

Copyright©2002 da Novatec Editora Ltda.

Todos os direitos reservados. É proibida a reprodução desta obra, mesmo parcial, por qualquer processo, sem prévia autorização, por escrito, do autor e da Editora.

ISBN: 85-7522-015-2

Novatec Editora Ltda.
Rua Cons. Moreira de Barros 1084 Conj. 01
02018-012 São Paulo - SP Brasil
Tel.: (0xx11) 6959-6529
Fax: (0xx11) 6950-8869
E-mail: novatec@novateceditora.com.br
Site: www.novateceditora.com.br

Sumário

Agradecimentos	9
Apresentação	11
Parte 1 Técnicas e ferramentas de ataque	13
1 Entrando no porão	15
O termo "hacker"	16
Dialeτισmos	18
Facções	19
Grupos e zines	21
Portais de segurança	22
Motivação e ferramentas	23
2 Ataques não-técnicos	25
Engenharia social	26
Segurança física	27
3 Ataques remotos	29
Análise do ambiente alvo	30
Mapeamento de redes	32
Ping	32
Traceroute	39
Strobe	40
Banners	41
Transferência de zona	43
Compartilhamento remoto de discos e partições	45
Showmount (Unix)	45
net (Windows)	46
SNMP - Simple Network Management Protocol	48
Mapeamento remoto moderno	52
QueSO	52
Nmap (Network Mapper)	54
Xprobe	59
SATAN (Security Administrator's Tool for Analyzing Networks)	60
Nessus	62
Ncat	65
Nêmesis	67
Ataques por procuração	69
Ataque em camadas	71
Tunelamento	72
Cavalos de tróia e portas dos fundos	75
Ataques a serviços	78
Servidores Web	78
Interface com bases de dados	83
Telnet	84

Seqüestro de sessão	85
Estouro de pilha (buffer overflow)	86
FTP	88
IMAP e POP3	89
RPC - Remote Procedure Call	90
Mapeamento passivo	91
POf (Passive OS Fingerprinting)	91
Ping	93
Coleta de informação em aplicações	98
Negação de serviço (Denial of Service)	99
4 Fraudes e falsificações (spoofing)	101
E-mail	102
Web	105
DNS	107
ICMP	110
UDP	112
TCP	113
5 Ataques locais	115
Analisadores de tráfego (Sniffer)	116
Contaminação de ARP e MAC	117
Como é possível forjar um endereço MAC?	117
Proxy ARP	118
Smit	118
Ataque do tipo homem no meio (man in the middle)	119
Quebra de senha (cracking)	120
Bibliotecas (Libs)	122
Rootkit (Unix e NT/W2k)	124
Módulos de kernel	129
Parte 2 Técnicas e ferramentas de defesa	131
6 Mitos	133
"Firewall é indispensável em redes ligadas à Internet"	134
"Senhas tem que ser trocadas regularmente"	135
"Firewal é para Internet, não faz sentido em redes locais"	136
"Para saber defender é preciso saber atacar"	137
Certificações	139
7 Lista de itens de segurança para servidores Web	143
Vulnerabilidades	144
Recomendações específicas para servidores Microsoft IIS	146
Atualização e publicação das páginas	153
8 Atualizações e correções	155
Perfil dos administradores	156
9 Vírus	159
Propagação	160
10 Códigos seguros	163
Estouro de pilha	164
Limites	165
Teste de parâmetros	166

11	Segurança dos hosts	167
	Serviços	168
	Sistemas de arquivos (File System)	170
	Criação de partições	170
12	Segurança em rede	173
	Formas de autenticação	174
	SKey/Opie	174
	Criptografia	179
	Chaves	179
	SSH	181
	Autenticação	181
	Método nome e senha	183
	Método chaves públicas	188
	Método chaves públicas + passprhase	188
	SSL/TLS	190
	Cartões inteligentes e biometria	202
13	Firewall	203
	Filtros de pacote	204
	Procurador (proxy) de aplicação	208
14	Detectores de intrusão	211
	Verificadores de integridade	212
	Analisadores pós-invasão	215
	Detectores de intrusos baseado em host	220
	Detectores de intrusos em rede (Network Intrusion Detection System - NIDS)	222
	Limitações	222
	Tcpdump	223
	Ngrep	225
	Snort	227
	Criação de regras	232
	Envio de alertas	232
	Detectores passivos X ativos	233
	Análise de logs	234
	Aquários ou potes de mel (honey pots)	236
15	Incidentes	237
	Critérios para caracterizar incidentes	238
	Por que relatar um incidente	239
	A quem reportar incidentes de segurança?	240
	Que informações devem constar em uma notificação de incidente?	241
	Como identificar o responsável por determinado domínio?	242
	Índice Remissivo	244