

Ejercicios prácticos de Captura de Información (Tema 1.7)

♦ Ejercicio 1 – Uso de Dmitry

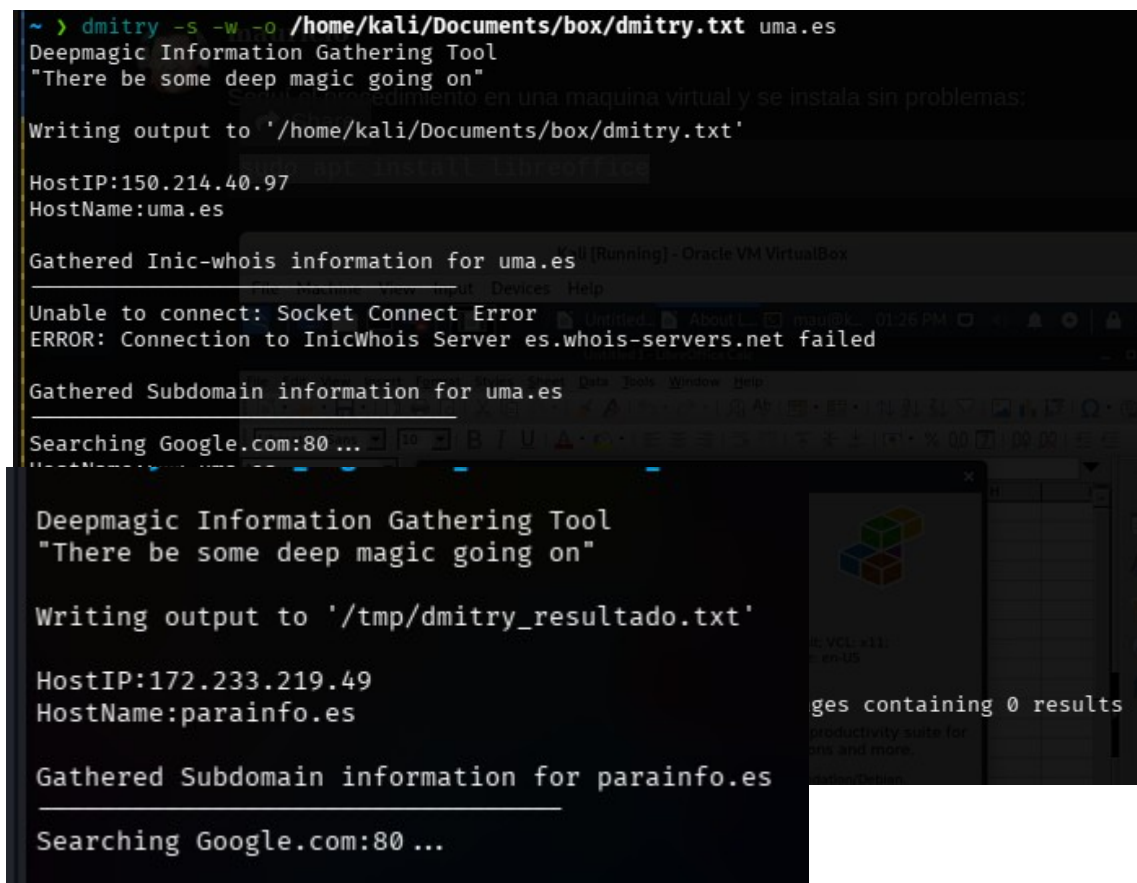
Objetivo: Capturar información básica de un dominio.

1. Abre una terminal en Kali Linux.
2. Ejecuta el comando:
3. `dmitry -s -e -o /home/usuario/dmitry_resultado.txt parainfo.es`
 - o `-s`: busca subdominios.
 - o `-e`: busca direcciones de correo.
 - o `-o`: guarda los resultados en un archivo.

Pregunta para reflexionar:

¿Qué tipo de información aparece en el archivo de salida?

Subdominios de la url pasada como argumento



```
~ > dmitry -s -w -o /home/kali/Documents/box/dmitry.txt uma.es
Deepmagic Information Gathering Tool
"There be some deep magic going on"
Writing output to '/home/kali/Documents/box/dmitry.txt'
HostIP:150.214.40.97
HostName:uma.es
Gathered Inic-whois information for uma.es
Unable to connect: Socket Connect Error
ERROR: Connection to InicWhois Server es.whois-servers.net failed
Gathered Subdomain information for uma.es
Searching Google.com:80 ...

Deepmagic Information Gathering Tool
"There be some deep magic going on"
Writing output to '/tmp/dmitry_resultado.txt'
HostIP:172.233.219.49
HostName:parainfo.es
Gathered Subdomain information for parainfo.es
Searching Google.com:80 ...
```

♦ Ejercicio 2 – Uso de DNSenum

Objetivo: Enumerar información de DNS.

1. En la terminal, escribe:
2. `dnsenum --enum -f /usr/share/dnsenum/dns.txt -o /home/usuario/dnsenum_resultado.xml parainfo.es`
 - o `--enum`: enumera información del dominio.
 - o `-f`: fichero de subdominios.
 - o `-o`: salida en XML.

Pregunta para reflexionar:

¿Qué registros DNS (A, MX, NS...) aparecen en el informe?. **MX**

```
~/Documents/box > dnsenum -f /usr/share/dnsenum/dns.txt -o dnsenum.xml uma.es
dnsenum VERSION:1.3.1

uma.es

Host's addresses:

Name Servers:

sun.rediris.es.          9153      IN      A       199.184.182.1
chico.rediris.es.       9270      IN      A       162.219.54.2
dns1.cica.es.           42619     IN      A       150.214.5.83
osiris.uma.es.          3600      IN      A       150.214.40.10
dns2.gssi.es.           86400     IN      A       90.161.204.137
dns1.gssi.es.           86400     IN      A       85.62.72.2
dns2.cica.es.           43200     IN      A       150.214.5.84
isis.uma.es.            192       IN      A       150.214.40.14

Mail (MX) Servers:

correoe2.uma.es.        7200      IN      A       150.214.47.232
correoe3.uma.es.        7200      IN      A       150.214.40.113
correoe1.uma.es.        7200      IN      A       150.214.47.231

Trying Zone Transfers and getting Bind Versions:

Trying Zone Transfer for uma.es on osiris.uma.es ...
AXFR record query failed: timed out

Trying Zone Transfer for uma.es on dns2.gssi.es ...
AXFR record query failed: REFUSED

Trying Zone Transfer for uma.es on dns1.gssi.es ...
AXFR record query failed: corrupt packet

Trying Zone Transfer for uma.es on dns2.cica.es ...
AXFR record query failed: SERVFAIL

Trying Zone Transfer for uma.es on sun.rediris.es ...
```

♦ Ejercicio 3 – Uso de Fierce

Objetivo: Detectar subdominios y hosts relacionados.

1. Ejecuta el comando:
2. `fierce --dnsserver dns.informatica-parainfo.es --dns parainfo.es --wordlist /usr/share/wordlists/dnsmap.txt -file /home/usuario/fierce_resultado.txt`
 - o `--dnsserver`: servidor DNS usado.
 - o `--dns`: dominio a escanear.
 - o `--wordlist`: lista de subdominios.
 - o `-file`: guarda resultados.

Pregunta para reflexionar:

¿Se han detectado subdominios activos? **No**

```
~/Documents/box > fierce --dnsserver dns.informatica-parainfo.es --dns parainfo.es wordlist /usr/share/wordlists/dns
map.txt -file fierce.txt
usage: fierce [-h] [--domain DOMAIN] [--connect] [--wide] [--traverse TRAVERSE] [--search SEARCH [SEARCH ...]]
             [--range RANGE] [--delay DELAY] [--subdomains SUBDOMAINS [SUBDOMAINS ...]] |
             --subdomain-file SUBDOMAIN_FILE] [--dns-servers DNS_SERVERS [DNS_SERVERS ...]] | --dns-file DNS_FILE]
             [--tcp]
fierce: error: ambiguous option: --dns could match --dns-servers, --dns-file
```

Ejercicio 3.3 – Uso de subfinder

- subfinder:

`subfinder -d parainfo.es -o /home/kali/subfinder_resultado.txt`

Este último funciona, hay que instalarlo, mejor usar kali

```
~/Doc/Ejercicios_seguridad_informatica_2025 main > subfinder -d parainfo.es -o /home/kali/subfinder_resultado.txt
[INF] Current subfinder version v2.6.0 (outdated)
[INF] Loading provider config from /home/kali/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for parainfo.es

wildcard.parainfo.es
ww1.parainfo.es
mail.parainfo.es
www.demo.parainfo.es
ebook.parainfo.es
profesores.parainfo.es
www.profesores.parainfo.es
www.professores.parainfo.es
alumnos.parainfo.es
www.parainfo.es
ebooks.parainfo.es
akumnos.parainfo.es
www.akumnos.parainfo.es
static.backend.parainfo.es
www.ebooks.parainfo.es
www.smtp.parainfo.es
www.intelligence.parainfo.es
www.pop.parainfo.es
intelligence.parainfo.es
www.webdisk.parainfo.es
whm.parainfo.es
admin.backend.parainfo.es
```

Ejercicio 4 – Uso de Metagoofil

Objetivo: Extraer metadatos de documentos públicos.

1. Escribe:
2. `metagoofil -d parainfo.es -t pdf,doc -l 30 -n 10 -o /home/usuario/goofil -f /home/usuario/goofil/resultados.html`
 - o `-d`: dominio a analizar.
 - o `-t`: tipo de archivo (pdf, doc, ppt...).
 - o `-l`: número de resultados de búsqueda.
 - o `-n`: número de archivos a descargar.
 - o `-o`: directorio de salida.
 - o `-f`: informe en HTML.

```
~/Documents/box > metagoofil -d parainfo.es -t pdf,doc -l 30 -n 10 -o . -f ./resultados.html  
[*] Searching for 30 .pdf files and waiting 30.0 seconds between searches
```