Índice

Introducción
Pablo Vs BotPGP.....11

Capítulo I
Contexto y metodologías..... 17
1. Objetivos..... 17
2. Seguridad de la información..... 17
Ciberseguridad..... 20
3. Entendiendo el contexto 21
ISO 27001 22
Análisis y gestión del riesgo 23
El desarrollo seguro 24
4. Hacking Ético 25
El hacking ético como un proyecto..... 25
Red Team 27
Blue Team 28
Relacionando y diferenciando conceptos 29
5. Metodología (y modelos) 30
OWASP..... 31
OSSTMM..... 33
PTES 33
ISSAF..... 34
FIRST..... 34
MITRE..... 36
6. Fases del pentesting..... 38

Capítulo II
Recopilación, escaneo y enumeración de información 41
1. Objetivos..... 41
2. Recopilación de información..... 41
Recopilación pasiva de información..... 42
Recopilación activa de información 48
3. Escaneo..... 51

Descubrimiento de máquinas (Host Discovery) 52
Metasploit: Discovery/arp_sweep 53
Escaneo de puertos (PortScan) 57
Técnica ACK Scan 62
Identificación del sistema operativo 62
Técnicas de identificación de versiones: Banner Grabbing y Server Header 63
4. NMap 66
Descubrimiento de máquinas 67
Escaneo de puertos 69
Lab: Descubriendo máquinas y escaneando puertos 72
Timing 84
NSE o Nmap Scripting Engine 86
Lab: Enumeración detallada e identificación con NSE 92
5. HPing3 104
Lab: Descubriendo máquinas y escaneando puertos con hping3 107
6. Enumeración 116
Protocolos 116
7. NetExec (o la antigua crackmapexec) 153
Netexec y SMB 155
Netexec y SSH 165
Netexec y RDP 167
La base de datos: nxcdb 169

Capítulo III
Fuerza bruta y acceso a sistemas 173
1. Objetivos 173
2. Fuerza bruta 173
Basado en diccionario 174
Password Spraying 177
Hydra 177
Metasploit 179
NCrack 181
Crunch 183
Netexec 185
Lab: Poniendo a prueba la fuerza bruta 186
3. Acceso a sistemas 190
Acceso a través de SMB 190
Acceso a través de WinRM 195
Metasploit 199
Acceso a través de SSH 200

Capítulo IV
Explotación 203
1. Objetivos 203
2. Vulnerabilidades 204
3. Análisis de vulnerabilidades 207
Herramientas comunes 208
4. Explotación de vulnerabilidades 213
Tipos de conexión: Bind y Reverse 213
Staged y Stageless 215
Shells 217
Searchsploit 223
Exploits 226
Metasploit 238
5. (Stack) Buffer Overflow 250

Capítulo V
Post-Explotación 269
1. Objetivos 269
2. Post-Explotación 270
3. Recopilación de información 271
Información a obtener 271
Windows 272
GNU/Linux 279
4. Escalada de privilegios (PrivEsc) 284
Metodología 284
Windows 285
GNU/Linux 293
5. Dumping Creds 300
6. Pivoting 308
7. Movimiento lateral (***lateral movement***) 315

Índice alfabético 317

Índice de imágenes 319

Índice de tablas 327

Otros libros publicados 329