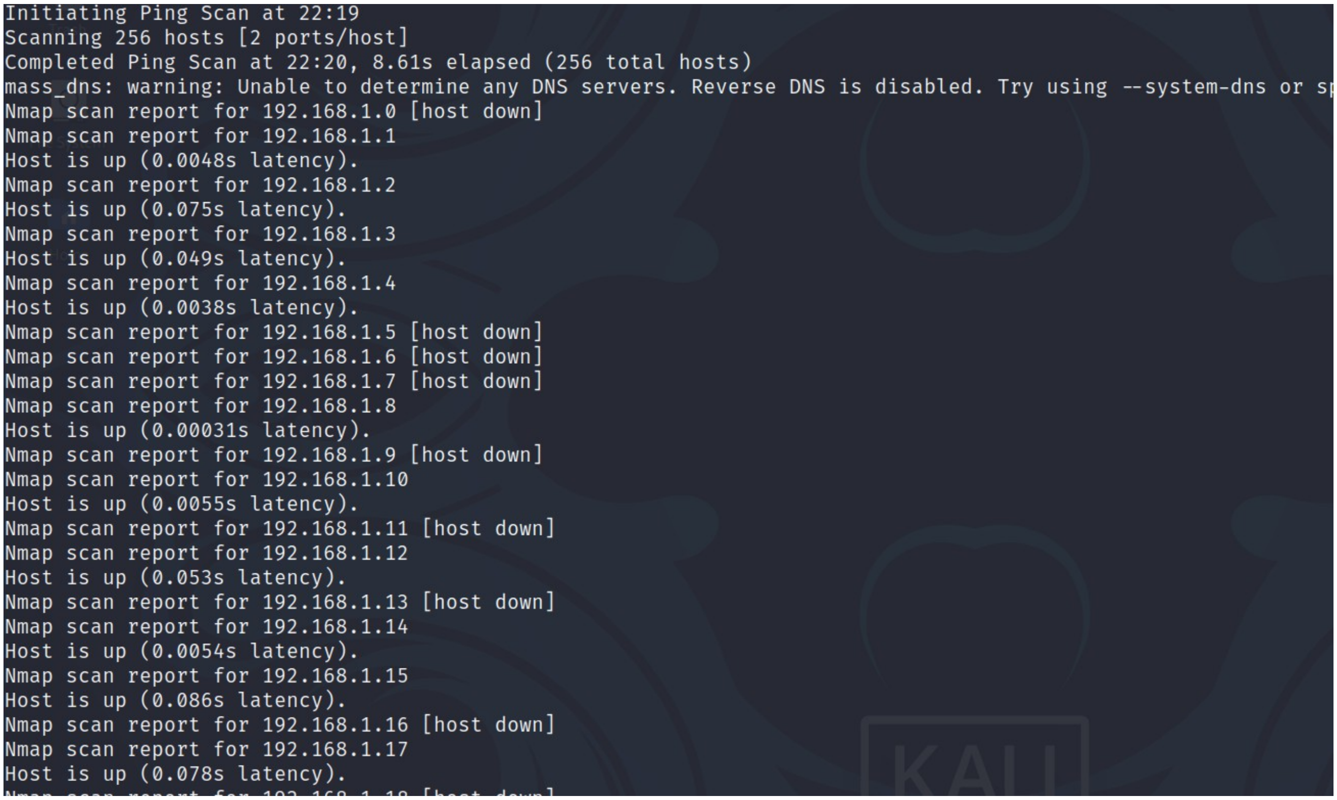
Reto 1

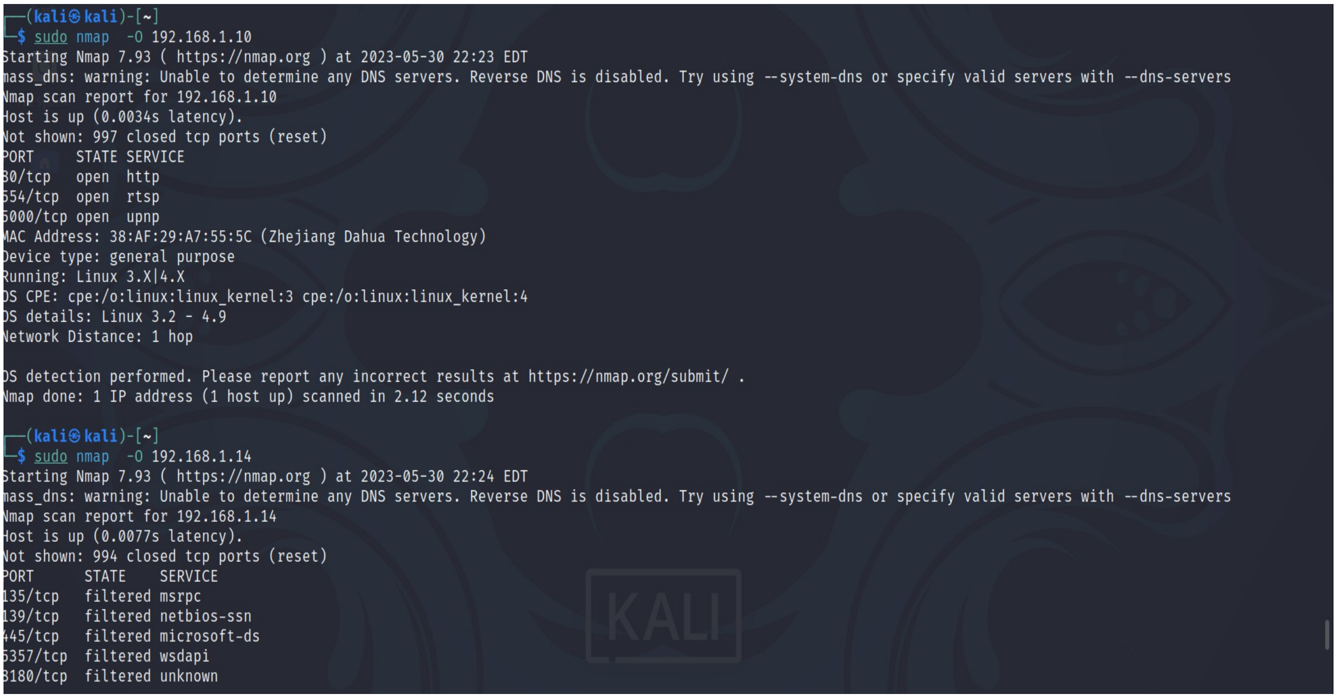
Nombre: Iván Zabdiel Díaz Sotelo.

Escaneo de host activos dentro de el mismo segmento de red de Kali linux



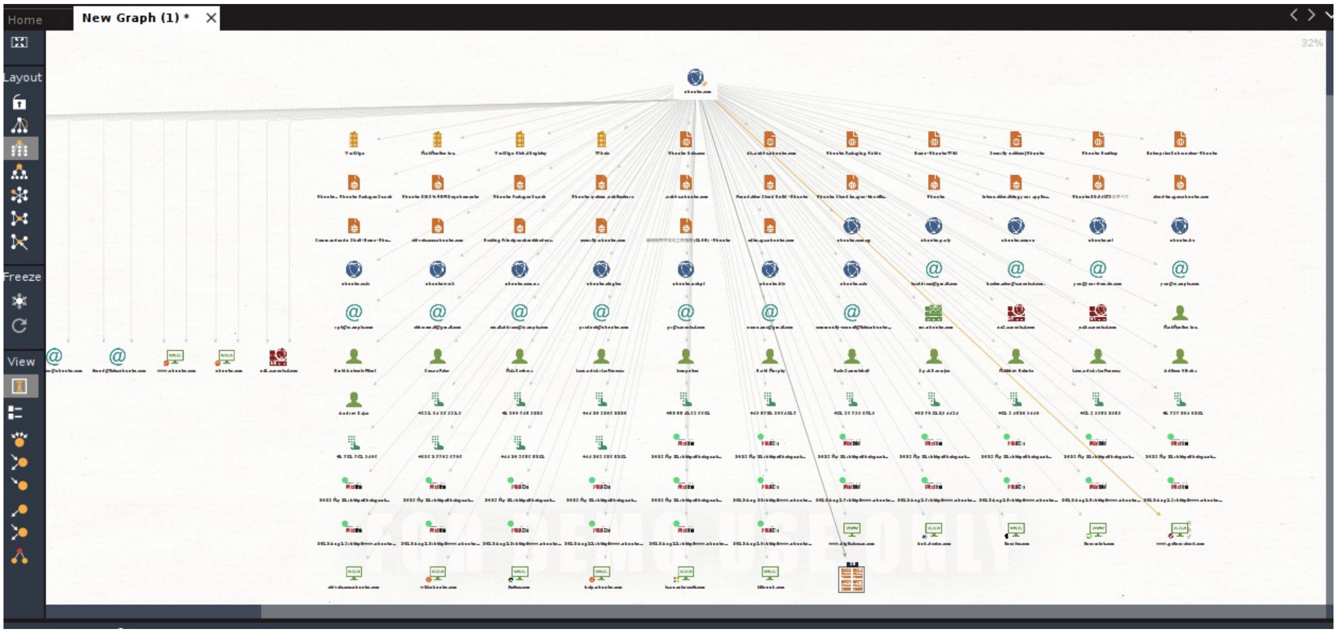
```
Initiating Ping Scan at 22:19
Scanning 256 hosts [2 ports/host]
Completed Ping Scan at 22:20, 8.61s elapsed (256 total hosts)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or sp
Nmap scan report for 192.168.1.0 [host down]
Nmap scan report for 192.168.1.1
Host is up (0.0048s latency).
Nmap scan report for 192.168.1.2
Host is up (0.075s latency).
Nmap scan report for 192.168.1.3
Host is up (0.049s latency).
Nmap scan report for 192.168.1.4
Host is up (0.0038s latency).
Nmap scan report for 192.168.1.5 [host down]
Nmap scan report for 192.168.1.6 [host down]
Nmap scan report for 192.168.1.7 [host down]
Nmap scan report for 192.168.1.8
Host is up (0.00031s latency).
Nmap scan report for 192.168.1.9 [host down]
Nmap scan report for 192.168.1.10
Host is up (0.0055s latency).
Nmap scan report for 192.168.1.11 [host down]
Nmap scan report for 192.168.1.12
Host is up (0.053s latency).
Nmap scan report for 192.168.1.13 [host down]
Nmap scan report for 192.168.1.14
Host is up (0.0054s latency).
Nmap scan report for 192.168.1.15
Host is up (0.086s latency).
Nmap scan report for 192.168.1.16 [host down]
Nmap scan report for 192.168.1.17
Host is up (0.078s latency).
Nmap scan report for 192.168.1.18 [host down]
```

Escaneo de puertos de algunos de los host activos. Como se puede ver se encontro un dispositivo Dahua conocido por la fabricación de camaras de CCTV

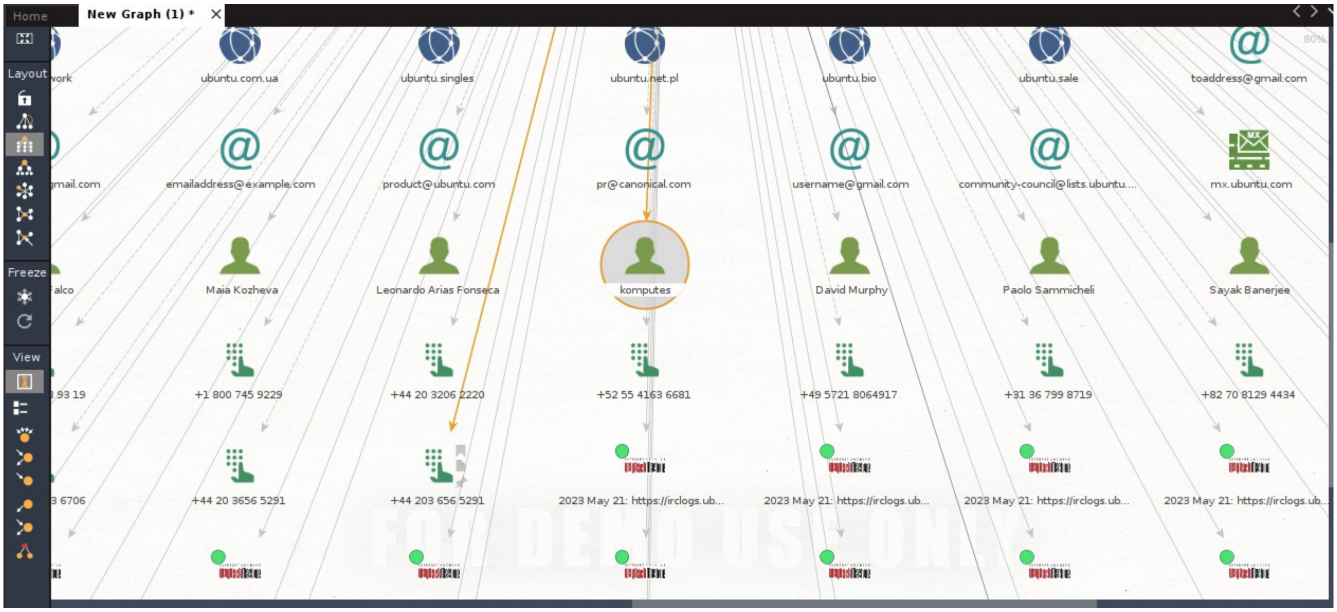


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap  -O 192.168.1.10
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-30 22:23 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.10
Host is up (0.0034s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
554/tcp  open  rtsp
5000/tcp open  upnp
MAC Address: 38:AF:29:A7:55:5C (Zhejiang Dahua Technology)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.12 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap  -O 192.168.1.14
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-30 22:24 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.14
Host is up (0.0077s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE    SERVICE
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
5357/tcp  filtered wsdapi
8180/tcp  filtered unknown
```

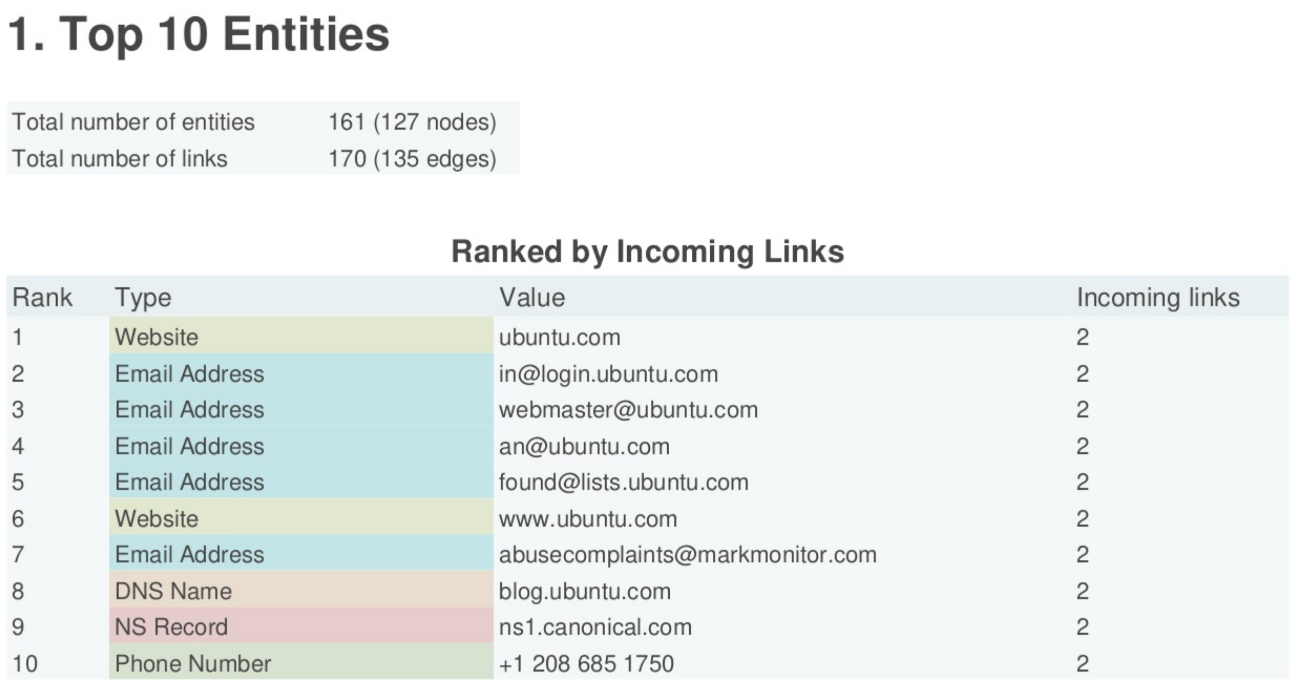
Transformacion aplicada a la web de Canonical (Ubuntu) con la herramienta de Maltego.



Como se puede ver se encotraron diversos numeros de contacto, correo y nombres públicos.



Reporte exportado por la herraminta Maltego.

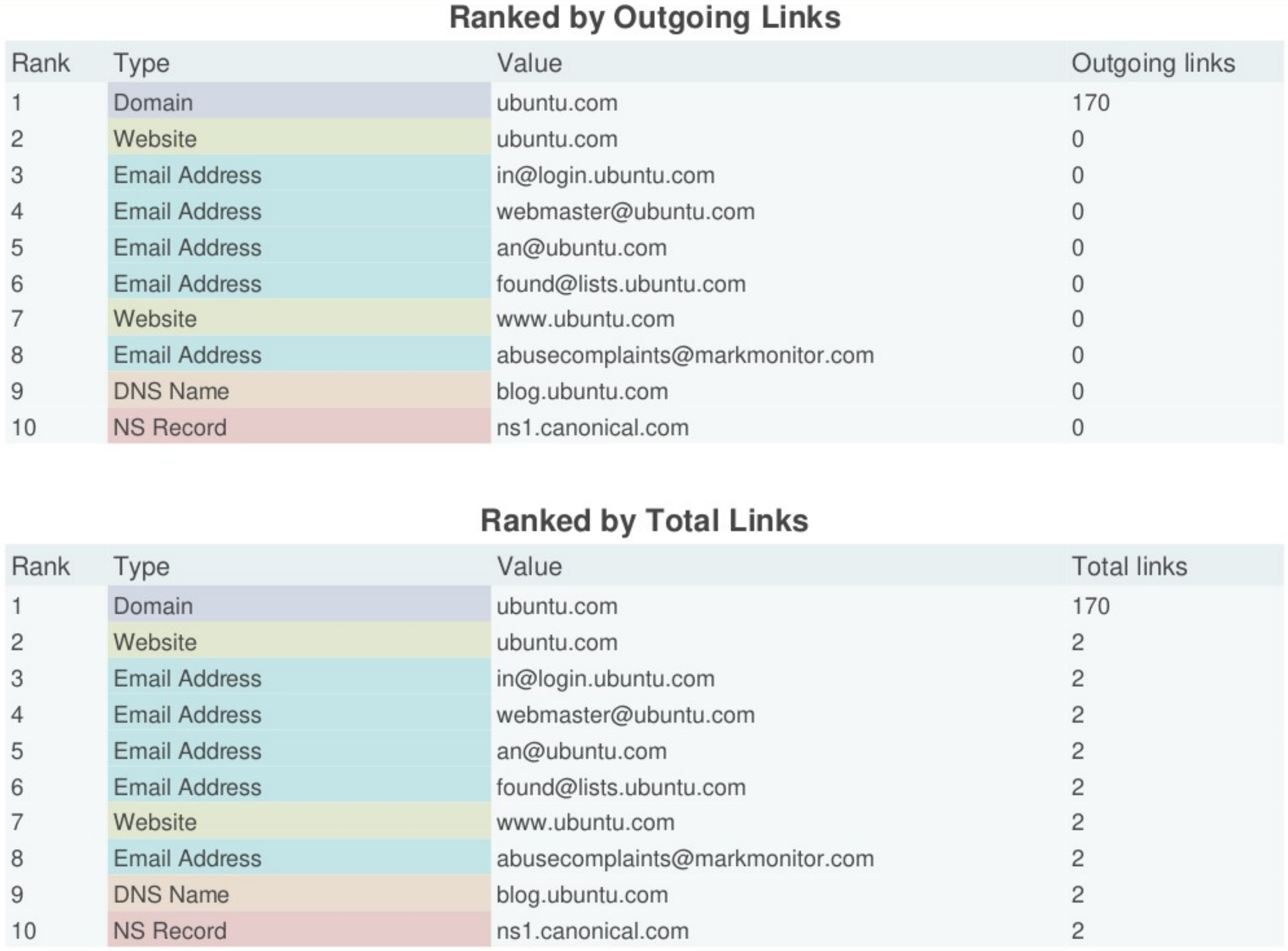


1. Top 10 Entities

Total number of entities	161 (127 nodes)
Total number of links	170 (135 edges)

Ranked by Incoming Links

Rank	Type	Value	Incoming links
1	Website	ubuntu.com	2
2	Email Address	in@login.ubuntu.com	2
3	Email Address	webmaster@ubuntu.com	2
4	Email Address	an@ubuntu.com	2
5	Email Address	found@lists.ubuntu.com	2
6	Website	www.ubuntu.com	2
7	Email Address	abusecomplaints@markmonitor.com	2
8	DNS Name	blog.ubuntu.com	2
9	NS Record	ns1.canonical.com	2
10	Phone Number	+1 208 685 1750	2



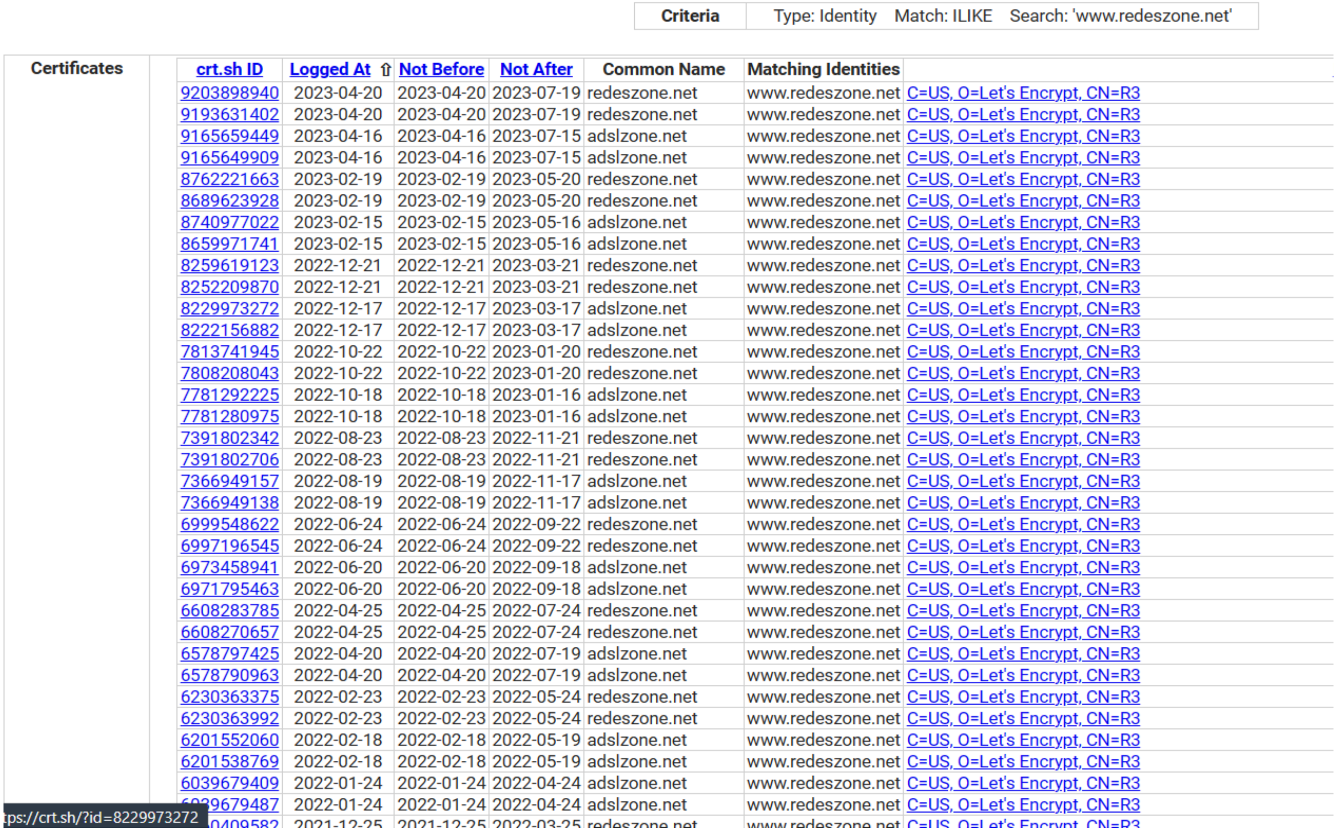
Ranked by Outgoing Links

Rank	Type	Value	Outgoing links
1	Domain	ubuntu.com	170
2	Website	ubuntu.com	0
3	Email Address	in@login.ubuntu.com	0
4	Email Address	webmaster@ubuntu.com	0
5	Email Address	an@ubuntu.com	0
6	Email Address	found@lists.ubuntu.com	0
7	Website	www.ubuntu.com	0
8	Email Address	abusecomplaints@markmonitor.com	0
9	DNS Name	blog.ubuntu.com	0
10	NS Record	ns1.canonical.com	0

Ranked by Total Links

Rank	Type	Value	Total links
1	Domain	ubuntu.com	170
2	Website	ubuntu.com	2
3	Email Address	in@login.ubuntu.com	2
4	Email Address	webmaster@ubuntu.com	2
5	Email Address	an@ubuntu.com	2
6	Email Address	found@lists.ubuntu.com	2
7	Website	www.ubuntu.com	2
8	Email Address	abusecomplaints@markmonitor.com	2
9	DNS Name	blog.ubuntu.com	2
10	NS Record	ns1.canonical.com	2

Escaneo de certificaciones de un blog hecho con la página crt.sh

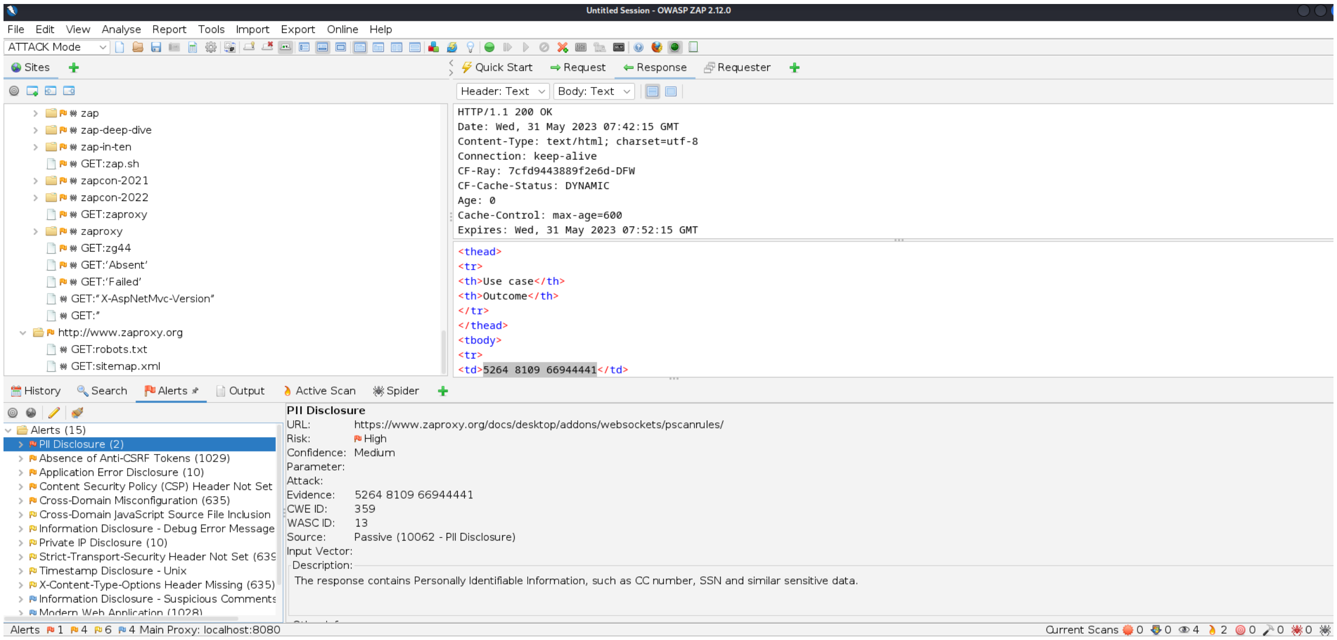


Criteria	Type: Identity Match: ILIKE Search: 'www.redeszone.net'

Certificates	crt.sh ID	Logged At ⇧	Not Before	Not After	Common Name	Matching Identities	
	9203898940	2023-04-20	2023-04-20	2023-07-19	redeszone.net	www.redeszone.net	C=US, O=Let's Encrypt, CN=R3
	9193631402	2023-04-20	2023-04-20	2023-07-19	redeszone.net	www.redeszone.net	C=US, O=Let's Encrypt, CN=R3
	9165659449	2023-04-16	2023-04-16	2023-07-15	adslzone.net	www.redeszone.net	C=US, O=Let's Encrypt, CN=R3
	9165649909	2023-04-16	2023-04-16	2023-07-15	adslzone.net	www.redeszone.net	C=US, O=Let's Encrypt, CN=R3
	8762221663	2023-02-19	2023-02-19	2023-05-20	redeszone.net	www.redeszone.net	C=US, O=Let's Encrypt, CN=R3
	8689623928	2023-02-19	2023-02-19	2023-05-20	redeszone.net	www.redeszone.net	C=US, O=Let's Encrypt, CN=R3
	8740977022	2023-02-15	2023-02-15	2023-05-16	adslzone.net	www.redeszone.net	C=US, O=Let's Encrypt, CN=R3
	8659971741	2023-02-15	2023-02-15	2023-05-16	adslzone.net	www.redeszone.net	C=US, O=Let's Encrypt, CN=R3
	8259619123	2022-12-21	2022-12-21	2023-03-21	redeszone.net	www.redeszone.net	C=US, O=Let's Encrypt, CN=R3
	8252209870	2022-12-21	2022-12-21	2023-03-21	redeszone.net	www.redeszone.net	C=US, O=Let's Encrypt, CN=R3
	8229973272	2022-12-17	2022-12-17	2023-03-17	adslzone.net	www.redeszone.net	C=US, O=Let's Encrypt, CN=R3
	8222156882	2022-12-17	2022-12-17	2023-03-17	adslzone.net	www.redeszone.net	C=US, O=Let's Encrypt, CN=R3
	7813741945	2022-10-22	2022-10-22	2023-01-20	redeszone.net	www.redeszone.net	C=US, O=Let's Encrypt, CN=R3
	7808208043	2022-10-22	2022-10-22	2023-01-20	redeszone.net	www.redeszone.net	C=US, O=Let's Encrypt, CN=R3
	7781292225	2022-10-18	2022-10-18	2023-01-16	adslzone.net	www.redeszone.net	C=US, O=Let's Encrypt, CN=R3
	7781280975	2022-10-18	2022-10-18	2023-01-16	adslzone.net	www.redeszone.net	C=US, O=Let's Encrypt, CN=R3
	7391802342	2022-08-23	2022-08-23	2022-11-21	redeszone.net	www.redeszone.net	C=US, O=Let's Encrypt, CN=R3
	7391802706	2022-08-23	2022-08-23	2022-11-21	redeszone.net	www.redeszone.net	C=US, O=Let's Encrypt, CN=R3
	7366949157	2022-08-19	2022-08-19	2022-11-17	adslzone.net	www.redeszone.net	C=US, O=Let's Encrypt, CN=R3
	7366949138	2022-08-19	2022-08-19	2022-11-17	adslzone.net	www.redeszone.net	C=US, O=Let's Encrypt, CN=R3
	6999548622	2022-06-24	2022-06-24	2022-09-22	redeszone.net	www.redeszone.net	C=US, O=Let's Encrypt, CN=R3
	6997196545	2022-06-24	2022-06-24	2022-09-22	redeszone.net	www.redeszone.net	C=US, O=Let's Encrypt, CN=R3
	6973458941	2022-06-20	2022-06-20	2022-09-18	adslzone.net	www.redeszone.net	C=US, O=Let's Encrypt, CN=R3
	6971795463	2022-06-20	2022-06-20	2022-09-18	adslzone.net	www.redeszone.net	C=US, O=Let's Encrypt, CN=R3
	6608283785	2022-04-25	2022-04-25	2022-07-24	redeszone.net	www.redeszone.net	C=US, O=Let's Encrypt, CN=R3
	6608270657	2022-04-25	2022-04-25	2022-07-24	redeszone.net	www.redeszone.net	C=US, O=Let's Encrypt, CN=R3
	6578797425	2022-04-20	2022-04-20	2022-07-19	adslzone.net	www.redeszone.net	C=US, O=Let's Encrypt, CN=R3
	6578790963	2022-04-20	2022-04-20	2022-07-19	adslzone.net	www.redeszone.net	C=US, O=Let's Encrypt, CN=R3
	6230363375	2022-02-23	2022-02-23	2022-05-24	redeszone.net	www.redeszone.net	C=US, O=Let's Encrypt, CN=R3
	6230363992	2022-02-23	2022-02-23	2022-05-24	redeszone.net	www.redeszone.net	C=US, O=Let's Encrypt, CN=R3
	6201552060	2022-02-18	2022-02-18	2022-05-19	adslzone.net	www.redeszone.net	C=US, O=Let's Encrypt, CN=R3
	6201538769	2022-02-18	2022-02-18	2022-05-19	adslzone.net	www.redeszone.net	C=US, O=Let's Encrypt, CN=R3
	6039679409	2022-01-24	2022-01-24	2022-04-24	adslzone.net	www.redeszone.net	C=US, O=Let's Encrypt, CN=R3
	6039679487	2022-01-24	2022-01-24	2022-04-24	adslzone.net	www.redeszone.net	C=US, O=Let's Encrypt, CN=R3
	0409582	2021-12-25	2021-12-25	2022-03-25	redeszone.net	www.redeszone.net	C=US, O=Let's Encrypt, CN=R3

tps://crt.sh/?id=8229973272

Escaneo de vulnerabilidade a la página de OWASAP con la misma herramienta.



```
zap
zap-deep-dive
zap-in-ten
GET:zap.sh
zapcon-2021
zapcon-2022
GET:zaproxy
zaproxy
GET:zg44
GET:'Absent'
GET:'Failed'
GET:"X-AspNetMvc-Version"
GET:"
http://www.zaproxy.org
GET:robots.txt
GET:sitemap.xml
```

```
HTTP/1.1 200 OK
Date: Wed, 31 May 2023 07:42:15 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
CF-Ray: 7cfd9443889f2e6d-DFW
CF-Cache-Status: DYNAMIC
Age: 0
Cache-Control: max-age=600
Expires: Wed, 31 May 2023 07:52:15 GMT
```

```
<thead>
<tr>
<th>Use case</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>5264 8109 66944441</td>
```

Alerts (15)
- PII Disclosure (2)
- Absence of Anti-CSRF Tokens (1029)
- Application Error Disclosure (10)
- Content Security Policy (CSP) Header Not Set
- Cross-Domain Misconfiguration (635)
- Cross-Domain JavaScript Source File Inclusion
- Information Disclosure - Debug Error Message
- Private IP Disclosure (10)
- Strict-Transport-Security Header Not Set (639
- Timestamp Disclosure - Unix
- X-Content-Type-Options Header Missing (635)
- Information Disclosure - Suspicious Comments
- Modern Web Application (1028)

PII Disclosure

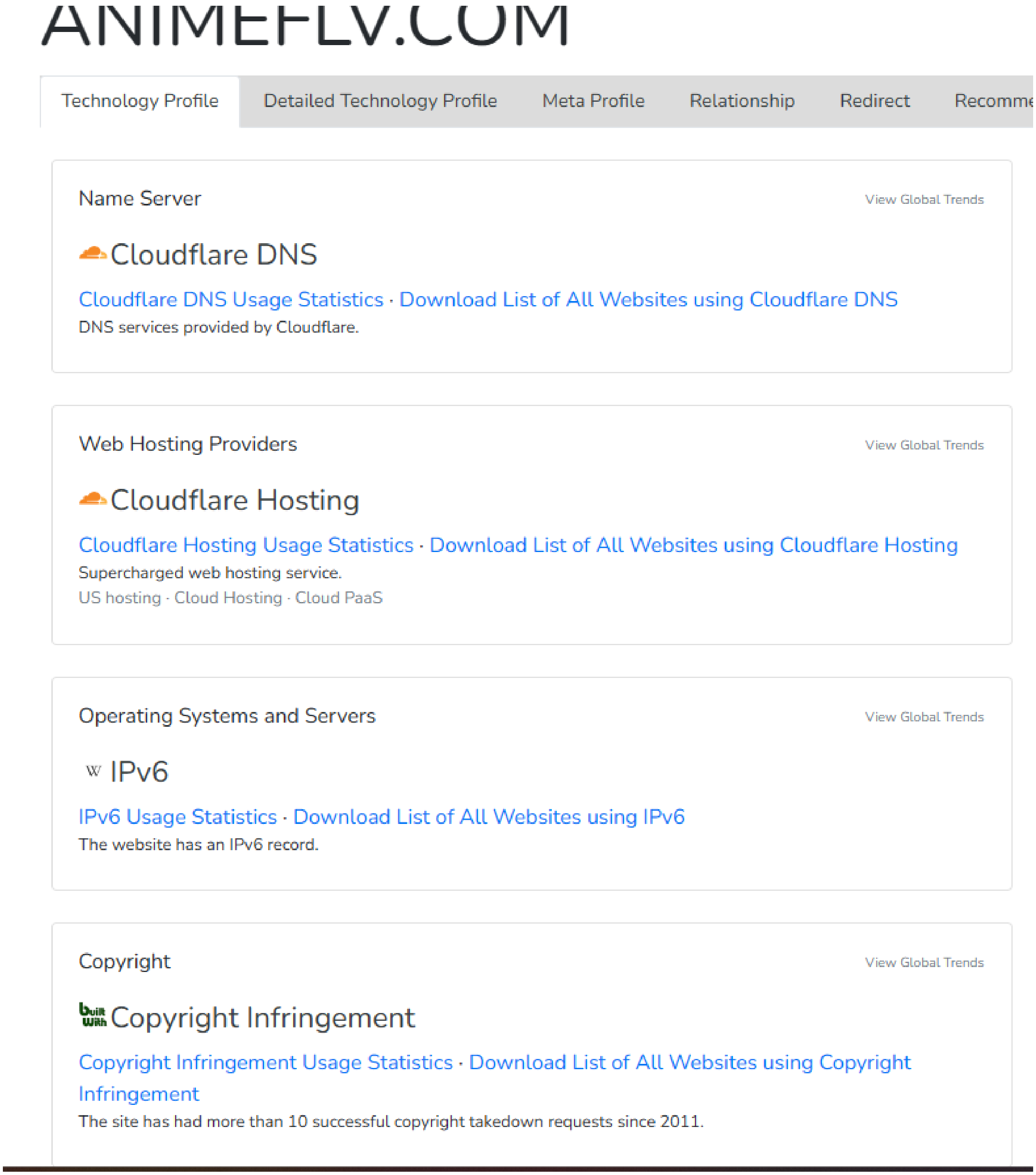
URL:	https://www.zaproxy.org/docs/desktop/addons/websockets/pscanrules/
Risk:	High
Confidence:	Medium
Parameter:	
Attack:	
Evidence:	5264 8109 66944441
CWE ID:	359
WASC ID:	13
Source:	Passive (10062 - PII Disclosure)
Input Vector:	

Description:
The response contains Personally Identifiable Information, such as CC number, SSN and similar sensitive data.

Alerts 1 4 6 4 Main Proxy: localhost:8080

Current Scans 0 0 4 2 0 0 0

Escaneo de herramientas con las que esta construida la web anime.flv popular para ver series animadas japonesas de forma pirata.



ANIMEFLV.COM

Name Server

View Global Trends

Cloudflare DNS

Cloudflare DNS Usage Statistics · Download List of All Websites using Cloudflare DNS

DNS services provided by Cloudflare.

Web Hosting Providers

View Global Trends

Cloudflare Hosting

Cloudflare Hosting Usage Statistics · Download List of All Websites using Cloudflare Hosting

Supercharged web hosting service.

US hosting · Cloud Hosting · Cloud PaaS

Operating Systems and Servers

View Global Trends

IPv6

IPv6 Usage Statistics · Download List of All Websites using IPv6

The website has an IPv6 record.

Copyright

View Global Trends

Copyright Infringement

Copyright Infringement Usage Statistics · Download List of All Websites using Copyright Infringement

The site has had more than 10 successful copyright takedown requests since 2011.