Segurança em Redes sem Fio

Aprenda a proteger suas informações em ambientes Wi-Fi e Bluetooth

Nelson Murilo de Oliveira Rufino

Novatec

Sumário

Agradecimentos **11**
Prefácio **13**
Introdução **15**

Capítulo 1 ▪ Conceitos **17**
1.1 Fundamentos de rede sem fio 17
1.1.1 Freqüências 17
1.1.2 Canais 18
1.1.3 Spread Spectrum 19
1.1.4 Frequency-Hopping Spread-Spectrum (FHSS) 19
1.1.5 Direct Sequence Spread Spectrum (DSSS) 19
1.1.6 Orthogonal Frequency Division Multiplexing/Modulation (OFDM) 19
1.1.7 Bandas de radiofreqüência públicas 20
1.1.8 Freqüência 2,4 GHz 20
1.1.9 Freqüência 5 GHz 20
1.1.10 Freqüências licenciadas 21
1.2 Características 21
1.2.1 Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) 21
1.2.2 Extended Service Set Identifier (ESSID) 22
1.2.3 BEACON 22
1.2.4 Meio compartilhado 22
1.3 Padrões atuais 25
1.3.1 Padrão 802.11b 25
1.3.2 Padrão 802.11a 26
1.3.3 Padrão 802.11g 27
1.3.4 Padrão 802.11i 27
1.3.5 Padrão 802.1n 27
1.3.6 Padrão 802.1x 28
1.4 Conclusões 29

Capítulo 2 ▪ Mecanismos de segurança **31**
2.1 Endereçamento MAC 31
2.2 Wired Equivalent Privacy (WEP) 33

2.2.1 Funcionamento 34
2.3 Wi-fi Protected Access (WPA) 35
2.3.1 Criptografia 35
2.3.2 Extensible Authentication Protocol (EAP) 36
2.4 Autenticação 37

Capítulo 3 ▪ Riscos e ameaças 39
3.1 Problemas de segurança física 39
3.2 Configurações de fábrica 41
3.3 Envio e recepção de sinal 44
3.4 Negação de serviço (Denial of Service – DoS) 45
3.5 Mapeamento do ambiente 46
3.5.1 Mapeamento passivo 46
3.5.2 Geração de mapas 47
3.5.3 Mapeamento ativo 49
3.5.4 Mapeamento específico para redes sem fio 54
3.5.5 Mapeamento em camadas de baixo nível 56
3.6 Captura de tráfego 57
3.7 Acesso não autorizado em configurações básicas 57
3.7.1 Configuração aberta 58
3.7.2 Configuração fechada 58
3.8 Vulnerabilidades nos protocolos WEP e WPA 59
3.8.1 WEP 60
3.8.2 WPA 62
3.9 Equipamentos sem fio em ambientes cabeados 65

Capítulo 4 ▪ Técnicas e ferramentas de ataque 67
4.1 Preparação do ambiente 67
4.2 Ferramentas disponíveis 71
4.2.1 Airtraf 72
4.2.2 Airsnort 75
4.2.3 BSD AirTools 76
4.2.4 Netstumbler 78
4.2.5 Kismet 80
4.2.6 FakeAP 87
4.2.7 AirJack 88
4.2.8 AirSnarf 88
4.2.9 Hotspotter 89
4.2.10 Wellenreiter I e II 90
4.3 Escuta de tráfego 92
4.3.1 Ngrep 94
4.3.2 Ethereal 95

4.4 Endereçamento MAC 98
4.5 Ataques do tipo "homem no meio" 100
4.6 Quebra de chaves WEP 101
4.6.1 Airsnort 101
4.6.2 WepCrack 102
4.6.3 WepAttack 102
4.6.4 Wep_tools 103
4.6.5 Weplab 104
4.6.6 AirCrack 104
4.7 Redes Privadas Virtuais (Virtual Private Network) 107
4.8 Negação de serviço (DoS) 108
4.8.1 Void11 109

Capítulo 5 ▪ Métodos de defesa 111
5.1 Configurações do concentrador 111
5.1.1 Defesa do equipamento 111
5.1.2 Defesa dos equipamentos clientes 120
5.2 Configurações dos clientes 121
5.2.1 Padrão 802.1x e RADIUS 122
5.2.2 WEP 124
5.2.3 EAP_TLS 125
5.2.4 EAP_TTLS 129
5.2.5 WPA 130
5.2.6 WPA-PSK 132
5.2.7 WPA infra-estrutura (Interprise) 135
5.2.8 Virtual Private Network (VPN) 138
5.3 Uso de criptografia 141
5.3.1 Senhas descartáveis (One-time Password – OTP) 142
5.3.2 Certificados digitais 147
5.3.3 WPA e SmartCard 156
5.4 Detecção de ataques e monitoramento 160
5.4.1 Concentradores 160
5.4.2 Widz 162
5.4.3 wIDS 164
5.4.4 Garuda 166
5.4.5 AirIDS 168
5.4.6 Kismet 169
5.4.7 Snort-Wireless 170
5.4.8 Distâncias diferentes, variações de potência e outras 172

Capítulo 6 ▪ Estudo de casos 173
6.1 Cenário doméstico/pequena empresa 174
6.2 Cenário média/grande empresa 176

Capítulo 7 ▪ Bluetooth 181
7.1 Histórico 181
7.2 Características 182
7.3 Varredura 182
7.4 Topologia 183
7.5 Exemplos de uso 184
7.5.1 Sincronismo de base de dados 184
7.5.2 Permitir acesso físico a locais e serviços 184
7.5.3 Redes ponto a ponto 185
7.5.4 Acesso discado 185
7.5.5 Redes IP (PAN to LAN) 185
7.6 Ferramentas 185
7.7 Riscos 187
7.7.1 Identificação dos componentes de uma rede 187
7.7.2 Autenticação 191
7.7.3 Negação de serviço 192
7.7.4 Escuta de tráfego 193
7.7.5 Falsificações 194
7.7.6 Acessos não autorizados em redes cabeadas ou Wi-Fi 196
7.8 Proteção 200

Capítulo 8 ▪ Conclusões 201

Apêndice ▪ Tabela ASCII 203
ìndice remissivo 205