

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
Ley Hacking 23 de Diciembre de 2010.....	27
5. Metodología.....	28
El equipo de auditoría	29
Alcance del proyecto.....	29
Selección e información del objetivo.....	31
Confección del ataque e intrusión controlada: Ampliación de miras.....	32
Revisión del proceso: Medidas correctoras.....	34
Documentación	34
Interlocutores y almacenamiento de la información	34
6. Publicación de una vulnerabilidad	35
Reservar CVE.....	35
Detalles técnicos para CVE.....	35
Ejemplo real: CVE-2013-5572	36



7. Nuevas tendencias	38
Pentesting by Design.....	38
8. Atacantes de sombrero.....	39

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
Nmap.....	55
Fingerprint Web.....	55
PoC: Nmap + scripts.....	58
PoC: Shodan.....	61
2. Google y cia.....	64
3. Creación del mapa de información.....	66
4. Orientando el pentesting hacia un APT.....	72
PoC: Obteniendo correos.....	73

Capítulo III

Confeccionando el ataque.....77

1. Entornos.....	77
2. Auditoría perimetral.....	77
Pruebas.....	78
Identificación de servicios.....	79
PoC: Identificación de vulnerabilidad explotable.....	80
Análisis de información.....	81
Crawling, bruteforce y otras técnicas.....	81
Localización de puntos de entrada.....	91
Métodos HTTP.....	92
Protección contra Clickjacking.....	94



Detección y explotación.....	94
Análisis SSL	95
Fuzzing	99
Manipulación de parámetros.....	100
Inclusión local y remota.....	102
Búsqueda de Path Disclosure.....	104
Acceso no autorizado.....	105
Subida de ficheros.....	106
Ataques a los puntos de entrada.....	108
Gestión de sesiones.....	109
Top 10 OWASP 2013	110
3. Auditoría interna	111
Pruebas	112
PoC: Escenario inicial de auditoría interna	114
Wireshark: El analizador amigo.....	122
PoC: Sniffing remoto con Wireshark	128
Satori y p0f herramientas: sniffer pasivo	129
Pintar tráfico de red.....	130
Immunity Stalker	131
PoC: Obtención del primer dato de interés	131
PoC: Pass The Hash (PtH Attack).....	137
PoC: Escalada de privilegios.....	140
PoC: Pivoting + PtH = Paseo por la organización	143
4. Interna con privilegios	144
Pruebas	145
PoC: Evaluación de configuraciones.....	145
5. Wireless & VOIP.....	147
Pruebas	148
PoC: Descubriendo el mundo inalámbrico en la empresa	150
Wifite	152
PoC: Análisis de seguridad en la red	153
La red de invitados.....	153
La red WPA/WPA2 con PSK.....	154
La red Enterprise.....	155
PoC: Rogue AP en la empresa.....	156
PoC: Rogue AP inyectando Javascript botnet	158
Otras PoC's posibles en distintos entornos Wireless.....	159
PoC: Conociendo el entorno VOIP de la organización	162
PoC: Recogida de información y evaluación de seguridad	162
6. DoS/DDoS.....	163
Historia de las técnicas DDoS.....	164



Técnicas	166
Objetivos en una auditoría	167
El proceso ético	168
Pruebas	169
Resumen: Ataques en general	169
PoC: Poco tiempo de actuación y mucho de preparación	170
PoC: Colapsando las conexiones	173
Herramientas utilizadas	175
7. APT	176
Historia de APT	177
Pruebas	178
PoC: Estudio del conjunto de muestra a auditar	179
PoC: Preparación y configuración de pruebas	181
PoC: Cebos para dispositivos móviles	184
8. Fuga de información	187
Pruebas	188
PoC: Powershell y obtención de sesión remota	189
PoC: Shellcodes no detectables	191
PoC: Evasiones de proxy con paciencia y pruebas	192

Capítulo IV

Recomendaciones del proceso	195
1. Las recomendaciones	195
2. Medidas correctoras en auditoría perimetral	196
Autenticación	196
Acceso	197
Criptografía y datos sensibles	198
Sesiones	199
Comunicaciones y protocolos	200
Entradas, codificación y errores	201
3. Medidas correctoras en auditoría interna	202
Medidas correctoras para ataques PtH	202
Configuración de elementos de seguridad en la red	206
Inventariado de máquinas y acotar responsabilidades	206
Evaluación de redes y recomendación	207
4. Medidas correctoras en auditoría de caja blanca	207
5. Medidas correctoras en DOS/DDOS	208
6. Otras medidas correctoras	209



Capítulo V

Generar informe.....	211
1. Nociones de un informe.....	211
2. Plantillas.....	212
Auditoría perimetral.....	212
Auditoría interna.....	213
Auditoría wireless.....	214
3. Control de cambios.....	215
4. Ejecutivo Vs Técnico.....	216
Ejemplo ejecutivo.....	216
5. Reportes automáticos.....	217
Análisis.....	217
Índice alfabético.....	221
Índice de imágenes.....	223
Índice de tablas.....	226
Libros publicados.....	227
Recover Messages.....	237
Cálculo Electrónico.....	238

