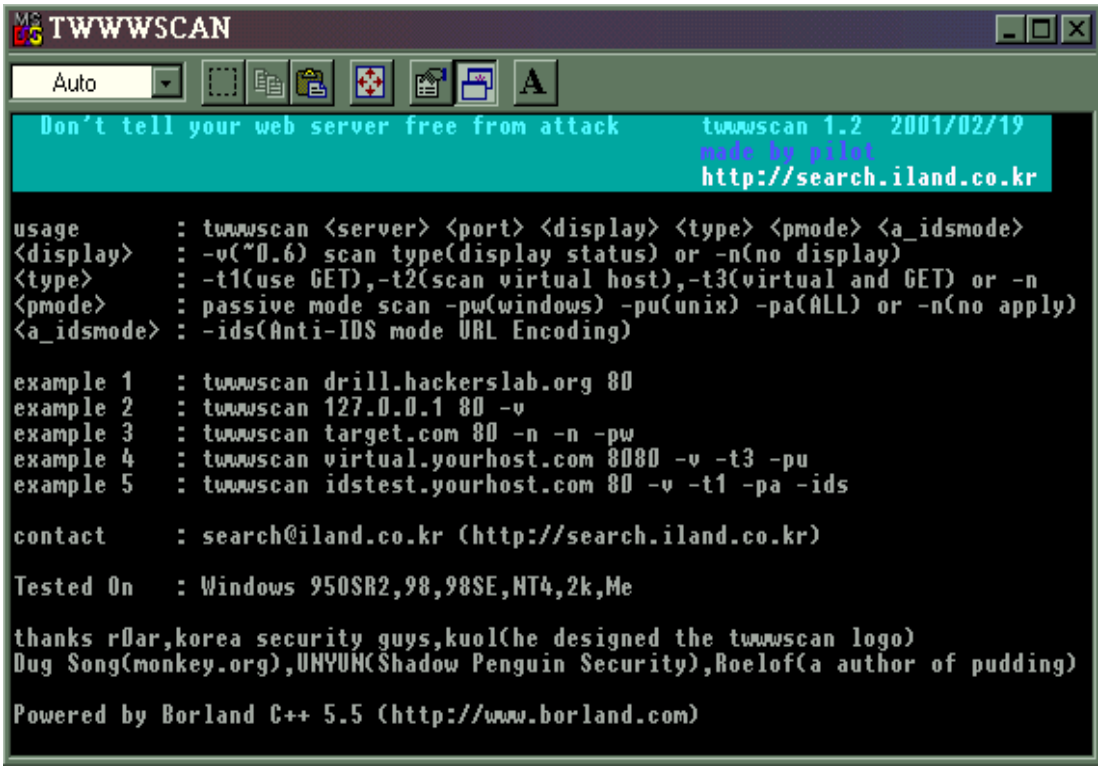
Se preferir, use o projecto R3X. Ele é mais rápido que o Shadow Scan e às vezes até mais eficiente, além de explorar um erro que descobre qualquer senha de Netbios do Windows 95, 98 e 98 SE, 2000 e XP.



Scanneando à procura de falhas

Nesse teste, utilizaremos algum dos scanners de vulnerabilidade para descobrir falhas em um host. Na minha opinião, o Shadow Security Scanner é o melhor par a Windows (ele é baseado no programa Retina do grupo EEYE) e o Nessus o melhor para Unix. Utilizaremos o TWWWSCAN como exemplo pois ele é bem simples.

1. Abra o prompt do ms-dos.
2. Execute o programa.
3. Após o programa mostrar essa tela, execute-o novamente com o seguinte comando: **twwwscan <endereço ip ou nome do host> 80 –v –t3 –pa –ids**



Pedimos ao scanner para utilizar a porta 80 (padrão), -v (mostrar o status), -t3 (utilizar dois tipos de métodos de teste), -pa (tentar erros de Unix e de Windows) e –ids (táctica para conseguir um resultado mais eficiente). O programa irá executar, testar diversas combinações e fornecer-lhe os erros encontrados.

Outros bons programas para serem testados:
Retina ***(www.eeye.com)***
Typhon *(visto no capítulo sobre falhas, pode ser pego em* http://sectools.org/)
Stealth (visto no capítulo sobre falhas, pode ser pego em http://sectools.org/*)*

NB: O segredo é bisbilhotar para descobrir as novidades. E isso é o que não falta. Visite sempre páginas como http://www.hackthissite.org/, http://sectools.org/ e http://www.hacker-soft.net/ **para obter novidades.**

Criptografia

Introdução

Criptografia é a arte da escrita oculta usada desde a antiguidade por exemplo: pelos Egípcios na sua antiga escrita. Ela é muito importante hoje em dia na internet. Mandar um e-mail confidencial da maneira convencional é muito inseguro ele pode ser interceptado no meio da transmissão ou posteriormente, por isto a necessidade do uso de programas eficientes, como o PGP. Esses programas possibilitam uma espécie de "código especial" entre você e o receptor da mensagem, fazendo com que mesmo que alguém consiga obtê-la no meio do caminho, ela será impossível de se ler.

Chaves públicas e privadas

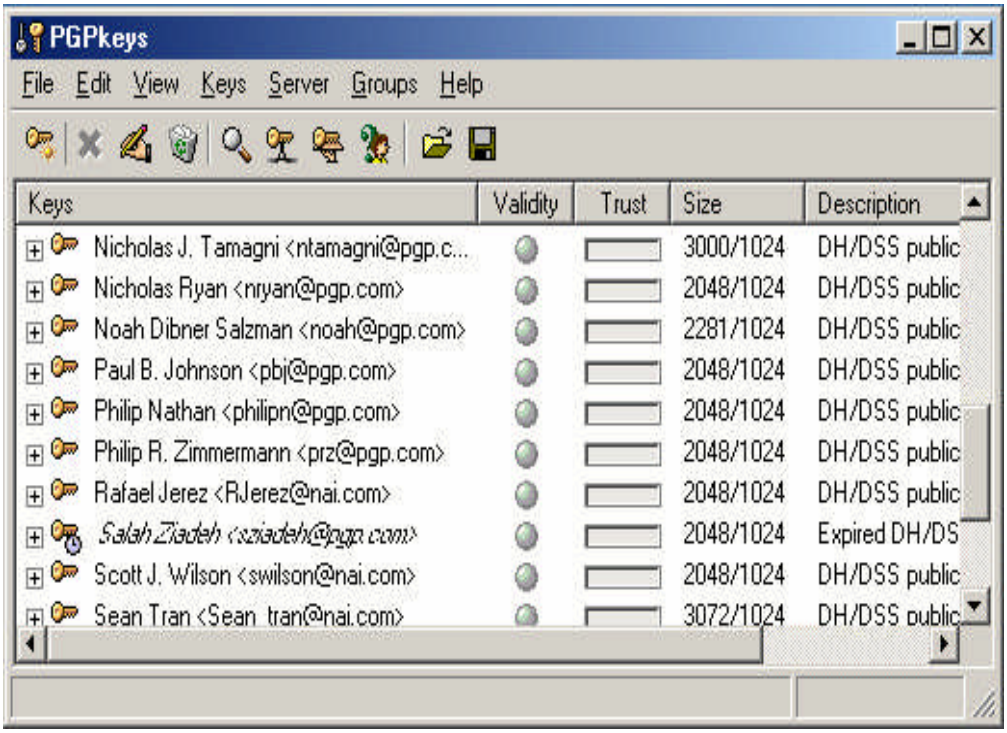
Na década de 1970 o patrão na criptografia era a criptografia simétrica onde tínhamos uma única chave (senha) para encriptar e desencriptar, tanto para o emissor quanto para o destinatário. O grande problema desse método era como transmitir com segurança esta senha.

No final da década de 70 foi desenvolvido o método da criptografia assimétrica e a tecnologia das chaves pública e privada. Você encriptava com a chave pública do destinatário e somente ele poderia desencriptar utilizando a sua chave privada, e também haveria como saber com certeza absoluta se a pessoa que mandou a mensagem era realmente quem dizia ser.

PGP

Nesse cenário foi desenvolvido o famoso programa PGP por Philip R. Zimmermann. Segundo as autoridades americanas ferindo as patentes do algoritmo RSA, ele foi processado e os voluntários da internet o ajudaram a pagar os advogados. Hoje as leis americanas já estão mais brandas e o PGP já é usado internacionalmente. Por fim a Network Associates (desenvolvedora do Mcafee Vírus Scan), comprou os direitos do PGP e hoje Zimmermann é seu empregado.

Até hoje, após várias versões desse programa ninguém nunca desencriptou uma única mensagem de 16bits do PGP e hoje ele trabalha com mais de 2000bits. Sempre gera uma nova criptografia a cada secção. Estima-se que dezenas de computadores Pentium levariam muito tempo para desencriptar uma simples mensagem de 16bits. Não é exagero. É a tecnologia. adquira o PGP no endereço **www.thepiratebay.org.** Com certeza é um bom software e vale a pena aprender a usá-lo. Mas lembre-se, apesar de difícil a criptografia não é impossível de ser decifrada. A prova disso é o grupo de internautas que conseguiu decifrar o código criptografado de um telemóvel de última geração (4G).



O programa PGP é largamente utilizado actualmente.

Saídas alternativas

Se o que você quer é apenas esconder alguns ficheiros na sua máquina para que ninguém os utilize ou encontre, há algumas saídas interessantes. Crie directórios usando caracteres ALT (secção, sobre DOS). O Windows não consegue aceder esses directórios. Esconda ficheiros comprimindo-os com GZIP ou TAR e renomeando-os (mude a extensão para DLL e coloque no directório SYSTEM do Windows, quero ver quem vai encontrar). O que manda, "mein freunds", é a imaginação. Tanto que a maioria dos hackers têm mais imaginação do que conhecimentos. Ou você acha que existe algum ser humano na face da Terra que saiba: **Pascal, Basic,Delphi, C, C++, C#, Fortran, Algol, Java, Assembler, PHP, ASP, .net, Flash, BeOS, Unix, Dec-10, Hardware, Novell, SQL, PL-Sql, Oracle, Windows, Linux, Macintosh, HP-UX, OS/2, Solaris e VAX/VMS, Virtual Server, VMWare, Redes Microsoft, Cisco, Alcatel**? Bem, se tiver alguém com certeza você encontrará o nome no "Livro do Guiness".

Crackeando

Conceito de "crackear"

Crackear no mundo da segurança significa utilizar-se de alguma técnica ou ferramenta para se descobrir algum dado criptografado ou uma senha. Actualmente é muito comum o "cracking". Conseguirem crackear o sistema de criptografia de um telemóvel novo, Video Game, um adolescente de 16 anos conseguiu quebrar a criptografia do sistema de DVD, resultando no programa DeCSS e no DivX (formato comprimido de filmes, como se fosse o mp3 da música). Sistemas simples de criptografia também são fáceis de serem decifrados. O Windows 3.11 utilizava o Trumpet Winsock para a conexão com a Internet. Após cerca de duas horas a brincar com ele, descobri como a sua criptografia funcionava. Os antigos jogos de DOS que precisavam de senhas, tal como Prince of Pérsia e Stunts são também facilmente crackeados.

O maior problema relacionado à segurança é com o descobrimento de senhas. É extremamente fácil descobri-las devido ao constante aumento da velocidade dos computadores e dos cada vez mais frágeis sistemas operacionais. Um simples cavalo de tróia ou um sniffer podem conseguir quebrar uma senha facilmente. Existem também alguns outros recursos utilizados por crackers, como utilização de wordlists e bruteforce.

Wordlists

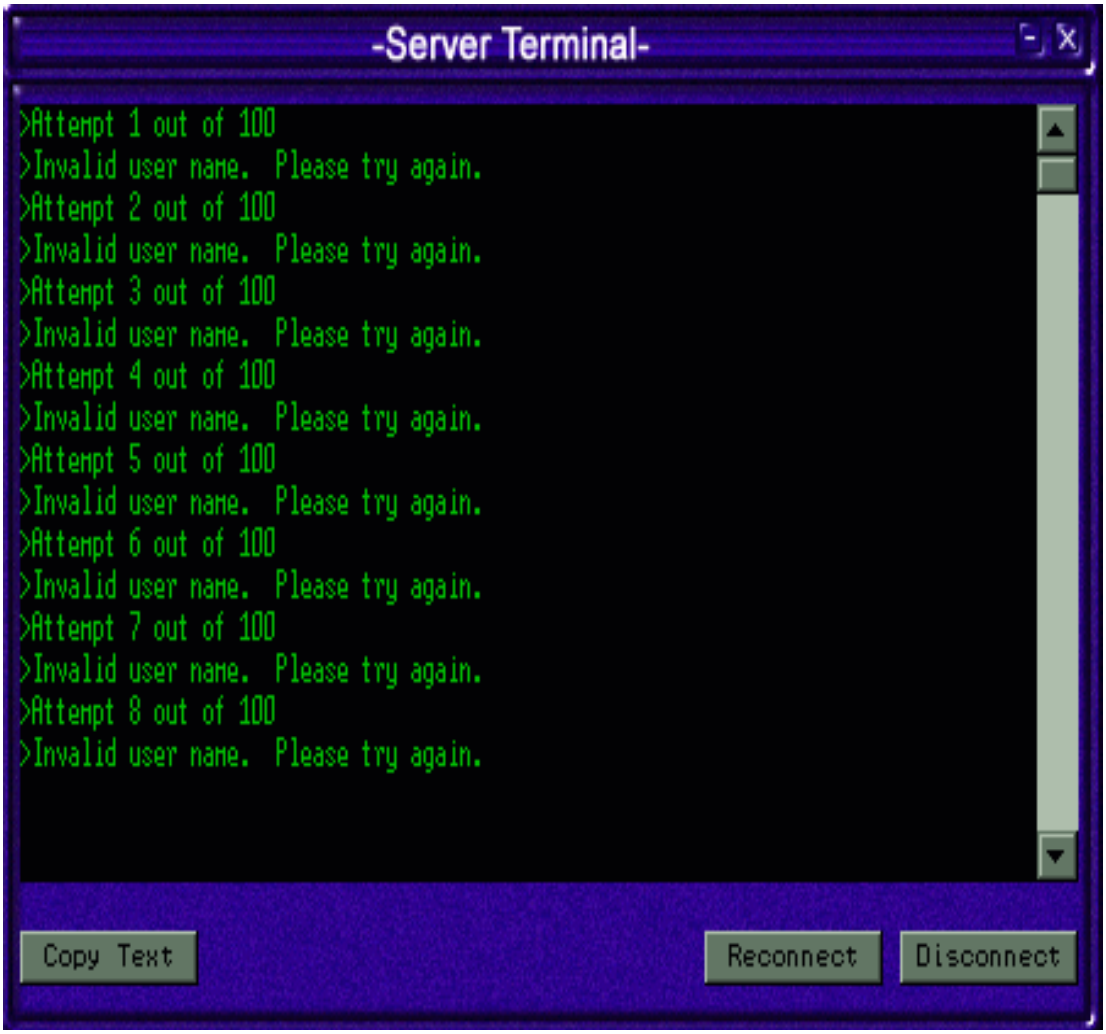
São listas de palavras criadas especialmente para se descobrir senhas. Quando você têm em mãos um ficheiro de senha do UNIX com o sistema de criptografia DES, por exemplo. A criptografia é inquebrável, mas você pode utilizar programas como o famoso **Cracker Jack** ou mesmo o **Shadow Scan**. Eles pegam num ficheiro criado por você com listas de palavras comuns (geralmente utilizadas como senhas, tal como alien3, tricolor, secreta, 101010 e outras) o criptografa utilizando o mesmo sistema das senhas de Unix (DES) e compara os ficheiros. Se o programa encontrar algum utilizador em que a criptografia tenha ficado exactamente igual, o nome lhe é informado. As palavras são colocadas verticalmente, uma em cada linha. Mais ou menos assim:

alien3
tricolor
secreta
101010

O processo de bruteforce

O método da força bruta é muito demorado. Pode levar horas, e as vezes dias. Mas continua a ser de longe o mais eficaz. Utiliza-se um programa que tenta conectar-se a um sistema utilizando todas as combinações possíveis de letras e números. Para um cracker que possui uma conexão de 56 kbps e utiliza um Pentium III 800, é improvável que consiga descobrir a senha. Para se ter alguma hipotese deve-se utilizar uma conexão dedicada (à cabo, via rádio e outras) e vários computadores. Tendo 20 computadores rápidos trabalhando cada um num sector (um a tentar descobrir senhas começadas por a, outro por b, outro por c, etc...) o tempo para se conseguir o prémio diminuirá consideravelmente. Existem alguns casos em que a força bruta é mais rápido, como quando se tenta quebrar um ficheiro de senhas localmente. Pode ser um passwd do Unix ou um mais fácil de se quebrar ainda, o PWL do Windows. O programa **CAIN**, **ShadowScan, Brutus e NAT (Netbios Auditing Tool)** são bons

programas para realizar o processo de bruteforce. Para encontrá-los já sabe: Google, Yahoo ou Bing.



Execução de um bruteforce em algum sistema vulnerável

Senhas padrão

Senhas padrões são senhas que já vêm configuradas com o sistema ou algum utilitário de actualização as configura. Existem não só nos sistemas operacionais mas também em dispositivos de hardware como roteadores. Asseguro que a lista a seguir é a maior que você já viu. Use-a para verificar se o seu sistema está vulnerável ou crie uma wordlist com as senhas padrões mais usadas de todos os sistemas. De qualquer maneira, tenho certeza que esses dados lhe serão muito interessantes. Uma falha de segurança muito comum resulta dos administradores de sistemas não trocarem as senhas padrão dos despositivos, isso abre brecha para invasões.

Lista de Senhas Padrão

Fabricante	Modelo	Versão	Tipo de acesso	Utilizador	Senha	Privilégios
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	debug	synnet	
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	tech	tech	
3COM	HiPerARC	v4.1.x	Telnet	adm	(none)	
3COM	LANplex	2500	Telnet	debug	synnet	
3COM	LANplex	2500	Telnet	tech	tech	
3COM	LinkSwitch	2000/2700	Telnet	tech	tech	
Huawei	E960			admin	admin	Admin
3COM	NetBuilder		SNMP		ILMI	snmp-read
3COM	Netbuilder		Multi	admin	(none)	Admin
3COM	Office Connect ISDN Routers	5x0	Telnet	n/a	PASSWORD	Admin
3COM	SuperStack II Switch	2200	Telnet	debug	synnet	
3COM	SuperStack II Switch	2700	Telnet	tech	tech	
3COM	OfficeConnect 812 ADSL		Multi	adminttd	adminttd	Admin
3COM	Wireless AP	QUALQUER	Multi	admin	comcomcom	Admin
3COM	CellPlex	7000	Telnet	tech	tech	User
3COM	cellplex	7000	Telnet	admin	admin	Admin
3COM	cellplex	7000		operator	(none)	Admin
3COM	HiPerARC	v4.1.x	Telnet	adm	(none)	Admin
3COM	3Com SuperStack 3 Switch 3300XM			security	security	Admin
3COM	superstack II	1100/3300		3comcso	RIP000	initialize
3COM	LANplex	2500	Telnet	tech	(none)	Admin
3COM	CellPlex		HTTP	admin	synnet	Admin
3COM	NetBuilder			(none)	admin	User
3COM	SuperStack II Switch	2700	Telnet	tech	tech	Admin
3COM	CellPlex	7000	Telnet	root	(none)	Admin
3COM	HiPerACT	v4.1.x	Telnet	admin	(none)	Admin
3COM	CellPlex	7000	Telnet	tech	(none)	Admin
3COM	CellPlex	7000	Telnet	admin	admin	Admin
3com	CellPlex	7000	Telnet	tech	tech	Admin
3com	super		Telnet	admin	(none)	Admin
3com	cellplex	7000	Multi	admin	admin	Admin
3COM	SuperStack 3	4XXX	Multi	admin	(none)	Admin
3COM	SuperStack 3	4XXX	Multi	monitor	monitor	User
3COM	SuperStack 3	4400-49XX	Multi	manager	manager	Change

3com	CellPlex	7000	Telnet	root	(none)	Admin
3com	Netbuilder		Multi	admin	(none)	Admin
3com	cellplex	7000	Telnet	operator	(none)	Admin
3com	OfficeConnect 812 ADSL	01.50-01	Multi	admin	(none)	Admin
3com	cellplex		Multi	admin	admin	Admin
3com	HiPerACT	v4.1.x	Telnet	admin	(none)	Admin
3com	3c16405		Multi	n/a	(none)	Admin
3com	3c16405		Console	Administrator	(none)	Admin
3com	Switch	3300XM	Multi	admin	admin	Admin
3com	SS III Switch	4xxx (4900 - sure)	Telnet	recovery	recovery	Fazer o reset para default
3com	OfficeConnect Wireless 11g Cable/DSL Gateway		HTTP	(none)	admin	Admin
3COM	Netbuilder		HTTP	Root	(none)	Admin
3com	3C16405		Multi	admin	(none)	Admin
3COM	3C16450		Multi	admin	(none)	Admin
3COM	3C16406		Multi	admin	(none)	Admin
3com	OfficeConnect 812 ADSL	01.50-01	Multi	admin	(none)	Admin
3com	cellplex		Multi	n/a	(none)	Admin
3com	cellplex		Multi	admin	admin	Admin
3com	HiPerACT	v4.1.x	Telnet	admin	(none)	Admin
3com	3c16405		Console	Administrator	(none)	Admin
3com	CellPlex	7000	Telnet	tech	(none)	Admin
3com	Switch	3300XM	Multi	admin	admin	Admin
3com	SS III Switch	4xxx (4900 - sure)	Telnet	recovery	recovery	Faz o reset para default
3com	OfficeConnect Wireless 11g Cable/DSL Gateway		HTTP	(none)	admin	Admin
3com	3CRADSL72	1.2	Multi	(none)	1234admin	Admin
3com	CB9000 / 4007	3	Console	Type User: FORCE	(none)	Admin
3com	officeconnect		Multi	n/a	(none)	Admin
3Com	Internet Firewall	3C16770	HTTP	admin	password	Admin
3com	superstack II Netbuilder	11.1	Multi	n/a	(none)	Admin
3COM	Office Connect ISDN Routers	5x0	Telnet?	n/a	PASSWORD	Admin
3M	VOL-0215 etc.		SNMP	volition	volition	Admin
Accelerated Networks	DSL CPE and DSLAM		Telnet	sysadm	anicust	
ACCTON	Wirelessrouter	T-online	HTTP	none	0	Admin
accton t-online	accton		Multi	(none)	0	Admin
accton t-online	accton		Multi	(none)	0	Admin
Aceex	Modem ADSL Router		HTTP	admin	(none)	Admin
Aceex	Modem ADSL Router		HTTP	admin	(none)	Admin
ADC Kentrox	Pacesetter Router		Telnet	n/a	secret	
ADIC	Scalar 100/1000		HTTP	admin	secure	Admin
ADIC	Scalar i2000		Multi	admin	password	Admin
adtran	MX2800		Telnet	n/a	adtran	Admin
adtran	Smart 16/16e		Telnet	n/a	(none)	Admin
adtran	Atlas 800/800Plus/810Plus/550		Telnet	n/a	Password	Admin
adtran	Smart 16/16e		Telnet	n/a	PASSWORD	Admin

adtran	NxIQ		Telnet	n/a	adtran	Admin
adtran	TSU IQ/DSU IQ		Telnet	n/a	(none)	Admin
adtran	Express 5110/5200/5210		Telnet	n/a	adtran	Admin
adtran	Agent Card		Telnet	n/a	ADTRAN	Admin
adtran	TSU Router Module/L128/L768/1.5		Telnet	n/a	(none)	Admin
adtran	T3SU 300		Telnet	n/a	adtran	Admin
Alcatel	PBX	4400	Port 2533	kermit	kermit	desconhecido
Alcatel	PBX	4400	Port 2533	dhs3mt	dhs3mt	desconhecido
Alcatel	PBX	4400	Port 2533	at4400	at4400	desconhecido
Alcatel	PBX	4400	Port 2533	mtch	mtch	desconhecido
Alcatel	PBX	4400	Port 2533	mtcl	mtcl	desconhecido
Alcatel	PBX	4400	Port 2533	root	letacla	desconhecido
Alcatel	PBX	4400	Port 2533	dhs3pms	dhs3pms	desconhecido
Alcatel	PBX	4400	Port 2533	adfexc	adfexc	desconhecido
Alcatel	PBX	4400	Port 2533	client	client	desconhecido
Alcatel	PBX	4400	Port 2533	install	llatsni	desconhecido
Alcatel	PBX	4400	Port 2533	halt	tlah	desconhecido
Alcatel	Office 4200		Multi	n/a	1064	Admin
Alcatel	OmniStack 6024		Telnet	admin	switch	Admin
Alcatel	Omnistack/Omniswitch		Telnet/Console	diag	switch	Admin
Alcatel	Omnistack/omniswitch		Telnet	diag	switch	Admin
Alcatel	Timestep VPN 1520	3.00.026	Permit config and console	root	permit	Admin
Alcatel	OXO	1.3	Multi	(none)	admin	User
Allied	Telesyn		Multi	manager	friend	Admin
Allied Telesyn	AT-8024(GB)		Console	n/a	admin	Admin
Allied Telesyn	AT-8024(GB)		HTTP	manager	admin	Admin
Allied Telesyn	AT Router		HTTP	root	(none)	Admin
ALLNET	T-DSL Modem	Software Version: v1.51	HTTP	admin	admin	Admin
Allnet	ALL0275 802.11g AP	1.0.6	HTTP	none	admin	Admin
Alteon	ACEDirector3		console	admin	(none)	
Alteon	ACEswitch	180e	HTTP	admin	admin	Admin
Alteon	ACEswitch	180e	Telnet	admin	(none)	
Alteon	ACEswitch	180e	HTTP	admin	linga	Admin
Alteon	AD4	9	Console	admin	admin	Admin
AMBIT	ADSL		Telnet	root	(none)	Admin
Ambit	Cable Modem 60678eu	1.12	Multi	root	root	Admin
Ambit	Cable Modem		Multi	root	root	Admin
Ambit	ntl:home 200	2.67.1011	HTTP	root	root	Admin
Amitech	wireless router and access point 802.11g 802.11b	qualquer	HTTP	admin	admin	Admin
Andover Controls	Infinity	qualquer	Console	acc	acc	Admin
AOC	zenworks 4.0		Multi	n/a	admin	Admin
APC	9606 Smart Slot		Telnet	n/a	backdoor	Admin
APC	USV Network Management Card		SNMP	n/a	TENmanUFactOryPOWER	Admin

apc	Smartups 3000		HTTP	apc	apc	Admin
APC	UPSes (Web/SNMP Mgmt Card)		HTTP	device	device	Admin
APC	Smart UPS		Multi	apc	apc	Admin
Apple	AirPort Base Station (Graphite)	2	Multi	(none)	public	public
Apple	Airport Base Station (Dual Ethernet)	2	Multi	n/a	password	Guest
Apple	Airport Extreme Base Station	2	Multi	n/a	admin	Guest
Arescom	modem/router	10XX	Telnet	n/a	atc123	Admin
ARtem	ComPoint - CPD-XT-b	CPD-XT-b	Telnet	(none)	admin	Admin
Asante	IntraSwitch		multi	IntraSwitch	Asante	Admin
Asante	IntraStack		multi	IntraStack	Asante	Admin
Asante	FM2008		Telnet	superuser	(none)	Admin
Ascend	Yurie		Multi	readonly	lucenttech2	
Ascend	Router		Telnet	n/a	ascend	Admin
Ascend	Sahara		Multi	root	ascend	
Ascom	Ascotel PBX	TODOS	Multi	(none)	3ascotel	Admin
Aspect	ACD	6	HTTP	customer	none	User
Aspect	ACD	6	Oracle	DTA	TJM	User
Aspect	ACD	7	Oracle	DTA	TJM	User
Aspect	ACD	8	Oracle	DTA	TJM	User
AVAYA	g3R	v6	Console	root	ROOT500	Admin
Avaya	Definity	G3Si	Multi	craft	(none)	Admin
Avaya	Cajun Pxxx		Multi	root	root	Admin
Avaya	Cajun	P550R P580 P880 and P882	Multi	diag	danger	Developer
Avaya	Cajun	P550R P580 P880 and P882	Multi	manuf	xxyyzz	Developer
Avaya	Pxxx	05/02/2014	Multi	diag	danger	Admin
Avaya	Pxxx	05/02/2014	Multi	manuf	xxyyzz	Admin
AVAYA	Cajun P33x	firmware before 3.11.0	SNMP	n/a	admin	Admin
Avaya	definity	up to rev. 6	qualquer	craft	crftpw	Admin
Avaya	CMS Supervisor	11	Console	root	cms500	Admin
Axis	NETCAM	200/240	Telnet	root	pass	Admin
Axis	All Axis Printserver	Todos	Multi	root	pass	Admin
Axis	Webcams		HTTP	root	pass	Admin
Axis	540/542 Print Server		Multi	root	pass	Admin
axis	2100		Multi	n/a	(none)	Admin
Axis	NETCAM	200/240		root	pass	
Bay Networks	Switch	350T	Telnet	n/a	NetICs	Admin
Bay Networks	SuperStack II		Telnet	security	security	Admin
Bay Networks	Router		Telnet	User	(none)	User
Bay Networks	Router		Telnet	Manager	(none)	Admin
Bay Networks	Router			User	(none)	User
Bay Networks	SuperStack II			security	security	Admin
Bay Networks	Switch	350T		n/a	NetICs	Admin

Belkin	F5D6130		SNMP	(none)	MiniAP	Admin
Belkin	F5D7150	FB	Multi	n/a	admin	Admin
Billion	Bipac 5100		HTTP	admin	admin	Admin
Bintec	Bianka Routers		Multi	admin	bintec	Admin
BinTec	Bianca/Brick	XM-5.1	SNMP	n/a	snmp-Trap	read/write
BinTec	x1200	37834	Multi	admin	bintec	Admin
BinTec	x2300i	37834	Multi	admin	bintec	Admin
BinTec	x3200	37834	Multi	admin	bintec	Admin
BMC	Patrol	6	Multi	patrol	patrol	User
BMC Software	Patrol	Todos	BMC unique	Administrator	the same Todos over	Admin
Breezecom	Breezecom Adapters	3.x		n/a	Master	Admin
Breezecom	Breezecom Adapters	2.x		n/a	laflaf	Admin
Breezecom	Breezecom Adapters	4.4.x	Console	n/a	Helpdesk	Admin
Breezecom	Breezecom Adapters	4.x		n/a	Super	
Breezecom	Breezecom Adapters	3.x		n/a	Master	
Breezecom	Breezecom Adapters	2.x		n/a	laflaf	
Brocade	Fabric OS	Todos	Multi	root	fivranne	Admin
Brocade	Silkworm	Todos	Multi	admin	password	Admin
Brocade	Fabric OS		Multi	admin	password	Admin
Brother	NC-3100h			(none)	access	network board access
Brother	NC-4100h			(none)	access	network board access
Brother	HL-1270n		Multi	n/a	access	network board access
Buffalo	Wireless Broadband Base Station-g	WLA-G54 WBR-G54	HTTP	root	(none)	Admin
Cabletron	Netgear modem/router and SSR			netman	(none)	Admin
Cayman	Cayman DSL			n/a	(none)	Admin
Celerity	Mediator	Multi	Multi	mediator	mediator	User
Celerity	Mediator		Multi	root	Mau'dib	Admin
Cellit	CCPro		Multi	cellit	cellit	Admin
Checkpoint	SecurePlatform	NG FP3	Console	admin	admin	Admin
CipherTrust	IronMail	Qualquer	Multi	admin	password	Admin
CISCO	Cache Engine		Console	admin	diamond	Admin
Cisco	ConfigMaker			cmaker	cmaker	Admin
cisco	cva 122		Telnet	admin	admin	Admin
Cisco	CNR	Todos	CNR GUI	admin	changeme	Admin
Cisco	Netranger/secure IDS		Multi	netrangr	attack	
Cisco	BBSM	5.0 and 5.1	Telnet or Named Pipes	bbsd-client	changeme2	database
Cisco	BBSD MSDE Client	5.0 and 5.1	Telnet or Named Pipes	bbsd-client	NULL	database
Cisco	BBSM Administrator	5.0 and 5.1	Multi	Administrator	changeme	Admin
Cisco	Netranger/secure IDS	3.0(5)S17	Multi	root	attack	Admin
Cisco	BBSM MSDE Administrator	5.0 and 5.1	IP and Named Pipes	sa	(none)	Admin
Cisco	Catalyst 4000/5000/6000	Todos	SNMP	(none)	public/private/secret	RO/RW/RW+change SNMP config
Cisco	PIX firewall		Telnet	(none)	cisco	User
Cisco	VPN Concentrator 3000 series	3	Multi	admin	admin	Admin
Cisco	Content Engine		Telnet	admin	default	Admin
cisco	3600		Telnet	Administrator	admin	Guest
Cisco	AP1200	IOS	Multi	Cisco	Cisco	Admin
cisco	GSR		Telnet	admin	admin	admin

Cisco	CiscoWorks 2000			guest	(none)	User
Cisco	CiscoWorks 2000			admin	cisco	Admin
Cisco	ConfigMaker			cmaker	cmaker	Admin
Cisco-Arrowpoint	Arrowpoint			admin	system	Admin
COM3	OLe		HTTP	admin	admin	User
Compaq	Insight Manager			administrator	administrator	Admin
Compaq	Insight Manager			anonymous	(none)	User
Compaq	Insight Manager			user	user	User
Compaq	Insight Manager			operator	operator	
Compaq	Insight Manager			user	public	User
Compaq	Insight Manager			PFCUser	240653C9467E45	User
conexant	ACCESS RUNNER ADSL CONSOLE PORT 3.27		Telnet	Administrator	admin	Admin
Corecess	Corecess 3112		HTTP	Administrator	admin	Admin
cyberguard	all firewalls	Todos	console + passport1	cgadmin	cgadmin	Admin
Cyclades	PR 1000		Telnet	super	surt	Admin
Cyclades	TS800		HTTP	root	tslinux	Admin
Dallas Semiconductors	TINI embedded JAVA Module	<= 1.0	Telnet	root	tini	Admin
Datacom	BSASX/101			n/a	letmein	Admin
Datawizard.net	FTPXQ server		FTP	anonymous	qualquer@	read/write on c:,
Davox	Unison		Multi	root	davox	Admin
Davox	Unison		Multi	admin	admin	User
Davox	Unison		Multi	davox	davox	User
Davox	Unison		Sybase	sa	(none)	Admin
Deerfield	MDaemon		HTTP	MDaemon	MServer	Admin
Demarc	Network Monitor		multi	admin	my_DEMARC	Admin
Deutsche Telekom	T-Sinus DSL 130		HTTP	admin	(none)	Admin
Develcon	Orbitor Default Console			n/a	BRIDGE	Admin
Develcon	Orbitor Default Console			n/a	password	Admin
Dictaphone	ProLog			PBX	PBX	
Dictaphone	ProLog			NETWORK	NETWORK	
Dictaphone	ProLog			NETOP	(none)	
Digicorp	Viper		Telnet	n/a	BRIDGE	Admin
Digicorp	Viper		Telnet	n/a	password	Admin
Digicorp	Router			n/a	BRIDGE	Admin
Digicorp	Router			n/a	password	Admin
Dlink	DSL-500		Multi	admin	admin	Admin
D-Link	hubs/switches		Telnet	D-Link	D-Link	
D-Link	DI-704	rev a	Multi	(none)	admin	Admin
D-Link	DI-804	v2.03	Multi	admin	(none)	Admin
D-Link	DWL 900AP		Multi	(none)	public	Admin
D-Link	DI-614+		HTTP	user	(none)	User
D-Link	DWL-614+	rev a rev b	HTTP	admin	(none)	Admin
D-Link	D-704P	rev b	Multi	admin	(none)	Admin
D-link	DWL-900AP+	rev a rev b rev c	HTTP	admin	(none)	Admin
D-Link	DI-604	rev a rev b rev c	Multi	admin	(none)	Admin

		rev e				
D-Link	DWL-614+	2.03	HTTP	admin	(none)	Admin
D-Link	D-704P		Multi	admin	admin	Admin
D-Link	DWL-900+		HTTP	admin	(none)	Admin
D-Link	DI-704		Multi	n/a	admin	Admin
D-Link	DI-604	1.62b+	HTTP	admin	(none)	Admin
D-Link	DI-624	Todos	HTTP	admin	(none)	Admin
D-Link	DI-624	Todos	HTTP	User	(none)	Admin
D-Link	DI-604	2.02	HTTP	admin	admin	Admin
D-Link	DWL 1000		HTTP	admin	(none)	Admin
D-Link	DI-514		Multi	user	(none)	Admin
D-Link	DI-614+	qualquer	HTTP	admin	(none)	Admin
D-Link	DWL 2100AP		Multi	admin	(none)	Admin
D-LINK	DSL-G664T	A1	HTTP	admin	admin	Admin
d-link	504g adsl router		HTTP	admin	admin	Admin
D-Link	DSL-302G		Multi	admin	admin	Admin
D-Link	DI-624+	A3	HTTP	admin	admin	Admin
D-Link	DWL-2000AP+	1.13	HTTP	admin	(none)	Admin
D-Link	DI-614+		HTTP	admin	admin	Admin
Draytek	Vigor	Todos	HTTP	admin	admin	Admin
Dynalink	RTA230		Multi	admin	admin	Admin
Edimax	Broadband Router	Hardware: Rev A. Boot Code: 1.0 Runtime Code 2.63	HTTP	admin	1234	Admin
Edimax	EW-7205APL	Firmware release 2.40a-00	Multi	guest	(none)	Admin
Efficient	Speedstream DSL		Telnet	n/a	admin	Admin
Efficient	5871 DSL Router	v 5.3.3-0	Multi	login	admin	Admin
Efficient	5851		Telnet	login	password	Admin
Efficient	Speedstream DSL			n/a	admin	Admin
Efficient Networks	Speedstream 5711	Teledanmark version (only .dk)	Console	n/a	4getme2	Admin
Efficient Networks	EN 5861		Telnet	login	admin	Admin
Efficient Networks	5851 SDSL Router	N/A	Console	(none)	hs7mwxkk	Admin
Elsa	LANCom Office ISDN Router	800/1000/1100	Telnet	n/a	cisco	Admin
Enterasys	ANG-1105	desconhecido	HTTP	admin	netadmin	Admin
Enterasys	ANG-1105	desconhecido	Telnet	(none)	netadmin	Admin
Enterasys	Vertical Horizon	QUALQUER	Multi	admin	(none)	Admin
Ericsson	Ericsson Acc			netman	netman	
ericsson	md110 pabx	up-to-bc9	Multi	(none)	help	varia dependendo da configuração
ericsson	ericsson acc		Multi	n/a	(none)	Admin
Ericsson	Ericsson Acc			netman	netman	
Ericsson ACC	Tigris Platform	Todos	Multi	public	(none)	Guest
E-Tech	ADSL Ethernet Router	Annex A v2	HTTP	admin	epicrouter	Admin
E-Tech	Wireless 11Mbps Router Model:WLRT03		HTTP	(none)	admin	Admin
E-Tech	Router	RTBR03	HTTP	(none)	admin	Admin
EverFocus	PowerPlex	EDR1600	Multi	admin	admin	Admin
EverFocus	PowerPlex	EDR1600	Multi	supervisor	supervisor	Admin

EverFocus	PowerPlex	EDR1600	Multi	operator	operator	Admin
Extreme Networks	All Switches		Multi	admin	(none)	Admin
F5	Bigip 540		Multi	root	default	Admin
F5-Networks	BIGIP		Multi	n/a	(none)	Admin
Flowpoint	2200 SDSL		Telnet	admin	admin	Admin
Flowpoint	DSL		Telnet	n/a	password	Admin
Flowpoint	100 IDSN		Telnet	admin	admin	Admin
Flowpoint	40 IDSL		Telnet	admin	admin	Admin
Flowpoint	Flowpoint DSL			admin	admin	Admin
Fortinet	Fortigate		Telnet	admin	(none)	Admin
Foundry Networks	IronView Network Manager	Version 01.6.00a(service pack) 0620031754	HTTP	admin	admin	Admin
Freetech	PC BIOS		Console	n/a	Posterie	Admin
Freetech	BIOS		Console	n/a	Posterie	Admin
Fujitsu Siemens	Routers		HTTP	(none)	connect	Admin
Funk Software	Steel Belted Radius	3.x	Proprietary	admin	radius	Admin
GVC	e800/rb4		HTTP	Administrator	admin	Admin
Hewlett Packard	Power Manager	3	HTTP	admin	admin	Admin
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	HPP187	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	HPP189	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	HPP196	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	INTX3	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	ITF3000	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	NETBASE	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	REGO	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	RJE	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	CONV	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	OPERATOR	SYS	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	OPERATOR	DISC	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	OPERATOR	SYSTEM	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	OPERATOR	SUPPORT	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	OPERATOR	COGNOS	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	PCUSER	SYS	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	RSBCMON	SYS	

Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	SPOOLMAN	HPOFFICE	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	WP	HPOFFICE	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	ADVMAIL	HPOFFICE DATA	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	ADVMAIL	HP	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	FIELD	SUPPORT	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	FIELD	MGR	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	FIELD	SERVICE	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	FIELD	MANAGER	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	FIELD	HPP187 SYS	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	FIELD	LOTUS	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	FIELD	HPWORD PUB	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	FIELD	HPONLY	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	HELLO	MANAGER. SYS	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	HELLO	MGR.SYS	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	HELLO	FIELD.SUPPORT	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	HELLO	OP.OPERATOR	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MAIL	MAIL	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MAIL	REMOTE	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MAIL	TELESUP	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MAIL	HPOFFICE	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MAIL	MPE	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MANAGER	TCH	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MANAGER	SYS	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MANAGER	SECURITY	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MANAGER	ITF3000	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MANAGER	HPOFFICE	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MANAGER	COGNOS	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MANAGER	TELESUP	
Hewlett-	HP 2000/3000 MPE/xx		Multi	MGR	SYS	

Packard						
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	CAROLIAN	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	VESOFT	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	XLSERVER	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	SECURITY	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	TELESUP	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	HPDESK	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	CCC	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	CNAS	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	WORD	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	COGNOS	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	ROBELLE	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	HPOFFICE	
Hewlett-Packard	HP 2000/3000 MPE/xx		Multi	MGR	HPONLY	
Hewlett-Packard	LaserJet Net Printers	Ones with Jetdirect on them	Telnet	(none)	(none)	Admin
Hewlett-Packard	LaserJet Net Printers	Ones with Jetdirect on them	HTTP	(none)	(none)	Admin
Hewlett-Packard	LaserJet Net Printers	Ones with Jetdirect on them	FTP	Anonymous	(none)	User
Hewlett-Packard	LaserJet Net Printers	Ones with Jetdirect on them	9100	(none)	(none)	User
Hewlett-Packard	webmin	0.84	HTTP	admin	hp.com	Admin
hp	sa7200		Multi	admin	admin	Admin
hp	sa7200		Multi	admin	(none)	Admin
IBM	Ascend OEM Routers		Telnet	n/a	ascend	Admin
IBM	A21m		Multi	n/a	(none)	Admin
IBM	390e		Multi	n/a	admin	Admin
ibm	a20m		Multi	n/a	admin	Admin
IBM	TotalStorage Enterprise Server		Multi	storwatch	specialist	Admin
IBM	8239 Token Ring HUB	2.5	Console	n/a	R1QTPS	Programa utilitário
sIBM	8224 HUB		Multi	vt100	public	Admin
IBM	3534 F08 Fibre Switch		Multi	admin	password	Admin
IBM	switch	8275-217	Telnet	admin	(none)	Admin
IBM	Directory - Web Administration Tool	5.1	HTTP	superadmin	secret	Admin
IBM	Hardware Management Console	3	ssh	hscroot	abc123	Admin
IMAI	Traffic Shaper	TS-1012	HTTP	n/a	(none)	Admin
Integral Technologies	RemoteView	4	Console	Administrator	letmein	Admin

Intel	Shiva		Multi	root	(none)	Admin
Intel	Express 9520 Router		Multi	NICONEX	NICONEX	User
Intel	Express 520T Switch		Multi	setup	setup	User
intel	netstructure	480t	Telnet	admin	(none)	Admin
Intel	Wireless AP 2011	2.21	Multi	(none)	Intel	Admin
Intel	Wireless Gateway	3.x	HTTP	intel	intel	Admin
Intel	Shiva			Guest	(none)	User
Intel	Shiva			root	(none)	Admin
Intel/Shiva	Mezza ISDN Router	Todos	Telnet	admin	hello	Admin
Intel/Shiva	Access Port	Todos	Telnet	admin	hello	Admin
Interbase	Interbase Database Server	Todos	Multi	SYSDBA	masterkey	Admin
Intermec	Mobile LAN	5.25	Multi	intermec	intermec	Admin
Intershop	Intershop	4	HTTP	operator	$chwarzepumpe	Admin
Intersystems	Cache Post-RDMS		Console	system	sys	Admin
intex	organizer		Multi	n/a	(none)	Admin
iPSTAR	iPSTAR Satellite Router/Radio	v2	HTTP	admin	operator	Admin
iPSTAR	iPSTAR Network Box	v.2+	HTTP	admin	operator	Admin
JD Edwards	WorldVision/OneWorld	Todos(?)	Console	JDE	JDE	Admin/SECOFR
JDE	WorldVision/OneWorld		Multi	PRODDTA	PRODDTA	Admin
JDS Microprocessing	Hydra 3000	r2.02	Console	hydrasna	(none)	Admin
Konica Minolta	magicolor 2300 DL		Multi	(none)	1234	Admin
Kyocera	EcoLink	7.2	HTTP	n/a	PASSWORD	Admin
Kyocera	Telnet Server IB-20/21		multi	root	root	Admin
Kyocera	Intermate LAN FS Pro 10/100	K82_0371	HTTP	admin	admin	Admin
LANCOM	IL11		Multi	n/a	(none)	Admin
Lantronics	Lantronics Terminal Server		TCP 7000	n/a	access	Admin
Lantronics	Lantronics Terminal Server		TCP 7000	n/a	system	Admin
Lantronix	Lantronix Terminal		TCP 7000	n/a	lantronix	Admin
Lantronix	SCS1620		Multi	sysadmin	PASS	Admin
Lantronix	SCS3200		EZWebCon downloaded from ftp.lantronix.com	login	access	Admin
Lantronix	SCS400		Multi	n/a	admin	Admin
Lantronix	SCS200		Multi	n/a	admin	Admin
Lantronix	SCS100		Multi	n/a	access	Admin
Lantronix	ETS4P		Multi	n/a	(none)	Admin
Lantronix	ETS16P		Multi	n/a	(none)	Admin
Lantronix	ETS32PR		Multi	n/a	(none)	Admin
Lantronix	ETS422PR		Multi	n/a	(none)	Admin
latis network	border guard		Multi	n/a	(none)	Admin
Linksys	WAP11		Multi	n/a	(none)	Admin
Linksys	DSL		Telnet	n/a	admin	Admin
Linksys	EtherFast Cable/DSL ROuter		Multi	Administrator	admin	Admin
Linksys	Linksys Router		HTTP	(none)	admin	Admin

	DSL/Cable					
Linksys	BEFW11S4	1	HTTP	admin	(none)	Admin
Linksys	BEFSR41	2	HTTP	(none)	admin	Admin
Linksys	WRT54G		HTTP	admin	admin	Admin
Linksys	WAG54G		HTTP	admin	admin	Admin
linksys	ap 1120		Multi	n/a	(none)	Admin
Linksys	Linksys DSL			n/a	admin	Admin
Livingston	IRX Router		Telnet	!root	(none)	
Livingston	Livingston Portmaster 3		Telnet	!root	(none)	
Livingston	Officerouter		Telnet	!root	(none)	
Livingstone	Portmaster 2R		Telnet	root	(none)	Admin
Lockdown Networks	All Lockdown Products	up to 2.7	Console	setup	changeme(exclamation)	User
longshine	isscfg		HTTP	admin	0	Admin
Lucent	B-STDX9000		Multi	(qualquer 3 characters)	cascade	
Lucent	B-STDX9000		debug mode	n/a	cascade	
Lucent	B-STDX9000	Todos	SNMP	n/a	cascade	Admin
Lucent	CBX 500		Multi	(qualquer 3 characters)	cascade	
Lucent	CBX 500		debug mode	n/a	cascade	
Lucent	GX 550		SNMP readwrite	n/a	cascade	
Lucent	MAX-TNT		Multi	admin	Ascend	
Lucent	PSAX 1200 and below		Multi	root	ascend	
Lucent	PSAX 1250 and above		Multi	readwrite	lucenttech1	Admin
Lucent	PSAX 1250 and above		Multi	readonly	lucenttech2	Admin
Lucent	Qualquermedia		Console	LUCENT01	UI-PSWD-01	Admin
Lucent	Qualquermedia		Console	LUCENT02	UI-PSWD-02	Admin
Lucent	PacketStar		Multi	Administrator	(none)	Admin
Lucent	Cellpipe 22A-BX-AR USB D		Console	admin	AitbISP4eCiG	Admin
LUCENT	M770		Telnet	super	super	Admin
Lucent	System 75			bciim	bciimpw	
Lucent	System 75			bcim	bcimpw	
Lucent	System 75			bcms	bcmspw	
Lucent	System 75			bcnas	bcnaspw	
Lucent	System 75			blue	bluepw	
Lucent	System 75			browse	browsepw	
Lucent	System 75			browse	looker	
Lucent	System 75			craft	craft	
Lucent	System 75			craft	craftpw	
Lucent	System 75			cust	custpw	
Lucent	System 75			enquiry	enquirypw	
Lucent	System 75			field	support	
Lucent	System 75			inads	indspw	
Lucent	System 75			inads	inads	
Lucent	System 75			init	initpw	
Lucent	System 75			locate	locatepw	
Lucent	System 75			maint	maintpw	
Lucent	System 75			maint	rwmaint	
Lucent	System 75			nms	nmspw	
Lucent	System 75			rcust	rcustpw	
Lucent	System 75			support	supportpw	
Lucent	System 75			tech	field	

Marconi	Fore ATM Switches		Multi	ami	(none)	Admin
maxdata	ms2137		Multi	n/a	(none)	Admin
medion	Routers		HTTP	n/a	medion	Admin
Megastar	BIOS		Console	n/a	star	Admin
Mentec	Micro/RSX		Multi	MICRO	RSX	Admin
Mentec	Micro/RSX			MICRO	RSX	Admin
MERCURY	234234	234234	SNMP	Administrator	admin	Admin
MERCURY	KT133A/686B		SNMP	Administrator	admin	Admin
Meridian	PBX	QUALQUER	Telnet	service	smile	System
Micronet	Access Point	SP912	Telnet	root	default	Admin
Micronet	Micronet SP5002		Console	mac	(none)	Admin
Microplex	Print Server		Telnet	root	root	Admin
microRouter	900i		Console/Multi	n/a	letmein	Admin
Mikrotik	Router OS	Todos	Telnet	admin	(none)	Admin
Mintel	Mintel PBX			n/a	SYSTEM	Admin
Mintel	Mintel PBX			n/a	SYSTEM	Admin
Mitel	3300 ICP	Todos	HTTP	system	password	Admin
Mitel	SX2000	Todos	Multi	n/a	(none)	Admin
Motorola	Cablerouter		Telnet	cablecom	router	Admin
Motorola	WR850G	4.03	HTTP	admin	motorola	Admin
Motorola	Wireless Router	WR850G	HTTP	admin	motorola	Admin
Motorola	SBG900		HTTP	admin	motorola	Admin
Motorola	Motorola Cablerouter			cablecom	router	Admin
motorola	vanguard		Multi	n/a	(none)	Admin
mro software	maximo	v4.1	Multi	SYSADM	sysadm	Admin
Mutare Software	EVM Admin	Todos	HTTP	(none)	admin	Admin
NAI	Intrushield IPS	1200/2600/4000	SSH + Web console	admin	admin123	Admin
NAI	Entercept		Management console	GlobalAdmin	GlobalAdmin	Admin
NEC	WARPSTAR-BaseStation		Telnet	n/a	(none)	Admin
Netcomm	NB1300		HTTP	admin	password	Admin
Netgea	FR314		HTTP	admin	password	Admin
NetGear	RM356	None	Telnet	(none)	1234	Admin
Netgear	MR-314	3.26	HTTP	admin	1234	Admin
Netgear	RT314		HTTP	admin	admin	Admin
Netgear	RP614		HTTP	admin	password	Admin
Netgear	RP114	3.26	Telnet	(none)	1234	Admin
Netgear	WG602	Firmware Version 1.04.0	HTTP	super	5777364	Admin
Netgear	WG602	Firmware Version 1.7.14	HTTP	superman	21241036	Admin
Netgear	WG602	Firmware Version 1.5.67	HTTP	super	5777364	Admin
Netgear	MR814		HTTP	admin	password	Admin
Netgear	FVS318		HTTP	admin	password	Admin
Netgear	DM602		FTP Telnet and HTTP	admin	password	Admin
netgear	FM114P		Multi	n/a	(none)	Admin
NetGear	WGT624	2	HTTP	admin	password	Admin
Netgear	FR114P		HTTP	admin	password	Admin

Netgear	ME102		SNMP	(none)	private	Admin
Netgear	WGR614	v4	Multi	admin	password	Admin
Netgear	RP114	3.20-3.26	HTTP	admin	1234	Admin
NetGenesis	NetAnalysis Web Reporting		HTTP	naadmin	naadmin	Admin
Netopia	Netopia 9500		Telnet	netopia	netopia	Admin
Netopia	R910		Multi	admin	(none)	Admin
Netopia	3351		Multi	n/a	(none)	Admin
Netopia	4542		Multi	admin	noway	Admin
Netopia	Netopia 7100			(none)	(none)	
Netopia	Netopia 9500			netopia	netopia	
Netport	Express 10/100		multi	setup	setup	Admin
Netscreen	Firewall		multi	netscreen	netscreen	Admin
netscreen	firewall		Telnet	Administrator	(none)	Admin
netscreen	firewall		Telnet	admin	(none)	Admin
netscreen	firewall		Telnet	operator	(none)	Admin
netscreen	firewall		HTTP	Administrator	(none)	Admin
Netstar	Netpilot		Multi	admin	password	Admin
Network Appliance	NetCache	qualquer	Multi	admin	NetCache	Admin
Network Associates	WebShield Security Appliance e500		HTTP	e500	e500changeme	Admin
Network Associates	WebShield Security Appliance e250		HTTP	e250	e250changeme	Admin
NGSec	NGSecureWeb		HTTP	admin	(none)	Admin
NGSec	NGSecureWeb		HTTP	admin	asd	Admin
Niksun	NetDetector		Multi	vcr	NetVCR	Admin
Nimble	PC BIOS		Console	n/a	xdfk9874t3	Admin
Nimble	BIOS		Console	n/a	xdfk9874t3	Admin
Nokia	DSL Router M1122	1.1 - 1.2	Multi	m1122	m1122	User
Nokia	MW1122		Multi	telecom	telecom	Admin
Nortel	Meridian Link		Multi	disttech	4tas	engineer account
Nortel	Meridian Link		Multi	maint	maint	Conta de manutenção
Nortel	Meridian Link		Multi	mlusr	mlusr	user
Nortel	Remote Office 9150		Client	admin	root	Admin
Nortel	Accelar (Passport) 1000 series routing switches		Multi	l2	l2	Camada 2 ler e escrever
Nortel	Accelar (Passport) 1000 series routing switches		Multi	l3	l3	camada3 (e camada2) Ler e escrever
Nortel	Accelar (Passport) 1000 series routing switches		Multi	ro	ro	Só leitura
Nortel	Accelar (Passport) 1000 series routing switches		Multi	rw	rw	Ler e escrever
Nortel	Accelar (Passport) 1000 series routing switches		Multi	rwa	rwa	Ler e escrever todos
Nortel	Extranet Switches		Multi	admin	setup	Admin
Nortel	Baystack 350-24T		Telnet	n/a	secure	Admin
Nortel	Meridian PBX		Serial	login	0	
Nortel	Meridian PBX		Serial	login	1111	
Nortel	Meridian PBX		Serial	login	8429	
Nortel	Meridian PBX		Serial	spcl	0	
Nortel	Meridian MAX		Multi	service	smile	general engineer account
Nortel	Meridian MAX		Multi	root	3ep5w2u	Admin
Nortel	Matra 6501 PBX		Console	(none)	0	Admin
Nortel	Meridian MAX		Multi	maint	ntacdmax	Conta de manutenção

Nortel	Meridian CCR		Multi	service	smile	Conta geral
Nortel	Meridian CCR		Multi	disttech	4tas	engineer account
Nortel	Meridian CCR		Multi	maint	maint	Conta de manutenção
Nortel	Meridian CCR		Multi	ccrusr	ccrusr	User account
Nortel	Meridian		Multi	n/a	(none)	Admin
Nortel	Meridian Link		Multi	service	smile	Conta geral
Nortel	Contivity	Extranet/VPN switches	HTTP	admin	setup	Admin
nortel	dms		Multi	n/a	(none)	Admin
Nortel	Business Communications Manager	3.5 and 3.6	HTTPS	supervisor	PlsChgMe	Admin
Nortel	Phone System	Todos	From Phone	n/a	266344	Installers
Nortel	Norstar		Console	266344	266344	Admin
nortel	p8600		Multi	n/a	(none)	Admin
olitec	sx 200 adsl modem router		Multi	admin	adslolitec	Admin
Omnitronix	Data-Link	DL150	Multi	(none)	SUPER	Admin
Omnitronix	Data-Link	DL150	Multi	(none)	SMDR	Admin
OMRON	MR104FH		Multi	n/a	(none)	Admin
OpenConnect	OC://WebConnect Pro		Multi	admin	OCS	Admin
OpenConnect	OC://WebConnect Pro		Multi	adminstat	OCS	Admin
OpenConnect	OC://WebConnect Pro		Multi	adminview	OCS	Admin
OpenConnect	OC://WebConnect Pro		Multi	adminuser	OCS	Admin
OpenConnect	OC://WebConnect Pro		Multi	adminview	OCS	Admin
OpenConnect	OC://WebConnect Pro		Multi	helpdesk	OCS	Admin
Openwave	WAP Gateway	Qualquer	HTTP	sys	uplink	Admin
Openwave	MSP	Qualquer	HTTP	cac_admin	cacadmin	Admin
Osicom	NETPrint	500 1000 1500 and 2000 Series	Telnet	Manager	Manager	Admin
Osicom	NETPrint and JETX Print	500 1000 1500 and 2000 Series	Telnet	sysadm	sysadm	Admin
Osicom	Osicom Plus T1/PLUS 56k		Telnet	write	private	
Osicom	NETCommuter	Telnet	debug	d.e.b.u.g	User	
Osicom	NETCommuter	Telnet	echo	echo	User	
Osicom	NETCommuter	Telnet	guest	guest	User	
Osicom	NETCommuter	Telnet	Manager	Manager	Admin	
Osicom	NETCommuter	Telnet	sysadm	sysadm	Admin	
Osicom	Osicom Plus T1/PLUS 56k			write	private	
Osicom	NETCommuter Remote Access Server		Telnet	sysadm	sysadm	Admin
Osicom	JETXPrint	1000E/B	Telnet	sysadm	sysadm	Admin
Osicom	JETXPrint	1000E/N	Telnet	sysadm	sysadm	Admin
Osicom	JETXPrint	1000T/N	Telnet	sysadm	sysadm	Admin
Osicom	JETXPrint	500 E/B	Telnet	sysadm	sysadm	Admin
Osicom	NETPrint	500	1000	1500	and 2000 Series	Telnet
Pacific	MAST 9500 Universal	ESM ver. 2.11 / 1	Console	pmd	(none)	Admin

Micro Data	Disk Array					
Panasonic	CF-28		Multi	n/a	(none)	Admin
panasonic	cf 27	4	Multi	n/a	(none)	Admin
Panasonic	CF-45		Multi	n/a	(none)	Admin
penril datability	vcp300 terminal server		Multi	n/a	system	Admin
PentaSafe	VigilEnt Security Manager	3	VigilEnt Security Manager Console	PSEAdmin	$secure$	Admin
Perle	CS9000	qualquer	Console	admin	superuser	Admin
Pirelli	Pirelli Router		Multi	admin	mu	Admin
Pirelli	Pirelli Router		Multi	admin	microbusines s	Admin
Pirelli	Pirelli Router		Multi	user	password	Admin
Planet	WAP-1900/1950/2000	02/05/2000	Multi	(none)	default	Admin
planet	Akcess Point		HTTP	admin	admin	Admin
Polycom	Soundpoint VoIP phones		HTTP	Polycom	SpIp	User
Polycom	ViewStation 4000	3.5	Multi	(none)	admin	Admin
Polycom	iPower 9000		Multi	(none)	(none)	Admin
Prestigio	Nobile	156	Multi	n/a	(none)	Admin
Psion Teklogix	9150		HTTP	support	h179350	Admin
Pyramid Computer	BenHur	Todos	HTTP	admin	admin	Admin
Radware	Linkproof		ssh	lp	lp	Admin
Radware	Linkproof	3.73.03	Multi	radware	radware	Admin
Raidzone	raid arrays			n/a	raidzone	
Ramp Networks	WebRamp			wradmin	trancell	
Ramp Networks	WebRamp			wradmin	trancell	
RedHat	Redhat 6.2		HTTP	piranha	q	User
RedHat	Redhat 6.2		HTTP	piranha	piranha	User
Research	PC BIOS		Console	n/a	Col2ogro2	Admin
Research	BIOS		Console	n/a	Col2ogro2	Admin
Ricoh	Aficio	AP3800C	HTTP	sysadmin	password	Admin
RM	RM Connect		Multi	setup	changeme	
RM	RM Connect		Multi	teacher	password	
RM	RM Connect		Multi	temp1	password	
RM	RM Connect		Multi	admin	rmnetlm	
RM	RM Connect		Multi	admin2	changeme	
RM	RM Connect		Multi	adminstrator	changeme	
RM	RM Connect		Multi	deskalt	password	
RM	RM Connect		Multi	deskman	changeme	
RM	RM Connect		Multi	desknorm	password	
RM	RM Connect		Multi	deskres	password	
RM	RM Connect		Multi	guest	(none)	
RM	RM Connect		Multi	replicator	replicator	
RM	RM Connect		Multi	RMUser1	password	
RM	RM Connect		Multi	topicalt	password	
RM	RM Connect		Multi	topicnorm	password	
RM	RM Connect		Multi	topicres	password	
RoamAbout	RoamAbout R2 Wireless Access Platform		Multi	admin	password	Admin

sagem	fast 1400w		Multi	root	1234	Admin
samsung	n620		Multi	n/a	(none)	Admin
Samsung	MagicLAN SWL-3500RG	2.15	HTTP	public	public	Admin
Senao	2611CB3+D (802.11b Wireless AP)		HTTP	admin	(none)	Admin
Server Technology	Sentry Remote Power Manager		Multi	GEN1	gen1	view/control
Server Technology	Sentry Remote Power Manager		Multi	GEN2	gen2	view/control
Server Technology	Sentry Remote Power Manager		Multi	ADMN	admn	Admin
sharp	AR-407/S402		Multi	n/a	(none)	Admin
Siemens	ROLM PBX			eng	engineer	
Siemens	ROLM PBX			op	op	
Siemens	ROLM PBX			op	operator	
siemens	hipath		Multi	n/a	(none)	Admin
Siemens	ROLM PBX			su	super	
Siemens	PhoneMail			poll	tech	
Siemens	PhoneMail			sysadmin	sysadmin	
Siemens	ROLM PBX			admin	pwp	
Siemens	PhoneMail			tech	tech	
SIEMENS	SE515		HTTP	admin	n/a	Admin
Siemens	5940 T1E1 Router	5940-001 v6.0.180-2	Telnet	superuser	admin	Admin
Siemens	PhoneMail			poll	tech	
Siemens	PhoneMail			sysadmin	sysadmin	
Siemens	PhoneMail			tech	tech	
Siemens	ROLM PBX			admin	pwp	
Siemens	ROLM PBX			eng	engineer	
Siemens	ROLM PBX			op	op	
Siemens	ROLM PBX			op	operator	
Siemens	ROLM PBX			su	super	
Siemens Nixdorf	PC BIOS		Console	n/a	SKY_FOX	Admin
Siemens Nixdorf	BIOS		Console	n/a	SKY_FOX	Admin
Siemens Pro C5	Siemens		Multi	n/a	(none)	Admin
Siips	Trojan	8974202	Multi	Administrator	ganteng	Admin
silex technology	PRICOM (Printserver)		Multi	root	(none)	Admin
sitara	qosworks		Console	root	(none)	Admin
Sitecom	All WiFi routers		Multi	(none)	sitecom	Admin
SmartSwitch	Router 250 ssr2500	v3.0.9	Multi	admin	(none)	Admin
SMC	Barricade 7004 AWBR		Multi	admin	(none)	Admin
SMC	Router	Todos	HTTP	admin	admin	Admin
SMC	SMC broadband router		HTTP	admin	admin	Admin
SMC	SMC2804WBR	v.1	HTTP	(none)	smcadmin	Admin
SMC	WiFi Router	Todos	HTTP	n/a	smcadmin	Admin
SMC	SMB2804WBR	V2	Multi	Administrator	smcadmin	Admin
SMC	7401BRA	1	HTTP	admin	barricade	Admin
SMC	7401BRA	2	HTTP	smc	smcadmin	Admin
SMC	Barricade7204BRB		HTTP	admin	smcadmin	Admin
SMC	2804wr		HTTP	(none)	smcadmin	Admin

Snapgear	Pro	Lite	and SOHO	1.79	Multi	root
Solution 6	Viztopia Accounts		Multi	aaa	often blank	Admin
SonicWALL	TODOS	TODOS	HTTP	admin	password	Admin
SOPHIA (Schweiz) AG	Protector		HTTPS	admin	Protector	Admin
SOPHIA (Schweiz) AG	Protector		SSH	root	root	Admin
Speedstream	5861 SMT Router		Multi	admin	admin	Admin
Speedstream	5871 IDSL Router		Multi	admin	admin	Admin
Speedstream	Router 250 ssr250		Multi	admin	admin	Admin
Speedstream	DSL		Multi	admin	admin	Admin
Speedstream	5667	R4.0.1	HTTP	(none)	admin	Admin
SpeedStrea m	5660		Telnet	n/a	adminttd	Admin
SpeedXess	HASE-120		Multi	(none)	speedxess	Admin
Spike	CPE		Console	enable	(none)	Admin
Sun	JavaWebServer	1.x 2.x	AdminSrv	admin	admin	Admin
Symbol	Spectrum	series 4100-4121	HTTP	n/a	Symbol	Admin
TANDBER G	TANDBERG	8000	Multi	(none)	TANDBERG	Admin
T-Comfort	Routers		HTTP	Administrator	(none)	Admin
Team Xodus	XeniumOS	2.3	FTP	xbox	xbox	Admin
Teklogix	Accesspoint		Multi	Administrator	(none)	Admin
Teledat	Routers		HTTP	admin	1234	Admin
Teletronics	WL-CPE-Router	03/05/2002	HTTPS	admin	1234	Admin
Telewell	TW-EA200		Multi	admin	password	Admin
Telindus	1124		HTTP	n/a	(none)	Admin
Telindus	SHDSL1421	yes	HTTP	admin	admin	Admin
Tellabs	Titan 5500	FP 6.x	Multi	tellabs	tellabs#1	Admin
Tellabs	7120		Multi	root	admin_1	Admin
Tiara	1400	3.x	Console	tiara	tiaranet	Admin
Troy	ExtendNet 100zx		Multi	admin	extendnet	Admin
TVT System	Expresse G5		Multi	craft	(none)	Admin
TVT System	Expresse G5 DS1 Module		Multi	(none)	enter	Admin
UNEX	Routers		HTTP	n/a	password	Admin
Unisys	ClearPath MCP		Multi	NAU	NAU	Privileged
Unisys	ClearPath MCP		Multi	ADMINISTRAT OR	ADMINISTR ATOR	Admin
Unisys	ClearPath MCP		Multi	HTTP	HTTP	Web Server Administration
US Robotics	USR8000	1.23 / 1.25	Multi	root	admin	Admin
US Robotics	USR8550	3.0.5	Multi	Qualquer	12345	Qualquer
US ROBOTICS	ADSL Ethernet Modem		HTTP	(none)	12345	Admin
US Robotics	SureConnect ADSL	SureConnect ADSL	Telnet	support	support	User
us21100060	hp omibook 6100		Multi	n/a	(none)	Admin
VASCO	VACMAN Middleware	2.x	Multi	admin	(none)	Admin
Verifone	Verifone Junior	2.05		(none)	166816	
Verilink	NE6100-4 NetEngine	IAD 3.4.8	Telnet	(none)	(none)	Guest
Visual Networks	Visual Uptime T1 CSU/DSU	1	Console	admin	visual	Admin
Watch guard	firebox 1000		Multi	admin	(none)	Admin

Watchguard	SOHO and SOHO6	Todos versions	FTP	user	pass	Admin
westell	2200		Multi	admin	password	Admin
Westell	Versalink 327		Multi	admin	(none)	Admin
Wyse	Winterm	5440XL	Console	root	wyse	Admin
Wyse	Winterm	5440XL	VNC	VNC	winterm	VNC
Wyse	Winterm	9455XL	BIOS	(none)	Fireport	BIOS
Wyse	winterm		Multi	root	(none)	Admin
Wyse	rapport	4.4	FTP	rapport	r@p8p0r+	ftp logon to controlling ftp server.
Xavi	7000-ABA-ST1		Console	n/a	(none)	Admin
Xavi	7001		Console	n/a	(none)	Admin
xd	xdd	xddd	Multi	xd	xd	Admin
Xerox	Multi Function Equipment		Multi	admin	2222	Admin
Xerox	WorkCenter Pro 428		HTTP	admin	admin	Admin
xerox	xerox		Multi	admin	admin	Admin
xerox	xerox		Multi	n/a	admin	Admin
Xerox	Document Centre 425		HTTP	admin	(none)	Admin
xerox	work centre pro 35		HTTP	admin	1111	Admin
X-Micro	X-Micro WLAN 11b Broadband Router	1.2.2 1.2.2.3 1.2.2.4 1.6.0.0	Multi	super	super	Admin
X-Micro	X-Micro WLAN 11b Broadband Router	1.6.0.1	HTTP	1502	1502	Admin
X-Micro	WLAN 11b Access Point	01/02/2002	Multi	super	super	Admin
Xylan	Omniswitch		Telnet	admin	switch	Admin
Xylan	Omniswitch		Telnet	diag	switch	Admin
Xylan	omniswitch		Multi	admin	switch	Admin
Xyplex	Routers		Port 7000	n/a	system	Admin
Xyplex	Terminal Server		Port 7000	n/a	access	User
Xyplex	Terminal Server		Port 7000	n/a	system	Admin
Xyplex	Routers		Port 7000	n/a	access	User
xyplex	switch	3.2	Console	n/a	(none)	Admin
Xyplex	Routers		Port 7000	n/a	access	User
Xyplex	Terminal Server		Port 7000	n/a	access	User
Xyplex	Terminal Server		Port 7000	n/a	system	Admin
Yakumo	Routers		HTTP	admin	admin	Admin
Zcom	Wireless		SNMP	root	admin	Admin
ZOOM	ZOOM ADSL Modem		Console	admin	zoomadsl	Admin
ZyXEL	Prestige		HTTP	n/a	1234	Admin
ZyXEL	Prestige		FTP	root	1234	Admin
ZyXEL	Prestige		Telnet	(none)	1234	Admin
ZyXEL	Prestige 643		Console	(none)	1234	Admin
ZyXEL	Prestige 652HW-31 ADSL Router		HTTP	admin	1234	Admin
ZyXEL	Prestige 100IH		Console	n/a	1234	Admin
Zyxel	ZyWall 2		HTTP	n/a	(none)	Admin
Zyxel	adsl routers	Todos ZyNOS Firmwares	Multi	admin	1234	Admin
ZyXEL	Prestige 650		Multi	1234	1234	Admin
Deutsch Telekomm	T-Sinus 130 DSL		HTTP	(none)	0	Admin
inchon	inchon	inchon	Multi	admin	admin	Admin
Benq	awl 700 wireless router	1.3.6 Beta-002	Multi	admin	admin	Admin
Konica/ Minolta	Di 2010f	n/a	HTTP	n/a	0	Admin

Sybase	EAServer		HTTP	jagadmin	(none)	Admin
Logitech	Logitech Mobile Headset		Bluetooth	(none)	0	audio access
Cisco	Ciso Aironet 1100 series	Rev. 01	HTTP	(none)	Cisco	Admin
HP	ISEE		Multi	admin	isee	Admin
IBM	3583 Tape Library		HTTP	admin	secure	Admin
Asus	wl503g	Todos	HTTP	admin	admin	Admin
Asus	wl500	Todos	HTTP	admin	admin	Admin
Asus	wl300	Todos	HTTP	admin	admin	Admin
Sigma	Sigmacoma IPshare	Sigmacom router v1.0	HTTP	admin	admin	Admin
Ricoh	Aficio 2228c		Multi	sysadmin	password	Admin
Linksys	WAP54G	2	HTTP	(none)	admin	Admin
Westell	Wirespeed		Multi	admin	password	Admin
Konica Minolta	magicolor 2430DL	Todos	Multi	(none)	(none)	Admin
KTI	KS-2260		Telnet	superuser	123456	special CLI
Oracle	Oracle RDBMS	Qualquer	Multi	system/manager	sys/change_on_install	Admin
Infosmart	SOHO router		HTTP	admin	0	Admin
Pansonic	KXTD1232		Multi	admin	1234	Admin
Areca	RAID controllers		Console	admin	0	Admin
Avaya	Definity		Multi	dadmin	dadmin01	Admin
Allied Telesyn	ALAT8326GB		Multi	manager	manager	Admin
Sun	Cobalt		HTTP	admin	admin	Admin
iblitzz	BWA711/All Models	Todos	HTTP	admin	admin	Admin
Netgear	dg834g		HTTP	admin	password	Admin
E-Con	Econ DSL Router		Router	admin	epicrouter	Admin
Allied Telesyn	AT8016F		Console	manager	friend	Admin
Dell	Laser Printer 3000cn / 3100cn		HTTP	admin	password	Admin
Sonic-X	SonicAnime	on	Telnet	root	admin	Admin
Siemens	SpeedStream 4100		HTTP	admin	hagpolm1	Admin
Wanadoo	Livebox		Multi	admin	admin	Admin
Pirelli	Pirelli AGE-SB		HTTP	admin	smallbusiness	Admin
McData	FC Switches/Directors		Multi	Administrator	password	Admin
BBR-4MG and BBR-4HG	BUFFALO	TODOS	HTTP	root	n/a	Admin
Swissvoice	IP 10S		Telnet	target	password	Admin
creative	2015U		Multi	n/a	(none)	Admin
Tandberg Data	DLT8000 Autoloader 10x		Console	n/a	10023	Manutenção
IBM	Infoprint 6700	http://www.phenoelit.de/dpl/dpl.html	Multi	root	(none)	Admin
ASUS	WL-500G	1.7.5.6	HTTP	admin	admin	Admin
Phoenix v1.14	Phoenix v1.14		Multi	Administrator	admin	Admin
asus	WL500g		HTTP	admin	admin	Admin
Symbol	AP-2412		Multi	n/a	Symbol	Admin
Symbol	AP-3020		Multi	n/a	Symbol	Admin
Symbol	AP-4111		Multi	n/a	Symbol	Admin
Symbol	AP-4121		Multi	n/a	Symbol	Admin
Symbol	AP-4131		Multi	n/a	Symbol	Admin

telindus	telindus	2002	Telnet	admin	admin	Admin
us robotic	adsl gateway wireless router		wireless router	support	support	super user access
D-Link	Dsl-300g+	Teo	Telnet	(none)	private	Admin
D-Link	DSL-300g+	Teo	HTTP	admin	admin	Admin
Billion	BIPAC-640 AC	640AE100	HTTP	(none)	(none)	Admin
Blue Coat Systems	ProxySG	3.x	HTTP	admin	articon	Admin
KTI	KS2600		Console	admin	123456	Admin
KTI	KS2260		Console	admin	123	Admin
Exabyte	Magnum20		FTP	anonymous	Exabyte	Admin
Sorenson	SR-200		HTTP	(none)	admin	Admin
D-Link	DI-524	Todos	HTTP	admin	(none)	Admin
McAfee	SCM 3100	4.1	Multi	scmadmin	scmchangeme	Admin
Zebra	10/100 Print Server		Multi	admin	1234	Admin
apple	airport5	1.0.09	Multi	root	admin	Admin
Xerox	DocuCentre 425		HTTP	admin	22222	Admin
NOKIA	7360		Multi	(none)	9999	Admin
Advantek Networks	Wireless LAN 802.11 g/b		Multi	admin	(none)	Admin
ZyXEL	Prestige 900		HTTP	webadmin	1234	Admin
LG	Aria iPECS	Todos	Console	(none)	jannie	Manutenção
Corecess	6808 APC		Telnet	corecess	corecess	User
NRG or RICOH	DSc338 Printer	1.19	HTTP	(none)	password	Admin
Xerox	Document Centre 405	-	HTTP	admin	admin	Admin
Proxim	Orinoco 600/2000	Todos	HTTP	(none)	(none)	Admin
SMC	Router/Modem	BR7401	Multi	admin	barricade	Admin
Netgear	Router/Modem		Multi	admin	password	Admin
Nullsoft	Shoutcast	01/09/2005	PLS	admin	changeme	Admin
Conexant	Router		HTTP	n/a	epicrouter	Admin
Network Everywhere	NWR11B		HTTP	(none)	admin	Admin
Netgear	MR314		Multi	admin	1234	Admin
Aethra	Starbridge EU		HTTP	admin	password	Admin
Milan	mil-sm801p		Multi	root	root	Admin
cisco	2600		Telnet	Administrator	admin	Admin
giga	8ippro1000		Multi	Administrator	admin	Admin
Netgear	GSM7224		HTTP	admin	(none)	Admin
Gericom	Phoenix		Multi	Administrator	(none)	Admin
Bausch Datacom	Proxima PRI ADSL PSTN Router4 Wireless		Multi	admin	epicrouter	Admin
Sun Microsystems	ILOM of X4100	1	HTTP	root	changeme	Admin
dlink	adsl		HTTP	admin	admin	Admin
Conexant	Router		HTTP	n/a	admin	Admin
Edimax	ES-5224RXM		Multi	admin	123	Admin
IronPort	Messaging Gateway Appliance		Multi	admin	ironport	Admin
3com	812		HTTP	Administrator	admin	Admin
Asante	FM2008		Multi	admin	asante	Admin
Broadlogic	XLT router		HTTP	webadmin	webadmin	Admin
Broadlogic	XLT router		Telnet	admin	admin	Admin
Broadlogic	XLT router		Telnet	installer	installer	Admin

Cisco	Aironet		Multi	(none)	_Cisco	Admin
Cisco	Aironet		Multi	Cisco	Cisco	Admin
Cisco	HSE		Multi	root	blender	Admin
Cisco	HSE		Multi	hsa	hsadb	Admin
Cisco	WLSE		Multi	root	blender	Admin
Cisco	WLSE		Multi	wlse	wlsedb	Admin
Digicom	Michelangelo		Multi	admin	michelangelo	Admin
Digicom	Michelangelo		Multi	user	password	User
Enterasys	Vertical Horizon	VH-2402S	Multi	tiger	tiger123	Admin
Pentaoffice	Sat Router		Telnet	(none)	pento	Admin
Pirelli	AGE ADSL Router		Multi	admin	microbusiness	Admin
Pirelli	AGE ADSL Router		Multi	user	password	User
System/32	VOS		Multi	install	secret	Admin
Tandem	TACL		Multi	super.super	(none)	Admin
Tandem	TACL		Multi	super.super	master	Admin
VxWorks	misc		Multi	admin	admin	Admin
VxWorks	misc		Multi	guest	guest	Guest
Wang	Wang		Multi	CSG	SESAME	Admin
Westell	Wang		Multi	CSG	SESAME	Admin
Westell	Wirespeed wireless router		Multi	admin	sysAdmin	Admin
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	n/a	admin	Admin
CNET	CNET 4PORT ADSL MODEM	CNAD NF400	Multi	admin	epicrouter	Admin
SMC	SMCWBR14-G	SMCWBR14-G	HTTP	(none)	smcadmin	Admin
asmack	router	ar804u	HTTP	admin	epicrouter	Admin
JAHT	adsl router	AR41/2A	HTTP	admin	epicrouter	Admin
D-Link	firewall	dfl-200	HTTP	admin	admin	Admin
ovislink	WL-1120AP		Multi	root	(none)	Admin
Linksys	WRT54G	Todos Revisions	HTTP	(none)	admin	Admin
cqualqueron	router		Multi	Administrator	admin	Admin
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	n/a	(none)	Admin
Kalatel	Calibur DSR-2000e		Multi	n/a	3477	Admin
Kalatel	Calibur DSR-2000e		on-screen menu system	n/a	8111	restaurar padrão de fabrica
IBM	T20		Multi	n/a	admin	Admin
3com	officeconnect		Multi	admin	(none)	Admin
3com	office connect	11g	Multi	admin	(none)	User
Asus	WL500g Deluxe		HTTP	admin	admin	Admin
IBM	IBM		Multi	n/a	(none)	Admin
Pentagram	Cerberus ADSL modem + router		HTTP	admin	password	Admin
SMC	Modem/Router		HTTP	cusadmin	highspeed	Customer Admin
ihoi	oihoh	lknlkn	HTTP	Administrator	pilou	Admin
corecess	3113		Multi	admin	(none)	Admin
AXUS	AXUS YOTTA		Multi	n/a	0	Admin
D-link	DSL500G		Multi	admin	admin	Admin
Asus	P5P800		Multi	n/a	admin	User
Dell	Remote Access Card		HTTP	root	calvin	Admin
d-link	di-524		HTTP	admin	(none)	Admin
ion	nelu	nel	Multi	n/a	admin	Admin
ion	nelu	nel	Multi	Administrator	admin	Admin

D-link	DSL-504T		HTTP	admin	admin	Admin
Planet	ADE-4110		HTTP	admin	epicrouter	Admin
Planet	XRT-401D		HTTP	admin	1234	Admin
ASMAX	AR701u / ASMAX AR6024		HTTP	admin	epicrouter	Admin
ASMAX	AR800C2		HTTP	admin	epicrouter	Admin
ASMAX	AR800C2		HTTP	admin	epicrouter	Admin
D-link	DSL-G604T		Multi	admin	admin	Admin
Cisco	Aironet 1200		HTTP	root	Cisco	Admin
D-link	Di-707p router		HTTP	admin	(none)	Admin
Linksys	model WRT54GC compact wireless-G broadband router		Multi	(none)	admin	Admin
Minolta QMS	Magicolor 3100	3.0.0	HTTP	operator	(none)	Admin
IBM	Remote Supervisor Adapter (RSA)		HTTP	USERID	PASSW0RD	Admin
IBM	BladeCenter Mgmt Console		HTTP	USERID	PASSW0RD	Admin
Draytek	Vigor 2600		HTTP	admin	(none)	Admin
LG	LAM200E / LAM200R		Multi	admin	epicrouter	Admin
Linksys	AG 241 - ADSL2 Gateway with 4-Port Switch		Multi	admin	admin	Admin
Micronet	3351 / 3354		Multi	admin	epicrouter	Admin
Planet	ADE-4000		Multi	admin	epicrouter	Admin
SAGEM	FAST 1400		Multi	admin	epicrouter	Admin
SMC	7204BRA		Multi	smc	smcadmin	Admin
U.S. Robotics	SureConnect 9003 ADSL Ethernet/USB Router		Multi	root	12345	Admin
U.S. Robotics	SureConnect 9105 ADSL 4-Port Router		HTTP	admin	admin	Admin
3COM	OfficeConnect ADSL Wireless 11g Firewall Router	3CRWDR100-72	HTTP	(none)	admin	Admin
ZyXEL	Prestige 645		HTTP	admin	1234	Admin
olitec (Trendchip)	sx 202 adsl modem router		HTTP	admin	admin	Admin
Entrust	getAccess	4.x and 7.x	Web Admin gui	websecadm	changeme	Admin
Cable And Wireless	ADSL Modem/Router		Multi	admin	1234	Admin
Telco Systems	Edge Link 100		Console	telco	telco	telco
ZyXEL ZyWALL Series	Prestige 660R-61C		Multi	n/a	admin	Admin
DI624	D-LINK	C3	HTTP	admin	password	Admin
SMC	SMCWBR14-G		HTTP	n/a	smcadmin	Admin
Ricoh	Aficio AP3800C	2.17	HTTP	(none)	password	Admin
Wyse	Winterm 3150		VNC	n/a	password	Admin
Ricoh	Aficio 2232C		Telnet	n/a	password	Admin
edimax	wireless adsl router	AR-7024	Multi	admin	epicrouter	Admin
Deutsche Telekom	T-Sinus 154 DSL	13.9.38	HTTP	(none)	0	Admin

Asmax	Ar-804u		HTTP	admin	epicrouter	Admin
aztech	DSL-600E		HTTP	admin	admin	Admin
comtrend	ct536+		Multi	admin	(none)	Admin
Quintum Technologies Inc.	Tenor Series	Todos	Multi	admin	admin	Admin
Alcatel	OmniPCX Office	4.1	FTP	ftp_inst	pbxk1064	Installer
Alcatel	OmniPCX Office	4.1	FTP	ftp_admi	kilo1987	Admin
Alcatel	OmniPCX Office	4.1	FTP	ftp_oper	help1954	Operator
Alcatel	OmniPCX Office	4.1	FTP	ftp_nmc	tuxalize	NMC
Netgear	ADSL Modem DG632	V3.3.0a_cx	HTTP	admin	password	Admin
Allied Telesyn	AT-AR130 (U) -10		HTTP	Manager	friend	Admin
Mikrotik	Router OS	02/09/2017	HTTP	admin	(none)	Admin
Netgear	WGT634U		HTTP	admin	password	Admin
D-Link	DI-524	Todos	HTTP	user	(none)	User
Ricoh	AP410N	1.13	HTTP	admin	(none)	Admin
3ware	3DM		HTTP	Administrator	3ware	Admin
Netgear	FWG114P		Multi	n/a	admin	password
ALCATEL	4400		Console	mtcl	(none)	User
Netgear	GS724t	V1.0.1_1104	HTTP	n/a	password	Admin
CTC Union	ATU-R130	81001a	Multi	root	root	Admin
3Com	Shark Fin	Comcast-supplied	HTTP	User	Password	Página de diagnóstico
Scientific Atlanta	DPX2100	Comcast-supplied	HTTP	admin	w2402	página de diagnóstico
Terayon	Desconhecido	Comcast-supplied	HTTP	(none)	(none)	página de diagnóstico
Terayon	Desconhecido	Comcast-supplied	HTTP	(none)	(none)	página de diagnóstico
Linksys	Comcast	Comcast-supplied	HTTP	comcast	1234	diagnóstico
NetGear	Comcast	Comcast-supplied	HTTP	comcast	1234	página de diagnóstico
Zyxel	Prestige 660HW		Multi	admin	admin	Admin
Atlantis	A02-RA141		Multi	admin	atlantis	Admin
Atlantis	I-Storm Lan Router ADSL		Multi	admin	atlantis	Admin
Linksys	WAG54GS		Multi	admin	admin	Admin
IBM	T42		HTTP	Administrator	admin	Admin
Huawei	MT880r		Multi	TMAR#HWMT8007079	(none)	Admin
OKI	C5700		HTTP	root	the 6 last digit of the MAC adress	Admin
Sagem	F@st 1200 (Fast 1200)		Telnet	root	1234	User
Minolta QMS	Magicolor 3100	3.0.0	HTTP	admin	(none)	Admin
Ricoh	Aficio 2020D		HTTP	admin	password	Admin
Juniper	ISG2000		Multi	netscreen	netscreen	Admin
Linksys/ Cisco	RTP300 w/2 phone ports	1	HTTP	admin	admin	Admin
Linksys/ Cisco	RTP300 w/2 phone ports	1	HTTP	user	tivonpw	update access
samsung	modem/router	aht-e300	Multi	admin	password	Admin
mediatrix 2102	mediatrix 2102		HTTP	admin	1234	Admin
Draytek	Vigor 2900+		HTTP	admin	admin	Admin
smc	smc 7904BRA		Multi	(none)	smcadmin	Admin
DLINK	604		Multi	n/a	admin	Admin
ZyXel	Prestige P660HW		Multi	admin	1234	Admin

topsec	firewall		Multi	superman	talent	Admin
US Robotics	USR9110		HTTP	admin	(none)	Admin
CNET	CSH-2400W	unk	HTTP	admin	1234	Admin
Psionteklogix	9160	1	HTTP	admin	admin	Admin
AirTies RT-210	AirTies RT-210	AirTies RT-210	Telnet	admin	admin	Admin
Siemens	SE560dsl		Multi	admin	admin	Admin
Psionteklogix	9160	1	HTTP	admin	admin	Admin
Netgear	WG602	1.7.x	HTTP	admin	password	Admin
SSA	BPCS	Up to 5.02	Multi	SSA	SSA	Admin
Minolta PagrPro	QMS 4100GN PagePro		HTTP	n/a	sysadm	Admin
Secure Computing	Webwasher	Todos	HTTP	admin	(none)	Admin
Cisco	CallManager		HTTP	admin	admin	Admin
Cisco	WSLE	Todos	Todos	wlseuser	wlsepassword	User
Cisco	WLSE	Todos	Console	enable	(none)	enable
Netgear	CG814CCR	2	Multi	cusadmin	highspeed	Admin
Brother	NC-2100p		Multi	(none)	access	Admin
Signamax	065-7726S		Multi	admin	admin	Admin
Panasonic	PBX TDA 100/200/400	Todos	Console	(none)	1234	Admin
Zyxel	Router	650-1	Telnet	(none)	1234	Admin
Huawei	mt820	V100R006C01B021	HTTP	admin	admin	Admin
Irongate	NetSurvibox 266	1	HTTP	admin	NetSurvibox	Admin
netgear	sc101		management software	admin	password	Admin
Bluecoat	ProxySG (all model)	SGOS 3 / SGOS4	HTTPS (8082)	admin	admin	Admin
SMC	smc7904wbrb		Multi	(none)	smcadmin	Admin
SMC	SMC7004VBR		HTTP	n/a	smcadmin	Admin
Symbol	CB3000	A1	HTTPS	admin	symbol	Admin
Xerox	240a		HTTP	admin	x-admin	Admin
Ericsson	MD110		Telnet	MD110	help	Admin
Ericsson	BP250		HTTP	admin	default	Admin
Cisco	Cisco Wireless Location Appliance	2700 Series prior to 2.1.34.0	Multi	root	password	Admin
Topcom	Wireless Webr@cer 1154+ PSTN (Annex A)	V 4.00.0	HTTP	admin	admin	Admin
Topcom	Wireless Webr@cer 1154+ PSTN (Annex A)	V 0.01.06	HTTP	admin	admin	Admin
Topcom	Wireless Webr@cer 1154+ PSTN (Annex A)	V 0.01.09	HTTP	admin	admin	Admin
Sercom	IP806GA		HTTP	admin	admin	Admin
Sercom	IP806GB		HTTP	admin	admin	Admin
draytek	Vigor3300 series		Telnet	draytek	1234	Admin
netgear	DG834GT	192.168.0.1	Multi	admin	Password	Admin
d-link	ads500g		HTTP	admin	admin	Admin
Konica Minolta	magicolor 5430 DL		HTTP	admin	administrator	Admin
planet	akcess point		HTTP	admin	admin	Admin
Sharp	AR-M355N		HTTP	admin	Sharp	Admin
Sharp	MX-3501n		HTTP	Administrator	admin	Admin
3com	LANplex	2500	Telnet	n/a	admin	Admin

Cisco	MeetingPlace		Console	technician	2 + last 4 of Audio Server chasis Serial case-sensitive + 561384	Admin
cuproplus	bus		Multi	n/a	(none)	Admin
wline	w3000g		HTTP	admin	1234	Admin
Tandberg	6000MXP		Multi	Admin	(none)	Admin
hp	2300		Multi	admin	admin	Admin
Actiontec	Wireless Broadband Router		Multi	admin	password	Admin
D-Link	DI-634M		Multi	admin	(none)	Admin
Silvercrest	WR-6640Sg		HTTP	admin	admin	Admin
Deutsche Telekom	T-Sinus 1054 DSL	Todos	HTTP	(none)	0	Admin
Netgear	FVS114	GR	HTTP	admin	password	Admin
Nokia	M1921		Telnet	(none)	nokai	Admin
Nokia	ADSL router M1921		Telnet	(none)	nokia	Admin
Siemens	Speedstream SS2614	Hardware V. 01	HTTP	n/a	admin	Admin
TrendNET	TEW-435BRM	1	HTTP	admin	password	Admin
Netgear	RO318		Multi	admin	1234	Admin
ZTE	ZXDSL 831	4.2	Multi	ADSL	expert03	Admin
Alcatel	7300 ASAM		TL1	SUPERUSER	ANS#150	Admin
Shoretel	Todos		HTTP	admin	changeme	Admin
stratacom	Todos	Todos	Multi	stratacom	stratauser	Admin
Toshiba	E-Studio 3511c		HTTP	Admin	123456	Admin
Xerox	WorkCentre 7132		Multi	11111	x-admin	Admin
Sharp	AL-1655CS		HTTP	admin	Sharp	Admin
3Com	3CRWDR100A-72	2.06 (Sep 21 2005 14:24:48)	HTTP	admin	1234admin	Admin
Juniper	Netscreen	3.2	Console	serial#	serial#	Admin
Cisco	ONS	Todos	Multi	CISCO15	otbu+1	Admin
Telewell	TW-EA501	v1	Multi	admin	admin	Admin
NOMADIX	AG5000		Telnet	admin	(none)	Admin
Mediatrix	MDD 2400/2600		Console	administrator	(none)	Admin
Dell	2161DS Console Switch		HTTP	Admin	(none)	Admin
digicom	Wavegate 54C		HTTP	Admin	(none)	Admin
Siemens	Hipath	3300-3750	Custom program	31994	31994	Admin
Sparklan	Wx-6215 D and G		HTTP	admin	admin	Admin
Applied Innovations	AIscout		Multi	scout	scout	supervisor
Planet	WAP 4000		Multi	admin	admin	Admin
fon	La fonera	0.7.1 r1	HTTP	admin	admin	Admin
Lanier	Digital Imager	LD124c	HTTP	admin	(none)	Admin
Netgear	WGT624		Serial console	Gearguy	Geardog	Admin
Dell	PowerConnect 2724		HTTP	admin	(none)	Admin
D-Link	DI-524	E1	Telnet	Alphanetworks	wrgg15_di524	Admin
DIGICOM	Michelangelo Wave108		HTTP	root	admin	Admin
US Robotics	USR9106		HTTP	admin	admin	Admin
SpeedStream 5200-Serie	SpeedStream		Telnet	Administrator	admin	Admin
Siemens	Gigaset	Todos	Multi	(none)	0	Admin

Comtrend	ct-536+		HTTP	admin	admin	Admin
Comtrend	ct-536+		HTTP	admin	1234	Admin
2wire	wifi routers	n/a	HTTP	none	Wireless	Admin
Sphairon	(Versatel WLAN-Router)		Multi	admin	passwort	Admin
HP	MSL Series Libraries		Multi	Factory	56789	Admin
Overland	NEO Series Libraries		Multi	Factory	56789	Admin
OKI	6120e and 421n		HTTP	admin	OkiLAN	Admin
siemen	speedstream 5400	059-e440-a02	HTTP	admin	(none)	Admin
Various	DD-WRT	v23 SP1 Final	HTTP	root	admin	Admin
Aztecj	DSL 600EU	62.53.2	Telnet	root	admin	Admin
Aztecj	DSL 600EU	62.53.2	HTTP	isp	isp	Admin
Linksys	rv082		Multi	admin	(none)	Admin
AVAYA	P333		Telnet	Administrator	ggdaseuaimhrke	Admin
AVAYA	P333		Telnet	root	ggdaseuaimhrke	Admin
Infoblox	INFOBLOX Appliance		Multi	admin	(none)	Admin
Avocent	Cyclade	Linux hostname 2.6.11 #1 Tue Mar 28 13:31:20 PST 2006 ppc desconhecido	Multi	root	tslinux	Admin
EMC	DS-4100B		Console	admin	(none)	Admin
Citel	Handset Gateway		HTTP	citel	password	Admin
Citel	Handset Gateway		Telnet	(none)	citel	Admin
Grandstream	GXP-2000		HTTP	admin	1234	Admin
SysMaster	M10		HTTP	admin	12345	Admin
pfSense	pfSense Firewall	1.0.1	Multi	admin	pfsense	Admin
ASUS	ASUS WL-330 Pocket Wireless Access Point		HTTP	admin	admin	Admin
Planex	BRL-04UR		Multi	admin	0	Admin
maxdata	7000x		Multi	n/a	(none)	Admin
Conceptronic	C54BRS4		Multi	admin	1234	Admin
OPEN Networks	812L		HTTP	root	0P3N	Admin
Thomson	Wireless Cable Gateway	DCW725	HTTP	(none)	admin	Admin
Thomson	SpeedTouch AP	180	HTTP	n/a	admin	Admin
KASDA	KD318-MUI	kasda adsl router and modem	Multi	admin	adslroot	Admin
Intracom	jetSpeed	520/520i	Multi	admin	admin	Admin
cisco	2600 router		Telnet	cisco	(none)	Admin
Edimax	EW-7206APG		HTTP	admin	1234	Admin
SMC	SMCWBR14-G		HTTP	(none)	smcadmin	Admin
ASUS	ASUS SMTA Router	Firmware: 3.5.1.3(C0.0.7.4) - Hardware: 1100(AVG6002 REV:2.26A)	HTTP + Telnet	admin	admin	Admin
linksys	wrt54g		Multi	admin	admin	Admin
Addon	GWAR3000/ARM8100		HTTP	admin	admin	Admin
ZyXeL	660HW		HTTP	admin	(none)	Admin
Netgear	Wifi Router	WGT 624 v3	HTTP	admin	password	Admin
Apache	Tomcat Web Server Administration Tool	5	HTTP	admin	(none)	Admin

Sitecom	WL-0xx up to WL-17x	all	Multi	admin	admin	Admin
greatspeed	DSL		HTTP	netadmin	nimdaten	Admin
Nokia	M1122	desconhecido	Multi	(none)	Telecom	Admin
Nortel	VPN Gateway		Console	admin	admin	Admin
Fortinet	Fortigate		Console	maintainer	bcpb+serial#	Admin
Fortinet	Fortigate		Console	maintainer	admin	Admin
Crossbeam	COS / XOS		Lilo boot	(none)	x40rocks	Admin
Edimax	Edimax Fast Ethernet Switch		HTTP	admin	password	Admin
Prolink	H9000 Series		HTTP	admin	password	Admin
netgear	dg834		Multi	n/a	admin	Admin
Brother	MFC-420CN	Firmware Ver.C	Multi	n/a	access	Admin
D-Link	DWL-G730AP	1.1	HTTP	admin	(none)	Admin
Fujitsu Siemens	Fibre Channel SAN storage FX 60		HTTP	manage	!manage	Admin
Fujitsu Siemens	Fibre Channel SAN storage FX 60		Telnet	manage	!manage	Admin
Spectra Logic	64000 Gator		Multi	administrator	(none)	Admin
Spectra Logic	64000 Gator		Multi	operator	(none)	User
HP	t5000 Thin Client series		Console	Administrator	admin	Admin
Huawei	MT880		HTTP	admin	admin	Admin
ATL	P1000		Multi	operator	1234	User
ATL	P1000		Multi	Service	5678	Service Maintenance Admin
Topcom	Skyr@cer Pro AP 554	1.93	HTTP	admin	admin	Admin
Netgear	FSM7326P 24+2 L3 mANAGED PoE Switch		HTTP	admin	(none)	Admin
seninleyimben	@skan	el rattani	FTP	admin	admin	Admin
Sagem	Livebox		Multi	admin	admin	Admin
Inventel	Livebox		Multi	admin	admin	Admin
INOVA	ONT4BKP (IP clock)	Todos	Telnet	iclock	timely	Admin
D-Link	G624T		Multi	admin	admin	Admin
Ricoh	Ricoh	Aficio MP 3500 1.0	Multi	admin	(none)	Admin
infacta	group mail		Multi	Administrator	(none)	Admin
Linksys	WRT54GS	V4	HTTP	admin	admin	Admin
Lanier	LD335		HTTP	supervisor	(none)	Admin
3COM	OfficeConnect 812 ADSL		Multi	Administrator	admin	Admin
Comcast Home Networking	Comcast Home Networking	TODOS	HTTP	comcast	(none)	Admin
SMC	SMC8013WG-CCR	2.11.19-1d	HTTP	mso	w0rkplac3rul3s	Admin
Zyxel	ES-2108		Multi	admin	1234	Admin
D-Link	WBR-1310	B-1	Multi	admin	(none)	Admin
Sharp	AR-M155		HTTP	admin	Sharp	Admin
Sharp	MX-5500		HTTP	admin	admin	Admin
Toshiba	E-Studio 4511c		HTTP	admin	123456	Admin
Leviton	47611-GT5		Multi	admin	leviton	Admin
Nortel	Passport 2430		Telnet	Manager	(none)	Admin
BUFFALO	WLAR-L11-L / WLAR-L11G-L		HTTP	root	(none)	Admin
Xerox	6204		Multi	n/a	0	Admin

iDirect	iNFINITY series	3000/5000/7000	Telnet	admin	P@55w0rd!	Admin
iDirect	iNFINITY series	3000/5000/7000	ssh	root	iDirect	Admin
US Robotics	USR5462		HTTP	n/a	admin	Admin
telecom	home hauwei		Multi	operator	(none)	Admin
Davolink	DV2020		HTTP	user	user	desconhecido
motorola	sgb900		HTTP	admin	motorola	Admin
zyxel	g-570s		Multi	n/a	admin	Admin
Beetel	ADSL Modem	220X	Multi	admin	password	Admin
Linksys	WAG354G	2	HTTP	admin	admin	Admin
QLogic	SANbox 5602 Fibre Channel Switch		Multi	admin	password	Admin
QLogic	SANbox 5602 Fibre Channel Switch		Multi	images	images	User
Lucent	Cellpipe	20A-GX-UK	Console	n/a	admin	Admin
Buffalo Technology	TeraStation		Multi	admin	password	Admin
linksys	wag354g		Telnet	admin	admin	User
Thomson	TCW-710		Multi	(none)	admin	Admin
Ricoh	Aficio 551		Multi	(none)	sysadm	Admin
Cisco	PIX	6.3	Console	enable	(none)	Admin
Guru	Wireless ADSL2		HTTP	admin	admin	Admin
Colubris	MSC		HTTP	admin	admin	User
Netgear	WGR614	v6	HTTP	admin	draadloos	Admin
T-Com	Speedport Router Family	Todos	HTTP	(none)	0	Admin
Mikrotik	Mikrotik		Telnet	admin	(none)	Admin
Zyxel	Prestige 650HW31	31	Telnet	192.168.1.1 60020	@dsl_xilno	Admin
Netgear	MR814	v1	HTTP	admin	password	Admin
Motorola	SURFboard	SBV5120	HTTP	admin	motorola	Admin
linksys	BEFW11S4	2	Multi	(none)	admin	Admin
WLAN_3D	Router		HTTP	Administrator	admin	Admin
Brother	HL5270DN		HTTP	admin	access	Admin
TrendMicro	InterScan 7.0		HTTP	admin	imss7.0	Admin
Promise	NS4300N NAS		Shell	engmode	hawk201	Admin
Ricoh	Aficio 1018d		HTTP	n/a	sysadm	Admin
Ricoh	Aficio 1013F		HTTP	n/a	sysadm	Admin
Polycom	SoundPoint IP Phones		HTTP	Polycom	456	Admin
Xerox	DocumentCenter 186	2007		admin	x-admin	admin
Netgear	ReadyNas Duo	RND2000		admin	netgear1	Admin
Netgear	ReadyNas Duo	RND2000		admin	infrant1	Admin
Konica Minolta	magicolor 1690MF			(non)	sysAdmin	Administrator
Konica Minolta	magicolor 1690MF			(non)	sysAdmin	Administrator
Kyocera	Printer	qualquer		(none)	admin00	
Buffalo	WHR-G300N			root		Administrator
Kyocera Printers	2020D			n/a	admin00	Admin
Westell	Ultraline Series3 A90-9100EM15-10	1.02.00.04		admin	password1	Admin
CNet	CWR- 500 Wireless-B Router			Admin	admin	Admin
ZyXel Based (Generic)	Broadband SOHO Router	925ahcd on circuit board print		admin	0000	Admin

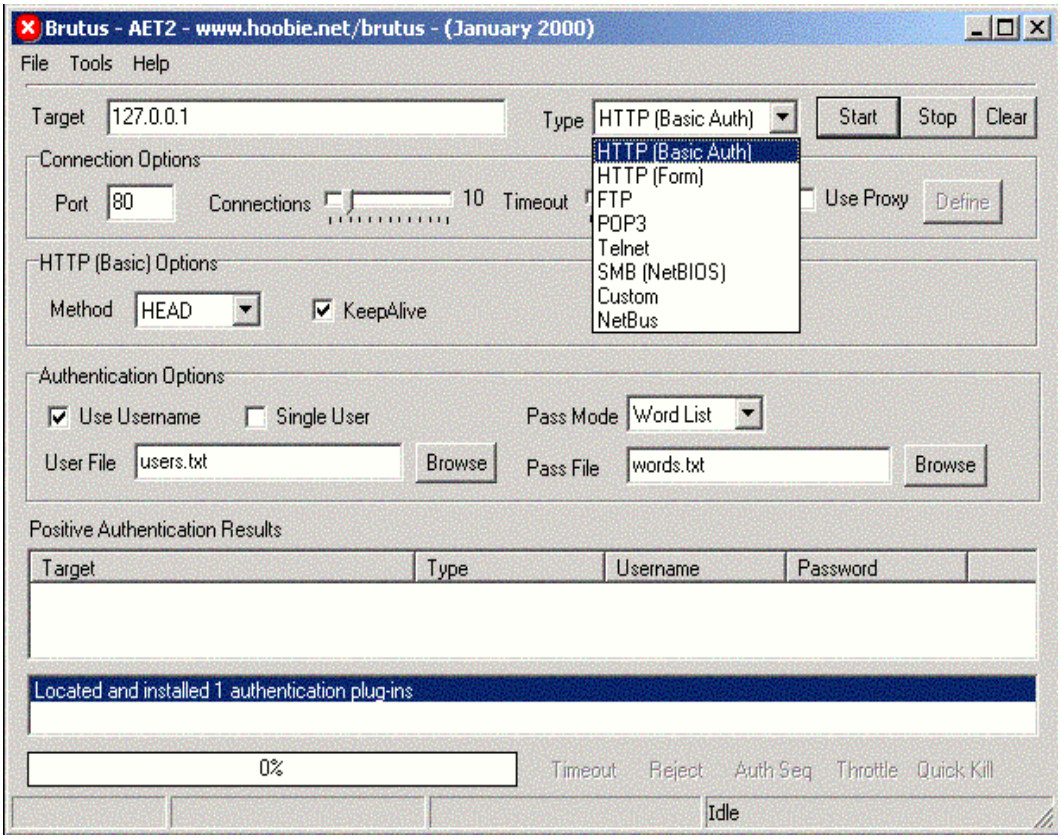
SWEEX				sweex	mysweex	Admin
D9287ar	Pavilion6640c			Clarissa		
Syabas Technology	Popcorn Hour A-110	Todos		nmt	1234	admin
Syabas Technology	Popcorn Hour C-200	Todos		nmt	1234	admin
Syabas Technology	Popcorn Hour A-110	Todos		ftpuser	1234	admin
Dell	WRTA-108GD			admin	admin	Admin
Linksys	ADSLME3			root	orion99	Admin
Areca	RAID controllers	Qualquer		admin	0000	Administrator
Edimax	PS-1208MFG			edimax	software01	Admin
SAF Tehnika	CFQ series modems			integrator	p1nacate	Integrator
SAF Tehnika	CFQ series modems			administrator	d1scovery	Admin
SAF Tehnika	CFQ series modems			operator	col1ma	Operator
SAF Tehnika	CFQ series modems			monitor	monitor	Monitor
McData	i10k Switch			McdataSE	redips	admin
Radware	AppXcel			radware	radware	Admin
AVM	Fritz!Box	qualquer		n/a	0000	admin
T-Com	Speedport	qualquer		n/a	0000	admin
T-Com	Speedport W701V	qualquer		n/a	0000	admin
T-Com	Speedport W900V	qualquer		n/a	0000	admin
Sempre	54M Wireless Router	V 1.00		admin	admin	
Radware	AppDirect			radware	radware	Admin
Bosch	NWC-0455 Dinion IP Cameras			service	service	admin
Bosch	NWC-0455 Dinion IP Cameras			user	user	regular user
Bosch	NWC-0455 Dinion IP Cameras			live	live	monitor - low priv
m0n0wall	m0n0wall	1.3		admin	mono	Administrator
m0n0wall	m0n0wall	1.3		admin	mono	Administrator
3com	corebuilder	7000/600/3500/2500		defug	synnet	
LAXO	IS-194G	1.0a		admin	admin	admin
LogiLink	WL0026	1.68		admin	1234	Admin
XAMPP	XAMPP Filezilla FTP Server			newuser	wampp	User
Pirelli	DRG A125G	4.5.3		admin	admin	Admin
Ricoh	Aficio MP 161L	(Printer MP 161L)		(none - Not required)	sysadm	Administration
Edimax	PS-1203/PS-1205Um/PS-3103	(not applicable)		admin	(none) OR su@psir	Administration
Sagem	Fast 3504 v2			Menara	Menara	admin
ALLNET	ALL 130DSL			admin	password	
AVM	Fritz!Box Fon	7270		n/a	n/a	
Watchguard	Firebox			(blank)	wg	admin
Sharp	AR-M237			admin	Sharp	Admin
Extended Systems	Print Servers	-		admin	extendnet	Admin
Symmetricom	NTS-200	Todos		operator	mercury	Admin

Symmetricom	NTS-200	Todos		guest	truetime	guest
Sharp	AR-M237			admin	Sharp	Admin
Netgear	WGR614	9		admin	password	Admin
Brother	MFC-7225			admin	access	admin
NETGEAR	DG834G	3		admin	password	
Ericsson	SBG	3.1		expert	expert	
huawei incorporate	k3765	9.4.3.16284		admin	admin	
Ricoh	Aficio	2016		(none)	password	all
T com	sinus	1054dsl		veda	12871	
Toshiba	Most e-Studio copiers			admin	123456	Admin
thomson	speedtouch 585 v7	2+		admin	password	administrator
ptcl	zxdsl831cii			admin	admin	
Brocade	Fabric OS	5320		user	password	user
Zyxel	NWA1100				1234	Admin
Zyxel	G570S	v2			1234	Admin
HP	E1200	Network Storage Router		root	password	admin
Kyocera	FS-2020D			-	admin00	Admin
Weidmüeller	IE-SW16-M			admin	detmond	admin
T-Com	Speedport 503V	qualquer			123456	

Multi-bruteforce

Existem muitos programas de bruteforce específicos, como o **WebCrack** (que quebra senhas de páginas web). Mas há também excelentes programas que conseguem decifrar senhas de vários tipos diferentes, como senhas de e-mail, netbios, web, unix, enfim, quase tudo. Já citei o **Shadow Scan**, mas mostrarei dois outros programas, excelentes, para essa tarefa:

Brutus: Excelente programa de bruteforce. Rápido e com uma configuração muito específica, produz excelentes resultados. Até senhas de netbus ele decifra. E salva as sessões.



Menu do Programa Brutus

Unsecure: Mais rápido que o brutus, esse excelente bruteforce é um dos mais utilizados para o Windows. Sabendo a porta do servidor (ftp, telnet, etc...), o programa faz o serviço para você.

Programa Unsecure em execução

Política de senhas não-craqueáveis

Não existe mistério para que se possa ter uma senha segura. Se você utilizar o sistema Unix, crie uma combinação não-lógica de letras e números. Como por exemplo:

FqTp78nH

Apesar de ser mais difícil de se decorar do que senhas normais, a boa combinação dificulta muito que se consiga craquear a senha. Nunca coloque seu nome como senha, número de telefone, data de aniversário, nome da esposa, dos filhos, animais de estimação, prato preferido, matrícula do carro, números sequenciais, cidade natal ou algo do género. Seja precavido. Para Windows existe um outro método muito bom para senhas, a utilização dos caracteres alt. Para ler mais sobre eles, consulte a secção sobre “recomendações de segurança”.

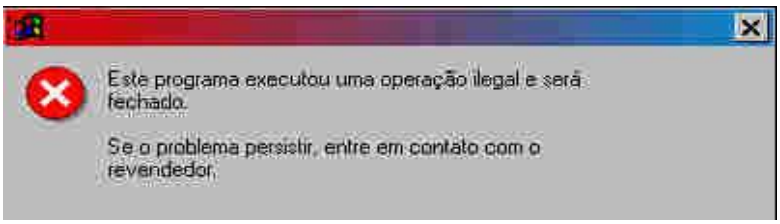
Falhas

Definição

Todos os sistemas têm falhas. Elas consistem em pequenos erros na criação dos programas, possibilitando que crackers os utilizem para tomar o controlo de alguma máquina. Existem em absolutamente todo tipo de software, desde um simples tocador de mp3, um aparentemente inofensivo editor de texto, um jogo de computador e até mesmo o próprio sistema operacional. Essas falhas por mais insignificantes que pareçam, podem comprometer a segurança de uma rede inteira. E a maior de todas as falhas é o desinteresse dos muitos administradores de hoje que acham que o termo bug é algum desenho do Walt Disney.

Como surge o bug

O bug, ou falha, surge a partir do momento que o programador comete um erro. Ou seja, indirectamente é um erro humano que gera a falha nos programas. Por serem pequenos erros e não aqueles "grandes" que fazem o compilador até rir do programador, muitas vezes passam despercebidos e só são descobertos por algum hacker ou analista de segurança. Os erros do Windows, por exemplo. A grande maioria das falhas descobertas, são os próprios utilizadors que descobrem. Os criadores mesmo que têm o codigo-fonte e conhecem o programa como a palma da mão raríssimas vezes percebem algum erro. Para ser mais seguro, um programa tem que ser testado de todas as maneiras possíveis. Coisa que não se faz mais hoje.



Exemplo de falha : General Protection Fault.

Exemplos de falhas

Algumas falhas são incríveis e difíceis de acreditar. Vou tomar como exemplo novamente o sistema Windows, pois de longe é o que possui mais falhas (claro, todas podem ser corrigidas). O Windows 98 possui muitos erros, mas três são interessantes. O primeiro é que não consegue executar nem abrir nenhum link com a url c:\con\con. Se você tentar ir em iniciar e executar, o sistema travará e mostrará a famosa tela azul. Os outros dois são do netbios. O primeiro possibilita que você aceda o directório system do Windows por uma partilha de impressora. É só mapear a partilha padrão **printer$.** O último possibilita que se descubra a senha do netbios sabendo apenas o primeiro carácter. Por exemplo: coloco no disco C partilhado a senha *"herodes"*. Se alguém tentar o primeiro h já consegue acesso à minha rede. O Windows 2000 também possui algumas falhas, como deixar o netbios activo na sua instalação. Saindo um pouco dos sistemas operacionais, alguns programas também possuem falhas graves.

Erros de Active X possibilitam que ao visitar um site, o Internet Explorer instale um programa no seu computador e o execute sem que você perceba. Preocupa-se em não abrir anexos de e-mail?

Erros no outlook fazem com que só de receber os e-mails os anexos sejam executados automaticamente. O Internet Information Server (IIS), servidor de websites da Microsoft, possui erros graves. Unicode, RDS, existem muitos. Um mais recente é uma falha no printer .isapi , fazendo com que se consiga acesso ao Windows 2000 pelo IIS 5.0 . O sistema Unix possui muitas falhas também, como no sendmail (chamado de maior bug da terra) e no Apache, mas é mais fácil exemplificar usando o maravilhoso sistema de Bill Gates. Um pequeno truque: abra o MS Word, digite a função =rand(100,100) e aperte enter.

Buffer overflows

O buffer overflow é um ataque usado a muito tempo e que ainda será muito usado. Compreende em lotar os buffers (memória disponível para aplicativos) de um servidor e incluir na sua lista de processos algum programa tal como um keylogger ou um cavalo de tróia. Todos os sistemas são vulneráveis a buffer overflows e a solução é a mesma, procurar se já existem correcções existentes. Novos erros desse tipo surgem todo dia, até o XP já têm alguns. Mantenha-se sempre actualizado para não ficar para trás.

Um dos usos famosos do buffer overflow é o **telnet reverso**. Ele consiste em fazer a máquina alvo conectar-se a um servidor no computador do cracker, fornecendo-lhe um shell (prompt) de comando. O **netcat**, chamado de "canivete suíço do TCP/IP", é uma espécie de "super-telnet", pois realiza conexões por UDP, serve como servidor, entre outras tarefas. Ele é o mais utilizado para a realização do telnet reverso, e pode ser usado tanto na arquitectura NT quanto no Unix. A versão para Windows está disponível em http://www.hacker-soft.net/.

Race condition

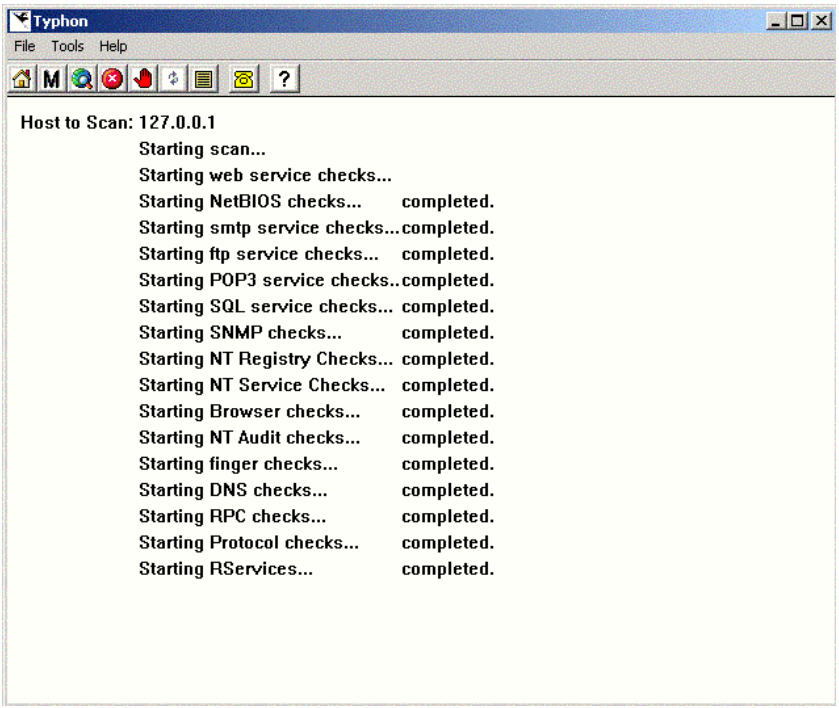
O Race condition ou condição de corrida é mais comum no Unix e no Linux. Consiste em fazer algum programa que execute como root (super-utilizador) executar alguma falha que possa lhe enviar para o shell do sistema. O programa que mais teve problemas de race condition até hoje é o sendmail, serviço de e-mail padrão do Unix. É possível encontrar falhas até em versões mais recentes.

Descobrindo se algum sistema tem falhas

Para o programador experiente é mais fácil verificar se um sistema tem falhas (se o programador for interessado e tiver boa vontade), utilizando de recursos de debug que procuram por erros de buffer overflow e outros. Para o utilizador é bem mais difícil descobrir algo, principalmente o utilizador comum. O interessante seria visitar páginas especializadas no assunto, que a cada dia publicam novos tipos de erros descobertos. Algumas muito boas são a International Computer Security Association http://www.icsa.net/ ou a insecure organization http://www.insecure.org/.

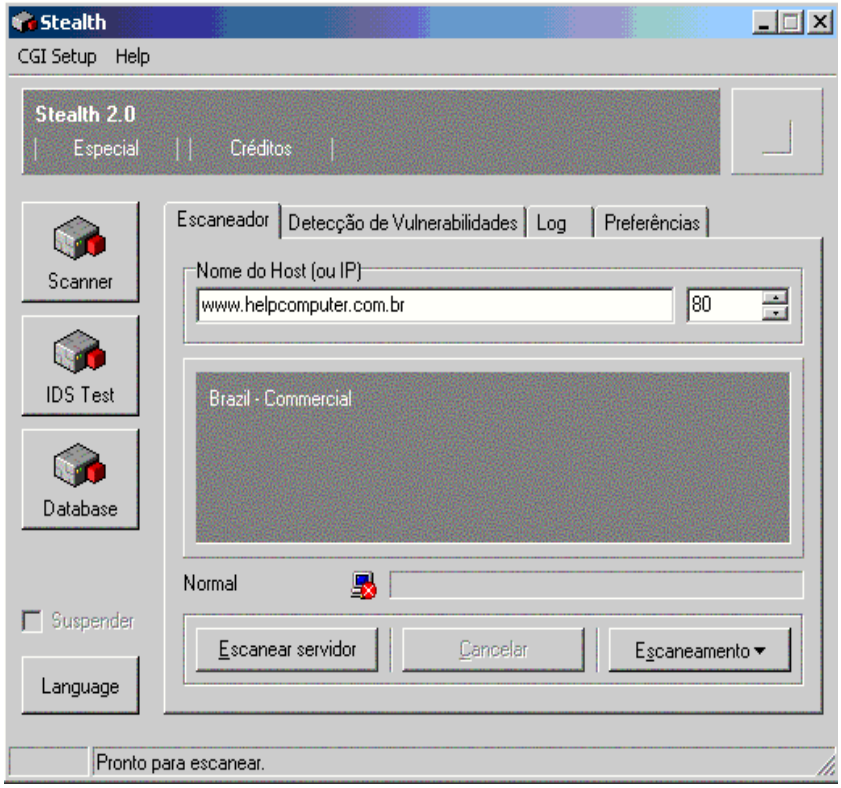
Anteriormente, na secção scanners, vimos alguns scanners de vulnerabilidade (ou falhas que quer dizer a mesma coisa). Veremos dois scanners melhores e mais potentes agora, o *Typhon* (http://www.insecure.org/.) e o *Stealth* **(http://www.nstalker.com/).**

Typhon (Apenas funciona em Windows NT/2000/XP)



Esse scanner é excelente pois é rápido e nos dá algumas informações muito importantes sobre possíveis falhas e desconfigurações do sistema alvo. Não é muito completo, mas é o ideal para se usar antes do magnífico **Stealth,** que como veremos, é inigualável**.**

Stealth



O melhor scanner de vulnerabilidades do mundo. Isso é pouco para descrever o fantástico programa **Stealth.** Programa de uma empresa brasileira (e em português), ele já ganhou destaque internacional pois consegue identificar cerca de 15000 falhas em sistemas. Poucos conseguem escapar ilesos a essa potente arma. Portanto, use-a para o bem!

Utilizando exploits

Exploits são programas criados para explorar falhas. O exemplo do printer .isapi do IIS 5.0, 6.0 e 7.0 que foi abordado anteriormente, possui um exploit chamado **iishack2000** .Ele possibilita que somente digitando o IP de algum computador, você consiga acesso direto ao interpretador de comandos (ou shell). Assim podendo fazer o que quiser com o sistema. Existe também o **iishack** (sem o 2000), que utiliza um erro de buffer overflow do IIS 4.0 para fazer com que você possa mandar o servidor executar qualquer tarefa (como um cavalo de tróia). Cada exploit corresponde a uma falha, por isso geralmente os grandes sites de segurança publicam os dois juntos. Geralmente vêm em código-fonte C, Perl e alguns poucos em executáveis comuns. Se quiser encontrar compiladores para rodar os exploits, procure na página **www.programmersheaven.com**. É uma excelente página web com muitos recursos de várias linguagens de programação. Se você não quiser arrumar um compilador, aí vai uma boa dica de exploit que analisa mais de 200 vulnerabilidades de Unicode (IIS). Adquira em:

http://tomktech.n3.net.

Instalando patches

Como já foi dito antes, a salvação está nos patches. Toda vez que um erro for descoberto, deve-se visitar a página do fabricante do programa e descarregar a correcção. Isso não pode ser feito de mês em mês, é no máximo de três em três dias. Os erros aparecem muito rápido, e um sistema é composto de muitos softwares. Todos devem ser analisados. É interessante também assinar uma lista de discussão sobre segurança, assim toda vez que uma falha for descoberta, você receberá um e-mail. A Microsoft (www.microsoft.com), a Securenet (**www.securenet.com.br**) e Security-focus (www.securityfocus.com) possuem algumas.

Anonimidade

Ser anónimo na rede

Ser anónimo na rede é algo muito discutido actualmente. Existe alguma forma de ser totalmente indetectável na Internet? Existe sim e é bem simples. Muitos programas e ferramentas prometem tornar o seu utilizador invisível mas são pura aldrabice. O que você precisa é de conhecimento, não de softwares. Um utilizador pode conseguir passar em computadores no Japão, Alemanha e Finlândia antes de atacar um site em Angola. Aí que se faz a fama dos armados a crackers". Um cracker pega o seu laptop, vai a um telefone público, utiliza uma conta roubada de internet, conecta-se a cinco computadores pelo mundo e utilizando-os conecta-se a um sistema de anonimidade. Após isso entra na página do FBI e apaga alguns ficheiros. Nunca, digo nunca realmente com muita ênfase, será apanhado. Todos os bons crackers não são apanhados, justamente pela facilidade de se esconder. Ou seja, não dependa de ferramentas de rastreamento, nem da polícia, nem nada. Apenas com a segurança do seu sistema. É a sua maior garantia.

Utilizando o anonymizer

O anonymizer é um dos muitos serviços gratuitos de anonimidade na net. Visitando a sua pagina web (*www.anonymizer.com*) ele possibilita que você digite algum endereço e seja redireccionado para ele. Exemplo: eu digito *www.mandivanet.co.ao* na página do serviço e ele me redirecionará para o provedor de Internet Mandiva, só que com o endereço IP do anonymizer. Ou seja, se os administradores da página consultarem o log, não verão o meu ip real endereço. Na sua versão básica (gratuita) o serviço possibilita apenas que você abra páginas HTTP. Ou seja, nada de FTP. Há ainda um serviço pago que pode ser conferido na página. Último detalhe: não é possível utilizar um anonymizer para conectar-se a outro.

Proxys

O proxy, antigo conhecido de muitas pessoas que mexem com rede, possibilita uma ponte entre um computador e um servidor. Para exemplificar melhor, imagine que você possua uma rede local, mas somente um dos seus computadores têm placa fax-modem. Então você conecta-se por ele e utiliza um proxy para que o outro computador da rede faça uma ponte e aceda a Internet pelo servidor. O endereço IP utilizado será do servidor. Acontece que existem muitos proxys gratuitos na Internet. Eles possibilitam que você navegue tranquilamente e às vezes ficam até mais rápidos do que com a conexão comum. O proxy também tem uma vantagem: você pode usar um proxy para entrar no anonymizer (assim escondendo seu endereço IP duas vezes). Endereços gratuitos de proxy podem ser encontrados no site *www.cyberarmy.com*.

Wingates

O Wingate parece muito com o proxy, mas a sua aplicação é um pouco mais perigosa por dois factores. Primeiro: o wingate é acedido por telnet, então possibilita a conexão a qualquer tipo de servidores, sejam telnet, ftp, smtp, pop, ou até algum cavalo de tróia. Segundo: ao contrário do anonymizer e do proxy que só pode ser usado uma vez, o wingate não tem limites. Você pode conectar-se a um wingate chinês, depois utilizá-lo para entrar num argentino e um italiano. A cada conexão, você terá um novo endereço IP. Imagine o trabalho para algum administrador descobrir quem invadiu o sistema. Terá que entrar em contacto com a autoridade de cada país e mesmo assim se ela quiser ajudar. É claro que a cada novo wingate a conexão vai ficando mais lenta. Só é bom

mesmo para quem possui uma conexão de alta velocidade. Existem alguns scanners que procuram subnets por wingates. Alguns deles podem ser descarregados em *www.thepiratebay.org*. Para uma lista de wingates, visite o site*: www.cyberarmy.com*.

Remailers

O Remailer é muito parecido com os outros, mas é somente para se enviar e-mails anonimamente. Com ele não é preciso utilizar um wingate para conectar-se a um servidor smtp, o próprio remailer já é um servidor anónimo. Mas por via das dúvidas, fique com o bom e velho wingate pois ele é mais garantido. Antes de sair mandando bombas de e-mail, saiba que esses serviços geralmente não conseguem manipular muitas mensagens num pequeno intervalo. Isso quer dizer que qualquer um que dê uma de esperto e queira inundar a caixa de e-mails de outra pessoa com centenas de e-mails provavelmente vai ter o seu endereço IP real revelado.

Shells

Uma vez alguém disse "O bom cracker não é o que consegue utilizar bem um sistema Unix e invadir uma rede. É o que utiliza Windows e consegue o mesmo resultado". Isso é uma verdade. Afinal, o Unix e o Linux podem até ser mais complicados de se usar mas existem centenas de óptimas ferramentas para eles. É só pensar que quase todos os exploits disponíveis na Internet hoje são código-fonte em C. Já o Windows não possui tantos recursos assim, o que torna mais difícil alguma invasão usando esse sistema. Para facilitar existem os shells, máquinas utilizando serviços Unix na Internet que possibilitam que você se conecte nelas por telnet e ftp e as utilize como se fossem locais. Execute programas, compile códigos-fonte, utilize o bom e velho VI, use o sendmail e tudo o mais. Para uma lista de shells consulte o site *www.cyberarmy.com* ou registe-se no endereço *http://cyberspace.org/*.

Outdials

Citarei esse método mais como estudo pois ele é bem difícil de ser feito. O Outdial consiste em se conectar via telnet em algum sistema que possibilite conexão via modem. Deixe-me explicar melhor: você quer invadir um sistema nos EUA. Não têm dinheiro para se conectar directamente (e pagar caro, apesar da propaganda das operadoras), então procura um outdial, conecta-se via telnet e indica o telefone do sistema a ser invadido. O computador que roda o outdial discará e você conectará no sistema sem pagar absolutamente nada. O problema é encontrar outdials hoje em dia. Não vai adiantar muito mas se quiser obter uma lista antiga de outdials, verifique o FAQ da 2600 em www.2600.com.

IP Spoof

A técnica mais antiga e devastadora de invasão de computadores. Trabalha a nível de protocolo, abaixo da camada dos aplicativos. É como o cavalo de tróia de ponte, mas bem mais eficaz. No caso do cavalo de tróia por exemplo, uma máquina era Windows, o que facilitou a sua instalação. Mas e uma rede que só existam máquinas Unix, mesmo assim fortemente seguras? Vamos supor que queremos invadir uma rede militar qualquer com 1000 computadores. O servidor central aonde ficam os dados confidenciais só se comunica com mais dois computadores, assim evitando o perigo de acesso pela Internet.

Ora, o erro está aí. Apesar de comunicar-se só com duas máquinas, elas têm acesso à rede externa. Existe então uma *relação de confiança* entre esses computadores e o servidor. Aí que entra o IP SPOOF. Ele consiste em estudar com um sniffer as sequências numéricas do cabeçalho ip que é enviado à máquina alvo. Supondo que a máquina alvo seja **A** (a que queremos invadir) e a que têm relação de confiança com ela seja **B**. Após aprender a sequência correcta, inundamos a máquina **B** com pacotes syn mal-formados (criando um denial of service para "amordaçá-la"). Então criamos um pacote IP com cabeçalho falso, fingindo ser a máquina **B** (que não pode falar). Além disso,

existem dois tipos de IP SPOOF.

Non-blind spoof

Esse spoof é realizado dentro da própria subnet em que se encontra o atacante. Ele é um spoof "não cego" pois permite que o atacante receba (usando um sniffer) a resposta da máquina A para a B após nosso ataque. Supondo que enviamos o comando:

< ip do hacker> >> /etc/rhosts

Esse é um comando para que o computador alvo passe a nos considerar "de confiança" cedendo-nos espaço para quando fizermos um rlogin. Mas como saber se o comando funcionou? Com o non-blind spoof isso é possível.

Blind spoof

Quando o ataque é feito a um computador fora de sua subnet. Com o blind spoof, a única coisa que se pode fazer é enviar o pacote spoofado com o comando e rezar para funcionar. Um programa que automatiza um pouco a tarefa do spoof é o **SendIP** (www.earth.li) para Linux (Unix). Já para Windows não existe ainda um programa decente que o faça.

Unix e Linux

Como tudo começou

O UNIX foi desenvolvido na década de 70 pela Bell Labs. Os seus criadores foram Ken Thompson e Dennis Ritchie, ajudados por uma equipe. O nome é uma ironia ao sistema Multics criado na década de 60 em que os dois se basearam. Enquanto ele tentava ser vários (Multi) o Unix era um só. Construíram um sistema operacional para programadores. Eles desejavam um resultado tão bom que a linguagem C foi desenvolvida só para ajudar a fazer melhores ferramentas para o projecto. A medida que o tempo foi passando, o UNIX foi se mostrando um sistema versátil e extremamente eficiente. Um pouco difícil para o utilizador inexperiente, mas muito eficaz. Com esse sucesso todo, o sistema evoluiu e teve várias distribuições, tais como, Digital Unix, Aix, Unix V, Xenix, Minix e muitas outras. Também inspirou a criação de sistemas operacionais como o DOS e OS/2.

A sua mais famosa adaptação é o Linux, criado por Linus Torvalds (daí provém o seu nome). É uma distribuição gratuita (coisa que nem todos os unix são) e portada para os computadores pessoais já que geralmente os outros sistemas são para grandes computadores (mainframes). O sistema UNIX vêm se mantendo a mais de 30 anos como o sistema mais seguro e poderoso de todos.

Não entrarei em detalhes sobre o UNIX, já que esse livro não se prende a um sistema. Darei uma visão geral sobre como é a sua estrutura e porquê difere tanto do Windows. O objectivo maior de um invasor num sistema com UNIX é obter o acesso ROOT. Ele pode fazê-lo tentando explorar alguma falha em algum servidor da vítima (veja secção falhas), como falhas em algum servidor (ou mesmo de algum kernel antigo), uma má-configuração, ou instalar um backdoor. Não importa. Se o invasor não conseguir acesso root ele não tem nada. E com certeza fará de tudo para consegui-lo.

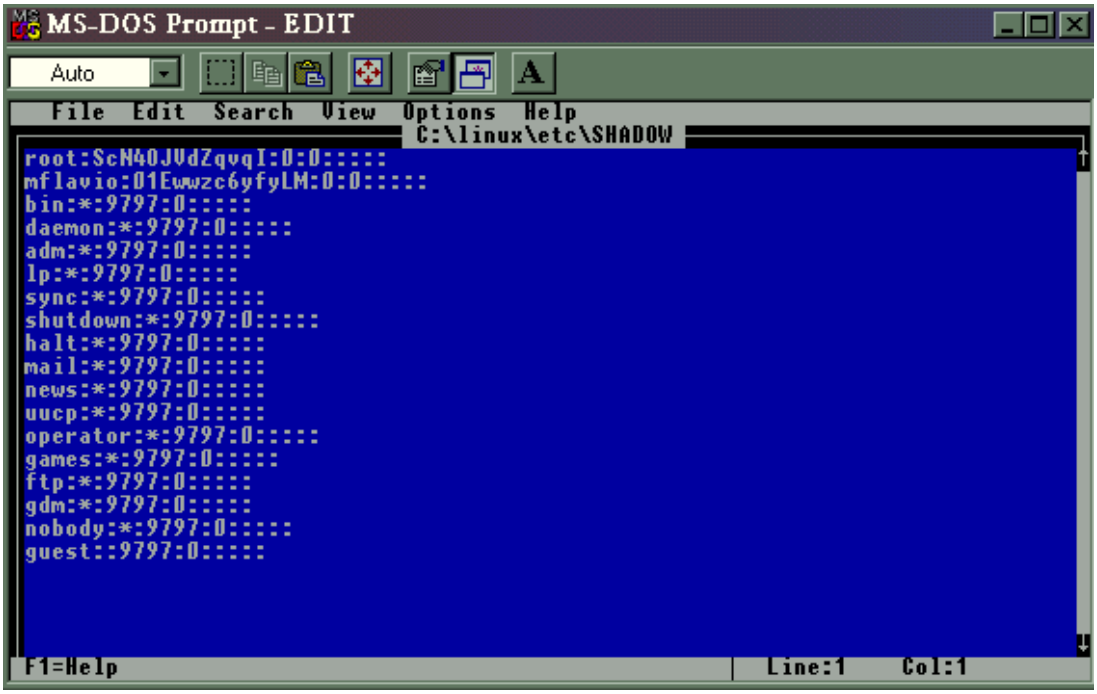
Autenticação de senhas – a criptografia DES

Sempre ao iniciar uma sessão, o sistema irá pedir-lhe nome de utilizador e senha. Mas onde ficam armazenados esses dados? O ficheiro **/etc/passwd** é o responsável por guardar as senhas no sistema. O processo de autenticação no UNIX é extremamente eficiente. Aqui um exemplo simples de como o ficheiro se organiza:

esantos : Edivaldo Santos :0 : 0: sEdkiUnbgFsbgTrVbgtTrfvfR : / : /bin/sh

A primeira sessão é o login do utilizador, no caso do exemplo é o **esantos**. Esse é o nome utilizado para acesso ao sistema. Logo depois vemos o nome completo do utilizador, que é **Edivaldo Santos**. Depois vêm dois números. Eles são os números de identificação de utilizador e grupo. Os chamados IDs. No UNIX cada utilizador pertence a um grupo, seja ele o root (administradores), webmasters, users, o que for. Quanto menor for o número que aparece no ficheiro passwd, maior é o poder do utilizador. No exemplo temos dois zeros, isso quer dizer que o utilizador têm poderes de administrador e pertence ao grupo root. Se fosse um utilizador comum, provavelmente o número estaria entre 20 e 60. A próxima secção é a mais interessante: a senha. Mas não a senha real, como é escrita ao se autenticar no sistema. Ela está criptografada usando um sistema chamado DES, desenvolvido especialmente para o UNIX. Contrariando alguns pensamentos, o DES não pode ser descriptografado. Mas ainda assim existem métodos para conseguir obter as senhas. Depois da senha criptografada temos o diretório padrão do utilizador (que no caso do root é a raiz "/") e seu interpretador de comandos ou shell (/bin/sh). Existem outros shells, como o shell C (/bin/csh). A utilização de cada um depende do gosto do utilizador.

Uma observação pertinente: em versões mais antigas do unix, usava-se o comando ln (que cria um link com algum ficheiro) para criar um link com o ficheiro de senha, mas agora acessível. Essa falha não mais existe. Seria mais ou menos assim: ln –l /etc/passwd/temp/teste . Isso faria com que no directório temp, existisse um link teste que poderia ser "acedido".



Exemplo de ficheiro de senhas simples

Shadowing

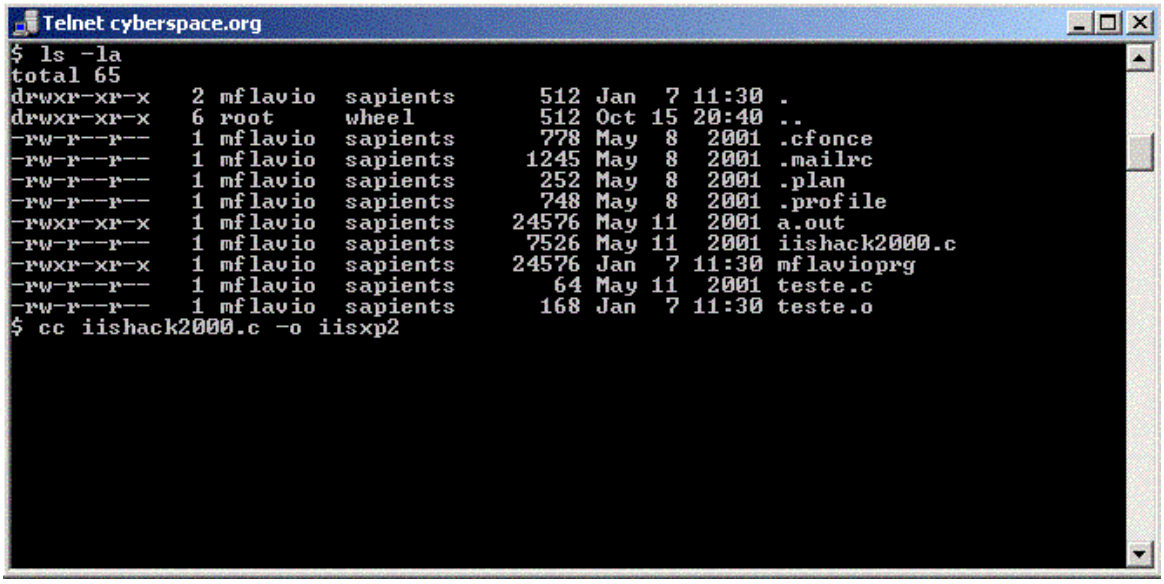
Na tentativa de segurar os invasores e impedir que consigam informações sobre o sistema, foi criado o sistema de Shadowing. Ele funciona da seguinte forma: deixa-se um ficheiro /etc/passwd "falso" para ser apanhado pelo cracker. Nesse ficheiro, geralmente no lugar das senhas criptografadas estará apenas um asterisco. Os administradores mais maldosos que querem ver o invasor perder o seu tempo, colocam algumas entradas criptografadas falsas de senhas. O ficheiro verdadeiro está bem guardado em algum lugar do sistema. Como isso varia de sistema para sistema e o local pode ser modificado, teriam que procurar muito para encontrá-lo. É uma medida de segurança a mais, mas ainda assim não segura um bom cracker, que nem necessita do ficheiro de senhas mais. Explora os erros.

SSH, Telnet e Rlogin

Os métodos de conexão remota são muito utilizados em sistemas UNIX. O Telnet e o Rlogin (remote login) por décadas foram largamente usados para que recursos externos distantes pudessem ser acedidos. É como o patrão que quer efectuar um login no sistema da empresa a partir de casa, e verificar os logs para ver se está tudo bem. Acontece que após a popularização do sniffer esses acessos remotos ficaram perigosos pois eles enviam dados a texto puro, sem nenhum tipo de criptografia. Esse problema foi resolvido com a criação do SSH (Secure Shell) que começa a criptografar mesmo antes do processo de login.

Hoje, o SSH têm sido usado demais nos sistemas Linux, até já vêm com as distribuições. O erro que algumas pessoas fazem é confiar demais na sua eficiência. Como qualquer outro programa, o Secure

Shell possui bugs graves. Até muitos se for comparado com outros serviços como o Apache. Portanto se o que você quer é a segurança do sistema, actualize sempre o seu SSH.



Como o utilitário telnet, consegue acesso a um sistema Unix.

Vírus e trojans

Essa é uma vitória do Unix. A coisa mais rara da face da Terra (mais raro que ganhar sozinho três vezes seguidas no totoloto) é aparecer algum vírus para esse sistema. Tanto que as empresas criadoras de anti-vírus iriam falir se fizessem versões exclusivas para Unix e Linux. Trojans também existem muito poucos, e esses só conseguem ser instalados com o poder de superutilizador (ou ROOT). Se você quiser livrar-se de uma vez por todas dos pequenos problemas como vírus de macro (Melissa), worms (Love Letter) e outros, uma boa solução seria migrar para sistemas Unix ou Linux. Não irá se arrepender.

Buffer overflows e condição de corrida

Leia a secção sobre falhas.

Aumentando a segurança do sistema

Para aumentar a segurança é o que chamamos de praxe: esteja sempre a actualizar o seu sistema por patches encontrados, teste-o com ferramentas de crackers para saber se é vulnerável. Configure os serviços que vão iniciar com o sistema no /etc/inet.conf. verifique as permissões e os logs do sistema todos os dias. Use o shadowing. Utilize um bom firewall. Confira se todas as senhas padrões estão desabilitadas.

Microsoft

Como tudo começou

A história da Microsoft é bem interessante e pode ser vista no filme "Piratas da Informática", produzido pela *TNT* . Bill Gates e Paul Allen estudavam em Harvard juntos. Um dia ficaram a saber do lançamento de um tipo de computador (desses que ainda funcionavam a base de perfurações de cartões) e ofereceram-se para criar o seu sistema operacional. Estava criada a *Microsoft*. Pouco tempo depois, um revolucionário chamado Steve Jobs lançou o primeiro computador pessoal do mundo, o **Apple II**. A apresentação do produto foi numa pequena feira de informática, em que Bill Gates estava presente. A *IBM* resolveu lançar um produto para concorrer com a *Apple* (empresa de Steve Jobs). Estava montado o projecto do **PC/XT** (vulgo 186). Só que não possuíam um sistema operacional. A Microsoft correu para a IBM e ofereceu o **Ms-Dos**. Só havia um problema. Eles não tinham um sistema para vender. Foi um bluff. Logo encontraram um programador que havia feito um sistema fácil de usar baseado no **Unix**, mas com muito menos comandos. Bill Gates comprou-o por alguns tostões e revendeu por um preço muito superior.

Esse foi o início de sua grande fortuna. A disputa Apple II e PC/XT continuou até que uma empresa chamada *XEROX* inventou o rato e a interface gráfica. Steve Jobs logo gostou do que viu e utilizou esses recursos no seu mais novo computador **Macintosh**. Percebendo o perigo a Microsoft ofereceu-se para trabalhar para a Apple, assim conseguiram três protótipos do Macintosh. Curiosamente a Microsoft lançou um produto quase igual ao sistema gráfico da Apple, chamado **Windows**. Steve Jobs perdeu o emprego e voltou anos depois à Apple, tendo agora Bill Gates como accionista. Os últimos lançamentos da sua empresa são o **Macbook Pro, Ipod, Iphone e Ipad**.

Diferenças entre as diferentes plataformas Windows (enriqueça isso)

O Windows possui duas hierarquias. A primeira, vem da sua primeira versão. Os mais antigos talvez se lembrem do **Windows 3.11**, aquele cheio das janelas. Pois é, depois dele vieram o **Windows 95** , o **98** e **Millennium (ME)**. Essa hierarquia possui muitas falhas, algumas tão antigas que vêm do próprio DOS (falha do *con* por exemplo). Isso porquê a cada nova versão eram acrescentadas novas tecnologias mas muitos erros não seram corrigidos. Isso junta os antigos problemas aos novos. Quem nunca mexeu com o Windows e recebeu o famoso erro "Esse programa executou uma operação ilegal e será finalizado"? A Segunda hierarquia é a do Windows NT, actualmente chamado de Windows 2000. É infinitamente mais estável pois a cada nova versão o código-fonte é praticamente reescrito, portanto é um sistema para empresas. Para se ter ideia era mais raro dar algum erro no Windows NT, além dele ter introduzido um novo sistema de ficheiros, o NTFS (NT File System), o que deixa o sistema mais seguro. Um bom exemplo para mostrar a diferença entre as duas hierarquias, é o programa **Anti-Trojans**. Na sua versão **1.5** há mais de 50 opções de portas para serem monitoradas, mais quatro portas extras. No Windows 98 tentei abrir 25 portas e deu erro. Memória insuficiente. Ou quando abria, nada mais funcionava, o Internet Explorer não tinha memória para carregar mais nenhuma página. No Windows 2000, abri todas as portas, inclusive as quatro extras, e ainda abri o ICQ, o Firefox e o Bearshare.

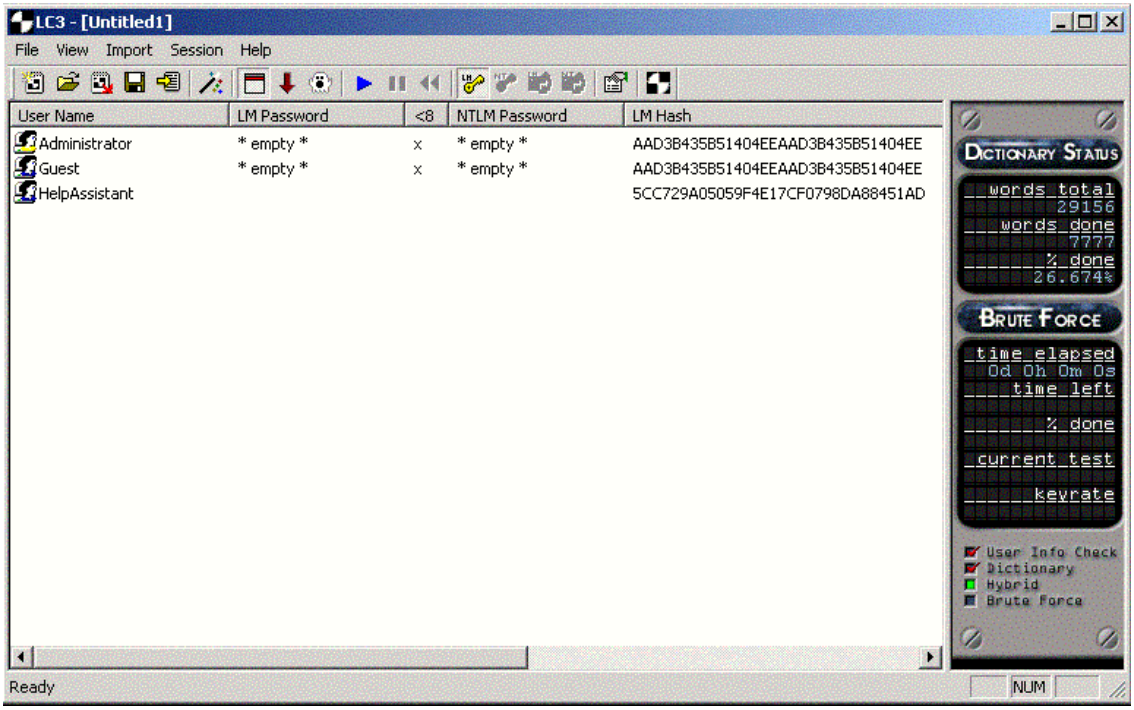
A tentativa de se criar um sistema misturando elementos do Windows ME e do NT resultou no famoso Windows XP. Mas ele é apenas uma versão "mais atraente" do NT, já que a maioria dos programas mais antigos (principalmente os do 95,98 ou ME) não funcionam nele.

Depois do Windows XP foi lançado o Windows Vista (na minha opinião um dos piores Sistemas Operacionais da Microsoft), que foi construído a partir de um novo kernel, mas que rapidamente revelou-se um fracasso, tendo obrigado a Microsoft num curto espaço de tempo lançar um novo

Sistema operacional baseado no Windows XP, o Windows 7 (Seven).

Autenticação de senhas

A autenticação no Windows NT é muito boa. Não tão quanto o Unix, claro. O processo é criptografado e oferece uma boa opção de segurança. Mas ao contrário do DES do Unix, pode ser decifrado mais facilmente. O excelente programa **LophtCrack** por exemplo, consegue descobrir senhas com uma velocidade fenomenal. E o NT (quando digo NT me refiro a todas as versões, inclusive o Windows 2000 que na verdade é o NT 5.0 e ao XP) não possui um recurso de shadowing, o que poderia ajudar a aumentar a segurança das senhas. Já a plataforma Windows 9x (actual ME) possui um método ridículo de autenticação de senhas. Na tela de login, só de você clicar em cancelar o sistema já inicializa. As senhas são gravadas em ficheiros PWL no directório do Windows, sendo extremamente fáceis de serem decifradas. Muitos programas fazem isso, mas o **CAIN** é um dos melhores.



O LophtCrack consegue descobrir senhas do Windows NT localmente, num sistema remoto (sendo admin) ou pela rede local como um sniffer. Ele tenta descobrir as senhas pelo LanMan, antigo algoritmo em que a autenticação do Windows NT se baseia.

Vírus e trojans

Michelângelo, Chernobil, Melissa, I Love You, várias gerações de um mesmo problema que atinge utilizadores do antigo DOS e do Windows por anos. Os malvados vírus. O que são exatamente os vírus? São programas em que a única função é causar danos ao computador, seja apagando ficheiros, deixando a máquina mais lenta, etc. Em comparação a outros sistemas como o do Mac OS (Macintosh) ou o Unix, o Windows ganha de longe na quantidade de vírus. Existem milhões e milhões de "bichinhos" para o Windows enquanto que para o Unix são apenas poucas dezenas. Vírus inofensivos (se é que podem ser chamados de vírus) como macros anexadas a documentos do office

ou um ficheiro vbscript têm causado muito pânico hoje em dia. Pense como as coisas são engraçadas: antigamente, quando se utilizava o DOS que é bem menos sofisticado e sem recursos, os vírus eram feitos por mestres da informática. Hackers e Crackers se utilizavam do assembler (linguagem de baixo nível) para criar os seus vírus. E essa é uma linguagem bem mais difícil de ser aprendida que as comuns de alto nível (como basic, pascal, C, Perl e outras).

Hoje, com o Windows sendo altamente sofisticado, um simples ficheiro VBScript causa muito estrago. Não precisa nem ser compilado e têm uma linguagem de programação extremamente fácil (baseado no Visal Basic). Infelizmente esse é o problema da geração Windows. Os que começaram o seu aprendizado pelo DOS têm mais malícia em relação aos vírus. Para quem não conhece nada sobre esse antigo sistema, consulte a secção que trata do MS DOS. A quantidade de trojans existente também é infinitamente maior no Windows do que em outros sistemas. Como disse no início do livro, não existe um sistema melhor que o outro. Depende do seu uso e do gosto pessoal de cada um. Se utilizá-lo na empresa, use o Unix. Pelo menos os vírus não irão rondar os seus sonhos à noite. Ou se preferir mesmo o Windows, adquira um bom anti-vírus (o **Nod32 e o Norton** são dos melhores). Eles ajudam muito.

Buffer overflows
Leia a secção sobre falhas.

Badwin
Badwin e Badcom são a mesma coisa, apenas um é para o sistema Windows e outro para o DOS. Podem ser feitos em Delphi ou VB e geralmente possuem comandos para apagar os ficheiros do computador. Não podem ser considerados vírus ou trojans pois não ficam residentes na memória e nem são enviados pela rede (como os worms). Um badwin é um programa extremamente simples, até mais do que os worms **vbscript**. Mas às vezes os programas são tão enfeitados (como aquele em que o botão corre) que as pessoas acabam caindo. E aí já é tarde.

Worms
Robert Morris Jr ficou famoso por ter criado o primeiro **worm** da história. O seu vírus especial conseguia atacar de rede em rede, causando danos enormes. E a diferença do vírus para o worm é essa: o worm é transmitido automaticamente pela rede, seja por e-mail, por ftp ou por tcp/ip. Causa danos como o vírus, mas sua proporção é maior. Alguns exemplos são o **Melissa** (worm de macro) e o **I Love You** (worm vbscript) que são enviados por e-mail. Os anti-vírus mais novos também costumam a detectar os worms, mas infelizmente como não são programas compilados (executáveis), são fáceis de serem alterados para enganar o software antivirus. Actualmente os chineses são os maiores desenvolvedores deste tipo de vírus, que é utilizado para diversos fins, desde a guerra cibernética á espionagem industrial.

Aumentando a segurança do sistema
Use o Windows XP, Windows 7 ou adopte um Unix (Linux, Macintosh, HP-UX, etc). Detesto ter que favorecer esse ou aquele sistema operativo, os amantes do open source de certeza que afirmariam que o Linux é o melhor sistema operativo, mais seguro, mais estável… etc, etc. eu como amante da informática digo que determinado software é melhor para aquilo que determinado utilizador necessita, ou seja, o que é melhor para um utilizador que apenas necessita de um computador para utilizar um processador de texto(MS Word, Writer) ou folhas de cálculos (MS Excel ou Calc) difere o que é melhor para um utilizador avançado que necessita de realizar tarefas robustas, executar aplicativos críticos e com elevados requisitos técnicos.

É verdade que o sistema operacional usado influencia no nível de segurança efectiva, mas isso não significa que por eu estar a utilizar o S.O "x" esteja mais seguro do que o utilizador que estiver a utilizar o sistema operacional "y" apenas porque o meu sistema operacional é supostamente mais seguro do que o "y", há outros detalhes que devem ser verificados, tais como:

Se o computador possui um anti-vírus actualizado;
Se o computador estiver na rede, verificar se a rede encontra-se protegida por algum firewall;
Garantir que os utilizadores pratiquem as melhores recomendações de segurança.

MS DOS

Porquê o MS DOS?

Ainda me recordo da primeira vez que experimentei-o. Fiquei maravilhado com toda aquela mágica de comandos. Expressões como **dir**, **cls** e **attrib** ainda faziam parte do nosso vocabulário. O **Qbasic** possibilitou-me dar os meus primeiros passos numa linguagem de programação. Era a época de grandes jogos como F1GP e Prince of Persia. É uma pena que o sistema operacional de disco (DOS) da Microsoft tende a não existir mais. A cada versão do Windows mata-se um pouco dele. No Windows 7, nem é possível mais executar a maioria dos programas. Uma grande pena para os utilizadores da era do clique.

Vemos pessoas assim chamar directórios de pastas, copiar ficheiros utilizando o Windows Explorer (sendo que não há nada melhor e mais emocionante de ser usado do que o comando copy do DOS). Recomendo a sua aprendizagem a todos que não o conhecem. Vocês ainda têm tempo antes de surgir uma versão do Windows que não suporte nenhum comando nativo do MS Dos. Foi em homenagem a ele que essa secção foi criada, mostrando truques e tácticas de segurança. E por considerar os seus comandos muito importantes para administradores de sistemas e webmasters e para estudantes que queiram entender melhor o funcionamento dos sistemas operativos da Microsoft.

Ficheiros BAT
Os ficheiros batch no DOS são pequenos scripts que possibilitam que se faça muitas tarefas de uma só vez. Possuem a extensão BAT e podem ser executados como se fossem executáveis. A linguagem batch é bem extensa e óptima para iniciantes aprenderem os primeiros passos em programação. O meu objectivo não é ensinar a linguagem e sim apenas mostrar como o processo funciona. Um exemplo de um ficheiro batch abaixo:

Dir/p

Cls

Mem

Digite no prompt do dos "edit teste.bat". Assim o editor padrão EDIT irá criar o ficheiro teste.bat. Escreva os três comandos acima, colocando-os um em cada linha. Salve o ficheiro e execute-o digitando teste ou teste.bat. O programa listará os ficheiros com pausa (dir/p), limpará o ecrã (cls) e mostrará o status da memória (mem).

Badcoms

Os badcoms são uma má utilização de ficheiros bat. Coloca-se no ficheiro comandos destrutivos, tais como "del *.*" ou "deltree /y *.*", que são comandos para apagar ficheiros e directórios. Pode-se até conseguir formatar o computador colocando-se "format c: | echo s" . O pipe (|) fará com que o comando echo envie o caracteres para o comando format c:. Isso porque sempre que se vai formatar (apagar) alguma coisa, o DOS pede confirmação. No caso, o batch daria a confirmação por si próprio. Um exemplo rápido de um badcom:

Cls

@deltree /y *.* > nul

Ao criar esse ficheiro BAT e executá-lo, o programa primeiro limpará o ecrã e logo depois usará o comando deltree para apagar os ficheiros e pastas do computador. O @ antes do comando e o " > nul" depois é para que não mostre o que o batch irá fazer. Se você digitasse esse comando sem esses dois termos (somente deltree /y *.*), iria aparecer a mensagem "Excluindo <pasta ou ficheiro> " . O erro do batch é que os utilizadors experientes nunca executarão seus comandos sem olhar seu conteúdo. Infelizmente foi criado o programa **bat2exe** que transforma o ficheiro bat em executável (podendo ser COM ou EXE).

Nesse exemplo, enviamos o caractere (echos) para o comando del, assim ao executar o ficheiro bat (ou badcom nesse caso) ele limpará a tela (cls), listará os dados (dir) e logo em seguida irá apagar o conteúdo do disco duro (drive c). E ainda não mostrará nada na tela (nul).

Caracteres ALT

São obtidos ao se pressionar e segurar a tecla ALT e alguma sequência de três ou quatro números do keypad numérico (esse à direita do teclado). Alguns exemplos são ALT + 987 (que desenha um quadrinho amarelinho), ALT + 167 (símbolo º), ALT + 255 (carácter vazio, óptimo para criar ficheiros sem nome) e muitos outros. Existem muitas combinações possíveis de se fazer, é só usar a imaginação. Os perigos dessa táctica é criar directórios usando caracteres ALT, assim o Windows não consegue acedê-los. Ou criar ficheiros ocultos sem nome. Também têm as suas vantagens, se você criar uma senha com esses caracteres, será extremamente mais difícil de ser descoberta. Pergunte ao seu provedor se o sistema deles admite o uso do ALT.

Macros do doskey

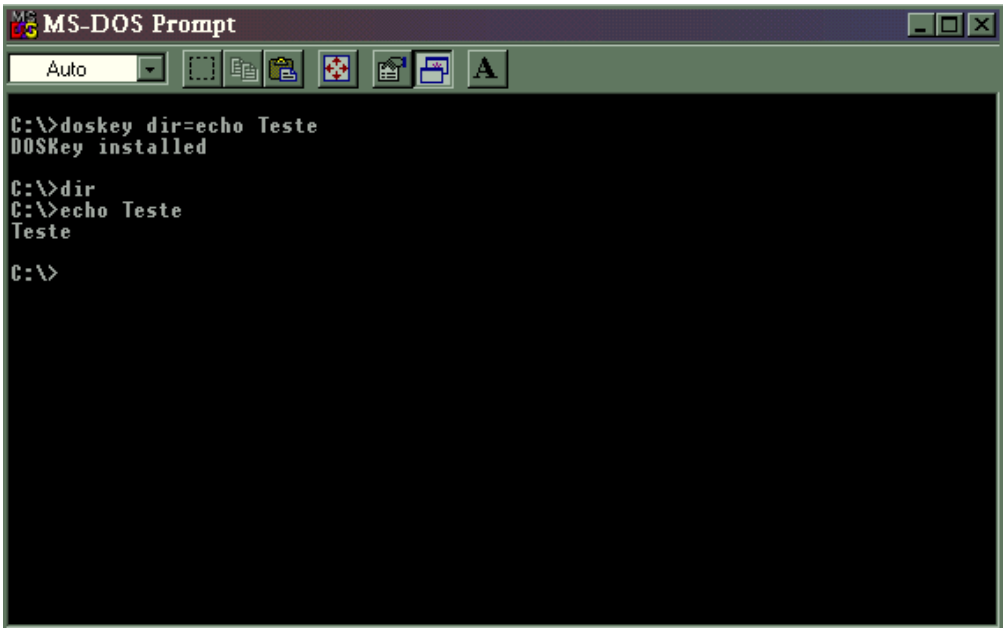
Os antigos utilizadores do DOS lembram-se muito bem do nome doskey. Ele era muito utilizado para repetir os comandos mais usados pelo utilizador ao apertar-se a tecla para cima. Algo como o botão voltar do Internet Explorer. Mas esse pequeno comando pode ser utilizado para outros fins interessantes, como a criação de macros. Vamos fazer um teste criando uma macro chamada listar.

Doskey listar=dir

Ao executarmos a macro listar (executando-a como se fosse um comando comum), ela Automaticamente dará um dir, ou seja, listará os directórios e ficheiros.

Doskey listar=dir/p $t mem

Neste exemplo, ao executarmos a macro listar o sistema dará um dir com pausa e executará logo em seguida o comando mem, que mostra o status da memória do sistema. Assim, usando o recurso $T podemos executar diversos comandos com uma só macro. Mas o interessante vem agora:



Doskey dir = cls $t ver $t mem

Nós conseguimos criar uma macro com o próprio comando dir. Assim quando alguém for listar directórios, tomará um enorme susto. Isso funciona para todos os comandos do Dos.

O exemplo a seguir mostra a criação de outra macro.

Para fazer o reset da macros, aperte alt + f10.

Variáveis do sistema

Vou abranger rapidamente essa secção dizendo apenas que existem muitas variáveis de sistema do DOS, e que todas podem ser mudadas usando o comando **set**. Demonstrarei um excelente exemplo:

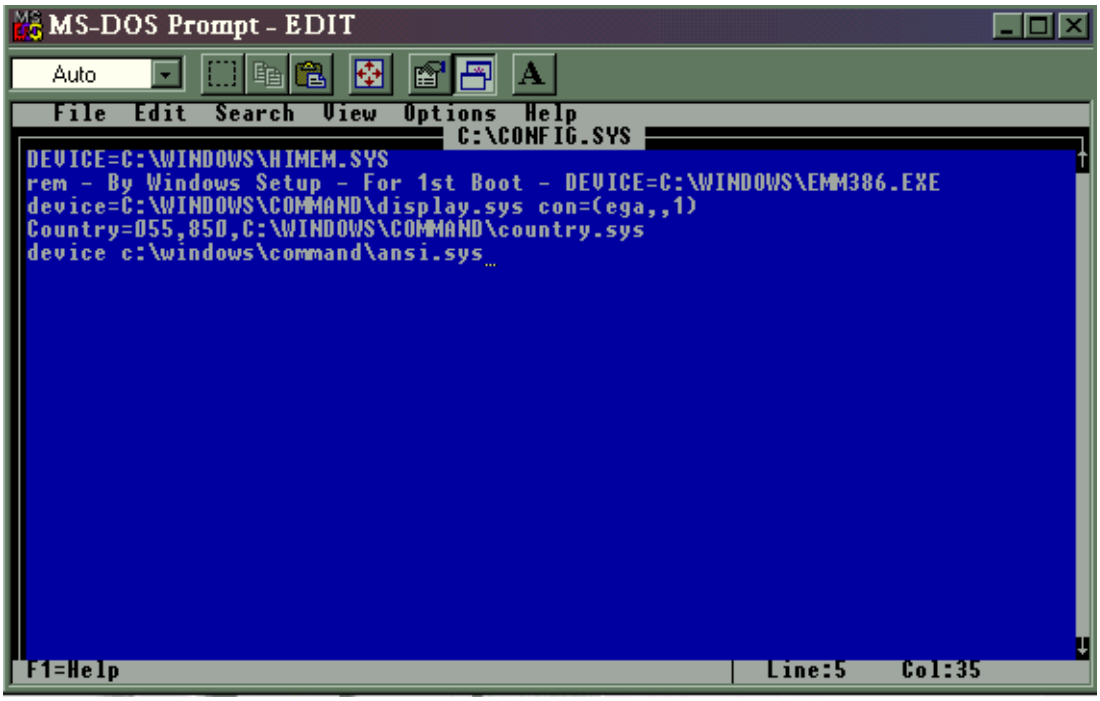
Set dircmd=@

Isso fará com que ao listar os directórios e ficheiros, não apareça nada. O significado do @ é esse, esconder. Mas você pode colocar como dircmd a opção /p ou /w ou alguma outra. Elas irão automatizar o processo de listar com pausa, etc. Se teve dúvidas, tente fazê-lo que irá entender.

Comandos ANSI

Esse é o mais interessante de todos. Antes de tudo, verifique se existe essa linha no seu config.sys (ele fica na raiz). Se não existir, inclua.

Device = c:\windows\command\ansi.sys

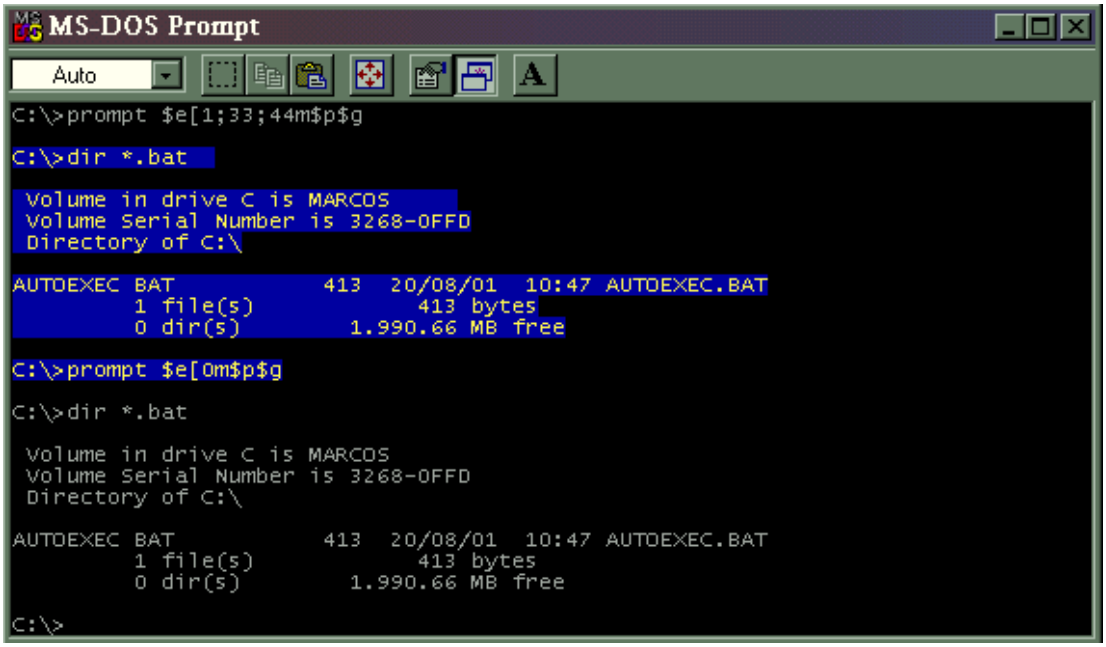


Agora reinicie o computador. Vá para o prompt do DOS depois que ele reiniciar.

Deixe-me explicar por partes: primeiro vamos definir algumas cores dos números:
0 – Preto
1 – Vermelho
2 – Verde
3 – Amarelo
4 – Azul
7 – Branco

E agora o status:
0 – Letra mais forte
1 – Letra mais fraca
5 – Intermitente
Ok, qual o significado de mostrar esses números? Tu entenderás.

C:\> prompt $e[1;33;44m$p$g



O comando prompt (atenção, o c:\> não é para ser digitado) é usado para alterar esse c:\> do DOS. Mas a sua opção $e é a de ANSI. O exemplo acima é dividido em três partes: o número 1 é o status. Logo depois ele é separado da dezena de 30 pelo ponto e vírgula. A dezena de 30 é a responsável pela letra, então colocamos o 3 (ficando 33) para que a letra seja amarela. Logo depois outro ponto e vírgula separando a dezena de 40. E colocamos a cor azul (ficando 44). O **m** é utilizado para terminar a sentença e o pg são para o prompt continuar o mesmo (ou seja, não mudar o c:\>). Acho que já deu para entender como se muda as cores, vamos mudar algumas teclas agora. Que tal o vírus cebolinha? Mudaremos a tecla r pela l.

C:\.> prompt $e[“r”;”l”p$p$g

Esse comando trocará a letra r pela l. Experimente pedir a alguém digitar seu nome. O **p** faz a mesma coisa que o **m** na cor. Mais dois exemplos apenas.

C:\> prompt $e[0;60;””;13p$p$g

Esse comando transforma a tecla F2 (cujo código é 0;60) em Enter (o 13p no final). Agora vai o comando mais malvado de todos.

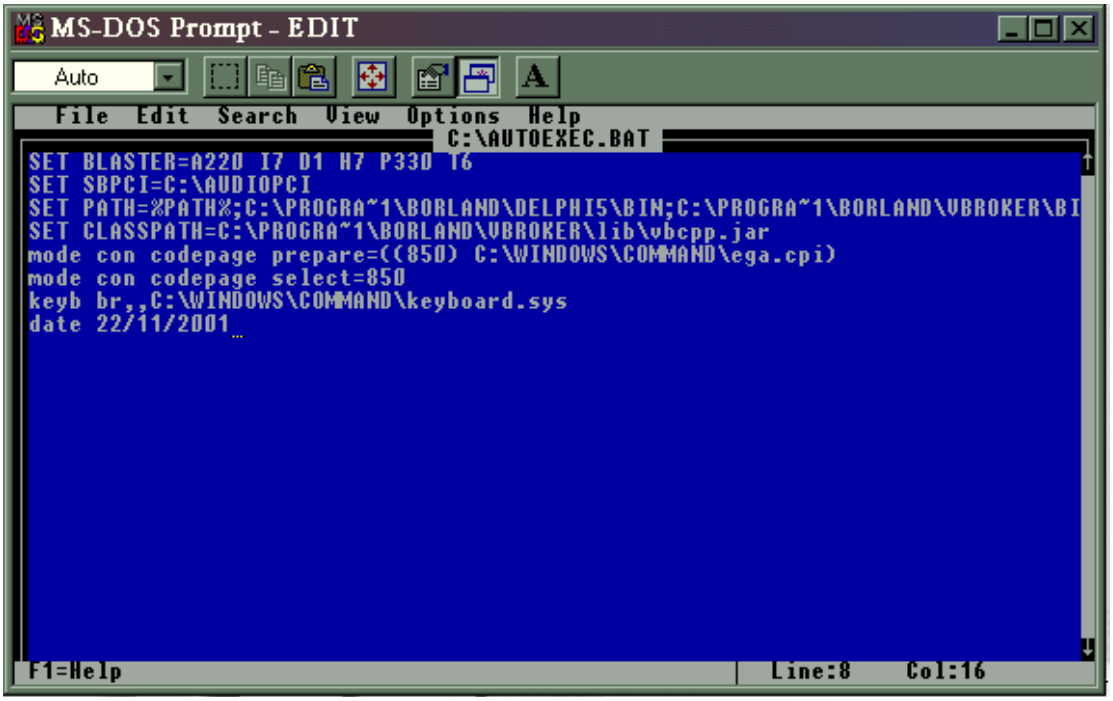
C:\> prompt $e[13;”deltree /y *.*”;13ppg

Cuidado ao executá-lo, ele fará com que só de pressionar a tecla Enter (código 13), se execute o comando deltree /y *.* que apagará todos os ficheiros. Troque o comando entre as aspas como teste. Para voltar as teclas ao normal, seria preciso saber o código delas. Há um método mais fácil. Feche o prompt do Dos ou reinicie o computador.

Velhos truques

O DOS é cheio de truques muito interessantes. Vou dar apenas uma palhinha pois o bom mesmo explorar e descobri-los por você mesmo. Mas tenho certeza de que essa dica será muito útil. Abra o ficheiro autoexec.bat (que está na raiz) e coloque o comando date mais a sua data actual. Mais ou menos assim:

Date 20/08/2001



Salve o ficheiro e reinicie o computador. Esse lhe trará duas vantagens: primeira: aqueles vírus com dias programados para atacar, nunca atacarão seu pc (e são mais de 30% dos vírus existentes) e segunda: os programas que você pode utilizar por 30 dias podem ser usados para sempre.

Aprenda a proteger-se

FRAUDES NA INTERNET

Engenharia Social

Nos ataques de engenharia social, normalmente, o atacante faz-se passar por outra pessoa e utiliza meios, como uma ligação telefônica ou *e-mail*, para persuadir o utilizador a fornecer informações ou realizar determinadas acções. Exemplos destas acções são: executar um programa, aceder uma página falsa de comércio eletrónico ou *Internet Banking* através de um *link* num *e-mail* ou numa página, etc.

O conceito de engenharia social, bem como alguns exemplos deste tipo de ataque, podem ser encontrados em "Problemas comuns de segurança". Exemplos específicos destes ataques, envolvendo diversos tipos de fraude, serão abordados mais adiante.

Como posso me proteger deste tipo de abordagem?

Em casos de engenharia social o bom senso é essencial. Fique atento para qualquer abordagem, seja via telefone, através de um *e-mail*, onde uma pessoa (em muitos casos falando em nome de uma instituição) solicita informações (principalmente confidenciais) a seu respeito.

Procure não fornecer muita informação e **não** forneça, sob hipótese alguma, informações sensíveis, como senhas ou números de cartões de crédito.

Nestes casos e nos casos em que receber mensagens, que tentam lhe induzir a executar programas ou clicar em algum *link* contido num *e-mail* ou página *Web*, é extremamente importante que você, **antes de realizar qualquer acção**, procure identificar e entrar em contacto com a instituição envolvida, para certificar-se sobre o caso.

Fraudes via Internet

Normalmente, não é uma tarefa simples atacar e falsificar dados num servidor de uma instituição bancária ou comercial. Então, os atacantes têm concentrado os seus esforços na exploração de fragilidades dos utilizadors, para realizar fraudes comerciais e bancárias através da Internet.

Para obter vantagens, os burladores têm utilizado amplamente *e-mails* com discursos que, na maioria dos casos, envolvem engenharia social e que tentam persuadir o utilizador a fornecer os seus dados pessoais e financeiros. Em muitos casos, o utilizador é induzido a instalar algum código malicioso ou aceder á uma página falsa, para que dados pessoais e sensíveis, como senhas bancárias e números de cartões de crédito, possam ser furtados. Desta forma, é muito importante que utilizadors de Internet tenham certos cuidados com os *e-mails* que recebem e ao utilizarem serviços de comércio eletrónico ou *Internet Banking*.

A secções a seguir ilustram algumas situações envolvendo estes tipos de fraudes. E faz uma descrição de alguns cuidados a serem tomados pelos utilizadors de Internet, ao acederem *sites* de comércio eletrónico ou *Internet Banking*.

O que é *scam* e que situações podem ser citadas sobre este tipo de fraude?

O *scam* (ou "burla") é qualquer esquema ou acção enganadora e/ou fraudulenta que, normalmente, tem como finalidade obter vantagens financeiras.

Abaixo apresento duas situações envolvendo este tipo de fraude, sendo que a primeira situação se dá através de páginas disponibilizadas na Internet e a segunda através do recebimento de *e-mails*. Observe que existem variantes para as situações apresentadas e outros tipos de *scam*. Além disso, novas formas de *scam* podem surgir, portanto é muito importante que você se mantenha informado sobre os tipos de *scam* que vêm sendo utilizados pelos burlões, através dos veículos de comunicação, como jornais, revistas e *sites* especializados.

Sites de leilões e de produtos com preços "muito atractivos"

Você acede um *site* de leilão ou de venda de produtos, onde os produtos oferecidos têm preços muito abaixo dos praticados pelo mercado.

Risco: ao efectivar uma compra, na melhor das hipóteses, você receberá um produto que não condiz com o que realmente foi solicitado. Na maioria dos casos, você não receberá nenhum produto, perderá o dinheiro e poderá ter os seus dados pessoais e financeiros furtados, caso a transação tenha envolvido, por exemplo, o número do seu cartão de crédito (permitam-me abrir um parentesis, para contar a história de um amigo meu, que comprou um htc modelo 2011 no maior site de scam "Alibaba.com"por cerca de USD 400,00 e recebeu um iphone Chinês que deve estar avaliado em USD 40,00).

Como identificar: faça uma pesquisa de mercado sobre preço do produto desejado e compare com os preços oferecidos. Então, você deve perguntar-se porquê que estão a oferecer um produto com preço tão abaixo do praticado pelo mercado.

É importante ressaltar que existem muitos *sites* confiáveis de leilões e de vendas de produtos, mas nesta situação a intenção é ilustrar casos de *sites* especificamente projectados para realizar actividades ilícitas.

A burla da Nigéria (*Nigerian 4-1-9 Scam*)

Você recebe um *e-mail* em nome de uma instituição governamental da Nigéria (por exemplo, o Banco Central), onde é solicitado que actues como intermediário numa transferência internacional de fundos. O valor mencionado na mensagem normalmente corresponde a dezenas ou centenas de milhões de dólares.

Como recompensa, terás direito a ficar com uma percentagem (que é normalmente alta) do valor mencionado na mensagem. Para completar a transação é solicitado que pagues antecipadamente uma quantia, normalmente bem elevada, para arcar com taxas de transferência de fundos, custos com advogados, entre outros.

Este tipo de burla também é conhecida como *Advance Fee Fraud*, ou "a fraude de antecipação de pagamentos", e já foram registados casos originados ou que mencionavam a África do Sul, Angola, Etiópia, Libéria, Marrocos, Serra Leoa, Tanzânia, Zaire, Zimbábue, Holanda, Jugoslávia, Austrália, Japão, Malásia e Taiwan, entre outros.

No nome dado a este tipo de fraude, *Nigerian 4-1-9 Scam*, o número "419" refere-se à secção do código penal da Nigéria que é violada por este tipo de burla.

Risco: ao responder a este tipo de mensagem e efectivar o pagamento antecipado, você não só perderá o dinheiro investido, mas também nunca verá os milhares ou milhões de dólares prometidos como recompensa.

Como identificar: normalmente, estas mensagens apresentam quantias astronômicas e abusam da utilização de palavras capitalizadas (todas as letras maiúsculas) para chamar a atenção do utilizador. Palavras como "URGENT" (urgente) e "CONFIDENTIAL" (confidencial) também são frequentemente utilizadas no assunto da mensagem para chamar a atenção do utilizador.

Tu tens que te questionar porquê que foste escolhido para receber estes "milhares ou milhões" de dólares, entre os inúmeros utilizadors que utilizam a Internet. Eu também já fui vitima desse tipo de burla no ano de 2009, enquanto frequentava uma formação na Africa do Sul, primeiro fui abordado via skype, o burlador disse-me que trabalhava para o banco do Ghana e que controlava uma conta não refundável que continha cerca de 2,5 milhões de dolares. Eles davam-me 40% desse valor se eu transfirisse os fundos para uma conta em meu nome no respectivo banco. A primeira falha deles foi no site do suposto banco que era www.bcg-ghana.com, enquanto o real site era www.gcb.com.gh.

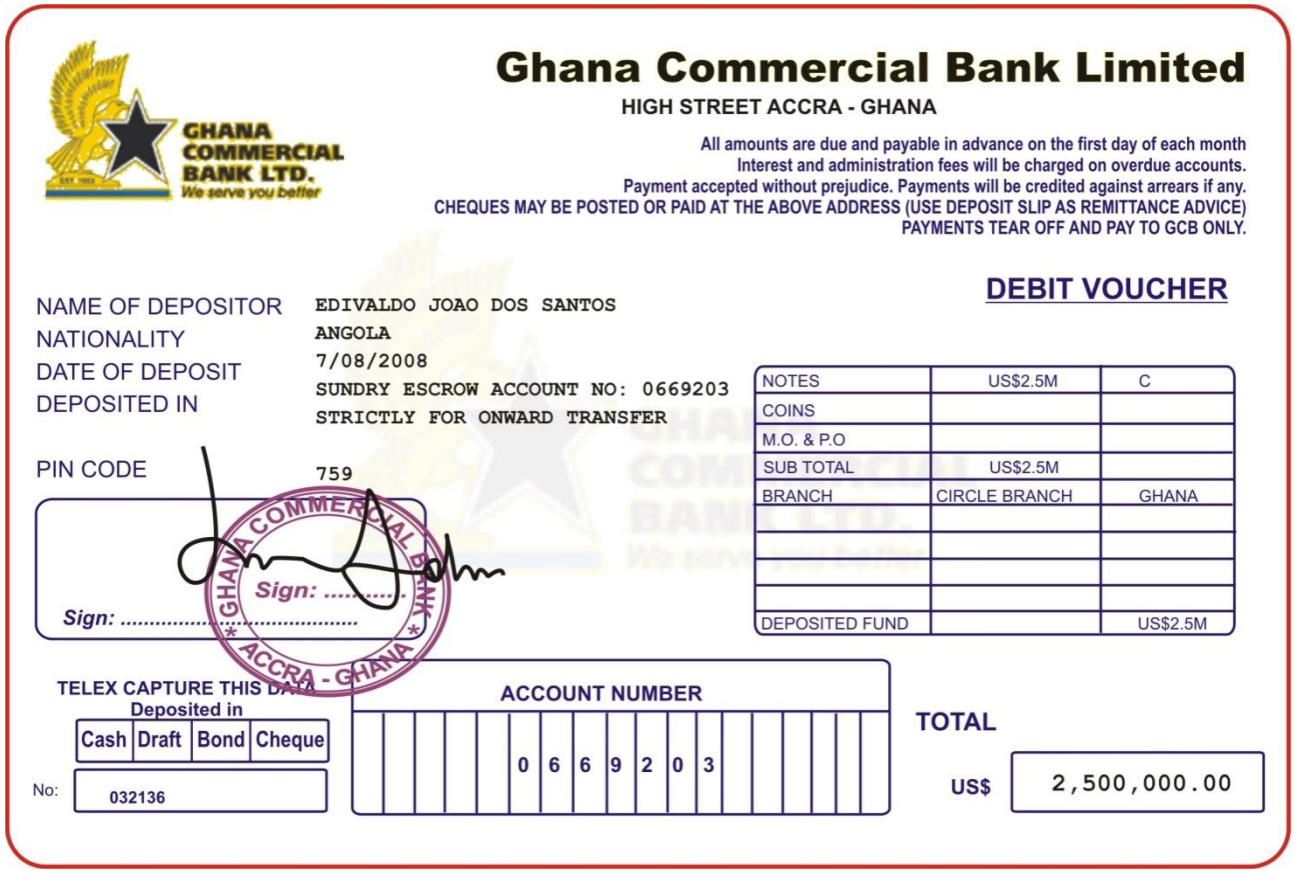


Figura: Suposto deposito bancário em meu nome

Depois de mantermos algumas correaspondências eles enviaram-me uns formulários para que eu preenchesse de formas a transferir os 2,5 milhões de dolares para o meu banco em Angola. Para que a suposta tranferência se efectivasse eles pediam-me para enviar-lhe 500 usd para pagar a transferência, e o mais estranho é que o referido pagamento tinha que ser feito via western union,

estranho não? E para parecer real eles ligam para si, usando as mais diversas técnicas de engenharia social. Tudo isso apenas para ilustrar como os burladores virtuais são muito criativos e extremamente profissionais, para iludirem a sua potencial vitima eles criam uma verdadeira entidade fictícia, com número telefónicos, e-mail proprio, domínio registado e website. É responsabilidade dos bancos garantir que nenhum dominio similar ao seu esteja registado, reservando para si todos os dominios similares.

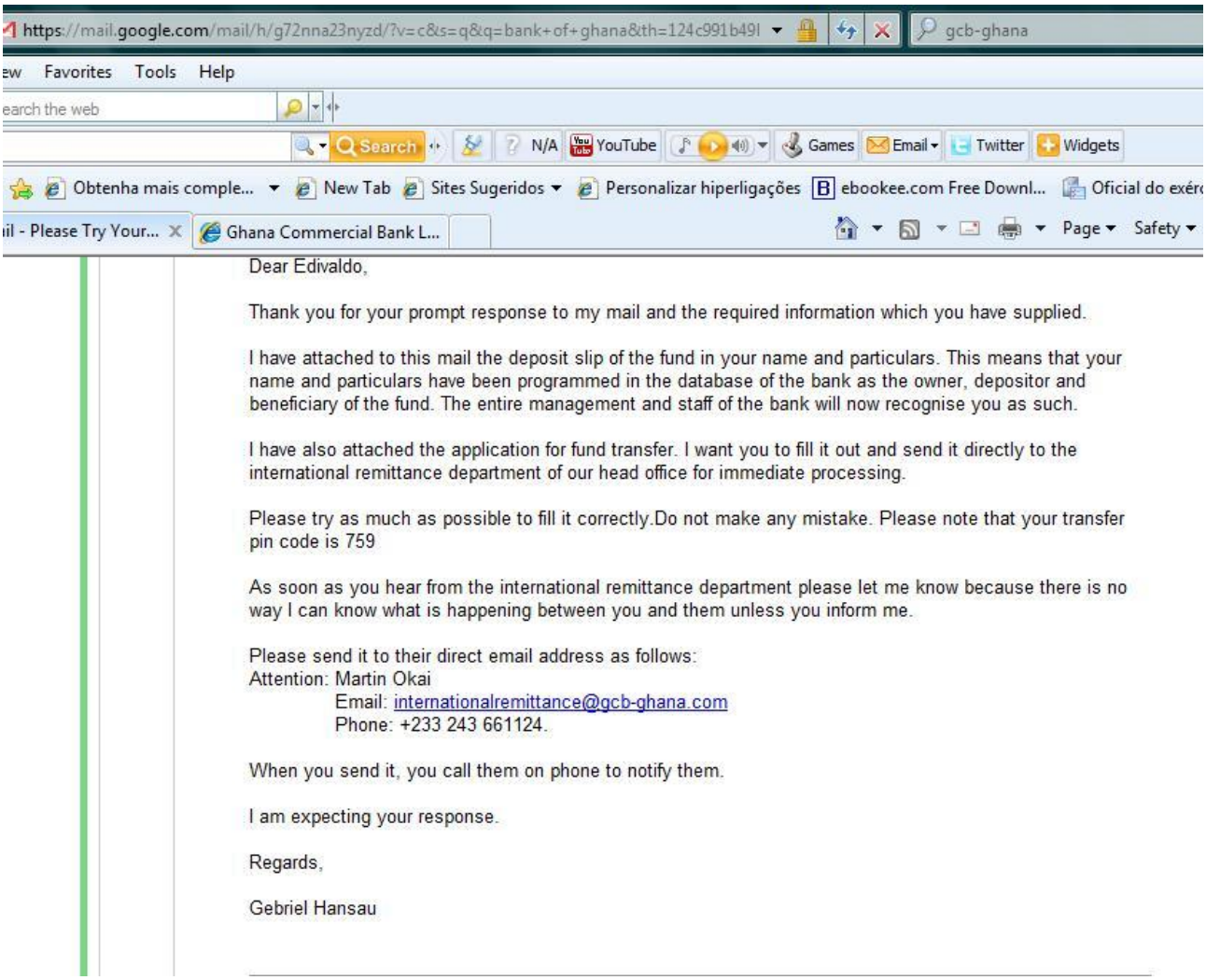


Figura: Correspondência entre mim e o suposto banco

O que é *phishing* e que situações podem ser citadas sobre este tipo de fraude?

Phishing, também conhecido como *phishing scam* ou *phishing/scam*, foi um termo originalmente criado para descrever o tipo de fraude que se dá através do envio de mensagem não solicitada, que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou *site* popular, e que procura induzir o acesso a páginas falsificadas, projectadas para furtar dados pessoais e financeiros de utilizadors.

A palavra *phishing* (de "*fishing*") vem de uma analogia criada pelos burlões, onde "iscas" (*e-mails*) são usadas para "pescar" senhas e dados financeiros de utilizadors da Internet.

Actualmente, este termo vêm sendo utilizado também para se referir aos seguintes casos:

- mensagem que procura induzir o utilizador à instalação de códigos maliciosos, projectados para furtar dados pessoais e financeiros;
- mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros dos utilizadores.

A subseções a seguir apresentam cinco situações envolvendo *phishing*, que são utilizadas por burladores na Internet. Observe que existem variantes para as situações apresentadas. Além disso, novas formas de *phishing* podem surgir, portanto é muito importante que você se mantenha informado sobre os tipos de *phishing* utilizados pelos burladores, através dos veículos de comunicação, como jornais, revistas e *sites* especializados.

Também é muito importante que você, ao identificar um caso de fraude via Internet, notifique a instituição envolvida, para que ela possa tomar as providências adequadas.

Mensagens que contêm *links* para programas maliciosos

Você recebe uma mensagem por *e-mail* ou via serviço de troca instantânea de mensagens, onde o texto procura atrair a sua atenção, seja por curiosidade, por caridade, pela possibilidade de obter alguma vantagem (normalmente financeira), entre outras. O texto da mensagem também pode indicar que a não execução dos procedimentos descritos acarretarão consequências mais sérias, como, por exemplo, a inclusão do seu nome no SPC/SERASA, o cancelamento de um registo, da sua conta bancária ou do seu cartão de crédito, etc. A mensagem, então, procura induzí-lo a clicar num *link*, para baixar e abrir/executar um ficheiro.

Alguns exemplos de temas e respectivas descrições dos textos encontrados em mensagens deste tipo são apresentados na tabela 1.

Tabela 1: Exemplos de temas de mensagens de *phishing*.

Tema	**Texto da mensagem**
Cartões virtuais	*Voxcards*, Humor Tadela, O Carteiro, *Emotioncard*, AACD/Teleton.
Álbuns de fotos	Pessoa supostamente conhecida, celebridades, relacionado com algum facto noticiado (em jornais, revistas, televisão), traição, nudez ou pornografia, serviço de acompanhantes.
Serviço de telefonia	Pendências de débito, aviso de bloqueio de serviços, detalhes de factura, créditos gratuitos para o celular.
Antivírus	a melhor opção do mercado, nova versão, actualização de vacinas, novas funcionalidades, eliminação de vírus do seu computador.
Notícias/boatos	factos amplamente noticiados (ataques terroristas, *tsunami*, terramotos, etc), boatos envolvendo pessoas conhecidas (morte, acidentes ou outras situações que comovem).
Reality shows	BigBrother, Estrelas ao palco, etc -- fotos ou vídeos envolvendo cenas de nudez ou eróticas.
Programas ou ficheiros diversos	Novas versões de *softwares*, correcções para o sistema operacional Windows, músicas, vídeos, jogos, acesso gratuito a canais de TV a cabo ou por satélite no computador, registo ou actualização de currículos.

Pedidos	Orçamento, cotação de preços, lista de produtos.
Diallers	Para conexão Internet gratuita, para aceder imagens ou vídeos restritos.
Sites de comércio electrónico	Actualização de registo, devolução de produtos, cobrança de débitos, confirmação de compra.
Convites	Convites para participação em *sites* de relacionamento (como o hi5, tagged, quepasa, badoo, facebook, orkut, etc) e outros serviços gratuitos.
Dinheiro fácil	Descubra como ganhar dinheiro na Internet.
Promoções	Diversos.
Prémios	Lotarias, instituições financeiras.
Propaganda	Produtos, cursos, treinamentos, concursos.

Cabe ressaltar que a lista de temas na tabela 1 não é exaustiva, nem tão pouco se aplica a todos os casos. Existem outros temas e novos temas podem surgir.

Risco: ao clicar no *link*, será apresentada uma janela, a solicitar que você salve o ficheiro. Depois de salvo, se você abrí-lo ou executá-lo, será instalado um programa malicioso (*malware*) no seu computador, por exemplo, um cavalo de tróia ou outro tipo de *spyware*, projectado para furtar os seus dados pessoais e financeiros, como senhas bancárias ou números de cartões de crédito. Caso o seu programa leitor de *e-mails (outlook ou outro qualquer)* esteja configurado para exibir mensagens em HTML, a janela solicitando que você salve o ficheiro poderá aparecer automaticamente, sem que você clique no *link*.

Ainda existe a possibilidade do ficheiro/programa malicioso ser baixado e executado no computador automaticamente, ou seja, sem a sua intervenção, caso o seu programa leitor de *e-mails* possua vulnerabilidades.

Esse tipo de programa malicioso pode utilizar diversas formas para furtar dados de um utilizador, dentre elas: capturar teclas digitadas no teclado; capturar a posição do cursor e o ecrã ou regiões da ecrã, no momento em que o *mouse* é clicado; sobrepor a janela do *browser* do utilizador com uma janela falsa, onde os dados serão inseridos; ou espionar o teclado do utilizador através da *Webcam* (caso o utilizador a possua e ela esteja apontada para o teclado). Mais detalhes sobre algumas destas técnicas podem ser vistos na secção de *keyloggers*.

Depois de capturados, os seus dados pessoais e financeiros serão enviados para os burladores. A partir daí, os burladores poderão realizar diversas operações, incluindo a venda dos seus dados para terceiros, ou utilização dos seus dados financeiros para efectuar pagamentos, transferir valores para outras contas, etc.

Como identificar: seguem algumas dicas para identificar este tipo de mensagem fraudulenta:

- leia atentamente a mensagem. Normalmente, ela conterá diversos erros gramaticais e de ortografia;
- os burladores utilizam técnicas para ofuscar o real *link* para o ficheiro malicioso, apresentando o que parece ser um *link* relacionado à instituição mencionada na mensagem. Ao passar o cursor do *mouse* sobre o *link*, será possível ver o real endereço do ficheiro malicioso na barra de *status* do programa leitor de *e-mails*, ou *browser*, caso esteja

actualizado e não possua vulnerabilidades. Normalmente, este *link* será diferente do apresentado na mensagem;
- qualquer extensão pode ser utilizada nos nomes dos ficheiros maliciosos, mas fique particularmente atento aos ficheiros com extensões ".exe", ".zip" e ".scr", pois estas são as mais utilizadas. Outras extensões frequentemente utilizadas por burladores são ".com", ".rar" e ".dll";
- fique atento às mensagens que solicitam a instalação/execução de qualquer tipo de ficheiro/programa;
- aceda a página da instituição que supostamente enviou a mensagem e procure por informações relacionadas com a mensagem que você recebeu. Em muitos casos, você vai observar que não é política da instituição enviar *e-mails* para utilizadors da Internet, de forma indiscriminada, principalmente contendo ficheiros anexados.

Recomendações:

- no caso de mensagem recebida por *e-mail*, o remetente **nunca** deve ser utilizado como parâmetro para atestar a veracidade de uma mensagem, pois pode ser facilmente forjado pelos burladores;
- se você ainda tiver alguma dúvida e acreditar que a mensagem pode ser verdadeira, entre em contacto com a instituição para certificar-se sobre o caso, antes de enviar qualquer dado, principalmente informações sensíveis, como senhas e números de cartões de crédito.

Páginas de comércio electrónico ou *Internet Banking* falsificadas

Você recebe uma mensagem por *e-mail* ou via serviço de troca instantânea de mensagens, em nome de um *site* de comércio electrónico ou de uma instituição financeira, por exemplo, um banco. Textos comuns neste tipo de mensagem envolvem o recadastamento ou confirmação dos dados do utilizador, a participação numa nova promoção, etc. A mensagem, então, tenta persuadí-lo a clicar num *link* contido no texto, numa imagem, ou página de terceiros.

Risco: o *link* pode direccioná-lo para uma página *Web* falsificada, semelhante ao *site* que realmente desejas aceder. Nesta página serão solicitados dados pessoais e financeiros, como o número, data de expiração e código de segurança do seu cartão de crédito, ou os números da sua agência e conta bancária, senha do cartão do banco e senha de acesso ao *Internet Banking*.

Ao preencher os campos disponíveis na página falsificada e clicar no botão de confirmação (em muitos casos o botão apresentará o texto "Confirm", "OK", "Submit", etc), os dados serão enviados para os burladores.

A partir daí, os burladores poderão realizar diversas operações, incluindo a venda dos seus dados para terceiros, ou utilização dos seus dados financeiros para efetuar pagamentos, transferir valores para outras contas, etc.

Como identificar: seguem algumas dicas para identificar este tipo de mensagem fraudulenta:

- os burladores utilizam técnicas para ofuscar o real *link* para a página falsificada, apresentando o que parece ser um *link* relacionado à instituição mencionada na mensagem. Ao passar o cursor do *mouse* sobre o *link*, será possível ver o real endereço da página falsificada na barra de *status* do programa leitor de *e-mails*, ou *browser*, caso esteja actualizado e não possua vulnerabilidades. Normalmente, este *link* será diferente do apresentado na mensagem;

- aceda a página da instituição que supostamente enviou a mensagem, seguindo os cuidados apresentados mais abaixo, e procure por informações relacionadas com a mensagem que você recebeu;
- *sites* de comércio eletrónico ou *Internet Banking* confiáveis **sempre** utilizam conexões seguras (vide "**Como verificar se a conexão é segura**") quando dados pessoais e financeiros de utilizadors são solicitados. Caso a página não utilize conexão segura, desconfie imediatamente. Caso a página falsificada utilize conexão segura, um novo certificado (que não corresponde ao *site* verdadeiro) será apresentado e, possivelmente, o endereço mostrado no *browser* será diferente do endereço correspondente ao *site* verdadeiro.

Recomendações:

- no caso de mensagem recebida por *e-mail*, o remetente **nunca** deve ser utilizado como parâmetro para atestar a veracidade de uma mensagem, pois pode ser facilmente forjado pelos burladores;
- se você ainda tiver alguma dúvida e acreditar que a mensagem pode ser verdadeira, entre em contacto com a instituição para certificar-se sobre o caso, antes de enviar qualquer dado, principalmente informações sensíveis, como senhas e números de cartões de crédito.

***E-mails* contendo formulários para o fornecimento de informações sensíveis**

Você recebe um *e-mail* em nome de um *site* de comércio electrónico ou de uma instituição bancária. O conteúdo da mensagem envolve o recadastamento ou confirmação dos seus dados, a participação numa nova promoção, etc.

A mensagem apresenta um formulário, com campos para a digitação de informações envolvendo dados pessoais e financeiros, como o número, data de expiração e código de segurança do seu cartão de crédito, ou os números da sua agência e conta bancária, senha do cartão do banco e senha de acesso ao *Internet Banking*. A mensagem, então, solicita que preenchas o formulário e apresenta um botão para confirmar o envio das informações preenchidas.

Risco: ao preencher os dados e confirmar o envio, as suas informações pessoais e financeiras serão transmitidas para burladores, que, a partir daí, poderão realizar diversas operações, incluindo a venda dos seus dados para terceiros, ou utilização dos seus dados financeiros para efetuar pagamentos, transferir valores para outras contas, etc.

Como identificar: o serviço de *e-mail* convencional não fornece qualquer mecanismo de criptografia, ou seja, as informações, ao serem submetidas, trafegarão em "texto puro" pela Internet. Qualquer instituição confiável **não** utilizaria este meio para o envio de informações pessoais e sensíveis dos seus utilizadores.

Comprometimento do serviço de resolução de nomes

Ao tentar aceder a um *site* de comércio electrónico ou *Internet Banking*, mesmo digitando o endereço directamente no seu *browser*, você é redirecionado para uma página falsificada, semelhante ao *site* verdadeiro.

Duas possíveis causas para este caso de *phishing* são:

- o atacante comprometeu o servidor de nomes do seu provedor (DNS), de modo que todos os acessos a determinados *sites* passaram a ser redirecionados para páginas falsificadas;

- o atacante o induziu a instalar um *malware*, por exemplo, através de uma mensagem recebida por *e-mail* (como mostrado acima), e este *malware* foi especificamente projectado para alterar o comportamento do serviço de resolução de nomes do seu computador, redirecionando os acessos a determinados *sites* para páginas falsificadas.

Apesar de não ter uma definição sólida até a data da publicação deste livo, veículos de comunicação têm utilizado o termo ***pharming*** para referir-se a casos específicos de *phishing*, que envolvem algum tipo de redirecção da vítima para *sites* fraudulentos, através de alterações nos serviços de resolução de nomes.

Risco: ao preencher os campos disponíveis na página falsificada e confirmar o envio dos dados, as suas informações pessoais e financeiras serão transmitidas para burladores, que, a partir daí, poderão realizar diversas operações, incluindo a venda dos seus dados para terceiros, ou utilização dos seus dados financeiros para efectuar pagamentos, transferir valores para outras contas, etc.

Como identificar: neste caso, onde burladores alteram o comportamento do serviço de resolução de nomes, para redirecionar acessos para páginas falsificadas, não são válidas dicas como digitar o endereço directamente no seu *browser*, ou observar o endereço apresentado na barra de *status* do *browser*.

Deste modo, a melhor forma de identificar este tipo de fraude é estar atento para o facto de que *sites* de comércio electrónico ou *Internet Banking* confiáveis **sempre** utilizam conexões seguras quando dados pessoais e financeiros de utilizadores são solicitados. Caso a página não utilize conexão segura, desconfie imediatamente. Caso a página falsificada utilize conexão segura, um novo certificado, que não corresponde ao *site* verdadeiro, será apresentado (mais adiante, veremos detalhes sobre verificação de certificados).

Recomendação: se ainda tiveres alguma dúvida e acreditar que a página pode ser verdadeira, mesmo não utilizando conexão segura, ou apresentando um certificado não compatível, entre em contacto com a instituição para certificar-se sobre o caso, antes de enviar qualquer dado, principalmente informações sensíveis, como senhas e números de cartões de crédito.

Utilização de computadores de terceiros

Você utiliza um computador de terceiros, por exemplo, numa *LAN house*, *cybercafe* ou *stand* de um evento, para aceder a um *site* de comércio electrónico ou *Internet Banking*.

Risco: como estes computadores são utilizados por muitas pessoas, você pode ter todas as suas acções monitoradas (incluindo a digitação de senhas ou número de cartões de crédito), através de programas especificamente projectados para este fim e que podem ter sido instalados previamente.

Recomendação: não utilize computadores de terceiros em operações que necessitem de seus dados pessoais e financeiros, incluindo qualquer uma das suas senhas.

Quais são os cuidados que devo ter ao aceder á *sites* de comércio electrónico ou *Internet Banking*?

Existem diversos cuidados que um utilizador deve ter ao aceder *sites* de comércio electrónico ou *Internet Banking*. Dentre eles, podem-se citar:

- realizar transacções somente em *sites* de instituições que consideres confiáveis;
- procurar sempre digitar no seu *browser* o endereço desejado. Não utilize *links* em páginas de terceiros ou recebidos por *e-mail*;
- certificar-se de que o endereço apresentado no seu *browser* corresponde ao *site* que você realmente queira aceder, antes de realizar qualquer acção;
- certificar-se que o *site* faz uso de conexão segura (ou seja, que os dados transmitidos entre o seu *browser* e o *site* serão criptografados) e utiliza um tamanho de chave considerado seguro;
- antes de aceitar um novo certificado, verificar junto à instituição que mantém o *site* sobre a sua emissão e quais são os dados nele contidos. Então, verificar o certificado do *site* antes de iniciar qualquer transação, para assegurar-se que ele foi emitido para a instituição que se deseja aceder e está dentro do prazo de validade;
- estar atento e prevenir-se dos ataques de engenharia social;
- não aceder *sites* de comércio electrónico ou *Internet Banking* através de computadores de terceiros;
- desligar a sua *Webcam* (caso você possua alguma), ao acessar um *site* de comércio electrónico ou *Internet Banking*.

Além dos cuidados apresentados anteriormente é muito importante que você tenha alguns cuidados adicionais, tais como:

- manter o seu *browser* sempre actualizado e com todas as correcções (*patches*) aplicadas;
- alterar a configuração do seu *browser* para restringir a execução de *JavaScript* e de programas *Java* ou *ActiveX*, excepto para casos específicos;
- configurar o seu *browser* para bloquear *pop-up windows* e permití-las apenas para *sites* conhecidos e confiáveis, onde forem realmente necessárias;
- configurar o seu programa leitor de *e-mails* para não abrir ficheiros ou executar programas automaticamente;
- não executar programas obtidos pela Internet, ou recebidos por *e-mail*.

Com estes cuidados adicionais você pode evitar que o seu *browser* contenha alguma vulnerabilidade, e que programas maliciosos (como os cavalos de tróia e outros tipos de *malware*) sejam instalados no seu computador para, dentre outras finalidades, furtar dados sensíveis e assumir a sua identidade para ter acesso aos seus *sites* de comércio electrónico ou *Internet Banking*.

Como verificar se a conexão é segura (criptografada)?

Existem pelo menos dois itens que podem ser visualizados na janela do seu *browser*, e que significam que as informações transmitidas entre o *browser* e o *site* visitado estão a ser criptografadas.

O primeiro pode ser visualizado no local onde o endereço do *site* é digitado. O endereço deve começar com https:// (diferente do http:// nas conexões normais), onde o **s** antes do sinal de dois-pontos indica que o endereço em questão é de um *site* com conexão segura e, portanto, os dados

serão criptografados antes de serem enviados. A figura abaixo apresenta o primeiro item, a indicar uma conexão segura, observado nos *browsers Firefox* e *Internet Explorer*, respectivamente.

Alguns *browsers* podem incluir outros sinais na barra de digitação do endereço do *site*, que indicam que a conexão é segura. No *Firefox*, por exemplo, o local onde o endereço do *site* é digitado muda de cor, ficando amarelo, e apresenta um cadeado fechado do lado direito.

Figura 1: **https** – a identificar um site com conexão segura.

O segundo item a ser visualizado corresponde a algum desenho ou sinal, indicando que a conexão é segura. Normalmente, o desenho mais adoptado nos *browsers* recentes é de um "**cadeado fechado**", apresentado na barra de *status*, na parte inferior da janela do *browser* (se o cadeado estiver aberto, a conexão não é segura).

A figura abaixo apresenta desenhos dos cadeados fechados, indicando conexões seguras, observados nas barras de *status* nos *browsers Firefox* e *Internet Explorer*, respectivamente.

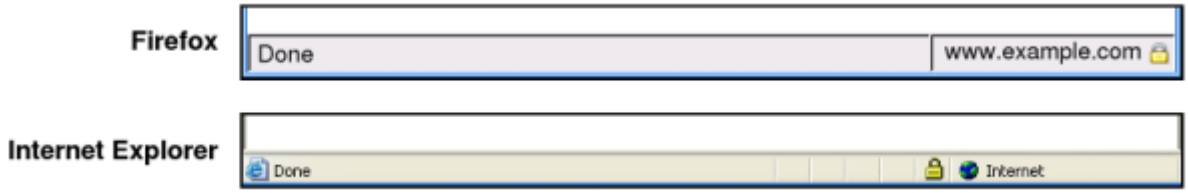


Figura 2: **Cadeado** -- identificando um site com conexão segura.

Ao clicar sobre o cadeado, será exibida um ecrã que permite verificar as informações referentes ao certificado emitido para a instituição que mantém o *site*, bem como informações sobre o tamanho da chave utilizada para criptografar os dados.

É muito importante que você verifique se a chave utilizada para criptografar as informações a serem transmitidas entre o seu *browser* e o *site* é de no mínimo 128 bits. Chaves menores podem comprometer a segurança dos dados a serem transmitidos.

Outro facor muito importante é que a verificação das informações do certificado deve ser feita clicando única e exclusivamente no cadeado exibido na barra *status* do *browser*. Atacantes podem tentar falsificar certificados, incluindo o desenho de um cadeado fechado no conteúdo da página. A figura abaixo ilustra esta situação no *browser Firefox*.

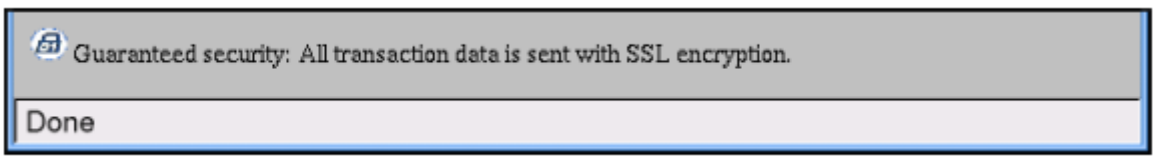


Figura 3: Cadeado falsificado.

Compare as barras de *status* do *browser Firefox* nas figuras 2 e 3. Observe que na figura 3 **não** é apresentado um cadeado fechado dentro da barra de *status*, indicando que a conexão **não** é segura.

Como posso saber se o *site* que estou a aceder não foi falsificado?

Existem alguns cuidados que um utilizador deve ter para certificar-se que um *site* não foi falsificado.

O primeiro cuidado é verificar se o endereço digitado permanece inalterado no momento em que o conteúdo do *site* é apresentado no *browser* do utilizador. Existem algumas situações, como visto acima, onde o acesso a um *site* pode ser redirecionado para uma página falsificada, mas normalmente nestes casos o endereço apresentado pelo *browser* é diferente daquele que o utilizador quer realmente aceder.

E um outro cuidado muito importante é verificar as informações contidas no certificado emitido para a instituição que mantém o *site*. Estas informações podem dizer se o certificado é ou não legítimo e, consequentemente, se o *site* é ou não falsificado.

Como posso saber se o certificado emitido para o *site* é legítimo?

É extremamente importante que o utilizador verifique algumas informações contidas no certificado. Um exemplo de um certificado, emitido para um *site* de uma instituição é mostrado abaixo:

This Certificate belongs to:	This Certificate was issued by:
www.mandiva.org	www.mandivasign.com/CPS Incorp.by Ref.
Terms of use at	LIABILITY LTD.(c)97 MandivaSign
www.mandivasign.com/dir (c)00	MandivaSign International Server CA -
UF Tecno	Class 3
Mandiva Group, Inc.	MandivaSign, Inc.
Cidade, Provincia, AO	

Serial Number:
70:DE:ED:0A:05:20:9C:3D:A0:A2:51:AA:CA:81:95:1A
This Certificate is valid from Sat Aug 20, 2009 to Sun Aug 20, 2010
Certificate Fingerprint:
92:48:09:A1:70:7A:AF:E1:30:55:EC:15:A3:0C:09:F0

O utilizador deve, então, verificar se o certificado foi emitido para o *site* da instituição que ele deseja aceder. As seguintes informações devem ser verificadas:

- o endereço do *site*;
- o nome da instituição (dona do certificado);
- o prazo de validade do certificado.

Ao entrar pela primeira vez num *site* que utiliza conexão segura, o seu *browser* apresentará uma janela a pedir para confirmar o recebimento de um novo certificado. Então, verifique se os dados do certificado correspondem à instituição que você realmente deseja aceder e se o seu *browser* reconheceu a Autoridade Certificadora que emitiu o certificado.

Se ao entrar num *site* com conexão segura, que você utilize com frequência, o seu *browser* apresentar uma janela a pedir para confirmar o recebimento de um novo certificado, fique atento. Uma situação possível seria que a validade do certificado do *site* tenha expirado, ou o certificado tenha sido revogado por outros motivos, e um novo certificado foi emitido para o *site*. Mas isto

também pode significar que você está a receber um certificado ilegítimo e, portanto, estará a aceder um *site* falsificado.

Uma dica para reconhecer esta situação é que as informações contidas no certificado normalmente não corresponderão às da instituição que você realmente deseja aceder. Além disso, o seu *browser* possivelmente informará que a Autoridade Certificadora que emitiu o certificado para o *site* não pôde ser reconhecida.

De qualquer modo, caso você receba um novo certificado ao aceder um *site* e tenha alguma dúvida ou desconfiança, não envie qualquer informação para o *site* antes de entrar em contacto com a instituição que o mantém, para esclarecer o ocorrido.

O que devo fazer se perceber que os meus dados financeiros estão a ser usados por terceiros?

Caso você acredite que terceiros possam estar a utilizar as suas informações pessoais e financeiras, como o número do seu cartão de crédito ou os seus dados bancários (senha de acesso e confirmação do *Internet Banking* e senha do cartão de banco), entre em contacto com a instituição envolvida (por exemplo, o seu banco ou operadora do seu cartão de crédito), informe-os sobre o caso e siga as orientações que serão transmitidas por eles.

Monitore regularmente as suas movimentações financeiras, por exemplo, através de extratos bancários e/ou de cartões de crédito, e procure por débitos, transferências ou cobranças inesperadas.

É recomendado que você procure uma esquadra de polícia, para apresentar uma queixa, caso tenha sido vítima de uma burla via Internet (esses crimes já estão tipificados na legislação Angolana, depois da aprovação da lei sobre "crimes Informáticos", que foi aprovada enquanto eu finalizava esse livro).

Boatos

Boatos (*hoaxes*) são *e-mails* que possuem conteúdos alarmantes ou falsos e que, geralmente, têm como remetente ou apontam como autora da mensagem alguma instituição, empresa importante ou órgão governamental. Através de uma leitura minuciosa deste tipo de *e-mail*, normalmente, é possível identificar no seu conteúdo mensagens absurdas e muitas vezes sem sentido.

Dentre os diversos boatos típicos, que chegam às caixas postais de utilizadores conectados à Internet, podem-se citar as correntes, pirâmides, mensagens sobre pessoas que estão prestes a morrer de câncer, entre outras.

Histórias deste tipo são criadas não só para espalhar desinformação pela Internet, mas também para outros fins maliciosos.

Quais são os problemas de segurança relacionados aos boatos?

Normalmente, o objectivo do criador de um boato é verificar o quanto ele se propaga pela Internet e por quanto tempo permanece propagando-se. De modo geral, os boatos não são responsáveis por grandes problemas de segurança, a não ser ocupar espaço nas caixa de *e-mails* de utilizadores.

Mas podem existir casos com conseqüências mais sérias como, por exemplo, um boato que procura induzir utilizadores de Internet a fornecer informações importantes (como números de documentos, de contas bancárias ou de cartões de crédito), ou um boato que indica uma série de acções a serem realizadas pelos utilizadores e que, se forem realmente efectivadas, podem resultar em danos mais sérios (como instruções para apagar um ficheiro que supostamente contém um vírus, mas que na verdade é parte importante do sistema operacional instalado no computador).

Além disso, *e-mails* de boatos podem conter vírus, cavalos de tróia ou outros tipos de *malware* anexados.

É importante ressaltar que um boato também pode comprometer a credibilidade e a reputação tanto da pessoa ou entidade referenciada como suposta criadora do boato, quanto daqueles que o repassam.

Como evitar a distribuição dos boatos?

Normalmente, os boatos se propagam pela boa vontade e solidariedade de quem os recebe. Isto ocorre, muitas vezes, porque aqueles que o recebem:

- confiam no remetente da mensagem;
- não verificam a procedência da mensagem;
- não verificam a veracidade do conteúdo da mensagem.

Para que você possa evitar a distribuição de boatos é muito importante verificar a procedência dos *e-mails*, e mesmo que tenham como remetente alguém conhecido, é preciso certificar-se que a mensagem não é um boato.

É importante ressaltar que você **nunca** deve repassar este tipo de mensagem, pois estará a aderir ou a concordar com o seu conteúdo.

Como posso saber se um *e-mail* é um boato?

Um boato normalmente apresenta pelo menos uma das características listadas abaixo. Observe que estas características devem ser utilizadas apenas como guia. Nem todo boato apresenta uma destas características e mensagens legítimas podem apresentar algumas delas.

Muitas vezes, um boato:

- sugere consequências trágicas se uma determinada tarefa não for realizada;
- promete ganhos financeiros ou prêmios mediante a realização de alguma acção;
- fornece instruções ou ficheiros anexados para, supostamente, proteger o seu computador de um vírus não detectado por programas antivírus;
- afirma não ser um boato;
- apresenta diversos erros gramaticais e de ortografia;
- apresenta uma mensagem contraditória;
- contém algum texto enfatizando que deves repassar a mensagem para o maior número de pessoas possível;
- já foi encaminhado diversas vezes (no corpo da mensagem normalmente é possível observar cabeçalhos de *e-mails* encaminhados por outras pessoas).

Existem *sites* especializados na Internet onde podem ser encontradas listas contendo os boatos que estão a circular e os seus respectivos conteúdos.

Alguns destes *sites* são:

- *Hoaxbusters* -- http://hoaxbusters.ciac.org/
- QuatroCantos -- http://www.quatrocantos.com/LENDAS/ (em português)
- *Urban Legends and Folklore* -- http://urbanlegends.about.com/
- *Urban Legends Reference Pages* -- http://www.snopes.com/
- *TruthOrFiction.com* -- http://www.truthorfiction.com/
- *Symantec Security Response Hoaxes* -http://www.symantec.com/avcenter/hoax.html
- *McAfee Security Virus Hoaxes* -- http://vil.mcafee.com/hoax.asp

Cuidados com os seus Dados Pessoais

Procure não fornecer os seus dados pessoais (como nome, *e-mail*, endereço e números de documentos) para terceiros. Também **nunca** forneça informações sensíveis (como senhas e números de cartão de crédito), a menos que esteja a ser realizada uma transacção (comercial ou financeira) e se tenha certeza da idoneidade da instituição que mantém o *site*.

Estas informações geralmente são armazenadas em servidores das instituições que mantêm os *sites*. Com isso, corre-se o risco destas informações serem repassadas sem a sua autorização para outras instituições ou de um atacante comprometer este servidor e obter acesso a todas as informações.

Fique atento aos ataques de engenharia social, vistos na Parte I - Noções de Segurança. Ao ter acesso a seus dados pessoais, um atacante poderia, por exemplo, utilizar seu *e-mail* em alguma lista de distribuição de *spams* ou fazer-se passar por você na Internet (através do uso de uma das suas senhas).

Realização de Cópias de Segurança (*Backups*)

Qual é a importância de fazer cópias de segurança?

Cópias de segurança dos dados armazenados num computador são importantes, não só para se recuperar de eventuais falhas, mas também das consequências de uma possível infecção por vírus, ou de uma invasão.

Quais são as formas de realizar cópias de segurança?

Cópias de segurança podem ser simples como o armazenamento de ficheiros em CDs ou DVDs, ou mais complexas como o espelhamento de um disco duro inteiro num outro disco de um computador.

Actualmente, uma unidade gravadora de CDs/DVDs e um *software* que possibilite copiar dados para um CD/DVD são suficientes para que a maior parte dos utilizadores de computadores realizem as suas cópias de segurança.

Também existem equipamentos e *softwares* mais sofisticados e específicos que, dentre outras actividades, automatizam todo o processo de realização de cópias de segurança, praticamente sem intervenção do utilizador. A utilização de tais equipamentos e *softwares* envolve custos mais elevados e depende de necessidades particulares de cada utilizador.

Com que frequência devo fazer cópias de segurança?

A frequência com que é realizada uma cópia de segurança e a quantidade de dados armazenados neste processo depende da periodicidade com que o utilizador cria ou modifica ficheiros. Cada utilizador deve criar a sua própria política para a realização de cópias de segurança.

Que cuidados devo ter com as cópias de segurança?

Os cuidados com cópias de segurança dependem das necessidades do utilizador. O utilizador deve procurar responder algumas perguntas antes de adoptar um ou mais cuidados com as suas cópias de segurança:

- Que informações realmente importantes precisam estar armazenadas nas minhas cópias de segurança?
- Quais seriam as consequências/prejuízos, caso as minhas cópias de segurança fossem destruídas ou danificadas?
- O que aconteceria se as minhas cópias de segurança fossem furtadas?

Baseado nas respostas para as perguntas anteriores, um utilizador deve atribuir maior ou menor importância a cada um dos cuidados discutidos abaixo (o mesmo aplica-se a ambientes empresariais ou organizacionais, apenas substitui-se o singular pelo colectivo).

Escolha dos dados. Cópias de segurança devem conter apenas ficheiros confiáveis do utilizador, ou seja, que não contenham vírus e nem sejam algum outro tipo de *malware*. Ficheiros do sistema operacional e que façam parte da instalação dos *softwares* de um computador não devem fazer parte das cópias de segurança. Eles podem ter sido modificados ou substituídos por versões maliciosas, que quando restauradas podem trazer uma série de problemas de segurança para um computador. O sistema operacional e os *softwares* de um computador podem ser reinstalados de mídias confiáveis, fornecidas por fabricantes confiáveis.

Mídia utilizada. A escolha da mídia para a realização da cópia de segurança é extremamente importante e depende da importância e da vida útil que a cópia deve ter. A utilização de alguns disquetes para armazenar um pequeno volume de dados que são modificados constantemente é perfeitamente viável. Mas um grande volume de dados, de maior importância, que deve perdurar por longos períodos, deve ser armazenado em mídias mais confiáveis, como por exemplo os CDs ou DVDs.

Local de armazenamento. Cópias de segurança devem ser guardadas num local condicionado (longe de muito frio ou muito calor) e restrito, de modo que apenas pessoas autorizadas tenham acesso a este local (segurança física).

Cópia em outro local. Cópias de segurança podem ser guardadas em locais diferentes. Um exemplo seria manter uma cópia em casa e outra no escritório. Também existem empresas especializadas em manter áreas de armazenamento com cópias de segurança dos seus clientes. Nestes casos é muito importante considerar a segurança física das suas cópias, como discutido no item anterior.

Criptografia dos dados. Os dados armazenados numa cópia de segurança podem conter informações sigilosas. Neste caso, os dados que contenham informações sigilosas devem ser armazenados em algum formato criptografado.

Que cuidados devo ter ao enviar um computador para a reparação?

É muito importante fazer cópias de segurança dos dados de um computador antes que ele apresente algum problema e seja necessário enviá-lo para a manutenção ou assistência técnica.

Em muitos casos, o computador pode apresentar algum problema que impossibilite a realização de uma cópia de segurança dos dados antes de enviá-lo para a manutenção. Portanto, é muito importante que o utilizador tenha disponível cópias de segurança recentes dos seus dados. Não se pode descartar a possibilidade de, ao receber o seu computador, ter a infeliz surpresa que todos os seus dados foram apagados durante o processo de manutenção.

Tenha sempre em mente que procurar uma assistência técnica de confiança é fundamental, principalmente se existirem dados sensíveis armazenados no seu computador, como documentos e outras informações sigilosas, certificados digitais, entre outros.

RISCOS ENVOLVIDOS NO USO DA INTERNET E MÉTODOS DE PREVENÇÃO

Programas Leitores de *E-mails*

Quais são os riscos associados ao uso de um software leitor de *e-mails*?

A maioria dos problemas de segurança envolvendo *e-mails* estão relacionados aos conteúdos das mensagens, que normalmente abusam das técnicas de engenharia social ou de características de determinados programas leitores de *e-mails*, que permitem abrir ficheiros ou executar programas anexados às mensagens automaticamente.

É possível configurar um programa leitor de *e-mails* de forma mais segura?

Sim. Algumas dicas de configuração para melhorar a segurança do seu programa leitor de *e-mails* são:

1. desligar as opções que permitem abrir ou executar automaticamente ficheiros ou programas anexados às mensagens;
2. desligar as opções de execução de *JavaScript* e de programas *Java*;
3. desligar, se possível, o modo de visualização de *e-mails* no formato HTML.

Estas configurações podem evitar que o seu programa leitor de *e-mails* propague automaticamente vírus e cavalos de tróia, entre outros. Existem programas leitores de *e-mails* que não implementam tais funções e, portanto, não possuem estas opções.

É importante ressaltar que se o utilizador seguir as recomendações dos itens 1 e 2, mas ainda assim abrir os ficheiros ou executar manualmente os programas que vêm anexados aos *e-mails*, poderá ter algum problema que resulte na violação da segurança do seu computador.

Que medidas preventivas devo adoptar no uso dos programas leitores de *e-mails*?

Algumas medidas preventivas que minimizam os problemas trazidos com os *e-mails* são:

- manter sempre a versão mais actualizada do seu programa leitor de *e-mails*;
- não clicar em *links* que, por ventura, possam aparecer no conteúdo do *e-mail*. Se você realmente quiser aceder a página do *link*, digite o endereço directamente no seu *browser*;
- evitar abrir ficheiros ou executar programas anexados aos *e-mails*, sem antes verificá-los com um antivírus;
- desconfiar sempre dos ficheiros anexados à mensagem, mesmo que tenham sido enviados por pessoas ou instituições conhecidas. O endereço do remetente pode ter sido falsificado e o ficheiro anexo pode ser, por exemplo, um vírus ou um cavalo de tróia;
- fazer o *download* de programas directamente do *site* do fabricante;
- evitar utilizar o seu programa leitor de *e-mails* como um *browser*, desligando o modo de visualização de *e-mails* no formato HTML.

Actualmente, utilizadores da Internet têm sido bombardeados com *e-mails* indesejáveis e, principalmente, com mensagens fraudulentas cuja finalidade é a obtenção de vantagens financeiras. Alguns exemplos são:

- mensagens a oferecer grandes quantias em dinheiro, mediante uma transferência electrónica de fundos;

- mensagens com ofertas de produtos com preços muito abaixo dos preços praticados pelo mercado;
- mensagens que procuram induzir o utilizador a aceder uma determinada página na Internet ou a instalar um programa, abrir um álbum de fotos, ver cartões virtuais, etc, mas cujo verdadeiro obectivo é fazer com que o utilizador forneça dados pessoais e sensíveis, como contas bancárias, senhas e números de cartões de crédito.

Mais detalhes sobre estes tipos de *e-mail*, bem como formas de prevenção, podem ser vistos na secção que fala sobre fraudes na Internet.

NB: Existem vírus e outros tipos de *software* malicioso que utilizam o *e-mail* como meio para sua propagação e quase sempre falsificam o endereço do remetente.

Browsers

Quais são os riscos associados ao uso de um *browser*?

Existem diversos riscos envolvidos na utilização de um *browser*. Dentre eles, podem-se citar:

- execução de *JavaScript* ou de programas *Java* hostis;
- execução de programas ou controlos *ActiveX* hostis;
- obtenção e execução de programas hostis em *sites* não confiáveis ou falsos;
- acesso a *sites* falsos, fazendo-se passar por instituições bancárias ou de comércio electrónico;
- realização de transacções comerciais ou bancárias via *Web*, sem qualquer mecanismo de segurança.

Nos dois primeiros casos o *browser* executa os programas automaticamente, ou seja, sem a interferência do utilizador.

Quais são os riscos associados à execução de *JavaScripts* e de programas *Java*?

Normalmente os *browsers* contêm módulos específicos para processar programas *Java*. Apesar destes módulos fornecerem mecanismos de segurança, podem conter falhas de implementação e, neste caso, permitir que um programa *Java* hostil cause alguma violação de segurança num computador.

JavaScripts, entre outros *scripts Web* disponíveis, são muito utilizados actualmente para incorporar maior funcionalidade e melhorar a aparência de páginas *Web*. Apesar de nem sempre apresentarem riscos, vêm sendo utilizados por atacantes para causar violações de segurança em computadores. Um tipo de ataque que envolve *JavaScript* consiste em redirecionar utilizadores de um *site* legítimo para um *site* falso, para que o utilizador instale programas maliciosos ou forneça informações pessoais.

Quais são os riscos associados à execução de programas *ActiveX*?

Antes de receber um programa *ActiveX*, o seu *browser* verifica sua procedência através de um esquema de certificados digitais. Se você optar por aceitar o certificado, o programa é executado no seu computador.

Ao serem executados, os programas *ActiveX* podem fazer de tudo, desde enviar um ficheiro qualquer pela Internet, até instalar programas (que podem ter fins maliciosos) no seu computador.

Quais são os riscos associados ao uso de *cookies*?

Muitos *sites* utilizam *cookies* para obter informações, como por exemplo, as preferências de um utilizador. Estas informações, muitas vezes, são partilhadas entre diversas entidades na Internet e podem afectar a privacidade do utilizador.

Quais são os riscos associados às *pop-up windows*?

Pop-up windows são janelas que aparecem automaticamente e sem permissão, sobrepondo a janela do *browser*, após o utilizador aceder um *site*. Este recurso tem sido amplamente utilizado para apresentar mensagens com propaganda para utilizadores da Internet e, por este motivo, tem sido também classificado como *pop-up spam*.

Em muitos casos, as mensagens contidas nas *pop-up windows* apresentam *links*, que podem redirecionar o utilizador para uma página falsa ou induzí-lo a instalar algum *software* malicioso para, por exemplo, furtar senhas bancárias ou números de cartões de crédito. Exemplos do uso malicioso de *pop-up windows* podem ser vistos na seccão que aborda a questão de "fraudes na Internet".

Quais são os cuidados necessários para realizar transacções via *Web*?

Normalmente as transacções, sejam comerciais ou bancárias, envolvem informações sensíveis, como senhas ou números de cartões de crédito.

Portanto, é muito importante que você, ao realizar transacções via *Web*, certifique-se da procedência dos *sites* e se estes *sites* são realmente das instituições que dizem ser. Também é fundamental que eles forneçam mecanismos de segurança para evitar que alguém conectado à Internet possa obter informações sensíveis de suas transacções, no momento em que estiverem a ser realizadas.

Que medidas preventivas devo adoptar no uso de *browsers*?

Algumas medidas preventivas para o uso de *browsers* são:

- manter o seu *browser* sempre actualizado;
- desactivar a execução de programas *Java* na configuração de seu *browser*. Se for absolutamente necessário o *Java* estar activado para que as páginas de um *site* possam ser vistas, basta activá-lo antes de entrar no *site* e, então, desactivá-lo ao sair;
- desactivar a execução de *JavaScripts* antes de entrar numa página desconhecida e, então, activá-la ao sair. Caso você opte por desactivar a execução de *JavaScripts* na configuração de seu *browser*, é provável que muitas páginas *Web* não possam ser visualizadas;
- permitir que programas *ActiveX* sejam executados no seu computador **apenas** quando vierem de *sites* conhecidos e confiáveis;
- manter maior controlo sobre o uso de *cookies*, caso você queira ter maior privacidade ao navegar na Internet (ver a secção privacidade)
- bloquear *pop-up windows* e permití-las apenas para *sites* conhecidos e confiáveis, onde forem realmente necessárias;
- certificar-se da procedência do *site* e da utilização de conexões seguras ao realizar transacções via;

- somente aceder *sites* de instituições financeiras e de comércio electrónico digitando o endereço directamente no seu *browser*, nunca clicando em algum *link* existente numa página ou em algum *e-mail*. Assim, você pode evitar ser redirecionado para uma página fraudulenta ou ser induzido a instalar algum *software* malicioso, que tem como objectivo furtar os seus dados pessoais.

Que características devo considerar na escolha de um *browser*?

Existem características muito importantes que você deve considerar no momento de escolher um *browser*. Algumas destas características são:

- histórico de vulnerabilidades associadas ao *browser* e o tempo decorrido entre a descoberta da vulnerabilidade e o lançamento da correcção;
- **não** instalação/execução automática de programas;
- facilidade para identificar se o *site* usa conexão segura e para visualizar dados do certificado digital;
- disponibilidade de mecanismos para desabilitar a execução de programas *Java*, *JavaScript*, *ActiveX*, entre outros;
- disponibilidade de mecanismos que permitam bloquear (incluindo bloqueio selectivo) *cookies* e *pop-up windows*.

Antivírus

Os antivírus são programas que procuram detectar e, de seguida, anular ou remover os vírus de computador. Actualmente, novas funcionalidades têm sido adicionadas aos programas antivírus, de modo que alguns procuram detectar e remover cavalos de tróia e outros tipos de código maliciosos, barrar programas hostis e verificar *e-mails*.

Que funcionalidades um bom antivírus deve possuir?

Um bom antivírus deve:

- identificar e eliminar a maior quantidade possível de vírus e outros tipos de *malware*;
- analisar os ficheiros que estão a ser obtidos através da Internet;
- verificar continuamente os discos duros (HDs), flexíveis (disquetes) e unidades removíveis, como CDs, DVDs e *pen drives*, de forma transparente ao utilizador;
- procurar vírus, cavalos de tróia e outros tipos de *malware* em ficheiros anexados aos *e-mails*;
- criar, sempre que possível, uma mídia de verificação (disquete ou CD de *boot*) que possa ser utilizado caso um vírus desactive o antivírus que está instalado no computador;
- actualizar as assinaturas de vírus e *malwares* conhecidos, pela rede, de preferência diariamente.

Alguns antivírus, além das funcionalidades acima, permitem verificar *e-mails* enviados, podendo detectar e barrar a propagação por *e-mail* de vírus, *worms*, e outros tipos de *malware*.

Como fazer uso correcto do seu antivírus?

As dicas para o bom uso do antivírus são simples:

- mantenha o antivírus e as suas assinaturas sempre actualizados;
- configure-o para verificar automaticamente ficheiros anexados aos *e-mails* e ficheiros obtidos pela Internet;
- configure-o para verificar automaticamente mídias removíveis (CDs, DVDs, *pen drives*, disquetes, discos para Zip, etc);
- configure-o para verificar todo e qualquer formato de ficheiro (qualquer tipo de extensão de ficheiro);
- se for possível, crie o disco de verificação e utilize-o esporadicamente, ou quando o seu computador estiver a apresentar um comportamento anormal (mais lento, gravando ou lendo o disco duro fora de hora, etc);

Algumas versões de antivírus são gratuitas para uso pessoal e podem ser obtidas pela Internet. Mas antes de obter um antivírus pela Internet, verifique a sua procedência e certifique-se que o fabricante • é confiável.

O que um antivírus não pode fazer?

Um antivírus não • é capaz de impedir que um atacante tente explorar alguma vulnerabilidade existente num computador. Também não • é capaz de evitar o acesso não autorizado a um *backdoor* instalado num computador.

Existem também outros mecanismos de defesa, conhecidos como *firewalls*, que podem prevenir contra tais ameaças.

Firewall

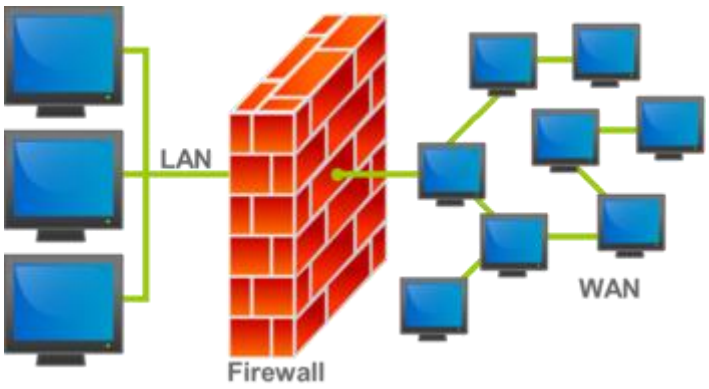
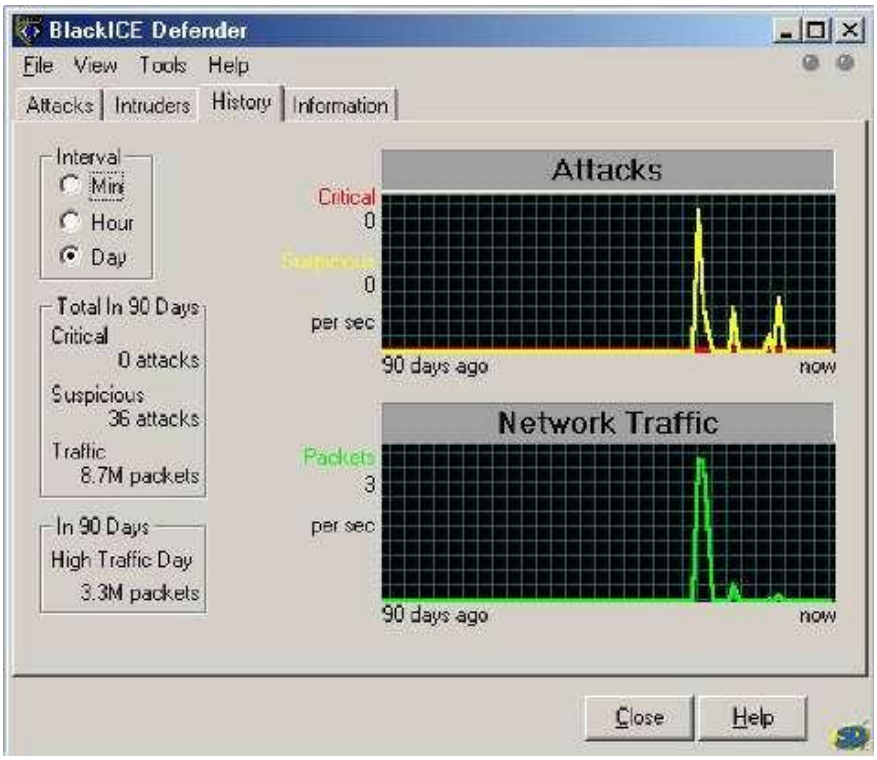


Figura: Firewall a separar duas redes

Conceito de Firewall

Firewall ou barreira de fogo é um artifício largamente usado em redes. A sua função é proteger o sistema de tentativas indevidas de acesso, principalmente vindas da Internet. Ele controla o tráfego, permitindo ou negando acesso a certas portas de serviços. Geralmente se deixa apenas a porta 80 (www) activa para que as pessoas consigam aceder o website da empresa. Resumidamente o firewall é o seguinte: um dispositivo que possui duas placas de rede, sendo uma ligada à rede interna e outra ligada à Internet. A partir disto pode-se implementar uma politica de segurança, que consiste num pacote que determina o que é ou não permitido passar de uma rede à outra. Podem ser feitos de software ou hardware.



Exemplo do firewall blackice em execução. (www.blackice.com)

Eficiência

Existem 2 tipos de firewall: um que analisa a camada de rede, o pacote IP, e outro que analisa a camada de aplicação, dentro do pacote IP.

Firewall analisando a camada de rede

Estes limitam-se ao nível de IP. Decidindo o destino dos pacotes (aceito ou não), tendo como base: remetente, porta IP utilizada e endereço do destinatário. Qualquer roteador pode ser configurado para firewall, mas será um firewall simples. Isto fará com que ele fique protegido contra crackers iniciantes, mas pode ser vítima de ataques comuns e bem clássicos. Como por exemplo: *o IP Spoof*

Em máquinas bem configuradas, a barreira de fogo concede acesso apenas a computadores considerados de confiança (endereços conhecidos). Para introduzir-se a uma máquina bem configurada é necessário fazer com que ela o considere confiável. Isto se chama spoofing. Consiste em mandar pacotes com o endereço legítimo de uma máquina da rede interna. A vítima acreditará que o invasor é de confiança e responderá enviando pacotes para o endereço do remetente. No entanto o cracker deve tomar precauções:

- Certificar-se que a máquina legítima não responda aos pacotes. Isto é feito garantindo-se que ela esteja off-line (desconectada);
- Garantir que aqueles pacotes sejam enviados para a Internet, já que a máquina legítima encontra-se dentro da rede interna.

Para isto é usado o " **source routing** ", que consiste numa técnica criada para testes. Ela permite que o computador que inicia a comunicação especifique qual a rota de todos os pacotes de uma certa conexão. Isto faz com que os pacotes sejam expelidos da rede para a Internet (veja em anonimidade uma explicação mais simples do IP Spoofing).

Firewalls mais sofisticados não permitem a uso do spoofing e do source-routing, pois eles, além de rotearem os pacotes para seus destinos também mantém informações sobre o estado das conexões e sobre o conteúdo do pacote, o que permite impedir que um pacote pertencente à rede interna seja mandado à Internet. O firewall irá caracterizar isto como um ataque e tomará as devidas providências.

Sofisticados, ou não, eles são transparentes e rápidos pois roteiam tráfegos directos e é exactamente isso que o impede de analisar o conteúdo efectivo do pacote e também exige que as máquinas na rede interna possuam um endereço IP válido.

Firewall analisando a camada de aplicação

Estes normalmente são CPUs de uso geral de rede que rodam programas chamados: "proxy servers". Este tipo de firewall não permite comunicações directas entre duas redes, pois requerem o estabelecimento de duas conexões. Uma delas do remetente proxy e a segunda entre o remetente e o destinatário. Todo pacote antes de ser ecoado é analisado pelo proxy server. Ele irá decidir se o pacote deve ou não ser descartado. Vale saber que devido a estas características o firewall de aplicação oferece uma segurança maior do que o firewall de rede, pois consegue perceber perigo num pacote que o de rede não conseguiria.

Dois exemplos de coisas que este tipo de defesa pode filtrar são:

- O primeiro é DEBUG do SMTP que é usado para pedir a um servidor de correio que forneça algumas informações de controlo. O que é considerado um risco.

- Um segundo exemplo são os Proxys FTP, que cortam o acesso de utilizadores externos, mas mesmo assim, permite que os funcionários copiem ficheiros da Internet para a rede.

Cada uma dessas vantagens depende do funcionamento do protocolo de defesa, sendo que estes não poderiam ser colocados nos firewalls de rede, já que não são capazes de analisar o conteúdo do pacote IP. Firewalls de rede são mais transparentes do que os de aplicação, já que os de aplicação exigem a existência de um proxy, além de proibir a comunicação directa entre o servidor e o cliente. É necessário que o programa cliente saiba que deve estabelecer com o proxy e determinar acções. Então basta configurar o browser correctamente.

Muitas vezes os clientes não são sofisticados o suficiente, e necessitam de conexões directas com o servidor. Neste caso utiliza-se o seguinte artifício: o utilizador se loga no proxy e este em vez de solicitar nome e senha (como seria de esperar), solicita o nome do servidor com o qual se deseja a conexão e a partir daí, tudo funciona normalmente.

Os firewalls são essenciais e importantíssimos, quando bem configurados. Possuem falhas (como visto anteriormente) assim como qualquer tipo de programa, e essas devem ser corrigidas. Nenhum firewall é 100% seguro, mas ajuda muito (e como ajuda). Compre já ! Ou utilize software livre. Veja alguns firewalls em: www.isohunt.com, www.thepiratebay.org ou www.superdownloads.com.br experimente alguns como o **Languard, Conseal PC Firewall , o Zone Alarm** e outros.

Nota: não sei se ficou claro, mas o Firewall também pode ser usado muito bem contra trojans, detectando praticamente tudo (mas ele não retira o trojan do Computador).

Como o *firewall* pessoal funciona?

Se alguém ou algum programa suspeito tentar conectar-se ao seu computador, um *firewall* bem configurado entra em acção para bloquear tentativas de invasão, podendo barrar também o acesso a *backdoors*, mesmo se já estiverem instalados no seu computador.

Alguns programas de *firewall* permitem analisar continuamente o conteúdo das conexões, filtrando vírus de *e-mail*, cavalos de tróia e outros tipos de *malware*, antes mesmo que os antivírus entrem em acção.

Também existem pacotes de *firewall* que funcionam em conjunto com os antivírus, fornecendo um nível de segurança maior para os computadores onde são utilizados.

Por que devo instalar um *firewall* pessoal no meu computador?

É comum observar relatos de utilizadores que acreditam ter computadores seguros por utilizarem apenas programas antivírus. O facto é que a segurança de um computador não pode basear-se apenas num mecanismo de defesa.

Um antivírus não é capaz de impedir o acesso a um *backdoor* instalado num computador. Já um *firewall* bem configurado pode bloquear o acesso a ele.

Além disso, um *firewall* poderá bloquear as tentativas de invasão ao seu computador e possibilitar a identificação das origens destas tentativas.

Alguns fabricantes de *firewalls* oferecem versões gratuitas dos seus produtos para uso pessoal. Mas antes de obter um *firewall*, verifique a sua procedência e certifique-se que o fabricante é confiável.

Como posso saber se alguém está a tentar invadir o meu computador?

Normalmente os *firewalls* criam ficheiros no seu computador, denominados ficheiros de registo de eventos (*logs*). Nestes ficheiros são armazenadas as tentativas de acesso não autorizado ao seu computador, para serviços que podem ou não estar habilitados.

Partilha de Recursos do Windows

Quais são os riscos associados ao uso da partilha de recursos?

Um recurso partilhado aparece no Explorer do Windows como uma "mãozinha" a segurar a parte de baixo do ícone (pasta, impressora ou disco), como mostra a figura 1.

Figura 1: Exemplos de ícones para recursos partilhados.

Alguns dos riscos envolvidos na utilização de recursos partilhados por terceiros são:

- abrir ficheiros ou executar programas que contenham vírus;
- executar programas que sejam cavalos de tróia ou outros tipos de *malware*.

Já alguns dos riscos envolvidos em partilhar recursos do seu computador são:

- permitir o acesso não autorizado a recursos ou informações sensíveis;
- permitir que um atacante possa utilizar tais recursos, sem quaisquer restrições, para fins maliciosos. Isto pode ocorrer se não forem definidas senhas para as partilhas.

Que medidas preventivas devo adoptar no uso da partilha de recursos?

Algumas medidas preventivas para o uso da partilha de recursos do Windows são:

- ter um bom antivírus instalado no seu computador, mantê-lo actualizado e utilizá-lo para verificar qualquer ficheiro ou programa partilhado, pois eles podem conter vírus ou cavalos de tróia, entre outros tipos de *malware*;
- estabelecer senhas para as partilhas, caso seja estritamente necessário partilhar recursos do seu computador. Procure elaborar senhas fáceis de recordar e difíceis de serem descobertas.

É importante ressaltar que você deve sempre utilizar senhas para os recursos que deseje partilhar, principalmente os que estão habilitados para leitura e escrita. E, quando possível, não partilhe recursos ou não deixe-os partilhados por muito tempo.

FAQ - Perguntas mais frequentes

Visando partilhar assuntos relacionados à segurança, criei este tópico. A principal finalidade dele é discutir e responder questões muito encontradas hoje em dia. Às vezes por falta de uma resposta concreta, digamos assim, muitos não sabem o que é verdade e o que é mentira em algumas ocasiões, principalmente na área da informática que é uma área profundamente complexa.

Acho que a segurança da informação é um detalhe essencial na vida de um internauta. E por isso achei interessante criar um FAQ deste tipo aqui no fórum. Mas vejam bem, a intenção não é apenas passar meu conhecimento ou querer parecer ser o único entendido do assunto, mas sim discutirmos sobre este assunto pois é muito importante.

Sintam-se à vontade para perguntarem, responderem, discutirem, acrescentarem, palpitarem, discordarem, enfim... de algo.

O que um vírus ou malware pode fazer se infectar meu sistema?

São diversos os problemas que você pode enfrentar quando está infectado. Dependendo do vírus, ele pode fazer praticamente tudo de ruim com seu computador, até mesmo impedi-lo de iniciar. Abaixo listei alguns dos principais problemas enfrentados com uma máquina infectada:

- Exclusão de ficheiros legítimos;
- Gerar erros em programas e ficheiros;
- Diminuir o espaço do HD;
- Gerar blue screen (tela azul) constantemente;
- Substituir a MBR (Master Boot Record) do disco rígido por códigos maliciosos;
- Criar partições fantasmas;
- Duplicar ou substituir os ficheiros;
- Impedi-lo de abrir o antivírus ou qualquer outro programa de segurança instalado na máquina;
- Impedi-lo de reiniciar em Modo de Segurança;
- Impedi-lo de aceder ao disco rígido ou algum directório;
- Impedi-lo de aceder à Internet;
- Impedi-lo de activar as opções de ver pastas e ficheiros ocultos;
- Impedi-lo de aceder aos consoles do Windows como: Gpedit.msc, services.msc;
- Impedi-lo de abrir o gestor de tarefas e o editor de registo (regedit);
- Impedi-lo de desligar o computador;
- Impedi-lo de instalar/desinstalar/baixar/rodar programas;
- Impedir o computador de iniciar;
- Criar/recriar malwares ou vírus em cada reboot da máquina;
- Baixar malwares ou vírus;
- Infectar ficheiros legítimos e documentos importantes (em geral);
- Interromper um scan com o antivirus ou outro programa de segurança;
- Desactivar a restauração do sistema;
- Causar lentidão no sistema e demora para iniciar;
- Modificar a data e hora do sistema;
- Aumentar o consumo de memória dos ficheiros;
- Roubar e enviar seus dados pessoais como: Senhas e documentos importantes;

● Gerar barulhos, ruídos e outras coisas do tipo;
● Exibir imagens de anúncios e de erros aleatoriamente;
● Aumentar o tamanho dos ficheiros e das pastas;
● Contaminar a rede;
● Abrir ou fechar portas cruciais e importantes do sistema;
● Causar problemas nas comunicações dos dispositivos de hardware, tais como algumas teclas do teclado não funcionarem e/ou saírem diferentes, com a impressora, com o modem, com o rato, etc;
● Fazer o computador dar logoff/reiniciar/desligar sozinho;
● Entre outros problemas.

Recordando também que muitos vírus, depois de terem sido removidos, deixam o sistema completamente instável. Sendo necessário uma reparação ou até mesmo uma formatação para que a instabilidade desapareça de vez.

Posso utilizar dois antivírus?

Na verdade, poder pode. Mas de forma alguma é recomendado. Ter dois, três, quatro, cinco, seis... antivírus instalados no computador não é sinónimo de mais segurança, ou seja, ter "dezenas" de antivírus instalados no PC não o deixará mais seguro. Isso apenas causará uma significativa perda de desempenho na máquina, além de gerar diversos conflitos, reduzindo também a fiabilidade e a eficácia dos programas. Pois os antivírus tentarão aceder um ficheiro ao mesmo tempo e isso irá gerar em um bloqueio do próprio sistema, causando os famosos travamentos.

Definitivamente, não é recomendado por nenhum especialista e perito em segurança possuir dois antivírus em um computador. Mesmo deixando um com protecção real-time e o outro como on-demand.

Isso vale também para anti-spywares, firewalls, anti-rootkits...?

Esta regra cabe apenas à antivírus e firewalls (que também não é recomendado instalar mais de um).

Para anti-spywares, anti-rootkits, anti-malwares esta regra não precisa ser aplicada. Você pode ter quantos anti-spywares quiser no PC. Mas, de fato, isso também acarretará em uma perda de desempenho, caso tenha dezenas de softwares deste tipo instalado.

Outros dois detalhes importantes é não manter todos os anti-spywares que estiverem instalados no arranque no computador, isso com certeza irá provocar uma demora para iniciar o sistema e poderá gerar erros. Também não deixe mais de um anti-spyware com protecção residente ligada.

A quarentena dos programas de segurança realmente funciona e é seguro?

Sim.

De um modo geral, é bem seguro e funcional mover um ficheiro encontrado pelo programa de proteção para a quarentena. Muitos não ligam para isso e logo excluem um ficheiro encontrado pelo programa, sem ao menos ver o nome do ficheiro e saber do que se trata, e isso é um erro que pode ser irreparável.

A quarentena existe principalmente porque às vezes um programa de segurança detecta falso-positivo (uma detecção errónea), classificando acidentalmente um ficheiro legítimo do sistema como vírus. Se o utilizador remove o ficheiro, e o mesmo é crucial ao sistema, a máquina se tornará

inoperante.
Assim sendo, a forma mais recomendada é enviar o item para a quarentena, claro, se você não souber distinguir se é ou não um vírus. O programa irá manter o ficheiro na quarentena, em uma pasta isolada, até que o banco de dados do produto seja actualizado, podendo assim corrigir o falso alerta, ou remover a infecção caso seja uma. Tenha em mente que isso pode levar semanas. Embora seja um procedimento que muitos consideram desagradável e insatisfatório, é a forma mais segura.

Com um antivírus apenas estou bem protegido?

Teoricamente, apenas o antivírus consegue proteger bem o computador pelo fato de possuir um banco de dados extenso, com vários tipos de vacinas para diversas infecções. Mas na prática, infelizmente, isso dificilmente ocorre. Anti-spyware é um software essencial, hoje em dia. Pois ambos possuem a mesma finalidade -- proteger seu computador. Mas ambos possuem maneiras de fazer isso completamente distintas. Um anti-spyware consegue detectar um malware que muitos antivírus não conseguem, e vice-versa... isso é fato! Coisa que ocorre também entre antivírus, um pode detectar malwares que o outro não consegue.

Resumindo, somente um antivírus **NÃO** consegue deixar seu computador devidamente protegido.

Um firewall de terceiros, ou seja, alternativo ao do Windows, é realmente necessário?

Bem, um firewall pessoal é uma das mais poderosas e eficientes medidas de protecção que você pode utilizar para proteger o seu PC. Ele permite que o utilizador possa controlar exactamente que tipo de acesso o seu computador vai aceitar, protegendo-o contra worms como o Blaster e o Sasser, e também dos novos como Conficker (também conhecido como Kido). Como todos sabem, o Windows XP SP2 e o Windows Vista vêm com o firewall do Windows ligado por default, e isto, na minha opinião, é o principal motivo pelo qual nós não temos nenhuma infecção massiva na Internet desde 2004.

Mas é aí que está: O firewall do Windows não monitora conexões e informações de saída, apenas de entrada.

Sim, é verdade. Mas pergunto: Qual é o valor de se ter um firewall controlando a comunicação que sai de um computador?

O controlo da comunicação de saída não impede que o seu computador seja infectado, e não oferece nenhuma protecção contra worms nem contra uma pessoa tentando aceder indevidamente o seu computador. Isto é um ponto pacífico. No entanto muitos fornecedores de firewall pessoal argumentam que o controlo de saída pode impedir que informação pessoal do seu computador seja enviada para um fora, e que o seu computador seja utilizado como "trampolim" para infectar outros PCs.

Este argumento tem valor na teoria, mas acho que não se confirma na prática. Para entender isso, é preciso saber que quando um malware toma conta do seu computador, ele pode fazer qualquer coisa. É relativamente trivial para este malware ultrapassar qualquer defesa que você tenha colocado, inclusive o firewall pessoal. Por exemplo, o Trojan.Srizbi, que é um cavalo de tróia que roda totalmente em modo kernel, e que por isso envia dados do utilizador para um sistema remoto ultrapassando qualquer defesa que esteja configurada no sistema -- inclusive firewalls pessoais. Não

existe como bloquear um componente malicioso do kernel de enviar dados pela rede.

Achar que um firewall pessoal vai impedir uma máquina infectada de se comunicar já é um conceito falso. Mas existe ainda um outro aspecto pior - estes firewalls ainda assumem que o utilizador vai poder diferenciar o tráfego de saída legítimo de um tráfego malicioso, o que também não é verdade. Por exemplo, um cavalo de tróia pode muito bem utilizar a API WinInet (leia-se: Internet Explorer) para enviar informações do utilizador para fora. O firewall vai enxergar o IE fazendo uma conexão externa, e das duas uma: Ou vai permitir já sem qualquer questionamento, ou vai perguntar para o utilizador se o IE pode falar com a Internet. E alguém aposta que o utilizador não vai autorizar essa conexão? Existe no entanto um cenário onde o controlo das conexões de saída é valioso, não como um recurso de segurança mas como um recurso de política corporativa. Por exemplo, uma empresa decide que nenhum dos seus PCs vai iniciar conexões para fora da sua rede sem passar pelo proxy, ou um banco configura os seus ATMs somente para falar com um conjunto específico de servidores. Se o utilizador do computador não tem privilégios administrativos, um administrador de rede pode forçar uma política obrigando os seus PCs a adoptarem a política da organização e seguirem estas regras.

Por estes motivos a Microsoft tomou a decisão de não colocar nenhum filtro de saída no firewall do Windows XP. Sem dúvida vários jornalistas iriam gostar disso, mas para o utilizador final não haveria nenhum ganho de segurança. Pelo contrário, ele somente daria uma falsa sensação de segurança. Para um utilizador caseiro, ter um firewall filtrando o tráfego de saída continua sendo inútil do ponto de vista de protecção e nada mais do que "teatro de segurança". Quando você ver um fornecedor de firewall usando este argumento, pense nisso.

Resumindo, não considero um firewall de terceiros **REALMENTE** necessário ou essencial.

Quanto aos downloads, como fazê-los com segurança?

Aqui também se encontra uma outra coisa que passa por desapercebido por muitos.

Muitos dizem: "*O download não é o perigo, apenas a execução do ficheiro descarregado!*"

Grande engano. Existem malwares/vírus que, com o download em andamento, já podem vir a infectar o sistema antes mesmo do download concluir ou de uma determinada execução do ficheiro. É o caso do famoso Trojan.Zlob.

Portanto, é recomendado sempre baixar programas pelo site do próprio desenvolvedor. E ainda assim, muito cuidado ao instalar o software (principalmente se for um freeware) pelo facto de que ele pode conter algum "software extra" para instalar, como o adware Ask.com que trata-se de uma toolbar presente em vários softwares conhecidos como: Foxit 3, COMODO Firewall, Zone Alarm, VDownloader, etc.

Porque baixar sempre do site do desenvolvedor? Apenas leia o link abaixo e tire as suas próprias conclusões:
http://www.linhadefensiva.org/forum/index.php?showtopic=100954

Uma vez uma pessoa amiga descarregou o famoso programa p2p Ares hospedado no Baixaki e recebeu um brinde: ficheiro falso contendo vírus!

Uma forma bem simples, para utilizadors não muito avançados, de descobrir se o programa que irá instalar está ok e obter mais informações de seus componentes, tais como adwares/spywares que possam estar presentes, é utilizando o **EULAlyzer (http://www.javacoolsoftware.com/eulalyzer.html)**. O EULAlyzer fará uma verificação dos acordos de licença do utilizador final (EULA) fornecendo-lhe uma lista detalhada de palavras e frases interessantes, podendo descobrir se o software que está prestes a instalar irá exibir anúncios pop-ups, recolherá informações pessoais do utilizador, usa identificadores únicos para monitorá-lo, e outras coisas.

Algumas dicas para se fazer um download com segurança:

● Use o bom senso: Tenha cuidado com solicitações para se fazer qualquer download suspeito ou algo urgentemente importante. Estas "ofertas" aparecem muitas vezes com um vistoso anúncio ou janela pop-up. Alguns chegarão como spam, alguns de forma muito inteligente, e muitas vezes com um anexo.

● Nunca baixe um ficheiro - incluindo foto e música - se você não tem a real certeza se a fonte é confiável

● Leia a descrição e recomendações sobre o software no site onde irá baixá-lo, seja do desenvolvedor ou não.

● Ao se interessar por algum programa, pesquise sobre o mesmo no Google antes de baixá-lo. Uma sugestão é digitar "nome do programa *spyware*" (sem aspas) na procura e veja o que encontrará

● Sempre faça um scan com seu antivírus ou com um verificador online (como o VirusTotal: http://www.virustotal.com/index.html) no ficheiro antes de executá-lo.

Como fiquei infectado?

Uma das perguntas mais comuns encontradas após uma limpeza de malwares da máquina é exactamente esta: "Como fiquei infectado?"

Há uma variedade de razões para isso. Um dos principais motivos pelos quais as pessoas se infectam é que estão com hábitos de navegação inseguro, ou seja, estão navegando em sites da Internet que trazem riscos para o sistema. A realidade é que a maioria das pessoas que estão infectadas com malwares são aquelas que clicam e acedem qualquer coisa. Não se preocupam com a segurança, saem clicando em determinado link porque é um link que você estava procurando ou é algo que chame a sua atenção. Lembrem-se que a real intenção dos criadores de pragas é focar a atenção do utilizador aonde está algo potencialmente perigoso (obviamente, muito bem camuflado em algo "externamente" seguro), fazendo-o de isca.

Outros motivos pelos quais as pessoas possam se infectar são:

● Através de dispositivos removíveis infectados: Pen drive, HD externo, celular, cartão de memória, MP3, MP4, etc;
● Sistema ou programas desactualizados: Actualizar o Windows e ter sempre as últimas versões dos programas instalados no PC é algo que reduz e MUITO você ser vítima de malwares;

● Instalando cracks e keygens;
● Aceder a sites pornográficos;
● Abrir um anexo infectado de um e-mail;
● Etc...

Programas P2P são seguros?

Não.
Apesar de ser um tipo de programa muito usado pela grande maioria dos utilizadores, o uso de programas partilhadores é sempre um risco, porque você nunca terá a real certeza se o download que fará é exactamente o ficheiro que pretende. Nem sempre é aquilo que aparece na pesquisa. Importante também é saber que muitos programas p2p também são empacotados com softwares indesejados (spyware/adware). Para descobrir quais são os p2p mais seguros para a utilização, dê visite este site: http://malwareremoval.com/p2pindex.php.

OBS: Faltou apenas o DreaMule que também é seguro, só que como é brasileiro não foi incluído na lista. E sinceramente, o DreaMule, na minha opinião, é o p2p mais seguro da actualidade. Além de possuir um detector de ficheiros falsos, possui servidores seguros e já vêm com uma pré-configuração bem segura.

Uma dica valiosa para utilizadores de partilhadores p2p, é utilizar o **PeerGuardian** (http://phoenixlabs.org/pg2/) que analisa o tráfego de entrada e saída do PC podendo bloquear algum endereço IP malicioso que esteja em seu banco de dados. O software não consome quase nada de memória e não prejudica seus downloads e uploads pelo compartilhador.

Posso apanhar um vírus quando leio os meus e-mails?

Apenas ler o e-mail não irá infectar seu computador.

Somente se o e-mail vier com um anexo, e nele conter um vírus e/ou malware e você abrir/executar este ficheiro anexado infectado, aí sim, seu PC será infectado.

Formatei meu computador e o vírus não saiu.

De duas uma: Ou você não formatou correctamente o seu disco duro, apagando todo o conteúdo do disco. Ou quando fez um backup dos seus documentos ou ficheiros importantes, salvou o vírus junto. Do contrário, impossível!

O que ocorre na maioria das vezes é exactamente o que foi dito acima, a pessoa faz backups de seus documentos e, despercebidamente, salva o vírus junto com o backup. Geralmente em pen drives ou CD/DVD. E logo após a formatação, insere a média removível no drive e passa tudo novamente para o computador, havendo assim uma re-infecção.

Um vírus ou malware pode danificar alguma parte física (hardware) da máquina?

Não.

Vírus são softwares, portanto, não podem afectar o hardware. O vírus pode corromper os dados do computador, incluindo os drivers que são utilizados para permitir que seus dispositivos de hardware

se comuniquem com o computador. Se isto vier a ocorrer, pode impedir que o seu dispositivo fique sem comunicação com o sistema, mas de maneira alguma o afectará fisicamente.

Existiu um vírus, bem antigo, chamado Chernobyl (conhecido também como CIH ou Spacefiller) que apagava o BIOS da placa-mãe. Na época, muitos técnicos e profissionais de informática diagnosticavam o PC e davam a placa-mãe como morta, o que na verdade era um grande equívoco por parte dos mesmos. Mais informações sobre o CIH em: http://pt.wikipedia.org/wiki/Win32/CIH.

Empresas antivírus criam vírus para aumentar os lucros. Verdade ou mentira?

Este é um argumento que existe na mente de muitos clientes de antivírus. Pois, às vezes, somente determinado antivírus remove determinada praga, e por isso, acham, que o malware foi criado pela empresa apenas para a mesma sair lucrando com tudo disso. Mas não é verdade.

1) Criar um vírus, que não é difícil (para quem é familiarizado com computadores e programação), não ajudaria na prevenção ou detecção do mesmo -- que é finalidade de uma empresa antivírus;
2) Uma empresa antivírus não poderia se proteger contra o vírus antes dele ter sido "disponibilizado" sem levantar suspeitas. Portanto, seria infectar o seu próprio produto causando insatisfação dos clientes;
3) O código que torna-se um vírus é analisado, reanalisado e comentado por dezenas de peritos de segurança. Analisando o código eles poderão traçar suas origens que serão voltadas à empresa antivírus;
4) A empresa antivírus seria responsabilizada pelo ato maléfico e ganancioso, de uma certa forma, por ter criado o vírus para lucrar com isso. Com isso, a empresa ficaria mal com os clientes que obviamente perderiam a confiança no mesmo, além do mais, acarretaria em um grande número de acções judiciais contra a empresa.

O que devo fazer se acho/tenho certeza que meu computador está infectado?

Muitas pessoas em um momento de susto, aflição ou desespero (e com razão) tendo seu computador infectado, acabam se precipitando e fazendo algo indevido, e isso pode vir a prejudicar mais ainda a situação do sistema. Pois, dependendo do vírus, quanto mais mexe no computador, mais o vírus o deixará instável.

Algumas medidas são recomendadas se você está com suspeitas, ou tem certeza, de que seu micro esteja infectado.

● De forma alguma utilize o computador para aceder internet banking (contas bancárias online), para fazer alguma compra online ou aceder algo que seja necessário inserir informações pessoais, como: Orkut, MSN, Facebook, MySpace, Skype, conta(s) de e-mail(s), jogos, internet banking, etc;

● Desconecte o computador da Internet e, caso possua, desconecte-o da rede também;

● Por enquanto, não faça backups de seus ficheiros, pois podem estar infectados -- dependendo do vírus;

● De preferência, caso esteja possibilitado a fazer, reinicie o computador em Modo de Segurança. Assim o vírus não ficará em actividade poupando-lhe dor de cabeça;

● Actualize e faça imediatamente uma varredura (scan) com seu antivírus, em modo seguro mesmo que é até melhor;

● Procure por ajuda profissional em fóruns para que a resolução de seu problema seja mais segura e rápida.

São medidas simples mas que podem lhe ajudar bastante e, principalmente, proteger seus dados pessoais.

Engenharia Social.

O termo é utilizado para descrever um método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do utilizador, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.

Quais são os riscos ao se usar o navegador web?

Existem diversos riscos envolvidos na utilização de um browser. Dentre eles, podem-se citar.

● Execução de JavaScripts maliciosos;
● Execução de controlos ActiveX maliciosos;
● Obtenção e execução de programas perigosos em sites mal intencionados ou falsos;
● Acesso a sites falsos, se fazendo passar por instituições bancárias ou de comércio electrónico;
● Realizações de transacções bancárias ou comerciais via web, sem qualquer mecanismo de segurança.

Nos dois primeiros casos o browser executa os programas automaticamente, ou seja, sem a interferência do utilizador.

Ficheiros de imagens, vídeos e músicas também podem ser infectados?

Sim. Normalmente.

Os ficheiros podem ser infectados em si, e podem ser alterados por um código malicioso. Neste caso há dois métodos:

Infecção directa: Este tipo de infecção ocorre quando o cavalo de tróia contamina um ficheiro de média ou imagem legítimo.

Ficheiros de vídeo e áudio como: MP3, .WMA, .WMV, .AVI, .MPEG, são na grande maioria das vezes infectadas pelo Trojan-Downloader.WMA.GetCodec. Este cavalo de tróia possui diversas variantes, as mais conhecidas são: Trojan.ASF.Hijacker.gen, TROJ_MEDPINCH.A, TSPY_LDPINCH.ASG. Este cavalo de tróia é muito perigoso porque além de possuir um alto nível de infecção, ele geralmente descarrega trojans vundos e backdoors para o computador do utilizador. Comummente é apanhado através de redes p2p e quase sempre resulta em perda total de seus ficheiros -- sem oportunidade de recuperação.

Já os ficheiros de imagens, são na grande maioria das vezes infectados por worms. O pioneiro, mais conhecido e o comummente encontrado em ficheiros de imagens, independente do tipo (se é .Bmp, .Jpg, .Gif), é o W32.Perrun. Porém, é difícil encontrarmos um ficheiro de imagem infectado hoje em dia. Ocorre mais com os ficheiros de mídia.

Infecção obscura: Neste tipo de infecção é utilizada uma técnica conhecida como *Malicious Double Extension*.

A artimanha usada pelos criadores neste tipo de técnica é bem simples de entender. O cracker define uma dupla extensão no ficheiro que é ocultada da vista do utilizador, onde somente se a opção de "*Ocultar as extensões dos tipos de ficheiros conhecidos*" (em Opções de pastas) estiver desmarcada é que o utilizador enxergará a segunda extensão maliciosa adicionada no ficheiro.

Por exemplo:

Se você baixa um ficheiro de música (**Música.mp3**) para o computador, e este ficheiro foi alterado por alguma pessoa mal intencionada que utilizou a técnica de extensão dupla dita acima, a real extensão deste ficheiro de mídia não será .MP3, mas sim:

Música.MP3**.bat**
Música.MP3**.exe**
Música.MP3**.vbs**
Música.MP3**.reg**

E por aí vai...

Ou seja, você foi enganado pensando ser um ficheiro de mídia sendo que era um executável malicioso. Esta técnica pode ser utilizada em qualquer tipo de ficheiro, seja de imagem, de texto, de música, de vídeo e etc.

O malware mais conhecido utilizado nesta técnica é o famoso worm "*I Love You*" (também conhecido como "*Love Bug*" ou "*Loveletter*"). Informações sobre o mesmo aqui.

No entanto, felizmente, os antivírus detectam estes dois tipos de infecções (técnicas) facilmente. É muito difícil um antivírus não detectar alguma das técnicas.

Como prevenir infecções via médias removíveis?

Este é o meio mais comum de se pegar vírus actualmente. De 100% dos utilizadors de hoje, 90% sofrem infecções via dispositivos removíveis, pen drive, HD externo, celular, cartão de memória e etc.

Mas há algumas maneiras bem eficazes de evitar este tipo de infecção.

Desactivar o recurso autorun (execução automática): Este é um dos passos mais eficazes para evitar esta infecção. Para desactivar este recurso tem vários modos, vou colocar os mais rápidos e eficazes.

A Microsoft lançou uma actualização que serve exactamente para desactivar o autorun do Windows. Para baixá-las, acedam ao link abaixo do seu respectivo sistema operacional:

Windows 2000: http://www.microsoft.com/downloads/details.aspx?FamilyID=3c6039f1-d84d-4294-8457-35aa8b4dcab8&displaylang=en

Windows XP Service Pack 2 e 3:
http://www.microsoft.com/downloads/details.aspx?FamilyID=c7dbcde3-7814-47c5-849e-e64ecfb35d74&displaylang=en

Windows Server 2003: http://www.microsoft.com/downloads/details.aspx?FamilyID=32b845ac-7681-468c-812b-2dcebdae9b40&displaylang=en

Existe também uma ferramenta chamada **AutoPlayConfig** que desactiva o recurso.

Também há meios manuais:

Windows XP: Vá em Iniciar -> Executar, digite **gpedit.msc** e dê um OK. No politicas, caminhe em Configuração do computador -> Modelos Administrativos -> Sistema.

Ao lado direito do painel, dê um duplo clique no item **Desactivar AutoExecutar**. Marque a opção ***Activado*** e mais abaixo coloque "*Todas as unidades*" -> OK.

Windows Seven e Vista: Clique em Start e na caixa de pesquisa digite **gpedit.msc** para abrir o group policy (politicas de grupo).

Expanda as chaves Administrative Templates -> Windows Components -> Autoplay Policies. Ao lado direito do painel, dê um duplo clique em "**Turn off AutoPlay**". Marque a opção **Enable** e em baixo marque a opção "*All drives*" -> OK.

Instalar softwares de protecções para médias removíveis: Existem alguns softwares muito bons que podem ser úteis na prevenção contra esta infecção. Os softwares são o **USB Firewall**, **USB WriteProtector** e **USBVaccine**. O primeiro programa deve ser instalado no próprio computador -- adianto que ele usa pouquíssimo consumo de memória e roda em background. Já o segundo programa é para ser instalado no dispositivo removível -- evitando contaminações no mesmo também. E o terceiro irá vacinar o dispositivo e o computador prevenindo-os contra infecções futuras.

Médias de terceiros: Tenha muito cuidado ao inserir uma média removível de terceiros em sua máquina, ou seja, de algum amigo, parente, namorada(o), etc. Procure ao máximo evitar conexões de médias de terceiros em seu PC.

Passar um scan: É altamente recomendado scanear com seu antivírus a mídia antes de abrí-lo(a). O scan pode ser feito com outras ferramentas específicas para isso também tais como: **UsbFix**, **PenClean**, **Flash_Disinfector**, **Malwarebytes' Anti-Malware**, entre outros.

Windows Explorer: Mesmo que o autorun esteja desactivado, é recomendado que ao abrir um dispositivo removível, aceda *Meu Computador* e ao ver a unidade removível listada junto com as outras, clique com o botão direito do mouse sobre ela, e escolha **Explorar**. Dessa maneira, caso o pen drive (ou qualquer outro dispositivo) esteja infectado, o *autorun.inf* presente na unidade não será executado, e consequentemente, o malware não irá infectar seu computador.

Como os vírus podem afectar os ficheiros?

Os vírus têm capacidade de contaminar qualquer tipo de ficheiro, porém, geralmente infectam ficheiros executáveis ou ficheiros de dados. Eis abaixo algumas tarefas exercidas pelos vírus ao infectar um ficheiro:

Aumentar o tamanho dos ficheiros: Ao infectar ficheiros, os vírus geralmente irão aumentar o tamanho do ficheiro, no entanto, com estas mudanças mais sofisticados os vírus podem ficar escondidos.

Apagar ficheiros quando o mesmo é executado: Como a maioria dos ficheiros são carregados na memória, uma vez que o programa está na memória o vírus pode apagar o ficheiro usado para executar o vírus.

Corromper ficheiros aleatoriamente: Alguns vírus destrutivos não são projectados para destruir dados aleatórios, mas sim aleatoriamente apagar ou corromper ficheiros.

Converter ficheiros: Os vírus podem usar um ficheiro separado para executar o programa e renomear o original para um outro de modo que a extensão "*. exe" é executada antes do "*.COM".

Reinicie ao executar: Inúmeros vírus podem fazer com que o computador reinicie automaticamente quando o ficheiro infectado é executado. O ficheiro é aleatório.

Barra de pesquisa (ou Motores de Procura) podem nos levar a algum malware?

Sim.

As barras de pesquisas não são fundamentalmente concebidas para encontrar sites confiáveis. Como resultado, muitos sites maliciosos frequentemente aparecem na pesquisa. Felizmente, há algumas medidas que você pode adoptar para reduzir tal risco.

Primeiro de tudo: Utilize um respeitável motor de pesquisa. Recentemente, tem havido uma proliferação de sites de pesquisas maliciosos, projectados para atrair os utilizadors para sites perigosos. Certifique-se de usar um motor de procura bem conhecido e seguro, como Google, SiteAdvisor ou Yahoo. Reputados motores de procura fazem filtragens para remover sites maliciosos, apesar de não poderem acompanhar o mundial "exército de bandidos internautas" de hoje em dia.

Existem também vários plug-ins que exibem informações de segurança junto dos resultados de pesquisa, como: **McAfee SiteAdvisor** (http://www.siteadvisor.com/), **Finjan** (http://securebrowsing.finjan.com/), **AVG Link Scanner** (http://linkscanner.avg.com/) e **WOT** (https://addons.mozilla.org/pt-PT/firefox/addon/3456) (somente para o Firefox), que são os plug-ins mais conceituados da actualidade.

Porém, acima de tudo: Pense antes de clicar.

Afinal, máquinas virtuais são realmente seguras? Posso executar qualquer tipo de coisa, incluindo vírus e malwares?

Primeiramente, virtualização não traz nenhuma protecção adicional ao software executando à máquina hóspede, ou seja, à máquina host (real). Se uma ferramenta maliciosa pode explorar um sistema real, esta mesma ferramenta pode ser utilizada para explorar uma VM (virtual machine, máquina virtual). Inclusive, já houve casos em que o PC real foi contaminado através de uma VM. Agora, virtualização pode ser utilizada como uma forma de isolamento, ou seja, separá-la da máquina real. Mas isso não quer dizer que um atacante virtual não possa comprometer este isolamento. Não é trivial, mas, infelizmente, é possível. Porém, é o melhor meio de se testar uma praga virtual.

O que devemos fazer com estas preocupações?

● Tenha sempre a última actualização da VM, mantendo sempre actualizada com os patches lançados pela empresa responsável pelo software;

● Mantenha a VM em um grupo de trabalho diferente do PC real;

● Desactive a partilha de ficheiros no PC real e na VM;

● Deixe o firewall activado no PC real e na VM;

● Não forneça informações pessoais e confidenciais na VM;

● Procure deixar a VM configurada como bridge ao invés de NAT que é a padrão. Pois em modo bridge a VM fará apenas a comunicação com sua placa de rede do PC real para aceder à Internet. Já no modo NAT a VM terá que se comunicar directamente com seu PC real e partilhar do mesmo IP para aceder à Internet podendo haver uma contaminação no PC real.

Estes são os conceitos necessários para usar a VM em testes com vírus e malwares.

OBS: Usar o nome de utilizador e senha do provedor de Internet na VM não tem perigo algum.

O que é e como me proteger de crimewares?

Crimewares não são malwares propriamente dito. Crimeware trata-se de um nome usado para descrever todos os malwares que possuem um objectivo comum: Obtenção de dinheiro ou informação confidencial. Os bots, keyloggers, trojans bankers, adwares, spywares, spams, phishings, dialers, por exemplo, são malwares considerados crimewares.

MPack é um dos instrumentos mais utilizados nesta técnica. Escrito por um grupo de programadores russos, MPack é um kit malware baseado em código PHP que filtram em servidores web comprometidos. Quando o utilizador navega para um servidor MPack'ed seus navegadores são afectados com um conjunto de exploits que tentam instalar bots, keyloggers, rootkits e outros malwares nas máquinas das vítimas.

Estes tipos de ferramentas são uma ameaça significativa para todos os internautas, pois representam um importante vector pelo qual o malware se propaga hoje em dia.

As melhores maneiras de se proteger contra crimewares são:

● Utilizando um browser seguro. Actualmente recomenda-se **Mozilla Firefox**, **Opera** e **Google Chrome** (considerado o mais seguro pelos testes da Acid3 (http://pt.wikipedia.org/wiki/Acid3));

● Mantendo o navegador devidamente actualizado, com todas as correcções e patches necessários;

● Mantendo softwares de protecção antivírus, anti-spyware e firewall actualizados e activos;

● Não baixar controlos ActiveX e outros plug-ins de sites desconhecidos, e ter cuidado até mesmo ao baixar de sites conhecidos;

● E o principal de tudo, tomar cuidado por onde navega.

Porquê que tu colocaste tão pouco de Linux / Unix no livro?

Uma excelente questão. Quem leu esse livro, do principio ao fim, deve ter percebido que dei apenas uma breve introdução sobre o Linux e sobre o Windows, e apesar de a maioria dos exemplos de programas ser para Windows não me peguei realmente a nenhum sistema operacional. Veja o seguinte: parece uma contradição, disse bem lá no início que o Linux é melhor que o Windows, certo? Mas por quê citei programas para Windows? Pressupõe-se que uma pessoa que tenha o Linux instalado em casa já tenha um conhecimento melhor do que uma que possui Windows.

Então será muito mais fácil para ela ler as secções e procurar um programa similar ao que foi usado como exemplo. Nos sites citados (inclusive no fim deste livro) existem excelentes ferramentas para Linux e Unix (entre outros sistemas, como Macintosh) que podem ser experimentadas sem maiores problemas. Resumindo: esse não é um livro sobre sistemas operacionais, é um livro sobre a segurança como um aspecto universal. Desejo que um utilizador de BeOS por exemplo possa ler e mesmo que seu sistema não seja citado nem de longe, aproveite muito dos conhecimentos aqui citados.

Tu ajudas-me a invadir o sistema "x" ou "y"?

Por favor, não me façam esse tipo de pergunta. Não porquê eu me ache o sabichão, coisa que sei que não sou e nunca serei pois sou apenas mais um a aprender. Como disse no prefácio, informática, internet e segurança é a minha paixão. Aprendi a ler e escrever num MSX. Comecei a conhecer sobre pascal ali. Confesso que quando era mais novo realmente fiz muitas "besteiras" com o computador e só não me arrependo delas pois elas me trouxeram conhecimento e me fizeram amadurecer muito.

Bem, como dizem, águas passadas não movem moinhos. Resumindo: não invado computadores, gosto apenas de divulgar o conhecimento que eu consegui obter e não quero causar prejuízos a ninguém. Tiro qualquer dúvida com o maior prazer, mas não me peçam fazer nada, por favor.

Aprenda mais sobre o assunto

Sites de segurança versus sites de hackers

Para utilizar a Internet como um excelente veículo de aprendizado, você terá que ter algumas coisas em mente. A questão dos sites de segurança, por exemplo. Para saber novidades você não precisa visitar aquelas páginas escuras horríveis, com programas como o Winnuke para download, caveiras para todo lado e o texto "Invasão por IP". O interesse real está nos sites empresariais de segurança. Esses sim têm um conteúdo excelente, desde ferramentas, novos bugs descobertos e ótimos xploits. Sites como o *Technotronic (www.technotronic.com)* ou o *Security-focus* (www.security-focus.com) são apenas alguns dos incríveis sites que existem por aí. Visite-o periodicamente e esteja sempre procurando por novos scanners, ferramentas, firewalls, enfim, tome gosto pela coisa. As recompensas à longo prazo serão grandes: evitar dores de cabeça.

A importância do profissional de segurança

A menos que você seja um administrador que fica sentado o dia inteiro sem fazer absolutamente nada, não tenha medo de sugerir aos seus superiores a contratação de um especialista em segurança. Eles não irão lhe despedir, pelo contrário, verão que você está realmente interessado no bem da empresa. Explique que a área da segurança é muito grande e que todos os dias alguém deve visitar os sites especializados e procurar por actualizações e correcções de bugs. E um especialista em segurança não é aquele que é PhD em ciências da computação. A informática muda muito rápido e as pessoas que fazem curso superior nessa área têm tanta coisa o que estudar que muitas vezes a segurança não é aprendida a fundo. Prefira os profissionais que fizeram cursos especiais e certificados internacionalmente (como cursos oficiais da ou E-council, Microsoft, da Conectiva ou da Cisco Systems).

Pense seriamente em contratar um "expert". Sendo uma pessoa que gosta do que faz, pode ter certeza que seu sistema estará bem seguro. Não seja levado por esse pensamento de que é perigoso possuir um "hacker" a trabalhar na empresa. Isso é irrelevante, pois ele é um funcionário como qualquer outro, com direito a promoções e a ser demitido. Faça um contrato com ele em que ele se responsabilizará se algum acto ilícito acontecer por sua causa. É constrangedor, mas elimina o medo que os patrões têm.

Sites com matérias sobre o assunto

A grande maioria dos sites é em inglês. Afie bem o seu *"vocabulary"* pois são as melhores paginas

web do mundo.
WEBSITES

Apendice I

Glossário

802.11 Refere-se a um conjunto de especificações desenvolvidas pelo IEEE para tecnologias de redes sem fio.

AC - consulte Autoridade certificadora.

ACL (Acess Control List: lista de controlo de acesso) – Tipicamente compreendidas por uma lista das mais importantes, uma lista de recursos e uma lista de permissões.

ACSE (Association Control Service Element) (Associação de Controlo de Elementos de service) – O metodo utilizado em OSI para estabelecer uma chamada entre dois aplicativos. Verifica as identidades e contextos das entidades de aplicativo e pode pedir uma verificação de autenticação de segurança.

Adjacência – Um relacionamento formado entre roteadores vizinhos selecionados com o objectivo de trocar informações de roteiro. Nem todos os pares de roteadores vizinhos tornam-se adjacentes.

ADMD (Administration Management Domain) (domínio de gerenciamento de adminstração) – Um transportador de serviço público X.400 Message Handling System.

ADSL - do Inglês ***A**symmetric **D**igital **S**ubscriber **L**ine*. Sistema que permite a utilização das linhas telefônicas para transmissão de dados em velocidades maiores que as permitidas por um *modem* convencional.

Adware - do Inglês ***Ad**vertising Soft**ware***. *Software* especificamente projetcado para apresentar propagandas. Constitui uma forma de retorno financeiro para aqueles que desenvolvem *software* livre ou prestam serviços gratuitos. Pode ser considerado um tipo de *spyware*, caso monitore os hábitos do utilizador, por exemplo, durante a navegação na Internet para direcionar as propagandas que serão apresentadas

Agente – no modelo cliente-servidor, a parte do sistema que realiza a preparação e troca de informações em nome de um aplicativo cliente ou servidor. Ver NMS. DUA, MTA.

Algoritmo assimétrico – Um algoritmo de criptografia que exige duas chaves diferentes para criptografia e decodificação. Estas chaves são comummente chamadas como chaves pública e privada. Algoritmos assimétricos são mais lentos que algoritmos simétricos.

Algoritmo simétrico – Um algoritmo onde a mesma chave pode ser usada para criptografar e decodificar.

ANSI (American National Standard Institute) (Instituto Nacional de Padronização Americano) – A secção de padronização dos Estados Unidos. ANSI é um membro da International Organization for Standardization (ISO).

Antivírus - programa ou *software* especificamente desenvolvido para detectar, anular e eliminar de um computador vírus e outros tipos de código malicioso.

AOW (Asia and Oceania workshop) (Seminário da Ásia e Oceânia) – Um dos três OSI Implementors Workshops regionais, equivale a OIW e EWOS.

AP - do Inglês ***A**ccess **P**oint*. Dispositivo que actua como ponte entre uma rede sem fio e uma rede tradicional.

API (Aplication Program Interface) (Interface de Programa Aplicativo) – Um conjunto de convenções de chamada definindo como um serviço é chamado através de um pacote de softwares.

Applet assinado – Um applet que é digitalmente assinado pela fonte que o fornece. Applets assinados têm sua integridade protegida e não podem ser falsificados enquanto em trânsito do servidor para o browser.

Archie – Uma ferramenta de procura para encontrar ficheiros e programas localizados em servidores FTP. O sistema Archie é composto de vários servidores Archie localizados nos Estados Unidos e no mundo.

Também, tem uma ferramenta de Internet que informa qual(is) site(s) da publicamente acessível(is) contém um ficheiro em particular. O ficheiro então precisa de ser obtido com o uso de FTP. Archie foi desenvolvido na Universidade McGill em Montreal.

ARP (Address Resolution Protocol) (Protocolo de resolução de endereço) – O protocolo Internet, utilizado para mapear dinamicamente endereços Internet para endereços físicos (hardware) em redes de área local. Limitando a redes que suportam hardware de transmissão.

ARPA (Advanced Research Projects Agency) (Agência de Projectos de Pesquisa Avançada) – Agora chamada de DARPA, a agência do governo dos USA que fundou a ARPANET.

ARPANET - Um pacote de transferência de rede desenvolvido nos finais dos anos 1970. ARPNET foi descompactibilizada em Junho de 1990.

Artefacto - de forma geral, artefacto é qualquer informação deixada por um invasor num sistema comprometido. Pode ser um programa ou *script* utilizado pelo invasor em actividades maliciosas, um conjunto de ferramentas usadas pelo invasor, *logs* ou ficheiros deixados num sistema comprometido, a saída gerada pelas ferramentas do invasor, etc.

Assinatura digital – um método para verificar qual mensagem originou-se de um principal e se não foi alterada em transito. A assinatura digital é tipicamente feita pela criptografia de um resumo da mensagem com a chave privada da parte assinando.

Atacante - pessoa responsável pela realização de um ataque. Consulte também Ataque.

Ataque - tentativa, bem ou mal sucedida, de acesso ou uso não autorizado a um programa ou computador. Também são considerados ataques as tentativas de recusa de serviço.

Ataque dicionário – Uma forma de ataque onde um atacante usa uma grande quantidade de combinações parecidas para descobrir uma segredo. Por exemplo, um atacante pode escolher um milhão de senhas usadas e tentá-las todas, até que a senha seja determinada.
Autoridade certificadora - entidade responsável por emitir certificados digitais. Estes certificados podem ser emitidos para diversos tipos de entidades, tais como: pessoa, computador, departamento de uma instituição, instituição, etc.

BackBone (a parte mais importante / espinha dorsal) – O principal mecanismo de conectividade de um sistema hierárquico distribuído. Todos os sistemas que têm conectividade com um sistema intermediário no backbone, têm garantia de conectividade entre si.
Isto não evita que os sistemas ajustem arranjos privados uns com outros para trespassar o backbone por razões de custo, desempenho ou segurança.

Backdoor - programa que permite a um invasor retornar ao computador comprometido. Normalmente este programa é colocado de forma a não ser notado.

Banda - consulte Largura de banda.

Bandwidth - consulte Largura de banda.

Bluetooth - termo que se refere a uma tecnologia de rádio-freqüência (RF) de baixo alcance, utilizada para a transmissão de voz e dados.
Boato - *e-mail* que possui conteúdo alarmante ou falso e que, geralmente, tem como remetente ou aponta como autora da mensagem alguma instituição, empresa importante ou órgão governamental. Através de uma leitura minuciosa deste tipo de *e-mail*, normalmente, é possível identificar no seu conteúdo mensagens sem lógica e muitas vezes sem sentido.

Bot - programa que, além de incluir funcionalidades de *worms*, sendo capaz de se propagar automaticamente através da exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados num computador, dispõe de mecanismos de comunicação com o invasor, permitindo que o programa seja controlado remotamente. O invasor, ao comunicar-se com o *bot*, pode orientá-lo a desferir ataques contra outros computadores, furtar dados, enviar *spam*, etc.

Botnets - redes formadas por diversos computadores infectados com *bots*. Podem ser usadas em actividades de recusa de serviço, esquemas de fraude, envio de *spam*, etc.

Cable modem - *modem* projectado para operar sobre linhas de Televisão a cabo.

Cavalo de tróia - programa, normalmente recebido como um "presente" (por exemplo, cartão virtual, álbum de fotos, protector de ecrã, jogo, etc), que além de executar funções para as quais foi aparentemente projectado, também executa outras funções normalmente maldosos e sem o conhecimento do utilizador.

Certificado digital - ficheiro eletrónico, assinado digitalmente, que contém dados de uma pessoa ou instituição, utilizados para comprovar sua identidade. Consulte também Assinatura digital.

Código maldoso - termo genérico que se refere a todos os tipos de programa que executam acções maldosas num computador. Exemplos de códigos maldosos são os vírus, *worms*, *bots*, cavalos de tróia, *rootkits*, etc.

Comércio electrónico - também chamado de *e-commerce*, é qualquer forma de transação comercial onde as partes interagem eletronicamente. Conjunto de técnicas e tecnologias computacionais utilizadas para facilitar e executar transacções comerciais de bens e serviços através da Internet.

Comprometimento - consulte Invasão.

Conexão segura - conexão que utiliza um protocolo de criptografia para a transmissão de dados, como por exemplo, HTTPS ou SSH.

Correcção de segurança - correcção especificamente desenvolvida para eliminar falhas de segurança num *software* ou sistema operacional.

Criptografia - ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas. É utilizada, dentre outras finalidades, para: autenticar a identidade de utilizadores; autenticar transacções bancárias; proteger a integridade de transferências eletrónicas de fundos, e proteger o sigilo de comunicações pessoais e comerciais.

DdoS - do Inglês ***D**istributed **D**enial **o**f **S**ervice*. Ataque de recusa de serviço distribuído, ou seja, **um conjunto** de computadores é utilizado para tirar de operação um ou mais serviços ou computadores conectados à Internet. Consulte Recusa de serviço.

DNS - do Inglês ***D**omain **N**ame **S**ystem*. Serviço que traduz nomes de domínios para endereços IP e vice-versa.

DoS - do Inglês ***D**enial **o**f **S**ervice*. Consulte Recusa de serviço.

E-commerce - consulte Comércio eletrónico.

Endereço IP - este endereço é um número único para cada computador conectado à Internet, composto por uma sequência de 4 números que variam de 0 até 255, separados por ".". Por exemplo: 192.168.34.25.

Engenharia social - método de ataque onde uma pessoa faz uso da persuasão, muitas vezes aproveitando-se da ingenuidade ou confiança do utilizador, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.

Exploit - programa ou parte de um programa malicioso projectado para explorar uma vulnerabilidade existente num *software* de computador.

Falsa identidade - acto onde o falsificador atribui-se identidade ilegítima, podendo se fazer passar por outra pessoa, com objectivo de obter vantagens indevidas, como por exemplo, obter crédito, furtar dinheiro de contas bancárias das vítimas, utilizar cartões de crédito de terceiros, entre outras.

Ficheiro de Assinatura – Um rodapé acrescentado no fundo de mensagem de e-mail.

Firewall - dispositivo constituído pela combinação de *software* e *hardware*, utilizado para dividir e controlar o acesso entre redes de computadores.

***Firewall* pessoal** - *software* ou programa utilizado para proteger **um** computador contra acessos não autorizados vindos da Internet. É um tipo específico de *firewall*.

GnuPG - conjunto de programas gratuitos e de código aberto, que implementa criptografia de chave única, de chaves pública e privada e assinatura digital.

GPG - consulte GnuPG.

Harvesting - técnica utilizada por *spammers*, que consiste em varrer páginas *Web*, ficheiros de listas de discussão, entre outros, a procura de endereços de *e-mail*.

Hoax - consulte Boato.

HTML - do Inglês ***H**yper**T**ext **M**arkup **L**anguage*. Linguagem universal utilizada na elaboração de páginas na Internet.

HTTP - do Inglês ***H**yper**T**ext **T**ransfer **P**rotocol*. Protocolo utilizado para transferir páginas *Web* entre um servidor e um cliente (por exemplo, o *browser*).

HTTPS - quando utilizado como parte de uma URL, especifica a utilização de HTTP com algum mecanismo de segurança, normalmente o SSL.

Identity theft - consulte Falsa identidade.

IDS - do Inglês ***I**ntrusion **D**etection **S**ystem*. Programa, ou um conjunto de programas, cuja função é detectar actividades maliciosas ou anómalas.

IEEE - acrônimo para *Institute of Electrical and Electronics Engineers*, uma organização composta por engenheiros, cientistas e estudantes, que desenvolvem padrões para a indústria de computadores e electro-eletrónicos.

Invasão - ataque bem sucedido que resulte no acesso, manipulação ou destruição de informações num computador.

Invasor - pessoa responsável pela realização de uma invasão (comprometimento). Consulte também Invasão.

InterNIC - (Internet Network Information Center) é uma organização do Departamento de Comércio do Governo norte-americano (U.S. Department of Commerce), responsável pelo registo de domínios utilizados na Internet.

IP - consulte Endereço IP.

Keylogger - Programa capaz de capturar e armazenar as teclas digitadas pelo utilizador no teclado de um computador. Normalmente, a activação do *keylogger* é condicionada a uma acção prévia do utilizador, como por exemplo, após o acesso a um *site* de comércio eletrónico ou *Internet Banking*, para a captura de senhas bancárias ou números de cartões de crédito.

Largura de banda - quantidade de dados que podem ser transmitidos num canal de comunicação, num determinado intervalo de tempo.

Log - registo de actividades geradas por programas de computador. No caso de *logs* relativos a incidentes de segurança, eles normalmente são gerados por *firewalls* ou por IDSs.

Malware - do Inglês ***Mal****icious soft****ware*** (*software* malicioso). Consulte Código maldoso.

MMS - do Inglês ***M****ultimedia* ***M****essage* ***S****ervice*. Tecnologia amplamente utilizada em telefonia móvel para a transmissão de dados, como texto, imagem, áudio e vídeo.

Modem - dispositivo que permite o envio e recebimento de dados utilizando as linhas telefónicas.

Número IP - consulte Endereço IP.

Opt-in - regra de envio de mensagens que define que é proibido mandar *e-mails* comerciais/*spam*, a menos que exista uma concordância prévia por parte do destinatário. Consulte também *Soft opt-in*.

Opt-out - regra de envio de mensagens que define que é permitido mandar *e-mails* comerciais/*spam*, mas deve-se fornecer um mecanismo para que o destinatário possa parar de receber as mensagens.

P2P - acrônimo para *peer-to-peer*. Arquitectura de rede onde cada computador tem funcionalidades e responsabilidades equivalentes. Difere da arquitetura cliente/servidor, onde alguns dispositivos são dedicados a servir outros. Este tipo de rede é normalmente implementada via *softwares* P2P, que permitem conectar o computador de um utilizador ao de outro para partilhar ou transferir dados, como MP3, jogos, vídeos, imagens, etc.

Password - consulte Senha.

Patch - consulte Correcção de segurança.

PGP - do Inglês ***P****retty* ***G****ood* ***P****rivacy*. Programa que implementa criptografia de chave única, de chaves pública e privada e assinatura digital. Possui versões comerciais e gratuitas. Consulte também GnuPG.

Phishing - também conhecido como *phishing scam* ou *phishing/scam*. Mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou *site* popular, e que procura induzir utilizadores ao fornecimento de dados pessoais e financeiros. Inicialmente, este tipo de mensagem induzia o utilizador a aceder a páginas fraudulentas na Internet. Actualmente, o termo também se refere à mensagem que induz o utilizador à instalação de códigos maldosos, além da mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros.

Porta dos fundos - consulte *Backdoor*.

Proxy - servidor que actua como intermediário entre um cliente e outro servidor. Normalmente é utilizado em empresas para aumentar a performance de acesso a determinados serviços ou permitir que mais de uma máquina se conecte à Internet. *Proxies* mal configurados podem ser abusados por atacantes e utilizados como uma forma de tornar anónimas algumas acções na Internet, como atacar outras redes ou enviar *spam*.

Recusa de serviço - Actividade maliciosa onde o atacante utiliza **um** computador para tirar de operação um serviço ou computador conectado à Internet.

Rede sem fio - Rede que permite a conexão entre computadores e outros dispositivos através da transmissão e recepção de sinais de rádio.

Rootkit - Conjunto de programas que tem como finalidade esconder e assegurar a presença de um invasor num computador comprometido. É importante ressaltar que o nome *rootkit* **não** indica que as ferramentas que o compõem são usadas para obter acesso privilegiado (*root* ou *Administrator*) num computador, mas sim para manter o acesso privilegiado num computador previamente comprometido.

Scam - esquemas ou acções enganadoras e/ou fraudulentas. Normalmente, têm como finalidade obter vantagens financeiras.

Scan - técnica normalmente implementada por um tipo de programa, projetado para efetuar varreduras em redes de computadores. Consulte *Scanner*.

Scanner - programa utilizado para efectuar analises em redes de computadores, com o intuito de identificar quais computadores estão activos e quais serviços estão a ser disponibilizados por eles. Amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados num computador.

Screenlogger - forma avançada de *keylogger*, capaz de armazenar a posição do cursor e o ecrã apresentada no monitor, nos momentos em que o *mouse* é clicado, ou armazenar a região que circunda a posição onde o *mouse* é clicado. Consulte também *Keylogger*.

Senha - conjunto de caracteres, de conhecimento único do utilizador, utilizado no processo de verificação da sua identidade, assegurando que ele é realmente quem diz ser.

Site - local na Internet identificado por um nome de domínio, constituído por uma ou mais páginas de hipertexto, que podem conter textos, gráficos e informações multimídia.

SMS - do Inglês ***S**hort **M**essage **S**ervice*. Tecnologia amplamente utilizada em telefonia móvel celular para a transmissão de mensagens de texto curtas. Diferente do MMS, permite apenas dados do tipo texto e cada mensagem é limitada em 160 caracteres alfanuméricos.

Sniffer - dispositivo ou programa de computador utilizado para capturar e armazenar dados que trafegam numa rede de computadores. Pode ser usado por um invasor para capturar informações sensíveis (como senhas de utilizadores), em casos onde estejam a ser utilizadas conexões inseguras, ou seja, sem criptografia.

Soft opt-in - regra semelhante ao *opt-in*, mas neste caso prevê uma excepção quando já existe uma relação comercial entre remetente e destinatário. Desta forma, não é necessária a permissão explícita por parte do destinatário para receber *e-mails* deste remetente. Consulte *Opt-in*.

Spam - termo utilizado para referir-se aos *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, este tipo de mensagem também é referenciada como UCE (do Inglês *Unsolicited Commercial E-mail*).

Spammer - pessoa que envia *spam*.

Spyware - termo utilizado para referir-se a uma grande categoria de *software* que tem o objectivo de monitorar actividades de um sistema e enviar as informações colectadas para terceiros. Podem ser utilizados de forma legítima, mas, na maioria das vezes, são utilizados de forma dissimulada, não autorizada e maldosa.

SSH - do Inglês ***S**ecure **Sh**ell*. Protocolo que utiliza criptografia para acesso a um computador remoto, permitindo a execução de comandos, transferência de ficheiros, entre outros.

SSID - do Inglês ***S**ervice **S**et **Id**entifier*. Conjunto único de caracteres que identifica uma rede sem fio. O SSID diferencia uma rede sem fio de outra e um cliente normalmente só pode conectar-se a uma rede sem fio se puder fornecer o SSID correcto.

SSL - do Inglês ***S**ecure **S**ockets **L**ayer*. Protocolo que fornece confidencialidade e integridade na comunicação entre um cliente e um servidor, através do uso de criptografia. Consulte também HTTPS.

Time zone - fuso horário.

Trojan horse - consulte Cavalo de tróia.

UCE - do inglês ***U**nsolicited **C**ommercial **E**-mail*. Termo usado para se referir aos *e-mails* comerciais não solicitados.

URL - do Inglês **U**niversal **R**esource **L**ocator. Sequência de caracteres que indica a localização de um recurso na Internet, como por exemplo,http://www.google.ao/.

Vírus - programa ou parte de um programa de computador, normalmente maldoso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e ficheiros de um computador. O vírus **depende** da execução do programa ou ficheiro hospedeiro para que possa se tornar activo e dar continuidade ao processo de infecção.

VPN - do Inglês ***V**irtual **P**rivate **N**etwork*. Termo utilizado para se referir à construção de uma rede privada utilizando redes públicas (por exemplo, a Internet) como infra-estrutura. Estes sistemas utilizam criptografia e outros mecanismos de segurança para garantir que somente utilizadores autorizados possam ter acesso a rede privada e que nenhum dado será interceptado enquanto estiver passando pela rede pública.

Vulnerabilidade - falha no projecto, implementação ou configuração de um *software* ou sistema operacional que, quando explorada por um atacante, resulta na violação da segurança de um computador ou sistema.

Web bug - imagem, normalmente muito pequena e invisível, que faz parte de uma página *Web* ou de uma mensagem de *e-mail*, e que é projectada para monitorar quem está a aceder esta página *Web* ou mensagem de *e-mail*.

WEP - do Inglês ***W**ired **E**quivalent **P**rivacy*. Protocolo de segurança para redes sem fio que implementa criptografia para a transmissão dos dados. Este protocolo apresenta algumas falhas de segurança.

Wi-Fi - do Inglês ***Wi**reless **Fi**delity*. Termo usado para se referir genericamente a redes sem fio que utilizam qualquer um dos padrões 802.11.

Wireless - consulte Rede sem fio.

WLAN - do Inglês ***W**ireless **L**ocal-**A**rea **N**etwork*. Refere-se a um tipo de rede que utiliza ondas de rádio de alta freqüência, ao invés de cabos, para a comunicação entre os computadores.

Worm - Programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o *worm* não embute cópias de si mesmo em outros programas ou ficheiros e não necessita ser explicitamente executado para se propagar. A sua propagação dá-se através da exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados nos computadores.

WPA - Do Inglês **W**i-Fi ***P**rotected **A**ccess*. Protocolo de segurança para redes sem fio desenvolvido para substituir o protocolo WEP, devido a suas falhas de segurança. Esta tecnologia foi projectada para, através de actualizações de *software*, operar com produtos Wi-Fi que disponibilizavam apenas a tecnologia WEP. Inclui duas melhorias em relação ao protocolo WEP que envolvem melhor criptografia para transmissão de dados e autenticação de utilizador.

Apendice II

Recomendações de segurança

Prevenção Contra Riscos e Programas Malignos (*Malware*)

Contas e senhas

- elaborar sempre uma senha que contenha pelo menos oito caracteres, compostos de letras, números e símbolos;
- jamais utilizar como senha o seu nome, apelidos, números de documentos, matriculas de carros, números de telefones, datas que possam ser relacionadas consigo ou palavras que façam parte de dicionários;
- utilizar uma senha diferente para cada serviço;
- alterar a senha com frequência;
- criar tantos utilizadors com privilégios normais, quantas forem as pessoas que utilizam seu computador;
- utilizar o utilizador *Administrador* (ou *root*) somente quando for estritamente necessário.

Vírus

- instalar e manter actualizado um bom programa antivírus;
- actualizar as assinaturas do antivírus, de preferência diariamente;
- configurar o antivírus para verificar os ficheiros obtidos pela Internet, discos duros (HDs), flexíveis (disquetes) e unidades removíveis, como CDs, DVDs e *pen drives*;
- desabilitar no seu programa leitor de *e-mails* a auto-execução de ficheiros anexados às mensagens;
- não executar ou abrir ficheiros recebidos por *e-mail* ou por outras fontes, mesmo que venham de pessoas conhecidas. Caso seja necessário abrir o ficheiro, certifique-se que ele foi verificado pelo programa antivírus;
- utilizar na elaboração de documentos formatos menos susceptíveis à propagação de vírus, tais como RTF, PDF ou *PostScript*;
- não utilizar, no caso de ficheiros comprimidos, o formato executável. Utilize o próprio formato compactado, como por exemplo Zip ou Gzip.

Worms, bots e botnets

- seguir todas as recomendações para prevenção contra vírus;
- manter o sistema operacional e demais *softwares* sempre actualizados;
- aplicar todas as correcções de segurança (*patches*) disponibilizadas pelos fabricantes, para corrigir eventuais vulnerabilidades existentes nos *softwares* utilizados;

- instalar um *firewall* pessoal, que em alguns casos pode evitar que uma vulnerabilidade existente seja explorada ou que um *worm* ou *bot* se propague.

Cavalos de tróia, backdoors, keyloggers e spywares

- seguir todas as recomendações para prevenção contra vírus, *worms* e *bots*;
- instalar um *firewall* pessoal, que em alguns casos pode evitar o acesso a um *backdoor* já instalado no seu computador, bloquear o recepção de um cavalo de tróia, etc;
- utilizar pelo menos uma ferramenta anti-*spyware* e mantê-la sempre actualizada.

Cuidados no Uso da Internet

Programas Leitores de E-mails

- manter o seu programa leitor de *e-mails* sempre actualizado;
- não clicar em *links* no conteúdo do *e-mail*. Se você realmente quiser acessar a página do *link*, digite o endereço diretamente no seu navegador (*browser)*;
- desligar as opções que permitem abrir ou executar automaticamente ficheiros ou programas anexados às mensagens;
- não abrir ficheiros ou executar programas anexados aos *e-mails*, sem antes verificá-los com um antivírus;
- desconfiar sempre dos ficheiros anexados à mensagem, mesmo que tenham sido enviados por pessoas ou instituições conhecidas. O endereço do remetente pode ter sido falsificado e o ficheiro anexo pode ser, por exemplo, um vírus ou um cavalo de tróia;
- fazer o *download* de programas directamente do *site* do fabricante;
- evitar utilizar o seu programa leitor de *e-mails* como um *browser*, desligando as opções de execução de *JavaScript* e *Java* e o modo de visualização de *e-mails* no formato HTML.

Browsers

- manter o seu *browser* sempre actualizado;
- desactivar a execução de programas *Java* na configuração de seu *browser*, a menos que seja estritamente necessário;
- desactivar a execução de *JavaScripts* antes de entrar numa página desconhecida e, então, activá-la ao sair;
- permitir que programas *ActiveX* sejam executados no seu computador **apenas** quando vierem de *sites* conhecidos e confiáveis;
- manter maior controlo sobre o uso de *cookies*, caso você queira ter maior privacidade ao navegar na Internet;
- bloquear *pop-up windows* e permití-las apenas para *sites* conhecidos e confiáveis, onde forem realmente necessárias;
- certificar-se da procedência do *site* e da utilização de conexões seguras ao realizar transacções via *Web*;
- somente acessar *sites* de instituições financeiras e de comércio eletrónico digitando o endereço directamente no seu *browser*, nunca clicando num *link* existente numa página ou num *e-mail*.

Programas de troca de mensagens

- manter o seu programa de troca de mensagens sempre actualizado;
- não aceitar ficheiros de pessoas desconhecidas (inclusive ficheiros ditos supostamente inofensivos como imagens, musicas, video e animações em flash), principalmente programas de computadores;
- utilizar um bom antivírus, sempre actualizado, para verificar todo e qualquer ficheiro ou *software* obtido, mesmo que venha de pessoas conhecidas;

- evitar fornecer muita informação, principalmente a pessoas que você acabou de conhecer;
- não fornecer, em hipótese alguma, informações sensíveis, tais como senhas ou números de cartões de crédito;
- configurar o programa para ocultar o seu endereço IP.

Programas de distribuição de ficheiros

- manter o seu programa de distribuição de ficheiros sempre actualizado e bem configurado;
- ter um bom antivírus instalado no seu computador, mantê-lo actualizado e utilizá-lo para verificar qualquer ficheiro obtido, pois eles podem conter vírus, cavalos de tróia, entre outros tipos de *malware*;
- certificar-se que os ficheiros obtidos ou distribuídos são **livres**, ou seja, não violam as leis de direitos autorais.

Partilha de recursos

- ter um bom antivírus instalado no seu computador, mantê-lo actualizado e utilizá-lo para verificar qualquer ficheiro ou programa compartilhado, pois eles podem conter vírus, cavalos de tróia, entre outros tipos de *malware*;
- estabelecer senhas para as partilhas, caso seja estritamente necessário partilhar recursos do seu computador.

Cópias de segurança (Backup)

- fazer cópias dos dados do computador regularmente;
- criptografar dados sensíveis;
- armazenar as cópias em local acondicionado, de acesso restrito e com segurança física;
- considerar a necessidade de armazenar as cópias num local diferente daquele onde está o computador ou servidores (Este local diferente pode ser por vezes numa sala diferente, edificio, bairro e em caso de aplicações criticas em provincias diferentes).

Fraude

Engenharia social

- não fornecer dados pessoais, números de cartões e senhas através de contacto telefônico;
- ficar atento a *e-mails* ou telefonemas solicitando informações pessoais;
- não acessar *sites* ou seguir *links* recebidos por *e-mail* ou presentes em páginas sobre as quais não se saiba a procedência;
- sempre que houver dúvida sobre a real identidade do autor de uma mensagem ou ligação telefônica, entrar em contacto com a instituição, provedor ou empresa para verificar a veracidade dos factos.

Cuidados ao realizar transacções bancárias ou comerciais

- seguir todas as recomendações sobre utilização do programa leitor de *e-mails* e do *browser* de maneira segura;
- estar atento e prevenir-se dos ataques de engenharia social;
- realizar transações somente em *sites* de instituições que você considere confiáveis;
- procurar sempre digitar no seu *browser* o endereço desejado. Não utilize *links* em páginas de terceiros ou recebidos por *e-mail*;
- certificar-se de que o endereço apresentado no seu *browser* corresponde ao *site* que você realmente quer acessar, antes de realizar qualquer acção;

- certificar-se que o *site* faz uso de conexão segura (ou seja, que os dados transmitidos entre o seu *browser* e o *site* serão criptografados) e utiliza um tamanho de chave considerado seguro;
- antes de aceitar um novo certificado, verificar junto à instituição que mantém o *site* sobre a sua emissão e quais são os dados nele contidos. Então, verificar o certificado do *site* antes de iniciar qualquer transacção, para assegurar-se que ele foi emitido para a instituição que se deseja acessar e está dentro do prazo de validade;
- não acessar *sites* de comércio electrónico ou *Internet Banking* através de computadores de terceiros;
- desligar a sua *Webcam* (caso você possua alguma), ao acessar um *site* de comércio electrónico ou *Internet banking*.

Boatos

- verificar sempre a procedência da mensagem e se o facto descrito na mesma é verídico;
- verificar em *sites* especializados e em publicações da área se o *e-mail* recebido já não está catalogado como um boato.

Privacidade

E-mails

- utilizar criptografia sempre que precisar enviar um *e-mail* com informações sensíveis;
- certificar-se que o seu programa leitor de *e-mails* grava as mensagens criptografadas, para garantir a segurança das mensagens armazenadas no disco.

Cookies

- desabilitar *cookies*, excepto para *sites* confiáveis e onde sejam realmente necessários;
- considerar o uso de *softwares* que permitem controlar o envio e recebimento de informações entre o *browser* e o *site* visitado.

Cuidados com dados pessoais em páginas Web, blogs e sites de redes sociais

- evitar disponibilizar os seus dados pessoais ou de familiares e amigos (*e-mail*, telefone, endereço, data de aniversário, etc);
- evitar disponibilizar dados sobre o seu computador ou sobre os *softwares* que utiliza;
- evitar fornecer informações sobre o seu quotidiano (como, por exemplo, hora que saiu e voltou para casa, data de uma viagem programada, horário que foi ao multicaixa, etc).
- **nunca** fornecer informações sensíveis (como senhas e números de cartão de crédito), a menos que esteja a ser realizada uma transacção (comercial ou financeira) e se tenha certeza da idoneidade da instituição que mantém o *site*.

Cuidados com os dados armazenados num disco duro

- criptografar todos os dados sensíveis, principalmente se for um *notebook*;
- sobrescrever os dados do disco rígido antes de vender ou se desfazer do seu computador usado.

Cuidados com telefones celulares, PDAs e outros aparelhos com bluetooth

- manter o *bluetooth* do seu aparelho desabilitado e somente habilite-o quando for necessário;
- ficar atento às notícias, principalmente àquelas sobre segurança, veiculadas no *site* do fabricante do seu aparelho;
- aplicar todas as correcções de segurança (*patches*) que forem disponibilizadas pelo fabricante do seu aparelho, para evitar que possua vulnerabilidades;
- caso você tenha comprado uma aparelho usado, restaurar as opções de fábrica e configurá-lo como no primeiro item, antes de inserir quaisquer dados.

Banda Larga e Redes Sem Fio (*Wireless*)

Protecção de um computador utilizando banda larga

- instalar um *firewall* pessoal e ficar atento aos registos de eventos (*logs*) gerados por este programa;
- instalar e manter actualizado um bom programa antivírus;
- actualizar as assinaturas do antivírus diariamente;
- manter os seus *softwares* (sistema operacional, programas que utiliza, etc) sempre actualizados e com as últimas correcções aplicadas;
- desligar a partilha de disco, impressora, etc;
- mudar, se possível, a senha padrão do seu equipamento de banda larga (modem ADSL, ou router por exemplo).

Protecção de uma rede utilizando banda larga

- instalar um *firewall* separando a rede interna da Internet;
- caso seja instalado algum tipo de *proxy* (como AnalogX, WinGate, WinProxy, etc), configurá-lo para que apenas aceite requisições a partir da rede interna;
- caso seja necessário partilhar recursos como disco ou impressora entre máquinas da rede interna, devem-se tomar os devidos cuidados para que o *firewall* não permita que este partilha seja visível pela Internet.

Cuidados com um cliente de rede sem fio

- instalar um *firewall* pessoal;
- instalar e manter actualizado um bom programa antivírus;
- actualizar as assinaturas do antivírus diariamente;
- aplicar as últimas correcções nos seus *softwares* (sistema operacional, programas que utiliza, etc);
- desligar partilha de disco, impressora, etc;
- desabilitar o modo *ad-hoc*. Utilize esse modo apenas se for absolutamente necessário e desligue-o assim que não precisar mais;
- usar WEP (*Wired Equivalent Privacy*) sempre que possível;
- verificar a possibilidade de usar WPA (Wi-Fi *Protected Access*) em substituição ao WEP, uma vez que este padrão pode aumentar significativamente a segurança da rede;
- considerar o uso de criptografia nas aplicações, como por exemplo o uso de PGP para o envio de *e-mails*, SSH para conexões remotas ou ainda o uso de VPNs;
- evitar o acesso a serviços que não utilizem conexão segura, ao usar uma rede sem fio em local público;
- habilitar a rede *wireless* somente quando for usá-la e desabilitá-la após o uso.

Cuidados com uma rede sem fio doméstica

- mudar as configurações padrão que acompanham o seu AP;
- verificar se os seus equipamentos suportam WPA (Wi-Fi *Protected Access*) e utilizá-lo sempre que possível;
- caso o WPA não esteja disponível, usar sempre que possível WEP (*Wired Equivalent Privacy*);
- se for utilizar WEP, trocar as chaves que acompanham a configuração padrão do equipamento. Procure usar o maior tamanho de chave possível (128 bits);
- desligar o seu AP quando não estiver a utilizar a sua rede.

Spam

- seguir todas as recomendações sobre utilização do programa leitor de *e-mails*;
- considerar a utilização de um *software* de filtragem de *e-mails*;
- verificar com o seu provedor ou com o administrador da rede se é utilizado algum *software* de filtragem no servidor de *e-mails*;
- evitar responder a um *spam* ou enviar um *e-mail* a solicitar a remoção da lista.

Incidentes de Segurança e Uso Abusivo da Rede

Registos de eventos (logs)

- verificar sempre os *logs* do *firewall* pessoal e de IDSs que estejam instalados;
- verificar se não é um falso positivo, antes de notificar um incidente.

Notificações de incidentes

- incluir *logs* completos, com data, horário, *time zone* (fuso horário), endereço IP de origem, portas envolvidas, protocolo utilizado e qualquer outra informação que tenha feito parte da identificação do incidente;
- enviar a notificação para os contactos da rede e para os grupos de segurança das redes envolvidas;
- manter abuso@seuprovedor.ao na cópia das mensagens (conforme foi abordado neste livro, os provedores de serviços de acesso a Internet têm por obrigação criar um email neste formato, aonde os utilizadors possam apresentar as suas reclamações sobre abusos sofridos na utilização de determinado serviço).

Bibliografia

Internet Security – Professional Reference, de Joel Snyder, Tom Sheldon, Tim Petru, New Riders Publishing, ISBN: 1-56-205760-X

Internet Security Secrets , John R. Vacca, IDG Books Worldwide, ISBN: 1-56-884457-3

Maximum Security: A Hacker's Guide to Protect Your Internet Site and Network, de anónimo, Sams, ISBN: 1-57-521268-4

Practical Unix and Internet Security, de Simson Garfinkel, Gene Spafford, O'Reilly & Associates, ISBN: 1-56-592148-8

Internet Privacy Kit, de Marcus Gonçalves, Que, ISBN: 0-78-971234-2

Internet and TCP/IP Network Security: Securing Protocols and Applications, de Uday O. Pabrai, Vijay K. Gurbani, McGraw-Hill, ISBN: 0-07-048215-2

Web Security SourceBook, de Avi Rubin, Daniel Geer, Marcus J. Ranum, Aviel D. Rubin, dan Geer, John Wiley & Sons, ISBN: 0-47-118148-X

Protecting Your Web Site With Firewalls, de Marcus Gonçalves, Prentice Hall, ISBN: 0-13-628207-5

Applied Cryptography: Protocols, Algorithms, and Source Code in C, de Bruce Shneier, John Wiley & Sons, ISBN: 0-47-111709-9

Lista de webliografia

Google (O meu melhor amigo na Internet) – http://www.google.com

Wikipedia – http://www.wikipedia.org

Actane – http://www.actane.com

Atlanta Internet Conections – http://www.axis-net.com

Check Point – http://www.checkpoint.com

Computer Security Information – http://www.alw.nih.gov/Security/security.html

Connect – http://www.csg.sterncomm.com

Cryptography – http://theory.lcs.mit.edu/~rives/crypto-security.html

Digicrime – http://www.digicrime.com

National Security Agency (NSA) – http://www.nsa.gov:8080/

Secure News, Newsletter – http://www.isecure.com/newslet.htm

Security Issues on the Internet – http://www.einet.net/galaxy/Engineering-and-Technology/Computer-Technology/Security.html

The Internet Privacy Coalition – http://www.privacy.org/