

# Sommario

<b>Prefazione alla seconda edizione</b>		<b>xiii</b>
<b>Prefazione alla prima edizione</b>		<b>xvii</b>
<b>Parte I</b>	<b>Nozioni preliminari</b>	<b>1</b>
<b>Capitolo 1</b>	<b>Introduzione</b>	<b>3</b>
	1.1 Assiomi sulla sicurezza .....	3
	1.2 Scelta di una politica della sicurezza .....	7
	1.3 Sicurezza basata sull'host .....	11
	1.4 Sicurezza perimetrale .....	11
	1.5 Strategie per una rete sicura .....	12
	1.6 Etica della sicurezza informatica .....	18
	1.7 ATTENZIONE .....	20
<b>Capitolo 2</b>	<b>Sicurezza dei protocolli: livelli inferiori</b>	<b>21</b>
	2.1 Protocolli di base .....	21
	2.2 Gestione di nomi e indirizzi .....	30
	2.3 IP version 6 .....	38
	2.4 Network Address Translator .....	41
	2.5 Sicurezza wireless .....	42
<b>Capitolo 3</b>	<b>Sicurezza: livelli superiori</b>	<b>45</b>
	3.1 Messaggistica .....	45
	3.2 Telefonia Internet .....	51
	3.3 Protocolli basati su RPC .....	52
	3.4 Protocolli per il trasferimento di file .....	58
	3.5 Login remoto .....	64
	3.6 Simple Network Management Protocol (SNMP) .....	69
	3.7 Network Time Protocol .....	70
	3.8 Servizi informativi .....	71
	3.9 Protocolli proprietari .....	76

	3.10 Reti peer-to-peer .....	77
	3.11 Il sistema a finestre X11 .....	78
	3.12 Piccoli servizi .....	80
<b>Capitolo 4</b>	<b>Il Web: pericolo o minaccia?</b>	<b>83</b>
	4.1 Protocolli Web .....	84
	4.2 Rischi dei client .....	90
	4.3 Rischi per il server .....	96
	4.4 Server web e firewall .....	100
	4.5 Web e database .....	102
	4.6 Considerazioni .....	103
<b>Parte II</b>	<b>Le minacce</b>	<b>105</b>
<b>Capitolo 5</b>	<b>Classi di attacchi</b>	<b>107</b>
	5.1 Furto di password .....	107
	5.2 Ingegneria sociale .....	111
	5.3 Bug e backdoor .....	112
	5.4 Fallimenti di autenticazione .....	115
	5.5 Fallimenti del protocollo .....	117
	5.6 Fuga di informazioni .....	118
	5.7 Attacchi esponenziali: virus e worm .....	119
	5.8 Attacchi denial-of-service .....	120
	5.9 Botnet .....	131
	5.10 Attacchi attivi .....	131
<b>Capitolo 6</b>	<b>Strumenti dell'hacker e altre munizioni</b>	<b>133</b>
	6.1 Introduzione .....	133
	6.2 Obiettivi dell'hacking .....	135
	6.3 Scansione di una rete .....	135
	6.4 Violazione dell'host .....	136
	6.5 La battaglia per l'host .....	137
	6.6 Occultamento delle tracce .....	141
	6.7 Metastasi .....	142
	6.8 Strumenti di hacking .....	143
	6.9 Tiger team .....	147
<b>Parte III</b>	<b>Strumenti e servizi più sicuri</b>	<b>149</b>
<b>Capitolo 7</b>	<b>Autenticazione</b>	<b>151</b>
	7.1 Ricordare le password .....	152
	7.2 Password monouso a tempo .....	158
	7.3 Password monouso challenge/response .....	159
	7.4 Algoritmo di Lamport per password monouso .....	160

	7.5 Smart card .....	161
	7.6 Biometrica .....	162
	7.7 RADIUS .....	163
	7.8 SASL: un framework di autenticazione .....	163
	7.9 Autenticazione host-to-host .....	164
	7.10 PKI .....	165
<b>Capitolo 8</b>	<b>Alcuni strumenti e servizi</b>	<b>167</b>
	8.1 Inetd: servizi in rete .....	168
	8.2 Ssh: accesso a terminali e file .....	168
	8.3 Syslog .....	173
	8.4 Strumenti per l'amministrazione della rete .....	174
	8.5 Chroot: isolamento di software sospetti .....	177
	8.6 Inserimento in una jail del server web Apache .....	179
	8.7 Aftpd: un semplice daemon FTP anonimo .....	183
	8.8 Agenti per il trasferimento di posta .....	184
	8.9 POP3 e IMAP .....	184
	8.10 Samba: un'implementazione di SMB .....	185
	8.11 Adattamento di Named .....	186
	8.12 Aggiunta del supporto SSL con Sslwrap .....	187
<b>Parte IV</b>	<b>Firewall e VPN</b>	<b>189</b>
<b>Capitolo 9</b>	<b>Tipi di firewall</b>	<b>191</b>
	9.1 Filtri di pacchetti .....	192
	9.2 Filtraggio a livello dell'applicazione .....	203
	9.3 Gateway a livello di trasporto .....	204
	9.4 Filtri dinamici di pacchetti .....	205
	9.5 Firewall distribuiti .....	212
	9.6 Quello che i firewall non possono fare .....	213
<b>Capitolo 10</b>	<b>Filtraggio di servizi</b>	<b>215</b>
	10.1 Servizi che è consigliabile filtrare .....	216
	10.2 Caccia al verme .....	224
	10.3 Servizi che non ci piacciono .....	226
	10.4 Altri servizi .....	228
	10.5 Novità .....	228
<b>Capitolo 11</b>	<b>Ingegneria dei firewall</b>	<b>231</b>
	11.1 Set di regole .....	234
	11.2 Proxy .....	235
	11.3 Costruzione di un firewall da zero .....	236
	11.4 Problemi dei firewall .....	248
	11.5 Test dei firewall .....	252

<b>Capitolo 12</b>	<b>Tunneling e VPN</b>	<b>255</b>
	12.1 Tunnel .....	256
	12.2 Virtual Private Network (VPN) .....	259
	12.3 Software e hardware .....	266
<b>Parte V</b>	<b>Sicurezza in un'azienda</b>	<b>269</b>
<b>Capitolo 13</b>	<b>Layout delle reti</b>	<b>271</b>
	13.1 Esplorazioni delle intranet .....	273
	13.2 Trucchi di instradamento su intranet .....	273
	13.3 Fiducia negli host .....	278
	13.4 Cintura e bretelle .....	280
	13.5 Classi di posizionamento .....	281
<b>Capitolo 14</b>	<b>Host sicuri in un ambiente ostile</b>	<b>285</b>
	14.1 Che cosa si intende per "sicuro"? .....	285
	14.2 Proprietà degli host sicuri .....	286
	14.3 Configurazione hardware .....	292
	14.4 Rimozione dei servizi di un host .....	293
	14.5 Caricamento di nuovo software .....	297
	14.6 Amministrazione di un host sicuro .....	298
	14.7 Senza rete: vita senza firewall .....	303
<b>Capitolo 15</b>	<b>Rilevamento delle intrusioni</b>	<b>305</b>
	15.1 Dove monitorare .....	307
	15.2 Tipi di IDS .....	307
	15.3 Amministrazione di un IDS .....	308
	15.4 Strumenti IDS .....	309
<b>Parte VI</b>	<b>Lezioni pratiche</b>	<b>311</b>
<b>Capitolo 16</b>	<b>Una serata con Berferd</b>	<b>313</b>
	16.1 Atti ostili .....	313
	16.2 Una serata con Berferd .....	316
	16.3 Il giorno dopo .....	320
	16.4 La jail .....	321
	16.5 Tracciamento di Berferd .....	323
	16.6 Torna a casa, Berferd .....	324
<b>Capitolo 17</b>	<b>La presa di Clark</b>	<b>327</b>
	17.1 Preludio .....	328
	17.2 CLARK .....	328
	17.3 Principi elementari di indagine .....	329
	17.4 Indagine su CLARK .....	330

	17.5 Il file delle password .....	335
	17.6 Come riuscirono a entrare? .....	336
	17.7 Tecniche investigative migliori .....	337
	17.8 Che cosa avete imparato .....	337
<b>Capitolo 18</b>	<b>Comunicazioni sicure su reti insicure</b>	<b>339</b>
	18.1 Il sistema di autenticazione Kerberos .....	340
	18.2 Cifratura a livello di collegamento .....	344
	18.3 Cifratura a livello di rete .....	345
	18.4 Cifratura a livello di applicazione .....	349
<b>Capitolo 19</b>	<b>E poi?</b>	<b>357</b>
	19.1 IPv6 .....	357
	19.2 DNSsec .....	358
	19.3 Microsoft e la sicurezza .....	359
	19.4 Ubiquità di Internet .....	359
	19.5 Sicurezza su Internet .....	359
	19.6 Conclusione .....	360
<b>Parte VII</b>	<b>Appendici</b>	<b>363</b>
<b>Appendice A</b>	<b>Introduzione alla crittografia</b>	<b>365</b>
	A.1 Notazione .....	367
	A.2 Crittografia a chiave segreta .....	367
	A.3 Modalità operative .....	369
	A.4 Crittografia a chiave pubblica .....	373
	A.5 Scambio di chiavi esponenziali .....	374
	A.6 Firme digitali .....	375
	A.7 Funzioni di hash sicuro .....	376
	A.8 Timestamp .....	378
<b>Appendice B</b>	<b>Aggiornamento</b>	<b>379</b>
	B.1 Mailing list .....	380
	B.2 Risorse web .....	381
	B.3 Pagine personali .....	382
	B.4 Siti dei produttori .....	382
	B.5 Conferenze .....	383
<b>Bibliografia</b>		<b>385</b>
<b>Elenco delle</b>		<b>415</b>
<b>Elenco degli acronimi</b>		<b>417</b>
<b>Indice analitico</b>		<b>421</b>