Análisis Forense Digital en Entornos Windows

Informática 64

www.informatica64.com

Juan Garrido Caballero

Juan Luis G. Rambla
Chema Alonso

Prólogo de Pedro Sánchez

Todos los nombres propios de programas, sistemas operativos, equipos hardware, etc... que aparecen en este libro son marcas registradas de sus respectivas compañias u organizaciones.

© Edición Informática64, 2009
Juan Ramón Jimenez, 8. 28932 Móstoles (Madrid)
ISBN: 978-84-613-3432-2
Printed in Spain

“A mi familia, mis amigos, mis compañeros y mi Triana”

Índice

Prólogo.....13

Capítulo I. Análisis forense e incidencias 17

1. Introducción..... 17
2. Delitos informáticos..... 20
3. Principio de Locard..... 21
4. Definición de análisis forense..... 23
5. Respuesta a incidentes..... 24
6. Incidentes más comunes..... 25
7. Evidencia digital..... 26
8. RFC 3227. Recolección y manejo de evidencias..... 27
9. Buenas prácticas para la recogida y análisis de los datos..... 30
   - Estudio preliminar..... 31
   - Equipos afectados..... 31
   - Utilización de herramientas..... 32
   - Tipo de copia del sistema..... 33
10. Conclusiones..... 34

Capítulo II. Respuesta a incidentes 35

1. Recogida de información..... 35
2. Datos físicos de los ordenadores afectados..... 35
3. Actualizaciones de seguridad: Service Packs, parches y hotfixes..... 37

■■■

Systeminfo 37
PsInfo (SysInternals) 38
MSINFO32 39

4. Procesos, puertos y servicios 40
Net statistics 40
Descubrimiento de servicios 41
Netstat 42
Tasklist 42
Fport (Foundstone) 43
Process Explorer (SysInternals) 44
Procesos y conexiones ocultas 45
5. DLL y verificación de firmas 48
ListDlls 49
Verificación de firmas digitales 49

6. Accesos a disco 53
Handle (SysInternals) 53
Comando DIR 54
MacMatch (FoundStone) 55

7. Captura de evidencias físicas 55
Procedimientos de adquisición 56

8. Recogida de evidencias 59
Captura de la memoria RAM 60
Instantáneas de volumen (Shadow Copy) 71
Recogida de las evidencias en discos físicos 78

9. Generación y montaje de imágenes para análisis offline 87

10.Conclusiones 91

Capítulo III. Análisis forense de discos 93

1. Línea temporal 94

2. Indexación de la información 99

3. Diferenciación de la información basada en ficheros y firma de ficheros 102

■ ■ ■

4. Búsqueda de datos 106

5. Recuperación de ficheros eliminados 114

6. La metainformación 120
La información EXIF 120
XMP 123
Metadatos en documentos ofimáticos 124
Imágenes incrustadas 126
Imágenes borradas 126

7. Conclusiones 129

Capítulo IV. Análisis de evidencias 131

1. La Papelera de reciclaje. Estructura y funcionamiento 131

2. Cookies 135
Limitaciones de las cookies 136
Riesgos reales de una cookie 136
Aplicación para visualizar cookies: Galleta 137

3. Index.dat y Microsoft Internet Explorer. Estructura y funcionamiento 137
Desde línea de comandos 139
Desde línea de comandos con herramientas de terceros 140

4. Auditoría de los accesos de usuario 141
Registro de inicios de sesión en sistemas Microsoft Windows 144
Netusers 147
PsLoggedOn 147
NtLast 148

5. Recuperación del Sistema (System Restore) 151

6. Registro de Microsoft Windows 154
Análisis del registro 157
Equipos ocultos 158
Most Recent Use & MRU 159
User Assist 161
Dispositivos USB 161
ARES P2P (Peer to Peer) 163

Autoruns 164
Exportación de datos 166
Ubicaciones físicas del registro de Microsoft Windows 167
RegView (Mitec Software) 169
UserAssist 170
Registry File Viewer (Mitec Software) 171
Windows Registry Recovery (Mitec Software) 171
RegRipper (Parsing Registry) 172

7. Conclusiones 174

Capítulo V. Ficheros temporales 175

1. Ficheros de impresión 175
Ubicación de la información de impresión 176
SPL (Microsoft Windows Spool File Format) 178
Archivos de tipo RAW 179
SHD (Shadow file format) 180
Herramientas de análisis 181

2. Memoria RAM 182
Comandos básicos WinDbg 186
Búsqueda de procesos 191
Volatility Framework 196
Análisis del archivo de paginación 200

3. Conclusiones 203

Capítulo VI. Reflexiones finales 205

Bibliografía 209

Índice de imágenes 213

Índice de tablas 216

Glosario 217

■ ■ ■