

# Práctica 1.3 A. Footprinting

Athos Orío Choperena

15/10/2017

## Contenido

¿Qué es footprinting? .....	2
Whois .....	2
Maltego .....	5
Theharvestest.....	12
La foca: .....	15
Robots.txt y sitemap.xml.....	17
Robots.txt .....	18
Sitemap.xml.....	18
La web .....	19
Fingerprinting:.....	20
Nmap .....	20
Nessus .....	22
Dnsenum .....	23
Whatweb.....	24
Wafw00f.....	24
wpscan.....	25
Detección del sistema operativo:.....	26

## ¿Qué es footprinting?

El término footprinting en ambiente de informática, se refiere a la recolección de información de una red específica, que normalmente se usa para la búsqueda de fallos en la red. Esta búsqueda de información se hace en bases de datos públicas, buscadores etc, es decir, sin la interacción directa con la red de la que queremos buscar información. Para realizar esta búsqueda de información existen diferentes técnicas y programas, las cuales explicaremos, detallaremos y haremos una prueba de concepto con cada una de ellas. Esto no quiere decir que no existan más programas o técnicas para realizarlo.

Repito, esta información se hace sin interactuar directamente con el usuario. Si lo hiciésemos, estaríamos haciendo fingerprinting, y podría ser ilegal si no disponemos del consentimiento explícito del objetivo. Este consentimiento, debería ser por escrito si queremos evitarnos problemas.

La búsqueda de información la vamos a realizar sobre el dominio proyecto.online.

La primera utilidad que vamos a utilizar es el whois, lo realizaremos a través de diferentes herramientas, el comando whois de consola de comandos y utilidades online que hay en la web, y compararemos los resultados.

### Whois

Línea de comandos:

```
root@athos:~# whois proyecto.online
Domain Name: PROYECTO.ONLINE
Registry Domain ID: D13806421-CNIC
Registrar WHOIS Server: whois.scip.es
Registrar URL:
Updated Date: 2017-07-09T07:42:22.0Z
Creation Date: 2015-12-12T17:43:47.0Z
Registry Expiry Date: 2018-12-12T23:59:59.0Z
Registrar: Soluciones Corporativas IP, S.L.U.
Registrar IANA ID: 1383
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: C138460181-CNIC
Registrant Name: Whois Privacy Service Protects this domain
Registrant Organization: Only contact by email, all postal mail will be rejected
Registrant Street: Ronda Institut, 24
Registrant City: Manacor
Registrant State/Province: Illes Balears
Registrant Postal Code: 07500
Registrant Country: ES
Registrant Phone: +34.871987733
Registrant Fax: +34.871986601
Registrant Email: proyecto.online@whoisprivacycontact.com
Registry Admin ID: C138460184-CNIC
Admin Name: Whois Privacy Service Protects this domain
Admin Organization: Only contact by email, all postal mail will be rejected
Admin Street: Ronda Institut, 24
Admin City: Manacor
Admin State/Province: Illes Balears
Admin Postal Code: 07500
Admin Country: ES
Admin Phone: +34.871987733
Admin Fax: +34.871986601
Admin Email: proyecto.online@whoisprivacycontact.com
Registry Tech ID: C138460193-CNIC
Tech Name: Whois Privacy Service Protects this domain
Tech Organization: Only contact by email, all postal mail will be rejected
Tech Street: Ronda Institut, 24
Tech City: Manacor
Tech State/Province: Illes Balears
Tech Postal Code: 07500
Tech Country: ES
Tech Phone: +34.871987733
Tech Fax: +34.871986601
```

```
Tech Email: proyecto.online@whoisprivacycontact.com
Name Server: NS2.PROYECTO.ONLINE
Name Server: NS1.PROYECTO.ONLINE
DNSSEC: unsigned
Registry Billing ID: C138460202-CNIC
Billing Name: Whois Privacy Service Protects this domain
Billing Organization: Only contact by email, all postal mail will be rejected
Billing Street: Ronda Institut, 24
Billing City: Manacor
Billing State/Province: Illes Balears
Billing Postal Code: 07500
Billing Country: ES
Billing Phone: +34.871987733
Billing Fax: +34.871986601
Billing Email: proyecto.online@whoisprivacycontact.com
Registrar Abuse Contact Email: info@scip.es
Registrar Abuse Contact Phone: +34.871986600
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2017-10-15T11:28:16.0Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

This whois service is provided by CentralNic Ltd and only contains
information pertaining to Internet domain names registered by our
our customers. By using this service you are agreeing (1) not to use any
information presented here for any purpose other than determining
ownership of domain names, (2) not to store or reproduce this data in
any way, (3) not to use any high-volume, automated, electronic processes
to obtain data from this service. Abuse of this service is monitored and
actions in contravention of these terms will result in being permanently
blacklisted. All data is (c) CentralNic Ltd https://www.centralnic.com/

Access to the whois service is rate limited. For more information, please
see https://registrar-console.centralnic.com/pub/whois_guidance.
```

Como podemos ver con este simple comando “whois proyecto.online” podemos sacar gran cantidad de información. Voy a ir detallando la información importante (que he ido marcando con líneas rojas) en orden de aparición.

Por un lado, podemos ver la fecha de creación del dominio así como la fecha de expiración, este es un dato importante ya que podríamos estar pendientes de la fecha de expiración y podríamos comprar el dominio si los dueños de este tienen un descuido. Si es un dominio con antigüedad, podría ser algo muy beneficioso desde el punto de vista del atacante.

Podemos ver también, el nombre fiscal de la empresa que compro el dominio, y el id del agente registrador, así como un teléfono, un fax y una dirección de correo. ¿Quién sabe, puede que nos pueda servir para hacer ingeniería social? ¿O mandarle un correo infectado?

También podemos ver cuáles son los servidores dns que tiene el dominio en el registro SOA, y posteriormente podríamos mirar si el servidor dns está mal configurado y podríamos hacer una transferencia de zona, y así conocer todas las maquinas que están relacionadas con el dominio.

Utilizando la herramienta online viewdns.info, en la sección de whois introducimos el dominio.

The screenshot shows the ViewDNS.info website interface. At the top, there's a navigation bar with 'Tools', 'API', 'Research', and 'Data' tabs. Below this, there's a grid of 18 tool cards. The 'Domain / IP Whois' tool is highlighted with a red border. It contains a text input field with 'proyecto.online' and a 'GO' button. Other tools include Reverse IP Lookup, Reverse Whois Lookup, IP History, DNS Report, Reverse MX Lookup, Reverse NS Lookup, IP Location Finder, Chinese Firewall Test, DNS Propagation Checker, Is My Site Down, Iran Firewall Test, Get HTTP Headers, DNS Record Lookup, Port Scanner, Traceroute, Spam Database Lookup, and Reverse DNS Lookup. Each tool has a brief description and a 'GO' button.

Tools	API	Research	Data
<b>Reverse IP Lookup</b> Find all sites hosted on a given server. Domain / IP GO	<b>Reverse Whois Lookup</b> Find domain names owned by an individual or company. Registrant Name or Email Address GO	<b>IP History</b> Show historical IP addresses for a domain. Domain (e.g. domain.com) GO	
<b>DNS Report</b> Provides a complete report on your DNS settings. Domain (e.g. domain.com) GO	<b>Reverse MX Lookup [NEW]</b> Find all sites that use a given mail server. Mail server (e.g. mail.google.com) GO	<b>Reverse NS Lookup</b> Find all sites that use a given nameserver. Nameserver (e.g. ns1.example.com) GO	
<b>IP Location Finder</b> Find the geographic location of an IP Address. IP GO	<b>Chinese Firewall Test</b> Checks whether a site is accessible from China. URL / Domain GO	<b>DNS Propagation Checker</b> Check whether recent DNS changes have propagated. Domain (e.g. domain.com) GO	
<b>Is My Site Down</b> Check whether a site is actually down or not. Domain (e.g. domain.com) GO	<b>Iran Firewall Test</b> Check whether a site is accessible in Iran. Site URL / Domain GO	<b>Domain / IP Whois</b> Lookup information on a Domain or IP address. Domain / IP proyecto.online GO	
<b>Get HTTP Headers</b> View the HTTP headers returned by a domain. Domain GO	<b>DNS Record Lookup</b> View all DNS records for a specified domain. Domain (e.g. domain.com) GO	<b>Port Scanner</b> Check if common ports are open on a server. Domain / IP GO	
<b>Traceroute</b> Trace the servers between ViewDNS and a remote host. Domain / IP GO	<b>Spam Database Lookup</b> Determine if your mail server is on any spam lists. IP GO	<b>Reverse DNS Lookup</b> View the reverse DNS entry for an IP address. IP GO	

No voy a poner el resultado ya que lo he cotejado y tenemos la misma información, pero dejo el enlace por si se quiere comprobar.

<http://viewdns.info/whois/?domain=proyecto.online>

## Maltego

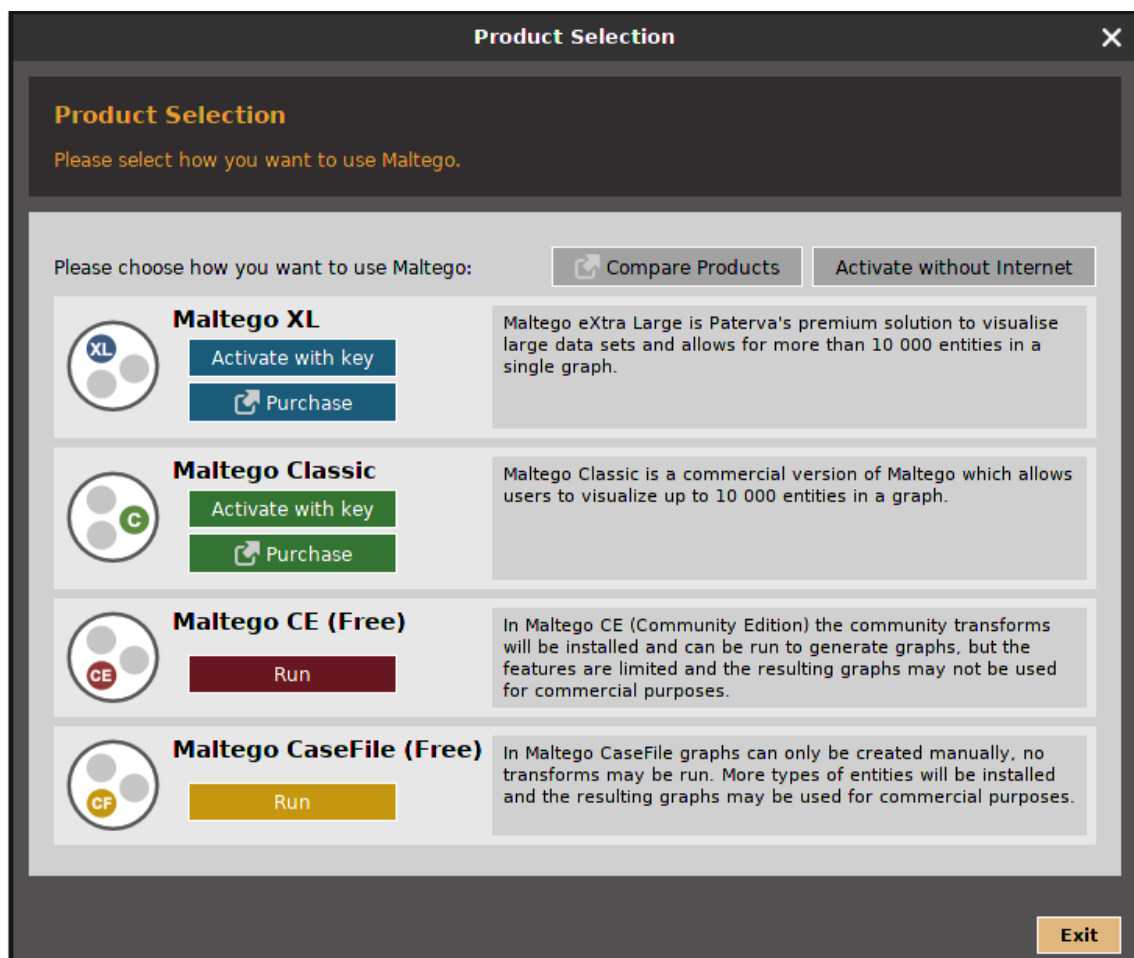
La siguiente herramienta que vamos a utilizar es maltego. Para ello, lo primero que vamos a hacer es instalarlo

```
root@athos:~# sudo aptitude install maltego
The following NEW packages will be installed:
  maltego
The following packages will be REMOVED:
  maltegoce{u}
0 packages upgraded, 1 newly installed, 1 to remove and 1 not upgraded.
Need to get 0 B/78.6 MB of archives. After unpacking 26.4 MB will be freed.
Do you want to continue? [Y/n/?] Y
dpkg: maltegoce: dependency problems, but removing anyway as you requested:
 maltego-teeth depends on maltego; however:
  Package maltego is not installed.
  Package maltegoce which provides maltego is to be removed.
kali-linux-full depends on maltego; however:
  Package maltego is not installed.
  Package maltegoce which provides maltego is to be removed.

(Reading database ... 328101 files and directories currently installed.)
Removing maltegoce (3.6.1.7809-0kali4) ...
Selecting previously unselected package maltego.
(Reading database ... 327029 files and directories currently installed.)
Preparing to unpack .../maltego_4.1.0.10552-0kali1_all.deb ...
Unpacking maltego (4.1.0.10552-0kali1) ...
Setting up maltego (4.1.0.10552-0kali1) ...

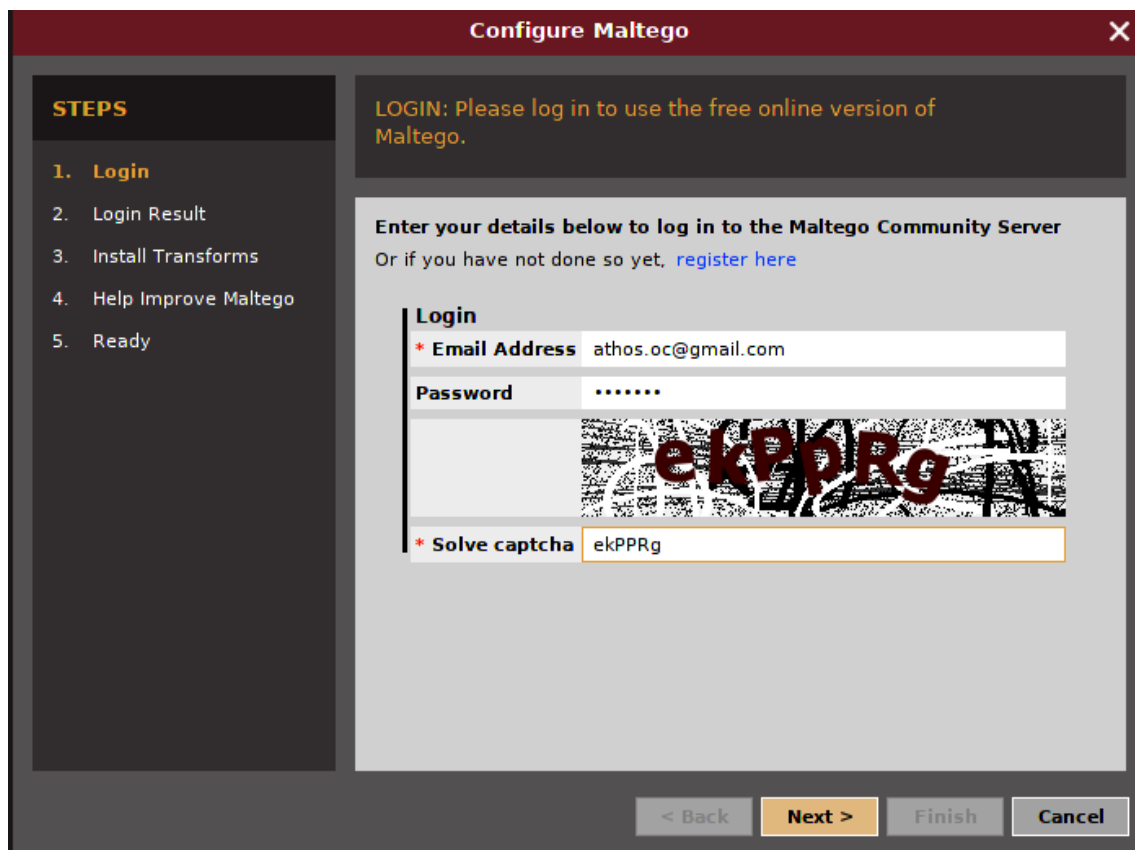
Current status: 1 (-1) upgradable.
root@athos:~# maltego
```

Tras instalarlo y ejecutarlo, vemos que tenemos que seleccionar una de las versiones del programa, en este caso, utilizaremos la versión “Maltego CE” que aunque tiene limitaciones, nos sirve para la prueba de concepto.



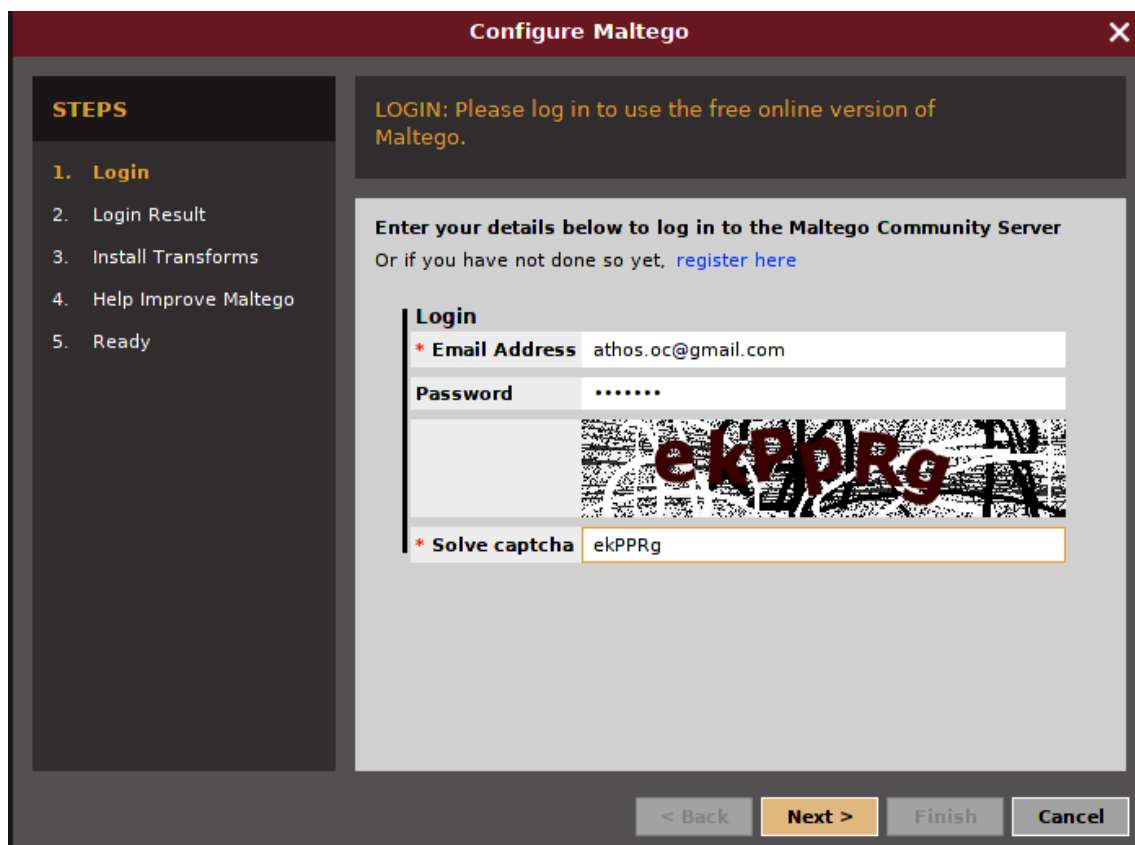


Nos pedirá una cuenta de usuario y que rellenemos un captcha



The screenshot shows the 'Configure Maltego' window with a dark red title bar. On the left, a 'STEPS' sidebar lists: 1. Login (highlighted), 2. Login Result, 3. Install Transforms, 4. Help Improve Maltego, and 5. Ready. The main area has a header 'LOGIN: Please log in to use the free online version of Maltego.' followed by instructions to enter details or register. The login form includes fields for 'Email Address' (athos.oc@gmail.com), 'Password' (masked with dots), a captcha image showing the text 'ekPPRg', and a 'Solve captcha' field containing 'ekPPRg'. At the bottom are buttons for '< Back', 'Next >', 'Finish', and 'Cancel'.

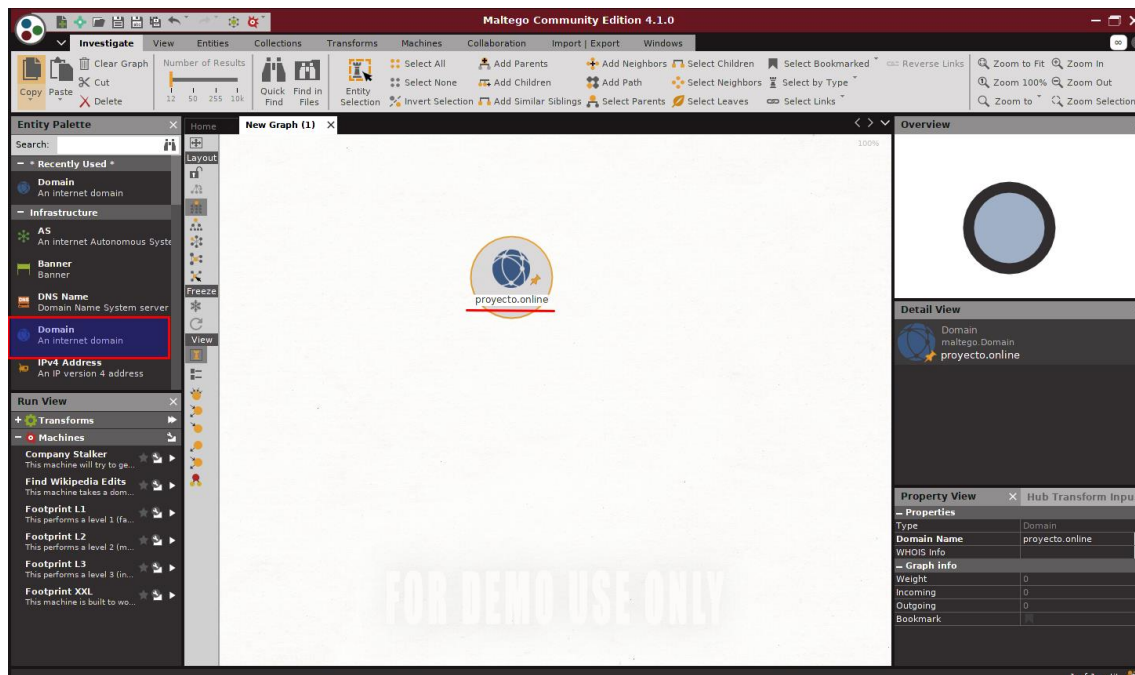
Y tras esto, nos dirá el resultado del login.



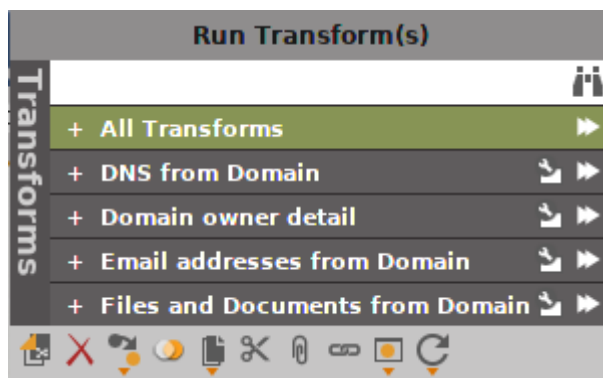
This is an identical screenshot to the one above, showing the 'Configure Maltego' window at the login step. It displays the same sidebar, instructions, login form with email 'athos.oc@gmail.com', masked password, captcha image 'ekPPRg', and 'Solve captcha' field 'ekPPRg', and the bottom navigation buttons.



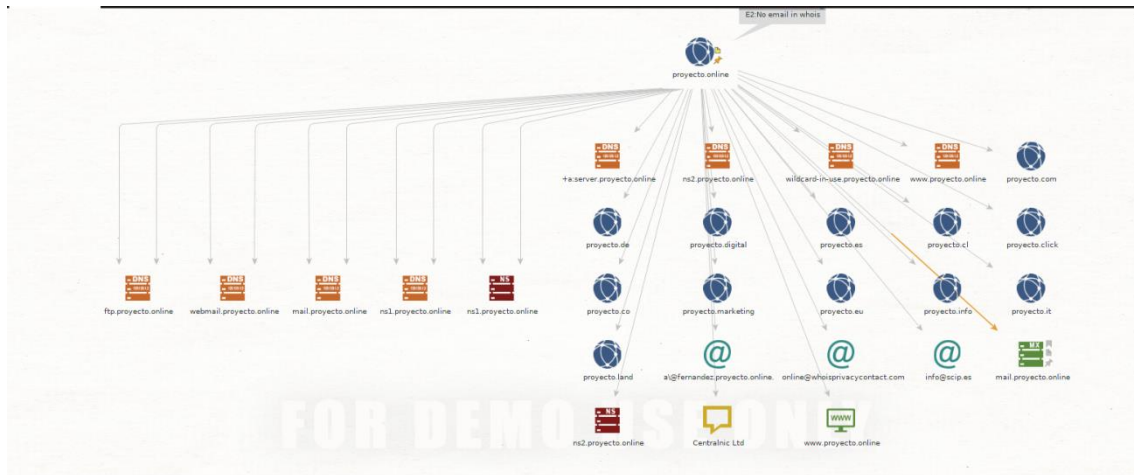
Ahora, tenemos que arrastrar de la paleta de la izquierda, dominio al área de trabajo, y poner el nombre del dominio del que queremos la información. Tal cual se muestra en la siguiente imagen:



Con el botón derecho sacaremos el menú en el que seleccionaremos el tiempo de transformaciones que queremos que se ejecuten, en este caso todas.



Maltego es una herramienta que saca gran cantidad de información, pero hay que tener cuidado porque parte de esa información puede no ser veraz, pero es un punto de partida.

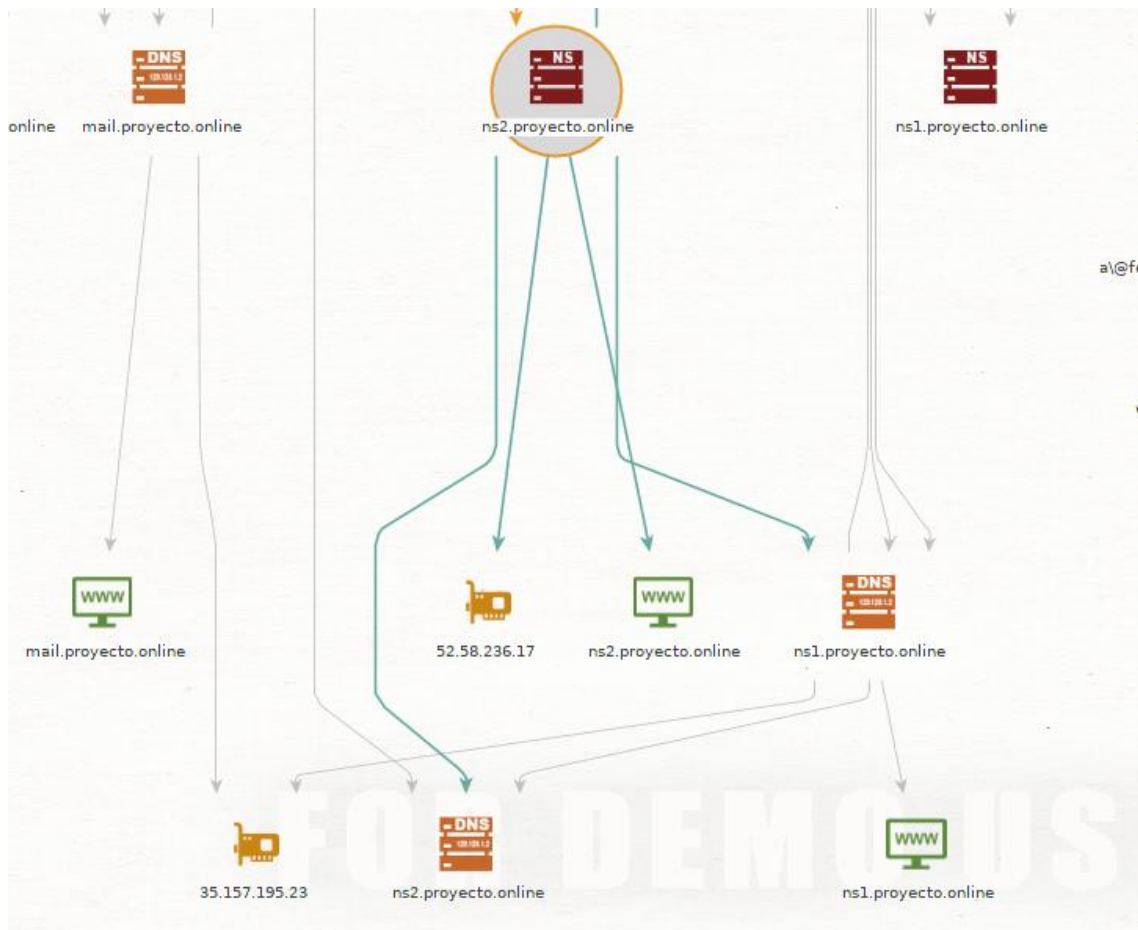


Como podemos ver en la imagen, vemos que los servidores dns que detecta coinciden con los del whois que hemos hecho anteriormente. Pero en el whois anterior, solo veíamos información de contacto sobre la empresa registradora y no sobre los dueños del dominio.

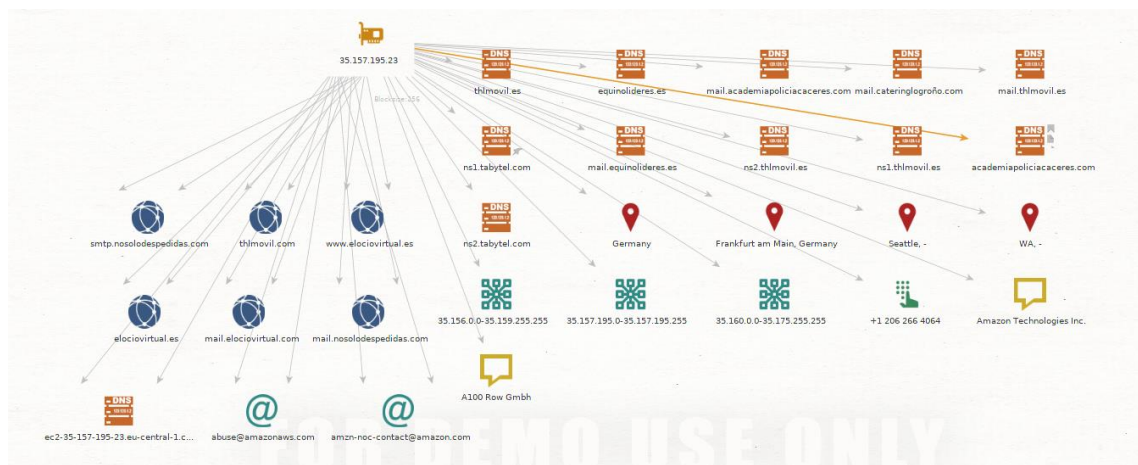
Pero ahora, vemos que existe un correo electrónico, que podría ser nuestro punto de entrada, vemos también los servidores de correo, entradas dns de ftp, webmail, mail etc...

A su vez, de cualquiera de los resultados, podríamos ejecutar más transformaciones.

Vamos a ejecutar más transformaciones de mail.proyecto.online, ns2.proyecto.online y ns2.proyecto.online y vemos que nos ha sacado las direcciones ips



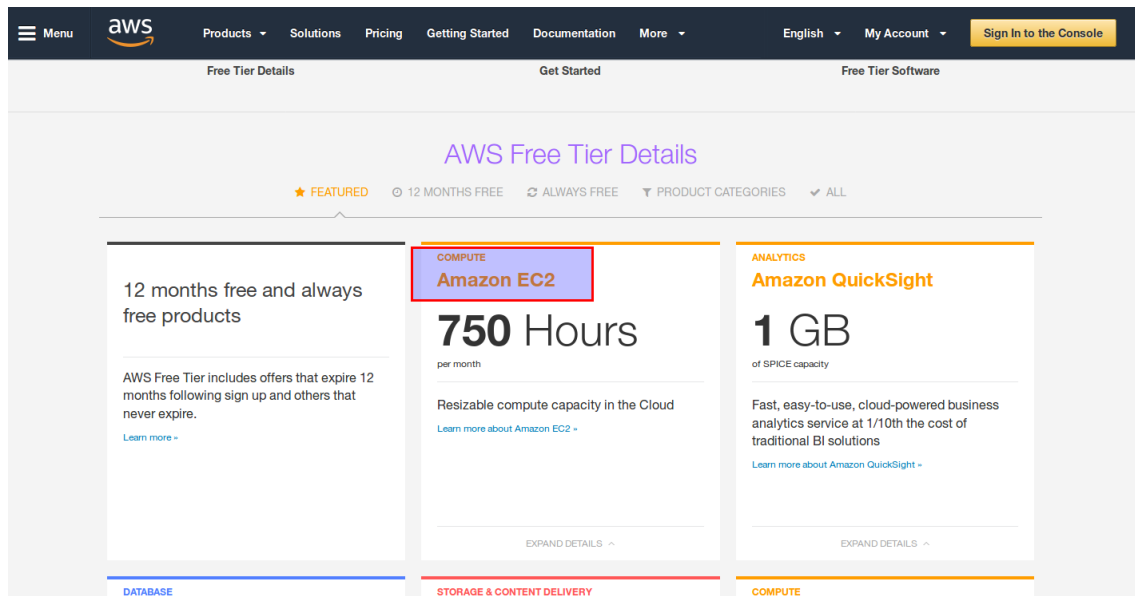
Si ejecutamos transformaciones a la ip 35.157.195.23 vemos lo siguiente



Aquí podemos ver información realmente útil, ya que vemos muchos dominios que están alojados en su servidor, estos dominios pueden contener páginas con fallos de seguridad que posteriormente podríamos estudiar y buscar fallos en el software.

Otra información importante que podemos sacar del grafico anterior es que el servidor es un equipo o equipo virtual alojado en Amazon, esto lo vemos por dos factores, por un lado, en la etiqueta "Amazon Technologies" y por otro lado, en la etiqueta dns ec2-35.... Que si estamos

puestos en el tema, sabremos que las máquinas virtuales que nos ofrece Amazon se llaman ec2.



También podemos ver, que el servidor está alojado en una de las siguientes ubicaciones:

Germany, Seattle o wa

Podríamos seguir ejecutando transformaciones para obtener más información, pero ahora vamos a utilizar otra herramienta:

## Theharvestest

[illegible]

Al programa theharvester le pasamos como parámetros el dominio, la profundidad de búsqueda en los resultados, y el origen de la búsqueda y con esto nos buscará información en los buscadores sobre el dominio que le hayamos dicho.

En este caso, no hemos encontrado gran información, pero bueno... no siempre vamos a conseguir lo que queremos.

Aun así, vamos a poner un ejemplo de la información que puede encontrar theharvester con otro dominio



```
File Edit View Search Terminal Help
[-] Searching in Bing..
    Searching 50 results...
    Searching 100 results...
    Searching 150 results...
    Searching 200 results...
    Searching 250 results...
    Searching 300 results...
    Searching 350 results...
    Searching 400 results...
    Searching 450 results...
    Searching 500 results...
[-] Searching in Exalead..
    Searching 50 results...
    Searching 100 results...
    Searching 150 results...
    Searching 200 results...
    Searching 250 results...
    Searching 300 results...
    Searching 350 results...
    Searching 400 results...
    Searching 450 results...
    Searching 500 results...
    Searching 550 results...

[+] Emails found:
-----
233980oficina@iescomercio.com
75aniversario@iescomercio.com
941-233980oficina@iescomercio.com
amlara@iescomercio.com
aquirce@iescomercio.com
direccion@iescomercio.com
igonzalez@iescomercio.com
jlandres@iescomercio.com
oficina@iescomercio.com

[+] Hosts found in search engines:
-----
[-] Resolving hostnames IPs...
192.232.216.164:aula.iescomercio.com
192.232.216.164:www.iescomercio.com
[+] Virtual hosts:
=====
root@athos:~#
```

Como vemos, unas cuantas direcciones de correo con las que podríamos plantearnos hacer algo de ingeniería social.

```
Full harvest..
[-] Searching in Google..
    Searching 0 results...
    Searching 100 results...
    Searching 200 results...
    Searching 300 results...
    Searching 400 results...
    Searching 500 results...
[-] Searching in PGP Key server..
[-] Searching in Bing..
    Searching 50 results...
    Searching 100 results...
    Searching 150 results...
    Searching 200 results...
    Searching 250 results...
    Searching 300 results...
    Searching 350 results...
    Searching 400 results...
    Searching 450 results...
    Searching 500 results...
[-] Searching in Exalead..
    Searching 50 results...
    Searching 100 results...
    Searching 150 results...
    Searching 200 results...
    Searching 250 results...
    Searching 300 results...
    Searching 350 results...
    Searching 400 results...
    Searching 450 results...
    Searching 500 results...
    Searching 550 results...

[+] Emails found:
-----
pixel-1508069289636470-web-@proyecto.online
pixel-1508069291386506-web-@proyecto.online

[+] Hosts found in search engines:
-----
[-] Resolving hostnames IPs...
[+] Virtual hosts:
=====
```

Otra cosa que podemos hacer para sacar más información del dominio es ver el código fuente de su página.



## Athos Orío Choperena



Como podemos ver en la imagen, he señalado algunas partes que nos brindan información útil, por un lado, vemos que una de sus imágenes se aloja en el directorio wp-content, que es un directorio de la estructura básica de un wordpress, así que ya sabemos que plataforma usa. Una de las cosas buenas (o malas) de wordpress, es que podemos aumentar su funcionalidad básica con plugins. Y por supuesto, estos plugins, pueden contener errores, así, que realizamos una búsqueda por el código fuente con la palabra clave “plugin” a ver que nos aparece:



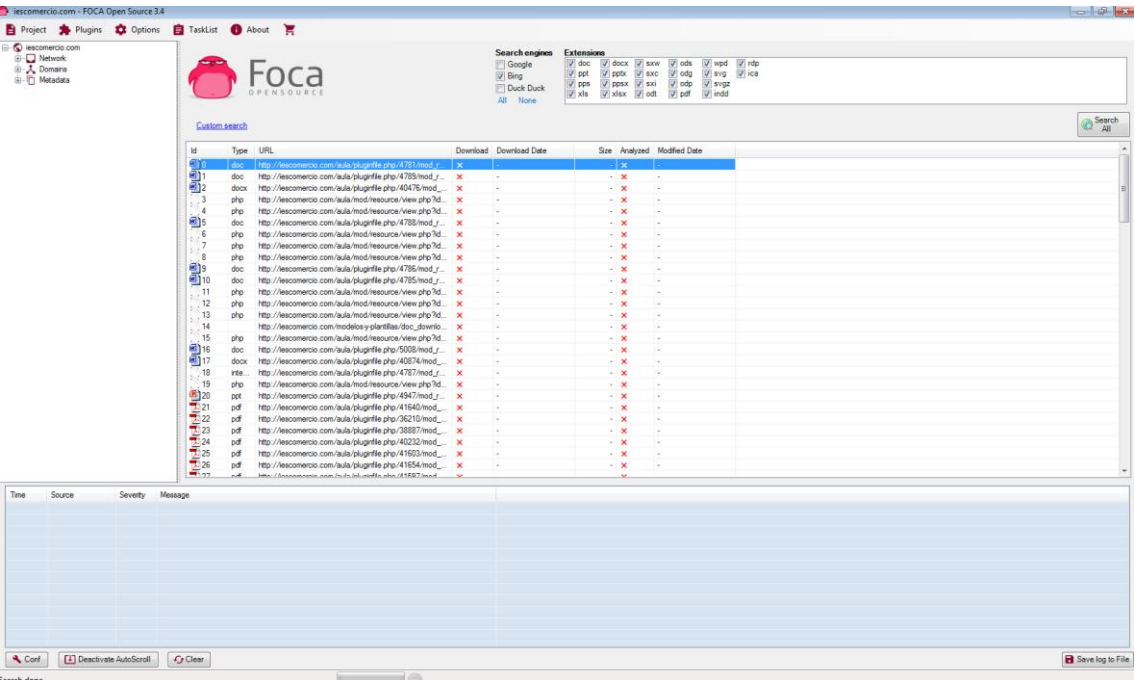
Como podemos ver, tiene diversos plugins instalados, en algunos, incluso sabemos la versión como es el caso de warfareplugins que tiene la versión 2.3.3, esto nos facilita enormemente la búsqueda de errores, ya que es posible que incluso ya estén reportados en la web

Bien. Vamos a pasar a otro software para sacar información:

## La foca:

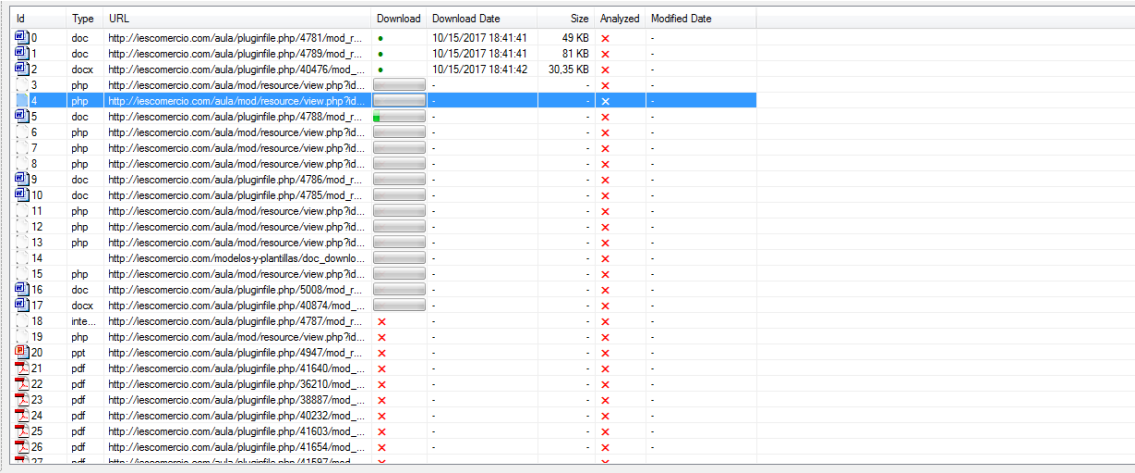
He realizado un escaneo en busca de documentos del dominio proyecto.online, y la foca no ha encontrado ningún resultado, no obstante, pondré una captura de pantalla para ver la información que se podría sacar de otro dominio a modo de ejemplo.

El ejemplo lo haremos con iescomercio

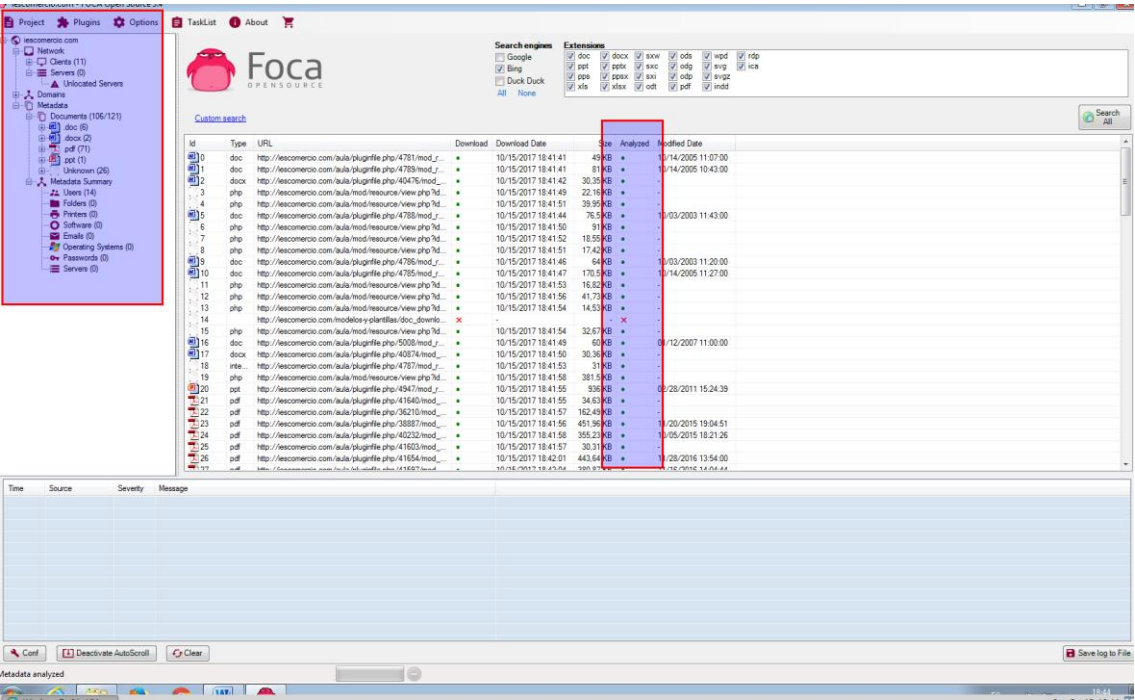


Como podemos ver, hay muchos documentos disponibles, así que vamos a descargarlos y que foca analice los metadatos por nosotros.

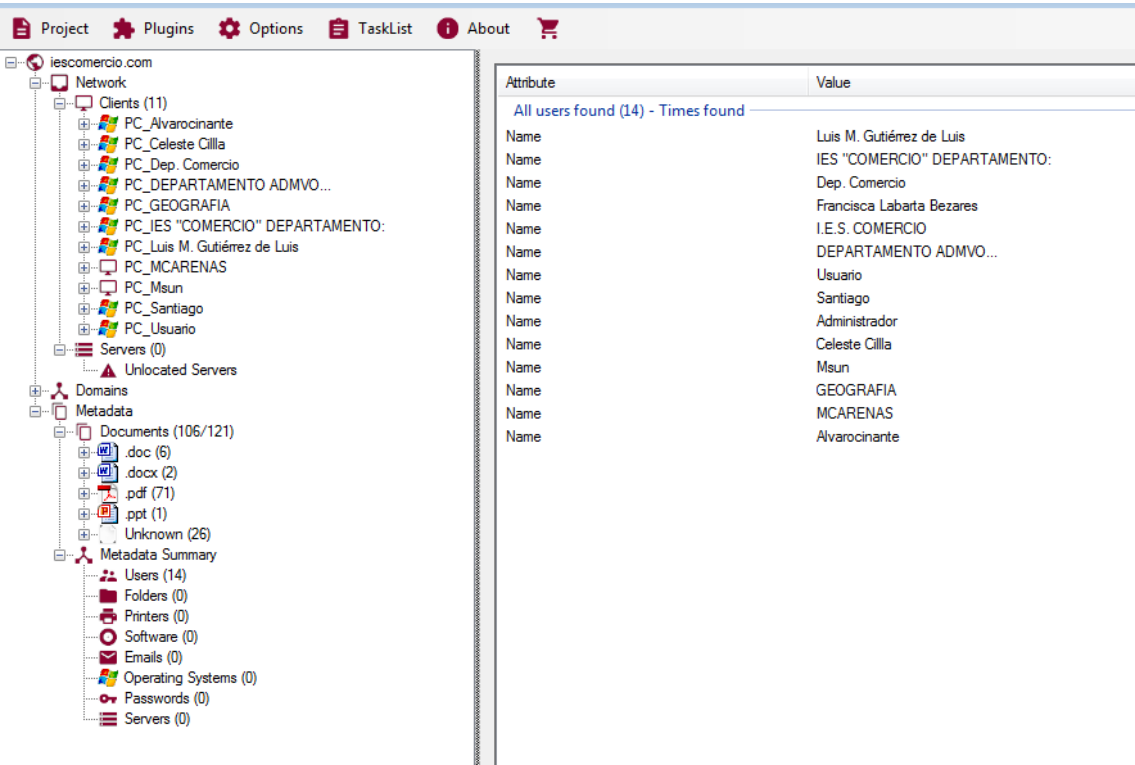
Con el botón derecho le daremos a descargar todo



Como podemos ver en la siguiente imagen, hay cantidad de documentos que tienen metadatos.



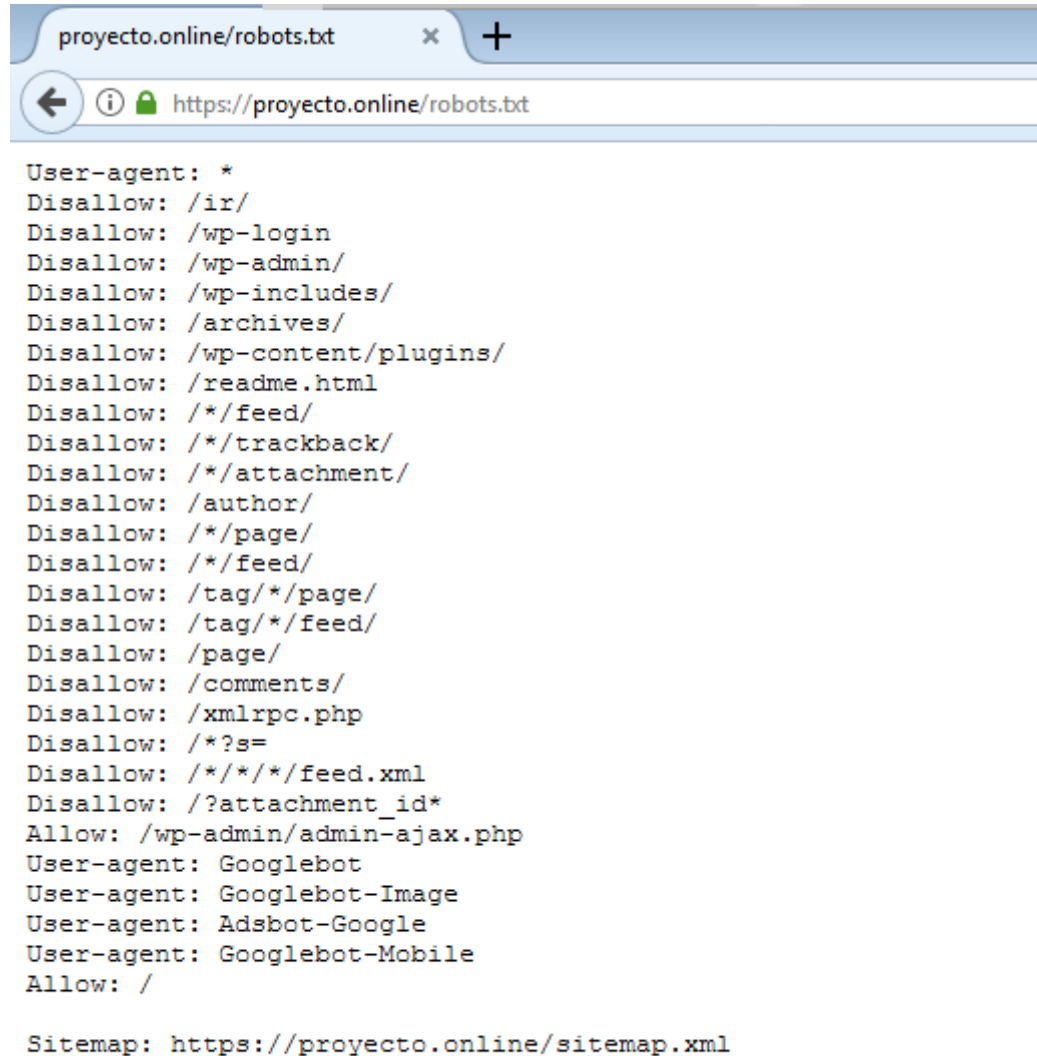
Podemos ver diferentes equipos y usuarios, esta información nos podría servir para volver a maltego, y realizar otras transformaciones por usuarios etc.



## Robots.txt y sitemap.xml

Otra de las cosas que podemos hacer para recabar información, es mirar dos archivos que suelen estar en muchos servidores web, uno es el robots.txt y otro el sitemap.xml

## Robots.txt



Como podemos ver, aquí tenemos información sobre directorios que el administrador de sistema quiere o no quiere que analicen los buscadores. Se sobreentiende, que esos directorios están en el servidor, y según lo que aparezca, puede ser una buena fuente de información.

## Sitemap.xml

Ahora vamos a mirar que tienen en el sitemap

## XML Sitemap Index

This is a XML Sitemap which is supposed to be processed by search engines which follow the XML Sitemap standard like Ask.com, Bing, Google and Yahoo. It was generated using the WordPress content management system and the [Google Sitemap Generator Plugin](#) by Arne Brachhold. You can find more information about XML sitemaps on [sitemaps.org](#) and Google's [list of sitemap programs](#).

This file contains links to sub-sitemaps, follow them to see the actual sitemap content.

URL of sub-sitemap	Last modified (GMT)
<a href="https://proyecto.online/sitemap-misc.xml">https://proyecto.online/sitemap-misc.xml</a>	2017-09-30 15:38
<a href="https://proyecto.online/sitemap-pt-post-2017-09.xml">https://proyecto.online/sitemap-pt-post-2017-09.xml</a>	2017-09-10 20:25
<a href="https://proyecto.online/sitemap-pt-post-2017-08.xml">https://proyecto.online/sitemap-pt-post-2017-08.xml</a>	2017-08-21 15:50
<a href="https://proyecto.online/sitemap-pt-post-2017-07.xml">https://proyecto.online/sitemap-pt-post-2017-07.xml</a>	2017-09-30 15:38
<a href="https://proyecto.online/sitemap-pt-page-2017-07.xml">https://proyecto.online/sitemap-pt-page-2017-07.xml</a>	2017-09-10 20:18
<a href="https://proyecto.online/sitemap-pt-page-2017-06.xml">https://proyecto.online/sitemap-pt-page-2017-06.xml</a>	2017-08-09 02:45
<a href="https://proyecto.online/sitemap-pt-page-2017-02.xml">https://proyecto.online/sitemap-pt-page-2017-02.xml</a>	2017-08-10 11:20
<a href="https://proyecto.online/sitemap-pt-page-2016-06.xml">https://proyecto.online/sitemap-pt-page-2016-06.xml</a>	2017-08-15 16:52

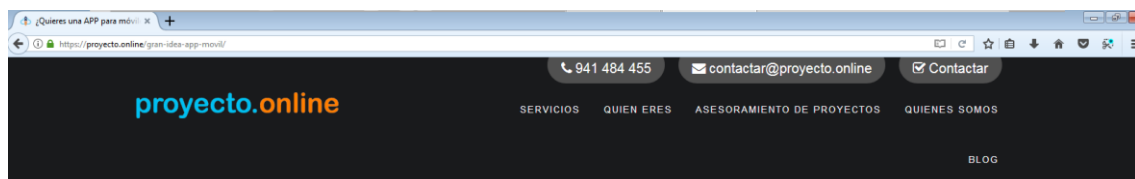
Generated with [Google \(XML\) Sitemaps Generator Plugin](#) for WordPress by [Arne Brachhold](#). This XSLT template is released under the CPL and free to use. If you have problems with your sitemap please visit the [plugin FAQ](#) or the [support forum](#).

Aquí tenemos también información, en primer lugar, nos damos cuenta que este sitemap esta generado por un plugin, concretamente el google xml sitemaps para wordpress, otro plugin del que podemos buscar información sobre bugs o vulnerabilidades.

Si fuésemos navegando por los enlaces, podríamos ir viendo las páginas que tiene el servidor, y quien sabe, es posible que encontrásemos más información.

## La web

Otro sitio donde podemos encontrar información, es en la misma página web del dominio donde queremos encontrar información, recorrerse la página web en busca de direcciones de correo, teléfonos, o es posible que hasta errores, puede sernos muy útil



También podemos encontrar incluso su dirección.



**proyecto.online**

📍 Avenida Lope de Vega, 43-45, Oficina 15, 26007 Logroño (La Rioja)

☎ 941 484 455

✉ [contactar@proyecto.online](mailto:contactar@proyecto.online)



## Fingerprinting:

Hasta aquí podemos llegar sin interactuar directamente con el servidor o la red de la que queremos información, a partir de aquí, tendríamos que tener cuidado por si hacemos algo que las leyes no lo permitan.

¿Qué es fingerprinting?

Fingerprinting es recolectar información sobre un sistema, para aprender sobre su configuración y comportamiento, esta etapa debe hacerse con el debido consentimiento del objetivo.

Esta parte de la práctica vamos a realizarla con la máquina que aloja el dominio athosnetwork.es (que es mío y tengo autorización).

Para ello, vamos a utilizar diferentes programas. Vamos a empezar por nmap.

## Nmap

Haciendo un escaneo no demasiado profundo, podemos ver puertos que tiene abierto el servidor del dominio.

```
root@athos:~# nmap -sS -sV athosnetwork.es
Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-15 19:19 CEST
Nmap scan report for athosnetwork.es (82.223.33.191)
Host is up (0.0010s latency).
rDNS record for 82.223.33.191: server.athosnetwork.es
Not shown: 989 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  tcpwrapped
22/tcp    open  tcpwrapped
25/tcp    open  tcpwrapped
53/tcp    open  tcpwrapped
80/tcp    open  tcpwrapped
143/tcp   open  tcpwrapped
443/tcp   open  tcpwrapped
587/tcp   closed submission
993/tcp   open  tcpwrapped
3306/tcp  open  tcpwrapped
8443/tcp  open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 46.19 seconds
root@athos:~#
```

Podemos ver, que tiene un servidor ftp en el puerto 21, servidor ssh en el 22, dns en el 53, servidor web con y sin ssl, servidor de correo, base de datos en el puerto 3306 y vemos también que tiene el puerto 8443 abierto que corresponde al panel de control plesk.

Por supuesto, también tenemos su dirección ip.

Ya tenemos por dónde empezar.

Vamos a hacer un telnet al puerto 80 de la maquina a ver que nos dice:

```
root@athos:~# telnet athosnetwork.es 80
Trying 82.223.33.191...
Connected to athosnetwork.es.
Escape character is '^]'.
help
HTTP/1.1 400 Bad Request
Server: nginx
Date: Sun, 15 Oct 2017 17:23:45 GMT
Content-Type: text/html
Content-Length: 166
Connection: close


<html>
<head><title>400 Bad Request</title></head>
<body bgcolor="white">
<center><h1>400 Bad Request</h1></center>
<hr><center>nginx</center>
</body>
</html>
Connection closed by foreign host.
root@athos:~#
```

Vemos que como servidor web, tiene nginx.

Esta operación, podríamos realizarla con los diferentes servicios que hemos detectado que están abiertos, pero como nos costaría bastante trabajo manual, vamos a seguir usando software que nos dará una información similar.

Vamos a instalar el plugin para Firefox passiverecon lo cual nos va a permitir, con un simple click sacar mucha información sobre el dominio.

Los dns:




Work in progress!  
Follow intoDNS on [Twitter](#)

Category	Status	Test name	Information	<a href="#">send feedback</a>
Parent		Domain NS records	<p>Nameserver records returned by the parent servers are:</p> <p>ns1.athosnetwork.es. [82.223.33.191] [TTL=86400] ns4.afraid.org. [70.39.97.253] (NO GLUE) [TTL=86400] ns1.afraid.org. [50.23.197.95] (NO GLUE) [TTL=86400] ns2.afraid.org. [208.43.71.243] (NO GLUE) [TTL=86400]</p>	

País donde se aloja



#### Network

Site	<a href="http://athosnetwork.es">http://athosnetwork.es</a>	Netblock Owner	<a href="#">arsys.es</a>
Domain	<a href="#">athosnetwork.es</a>	Nameserver	ns2.athosnetwork.es
IP address	82.223.33.191	DNS admin	athos.oc@gmail.com
IPv6 address	Not Present	Reverse DNS	server.athosnetwork.es
Domain registrar	unknown	Nameserver organisation	unknown
Organisation	unknown	Hosting company	United Internet
Top Level Domain	Spain (.es)	DNS Security Extensions	unknown
Hosting country	 ES		

#### Dirección ip del servidor de correo

```
athosnetwork.es. IN MX 10 mail.athosnetwork.es.  
--> mail.athosnetwork.es. = 82.223.33.191  
  
athosnetwork.es. IN A 82.223.33.191
```

También nos da más información, que posiblemente pueda clasificarse dentro de footprinting, pero lo dejo por ver la información de una herramienta más.

## Nessus

Nessus es un software que nos sirve para buscar posibles vulnerabilidades en los servicios que se encuentren abiertos en un servidor.

athosnetwork.es / athosnetwork.es Configure


[Back to Hosts](#)

Vulnerabilities 45

Filter Search Vulnerabilities 45 Vulnerabilities

Sev	Name	Family	Count
CRITICAL	PHP 5.6.x < 5.6.31 Multiple Vulnerabilities	CGI abuses	1
MEDIUM	SSL Certificate Cannot Be Trusted	General	4
MEDIUM	SSL Certificate Expiry	General	3
MEDIUM	SSL Self-Signed Certificate	General	3
MEDIUM	SSH Weak Algorithms Supported	Misc.	1
LOW	SMTP Service Cleartext Login Permitted	SMTP problems	1
LOW	SSH Server CBC Mode Ciphers Enabled	Misc.	1
LOW	SSH Weak MAC Algorithms Enabled	Misc.	1
INFO	Nessus SYN scanner	Port scanners	8
INFO	Service Detection	Service detection	8

**Host Details**  
IP: 82.223.33.191  
DNS: athosnetwork.es  
OS: Linux Kernel 3.2 on Debian 7.0 (wheezy)  
Start: Today at 7:35 PM

**Vulnerabilities**  


- Critical
- High
- Medium
- Low
- Info

Como podemos ver, nessus ha detectado una vulnerabilidad crítica (que solucionare enseguida.)

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Scanners

CRITICAL

PHP 5.6.x < 5.6.31 Multiple Vulnerabilities

Description

According to its banner, the version of PHP running on the remote web server is 5.6.x prior to 5.6.31. It is, therefore, affected by the following vulnerabilities :  
  
- An out-of-bounds read error exists in the PCRE library in the compile\_bracket\_matchingpath() function within file pcre\_jit\_compile.c. An unauthenticated, remote attacker can exploit this, via a specially crafted regular expression, to crash a process linked to the library, resulting in a denial of service condition. (CVE-2017-6004)  
  
- An out-of-bounds read error exists in the GD Graphics Library (LibGD) in the gdImageCreateFromGifCtx() function within file gd\_gif\_in.c when handling a specially crafted GIF file. An unauthenticated, remote attacker can exploit this to disclose sensitive memory contents or crash a process linked to the library. (CVE-2017-7890)  
  
- An out-of-bounds read error exists in Origenuma in the match\_at() function within file regex.c. An unauthenticated, remote attacker can exploit this to disclose sensitive memory contents or crash a process linked to the library. (CVE-2017-9224)  
  
- An out-of-bounds write error exists in Origenuma in the next\_state\_val() function during regular expression compilation. An unauthenticated, remote attacker can exploit this to execute arbitrary code. (CVE-2017-9226)  
  
- An out-of-bounds read error exists in Origenuma in the mbc\_enc\_len() function within file utf8.c. An unauthenticated, remote attacker can exploit this to disclose memory contents or crash a process linked to the library. (CVE-2017-9227)  
  
- An out-of-bounds write error exists in Origenuma in the bitsel\_set\_range() function during regular expression compilation. An unauthenticated, remote attacker can exploit this to execute arbitrary code. (CVE-2017-9228)  
  
- An invalid pointer reference flaw exists in Origenuma in the left\_adjust\_char\_head() function within file regex.c during regular expression compilation. An unauthenticated, remote attacker can exploit this to crash a process linked to the library, resulting in a denial of service condition. (CVE-2017-9229)  
  
- A denial of service condition exists in PHP when handling overlarge POST requests. An unauthenticated, remote attacker can exploit this to exhaust available CPU resources. (CVE-2017-11142)  
  
- An extended invalid free error exists in PHP in the php\_wddx\_push\_element() function within file ext/wddx/wddx.c when parsing empty boolean tags. An unauthenticated, remote attacker can exploit this to cause a denial of service condition. (CVE-2017-11143)  
  
- A flaw exists in OpenSSL in the EVP\_SealInt() function within file crypto/evp/evp.c due to returning an undocumented value of '-1'. An unauthenticated, remote attacker can exploit this to cause an unspecified impact. (CVE-2017-11144)

Plugin Details

Severity: Critical  
ID: 101525  
Version: \$Revision: 1.4 \$  
Type: remote  
Family: CGI abuses  
Published: July 13, 2017  
Modified: August 18, 2017

Risk Information

Risk Factor: Critical  
CVSS Base Score: 10.0  
CVSS Temporal Score: 7.8  
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C  
/I:C/A:C  
CVSS Temporal Vector: CVSS2#E:POC/RL:OF  
/RC:N/D  
IAVM Severity: I

Vulnerability Information

CPE: cpe:/a:php:php  
Exploit Available: true  
Exploit Ease: Exploits are available  
Patch Pub Date: July 6, 2017  
Vulnerability Pub Date: December 23, 2016

Reference Information

BID: 96296, 99492, 99501  
IAVb: 2017-B-0088  
OSVDB: 151860, 152175, 157903, 157904, 158016, 158017, 158029, 160494, 160497, 160498,

Podemos ver como existen exploits para esta vulnerabilidad y que se ataca de forma remota.

Vulnerability Feeds & Widgets

www.esecdb.com

PHP » PHP » 5.6.30 : Security Vulnerabilities

Cpe Name:cpe:/a:php:php:5.6.30  
CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9  
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending  
Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	<a href="#">CVE-2017-12933</a>	119		Overflow	2017-08-17	2017-09-19	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
The finish_nested_data function in ext/standard/var_unserializer.re in PHP before 5.6.31, 7.0.x before 7.0.21, and 7.1.x before 7.1.7 is prone to a buffer over-read while unserializing untrusted data. Exploitation of this issue can have an unspecified impact on the integrity of PHP.														
2	<a href="#">CVE-2017-11628</a>	119		DoS Overflow	2017-07-25	2017-09-25	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
In PHP before 5.6.31, 7.x before 7.0.21, and 7.1.x before 7.1.7, a stack-based buffer overflow in the zend_ini_do_op() function in Zend/zend_ini_parser.c could cause a denial of service or potentially allow executing code. NOTE: this is only relevant for PHP applications that accept untrusted input (instead of the system's php.ini file) for the parse_ini_string or parse_ini_file function, e.g., a web application for syntax validation of php.ini directives.														
3	<a href="#">CVE-2017-11145</a>	200		Info	2017-07-10	2017-07-23	5.0	None	Remote	Low	Not required	Partial	None	None
In PHP before 5.6.31, 7.x before 7.0.21, and 7.1.x before 7.1.7, an error in the date extension's timelib_meridian parsing code could be used by attackers able to supply date strings to leak information from the interpreter, related to ext/date/lib/parse_date.c out-of-bounds reads affecting the php_parse_date function. NOTE: the correct fix is in the e8b7698f5ee757ce2c8bd1a192a491a498f891c commit, not the bd77ac90d3bdf31ce2a5251ad92e9e75 gist.														
4	<a href="#">CVE-2017-11144</a>	754			2017-07-10	2017-07-14	5.0	None	Remote	Low	Not required	None	None	Partial
In PHP before 5.6.31, 7.x before 7.0.21, and 7.1.x before 7.1.7, the openssl extension PEM sealing code did not check the return value of the OpenSSL sealing function, which could lead to a crash of the PHP interpreter, related to an interpretation conflict for a negative number in ext/openssl/openssl.c, and an OpenSSL documentation omission.														
5	<a href="#">CVE-2017-11143</a>	502			2017-07-10	2017-07-17	5.0	None	Remote	Low	Not required	None	None	Partial
In PHP before 5.6.31, an invalid free in the WDDX deserialization of boolean parameters could be used by attackers able to inject XML or deserialization to crash the PHP interpreter, related to an invalid free for an empty boolean element in ext/wddx/wddx.c.														
6	<a href="#">CVE-2017-11142</a>	400		DoS	2017-07-10	2017-07-18	7.8	None	Remote	Low	Not required	None	None	Complete
In PHP before 5.6.31, 7.x before 7.0.17, and 7.1.x before 7.1.3, remote attackers could cause a CPU consumption denial of service attack by injecting long form variables, related to main/php_variables.c.														
7	<a href="#">CVE-2017-7890</a>	200		Info	2017-08-02	2017-08-15	4.3	None	Remote	Medium	Not required	Partial	None	None
The GIF decoding function gdImageCreateFromGifCtx in gd_gif_in.c in the GD Graphics Library (aka libgd), as used in PHP before 5.6.31 and 7.x before 7.1.7, does not zero colorMap arrays before use. A specially crafted GIF image could use the uninitialized tables to read ~700 bytes from the top of the stack, potentially disclosing sensitive information.														
Total number of vulnerabilities : 7 Page : 1 (This Page)														

Como podemos ver, es una vulnerabilidad crítica, pero que en principio no da acceso al sistema. Así que lo solucionaré más adelante.

## Dnsenum

Dnsenum es una herramienta de línea de comandos que nos permite saber si el servidor dns permite transferencias de zona, y así poder conocer más de la red que estamos escaneando.

```
root@athos:~# dnsenum athosnetwork.es
Smartmatch is experimental at /usr/bin/dnsenum line 698.
Smartmatch is experimental at /usr/bin/dnsenum line 698.
dnsenum VERSION:1.2.4

-----  athosnetwork.es  -----

Host's addresses:
_____

Name Servers:
_____

ns2.athosnetwork.es.      5      IN      A      82.223.33.191
ns1.athosnetwork.es.      5      IN      A      82.223.33.191

Mail (MX) Servers:
_____

Trying Zone Transfers and getting Bind Versions:
_____

Trying Zone Transfer for athosnetwork.es on ns2.athosnetwork.es ...
AXFR record query failed: REFUSED

Trying Zone Transfer for athosnetwork.es on ns1.athosnetwork.es ...
AXFR record query failed: REFUSED

brute force file not specified, bay.
root@athos:~#
```

Como podemos ver, ejecutando el comando sobre el dominio, intenta hacer transferencia de zonas sobre los dns, y en este caso, está bien configurado ya que no permite hacerla.

## Whatweb

Con whatweb, podemos sacar información sobre el servidor web, como vemos en la imagen, el servidor web es nginx, usa la versión php 5.6.30, usa wordpress 4.7.6 y está sobre plesk como gestor del servidor.

```
root@athos:~# whatweb athosnetwork.es
http://athosnetwork.es [301 Moved Permanently] Country[SPAIN][ES], HTTPServer[nginx], IP[82.223.33.191], PHP[5.6.30], Plesk[Lin], RedirectLocation[https://athosnetwork.es/], X-Powered-By[PHP/5.6.30, PleskLin], nginx
https://athosnetwork.es/ [200 OK] Country[SPAIN][ES], HTML5, HTTPServer[nginx], IP[82.223.33.191], JQuery[1.12.4], MetaGenerator[WordPress 4.7.6], PHP[5.6.30], Plesk[Lin], Script[text/javascript], Title[AthosNetwork.es &#8211; Sistemas, programación, seo, pentesting], UncommonHeaders[link], WordPress[4.7.6], X-Powered-By[PHP/5.6.30, PleskLin], nginx
root@athos:~#
```

## Wafw00f

Wafw00f nos va a permitir hacer un chequeo para saber si el sistema cuenta con un ids (sistema de detección de intrusos). En este caso no lo tiene.



```
[+] WordPress theme in use: modern - v1.4.6

[+] Name: modern - v1.4.6
| Latest version: 1.4.6 (up to date)
| Last updated: 2015-10-07T00:00:00.000Z
| Location: https://athosnetwork.es/wp-content/themes/modern/
| Style URL: https://athosnetwork.es/wp-content/themes/modern/style.css

[+] Enumerating plugins from passive detection ...
| 5 plugins found:

[+] Name: download-monitor - v1.9.6
| Latest version: 2017-10-06T15:37:00.000Z
| Location: https://athosnetwork.es/wp-content/plugins/download-monitor/
| Readme: https://athosnetwork.es/wp-content/plugins/download-monitor/readme.txt
[!] The version is out of date, the latest version is 1.9.8

[!] Title: Download Monitor <= 1.9.6 - Unauthenticated Downloading of Logs
Reference: https://wpvulndb.com/vulnerabilities/8810
Reference: https://wordpress.org/plugins/download-monitor/
Reference: https://github.com/download-monitor/download-monitor/commit/72d76b34a372101f0f68e904c1665f688797b662
[i] Fixed in: 1.9.7

[+] Name: google-analytics-for-wordpress - v6.1.7
| Latest version: 2017-10-06T14:30:00.000Z
| Location: https://athosnetwork.es/wp-content/plugins/google-analytics-for-wordpress/
| Readme: https://athosnetwork.es/wp-content/plugins/google-analytics-for-wordpress/readme.txt
[!] The version is out of date, the latest version is 6.2.4

[+] Name: google-syntax-highlighter - v1.5.1
| Latest version: 1.5.1 (up to date)
| Last updated: 2007-08-14T16:02:00.000Z
| Location: https://athosnetwork.es/wp-content/plugins/google-syntax-highlighter/
| Readme: https://athosnetwork.es/wp-content/plugins/google-syntax-highlighter/readme.txt

[+] Name: simple-code-highlighter - v4.0
| Latest version: 1.2 (up to date)
| Last updated: 2015-12-24T17:14:00.000Z
| Location: https://athosnetwork.es/wp-content/plugins/simple-code-highlighter/
| Readme: https://athosnetwork.es/wp-content/plugins/simple-code-highlighter/readme.txt

[+] Name: youtube-embed-plus - v11.7.1
| Latest version: 2017-07-19T05:34:00.000Z
| Location: https://athosnetwork.es/wp-content/plugins/youtube-embed-plus/
| Readme: https://athosnetwork.es/wp-content/plugins/youtube-embed-plus/readme.txt
[!] The version is out of date, the latest version is 11.8.2

[!] Title: YouTube Embed <= 11.8.1 - Cross-Site Request Forgery (CSRF)
Reference: https://wpvulndb.com/vulnerabilities/8873
Reference: https://security.daw.com/advisories/csrf-in-youtube-plugin/
Reference: http://seclists.org/fulldisclosure/2017/Jul/64
[i] Fixed in: 11.8.2

[+] Finished: Sun Oct 15 19:44:51 2017
[+] Requests Done: 89
[+] Memory used: 138.258 MB
[+] Elapsed time: 00:00:14
root@athos:~#
```

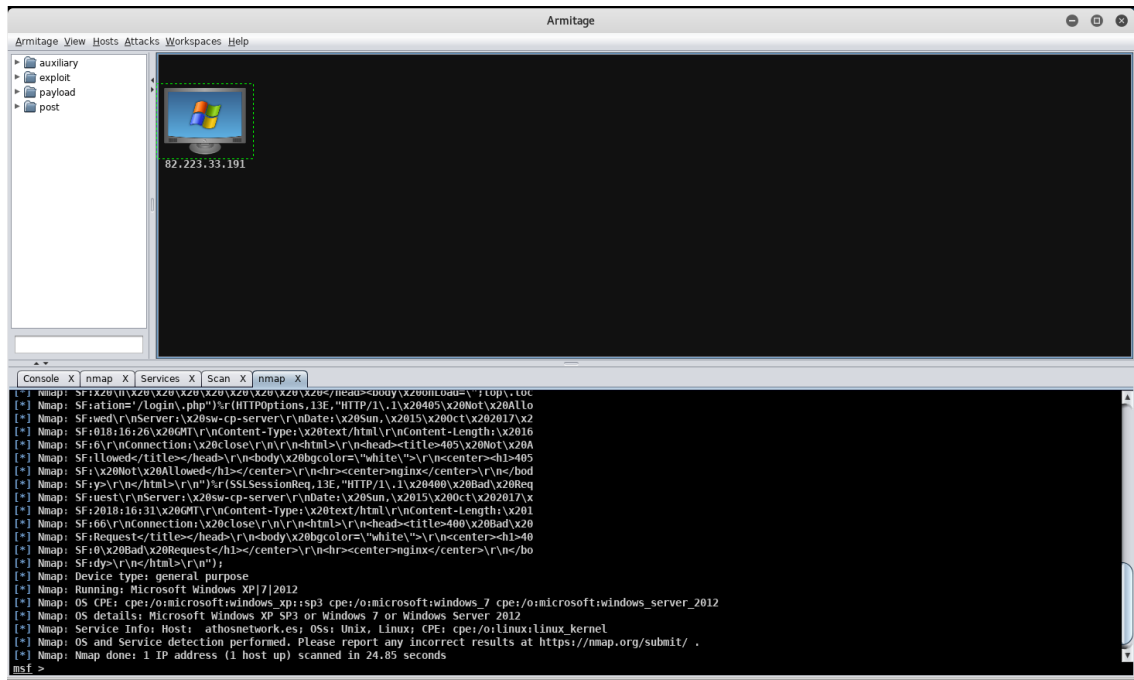
Como podemos ver, gracias a esta herramienta, hemos podido localizar vulnerabilidades, una de cross site request forgery, inyección de cabeceras en reseteo de password, y descarga de logs sin autenticación.

Además de los posibles fallos de seguridad, nos da también información sobre las vulnerabilidades.

### Detección del sistema operativo:

Haciendo un escaneo con armitage, vemos que el sistema operativo que detecta es Windows, lo cual es un error, ya que el servidor es Linux





Si realizamos el escaneo directamente con nmap, vemos algo más de luz, ya que el sistema operativo que tiene esa máquina es debían

```
root@athos:~# nmap -O -sSU 82.223.33.191

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-15 20:20 CEST
Nmap scan report for 82.223.33.191
Host is up (0.00037s latency).
All 2000 scanned ports on 82.223.33.191 are filtered (1000) or open|filtered (1000)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS details: Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Linux 4.4, Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012, VMware Player virtual NAT device
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.74 seconds
root@athos:~#
```