

Índice

Prólogo	15
Capítulo I	
Introducción	17
1. Ejercicios Red Team.....	17
2. Definición.....	17
3. Diferencias entre auditoría, test de intrusión y ejercicio Red Team.....	20
4. Distinción de los equipos involucrados.....	22
Red Team.....	23
Blue Team	23
White Team	23
Purple Team.....	24
5. Objetivo del ejercicio.....	24
6. Pensamiento crítico	27
7. Beneficios.....	28
8. Uso de los ejercicios para la toma de decisiones	29
9. Metodología.....	30
Ejecución como proceso continuo	32
Organización del equipo	33
Pautas para la ejecución	33
Capítulo II	
Planificación del ejercicio	35
1. Investigación preliminar	35
2. Identificación de objetivos	36
Definición de activos genéricos	37
Definición de activos granulares	38

Hitos conseguidos y grado de acceso.....	39
Modelado de amenazas	39
3. Definición de vectores.....	40
4. Despliegue de la infraestructura necesaria	41
Uso de los sistemas de salto	42
Contratación de la infraestructura	45
5. Evitar la detección del equipo	46
Durante el proceso inicial de enumeración	47
Pautas generales para la intrusión	47
6. Uso de software no detectable por sistemas de seguridad	49
Verificación de software sin firmas	50

Capítulo III

Vectores de acceso digitales.....53

1. Descripción.....	53
2. Intrusión a nivel de perímetro.....	55
Enumeración	56
Aspectos previos para tener en cuenta	59
Detección de sistemas autónomos y rangos de red	61
Detección de dominios y subdominios	71
Extracción de información	79
Enumeración activa.....	81
Identificación de un vector de acceso.....	83
Acceso a redes internas e implantación de persistencia.....	84
Acceso interactivo al sistema.....	86
Ejemplos de vectores reales	87
Escenario 1: Intrusión mediante SQL Injection	87
Escenario 2: Intrusión mediante la interacción con servidores internos	87
Escenario 3: Intrusión mediante SAP público.....	88
3. Intrusión mediante redes y clientes Wi-Fi.....	89
Enumeración pasiva	90
Identificación de localizaciones de objetivos	90
Análisis de activos.....	91
Selección de activos	92
Búsqueda de información sensible.....	93
Preparación de la infraestructura.....	93
Enumeración activa.....	94
Vector de acceso.....	95
Proceso para la intrusión interna.....	96

Capítulo IV

Vectores de acceso físicos.....	97
1. Descripción.....	97
2. Metodología.....	98
Investigación previa sobre la organización y ubicaciones de la misma.....	98
Definición de ubicaciones objetivo y enfoque de la intrusión.....	99
Análisis activo del entorno físico.....	100
Análisis y planificación de los posibles vectores.....	104
Desarrollo de pretextos para la interacción con empleados y/o seguridad.....	104
Práctica interna del equipo.....	104
Ejecución de las pruebas para la intrusión física.....	105
Intrusión interna en la organización.....	105
3. Técnicas para el desarrollo del vector.....	105
Evasión del control de acceso.....	105
Evasión de medidas de seguridad.....	106
Apertura de cerraduras - Lockpicking.....	107
4. Acceso a la red interna.....	107
Despliegue de dispositivo externo.....	108
Acceso a sistema interno de un empleado.....	108

Capítulo V

Vectores de acceso mediante Ingeniería Social.....	111
1. Descripción.....	111
2. Metodología.....	113
Investigación previa sobre la organización y empleados de la misma.....	113
Análisis y planificación de los posibles vectores.....	115
Definición de empleados objetivo y análisis en profundidad.....	116
Desarrollo de pretextos y escenarios completos.....	117
Despliegue de la infraestructura necesaria.....	118
Ejecución de las pruebas.....	118
Intrusión interna en la organización.....	118
3. Pautas para la creación de escenarios.....	118
4. Técnicas para el desarrollo del vector.....	121
Interacción mediante correo o web (Phishing).....	122
Envío de correo fraudulento requiriendo información.....	122
Redirección a página falsa.....	122
Código malicioso en documentos ofimáticos.....	123
Uso de malware.....	127
Automatización mediante herramientas.....	127

Interacción telefónica (Vishing).....	128
Interacción personal	129
Uso de dispositivos externos.....	131
5. Acceso a la red interna de la organización	131

Capítulo VI

Compromiso inicial y enumeración interna 133

1. Descripción.....	133
2. Análisis del sistema accedido.....	133
Verificar privilegios del usuario e información básica.....	134
Identificación de la configuración de red	134
Verificación de acceso a Internet.....	135
Identificación de conexiones establecidas	136
Identificación de usuarios.....	137
Identificación de software instalado.....	137
Acceso a recursos internos.....	138
Identificación de comandos ejecutados y conexiones RDP previas.....	138
3. Elevación de privilegios en el sistema.....	139
4. Despliegue de persistencia	140
5. Enumeración interna	140
6. Recomendaciones adicionales.....	143
Cambio de fechas	144
Mediante el uso de PowerShell	144
Mediante el uso de software externo como nircmd	144
Uso de directorios y recursos existentes	145
Identificación de sistemas colindantes o similares.....	145

Capítulo VII

Intrusión Interna y Elevación de Privilegios..... 147

1. Descripción.....	147
2. Pautas generales para la intrusión interna	148
Configuraciones por defecto	148
Incorrecta segmentación de red.....	148
Reutilización de credenciales.....	149
Identificación de credenciales de administradores de dominio	150
3. Técnicas para la obtención de credenciales de dominio.....	150
Análisis de SYSVOL y Group Policy Preferences (GPP)	151
Extracción de credenciales mediante Mimikatz.....	153

Extracción de credenciales mediante volcado del proceso lsass.exe	154
Revisión del histórico de credenciales	155
Extracción de SPN Services Accounts mediante Kerberoast.....	156
Spoofing y uso de servicios falsos	157
4. Extracción de usuarios internos.....	158
Extracción selectiva de usuarios	158
Extracción masiva de usuarios	158
Extracción local del recurso NTDS.DIT.....	158
Extracción remota de hash de usuarios	159
5. Principales técnicas para la elevación de privilegios local.....	160
En entornos Windows	161
Elevación de privilegios manual	161
Verificación automática.....	165
En entornos Unix.....	166
Elevación de privilegios manual	166
Verificación automática.....	169
6. Ataques dirigidos de fuerza bruta.....	169
Pautas para la creación de diccionarios.....	170
Ataques en anchura	171
Ataques masivos contra sistemas internos	172
Cracking del hash NTLM en base al hash LM	174
7. Recursos adicionales.....	175
Enumeración de usuarios	175
Habilitación de funcionalidades para la extracción de credenciales	176
Análisis de sistemas internos en busca de credenciales	176
Captura de teclas mediante Powershell.....	178
Identificación de sistemas de seguridad internos	179
Cambio del nombre de los sistemas origen utilizados	179

Capítulo VIII

Movimiento Lateral	181
1. Descripción.....	181
2. SMB	182
SMBclient	182
PSEXEC	183
PSTools.....	185
Pass the Hash mediante WCE y PSEXEC	186
Otras herramientas útiles.....	187
3. WMI.....	188

WMIC	189
WMIS	189
Wmiexe	190
Otras herramientas útiles	190
4. COM	191
5. RDP	191
Acceso mediante Pass the Hash	193
Secuestro de sesión	193
Habilitar múltiples sesiones RDP	194
Activación del servicio RDP	194
6. Powershell	195
Conexion remota mediante Powershell	195
Descarga y ejecución directamente en memoria	195
Frameworks relevantes	196
Scripts individuales	196
7. Redirección de puertos y túneles	198
Sistemas Windows	198
Sistemas Unix	199
8. Conexiones inversas	200
9. Recursos adicionales	201

Capítulo IX

Despliegue de persistencia	203
1. Descripción	203
2. Tipos de persistencias	203
3. Aspectos previos a tener en cuenta	205
4. Implantación de persistencia en servidores accesibles desde Internet (DMZ) ..	207
5. Generación de claves	208
6. Implantación de persistencia en Windows	209
Conexion directa a Internet	210
Conexion mediante proxy con o sin credenciales	210
Conexion mediante proxy con autenticación NTLM	211
Ejemplo	212
7. Implantación de persistencia en Linux	213
Conexion directa a Internet	213
Conexion mediante proxy con o sin credenciales	213
Conexion mediante proxy con autenticación NTLM	214

Ejemplo	214
8. Ejecución periódica	215
Windows.....	215
Unix.....	216
9. Evasión de AppLocker	217
Evasión mediante Bitsadmin y Regsvr32	217
Evasión mediante Powershell (CL_Invocation/CL_LoadAssembly)	218
10. Persistencias alternativas.....	218
Desinstalar actualizaciones	218
Modificación de binarios.....	218
Backdoor Wi-Fi.....	219
Uso de otros protocolos	220

Capítulo X

Análisis interno de la organización y acceso a activos críticos221

1. Descripción.....	221
2. Análisis del directorio activo e infraestructura	222
Identificación de usuarios, grupos y privilegios.....	223
Identificación de sites y subredes.....	224
Identificación de relaciones de confianza.....	224
Identificación de recursos compartidos.....	226
Análisis e identificación de sistemas críticos o sensibles.....	227
Principales herramientas	227
3. Análisis por departamentos internos	228
Análisis de los puestos de usuario.....	228
Análisis de recurso compartidos del departamento.....	229
Identificación y acceso a aplicaciones internas del departamento	230
Grabación de actividad de los empleados	230
4. Exfiltración de información.....	232
Exfiltración mediante SMB y conexión RDP	232
Uso de conexiones SSH con los VPSs.....	232
Uso de servicios públicos.....	232
Subida de ficheros a aplicaciones públicas en Internet.....	233
5. Evitar dejar huellas en los sistemas	233
Evitar el registro de comandos ejecutados.....	233
Alteración de los recursos	234
Evitar modificaciones internas	234
6. Reacción frente a la pérdida de acceso interno	234

7. Conclusiones	235
Índice alfabético	237
Índice de imágenes	241
Otros títulos de la colección	245