

Índice

Capítulo I

Autenticación y autorización en Windows.....	13
1. Introducción.....	13
2. Windows Logon	14
3. Autenticación y procesamiento de credenciales.....	14
Single Sign-On.....	18
Local Security Authority	18
Almacenamiento de credenciales.....	20
4. Access tokens.....	21
Robo y suplantación de tokens.....	26
5. Control de Cuentas de Usuario (UAC).....	29
6. Bypass UAC	33
Bypass UAC mediante CompMgmtLauncher	36
Bypass UAC mediante App Paths.....	41
Bypass UAC fileless mediante Eventvwr	44
Bypass UAC fileless mediante Sdclt.....	48

Capítulo II

NT LAN Manager (NTLM)	51
1. Introducción.....	51
2. LAN Manager (LM).....	56
Hashes LM	56
3. NTLMv1	58
Hashes NT	58
Protocolo de autenticación NTLMv1	58
4. NTLMv2.....	60
Protocolo de autenticación NTLMv2.....	60

5. Extracción de credenciales LM y NT de SAM.....	61
Extracción de credenciales de SAM con Metasploit.....	62
Extracción de credenciales de SAM con PwDump7.....	63
Extracción de credenciales de SAM con Mimikatz.....	63
6. Extracción de credenciales NTLM en memoria	64
Extracción en memoria con Mimikatz.....	64
Extracción en memoria con Windows Credentials Editor (WCE).....	65
7. Cracking de hashes LM y NT.....	66
Cracking con John the Ripper.....	67
Cracking con Hashcat.....	68
8. Pass-The-Hash	69
Pass-The-Hash con Mimikatz.....	71
Pass-The-Hash con Windows Credentials Editor (WCE).....	76
Pass-The-Hash para PsExec.....	77
9. Ataque NTLM Relay	78
NTLM Relay con Metasploit.....	79
NTLM Relay con Impacket.....	83
10. Obtención de credenciales NTLM con Responder.py	87
11. Conclusiones.....	92

Capítulo III

Kerberos.....95

1. Introducción a Kerberos.....	95
Funcionamiento.....	96
2. Puntos débiles del protocolo Kerberos	103
Overpass-the-Hash.....	105
Pass-the-Ticket.....	110
Golden Ticket.....	115
Silver Ticket.....	123
Creación de tickets con PowerShell.....	128
Creación de tickets con Metasploit.....	130
ASREPROasting.....	132
Kerberoasting.....	134
3. Reflexión sobre Kerberos.....	137

Capítulo IV

Ataques a Active Directory.....139

1. Introducción a Active Directory.....	140
--	------------

Conceptos básicos	141
Cuentas locales en Active Directory	142
2. Reconocimiento en Active Directory.....	143
Comandos Windows de dominio	143
PowerView	147
BloodHound	150
3. Escalada de privilegios mediante CVE-2014-6324.....	157
4. Escalada de privilegios mediante CVE-2020-1472 “Zerologon”	159
5. Obtener otras credenciales de Active Directory	163
6. Base de datos de credenciales NTDS.dit.....	164
7. Obtener base de datos NTDS.dit.....	165
Copiar NTDS.dit mediante servicio Volume Shadow Copy	166
Copiar NTDS.dit mediante Ntdsutil.....	168
Copiar NTDS.dit mediante Invoke-NinjaCopy con PowerShell	169
Extraer credenciales de la base de datos NTDS.dit.....	170
8. Extraer credenciales de dominio mediante Metasploit.....	171
9. Extraer credenciales de dominio con Mimikatz	172
10. Extraer credenciales de dominio con DCSync de Mimikatz	176
11. Ejecución de código en remoto	179
Ejecución de código en remoto mediante AT.....	180
Ejecución de código en remoto mediante Schtasks	180
Ejecución de código en remoto mediante SC	181
Ejecución de código en remoto mediante WMIC	183
Ejecución de código en remoto mediante PsExec.....	184
Ejecución de código en remoto mediante WinRM	185
12. Persistencia en Active Directoy	187
Golden ticket y KRBTGT	187
Skeleton Key	190
13. Conclusiones	191

Capítulo V

Escalada de privilegios	193
1. Unquoted Service Paths	193
2. Servicios con privilegios mal configurados	197
Permisos mal configurados en el registro.....	197
Permisos de los servicios vulnerables	199

3. AlwaysInstallElevated	201
4. Programador de tareas	204
5. DLL Hijacking	205
DLL Hijacking a Ole32 y bypass de UAC	211
6. Credenciales almacenadas	214
Contraseñas de red	215
7. Kernel exploits	217
Hot Potato y Rotten Potato	219
CVE-2020-0787	222
CVE-2020-0796	222
CVE-2021-1732	223
8. Herramientas automatizadas de escalada de privilegios	224
WinPEAS	225
9. Sobre los Payloads	228
Servidor Telnet	228
UltraVNC	229
El registro de Windows	231
Herramientas de evasión de antivirus	236
10. Conclusiones y reflexiones	242

Capítulo VI

Ataques a protecciones y servicios.....	245
1. SNMP.....	245
Ataques a SNMP	246
Obtener información sobre el servicio SNMP	247
Información que se obtiene	248
Fuerza bruta a SNMP	250
Modificar objetos MIB	252
Finalizando	253
2. SMB	253
Obtener equipos	254
Enumerar recursos compartidos	256
Enumerar usuarios	259
Fuerza bruta a SMB	261
Redirección a SMB	262
3. Escritorios Remotos	266
Escritorios desde Internet	267
Búsqueda de servidores remotos con Nmap	273

Fuerza bruta a RDP	274
Jailbreak sobre las restricciones de las aplicaciones	275

4. Conclusiones	293
------------------------------	------------

Capítulo VII

Acceso físico al equipo	295
--------------------------------------	------------

1. BIOS	295
----------------------	------------

BIOS	296
------------	-----

UEFI	297
------------	-----

Ataques sobre BIOS y UEFI	299
---------------------------------	-----

2. Memoria RAM	304
-----------------------------	------------

Cold boot	304
-----------------	-----

Ataque DMA	306
------------------	-----

3. Acceso físico y obtención de control	307
--	------------

Rubber Ducky	308
--------------------	-----

Sticky Keys	311
-------------------	-----

Chntpw: Modificando la SAM	313
----------------------------------	-----

Kon-Boot y NetHunter	315
----------------------------	-----

PowerShell: Ejecución de payloads	316
---	-----

7 formas de hacer bypass a la política de ejecución de PowerShell	319
---	-----

Bots en PowerShell	320
--------------------------	-----

VSS: Copia ficheros del sistema	324
---------------------------------------	-----

SAM: Carpeta repair	325
---------------------------	-----

Bypass de BitLocker	326
---------------------------	-----

Índice de imágenes	333
---------------------------------	------------

Índice alfabético	345
--------------------------------	------------

Otros libros publicados	347
--------------------------------------	------------

