

Sumário

Agradecimentos	7
Prefácio	13
Introdução	15
Capítulo 1 – Conceitos	17
1.1 Fundamentos de rede sem fio	17
1.1.1 Frequências	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)	20
1.1.6 Orthogonal Frequency Division Multiplexing/Modulation (OFDM)	20
1.1.7 Bandas de radiofrequência públicas	20
1.1.8 Frequência 2,4 GHz	21
1.1.9 Frequência 5 GHz	21
1.1.10 Frequências licenciadas	21
1.2 Características	22
1.2.1 Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)	22
1.2.2 Extended Service Set Identifier (ESSID)	23
1.2.3 BEACON	23
1.2.4 Meio compartilhado	23
1.3 Padrões atuais	26
1.3.1 Padrão 802.11b	26
1.3.2 Padrão 802.11a	28
1.3.3 Padrão 802.11g	28
1.3.4 Padrão 802.11i	29
1.3.5 Padrão 802.1n	29
1.3.6 Padrão 802.1x	29
1.4 Conclusões	31
Capítulo 2 – Mecanismos de segurança	33
2.1 Endereçamento MAC	33
2.2 Wired Equivalent Privacy (WEP)	35
2.2.1 Funcionamento	36
2.3 Wi-fi Protected Access (WPA)	37
2.3.1 Criptografia	38
2.3.2 Extensible Authentication Protocol (EAP)	39
2.4 Autenticação	40

Capítulo 3 – Riscos e ameaças.....	43
3.1 Problemas de segurança física	43
3.2 Configurações de fábrica	45
3.3 Envio e recepção de sinal	48
3.4 Negação de serviço (Denial of Service - DoS).....	49
3.5 Mapeamento do ambiente.....	50
3.5.1 Mapeamento passivo.....	51
3.5.2 Geração de mapas	51
3.5.3 Mapeamento ativo.....	54
3.5.4 Mapeamento específico para redes sem fio	60
3.5.5 Mapeamento em camadas de baixo nível	61
3.6 Captura de tráfego	62
3.7 Acesso não autorizado em configurações básicas.....	63
3.7.1 Configuração aberta	63
3.7.2 Configuração fechada.....	64
3.8 Vulnerabilidades nos protocolos WEP e WPA	65
3.8.1 WEP	65
3.8.2 WPA	68
3.9 Equipamentos sem fio em ambientes cabeados	71
Capítulo 4 – Técnicas e ferramentas de ataque	73
4.1 Preparação do ambiente	73
4.2 Ferramentas disponíveis.....	77
4.2.1 Airtraf	78
4.2.2 Airsnort	81
4.2.3 BSD AirTools	83
4.2.4 Netstumbler	85
4.2.5 Kismet	87
4.2.6 FakeAP	95
4.2.7 AirJack	96
4.2.8 AirSnarf.....	96
4.2.9 Hotspotter	96
4.2.10 Wellenreiter I e II	97
4.3 Escuta de tráfego	100
4.3.1 Ngrep	102
4.3.2 Ethereal	104
4.4 Endereçamento MAC.....	106
4.5 Ataques do tipo “homem no meio”	109
4.6 Quebra de chaves WEP	110
4.6.1 Airsnort	110
4.6.2 WepCrack	111
4.6.3 WepAttack.....	111
4.6.4 Wep_tools.....	112
4.6.5 Weplab	113
4.6.6 AirCrack	114
4.7 Redes Privadas Virtuais (Virtual Private Network)	117
4.8 Negação de serviço (DoS)	118
4.8.1 Void11	118

Capítulo 5 – Métodos de defesa	121
5.1 Configurações do concentrador.....	121
5.1.1 Defesa do equipamento	121
5.1.2 Defesa dos equipamentos clientes	130
5.2 Configurações dos clientes	132
5.2.1 Padrão 802.1x e RADIUS.....	133
5.2.2 WEP	135
5.2.3 EAP_TLS	136
5.2.4 EAP_TTLS	140
5.2.5 WPA	141
5.2.6 WPA-PSK	144
5.2.7 WPA infra-estrutura (Enterprise).....	147
5.2.8 Virtual Private Network (VPN)	150
5.3 Uso de criptografia	154
5.3.1 Senhas descartáveis (One-time Password – OTP)	155
5.3.2 Certificados digitais.....	160
5.3.3 WPA e SmartCard.....	169
5.4 Detecção de ataques e monitoramento	173
5.4.1 Concentradores	174
5.4.2 Wids.....	175
5.4.3 wIDS	178
5.4.4 Garuda	180
5.4.5 AirIDS.....	182
5.4.6 Kismet.....	183
5.4.7 Snort-Wireless.....	184
5.4.8 Distâncias diferentes, variações de potência e outras	186
Capítulo 6 – Estudo de casos.....	187
6.1 Cenário doméstico/pequena empresa	188
6.2 Cenário média/grande empresa	190
Capítulo 7 – Bluetooth	195
7.1 Histórico	195
7.2 Características	196
7.3 Varredura.....	196
7.4 Topologia.....	197
7.5 Exemplos de uso	198
7.5.1 Sincronismo de base de dados	198
7.5.2 Permitir acesso físico a locais e serviços	198
7.5.3 Redes ponto a ponto.....	199
7.5.4 Acesso discado.....	199
7.5.5 Redes IP (PAN to LAN)	199
7.6 Ferramentas.....	200
7.7 Riscos	201
7.7.1 Identificação dos componentes de uma rede.....	201
7.7.2 Autenticação	205
7.7.3 Negação de serviço	206

7.7.4 Escuta de tráfego	208
7.7.5 Falsificações	209
7.7.6 Acessos não autorizados em redes cabeadas ou wi-fi.....	211
7.8 Proteção.....	214
Capítulo 8 – Conclusões.....	217
Apêndice A – Tabela ASCII.....	219
Índice Remissivo	221