



Curso de Hacking ético Master. D

Ejercicio 2 - RECOPIACIÓN
DE INFORMACIÓN

Alumno: Julián Gordon

Índice

Introducción	3
Openteneas	4
Google Dorks	9
Security Trails	10
TheHarvester	12
Whois	13
Nslookup - Ping	14
Traceroute	16
DNSDumpster	17
Shodan	21
Maltego	23
Foca - Obtención y Análisis de Metadatos	25
Conclusión	27

Introducción

En este ejercicio, recogeremos toda la información posible sobre el dominio “aspasios.com”. Para ello, utilizamos diferentes herramientas y comandos como Whois, Ping, nslookup, Openteneo, Security Trails, Shodan, Google Dorks, DNSDumpster, Maltego, TheHarvester, Foca para la obtención de Metadatos, etc.

Openteneea

Empezaremos esta etapa del pentesting con la herramienta Openteneea. A través de su página web, logramos recoger información sobre el nombre de las empresas relacionadas con nuestro objetivo. En las siguientes imágenes podemos observar que hay 3 empresas relacionadas con nuestro objetivo.



ASPASIOS MIDSTAY S.L

Información de la empresa **ASPASIOS MIDSTAY S.L**

Objeto social	EXPLOTACION DE VIVIENDAS Y APARTAMENTOS TURISTICOS, CON FINALIDAD TURISTICA O DE CORTA ESTANCIA, ASI COMO APARTOTELES, HOTELES, HOSTALES Y PENSIONES, YA SEA MEDIANTE ACUERDOS DE GESTION, CESION O ARRENDAMIENTO, ETC.		
Capital social	100.000,00 €		
Dirección	RD DE SANT PERE NUM.39 P.2 PTA		
Población	BARCELONA	Provincia	BARCELONA

La última actualización de la empresa **Aspasios Midstay S.L** de BARCELONA (BARCELONA) es del 21 de Febrero de 2023.

En el historial de **Aspasios Midstay S.L** aparecen 3 empresarios. Actualmente todos siguen ejerciendo en **Aspasios Midstay S.L**.

Destacamos la figura de **SALZBERG BARENBLIT EZEQUIEL** como cargo más veterano de **Aspasios Midstay S.L** ejerciendo de Administrador Único durante 7 meses, cargo que actualmente sigue ocupando.

El último cambio respecto a los empresarios de **Aspasios Midstay S.L** es de **MOLINA MARTINEZ OLGA** que ha sido nombrado como apoderad.sol en 21 de Febrero de 2023.



ASPASIOS MADRID SL

Información de la empresa **ASPASIOS MADRID SL**

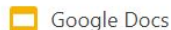
Objeto social	CNAE 5510:LA EXPLOTACION,INCLUSO MEDIANTE FRANQUICIA,DE LOS NEGOCIOS DE HOTELES,APARTAMENTOS TURISTICOS,BARES,RESTAURANTES,CAFETERIAS,SNACKS,SALAS DE FIESTA,Y EN GENERAL CUANTOS ESTABLECIMIENTOS PUEDAN INCLUIRSE EN LOS RAMO		
Capital social	200.000,00 €		
Dirección	RD DE SANT PERE Num.39 P.3 PTA		
Población	BARCELONA	Provincia	BARCELONA

La última actualización de la empresa **Aspasios Madrid SI** de BARCELONA (BARCELONA) es del 07 de Noviembre de 2016.

En el historial de **Aspasios Madrid SI** aparecen 3 empresarios. Actualmente 2 siguen ejerciendo en **Aspasios Madrid SI**.

Destacamos la figura de **SALZBERG BARENBLIT EZEQUIEL** como cargo más veterano de **Aspasios Madrid SI** ejerciendo de Administrador Solidario durante 12,2 años, cargo que actualmente sigue ocupando.

El último cambio respecto a los empresarios de **Aspasios Madrid SI** es de **SALZBERG BARENBLIT EZEQUIEL** que ha sido revocado como adminstr. en 07 de Noviembre de 2016.



RIGHTPLACE REAL ESTATE S.L

Información de la empresa **RIGHTPLACE REAL ESTATE S.L**

Objeto social	COMPRAVENTA DE FINCAS RUSTICAS Y URBANAS,DE TERRENOS Y DEMAS BIENES INMUEBLES,ESPECIALMENTE EDIFICACIONES,EN BLOQUE O POR DEPARTAMENTOS,ASI COMO SU CESION Y EXPLOTACION DIRECTA POR CUALQUIER TITULO ADMITIDO EN DERECHO,ETC.		
Capital social	3.000,00 €		
Dirección	CL RONDA DE SANT PERE NUM.39 P.4 PTA		
Población	BARCELONA	Provincia	BARCELONA

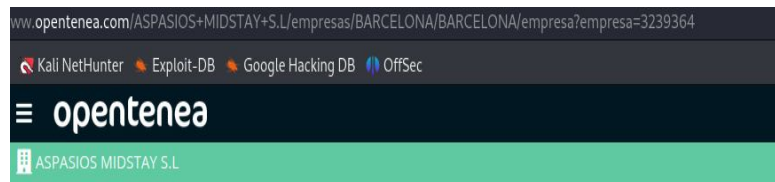
La última actualización de la empresa **Rightplace Real Estate S.L** de BARCELONA (BARCELONA) es del 10 de Noviembre de 2022.

En el historial de **Rightplace Real Estate S.L** aparecen 12 empresarios. Actualmente 10 siguen ejerciendo en **Rightplace Real Estate S.L**.

Destacamos la figura de **CASTELLO LOPEZ JOAN. REPR** como cargo más veterano de **Rightplace Real Estate S.L** ejerciendo de Consejero durante 2,1 años, cargo que actualmente sigue ocupando.

El último cambio respecto a los empresarios de **Rightplace Real Estate S.L** es de **FLAQUER BADELL LUIS IGNACIO** que ha sido revocado como consejero en 10 de Noviembre de 2022.

Una vez que ya tenemos los nombres reales de las empresas que están relacionadas con nuestro objetivo, podemos verificar los miembros con cargos más importantes.



Empresarios de la empresa **ASPASIOS MIDSTAY S.L.**

Mostrando 10 registros por página

Empresario	Cargo	Nombramiento	Cese	Antigüedad
MOLINA MARTINEZ OLGA	APODERAD.SOL	2023-02-21		7 meses
ROS VALLS ALEXANDRE	APODERAD.SOL	2023-02-21		7 meses
SALZBERG BARENBLIT EZEQUIEL	Administrador Único	2023-02-16		7 meses

Mostrando página 1 de 1



Empresarios de la empresa **ASPASIOS MADRID SL**

Mostrando 10 registros por página

Empresario	Cargo	Nombramiento	Cese	Antigüedad
ARDID VITURRO MIGUEL	Administrador Solidario	2016-11-07		6,9 años
FRAUKJE VAN BOHEEMEN	Administrador Solidario	2011-07-05	2012-02-10	7 meses
SALZBERG BARENBLIT EZEQUIEL	Administrador Solidario	2011-07-05		12,2 años

Mostrando página 1 de 1



Empresario	↑↓	Cargo	↑↓	Nombramiento	↑↓	Cese	↑↓	Antigüedad	↑↓
CASANOVAS DOMENECH JORGE		Consejero		2022-11-10				10 meses	
CASANOVAS GIMENEZ CARLOS		43 RRM		2022-11-10				10 meses	
LAOCOONTE VENTURES IBERIA SL. REPR		Consejero		2022-11-10				10 meses	
CASTELLO LOPEZ JOAN. REPR		Consejero		2021-08-23				2,1 años	
CASTELLO LOPEZ YOLANDA		43 RRM		2021-08-23				2,1 años	
FLAQUER BADELL LUIS IGNACIO		Consejero		2021-08-23		2022- 11-10		1,2 años	
MOLINA MARTINEZ OLGA		Consejero		2021-08-23				2,1 años	
MOLINA MARTINEZ OLGA		ol.		2021-08-23				2,1 años	
ROS VALLS ALEXANDRE		Consejero		2021-08-23		2022- 11-10		1,2 años	
SALZBERG BARENBLIT EZEQUIEL		Consejero		2021-08-23				2,1 años	

GOOGLE DORKS

A través del uso de Google dorks, `inurl:aspasios.com filetype:pdf` y `site:rightplace.es filetype:pdf`, obtuvimos varios archivos que luego utilizaremos con la herramienta Foca, para extraer sus metadatos.

Google dorks: `inurl:aspasios.com admin`

Encontramos este link de acceso para administradores que nos puede servir para intentar acceder a nuestro objetivo:

<https://longtermrentalsbarcelona.aspasios.com/administrator/>

Google dorks: `inurl:/user site:aspasios.com`

Nos devuelve este link de acceso: <https://limpieza.aspasios.com/user/login> que también nos puede servir para intentar acceder a nuestro objetivo.

Security Trails

A través de la herramienta Security Trails obtuvimos los siguientes datos relacionados con nuestro objetivo:

Correos electrónicos: office@aspasios.com, longterm@aspasios.com, mantenimiento@aspasios.com, check-in@aspasios.com, living-madrid@aspasios.com

"Administraciononline.aspasios.com:20.160.173.81", "app.aspasios.com:178.32.60.159",
"concurso.aspasios.com:178.32.60.159", "devel.aspasios.com:178.32.60.159",
"gestion.aspasios.com:88.99.121.217", "intranet.aspasios.com:178.32.60.159",
"limpieza-madrid.aspasios.com:88.99.121.217", "limpieza.aspasios.com:88.99.121.217",
"longtermrentalsbarcelona.aspasios.com:46.105.249.217",
"revenue.aspasios.com:88.99.121.217", "webmail.aspasios.com:142.250.200.83",
"www.aspasios.com:88.99.121.217", "www.limpieza.aspasios.com:88.99.121.217"

Security Trails

Estos links que obtuvimos, son muy valiosos porque son links de acceso para administradores que trabajan en la empresa de nuestro objetivo. Podemos probar, con algunas de las direcciones de correo electrónico de usuarios que ya obtuvimos, y luego solo nos faltaría, crear un diccionario para intentar un ataque de fuerza bruta, para obtener la contraseña. Para crear este diccionario también podemos obtener información sobre el usuario de nuestro objetivo a través de redes sociales como LinkedIn, Facebook ó X(ex Twitter)

TheHarvester

Con la herramienta TheHarvester obtuvimos los siguientes correos electrónicos relacionados con nuestro objetivo:

ezequiel@aspasios.com

fuster@aspasios.com

info@aspasios.com

living-barcelona@aspasios.com

marketing@aspasios.com

olga@aspasios.com

Whois

Aqui utilizamos la herramienta Whois, sobre nuestro objetivo. Nos brinda información sobre el registro del dominio, la fecha de creación y la de caducidad del registro.

```
Archivo Acciones Editar Vista Ayuda
(kali@kali)-[~]
$ whois aspasios.com
Domain Name: ASPASIOS.COM
Registry Domain ID: 139991977_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.ovh.com
Registrar URL: http://www.ovh.com
Updated Date: 2023-01-11T11:45:54Z
Creation Date: 2005-01-19T10:54:39Z
Registry Expiry Date: 2024-01-19T10:54:39Z
Registrar: OVH sas
Registrar IANA ID: 433
Registrar Abuse Contact Email: abuse@ovh.net
Registrar Abuse Contact Phone: +33.972101007
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: DNS107.OVH.NET
Name Server: NS107.OVH.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-09-21T10:21:36Z <<<

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

Nslookup - Ping

Ahora utilizamos las herramientas nslookup y ping. Esto nos arroja una información muy importante, los valores por defecto de un sistema operativo de la respuesta a ping. Con el ttl, que luego contrastaremos con el comando traceroute, podemos hacer una estimación sobre qué tipo de sistema operativo tiene nuestro objetivo.

```
(root@kali)-[/home/kali]
# nslookup aspasios.com
Server:      10.254.150.1
Address:     10.254.150.1#53
```

```
Non-authoritative answer:
Name:   aspasios.com
Address: 88.99.121.217
```

```
(root@kali)-[/home/kali]
# ping 10.254.150.1
```

```
PING 10.254.150.1 (10.254.150.1) 56(84) bytes of data:
64 bytes from 10.254.150.1: icmp_seq=1 ttl=116 time=16.1 ms
64 bytes from 10.254.150.1: icmp_seq=2 ttl=116 time=16.0 ms
64 bytes from 10.254.150.1: icmp_seq=3 ttl=116 time=17.0 ms
64 bytes from 10.254.150.1: icmp_seq=4 ttl=116 time=15.6 ms
64 bytes from 10.254.150.1: icmp_seq=5 ttl=116 time=17.5 ms
64 bytes from 10.254.150.1: icmp_seq=6 ttl=116 time=16.8 ms
64 bytes from 10.254.150.1: icmp_seq=7 ttl=116 time=16.0 ms
64 bytes from 10.254.150.1: icmp_seq=8 ttl=116 time=13.6 ms
64 bytes from 10.254.150.1: icmp_seq=9 ttl=116 time=17.5 ms
64 bytes from 10.254.150.1: icmp_seq=10 ttl=116 time=17.7 ms
64 bytes from 10.254.150.1: icmp_seq=11 ttl=116 time=15.2 ms
64 bytes from 10.254.150.1: icmp_seq=12 ttl=116 time=15.2 ms
^C
```

```
— 10.254.150.1 ping statistics —
12 packets transmitted, 12 received, 0% packet loss, time 11080ms
```

Traceroute

Ahora utilizaremos la herramienta Traceroute, para contrastar con el ttl que obtuvimos al usar el comando Ping. El ttl es 116 y con Traceroute verificamos que hace 3 saltos. Por lo que seria 113, y se aproxima a 128. Podemos concluir que el sistema operativo es un Windows

trace route

Host & IP Address Visual Traceroute ::

[Site Info](#) [Whois](#) [Traceroute](#) [RBL Check](#)


[Site Info](#) [Who Is](#) [Trace Route](#) [RBL Check](#) [What's My IP?](#) [Web Search](#)

Enter Domain Name or IP Address:

aspasios.com

Traceroute



Hop	Min	Max	Avg	IP address	Host	Geo Information	Latitude	Longitude	Distance
1	0.150 ms	0.195 ms	0.171 ms	192.168.0.10	192.168.0.10	--	--	--	--
2	0.742 ms	1.091 ms	0.917 ms	192.168.1.1	192.168.1.1	--	--	--	--
3	2.384 ms	3.369 ms	3.004 ms	87.243.116.2	87-243-116-2.ip.btc-net.bg	 Bulgaria, Selanovci	43°68'33" N	24°01'67" E	8357.76 km
4	*	*	*						
4	*	*	*						

DNSDumpster

Otra herramienta interesante que podemos utilizar para recopilación de información es DNSDumpster. En las siguiente imágenes, se pueden ver mapas de información sobre el dominio y los distintos servidores que alojan distintos subdominios de nuestro objetivo.

Hostname	IP Address	TXTV	Reverse DNS	Netblock	Country	Tech / Apps	HTTP / Title	HTTPS / Title	FTP / SSH / Telnet
longtermrentalsbarcelona.aspasios.com	46.105.249.217	A	dns23.labtres.com	OVH	France	PHP 5.4.45 CentOS Apache, 2.4.6	Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips mod_fcgid/2.3.9 title: Site Maintenance	Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips mod_fcgid/2.3.9 title: 403 Forbidden	ftp: 220 (vsFTPd 3.0.2) ssh: SSH-2.0-OpenSSH_6.6.1
limpieza.aspasios.com	88.99.121.217	A	static.217.121.99.88.clients.your-server.de	HETZNER-AS	Germany				
www.limpieza.aspasios.com	88.99.121.217	A	static.217.121.99.88.clients.your-server.de	HETZNER-AS	Germany				
concurso.aspasios.com	178.32.60.159	A	www.aspasios.com	OVH	United Kingdom				
limpieza-madrid.aspasios.com	88.99.121.217	A	static.217.121.99.88.clients.your-server.de	HETZNER-AS	Germany				
revenue.aspasios.com	88.99.121.217	A	static.217.121.99.88.clients.your-server.de	HETZNER-AS	Germany				
gestion.aspasios.com	88.99.121.217	A	static.217.121.99.88.clients.your-server.de	HETZNER-AS	Germany				
ns107.ovh.net.	213.251.128.151	NS	ns107.ovh.net	OVH	France				
dns107.ovh.net.	213.251.188.151	NS	dns107.ovh.net	OVH	France				
30 aspmx5.googlemail.com.	172.217.197.26	MX	qa-in-f26.1e100.net	GOOGLE	United States				
20 alt2.aspmx.l.google.com.	173.194.219.26	MX	ya-in-f26.1e100.net	GOOGLE	United States				
30 aspmx3.googlemail.com.	173.194.219.26	MX	ya-in-f26.1e100.net	GOOGLE	United States				
20 alt1.aspmx.l.google.com.	172.253.126.26	MX	gd-in-f26.1e100.net	GOOGLE	United States				
30 aspmx4.googlemail.com.	142.250.112.27	MX	ga-in-f27.1e100.net	GOOGLE	United States				
10 aspmx.l.google.com.	74.125.69.26	MX	iq-in-f26.1e100.net	GOOGLE	United States				
30 aspmx2.googlemail.com.	172.253.126.27	MX	gd-in-f27.1e100.net	GOOGLE	United States				

FTP: 220 (vsFTPD 3.0.20)

SSH: SSH-2.0-OpenSSH_6.6.1

OVH

213.251.128.151

ns107.ovh.net.

213.251.188.151

dns107.ovh.net.

46.105.249.217

longtermrentalsbarcelona.aspasios.com

178.32.60.159

concurso.aspasios.com

A

NS

HETZNER-AS

88.99.121.217

limpieza.aspasios.com
www.limpieza.aspasios.com
limpieza-madrid.aspasios.com
revenue.aspasios.com
gestion.aspasios.com

aspasios.com

MX

GOOGLE

142.250.112.27

30 aspmx4.googlemail.com.

172.217.197.26

30 aspmx5.googlemail.com.

172.253.126.26

20 alt1.aspmx.l.google.com.

74.125.69.26

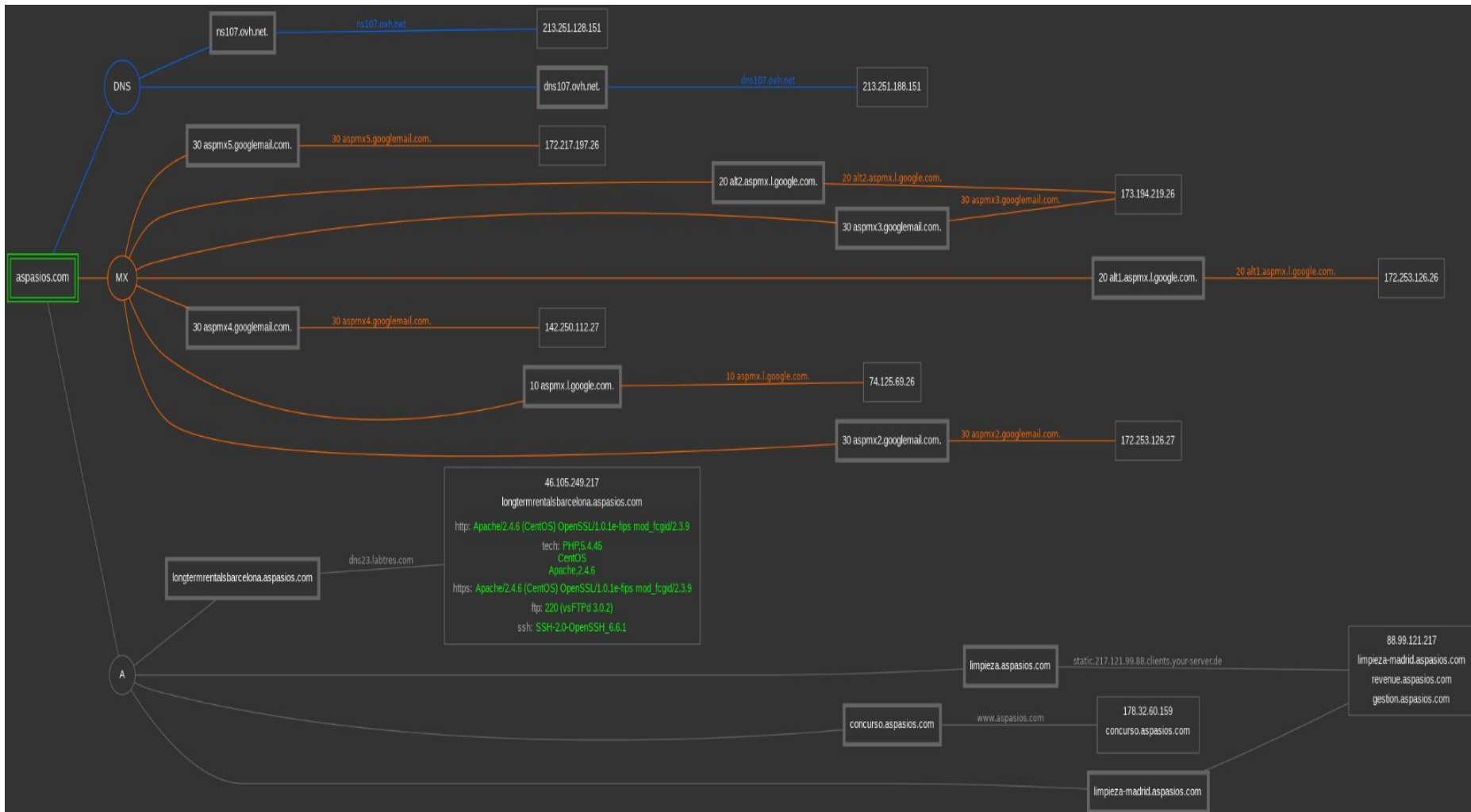
10 aspmx.l.google.com.

172.253.126.27

30 aspmx2.googlemail.com.

173.194.219.26

20 alt2.aspmx.l.google.com.
30 aspmx3.googlemail.com.



Shodan

Ahora que ya tenemos direcciones IP de dominios relacionados con `aspasios.com`, utilizamos la herramienta Shodan para encontrar dispositivos conectados a internet.

La consulta por el ip `88.99.121.217`, que obtuvimos a través del comando `nslookup`, nos devuelve la siguiente información.

88.99.121.217

Regular View

> Raw Data



© OpenMapTiles, Satellite | © MapTiler © OpenStreetMap contributors

// TAGS: self-signed starttls

// LAST SEEN: 2023-10-02

General Information

Hostnames
aspasios.com
www.aspasios.com
static.217.121.99.88.clients.your-server.de

Domains
ASPASIOS.COM
YOUR-SERVER.DE

Country
Germany

City
Gunzenhausen

Organization
Hetzner Online GmbH

ISP
Hetzner Online GmbH

ASN
AS24940

Open Ports

21

80

222

443

// 21 / TCP

-1944571549 | 2023-09-07T05:42:07.352514

```
220 ProFTPD Server (Bienvenido al FTP) [88.99.121.217]
550 SSL/TLS required on the control channel
550 SSL/TLS required on the control channel
211-Features:
AUTH TLS
CCC
CLNT
EPRT
EPSV
HOST
LANG ru-RU;ja-JP;es-ES;bg-BG;fr-FR;zh-TW;ko-KR;it-IT;zh-CN;en-US
MDTM
MFF modify;UNIX.group;UNIX.mode;
MFMT
MLST modify*;perm*;size*;type*;unique*;UNIX.group*;UNIX.groupname*;UNIX.mode*;UNIX.owner*;UNIX.ownername*;
PBSZ
PROT
RANG STREAM
```

Maltego

Otra herramienta muy útil para recopilación de información es Maltego. Con esta herramienta centralizamos distintos motores de búsqueda, instalando distintos Transforms para que nos devuelva información importante. En este caso, utilizamos la herramienta “Have i been pwned” . Sirve para saber si la dirección de correo electrónico, que obtuvimos en pasos anteriores, fue comprometida por violaciones de datos. Se puede ver en la siguiente imagen, los distintos sitios que se utilizó esta dirección de correo y que tuvo filtraciones de datos.



ezequiel@aspasios.com

Get all breaches of an e-mail address [v3 @haveibeenpwned]

Get all breaches of an e-mail address [v3 @haveibeenpwned]

Get all breaches of an e-mail address [v3 @haveibeenpwned]

Get all breaches of an e-mail address [v3 @haveibeenpwned]

Get all breaches of an e-mail address [v3 @haveibeenpwned]

Get all breaches of an e-mail address [v3 @haveibeenpwned]

Get all breaches of an e-mail address [v3 @haveibeenpwned]

Get all breaches of an e-mail address [v3 @haveibeenpwned]

Get all pastes featuring the e-mail address [v3 @haveibeenpwned]

Get all breaches of an e-mail address [v3 @haveibeenpwned]

Get all breaches of an e-mail address [v3 @haveibeenpwned]



@haveibeenpwned - Not Listed wi...



OnlinerSpambot



PDL



deezer.com



linkedin.com



apollo.io



gravatar.com



dropbox.com



houzz.com



epik.com



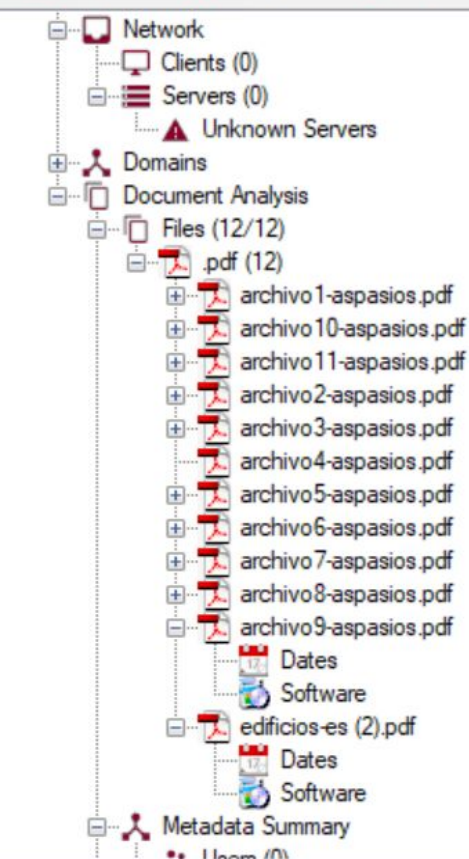
bitly.com



moneybookers.com

Foca - Obtención y Análisis de Metadatos

La herramienta Foca, se usa principalmente para encontrar archivos desarrollados por nuestro objetivo y para analizar los metadatos que contienen esos archivos. Luego de utilizar esta herramienta, encontramos 12 archivos .pdf, que al extraer sus metadatos nos arrojó 2 tipos de información. El primer tipo de información, es el tipo de software que se usó para crear ó modificar esos archivos, y el segundo son las fechas de creación y modificación de esos archivos. En esta ocasión no nos devolvió información como nombres de usuarios o geolocalización, porque seguramente borraron estos metadatos, antes de subirlos a sus páginas web. Se puede ver en la siguiente imagen un resumen de los 6 softwares que se usaron.



Attribute

Value

All software found (6) - Times found

Software	Adobe InDesign CS6 (Macintosh)
Software	Adobe PDF Library 10.0.1
Software	Adobe InDesign CC 2017 (Macintosh)
Software	Adobe InDesign 15.0 (Macintosh)
Software	Adobe PDF Library 15.0
Software	iLovePDF

Conclusiones

Luego de utilizar todas estas herramientas de recopilación de información OSINT, obtuvimos mucha información pública valiosa sobre distintos dominios asociados a nuestro objetivo. Recolectamos distintas direcciones de correos electrónicos, que luego podremos intentar vulnerar. Logramos obtener también, distintos links de acceso de administradores, que con la aplicación de técnicas que veremos a futuro, pueden hacer que logremos hacernos con el control de las páginas web o aplicaciones de nuestro objetivo.