

Índice

| | |
|--|-----------|
| Introducción | 11 |
| Capítulo I | |
| Recolección de Información y Escaneo | 15 |
| 1.1 La información es la base en el mundo del hacking | 15 |
| 1.2 Definición del sistema objetivo..... | 15 |
| 1.3 Recolección de Información con Python..... | 16 |
| 1.3.1 Extraer información en servidores DNS utilizando DNSPython..... | 16 |
| 1.3.2 Ejecutar consultas WHOIS con pythonwhois | 18 |
| 1.3.3 GeoLocalización del objetivo con PyGeoIP | 20 |
| 1.4 Utilizar motores de búsqueda para recolectar información sobre un objetivo..... | 22 |
| 1.4.1 Google Hacking | 22 |
| 1.4.2 Shodan Hacking | 24 |
| 1.5 Ingeniería Social..... | 29 |
| 1.5.1 Social Engineering Framework..... | 29 |
| 1.5.2 Maltego | 36 |
| 1.6 Análisis de Metadatos con Python..... | 43 |
| 1.6.1 Análisis de metadatos en documentos PDF con PyPDF2 | 44 |
| 1.6.2 Análisis de metadatos EXIF con PIL (Python Imaging Library) | 45 |
| Capítulo II | |
| Escaneo, enumeración y detección de vulnerabilidades..... | 47 |
| 2.1 Reconocimiento y enumeración con Scapy..... | 47 |
| 2.1.1 TCP Connect Scan..... | 47 |
| 2.1.2 TCP Stealth Scan..... | 48 |
| 2.1.3 Escaneo UDP..... | 49 |
| 2.1.4 ACK Scan..... | 50 |
| 2.1.5 XMAS Scan | 51 |
| 2.1.6 FIN Scan..... | 52 |
| 2.1.7 NULL Scan | 53 |



| | |
|--|------------|
| 2.1.8 Window Scan | 53 |
| 2.2 Utilizando NMAP desde Python | 54 |
| 2.2.1 Script Engine | 54 |
| 2.2.2 Idle Scanning..... | 58 |
| 2.2.3 Timing Scanning | 59 |
| 2.2.4 Evasión de IDS/IPS..... | 60 |
| 2.2.5 Uso de la librería python-nmap..... | 63 |
| 2.3 Banner Grabbing para detección servicios vulnerables..... | 67 |
| 2.4 Integración de Nessus y Python..... | 68 |
| 2.4.1 PyNessus-rest para consultar la API REST de Nessus..... | 69 |
| 2.5 Integración de Metasploit Framework y Python..... | 72 |
| 2.5.1 Uso de python-msfrpc y el plugin MSGRPC de Metasploit Framework | 73 |
| 2.6 Integración de NeXpose y Python | 78 |
| 2.6.1 Pynexpose para utilizar NeXpose desde Python | 78 |
| 2.7 Integración de Latch y Python | 81 |
| 2.8 Conceptos básicos sobre el protocolo SNMP..... | 84 |
| 2.8.1. Atacando servicios SNMP con PySNMP | 85 |
| 2.9. Conceptos básicos sobre el protocolo SMB | 87 |
| 2.9.1. Aprovechando Sesiones SMB Nulas..... | 88 |
| 2.9.2. Atacando servicios SMB con PySMB..... | 90 |
| 2.10 Identificación de vulnerabilidades en aplicaciones web | 92 |
| 2.10.1 Uso de librerías en Python para entornos web | 92 |
| 2.10.2 OWASP TOP 10 | 100 |
| 2.10.3 W3AF para identificar vulnerabilidades en aplicaciones web | 126 |
| 2.11 Vulnerabilidades en servidores HTTP..... | 133 |
| 2.11.1 Ataques comunes contra arquitecturas web | 133 |
| 2.11.2 Nikto para auditorias de servidores web | 136 |
| 2.12 Identificación y Ataque de versiones vulnerables de OpenSSL..... | 140 |
| 2.12.1 SSLv2 Malformed Client Key Remote Buffer Overflow Vulnerability | 140 |
| 2.12.2 Predictable PRNG (Pseudo Random Number Generator) | 142 |
| 2.12.3 TLS Heartbeat Extension - Memory Disclosure (HeartBleed Vulnerability)..... | 147 |
| 2.13 Conceptos básicos sobre el protocolo FTP..... | 152 |
| 2.13.1 Implementaciones vulnerables de FTP | 153 |
| 2.13.2 Encontrando servidores FTP mal configurados | 157 |
| 2.14 Conceptos básicos sobre el protocolo SSH..... | 158 |
| 2.14.1. Atacando servicios SSH con Paramiko | 159 |
| 2.14.2. Creación de una Botnet SSH utilizando Fabric..... | 162 |



| | |
|--|------------|
| 2.15. Conceptos básicos sobre el protocolo SMTP | 165 |
| 2.15.1 Enumerando usuarios en servidores SMTP mal configurados..... | 166 |
| Capítulo III | |
| Elevación de privilegios y Garantizando el acceso..... | 169 |
| 3.1 Enumeración y recolección de información | 169 |
| 3.1.1 Enumeración en sistemas Windows | 170 |
| 3.1.2 Enumeración en sistemas Linux..... | 197 |
| 3.2 Control Remoto y puertas traseras | 224 |
| 3.2.1 Implementación de consolas bind e inversas | 224 |
| 3.2.2 Implementación de una consola inversa utilizando un tunel SSH cifrado..... | 227 |
| 3.2.3 Scripts en Metasploit Framework para crear puertas traseras..... | 230 |
| Capítulo IV. | |
| Ataques en el segmento de red local | 233 |
| 4.1 Python y Scapy para creación de paquetes y análisis de la red | 233 |
| 4.1.1 Fingerprint pasivo con p0f y Scapy | 239 |
| 4.1.2 Uso práctico de Scapy para ejecutar y detectar ataques en redes de datos locales | 243 |
| 4.2 Expandir el ataque en la red local de la víctima | 245 |
| 4.2.1 Identificando el segmento de red y las máquinas accesibles..... | 246 |
| 4.2.2 Redirección de Puertos y Forwarding de conexiones con SSH | 247 |
| 4.3 Usando Twisted en el segmento de red local..... | 249 |
| 4.4 Ataques de Hombre en medio (MITM) con Scapy y Python | 257 |
| 4.5 Ataques de DNS Spoofing con Scapy y Python | 259 |
| 4.6 Conceptos básicos y ataques en redes de datos IPv6 | 265 |
| 4.6.1 Enumeración de redes IPv6..... | 266 |
| 4.6.2 Ataque Neighbor Spoofing y MITM sobre IPv6..... | 267 |
| 4.6.3 Router Falso sobre IPv6..... | 269 |
| 4.6.4 Problemas de redirección | 270 |
| 4.7 Conceptos básicos y ataques en redes inalámbricas | 272 |
| 4.7.1 Sniffing en redes inalámbricas | 273 |
| 4.7.2 Estructura de los paquetes en un entorno de red inalámbrica | 274 |
| 4.7.3 Autenticación y asociación entre un cliente y un punto de acceso | 278 |
| 4.7.4 Ataques en redes inalámbricas | 286 |
| Índice alfabético | 313 |
| Índice de imágenes | 317 |
| Otros libros Publicados | 319 |

