

Índice

Introducción	11
Capítulo I	
Ataques en el segmento de red local	13
1.1 Redes Virtuales Privadas.....	13
1.1.1 OpenVPN	14
1.1.2 Hamachi	20
1.2 Tráfico sobre ICMP.....	24
1.2.1 ICMP SHELL – ISHELL	24
1.2.2 SoICMP.....	26
1.2.3 ICMPSH.....	27
Capítulo II	
Fuzzing y depuración de software	29
2.1 Procesos de fuzzing con Sulley Framework.....	29
2.1.1 Sulley Framework vs Ability Server.....	30
2.1.2 Vulnerabilidades en Software.....	33
2.2 Hooking de funciones en librerías con PyDBG	35
2.3 Rutinas de depuración con Immunity Debugger.....	38
2.3.1 Uso de Mona.py en Immunity Debugger.....	38
2.3.2 Uso de la API de Immunity Debugger	40
2.4 Desensamblaje y análisis de ficheros ejecutables	46
2.4.1 Análisis de ficheros con formato PE (Portable Executable) con PEFile.....	46
2.4.2 Desensamblaje de ficheros ejecutables con PyDASM.....	51
2.5 Análisis de memoria	52
2.5.1 Volcado y generación de imágenes de memoria con MDD y ProcDump.....	53
2.5.2 Volatility Framework.....	55
2.6 Análisis de Malware con Cuckoo Sandbox.....	72
2.6.1 Configuración de la máquina donde se ejecuta el motor de análisis.....	73



2.6.2 Configuración de las máquinas virtuales.....	77
2.6.3 Envío y análisis de muestras de Malware utilizando Cuckoo.....	78
2.7 Evasión de antivirus.....	82
2.7.1 Ofuscar shellcodes en Python.....	82
2.7.2 Veil Framework para evasión de Anti-Virus.....	84

Capítulo III

Anonimato con Python..... 91

3.1 Conceptos básicos de TOR (The Onion Router).....	92
3.1.1 Uso de STEM para controlar una instancia local de TOR.....	94
3.1.2 Consultando información sobre los repetidores disponibles en la red.....	97
3.1.3 Estableciendo conexiones contra circuitos de TOR desde Python.....	99
3.1.4 Túneles VPN sobre Hidden services en TOR con OnionCat.....	101
3.1.5 Ataques comunes en TOR.....	105
3.1.6 Utilizando Tortazo para atacar repetidores de salida en TOR.....	111
3.2 Conceptos Básicos y arquitectura de I2P.....	130
3.2.1 Servicio de NetDB en I2P para la construcción de túneles.....	135
3.2.2 Clientes y servicios en I2P.....	139
3.2.3 Definición y administración de servicios, EEPsITES y Plugins en I2P.....	140
3.2.4 Configuración de OnionCat/Garlicat en I2P.....	155
3.2.5 Streaming Library y BOB en I2P.....	158
3.3 Análisis comparativo entre I2P, TOR y Freenet.....	171
3.3.1 TOR vs I2P.....	172
3.3.2 Freenet vs TOR.....	173
3.3.3 I2P vs Freenet.....	174

Capítulo IV

Amenazas Persistentes Avanzadas..... 177

4.1 ¿Qué es una APT? (Advanced Persistent Threat).....	177
4.2 ¿Qué no es una APT?.....	179
4.3 Grupos y colectivos involucrados en campañas APT.....	179
4.3.1 Hacktivistas.....	180
4.3.2 Grupos y sindicatos criminales.....	181
4.3.3 Equipos de seguridad ofensiva apoyados por gobiernos.....	182
4.4 Anatomía de una campaña APT.....	182
4.4.1 Perfilar el objetivo.....	182
4.4.2 Comprometer el objetivo.....	183
4.4.3 Reconocer el entorno del objetivo.....	183



4.4.4 Extender el ataque desde el interior	184
4.4.5 Recolección, categorización y filtrado de información.....	184
4.4.6 Gestión y Mantenimiento.....	184
4.5 Herramientas y técnicas comunes en campañas APT	185
4.5.1 Inyección de código malicioso en procesos bajo sistemas Windows	186
4.5.2 Inyección de código malicioso en procesos bajo sistemas Linux	195
4.5.3 Inyección de código malicioso en procesos Python sobre sistemas Linux con Pyrasite	203
4.5.4 Creación de herramientas para espiar y registrar la actividad de las víctimas.....	209
4.5.5 Uso de PyMal para el análisis de Malware	246
4.5.6 Uso de Yara para el análisis de Malware.....	255
4.6 Usando de Django para localizar y representar visualmente servidores en Internet	259
4.6.1 Introducción a Django.....	259
4.6.2 Panel de control básico para una botnet utilizando Django y GeoDjango.....	260
4.6.3 Representación Geográfica de los nodos de salida de TOR usando Django y GeoDjango .	273
Índice alfabético	279
Índice de imágenes	283

