

# Pentesting con FOCA

Chema Alonso

con la colaboración de :  
Pablo González, Ioseba Palop,  
Enrique Rando, Rubén Alonso,  
Jesús Moreno y Manuel Fernández

Más de 3000 ejemplares vendidos

FEAR THE



**0xWORD**

# **Pentesting con FOCA**

**ZeroXword Computing**

**[www.0xword.com](http://www.0xword.com)**

**Chema Alonso**

**con la colaboración de:**

**Pablo González, Ioseba Palop,**

**Enrique Rando, Rubén Alonso,**

**Jesús Moreno y Manuel Fernández**

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

Reservados todos los derechos. El contenido de esta obra está protegido por la ley, que establece penas de prisión y/o multas, además de las correspondientes indemnizaciones por daños y perjuicios, para quienes reprodujesen, plagiaran, distribuyeren o comunicasen públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la preceptiva autorización.

© Reimpresión ZeroxWord Computing S.L. 2016.

© Reimpresión ZeroxWord Computing S.L. 2015.

© Edición ZeroxWord Computing S.L. 2013.

Juan Ramón Jiménez, 8. 28932 Móstoles (Madrid).

Depósito legal: M-35705-2013

ISBN: 978-84-616-6319-4

Printed in Spain

Proyecto gestionado por Eventos Creativos: <http://www.eventos-creativos.com>

# Índice

<b>Introducción:</b>	
<b>Fear the FOCA!</b> .....	<b>13</b>
<b>Capítulo I</b>	
<b>Los metadatos</b> .....	<b>17</b>
<b>1. Metadatos, información oculta y datos perdidos</b> .....	<b>18</b>
<b>2. Metadatos en documentos ofimáticos</b> .....	<b>20</b>
Metadatos en Microsoft Office.....	20
Datos del usuario .....	20
Propiedades del documento .....	21
Ficheros incrustados .....	22
Desvinculado de ficheros gráficos incrustados .....	24
Revisiones y modificaciones.....	25
Notas, Encabezados y Pies de páginas .....	26
Información oculta por formato.....	26
Otros lugares donde se almacena la información .....	26
Información oculta.....	27
Conexiones a bases de datos.....	27
Impresoras.....	28
Metadatos en OpenOffice.....	30
Datos personales .....	31
Impresoras.....	32
Plantillas .....	32
Documentos vinculados e incrustados.....	34
Modificaciones.....	36
Párrafos ocultos .....	37
Notas, Encabezados, Pies, Comentarios.....	38
Metadatos personalizados .....	38
Bases de datos.....	39
Versiones de documentos.....	40
Metadatos en Apple iWork.....	41



El fichero BuildVersionHistory.plist.....	42
Vista previa en la carpeta QuickLook: Preview.PDF y Thumbnail.jpg.....	43
Carpeta thumbs y archivos incrustados .....	44
El perfil de color y los documentos gráficos.....	44
Archivos con extensión chrtshr .....	45
Los archivos maestros: Index.XML e Index.apxl.....	45
Objeto Metadata.....	46
Información Oculta.....	47
Rutas locales en atributos path .....	47
Versiones y fechas del documento.....	47
Información de impresoras .....	48
Versión del sistema operativo .....	48
Control de Cambios .....	48
Las pistas en los documentos Apple iWork.....	49
Metadatos en otros archivos de MS Office .....	50
Archivos de autorecuperación .....	50
Otros formatos de documentos en Microsoft Excel .....	51
Metadatos en formatos Postscript y PDF .....	53
(XML) Forms Data Format .....	54

## Capítulo II

### **Análisis y limpieza de Metadatos.....57**

<b>1. Análisis de metadatos con FOCA.....</b>	<b>57</b>
Metadatos como parte de una investigación forense.....	62
El informe Blair .....	62
Localización de un defacer .....	63
Seguimiento de movimientos .....	65
Piratería de software .....	67
<b>2. Information gathering con FOCA.....</b>	<b>68</b>
<b>3. Riesgos asociados a una mala gestión de los metadatos.....</b>	<b>80</b>
Creepy .....	81
Stolen Camara Finder.....	82
Flame y los metadatos.....	83
Esquema Nacional de Seguridad.....	84
Limpieza de documentos .....	84
<b>4. Eliminación de metadatos .....</b>	<b>85</b>
Eliminación de metadatos de forma manual .....	85
Documentos Microsoft Office .....	85
Microsoft Office para Mac.....	86
Documentos OpenOffice .....	87
Eliminación de metadatos en imágenes .....	89

