

Índice general

Índice general	3
1. Antes de comenzar...	13
1.1. Introducción	13
1.2. Estado actual del tema	14
1.3. Objetivos y Requisitos	14
1.4. Metodología seguida durante el desarrollo del proyecto	15
1.5. Recursos utilizados	15
I Comprometiendo un sistema	17
2. Ingeniería Social	21
2.1. Una historia real	21
2.2. ¿Qué es exactamente la Ingeniería Social?	22
2.3. Objetivo y Ataques	22
2.3.1. Nivel Físico	22
2.3.2. Nivel Psicológico	24
2.4. ¿Cómo defendernos de la Ingeniería Social?	26
2.4.1. Prevenir los ataques físicos	26
2.4.2. Seguridad telefónica	26
2.4.3. Entrenamiento de los empleados	26
2.4.4. Respondiendo a los ataques de ingeniería social	27
2.4.5. Un último consejo	27
3. Selección de víctimas y recolección de información	29
3.1. Planificando el ataque	29
3.2. Whois	30
3.3. Mapeo de red	31
3.3.1. Mapeos ICMP	31
3.3.2. Mapeos TCP	36
3.3.3. Mapeos UDP	39
3.4. Adquirir información valiosa a través del DNS	40
3.4.1. nslookup	40
3.4.2. dig	42
3.4.3. host	43
3.5. ¿Qué servicios ofrece el objetivo?	44

3.5.1.	Escaneo de puertos	44
3.5.2.	Banner Checking	53
3.5.3.	Banner Checking... la evolución	57
3.5.4.	Medidas de protección	58
3.6.	Obteniendo información a partir de ciertos servicios	59
3.6.1.	Finger	59
3.6.2.	RPC	59
3.6.3.	SNMP	61
3.6.4.	SMTP	62
3.7.	Detección del Sistema Operativo	64
3.7.1.	Técnicas clásicas	64
3.7.2.	OS Fingerprint	65
3.8.	Herramientas	67
3.8.1.	HPING	67
3.8.2.	NMap	68
4.	Password Cracking	69
4.1.	Enfoques: Dónde y Cómo utilizar el Password Cracking	69
4.1.1.	Ataque Remoto	69
4.1.2.	Ataques a ficheros de contraseñas	70
4.2.	Categorías de Password Cracking	72
4.2.1.	Contraseñas realmente débiles	72
4.2.2.	Ataques basados en diccionarios	73
4.2.3.	Ataques por fuerza bruta	73
4.3.	Herramientas	73
4.3.1.	Hydra	73
4.3.2.	55hb	74
4.3.3.	John The Ripper	75
4.3.4.	Ficheros de diccionario	75
4.4.	Medidas Preventivas	76
5.	Fallos de Configuración	79
5.1.	NFS	80
5.2.	SNMP y TFTP	83
5.3.	FTP	86
5.4.	FTP y WEB	87
5.5.	Scripts CGI, PHP, ASP...	88
5.6.	Recomendaciones Generales	89
6.	Fallos en el software	91
6.1.	Buffer Overflow (Desbordamiento de Buffer)	91
6.1.1.	Stack Overflow	92
6.2.	Format String	101
6.2.1.	¿Pero que es un format string?	101
6.2.2.	Usando los format string para leer el stack	102
6.2.3.	Leyendo una ristra situada en casi cualquier posición de la memoria del proceso	103
6.2.4.	Escribiendo un entero en cualquier posición de la memoria del proceso	105

6.3.	Otros tipos de fallos	106
6.3.1.	Race Condition	107
6.3.2.	Combinaciones inesperadas	107
6.3.3.	Entradas no tratadas	107
6.4.	Recomendaciones generales	108
6.4.1.	Parchear las aplicaciones	108
6.4.2.	Escribir código seguro	109
6.4.3.	Otras contramedidas	109
7.	Fallos de Diseño	111
7.1.	Rastreado la red (Sniffing)	111
7.2.	Falsificación de paquetes (Spoofing)	112
7.3.	Ataques de enrutamiento (Routing Attacks)	112
7.4.	Denegación de Servicio	113
7.5.	¿Cómo evitarlos?	113
8.	Ocultando la fuente del ataque	115
8.1.	Saltando entre máquinas	115
8.2.	Utilizando proxys	115
8.3.	Troyanos	117
8.4.	Cuestión de distancia	117
II	Utilizando el sistema comprometido	119
9.	Eliminando las huellas	123
9.1.	Syslogd y sus alternativas	123
9.2.	Klogd, el sistema de logs del kernel	124
9.3.	El sistema de Accounting (o de contabilidad)	124
9.4.	Otros ficheros de logs	125
9.4.1.	UTMP	125
9.4.2.	WTMP	125
9.4.3.	Lastlog	126
9.4.4.	History	126
9.5.	Borrando las huellas	126
9.5.1.	Fase 1: desapareciendo del UTMP, WTMP y Lastlog	127
9.5.2.	Fase 2: eliminando la información guardada por el syslog y por otros demonios	128
9.5.3.	Fase 3: eliminando los posibles rastros dejados por los exploits	129
9.5.4.	Fase 4: silenciando al Klogd	129
9.5.5.	Fase 5: eliminando el historial	129
9.5.6.	Fase 6: eliminado la información de Accounting	130
9.5.7.	Simplificando el trabajo: vanish2	131
9.6.	Contramedidas	131

10.Mantener el control	133
10.1. Troyanos y Puertas Traseras (Elevar los privilegios, acceder al sistema)	133
10.1.1. Añadir un nuevo usuario al sistema	134
10.1.2. La SUSHI y sus variantes	134
10.1.3. Shells Remotas	136
10.1.4. Shells Remotas Inversas	138
10.1.5. Instalando troyanos en el <i>inetd</i>	139
10.1.6. Troyanizar aplicaciones	140
10.1.7. CGI/PHP Backdoors	142
10.1.8. Troyanos en el CRON	143
10.1.9. Otras artimañas	143
10.2. El arcano arte de la invisibilidad	144
10.2.1. Rootkits	144
10.2.2. Luchando contra los rootkits	147
10.2.3. LKM Rootkits	148
10.2.4. Luchando contra los LKM Rootkits	151
10.3. Backdoors avanzadas	152
10.3.1. ¿Cómo se solucionan estos problemas?	153
10.3.2. Algunos ejemplos reales	156
11.Acceso Pasivo	159
11.1. Tareas automatizadas	159
11.2. Rastreado la red (Sniffing)	160
11.3. Troyanizar aplicaciones	160
11.4. Keyloggers	160
11.5. TTY Hijacking	161
12.Rastreado la red (Sniffing)	163
12.1. Conceptos sobre Ethernet	163
12.2. Rastreado la red (Sniffing)	164
12.2.1. ¿Qué es un sniffer?	164
12.2.2. ¿Por qué constituyen una amenaza?	165
12.2.3. ¿Cómo algo así puede ser útil al administrador de la red?	165
12.2.4. Profundizando en los sniffers	166
12.2.5. Algunos sniffers importantes	167
12.2.6. Detectando sniffers	167
12.2.7. Evitando la detección	171
12.2.8. Cómo protegerse	172
12.2.9. Sniffers en redes conmutadas	173
13.Creando paquetes falsos (Spoofing)	177
13.1. ARP Spoofing	177
13.1.1. Herramientas capaces de llevar a cabo el ARP Spoofing	178
13.1.2. ¿Cómo detectar este ataque?	178
13.2. IP Spoofing	179
13.2.1. La historia	179
13.2.2. Detalles técnicos	179
13.2.3. Ataques basados en IP Spoofing	181

13.2.4. El Ataque Mitnick	185
13.2.5. Defensas contra el spoofing	196
13.3. DNS Spoofing	196
13.3.1. Funcionamiento del protocolo DNS	197
13.3.2. Los ataques	202
14. Ataques Man in the Middle	211
14.1. Escenario del ataque	211
14.2. Técnicas para colocarse “en medio” de una conexión	211
14.2.1. Ataque Local	212
14.2.2. Ataque Local a Remoto (a través de una pasarela)	213
14.2.3. Ataque Remoto	217
14.2.4. Herramientas	217
14.3. Una vez en medio.	218
14.3.1. Inyectar y modificar paquetes	218
14.3.2. Manipulación de claves (Key Manipulation)	219
14.3.3. Upgrading, Downgrading y otras variantes del ataque	223
14.3.4. Filtrado y Modificación	226
14.4. ¿Cómo Defenderse?	227
14.4.1. ARP Poisoning	227
14.4.2. Port Stealing	227
14.4.3. DNS Spoofing	228
14.4.4. DNS Poisoning	228
14.4.5. IRDP Spoofing y ICMP Redirection	228
14.4.6. Route Mangling y Traffic Tunneling	228
III Ataques de Denegación de Servicio	229
15. Ataques de Denegación de Servicio (DoS)	233
15.1. Motivaciones del atacante	233
15.2. Ataques DoS clásicos	234
15.2.1. IP Flooding	234
15.2.2. Difusión	235
15.2.3. Smurf	235
15.2.4. Teardrop / Boink / Bonk / Nestea	236
15.2.5. ECHO-CHARGEN / Snork	237
15.2.6. DOOM / QUAKE	238
15.2.7. LAND	238
15.2.8. Ping de la Muerte (Ping of Death)	240
15.3. Ataques DoS modernos	241
15.3.1. IPTables + Linux Kernel 2.6 (Junio del 2004)	241
15.3.2. Apache 2.x (Agosto del 2004)	241
15.3.3. Titan FTP Server (Mayo del 2004)	241
15.3.4. Vulnerabilidades en TCP (Abril del 2004)	242
15.4. Defensas contra los ataques DoS	242

16. Ataques DoS Distribuidos (DDoS)	243
16.1. TRINOO / TRIN00	244
16.2. Tribe Flood Network (TFN)	245
16.3. Tribe Flood Network 2000 (TFN2K)	245
16.4. Stacheldraht	247
16.5. Shaft	248
16.6. Mstream	251
16.7. Métodos de propagación de las herramientas de ataque	253
16.7.1. Propagación de código centralizada	253
16.7.2. Propagación encadenada	254
16.7.3. Propagación Autónoma	255
16.8. Defensas contra los ataques DDoS	255
IV Defensas genéricas	257
17. Recetario básico de defensa	261
17.1. Sobre la arquitectura de la red...	261
17.1.1. Diseñar la red teniendo en cuenta la seguridad	261
17.1.2. Separación preliminar de los servicios de red	262
17.1.3. Agregar tantas subdivisiones y capas de seguridad como sean necesarias	262
17.1.4. Utilizar redes diferentes para diferentes servicios	265
17.1.5. Protección física y ambiental del hardware	265
17.1.6. Estandarizar todas las configuraciones	265
17.1.7. Control de acceso a la red	266
17.2. Sobre los servidores...	266
17.2.1. Seguridad de la BIOS	266
17.2.2. Seguridad en el gestor de arranque (LILO o GRUB)	266
17.2.3. Realizar copias de seguridad regularmente	266
17.2.4. Deshabilitar todas las cuentas especiales	267
17.2.5. Elegir las contraseñas adecuadas	267
17.2.6. Activar el soporte para contraseñas shadow	267
17.2.7. Salida automática de la shell	267
17.2.8. Restringir el uso del comando <code>su</code>	267
17.2.9. Deshabilitar los programas SUID/SGID sin utilizar	268
17.2.10. Deshabilitar y desinstalar todos los servicios sin utilizar	268
17.2.11. Control de acceso	268
17.2.12. Eliminar los banner	268
17.2.13. Utilizar demonios con capacidad de cifrado para el acceso al sistema	268
17.2.14. Enviar los logs a otra máquina	269
17.2.15. Analizar los logs	269
17.2.16. Estar informados y actualizados	269
17.2.17. Realizar auditorías	270
17.3. Políticas de seguridad	270

18. Cortafuegos	273
18.1. Introducción	273
18.2. Características de diseño	276
18.3. Elementos de un cortafuegos	277
18.3.1. Filtrado de paquetes	277
18.3.2. Proxy de aplicación	279
18.3.3. Monitorización y detección de actividad sospechosa	280
18.4. Arquitecturas de Cortafuegos	280
18.4.1. Cortafuegos de filtrado de paquetes	280
18.4.2. Dual-Homed Host	281
18.4.3. Screened Host	282
18.4.4. Screened Subnet (DMZ)	283
18.5. Software cortafuegos	285
18.5.1. Firewall-1	285
18.5.2. IPFWADM/IPCHAINS/IPTABLES	286
18.5.3. IPFilter	287
18.5.4. PIX Firewall	287
18.6. Algunos consejos para montar un host bastión	288
18.6.1. Principios básicos	288
18.6.2. Los pasos básicos	289
19. Sistemas de Detección de Intrusos	293
19.1. Un poco de historia.	293
19.2. Definición formal	294
19.3. Clasificación de los IDS	294
19.4. Requisitos de un IDS	296
19.5. Sistemas de detección basados en Host (HIDS)	297
19.6. Sistemas de detección basados en Red (NIDS)	299
19.7. Algunas herramientas actuales	301
20. Honeypots y Honeynets	305
20.1. ¿Qué es un Honeypot?	306
20.2. ¿Qué son las Honeynets?	307
20.3. ¿Dónde situar nuestro honeypot/honeynet?	307
20.4. Principios básicos	308
20.4.1. Control de datos	309
20.4.2. La captura de datos	309
20.5. El riesgo	310
21. Tests de Intrusión y Auditorías de seguridad	311
21.1. Tests de Intrusión	311
21.2. Auditorías de Seguridad	313
21.2.1. Análisis de Riesgos	313
21.2.2. Fases de una auditoría	314
21.3. Algunas herramientas interesantes	317

22. ¿Qué hacer después del compromiso?	321
22.1. Antes de comenzar	321
22.1.1. Consulta tu política de seguridad	321
22.1.2. Si no tenemos una política de seguridad...	321
22.1.3. Documenta todos los pasos realizados durante la recuperación	322
22.2. Recuperar el control	322
22.2.1. Desconecta el sistema comprometido de la red	322
22.2.2. Copiar una imagen del sistema comprometido	323
22.3. Analizar la intrusión	323
22.3.1. Buscar modificaciones en el software del sistema y en los archivos de configuración	323
22.3.2. Busca modificaciones en los datos	324
22.3.3. Busca herramientas y datos dejados por el atacante	324
22.3.4. Revisar los ficheros de logs	325
22.3.5. Buscar un sniffer	326
22.3.6. Chequea otros sistemas en la red	327
22.3.7. Comprueba los sistemas remotos involucrados o afectados	327
22.4. Contactar con los CISTR adecuados y con los sitios remotos involucrados	327
22.4.1. Informar del incidente	327
22.4.2. Contactar con el Centro Coordinador del CERT	328
22.4.3. Obtener la dirección de contacto de los otros sitios involucrados en el ataque	329
22.5. Recuperándose de la intrusión	329
22.5.1. Instalar una versión limpia del sistema operativo	329
22.5.2. Precaución durante la recuperación desde las copias de seguridad	329
22.6. Mejorar la seguridad del sistema y de la red	330
22.6.1. Revisa la seguridad de tus máquinas usando guías	330
22.6.2. Revisar los documentos sobre herramientas de seguridad	330
22.6.3. Instala las herramientas de seguridad	330
22.6.4. Revisa el sistema de logs	330
22.6.5. Reconfigura los cortafuegos	330
22.7. Volver a conectar el host	331
22.8. Actualiza tu política de seguridad	331
22.8.1. Documentar las lecciones aprendidas desde el principio del compromiso	331
22.8.2. Calcular el coste del incidente	331
22.8.3. Incorporar los cambios necesarios en la política de seguridad	331
23. Palabras finales	333
Bibliografía	335