

Contenido

Prólogo	23
Sobre Bob Ayers	26
Prefacio	27
Estándares de evaluación reconocidos	28
NSA IAM	28
CESG CHECK	29
Definición de Hacker	31
Organización	31
¿A quién va dirigido este libro?	33
Encontrar las herramientas mencionadas en este libro	33
Utilizar los ejemplos de código	34
Reconocimientos	34
Capítulo 1. Evaluación de la seguridad de redes	37
Los beneficios empresariales	37
IP: la creación de Internet	38
Clasificación de los atacantes basados en Internet	39
Definiciones de servicios de evaluación	40
Metodología de evaluación de la seguridad de una red	41

Enumeración de servidores y redes de Internet	41
Rastreo masivo y sondeo de la red	42
Investigación de vulnerabilidades	43
Explotación de las vulnerabilidades	44
La aproximación de la evaluación cíclica	44
Capítulo 2. Las herramientas necesarias	47
Los sistemas operativos	47
Las plataformas de la familia Windows NT	48
Linux	48
Mac OS X	48
VMware	49
Herramientas de rastreo de red gratuitas	49
nmap	49
Nessus	49
NSAT	50
Foundstone SuperScan	51
Herramientas comerciales de rastreo de redes	51
Herramientas de evaluación dependientes del protocolo	52
Microsoft NetBIOS, SMB y CIFS	52
Herramientas de enumeración y obtención de información	52
Herramientas de ruptura de contraseñas mediante fuerza bruta	53
DNS	54
HTTP y HTTPS	54
Capítulo 3. Enumeración de servidores de Internet y de redes	57
Motores de búsqueda Web	57
Funcionalidad de búsqueda avanzada de Google	58
Enumerar detalles de contacto de la CIA con Google	59
Cadenas de búsqueda eficaces	60
Buscar en grupos de noticias	61
Consultas NIC	62
Herramientas y ejemplos de consultas NIC	62
Utilizar el cliente Sam Spade Windows	62
Utilizar la utilidad whois de Unix	63
Consultar ARIN directamente	64

Recopilar detalles de los usuarios mediante WHOIS	64
Consultas DNS	66
Consultas DNS avanzadas	67
Consultas DNS avanzadas utilizando nslookup	67
Consultas DNS avanzadas utilizando host	68
Consultas DNS avanzadas utilizando dig	68
Información obtenida mediante consultas DNS avanzadas	69
Técnicas de transferencia de zona DNS	69
Realizar transferencias de zona DNS con nslookup	70
Información obtenida mediante la transferencia de zona DNS	72
Realizar transferencias de zona DNS utilizando host y dig	73
Consultas avanzadas	73
Realizar mapas de subdominios utilizando host	73
Ejemplo de rechazo en la realización de una transferencia de zona DNS	74
Barrido de DNS inverso	74
Sondeo SMTP	75
Resumen de las técnicas de enumeración	76
Contramidas para la enumeración	77
Capítulo 4. Exploración de redes IP	79
Sondeo ICMP	80
SING	82
nmap	83
Obtener direcciones IP internas	84
Identificar direcciones de amplia difusión para subredes	85
Explorar puertos TCP	86
Métodos de rastreo estándar	86
Rastreo vainilla connect()	87
Rastreo de indicador SYN medio abierto	88
Métodos sigilosos de rastreo TCP	91
Rastreo de indicador TCP inverso	91
Rastreo de sondeo de indicador ACK	93
Métodos de rastreo TCP desde terceras partes y con suplantación de identidad	94
Rastreo de rebote FTP	94

Rastreo de rebote en proxy	96
Rastreo de identidad suplantada basado en sniffer	97
Rastreo de cabecera del identificador de IP	98
Rastreo de puertos UDP	100
Herramientas que realizan el rastreo de puertos UDP	101
Eludir los sistemas IDS y burlar el filtrado	102
Fragmentar paquetes de sondeo	103
fragtest	103
fragroute	104
nmap	105
Simular múltiples equipos atacantes	106
Direccionamiento de origen	107
Evaluar vulnerabilidades del direccionamiento de origen	109
Utilizar puertos de origen TCP y UDP específicos	111
Evaluación IP de bajo nivel	113
Analizar las respuestas a los sondeos TCP	113
hping2	114
firewalk	115
Monitorizar pasivamente las respuestas ICMP	117
Marcaje para la identificación de IP	117
Secuencia TCP e incremento del ID de IP	119
Resumen del rastreo de redes	119
Contra medidas contra el rastreo de redes	121
Capítulo 5. Evaluar servicios de información remotos	123
Servicios de información remotos	123
systat y netstat	124
DNS	125
Obtener información sobre la versión de los servicios DNS	126
Transferencias de zona DNS	127
Fugas de información DNS y ataques de búsqueda inversa	128
Vulnerabilidades BIND	130
Vulnerabilidad de desbordamiento TSIG de BIND	131
Vulnerabilidades del servicio DNS de Microsoft	131
Vulnerabilidades remotas en el servidor DNS de Microsoft	132
finger	132

Fugas de información finger	133
Redirección finger	134
Fallos finger directamente explotables	135
auth	136
Vulnerabilidades de manipulación de procesos de auth	136
SNMP	137
ADMSnmp	137
snmpwalk	138
Cadenas de comunidad predeterminadas	139
Comprometer dispositivos mediante la lectura desde SNMP	139
Comprometer dispositivos mediante la escritura a SNMP	140
Vulnerabilidades de manipulación de procesos SNMP	141
LDAP	142
Acceso LDAP anónimo	142
Ataques de fuerza bruta LDAP	143
Active Directory Global Catalog	144
Vulnerabilidades de manipulación de procesos LDAP	144
rwho	145
RPC rusers	145
Contra medidas relacionadas con los servicios de información de acceso remoto	146
Capítulo 6. Evaluar servicios Web	149
Servicios Web	149
Identificar servicios Web	150
HTTP HEAD	151
HTTP OPTIONS	153
Respuestas más comunes para HTTP OPTIONS	154
Identificación automática de servicios Web	155
WebServerFP	155
hmap	156
404print	157
Identificar el servicio Web mediante un túnel SSL	158
Identificar subsistemas y componentes	159
ASP.NET	160
WebDAV	161

Microsoft FrontPage	161
Microsoft Outlook Web Access	162
Fuga de información de las carpetas públicas de Exchange 5.5 OWA	162
Extensiones IIS ISAPI predeterminadas	164
PHP	166
OpenSSL	166
Investigar vulnerabilidades de los servicios Web	167
Las herramientas	167
nikto	167
N-Stealth	169
Sitios Web y listas de correo sobre seguridad	170
Vulnerabilidades de Microsoft IIS	171
Herramientas y secuencias de comando ASP de IIS de ejemplo	171
Exposiciones de la extensión HTR (ISM.DLL)	172
Exposiciones a la extensión HTW (WEBHITS.DLL)	175
Vulnerabilidad IIS Unicode	176
Desbordamiento de la extensión PRINTER (MSW3PRT.DLL)	179
Desbordamiento de la extensión IDA (IDQ.DLL)	180
Vulnerabilidad WebDAV de IIS	181
Vulnerabilidades de Microsoft FrontPage	182
Permisos de IIS deficientemente configurados	184
Vulnerabilidades de Apache	186
Vulnerabilidad de gestión de fragmentos de Apache	186
Otras exposiciones y vulnerabilidades de Apache	189
Vulnerabilidades de OpenSSL	190
Desbordamiento de la clave de cliente en OpenSSL	191
Otras vulnerabilidades y exposiciones de OpenSSL	193
Exposiciones del componente proxy HTTP	194
HTTP CONNECT	194
HTTP POST	196
HTTP GET	196
Examinar proxies HTTP	197
Evaluar información pobremente protegida	198
Forzar la autenticación HTTP mediante fuerza bruta	199

Evaluar secuencias de comandos CGI y páginas ASP personalizadas	200
Manipulación de parámetros y eludir sistemas de filtrado	201
Manipulación de cadenas de consulta URL	201
Manipulación de cookies de usuario	202
Manipulación de campos de formulario	204
Eludir los sistemas de filtrado	205
Problemas en la gestión de errores	206
Introducción de comandos del sistema operativo	207
Ejecutar comandos de sistema	207
Modificar parámetros pasados a comandos del sistema	207
Ejecutar comandos adicionales	208
Medidas contra la introducción de comandos del sistema operativo	209
Introducción de comandos SQL	209
Metodología de comprobación básica	210
Invocación de procedimientos almacenados	211
Comprometer datos utilizando SELECT e INSERT	213
Herramientas de evaluación de aplicaciones Web	214
Achilles	215
Contramidas en los servicios Web	215
Capítulo 7. Evaluar servicios de mantenimiento remoto	219
Servicios de mantenimiento remoto	219
SSH	220
Identificación SSH	221
Obtención de contraseñas SSH mediante fuerza bruta	222
Vulnerabilidades SSH	222
Vulnerabilidad de compensación SSH1 CRC32	223
Explotación de la vulnerabilidad de compensación SSH1 CRC32	223
Vulnerabilidad de respuesta de desafío de OpenSSH	226
Explotación de la vulnerabilidad de respuesta de desafío de OpenSSH	226
Otros fallos de SSH explotables de forma remota	227
Telnet	228
Identificación del servicio Telnet	228
telnetfp	228

Identificación manual telnet	230
Romper las contraseñas mediante fuerza bruta a través de Telnet	231
Contraseñas habituales de dispositivos mediante Telnet	231
Archivos diccionario y listas de palabras	232
Vulnerabilidades Telnet	232
Vulnerabilidad de desbordamiento estático del programa /bin/login de System V	233
Explotación de la vulnerabilidad de desbordamiento estático del programa /bin/login en Solaris	233
Vulnerabilidad de desbordamiento de la memoria libre telrcv() de BSD	235
Explotación de la vulnerabilidad de desbordamiento de memoria libre telrcv() de FreeBSD	235
Otros fallos de Telnet explotables de forma remota	236
Servicios R	237
Acceder directamente a los servicios R	237
Archivos ~/.rhosts y /etc/hosts.equiv de Unix	238
Utilizar técnicas de fuerza bruta con los servicios R	239
Suplantar conexiones RSH	240
Vulnerabilidades conocidas de los servicios R	241
X Windows	241
Autenticación X Windows	242
xhost	242
xauth	242
Evaluar servidores X	242
Realizar un listado de las ventanas abiertas	243
Capturar instantáneas de ventanas abiertas específicas	244
Capturar pulsaciones de teclado en ventanas específicas	244
Enviar pulsaciones de teclado a una ventana específica	245
Vulnerabilidades conocidas del sistema X Windows	246
Protocolo de escritorio remoto de Microsoft	246
Romper contraseñas RDP mediante fuerza bruta	246
Vulnerabilidades RDP	247
VNC	248

Ruptura de la contraseña VNC mediante fuerza bruta	249
Citrix	251
Utilizar el cliente Citrix ICA	251
Acceso a aplicaciones no públicas	251
Vulnerabilidades de Citrix	253
Contra medidas para los servicios de mantenimiento remoto	254
Capítulo 8. Evaluar servicios FTP y de bases de datos	255
FTP	255
Enumeración y obtención de la cabecera FTP	256
Analizar las cabeceras FTP	257
Evaluar permisos FTP	258
Obtención de contraseñas FTP mediante fuerza bruta	261
Ataques FTP de rebote	261
Rastreo de rebote de puertos FTP	261
Explotación de la entrega de la carga mediante rebote FTP	262
Evitar filtros utilizando FTP	263
PORT y PASV	263
Ataques de manipulación de procesos FTP	266
Problemas FTP Globbing en Solaris y BSD	267
Vulnerabilidades WU-FTPD	268
Explotar vulnerabilidades de WU-FTPD 2.6.1 en Linux con 7350wurm	269
Vulnerabilidades de ProFTPD	271
Microsoft IIS FTP Server	272
Contra medidas para los servicios FTP	273
Servicios de base de datos	273
Microsoft SQL Server	274
Enumeración SQL Server	274
Técnicas de fuerza bruta en SQL Server	275
SQLAT	276
Vulnerabilidades de manipulación de procesos en SQL Server	276
Oracle	278
Enumeración de TNS Listener y ataques de fuga de información	279
Realizar pings al servicio TNS Listener	279

Obtener información sobre la versión de Oracle y la plataforma operativa	280
Otros comandos de TNS Listener	280
Obtener el estatus actual del servicio TNS Listener	281
Realizar un ataque de fuga de información	281
Vulnerabilidades de manipulación de procesos del servicio	
TNS Listener	282
Explotación del desbordamiento de pila COMMAND en TNS Listener	283
Crear archivos utilizando el servicio TNS Listener (CVE-2000-00818)	283
Técnicas de fuerza bruta y problemas post autenticación	
en Oracle	284
OAT	285
MetaCoretex	285
MySQL	286
Enumeración de MySQL	286
Fuerza bruta en MySQL	286
Vulnerabilidades de manipulación de procesos en MySQL	287
Contra medidas en los servicios de base de datos	288
Capítulo 9. Evaluar servicios de red Windows	289
Servicios de red de Microsoft Windows	289
SMB, CIFS y NetBIOS	289
Servicios RPC de Microsoft	290
Enumerar información del sistema	291
epdump	291
Valores IFID conocidos	293
rpdump e ifids	294
RpcScan	297
Obtener detalles de usuario mediante las interfaces SAMR y LSARPC	297
walksam	297
rpcclient	300
Obtener contraseñas de administración mediante fuerza bruta	301
Ejecutar comandos arbitrarios	302

Explotar los servicios RPC directamente	302
Servicio de nombres NetBIOS	305
Enumerar detalles del sistema	305
Atacar el servicio de nombres NetBIOS	307
Servicio de datagrama de NetBIOS	307
El servicio de sesión de NetBIOS	308
Enumerar detalles del sistema	309
enum	310
winfo	311
GetAcct	313
Obtener contraseñas de usuario mediante fuerza bruta	313
Autenticación con NetBIOS	314
Ejecutar comandos	315
Acceder y modificar claves de registro	315
Acceder a la base de datos SAM	317
El servicio CIFS	318
Enumeración mediante CIFS	318
Enumeración de usuarios mediante smbdumpusers	318
Técnicas de fuerza bruta con CIFS	319
Vulnerabilidades del sistema Samba para Unix	321
Contra medidas para los servicios de red Windows	322
Capítulo 10. Evaluar servicios de correo electrónico	325
Protocolos de los servicios de correo electrónico	325
SMTP	326
Identificación del servicio SMTP	326
Sendmail	327
Exposiciones de fuga de información en Sendmail	328
Enumeración automática de usuarios en Sendmail	330
Vulnerabilidades de manipulación de procesos de Sendmail	331
El servicio SMTP de Microsoft Exchange	332
Comprobación de la transmisión de SMTP abierto	333
Transmisión SMTP y formas de eludir los antivirus	334
POP-2 y POP-3	336
Obtención de contraseñas en POP-3 mediante fuerza bruta	336
Ataques de manipulación de procesos en POP-3	337

Vulnerabilidades de manipulación de procesos de Qualcomm QPOP	337
Vulnerabilidades de procesos POP-3 en Microsoft Exchange	338
IMAP	339
Técnicas de fuerza bruta con IMAP	339
Ataques de manipulación de procesos con IMAP	339
Contra medidas para los servicios de correo electrónico	341
Capítulo 11. Evaluar servicios IP VPN	343
IPsec VPN	343
ISAKMP e IKE	344
Modo principal de IKE	344
Modo agresivo de IKE	345
Atacar a IPsec VPN	346
Enumeración IPsec	346
Sondeo inicial del servicio ISAKMP	347
Investigar debilidades conocidas de ISAKMP e IKE	348
Ruptura PSK del modo IKE agresivo	349
Problemas de seguridad en Check Point VPN	350
Enumeración de nombres de usuario en Check Point IKE	351
Enumeración de usuarios del servicio Telnet de Check Point	352
Ataques de fuga de información contra Check Point SecuRemote	353
Obtener direcciones IP de las interfaces	353
Descargar información de la topología de red mediante SecuRemote	354
Vulnerabilidad de eludir el cortafuegos Check Point RDP	355
Microsoft PPTP	355
Contra medidas para los servicios VPN	356
Capítulo 12. Evaluar servicios RPC de Unix	359
Servicios RPC de Unix	359
Identificar los servicios RPC sin el asignador de puertos	360
Vulnerabilidades de los servicios RPC	361
Vulnerabilidad rpc.mountd (100005)	362
CVE-1999-0002	363
CVE-2003-0252	363

Enumerar y acceder a directorios exportados mediante mountd y NFS 363

Vulnerabilidades rpc.statd (100024) en múltiples sistemas 364

 CVE-1999-0018 y CVE-1999-0019 364

 CVE-1999-0493 365

 CVE-2000-0666 365

Vulnerabilidades de rpc.sadmind (100232) en Solaris 366

 CVE-1999-0977 366

 CVE-2003-0722 366

Vulnerabilidad rpc.cachefs (100235) en Solaris 367

Vulnerabilidad rpc.snmpXdmid (100249) en Solaris 367

Vulnerabilidades rpc.cmsd (100068) en múltiples sistemas 368

Vulnerabilidad rpc.ttdbserverd (100083) en múltiples sistemas 370

 Utilidad de explotación de rpc.ttdbserverd para Solaris 370

 Utilidad de explotación de rpc.ttdbserverd para IRIX 371

Contra medidas para los servicios RPC de Unix 371

Capítulo 13. Riesgos a nivel aplicación 373

El concepto fundamental de hacking 373

Los motivos por los que el software es vulnerable 374

Vulnerabilidades y ataques de los servicios de red 375

 Ataques de manipulación de memoria 375

 Organización de la memoria en ejecución 376

 El segmento de texto 376

 Los segmentos de datos y BSS 377

 La pila 377

 La memoria libre 378

 Registros y memoria del procesador 379

Vulnerabilidades clásicas de desbordamiento de buffer 380

 Desbordamientos de pila 380

 Aplastamiento de la pila (sobrescritura del puntero de instrucción guardado) 381

 Provocar un bloqueo del programa 382

 Comprometer el flujo lógico del programa 384

 Analizar el bloqueo del programa 384

 Crear e introducir el shellcode 386

Ataque off-by-one de la pila (sobrescritura del puntero del marco guardado)	387
Analizar el bloqueo del programa	388
Explotar una vulnerabilidad off-by-one para modificar el puntero de instrucción	390
Explotar una vulnerabilidad off-by-one para modificar datos en el marco de la pila de la función padre	391
Eficacia del ataque off-by-one en distintas arquitecturas de procesador	392
Desbordamientos de la memoria libre	392
Desbordar la memoria libre para comprometer el flujo del programa	393
Otros ataques de corrupción de la memoria libre	399
Fallos off-by-one y off-by-five de la memoria libre	399
Fallos double-free	399
Lecturas recomendadas	400
Desbordamientos de número entero	400
Ataques de bucle de memoria libre	401
Fallos de tamaño negativo	402
Fallos de cadena de formato	404
Leer elementos adyacentes en la pila	404
Leer datos de cualquier dirección de la pila	406
Sobrescribir cualquier palabra de la memoria	409
Lecturas recomendadas sobre fallos de cadena de formato	411
Resumen de los ataques de manipulación de memoria	411
Reducir los riesgos de la manipulación de procesos	413
Implementación no ejecutable de la pila y la memoria libre	413
Utilización de valores de alerta	414
Utilizar arquitecturas de servidor inusuales	414
Compilar las aplicaciones desde la fuente	415
Monitorización activa de las llamadas del sistema	415
Lecturas recomendadas sobre desarrollo seguro	415
Capítulo 14. Ejemplo de metodología de evaluación	417
Rastreo de la red	417
Rastreo inicial de la red	418

Rastreo completo de la red	419
Pruebas de red de bajo nivel	421
Generación de secuencias TCP ISN	422
Generación de identificadores de IP.....	422
Comprobación del direccionamiento del origen	423
Otras pruebas	424
Identificación de servicios de red accesibles	424
Evaluación inicial del servicio Telnet	424
Evaluación inicial del servicio SSH	425
Evaluación inicial del servicio SMTP	426
Evaluación inicial de servicios Web	427
Investigación ASPNET	428
Enumeración de extensiones ISAPI	429
Rastreo automático de componentes FrontPage y OWA	430
Investigación del servicio Web SSL.....	431
Investigación de vulnerabilidades conocidas	431
Vulnerabilidades de los servicios accesibles de Cisco IOS	431
Vulnerabilidades de los servicios accesibles de Solaris 8	432
Vulnerabilidades de los servicios accesibles de Windows 2000	434
Examen de los servicios de red	436
Router Cisco IOS (192.168.10.1)	436
Servidor de correo electrónico Solaris (192.168.10.10)	438
Servidor Web Windows 2000 (192.168.10.25)	440
Diagrama de flujo de la metodología	441
Recomendaciones	441
Recomendaciones de acciones inmediatas	442
Router Cisco IOS.....	442
Servidor de correo electrónico Solaris	442
Servidor Web Windows 2000	442
Recomendaciones a largo plazo.....	444
Comentarios finales	445
Apéndice A. Puertos TCP y UDP y tipos de mensajes ICMP	447
Puertos TCP	447
Puertos UDP	451
Tipos de mensajes ICMP	452

Apéndice B. Fuentes de información sobre vulnerabilidades	455
Listas de correo electrónico sobre seguridad	455
Bases de datos y listas de vulnerabilidades	456
Sitios Web underground	456
Eventos y conferencias sobre seguridad	457
Índice alfabético	459