

EJERCICIOS OSINT

Instalación de herramientas osint

1) theHarvester

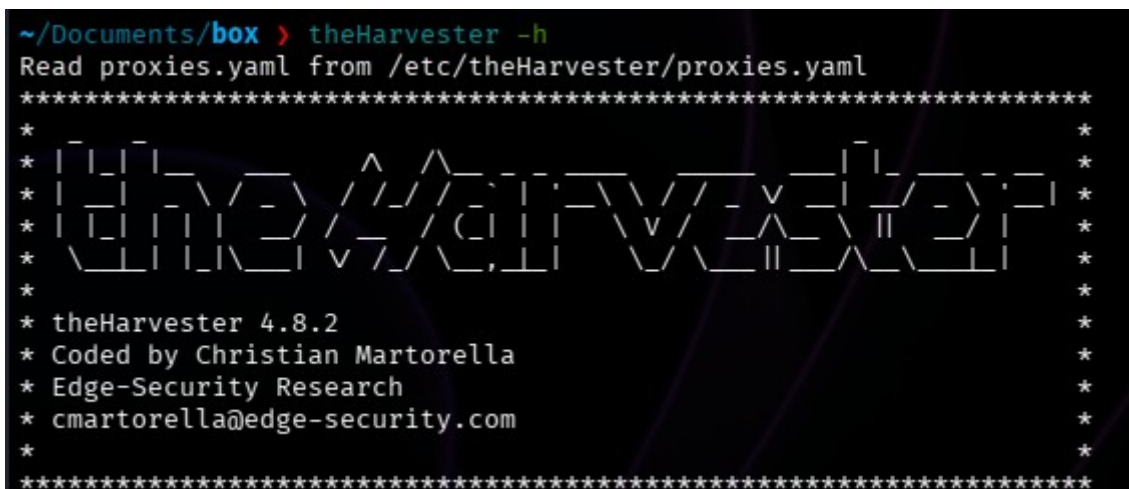
Kali Linux (recomendado):

```
sudo apt update
sudo apt install theharvester -y
# comprobar
theharvester -h
```

Instalación desde pip (alternativa, virtualenv recomendado):

```
python3 -m pip install --user theHarvester
# si falla, instala dependencias: sudo apt install libssl-dev libffi-dev build-essential -y
```

Windows/macOS: usar Python + pip install theHarvester o usar WSL en Windows.

A terminal window with a dark background and light green text. The prompt is ~/Documents/box >. The command theHarvester -h has been entered. The output shows the program's name in a large, stylized ASCII art font, followed by version information and contact details. The text is enclosed in a rectangular border of asterisks.

```
~/Documents/box > theHarvester -h
Read proxies.yaml from /etc/theHarvester/proxies.yaml
*****
*
* theHarvester
*
* theHarvester 4.8.2
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
*****
```

2) Maltego CE (Community Edition)

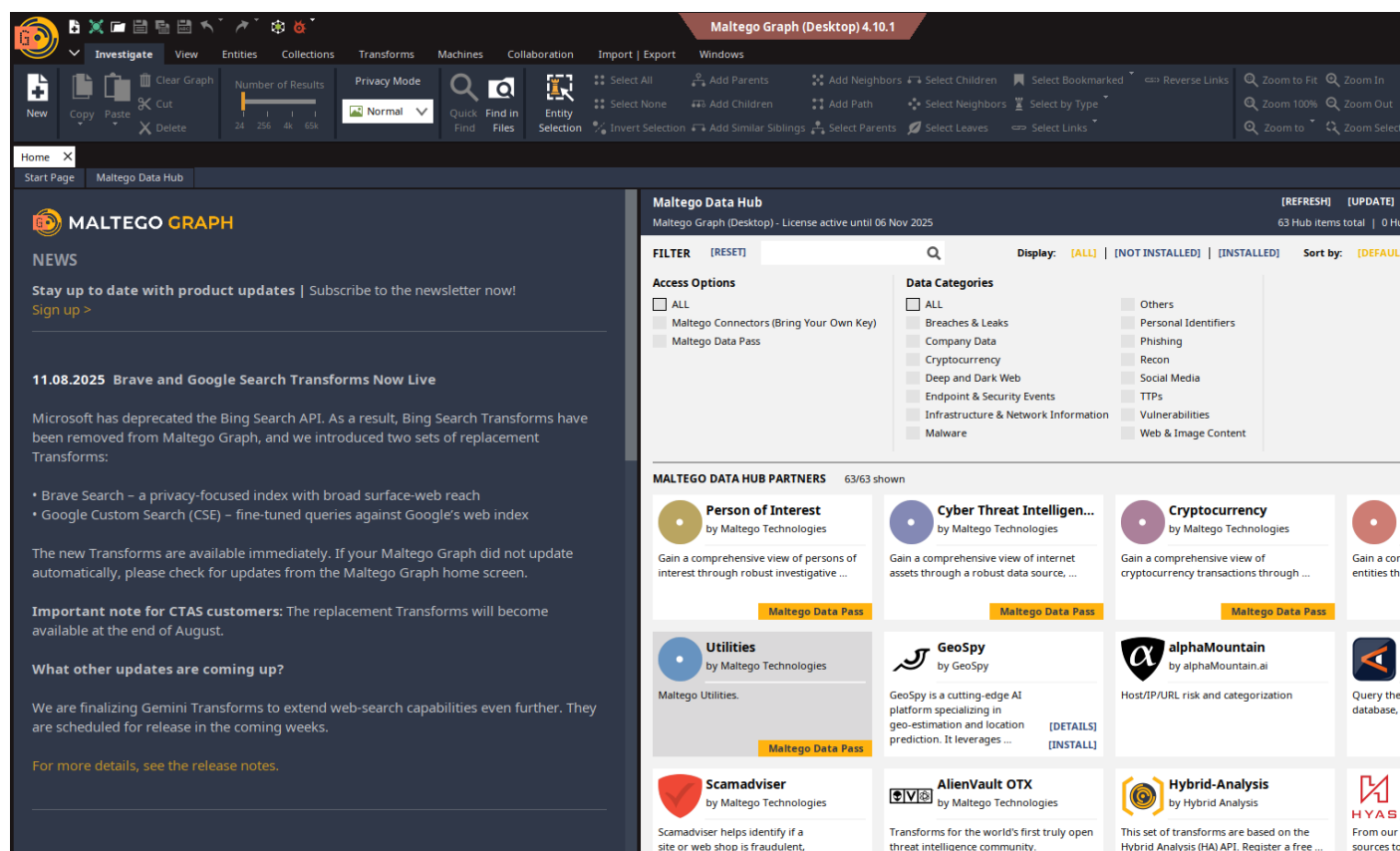
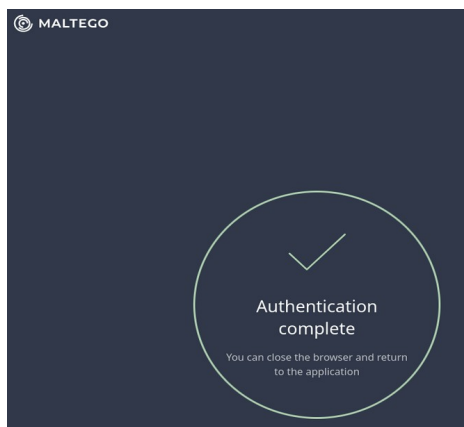
Kali Linux (paquete disponible) — opción rápida:

```
sudo apt update
sudo apt install maltego -y
# iniciar
maltego
```

Instalación oficial (recomendado para obtener la última versión):

1. Descargar el instalador desde la web de Maltego (Maltego CE).
2. Ejecutar el instalador (.deb en Debian/Kali o .rpm) o el instalador para Windows/macOS.
3. Crear cuenta Maltego y activar la licencia CE (gratuita).

Maltego es GUI — requiere entorno gráfico. En Kali con Xfce/Plasma funciona sin problemas.



3) Metagoofil

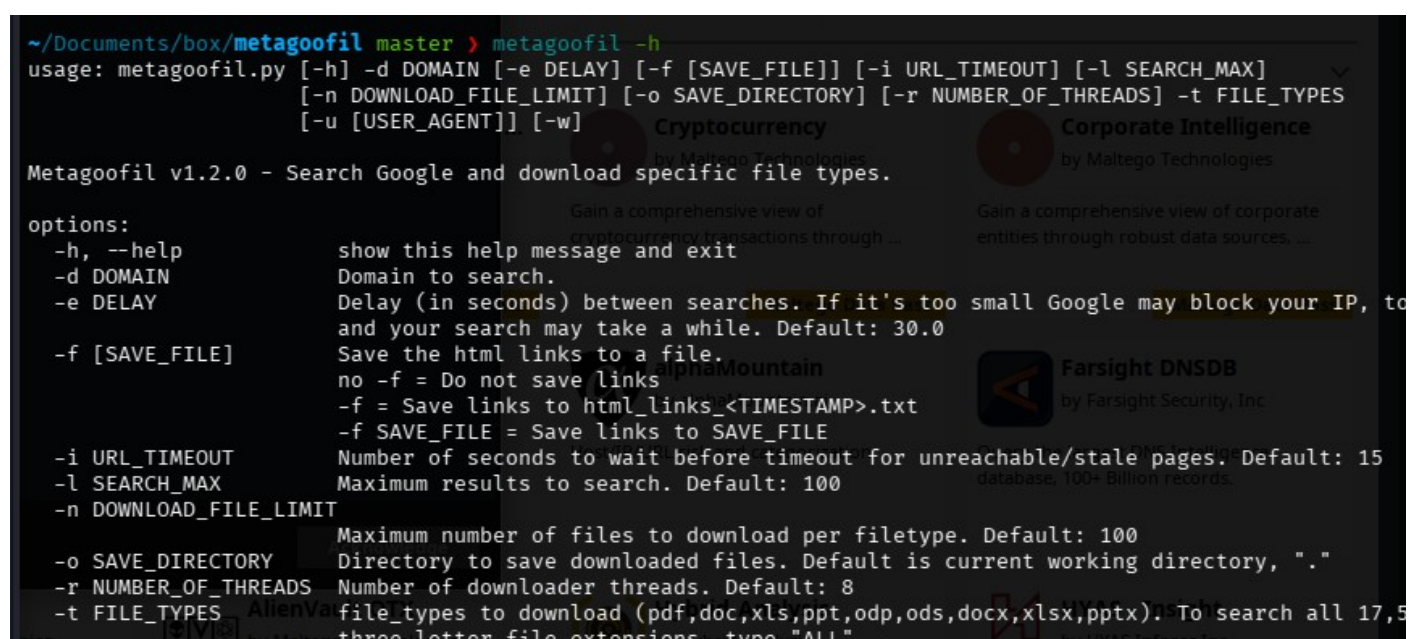
Kali Linux:

Metagoofil suele venir en los repositorios de Kali o en /usr/share/metagoofil. Para instalar desde git:

```
sudo apt update
sudo apt install git python3 -y

cd metagoofil
# si precisa dependencias:
python3 -m pip install -r requirements.txt --user
# ejecutar
python3 metagoofil.py -h
```

Windows/macOS: clonar repositorio y ejecutar con Python 3 (instalar dependencias).



```
~/Documents/box/metagoofil master > metagoofil -h
usage: metagoofil.py [-h] -d DOMAIN [-e DELAY] [-f [SAVE_FILE]] [-i URL_TIMEOUT] [-l SEARCH_MAX]
                    [-n DOWNLOAD_FILE_LIMIT] [-o SAVE_DIRECTORY] [-r NUMBER_OF_THREADS] [-t FILE_TYPES]
                    [-u [USER_AGENT]] [-w]

Metagoofil v1.2.0 - Search Google and download specific file types.

options:
  -h, --help            show this help message and exit
  -d DOMAIN              Domain to search.
  -e DELAY              Delay (in seconds) between searches. If it's too small Google may block your IP, too
                        and your search may take a while. Default: 30.0
  -f [SAVE_FILE]        Save the html links to a file.
                        no -f = Do not save links
                        -f = Save links to html_links_<TIMESTAMP>.txt
                        -f SAVE_FILE = Save links to SAVE_FILE
  -i URL_TIMEOUT        Number of seconds to wait before timeout for unreachable/stale pages. Default: 15
  -l SEARCH_MAX         Maximum results to search. Default: 100
  -n DOWNLOAD_FILE_LIMIT
                        Maximum number of files to download per filetype. Default: 100
  -o SAVE_DIRECTORY     Directory to save downloaded files. Default is current working directory, "."
  -r NUMBER_OF_THREADS  Number of downloader threads. Default: 8
  -t FILE_TYPES         file_types to download (pdf,doc,xls,ppt,odp,ods,docx,xlsx,pptx). To search all 17,5
                        three-letter file extensions, type "All"
```

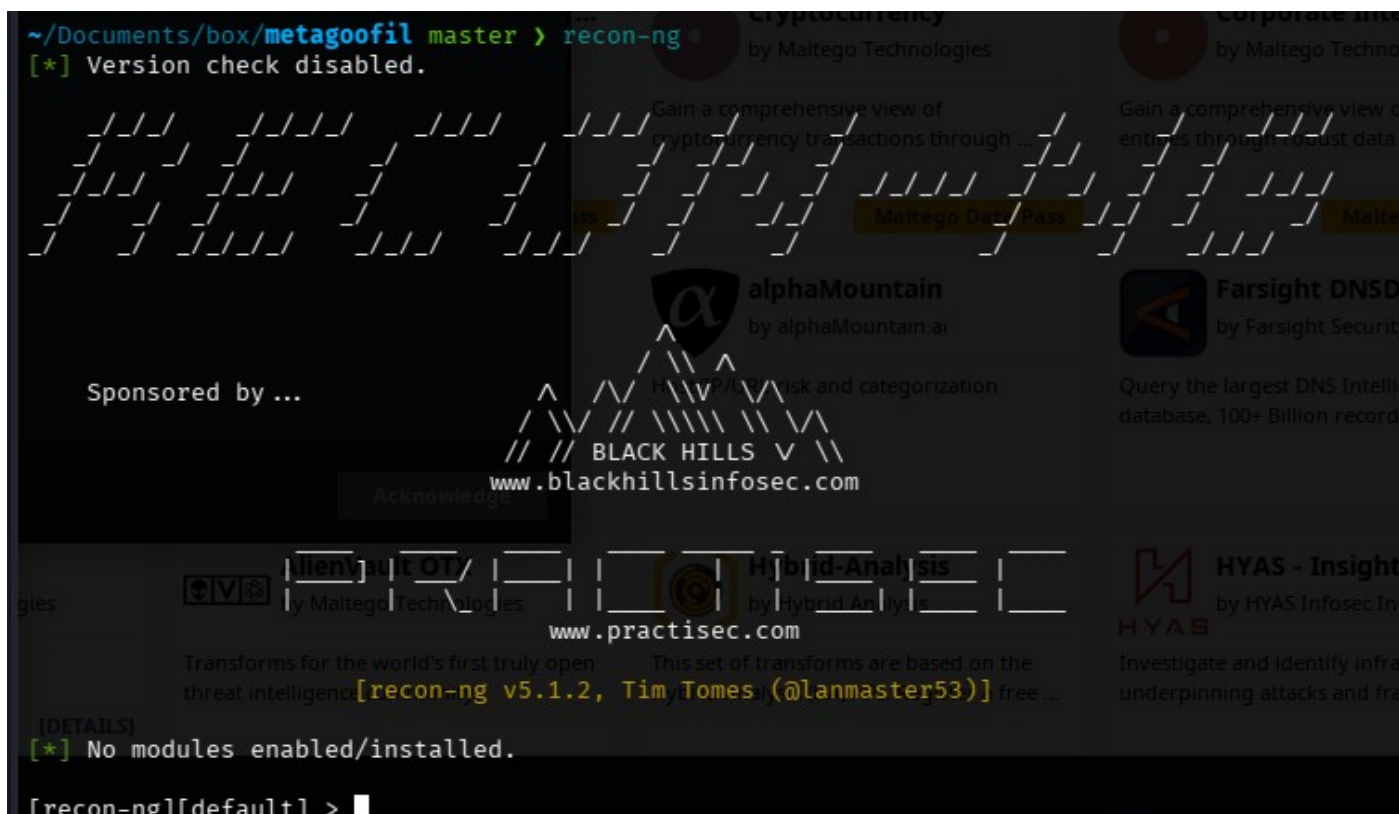
4) Recon-ng

Kali Linux (repo oficial):

```
sudo apt update
sudo apt install recon-ng -y
# comprobar
recon-ng --version
```

Instalación manual via pip (si hace falta):

```
git clone https://github.com/lanmaster53/recon-ng.git
cd recon-ng
python3 -m pip install -r REQUIREMENTS
python3 recon-ng
```



5) dnsenum

Kali Linux:

```
sudo apt update
sudo apt install dnsenum -y
# comprobar
dnsenum --help
```

Nota: dnsenum es un script Perl; puede requerir módulos Perl adicionales. Si hay errores, instalar paquetes perl relacionados (libnet-dns-perl, etc.).

```

~/Documents/box/metagoofil master > dnsenum --help
dnsenum VERSION:1.3.1
Usage: dnsenum [Options] <domain>
[Options]:
Note: If no -f tag supplied will default to /usr/share/dnsenum/dns.txt or
the dns.txt file in the same directory as dnsenum
GENERAL OPTIONS:
  --dnsserver <server>      Use this DNS server for A, NS and MX queries.
  --enum                    Shortcut option equivalent to --threads 5 -s 15 -w.
  -h, --help                Print this help message.
  --noreverse               Skip the reverse lookup operations.
  --nocolor                 Disable ANSIColor output.
  --private                 Show and save private ips at the end of the file domain_ips.txt.
  --subfile <file>          Write all valid subdomains to this file.
  -t, --timeout <value>    The tcp and udp timeout values in seconds (default: 10s).
  --threads <value>         The number of threads that will perform different queries.
  -v, --verbose              Be verbose: show all the progress and all the error messages.
GOOGLE SCRAPING OPTIONS:
  -p, --pages <value>      The number of google search pages to process when scraping names,
                           the default is 5 pages, the -s switch must be specified.
  -s, --scrap <value>      The maximum number of subdomains that will be scraped from Google (de
BRUTE FORCE OPTIONS:
  -f, --file <file>        Read subdomains from this file to perform brute force. (Takes priorit
  -u, --update <alg|rlz>   Update the file specified with the -f switch with valid subdomains.
                           a (all)      Update using all results.
                           g            Update using only google scraping results.
                           r            Update using only reverse lookup results.

```

6) exiftool

Kali Linux:

```

sudo apt update
sudo apt install libimage-exiftool-perl -y
# comprobar
exiftool --version

```

Windows: descargar ExifTool para Windows (exiftool(-k).exe) y usar desde cmd.

macOS: brew install exiftool (si tienes Homebrew).

```

~/Documents/box/metagoofil master > exiftool --version
Syntax:  exiftool [OPTIONS] FILE
Consult the exiftool documentation for a full list of options.

```

7) whois / dig

(Útiles para consultas WHOIS y DNS)

Kali Linux:

```
sudo apt update
sudo apt install whois dnsutils -y
# comprobar
whois ejemplo.com
dig ejemplo.com any
```

```
~/Documents/box/metagoofil master > whois example.com
Domain Name: EXAMPLE.COM Display: [ALL] | [NOT INSTALLED] |
Registry Domain ID: 2336799_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.iana.org
Registrar URL: http://res-dom.iana.org Others
Updated Date: 2025-08-14T07:01:39Z
```

```
~/Documents/box/metagoofil master > dig example.com
; <<>> DiG 9.20.11-4+b1-Debian <<>> example.com
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 19255
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;example.com.                IN      A
;; ANSWER SECTION:
example.com. 90      IN      A      23.215.0.136
example.com. 90      IN      A      23.215.0.138
example.com. 90      IN      A      23.220.75.232
example.com. 90      IN      A      23.220.75.245
example.com. 90      IN      A      23.192.228.80
example.com. 90      IN      A      23.192.228.84
;; Query time: 16 msec
;; SERVER: 80.58.61.254#53(80.58.61.254) (UDP)
;; WHEN: Tue Oct 07 12:40:18 CEST 2025
;; MSG SIZE rcvd: 136
```

8) Shodan (CLI / API) — opcional para theHarvester y búsquedas pasivas

Instalar shodan CLI (requiere account + API key):

```
python3 -m pip install --user shodan
# configurar
shodan init TU_API_KEY
# ejemplo consulta
shodan host 8.8.8.8
```

Necesitas registrarte en Shodan para obtener la API key. En clase puedes usar la salida de theHarvester sin Shodan si no hay clave.

9) Herramientas complementarias (jq, pip, git)

Recomendable instalarlas:

```
sudo apt install jq git python3-pip -y
```


Ejercicio 1 — Recolectar correos y subdominios básicos

Objetivo: Obtener correos y subdominios públicos de un dominio de laboratorio.

Herramienta: theHarvester

Prerrequisitos: Kali Linux / red con salida a Internet (o laboratorio aislado). Usar dominioficticio.com.

Pasos / comandos:

1. theHarvester -d dominioficticio.com -b bing -l 200 -f salida1.html

```
~/Documents/box/metagoofil master ?2 > theHarvester -d example.com -b yahoo -l 200 -f salida1.html
Read proxies.yaml from /etc/theHarvester/proxies.yaml
*****
*                               *
*                               *
*                               *
*                               *
*                               *
*                               *
* theHarvester 4.8.2            *
* Coded by Christian Martorella *
* Edge-Security Research        *
* cmartorella@edge-security.com *
*                               *
*****
[*] Target: example.com
[*] Searching Yahoo.
[*] No IPs found.
[*] Emails found: 30
'john.doe@example.com
admin@example.com
administrator@example.com
anything@mailexample.com
email@example.com
firstname@example.com
foo-bar@example.com
j-doe@example.com
john-d@example.com
john-doe@example.com
john.doe@example.com
john.doe@hello.example.com
john@example.com
john_p_smith_lawyer@example.com
johndoe@example.com
jsmith@example.com
mail@example.com
my.name@example.com
myname@example.com
name@example.com
postmaster@example.com

Cyber Threat Intelligence...
by Maltego Technologies

Cryptocurrency
by Maltego Technologies

Corporate Intelligence
by Maltego Technologies

Gain a comprehensive view of
cryptocurrency transactions through ...

Gain a comprehensive view of corpora
entities through robust data sources, ...

Maltego Data Pass
Maltego Data

alphaMountain
by alphaMountain.ai

Host/IP/URL risk and categorization

Farsight DNSDB
by Farsight Security, Inc

Query the largest DNS Intelligence
database. 100+ Billion records
```



```
[*] No people found.
[*] Hosts found: 9
.example.com
www.example.com
finance.example.com
hello.example.com
mail.example.com
server.example.com
static.example.com
sub1.example.com
sub2.example.com
[*] Reporting started.
[*] XML File saved.
[*] JSON File saved.
```

2. Abrir salida1.html y exportar lista en CSV.

Entregable: CSV con correos y subdominios + 1 página con: resumen (máx. 10 líneas) y 3 hallazgos relevantes.

Criterios: Correcta ejecución del comando (30%), limpieza/formato del CSV (30%), análisis claro y riesgos identificados (40%).

```
~/Documents/box/metagoofil master. ?2 > cat salida1.json
{"cmd": "-d example.com -b yahoo -l 200 -f salida1.html", "emails": ["'john.doe@example.com'", "admin@example.com", "admin", "istrator@example.com", "anything@mailexample.com", "email@example.com", "firstname@example.com", "foo-bar@example.com", "j-doe@example.com", "john-d@example.com", "john-doe@example.com", "john.doe@example.com", "john.doe@hello.example.com", "john@example.com", "john_p_smith_lawyer@example.com", "johndoe@example.com", "jsmith@example.com", "mail@example.com", "my.name@example.com", "myname@example.com", "name@example.com", "postmaster@example.com", "someone@example.com", "test1@example.com", "test@example.com", "test@finance.example.com", "test@mail.example.com", "testing@example.com", "user@example.com", "user@server.example.com", "you@example.com"], "hosts": [".example.com", "www.example.com", "finance.example.com", "hello.example.com", "mail.example.com", "server.example.com", "static.example.com", "sub1.example.com", "sub2.example.com"], "shodan": []}
```

Ejercicio 2 — Búsqueda ampliada por fuentes

Objetivo: Comparar resultados entre fuentes (Google, Bing, Shodan, LinkedIn).

Herramienta: theHarvester

Prerrequisitos: API/entorno que permita búsquedas (si se usa Shodan puede requerir API key).

Pasos / comandos:

1. theHarvester -d dominioficticio.com -b google,bing,shodan,linkedin -l 500 -f salida2.html

```
~/Documents/box/metagoofil master ?4 > theHarvester -d yahoo.com -b bing,shodan,linkedin -l 500 -f salida2.html
Read proxies.yaml from /etc/theHarvester/proxies.yaml
*****
* active until 06 Nov 2025
*
* [Refresh] [Update]
* 63 Hub items total. | 1 Hub items installed (185 Transforms)
*
* [ALL] [NOT STARTED] [UNSTARRED]
*
* theHarvester 4.8.2
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
* Deep and Dark Web
* Endpoint & Security Events
* Infrastructure & Network Information
* Malware
* Others
* Personal Identifiers
* Phishing
* Recon
* Social Media
* Threat Intelligence
* Vulnerabilities
* Web & Image Content
*
* [!] Target: yahoo.com
*
* Read api-keys.yaml from /etc/theHarvester/api-keys.yaml
* Read api-keys.yaml from /etc/theHarvester/api-keys.yaml
*
* [!] Missing API key for Shodan.
* Searching 0 results.
* [!] Searching Bing.
*
* [!] No LinkedIn users found.
*
* [!] LinkedIn Links found: 0
*
* [!] No IPs found.
* [!] No emails found.
* [!] No people found.
* [!] Hosts found: 1
*
* cn.briefcase.yahoo.com
```

2. Separar resultados por fuente y contar elementos únicos.

Entregable: Tabla comparativa (fuente → nº correos → nº hosts) + breve conclusión.

Criterios: Tabla correcta (40%), justificación de diferencias entre fuentes (60%).

```
~/Documents/box/metagoofil master ?4 > cat salida2.json
{"cmd":"-d yahoo.com -b bing,shodan,linkedin -l 500 -f salida2.html","hosts":["cn.briefcase.yahoo.com"],"shodan":[]}
```

Ejercicio 3 — Mapa de relaciones con Maltego CE

Objetivo: Generar un grafo de relaciones (dominio → correos → perfiles).

Herramienta: Maltego CE

Prerrequisitos: Instalar Maltego CE y conocer transforms básicos.

Pasos:

1. Crear nuevo graph.
2. Añadir entidad Domain con dominioficticio.com.
3. Ejecutar transforms: DNS, Email Addresses, Social Profiles.
4. Exportar gráfico PNG.

Entregable: PNG del grafo + 1 párrafo explicando 3 vínculos relevantes y su riesgo.

Criterios: Grafo legible (40%), transforms adecuados (30%), análisis coherente (30%).

Ejercicio 4 — Extracción masiva de metadatos con Metagoofil

Objetivo: Encontrar metadatos en documentos públicos del dominio.

Herramienta: metagoofil

Prerrequisitos: Acceso a Internet y espacio temporal /tmp.

Pasos / comando:

1. metagoofil -d dominioficticio.com -t pdf,docx,xls -l 100 -n 50 -o /tmp/metadatos
2. Revisar archivos en /tmp/metadatos.

Entregable: Fichero metadatos.txt con autor/usuario/software extraído + recomendaciones.

Criterios: Resultados exportados (40%), identificación de metadatos sensibles (40%), recomendaciones (20%).

Ejercicio 5 — Analizar metadatos con exiftool

Objetivo: Detectar metadatos relevantes en PDF/imágenes.

Herramienta: exiftool

Prerrequisitos: Descargar 2-3 archivos (laboratorio).

Pasos / comandos:

1. exiftool documento.pdf
2. exiftool imagen.jpg
3. Identificar campos: Creator, Producer, Software, GPS.

Entregable: Tabla (archivo → campo → valor) + posible impacto.

Criterios: Exhaustividad (50%), interpretación del riesgo (50%).

```
~/Doc/Ejercicios_seguridad_informatica_2025/P/MODULO 2 AUDITORIA DE SEGURIDAD INFORMATICA main t13 ?1 > exiftool unidad\ 1\ Criterios\ generales.pptx
ExifTool Version Number      : 13.25
File Name                    : unidad 1 Criterios generales.pptx
Directory                   : .
File Size                    : 209 kB
File Modification Date/Time  : 2025:10:07 12:11:41+02:00
File Access Date/Time       : 2025:10:07 12:11:43+02:00
File Inode Change Date/Time  : 2025:10:07 12:11:41+02:00
File Permissions             : -rw-rw-r--
File Type                    : PPTX
File Type Extension          : pptx
MIME Type                    : application/vnd.openxmlformats-officedocument.presentationml.presentation
Zip Required Version         : 20
Zip Bit Flag                  : 0x0006
Zip Compression              : Deflated
Zip Modify Date              : 1980:01:01 00:00:00
Zip CRC                      : 0x064a11e3
Zip Compressed Size          : 790
Zip Uncompressed Size        : 4149
Zip File Name                 : ppt/presentation.xml
Preview Image                 : (Binary data 8313 bytes, use -b option to extract)
Title                        :
Creator                       : Alberto Ruiz
Last Modified By              : Alberto Ruiz
Revision Number               : 1
```

Ejercicio 6 — Enumeración de subdominios con dnsenum

Objetivo: Descubrir subdominios y registros DNS relevantes.

Herramienta: dnsenum

Prerrequisitos: Permisos y dominio de laboratorio.

Pasos / comando:

1. dnsenum dominioficticio.com --enum -o salida_dns.txt
2. Extraer MX, NS, A, CNAME.

Entregable: Informe con lista de subdominios y servidores MX/NS + recomendaciones (ej. restringir servicios, WAF).

Criterios: Cobertura de registros (50%), recomendaciones prácticas (50%).

```
~/Documents/box > dnsenum example.com --enum -o salida_dns.txt
dnsenum VERSION:1.3.1

----- example.com -----

Host's addresses:
-----
example.com.          107      IN      A       23.192.228.84
example.com.          107      IN      A       23.215.0.136
example.com.          107      IN      A       23.215.0.138
example.com.          107      IN      A       23.220.75.232
example.com.          107      IN      A       23.220.75.245
example.com.          107      IN      A       23.192.228.80

Name Servers:
-----
a.iana-servers.net.  1411     IN      A       199.43.135.53
b.iana-servers.net.  1057     IN      A       199.43.133.53
```

Ejercicio 7 — WHOIS y análisis de fechas

Objetivo: Analizar datos de registro y fechas críticas.

Herramienta: whois, dig

Prerrequisitos: Acceso a whois.

Pasos / comandos:

1. whois dominioficticio.com > whois.txt
2. dig +short dominioficticio.com

Entregable: Ficha con registrante, fecha creación/expiración, servidores DNS y un párrafo de riesgos (p. ej. expiración próxima).

Criterios: Exactitud de extracción (50%), identificación de riesgos (50%).

```
~/Documents/box > whois example.com > whois.txt

~/Documents/box > cat whois.txt
Domain Name: EXAMPLE.COM
Registry Domain ID: 2336799_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.iana.org
Registrar URL: http://res-dom.iana.org
Updated Date: 2025-08-14T07:01:39Z
Creation Date: 1995-08-14T04:00:00Z
Registry Expiry Date: 2026-08-13T04:00:00Z
Registrar: RESERVED-Internet Assigned Numbers Authority
Registrar IANA ID: 376
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
```

Ejercicio 8 — Buscar servicios expuestos (información pasiva)

Objetivo: Localizar servicios públicos asociados al dominio (puertos, banners).

Herramienta: theHarvester (Shodan) / resumen con Shodan si procede.

Prerrequisitos: API Shodan o entorno de laboratorio.

Pasos / comandos:

1. theHarvester -d dominioficticio.com -b shodan -l 200
2. Listar IPs y servicios encontrados.

Entregable: Tabla IP → servicio → puerto → posible vulnerabilidad + prioridad de mitigación.

Criterios: Identificación correcta (40%), priorización (60%).

```
~/Documents/box > theHarvester -d example.com -b shodan -l 200
Read proxies.yaml from /etc/theHarvester/proxies.yaml
*****
*                                                                 *
*  _ _ _ _ _  ^  ^  _ _ _ _ _  _ _ _ _ _  _ _ _ _ _  _ _ _ _ _  *
*  | | | | | / \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / | *
*  | | | | | / \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / | *
*  \_|_|_|_|_| \_/_/_/_/_ \_/_/_/_/_ \_/_/_/_/_ \_/_/_/_/_ \_/_/_/_/_ *
*                                                                 *
* theHarvester 4.8.2                                           *
* Coded by Christian Martorella                               *
* Edge-Security Research                                       *
* cmartorella@edge-security.com                               *
*                                                                 *
*****

[*] Target: example.com

Read api-keys.yaml from /etc/theHarvester/api-keys.yaml

[!] Missing API key for Shodan.

[*] No IPs found.

[*] No emails found.

[*] No people found.

[*] No hosts found.
```


Ejercicio 9 — Recon-ng: workspace y módulos básicos

Objetivo: Usar recon-ng para almacenar y modularizar la recolección.

Herramienta: recon-ng

Prerrequisitos: Recon-ng instalado.


Pasos:

1. recon-ng → workspaces create practica1
2. add domains dominioficticio.com
3. modules load recon/domains-hosts/brute_hosts (u otros) → configurar y run
4. db export para salida.

Entregable: Export DB (CSV) + README con módulos usados y resultados clave.

Criterios: Uso correcto de workspace (30%), elección de módulos (30%), análisis (40%).

```
~/Documents/box > recon-ng  
[*] Version check disabled.
```



```
Sponsored by ...  
  
      ^   ^   ^  
     / \ / \ / \  
    /  \ //  \\ V  \  
   //  // BLACK HILLS V  \  
www.blackhillsinforesec.com
```



```
www.practisec.com
```

```
[recon-ng v5.1.2, Tim Tomes (@lanmaster53)]
```

```
[*] No modules enabled/installed.
```

```
[recon-ng][default] > add domains example.com  
[!] Invalid command: add domains example.com.  
[recon-ng][default] > help
```

```
Commands (type [help|?] <topic>):
```

back	Exits the current context
dashboard	Displays a summary of activity
db	Interfaces with the workspace's database
exit	Exits the framework
help	Displays this menu
index	Creates a module index (dev only)
keys	Manages third party resource credentials
marketplace	Interfaces with the module marketplace
modules	Interfaces with installed modules
options	Manages the current context options
pdb	Starts a Python Debugger session (dev only)
script	Records and executes command scripts
shell	Executes shell commands
show	Shows various framework items
snapshots	Manages workspace snapshots
spool	Spools output to a file
workspaces	Manages workspaces

```
[recon-ng][default] > modules load recon/domains-hosts/brute_host  
[!] Invalid module name.  
[recon-ng][default] >
```

Ejercicio 10 — Identificación de correos en redes sociales

Objetivo: Encontrar correos o usuarios vinculados a personas ficticias.

Herramienta: Maltego / theHarvester / búsquedas manuales.

Prerrequisitos: Nombre ficticio y dominio de la organización.

Pasos:

1. Buscar en LinkedIn, GitHub, Twitter y Maltego transforms de persona.
2. Registrar correos / cuentas encontradas.

Entregable: Lista de perfiles con evidencia (capturas) y valoración de riesgo para ingeniería social.

Criterios: Evidencia (40%), valoración de riesgo (60%).

Ejercicio 11 — Auditoría de huella pública de una persona

Objetivo: Evaluar la exposición pública de un perfil profesional.

Herramienta: Navegador + Maltego + theHarvester

Prerrequisitos: Perfil ficticio con nombre y empresa.

Pasos:

1. Recolectar LinkedIn, GitHub, blogs, fotos públicas.
2. Resumir credenciales expuestas y posibles vectores de ataque.

Entregable: Informe de 1 página: datos expuestos y 5 recomendaciones de mitigación.

Criterios: Identificación completa (50%), recomendaciones aplicables (50%).

Ejercicio 12 — Google Dorks y documentos públicos

Objetivo: Encontrar documentos públicos y evaluar sensibilidad.

Herramienta: Búsqueda avanzada (site:, filetype:) y theHarvester.

Prerrequisitos: Motor de búsqueda (entorno educativo).

Pasos / ejemplo:

1. site:dominioficticio.com filetype:pdf
2. Descargar 3 documentos y analizarlos con exiftool/visor.

Entregable: Lista de documentos + 3 ejemplos de información sensible encontrada.

Criterios: Relevancia de documentos (40%), análisis de sensibilidad (60%).

```
~/Downloads > exiftool libro.pdf
ExifTool Version Number      : 13.25
File Name                    : libro.pdf
Directory                   : .
File Size                    : 953 kB
File Modification Date/Time   : 2025:10:07 13:27:20+02:00
File Access Date/Time        : 2025:10:07 13:27:20+02:00
File Inode Change Date/Time   : 2025:10:07 13:27:20+02:00
File Permissions              : -rw-rw-r--
File Type                    : PDF
File Type Extension          : pdf
MIME Type                    : application/pdf
PDF Version                  : 1.5
Linearized                   : Yes
Author                       : marbeto
Create Date                  : 2012:09:28 13:02:34-05:00
Modify Date                  : 2012:09:28 13:02:34-05:00
XMP Toolkit                  : Adobe XMP Core 4.2.1-c041 52.342996, 2008/05/07-20:48:00
Creator Tool                 : PScript5.dll Version 5.2.2
Producer                    : Acrobat Distiller 9.0.0 (Windows)
Format                      : application/pdf
Title                       : Microsoft Word - J.R.R. Tolkien - La Comunidad del anillo I.doc
Creator                     : marbeto
Document ID                 : uuid:741e49d1-186c-4ae3-87a6-20abfe1df132
Instance ID                 : uuid:ebe75dc4-dec1-41d7-82e8-0db3c5b7ddef
Page Count                  : 183
```

Ejercicio 13 — Cabeceras y metadatos en imágenes

Objetivo: Extraer GPS, software o data incrustada en imágenes públicas.

Herramienta: exiftool

Prerrequisitos: Colección de 3 imágenes de laboratorio.

Pasos / comandos:

1. exiftool imagen1.jpg > meta1.txt (repetir para las otras).
2. Extraer GPS, DateTime, Software.

Entregable: Tabla con metadatos y propuesta de eliminación/limpieza (ej. strip metadata).

Criterios: Exactitud de extracción (50%), medidas de mitigación (50%).

```
~/Downloads > exiftool slider-img-3.jpg
ExifTool Version Number      : 13.25
File Name                    : slider-img-3.jpg
Directory                   : .
File Size                    : 1050 kB
File Modification Date/Time  : 2025:10:07 13:29:47+02:00
File Access Date/Time       : 2025:10:07 13:29:47+02:00
File Inode Change Date/Time  : 2025:10:07 13:29:47+02:00
File Permissions             : -rw-rw-r--
File Type                    : JPEG
File Type Extension         : jpg
MIME Type                    : image/jpeg
JFIF Version                 : 1.01
Exif Byte Order              : Big-endian (Motorola, MM)
Photometric Interpretation   : RGB
Image Description            : Programmer working in a software development and coding technologies. Website desi
gn.Technology concept.
Make                         : FUJIFILM
Camera Model Name           : X-T1
Orientation                  : Horizontal (normal)
X Resolution                 : 300
Y Resolution                 : 300
Resolution Unit              : inches
Software                     : Adobe Photoshop CC 2018 (Macintosh)
Modify Date                  : 2018:12:24 01:17:13
Exposure Time                : 1/80
F Number                     : 3.2
Exposure Program             : Manual
ISO                          : 640
Sensitivity Type             : Standard Output Sensitivity
Exif Version                 : 0230
Date/Time Original           : 2018:12:21 13:22:51
Create Date                  : 2018:12:21 13:22:51
Shutter Speed Value          : 1/80
Aperture Value               : 3.2
Brightness Value             : 1.01
Exposure Compensation        : 0
Max Aperture Value           : 2.8
Metering Mode                : Multi-segment
Light Source                  : Unknown
Flash                       : No Flash
Focal Length                  : 18.0 mm
```

Ejercicio 14 — Correlación DNS ↔ metadatos

Objetivo: Encontrar coincidencias entre rutas/servidores en metadatos y subdominios DNS.

Herramienta: dnsenum, metagoofil, Maltego

Prerrequisitos: Resultados previos de ejercicios 4 y 6.

Pasos:

1. Comparar rutas/hosts en metadatos con subdominios listados.
2. Identificar 3 coincidencias relevantes.

Entregable: Mapa simple (texto o gráfico) y 3 conclusiones.

Criterios: Coincidencias correctas (60%), impacto explicado (40%).

Ejercicio 15 — Crear wordlist de correos/usuarios

Objetivo: Generar una wordlist útil para pruebas defensivas (gestión de accesos).

Herramienta: Salida de theHarvester + scripts (grep/awk).

Prerrequisitos: CSV de correos.

Pasos / comandos:

1. `cat salida.csv | cut -d',' -f1 | sort -u > wordlist_emails.txt`
2. Limpiar dominios irrelevantes.

Entregable: wordlist_emails.txt + explicación de uso legítimo.

Criterios: Calidad de la lista (60%), justificación ética/uso (40%).

Ejercicio 16 — Enumeración inversa de DNS

Objetivo: Relacionar IPs con dominios mediante reverse lookup.

Herramienta: dig, dnsenum

Prerrequisitos: Lista de IPs del dominio (ejercicio 8).

Pasos / comando:

1. `dig -x <IP> +short` por cada IP.
2. Registrar coincidencias.

Entregable: Tabla IP → reverse DNS → observaciones (hosting compartido, colisiones).

Criterios: Exhaustividad (50%), interpretación (50%).

```
~/Downloads > dig -x 23.220.75.232

; <<>> DiG 9.20.11-4+b1-Debian <<>> -x 23.220.75.232
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 42143
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;232.75.220.23.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
232.75.220.23.in-addr.arpa. 43200 IN      PTR      a23-220-75-232.deploy.static.akama

;; Query time: 375 msec
;; SERVER: 80.58.61.254#53(80.58.61.254) (UDP)
;; WHEN: Tue Oct 07 13:32:41 CEST 2025
;; MSG SIZE rcvd: 120

~/Downloads > dnsenum example.com
dnsenum VERSION:1.3.1

----- example.com -----

Host's addresses:
-----
```

example.com.	60	IN	A	23.220.75.232
example.com.	60	IN	A	23.220.75.245
example.com.	60	IN	A	23.192.228.80
example.com.	60	IN	A	23.192.228.84
example.com.	60	IN	A	23.215.0.136
example.com.	60	IN	A	23.215.0.138

Ejercicio 17 — Análisis temporal (historial WHOIS/DNS)

Objetivo: Crear una línea temporal con cambios críticos en WHOIS/DNS.

Herramienta: Recon-ng (módulos históricos) o búsquedas en servicios históricos (en laboratorio).

Prerrequisitos: Acceso a historial (si no, simular cambios en laboratorio).

Pasos:

1. Extraer snapshots (2-3) y comparar cambios.
2. Identificar cambios de registrante, IP o MX.

Entregable: Línea temporal + 2 riesgos derivados (ej. takeover, cambio proveedor).

Criterios: Claridad temporal (50%), análisis de impacto (50%).

Ejercicio 18 — Informe ejecutivo OSINT (1 página)

Objetivo: Sintetizar hallazgos OSINT para dirección.

Herramienta: Cualquier (Word/PDF)

Prerrequisitos: Resultados de ejercicios anteriores.

Pasos:

1. Seleccionar 5 hallazgos clave.
2. Redactar: resumen ejecutivo, riesgos, 5 recomendaciones.

Entregable: PDF de 1 página.

Criterios: Claridad y concisión (60%), relevancia de recomendaciones (40%).

Ejercicio 19 — Proteger la huella digital (plan de medidas)

Objetivo: Diseñar medidas para reducir la exposición pública.

Herramienta: Resultados previos + documento.

Prerrequisitos: Identificación de vectores (metadatos, perfiles, subdominios).

Pasos:

1. Proponer 6 medidas (técnicas y organizativas).
2. Asociar cada medida a un actor responsable.

Entregable: Checklist implementable (6 medidas) + priorización.

Criterios: Practicidad (50%), priorización y responsables claros (50%).

Ejercicio 20 — Auditoría OSINT completa (mini-proyecto)

Objetivo: Realizar un proceso OSINT integral y proponer plan de remediación.

Herramienta: Todas las anteriores (theHarvester, metagoofil, dnsenum, recon-ng, exiftool, Maltego)

Prerrequisitos: Haber completado ejercicios 1–19 (o usar datos de laboratorio).

Pasos:

1. Ejecutar recolección masiva.
2. Correlacionar resultados.
3. Documentar metodología, evidencia y riesgos.
4. Proponer plan de remediación de máximo 6 pasos.

Entregable: Informe final (máx. 4 páginas) + anexos (salida comandos, gráficos).

Criterios: Metodología reproducible (30%), evidencia suficiente (30%), calidad del plan de remediación (40%).