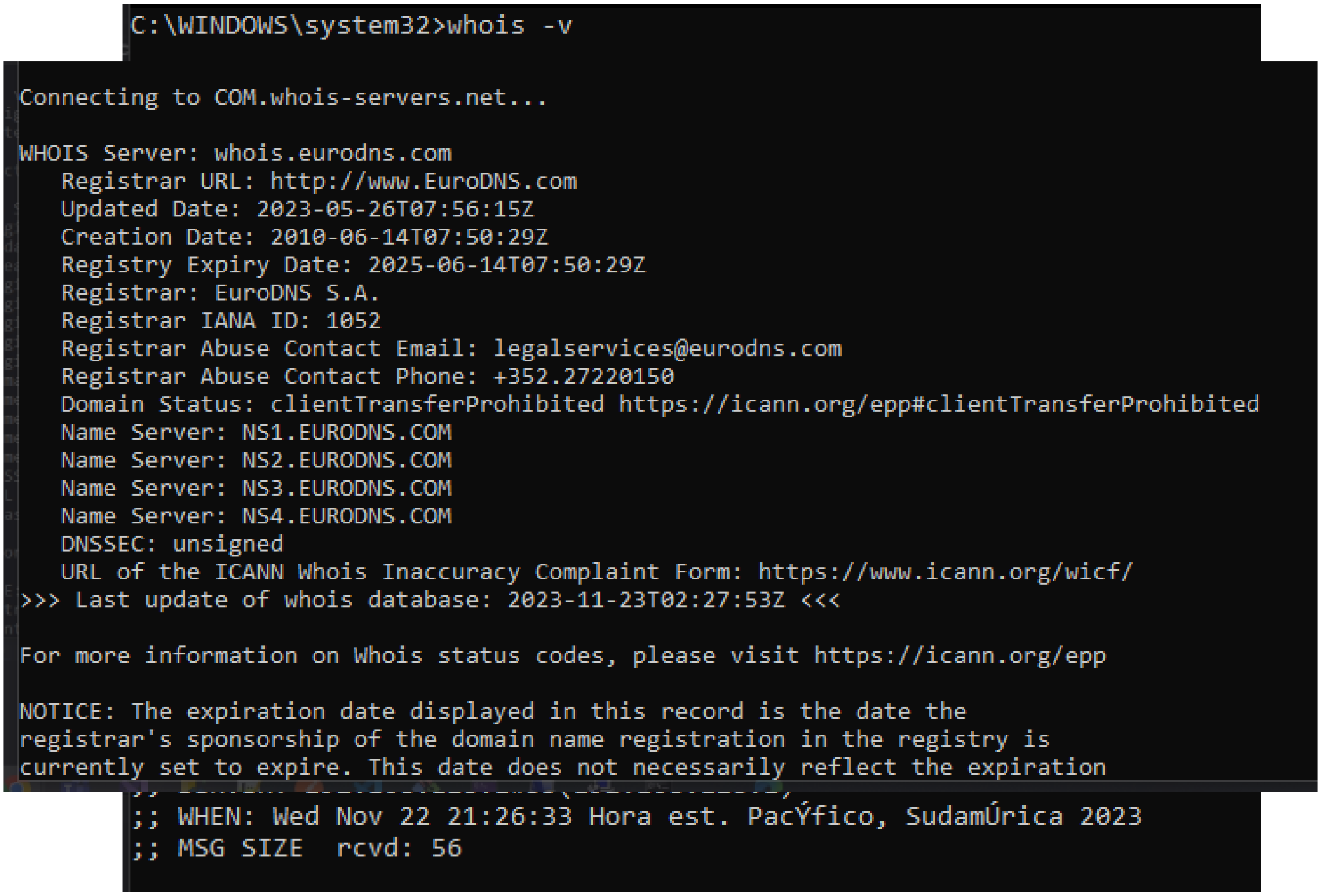
Desafio 10

1. Dig y whois

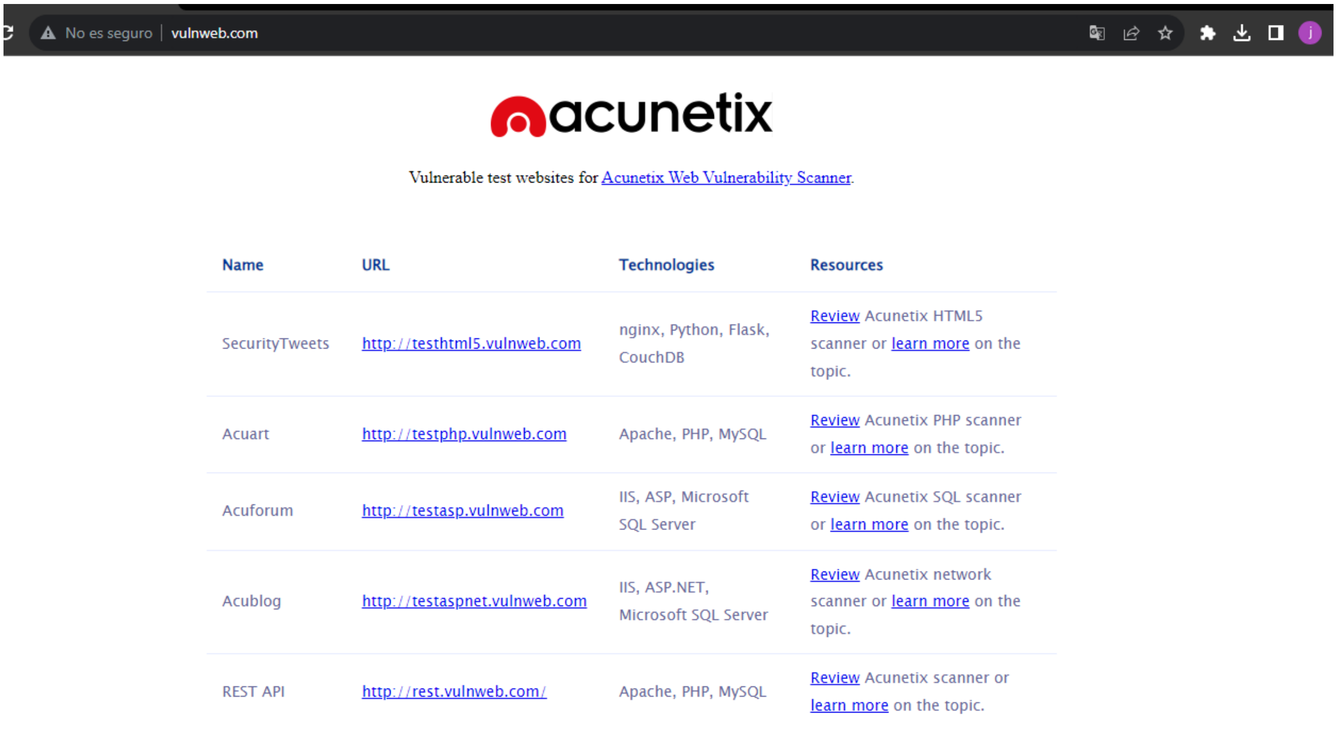


```
C:\WINDOWS\system32>whois -v
```

```
Connecting to COM.whois-servers.net...

WHOIS Server: whois.eurodns.com
   Registrar URL: http://www.EuroDNS.com
   Updated Date: 2023-05-26T07:56:15Z
   Creation Date: 2010-06-14T07:50:29Z
   Registry Expiry Date: 2025-06-14T07:50:29Z
   Registrar: EuroDNS S.A.
   Registrar IANA ID: 1052
   Registrar Abuse Contact Email: legalservices@eurodns.com
   Registrar Abuse Contact Phone: +352.27220150
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: NS1.EURODNS.COM
   Name Server: NS2.EURODNS.COM
   Name Server: NS3.EURODNS.COM
   Name Server: NS4.EURODNS.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-11-23T02:27:53Z <<<

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

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
```

```
;; WHEN: Wed Nov 22 21:26:33 Hora est. PacÝfico, SudamÚrica 2023
;; MSG SIZE  rcvd: 56
```

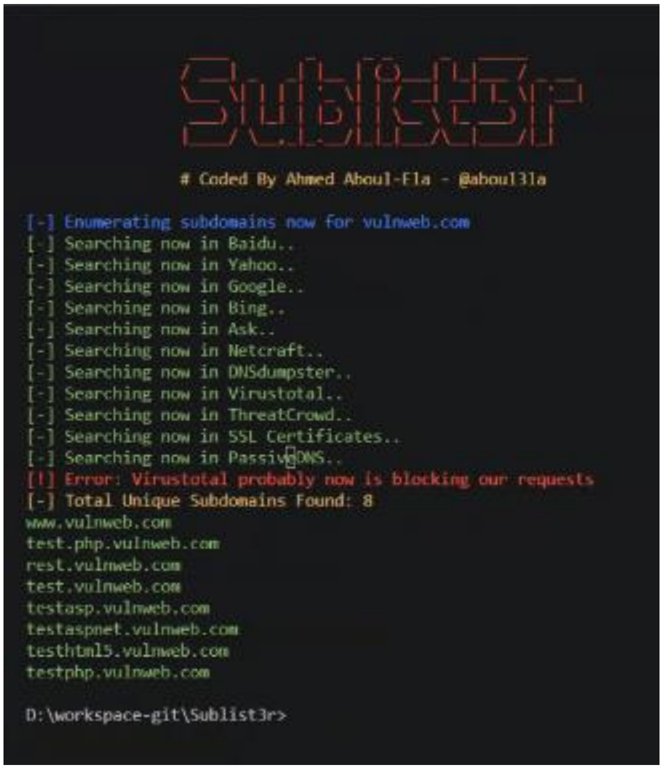
Dominio Vulnweb



Vulnerable test websites for Acunetix Web Vulnerability Scanner.

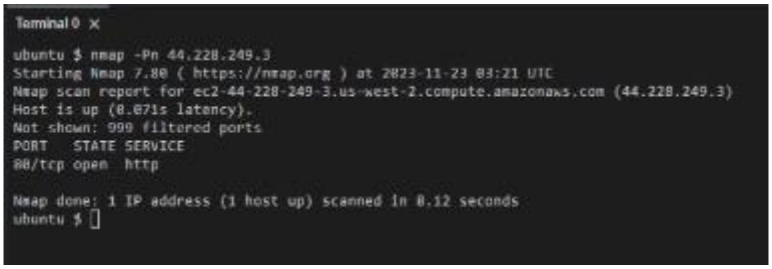
Name	URL	Technologies	Resources
SecurityTweets	http://testhtml5.vulnweb.com	nginx, Python, Flask, CouchDB	Review Acunetix HTML5 scanner or learn more on the topic.
Acuart	http://testphp.vulnweb.com	Apache, PHP, MySQL	Review Acunetix PHP scanner or learn more on the topic.
Acuforum	http://testasp.vulnweb.com	IIS, ASP, Microsoft SQL Server	Review Acunetix SQL scanner or learn more on the topic.
Acublog	http://testaspnet.vulnweb.com	IIS, ASP.NET, Microsoft SQL Server	Review Acunetix network scanner or learn more on the topic.
REST API	http://rest.vulnweb.com/	Apache, PHP, MySQL	Review Acunetix scanner or learn more on the topic.

3 Sitios web hosteados



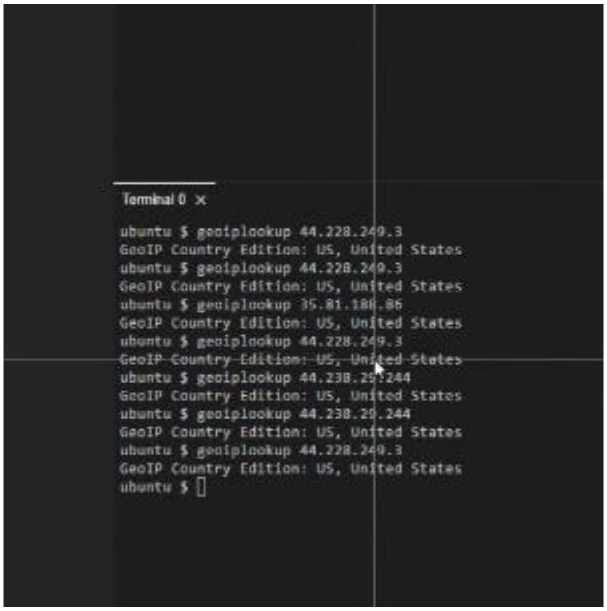
```
                 # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for vulnweb.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 8
www.vulnweb.com
test.php.vulnweb.com
rest.vulnweb.com
test.vulnweb.com
testasp.vulnweb.com
testaspnet.vulnweb.com
testhtml5.vulnweb.com
testphp.vulnweb.com

D:\workspace-git\Sublist3r>
```

5 direccion Ip



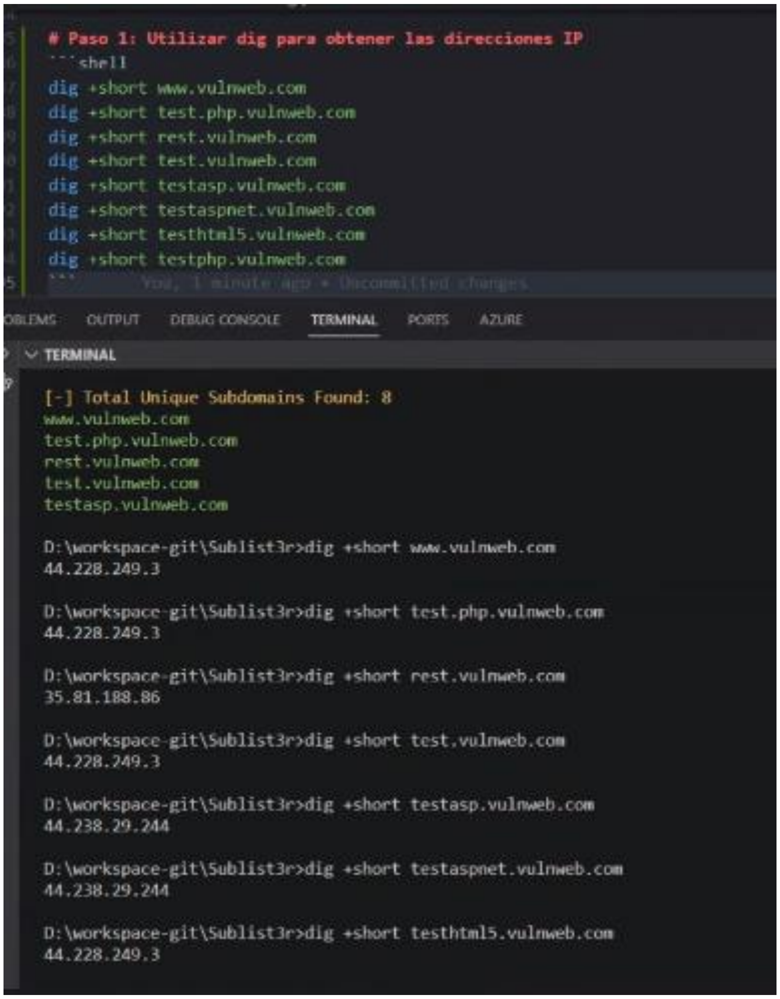
```
ubuntu $ nmap -Pn 44.228.249.3
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-23 03:21 UTC
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.071s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
ubuntu $
```

6. Geo IP



```
ubuntu $ geoiplookup 44.228.249.3
GeoIP Country Edition: US, United States
ubuntu $ geoiplookup 44.228.249.3
GeoIP Country Edition: US, United States
ubuntu $ geoiplookup 35.81.188.86
GeoIP Country Edition: US, United States
ubuntu $ geoiplookup 44.228.249.3
GeoIP Country Edition: US, United States
ubuntu $ geoiplookup 44.238.29.244
GeoIP Country Edition: US, United States
ubuntu $ geoiplookup 44.238.29.244
GeoIP Country Edition: US, United States
ubuntu $ geoiplookup 44.228.249.3
GeoIP Country Edition: US, United States
ubuntu $
```

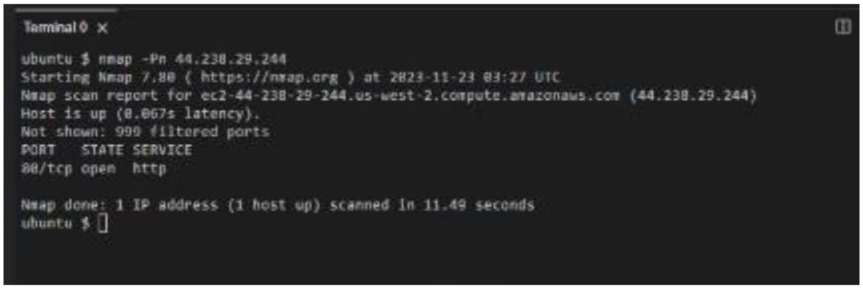
7. Geolocalizacion de cada Ip



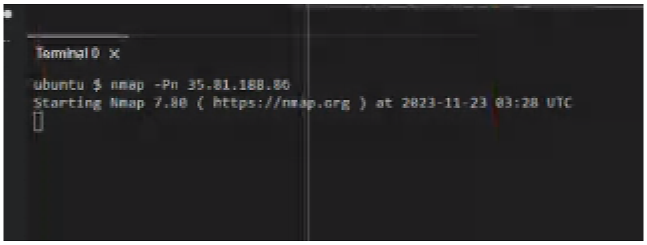
~~~
# Paso 1: Utilizar dig para obtener las direcciones IP
```shell
dig +short www.vulnweb.com
dig +short test.php.vulnweb.com
dig +short rest.vulnweb.com
dig +short test.vulnweb.com
dig +short testasp.vulnweb.com
dig +short testaspnet.vulnweb.com
dig +short testhtml5.vulnweb.com
dig +short testphp.vulnweb.com
```
~~~

```
[-] Total Unique Subdomains Found: 8
www.vulnweb.com
test.php.vulnweb.com
rest.vulnweb.com
test.vulnweb.com
testasp.vulnweb.com

D:\workspace-git\Sublist3r>dig +short www.vulnweb.com
44.228.249.3

D:\workspace-git\Sublist3r>dig +short test.php.vulnweb.com
44.228.249.3

D:\workspace-git\Sublist3r>dig +short rest.vulnweb.com
35.81.188.86

D:\workspace-git\Sublist3r>dig +short test.vulnweb.com
44.228.249.3

D:\workspace-git\Sublist3r>dig +short testasp.vulnweb.com
44.238.29.244

D:\workspace-git\Sublist3r>dig +short testaspnet.vulnweb.com
44.238.29.244

D:\workspace-git\Sublist3r>dig +short testhtml5.vulnweb.com
44.228.249.3
```

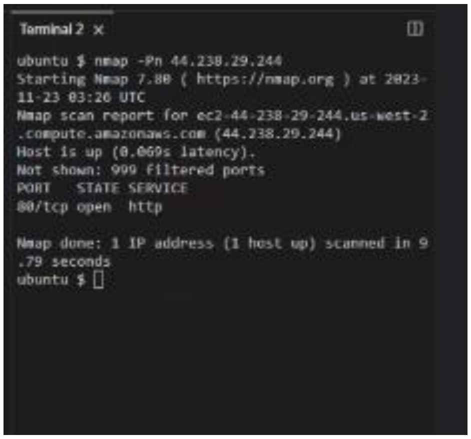
8. nmap



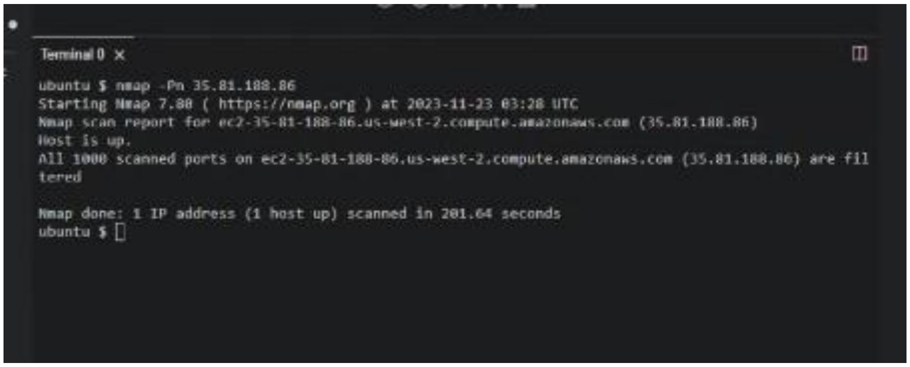
```
ubuntu $ nmap -Pn 44.238.29.244
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-23 03:27 UTC
Nmap scan report for ec2-44-238-29-244.us-west-2.compute.amazonaws.com (44.238.29.244)
Host is up (0.067s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 11.49 seconds
ubuntu $ 
```



```
ubuntu $ nmap -Pn 35.81.188.86
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-23 03:28 UTC
```



```
ubuntu $ nmap -Pn 44.238.29.244
Starting Nmap 7.80 ( https://nmap.org ) at 2023-
11-23 03:26 UTC
Nmap scan report for ec2-44-238-29-244.us-west-2
.compute.amazonaws.com (44.238.29.244)
Host is up (0.069s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 9
.79 seconds
ubuntu $
```



```
ubuntu $ nmap -Pn 35.81.188.86
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-23 03:28 UTC
Nmap scan report for ec2-35-81-188-86.us-west-2.compute.amazonaws.com (35.81.188.86)
Host is up.
All 1000 scanned ports on ec2-35-81-188-86.us-west-2.compute.amazonaws.com (35.81.188.86) are fil
tered

Nmap done: 1 IP address (1 host up) scanned in 201.64 seconds
ubuntu $
```

Conclusion: En base a los resultados obtenidos, se ha identificado que los sitios web alojados en 'vulnweb.com' tienen ciertos riesgos de seguridad, como la exposición de información sensible en puertos abiertos. Esto podría proporcionar una superficie de ataque potencial para ataques como escaneo de puertos y posibles vulnerabilidades. Se recomienda una revisión más detallada de la configuración de seguridad y la implementación de medidas para mitigar posibles amenazas."