

Indice generale

Gli autori	xvii
Presentazione	xxi
Prefazione	xxiii
Introduzione	xxv
Parte I	Inquadrare il bersaglio
Caso di studio	2
L'anonimato è fondamentale.....	2
Capitolo 1	La raccolta di informazioni: il footprinting.....7
Che cos'è il footprinting?.....	8
Perché è necessario il footprinting.....	8
Footprinting su Internet.....	9
Passo 1: definire l'ambito delle proprie attività	10
Passo 2: ottenere le opportune autorizzazioni	10
Passo 3: informazioni accessibili al pubblico.....	10
Informazioni accessibili al pubblico.....	10
Pagine web dell'organizzazione.....	11
Organizzazioni correlate.....	12
Dettagli sulla sede	12
Dipendenti: numeri di telefono, nomi di contatto, indirizzi e-mail e dettagli personali	14
Eventi in corso	14
Politiche per la privacy e la sicurezza e dettagli tecnici che indicano i meccanismi di sicurezza attivi.....	15
Informazioni archiviate.....	16
Dipendenti scontenti	16
Motori di ricerca, Usenet e curricula	18
Altre informazioni di interesse	21
Contromisure per la sicurezza dei database pubblici.....	21
Passo 4: enumerazione di server WHOIS e DNS	22
Ricerche relative ai domini.....	24
Ricerche relative all'IP.....	26
Altre contromisure per la sicurezza dei database pubblici	29
Passo 5: interrogazione del DNS	30
Trasferimenti di zona	30
Determinare i record MX (Mail eXchange).....	33
Contromisure per la sicurezza del DNS	34
Passo 6: riconoscimento della rete	34
Tracerouting.....	34
Contromisure contro il riconoscimento della rete	37
Riepilogo.....	37

Capitolo 2 La scansione39

Determinare se il sistema è attivo.....	39
Ping sweep di rete	40
Contromisure contro i ping sweep	46
Query ICMP	47
Contromisure contro le query ICMP.....	48
Determinare quali servizi sono in esecuzione o in ascolto	49
Scansione di porte	49
Tipi di scansioni	49
Individuare i servizi TCP e UDP in esecuzione.....	51
strobe	51
udp_scan	52
netcat	52
Network Mapper (nmap).....	53
Scanner di porte per Windows	56
SuperScan	56
WUPS	57
ScanLine	58
Riepilogo degli strumenti per la scansione di porte	60
Contromisure contro la scansione di porte.....	61
Rilevamento del sistema operativo.....	62
Rilevamento del sistema operativo attivo	62
Fingerprinting attivo dello stack.....	63
Contromisure contro il rilevamento del sistema operativo	65
Identificazione passiva del sistema operativo	66
Fingerprinting passivo dello stack.....	66
Segnature passive	67
Contromisure contro il rilevamento passivo del sistema operativo.....	68
Strumenti di rilevamento automatico.....	68
Contromisure contro gli strumenti di rilevamento automatico	69
Riepilogo.....	69

Capitolo 3 L'enumerazione71

Cattura di banner	72
Le basi per la cattura di banner: telnet e netcat	73
Contromisure contro la cattura di banner.....	74
Enumerazione dei servizi di rete comuni	75
Enumerazione di FTP,TCP 21	75
Contromisure contro l'enumerazione di FTP.....	76
Enumerazione di telnet,TCP 23	76
Contromisure contro l'enumerazione di telnet.....	77
Enumerazione di SMTP,TCP 25	78
Contromisure contro l'enumerazione di SMTP	79
Enumerazione del DNS,TCP/UDP 53	79
Contromisure contro l'enumerazione del DNS	82
Enumerazione di TFTP,TCP/UDP 69	84
Contromisure contro l'enumerazione di TFTP.....	85
Enumerazione di finger,TCP/UDP 79.....	85
Contromisure contro l'enumerazione di finger.....	86
Enumerazione di HTTP,TCP 80.....	86
Contromisure contro l'enumerazione di HTTP	88
Enumerazione di MSRPC (Microsoft RPC Endpoint Mapper),TCP 135	89
Contromisure contro l'enumerazione di MSRPC.....	90
Enumerazione del servizio nomi NetBIOS, UDP 137.....	91
Bloccare l'enumerazione dei servizi di nomi NetBIOS	95
Enumerazione tramite sessione NetBIOS,TCP 139/445.....	96
Contromisure contro le sessioni null SMB	106
Enumerazione di SNMP,UDP 161.....	111
Contromisure contro l'enumerazione di SNMP.....	115
Enumerazione di BGP,TCP 179.....	115
Contromisure contro l'enumerazione di BGP	118

Enumerazione di LDAP di Windows Active Directory, TCP/UDP 389 and 3268	118
Contromisure contro l'enumerazione di Active Directory	120
Enumerazione di Novell NetWare, TCP 524 e IPX	122
Contromisure contro l'enumerazione di NetWare	125
Enumerazione di RPC UNIX, TCP/UDP 111 e 32771	126
Contromisure contro l'enumerazione di RPC	128
rwho (UDP 513) e rusers (RPC Program 100002)	128
Contromisure contro l'impiego di rwho e rusers	128
Enumerazione di NIS, programma RPC 100004	129
Contromisure contro l'enumerazione di NIS	129
Enumerazione del servizio di risoluzione SQL, UDP 1434	129
Contromisure contro l'enumerazione di istanze SQL	130
Enumerazione di Oracle TNS, TCP 1521/2483	131
Contromisure contro l'enumerazione di Oracle TNS	132
Enumerazione di NFS, TCP/UDP 2049	133
Contromisure contro l'enumerazione di NFS	133
Riepilogo	133

Parte II **Hacking del sistema**

Caso di studio: i rischi del DNS	136
--	-----

Capitolo 4 **Hacking di Windows 139**

Panoramica	141
Argomenti non trattati	141
Attacchi senza autenticazione	142
Attacchi con falsificazione dell'autenticazione	142
Determinare la password da remoto	142
Contromisure contro l'individuazione delle password	145
Spiare lo scambio di password in rete	149
Contromisure contro lo sniffing delle procedure di autenticazione Windows	151
Attacchi Man-In-The-Middle	152
Contromisure contro gli attacchi MITM	153
Exploit senza autenticazione da remoto	154
Exploit dei servizi di rete	154
Contromisure contro l'exploit di servizi di rete	156
Exploit di applicazioni dell'utente finale	157
Contromisure contro l'exploit di applicazioni dell'utente finale	158
Exploit dei driver di periferica	159
Contromisure contro l'exploit dei driver	160
Attacchi con autenticazione	160
Scalata dei privilegi	161
Prevenire la scalata dei privilegi	162
Estrazione e cracking di password	162
Catturare gli hash di password	163
Contromisure contro pwdump	164
Cracking delle password	165
Contromisure contro il cracking delle password	170
Dumping di password memorizzate nella cache	171
Contromisure contro il dumping delle password memorizzate nella cache	174
Controllo remoto e backdoor	174
Strumenti per il controllo remoto dalla riga di comando	174
Controllo remoto con GUI	176
Reindirizzamento delle porte	178
fpipe	179
Coprire le proprie tracce	180
Disabilitare il controllo di Windows (auditing)	180
Cancellazione del registro di eventi	181
Nascondere i file	181
Contromisure contro gli ADS	182

Rootkit.....	182
Contromisure generali contro la violazione della procedura di autenticazione	183
Nomi di file	183
Voci del registro di sistema.....	184
Processi	185
Porte	186
Funzionalità di sicurezza di Windows.....	187
Windows Firewall.....	187
Aggiornamenti automatici	187
Centro sicurezza PC	189
Criteri di protezione e criteri di gruppo	190
Bitlocker ed EFS (Encrypting File System).....	192
Contromisure contro l'attacco di avvio a freddo.....	193
Protezione di risorse Windows con WRP.....	194
Livelli di integrità, UAC e LoRIE.....	194
Protezione esecuzione programmi.....	196
Rafforzare la protezione dei servizi	197
Isolamento del servizio	197
Servizi con privilegi minimi	198
Refactoring del servizio	198
Accesso di rete ristretto.....	199
Isolamento della sessione 0	199
Miglioramenti basati sul compilatore.....	201
Il peso della sicurezza di Windows.....	202
Riepilogo.....	202

Capitolo 5 Hacking di Unix..... 205

Alla conquista di root.....	205
Un breve riepilogo	206
Mappatura delle vulnerabilità	206
Accesso remoto e accesso locale.....	207
Accesso remoto.....	208
Attacchi di forza bruta.....	209
Contromisura contro gli attacchi di forza bruta	210
Attacchi data-driven	212
Attacchi di buffer overflow	212
Contromisure contro l'attacco di buffer overflow	214
Attacchi con stringhe di formato	216
Contromisure contro l'attacco con stringa di formato	218
Attacchi a validazione dell'input	219
Contromisura contro l'attacco a validazione dell'input	220
Attacchi integer overflow e integer sign	220
Contromisure contro l'attacco di integer overflow	224
Attacchi dangling pointer (puntatore pendente).....	224
Contromisure contro i puntatori pendenti	225
Voglio la mia shell.....	225
Telnet inverso e canali di ritorno	226
Contromisura contro gli attacchi con canale di ritorno	229
Tipi comuni di attacchi remoti	229
FTP	230
Contromisure contro gli attacchi a FTP.....	231
Sendmail	231
Contromisure contro gli attacchi a sendmail.....	231
Servizi RPC (Remote Procedure Call).....	232
Contromisure contro gli attacchi a servizi RPC (Remote Procedure Call)	234
SNMP (Simple Network Management Protocol).....	235
Contromisure contro gli attacchi a SNMP	235
NFS	236
Contromisure contro gli attacchi a NFS.....	240
Vulnerabilità di X.....	241

Contromisure contro le vulnerabilità di X.....	243
DNS (Domain Name System).....	243
Avvelenamento della cache DNS.....	244
Attacchi di overflow dello TSIG DNS.....	245
Contromisure all'attacco di overflow dello TSIG DNS.....	246
Vulnerabilità di SSH.....	247
Vulnerabilità challenge-response di OpenSSH.....	247
Contromisure contro le vulnerabilità di SSH.....	248
Attacchi di overflow OpenSSL.....	248
Contromisure contro le vulnerabilità di OpenSSL.....	249
Attacchi ad Apache.....	250
Contromisure contro le vulnerabilità di Apache.....	250
Attacchi in modalità promiscua.....	251
Contromisure contro gli attacchi in modalità promiscua.....	252
Accesso locale.....	252
Vulnerabilità della password.....	253
John the Ripper.....	254
Contromisure contro le vulnerabilità delle password.....	257
Buffer overflow locale.....	258
Contromisure contro il buffer overflow locale.....	259
Collegamenti simbolici.....	259
Contromisura contro la vulnerabilità dei collegamenti simbolici.....	260
Corse critiche (race condition).....	260
Contromisure contro la vulnerabilità nella gestione dei segnali.....	261
Manipolazione dei file core.....	262
Contromisure contro la vulnerabilità dei file core.....	262
Librerie condivise.....	262
Contromisure contro le vulnerabilità delle librerie condivise.....	263
Difetti del kernel.....	263
Contromisure contro i difetti del kernel.....	264
Errori di configurazione del sistema.....	264
Permessi su file e directory.....	265
Contromisure contro le vulnerabilità dei file SUID.....	266
Contromisure contro la vulnerabilità dei file accessibili a tutti in scrittura.....	268
Accesso di root ottenuto: e ora?.....	268
Rootkit.....	268
Trojan.....	269
Contromisure contro i trojan.....	270
Sniffer.....	271
Che cos'è uno sniffer?.....	271
Funzionamento degli sniffer.....	272
Alcuni sniffer noti.....	273
Contromisure contro gli sniffer.....	273
Cancellazione dei log.....	274
Contromisure contro la cancellazione dei log.....	279
Rootkit del kernel.....	279
Contromisure contro i rootkit del kernel.....	281
Che cosa fare in caso di attacco con rootkit.....	282
Riepilogo.....	283

Parte III Hacking delle infrastrutture

Caso di studio: leggi e WEP.....	286
----------------------------------	-----

Capitolo 6 Connettività remota e hacking VoIP 289

Preparazione alla connessione dial-up.....	290
Footprinting del numero telefonico.....	290
Contromisure contro le fughe di notizie.....	292
War-dialing.....	292
Hardware.....	292
Aspetti legali.....	293
Costi accessori.....	294

Software	294
ToneLoc.....	295
File batch per ToneLoc	298
THC-Scan	300
PhoneSweep	303
Tecniche di exploit del carrier	306
Script di forza bruta: il fai-da-te.....	308
LHF (Low Hanging Fruit).....	310
Autenticazione singola, tentativi illimitati	310
Autenticazione singola, tentativi limitati	314
Autenticazione duale, tentativi illimitati	315
Autenticazione duale, tentativi limitati	316
Nota conclusiva sugli script per attacchi di forza bruta.....	317
Misure di sicurezza per le connessioni dial-up.....	318
Hacking di centralini telefonici	319
Login su reti voicemail Octel.....	320
Centralini Williams/Northern Telecom.....	320
Centralini Meridian Links	321
Centralini Rolm PhoneMail.....	321
Centralini ATT Definity G / System 75	322
Centralino protetto da ACE/Server	323
Contromisure contro l'hacking dei centralini	323
Hacking di sistemi voicemail.....	323
Hacking di sistemi voicemail a forza bruta	323
Contromisure contro gli attacchi di forza bruta a voicemail.....	328
Hacking delle reti VPN (Virtual Private Network).....	328
Attacchi a Microsoft PPTP	329
Rimedi per le vulnerabilità di PPTP.....	330
Analisi di IPSec da parte degli esperti:	
entrano in gioco Schneier e Ferguson.....	331
Nozioni di base sulle VPN IPSec.....	331
Autenticazione e impostazione del tunnel in reti VPN IPSec.....	332
Google hacking per VPN.....	332
Contromisure contro il Google Hacking per VPN	333
Attacchi a server VPN IPSec	334
Contromisure contro gli attacchi a VPN IPSec.....	335
Attacco all'aggressive mode di IKE	335
Contromisure contro gli attacchi all'aggressive mode di IKE	337
Attacchi a Voice over IP.....	337
Vari tipi di attacchi a VoIP	338
Scansione SIP.....	338
Contromisure contro la scansione SIP.....	339
Saccheggiare TFTP alla ricerca di tesori VoIP	339
Contromisure contro il saccheggio di TFTP.....	340
Enumerazione di utenti SIP.....	340
Enumerazione dell'utente con REGISTER di Asterisk.....	341
Enumerazione dell'utente con OPTIONS di SIP EXpress Router.....	343
Enumerazione dell'utente automatizzata	344
Contromisure contro l'enumerazione SIP	347
Attacco di intercettazione	347
Contromisure contro l'intercettazione.....	350
Flood SIP INVITE.....	351
Contromisure contro il flood SIP INVITE	352
Riepilogo.....	352

Capitolo 7 Dispositivi di rete..... 353

Individuazione del bersaglio	354
Rilevamento.....	354
Profilazione	354
dig	354
Contromisure contro l'uso di dig.....	356
traceroute.....	356
Contromisure contro l'uso di traceroute	357

Ricerca dell'indirizzo IP.....	357
Ricerca di un sistema autonomo	358
traceroute normale.....	358
traceroute con ASN.....	358
show ip bgp.....	359
Newsgroup pubblici.....	360
Contromisure contro la profilazione	360
Rilevamento di un servizio	361
nmap.....	361
Contromisure contro il rilevamento dei servizi	363
Identificazione del sistema operativo	364
Contromisure contro l'identificazione del sistema operativo	365
Cattura ed enumerazione del banner Cisco.....	365
Contromisure contro la cattura e l'enumerazione di banner Cisco.....	366
Vulnerabilità delle reti	366
Livello OSI 1	366
Livello OSI 2.....	368
Rilevamento di media livello 2	368
Sniffing sugli switch.....	369
Reindirizzamento ARP.....	369
Contromisure contro il reindirizzamento ARP.....	372
Sniffing di traffico broadcast	373
Contromisure contro lo sniffing di traffico broadcast.....	376
Saltare da una VLAN all'altra	376
Contromisure contro il salto da una VLAN all'altra	378
IRPAS (Internetwork Routing Protocol Attack Suite) e CDP (Cisco Discovery Protocol)	378
Contromisure contro CDP.....	379
Attacchi STP (Spanning Tree Protocol).....	379
Contromisure contro il ricalcolo STP.....	380
Attacchi VTP (VLAN Trunking Protocol).....	380
Contromisure contro gli attacchi VTP.....	380
Livello OSI 3.....	381
IPv4 (Internet Protocol Version 4)	381
Previsione del numero di sequenza TCP	381
IPv6 (IP Version 6) o IPng (IP: Next Generation)	381
tcpdump.....	382
Contromisure contro lo sniffing.....	382
dsniff.....	383
Contromisure contro dsniff.....	385
Ettercap.....	385
Contromisure contro Ettercap	385
Errori di configurazione	385
MIB di lettura/scrittura	386
Contromisure contro il MIB write net per Cisco	388
Cifratura debole di Cisco.....	389
Contromisure contro la decifrazione delle password Cisco.....	390
Download di TFTP	390
Contromisure contro le vulnerabilità di TFTP	391
Hacking del protocollo di routing.....	391
Spoofing RIP.....	391
IGRP (Interior Gateway Routing Protocol)	393
OSPF (Open Shortest Path First).....	395
BGP.....	396
Iniezione di pacchetti BGP contraffatti	397
Contromisure contro gli attacchi al protocollo di routing.....	400
Hacking del protocollo di gestione.....	400
SNMP Request e Trap Handling	400
Contromisure per SNMP Request e Trap Handling.....	401
Buffer overflow basati sullo heap e sistema IOS.....	401
Riepilogo.....	403

Capitolo 8	Hacking delle reti wireless	405
	Footprinting in ambiente wireless.....	406
	Apparecchiature.....	407
	Schede	407
	Antenne	408
	GPS	410
	Software per war-driving.....	413
	NetStumbler	413
	Contromisure contro NetStumbler.....	415
	Kismet	415
	Contromisure contro Kismet	417
	Mappatura wireless	417
	StumbVerter.....	417
	GPSMap	418
	JiGLE.....	419
	Scansione ed enumerazione wireless.....	420
	Sniffer wireless.....	422
	Cattura di pacchetti e risorse per l'analisi	422
	Configurazione di schede wireless in Linux per la modalità promiscua	423
	Strumenti per il monitoraggio wireless.....	424
	tcpdump.....	425
	Wireshark.....	426
	Airtart	426
	OmniPeek NX.....	427
	WifiScanner	428
	Difese e contromisure contro l'identificazione delle reti wireless	429
	SSID.....	429
	Controllo degli accessi MAC	431
	void11	432
	WEP/WPA.....	433
	Ottenere l'accesso (hacking del protocollo 802.11)	433
	SSID.....	434
	Controllo accessi con l'indirizzo MAC.....	435
	WEP.....	436
	Attacchi all'algoritmo WEP.....	436
	Strumenti che sfruttano la debolezza del WEP.....	437
	AirSnort.....	438
	Contromisure contro AirSnort	438
	DWEPCrack	439
	Contromisure contro DWEPCrack.....	440
	WEPAttack	440
	Contromisure contro WEPAttack	441
	Contromisure contro gli attacchi al WEP	441
	LEAP.....	441
	Anwrap.....	442
	Contromisure contro Anwrap	442
	Asleep	442
	Contromisure contro Asleep	443
	WPA.....	443
	Attacchi all'algoritmo WPA.....	443
	Aircrack-ng.....	444
	Denial of Service.....	444
	Mettere in sicurezza WPA.....	444
	Risorse aggiuntive.....	445
	Riepilogo.....	447
Capitolo 9	Hacking di dispositivi hardware.....	449
	Accesso fisico: giungere alla porta.....	450
	Lock bumping.....	450
	Contromisure contro le bump key	451
	Clonazione delle carte di accesso	452

Contromisure contro la clonazione delle carte di accesso.....	456
Dispositivi di hacking.....	456
Bypass della sicurezza con password ATA	456
Contromisure contro l'hacking di password ATA	458
Hacking di USB U3.....	458
Contromisure contro l'hacking di USB U3.....	460
Configurazioni predefinite	461
Vulnerabilità preconfigurata	461
Password standard	461
Bluetooth	461
Reverse engineering di dispositivi hardware	462
Mappatura del dispositivo.....	462
Sniffing applicato ai dati del bus	464
Reversing del firmware.....	464
JTAG.....	468
Riepilogo.....	469

Parte IV Hacking di applicazioni e dati

Caso di studio: session riding.....	472
-------------------------------------	-----

Capitolo 10 Hacking del codice..... 475

Tecniche di exploit comuni.....	476
Buffer overflow e difetti di progettazione	476
Buffer overflow basati sullo stack.....	476
Contromisure contro i buffer overflow basati sullo stack.....	477
Overflow di heap/BSS/dati	479
Contromisure contro gli overflow basati su heap/BSS/dati	479
Attacchi attraverso stringa di formato.....	480
Contromisure contro gli attacchi con stringa di formato	481
Errori off-by-one	481
Contromisure contro gli errori off-by-one.....	481
Attacchi per validazione dell'input	482
Attacchi per canonicalizzazione	482
Contromisure contro la canonicalizzazione	484
Attacchi alle applicazioni web e ai database	484
Contromisure contro gli attacchi alle applicazioni web e ai database	484
Contromisure comuni	485
Cambiare la cultura delle persone.....	485
Parlare a bassa voce	485
Portate un grosso bastone	485
La sicurezza migliora la qualità e l'efficienza	485
Portate la sicurezza dentro la governance.....	486
Misurate, misurate, misurate	486
Responsabilità	487
Processo: SDL (Security in the Development Lifecycle).....	487
Definite un ruolo di collegamento con il team di sviluppo.....	487
Formazione, formazione, formazione	488
Modellazione delle minacce.....	488
Checklist per il codice	489
Test sulla sicurezza	490
Auditing o revisione finale della sicurezza.....	493
Manutenzione	493
Mettere insieme il tutto	494
Tecnologia	494
Ambienti di esecuzione controllata.....	494
Librerie di validazione dell'input	495
Miglioramenti della piattaforma	495
Lettere consigliate	496
Riepilogo.....	496

Capitolo 11 Hacking del Web 497

Hacking di server web.....	498
File di esempio	499
Accesso al codice sorgente	500
Canonicalizzazione	500
Estensioni del server.....	501
Buffer overflow.....	503
Scanner di vulnerabilità per server web	504
Nikto	505
Nessus.....	505
Hacking di applicazioni web	506
Trovare applicazioni web vulnerabili con Google.....	506
Web crawling.....	507
Strumenti per il web crawling.....	507
Valutazione delle applicazioni web	509
Plug-in per i browser.....	509
Suite di strumenti.....	511
Scanner di sicurezza per applicazioni web	515
Le vulnerabilità più frequenti delle applicazioni web.....	519
Attacchi di Cross-Site Scripting (XSS).....	520
Contromisure contro il Cross-Site Scripting	522
SQL injection.....	522
Contromisure contro l'SQL injection	524
CSRF (Cross-Site Request Forgery).....	525
Contromisure contro il CSRF (Cross-Site Request Forgery)	526
HTTP Response Splitting	526
Contromisure contro l'HTTP Response Splitting.....	529
Uso errato dei tag nascosti.....	530
Contromisure contro la vulnerabilità dei tag nascosti.....	531
SSI (Server Side Include).....	531
Contromisure contro SSI.....	532
Riepilogo.....	532

Capitolo 12 Hacking dell'utente Internet 533

Vulnerabilità dei client Internet	534
Breve storia dell'hacking dei client Internet.....	534
Microsoft ActiveX	534
Contromisure contro gli abusi di ActiveX	536
Java	536
Contromisure contro gli abusi su Java.....	538
JavaScript e Active Scripting.....	538
Contromisure contro gli abusi su JavaScript/Active Scripting	538
Cookie	539
Contromisure contro gli abusi sui cookie	539
Cross-Site Scripting (XSS).....	540
Contromisure contro XSS	541
Vulnerabilità cross-frame/domain	541
LMZ (Local Machine Zone)	542
Il tag IFRAME.....	542
Controllo ActiveX per la guida in HTML.....	542
Attacchi SSL	542
Attacchi omografi.....	544
Contromisure per SSL	544
Payload e punti di inserimento.....	545
Hacking della posta elettronica.....	546
File allegati	546
MIME.....	548
Worm della Rubrica.....	548
Contromisure contro l'hacking della posta elettronica	549
Messaggistica istantanea.....	550
Exploit e contromisure per i client Internet di Microsoft.....	551

Buffer overflow nell'elaborazione GDI+ JPEG (IE6 SP1).....	551
Contromisure contro il buffer overflow nell'elaborazione GDI+ JPEG	552
Impropria canonicalizzazione dell'URL in IE	553
Contromisure contro l'impropria canonicalizzazione dell'URL in IE.....	554
Esecuzione locale del controllo della guida HTML in IE	555
Contromisure contro l'esecuzione in locale del controllo della guida HTML in IE.....	555
Contromisure generali lato client di Microsoft.....	556
Uso del controllo genitori di Windows Vista	557
Leggere i messaggi di posta elettronica in testo normale	558
Non siate creduloni in Internet.....	559
Perché non utilizzare client non Microsoft?	560
Attacchi socio-tecnici: phishing e furto d'identità	561
Tecniche di phishing.....	562
Contromisure contro il phishing.....	564
Software fastidioso e ingannevole: spyware, adware e spam	565
Tecniche comuni di inserimento	566
ASEP	566
Componenti aggiuntivi del browser web	566
Blocco, rilevamento e pulizia dei software fastidiosi e ingannevoli.....	567
Malware.....	568
Varianti di malware e tecniche comuni.....	569
Virus e worm.....	569
Rootkit e backdoor.....	570
Hacker Defender.....	573
Altri rootkit comuni.....	574
Bot e zombie.....	575
Rilevamento e pulizia del malware	576
Azioni immediate.....	576
Backup, azzeramento e ricostruzione	577
Rilevamento e pulizia.....	577
Riepilogo.....	580

Appendice A Porte..... 581

Appendice B Le 14 vulnerabilità più importanti 585

**Appendice C Attacchi DoS(Denial of Service)
e DDoS (Distributed Denial of Service) 587**

Indice analitico..... 591