

Índice

Prólogo a la Silver Edition	13
Introducción	
Fear the FOCA!.....	15
Capítulo I	
FOCA Open Source	19
1. Diferencias entre FOCA Pro y FOCA Open Source	20
Arquitectura FOCA Open Source	21
2. Descarga e instalación de FOCA Open Source	22
3. Ámbito de uso de la herramienta	24
4. Github de FOCA Open Source	24
5. FOCA Versión 3.4.6.X.....	27
6. FOCA Versión 3.4.7 y la integración con DIARIO	30
Capítulo II	
Los metadatos.....	25
1. Metadatos, información oculta y datos perdidos.....	26
2. Metadatos en documentos ofimáticos	28
Metadatos en Microsoft Office.....	28
Datos del usuario	28
Propiedades del documento	29
Ficheros incrustados	30
Desvinculado de ficheros gráficos incrustados	32
Revisiones y modificaciones.....	33
Notas, encabezados y pies de páginas	33
Información oculta por formato.....	34
Otros lugares donde se almacena la información	34

Información oculta.....	35
Conexiones a bases de datos.....	35
Impresoras.....	36
Metadatos en OpenOffice.....	38
Datos personales.....	39
Impresoras.....	40
Plantillas.....	40
Documentos vinculados e incrustados.....	42
Modificaciones.....	44
Párrafos ocultos.....	45
Notas, Encabezados, Pies, Comentarios.....	46
Metadatos personalizados.....	46
Bases de datos.....	47
Versiones de documentos.....	48
Metadatos en Apple iWork.....	49
El fichero BuildVersionHistory.plist.....	50
Vista previa en la carpeta QuickLook: Preview.PDF y Thumbnail.jpg.....	51
Carpeta thumbs y archivos incrustados.....	52
El perfil de color y los documentos gráficos.....	52
Archivos con extensión chrtshr.....	53
Los archivos maestros: Index.XML e Index.apxl.....	53
Objeto Metadata.....	54
Información Oculta.....	55
Rutas locales en atributos path.....	55
Versiones y fechas del documento.....	55
Información de impresoras.....	56
Versión del sistema operativo.....	56
Control de Cambios.....	56
Las pistas en los documentos Apple iWork.....	57
Metadatos en otros archivos de MS Office.....	58
Archivos de autorecuperación.....	58
Otros formatos de documentos en Microsoft Excel.....	59
Metadatos en formatos Postscript y PDF.....	61
(XML) Forms Data Format.....	62

Capítulo III

Análisis y limpieza de metadatos.....65

1. Análisis de metadatos con FOCA..... 65

Metadatos como parte de una investigación forense.....	70
El informe Blair.....	70
Localización de un defacer.....	71
Seguimiento de movimientos.....	73

Piratería de software	74
2. Information gathering con FOCA.....	75
Preparando un ataque dirigido con FOCA	82
3. Riesgos asociados a una mala gestión de los metadatos.....	86
Creepy	86
Stolen Camara Finder.....	88
Flame y los metadatos	89
Esquema Nacional de Seguridad.....	90
Limpieza de documentos	90
4. Eliminación de metadatos	91
Eliminación de metadatos de forma manual	91
Documentos Microsoft Office	91
Microsoft Office para Mac.....	92
Documentos OpenOffice	93
Eliminación de metadatos en imágenes	95
Eliminación de metadatos de forma automática	96
MetaShield Protector	96
MetaShield Protector for IIS y MetaShield Protector for SharePoint	97
MetaShield Protector for Client.....	101
MetaShield Analyzer	102
Manipulando metadatos para engañar a la FOCA.....	102
Fuga de información en empresas líderes en Data Loss Prevention.....	104
FOCA Core.....	107
Core: Detección y análisis de Metadatos	107

Capítulo IV

Descubrimiento de la red..... 111

1. Opciones de descubrimiento de red	112
WebSearcher: Localización de URLs en buscadores de Internet	112
DNS.....	113
Análisis del DNS con Diccionario y Transferencias de Zona	116
DNS Prediction	121
Bing IP.....	122
PTR Scanning.....	123
Shodan	125
Descubrimiento de la red mediante agentes SNMP.....	127
Certificados digitales.....	129
Google Slash Trick.....	132
Core: Creación mapa dominios y configuración.....	134
2. Opciones de fingerprinting	136

Fingerprinting con banners y mensajes de error.....	136
Fingerprinting de versiones en servidores DNS	137
Configuración de opciones de fingerprinting.....	138
3. Vista de red y de roles	139
Conclusiones finales del Network Discovery	140

Capítulo V

Búsqueda de vulnerabilidades143

1. Tipos de vulnerabilidades analizadas por FOCA.....	143
Backups.....	143
Listado de directorios.....	144
Búsqueda de malware y BlackSEO con patrones de Directory Listing	145
DNS Cache Snooping	146
Escenarios de ataque aprovechando DNS Cache Snooping	149
Ficheros .DS_Store	151
Métodos HTTP inseguros.....	153
Subida de WebShells con métodos PUT.....	155
Hijacking de cookies HTTP-Only con XSS usando TRACE.....	157
Juicy files.....	159
Ficheros .listing.....	160
Multiple Choices: mod_negotiation.....	162
Ficheros .svn/entries de repositorios Subversion	163
Descarga de ficheros con Pristine y wc.db en repositorios Subversion.....	164
Búsqueda de servidores Proxy	166
Data Leaks: Fugas de información.....	167
Generación de Errores y Data Leaks en las URLs parametrizadas	168
IIS URL Short name	170
Directorios de usuarios.....	171
2. El algoritmo paso a paso.....	172
3. Un ejemplo con FOCA.....	174

Capítulo VI

Plugins, informes y otros trucos177

1. Funciones avanzadas de FOCA.....	178
Cómo ha localizado FOCA la información.....	178
Búsqueda personalizada.....	179
Obtención de URLs en Dominios muy grandes.....	180
Personalizar el valor del User-agent de FOCA	181
Monitorización de FOCA: Tareas y Logs	183

2. Integración de FOCA con otras herramientas.....	185
Uso de FOCA con herramientas de Spidering	185
FOCA Intruder: FOCA + Burp Suite + Intruder	187
Malware vía actualizaciones: FOCA + Evilgrade.....	189
Ataques Spear Phising: FOCA + Metasploit.....	191
URLs desde el pasado: FOCA + Archive.org.....	193
3. Plugins en FOCA.....	195
Plugin SVN Downloader.....	196
Plugin IIS Shortname	197
Plugin SQLi	198
4. Gestor de informes	201
FOCA Online y Metashield Clean-up	203
5. Más trucos con FOCA.....	204
 Capítulo VII	
Cómo crear plugins para FOCA	207
1. Creación de un plugin básico	207
Creación inicial del plugin e Integración de la API de FOCA.....	208
Desarrollo de la funcionalidad del plugin	210
2. GUI del plugin	211
Capturar eventos	214
Importar elementos desde el plugin a la FOCA	216
Final.....	220
Índice alfabético	221
Índice de imágenes	223