



# TÉCNICAS OSINT

## INFORME

C.E.S ACADEMIA LOPE DE VEGA

CFGS: 2º Administración de Sistemas Informáticos en Red

Curso: 2017/2018

Asignatura: Seguridad y Alta Disponibilidad

Prof. Miguel Angel González

Autor: Rafael Osuna Ventura

## 1. ¿QUÉ SON LAS TÉCNICAS OSINT?

Open Source Intelligence (OSINT), que se traduce en inteligencia con fuentes abiertas. El concepto se refiere a la recolección de información de una persona o empresa utilizando fuentes de acceso público como internet, redes sociales, buscadores, foros, fotografías, wikis, bibliotecas online, conferencias, metadatos, etc.

Existe una gran variedad de herramientas para la adquisición, procesamiento y análisis de la información. La recopilación de datos e información a gran escala, el análisis y visualización conllevan el uso de distintas herramientas, algunas libres y otras con versiones pago, que son usadas dependiendo de la necesidad y de la forma en la que se quieran utilizar los datos.

## 2. INFORME DE UNA PÁGINA UTILIZANDO OSINT

Para esta práctica he elegido la página web del ayuntamiento de mi pueblo [www.espejo.es](http://www.espejo.es).

Lo primero que he hecho ha sido buscar metadatos, para ello, he usado varias herramientas tanto online como de forma local (FOCA, Jeffrey, extractmetadata....). De las herramientas que he probado solo me ha aparecido información relevante en FOCA.

ayuntamiento espejo - FOCA (final version) 3.4

Project Report Tools Options TaskList Plugins About

PC\_teresa casado trenas  
PC\_UNIDAD INST DIURNA  
PC\_usuario  
PC\_usuario9  
Servers (1)  
195.57.20.0  
Unlocated Servers  
espejo.es

Domains  
Roles  
Vulnerabilities  
Metadata  
Documents (62/62)  
pdf (55)  
Unknown (7)  
Metadata Summary  
Users (13)  
Folders (0)  
Printers (0)  
Software (17)  
Emails (0)  
Operating Systems (0)  
Passwords (0)  
Servers (0)

FOCA

Search engines  
☒ Google  
☒ Bing  
☐ Exalead  
All None

Extensions  
☒ doc ☒ xls ☒ pptx ☒ sxc  
☒ ppt ☒ docx ☒xlsx ☒ sxi  
☐ pps ☐ pptx ☐ sxw ☐ odt

Custom search

Id	Type	URL	Download	Download Date	Size	Anali
0	df	https://www.espejo.es/contratacion/archivos/perfilcontr...	●	09/01/2018 14:03:59	1,22 MB	●
1	pdf	http://www.espejo.es/sites/default/files/pleno_extraordi...	●	09/01/2018 14:03:55	177,76 KB	●
2	pdf	http://www.espejo.es/sites/default/files/ordenanza_ca...	●	09/01/2018 14:03:56	675,98 KB	●
3	df	https://www.espejo.es/contratacion/archivos/perfilcontr...	●	09/01/2018 14:04:00	393,33 KB	●
4	pdf	http://www.espejo.es/sites/default/files/ordenanza_trafi...	●	09/01/2018 14:03:56	161,79 KB	●
5	pdf	http://www.espejo.es/sites/default/files/animales_peligr...	●	09/01/2018 14:03:59	595,48 KB	●
6	df	https://www.espejo.es/contratacion/archivos/perfilcontr...	●	09/01/2018 14:04:01	613,21 KB	●
7	pdf	http://www.espejo.es/sites/default/files/ordenanzadomi...	●	09/01/2018 14:04:01	211,44 KB	●
8	pdf	http://www.espejo.es/sites/default/files/modificacion_or...	●	09/01/2018 14:04:01	254,57 KB	●
9	pdf	http://www.espejo.es/sites/default/files/cuadro_infracci...	●	09/01/2018 14:04:02	234,64 KB	●
10	pdf	http://www.espejo.es/sites/default/files/reglamento_de...	●	09/01/2018 14:04:03	631,72 KB	●
11	df	https://www.espejo.es/contratacion/archivos/perfilcontr...	●	09/01/2018 14:04:02	39,81 KB	●

Time	Source	Severity	Message
8:11:42	MetadataSearch	low	Document metadata extracted: C:\Users\rafao\AppData\Local\Temp\dptico_bases_de_participacio...
8:11:42	MetadataSearch	low	Document metadata extracted: C:\Users\rafao\AppData\Local\Temp\propuestaformacion-empleo.pdf
8:11:43	MetadataSearch	low	Document metadata extracted: C:\Users\rafao\AppData\Local\Temp\proyecto_reto_solidario_aira_s...
8:11:43	MetadataSearch	low	Document metadata extracted: C:\Users\rafao\AppData\Local\Temp\cortes_de_suministro.pdf
8:11:46	MetadataSearch	low	Document metadata extracted: C:\Users\rafao\AppData\Local\Temp\libro_ordenanzas_fiscales_20...
8:11:52	MetadataSearch	low	Document metadata extracted: C:\Users\rafao\AppData\Local\Temp\mejora_travesia.pdf

Conf Deactivate AutoScroll Clear Save log to File

Metadata analyzed!

Attribute	Value	Attribute	Value
All software found (17) - Times found		All users found (13) - Times found	
RICOH MP C2011	6	usuario	2
Microsoft Office XP	12	teresa casado trenas	1
Microsoft Office	4	UNIDAD INST DIURNA	5
GPL Ghostscript 8.61	5	Antonio Moral	1
PDFCreator 0.9.5 Windows XP	5	Secretaria	6
Microsoft? Publisher 2010	1	Policia	1
Acrobat Distillier 7.0	1	usuario9	1
PScript5.dll Version 5.2.2	5	Antonio Miguel Admin	1
iText 2.1.7 by 1T3XT	1	irc125	2
GPL Ghostscript 9.07	6	jbn01	4
PDFCreator 1.7.1 Windows XP	2	ANONIMOUS	1
FREE PDFfill PDF and Image Writer	4	pc14	1
Microsoft Office 2007	2	Coordinadora Web	1
www.ilovepdf.com	1		
KMBT_C220	2		
KONICA MINOLTA bizhub C220	2		
Microsoft? Publisher 2013	1		

Los metadatos que he obtenido han sido números pdf con información sobre actividades que se han realizado en el pueblo, actas de reuniones tanto del equipo directivo actual como de años anteriores. También aparecen los diferentes usuarios que hay en la gestión del ayuntamiento, así como los sistemas operativos y el software que utilizan.

A partir de toda esta información he sacado en claro que el ayuntamiento utiliza sistemas operativos y programas bastante desactualizados y antiguos como Windows XP y office 2007. También mirando en los documentos extraídos he podido encontrar los nombres de todo el cuerpo administrativo del ayuntamiento tanto del actual como el formado en otras legislaturas.

Tras esto he pasado a buscar en las redes sociales alguno de los nombres que he obtenido, por ejemplo, el del alcalde. Este tiene solamente Facebook, pero en él no tiene puesta mucha información, lo único relevante sería que tiene indicadas las algunas relaciones familiares.

La localización la he obtenido también a partir de los documentos obtenidos a través de foca ya que con otras herramientas no nos localización la ubicación.

La siguiente herramienta que he utilizado ha sido TheHarvester. Esta herramienta no me ha encontrado información sobre la página.

```
root@kali:~# theharvester -d espejo.es -l 500 -b google

*****
*
*  TheHarvester
*
*  TheHarvester Ver. 2.7
*  Coded by Christian Martorella
*  Edge-Security Research
*  cmartorella@edge-security.com
*
*****

[-] Searching in Google:
    Searching 0 results...
    Searching 100 results...
    Searching 200 results...
    Searching 300 results...
    Searching 400 results...
    Searching 500 results...

[+] Emails found:
-----
No emails found

[+] Hosts found in search engines:
-----
No hosts found
```

Lo siguiente ha sido buscar información sobre el dominio, para ello he probado diferentes paginas como por ejemplo who.is, dondominio.com.... pero no me proporcionaban ninguna información o no encontraban el dominio. Al final encontré la página nic.es , esta pertenece al gobierno.



DATOS DEL TITULAR	
Nombre del Dominio	espejo.es
Estado	Activado
Identificador	ADE230-ESNIC-F4
Titular	Ayuntamiento de Espejo
Fecha de Alta	17-06-2009
Fecha de Caducidad	17-06-2018
Agente Registrador	TECNOCRATICA
PERSONA DE CONTACTO ADMINISTRATIVO	
Identificador	FAMR19-ESNIC-F4
Nombre	Francisco Antonio Medina Raso
Email	administracion@eprinsa.es
PERSONA DE CONTACTO TECNICO	
Identificador	FAMR19-ESNIC-F4
Nombre	Francisco Antonio Medina Raso
Email	administracion@eprinsa.es
SERVIDORES DNS	
Nombre Servidor	IP
proxy.eprinsa.es	195.57.20.7
proxy2.eprinsa.es	194.224.112.2



Destacamos como información relevante que la fecha de caducidad es en 5 meses, que el titular administrativo es Francisco Antonio Medina Raso, este fue alcalde en la anterior legislatura y aún sigue puesto como titular. El proveedor es Tecnocratica y la asistencia la ofrece Eprinsa.

También aparece un correo electrónico, este al comprobar si ha tenido alguna vulnerabilidad en la página [www.haveibeenpwned.com](http://www.haveibeenpwned.com) nos aparece que ha tenido una en Adobe.

### Oh no — pwned!


Pwned on 1 [breached site](#) and found no [pastes](#) ([subscribe](#) to search sensitive breaches)

 [Notify me when I get pwned](#)  [Donate](#)

### Breaches you were pwned in

A "breach" is an incident where a site's data has been illegally accessed by hackers and then released publicly. Review the types of data that were compromised (email addresses, passwords, credit cards etc.) and take appropriate action, such as changing passwords.



**Adobe:** In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

**Compromised data:** Email addresses, Password hints, Passwords, Usernames

Rafael Osuna Ventura  
2ºASIR

La página utiliza un protocolo http esto se debería de cambiar por un protocolo https ya que de esta forma la conexión cliente servidor se realiza de forma segura. En la página hay una sección de administración virtual, este si cuenta con https.