

Índice

Introducción	13
Capítulo I	
Ethical Hacking.....	17
1. Objetivos.....	17
2. Tipos de auditoría.....	18
3. Agregados al proceso.....	20
Pruebas de stress: DOS/DDOS	20
APT: Amenazas avanzadas persistentes.....	21
Fuga de información interna	21
Comunicaciones wireless & VOIP.....	22
La importancia del rol	22
4. Evaluación de seguridad	23
Vulnerabilidades.....	23
Estándares y modelos	24
Metodología	27
El equipo de auditoría	28
Alcance del proyecto.....	28
Selección e información del objetivo.....	30
Confección del ataque e intrusión controlada: Ampliación de miras.....	31
Revisión del proceso: Medidas correctoras.....	33
Documentación	33
Interlocutores y almacenamiento de la información	33
5. Publicación de una vulnerabilidad	34
Reservar CVE.....	34
Detalles técnicos para CVE.....	34
Ejemplo real: CVE-2013-5572	35
6. Nuevas tendencias	37
Pentesting by Design.....	37

7. Atacantes de sombrero.....	38
-------------------------------	----

Capítulo II

La información es poder.....	41
------------------------------	----

1. Procesos asociados.....	41
Footprinting.....	42
PoC: Shared hosting.....	44
PoC: DNS Caché Snooping y Evilgrade.....	47
PoC: El correo.....	49
Fingerprinting.....	53
Half Scan.....	53
ACK Scan.....	53
Null Scan.....	53
Xmas Scan.....	54
FIN Scan.....	54
Idle Scan.....	54
Técnicas de escaneo para evasión de protecciones.....	55
Nmap.....	61
Fingerprint Web.....	61
PoC: Nmap + scripts.....	64
PoC: Shodan.....	67
2. Google y cia.....	70
3. Creación del mapa de información.....	72
4. Orientando el pentesting hacia un APT.....	78
PoC: Obteniendo correos.....	79

Capítulo III

Confeccionando el ataque.....	83
-------------------------------	----

1. Entornos.....	83
2. Auditoría perimetral.....	83
Pruebas.....	84
Identificación de servicios.....	85
PoC: Identificación de vulnerabilidad explotable.....	86
Análisis de información.....	87
Crawling, bruteforce y otras técnicas.....	87
Localización de puntos de entrada.....	97
Métodos HTTP.....	98
Protección contra Clickjacking.....	100
Detección y explotación.....	100

Análisis SSL	101
Fuzzing	105
Manipulación de parámetros.....	106
Inclusión local y remota.....	108
Búsqueda de Path Disclosure.....	110
Acceso no autorizado.....	111
Subida de ficheros.....	112
Ataques a los puntos de entrada.....	114
Gestión de sesiones.....	115
Top 10 OWASP 2017	116
Top 10 OWASP 2021	117
3. Auditoría interna	118
PTES: Penetration Testing Execution Standard	119
Pruebas	120
PoC: Escenario inicial de auditoría interna.....	122
Wireshark: El analizador amigo.....	129
PoC: Sniffing remoto con Wireshark	135
Satori y p0f herramientas: sniffer pasivo.....	137
Pintar tráfico de red.....	138
Immunity Stalker	138
PoC: Obtención del primer dato de interés	139
PoC: Pass The Hash (PtH Attack).....	144
4. Escalada de privilegios en sistemas Windows.....	148
PoC: DLL Hijacking en Windows	152
5. Escalada de privilegios en sistemas GNU/Linux	153
PoC: Escalando en Linux	154
PoC: Escalada de privilegios.....	158
PoC: Pivoting + PtH = Paseo por la organización	161
6. Interna con privilegios	162
Pruebas	162
PoC: Evaluación de configuraciones.....	163
7. Wireless & VOIP.....	165
Pruebas	165
PoC: Descubriendo el mundo inalámbrico en la empresa	167
Wifite	169
PoC: Análisis de seguridad en la red	170
La red de invitados.....	170
La red WPA/WPA2 con PSK.....	171
La red Enterprise.....	172
PoC: Rogue AP en la empresa.....	173
PoC: Rogue AP inyectando Javascript botnet.....	175

Otras PoC's posibles en distintos entornos Wireless.....	176
PoC: Conociendo el entorno VOIP de la organización.....	179
PoC: Recogida de información y evaluación de seguridad	179
8. DoS/DDoS.....	180
Historia de las técnicas DDoS.....	181
Técnicas	183
Objetivos en una auditoría	184
El proceso ético	185
Pruebas	186
Resumen: Ataques en general.....	186
PoC: Poco tiempo de actuación y mucho de preparación.....	187
PoC: Colapsando las conexiones	190
Herramientas utilizadas.....	192
9. APT	193
Historia de APT.....	194
Pruebas	195
PoC: Estudio del conjunto de muestra a auditar	196
PoC: Preparación y configuración de pruebas	198
PoC: Cebos para dispositivos móviles.....	200
10. Fuga de información	204
Pruebas	205
PoC: Powershell y obtención de sesión remota	206
PoC: Shellcodes no detectables.....	208
PoC: Evasiones de proxy con paciencia y pruebas	209
11. PoC: Data Exfiltration Toolkit	210

Capítulo IV

Recomendaciones del proceso	213
1. Las recomendaciones	213
2. Medidas correctores en auditoría perimetral	214
Autenticación	214
Acceso	215
Criptografía y datos sensibles	216
Sesiones.....	217
Comunicaciones y protocolos	218
Entradas, codificación y errores.....	219
3. Medidas correctoras en auditoría interna.....	220
Medidas correctoras para ataques PtH	220
Configuración de elementos de seguridad en la red.....	224

Inventariado de máquinas y acotar responsabilidades	224
Evaluación de redes y recomendación	225
4. Medidas correctoras en auditoría de caja blanca.....	225
5. Medidas correctoras en DOS/DDOS	226
6. Otras medidas correctoras	227
 Capítulo V	
Generar informe.....	229
1. Nociones de un informe.....	229
2. Plantillas	230
Auditoría perimetral.....	230
Auditoría interna	231
Auditoría wireless	232
3. Control de cambios.....	233
4. Ejecutivo Vs Técnico	233
Ejemplo ejecutivo.....	234
5. Reportes automáticos	234
Análisis.....	235
 Índice de imágenes	 237
 Índice alfabético	 243

