

# CONTENIDO

<b>Acerca de los autores</b> .....	xvii
<b>Agradecimientos</b> .....	xxi
<b>Prefacio</b> .....	xxiii
<b>Introducción</b> .....	xxvii

## PARTE I Identificar el problema

<b>1. Seguir el rastro. Consecución de objetivos</b> .....	3
¿Qué es seguir el rastro? .....	5
¿Por qué es necesario seguir el rastro? .....	6
Seguir el rastro por Internet .....	7
Paso 1. Determinación del ámbito de sus actividades.	7
Paso 2. Enumeración de la red .....	11
Paso 3. Interrogación del DNS .....	19
Paso 4. Reconocimiento de la red .....	25
Resumen .....	29
<b>2. Exploración</b> .....	31
Barridos ping de red .....	32
Contramedidas para barridos Ping .....	37
Consultas ICMP .....	39
Contramedidas para consultas ICMP .....	40

Exploración de puertos .....	41
Tipos de exploración .....	42
Cómo identificar la ejecución de servicios TCP y UDP .....	43
Desglose de la exploración de puertos .....	50
Contramedidas para la exploración de puertos .....	51
Detección del sistema operativo .....	55
Rastreo de pilas .....	55
Contramedidas para la detección de sistemas operativos .....	58
El revoltillo completo: herramientas automáticas de descubrimiento .....	59
Contramedidas para las herramientas automáticas de descubrimiento ...	59
Resumen .....	60
<b>3. Enumeración .....</b>	<b>61</b>
Introducción .....	62
Windows NT .....	62
Enumeración Novell .....	77
Enumeración en UNIX .....	81
Resumen .....	89
<b>PARTE II</b>	
<b>Hacking del sistema</b>	
<b>4. Hacking de Windows 95/98 .....</b>	<b>93</b>
Introducción .....	94
Asalto Remoto a Win 9x .....	94
Conexión directa a recursos compartidos de Win 9x .....	96
Puertas traseras en Win 9x .....	102
Vulnerabilidades conocidas de aplicaciones de servidor .....	106
Negación de servicio en Win 9x .....	106
Hacking de Win 9x desde la consola .....	107
Cómo saltarse la seguridad en Win 9x: ¡Reiniciar! .....	107
Métodos furtivos I: ejecución automática y descifrado de la contraseña del salvapantallas .....	108
Métodos furtivos II: mostrar las contraseñas de Win 9x en memoria .....	110
Métodos furtivos III: cracking .....	111
Resumen .....	114
<b>5. Hacking de Windows NT .....</b>	<b>115</b>
Un breve resumen .....	117
Hacia dónde nos dirigimos .....	117
La búsqueda del administrador .....	118
Adivinar contraseñas en la red .....	119
Contramedidas: cómo defenderse de la adivinación de contraseñas .....	124

Ataques remotos: negación de servicio y desbordamiento de memoria búfer.....	132
Escalada de privilegios .....	134
Cómo consolidar la posición .....	142
Cómo hacer cracking del SAM .....	142
Abuso de confianza .....	153
Control remoto y puertas traseras .....	159
Puertas traseras y contramedidas generales .....	168
Cómo ocultar el rastro .....	173
Cómo desactivar la auditoría .....	173
Cómo borrar el registro de sucesos .....	174
Cómo ocultar archivos .....	174
Resumen .....	176
<b>6. Hacking de Novell NetWare .....</b>	<b>179</b>
Cómo conectarse sin tocar .....	180
On-Site Admin ( <i>ftp://ftp.cdrom.com/.1.novell/onsite.zip</i> ).....	181
snlist ( <i>ftp://ftp.it.ru/pub/netware/util/NetWare4.Toos/snlist.exe</i> ) y nslis ( <i>http://www.nmrc.org/files/snetware/nutl8.zip</i> ).....	182
Contramedida para la conexión.....	182
Enumeración de enlaces y árboles .....	182
userinfo ( <i>ftp://ftp.cdrom.com/.1/novell/userinfo.zip</i> ) .....	183
userdump ( <i>ftp://ftp.cdrom.com/.1/novell/userdump.zip</i> ) .....	183
finger ( <i>ftp://ftp.cdrom.com/.1/novell/finger.zip</i> ).....	183
bindery ( <i>http://www.nmrc.org/files/netware/bindery.zip</i> ) .....	184
bindin ( <i>ftp://ftp.edv-himmelbauer.co.at/Novell.3x/TESTPROG/BIN-             DIN.EXE</i> ) .....	184
nlist ( <i>SYS:PUBLIC</i> ).....	185
cx ( <i>SYS:PUBLIC</i> ) .....	186
Administrador de On-Site.....	188
Contramedida para enumeración.....	188
Cómo abrir las puertas no bloqueadas .....	189
chknul ( <i>http://www.nmrc.org/files/netware/chknul.zip</i> ) .....	189
Contramedida para chknul.....	190
Enumeración autenticada .....	190
userlist /a .....	191
Administrador On-Site .....	191
NDSsnoop ( <i>ftp://ftp.iae.univ-poitiers.fr/pc/netware/UTIL/ndssnoop.             exe</i> ). .....	192
Detección del bloqueo de intruso.....	192
Contramedida para la detección de bloqueo de intruso .....	195
Cómo obtener la cuenta del Administrador.....	195
Saqueo .....	195
Contramedida para el saqueo .....	196

Nwpcrack ( <a href="http://www.nmrc.org/files/netware/nwpcrack.zip">http://www.nmrc.org/files/netware/nwpcrack.zip</a> ) .....	196
Contramedidas para Nwpcrack .....	197
Vulnerabilidades de aplicación .....	198
NetWare Perl ( <a href="http://www.insecure.org/sploits/netware.perl.nlm.html">http://www.insecure.org/sploits/netware.perl.nlm.html</a> ) .....	198
Contramedida para NetWare Perl .....	199
NetWare FTP ( <a href="http://www.nmrc.org/faqs/netwar/nw_sec12.html#12-2">http://www.nmrc.org/faqs/netwar/nw_sec12.html#12-2</a> ) .....	199
Contramedida para NetWare FTP .....	199
Servidor NetWare Web ( <a href="http://www.nmrc.org/faqs/netware/nt_sec12.html@12-1">http://www.nmrc.org/faqs/netware/nt_sec12.html@12-1</a> ) .....	200
Contramedida para el servidor NetWare Web .....	200
Ataques con trampas (Pandora) .....	200
Gameover .....	201
Contramedida para Pandora .....	202
Una vez obtenidos los privilegios de Administrador en un servidor .....	203
Hacking de rconsole .....	203
Contramedida para rconsole (contraseñas sin cifrar) .....	204
Apropiación de los archivos NDS .....	205
NetBasic.nlm (SYS:SYSTEM) .....	205
Dsmaint ( <a href="http://www.support.novell.com/cgi-bin/search/patlstfind.cgi?2947447">http://www.support.novell.com/cgi-bin/search/patlstfind.cgi?2947447</a> ) .....	206
Jcmd ( <a href="ftp://ftp.cdrom.com/1/novell/jrb400a.zip">ftp://ftp.cdrom.com/1/novell/jrb400a.zip</a> o <a href="http://www.jrbsoftware.com">http://www.jrbsoftware.com</a> ) .....	207
Contramedida para Grabbing NDS (captura de NDS) .....	208
Cracking de los archivos NDS .....	208
Manipulación de registros .....	210
Desactivación de Auditoría .....	211
Modificación de la historia de archivos .....	211
Console Logs (registros de consola) .....	212
Contramedida para la manipulación del registro .....	212
Puertas traseras .....	212
Contramedida para puerta trasera .....	214
Recursos adicionales .....	215
Kane Security Analyst ( <a href="http://www.intrusion.com">http://www.intrusion.com</a> ) .....	215
Web Sites ( <a href="ftp://ftp.novell.com/pub/updates/nw/nw411/">ftp://ftp.novell.com/pub/updates/nw/nw411/</a> ) .....	215
Grupos usenet .....	215
<b>7. UNIX</b> .....	<b>217</b>
La búsqueda del directorio raíz .....	218
Un breve repaso .....	218
Mapa de vulnerabilidades .....	219
Acceso remoto frente a acceso local .....	220
Acceso remoto .....	220
Ataques de fuerza bruta .....	222
Contramedida para la fuerza bruta .....	223

Ataques dirigidos a datos .....	223
Ataques con validación de entrada .....	228
Yo quiero mi Shell .....	230
Tipos comunes de ataques remotos .....	234
Acceso local .....	248
Vulnerabilidades de composición de contraseña .....	249
Desbordamiento de búfer local .....	252
Symlink .....	254
Ataques mediante descriptor de archivos .....	256
Condiciones de carreras .....	258
Manipulación de archivos core .....	259
Bibliotecas compartidas .....	260
Mala configuración del sistema .....	261
Ataques a la shell .....	265
Después de hacer hacking a la cuenta del Administrador .....	267
Rootkits .....	267
Troyanos .....	267
Sniffers .....	269
Limpieza del registro .....	272
Resumen .....	275

**PARTE III**  
**Hacking de la red**

<b>8. Hacking de VPN y del acceso telefónico .....</b>	<b>281</b>
Introducción .....	282
Identificación del número telefónico .....	283
Contra medida: detenga las filtraciones .....	286
Wardialing .....	287
Hardware .....	287
Temas legales .....	288
Costes adicionales .....	288
Software .....	288
Técnicas de explotación de la portadora .....	299
Medidas de seguridad para marcación telefónica .....	301
Hacking a la Red Privada Virtual (VPN) .....	303
Resumen .....	306
<b>9. Dispositivos de red .....</b>	<b>309</b>
Descubrimiento .....	310
Detección .....	310
SNMP .....	316

Puertas traseras .....	319
Cuentas predeterminadas .....	319
Rebajar las puertas (vulnerabilidades) .....	322
Compartido frente a conmutado .....	329
Detectar el medio donde estamos .....	330
Captura de información SNMP .....	331
Grupos SNMP .....	332
Contramedida para grupos SNMP .....	333
Engaño RIP .....	333
Contramedida para el engaño RIP .....	333
Resumen .....	333
<b>10. Cortafuegos .....</b>	<b>335</b>
Panorámica de los cortafuegos .....	336
Identificación de cortafuegos .....	337
Exploración directa: la técnica ruidosa .....	337
Contramedidas .....	338
Trazado de ruta .....	339
Contramedidas .....	340
Captura de mensajes .....	341
Contramedida .....	342
Cómo descubrir el cortafuegos avanzado .....	342
Identificación de puertos .....	346
Contramedidas .....	346
Exploración a través de los cortafuegos .....	347
hping .....	347
Contramedida .....	349
Firewalking .....	349
Contramedida .....	350
Filtrado de paquetes .....	350
ACL tolerantes .....	350
Contramedida .....	350
El truco de Check Point .....	351
Contramedida .....	351
Tunelización ICMP y UDP .....	352
Contramedida .....	353
Vulnerabilidades de proxy de aplicación .....	353
Hostname: localhost .....	353
Contramedida .....	354
Acceso proxy externo sin autenticar .....	354
Contramedida .....	355
Vulnerabilidades WinGate .....	355
Resumen .....	360

<b>11. Ataques de negación de servicio (DoS)</b> .....	<b>363</b>
Motivación de los atacantes DoS .....	364
Tipos de ataques DoS .....	365
Consumo de ancho de banda .....	365
Inanición de recursos .....	366
Defectos de programación .....	366
Ataques DNS y de enrutamiento .....	367
Ataque DoS genérico .....	367
Smurf .....	368
Inundación SYN .....	371
Ataques DNS .....	375
DoS en UNIX y Windows NT .....	376
Ataque DoS remoto .....	376
Ataques DoS locales .....	378
Resumen .....	380

PARTE IV  
**Hacking del software**

<b>12. Inseguridades de control remoto</b> .....	<b>383</b>
Descubrir el software de control remoto .....	385
Conectarse .....	386
Debilidades .....	387
Nombres de usuario y contraseñas sin encriptar .....	387
Contraseñas ocultas .....	388
Contraseñas reveladas .....	388
Carga de perfiles .....	389
Contra medidas .....	390
Habilitar contraseñas .....	390
Contraseñas fuertes .....	391
Obligar a la autenticación alternativa .....	391
Archivos de configuración y archivos de perfiles de protección de contraseñas .....	392
Cierre de sesión del usuario una vez finalizada la llamada .....	393
Encriptar el tráfico de la sesión .....	393
Limitar los intentos de inicio de sesión .....	393
Registrar los intentos fallidos .....	393
Bloqueo de usuarios fallidos .....	394
Cambiar el puerto de escucha predeterminado .....	394
¿Qué paquete de software es el mejor en términos de seguridad? .....	394
pcAnywhere .....	394
ReachOut .....	395
Remotely Anywhere .....	395

Remotely Possible/ControlIT .....	396
Timbuktu .....	397
Virtual Network Computing (VNC) .....	397
Citrix .....	397
Resumen .....	398
<b>13. Técnicas avanzadas .....</b>	<b>399</b>
Hijacking de sesión .....	400
Juggernaut .....	400
Hunt .....	401
Contramedidas para el hijacking .....	403
Puertas traseras .....	403
Cuentas de usuario .....	403
Archivos de inicio .....	404
Trabajos programados .....	405
Puertas traseras con control remoto .....	407
Contramedidas para el control remoto .....	412
Contramedidas globales para las puertas traseras .....	417
Troyanos .....	417
Whack-A-Mole .....	418
BoSniffer .....	418
eLiTeWrap .....	418
Windows NT FPWNCLNT.DLL .....	419
Resumen .....	420
<b>14. Hacking en la Web .....</b>	<b>423</b>
Sisar en la web .....	424
Página a página .....	424
¡Simplificar! .....	425
Contramedida al pilfering de la Web .....	427
Buscar vulnerabilidades conocidas .....	427
Scripts automatizados para los «Script Kiddies» .....	428
Aplicaciones automatizadas .....	429
Insuficiencias de script: ataques de validación de entrada .....	431
Vulnerabilidad IIS 4.0 MDAC RDS .....	432
Vulnerabilidades de Active Server Pages (ASP) .....	439
Vulnerabilidades Cold Fusion .....	441
Desbordamientos de búfer .....	442
Vulnerabilidad PHP .....	443
Diseño web pobre .....	445
Empleo erróneo de las etiquetas ocultas .....	445
Server Side Includes (SSI) .....	446
Añadir a archivos .....	447
Resumen .....	447



Parte V  
**Apéndices**

<b>A. Puertos</b> .....	451
<b>B. Temas de seguridad en Windows 2000</b> .....	455
Identificación .....	457
Exploración .....	458
Enumeración .....	460
El objetivo evidente: directorio activo .....	460
Sesiones nulas .....	462
Penetración .....	463
Estimación de la compartición de archivos de NetBIOS .....	463
Escuchando los hashes de la contraseña .....	463
Desbordamiento de búfer .....	463
Negación de servicio .....	464
Escalada de privilegios .....	464
getadmin y sechole .....	464
Cómo hacer cracking a las contraseñas .....	464
Pilfering .....	465
Cómo sacar partido de la confianza .....	465
Borrado de huellas .....	466
Desactivación de la auditoría .....	467
Borrado del registro de sucesos .....	467
Ocultación de archivos .....	467
Puertas traseras .....	468
Manipulación de inicio .....	468
Control remoto .....	468
Registros de pulsaciones de teclas .....	469
Contra medidas de tipo general: nuevas herramientas de seguridad para Windows .....	469
Directiva de grupo .....	469
Resumen .....	472
<b>C. Recursos y enlaces</b> .....	473
Conferencias .....	474
Diccionarios .....	474
Encriptación .....	475
Hackers famosos .....	475
Footprinting .....	475
Servicios gateway .....	475
Sitios de seguridad general .....	476
Gobierno .....	476
Endurecimiento .....	477

Información warfare .....	477
Canales irc .....	477
Legal .....	478
Listas de correo y boletines .....	478
Noticias y editoriales .....	478
Grupos de seguridad .....	478
Organismos estándar .....	479
Contactos con fabricantes .....	479
Vulnerabilidades y programas de ataque .....	479
Web y seguridad de aplicaciones .....	480
<b>D. Herramientas .....</b>	<b>481</b>
One-stop tool shopping .....	482
Herramientas de contramedida .....	482
Negación de servicio .....	483
Herramientas de enumeración .....	483
Herramientas de Footprinting .....	484
Conseguir acceso .....	484
Herramientas de penetración y puertas traseras .....	485
Pilfering .....	485
Rootkits y ocultación de huellas .....	486
Herramientas de exploración .....	486
Herramientas de guerra telefónica .....	486
<b>E. Las catorce principales vulnerabilidades de seguridad .....</b>	<b>487</b>
Las catorce principales vulnerabilidades de la seguridad .....	488
<b>F. Nuestra página Web .....</b>	<b>489</b>
Novell .....	490
Unix .....	490
Windows NT .....	491
Listas de palabras y diccionarios .....	492
Guerra telefónica .....	492
Scripts de enumeración .....	492
<b>Índice .....</b>	<b>493</b>