Índice

Introducción:
Fear the FOCA!.....11

Capítulo I.
Los metadatos.....15

1. Metadatos, información oculta y datos perdidos.....16

2. Metadatos en documentos ofimáticos.....18

Metadatos en Microsoft Office.....18
Datos del usuario.....19
Propiedades del documento.....20
Ficheros incrustados.....20
Desvinculado de ficheros gráficos incrustados.....22
Revisiones y modificaciones.....23
Notas, Encabezados y Pies de páginas.....23
Información oculta por formato.....24
Otros lugares donde se almacena la información.....24
Información oculta.....25
Conexiones a bases de datos.....25
Impresoras.....26
Metadatos en OpenOffice.....28
Datos personales.....29
Impresoras.....30
Plantillas.....31
Documentos vinculados e incrustados.....32
Modificaciones.....34
Párrafos ocultos.....35
Notas, Encabezados, Pies, Comentarios.....36
Metadatos personalizados.....36
Bases de datos.....37
Versiones de documentos.....38
Metadatos en Apple iWork.....39

El fichero BuildVersionHistory.plist 40
Vista previa en la carpeta QuickLook: Preview.PDF y Thumbnail.jpg 41
Carpeta thumbs y archivos incrustados 42
El perfil de color y los documentos gráficos 42
Archivos con extensión chrtshr 43
Los archivos maestros: Index.XML e Index.apxl 43
Objeto Medatada 44
Información Oculta 45
Rutas locales en atributos path 45
Versiones y fechas del documento 45
Información de impresoras 46
Versión del sistema operativo 46
Control de Cambios 47
Las pistas en los documentos Apple iWork 47
Metadatos en otros archivos de MS Office 48
Archivos de autorecuperación 48
Otros formatos de documentos en Microsoft Excel 49
Metadatos en formatos Postscript y PDF 51
(XML) Forms Data Format 52

Capítulo II.
Análisis y limpieza de metadatos 55

1. Análisis de metadatos con FOCA 55
Metadatos como parte de una investigación forense 60
El informe Blair 60
Localización de un defacer 61
Seguimiento de movimientos 63
Piratería de software 65

2. Information gathering con FOCA 66

3. Riesgos asociados a una mala gestión de los metadatos 78
Creepy 79
Stolen Camara Finder 80
Flame y los metadatos 81
Esquema Nacional de Seguridad 82
Limpieza de documentos 82

4. Eliminación de metadatos 83
Eliminación de metadatos de forma manual 83
Documentos Microsoft Office 83
Microsoft Office para Mac 84
Documentos OpenOffice 85
Eliminación de metadatos en imágenes 87

Eliminación de metadatos de forma automática 88
MetaShield Protector 88
MetaShield Protector for IIS y MetaShield Protector for SharePoint 89
MetaShield Protector for Client 94
Manipulando metadatos para engañar a la FOCA 95
Fuga de información en empresas líderes en Data Loss Prevention 97

Capítulo III
Descubrimiento de la red 101

1. Opciones de descubrimiento de red 102
WebSearcher: Localización de URLs en buscadores de Internet 102
DNS 104
Análisis del DNS con Diccionario y Transferencias de Zona 106
DNS Prediction 111
Bing IP 112
PTR Scanning 113
Shodan 115
Descubrimiento de la red mediante angentes SNMP 117
Robtex 119
Certificados digitales 121
Google Slash Trick 124

2. Opciones de fingerprinting 125
Fingerprinting con banners y mensajes de error 126
Fingerprinting de versiones en servidores DNS 127
Configuración de opciones de fingerprinting 128

3. Vista de red y de roles 129
Conclusiones finales del Network Discovery 132

Capítulo IV
Búsqueda de Vulnerabilidades 133

1. Tipos de vulnerabilidades analizadas por FOCA 133
Backups 133
Listado de directorios 135
Búsqueda de malware y BlackSEO con patrones de Directory Listing 136
DNS Cache Snooping 137
Escenarios de ataque aprovechando DNS Cache Snooping 140
Ficheros .DS_Store 142
Bug PHP CGI Code Execution 144
Métodos HTTP inseguros 146
Subida de WebShells con métodos PUT 148

Hijacking de cookies HTTP-Only con XSS usando TRACE 150
Juicy files 152
Ficheros .listing 154
Multiple Choices: mod_negotiation 156
Ficheros .svn/entries de repositorios Subversion 157
Descarga de ficheros con Pistine y wc.db en repositorios Subversion 158
Búsqueda de servidores Proxy 160
Data Leaks: Fugas de información 161
Generación de Errores y Data Leaks en las URLs parametrizadas 162
IIS Url Short name 164
Directorios de usuarios 165

2. El algoritmo paso a paso 166

3. Un ejemplo con FOCA 168

Capítulo V.
Plugins, informes y otros trucos. 173

1. Funciones avanzadas de FOCA 174
Cómo ha localizado FOCA la información 174
Búsqueda personalizada 175
Obtención de URLs en Dominios muy grandes 176
Personalizar el valor del User-agent de FOCA 177
Monitorización de FOCA: Tareas y Logs 179

2. Integración de FOCA con otras herramientas 181
Uso de FOCA con herramientas de Spidering 181
FOCA Intruder: FOCA + Burp Suite + Intruder 183
Malware vía actualizaciones: FOCA + Evilgrade 186
Ataques Spear Phising: FOCA + Metasploit 188
URLs desde el pasado: FOCA + Archive.org 190

3. Plugins en FOCA 192
Plugin .svn/entries parser 193
Plugin Web Fuzzer 194
Plugin IIS Shortname Extractor 195
NTFS Based Server Enumerator 196
Plugin Auto SQLi searcher 199

4. Gestor de informes 202
FOCA Online 205

5. Más trucos con FOCA 206

Capítulo VI
Cómo crear plugins para FOCA 209

1. Creación de un plugin básico 209
Creación del proyecto para el plugin en Visual Studio 210
Creación inicial del plugin e Integración de la API de FOCA 211
Desarollo de la funcionalidad del plugin 212

2. GUI del plugin 214
Capturar eventos 217
Importar elementos desde el plugin a la FOCA 219

3. Final 223

Índice alfabético 225

Libros publicados 228