

Pentest em Redes Sem Fio

Daniel Moreno

© Novatec Editora Ltda. 2016.

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: Marcia Nunes

Capa: Carolina Kuwabata

ISBN: 978-85-7522-483-0

Histórico de impressões:

Março/2016 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 ■ Sobre o pentest	16
1.1 O que é o pentest?	16
1.2 A legislação brasileira e crimes digitais	18
1.3 Distribuições de pentest	18
Capítulo 2 ■ Preparando o ambiente de teste	20
2.1 Adaptador wireless	20
2.2 Antenas	23
2.3 Observações iniciais	25
2.3.1 Instalação do sistema operacional Kali Linux	26
2.3.2 Processos que interferem na suíte Aircrack-ng	26
2.3.3 Interface em modo monitor	28
2.3.4 Nomenclatura e padronização do texto	30
Capítulo 3 ■ Redes wireless	31
3.1 Padrão IEEE 802.11	32
3.1.1 Padrão 802.11	33
3.1.2 Padrão 802.11b	34
3.1.3 Padrão 802.11a	35
3.1.4 Padrão 802.11g	36
3.1.5 Padrão 802.11n	36
3.1.6 Padrão 802.11ac	37
3.1.7 Padrão 802.11ad	37
3.1.8 Outros padrões	37
3.2 Terminologia	38
3.3 Tipos de rede wireless	41
3.4 Modos promíscuo, monitor e managed	42

3.5 Laboratórios iniciais	42
3.5.1 Laboratório managed	43
3.5.2 Laboratório monitor	46
3.6 iwlist, iwconfig e iw	50
3.6.1 iwconfig	50
3.6.2 iwlist	51
3.6.3 iw	51
3.7 Domínios regulatórios	56
Capítulo 4 = Funcionamento de redes wireless	61
4.1 Campo Type: Control frame	64
4.1.1 PS-POLL	65
4.1.2 RTS/CTS	65
4.1.3 ACK	65
4.2 Campo Type: Management frames	66
4.2.1 Association request	67
4.2.2 Association response	67
4.2.3 Reassociation Request	67
4.2.4 Reassociation Response	68
4.2.5 Probe Request	68
4.2.6 Probe Response	68
4.2.7 Beacon	68
4.2.8 Disassociation	68
4.2.9 Authentication	68
4.2.10 Deauthentication	69
4.3 Campo Type: Data Frame	69
Capítulo 5 = Sistemas de criptografia	70
5.1 Criptografia OPN	70
5.1.2 Capturando conexões OPN	71
5.2 Criptografia WEP	77
5.2.1 Algoritmo RC4	77
5.2.2 Autenticação WEP	81
5.3 Criptografia WPA/WPA2 PSK	91
5.3.1 Capturando o beacon WPA TKIP	93
5.3.2 Capturando o beacon WPA2 CCMP	95
5.3.3 Capturando o 4-way handshake	98
5.4 Chave PTK	101

Capítulo 6 = Quebra do sistema de criptografia	103
6.1 Suíte Aircrack-ng.....	103
6.1.1 Airmon-ng	103
6.1.2 Airodump-ng.....	104
6.1.3 Aireplay-ng.....	108
6.1.4 Packetforge-ng	115
6.1.5 Aircrack-ng.....	116
6.1.6 Airolib-ng.....	118
6.1.7 Wpactclean	119
6.2 Quebra do WEP OPN	119
6.3 Quebra do WEP OPN (sem clientes)	122
6.4 Quebra do WEP SKA.....	124
6.5 Quebra do WEP com dicionário	126
6.6 Quebra do WPA/WPA2 PSK	126
6.7 John the ripper	128
6.7.1 Modo força bruta	130
6.7.2 Wordlist	130
6.7.3 Wordlist com rules.....	131
6.7.4 Restaurando a sessão.....	131
6.7.5 John the ripper jumbo	132
 Capítulo 7 = Acelerando o processo de quebra de senhas	 134
7.1 Chave PMK.....	134
7.2 Rainbow tables.....	135
7.2.1 GENPMK	135
7.2.2 COWPATTY	135
7.2.3 PYRIT	135
7.3 Quebra de senhas via GPU.....	138
7.4 Quebra de senhas via cluster	138
 Capítulo 8 = Conectando e capturando o tráfego em redes criptografadas.....	 141
8.1 Conectando em redes OPN	141
8.2 Conectando em redes WEP OPN	141
8.3 Conectando em redes WEP SKA	142
8.4 Conectando em redes WPA/WPA2 PSK	142
8.5 Conectando em redes WPA/WPA2 PSK ocultas	143
8.6 Conectando em redes WPA Enterprise	143
8.6.1 Conectando em redes EAP-TLS.....	143
8.6.2 Conectando em redes EAP-TTLS.....	144
8.7 Capturando tráfego WEP com o Wireshark	145
8.8 Capturando tráfego WPA/WPA2 PSK com o Wireshark.....	146
8.9 Airdecap-ng	147

Capítulo 9 ■ Burlando autenticações	148
9.1 Redes ocultas (Hidden SSIDs)	148
9.2 Filtros de MAC (MAC Filter)	150
9.3 Isolação do cliente (AP Isolation)	153
9.4 Injeção do tráfego via Airtun-ng	154
Capítulo 10 ■ Atacando a infraestrutura.....	156
10.1 Negação de serviço (Denial of Service)	156
10.1.1 Aireplay-ng	156
10.1.2 Ataques Deauth em Python	157
10.1.3 MDK3	159
10.2 Ataques diretos ao roteador	161
10.2.1 Vulnerabilidade CSRF	161
10.2.2 Quebra de senhas	163
Capítulo 11 ■ Ataques de falsificação	171
11.1 Evil Twin	171
11.1.1 Airbase-ng	172
11.2 Rogue Access Point.....	173
11.3 Honeypot.....	177
11.4 Man-in-the-Middle.....	178
Capítulo 12 ■ Ataques avançados.....	179
12.1 Redes Enterprise.....	179
12.1.1 Atacando WPA-Enterprise.....	181
12.2 Protocolo WPS.....	184
12.2.1 Wash	188
12.2.2 Bully	189
12.2.3 Reaver	191
12.2.4 Pixie dust attack	194
Capítulo 13 ■ Atacando o cliente.....	197
13.1 Caffè-Latte	198
13.2 Hirte Attack.....	199
13.3 Quebra do WPA/WPA2 PSK.....	200
13.4 Múltiplos pontos de acesso	200
13.4.1 Karma.....	203
13.5 Exploits	203
13.5.1 Framework Metasploit.....	204

Capítulo 14 = Ferramentas automatizadas	209
14.1 Gerix Wifi Cracker	209
14.1.1 Quebra do WEP OPN	210
14.1.2 Quebra do WEP SKA	212
14.2 WiFite	213
Capítulo 15 = Sistemas de defesa	214
15.1 Wireless Intrusion Detection System (wIDS)	214
15.1.1 wIDS SYWorks	215
15.1.2 wIDS para detectar ataques Deauth (Python)	219
15.2 wIPS Wireless Intrusion Detection System (WAIDPS SYWorks)	219
Capítulo 16 = Acessando redes wireless de forma segura	227
16.1 Criando um hostname	229
16.2 PPTP VPN	231
16.3 OpenVPN	237
16.3.1 OpenVPN com chaves estáticas	238
16.3.2 OpenVPN com certificados digitais	242
Capítulo 17 = Construindo redes wireless de forma segura	251
17.1 EAP-TLS	251
17.2 EAP-TTLS	271
Capítulo 18 = Metodologia wireless pentest	278
18.1 Planejamento	278
18.2 Descoberta	279
18.3 Ataque	279
18.4 Contra medidas	280
18.5 Relatório Final	280
18.6 Realizando um wireless pentest	281
18.6.1 Planejamento	281
18.6.2 Descoberta	281
18.6.3 Ataque	282
18.6.4 Contra medidas	284
Capítulo 19 = Afinal, estamos seguros?	286
19.1 Escopo	286
19.2 Descoberta	287
19.3 Ataque	287

Apêndice A ■ Instalação do Kali Linux	291
Apêndice B ■ Script em Python para captura do Probe Request.....	301
Apêndice C ■ Arquivos de configuração do HostAPd	302
Rede OPN	302
Rede WEP	302
Rede WPA/WPA2 PSK	302
Rede EAP-TTLS	303
Apêndice D ■ Mapeamento físico de redes sem fio	304
Apêndice E ■ Relatório de wireless pentest.....	310
E.1 Sumário executivo	310
E.2 Resultados	311
E.3 Narrativa do ataque	311
E.4 Medidas corretivas	313
Referências	314
Sites	314
Livros	316