Introdução ao PENTEST

2ª Edição

Daniel Moreno

Novatec

São Paulo | 2019

Editor: Rubens Prates
Editoração eletrônica: Carolina Kuwabata
Revisão gramatical: Tássia Carvalho
Capa: Carolina Kuwabata

ISBN: 978-85-7522-807-4

Histórico de impressões:

Outubro/2019	Segunda edição
Junho/2017	Segunda reimpressão
Fevereiro/2016	Primeira reimpressão
Maio/2015	Primeira edição (ISBN: 978-85-7522-431-1)

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**

Isenção de responsabilidade **14**

Sobre o autor **15**

Prefácio da primeira edição **16**

Prefácio da segunda edição **17**

Capítulo 1 ▪ Introdução à segurança da informação e ao Kali Linux **18**

1.1 Princípios de segurança da informação e proteção de dados 18
1.2 Conhecendo o Kali Linux 21

Capítulo 2 ▪ Preparando o ambiente de teste **22**

2.1 Recursos necessários 22
2.2 Obtendo o Kali Linux 23
2.3 Instalação de uma máquina virtual 24
2.4 Configurando a rede no Kali Linux 38
2.5 Terminal de comandos 38
2.6 Atualizando o Kali Linux 39
2.7 Backup da máquina virtual 39

Capítulo 3 ▪ Pentest **43**

3.1 O que é o pentest? 43
3.2 Por que o realizar? 44
3.3 Tipos de pentest 44
    3.3.1 Black-box 44
    3.3.2 White-box 45
    3.3.3 Gray-box 46
3.4 Análise de vulnerabilidade 47
3.5 Metodologias de pentest 47
    3.5.1 Metodologia OSSTMM 48
    3.5.2 Metodologia ISSAF 49
    3.5.3 PTES 49
    3.5.4 Metodologia OWASP 49
    3.5.5 Metodologia Kali Linux 51

Capítulo 4 ▪ Planejamento do projeto 52
4.1 Informações gerais 52
4.2 Objetivo do pentest 53
4.3 Limitações 53
4.4 Contrato de acordo 54
4.5 Linha do tempo 55

Capítulo 5 ▪ Footprinting 56
5.1 DNS 60
5.1.1 Tipos de registro DNS 61
5.2 Configurando o bind9 62
5.3 Programas para enumeração DNS 71
5.3.1 DNSenum 71
5.3.2 DNSmap 74
5.3.3 DNSrecon 75
5.3.4 Fierce 76
5.3.5 Dig 76
5.4 Coleta de emails 78
5.5 Firewall iptables 78
5.5.1 Comandos para gerenciamento do iptables 79
5.6 Informações de rota 82
5.6.1 Traceroute 82
5.6.2 TCPtraceroute 83

Capítulo 6 ▪ Fingerprinting 86
6.1 Fingerprinting passivo 86
6.1.1 P0f 86
6.2 Fingerprinting ativo 87
6.2.1 Ping 87
6.2.2 Fping 89
6.2.3 Arping 89
6.2.4 Netdiscover 89
6.2.5 Hping3 90
6.2.6 Xprobe2 95
6.2.7 Enumeração e exploração de sessão nula 95
6.2.8 Maltego 95

Capítulo 7 ▪ Enumeração 102
7.1 Modelo OSI 102
7.2 Protocolo TCP/IP 103
7.3 Port scanner 107
7.3.1 Nmap 108

7.4 Canivete suíço Netcat 112
7.5 Configurando o postfix 115
7.5.1 Enumeração de usuários 120
7.5.2 Força bruta (SMTP) 121
7.5.3 Envio de emails falsos (Open Relay) 121
7.5.4 Envio de emails falsos (PHP) 124
7.6 Enumeração SNMP 125
7.6.1 SNMPcheck 125
7.6.2 OneSixtyOne 125
7.6.3 SNMPWalk 126
7.6.4 Medusa 126
7.6.5 Hydra 126
7.6.6 Nmap 126
7.6.7 Metasploit 126

Capítulo 8 ■ Mapeamento de vulnerabilidades 127

8.1 Tipos de vulnerabilidades 127
8.1.1 Vulnerabilidade local 127
8.1.2 Vulnerabilidade remota 128
8.2 Scanners de vulnerabilidade 128
8.2.1 OpenVAS 128
8.2.2 Nessus 137

Capítulo 9 ■ Exploração do alvo 142

9.1 Metasploit 142
9.1.1 Msfconsole 143
9.1.2 EasyFTP CWD Command Stack Buffer Overflow 146
9.1.3 Payload Meterpreter 148
9.2 Desenvolvimento de exploits 166
9.2.1 Desenvolvimento de shellcode 181
9.3 MS12-020 188
9.4 MS17-010 190
9.5 Shellshock 192
9.6 Explorando servidores NFS mal configurados 193
9.7 Explorando X Window System 196

Capítulo 10 ■ Engenharia social 198

10.1 Processo de ataque 198
10.2 Tipos de engenharia social 199
10.3 SET (Social Engineering Toolkit) 199
10.3.1 Java Applet Attack Method 200
10.3.2 Credential Harvester Attack Method 205

10.3.3 PowerShell Attack Vectors 207
10.4 Evasão da autenticação de dois fatores (2FA) 208
10.5 Office 2010 pptimpconv DLL hijacking 214
10.6 Macros maliciosas 215
10.7 DDE 217
10.8 MS14-064 218
10.9 Firefox Add-on 221
10.10 Unitrix Exploit 221
10.11 Acesso físico 222
10.11.1 Sethc 223
10.11.2 BadUSB 225
10.11.3 SSH reverso com Raspberry 228
10.12 Phishing local de usuários 231
10.13 Ofuscando IPs 232

Capítulo 11 ▪ Escalonamento de privilégios 233

11.1 Criação de lista de palavras (wordlist) 233
11.1.1 Common User Passwords Profiler 234
11.1.2 Crunch 235
11.1.3 Cewl 237
11.2 Escalonamento de privilégios vertical 237
11.2.1 Descoberta de senhas 253
11.3 Escalonamento de privilégios horizontal 257
11.3.1 Pivoting com Metasploit 257
11.3.2 xHydra 262
11.3.3 Hydra 265
11.3.4 Medusa 266
11.3.5 Sniffers 267
11.4 Bloqueando o Arp Spoofing 280

Capítulo 12 ▪ Manutenção do acesso 281

12.1 Backdoors 281
12.1.1 Backdoors de conexão direta 281
12.1.2 Backdoors de conexão reversa 282
12.1.3 Meterpreter RC4 284
12.1.4 Meterpreter HTTPS 285
12.1.5 Backdoor sbd 285
12.2 Cavalos de Troia 286
12.3 EXE Joiner 287
12.3.1 Iexpress 288
12.3.2 Winrar 290
12.4 Burlando antivírus (Bypass A.V) 293

12.4.1 Burlando antivírus com Python 294
12.4.2 Burlando antivírus com PowerShell 297
12.4.3 Burlando antivírus com C 306
12.4.4 Ofuscador de código-fonte Python 307
12.5 Conexão reversa com Pycat 310
12.6 Compilando scripts Python 313
12.7 Executando o Python via WebDAV no Windows 316
12.8 VNC oculto 319
12.9 Empire 321
12.10 Koadic 325
12.11 OpenSSL 329
12.12 Keylogger 330
12.13 Honeypots 332
12.13.1 Valhala Honeypot 333
12.14 Rootkits 334
12.14.1 Userland 334
12.14.2 Kernel Land 337

Capítulo 13 ▪ Apagando rastros 338

Capítulo 14 ▪ Tunneling 340

14.1 SSH Tunneling 342
14.2 UDP tunneling 343
14.3 DNS tunneling 343
14.4 ICMP Tunneling 344
14.5 Conexões encobertas via tunneling 346
14.6 HTTP Tunnel 347
14.7 Ngrok 348
14.8 Redes TOR 349

Capítulo 15 ▪ DoS – Denial of Service 350

15.1 Layer 7 350
15.2 Layer 4 351
15.2.1 Negação de serviço distribuída (DDoS) 352
15.3 Layer 2 356

Capítulo 16 ▪ Documentação técnica 357

16.1 Tipos de relatórios 357
16.1.1 Relatório Executivo 357
16.1.2 Relatório técnico 358
16.1.3 Relatório comercial 359

16.2 Criptografando relatórios com o Truecrypt 359
16.2.1 Criando um arquivo criptografado 359
16.2.2 Criando um pendrive criptografado 367

Apêndice ■ Relatório de pentest 370

1 Sumário executivo 370
2 Resultados 371
3 Narrativa do ataque 372
3.1 Vulnerabilidade na rede sem fio 372
3.2 Vulnerabilidades no Windows 7 373
4 Contramedidas 375
4.1 TP-LINK 375
4.2 Windows 7 375
5 Sobre o relatório final 376

Referências 377

Livros: 377