Índice

Capítulo I
Acceso físico al equipo 13

1. BIOS 13
BIOS 14
UEFI 15
Ataques sobre BIOS y UEFI 17

2. Memoria RAM 22
Cold boot 22
Ataque DMA 24

3. Acceso físico y obtención de control 25
Rubber Ducky 26
Sticky keys 28
Chntpw: Modificando la SAM 31
Kon-Boot y NetHunter 33
PowerShell: Ejecución de payloads 34
7 formas de hacer bypass a la política de ejecución de PowerShell 37
Bots en PowerShell 38
VSS: Copia ficheros del sistema 42
SAM: Carpeta repair 43
Bypass de BitLocker 43

Capítulo II
Autenticación y autorización en Windows 49

1. Introducción 49

2. Windows Logon 50

3. Autenticación y procesamiento de credenciales 50
Single Sign-On 54
Local Security Authority 54
Almacenamiento de credenciales 56

4. Access tokens 57
Robo y suplantación de tokens 62
5. Control de Cuentas de Usuario (UAC) 65
6. Bypass UAC 69
Bypass UAC mediante CompMgmtLauncher 72
Bypass UAC mediante App Paths 77
Bypass UAC fileless mediante Eventvwr 80
Bypass UAC fileless mediante Sdclt 84

Capítulo III
NT LAN Manager (NTLM) 87
1. Introducción 87
2. LAN Manager (LM) 92
Hashes LM 92
3. NTLMv1 94
Hashes NT 94
Protocolo de autenticación NTLMv1 94
4. NTLMv2 96
Protocolo de autenticación NTLMv2 96
5. Extracción de credenciales LM y NT de SAM 97
Extracción de credenciales de SAM con Metasploit 98
Extracción de credenciales de SAM con PwDump7 99
Extracción de credenciales de SAM con Mimikatz 99
6. Extracción de credenciales NTLM en memoria 100
Extracción en memoria con Mimikatz 100
Extracción en memoria con Windows Credentials Editor (WCE) 101
7. Cracking de hashes LM y NT 102
Cracking con John the Ripper 103
Cracking con Hashcat 104
8. Pass-The-Hash 105
Pass-The-Hash con Mimikatz 107
Pass-The-Hash con Windows Credentials Editor (WCE) 112
Pass-The-Hash para PsExec 113
9. Ataque NTLM Relay 114
NTLM Relay con Metasploit 115
NTLM Relay con Impacket 119
10. Obtención de credenciales NTLM con Responder.py 123
11. Conclusiones 128

Capítulo IV
Kerberos.....131

1. Introducción a Kerberos.....131
Funcionamiento.....132

2. Puntos débiles del protocolo Kerberos.....139
Overpass-the-Hash.....141
Pass-the-Ticket.....146
Golden Ticket.....151
Silver Ticket.....159
Creación de tickets con PowerShell.....164
Creación de tickets con Metasploit.....166
Kerberoasting: Cracking de Tickets.....168

3. Reflexión sobre Kerberos.....168

Capítulo V
Ataques a Active Directory.....171

1. Introducción a Active Directory.....172
Conceptos básicos.....173
Cuentas locales en Active Directory.....174

2. Reconocimiento en Active Directory.....175
Comandos Windows de dominio.....175
PowerView.....179
BloodHound.....181

3. Explotar MS14-068 para escalar privilegios a administrador de dominio.....189

4. Obtener otras credenciales de Active Directory.....191

5. Base de datos de credenciales NTDS.dit.....192

6. Obtener base de datos NTDS.dit.....193
Copiar NTDS.dit mediante servicio Volume Shadow Copy.....194
Copiar NTDS.dit mediante Ntdsutil.....196
Copiar NTDS.dit mediante Invoke-NinjaCopy con PowerShell.....197
Extraer credenciales de la base de datos NTDS.dit.....198

7. Extraer credenciales de dominio mediante Metasploit.....199

8. Extraer credenciales de dominio con Mimikatz.....200

9. Extraer credenciales de dominio con DCSync de Mimikatz.....204

10. Ejecución de código en remoto.....207
Ejecución de código en remoto mediante AT.....208
Ejecución de código en remoto mediante Schtasks.....209

Ejecución de código en remoto mediante SC 210
Ejecución de código en remoto mediante WMIC 211
Ejecución de código en remoto mediante PsExec 213
Ejecución de código en remoto mediante WinRM 214

11. Persistencia en Active Directoy 215
Golden ticket y KRBTGT 215
Skeleton Key 218

12. Conclusiones 220

Capítulo VI
Escalada de privilegios 223

1. Unquoted Service Paths 223

2. Servicios con privilegios mal configurados 227
Permisos mal configurados en el registro 227
Permisos de los servicios vulnerables 229

3. AlwaysInstallElevated 231

4. Programador de tareas 234
Windows XP SP3 y Sysax **FTP 5.33** 235

5. DLL Hijacking 236
DLL Hijacking a Ole32 y bypass de UAC 243

6. Credenciales almacenadas 246

7. Kernel exploits 247
Hot Potato y Rotten Potato 249
Bug MS16-135 252
Windows 7 SP1 y el CVE-2014-4113 254
Windows 8.1 y el CVE-2015-0004 255
Windows 8.1 y el CVE-2015-0002 257

8. Sobre los Payloads 258
Servidor Telnet 258
UltraVNC 259
El registro de Windows 261
Herramientas de evasión de antivirus 267

9. Conclusiones y reflexiones 271

Capítulo 7
Ataques a servicios y aplicaciones 273

1. SNMP 273
Ataques a SNMP 274

Obtener información sobre el servicio SNMP 275
Información que se obtiene 276
Fuerza bruta a SNMP 278
Modificar objetos MIB 280
Finalizando 281

2. SMB 281
Obtener equipos 282
Enumerar recursos compartidos. 284
Enumerar usuarios 287
Fuerza bruta 289
Redirección a SMB 290

3. Escritorios Remotos 294
Escritorios desde Internet 295
Jailbreak sobre las restricciones de las aplicaciones 302
Dame tu sesión RDP 311

4. No solo es Windows 313
Impresoras 313
MS Office 317
EMET 318

Índice alfabético 321

Índice de imágenes 323