O livro de segurança informática mais vendido em Portugal

TÉCNICAS *para* HACKERS

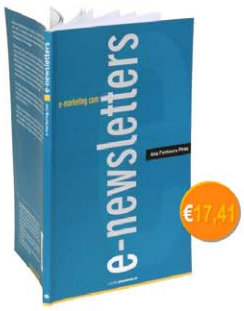
soluções para segurança

VERSÃO 2

Wilson Oliveira

€22,20

€19,70



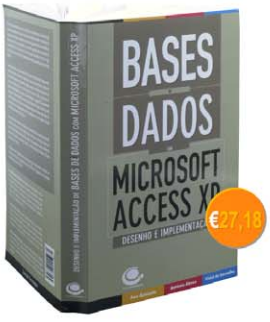
€17,41

€22,20

€24,69

€22,20

€22,20



€27,18

€27,18

Nota de Encomenda

Pode ser fotocopiada

Dirija as suas encomendas para: Centro Atlântico - Ap. 413 - 4764-901 V. N. de Famalicão

TÍTULO	Preço Unitário	Quant.	Sub-total

Total: € ☐☐☐,☐☐

SIM, desejo receber os títulos que assinalei sem qualquer despesa de envio.

☐ Envio cheque/Vale nº _____ à ordem do Centro Atlântico.

☐ Prefiro que debitem no meu cartão de crédito:

Número do cartão de crédito ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

Cartão em nome de _____

Últimos três dígitos nas costas do Cartão: ☐☐☐ Validade: ☐☐☐☐ ☐ Mastercard ☐ Visa ☐ American Express

Empresa _____

Nome _____

Morada _____

CP ☐☐☐☐-☐☐☐ ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐ Tel. ☐☐☐☐☐☐☐☐☐

E-Mail _____ Contribuinte ☐☐☐☐☐☐☐☐☐

Sem despesas de envio. As encomendas directas ao Centro Atlântico, para Portugal, não pagam custos de portes. Envios à cobrança são onerados em €2,5 por encomenda. Envios internacionais são onerados em €5.

Os dados recolhidos são processados automaticamente, sendo o seu fornecimento facultativo.

É garantido, nos termos da Lei, o direito de acesso e de rectificação bem como de não divulgação a terceiros, devendo dirigir-se para tal ao Centro Atlântico. Se não desejar receber informações sobre os nossos produtos e serviços assinale aqui com uma cruz ☐

Todos os preços já incluem IVA à taxa em vigor.

CENTROATLANTICO.PT

Apartado 413
4764-901 V. N. Famalicão

Rua da Misericórdia, 76
1200-273 Lisboa

Tel.: 808 20 22 21
geral@centroatlantico.pt

Wilson Oliveira

Técnicas para Hackers

Soluções para Segurança

versão 2

Portugal/2003

Reservados todos os direitos por Centro Atlântico, Lda.
Qualquer reprodução, incluindo fotocópia, só pode ser feita com autorização expressa dos editores da obra.

TÉCNICAS PARA HACKERS - SOLUÇÕES PARA SEGURANÇA - VERSÃO 2
Colecção: Tecnologias
Autor: Wilson Oliveira

Direcção gráfica: Centro Atlântico
Revisão: Centro Atlântico
Capa: Paulo Buchinho

© Centro Atlântico, Lda., 2003
Ap. 413 - 4764-901 V. N. Famalicão
Porto - Lisboa
Portugal
Tel. 808 20 22 21

geral@centroatlantico.pt
www.centroatlantico.pt

Fotolitos: Centro Atlântico
Impressão e acabamento: Rolo & Filhos
1ª edição: Janeiro de 2003

ISBN: 972-8426-63-1
Depósito legal: 190.037/03

Marcas registadas: todos os termos mencionados neste livro conhecidos como sendo marcas registadas de produtos e serviços, foram apropriadamente capitalizados. A utilização de um termo neste livro não deve ser encarada como afectando a validade de alguma marca registada de produto ou serviço.
O Editor e os Autores não se responsabilizam por possíveis danos morais ou físicos causados pelas instruções contidas no livro nem por endereços Internet que não correspondam às *Home-Pages* pretendidas.

ÍNDICE

Técnicas de Invasão

Uma invasão é a entrada num *site*, servidor, computador ou serviço por alguém não autorizado. Mas, antes da invasão propriamente dita, o invasor poderá fazer um teste de invasão, que é uma tentativa de invasão em partes, onde o objectivo é avaliar a segurança de uma rede e identificar os seus pontos vulneráveis.

Mas não existe invasão sem um invasor, que pode ser conhecido, na maioria das vezes, como *hacker* ou *cracker*. Ambos usam os seus conhecimentos para se dedicarem a testar os limites de um sistema, ou para estudo e procura de conhecimento ou por curiosidade, ou para encontrar formas de quebrar a sua segurança, ou ainda, por simples prazer.

Mas também pode ser por mérito, para promoção pessoal, pois as suas descobertas e ataques são divulgados nos media e eles tornam-se conhecidos no seu universo; a diferença é que o *cracker* utiliza as suas descobertas para prejudicar financeiramente alguém, em benefício próprio, ou seja, são os que utilizam os seus conhecimentos para o lado mau.

Existem muitas ferramentas para facilitar uma invasão e a cada dia aparecem novidades a esse respeito. De seguida serão descritas algumas das mais conhecidas.

Spoofing

Nesta técnica, o invasor convence alguém de que ele é algo ou alguém que não é, sem ter permissão para isso, conseguindo autenticação para aceder ao que não deveria ter acesso, falsificando o seu endereço de origem. É uma técnica de ataque contra a autenticidade, onde um utilizador externo se faz passar por um utilizador ou computador interno.

Sniffers

É um programa de computador que monitoriza passivamente o tráfego de rede. Pode ser utilizado legitimamente, pelo administrador do sistema para verificar problemas de rede, ou pode ser usado ilegitimamente por um intruso, para roubar nomes de utilizadores e *passwords*. Este tipo de programa explora o facto dos pacotes das aplicações de TCP/IP não serem criptografados.

Entretanto, para utilizar o *sniffer*, é necessário que ele esteja instalado algures na rede, onde passe tráfego de pacotes de interesse para o invasor ou administrador.

Ataque do tipo DoS

É um ataque de recusa de serviço; estes ataques são capazes de anular um *site*, indisponibilizando os seus serviços. É baseado na sobrecarga de capacidade ou numa falha não esperada.

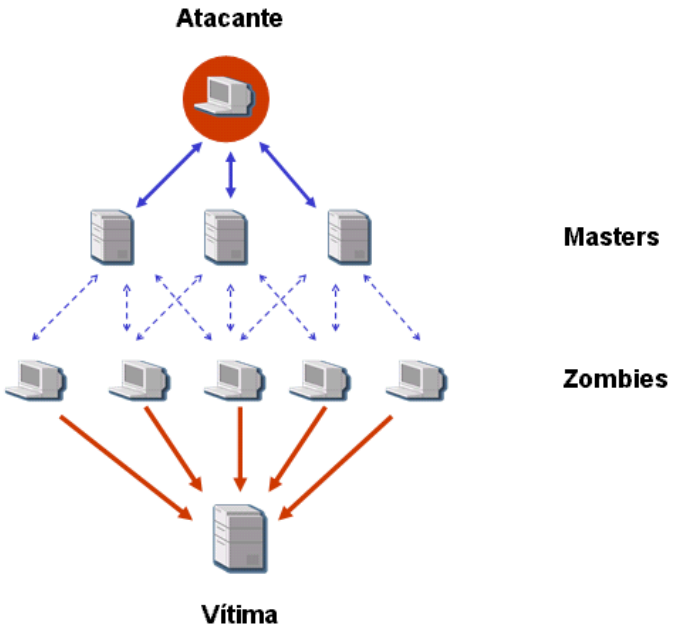
Um dos motivos para existirem este tipo de falhas nos sistemas deve-se a um erro básico de programadores, em que no momento de testar um sistema, muitas vezes não testam o que acontece se o sistema for forçado a dar um erro, se receber muitos pacotes em pouco tempo ou se receber pacotes com erro; normalmente é testado se o sistema faz o que deveria fazer e alguns erros básicos. O invasor parte deste princípio e faz diversos tipos de testes de falhas, até acontecer um erro e o sistema parar.

Este tipo de ataque não causa perda ou roubo de informações, mas é um ataque preocupante, pois os serviços do sistema atacado ficarão indisponíveis por um tempo indeterminado. Dependendo da equipa existente na empresa para o disponibilizar novamente e dependendo do negócio da empresa, este tempo de indisponibilidade pode trazer muitos prejuízos.

Em Maio de 2001 foram descobertos novos tipos de ataques DoS. Esta nova geração inclui o *.pulsing zombies.*, que envia curtas emissões de tráfego a um alvo determinado e não contínuo, como no ataque já conhecido, que podem ser rastreados. Esta nova maneira de ataque dificulta ainda mais a detecção. Além disso, técnicos da empresa Asta Networks, responsáveis por esta identificação, descobriram que, neste novo tipo de ataque, em vez de se paralisar totalmente o servidor, ele apenas restringe os seus serviços. Os servidores atacados desta maneira não ficam sobrecarregados, mas sim, confusos com o grande número de actividades de rede.
E, de acordo com um estudo da Universidade da Califórnia, os *crackers* tentam realizar em torno de 4 mil ataques do tipo DoS por semana. O alvo mais comum são as grandes empresas.

Ataque do tipo DDoS

São ataques semelhantes aos DoS, tendo como origem diversos e até milhares de pontos disparando ataques DoS para um ou mais *sites* determinados. Para isto, o invasor coloca agentes para dispararem o ataque numa ou mais vítimas. As vítimas são máquinas escolhidas pelo invasor por possuírem alguma vulnerabilidade. Estes agentes ao serem executados transformam-se num ataque DoS de grande escala, como se mostra na ilustração a seguir:



DNS Spoofing

O objectivo principal do DNS Spoofing é o de destruir o servidor de nomes e com isto permitir que máquinas não confiáveis, que podem ser as do invasor, sejam consideradas confiáveis, pois passarão pelas confiáveis. Para realizar este ataque, o invasor precisa ter o controlo sobre a máquina servidora de DNS, Domain Name Server, onde constam todos os nomes das máquinas confiáveis e os endereços destas máquinas, que são os números IP. Além disso, o invasor precisará saber o nome de uma destas máquinas confiáveis.

Na posse destes dados, o invasor altera o registo do DNS que mapeia o endereço IP da máquina confiável escolhida, modificando para que contenha o endereço da máquina do invasor. A partir desta alteração, o invasor terá livre acesso a serviços que necessitam da autenticação deste servidor de nomes.

A maioria dos novos sistemas possui métodos contra o DNS Spoofing, utilizando uma técnica chamada *cross-check*. Nesta técnica, o nome retornado pela consulta é testado novamente pelo DNS. Se o endereço utilizado para a conexão é diferente do retornado pelo *cross-ckeck*, a

conexão é bloqueada e é gerado um alerta. Esta técnica pode ser implementada no servidor de DNS ou nos servidores dos serviços com autenticação baseada no DNS. Mas, existem variantes do DNS Spoofing, onde o invasor tenta enganar o *cross-check*, esgotando o servidor de DNS com pedidos.

Quebra de *passwords*

Para aceder a algo é necessário uma *password* de acesso. Muitos invasores tentam descobrir estas *passwords* através de técnicas de quebra de *passwords*, como tentar as *passwords* standards de sistemas ou as *passwords* simples como nomes pessoais, nome da empresa, datas, entre outros. Mas para facilitar a descoberta da *password*, existem diversos programas, como dicionários de *passwords* e programas que tentam todas as combinações possíveis de caracteres para descobrir as *passwords*.

Vírus

Os vírus de computadores são outro exemplo de programas de computador, utilizados maliciosamente ou não, que se reproduzem introduzindo-se em outros programas. Quando estes programas são executados, o vírus é activado e pode se espalhar ainda mais, geralmente danificando sistemas e ficheiros do computador onde ele se encontra; um exemplo deste tipo de programa é o *Worm*.

Outro tipo de vírus muito conhecido é o *Trojan*, que insere um pedaço de código num programa aparentemente inofensivo, colocando assim um hospedeiro no *site* invadido, para que o invasor fique com o controlo remoto do sistema. Segundo uma pesquisa realizada por uma empresa britânica de anti-vírus, o número de ataques de vírus triplicou em 2001. Nesta pesquisa também pode ser concluído que as ferramentas para protecção efectiva contra os vírus não terão o mesmo crescimento.

Demais considerações sobre Técnicas de Invasão

Por fim, o invasor pode utilizar-se da evasão, que é a arte de não deixar pistas de quem invadiu e como isto aconteceu; quando isto é feito com êxito, dificulta ainda mais a descoberta desta vulnerabilidade e, assim, da correcção da mesma, para protecção de novos ataques.

Ferramentas de segurança

Existem no mercado diversos tipos de ferramentas, para protegerem

sistemas ou detectar invasões. Em seguida serão descritas algumas mais conhecidas.

Firewalls

Quando o assunto é segurança, uma das primeiras ferramentas mencionadas é a Firewall. No sentido amplo, ela nega o acesso de utilizadores não autorizados a um determinado *host* ou ficheiro, em sentido restrito; examina cada pacote e determina a sua origem; se está numa lista aprovada ela permite o acesso, senão, não. Já numa definição mais usual a Firewall é uma barreira de protecção entre duas redes, e geralmente fica entre a rede local e a Internet.

Chama-se *firewall* ao equipamento que garante o controlo da conexão entre duas ou mais redes, ou seja, trata-se de um equipamento que executa uma aplicação específica de controlo de acesso e que é responsável por interligar, de forma segura, duas ou mais redes, garantindo o controlo, a verificação e o *log* (auditoria) dos pacotes que passam entre elas. O seu nome teve origem nas paredes corta-fogo, existentes para impedir a passagem do fogo nos prédios.

A *firewall* filtra os acessos feitos da empresa para a Internet e da Internet para a empresa; apesar de ser uma ferramenta de extrema importância para a protecção da empresa de acessos indevidos externos, a sua utilização isoladamente não garante segurança.

A solução é implementar duas medidas de segurança, Política e Controlo. A empresa deve ter uma Política de Segurança que descreva o papel dos recursos de TI dentro da empresa, e elaborar mecanismos para controlar estas políticas.

Isto mostra que a *firewall* protege a rede interna de ataques externos, mas não de ataques internos. Além disso, a *firewall* quanto instalada correctamente é uma barreira contra ataques, mas caso o invasor consiga quebrar a segurança da *firewall* ou esta estiver mal configurada, o invasor terá acesso ao sistema.

Sistemas de Detecção de Intrusão

São sistemas inteligentes, capazes de detectar tentativas de invasões em tempo real. Estes sistemas podem não apenas alertar sobre a invasão, como também, aplicar acções necessárias contra o ataque. Eles podem ser sistemas baseados em regras ou adaptáveis; no primeiro caso, as

regras de tipos de invasões e a acção a ser executada são previamente registadas. O problema é que a cada dia surgem novos tipos de ataques e estas regras precisam estar sempre actualizadas para o sistema ser eficaz. No segundo tipo, são empregadas técnicas mais avançadas, inclusive de inteligência artificial, para detectarem novos ataques, sempre que surgirem.

Além disso, o sistema de detecção de intrusão pode ser classificado como NIDS (sistema de detecção de intrusão de redes) e HIDS (sistema de detecção de intrusão de *hosts*).

Logs

Os *Logs* são registos gerados pelos sistemas ou aplicações, com informações dos eventos ocorridos. São considerados uma medida básica de segurança, mas muitas vezes não são utilizados pelos administradores, ou por que estão desactivados, pois dependendo do sistema e do hardware a geração do *Log* pode tornar-se lenta, ou porque foram esquecidos ou porque não os querem analisar, já que os *Logs* geralmente são relatórios enormes. Mas é uma ferramenta muito útil para auditorias de acessos, para verificação do que está a ser utilizado, possíveis falhas nos sistemas, etc.

Anti-vírus

Software que verifica a existência de vírus em computadores, pastas ou ficheiros e ao encontrá-los executa a sua limpeza. A maneira como ele fará isso pode ser totalmente configurada pelo utilizador. O normal é o anti-vírus analisar e quando encontrar algum vírus tentar eliminar apenas o vírus, e caso não consiga, se o utilizador autorizar, ele removerá também o ficheiro. Uma vez instalado o anti-vírus, ele pode ser configurado, dependendo das suas características, para ficar activo e analisar todos os ficheiros que forem abertos, e caso apareça algum vírus, ele avisar imediatamente.

Mas, como diariamente surgem novos tipos de vírus, diariamente também, a lista de vírus dos anti-vírus é actualizada, e neste caso, é importante o utilizador estar atento e actualizar o seu anti-vírus sempre que possível.

Backup

Uma das ferramentas existentes para segurança dos dados é o software de *backup* e *restore*, que servem para fazer cópias de segurança das informações e sistemas de uma empresa e recuperar as informações

quando necessário. Todos os dados e sistemas de uma empresa devem possuir cópias de segurança íntegras, actuais e armazenadas em local seguro.

Em geral, o *backup* é feito em fita, disquete, CD-R ou outra suporte portátil que pode ser armazenado para futura utilização, como no caso de algum desastre ou perda de informações. As informações podem ser perdidas por causa de acidentes, desastres, ataques, erros de sistemas ou hardware ou falha humana, entre outros motivos.

Com as informações actualizadas copiadas através de *backups* para algum suporte, quando acontecer uma perda de dados, basta restaurar estas informações.

Legislação

"Durante anos, a Internet foi considerada uma «terra de ninguém» onde tudo era permitido, sem regulamentação, fiscalização ou punição para conteúdos e actos idênticos considerados ilegais offline. O anonimato potenciado pela rede, que facilitava o encobrimento da autoria, fazia dela um terreno fértil para a prática de actos ilícitos. No final dos anos 80, levantaram-se questões como a pornografia e a xenofobia online, ao mesmo tempo que se propagaram as actividades que se prendem com a violação de redes e sistemas informáticos alheios.

Por outro lado, a facilidade com que a mensagem é difundida através da rede, alastrando-se potencialmente aos quatro cantos do mundo, fez disparar a prática online de crimes contra a honra, consideração ou bom nome.
A net é talvez hoje um dos mais poderosos e perigosos veículos de actos difamatórios. Pelo seu carácter global, chegando com a mesma facilidade aos mais variados pontos do globo, e pela rapidez com que a informação é difundida, a difamação via Internet pode causar danos maiores e mais dificilmente reparáveis do que através dos meios ditos tradicionais.

No entanto, há hoje regras específicas aplicáveis ao mundo online no que toca à criminalidade e à sua repressão e prevenção. A questão está na ordem do dia.
Foi no dia 23 de Novembro de 2001 assinada a Convenção Internacional sobre a Cibercriminalidade, o primeiro texto jurídico a debruçar-se sobre o assunto à escala internacional. E em Portugal já existe alguma legislação

específica sobre a matéria. Apesar da difícil resolução do problema da fiscalização, a lei e o direito avançam hoje para a regulação em sede de direito criminal deste admirável mundo novo.

A legislação sobre matéria informática é relativamente recente. Esta é uma das típicas matérias em que a lei anda atrás da evolução tecnológica e do uso que é feito pelo Homem das novas ferramentas e instrumentos que são colocados à sua disposição. O direito da informática nasceu sobretudo nos tribunais, fruto da necessidade de dirimir litígios emergentes entre partes em confronto.

O Código Penal, como lei criminal fundamental, tem algumas regras aplicáveis aos crimes informáticos ou praticados via Internet. É o caso, por exemplo, do art. 180º do Código Penal, que versa sobre difamação, e que é aplicável às afirmações que sejam feitas através da Web imputando a outra pessoa um facto ou formulando um juízo ofensivo da sua honra ou consideração. Ou as regras dos artigos 153º, 154º e 155º sobre ameaça e co-acção que são aplicáveis aos actos cometidos através da rede.

Mas desde 1991 que existem regras específicas no que toca à área da criminalidade informática em particular, matéria que dada a sua complexidade e especificidade mereceu pelo legislador um tratamento em diploma autónomo.
A Lei 109/91 de 17 de Agosto, conhecida como Lei da Criminalidade Informática, versa por exemplo sobre crimes como a falsidade e a sabotagem informáticas, os danos relativos a dados ou programas, o acesso ilegítimo a sistemas ou redes, a intercepção ilegítima ou a reprodução de programas. Note-se que as regras incluídas neste diploma aplicam-se às empresas e outras pessoas colectivas, conforme está estabelecido nos artigos 3º e 10º e que podem ser aplicadas aos actos cometidos através da Internet.

A falsidade informática é um dos crimes previstos e punidos nesta lei, pretendendo-se proteger interesses idênticos aos que são protegidos no crime de falsificação.
Quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados ou programas informáticos, ou interferir num tratamento informático de dados quando podem servir como meio de prova, será punido com pena de prisão até cinco anos ou multa de 120 a 600 dias. Na mesma pena incorre quem se limitar a usar, em seu benefício ou de terceiros, um documento assim alterado.

A sabotagem informática, de menor gravidade do que o anterior, é outro dos crimes previstos nesta lei. Quem se decidir a entravar ou perturbar o funcionamento de um determinado sistema informático ou de comunicação de dados à distância, pode habilitar-se a uma pena de prisão de 5 anos ou a uma multa até 600 dias. Diferente é o mero acesso ilegítimo, em que é punida apenas a entrada em sistemas ou redes informáticas.

Outra disposição especialmente importante prevista nesta lei tem que ver com a reprodução ilegítima de programas protegidos, ou seja, com a questão do software ilegal."

(excerto do livro "**101 PERGUNTAS E RESPOSTAS DO DIREITO DA INTERNET E DA INFORMÁTICA**", da colecção Direito das Novas Tecnologias, do Centro Atlântico, escrito por Ana Margarida Marques, Mafalda Anjos e Sónia Queiróz Vaz)

Demais aspectos

Outros aspectos importantes na área de segurança da informação são sobre as falhas dos sistemas, os *Bugs* e as vulnerabilidades, que por serem familiares se torna importante explicar um pouco do significado destes termos.

Um Bug é uma falha ou fraqueza de programação num sistema, que o faz executar incorrectamente, resultando em mensagens de erro ou simplesmente parando completamente o sistema. Já uma vulnerabilidade refere-se a qualquer fraqueza, ou *bug*, em quaisquer sistemas, seja de hardware ou software, que permite que invasores obtenham acessos não autorizados ou neguem algum serviço.

Esses aspectos serão estudados com mais detalhes no decorrer deste livro.

3. Ferramentas de Segurança

Nos dias de hoje, os administradores de sistemas e de redes devem conhecer os principais recursos disponíveis para a implementação de um ambiente seguro, com algum grau de protecção contra os perigos mais comuns existentes em redes de computadores.

Apresentamos uma série de ferramentas que auxiliam na manutenção da segurança de um sistema.

Introdução

Sniffers, crackers, spoofing, syn_flooder, dnskiller, ping o'death, winnuke... nomes assustadores que parecem ter saído de filmes como "Mad Max" ou "Robocop" mas que na verdade são companheiros inseparáveis de um certo tipo indesejável de utilizadores de rede: os *hackers* ou *crackers*, ou ainda, invasores.

Como obter um ambiente computacional confiável e seguro, diante de tais ameaças? Principalmente reconhecendo a importância de um bom trabalho de administração de sistemas e lançando mão do equivalente benigno de tais programas, as chamadas ferramentas de segurança.

A lista de programas e pacotes dessa área é extensa, e certamente uma descrição detalhada de todas elas mereceria um livro, talvez com mais de um volume. Em poucas linhas tentaremos apresentar as que consideramos mais úteis, dentro do contexto Internet, software de domínio público e sistema operativo UNIX, que, por razões históricas, é o sistema mais estudado neste aspecto.

Simplifique

Antes de começar a utilizar as ferramentas de segurança, é importante estabelecer alguns objectivos e definir algumas premissas.

A primeira meta é tentar simplificar o ambiente. Ofereça somente os

serviços necessários. Retire tudo o que não está a ser usado. Tente limitar o número de opções e facilidades disponíveis.

É um objectivo difícil de ser conquistado, mas vale a pena. Ter um sistema conhecido e controlado é mais de metade do caminho para se conseguir um ambiente seguro.

A principal premissa na utilização de ferramentas de segurança acaba decorrendo da meta anterior. Esse recurso deve ser utilizado apenas em sistemas não comprometidos. Instalar tais ferramentas em máquinas recentemente invadidas, sem que se tenha uma ideia precisa do estado do sistema, pode atrapalhar muito mais que ajudar.

É importante também que os componentes do sistema estejam a funcionar de forma razoavelmente correcta, já que praticamente todas as ferramentas dependem dessa condição. Portanto, todos os *patches* necessários devem ter sido aplicados.

E nunca deve perder-se de vista que a utilização dessas ferramentas deve ser somente uma parte de algo bem maior, que consiste na definição e adopção de uma política de segurança para a Organização.

Tipos de Ferramentas

As ferramentas de segurança podem ser classificadas inicialmente quanto ao seu objectivo:

Ferramentas de segurança de hosts

São dirigidas para a análise, correcção e implementação de novos controlos em sistemas computacionais. Como exemplo, temos ferramentas como o *crack*, para verificação de *passwords*.

Ferramentas de segurança de rede

Estão direccionadas para a verificação e implementação de controlos sobre o tráfego de uma rede. O exemplo mais conhecido são os filtros de pacotes.

Outra categorização é referente à função: