

Indice

Gli autori	xv
Prefazione	xxi
Introduzione	xxiii
Parte I	Inquadrare il bersaglio	1
	Caso di studio	2
	L'anonimato è fondamentale.....	2
	Tor-mentare le brave persone.....	3
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.....	13
	Informazioni sul personale.....	15
	Eventi in corso	17
	Politiche per la privacy e la sicurezza e dettagli tecnici che indicano i meccanismi di sicurezza attivi.....	19
	Informazioni archiviate.....	19
	Motori di ricerca e relazioni tra i dati	20
	Altre informazioni di interesse	24
	Contromisure per la sicurezza dei database pubblici.....	25
	Passo 4: enumerazione di server WHOIS e DNS	25
	Ricerche relative ai domini.....	27
	Ricerche relative all'IP.....	29
	Altre contromisure per la sicurezza dei database pubblici	32
	Passo 5: interrogazione del DNS	33
	Trasferimenti di zona.....	33
	Determinare i record MX (Mail eXchange).....	38
	Contromisure per la sicurezza del DNS	38
	Passo 6: riconoscimento della rete	39
	Tracerouting.....	39
	Contromisure contro il riconoscimento della rete	41
	Riepilogo.....	42
Capitolo 2	La scansione	43
	Determinare se il sistema è attivo.....	44
	Ping sweep di rete	44
	Ricerca di host ARP.....	44
	Arp-scan	44
	La ricerca di host ICMP	47
	Gli strumenti dei sistemi operativi.....	48
	Strumenti di rete	48

La ricerca di host TCP/UDP	51
Contromisure contro i ping sweep	54
Determinare quali servizi sono in esecuzione o in ascolto	56
Scansione di porte	56
Tipi di scansioni	56
Individuare i servizi TCP e UDP in esecuzione	58
Nmap	58
SuperScan	60
ScanLine	62
netcat	63
Contromisure contro la scansione di porte	64
Rilevamento del sistema operativo	65
Rilevamento del sistema operativo attivo	65
Ipotesi basate sulle porte disponibili	66
Fingerprinting attivo dello stack	66
Contromisure contro il rilevamento del sistema operativo	69
Identificazione passiva del sistema operativo	69
Fingerprinting passivo dello stack	70
Segnature passive	70
Contromisure contro il rilevamento passivo del sistema operativo	72
Elaborare e memorizzare i dati di una scansione	72
Gestire i dati di scansione con Metasploit	72
Riepilogo	74

Capitolo 3 L'enumerazione75

Fingerprinting di servizi	76
Scansione delle informazioni di versione con Nmap	77
Scansione delle informazioni di versione con Amap	78
Scanner di vulnerabilità	78
Scansione con Nessus	78
Contromisure contro la scansione con Nessus	79
Script NSE di Nmap	80
Cattura di banner	81
Le basi per la cattura di banner: telnet e netcat	81
Contromisure contro la cattura di banner	83
Enumerazione dei servizi di rete comuni	83
Enumerazione di FTP,TCP 21	83
Contromisure contro l'enumerazione di FTP	84
Enumerazione di telnet,TCP 23	85
Contromisure contro l'enumerazione di telnet	86
Enumerazione di SMTP,TCP 25	86
Contromisure contro l'enumerazione di SMTP	87
Enumerazione del DNS,TCP/UDP 53	87
Contromisure contro l'enumerazione del DNS	91
Enumerazione di TFTP,TCP/UDP 69	92
Contromisure contro l'enumerazione di TFTP	93
Enumerazione di finger,TCP/UDP 79	93
Contromisure contro l'enumerazione di finger	94
Enumerazione di HTTP,TCP 80	94
Contromisure contro l'enumerazione di HTTP	97
Enumerazione di MSRPC (<i>Microsoft RPC Endpoint Mapper</i>),TCP 135	98
Contromisure contro l'enumerazione di MSRPC	99
Enumerazione del servizio nomi NetBIOS, UDP 137	100
Bloccare l'enumerazione dei servizi di nomi NetBIOS	104
Enumerazione tramite sessione NetBIOS,TCP 139/445	104
Contromisure contro le sessioni null SMB	115
Enumerazione di SNMP, UDP 161	120
Contromisure contro l'enumerazione di SNMP	124
Enumerazione di BGP,TCP 179	125
Contromisure contro l'enumerazione di BGP	127
Enumerazione di LDAP di Windows Active Directory, TCP/UDP 389 e 3268	127
Contromisure contro l'enumerazione di Active Directory	129

Enumerazione di RPC UNIX, TCP/UDP 111 e 32771	131
Contromisure contro l'enumerazione di RPC	133
rwwho (UDP 513) e rusers (RPC Program 100002)	133
Contromisure contro l'impiego di rwho e rusers	133
Enumerazione di NIS, programma RPC 100004	134
Contromisure contro l'enumerazione di NIS	134
Enumerazione del servizio di risoluzione SQL, UDP 1434	134
Contromisure contro l'enumerazione di istanze SQL	135
Enumerazione di Oracle TNS, TCP 1521/2483	136
Contromisure contro l'enumerazione di Oracle TNS	136
Enumerazione di NFS, TCP/UDP 2049	137
Contromisure contro l'enumerazione di NFS	138
Enumerazione di IPSec/IKE, UDP 500	138
Contromisure contro l'enumerazione di IPSec/IKE	139
Riepilogo	140

Parte II Hacking del sistema..... 141

Caso di studio: intrigo internazionale	142
--	-----

Capitolo 4 Hacking di Windows 143

Panoramica	144
Argomenti non trattati	145
Attacchi senza autenticazione	145
Attacchi con falsificazione dell'autenticazione (spoofing)	146
Determinare la password da remoto	146
Contromisure contro l'individuazione delle password	149
Spiare lo scambio di password in rete	153
Contromisure contro lo sniffing delle procedure di autenticazione Windows	155
Attacchi Man-in-the-Middle	156
Contromisure contro gli attacchi MITM	158
Pass-the-Hash	158
Contromisure per l'attacco Pass-the-hash	159
Pass the Ticket per Kerberos	160
Exploit senza autenticazione da remoto	161
Exploit dei servizi di rete	161
Contromisure contro l'exploit di servizi di rete	163
Exploit di applicazioni dell'utente finale	164
Contromisure contro l'exploit di applicazioni dell'utente finale	165
Exploit dei driver di periferica	166
Contromisure contro l'exploit dei driver	167
Attacchi con autenticazione	167
Scalata dei privilegi	168
Prevenire la scalata dei privilegi	168
Estrazione e cracking di password	169
Catturare gli hash di password	170
Contromisure contro pwdump	172
Cracking delle password	172
Contromisure contro il cracking delle password	177
Dumping di password memorizzate nella cache	178
Contromisure contro il dumping delle password memorizzate nella cache	181
Dumping di hash registrati in memoria	181
Contromisure contro il dumping di hash registrati in memoria	182
Controllo remoto e backdoor	183
Strumenti per il controllo remoto dalla riga di comando	183
Controllo remoto con GUI	184
Reindirizzamento delle porte	186
fpipe	187
Coprire le proprie tracce	189
Disabilitare il controllo di Windows (auditing)	189
Cancellazione del registro di eventi	189
Nascondere i file	190

Contromisure contro gli ADS	191
Rootkit	191
Contromisure generali contro	
la violazione della procedura di autenticazione	191
Nomi di file	192
Voci del registro di sistema	192
Processi	194
Porte	194
Funzionalità di sicurezza di Windows	195
Windows Firewall	195
Aggiornamenti automatici	196
Centro sicurezza PC Windows	197
Criteri di protezione e criteri di gruppo	198
Microsoft Security Essentials	200
Enhanced Mitigation Experience Toolkit	200
Bitlocker e l'Encrypting File System	200
Contromisure contro l'attacco di avvio a freddo	201
Protezione di risorse Windows con WRP	202
Livelli di integrità, UAC e PMIE	203
Protezione esecuzione programmi	204
Windows Service Hardening: protezione avanzata di servizi Windows	205
Isolamento del servizio	205
Servizi con privilegi minimi	206
Refactoring di servizi	207
Accesso di rete ristretto	207
Isolamento della sessione 0	207
Miglioramenti basati sul compilatore	209
Il peso della sicurezza di Windows	210
Riepilogo	210

Capitolo 5 Hacking di UNIX 213

Alla conquista di root	213
Un breve riepilogo	214
Mappatura delle vulnerabilità	214
Accesso remoto e accesso locale	215
Accesso remoto	216
Attacchi di forza bruta	217
Contromisure contro gli attacchi di forza bruta	218
Attacchi data-driven	220
Attacchi di buffer overflow	220
Contromisure contro l'attacco di buffer overflow	221
Attacchi return-to-libc	224
Contromisure per gli attacchi return-to-libc	225
Attacchi con stringhe di formato	226
Contromisure contro l'attacco con stringa di formato	227
Attacchi a validazione dell'input	228
Contromisura contro l'attacco a validazione dell'input	229
Attacchi integer overflow e integer sign	229
Contromisure contro l'attacco di integer overflow	233
Attacchi dangling pointer (puntatore pendente)	233
Contromisure contro i puntatori pendenti	234
Voglio la mia shell	234
Telnet inverso e canali di ritorno	235
Contromisure contro gli attacchi con canale di ritorno	238
Tipi comuni di attacchi remoti	238
FTP	238
Contromisure contro gli attacchi a FTP	239
Sendmail	240
Contromisure contro gli attacchi a sendmail	240
Servizi RPC (<i>Remote Procedure Call</i>)	241
Contromisure contro gli attacchi a servizi RPC	242
NFS	242
Contromisure contro gli attacchi a NFS	247

Vulnerabilità di X	247
Contromisure contro le vulnerabilità di X.....	249
DNS (<i>Domain Name System</i>)	249
Avvelenamento della cache DNS.....	249
Contromisure all'attacco del DNS	251
Vulnerabilità di SSH	251
Vulnerabilità challenge-response di OpenSSH.....	252
Contromisure per SSH	253
Attacchi a OpenSSL	253
Contromisure per attacchi a OpenSSL.....	254
Attacchi contro Apache	254
Contromisure per attacchi contro Apache	255
Accesso locale	255
Vulnerabilità della password	255
John the Ripper	257
Contromisure contro le vulnerabilità delle password.....	260
Buffer overflow locale.....	260
Contromisure contro il buffer overflow locale	261
Collegamenti simbolici	261
Contromisure contro la vulnerabilità dei collegamenti simbolici.....	262
Corse critiche (race condition)	262
Contromisure contro la vulnerabilità nella gestione dei segnali	264
Manipolazione dei file core	264
Contromisure contro la vulnerabilità dei file core.....	264
Librerie condivise	264
Contromisure contro le vulnerabilità delle librerie condivise	265
Difetti del kernel	265
Contromisure contro i difetti del kernel.....	266
Errori di configurazione del sistema	266
Permessi su file e directory	267
Contromisure contro le vulnerabilità dei file SUID.....	269
File accessibili a tutti in scrittura	269
Contromisure contro la vulnerabilità dei file accessibili a tutti in scrittura.....	270
Accesso di root ottenuto: e ora?	271
Rootkit	271
Trojan	271
Contromisure contro i trojan	272
Sniffer	274
Che cos'è uno sniffer?	274
Funzionamento degli sniffer	275
Alcuni sniffer noti.....	275
Contromisure contro gli sniffer.....	276
Cancellazione dei log	277
Contromisure contro la cancellazione dei log.....	281
Rootkit del kernel.....	281
Contromisure contro i rootkit del kernel	283
Che cosa fare in caso di attacco con rootkit.....	284
Riepilogo.....	285

Capitolo 6

Crimini cibernetici

e minacce avanzate persistenti (APT) 287

Che cos'è un APT?	288
Operazione Aurora	291
Anonymous.....	294
RBN.....	294
Che cosa non sono gli APT.....	295
Esempi di strumenti e tecniche APT	296
Attacco Gh0st	296
Email malevola	297
Indicatori di compromissione	298
Immagine della memoria.....	299

Riepilogo dell'attacco Gh0St.....	318
Attacco APT a Linux.....	318
Host linux perso.....	319
Indicatori di compromissione.....	320
Riepilogo dell'attacco APT a Linux.....	326
Poison Ivy.....	326
TDSS (TDL1-4).....	329
Indicatori comuni di APT.....	330
Rilevamento di attacchi APT.....	333
Contromisure contro gli attacchi APT.....	335
Riepilogo.....	335

Parte III **Hacking delle infrastrutture 337**

Caso di studio: leggi e WEP.....	338
----------------------------------	-----

Capitolo 7 **Connettività remota e hacking VoIP 341**

Preparazione alla connessione dial-up.....	342
Footprinting del numero telefonico.....	342
Contromisure contro le fughe di informazioni.....	344
Wardialing.....	344
Hardware.....	344
Aspetti legali.....	345
Costi accessori.....	346
Software.....	346
WarVOX.....	347
TeleSweep.....	352
PhoneSweep.....	354
Tecniche di exploit del carrier.....	357
Script di forza bruta: il fai-da-te.....	359
LHF (<i>Low Hanging Fruit</i>).....	361
Autenticazione singola, tentativi illimitati.....	361
Autenticazione singola, tentativi limitati.....	365
Autenticazione duale, tentativi illimitati.....	366
Autenticazione duale, tentativi limitati.....	367
Nota conclusiva sugli script per attacchi di forza bruta.....	368
Misure di sicurezza per le connessioni dial-up.....	368
Hacking di centralini telefonici.....	370
Login su reti voicemail Octel.....	371
Centralini Williams/Northern Telecom.....	371
Centralini Meridian Links.....	372
Centralini Rolm PhoneMail.....	372
Centralino protetto da RSA SecurID.....	373
Contromisure contro l'hacking dei centralini.....	373
Hacking di sistemi voicemail.....	373
Hacking di sistemi voicemail a forza bruta.....	373
Contromisure contro gli attacchi di forza bruta a voicemail.....	377
Hacking di DISA (<i>Direct Inward System Access</i>).....	377
Contromisure per l'hacking di DISA.....	378
Hacking delle reti VPN (<i>Virtual Private Network</i>).....	378
Nozioni di base sulle VPN IPSec.....	379
Autenticazione e impostazione del tunnel in reti VPN IPSec.....	380
Google hacking per VPN.....	380
Contromisure contro Google hacking per VPN.....	381
Attacchi a server VPN IPSec.....	382
Contromisure contro gli attacchi a VPN IPSec.....	383
Attacco all'aggressive mode di IKE.....	383
Contromisure contro gli attacchi all'aggressive mode di IKE.....	385
Hacking della soluzione VPN di Citrix.....	385
La Guida.....	387
Microsoft Office.....	388
Internet Explorer.....	390
Giochi e Calcolatrice Microsoft.....	393
Gestione attività.....	393

La stampa	394
I link	395
Accesso a Internet	396
EULA/Editor di testo.....	398
Salva con nome/Accesso al file system	398
Contromisure per l'hacking di Citrix	400
Attacchi a Voice over IP.....	402
Vari tipi di attacchi a VoIP	403
Scansione SIP.....	404
Contromisure contro la scansione SIP	405
Saccheggiare TFTP alla ricerca di tesori VoIP	405
Contromisure contro il saccheggio di TFTP.....	406
Enumerazione di utenti SIP.....	406
Enumerazione dell'utente con REGISTER di Asterisk	407
Enumerazione dell'utente con OPTIONS di SIP EXpress Router.....	409
Enumerazione dell'utente automatizzata	410
Il processo di avvio dei telefoni IP Cisco.....	413
Enumerazione degli utenti Cisco	414
Contromisure contro l'enumerazione SIP	414
Attacco di intercettazione	414
Attacchi offline.....	419
Contromisure contro l'intercettazione.....	421
DoS (<i>Denial of Service</i>).....	422
Contromisure contro il flood SIP INVITE	423
Riepilogo.....	423

Capitolo 8 Hacking di reti wireless 425

Nozioni di base.....	426
Frequenze e canali	426
Avvio della sessione	427
Meccanismi di sicurezza	428
Meccanismi di base.....	428
Autenticazione	428
Cifratura.....	429
Strumenti di hacking.....	430
Adattatori wireless	430
Chipset	430
Compatibilità con le bande.....	431
Compatibilità con le antenne.....	431
Interfaccia	431
Sistemi operativi	432
Accessori vari	432
Antenne	432
GPS	433
Access point	433
Ricerca e monitoraggio di reti wireless.....	434
Ricerca di reti wireless.....	434
Rilevamento attivo	434
Contrastare il rilevamento attivo	434
Rilevamento passivo	434
Strumenti di ricerca.....	435
Proteggersi dal rilevamento passivo	437
Sniffing del traffico wireless.....	437
Wireshark.....	437
Proteggersi dallo sniffing wireless.....	438
Attacchi DoS (<i>Denial of Service</i>)	438
Attacco di deautenticazione	439
aireplay-ng	439
Evitare gli attacchi di deautenticazione.....	439
Attacchi contro i sistemi di cifratura	440
Attacchi contro l'algoritmo WEP	440
Attacco passivo	441
ARP replay con falsa autenticazione	442

Contromisure per l'attacco contro algoritmi WEP.....	444
Attacchi contro i sistemi di autenticazione.....	444
Chiave precondivisa WPA.....	444
Intercettare la procedura di handshaking a quattro vie.....	445
Forza bruta.....	445
Riduzione dei rischi legati a WPA-PSK.....	448
WPA Enterprise.....	449
Identificare i tipi di EAP.....	449
LEAP.....	450
Protezione di LEAP.....	451
EAP-TTLS e PEAP.....	451
Protezione di EAP-TTLS PEAP.....	453
Riepilogo.....	453

Capitolo 9 Hacking di dispositivi hardware..... 455

Accesso fisico: giungere alla porta.....	456
Lock bumping.....	456
Contromisure contro le bump key.....	457
Clonazione delle carte di accesso.....	458
Contromisure contro la clonazione delle carte di accesso.....	461
Dispositivi di hacking.....	462
Bypass della sicurezza con password ATA.....	462
Contromisure contro l'hacking di password ATA.....	464
Hacking dello standard U3 USB.....	464
Contromisure contro l'hacking di standard U3 di USB.....	466
Configurazioni predefinite.....	466
Vulnerabilità preconfigurata.....	467
Password standard.....	467
Bluetooth.....	467
Reverse engineering di dispositivi hardware.....	468
Mappatura del dispositivo.....	469
Rimuovere le protezioni fisiche.....	469
Identificare i chip del circuito integrato.....	469
Le interfacce esterne.....	471
Sniffing applicato ai dati del bus.....	472
Sniffing dell'interfaccia wireless.....	474
Reversing del firmware.....	475
I programmatori di EEPROM.....	479
Strumenti di sviluppo per microcontrollori.....	480
Gli strumenti ICE.....	480
JTAG.....	481
Riepilogo.....	483

Parte IV Hacking di applicazioni e dati..... 485

Capitolo 10 Hacking del Web e di database..... 487

Hacking di server web.....	488
File di esempio.....	489
Accesso al codice sorgente.....	490
Attacchi di canonicalizzazione.....	490
Estensioni del server.....	491
Buffer overflow.....	493
DoS (<i>Denial of Service</i>).....	494
Scanner di vulnerabilità per server web.....	495
Nikto.....	495
Nessus.....	496
Hacking di applicazioni web.....	496
Trovare applicazioni web vulnerabili con Google (Googledorks).....	496
Web crawling.....	497
Strumenti per il web crawling.....	498
Valutazione delle applicazioni web.....	499
Plug-in per i browser.....	500
Suite di strumenti.....	501

Scanner di sicurezza per applicazioni web	504
Le vulnerabilità più frequenti delle applicazioni web	510
Attacchi di Cross-Site Scripting (XSS)	511
Contromisure contro il Cross-Site Scripting	512
SQL injection.....	512
Contromisure contro l'SQL injection	515
CSRF (<i>Cross-Site Request Forgery</i>)	516
Contromisure contro il CSRF (<i>Cross-Site Request Forgery</i>)	517
HTTP Response Splitting	517
Contromisure contro l'HTTP Response Splitting.....	519
Uso errato dei tag nascosti	520
Contromisure contro la vulnerabilità dei tag nascosti.....	521
SSI (<i>Server Side Include</i>)	521
Contromisure contro SSI.....	522
Hacking di database	522
Ricerca e individuazione di database.....	522
Contromisure contro la ricerca e l'individuazione di database.....	524
Vulnerabilità dei database	524
Attacchi di rete.....	524
Contromisure contro gli attacchi di rete.....	527
Bug del motore di database.....	527
Contromisure contro i bug del motore di database	528
Oggetti del database vulnerabili	528
Contromisure contro gli oggetti del database vulnerabili	531
Password deboli o predefinite.....	531
Contromisure contro le password deboli o predefinite.....	534
Configurazioni errate	534
Contromisure contro le configurazioni errate	535
Attacchi indiretti	535
Contromisure contro gli attacchi indiretti	536
Altre considerazioni	536
Riepilogo.....	537

Capitolo 11 Hacking nel mondo mobile..... 539

Hacking di Android.....	540
Fondamenti di Android.....	542
Strumenti Android utili	545
Approccio ad Android	547
Hacking del vostro Android	547
Strumenti per il rooting di Android	548
Rooting di un Kindle Fire.....	550
L'Android Market ufficiale sul vostro Kindle	552
Applicazioni interessanti per periferiche Android rootate.....	554
App native su Android	555
Installazione di eseguibili nativi di sicurezza	
in un dispositivo Android rootato	557
Trojan app.....	559
Hacking di dispositivi Android altrui	561
Remote Shell via WebKit	562
Contromisure alla vulnerabilità dei floating point in WebKit	563
Rooting di un Android: RageAgainstTheCage.....	564
Contromisure per RATC	565
Vulnerabilità di furto dei dati	566
Contromisure alla vulnerabilità di furto dei dati	568
Shell remota con zero permessi.....	568
Contromisure agli attacchi di bypass dei permessi.....	571
Capability leak.....	571
Contromisure ai capability leak	572
Malware su URL.....	572
Contromisure al malware su URL	572
Vulnerabilità di Skype.....	573
Contromisure alle vulnerabilità di Skype.....	574
Carrier IQ	575

Contromisure per Carrier IQ	577
HTC Logger	577
Contromisure per HTC Logger	578
Crack del PIN di Google Wallet	578
Contromisure per il crack del PIN di Google Wallet	579
Android come piattaforma di hacking portatile	580
Difendere il proprio Android	583
iOS	584
Conoscere iPhone	585
iOS è sicuro?	587
Jailbreaking: sciogliamo le briglie!	588
Jailbreaking basato sul processo di boot	589
Jailbreak remoto	592
Hacking di telefoni altrui	593
Le vulnerabilità di JailbreakMe 3.0	596
Contromisure contro la vulnerabilità di JBME 3.0	597
Attacchi iKee!	597
Contromisure contro worm iKee/credenziali di default SSH	599
Attacco man-in-the-middle (FOCUS 11)	600
Contromisure contro l'hack di FOCUS 11	601
App malevole: Handy Light, InstaStock	602
Contromisure contro il malware sull'App Store	605
App vulnerabili: in bundle e di terze parti	605
Contromisure contro le vulnerabilità delle app	607
Accesso fisico	607
Contromisure per l'accesso fisico	608
Riepilogo	609

Capitolo 12 Ricettario di contromisure 611

Strategie generali	612
Spostare o eliminare gli elementi di valore	613
Separare i compiti	613
Prevenire, individuare e rispondere	613
Persone, processi e tecnologie	614
Verifiche e rendiconti	614
Autenticare, autorizzare e controllare	615
Stratificare	615
Miglioramento adattativo	617
Gestire i fallimenti	618
Criteri di protezione e formazione	618
Semplice, economico e facile	619
Scenari di esempio	619
Scenari desktop	619
Scenari server	620
Limitare i privilegi amministrativi	621
Ridurre al minimo la superficie esposta all'attacco	623
Curare particolarmente la manutenzione	624
Monitoraggio attivo, backup e risposta	625
Scenari di rete	625
Scenari di applicazioni web e database	626
Scenari nel mondo mobile	628
Riepilogo	629

Appendice A Porte..... 631

Appendice B Le 10 vulnerabilità più importanti 635

Appendice C Attacchi DoS (*Denial of Service*) e DDoS (*Distributed Denial of Service*) 637

Contromisure	639
--------------------	-----

Indice analitico..... 641