ÍNDICE DETALLADO DE CONTENIDOS

PRÓLOGO A LA PRIMERA EDICIÓN xv

AGRADECIMIENTOS xix

AGRADECIMIENTOS ESPECIALES xxi

INTRODUCCIÓN. xxiii

¿Por qué hacer una prueba de intrusión? xxiv
¿Por qué Metasploit? xxiv
¿Qué contiene este libro? xxv
Novedades en esta edición. xxvi
Un apunte sobre ética. xxvii

1. ASPECTOS BÁSICOS DE LAS PRUEBAS DE INTRUSIÓN. 1

Fases del PTES. 2
Interacciones previas al encargo. 2
Recopilación de información 2
Modelado de amenazas 2
Análisis de vulnerabilidades. 3
Ataque 3
Postataque 3
Elaboración de informes 4
Tipos de pruebas de intrusión 4
Pruebas abiertas. 5
Pruebas encubiertas 5
Escaneos de vulnerabilidades 5
Instalación de Kali, Metasploit y Metasploitable. 6
Resumiendo. 6

2. ASPECTOS BÁSICOS DE METASPLOIT 7

Terminología 8
Vulnerabilidad 8
Carga útil 8
Código shell. 8
Módulo 8
Receptor 9
Interfaces de Metasploit 9
MSFconsole 9
Scripts de recursos 10
Armitage y Cobalt Strike 11
Utilidades de Metasploit 11
MSFvenom. 11
NASM Shell. 13
Metasploit Pro 13
Resumiendo. 13

3. RECOPILACIÓN DE INFORMACIÓN 15

Recopilación de información pasiva 16
El buscador Whois 16
Netcraft 17
Análisis de DNS 18
Recopilación de información activa 19
Escaneo de puertos con Nmap 19
Escaneo de puertos con Metasploit 26
Escaneos dirigidos 27
Escaneo para protocolos SMB 27
A la caza de servidores Microsoft SQL mal configuradas. 28
Buscar Buckets S3 30
Buscar versiones de servidores SSH 30
Buscar servidores FTP 31
Barridos de protocolo simple de gestión de red (SNMP) 32
Escribir un escáner personalizado 33
Resumiendo. 35

4. ANÁLISIS DE VULNERABILIDADES 37

El escaneo básico de vulnerabilidades 38
Escanear con Nexpose 39
Configurar Nexpose 40
Importar informes a Metasploit 42
Ejecutar Nexpose en MSFconsole 43
Escanear con Nessus 44
Configurar Nessus 45
Crear escaneos. 46
Crear políticas de escaneo. 46
Visualizar informes 47
Importar los resultados a Metasploit 47
Escanear con Nessus en Metasploit. 48
Escáneres de vulnerabilidades especializados 51
Validar inicios de sesión SMB. 51
Buscar escáneres para nuevas vulnerabilidades 52
Resumiendo. 53

5. EL PLACER DE ATACAR 55

Ataques básicos. 56
En busca de un ataque 56
searchsploit 57
info 58
Seleccionar un ataque 60
show payloads 61
show targets. 62
set y unset 63
setg y unsetg 63
save 63
exploit 64
Atacar una máquina Windows 64
Atacar una máquina Ubuntu 67
Resumiendo. 70

6. METERPRETER 71

Comprometer una máquina virtual Windows 72
Escaneo de puertos con Nmap 72
Fuerza bruta para autenticar el servidor MySQL 73
Cargar funciones definidas por el usuario 73
Comandos básicos de Meterpreter 75
Realizar capturas de pantalla 75
Buscar información de la plataforma 75
Captura pulsaciones de teclas 76
Extraer hashes de contraseñas 77
Pasar el Hash 78
Mimikatz y Kiwi 79
Escalado de privilegios 81
Técnicas de movimiento lateral 84
Suplantación del token 85
Ataques DCSync y Golden Ticket 87
Otros comandos útiles de Meterpreter 89
Activar los servicios de escritorio remoto 89
Visualizar todo el tráfico de un objetivo 89
Rastrear un sistema 90
Establecer la persistencia 90
Manipular las API de Windows con Railgun 94
Saltar a otros sistemas 95
Resumiendo 95

7. EVITAR DETECCIONES 97

Crear binarios independientes con MSFvenom 98
Codificar con MSFvenom 100
Empaquetar ejecutables 102
Plantillas de ejecutables personalizadas 103
Lanzar cargas útiles sigilosamente 104
Módulos de evasión 105
Desarrollar cargas útiles personalizadas 107
Generar ejecutables a partir de archivos de Python 110
Resumiendo 112

8. INGENIERÍA SOCIAL 113

Actualizar y configurar el Social-Engineer Toolkit 114
Ataques Spear-Phishing 115
Configurar un servidor de correo electrónico 115
Envío de correo electrónico malicioso 116
Suplantar la identidad con Gophish 118
Ataques web 119
Robo de nombres de usuario y contraseñas 120
Técnica del tabnabbing 122
Eludir la autenticación de doble factor 123
Ataques del tipo Infectious Media Generator 124
Resumiendo 125

9. ATAQUES DEL LADO DEL CLIENTE. 127

Ataques basados en navegador 128
Buscar ataques en Metasploit 129
Automatizar ataques con AutoPwn2 131
Buscar los ataques más recientes 132
Ataques de formato de archivo 133
Atacar documentos de Word 133
Enviar cargas útiles 134
Resumiendo. 135

10. ATAQUES INALÁMBRICOS. 137

Conectarse a adaptadores inalámbricos 138
Monitorizar el tráfico wifi 139
Ataques de desautenticación y DoS 140
Capturar y descifrar *handshakes* 141
Ataques Evil Twin 142
Analizar el tráfico con Metasploit. 145
Recolectar credenciales con WiFi Pineapple 146
Resumiendo. 149

11. MÓDULOS AUXILIARES 151

Conocer los módulos auxiliares 151
Buscar módulos HTTP 154
Crear un módulo auxiliar 155
Escribir el módulo 156
Ejecutar el módulo 158
Depurar el módulo 159
Resumiendo. 160

12. IMPORTAR ATAQUES AL FRAMEWORK 161

Conceptos básicos del lenguaje ensamblador 162
Registros EIP y ESP 162
El conjunto de instrucciones JMP 162
NOP y NOP slides 162
Deshabilitar protecciones 163
Importar desbordamientos de búfer 163
Desmontar vulnerabilidades existentes 165
Configurar la definición del ataque 166
Probar el ataque básico. 167
Implementar características del framework 168
Añadir aleatoriedad 169
Eliminar el NOP Slide 169
Eliminar el código shell ficticio 170
Importar un ataque de sobreescritura SEH 172
Resumiendo. 177

13. CONSTRUIR SUS PROPIOS MÓDULOS 179

Ejecutar comandos en MS SQL 180
Habilitar procedimiento a nivel de administrador 180
Ejecutar el módulo 181

Explorar el código del módulo 182
Crear un módulo nuevo 184
Editar un módulo existente 185
Ejecutar el ataque shell 186
Definir el ataque 186
Cargar los scripts de PowerShell 187
Ejecutar el ataque 190
Resumiendo 191

14. CREAR SUS PROPIOS ATAQUES 193

El arte del fuzzing 194
Descargar la aplicación de prueba 194
Escribir el fuzzer 194
Probar el fuzzer 195
Controlar el gestor de excepciones estructuradas 198
Saltarse las restricciones 200
Obtener una dirección de retorno 202
Incluir saltos hacia atrás y saltos cercanos 204
Añadir una carga útil 206
Caracteres erróneos y ejecución remota de código 206
Resumiendo 209

15. PRUEBA DE INTRUSIÓN SIMULADA 211

Interacciones previas al ataque 212
Recopilación de información 212
Modelado de amenazas 213
El ataque 214
Ejecutar el ataque 215
Establecer la persistencia 215
Postataque 216
Escanear el sistema Linux 217
Identificar servicios vulnerables 219
Atacar Apache Tomcat 220
Atacar servicios oscuros 222
Cubrir el rastro 223
Resumiendo 226

16. PRUEBAS DE INTRUSIÓN EN LA NUBE 227

Aspectos básicos de la seguridad en la nube 228
Gestión de identidades y accesos 228
Funciones sin servidor 229
Almacenamiento 231
Contenedores de Docker 231
Configurar entornos de prueba en la nube 233
Adquisición de contenedores 235
Escapar de los contenedores de Docker 238
Kubernetes 240
Resumiendo 240

A. CONFIGURAR UN ENTORNO DE PRUEBA 241
x86 y AMD64 242
ARM y Apple Silicon 243
Instalar metapaquetes de Kali 245

B. PÁGINAS DE REFERENCIA 247
MSFconsole 247
Meterpreter 249
MSFvenom 250
Meterpreter para después del ataque 251