

O livro de **segurança informática** mais vendido em Portugal

TÉCNICAS

para

HACKERS

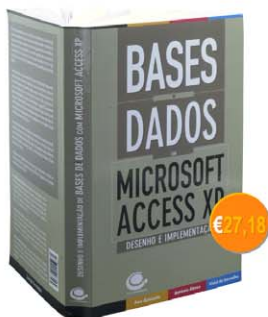
soluções para segurança

VERSÃO
2



CENTROATLANTICO.PT

Wilson Oliveira



Nota de Encomenda Podem ser fotocopiada
 Dirija as suas encomendas para: Centro Atlântico - Ap. 415 - 4764-901 V. N. de Famalicão

TÍTULO	Preço Unitário	Quant.	Sub-total

Total: €

SIM, desejo receber os títulos que assinalo 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 na 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 assinala aqui com uma cruz

CENTRO ATLÂNTICO PT
 Apartado 413
 4764-901 V. N. Famalicão
 Rua da Misericórdia, 76
 1200-273 Lisboa
 Tel.: 808 20 22 21
 geral@centroatlantico.pt

Todos os preços já incluem IVA à taxa em vigor.

Wilson Oliveira

Técnicas para Hackers

Soluções para Segurança

versão 2



CENTRO **ATLANTICO**.PT

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

AGRADECIMENTOS	19
SOBRE O AUTOR	19
SOBRE ESTA OBRA	21
1. INTRODUÇÃO	23
Definições	25
Como se tornar um Hacker?	27
2. SEGURANÇA DA INFORMAÇÃO	29
Segurança	30
Crescimento do Risco	30
Necessidades de Segurança	31
Standards de Segurança na Internet	31
Alvos dos Hackers na Internet	31
Técnicas Utilizadas	31
Quem são as ameaças?	32
Aspectos Importantes na Segurança de Sistemas	32
Autenticação	32
Criptografia	33
Técnicas de Invasão	37
Spoofing	37
Sniffers	37
Ataque do tipo DoS	38
Ataque do tipo DDoS	38
DNS Spoofing	39
Quebra de <i>passwords</i>	40
Vírus	40
Demais considerações sobre Técnicas de Invasão	40
Ferramentas de segurança	40
Firewalls	41
Sistemas de Detecção de Intrusão	41
Logs	42
Anti-vírus	42
Backup	42
Legislação	43
Demais aspectos	45
3. FERRAMENTAS DE SEGURANÇA	47
Introdução	47
Simplifique	47
Tipos de Ferramentas	48
Ferramentas de segurança de hosts	48
Ferramentas de segurança de rede	48
Tcp_wrapper	49
Crack	50
Tripwire	51

Tiger	53
Swatch	54
Strobe	55
ISS	55
Gabriel/Courtney	56
Conclusão	56
4. O UNIVERSO COMPUTACIONAL	57
Segurança Física	57
Segurança Lógica	57
Palavras-chave (passwords)	58
Regras para Utilizadores e Palavras-chave	58
5. HACKERS	61
Atitudes de um Hacker	61
Habilidades básicas	63
6. WINDOWS 95/98 E NT	67
Windows 95/98	67
Configurando as palavras-chave do Windows 95/98 de forma eficiente	67
Método de invasão (quando as palavras-chave não são configuradas eficientemente)	70
Windows NT	70
Workgroup	71
Domínio	71
Vulnerabilidade do Windows NT	72
Bug da Port 80	72
Conhecendo um pouco sobre o Registo do Windows	73
Tipos de Dados do Registry (Registo)	76
Procurando informações no Registry	77
Editando o Registry	78
Removendo Entradas	78
Desactivando a <i>password</i> de <i>Caching</i>	78
Não mostra o Network Neighborhood	79
Arrumando o Registry corrompido	79
Configurando um tamanho mínimo para palavras-chave (<i>passwords</i>)	80
Bloqueando o Acesso Anonymous (NetBios)	80
Restringir acesso remoto ao Registry (contra o dump de 'palavra-chave')	80
Desactivar o botão de ShutDown no Logon	82
Conhecendo o NetBios	82
O que é o NetBios?	82
Serviço de Nomes no NetBios	83
Vulnerabilidades NetBios (NAT)	84
O Comando NBTSTAT	85
Introdução aos Comandos NET	86
Secção e Ataque NetBios usando Net View e Net Use	87
Uma secção de Ataque NetBios usando NAT.EXE	88
Protocolos possíveis numa rede Windows	90
NetBIOS Extended User Interface	90
NetBEUI	90
NWLink	91
TCP/IP	91

Bug's do Windows	91
Bug no Autorun	91
Insegurança no Windows 95	92
Invadindo o Windows NT	93
CD Bug	93
Ficheiros .SAM	94
Registos	94
CMD.EXE	94
Invadindo o Windows NT	95
7. UNIX	97
Linux	100
Implementando a Segurança no Linux	101
Ligando e Configurando	103
TCP Wrappers	105
8. VÍRUS	107
O que é um Vírus?	107
Como é que os Vírus trabalham?	108
Vírus de disco	108
Vírus de Ficheiro	108
Vírus Multi-partite	108
Vírus Tipo DIR-II	108
Porque é que os Vírus são escritos?	108
O que é um Vírus de Macro?	109
Como criar um Vírus de Macro?	111
Tipos de Vírus de Macro	113
Nível 1	113
Nível 2	114
Nível 3	114
Funcionamento do Vírus de Macro do Word	115
Como evitar os Vírus de Macro?	116
Remover Vírus do Word	117
Como identificar e limpar um Vírus de MACRO sem ter anti-vírus?	117
Como eliminar as mazelas dos Vírus?	118
Exemplos de WordBasic	119
Como criar um AUTOEXEC.BAT destrutivo	119
Sair do Windows	119
Controlo da Aplicação	123
Obter informações do sistema	123
Verificando que aplicações estão a ser executadas	124
Activando uma Janela	125
Fechando uma Janela	125
Ocultando uma Janela	125
Voltando a exibir uma Janela	125
Executando uma Aplicação	126
Copiar Macros	126
Criando um Vírus	127
Infect	129
Autoclose	130
Autoopen	130
Autoexec	130

Libvírus	131
Destruct	139
Ficheiro guardarcomo	139
Ficheiro imprimir	141
Ficheiro imprimirpadrao	141
Imprearq	141
E-mail	141
Conclusão	145
Criando Pseudo Vírus com JavaScript	145
Abrir a mesma Home-Page infinitamente	145
Exibir continuamente uma mensagem no ecrã	146
“Bomba” arraga Lammer	146
Criando um Vírus em Pascal	146
Problemas	147
Possíveis soluções	147
Outras questões	148
O Código do Vírus	148
Iniciando a infecção	148
Infecção do vírus	149
Corpo Principal do Vírus	150
Programas necessário à execução do Vírus	151
Acções do vírus	153
Exemplos de acções do vírus	153
Constantes a serem usadas	157
Variáveis globais a serem usadas	157
Bibliotecas de funções necessárias ao funcionamento	158
Listagem do programa como ele deveria ficar	158
Testando o vírus	164
Considerações	164
Criando um Trojan com Java	165
Aprendendo a construir um Trojan	165
Trojan T25	166
Criando um Trojan em Delphi (similar ao Back Orifice)	167
Como é que este Trojan funciona?	167
A Infecção	167
Conectando a parte Cliente	168
Comandos	168
Fonte em Delphi 4/5 da parte Cliente	169
Fonte em Delphi 4/5 da parte Servidora	189
9. TCP/IP	201
Pilha	201
Visão Geral do Protocolo	202
Principais Protocolos	203
DNS (Domain Name System)	203
DHCP (Dynamic Host Configuration Protocol)	204
SMTP (Simple Mail Transfer Protocol)	205
POP3 (Post Office Protocol 3)	207
NNTP (Network News Transport Protocol)	207
ICMP (Internet Control Message Protocol)	207
Portas e Protocolos	207
Utilitários do TCP/IP	210
Ipconfig	210

NetStat	211
ARP	212
Ping	213
FTP (File Transfer Protocol)	214
TraceRT (Trace Route)	215
Telnet	216
Como usar Telnet num computador com Windows	216
Telnet em Visual Basic	218
Fonte em Visual Basic do Servidor Telnet	219
10. ATAQUES D.O.S (DENIAL OF SERVICE)	223
Ataque OOB	223
Ataques Teardrop I, II, Newtear, Bonk, Boink	223
Land Attack	224
Ataque Smurf	228
SYN Flooder	231
11. IRC	239
O que é o IRC?	239
Mais um pouco de IRC	240
Quem são os OPs?	241
Principais comandos	241
Como funciona?	243
Noções gerais	243
Termos mais utilizados no IRC	246
Comandos básicos	251
Comandos avançados	252
Noções aprofundadas	254
O Bot	256
Modos de um canal	258
Configurando os modos de um canal	258
Modos do utilizador	259
Configurando os modos de um utilizador:	259
O Hacker no IRC	259
Take Over	259
Guerra Básica	260
Flood	260
Colisão de Nicks	261
Tomar Canais	261
Flood no Canal	261
Netsplit	262
Pedindo ao OP	262
Guerra Avançada	263
Nuke	263
Bombas ICMP	263
Botnet/Floodnet	264
12. HACKEANDO O PC	265
Password da BIOS	265
Password do Windows	265
Password do screen saver do Windows	266
Crackeando as Passwords do NT	266

13. AS FIREWALLS	273
O que são?	273
Componentes de uma firewall	274
Como proteger o servidor Web com uma Firewall	274
Firewalls e a Política de Segurança	275
Packet Filters	276
Regras de filtragem em screening router	279
Operações de Packet Filter	280
Vantagens	281
Desvantagens	281
Acções Screening Router	281
Riscos na filtragem	282
Múltiplos routers	283
Bastion host	284
Tipos Especiais	285
Criando um Bastion host	286
Proxy Systems	287
Funcionamento do Proxy Server	288
Vantagens e Desvantagens	290
Vantagens	290
Desvantagens	290
Screened Host	291
Screened Subnet	292
Estratégias de Segurança	294
Criando uma screened subnet	295
Tipos de Firewall	296
Arquitectura firewall baseada em proxy	296
Arquitectura baseada em Firewall central	297
Uma visão geral dos firewalls pessoais	297
Introdução	297
Personal firewalls	298
Opções disponíveis	298
Aplicações freeware	299
ZoneAlarm	299
Tiny Personal Firewall	304
Sygate Personal Firewall	308
Aplicações comerciais	316
Norton Personal Firewall	316
Blacklce	320
Pontos positivos e negativos	324
Tiny Personal Firewall	325
Sygate Personal Firewall	325
Norton Personal Firewall	325
Blacklce Defender	326
Escolhendo o Personal Firewall mais adequado	326
Recomendações	327
Problemas com Personal Firewalls	328

14. FERRAMENTAS DE IDS-INTRUSION DETECTION SYSTEM	329
Introdução	329
O Sistema de Defesa dos Humanos e as Ferramentas de IDS	329

Intrusão: O que vem a ser?	332
O Intruso	332
A Classificação das Intrusões	332
A Detecção de uma Intrusão	334
A Anatomia de uma Ferramenta de IDS	335
O Modelo Conceptual de uma Ferramenta de IDS	335
O Gerador de Eventos - (E-box)	336
O Analisador de Eventos - (A-box)	336
A Base de Dados de Eventos - (D-box)	336
A Unidade de Resposta - (R-box)	336
A Comunicação entre Componentes	336
15. ROUTERS	337
Introdução	337
Os Três As (AAA)	337
Componentes Básicos do Hardware	338
O Processo de Inicialização do Router	340
O Fluxo dos Dados	342
Controle do Tráfego com ACL	344
Como Funciona a ACL	345
O Fluxo dos Pacotes através das Listas de Acesso	345
Tipos de Listas de Acesso	347
Identificando as Listas de Acesso	348
Implementando ACL	349
O funcionamento dos wildcards em routers Cisco	349
Como configurar routers Cyclades para bloquear Spam	353
Como configurar Routers Cisco para bloquear Spam	358
Como configurar o Exchange para bloquear Spam	359
16. SNIFFERS	363
O que é um Sniffer?	363
Como detectar um ataque de um sniffer?	363
Exemplo de um Port Sniffer em Visual Basic	364
O código fonte do Sniffer em Visual Basic	364
17. SSL - SECURE SOCKET LAYER	367
Criptografia SSL	367
Serviços SSL	368
18. TÉCNICAS DE ATAQUE	369
O que é um Script Kiddie?	370
Ameaça	370
Metodologia	371
Ferramentas	372
Criando um Port Scanner (em Delphi)	373
Como se proteger?	376
19. TÉCNICAS DOS CRACKERS PARA INVASÃO DE REDES	377
Vulnerabilidade	377
Perfil de um Cracker	378
Formas de conexão mais adoptadas	378

Entendendo as vulnerabilidades das redes	379
Técnicas usadas pelos invasores para ocultar a sua localização	380
Recolha de informações	381
Identificando componentes de rede confiáveis	382
Identificando componentes vulneráveis de uma rede	382
Tirando vantagem dos componentes vulneráveis de uma rede	384
Quando o acesso a componentes vulneráveis da rede é obtido	385
Fazendo a transferência de informações sigilosas	386
Explorando outros hosts e redes confiáveis	386
Instalando farejadores	386
Tomando conta de redes	388
Como os Hackers/Crackers invadem uma rede dial-up	388
Falhas mais comuns	390
20. COOKIES	393
O que são os Cookies?	393
O perigo dos Cookies	393
Solução	393
21. ICQ	395
Invadindo o ICQ	395
1º Passo - Como se ligar à máquina	395
2º Passo - Leitura e gravação de um ficheiro (exemplo: win.ini)	395
3º Passo - Como 'roubar' as palavras-chave desses utilizadores	396
Segurança no ICQ	397
Principais problemas com o ICQ	397
Utilização de versão desactualizada	397
Comportamento do utilizador	397
Receber um pedido de inclusão de alguém desconhecido	398
Receber correntes e boatos (hoaxes) de algum utilizador da lista de contactos	398
Tentativa de enviar um ficheiro	398
Existência de versões novas do ICQ	398
Ataques locais	399
Ataque contra a <i>password</i> do utilizador	399
Acesso ou cópia da lista de contactos ou históricos de conversas do utilizador	399
Acesso à <i>password</i> do correio-electrónico	400
Ataques remotos	400
Inundação (flood) de mensagens	400
Ser adicionado sem autorização	400
Spoofing de mensagens	401
Detectar a presença de alguém em modo invisível	401
Parar o ICQ	401
Enviar ficheiros falsos	402
Configuração segura do ICQ	402
Configurações básicas	403
Configuração do menu Security & Privacy	406
Configuração do menu Connections	409
Aplicações para ICQ	410
22. NUKES E TROJANS	413
Nukes	413
História	413
Como utilizar um Nuke	414

OOB bug (o bug da porta 139)	415
Pinga Bom	415
Um pouco mais sobre o Ping	415
WinNuke	416
Fonte do WinNuke	416
Nukando IPs	417
Descobrimdo o IP/HOST de um fornecedor	418
Protegendo-se de nukes	419
Trojan Horse ou Cavalo de Tróia	419
Principais Trojans	420
BACK ORIFICE (BO)	420
O Protocolo do Back Orifice (BO)	421
Formato dos Pacotes	421
Operações do BO	422
O que é o NETBUS	427
1º - Enviar o <i>patch</i> cliente para a vítima	428
2º - Depois de instalado, fazer a ligação	428
Comandos do NetBus	428
Novidades do NetBus 2.0	430
Facilidades para iniciantes	430
Múltiplos gestores	431
Informações do sistema e lista de palavras-chave	431
Identificação e limpeza do sistema	431
IP Spoofing	432
Como é um ataque IP Spoofing?	433
Protecção com palavras-chave	434
Como se prevenir?	434
23. BACKDOORS	435
O que são realmente as Backdoors?	435
O que são Sockets de Troie?	436
Como limpar o Back Oriffice e as Backdoors?	436
Detalhes do funcionamento do programa	437
Um pouco mais sobre Backdoors	445
Trojan do ICKILLER	446
Trojan de Games	446
Verificação da ocupação de portas TCP e UDP	447
Verificar a conexão da Internet	449
Desligar todas as conexões da Internet activas	450
24. PREVENINDO-SE DAS INVASÕES	453
Principais Problemas	454
Acessos indevidos, internos e externos	454
Vulnerabilidade do software	456
Utilizadores sem conhecimentos necessários	457
Vírus de computador	457
Ataques de Hackers, ex-funcionários ou funcionários insatisfeitos	458
O problema dos utilizadores não se preocuparem com a segurança	459
Plano de continuidade de negócios inexistente ou nunca testado	460
Não existência de cópias de segurança das informações	461
Uso de notebooks	461
Pirataria	462

Detectando o problema	462
Eliminando o problema	464
Medidas de Segurança	465
Controlo de acessos	465
Política de segurança	467
Auditorias permanentes	469
Política de backup's	470
Formação e disseminação do conhecimento	472
Actualização e legalização do software	473
Actualização dos antivírus	474
Plano de continuidade do negócio	474
Firewall	475
Segurança na Sala dos Servidores	476
25. BRECHAS DE SEGURANÇA	477
EM BASES DE DADOS	477
Palavras-chave Universais/Genéricas no Paradox	477
26. CRIPTOGRAFIA	479
Algoritmos Criptográficos	480
Esquemas Simétricos	481
Esquemas Criptográficos Assimétricos	481
Autenticação de Esquemas Assimétricos	482
Protocolo Desafio	483
Certificação dos Utilizadores	483
Assinatura Digital + Certificado	484
Esquema Híbrido (RSA + simétrico)	484
Autenticação da identidade de ambos os lados usando assinaturas digitais RSA e certificados	484
SET - Secure Electronic Transaction	484
SSL - Secure Sockets Layer	485
Complementação ao nível das Aplicações	485
VPN - Virtual Private Networks	486
Tipos de Ataque	486
1. Ataque do texto cifrado (Cyphrtext-Only)	486
2. Ataque do texto conhecido (Known-Plaintext)	486
3. Ataque adaptativo do texto escolhido (Adaptative-Choosen-Plaintext)	486
4. Ataque do texto cifrado escolhido (Choosen-Ciphertext)	487
5. Ataque de chave escolhida (Choosen-Key)	487
Métodos da criptografia tradicional	487
Usando Cifras de Substituição	487
Cifras de Transposição	488
Códigos e Máquinas de Cifragem	488
Criptografia Computacional de Chave Única	488
Modo do Livro de Códigos (Electronic Code Book - ECB)	489
Modo de Encadeamento de Blocos (Cipher Block Chaining - CBC)	490
Modo de Realimentação de Cifra (Cipher Feedback - CFB)	490
Modo de Encadeamento de Blocos (Block Chaining)	490
Modo de Encadeamento Propagado (Propagating Cipher Block Chaining-PCBC) ..	490
Código simples de criptografia de dados em Pascal	490
Código simples de criptografia de dados em C	492
Segurança no e-mail	494
Chave Privada e Chave Pública	495

27. NAVEGANDO ANONIMAMENTE	497
Ser anónimo na Internet	497
Como descobrir o IP - em Delphi	500
28. WINDOWS 2000	503
TCP/IP com Windows 2000	503
Histórico	503
Classes de endereços	503
Máscara da rede	504
Endereçamento	504
Estático	504
Dinâmico (DHCP)	504
Vantagens do DHCP	504
Vantagens do WINS	504
Vantagens do DNS	505
Definição de Windows DNA	505
Papel da camada de apresentação	505
Papel da camada de Lógica de Negócio	506
Papel da camada de acesso a dados	506
Principais benefícios do Windows DNA	506
Confiabilidade do Windows DNA	506
29. PROTEGENDO O WINDOWS 2000 – BACKDOORS.....	507
O básico	507
As dicas	509
TCP/IP	509
Contas	510
Serviços	511
Teste a sua segurança	512
Patches	514
O bom e velho firewall	515
Spywares	516
30. IMPLEMENTANDO PROTECÇÕES CONTRA DESASTRES NO WINDOWS 2000	519
Visão Geral	519
Características da protecção contra desastres no Windows 2000	519
Usando volumes tolerantes a erros	520
Implementando volumes tolerantes a erros	520
Recuperar um volume de espelho que falha	521
Recuperando um volume de espelho com um disco identificado como Offline ou Perdido	521
Recuperando um volume de espelho com um disco id.como Online (Erros)	522
Substituir um disco e criar um novo volume espelho	522
Recuperar um volume RAID-5 falhado	522
Recuperar um RAID-5 com o identificador em Offline ou Perdido	522
Recuperando um RAID-5 com o identificador em Online (Erros)	523
Substituir um disco e voltar a gerar o volume RAID-5	523
Examinar as opções avançadas de inicialização	523
Examinar a consola de recuperação	524
Usar o BackUp	526
BackUp de ficheiros e pastas	526

BIBLIOGRAFIA

527

ANEXO 1

CORTAR A CONEXÃO DE UM INTERNAUTA COM WINDOWS 95/98
E NT4/2000 529

ANEXO 2

IMPEDIR A LIGAÇÃO DE UM INTERNAUTA COM WINDOWS 95/98/
ME/NT4/2000 535

ANEXO 3

COMO É QUE OS *HACKERS* CONSEGUEM CONGELAR A MÁQUINA
DE UM INTERNAUTA COM WINDOWS NT4/2000? 541

ANEXO 4

PARAR UM SERVIDOR WEB 545

ANEXO 5

ALTERAR UM *SITE* 549

ANEXO 6

COMO OBTER O CÓDIGO ASP DE *SITES* NA WEB? 553

ANEXO 7

ACESSO *ROOT* NO LINUX 557

ANEXO 8

CONSEGUIR *PASSWORDS* DE UTILIZADORES NO LINUX 569

ANEXO 9	
DESCOBRIR VULNERABILIDADES EM SERVIDORES	581
ANEXO 10	
DESCOBRIR <i>PASSWORDS</i> DE PARTILHAS DO WIN 95/98/ME .	591
ANEXO 11	
PARAR O PERSONAL WEB SERVER	597
ANEXO 12	
OBTER DIREITOS DE ADMINISTRADOR NO WINDOWS 2000 SERVER	601
ANEXO 13	
COMO PROTEGER O WINDOWS NT4/2000	603

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.

Spoofting

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.

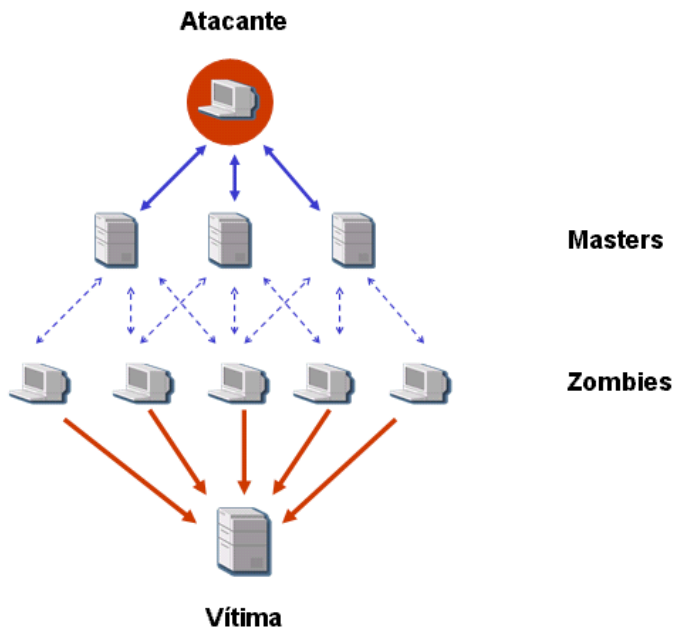
Este tipo de ataque não causa perda ou roubo de informações, mas é um ataque preocupante, pois os serviços do sistema atacado ficarão indisponíveis por um tempo indeterminado. Dependendo da equipa existente na empresa para o disponibilizar novamente e dependendo do negócio da empresa, este tempo de indisponibilidade 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-check*, 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 interceptação 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 entrar 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, dnsskiller, 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: