Índice

Prólogo **9**

Capítulo I Análisis forense e incidencias **13**

1. Introducción 13
2. Delitos informáticos 15
3. Principio de Locard 16
4. Definición de análisis forense 17
5. Respuesta a incidentes 18
6. Incidentes más comunes 19
7. Evidencia digital 20
8. RFC 3227. Recolección y manejo de evidencias 20
9. Buenas prácticas para la recogida y análisis de los datos 23
   - Estudio preliminar 23
   - Equipos afectados 24
   - Utilización de herramientas 24
   - Tipo de copia del sistema 25
10. Conclusiones 25

Capítulo II Respuesta a incidentes **27**

1. Recogida de información 27
2. Datos físicos de los ordenadores afectados 27
3. Actualizaciones de seguridad: Service Packs, parches y hotfixes 28
   - Systeminfo 29
   - PsInfo (SysInternals) 30
   - MSINFO32 30
   - Net statistics 31
   - Descubrimiento de servicios 31
   - Netstat 32
   - Tasklist 33
   - Fport (Foundstone) 34
   - Process Explorer (SysInternals) 34
   - Procesos y conexiones ocultas 36

5. DLL y verificación de firmas 38
ListDlls 38
Verificación de firmas digitales 39
SigCheck (Microsoft SysInternals) 40
6. Accesos a disco 42
Handle (SysInternals) 42
Comando DIR 42
MacMatch (FoundStone) 43
7. Captura de evidencias físicas 43
Procedimientos de adquisición 44
Captura de la memoria RAM 47
Instantáneas de volumen (Shadow Copy) 56
Recogida de las evidencias en discos físicos 62
9. Generación y montaje de imágenes para análisis offline 70
10. Conclusiones 74

Capítulo III Análisis forense de discos 75
1. Línea temporal 76
2. Indexación de la información 80
3. Diferenciación de la información basada en ficheros y firma de ficheros 82
4. Búsqueda de datos 85
5. Recuperación de ficheros eliminados 92
6. La metainformación 96
La información EXIF 97
XMP 99
Metadatos en documentos ofimáticos 100
Imágenes incrustadas 101
Imágenes borradas 102
7. Forensic FOCA 104
Análisis de datos con Forensic FOCA 105
Ejemplos de casos reales de utilización de metadatos 107
8. Conclusiones 108

Capítulo IV Análisis de evidencias 109
1. La Papelera de reciclaje. Estructura y funcionamiento 109
2. Cookies. Estructura, funcionamiento y metodología de acceso a la información 112
Limitaciones de las cookies 113
Riesgos reales de una cookie 113
Aplicación para visualizar cookies: Galleta 113
3. Index.dat y Microsoft Internet Explorer. Estructura y funcionamiento 113
Desde línea de comandos 115
Desde línea de comandos con herramientas de terceros 115

4. Auditoría de los accesos de usuario ... 117
Registro de inicios de sesión en sistemas Microsoft Windows ... 118
Netusers ... 121
PsLoggedOn ... 121
NtLast ... 122
5. Recuperación del Sistema (System Restore) ... 124
6. Registro de Microsoft Windows ... 126
Análisis del registro ... 129
Equipos ocultos ... 129
Most Recent Use & MRU ... 130
User Assist ... 131
Dispositivos USB ... 132
ARES P2P (Peer to Peer) ... 133
Autoruns ... 134
Exportación de datos ... 135
Ubicaciones físicas del registro de Windows ... 136
RegView (Mitec Software) ... 138
UserAssist ... 138
Registry File Viewer (Mitec Software) ... 139
Windows Registry Recovery (Mitec Software) ... 140
RegRipper (Parsing Registry) ... 140
7. Conclusiones ... 142

Capítulo V Ficheros temporales ... 143

1. Ficheros de impresión ... 143
Ubicación de la información de impresión ... 144
SPL (Microsoft Windows Spool File Format) ... 145
Archivos de tipo RAW ... 146
SHD (Shadow file format) ... 146
Herramientas de análisis ... 147
2. Memoria RAM ... 149
Comandos básicos WinDbg ... 152
Acceso al registro a través de WinDbg ... 155
Búsqueda de procesos ... 156
Volatility Framework ... 160
Análisis del archivo de paginación ... 163
3. Conclusiones ... 165

Capítulo VI Análisis forense de tramas de red ... 167

1. Introducción al análisis de paquetes de red ... 168
Cómo trabaja un analizador de protocolos ... 169
Captura de información ... 169
2. Análisis de correo electrónico ... 171
MIME, S/MIME y SMTP ... 172
Comandos SMTP ... 172

Protocolo extendido SMTP ... 173
Post Office Protocol e Internet Message Access Protocol ... 174
Internet Message Access Protocol (IMAP) ... 174
Análisis ... 175
3. Análisis de un escaneo de puertos (PORT SCAN) ... 179
Tipos de escaneos ... 184
4. Detección de escaneos ... 187
5. Detección de herramientas ... 188
Detección de Nessus ... 188
Detección de Nmap ... 189
6. Conclusiones ... 191

Capítulo VII Análisis forense de malware ... 193
1. Introducción ... 193
2. ¿Qué es un malware? ... 193
Tipos de malware ... 193
Vías de infección ... 194
3. Antecedentes ... 196
Preparación de un entorno de análisis ... 196
4. Tipos de análisis ... 201
Análisis estático ... 201
Análisis en base a comportamiento ... 206
Análisis dinámico ... 211
5. Análisis con VirusTotal ... 212
Múltiples motores de antivirus ... 213
Múltiples analizadores de URL ... 213
Caracterización y catalogación de muestras ... 214
Envío de muestras a VirusTotal ... 215
API pública ... 215

Capítulo VIII Reflexiones finales ... 221

Bibliografía ... 225

Índice de imágenes ... 227

Índice de tablas ... 233

Índice alfabético ... 235

Libros publicados ... 239

Productos ... 249

Servicios de Auditoría en Informática 64 ... 255

■ ■ ■