

Introdução ao **PENTEST**

Daniel Moreno

© Novatec Editora Ltda. 2015.

Todos os direitos reservados e protegidos pela Lei 9610 de 19/02/1998. É proibida a reprodução desta obra, mesmo parcial, por qualquer processo, sem prévia autorização, por escrito, do autor e da Editora.

Editor: Rubens Prates

Assistente editorial: Priscila A. Yoshimatsu

Editoração eletrônica: Carolina Kuwabata

Revisão gramatical: Mari Kumagai

Capa: Carolina Kuwabata

ISBN: 978-85-7522-431-1

Histórico de impressões:

Maio/2015 Primeira edição

Novatec Editora Ltda.

Rua Luís Antônio dos Santos 110

02460-000 – São Paulo, SP – Brasil

Tel.: +55 11 2959-6529

Email: novatec@novatec.com.br

Site: www.novatec.com.br

Twitter: twitter.com/novateceditora

Facebook: facebook.com/novatec

LinkedIn: linkedin.com/in/novatec

Sumário

Agradecimentos	13
Sobre o autor	14
Prefácio	15
Capítulo 1 ■ Introdução à segurança da informação e ao Kali Linux	17
1.1 Princípios de segurança da informação e proteção de dados	17
1.2 Conhecendo o Kali Linux	20
Capítulo 2 ■ Preparando o ambiente de teste	22
2.1 Recursos necessários	22
2.2 Obtendo o Kali Linux	23
2.2.1 Instalação do VirtualBox	24
2.2.2 Instalação de uma máquina virtual	28
2.3 Configurando a rede no Kali Linux	44
2.4 Terminal de comandos	45
2.5 Atualizando o Kali Linux	46
2.6 Instalação do Debian	46
2.7 Backup da máquina virtual	47
Capítulo 3 ■ Pentest	51
3.1 O que é pentest?	51
3.2 Porque realizá-lo?	52
3.3 Tipos de pentest	52
3.3.1 Black-box	53
3.3.2 White-box	53
3.3.3 Gray-box	54
3.4 Análise de vulnerabilidade	55
3.5 Metodologias de pentest	56
3.5.1 Metodologia ISSAF	56
3.5.2 Metodologia OWASP	57
3.5.3 Metodologia OSSTMM	58
3.5.4 Metodologia Backtrack	59

Capítulo 4 = Planejamento do projeto	61
4.1 Informações gerais	61
4.2 Objetivo do pentest	62
4.3 Limitações	62
4.4 Contrato de acordo.....	63
4.5 Linha do tempo	64
 Capítulo 5 = Footprinting.....	 65
5.1 DNS	68
5.1.1 Tipos de registro DNS	70
5.2 Laboratório – Enumeração DNS	72
5.3 Programas para enumeração DNS	76
5.3.1 DNSenum.....	76
5.3.2 DNSmap	80
5.3.3 DNSrecon.....	81
5.3.4 Fierce	82
5.4 Coleta de email.....	84
5.5 Firewall iptables	85
5.5.1 Comandos para gerenciamento do iptables.....	86
5.6 Informações de rota	88
5.6.1 Traceroute	89
5.6.2 TCPtraceroute	90
 Capítulo 6 = Fingerprinting.....	 92
6.1 Fingerprinting passivo	92
6.1.1 P0f.....	92
6.2 Fingerprinting ativo	93
6.2.1 Ping.....	93
6.2.2 Fping.....	95
6.2.3 Arping	95
6.2.4 Netdiscover	96
6.2.5 Hping3	96
6.2.6 Xprobe2.....	100
6.2.7 Maltego.....	100
 Capítulo 7 = Enumeração.....	 110
7.1 Modelo OSI	110
7.2 Protocolo TCP/IP	112
7.3 Port scanner	115
7.3.1 Nmap	116
7.4 O canivete suíço Netcat	121
7.4.1 Laboratório Netcat	122

7.5 Enumeração SMTP	125
7.5.1 Laboratório email.....	125
7.5.2 STMPUser enum	127
7.5.3 Como enviar emails falsos (via PHP)	127
7.5.4 Como enviar emails falsos (via Open Relay)	129
7.6 Enumeração SNMP	130
7.6.1 SNMPcheck	131
7.6.2 OneSixtyOne	131
Capítulo 8 = Mapeamento de vulnerabilidades.....	132
8.1 Tipos de vulnerabilidades.....	132
8.1.1 Vulnerabilidade local.....	132
8.1.2 Vulnerabilidade remota.....	134
8.2 Scanners de vulnerabilidade	134
8.2.1 OpenVAS.....	134
8.2.2 Nessus	144
Capítulo 9 = Exploração do alvo	148
9.1 Metasploit	149
9.1.1 Msfconsole	150
9.1.2 Comandos básicos	150
9.2 A vulnerabilidade MS12-020-maxchannelids.....	151
9.3 Explorando Windows vulnerável	152
9.4 Payload Meterpreter.....	154
9.4.1 Core commands	154
9.4.2 File system commands	155
9.4.3 Networking commands.....	156
9.4.4 System commands.....	156
9.4.5 User Interface commands.....	158
9.5 Pivoting com Metasploit	159
9.6 VPN Pivoting (Pivoting via Layer 2)	161
9.7 Vulnerabilidade shellshock.....	167
9.8 Explorando servidores NFS mal configurados.....	169
9.9 Explorando X Window System	171
Capítulo 10 = Engenharia social	174
10.1 Processo de ataque	175
10.2 Tipos de engenharia social	175
10.3 SET (Social Engineering Toolkit)	176
10.4 Office 2010 pptimpcnv DLL hijacking.....	184
10.5 Macros maliciosas.....	186
10.6 Internet Explorer ms10_046.....	188

10.7 Internet Explorer < 11 – OLE Automation Array Remote Code Execution...	188
10.8 Firefox Add-on	189
10.9 Unixitrix Exploit	189
10.10 BadUSB	190
10.10.1 Laboratório BadUSB	191

Capítulo 11 – Escalonamento de privilégios195

11.1 Escalonamento de privilégios offline	195
11.1.1 Common User Passwords Profiler	196
11.2 Escalonamento de privilégios online	203
11.2.1 Cewl	204
11.2.2 xHydra	204
11.2.3 Hydra	206
11.3 Sniffers.....	207
11.3.1 Sniffer tcpdump.....	208
11.3.2 Sniffer Wireshark.....	210
11.4 Ataques Man-in-the-Middle (MitM)	214
11.4.1 ARP Spoofing	214
11.4.2 Arpspoof.....	218
11.4.3 Nping	219
11.4.4 DNS Spoofing	219
11.4.5 Dnsspoof	220
11.4.6 SSLStrip	221
11.4.7 SSLSplit.....	221
11.4.8 Ataque SSLStrip, DNS Spoofing e Java Applet.....	222
11.4.9 Bloqueando o Arp Spoofing.....	224

Capítulo 12 – Manutenção do acesso.....226

12.1 Backdoors	226
12.1.1 Backdoors de conexão direta	227
12.1.2 Backdoors de conexão reversa	227
12.2 Backdoor sbd.....	229
12.2 Cavalos de Troia.....	230
12.3 EXE Joiner.....	230
12.4 Bypass A.V.....	235
12.4.1 Compressores de arquivos.....	235
12.4.2 Crypters/Encoders	235
12.4.3 Veil-Framework.....	236
12.5 Keylogger.....	237
12.6 Honey pots.....	238
12.6.1 Valhala Honey pot	240
12.6.2 Honeyd	241

12.7 Rootkits.....	244
12.7.1 Userland.....	244
12.7.2 Kernel Land	247
Capítulo 13 = Apagando rastros	248
Capítulo 14 = Tunneling.....	250
14.1 Laboratório Tunneling.....	251
14.2 SSH Tunneling.....	252
14.3 UDP tunneling.....	253
14.4 DNS tunneling.....	254
14.5 ICMP Tunneling	256
14.6 Canais encobertos via tunneling	256
14.7 HTTP Tunnel.....	259
14.8 Redes TOR.....	260
Capítulo 15 = DoS – Denial of Service	262
15.1 SYN Flood	263
15.1.1 T50	263
15.2 Slowloris	264
15.3 DDoS (Distributed Denial Of Service).....	265
15.4 Projeto Perl-Bot	266
Capítulo 16 = Documentação técnica	268
16.1 Tipos de relatórios	268
16.1.1 Relatório Executivo	268
16.1.2 Relatório técnico	269
16.1.3 Relatório comercial.....	270
16.2 Criptografando relatórios com o Truecrypt	270
16.2.1 Criando um arquivo criptografado.....	270
16.2.2 Criando um pendrive criptografado	278
Capítulo 17 = Pentest em redes sem fio	280
Apêndice = Relatório de pentest	285
Referências	293