

Internal Hacking y contramedidas en entorno Windows

Piratería interna, medidas de protección, desarrollo de herramientas (2ª edición)

Introducción

1. Preámbulo	17
2. Desciframiento de un ataque conseguido	19
3. Descifrado de contramedidas eficaces	20
3.1 Análisis de riesgos reales	20
3.2 Consideraciones técnicas	21
3.3 Consideraciones sobre la gestión	21
4. ¿ Qué acciones, para qué roles ?	22
4.1 ¿ Qué puede hacer un administrador local ?	23
4.2 ¿ Qué puede hacer un administrador de dominio ?	23
4.3 ¿ Qué puede hacer un usuario ?	24
5. Formaciones y certificaciones CSH	24

Búsqueda de información

1. ¿ Qué informaciones son interesantes ?	27
1.1 Tipos de búsquedas	28

Internal Hacking y contramedidas en entorno Windows

Piratería interna, medidas de protección, desarrollo de herramientas (2ª edición)

1.2 ¿ Qué se debe anotar ?	29
2. ¿ Cómo encontrar las informaciones locales útiles ?	30
2.1 Configuraciones del sistema	30
2.1.1 Informaciones de la red	30
2.1.2 Variables de entorno	31
2.1.3 Usuarios y grupos	32
2.2 Las directivas de grupo	34
2.2.1 Con la consola de gestión	34
2.2.2 Con la línea de comandos	35
2.2.3 Con el editor del registro	36
2.3 El cortafuegos	37
2.3.1 Con el panel de configuración	37
2.3.2 Con la línea de comandos	39
2.4 Las carpetas y los archivos	41
2.4.1 Carpetas públicas	41
2.4.2 Carpeta temporal	42
2.4.3 Documentos de Office	44
3. Las informaciones remotas	46
3.1 Configuración de sistema	46
3.1.1 Carpetas compartidas	46

Internal Hacking y contramedidas en entorno Windows

Piratería interna, medidas de protección, desarrollo de herramientas (2ª edición)

3.1.2 Usuario y grupos	46
3.2 Configuración de red	48
3.2.1 Búsqueda del nombre del servidor que hospeda un servicio	50
3.2.2 Búsqueda de servicios con PortQry de Microsoft	51
3.2.3 Búsqueda de servicios con Nmap	52
4. Contramedidas	54
4. Contramedidas	56
Tomar el rol de administrador o de sistema	
1. Utilizar un medio de instalación de Windows oficial o una imagen de arranque PXE	57
1.1 Arranque sobre el sistema	57
1.2 Modificación del registro offline	60
1.3 Utilización del hack sobre distintos sistemas	65
1.4 Contramedidas	69
2. Trucar una aplicación con las herramientas integradas en Windows	70
2.1 Tomar el rol de sistema en su puesto de trabajo o su servidor	70
2.2 Tomar el rol de System en un servidor remoto o en un controlador de dominio	81
2.3 Llegar a ser administrador del dominio	86
2.4 Contramedidas	88

Internal Hacking y contramedidas en entorno Windows

Piratería interna, medidas de protección, desarrollo de herramientas (2ª edición)

3. Engañar con un documento de Office	88
3.1 Ejecutar un script o un programa	88
3.2 Esquivar la seguridad de las macros	91
3.3 Contramedidas	96
4. Modificar un correo electrónico para arrancar una aplicación	97
4.1 Enviar un PDF falso desde el exterior	97
4.2 Enviar desde dentro un PowerPoint modificado	102
4.3 Hacer descargar una aplicación oculta y ejecutarla	104
4.4 Desactivar SmartScreen	107
4.5 Contramedidas	109

Encriptado y CryptoLocker

1. Introducción	111
2. Dos principios del encriptado	111
3. Utilización del encriptado simétrico con DPAPI	112
3.1 ¿ Cómo funciona DPAPI ?	113
3.2 Encriptar utilizando DPAPI y PowerShell	114
3.3 Encriptar utilizando DPAPI y Visual Studio	114

Internal Hacking y contramedidas en entorno Windows

Piratería interna, medidas de protección, desarrollo de herramientas (2ª edición)

	115
4. Utilización del encriptado asimétrico con certificados	119
4.1 Encriptar un archivo usando EFS	119
4.2 Encriptar un archivo mediante certificado	120
4.3 Exportar un certificado y su clave privada	121
4.4 Eliminar los certificados del almacén	122
5. Cryptoware	123
5.1 Las bases de un cryptoware utilizando EFS	123
5.2 Las bases de un cryptoware utilizando DPAPI	124
6. Ejemplo de encriptado con EFS, certificado y DPAPI	128
7. Contramedidas	133
Extraer, romper, cambiar una contraseña	
1. Cómo extraer una contraseña en un equipo o un controlador de dominio	135
1.1 Herramientas de extracción de contraseñas de sesión	136
1.1.1 La SAM en detalle	136
1.1.2 Extraer las contraseñas de la SAM	141
1.1.3 Extraer las contraseñas de un controlador de dominio	

Internal Hacking y contramedidas en entorno Windows

Piratería interna, medidas de protección, desarrollo de herramientas (2ª edición)

1.2 Herramientas de extracción de otras contraseñas	142
1.2.1 Analizar el funcionamiento de una aplicación	144
1.2.2 Recuperar la contraseña de una conexión inalámbrica guardada en el PC	144
1.2.3 Crear una herramienta de recuperación de una conexión inalámbrica	148
1.2.4 Recuperar las contraseñas wifi con un script	151
1.2.5 Recuperar las contraseñas Office 365 almacenadas	155
1.2.6 Otras herramientas	157
1.3 Contramedidas	159
2. ¿ Cómo recuperar una contraseña desde la red ?	163
2.1 Utilización de un proxy	163
2.1.1 Configurar el objetivo	164
2.1.2 Usar Burp Proxy	164
2.2 Introducción a los certificados y a HTTPS	164
2.2.1 Principio de funcionamiento de HTTPS	167
2.2.2 Pedir un certificado web o de firma de código	167
2.2.3 Configurar Burp Proxy para analizar HTTPS	169
2.2.4 Instalar un root CA con los permisos de usuarios	179
2.3 Script que permite capturar el teclado en una página web	180
2.3.1 La página web de recepción	182
2.3.2 El código JavaScript	183

Internal Hacking y contramedidas en entorno Windows

Piratería interna, medidas de protección, desarrollo de herramientas (2ª edición)

2.3.3 Añadir el script en una página SharePoint	184
2.3.4 Inyección del script en una página con vulnerabilidad XSS	184
2.4 Usar un sitio web falso copiado	187
2.4.1 Descargar el sitio web	190
2.4.2 Modificar el sitio	191
2.5 Redirección de puertos, falso wifi y escucha de la red	194
2.5.1 Crear un falso wifi	194
2.5.2 Configuración de la redirección de puerto	196
2.5.3 Enviar el objetivo a nuestro sitio web	197
2.5.4 Escuchar y analizar el tráfico de red con herramientas internas	198
2.5.5 Escuchar y analizar el tráfico con herramientas externas	202
2.6 ARP poisoning en Windows	204
2.6.1 ARP, ¿ qué es ?	205
2.6.2 ARP poisoning con Cain & Abel	206
2.6.3 Configurar Cain & Abel para analizar el tráfico HTTPS	207
2.6.4 Usar Cain & Abel para encontrar la contraseña de un usuario del dominio	214
2.7 Software y herramientas para romper las contraseñas	217
2.7.1 Tipos de cifrado	218
2.7.2 Principios para romper las contraseñas	218
2.7.3 Fuerza bruta	219
2.7.4 Diccionario	220

Internal Hacking y contramedidas en entorno Windows

Piratería interna, medidas de protección, desarrollo de herramientas (2ª edición)

2.7.5 Rainbow table	222
2.7.6 SQL	223
2.7.7 Herramientas en línea	227
2.7.8 Usando la tarjeta gráfica	227
2.8 Contramedidas	228
	229

Desarrollar sus propias herramientas de hacking

1. Introducción a .NET	231
1.1 ¿Cómo compilar su programa sin Visual Studio ?	233
2. Forzar la ejecución de una aplicación	237
2.1 Los medios clásicos	237
2.2 Los medios no convencionales	239
3. Filtrar datos en diferencial	243
3.1 Usar una carpeta compartida como destino	244
3.2 Configurar un servidor con WebDAV como destino	245
3.3 Configurar SharePoint como destino	249
3.4 Crear la aplicación	250
3.5 Compilar el programa	256

Internal Hacking y contramedidas en entorno Windows

Piratería interna, medidas de protección, desarrollo de herramientas (2ª edición)

4. Crear una ventana de autenticación	256
4.1 Principios básicos	256
4.2 Crear el programa para Outlook	257
4.3 Crear el programa para IE	262
4.4 Crear el programa para una aplicación de gestión	264
5. Crear un keylogger	266
5.1 Principios básicos	267
5.2 Crear la aplicación	268
5.3 Compilar la aplicación	269
6. Capturar la pantalla	271
6.1 Principios básicos	271
6.2 Crear la aplicación	271
6.3 Compilar la aplicación	273
7. Grabar el sonido	273
7.1 Principios básicos	274
7.2 Crear la aplicación	274
7.3 Compilar la aplicación	277
8. Romper una contraseña	

Internal Hacking y contramedidas en entorno Windows

Piratería interna, medidas de protección, desarrollo de herramientas (2ª edición)

	277
8.1 Principios básicos	278
8.2 Crear la aplicación	279
8.3 Compilar la aplicación	282
8.4 Usar la GPU	283
9. Gobernar un equipo remoto	283
9.1 Principios básicos	284
9.2 Crear la aplicación	285
9.3 Compilar la aplicación	286
10. Esquivar la seguridad de la UAC	287
10.1 Principios básicos	287
10.2 Extraer los iconos de una aplicación	288
10.3 Firmar el código	289
10.4 Trucar la aplicación para la víctima	291
10.5 Probar las modificaciones	293
11. Cambiar el código PIN BitLocker con permisos de usuario	296
11.1 Principios básicos	296
11.2 Crear un servicio de Windows	298
11.3 Compilar e instalar un servicio de Windows	301

Internal Hacking y contramedidas en entorno Windows

Piratería interna, medidas de protección, desarrollo de herramientas (2ª edición)

11.4 Crear la aplicación cliente	301
11.5 Compilar la aplicación cliente	302
12. Contramedidas	303
Hacer ejecutar sus aplicaciones trampa	
1. Entender a la persona, sus necesidades y sus deseos	305
1.1 La toma de decisiones	305
1.2 Entender al usuario	306
2. Las necesidades del usuario	307
2.1 El modelo de Maslow	307
2.2 El modelo de valor de inventario de Shalom Schwartz	308
3. Técnicas de manipulación	310
3.1 Introducción a la manipulación	310
3.2 Las sugerencias verbales	311
4. Creación de la fase de ataque	312
4.1 Enviar un documento de Office trucado	313
4.2 Enviar una aplicación trampa	314

Internal Hacking y contramedidas en entorno Windows

Piratería interna, medidas de protección, desarrollo de herramientas (2ª edición)

5. Contramedidas	316
Superar las restricciones de software	
1. Superar las directivas de grupo	317
1.1 Principio de las directivas de grupo	317
1.2 Bloquear la ejecución de las GPO	318
1.2.1 Bloquear las directivas de grupo de usuario	318
1.2.2 Bloquear las directivas de grupo del equipo	323
1.3 Contramedidas	325
2. Esquivar las restricciones corrientes	326
2.1 El explorador de Windows	327
2.1.1 Principio de funcionamiento	327
2.1.2 Esquivar para explorar los archivos	327
2.2 El registro	329
2.2.1 Principio de funcionamiento	329
2.2.2 Las modificaciones para ver o modificar el registro	330
2.3 El administrador de tareas	332
2.3.1 Principio de funcionamiento	332
2.3.2 Las modificaciones para ver, destruir o crear un proceso	

Internal Hacking y contramedidas en entorno Windows

Piratería interna, medidas de protección, desarrollo de herramientas (2ª edición)

2.4 Gestión de archivos con FSRM	332
2.4.1 Principio de funcionamiento	334
2.4.2 Esconder un archivo con la ayuda de otro documento	335
2.4.3 Esconder un archivo con los flujos alternativos	336
2.4.4 Encontrar los flujos alternativos	338
2.5 Ejecutar otras aplicaciones que no sean las previstas en un Terminal Server	341
2.5.1 Principio de funcionamiento	341
2.5.2 Esquivar con un acceso directo	342
2.5.3 Esquivar con un documento de Office	343
2.5.4 Esquivar con el login	345
2.6 Pasarela de mail	347
2.6.1 Principio de funcionamiento	347
2.6.2 Esquivar para filtrar archivos	347
2.7 Proxy web	348
2.7.1 Principio de funcionamiento	348
2.7.2 Esquivar para cargar o descargar archivos	348
2.7.3 Esquivar para navegar	349
2.8 Contramedidas	351

Tomar el control remotamente

Internal Hacking y contramedidas en entorno Windows

Piratería interna, medidas de protección, desarrollo de herramientas (2ª edición)

1. Tomar el control de un equipo remoto	353
1.1 Utilización de las herramientas de administración de Windows	353
1.1.1 Instalar Telnet Server	354
1.1.2 Usar el cliente Telnet	354
1.1.3 Usar PuTTY	355
1.2 Usar una aplicación NetCommand en .NET	356
1.2.1 Crear una aplicación de servidor	356
1.2.2 Compilar la aplicación	358
1.2.3 Usar el servidor	358
1.2.4 Conectarse al servidor	359
1.3 Uso de una herramienta de escritorio remoto	361
1.3.1 El escritorio remoto (RDP)	361
1.3.2 VNC con conexión directa	362
1.3.3 VNC en conexión inversa	365
1.4 Contramedidas	366
2. Tomar el control mediante vulnerabilidades del sistema operativo o de las aplicaciones	366
2.1 Las vulnerabilidades del sistema operativo y de las aplicaciones	366
2.1.1 Base de datos CVE	367
2.1.2 Búsqueda de vulnerabilidades con Nessus	368
2.2 Metasploit y Armitage	374

Internal Hacking y contramedidas en entorno Windows

Piratería interna, medidas de protección, desarrollo de herramientas (2ª edición)

2.2.1 Instalar Metasploit en Windows	374
2.2.2 Instalar Armitage en Windows	379
2.2.3 Analizar una red con Armitage	380
2.2.4 Utilizar una vulnerabilidad del sistema operativo o de una aplicación con Armitage	382
2.2.5 Atacar desde la interfaz web de Metasploit	387
2.2.6 Utilizar un falso sitio web copiado con Metasploit Pro	389
2.3 Contramedidas	394

Guardar una puerta abierta

1. Introducción a las puertas traseras activas y pasivas	395
2. Conservar discretamente un acceso a un servidor o a un PC	395
2.1 Puerto de escucha para Terminal Server	395
2.2 Programa .NET	396
3. Conservar discretamente un acceso a un servidor web o de mensajería	397
3.1 Tener acceso a todas las cuentas de correo electrónico de un servidor Exchange	397
3.1.1 Grupos de seguridad	397
3.1.2 Apertura de una cuenta de correo electrónico	399
3.1.3 PowerShell	399
3.2 Modificar una aplicación web para conservar un acceso desde el exterior	

Internal Hacking y contramedidas en entorno Windows

Piratería interna, medidas de protección, desarrollo de herramientas (2ª edición)

3.2.1 Añadir un grupo de aplicaciones	400
3.2.2 Añadir una aplicación web	400
3.2.3 Añadir una página web para ejecutar comandos	403
3.2.4 Utilizar el acceso web PowerShell	405
3.3 Contramedidas	407
	409
4. Conservar discretamente un medio de tomar el control en un PC o un servidor	409
4.1 Añadir un protocolo y trucar la navegación	409
4.1.1 Modificar el registro	410
4.1.2 Usar la modificación	411
4.1.3 Enmascarar el script	412
4.2 Añadir o modificar una extensión	414
4.2.1 Modificar el registro	415
4.2.2 Usar la modificación	416
4.3 Añadir un certificado raíz	417
4.4 Esconder una cuenta de usuario	418
4.4.1 Esconder un usuario local	418
4.4.2 Esconder un usuario en el Active Directory	419
4.5 Contramedidas	423

Internal Hacking y contramedidas en entorno Windows

Piratería interna, medidas de protección, desarrollo de herramientas (2ª edición)

Esconderse y eliminar sus huellas

1. Usar la virtualización

	425
1.1 Hyper-V en Windows 8 y las versiones superiores	425
1.1.1 Instalar Hyper-V	425
1.1.2 Configurar Hyper-V	426
1.1.3 Crear una máquina virtual	428
1.1.4 Usurpar una dirección MAC	429
1.1.5 PowerShell para Hyper-V	429
1.2 Otras herramientas de virtualización	430
1.2.1 Otras plataformas de virtualización	430
1.2.2 Copiar un disco físico en uno virtual	431
1.2.3 Conectar/crear un disco virtual directamente en Windows	431
1.2.4 Impedir el acceso a su disco duro	433
1.2.5 La virtualización de aplicaciones	434
1.3 Contramedidas	435

2. Utilizar la cuenta de sistema

	435
2.1 Utilizar la cuenta de sistema directamente	435
2.2 Utilizar la cuenta de sistema indirectamente	436
2.3 Contramedidas	437

3. Eliminar los logs

Internal Hacking y contramedidas en entorno Windows

Piratería interna, medidas de protección, desarrollo de herramientas (2ª edición)

	437
3.1 Los logs de eventos de Windows	438
3.2 Los logs del cortafuegos local	439
3.3 Los logs de los servicios web	440
3.3.1 Contramedidas	442

Las contramedidas técnicas

1. Los medios integrados en los entornos Microsoft

	443
1.1 Impedir el arranque del sistema	444
1.1.1 SysKey	444
1.1.2 Concepto y requisitos de BitLocker	445
1.1.3 Almacenar las claves de recuperación en el Active Directory	446
1.1.4 Activar BitLocker en un equipo	447
1.1.5 Configurar un código PIN	448
1.2 Instalar y configurar un controlador de dominio en modo de solo lectura	449
1.2.1 Crear el equipo	449
1.2.2 Configurar las contraseñas no replicadas	450
1.3 Instalar y configurar una autoridad de certificación	450
1.3.1 Planificación de la instalación	451
1.3.2 Instalación y configuración	452

Internal Hacking y contramedidas en entorno Windows

Piratería interna, medidas de protección, desarrollo de herramientas (2ª edición)

1.3.3 Modificar y añadir modelos de certificados	454
1.3.4 Configurar el certificado Root en los PC internos	454
1.3.5 Usar contraseñas para proteger las claves privadas	455
1.3.6 Utilizar una virtual smart card para proteger las claves privadas	458
1.3.7 Utilizar un módulo HSM para proteger las claves privadas	462
1.4 Instalar y configurar NAP	463
1.4.1 Configurar el DHCP con una lista blanca	463
1.4.2 Instalar los servicios para NAP	464
1.4.3 Configurar NAP para utilizar IPsec en los servidores	465
1.4.4 Configurar los clientes para soportar NAP	465
1.5 Instalar y configurar WSUS	466
1.5.1 Instalar WSUS	466
1.5.2 Configurar los clientes para utilizar WSUS	467
1.6 Las directivas de grupo	468
1.6.1 Configurar las cuentas restringidas	468
1.6.2 Configurar la seguridad de las contraseñas	469
1.6.3 Configurar el cortafuegos	471
1.6.4 Configurar el control de la cuenta de usuario	472
1.6.5 Restricción del registro y de archivos	473
1.7 Configurar la restricción de software	474
1.7.1 ¿ Autorizar o bloquear por defecto ?	475

Internal Hacking y contramedidas en entorno Windows

Piratería interna, medidas de protección, desarrollo de herramientas (2ª edición)

1.7.2 Bloquear una aplicación	475
1.7.3 Bloquear las aplicaciones en los medios removibles	476
1.7.4 Estrategia de bloqueo de aplicaciones	477
1.8 La gestión de los archivos y de los permisos	478
1.8.1 Los grupos de seguridad	478
1.8.2 Las carpetas temporales o Temp	480
1.8.3 La compartición de archivos	482
1.8.4 La gestión de archivos con FSRM	484
1.8.5 La clasificación de archivos	488
1.8.6 Microsoft RMS	494
1.9 Firmar las macros VBA y los scripts PowerShell	500
1.9.1 Solicitar un certificado	500
1.9.2 Firmar una macro VBA	501
1.9.3 Firmar un script PowerShell	501
1.9.4 Autorizar la ejecución de objetos firmados	502
1.10 Herramientas de auditoría y de seguridad de Microsoft	504
1.10.1 Herramientas de auditoría	504
1.10.2 Herramientas de seguridad	506
2. Configurar una autenticación fuerte	507
2.1 Reforzar la autenticación Windows con un OTP	509

Internal Hacking y contramedidas en entorno Windows

Piratería interna, medidas de protección, desarrollo de herramientas (2ª edición)

2.1.1 Instalar y utilizar la versión autónoma de otpOne	510
2.1.2 Instalar y configurar la versión profesional de otpOne	514
2.2 Garantizar la identidad al registrar el OTP	516
2.3 Reforzar la autenticación de aplicaciones con un OTP	519
2.4 Reforzar la seguridad de carpetas compartidas con OTP	520
2.5 Reforzar la autenticación de Keepass con un OTP	521
2.6 Utilizar el SDK integrado con C# y Powershell	524
2.7 Reforzar la autenticación ADFS y VPN	525
3. Otros medios técnicos	526
3.1 La disociación	526
3.1.1 Disociación de redes físicas	526
3.1.2 Uso de VLAN	526
3.1.3 Antivirus	527
3.1.4 Software cortafuegos	527
3.1.5 Cortafuegos físico	528
3.2 Herramientas de monitoring y de vigilancia	529
3.2.1 IDS e IPS	529
3.2.2 Vigilancia de los sistemas y los elementos de seguridad	530
3.3 Herramientas de auditoría y de prueba de vulnerabilidades	531
3.3.1 Programas personales	531

Internal Hacking y contramedidas en entorno Windows

Piratería interna, medidas de protección, desarrollo de herramientas (2ª edición)

3.3.2 Programas de empresa	532
La gestión de los sistemas de información	
1. Los retos de la gestión	535
2. El impacto y las consecuencias del internal hacking en la gestión	536
3. Unas buenas prácticas que nos pueden ayudar	537
3.1 Norma o buenas prácticas	537
3.2 COBIT, Val IT y Risk IT	538
4. Poner en marcha la gestión de los SI con la ayuda de COBIT	540
4.1 Marco general	540
4.2 ¿ Qué es un objetivo de control ?	542
4.3 El procedimiento «Puesta en marcha de la gestión de los SI»	542
4.3.1 Puesta en marcha de un cuadro de gestión de los SI - SE4.1	542
4.3.2 Alineamiento estratégico - SE4.2	543
4.3.3 Valor añadido - SE4.3	543
4.3.4 Gestión de recursos - SE4.4	543
4.3.5 Gestión de riesgos - SE4.5	543
4.3.6 Medida del rendimiento - SE4.6	544

Internal Hacking y contramedidas en entorno Windows

Piratería interna, medidas de protección, desarrollo de herramientas (2ª edición)

4.3.7 Seguro independiente - SE4.7	544
4.4 ¿ Por dónde empezar ?	544
4.4.1 Nivel de madurez	544
4.4.2 Procedimientos de partida	545
5. Administrar el riesgo	546
5.1 Definiciones	546
5.2 Estimación del riesgo	547
5.3 Los factores de riesgo	548
5.4 La clasificación del riesgo	549
5.5 El tratamiento de un riesgo	550
5.6 Los otros elementos de la gestión de riesgos	551
6. Tratar el internal hacking desde el punto de vista de la gestión	551
6.1 La gestión de los administradores	552
6.2 La gestión de los usuarios	554
6.3 La gestión de los sistemas	555
6.4 La gestión de las aplicaciones	557
6.5 La gestión de la información	559
6.6 La gestión de los problemas y de los incidentes	559

Internal Hacking y contramedidas en entorno Windows

Piratería interna, medidas de protección, desarrollo de herramientas (2ª edición)

índice

563