

10 [OSINT] Reconocimiento de dominios por terminal y scripting

Instalar Amass

- `sudo apt update && sudo apt install amass`

Si este comando no funciona, puede utilizar el siguiente comando para descargar:

- `sudo apt update && sudo snap install amass`

```
ub@ub:~$ sudo snap install amass
amass v3.19.2 desde Jeff Foley (caffix) installed
```

Comprueba la versión para verificar si la instalación se ha completado correctamente

- `amass version`

```
ub@ub:~$ amass version

.+++..
+W@#@#@#@#@
&@#+ .o@#.#.
+@& &@& #@@ +@W@&@&@+
8@ @ 8@o 8@& WW .@W W@+ .@W.
WW &@o &@: o@+ o@+ #@. 8@o +W@#+.
#@ :@W &@+ &@+ @& :@o o@o oW@W@W+
o@+ @@& &@+ &@+ #@ &@. .W@W .+@&
WW +@W@&. &@+ :& o@+ #@ :@W&@& &@:
:@W: o@# +Wo &@+ :W: +@W&o++o@W. &@& 8@#o+&@W.
:W@W@W@W@W@&@& + :&W@#@#@& &W .o#@@W&.
+o&&&&&+.

v3.19.2
OWASP Amass Project - @owaspamass
In-depth Attack Surface Mapping and Asset Discovery

Usage: amass intel|enum|viz|track|db [options]

-h Show the program usage message
-help Show the program usage message
-version Print the version number of this Amass binary
```

Uso básico (modo pasivo)

- `amass enum -passive -d ejemplo.com`

```
ub@ub:~$ amass enum -passive -d ejemplo.com
ejemplo.com

The enumeration has finished
Discoveries are being migrated into the local database
```

Uso con salida a archivo

Esto es clave para:

- Documentar
- Analizar después
- Usar como entrada para otras herramientas

```

ub@ub:~$ amass enum -passive -d ejemplo.com -o subdominios.txt
workspace.ejemplo.com
ns.ejemplo.com
suempresa.ejemplo.com
smtp.ejemplo.com
imap.ejemplo.com
www.ejemplo.com
auth.ejemplo.com
owa.ejemplo.com
seguimiento.ejemplo.com
tienda.ejemplo.com
deathstar.ejemplo.com
hotmail.ejemplo.com
sql.ejemplo.com
smt.ejemplo.com
4.ejemplo.com
ejemplo.ejemplo.com
estelinknosirve.ejemplo.com
otro.ejemplo.com
hatt.www.ejemplo.com
sitio.ejemplo.com
cdn.ejemplo.com

```

Enumeración con múltiples dominios

Crea el archivo de dominio

- sudo nano dominios.txt

```

ub@ub:~$ sudo nano dominios.txt
[sudo] contraseña para ub:

```

```

GNU nano 7.2 dominios.txt
ejemplo.com
ejemplo.org
ejemplo.net

```

- amass enum -passive -df dominios.txt -o resultados.txt

```

ub@ub:~$ amass enum -passive -df dominios.txt -o resultados.txt
docs.ejemplo.com
remote.ejemplo.com
estelinknosirve.ejemplo.com
auth.ejemplo.com
xn--pgina-xqa.ejemplo.com
suempresa.ejemplo.com
ww1.ejemplo.com
smt.ejemplo.com
yourcompany.ejemplo.com
sip.ejemplo.com
subdominio.ejemplo.com
my.ejemplo.com

```

Instalar Subfinder

- ```
ub@ub:~$ sudo snap install subfinder
```

```
ub@ub:~$ subfinder -d ejemplo.com
```



projectdiscovery.io

```
[INF] Current subfinder version v2.10.1 (latest)
[INF] Loading provider config from /home/ub/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for ejemplo.com
post.hotmail.ejemplo.com
www2.hotmail.ejemplo.com
www.es.ejemplo.com
api.ejemplo.com
foro.ejemplo.com
www.todomodas.ejemplo.com
authsmtp.foo.ejemplo.com
www1.host.ejemplo.com
smtp.mail.ejemplo.com
```

```

ub@ub:~$ subfinder -d ejemplo.com -o subfinder.txt

 -- _--_ _--_ _--_ _--_
 / / / / / / / / / / / / / / / /
 () () () () () () () ()
 / / / / / / / / / / / / / / / /
 / / / / / / / / / / / / / / / /
 / / / / / / / / / / / / / / / /

projectdiscovery.io

[INF] Current subfinder version v2.10.1 (latest)
[INF] Loading provider config from /home/ub/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for ejemplo.com
escena.ejemplo.com
sipinternal.ejemplo.com
smtp1.gmail.ejemplo.com
www.ns.ejemplo.com
mail.tudominio.ejemplo.com
mailout.hotmail.ejemplo.com
blog.ejemplo.com
authsmtp.ms1.ejemplo.com

```

## Geolocalización – Poniendo los pies en la Tierra

### Geolocalización de IP con whois

- whois 8.8.8.8

```
ub@ub:~$ whois 8.8.8.8

#
ARIN WHOIS data and services are subject to the Terms of Use
available at: https://www.arin.net/resources/registry/whois/tou/
#
If you see inaccuracies in the results, please report at
https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#

NetRange: 8.8.8.0 - 8.8.8.255
CIDR: 8.8.8.0/24
NetName: GOGL
NetHandle: NET-8-8-8-0-2
Parent: NET8 (NET-8-0-0-0-0)
NetType: Direct Allocation
OriginAS:
Organization: Google LLC (GOGL)
RegDate: 2023-12-28
Updated: 2023-12-28
Ref: https://rdap.arin.net/registry/ip/8.8.8.0

OrgName: Google LLC
OrgId: GOGL
Address: 1600 Amphitheatre Parkway
City: Mountain View
StateProv: CA
PostalCode: 94043
Country: US
RegDate: 2000-03-30
```

### Uso de geoiplookup

#### Instalación

- sudo apt install geoip-bin

```
ub@ub:~$ sudo apt install geoip-bin
```

#### Uso

- geoiplookup 8.8.8.8

```
ub@ub:~$ geoiplookup 8.8.8.8
GeoIP Country Edition: US, United States
```

### Usando la API (curl)

- curl ipinfo.io/8.8.8.8

```
ub@ub:~$ curl ipinfo.io/8.8.8.8
{
 "ip": "8.8.8.8",
 "hostname": "dns.google",
 "city": "Mountain View",
 "region": "California",
 "country": "US",
 "loc": "38.0088,-122.1175",
 "org": "AS15169 Google LLC",
 "postal": "94043",
 "timezone": "America/Los_Angeles",
 "readme": "https://ipinfo.io/missingauth",
 "anycast": true
}
```

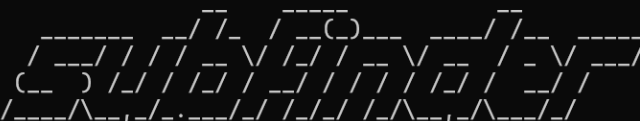
#### Combinar resultados de subdominios

- amass enum -passive -d ejemplo.com -o amass.txt

```
ub@ub:~$ amass enum -passive -d ejemplo.com -o amass.txt
vpn.ejemplo.com
api.ejemplo.com
estelinknosirve.ejemplo.com
sitio.ejemplo.com
subdominio.ejemplo.com
smtp.ejemplo.com
connect.ejemplo.com
www.ejemplo.com
rk02.ejemplo.com
nmysmtp.ejemplo.com
remote.ejemplo.com
ftp.ejemplo.com
owa.ejemplo.com
```

- subfinder -d ejemplo.com -o subfinder.txt

```
ub@ub:~$ subfinder -d ejemplo.com -o subfinder.txt
```



projectdiscovery.io

```
[INF] Current subfinder version v2.10.1 (latest)
[INF] Loading provider config from /home/ub/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for ejemplo.com
spanish.el.ejemplo.com
rk04.ejemplo.com
xn--pgina-xqa.ejemplo.com
mailserver.extranet.ejemplo.com
www1.host.ejemplo.com
spam.gmail.ejemplo.com
relay2.hotmail.ejemplo.com
www.ftp.ejemplo.com
www.ejemplo.ejemplo.com
blog.ejemplo.com
deathstar.ejemplo.com
m.ejemplo.com
zimbra8.ejemplo.com
```

```
ub@ub:~$ sort amass.txt subfinder.txt | uniq > subdominios_finales.txt
```

## Resolución de subdominio a dirección IP

```
ub@ub:~$ while read sub; do
 echo "Resolviendo $sub"
 host $sub
done < subdominios_finales.txt
Resolviendo 10mailserver.ejemplo.com
10mailserver.ejemplo.com has address 3.33.243.145
10mailserver.ejemplo.com has address 15.197.204.56
10mailserver.ejemplo.com mail is handled by 0 .
Resolviendo 123.ejemplo.com
123.ejemplo.com has address 15.197.204.56
123.ejemplo.com has address 3.33.243.145
123.ejemplo.com mail is handled by 0 .
Resolviendo 1.6www.ejemplo.com
1.6www.ejemplo.com has address 15.197.204.56
1.6www.ejemplo.com has address 3.33.243.145
1.6www.ejemplo.com mail is handled by 0 .
Resolviendo 1.7www.ejemplo.com
1.7www.ejemplo.com has address 15.197.204.56
1.7www.ejemplo.com has address 3.33.243.145
1.7www.ejemplo.com mail is handled by 0 .
```