

Práctica 1: OSINT con Recon-ng y SpiderFoot

Objetivo

Aplicar técnicas avanzadas de **OSINT (Open Source Intelligence)** para recolectar información sobre un objetivo simulado o real utilizando **Recon-ng** y **SpiderFoot**.

1. Entorno virtualizado recomendado

Máquina atacante (Kali Linux)

- SO: *Kali Linux 2025.2* <https://www.kali.org/get-kali/#kali-installer-images>
- RAM: 2 GB
- Herramientas: *Recon-ng*, *SpiderFoot*, *Firefox*
- Red: *NAT* o red interna (según simulación deseada)

Máquina objetivo ficticia (simulada)

No es necesario levantar una máquina objetivo real para esta práctica, ya que se usará **información pública** y/o simulada de un dominio (por ejemplo, *tesla.com*).

2. Instalación y preparación

En Kali Linux:

```
# Actualiza repositorios
sudo apt update && sudo apt upgrade -y
sudo apt autoremove
sudo apt dist-upgrade
# Para poner teclado en español rápidamente
setxkbmap es
```

Crear una instantánea del estado completo de la máquina actualizada (*Snapshot*) para volver a ese estado cuando sea necesario:

```
# Instalar Recon-ng (si no está instalado)
sudo apt install recon-ng -y

# Instalar SpiderFoot (si no está instalado)
sudo apt install git python3-pip -y
git clone https://github.com/smicallef/spiderfoot.git
cd spiderfoot
pip3 install -r requirements.txt
```

Para lanzar SpiderFoot con interfaz web:

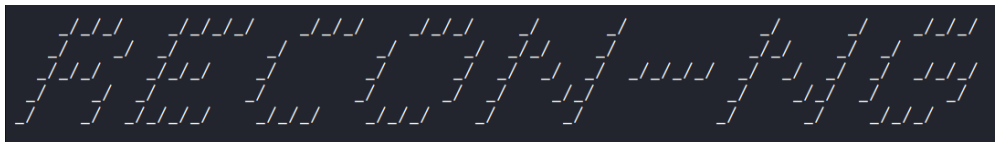
```
python3 sf.py
```

O

```
spiderfoot -l 127.0.0.1:5001
```

Luego accede desde el navegador a: <http://127.0.0.1:5001>

3. Guía paso a paso: Recon-ng



1 - Iniciar Recon-ng

```
recon-ng
```

2 - Crear un workspace

```
workspaces create osint_practice
```

3 - Insertar dominio

```
db insert domains
```

Introducir: tesla.com

Introducir: Web vulnerable OSINT

```
show domains
```

```
[recon-ng][osint_practice][whois_pocs] > db insert domains
domain (TEXT): tesla.com
notes (TEXT): TESLA web pruebas
[*] 1 rows affected.
[recon-ng][osint_practice][whois_pocs] > show domains

+-----+-----+-----+-----+
| rowid | domain | notes | module |
+-----+-----+-----+-----+
| 1     | tesla.com | TESLA web pruebas | user_defined |
+-----+-----+-----+-----+

[*] 1 rows returned
```

4 - Cargar módulos automáticos

Ver módulos instalados

```
marketplace search
```

```
[recon-ng][osint_practice] > marketplace search
```

Path	Version	Status	Updated	D	K
discovery/info_disclosure/cache_snoop	1.1	not installed	2020-10-13		
discovery/info_disclosure/interesting_files	1.2	not installed	2021-10-04		
exploitation/injection/command_injector	1.0	not installed	2019-06-24		
exploitation/injection/xpath_bruter	1.2	not installed	2019-10-08		
import/csv_file	1.1	not installed	2019-08-09		
import/list	1.1	not installed	2019-06-24		
import/masscan	1.0	not installed	2020-04-07		
import/nmap	1.1	not installed	2020-10-06		
recon/companies-contacts/bing_linkedin_cache	1.0	not installed	2019-06-24		*
recon/companies-contacts/censys_email_address	2.1	not installed	2022-01-31	*	*
recon/companies-contacts/pen	1.1	not installed	2019-10-15		
recon/companies-domains/censys_subdomains	2.1	not installed	2022-01-31	*	*
recon/companies-domains/pen	1.1	not installed	2019-10-15		
recon/companies-domains/viewdns_reverse_whois	1.1	not installed	2021-08-24		
recon/companies-domains/whoxy_dns	1.1	not installed	2020-06-17		*
recon/companies-multi/censys_org	2.1	not installed	2022-01-31	*	*

Instalar todos los módulos

```
marketplace install all
```

```
[recon-ng][osint_practice] > marketplace install all
[*] Module installed: discovery/info_disclosure/cache_snoop
[*] Module installed: discovery/info_disclosure/interesting_files
[*] Module installed: exploitation/injection/command_injector
[*] Module installed: exploitation/injection/xpath_bruter
[*] Module installed: import/csv_file
[*] Module installed: import/list
[*] Module installed: import/masscan
[*] Module installed: import/nmap
[*] Module installed: recon/companies-contacts/bing_linkedin_cache
[*] Module installed: recon/companies-contacts/censys_email_address
[*] Module installed: recon/companies-contacts/pen
```

- Algunos módulos requieren **API keys** (Shodan, Bing, Google, etc.). Se configuran con:

```
keys add shodan_api <tu_api_key>
keys list
```

```
[recon-ng][osint_practice] > keys add shodan_api 123456
[*] Key 'shodan_api' added.
[recon-ng][osint_practice] > keys list
```

Name	Value
binaryedge_api	
bing_api	
builtwith_api	
censysio_id	
censysio_secret	
flickr_api	
fullcontact_api	
github_api	
google_api	
hashes_api	
hibp_api	
hunter_io	
ipinfodb_api	
ipstack_api	
namechk_api	
shodan_api	123456
spyse_api	
twitter_api	
twitter_secret	
virustotal_api	
whoxy_api	

```
[recon-ng][osint_practice] > [recon-ng][osint_practice] > █
```

- Los que no necesitan API funcionan directamente (ejemplo: whois, brute_hosts).

Ejemplo con módulo de WHOIS:

```
modules load recon/domains-contacts/whois
```

```
[recon-ng][osint_practice] > [recon-ng][osint_practice] > modules load recon/domains-contacts/whois
[recon-ng][osint_practice][whois_pocs] > info
```

```
Name: Whois POC Harvester
Author: Tim Tomes (@lanmaster53)
Version: 1.0
```

Description:

Uses the ARIN Whois RWS to harvest POC data from whois queries for the given domain. Updates the 'contacts' table with the results.

Options:

Name	Current Value	Required	Description
SOURCE	default	yes	source of input (see 'info' for details)

Source Options:

```
default      SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
<string>     string representing a single input
<path>       path to a file containing a list of inputs
query <sql>  database query returning one column of inputs
```

```
[recon-ng][osint_practice][whois_pocs] > █
```

Run

```
[recon-ng][osint_practice][whois_pocs] > modules load recon/domains-contacts/whois
[recon-ng][osint_practice][whois_pocs] > options set SOURCE tesla.com
SOURCE ⇒ tesla.com
[recon-ng][osint_practice][whois_pocs] > run
```

TESLA.COM

```
[*] URL: http://whois.arin.net/rest/pocs;domain=tesla.com
[*] URL: http://whois.arin.net/rest/poc/LEWIS987-ARIN
[*] Country: United States
[*] Email: chelewis@tesla.com
[*] First_Name: Cheri
[*] Last_Name: Lewis-Carey
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Palo Alto, CA
[*] Title: Whois contact
[*]
[*] URL: http://whois.arin.net/rest/poc/LEWIS994-ARIN
[*] Country: United States
[*] Email: chelewis@tesla.com
[*] First_Name: CHERI
[*] Last_Name: LEWIS
[*] Middle_Name: None
[*] Notes: None
```

Otros módulos útiles:

- recon/domains-hosts/bing_domain_web

```
[recon-ng][osint_practice][brute_hosts] > modules load recon/domains-hosts/bing_domain_web
[recon-ng][osint_practice][bing_domain_web] > run
```

TESLA.COM

```
[*] URL: https://www.bing.com/search?first=0&q=domain%3Atesla.com
[recon-ng][osint_practice][bing_domain_web] > █
```

- recon/domains-hosts/brute_hosts

```
[recon-ng][osint_practice] > modules load recon/domains-hosts/brute_hosts
[recon-ng][osint_practice][brute_hosts] > run
```

TESLA.COM

```
[*] No Wildcard DNS entry found.
[*] 0.tesla.com ⇒ No record found.
[*] 01.tesla.com ⇒ No record found.
[*] 03.tesla.com ⇒ No record found.
[*] 02.tesla.com ⇒ No record found.
[*] 1.tesla.com ⇒ No record found.
[*] 12.tesla.com ⇒ No record found.
[*] 10.tesla.com ⇒ No record found.
[*] 11.tesla.com ⇒ No record found.
[*] 14.tesla.com ⇒ No record found.
[*] 15.tesla.com ⇒ No record found.
[*] 13.tesla.com ⇒ No record found.
[*] 16.tesla.com ⇒ No record found.
[*] 17.tesla.com ⇒ No record found.
[*] 19.tesla.com ⇒ No record found.
[*] 18.tesla.com ⇒ No record found.
[*] 2.tesla.com ⇒ No record found.
[*] 3.tesla.com ⇒ No record found.
[*] 6.tesla.com ⇒ No record found.
[*] 20.tesla.com ⇒ No record found.
[*] 4.tesla.com ⇒ No record found.
```

- recon/domains-hosts/google_site_web

```
[recon-ng][osint_practice][bing_domain_web] > modules load recon/domains-hosts/google_site_web
[recon-ng][osint_practice][google_site_web] > run

TESLA.COM

[*] Searching Google for: site:tesla.com
[!] Google CAPTCHA triggered. No bypass available.
[recon-ng][osint_practice][google_site_web] > █
```

- recon/hosts-hosts/resolve

```
[recon-ng][osint_practice][google_site_web] > modules load recon/hosts-hosts/resolve
[recon-ng][osint_practice][resolve] > run
[*] accounts.tesla.com.edgekey.net => 2.20.40.60
[*] accounts.tesla.com => 2.20.40.60
[*] e1792.dsca.akamaiedge.net => 2.20.40.60
[*] apps.tesla.com.edgekey.net => 2.19.200.56
[*] apps.tesla.com => 2.19.200.56
[*] e1792.x.akamaiedge.net => 2.19.200.56
[*] auth.tesla.com.edgekey.net => 2.19.200.56
[*] auth.tesla.com => 2.19.200.56
[*] e1792.dscx.akamaiedge.net => 2.19.200.56
[*] autodiscover.outlook.com => 40.99.155.56
[*] autodiscover.outlook.com => 52.97.233.88
[*] autodiscover.outlook.com => 52.97.201.40
[*] autodiscover.outlook.com => 52.97.201.56
[*] autodiscover.tesla.com => 40.99.217.152
[*] autodiscover.tesla.com => 40.99.220.136
[*] autodiscover.tesla.com => 40.99.153.152
[*] autodiscover.tesla.com => 40.101.138.8
[*] atod-g2.tm-4.office.com => 52.97.233.40
[*] atod-g2.tm-4.office.com => 52.98.178.184
[*] atod-g2.tm-4.office.com => 52.98.228.248
[*] atod-g2.tm-4.office.com => 52.98.151.232
[*] billing.tesla.com.edgekey.net => 2.19.200.56
[*] billing.tesla.com => 2.19.200.56
[*] ipa.teslazta.net.srip.net => 92.122.158.211
```

- Buscar y probar varios módulos más

5 - Exportar resultados

```
modules load reporting/html
options set CREATOR "Nombre Alumno"
options set CUSTOMER "Cliente X"
run
```

```
[recon-ng][osint_practice][resolve] > modules load reporting/html
[recon-ng][osint_practice][html] > options set CREATOR "Nombre Alumno"
CREATOR => "Nombre Alumno"
[recon-ng][osint_practice][html] > options set CUSTOMER "Cliente X"
CUSTOMER => "Cliente X"
[recon-ng][osint_practice][html] > run
[*] Report generated at '/root/.recon-ng/workspaces/osint_practice/results.html'.
[recon-ng][osint_practice][html] > █
```

El informe se guarda en:

~/recon-ng/workspaces/<tu_workspace>/reports/

"Cliente X" www.recon-ng.com

Recon-ng Reconnaissance Report

[-] Summary

table	count
domains	1
companies	0
netblocks	0
locations	0
vulnerabilities	0
ports	0
hosts	99
contacts	6
credentials	0
leaks	0
pushpins	0
profiles	0
repositories	0

[-] Domains

domain	notes	module
tesla.com	TESLA web pruebas	user_defined

[-] Hosts

host	ip_address	region	country	latitude	longitude	notes	module
shop.tesla.com.edgekey.net	2.19.200.56						brute_hosts
static.tesla.com	2.19.200.56						brute_hosts
static.tesla.com	2.19.200.56						brute_hosts
static.tesla.com.edgekey.net	2.19.200.56						brute_hosts
suppliers.tesla.com	2.19.200.56						brute_hosts
suppliers.tesla.com	2.19.200.56						brute_hosts
suppliers.tesla.com.edgekey.net	2.19.200.56						brute_hosts
teslamotors.vanity3.ca1.qualtrics.com	184.31.175.214						brute_hosts
vpn2.tesla.com	8.47.24.215						brute_hosts
warehouse.tesla.com	2.20.40.60						brute_hosts
warehouse.tesla.com	2.20.40.60						brute_hosts
warehouse.tesla.com.edgekey.net	2.20.40.60						brute_hosts
wire.tesla.com	92.122.158.211						brute_hosts
wire.tesla.com	92.122.158.211						brute_hosts
www.tesla.com	2.19.200.56						brute_hosts
www.tesla.com	2.19.200.56						brute_hosts
www.tesla.com.edgekey.net	2.19.200.56						brute_hosts
xmail.tesla.com	204.74.99.100						brute_hosts

[-] Contacts

first_name	middle_name	last_name	email	title	region	country	phone	notes	module
CHERI		LEWIS	chelewis@tesla.com	Whois contact	Columbus, OH	United States			whois_pocs
Cheri		Lewis-Carey	chelewis@tesla.com	Whois contact	Palo Alto, CA	United States			whois_pocs
JIAN		GU	jiangu@tesla.com	Whois contact	Palo Alto, CA	United States			whois_pocs
Mahesh		Desai	mahdesai@tesla.com	Whois contact	Palo Alto, CA	United States			whois_pocs
TERRY		CHI	tchi@tesla.com	Whois contact	Portland, OR	United States			whois_pocs
Terry		Chi	tchi@tesla.com	Whois contact	Palo Alto, CA	United States			whois_pocs

4. Guía paso a paso: SpiderFoot (Web GUI)



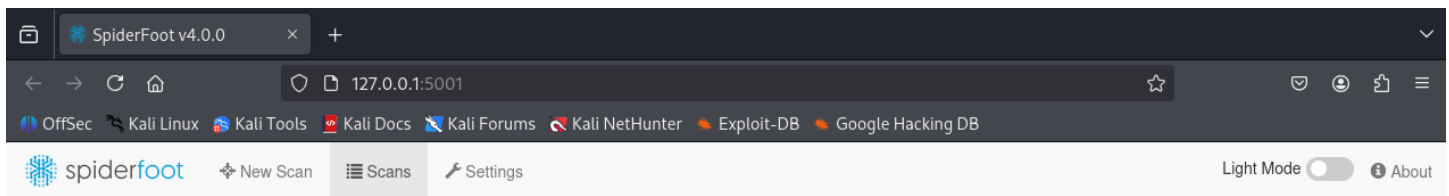
1 - Ejecutar interfaz

```
cd spiderfoot  
python3 sf.py
```

0

```
spiderfoot -l 127.0.0.1:5001
```

Navegar a: <http://127.0.0.1:5001>



Scans

No scan history

There is currently no history of previously run scans. Please click 'New Scan' to initiate a new scan.

♥ Join the SpiderFoot community Discord!

2 - Crear un nuevo scan

- Target: tesla.com
- Scan name: osint-practice
- Escoger todos los módulos (o al menos: WHOIS, DNS, subdominios, IPs, leaks)

osint-practice **RUNNING**

Summary Correlations Browse Graph Scan Settings Log

Browse / Domain Whois

Data Element	Source Data Element	Source Module	Identified
<p>Domain Name: TESLA.COM</p> <p>Registry Domain ID: 187982_DOMAIN_COM-VRSN</p> <p>Registrar WHOIS Server: whois.markmonitor.com</p> <p>Registrar URL: http://www.markmonitor.com</p> <p>Updated Date: 2024-10-02T10:15:20Z</p> <p>Creation Date: 1992-11-04T05:00:00Z</p> <p>Registry Expiry Date: 2026-11-03T05:00:00Z</p> <p>Registrar: MarkMonitor Inc.</p> <p>Registrar IANA ID: 292</p> <p>Registrar Abuse Contact Email: abusecomplaints@markmonitor.com</p> <p>Registrar Abuse Contact Phone: +1.2086851750</p> <p>Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited</p> <p>Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited</p> <p>Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited</p> <p>Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited</p>	tesla.com	sfp_whois	2025-09-10 12:16:00

spiderfoot New Scan Scans Settings Light Mode About

osint-practice **RUNNING**

Summary Correlations Browse Graph Scan Settings Log

Browse / Web Server

Data Element	Source Data Element	Source Module	Identified
AkamaiHost	tesla.com	sfp_urlscan	2025-09-10 12:16:07
AkamaiHost	www.tesla.com	sfp_urlscan	2025-09-10 12:16:09
AkamaiHost	ir.tesla.com	sfp_urlscan	2025-09-10 12:16:14
nginx	ir.tesla.com	sfp_urlscan	2025-09-10 12:16:14

- Exporta reporte en CSV o Excel

spiderfoot New Scan Scans Settings Light Mode About

osint-practice **RUNNING**

Summary Correlations Browse Graph Scan Settings Log

Browse / Linked URL - Internal

CSV
Excel

Data Element	Source Data Element	Source Module	Identified
https://ir.tesla.com	ir.tesla.com	sfp_urlscan	2025-09-10 12:16:14

5. Actividades de evaluación

Actividad	Detalle
Informe Recon-ng	Informe HTML con dominios, hosts, emails
Informe SpiderFoot	Análisis de fugas, redes sociales, etc.
Captura de evidencias	Screenshots y resultados exportados
Análisis crítico	Evaluar qué info sería útil para un atacante

Plantilla de informe OSINT

Un esquema de informe que puedes rellenar con tus resultados (en Word, Markdown o PDF):

Informe de Práctica – OSINT con Recon-ng y SpiderFoot

Alumno: [Tu nombre]

Cliente simulado: Example Corp

Fecha: [dd/mm/aaaa]

1. Objetivo

Recolectar información OSINT sobre `tesla.com` para evaluar posibles riesgos de exposición pública.

2. Metodología

- **Herramientas usadas:** Recon-ng, SpiderFoot
- **Técnicas aplicadas:** WHOIS, DNS, subdominios, fugas de credenciales

3. Hallazgos principales

- **Dominios y subdominios:**
 - `mail.tesla.com`
 - `vpn.tesla.com`
 - `intranet.tesla.com`
- **IPs asociadas:** [ejemplo: 192.0.2.5]
- **Emails encontrados:** [ejemplo: `admin@tesla.com`]
- **Fugas detectadas:** Ninguna / [detalle si existiera en SpiderFoot]

4. Evidencias (screenshots)

(inserta capturas de Recon-ng y SpiderFoot)

5. Análisis crítico

- Los subdominios expuestos podrían ser objetivo de ataques de fuerza bruta.
- La presencia de correos en fuentes públicas facilitaría phishing.
- No se detectaron fugas de credenciales, lo que reduce el riesgo actual.

6. Conclusiones

La superficie expuesta de Tesla es limitada pero contiene activos sensibles (VPN e intranet). Recomendaciones: hardening de acceso remoto y monitoreo de fugas.