



Sommario

PREFAZIONE	11
Struttura del libro	13
Convenzioni di scrittura	14
A chi è indirizzato questo testo.....	15
I sistemi operativi considerati	15
1. INFORMATION TECHNOLOGY E SICUREZZA	17
1.1 Introduzione.....	17
1.2 Il problema della sicurezza informatica.....	18
1.3 Analisi dei rischi	21
1.4 La diffusione delle informazioni.....	23
1.5 Hacker, cracker e script kiddies	25
1.6 Le società del terzo millennio.....	27
1.7 Identità digitale	28
1.8 Il potere nel nuovo mondo digitale.....	30
1.9 Conclusioni	31
2. LE RETI INFORMATICHE	33
2.1 In cosa consiste una rete	33
2.2 Le RFC	36
2.3 La rete Internet	37
2.4 La rete Ethernet.....	39
2.5 Identificare gli elementi di una rete.....	40
2.6 Le modalità client/server e peer to peer	58
2.7 Sistemi operativi di rete.....	59
2.8 Tassonomia delle reti.....	77
2.9 Cablaggi di rete.....	78
2.10 Topologia fisica delle reti.....	82
2.11 Topologia logica delle reti.....	86
2.12 I protocolli di rete	95

2.13	Instaurare una connessione tra due host.....	106
2.14	Terminare una connessione tra due host.....	108
2.15	Stati delle connessioni TCP	109
2.16	Il meccanismo delle finestre scorrevoli.....	111
2.17	Controllo delle congestioni del TCP	112
2.18	Dispositivi di rete.....	115
2.19	Struttura dei protocolli di rete	131
2.20	Il routing dei pacchetti	153
2.21	Accesso remoto alle reti: SLIP, PPP e VPN.....	157
2.22	Le tecnologie xDSL.....	158
3.	LE RETI WIRELESS	161
3.1	Introduzione.....	161
3.2	Reti cablate o wireless?	163
3.3	Gli elementi costituenti una rete wireless.....	165
3.4	Prima messa in opera di un access point.....	166
3.5	Configurazione di base dell'access point	168
3.6	Configurazione avanzata dell'access point.....	172
3.7	Configurazione delle macchine in rete	176
3.8	Sistemi di protezione wireless	178
3.9	Schemi di funzionamento delle reti wireless.....	182
3.10	Hot spot: il wireless pubblico	186
3.11	Tecniche di war driving	187
3.12	Hacking delle reti wireless	188
4.	TECNICHE DI INDAGINE.....	221
4.1	Introduzione.....	221
4.2	Ricerca e utilizzo delle informazioni.....	222
4.3	Tecniche di social engineering	223
4.4	Esposizione di dati sensibili.....	231
4.5	Tecniche di dumpster diving	232
4.6	Tecniche di shoulder surfing.....	234
5.	TECNICHE DI VERIFICA	237
5.1	Introduzione.....	237
5.2	Interrogazione dei DNS.....	238
5.3	Scansione delle reti.....	242
5.4	Lo strumento di scansione Nmap.....	246
5.5	Enumerazione delle reti.....	252
5.6	Identificazione del sistema operativo	256

5.7	Enumerazione SNMP	259
5.8	Rilevazione dei banner tramite Telnet	259
5.9	Individuare la presenza di un firewall.....	261
5.10	Tecniche di war dialing	263
6.	TECNICHE DI ACCESSO E MASCHERAMENTO	265
6.1	Introduzione.....	265
6.2	Attacchi di tipo DoS	266
6.3	Introduzione allo spoofing.....	272
6.4	Altre tecniche per l'anonimato: i server proxy.....	277
6.5	Utilizzo dei Wingate.....	281
6.6	Tecnica dell'FTP bounce.....	281
6.7	Tecnica del buffer overflow.....	283
6.8	I rootkit	288
6.9	Attacchi di tipo shellcode.....	290
6.10	SQL injection	291
7.	TECNICHE DI PROTEZIONE	297
7.1	La protezione dai rischi locali	297
7.2	Backup e cancellazione sicura dei dati	314
7.3	La protezione dagli attacchi remoti	320
7.4	La difesa proattiva	350
8.	TECNICHE DI CRITTOGRAFIA.....	361
8.1	Algoritmi di crittografia	361
8.2	Crittografia asimmetrica e firma digitale	367
8.3	Lo standard X.509.....	369
8.4	Conclusioni	370
9.	VIRUS E ALTRI AGENTI NOCIVI	373
9.1	I virus informatici.....	373
9.2	Spyware e adware.....	383
9.3	Le backdoor.....	389
9.4	I dialer.....	397
10.	APPROFONDIMENTI	401
10.1	Breve storia dell'hacker più famoso del mondo	401
10.2	Captain Crunch - il re del phreaking.....	403
10.3	Autocostruzione di un firewall hardware.....	405
APPENDICE A – ELENCO DELLE PORTE PRIVILEGIATE.....		415

APPENDICE B – CODICI DI PROTOCOLLO 421

APPENDICE C – ELENCO DEI COMANDI NMAP 429

APPENDICE D – GLOSSARIO 435