

Marcos Flávio Araújo Assunção

Segredos do Hacker Ético

2ª Edição

Visual **Books**

Sumário

Prefácio	21
Introdução	23
1 Entendendo o Assunto	25
1.1 Bem-vindo ao Obscuro Mundo da Segurança Digital	25
1.2 Por que a Insegurança Existe?	27
1.3 Breve História do Hacking	29
1.4 Que Termo é Este?	30
1.5 Divisão do Livro	32
2 TCP/IP Básico	35
2.1 TCP/IP	35
2.2 Camada de Aplicação	35
2.2.1 Protocolos	36
2.2.1.1 SMTP	36
2.2.1.2 POP	36
2.2.1.3 FTP	36
2.2.1.4 HTTP	36
2.2.1.5 SNMP	37
2.2.1.6 DNS	37
2.2.1.7 Telnet	38
2.2.1.8 SSL	38
2.2.1.9 SSh	38
2.2.2 Comandos	39
2.2.2.1 FTP	39
2.2.2.2 Telnet	42
2.3 Camada de Transporte	43
2.3.1 Protocolos	43

2.3.1.1 TCP	43
2.3.1.2 UDP	43
2.3.1.3 Portas	44
2.3.2 Comandos	46
2.3.2.1 Netstat	46
2.4 Camada de Internet	47
2.4.1 Protocolos	47
2.4.1.1 IP	47
2.4.1.2 ICMP	48
2.4.1.3 ARP	48
2.4.2 Comandos	49
2.4.2.1 ARP	49
2.4.2.2 Ipconfig	50
2.4.2.3 Ping	51
2.4.2.4 Tracert	52
2.4.3 Camada de Rede	53
2.5 Tipos de Transmissão de Dados	53
2.5.1 Unicast	53
2.5.2 Broadcast	53
2.5.3 Multicast	53
3 Organizando o Penetration Test	55
3.1 Partindo do Zero	55
3.2 FootPrinting	56
3.3 Varredura	57
3.4 Enumeração	57
3.5 Procura por Falhas e Problemas	57
3.6 Métodos de Burlar a Proteção	57
3.7 Engenharia Social	58
3.8 Explorando Falhas	58
3.9 Explorando Má Configuração	58
3.10 Recusa de Serviço	58
3.11 Segurança	59

4 Footprinting	61
4.1 Pesquisa Manual	61
4.2 Pesquisa Automatizada	62
4.3 Google	62
4.3.1 Considerações Importantes	63
4.3.2 Alguns Comandos do Google	63
4.4 Softwares	67
4.4.1 Windows	67
4.4.2 Linux	67
4.5 Solução	67
5 Varredura	69
5.1 Descobrimo Computadores na Rede	69
5.1.1 Ping 200.195.16.1	70
5.2 Descobrimo Portas Abertas nos Computadores	70
5.2.1 Tipos de Scanneamento	71
5.3 Softwares	74
5.3.1 Windows	74
5.3.2 Linux	74
5.4 Solução	75
6 Enumeração	77
6.1 Descoberta do Sistema Operacional	77
6.1.1 Pesquisar Páginas não Indexadas	77
6.1.2 Fingerprint	78
6.2 Enumeração dos Serviços	78
6.2.1 Leitura de Banners	78
6.3 Enumeração de Usuários	79
6.3.1 Usuários pelo SMTP	79
6.3.2 Usuários por Sessão Nula	81
6.3.2.1 NTInfoScan	81
6.3.2.2 Netbios Enumeration Utility	82
6.4 Softwares	83

6.4.1 Windows	83
6.4.2 Linux	84
6.5 Solução	84
7 Falhas e Problemas	85
7.1 Buffer Overflow	86
7.2 Race Conditions	86
7.3 SQL Injection	87
7.4 PHP Injection	88
7.5 Cross Site Scripting	89
7.6 Pesquisa Manual	90
7.7 Pesquisa Automatizada	95
7.7.1 Languard	95
7.7.2 Shadow Security Scanner	96
7.7.3 Syhunt TrustSight	97
7.7.4 Nessus	98
7.8 Softwares	103
7.8.1 Windows	103
7.8.2 Linux	104
7.9 Solução	104
8 Burlando Proteções	105
8.1 Burlando o Antivírus	105
8.1.1 Alteração em Hexadecimal	106
8.1.2 Apagando Recursos do Executável	107
8.1.3 Compressão de Executáveis	108
8.1.4 Alternate Data Streams	111
8.2 Burlando o Firewall	112
8.2.1 Servidores Proxy	113
8.2.2 Spoofing	115
8.2.3 IP Spoofing Não-cego	115
8.2.4 IP Spoofing Cego	116
8.2.5 Stern	116

8.2.6 Netwox	118
8.2.7 DNS Spoofing	119
8.2.8 Conexão Reversa	120
8.2.9 Tunneling	126
8.2.9.1 WWW_Shell_Reverso	128
8.3 Burlando o IDS	129
8.3.1 Combinando Métodos	131
8.3.2 Codificação de URL	131
8.3.3 Barras Duplas e Triplas	132
8.3.4 Travessia de Diretórios	132
8.3.5 Diretórios com Auto-referência	132
8.4 Softwares	133
8.4.1 Windows	133
8.4.2 Linux	134
8.5 Solução	134
8.5.1 Burlar o Antivírus	134
8.5.2 Burlar o Firewall	134
8.5.3 Burlar o IDS	135

9 Engenharia Social 137

9.1 Manipulando os Sentimentos	138
9.1.1 Curiosidade	138
9.1.2 Confiança	139
9.1.3 Simpatia	140
9.1.4 Culpa	142
9.1.5 Medo	143
9.2 Como Lidar com Diferentes Pessoas	144
9.3 Dicas de um Engenheiro Social Anônimo	146
9.4 Truques Aplicados na Informática	146
9.4.1 E-mail Phishing	147
9.4.2 E-mail Falso	149
9.4.3 Messengers Instantâneos	152
9.5 Solução	152

10 Malware	153
10.1 Backdoors	153
10.1.1 Backdoor Simples	153
10.1.2 Backdoor de Login	153
10.1.3 Backdoor de Telnet	154
10.1.4 Backdoor com Protocolos Incomuns	154
10.1.5 Backdoor de Serviço	154
10.1.6 Rootkit	155
10.2 Cavalos de Tróia	155
10.2.1 Diferenças	156
10.2.1.1 Trojans Comuns	156
10.2.1.2 Trojans Webdownloaders	157
10.2.1.3 Trojans de Notificação	157
10.2.1.4 Trojans Comerciais	158
10.2.2 Joiners	158
10.2.3 Identificando o Endereço IP do Alvo	160
10.2.4 Maneiras de se Iniciar um Trojan	162
10.2.4.1 Pasta Auto-iniciar	162
10.2.4.2 Win.ini	163
10.2.4.3 System.ini	163
10.2.4.4 C:\windows\winstart.bat	163
10.2.4.5 Registro	163
10.2.4.6 C:\windows\wininit.ini	164
10.2.4.7 Autoexec.bat	164
10.2.4.8 Shell no Registro	164
10.2.4.9 ICQ Inet	165
10.2.4.10 Explorer	165
10.2.4.11 Componente Active-X	165
10.2.4.12 Informação Interessante	165
10.2.5 Beast	166
10.2.5.1 Server Settings	166

10.2.5.2	Notifications	167
10.2.5.3	Startup	167
10.2.5.4	Antivírus-Firewall Kill	168
10.2.5.5	Misc	169
10.2.5.6	ExeIcon	169
10.3	Keyloggers	171
10.3.1	Keyloggers Locais	171
10.3.2	Keyloggers Remotos	172
10.4	Screenloggers	173
10.5	Softwares	175
10.5.1	Windows	175
10.5.2	Linux	175
10.6	Solução	175
11	Explorando Falhas	177
11.1	Explorando Injection	177
11.1.1	Introdução	177
11.1.2	Obtendo Informações de Mensagens de Erro	179
11.1.3	Limites de Tamanho	181
11.1.4	Outras Strings	182
11.2	Explorando CSS	182
11.3	Exploits	184
11.3.1	Payloads	184
11.3.2	Encontrando Exploits na Web	185
11.3.3	Executando os Exploits	187
11.3.4	Multiexploradores	188
11.3.4.1	Core Impact	188
11.3.4.2	Metasploit	189
11.3.4.3	Selecionando o Exploit no Metasploit	192
11.3.4.4	Selecionando o Payload	194
11.3.4.5	Configurando os Parâmetros para o Payload	195
11.3.4.6	Finalmente - Explorando com Metasploit	196

11.3.4.7 BackTrack	197
11.4 Softwares	198
11.4.1 Windows	198
11.4.2 Linux	198
11.5 Solução	198
12 Má Configuração e Senhas	201
12.1 Introdução às Senhas	201
12.1.1 Senhas Fáceis	201
12.1.2 Senhas Padrões	202
12.2 Descobrindo Senhas	207
12.3 Força-bruta Remota	208
12.3.1 Authentication Options (Opções de Autenticação)	211
12.4 Força-bruta Local	213
12.5 Rainbow Tables	216
12.6 Sniffers	217
12.7 Farejando Redes Wireless (802.11)	220
12.8 Man in the Middle	221
12.8.1 Man in the Middle Remoto	223
12.8.2 Man in the Middle Local	226
12.9 Outras Técnicas de Senhas	226
12.10 Netbios	228
12.11 Softwares	230
12.11.1 Windows	230
12.11.2 Linux	230
12.12 Solução	230
13 Denial of Service	233
13.1 DoS através de Falhas	233
13.2 Ataques Comuns	234
13.3 DDoS	235
13.4 Software	235
13.5 Solução	235

14 Segurança	237
14.1 Dicas Básicas	237
14.2 Firewall	238
14.3 IDS	241
14.4 Honeypots	242
14.5 Monitoradores do Sistema	245
14.5.1 Monitorador de Registro	246
14.5.2 Monitorador de Arquivos	246
14.6 Limpeza de Rastros	247
14.7 Checksums	248
14.8 Softwares	248
14.8.1 Windows	248
14.8.2 Linux	249