

Práctica 3: Enumeración DNS con Amass y Subfinder

Objetivo: Utilizar herramientas modernas para identificar subdominios, relaciones DNS y estructuras internas de una organización, lo cual es fundamental en la fase de reconocimiento de un pentest profesional.

1. Entorno virtualizado recomendado

Máquina atacante

- **SO:** Kali Linux 2025.2
- **RAM:** 2 GB
- **Red:** NAT (si se hacen consultas reales), o Interna (para entorno controlado)
- **Herramientas:** Amass, Subfinder, dnsx (opcional, para validación)

2. Instalación de herramientas

Instalar Amass (ya incluido en Kali normalmente)

```
sudo apt install amass -y
```

```
(osint-venv)-(kali@kali)-[~]
└─$ sudo apt install amass -y
[sudo] password for kali:
amass is already the newest version (4.2.0-0kali1).
amass set to manually installed.
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0
(kali@kali)-[~]
└─$
```

Instalar Subfinder (de ProjectDiscovery)

```
sudo apt install golang -y
```

```
(osint-venv)-(kali@kali)-[~]
└─$ sudo apt install golang -y
Installing:
  golang

Installing dependencies:
  golang-1.24      golang-1.24-go  golang-doc  golang-src  pkgconf
  golang-1.24-doc  golang-1.24-src  golang-go  libpkgconf3  pkgconf-bin

Suggested packages:
  bzip2 | brz  mercurial

Summary:
  Upgrading: 0, Installing: 11, Removing: 0, Not Upgrading: 0
  Download size: 50.1 MB
  Space needed: 259 MB / 60.0 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 golang-1.24-doc all 1.24.4-1 [112 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 golang-1.24-src all 1.24.4-1 [21.2 MB]
Get:6 http://http.kali.org/kali kali-rolling/main amd64 golang-go amd64 2:1.24-2 [44.3 kB]
Get:10 http://mirror.es.cdn-perfprod.com/kali kali-rolling/main amd64 pkgconf-bin amd64 1.8.1-4 [30.2 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 golang-1.24-go amd64 1.24.4-1 [28.7 MB]
Get:4 http://kali.download/kali kali-rolling/main amd64 golang-1.24 all 1.24.4-1 [16.2 kB]
Get:5 http://http.kali.org/kali kali-rolling/main amd64 golang-src all 2:1.24-2 [5,136 B]
Get:7 http://http.kali.org/kali kali-rolling/main amd64 golang-doc all 2:1.24-2 [5,148 B]
Get:8 http://http.kali.org/kali kali-rolling/main amd64 golang amd64 2:1.24-2 [5,088 B]
Get:9 http://kali.download/kali kali-rolling/main amd64 libpkgconf3 amd64 1.8.1-4 [36.4 kB]
Get:11 http://kali.download/kali kali-rolling/main amd64 pkgconf amd64 1.8.1-4 [26.2 kB]
Fetched 50.1 MB in 3s (18.0 MB/s)
```

```
go install -v github.com/projectdiscovery/subfinder/v2/cmd/subfinder@latest
```

```
(osint-venv)-(kali@kali)-[~]
└─$ go install -v github.com/projectdiscovery/subfinder/v2/cmd/subfinder@latest
go: downloading github.com/projectdiscovery/subfinder/v2 v2.8.0
go: downloading github.com/projectdiscovery/subfinder v2.8.0+incompatible
go: downloading github.com/projectdiscovery/fdmax v0.0.4
go: downloading github.com/projectdiscovery/gologger v1.1.54
go: downloading github.com/hako/durafmt v0.0.0-20210316092057-3a2c319c1acd
go: downloading github.com/json-iterator/go v1.1.12
go: downloading github.com/projectdiscovery/chaos-client v0.5.2
go: downloading github.com/projectdiscovery/dnsx v1.2.2
go: downloading github.com/projectdiscovery/goflags v0.1.74
go: downloading github.com/projectdiscovery/utils v0.4.20
go: downloading golang.org/x/exp v0.0.0-20250106191152-7588d65b2ba8
go: downloading gopkg.in/yaml.v3 v3.0.1
go: downloading github.com/modern-go/concurrent v0.0.0-20180306012644-bacd9c7ef1dd
go: downloading github.com/modern-go/reflect2 v1.0.2
go: downloading github.com/logrusorg/gru/aurora v2.0.3+incompatible
go: downloading github.com/projectdiscovery/ratelimit v0.0.81
```

```
export PATH=$PATH:$(go env GOPATH)/bin
```

```
(osint-venv)-(kali@kali)-[~]
└─$ export PATH=$PATH:$(go env GOPATH)/bin
└─(osint-venv)-(kali@kali)-[~]
```

Instalar dnsx (validación)

```
go install -v github.com/projectdiscovery/dnsx/cmd/dnsx@latest
```

```
(osint-venv)-(kali@kali)-[~]
└─$ go install -v github.com/projectdiscovery/dnsx/cmd/dnsx@latest
go: downloading github.com/projectdiscovery/gologger v1.1.42
go: downloading github.com/miekg/dns v1.1.56
go: downloading github.com/projectdiscovery/asnmap v1.1.1
go: downloading github.com/projectdiscovery/clistats v0.1.1
go: downloading github.com/projectdiscovery/goconfig v0.0.1
go: downloading github.com/projectdiscovery/goflags v0.1.65
go: downloading github.com/projectdiscovery/hmap v0.0.77
go: downloading github.com/projectdiscovery/mapcidr v1.1.34
go: downloading github.com/projectdiscovery/ratelimit v0.0.69
go: downloading github.com/projectdiscovery/retryabledns v1.0.94
go: downloading github.com/projectdiscovery/utils v0.4.7
go: downloading golang.org/x/net v0.33.0
go: downloading github.com/projectdiscovery/cdncheck v1.1.0
go: downloading github.com/projectdiscovery/freeport v0.0.7
go: downloading golang.org/x/exp v0.0.0-20230420155640-133eef4313cb
go: downloading golang.org/x/sys v0.28.0
go: downloading gopkg.in/ini.v1 v1.67.0
go: downloading github.com/projectdiscovery/retryablehttp-go v1.0.97
go: downloading golang.org/x/term v0.27.0
```

3. Guía paso a paso: Enumeración con Amass

1 - Enumeración pasiva

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

```
(osint-venv)-(kali@kali)-[~]
$ amass enum -passive -d tesla.com
tesla.com (FQDN) → mx_record → tesla-com.mail.protection.outlook.com (FQDN)
mobile.tesla.com (FQDN) → cname_record → mobile.tesla.com.edgekey.net (FQDN)
cx.tesla.com (FQDN) → cname_record → cx.tesla.com.edgekey.net (FQDN)
origin-auth.tesla.com (FQDN) → cname_record → clsiamp.tesla.com.akadns.net (FQDN)
akamai-apigateway-stg-shipmentplanningapi.tesla.com (FQDN) → cname_record → akamai-apigateway-stg-shipmentplanningapi.tesla.com.edgekey.net (FQDN)
view.email.tesla.com (FQDN) → cname_record → view.virt.s7.exacttarget.com (FQDN)
origin-assets-contactus.tesla.com (FQDN) → cname_record → origin-assets-contactus.tesla.com.edgekey.net (FQDN)
accounts.tesla.com (FQDN) → cname_record → accounts.tesla.com.edgekey.net (FQDN)
solarbonds.tesla.com (FQDN) → cname_record → solarbonds.tesla.com.edgekey.net (FQDN)
static-assets-pay.tesla.com (FQDN) → cname_record → static-assets-pay.tesla.com-v1.edgekey.net (FQDN)
mobile.tesla.com.edgekey.net (FQDN) → cname_record → e1792.dscx.akamaiedge.net (FQDN)
origin-assets-contactus.tesla.com.edgekey.net (FQDN) → cname_record → e1792.dscx.akamaiedge.net (FQDN)
static-assets-pay.tesla.com-v1.edgekey.net (FQDN) → cname_record → e1792.dscx.akamaiedge.net (FQDN)
link.tesla.com (FQDN) → cname_record → link.tesla.com.edgekey.net (FQDN)
akamai-apigateway-captiveunderwriting.tesla.com (FQDN) → cname_record → akamai-apigateway-captiveunderwriting.tesla.com.edgekey.net (FQDN)
static-assets-profile-settings.tesla.com (FQDN) → cname_record → external-na-pop1.edgekey.net (FQDN)
pub.email.tesla.com (FQDN) → cname_record → pub.s7.exacttarget.com (FQDN)
forums.tesla.com (FQDN) → cname_record → site-6030136.onvanilla.net (FQDN)
errlog.tesla.com (FQDN) → cname_record → errlog.tesla.com.edgekey.net (FQDN)
proteus-api.eng.usw2.vn.cloud.tesla.com (FQDN) → cname_record → dpupr-eng.usw2.vn.cloud.tesla.com (FQDN)
fleet-api.prd.eu.vn.cloud.tesla.com (FQDN) → cname_record → epuca-prd.euw1.vn.cloud.tesla.com (FQDN)
```

2 - Modo activo con brute forcing

```
amass enum -brute -d tesla.com
```

```
(osint-venv)-(kali@kali)-[~]
$ amass enum -brute -d tesla.com
tesla.com (FQDN) → mx_record → tesla-com.mail.protection.outlook.com (FQDN)
tesla.com (FQDN) → ns_record → a1-12.akam.net (FQDN)
tesla.com (FQDN) → ns_record → edns69.ultradns.com (FQDN)
tesla.com (FQDN) → ns_record → a9-67.akam.net (FQDN)
tesla.com (FQDN) → ns_record → a12-64.akam.net (FQDN)
tesla.com (FQDN) → ns_record → a7-66.akam.net (FQDN)
tesla.com (FQDN) → ns_record → a10-67.akam.net (FQDN)
tesla.com (FQDN) → ns_record → a28-65.akam.net (FQDN)
akamai-apigateway-stg-shipmentplanningapi.tesla.com (FQDN) → cname_record → akamai-apigateway-stg-shipmentplanningapi.tesla.com.edgekey.net (FQDN)
origin-bolt-forms.tesla.com (FQDN) → cname_record → origin-bolt-forms.tesla.com.akadns.net (FQDN)
ir.tesla.com (FQDN) → cname_record → ir.tesla.com.edgekey.net (FQDN)
cua-help-me-charge-ui.tesla.com (FQDN) → cname_record → cua-help-me-charge-ui.tesla.com.edgekey.net (FQDN)
sso.tesla.com (FQDN) → cname_record → tslaso.edgekey.net (FQDN)
```

3 - Salida a archivo

```
amass enum -d tesla.com -o subdomains.txt
cat subdomains.txt
```

```
(osint-venv)-(kali@kali)-[~]
$ cat subdomains.txt
tesla.com (FQDN) → mx_record → tesla-com.mail.protection.outlook.com (FQDN)
tesla.com (FQDN) → ns_record → a1-12.akam.net (FQDN)
tesla.com (FQDN) → ns_record → edns69.ultradns.com (FQDN)
tesla.com (FQDN) → ns_record → a9-67.akam.net (FQDN)
tesla.com (FQDN) → ns_record → a12-64.akam.net (FQDN)
tesla.com (FQDN) → ns_record → a7-66.akam.net (FQDN)
tesla.com (FQDN) → ns_record → a10-67.akam.net (FQDN)
tesla.com (FQDN) → ns_record → a28-65.akam.net (FQDN)
mobile.tesla.com (FQDN) → cname_record → mobile.tesla.com.edgekey.net (FQDN)
mobile.tesla.com.edgekey.net (FQDN) → cname_record → e1792.dscx.akamaiedge.net (FQDN)
origin-assets-contactus.tesla.com (FQDN) → cname_record → origin-assets-contactus.tesla.com.edgekey.net (FQDN)
origin-assets-contactus.tesla.com.edgekey.net (FQDN) → cname_record → e1792.dscx.akamaiedge.net (FQDN)
```

4. Subfinder

1 - Configurar claves para APIs externas (opcional)

Puedes usar claves para mejorar resultados (Shodan, Censys, etc.), configurando
~/ .config/subfinder/provider-config.yaml.

```
(osint-venv)-(kali@kali)-[~]
$ cat /home/kali/.config/subfinder/provider-config.yaml

bevigil: []
bufferover: []
builtwith: []
c99: []
censys: []
certspotter: []
chaos: []
chinaz: []
digitalyama: []
dnsdb: []
dnsdumpster: []
dnsrepo: []
facebook: []
fofa: []
fullhunt: []
github: []
hunter: []
intelx: []
leakix: []
netlas: []
pugrecon: []
quake: []
redhuntlabs: []
robtex: []
rsecloud: []
securitytrails: []
shodan: []
threatbook: []
virustotal: []
whoisxmlapi: []
zoomeyeapi: []
```

2 - Ejecutar subfinder

```
subfinder -d tesla.com -o found.txt
```

```
(osint-venv)-(kali@kali)-[~]  
$ subfinder -d tesla.com -o found.txt  
  
subfinder  
projectdiscovery.io  
  
[INF] Current subfinder version v2.8.0 (latest)  
[INF] Loading provider config from /home/kali/.config/subfinder/provider-config.yaml  
[INF] Enumerating subdomains for tesla.com  
e.tesla.com  
aaa-dr.tesla.com  
mobile-ops-links.prn.vn.cloud.tesla.com  
teslacmgus01.tesla.com  
nuget.github.tesla.com  
codeload.github-it.tesla.com  
ciscoguest.tesla.com  
factory-berlin.tesla.com  
dex.ops.bn.na.vn.cloud.tesla.com  
akamai-apigateway-vehicleextinfo-gw-stgsvc-st.tesla.com  
cxadmin-apac.tesla.com  
c382p434p572c.tesla.com  
rumipv6.tesla.com  
stage.tesla.com  
mta5.emails.tesla.com  
solarbonds.tesla.com  
sca.tesla.com  
static.tesla.com  
fleetview.prn.na.fn.tesla.com  
reply.extgithub.tesla.com  
vehicle-files.eng.vn.cloud.tesla.com  
lionpayshare.tesla.com  
ai-api.tesla.com  
github-fw.tesla.com  
rubygems.github-it.tesla.com  
x3-prod.obs.tesla.com  
gfb.vdi.tesla.com  
dal11-gpgw1.tesla.com  
gist.github-ap.tesla.com  
codeload.extgithub.tesla.com  
[INF] Found 543 subdomains for tesla.com in 24 seconds 75 milliseconds  
  
(osint-venv)-(kali@kali)-[~]
```

Con API de Shodan

```
energy-firmware-stage.tesla.com
stream.tesla.com
akamai-apigateway-roaming-stg.tesla.com
apigateway-hrosappapi.tesla.com
errlog.tesla.com
vpn2.tesla.com
apigateway-vfx-relay.tesla.com
origin-tcc-gw-stg.tesla.com
origin-warpcxml-uat.tesla.com
url4211.tesla.com
tss.tesla.com
akamai-apigateway-stg-warpasetapi.tesla.com
logcollection.tesla.com
[INF] Found 1207 subdomains for tesla.com in 12 seconds 239 milliseconds
```

3 - Validar con dnsx

```
dnsx -l found.txt -silent
```

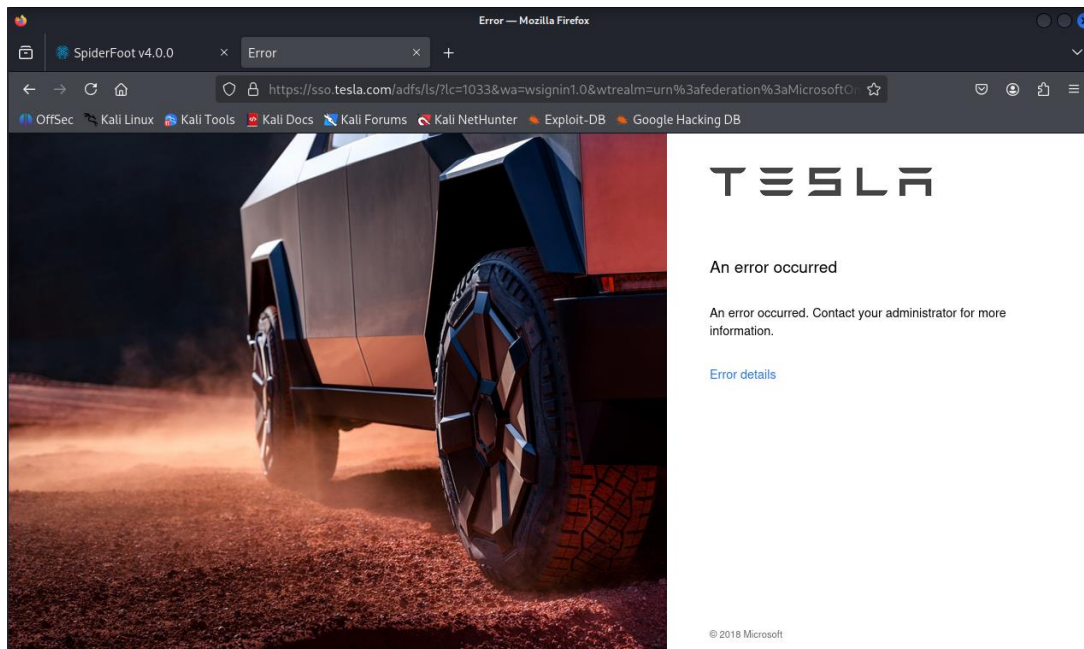
```
(osint-venv)-(kali@kali)-[~]
└─$ dnsx -l found.txt -silent
akamai-apigateway-deliveryopsvitu.tesla.com
akamai-apigateway-stg-finplateng.tesla.com
akamai-apigateway-bender.tesla.com
akamai-apigateway-deliveryopsapi1.tesla.com
accounts.tesla.com
akamai-apigateway-stg-packaging2.tesla.com
akamai-apigateway-clmapi-uat.tesla.com
akamai-apigateway-deliveryopsapi.tesla.com
akamai-apigateway-stg-inventorytxnextapi.tesla.com
akamai-apigateway-charging-ownership-stage.tesla.com
akamai-apigateway-clmapi.tesla.com
akamai-apigateway-bolt-forms.tesla.com
akamai-apigateway-ehs-stg.de.tesla.com
akamai-apigateway-chargebackapi.tesla.com
akamai-apigateway-automation-billing.tesla.com
advent-gfbb-dev.tesla.com
akamai-apigateway-stg-materials.tesla.com
akamai-apigateway-gallagher-external-api.tesla.com
akamai-apigateway-claims-integration-api.tesla.com
13494342.tesla.com
```



```
view.emails.tesla.com
ul.engage.tesla.com
xmail.tesla.com
www.engage.tesla.com
x3-eng.obs.tesla.com
x3-prod.obs.tesla.com
wdm.kronos.tesla.com
web-api.prd.na.vn.cloud.tesla.com
x3-static.obs.tesla.com
vehicle-files.eng.usw2.vn.cloud.tesla.com
vehicle-files.prd.euw1.vn.cloud.tesla.com
wire.tesla.com
```

```
└─(osint-venv)-(kali@kali)-[~]
```

```
└─(osint-venv)-(kali@kali)-[~]
└─$ ping xmail.tesla.com
PING xmail.tesla.com (204.74.99.100) 56(84) bytes of data:
64 bytes from crs.ultradns.net (204.74.99.100): icmp_seq=1 ttl=128 time=43.4 ms
64 bytes from crs.ultradns.net (204.74.99.100): icmp_seq=2 ttl=128 time=43.7 ms
64 bytes from crs.ultradns.net (204.74.99.100): icmp_seq=3 ttl=128 time=43.3 ms
64 bytes from crs.ultradns.net (204.74.99.100): icmp_seq=4 ttl=128 time=43.8 ms
^C
  xmail.tesla.com ping statistics —
  4 packets transmitted, 4 received, 0% packet loss, time 3016ms
 rtt min/avg/max/mdev = 43.321/43.559/43.816/0.198 ms
└─(osint-venv)-(kali@kali)-[~]
└─$
```



```
dnsx -l found.txt -silent -resp-only -o resolved.txt
```

```
(osint-venv)-(kali@kali)-[~]  
$ dnsx -l found.txt -silent -resp-only -o resolved.txt  
23.1.248.65  
104.83.192.56  
2.19.200.56  
104.83.192.56  
104.83.192.56  
104.83.192.56  
2.19.200.56  
104.83.192.56  
23.1.248.65  
23.1.248.65  
54.216.50.79  
18.158.228.216  
46.51.200.92  
3.79.130.38  
2.17.152.69  
2.19.200.56  
23.50.143.85  
2.20.100.70  
104.83.192.56  
104.83.192.56  
23.1.248.65
```

```
go install -v github.com/projectdiscovery/httpx/cmd/httpx@latest  
export PATH=$PATH:~/go/bin  
/home/kali/go/bin/httpx -l resolved.txt -title -tech-detect -o webservices.txt
```

```
(osint-venv)-(kali@kali)-[~]  
$ /home/kali/go/bin/httpx -l resolved.txt -title -tech-detect -o webservices.txt  
  
projectdiscovery.io  
  
[INF] Current httpx version v1.7.1 (latest)  
[WRN] UI Dashboard is disabled, Use -dashboard option to enable  
https://151.101.130.1 [HSTS]  
https://104.121.15.206 [Invalid URL]  
https://151.101.194.1 [HSTS]  
https://104.83.192.56 [Invalid URL]  
https://151.101.66.92 [HSTS]  
https://151.101.194.92 [HSTS]  
https://151.101.130.92 [HSTS]  
https://151.101.2.1 [HSTS]  
http://104.107.108.211  
https://151.101.66.1 [HSTS]  
http://104.107.108.68  
https://151.101.2.92 [HSTS]  
http://18.154.29.109 [ERROR: The request could not be satisfied] [Amazon CloudFront,Amazon Web Services]  
http://18.154.48.20 [ERROR: The request could not be satisfied] [Amazon CloudFront,Amazon Web Services]  
http://18.154.29.56 [ERROR: The request could not be satisfied] [Amazon CloudFront,Amazon Web Services]  
http://18.154.29.96 [ERROR: The request could not be satisfied] [Amazon CloudFront,Amazon Web Services]
```


Ejemplo de resultado esperado

```
vpn.example-corp.com  
mail.example-corp.com  
intranet.example-corp.com  
adminpanel.example-corp.com
```

Puedes usar un DNS simulado o usar `hosts` para reproducir otro escenario.

5. Actividades de evaluación

Actividad	Detalle
Resultado de Amass/Subfinder	Listado de subdominios con evidencia
Comparación de herramientas	¿Cuál da más resultados y por qué?
Detección de patrones	Subdominios sensibles: admin, dev, test...
Validación manual	Confirmar existencia vía navegador o dig