

Sommario

INTRODUZIONE.....	11
1. RETI DI CALCOLATORI.....	15
Introduzione	15
Parametri di rete.....	21
L'indirizzo IP.....	22
La maschera di sottorete.....	25
Protocollo IPv4 e IPv6	28
Supporto IPv6 in Windows Vista	30
Il sistema numerico esadecimale	32
Il servizio di risoluzione dei nomi	33
Le porte e i servizi	35
Modalità operative di rete	37
I sistemi operativi di rete	38
La sicurezza dei sistemi operativi	39
Utilizzo delle risorse di rete	40
Il controllo degli accessi in Windows	42
Il controllo degli accessi in Linux.....	46
I protocolli di rete	48
Protocolli di tipo punto-punto	48
La famiglia di protocolli TCP/IP.....	49
Instaurare una connessione TCP	50
Terminare una connessione TCP	51
Stato delle connessioni TCP.....	52
Dispositivi e cablaggi di rete	54
Adattatore di rete.....	54
Repeater, HUB e switch.....	55
Router.....	58
Transceiver	58
Gateway	59
Bridge.....	60
Modem.....	60
Access Point	61
Dispositivi di tipo HomePlug	62
Il cablaggio di rete	64
Comandi di rete in Windows Vista	66
Gli indirizzi MAC	68

2. INSTALLARE E CONFIGURARE UNA RETE WIRELESS	69
Introduzione	69
Reti cablate o wireless?	71
Elementi costituenti una rete wireless	72
Prima configurazione di un access point	73
Accesso al dispositivo	74
Configurazione di base	75
Configurazione del SSID	77
Configurazione del server DHCP	78
Configurazione del filtro MAC	79
Configurazione del firewall interno	79
Ulteriori impostazioni	79
Configurazione delle macchine in rete	80
Modalità operative delle reti wireless	82
La modalità infrastructure	82
Modalità ad hoc	83
Applicazioni particolari in ambito wireless	85
Punti di accesso hotspot	85
La tecnologia WiMax	85
Il bridging tra le reti	86
Introduzione ai sistemi di protezione	87
Configurazione wireless in Windows Vista	88
Accedere alle proprietà di rete	88
Selezionare la modalità di gestione delle connessioni di rete	89
Visualizzare le connessioni di rete esistenti	89
Visualizzare le reti wireless attive	90
Connettersi a una rete protetta	91
Specificare la tipologia di rete	93
La scelta dei dispositivi	94
L'access point	95
Le interfacce di rete wireless	98
La certificazione Wi-Fi	99
Alcune tecnologie non standard	99
Configurazione guidata di un access point	100
Panoramica generale del dispositivo	101
Configurazione dell'indirizzo IP	102
Accesso alle pagine di configurazione	103
Utilizzo della configurazione guidata	104
Verifica del funzionamento	106
Le opzioni relative alla sezione firewall	107
Opzioni relative alla sicurezza wireless	109
Opzioni relative alla rete	111
Opzioni avanzate	112
Ulteriori opzioni	113
Il posizionamento dei dispositivi wireless	115
Omogeneità hardware e aggiornamento del software	115

Posizionamento dell'access point	115
Selezione del canale radio	117
Scelta dell'antenna	117
Conclusioni	118
3. HACKING DELLE RETI WIRELESS	119
Introduzione	119
Le tecniche e gli strumenti	120
Articolazione di un attacco	122
Fase 1 - Utilizzo di airmon-ng	123
Fase 2 - Utilizzo di airodump-ng	124
Fase 3 - Utilizzo di aireplay-ng	127
Attacco di tipo Deauthentication	128
Attacco di tipo Fake Authentication	129
Attacco di tipo interactive packet replay	130
Attacco di tipo ARP request replay	131
Attacco di tipo KoreK chopchop	131
Attacco di tipo fragmentation	132
Attacco di tipo injection test	133
Fase 4 - Utilizzo di Aircrack-ng	134
Fase 5 - Spoofing dell'indirizzo	137
Fase 6 - Accesso alla rete	138
Verifica della chiave con Airdecap-ng	139
Utilizzo di Packetforge-ng	139
Utilizzo di Airtun-ng	141
Mappare la rete su Google Earth con KNSGEM	142
Rivelatori portatili di reti wireless	145
4. TECNICHE DI PROTEZIONE	147
Introduzione	147
La protezione wired	148
La protezione perimetrale tramite firewall	148
La zona demilitarizzata	152
La protezione firewall di Windows XP e Vista	153
La protezione perimetrale tramite NAT	154
La protezione non perimetrale tramite IDS	158
La protezione non perimetrale tramite checksum	159
La protezione non perimetrale tramite honeypot	160
La protezione wireless	161
Verificare costantemente gli aggiornamenti	162
Impostare le password sull'access point	163
Intervenire sul SSID	164
Abilitare il filtro MAC	164
Limitare l'emissione radio	164
Suddividere in sottoreti	165
Crittografare le comunicazioni	165
Il sistema di protezione WEP	166
Il sistema di protezione WPA	167

Il sistema di protezione WPA2.....	168
Identificare gli intrusi sulla rete.....	168
Utilizzo del software AirSnare.....	169
Utilizzo di Ethereal/Wireshark in ambiente 802.11.....	172
Monitorare l'ambiente circostante con NetStumbler.....	179
Kismet e il packet sniffing passivo.....	181
Conclusioni.....	182
5. IL MOBILE COMPUTING.....	183
Introduzione.....	183
Analisi dei rischi.....	185
La sicurezza fisica.....	186
La sicurezza hardware.....	187
La sicurezza logica.....	187
La nascita degli smartphone.....	189
I sistemi operativi utilizzati.....	189
Il sistema operativo Symbian.....	190
Vulnerabilità.....	191
Tipologia di malware.....	192
Lo smartphone Nokia 5800.....	194
Il sistema operativo Windows Mobile.....	196
Il backup dei dati.....	197
La cifratura dei dati.....	198
Lo smartphone Touch.....	199
Il sistema operativo Palm OS.....	200
Alcuni consigli per la sicurezza.....	201
Alcuni malware storici: Liberty.A, Palm_Phage.A e Palm_Vapor.A.....	202
Lo smartphone Palm Centro.....	203
Il sistema BlackBerry.....	204
L'infrastruttura BlackBerry.....	204
BlackBerry Internet Service.....	205
BlackBerry Enterprise Server.....	206
BlackBerry Desktop Redirector.....	209
Accesso remoto alla rete aziendale.....	210
La cancellazione remota/locale del contenuto.....	211
Avvio d'emergenza del dispositivo.....	212
Trasferimento di dati tra dispositivi differenti.....	212
Procedure per la cessione/acquisto di un dispositivo usato.....	213
Configurazione della rete e del firewall integrato.....	214
La protezione locale.....	214
Cancellazione della cache.....	215
Problemi a monte dell'utente.....	217
La protezione dai virus.....	219
Attacchi diretti al dispositivo.....	219
GPS integrato e BlackBerry Connect software.....	220
Simulatore BlackBerry.....	221
Il sistema operativo BREW.....	222
Il sistema operativo iPhone OS.....	223

Lo smartphone Apple iPhone	224
Le prime vulnerabilità riscontrate.....	227
La connessione alle reti	228
Impostazioni di rete	231
Cookie, plug-in, pop-up e JavaScript	232
La posta elettronica	235
Gestione remota delle politiche di sicurezza	236
La connettività in ambiente 802.11x.....	237
Sistemi operativi basati su Linux.....	237
Il sistema operativo Android	238
Prime vulnerabilità del sistema Android	239
Lo smartphone GPhone	240
I dispositivi EEE-PC	241
La distribuzione Xandros.....	242
Avvertenze particolari.....	243
Lo standard Bluetooth	249
Scanner e attacchi Bluetooth	252
Contromisure per gli attacchi Bluetooth	255
La sicurezza delle informazioni	256
Paradigmi di protezione dei dati.....	257
Utilizzo corretto delle password	257
Attacchi di tipo MITM	259
Intercettazione delle comunicazioni.....	261
Tecniche di social engineering.....	262
Il fattore di rischio insider.....	264
Il rischio shoulder surfing	265
Soluzioni antivirus.....	266
Pianificazione dei backup.....	267
Protezione della memory card	268
Furto/perdita dello smartphone.....	269
Esempi di malware: Onehop, Skull.S e Cardtrap	269
Lo smartphone come strumento d'attacco	270
Scansione delle reti con Airomap	271
Il software Sniffi	272
Conclusioni.....	273
Politiche di sicurezza.....	273
General policy	274
Connectivity policy.....	275
Enterprise policy	277
Conclusioni.....	277
Altri dispositivi wireless.....	278
Protezione inversa tramite jammer.....	278
Servizi di localizzazione wireless.....	279
Il sistema di identificazione RFID	281
Tecnologie ottiche basate su infrarosso e laser.....	282
Wireless, elettromog e salute	284
Conclusioni.....	286

6. PRINCIPI DI GUERRA ELETTRONICA.....	287
Introduzione	287
Sistemi di attacco elettronico.....	288
Sistemi di protezione elettronica.....	291
Sistemi di supporto elettronico.....	292
Attività di cyberwarfare.....	293
Azioni di defacement	293
Attacchi di tipo Denial of Service.....	295
Sistemi tempest.....	295
Tempest for Eliza	296
Sistemi avanzati di intercettazione	298
Tecniche di protezione	298
Differenti tecnologie tempest	300
APPENDICE A. ELENCO DELLE PORTE PIÙ COMUNI	303
APPENDICE B. ONDE ELETTROMAGNETICHE.....	305
APPENDICE C. GLOSSARIO	307
INDICE ANALITICO	327