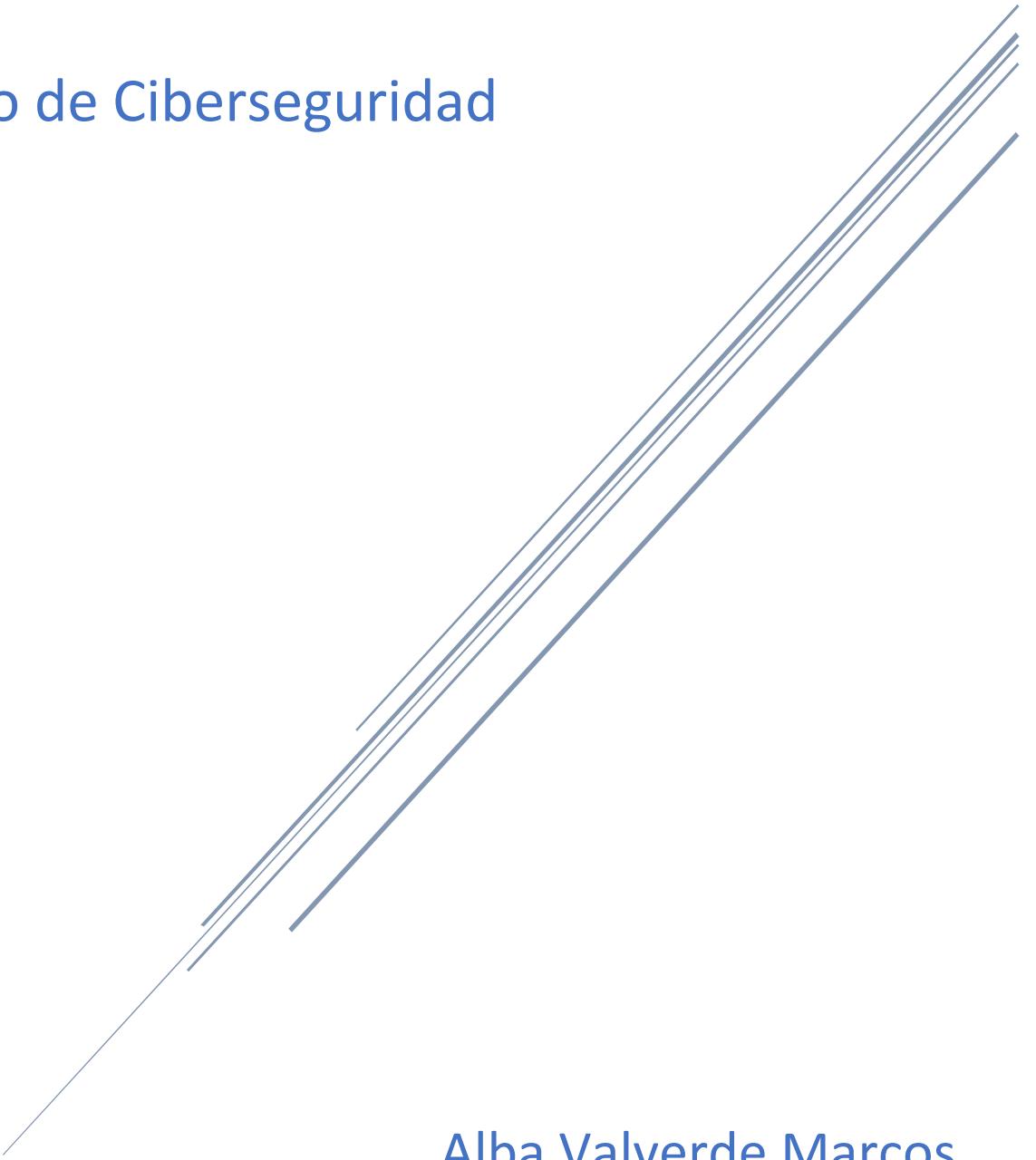


MANUAL

MODULO 4

Curso de Ciberseguridad



Alba Valverde Marcos

1.	<i>ANONIMATO</i>	2
2.	<i>INSTALAR USCRAPPER PARA LINUX (MÁQUINA VIRTUAL)</i>	5
2.	RECUPERACIÓN DE INFORMACIÓN (BLACK BOX).....	7
3.	<i>WAYBACKPAK</i>	7
4.	<i>METADATOS</i>	8
5.	<i>OSINT (ESTUDIO DE REDES ABIERTAS)</i>	12
3.	INGENIERÍA SOCIAL.....	29
6.	29
7.	<i>TIPOS DE PHISING</i>	30
8.	<i>CREAR QR</i>	31
9.	<i>CLICKJACKING</i>	32
10.	<i>IFRAME</i>	32
11.	<i>JACK</i>	33
12.	<i>PASTEJACKING</i>	34
13.	<i>EMAIL SPUFFING</i>	36
14.	<i>VISHING</i>	39
15.	<i>ESTUDIA A TU OPONENTE: ENEATIPO</i>	41
16.	<i>PRINCIPIOS SOCIOLOGICOS DE EFECTIVIDAD</i>	45
17.	<i>CREACIÓN DE PRETEXTOS: COMPORTAMIENTOS Y POSTURAS</i>	46
4.	ESCANEOS NMAP	49
18.	<i>TIPOS DE ESCANEOS</i>	49
19.	<i>PING SWEEPER -sn / -sP</i>	50
20.	<i>ESCANEO TCP</i>	51
21.	<i>DEFINICIÓN DE IP'S</i>	52
22.	<i>DEFINICIÓN DE PUERTOS</i>	53
23.	<i>RESULTADOS DE NMAP</i>	53
24.	<i>EVASIÓN DE FILTROS DE PAQUETES, IDS, FIREWALL</i>	54
25.	<i>CATEGORÍA DE LA BIBLIOTECA DE SCRIPTS</i>	59
26.	<i>NSE – BÚSQUEDA DE SCRIPTS</i>	60
27.	<i>APLICACIONES PARA NMAP</i>	61
28.	<i>WAF</i>	64
29.	<i>EJEMPLOS DE SERVICIOS VULNERABLES</i>	64
5.	CAMPAÑA DE PHISHING.....	66
30.	<i>GOPHISH</i>	66

1. ANONIMATO

Creamos un archivo tipo .txt en Desktop al que añadimos el código básico para una página web, que actuará como index:

```
1 <html>
2 <head>
3 <title> Página Dark Web </title>
4 </head>
5 <body>
6 <p> Ejemplo para MadridS </p>
7 </body>
8 </html>
```

Utilizamos el comando chmod con el código 777 para otorgar todos los permisos a la carpeta *html* (permisos de lectura, escritura y ejecución), aportando el path a dicha carpeta.

```
[root@kali ~]# chmod 777 -R '/var/www/html'
```

Se necesita añadir permisos a la carpeta *html* para poder añadir el archivo .txt que hemos creado, ya que de manera predefinida no los tiene y no se podría agregar archivos a esta carpeta sin dichos permisos.

- R es para la recursividad, es decir, hacer que todos los archivos que se añadan a la carpeta *html* de ahora en adelante van a tener permisos (leer, editar y ejecutar) sin tener que repetir este proceso.

```
[root@kali ~]# ls -l '/var/www/html'
total 20
-rwxrwxrwx 1 root root 10701 Aug 21 14:58 index.html
-rwxrwxrwx 1 root root    615 Aug 21 14:57 index.nginx-debian.html
-rwxrwxrwx 1 kali kali   109 Oct 17 10:04 index.txt
```

Usamos `ls -l` para comprobar que los archivos de la carpeta ahora cuentan con todos los permisos.

Procedemos a renombrar el archivo .txt a index1.html para poder visualizar el contenido de la página web que hemos creado en el navegador.

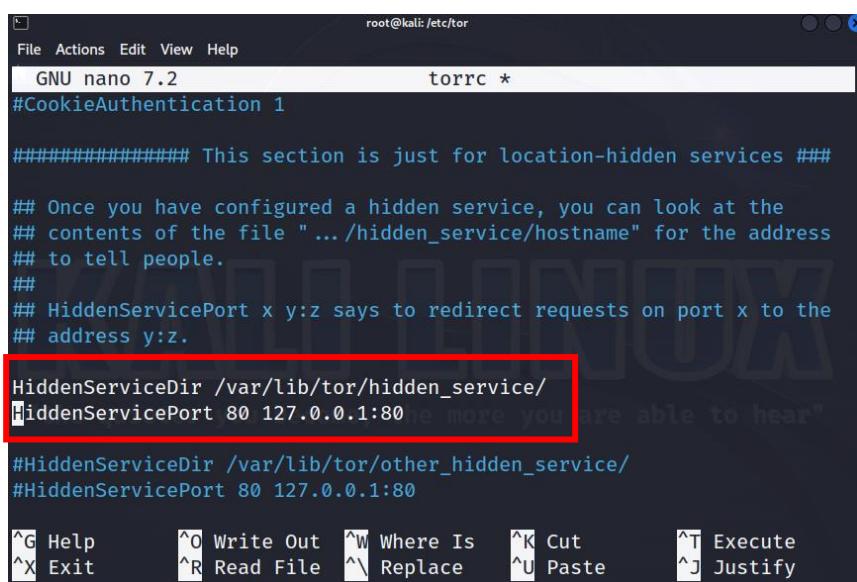
Para poder actuar con anonimato, lo primero que haremos será crear una copia de seguridad del archivo `torrc`, la cual llamaremos `torrc2`. Usamos el comando `ls` para comprobar que se ha creado correctamente.

```
(root㉿kali)-[~/Documents]
# ls
torrc  torsocks.conf

(root㉿kali)-[~/Documents]
# cp torrc torrc2

(root㉿kali)-[~/Documents]
# ls
torrc  torrc2  torsocks.conf
```

Usamos el comando `nano` para editar el archivo `torrc`, modificando estas 2 líneas señaladas, descomentándolas para que sean ejecutables.



```
File Actions Edit View Help
root@kali:~/Documents
GNU nano 7.2          torrc *
#CookieAuthentication 1

#####
## This section is just for location-hidden services ##

## Once you have configured a hidden service, you can look at the
## contents of the file ".../hidden_service/hostname" for the address
## to tell people.
##
## HiddenServicePort x y:z says to redirect requests on port x to the
## address y:z.

HiddenServiceDir /var/lib/tor/hidden_service/
HiddenServicePort 80 127.0.0.1:80

#HiddenServiceDir /var/lib/tor/other_hidden_service/
#HiddenServicePort 80 127.0.0.1:80

^G Help      ^O Write Out  ^W Where Is  ^K Cut      ^T Execute
^X Exit      ^R Read File  ^\ Replace   ^U Paste    ^J Justify
```

Copiar path del HiddenServiceDir para tenerlo guardado para más adelante: **/var/lib/tor/hidden_service/**

Procederemos a parar los servicios de tor y apache2; y ejecutaremos la siguiente línea de comando para crear los nodos tor de nuestra futura página web (de entrada, intermedio y de salida).

```
[root@kali]~[/etc/tor]
# service tor stop && service apache2 stop

[root@kali]~[/etc/tor]
# sudo -u debian-tor tor
```

Con esto hecho, inicializamos los servicios tor y apache2.

```
[root@kali]~[/etc/tor]
# service tor start && service tor status

[root@kali]~[/etc/tor]
# service apache2 start && service apache2 status
```

Usamos el comando cat para crear un enlace en un archivo .onion para acceder a nuestra página web. Si buscamos el enlace .onion en el navegador debe de salir el contenido de nuestra página web.

```
[root@kali]~[/etc/tor]
# cat /var/lib/tor/hidden_service/hostname
nzixydgngvc4occ35oordmk43qjspj4njxdielrhxivdgi5rby35l3qd.onion
```

Si no tenemos archivo index se mostraría en el navegador el contenido de la carpeta *html*. Para solucionarlo podemos obtener y copiar una página web de internet para guardarla como nuestro index.

```
[root@kali]~[/etc/tor]
# wget www.sport.es -O '/var/www/html/index'
```

2. INSTALAR USCRAPPER PARA LINUX (MÁQUINA VIRTUAL)

Uscraper es un programa de recopilación de datos/información de la página web que le indiques.

Para instalarlo, buscamos el código en github y clonamos el directorio en Linux.

```
(root㉿kali)-[~/home/kali]
└─# git clone https://github.com/z0m31en7/Uscraper.git
```

Nos vamos al directorio donde se ha descargado Uscraper y procedemos a otorgar permisos de ejecución e instalar el programa.

```
(root㉿kali)-[~/home/kali/Uscraper/install]
└─# chmod +x ./install.sh && ./install.sh
```

Volvemos al directorio anterior que contiene Uscraper y procedemos a ejecutar el programa. Al ser un archivo .py debemos ejecutarlo con el comando *Python*.

```
(root㉿kali)-[~/home/kali/Uscraper]
└─# python Uscraper-v2.0.py -h
```

Procedemos a ejecutar el programa en una página web:

```
(root㉿kali)-[~/home/kali/Uscraper]
└─# python Uscraper-v2.0.py -u sport.es -c5 -t4
```

-c5 es el número de dominios que quieras sacar

-t4 es los hilos que quieras utilizar

[+] Email Addresses:

?subject=Resultados de los partidos de LaLiga Hypermotion en directo&body=http://www.sport.es/deportes/futbol/segunda-division/

[+] Social Media Links:

<https://www.youtube.com/user/eldiariosport>

<https://twitter.com/SPORT>

<https://www.facebook.com/sport.es>

<https://www.instagram.com/diariosport/?hl=es>

<https://www.facebook.com/sharer/sharer.php?u=http://www.sport.es/deportes/futbol/segunda-division/>

Si pinchamos en el código del comit podemos obtener el correo electrónico de la persona que hizo dicho commit.



z0m31en7 Update Usrapper-v2.0.py

fb91569 on Aug 24 45 commits

Al pinchar nos lleva a otra página. Copiamos la url y buscamos en Firefox dentro de la máquina virtual añadiendo al final .patch. Al buscar nos proporciona varios datos del usuario que ha realizado el código, entre los cuales está el correo electrónico.

```
From fb91569faf61e6bc38fc37bfeab6fbdd59ac304 Mon Sep 17 00:00:00 2001
From: Pranjal Goel <Pranjal.goel6@gmail.com>
Date: Thu, 24 Aug 2023 20:59:39 +0530
Subject: [PATCH] Update Usrapper-v2.0.py

---
Usrapper-v2.0.py | 2 ++
1 file changed, 1 insertion(+), 1 deletion(-)

diff --git a/Usrapper-v2.0.py b/Usrapper-v2.0.py
index be63fe0..2b5380b 100644
--- a/Usrapper-v2.0.py
+++ b/Usrapper-v2.0.py
@@ -235,7 +235,7 @@ def printlist():

    if geolocations0:
        print(colored("\n[+] Geolocations:", "cyan"))
-        geolocations1 = list(OrderedDict.fromkeys(geolocation0))
+        geolocations1 = list(OrderedDict.fromkeys(geolocations0))
        for location in geolocations1:
            print(location)
```

2. RECUPERACIÓN DE INFORMACIÓN (BLACK BOX)

3. WAYBACKPAK

Con Waybackpack podemos enumerar o descargar las páginas web del entorno que busques según el comando que indiquemos.

Al igual que con Uscraper, clonamos el programa de GitHub y lo instalamos en Linus.

```
└─(root㉿kali)-[~/home/kali/Uscraper]
  └─# git clone https://github.com/jsvine/waybackpack.git
```

```
└─(root㉿kali)-[~/home/kali]
  └─# pip install waybackpack.py
```

Para imprimir lista de resultados de la página web que hemos decidido buscar, ejecutamos el comando `--list`.

```
└─(root㉿kali)-[~/home/kali]
  └─# waybackpack http://www.sport.es/ --list
```

En otro caso, para poder descargar los archivos `.html` de la web utilizamos el siguiente comando:

```
└─(root㉿kali)-[~/home/kali]
  └─# waybackpack http://www.sport.es/ -d /home/kali/Desktop/sportarchive --from-date
    2020 --to-date 2023
```

`-d` crea directorio donde quieras que descargue los archivos

`--from-date` desde que fecha buscar

`--to-date` hasta que fecha buscar

Puede que no se cree con este comando el directorio donde queremos guardar los archivos, por lo que habría que crearla con *mkdir* y volver a ejecutar el comando anterior.

Utilizando el comando *tree* y el path del directorio podemos ver en un esquema en forma de árbol los archivos descargados.

```
(root㉿kali)-[~/home/kali/Desktop]
# tree /home/kali/Desktop/sportarchive
/home/kali/Desktop/sportarchive
├── 20200101040855
│   └── www.sport.es
│       └── index.html
└── 20200101050042
    └── www.sport.es
        └── index.html
└── 20200101180355
    └── www.sport.es
        └── index.html
```

4. METADATOS

DATOS EXIF

Para ver los metadatos de una foto vamos a verexif.com y cargamos la imagen que queramos.

DATOS EXIF DE LA IMAGEN			
Fabricante de la cámara :	HUAWEI	Balance de blancos :	Auto
Modelo de la cámara :	HUAWEI P10-L10	Light Source :	Daylight
Fecha y hora :	01/07/2018 19:28:22	Modo de medida :	average
Resolución :	4160 x 3120	Exposición :	program (auto)
Usó flash :	No (auto)	Latitud GPS :	N 43° 44' 4.718612"
Distancia Focal :	3.8mm (35mm equivalent 28mm)	Longitud GPS :	E 7° 15' 10.154481"
Tiempo de exposición :	0.033 s (1/30)	Altitud GPS :	188.84m
Apertura :	f/2.0	JPEG Quality :	94
ISO equiv. :	89	Comentarios :	Hisilicon Balong

Exiftool

Exiftool es un programa que nos permite ver los metadatos de un archivo en con Linux. Descargamos exiftool de github y lo instalamos en la máquina virtual.

```
[root@kali ~]# git clone https://github.com/exiftool/exiftool.git
```

```
[root@kali ~]# apt install exiftool
```

Nos movemos al directorio *exiftool* y ejecutamos *ls -l* para poder ver los permisos de los archivos que hay en la carpeta.

Procedemos a ejecutar *exiftool* para ver los metadatos de un archivo, en este caso una imagen .jpg (la misma que utilizamos en *verexif.com*).

```
[root@kali ~]# ./exiftool '/home/kali/Desktop/ejemplo exif con mock.jpg'  
ExifTool Version Number : 12.68  
File Name : ejemplo exif con mock.jpg  
Directory : /home/kali/Desktop  
File Size : 3.1 MB  
File Modification Date/Time : 2023:10:18 06:16:29-04:00  
File Access Date/Time : 2023:10:18 06:16:29-04:00  
File Inode Change Date/Time : 2023:10:18 06:16:29-04:00  
File Permissions : -rw-rw-rw-
```

Podemos meter los metadatos en un archivo .txt

```
[root@kali ~]# ./exiftool '/home/kali/Desktop/ejemplo exif con mock.jpg' > metadatos.txt
```

Añadiendo a *exiftool* el comando | grep GPS nos muestra únicamente los metadatos de GPS.

```
[root@kali)-[/home/kali/Desktop/exiftool]
# ./exiftool '/home/kali/Desktop/ejemplo exif con mock.jpg' | grep GPS
GPS Version ID : 2.2.0.0
GPS Latitude Ref : North
GPS Longitude Ref : East
GPS Altitude Ref : Above Sea Level
GPS Time Stamp : 17:28:20
GPS Processing Method : GPS
GPS Date Stamp : 2018:07:25
GPS Altitude : 188.8 m Above Sea Level
GPS Date/Time : 2018:07:25 17:28:20Z
GPS Latitude : 43 deg 44' 4.72" N
GPS Longitude : 7 deg 15' 10.15" E
GPS Position : 43 deg 44' 4.72" N, 7 deg 15' 10.15" E
```

Modificar coordenadas GPS de un archivo

Sabiendo las coordenadas de un archivo se puede proceder a cambiarlas con Linux. Al ejecutar el comando crea un archivo nuevo con las coordenadas originales (nombrado con -original). Al archivo que utilizamos se le cambian las coordenadas con los comandos:

```
[root@kali)-[/home/kali/Desktop/exiftool]
# exiftool -exif:gpslatitude=2deg30.2 -exif:gpslatituderef=N -exif:gpslongitude=36deg30.4 -exif:gpslongituderef=E '/home/kali/Desktop/ejemplo exif con mock.jpg'
```

Volviendo a ejecutar *exiftool* sobre el mismo archivo vemos que las coordenadas han sido modificadas.

```
[root@kali)-[/home/kali/Desktop/exiftool]
# ./exiftool '/home/kali/Desktop/ejemplo exif con mock.jpg' | grep GPS
GPS Version ID : 2.2.0.0
GPS Latitude Ref : North
GPS Longitude Ref : East
GPS Altitude Ref : Above Sea Level
GPS Time Stamp : 17:28:20
GPS Processing Method : GPS
GPS Date Stamp : 2018:07:25
GPS Altitude : 188.8 m Above Sea Level
GPS Date/Time : 2018:07:25 17:28:20Z
GPS Latitude : 2 deg 30' 12.00" N
GPS Longitude : 36 deg 30' 24.00" E
GPS Position : 2 deg 30' 12.00" N, 36 deg 30' 24.00" E
```

Cambiar el focal lenght

```
[root@kali]~/Desktop/exiftool  
└─# exiftool -exif:FocalLength=4.2 '/home/kali/Desktop/ejemplo exif con mock.jpg'
```

Cambiar fecha y hora

```
[root@kali]~/Desktop/exiftool  
└─# exiftool -exif:FocalLength=4.2 '/home/kali/Desktop/ejemplo exif con mock.jpg'
```

Borrar metadatos

```
[root@kali]~/Desktop/exiftool  
└─# exiftool -all '/home/kali/Desktop/ejemplo exif con mock.jpg'
```

PDFTK

Extraer metadatos de un pdf en un documento de texto que se crea automáticamente

```
[root@kali]~/Desktop/exiftool  
└─# pdftk '/home/kali/Desktop/pdf.pdf' dump_data output /home/kali/Desktop/meta1.txt
```

Abrimos con *nano* el archivo *meta1.txt* y modificamos los metadatos, creando un nuevo archivo *meta2.txt*

Actualizamos los metadatos del archivo pdf, guardando el archivo con los metadatos cambiados en un pdf nuevo.

```
[root@kali]~/Desktop/exiftool  
└─# pdftk '/home/kali/Desktop/pdf.pdf' update_info '/home/kali/Desktop/meta2.txt' output '/home/kali/Desktop/pdf2.pdf'
```

Creamos un nuevo archivo de texto para comprobar que han sido modificados los metadatos.

```
[root@kali)-[/home/kali/Desktop/exiftool]
# pdftk '/home/kali/Desktop/pdf2.pdf' dump_data output /home/k
i/Desktop/hola.txt
```

5. OSINT (ESTUDIO DE REDES ABIERTAS)

OSINT o *Open Source Intelligence* es conjunto de técnicas y herramientas para recopilar información pública, analizar los datos y convertirlos en conocimiento útil.



Sirve para tomar decisiones basadas en evidencias.

Encontrar la información adecuada es la base de una buena planificación.

En OSINT vamos a sacar información publicada (subida por usuarios, no contrastada) y pública (sale del registro, contrastada).

Lo primero que hay que hacer es crearse un sockpuppet o perfil falso, dentro de una maquina virtual para evitar dejar fingerprint.

Osint Framework ofrece varios entornos de temas diversos para hacer osint (<https://osintframework.com/>).

CARACTERÍSTICAS

- **Eficiente:** Desde el punto de vista de la inversión de recursos y el equilibrio que mantienen con el tiempo y los beneficios generados, el OSINT es la forma de inteligencia que permite obtener más con menos y en el menor plazo.
 - **Rápido:** El acceso a la información abierta permite efectuar de la forma más ágil el ciclo de inteligencia.
 - **Intermediado:** Cuando se hace OSINT se pesca en el mar de datos e información que otros han generado, de tal forma que las fuentes normalmente han pasado por al menos un intermediario, cuando no varios.
 - **Dependiente:** La existencia de intermediarios también indica la presencia de dos extremos, una fuente y un receptor, que respectivamente generan y sufren una dependencia, asimismo tienden a existir numerosos intermediarios en la forma de editores, periodistas, usuarios, medios, etcétera.
 - **Accesible:** El reducido coste económico de los medios que permiten a los individuos llenar el mar de información, es el mismo coste reducido que permite a los buscadores de información hacer OSINT, así pues, cualquier individuo u organización pequeña o grande, rica o pobre, puede hacer uso de esta forma de inteligencia.
 - **Voluminoso:** Con la llegada de Internet, en la que cualquier individuo es una fuente de información, el volumen total se ha disparado hasta convertir a la fase de procesamiento, y no a la de obtención, en el mayor reto.
-

CAMPOS DE APLICACIÓN

PENTESTING

Se utiliza en la etapa de reconocimiento de un pentesting.

Descubrir hosts de una organización, información de Whois, encontrar subdominios, información de DNS, encontrar ficheros de configuración, passwords, etc...

POLICÍA / JUSTICIA

Encontrar las pistas, datos y pruebas necesarias para realizar una investigación.

Verificar la información para poder presentarla ante un juez.

Anticiparse a posibles sucesos delictivos.

RECURSOS HUMANOS

Conocer en profundidad los perfiles de los candidatos reclutados.

Evaluar relaciones entre las personas.

MARKETING

Realizar análisis de la situación del mercado.

Búsqueda de tendencias actuales.

OSR FRAMEWORK

Asegurarse de tener instalado Python y Python-pip. Instalar osrframework y hacerle upgrade.

```
[root@kali]~# apt-get install python3-pip -y
[root@kali]~# pip3 install osrframework
[root@kali]~# pip3 install osrframework --upgrade
```

Con el módulo *usufy* podemos buscar con el nombre de usuario de alguien en todos los sitios de redes sociales. Si ponemos -p podemos especificar la plataforma para la búsqueda.

```
(root㉿kali)-[~/home/kali]
# usufy -n lionelmessi
```

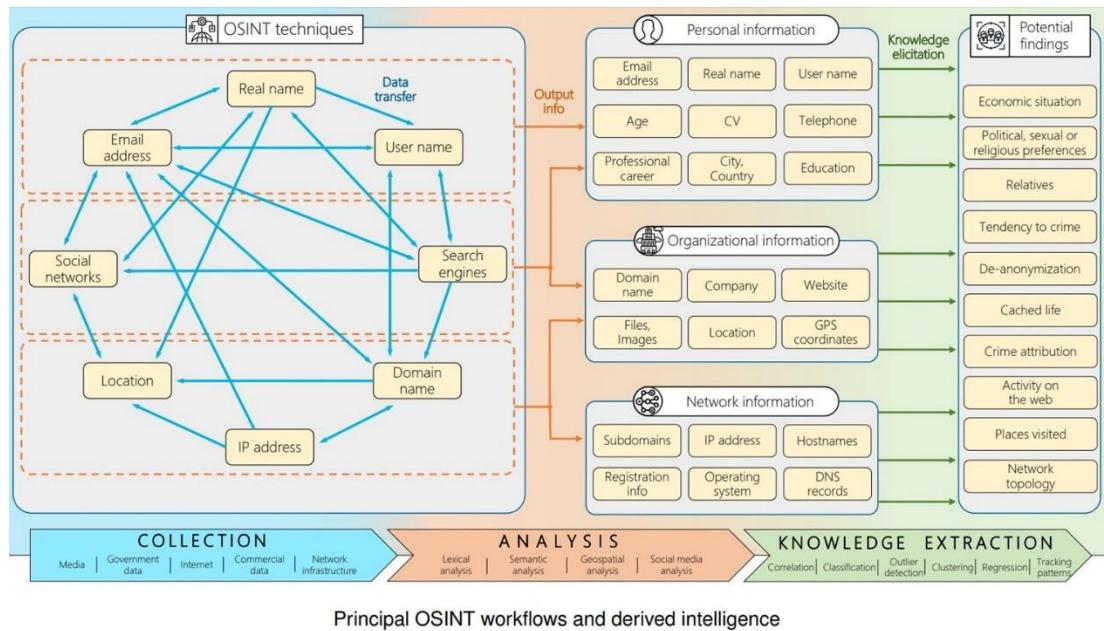
Con el modulo *mailfy* podemos buscar si un correo electrónico se ha utilizado para registrarse en plataformas web. (suele dar falsos positivos).

```
(root㉿kali)-[~/home/kali]
# mailfy -m albaavalverdemarcos@gmail.com
```

Con el módulo *phonefy* podemos buscar si un teléfono esta listado en SPAM.

```
(root㉿kali)-[~/home/kali]
# phonefy -n +034634220056
```

Recopilatorio de OSINT



OSINT DE RECONOCIMIENTO

SHERLOCK

Programa para encontrar Usernames en las redes sociales.

Clonamos el programa Sherlock de GitHub y lo instalamos en Linux en la máquina virtual. Nos vamos a la carpeta *Sherlock* que crea.

```
└─(root㉿kali)-[~/home/kali]
└─# git clone https://github.com/sherlock-project/sherlock.git
```

Instalamos las dependencias que necesita el programa Sherlock para funcionar.

```
└─(root㉿kali)-[~/home/kali/sherlock]
└─# pip3 install -r requirements.txt
```

Dentro de la carpeta Sherlock, hay otra llamada Sherlock (igual) que contiene el archivo *Sherlock.py* que necesitamos para ejecutar el programa con Python y lo ejecutamos con el nombre de usuario que queremos buscar.

```
└─(root㉿kali)-[~/home/kali/sherlock/sherlock]
└─# python3 sherlock.py avalmar
[*] Checking username avalmar on:

[+] Blogger: https://avalmar.blogspot.com
[+] Chess: https://www.chess.com/member/avalmar
[+] Duolingo: https://www.duolingo.com/profile/avalmar
[+] Fiverr: https://www.fiverr.com/avalmar
[+] G2G: https://www.g2g.com/avalmar
```

(estos son solo alguno de los encontrados)

Si queremos que guardar los sitios encontrados en una carpeta podemos añadir el comando *-fo* para crear una carpeta (folder).

```
[└(root㉿kali)-[/home/kali/sherlock/sherlock]
└# python3 sherlock.py avalmar -fo avalmar
```

Otro programa parecido a Sherlock sería Userrecon.

PROFIL3R

Busca perfiles y hace la conjugación de todo el perfil.

Buscar programa en GitHub y seguir las instrucciones para instalar.

```
[└(root㉿kali)-[/home/kali]
└# git clone https://github.com/Greyjedix/Profil3r.git
```

```
[└(root㉿kali)-[/home/kali/Profil3r]
└# python3 setup.py install
```

Ejecutamos y buscamos el nombre que queramos, entre comillas para que no haga conjugación de todo y no tarde tanto.

```
[└(root㉿kali)-[/home/kali/Profil3r]
└# python3 profil3r.py "Alba Valverde Marcos"
```

Resultados (probablemente falso positivo):

```

└ EMAIL ✓
  └ alba valverde marcos@gmail.com      [SAFE]
    └ alba valverde marcos@yahoo.com     [SAFE]
      └ alba valverde marcos@hotmail.com [SAFE]

└ FACEBOOK ✓
  └ https://facebook.com/alba valverde marcos
```

TWITTER

Dentro de la aplicación:

- Interacciones entre 2 usuarios durante el primer semestre de 2023 donde no se incluyen retuits

(from:Jorge to:twitter) OR (from:twitter to:Jorge) since:2023-01-01 until:2023-06-30 RT

- Extraccion de tuis con más de 1000 retuits que contengan el hashtag #elecciones10N e incluyen imágenes o vídeos

#elecciones10n(filter:images OR filter:videos)min_retweets:1000

- Extraer tuits publicados el día 08-02-2023 desde el aeropuerto Internacional Región de Murcia, popularmente conocido como Aeropuerto de Corvera, en un radio de 5km, en los que se incluyan imágenes y se excluyan retuits.

filter:images geocode:39.4467968,-6.3928382,5km since:2023-02-08 until:2023-03-16

- *Hummint*: Técnicas de recopilación información a partir del lenguaje no verbal de las personas.
 - *Signint*: Estudio de las señales
 - *Masint*: Estudio de firmas de radares y cosas así.
 - *Geoint*: Estudio de posicionamiento a partir de imágenes de satélite.
 - *Wardrivers*: Localización de wifi conduciendo.
-

GEOLOCALIZAR A UN USUARIO

1. GPS del móvil -> Longitud y latitud
 2. Dirección IP
 3. Token de tu móvil usando HTML5
 4. Antenas de telefonía:
 - a. Cell ID()-CID/BID
 - b. Local Area Code (LAC)
 - c. Mobile Country Code (MCC)
 - d. Mobile Network Code (m|MNC/SID)
 5. Redes inalámbricas -> MAC de los AP e intensidad
 6. GoogleMaps
-

GEOWIFI

Clonar de Github e instalar.

```
└─(root㉿kali)-[/home/kali/Profil3r]
  └─# git clone https://github.com/GONZOsint/geowifi.git

└─(root㉿kali)-[/home/kali/Desktop/geowifi]
  └─# python3 -m pip install -r requirements.txt

└─(root㉿kali)-[/home/kali/Desktop/geowifi]
  └─# python3 geowifi.py -s ssid eduroam -o map
```

-s buscar por ssid

-o para guardar el nombre (eduroam)

Al ejecutar empieza a escanear para ver dónde está el wifi. Dice que ha buscado cosas que no se han podido cargar porque no se ha encontrado la API, pero sí que se ha guardado.

Para abrirlo, no se puede ejecutar el comando Firefox siendo root, tiene que ser un usuario normal. Se puede hacer exit o abrir una nueva pestaña.

```
(kali㉿kali)-[~]
$ firefox '/home/kali/Desktop/geowifi/results/eduroam.html'
```

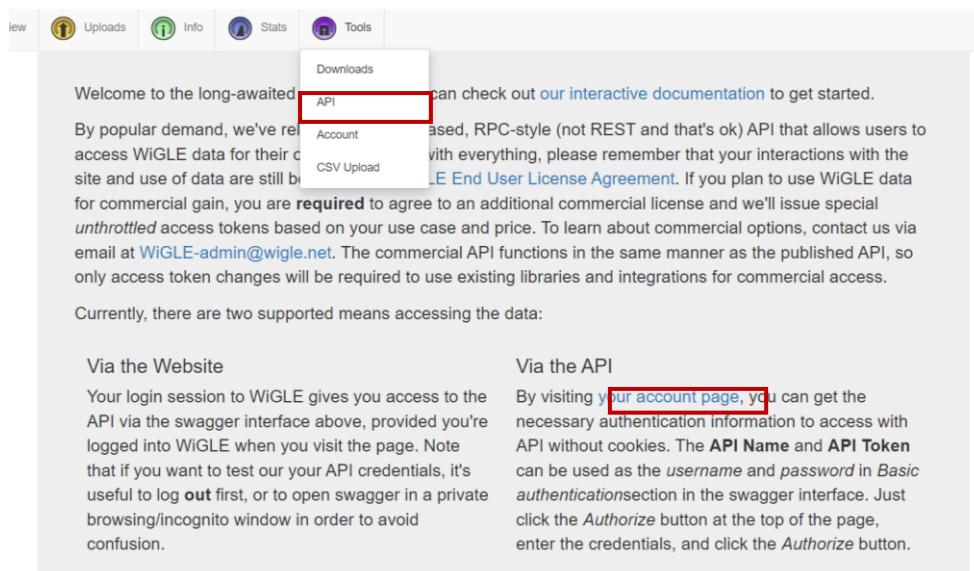
Una vez ejecutado el comando *Firefox* se nos abrirá una ventana en el navegador con ese *.html*.

Para instalar las APIs, nos vamos a la carpeta *gw_utils* y editamos el archivo *config.yaml*.

```
(root㉿kali)-[/home/kali/Desktop/geowifi/gw_utils]
# ls
config.yaml
```

En la página de Github, en el apartado de APIs and configuration file, clicamos en el enlace *obtain an API*. Nos registramos en *wigle.net* con datos aleatorios, ya que no nos van a mandar nada. Asegurarse de poner el @ y .com en el email.

Nos vamos a la pestaña de Tools>API y en *Via de API* le damos a *your account page*. Una vez ahí clicamos en *show my token*. Copiamos el token indicado en *Encoded for use*.



Encoded for use:

QULEMjJmZjcxZjFmMGI5MlI3MDAyZWViNzBmNzRlOTlkNzA6YjUzYzA40WFmMDVmNTQyNzg2ZDYyOThizGQ1NjdjNGQ=

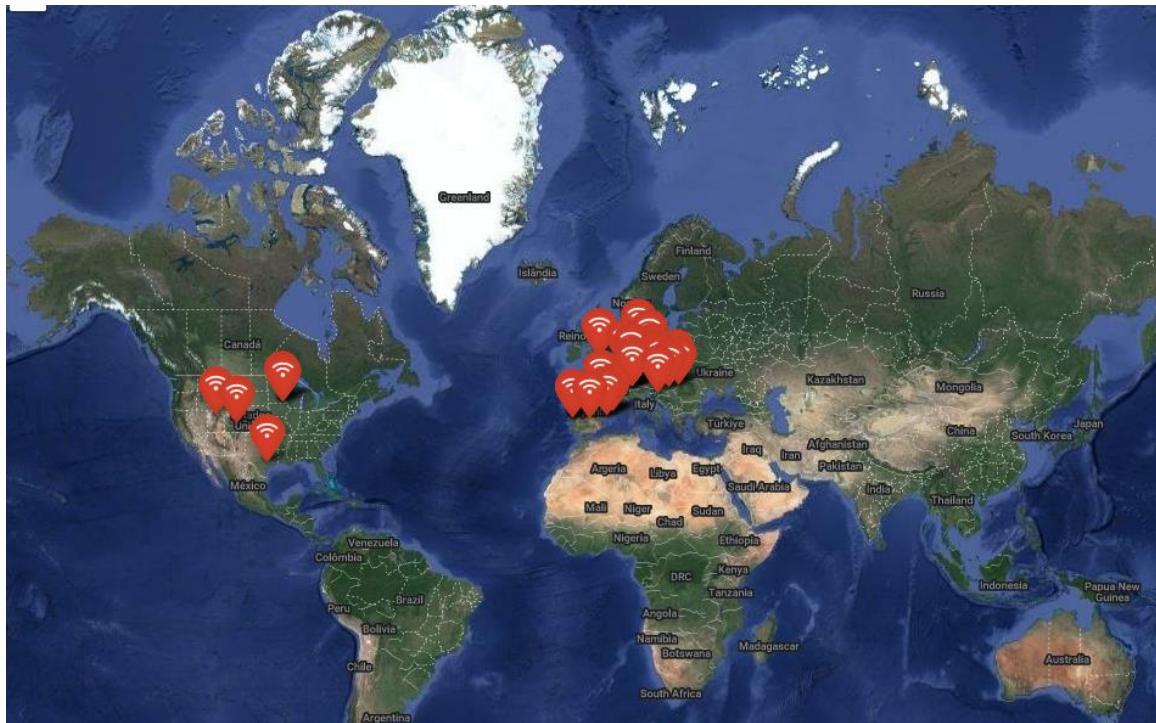
Abrimos con nano *config.yaml* y lo ponemos en wigle. Podemos hacer lo mismo con Google_api y combain_api para tener una mayor base. En la de Google hay que pagar.

```
GNU nano 7.2          config.yaml *
wigle_auth: QULEMjJmZjcxZjFmMGI5MlI3MDAyZWViNzBmNzRlOTlkNzA6Yj>
google_api: XXXX
combain_api: 41ed4ebb3c0cdb455a79
no-ssl-verify: yes
```

Volvemos a ejecutar el mismo comando para ejecutar geowifi. Ahora si que nos saldrían varias localizaciones de la wifi eduroam. Se guardan en el archivo eduroam.html.

```
[root@kali)-[/home/kali/Desktop/geowifi]
# python3 geowifi.py -s ssid eduroam -o map
```

Search Results				
Module	BSSID	SSID	Latitude	Longitude
openwifimap	x	x	x	x
freifunk-karte	x	x	x	x
wigle	00:00:00:00:81:A6	eduroam	30.1782608	-96.91549683
wigle	00:00:00:00:82:AC	eduroam	39.38206863	-105.79504395
wigle	00:00:5E:80:00:21	eduroam	45.79812241	15.97046089
wigle	00:00:6C:B9:5B:0E	eduroam	44.0267067	-92.49004364
wigle	00:00:71:7F:A4:DE	eduroam	52.53739929	13.43200016



OSINT DE LOCALIZACIÓN DE UBICACIÓN

R4VEN

Clonar de GitHub, instalar y ejecutar. Otorgamos permisos con chmod +x.

```
└──(root㉿kali)-[/home/kali]
    └──# git clone https://github.com/spyboy-productions/r4ven.git
```

```
└──(root㉿kali)-[/home/kali/r4ven]
    └──# pip3 install -r requirements.txt
```

```
└──(root㉿kali)-[/home/kali/r4ven]
    └──# chmod +x r4ven.py
```

```
└──(root㉿kali)-[/home/kali/r4ven]
    └──# python3 r4ven.py
```

Nos vamos a discord y copiamos la url de Webhook

>Crear servidor>Ajustes del canal>Integraciones>Crear webhook> Copiar url

Insertar webhook url

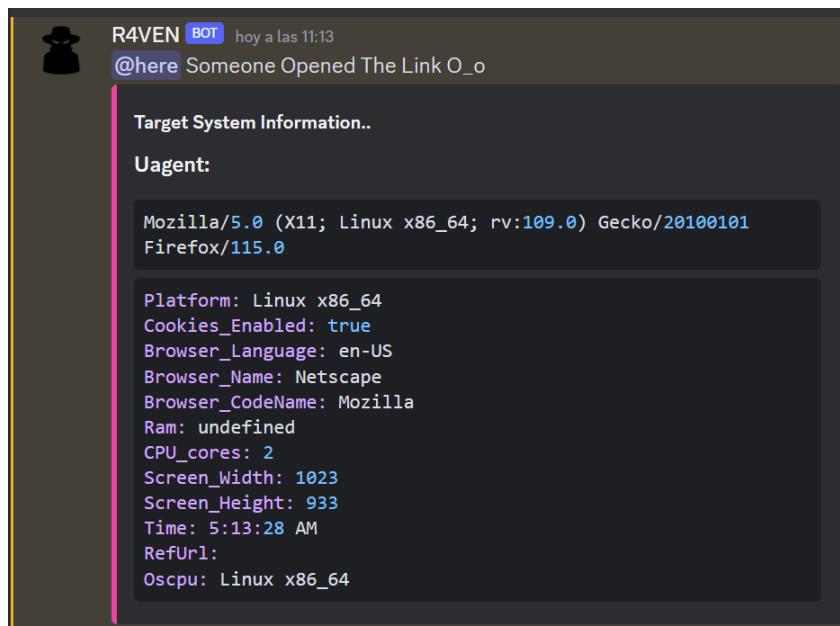
```
Enter Discord Webhook url:  
https://discord.com/api/webhooks/1164491140486139946/WbZ5dQobLdof88  
Q2mJ02DGJz7FilFDQChk-NMmAT9p7gSwMfeHjAAhPUgyact-mAfuv9█
```

Nos salen los siguientes enlaces

```
* Running on all addresses (0.0.0.0)  
* Running on http://127.0.0.1:8000  
* Running on http://192.168.109.109:8000
```

Si nos metemos en la 127 y el hecho de abrir esa página web has mandado tu ip al servidor webhook. Se te manda al discord.

Lo estamos haciendo en red local, la intención es hacerlo para que al mandárselo a alguien y pinche en el enlace saber donde está.



```
IP Address Reconnaissance
success

Continent: Europe
ContinentCode: undefined
Country: Spain
Countrycode: undefined
Regionname: Madrid
Region: MD
City: Madrid
District:
Zip: 28008
Time_zone: undefined
Name: undefined
As: AS12430 VODAFONE ESPANA S.A.U.
Isp: Vodafone Espana S.A.U.
Reverse: 31-4-241-105.red-acceso.airtel.net
Offset: 7200
Currency: EUR
Proxy: false
Mobile: true
Lat: 40.4186
Lon: -3.7323

Target Ip
31.4.241.105
IP Details: https://ip-api.com/#31.4.241.105
Geographic location based on IP address is NOT accurate, it provides the approximate
location of the ISP.
```

SEEKER

Permite capturar el geoposicionamiento de una persona a través de la IP.

IMINT

Estudio de imágenes/video

Cleanup.pictures página q permite borrar elementos de una imagen. Utiliza un IA para reconstruir las imágenes.

HUNTER.IO

Página web que sirve para evaluar el patrón de creación de emails de una empresa.

Poniendo en el buscador una web o empresa será capaz de proporcionarnos un listado con todos los emails encontrados en fuentes de información públicas. Lo que sí queremos tener en cuenta es que necesitaremos registro para saber las direcciones de correo electrónico. Para un usuario normal el servicio es totalmente gratuito, pero si por ejemplo queremos realizar más de 100 solicitudes habrá que pagar la suscripción.

THE HARVESTER

```
[root@kali]~ [~/home/kali/r4ven]
# theHarvester -d ucam.edu -l500 -b all -f resultados
```

-d de qué directorio

-l500 limitar a 500 resultados

-b con q buscador quieras buscar

-f va a descargar toda la información de resultados

Comandos para la recopilación de datos

whois comando para ver datos de un dominio.

curl ipinfo.io para información de tu ip.

curl -I (*ejemplo de web http*) datos de la web.

dig (*ej.web*) dice la ip donde se ejecuta el dominio.

Páginas web para la recopilación de datos

<https://www.robtex.com/>

<https://bgp.he.net>

Al poner un dominio te saca la IP y qué IPs están relacionadas con ese dominio. Se pueden usar para ataques *waterhole*.

Con las IPs obtenidas, hacemos ping para ver si están activas.

HERRAMIENTAS AUTOMATIZADAS: CORRELACIÓN DE DATOS

[MALTEGO](#)

Aplicación (preinstalada en Kali)

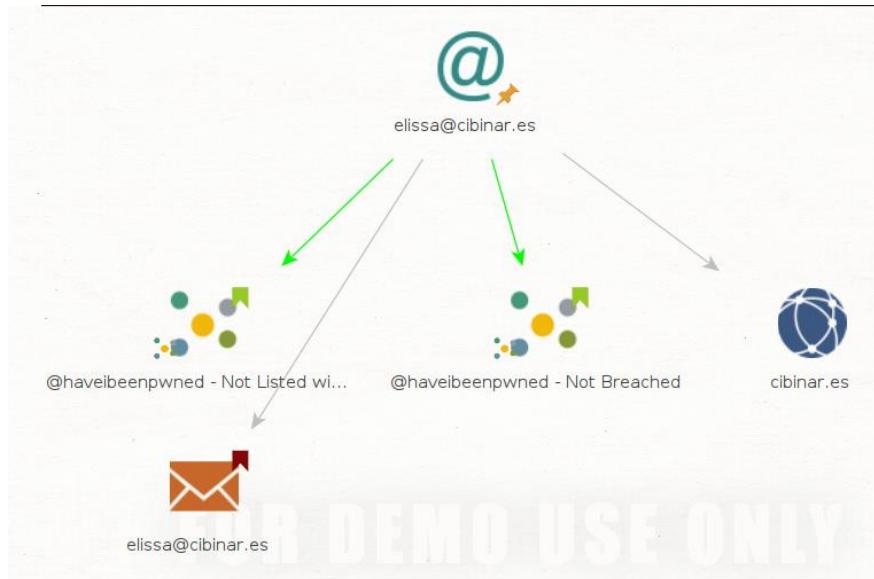
Esta pagina nos da cuentas para hacer login:

<https://bugmenot.com/view/maltego.com>

Tras instalar los módulos que queramos, abrimos un nuevo gráfico.

Seleccionamos email para obtener los datos de un correo electrónico.

Al hacer todas las trasformadas esto es lo que sale:



También puede hacerse para un dominio (domain) o para un número telefónico (phone number).

LAMPYRE

Misma funcionalidad que maltego. En lugar de con una suscripción funciona con saldo (créditos).

IKY PROJECT

Proyecto IKy es una herramienta que recopila información de un correo electrónico y muestra los resultados en una interfaz visual agradable.

Algunas cuestiones para tener en cuenta con la herramienta nació como una PC en un ámbito informático, por lo cual los módulos actuales están muy apuntados a este perfil y estamos trabajando en abrirlo cada vez más. Si bien es una herramienta de “botón gordo” no reemplaza en lo absoluto al ser humano quien debe realizar una validación más profunda de la información presentada.

```
[root@kali ~]# wget http://download.redis.io/redis-stable.tar.gz
[root@kali ~]# tar xvzf redis-stable.tar.gz
[root@kali ~]# make
[root@kali ~]# make install redis-server
[root@kali ~]# redis-server
```

Dejamos la consola con *redis* sin tocar y abrimos una nueva ventana.

Descargamos iKy de <https://kennbroorg.gitlab.io/ikyweb/> y descomprimimos el archivo.

En otra consola nos vamos al directorio donde hemos extraído la carpeta descomprimida de iKy.

```
[root@kali ~]# pip3 install -r requirements.txt
```

Añadimos al PATH la siguiente línea para poder utilizar el servicio *celery*.

```
[root@kali ~]# export PATH=$PATH:/home/kali/.local/bin
```

Navegamos al directorio backend y ejecutamos el script python3:

```
[root@kali ~]# cd /home/kali/Desktop/iky-pack/backend
[root@kali ~]# python3 app.py -e prod
```

3. INGENIERÍA SOCIAL

El eslabón más débil de la seguridad somos las personas.

La ingeniería social es el conjunto de técnicas psicológicas y habilidades sociales (la influencia, la persuasión y la sugestión) implementadas hacia un usuario directa o indirectamente para lograr que este revele información sensible o datos útiles sin estar conscientes de su maliciosa utilización eventual. Pueden ser llevadas a cabo mediante el trabajo con tecnología y ordenadores o a través del trato personal.

El aprovechamiento será tanto de circunstancias intencionales como también de las azarosas.

Mediante la tecnología y ordenadores atacará con configuraciones incorrectas como:

- Falta de parches.
 - Claves por defecto.
 - Sistemas sin soporte.
 - Reuso de claves.
 - Publicación insegura de servicios.
 - Usuarios que hacen click en todo.
 - Claves débiles.
 - Falta de cifrado.
 - Servidores de archivos sin restricción.
-

6.

7. TIPOS DE PHISING

Wire phishing

Tras el análisis a la víctima, descubre que le gustan los perros chiguaga, se le envía una revista plastificada con un cd o dvd serigrafiado a tope de malware. Técnicas de phishing avanzado como **IUWeb Wiew** que permite embeber webs dentro de las aplicaciones móviles y donde hasta hace poco no aparecía el dominio de la web sino tan solo el título de la misma, facilitando así la realización de un phishing.

QRLJacking secuestra un código QR, algunos servicios muy conocidos permiten el acceso a la sesión mediante uno de estos códigos como es el caso de WhatsApp.

Pastejacking

Malware que reemplaza el contenido del portapapeles por otro comando como una url maliciosa, una contraseña u otra información confidencial; de esta manera, cuando pegue y ejecute el comando en la terminal de Linux o PowerShell, su máquina se verá comprometida.

Typo Squatting

O URL hijacking consiste en utilizar un nombre de dominio muy similar al del dominio legítimo, con el fin de poder suplantarla. Se suele utilizar errores tipográficos de los usuarios.

Hay programas como *MaskPhish*.

Páginas como <https://suip.biz/?act=urlcrazy> te permiten identificar posibles alteraciones de un dominio, comprobando en tiempo real si existen y qué servicio se esconde tras el citado dominio para detectar errores tipográficos, secuestro de URL, phishing y espionaje corporativo.

Rogue Apps

Son aplicaciones que aparentan servir para algo, realmente roban datos
SAPPO Spear App o Auth tokens, que es la autenticación delegada y que tan extendida está en la mayoría de los servicios web.

8. CREAR QR

Para una URL maliciosa o un punto de acceso WIFI malicioso.

Si codificamos la siguiente cadena en un código QR, cualquier persona que escanee el código se encontraría automáticamente registrado en la red WIFI codificada.

WIFI:S:{SSID name of your network}; T:{security type -WPA or WEP}; P:{the network password};;

Para obtener códigos QR maliciosos tenemos *MalQR*. Básicamente, es una colección de códigos QR y de códigos de barras maliciosos con cargas comunes como SQLi, XSS, inyección de comandos y fuzzing.

QRGen es una herramienta de Python y viene con una biblioteca integrada que contiene varias cargas útiles/vulneraciones como SQLi, XSS, inyección de comandos, cadena de formato, XXE, Fuzzing de cadenas y LFI/recorrido de directorios.

OHMYQR

Herramienta que genera muchos códigos qr que hace un tipo de ataque

REVEAL QR

Página web tipo app que recoge lo que hace un qr y lo pasa por virus total.

9. CLICKJACKING

Clickjacking, también llamado UI Redress Attack, es cuando un pirata informático utiliza varias capas sólidas para engañar a un usuario para que haga clic en la capa superior sin que se de cuenta. Entonces este ataque está “secuestrando” los clics que no están destinados a la página exacta, sino a una página donde el atacante quiere que esté.

10. IFRAME

Iframe es un elemento de HTML que permite incrustar un documento HTML (una web o fragmento) dentro de otro documento HTML principal (web principal).

Los iframes también cargan las cookies que tengan almacenadas sobre la página en cuestión, por lo que, si tenemos la sesión del blog guardada en el navegador, al cargar el iframe, estaré logueado en mi sesión.

SOLUCIONES

La solución: añadir a la cabecera de la web una de estos dos tipos de cabeceras HTT:

X-Frame-Options

- *X-Frame-Options: deny* – No permite nunca que la web pueda ser incrustada en un iframe.

- *X-Frame-Options: sameorigin* – Solo las webs que sean del mismo origen pueden incrustar la web.
- *X-Frame-Options: allow from <url>* - Para permitir que una web de un origen distinto pueda cargar en un iframe nuestra web.

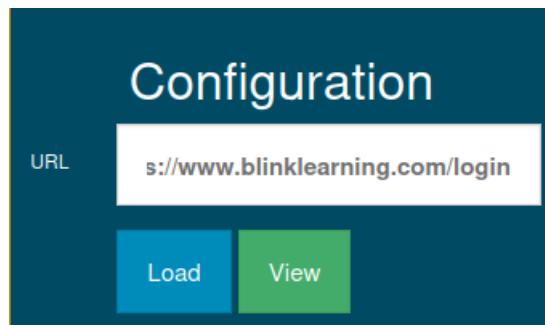
Content Security Policy (CPS)

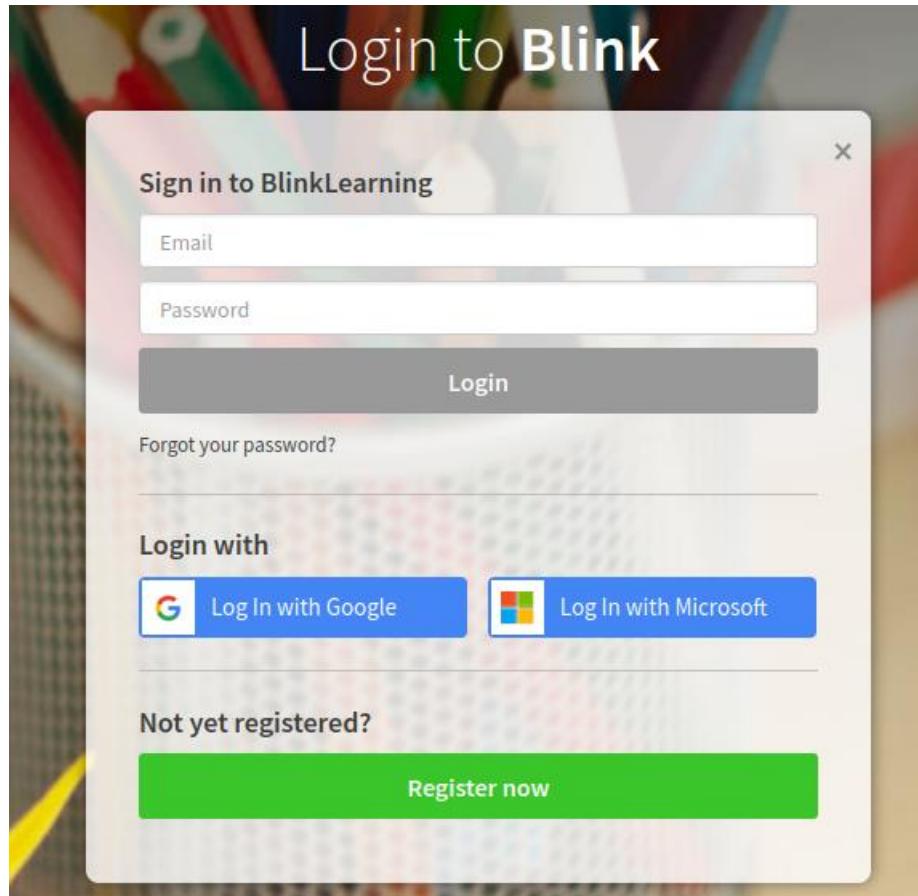
Es más flexible que X-Frame-Options. Puedes poner varios dominios si queremos permitir varios orígenes, e incluso usar asteriscos, por ejemplo:

Content-Security-Policy:'self'https://web.com [https://.ejemplo-web.com](https://*.ejemplo-web.com)*

- *Content-Security-Policy: frame-ancestors'none'* – Equivale a X-Frame-Options:deny.
- *Content-Security-Policy: frame-ancestors'self'* – Equivale a X-Frame-Options:sameorigin.
- *Content-Security-Policy: frame-ancestors<dominio>* - Equivale a X-Frame-Options: allow from <url>

11. JACK





12. PASTEJACKING

Se utiliza un programa malicioso para reemplazar el contenido del portapapeles por otro comando, como una url maliciosa, una contraseña, monedero virtual de cripto u otra información confidencial. De esta manera, cuando pegue y ejecute el comando en la terminal de Linux o PowerShell su máquina se verá comprometida.

Es posible realizarlo de varias maneras:

- Activarlo desde sitios web, lo que requiere conocimientos de desarrollo web.
- Usando scripts automatizados como PasteJacker.

PASTEJACKER

Clonamos PasteJacker de Github y lo instalamos.

```
[root@kali ~]# git clone https://github.com/D4Vinci/PasteJacker.git  
[root@kali ~]# python3 -m pip install ./PasteJacker
```

Ejecutamos pastejacker y completamos los siguientes apartados.

```
[1] Windows  
[2] Linux  
[3] Exit  
[PasteJacker]—[~]—[menu]: 2  
[PasteJacker]—[~]—[What to do with target]: 3  
[PasteJacker]—[~]—[Enter your one-liner]: echo "codigo molón"  
[PasteJacker]—[~]—[Choose template]: 1  
[PasteJacker]—[~]—[Port to serve on (80)]: 80  
[+] Enter the text you want user to see (Press enter twice to finish ... )  
>>> echo "pincha aquí"
```

Abrimos local host en Firefox (127.0.0.1) y copiamos el texto de la cabecera (pondrá echo “pincha aquí”). Abrimos una nueva consola y pegamos, saldrá esto:

```
(kali㉿kali)-[~]$ echo &>/dev/null; clear; echo "codigo sjupesup molón" && clear; # "pi  
ncha aquí"
```

DNS TWIST

Clonamos DNS Twist de Github e instalamos.

```
[root@kali] [/home/kali]
# git clone https://github.com/elceef/dnsth twist.git
[root@kali] [/home/kali/tools/dnsth twist]
# pip3 install -r requirements.txt
```

Ejecutamos DNS Twist. Si es un repositorio grande tarda bastante en escanear las permutaciones.

```
[root@kali] [/home/kali/tools/dnsth twist]
# ./dnsth twist.py facebook.com
```

13. EMAIL SPUFFING

Los servicios Fake Mailers, o servicios de envío de correos falsos son utilizados para enviar correos falsos a los objetivos del phishing, pudiendo incluso suplantar la identidad del remitente.

Esta vía de ingeniería social es muy utilizada por los “phishers”, ya que muchos usuarios confían que un correo es legítimo porque el remitente es una persona conocida, y además, así lo indica el “correo remitente”. Un ejemplo de este servicio es *Emkei’s Mailer*.

Es recomendable realizar un listado con los servicios de Fake Mailers y sus registros MX asociados, para incluirlos en una lista negra para integrarla en nuestra seguridad perimetral o en el propio servidor de correo si lo tenemos externalizado.

Ejemplo de práctica

Se enviaría un correo falso con brevo

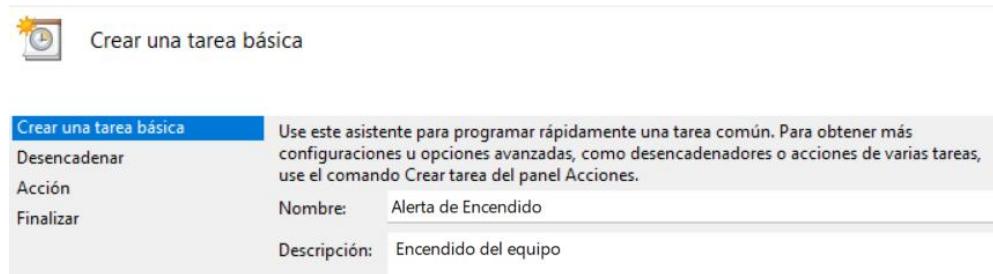
```
[root@kali]~ [~/home/kali/tools/dnstwist]
# sendemail -xu alba.v.m.av@gmail.com -xp 1R -s smtp-relay.brevo.com:587
-f mik@barcelona.com -t albavalverdemarcos@gmail.com -u "Oferta de fichaje"
-m "Hola Alba, hemos estado siguiéndote, eres muy buena y queremos ficharte, te mando la url para llenar tus datos: www.webconacortador.com" -o
```

- -xu correo desde
- -f el correo electrónico que estás suplantando
- -t correo al que vas a mandar el email
- -u asunto (entre comillas)
- -m mensaje (entre comillas)
- -o tls=no (va a salir un fallo que esto evita que pare el programa)

PROGRAMADOR DE TAREAS

Crear alerta para cuando se encienda el ordenador.

Nos vamos al programador de tareas de windows.



Crear una tarea básica

Desencadenar

Acción

- Iniciar un programa
- Enviar un correo electrónico (desusado)
- Mostrar un mensaje (desusado)

Crear una tarea básica

Desencadenar

Acción

Finalizar

- Diariamente
- Semanalmente
- Mensualmente
- Una vez
- Al iniciarse el equipo
- Al iniciar sesión
- Cuando se registre un evento específico

Crear una tarea básica

Desencadenar

Acción

Enviar un correo electrónico

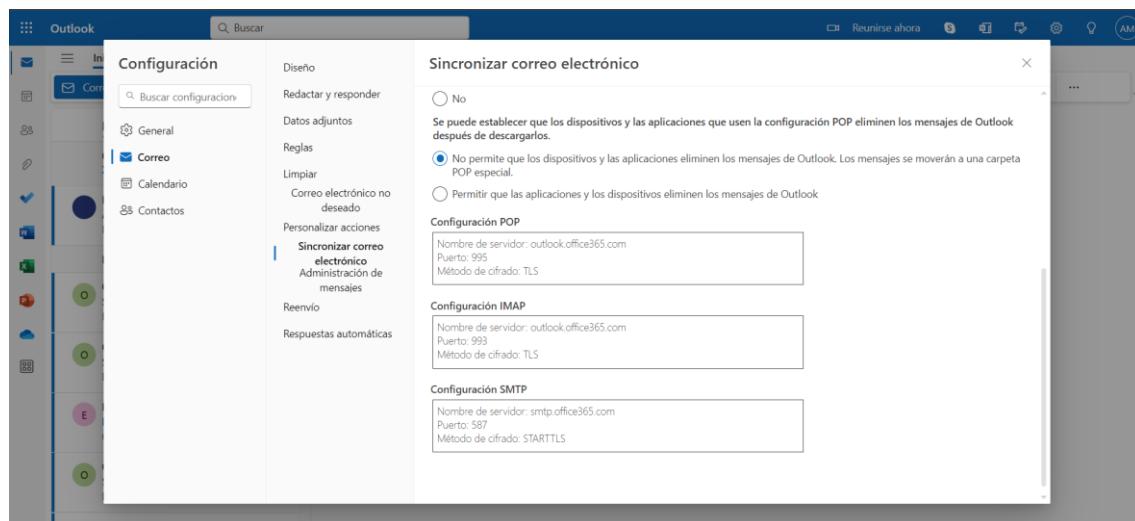
Finalizar

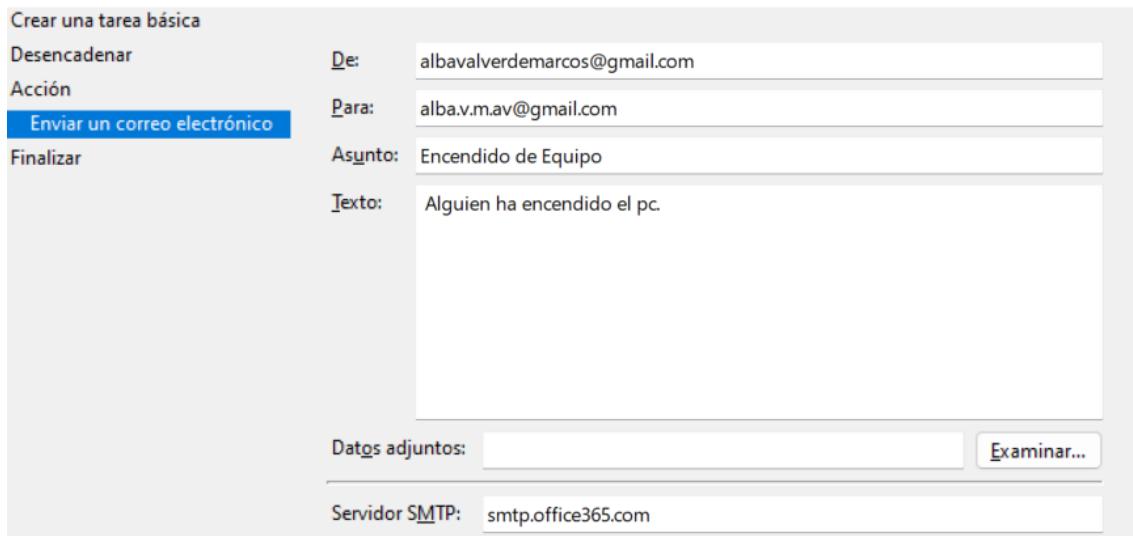
<u>De:</u>	albaivalverdemarcos@gmail.com
<u>Para:</u>	alba.v.m.av@gmail.com
<u>Asunto:</u>	Encendido de Equipo
<u>Texto:</u>	Alguien ha encendido el pc.

Datos adjuntos: Examinar...

Servidor SMTP:

En la página web de outlook copiamos el servidor SMTP





14. VISHING

Engañar a través de audios. Ej. Llamada con guión para sonsacar información.

Como la estafa del sí (graban un audio con tu afirmación y la usan para suplantarte) o estafa del ceo.

ANTI SPOOFING DE DEEP FAKE O DETECCIÓN DE VOZ VIVA

Capacidad de detectar una voz viva de una voz grabada o sintética, estas son imperceptibles para el oído humano pero es posible detectarlas por software basado en IA, entrenados para detectar artefactos que no se encuentran en una voz en vivo

Se pueden meter armónicos (medida, antifakenews).

SMISHING O SMS SPOOFING

Es una estafa en la cual, por medio de mensajes SMS, se solicitan datos o se pide que se llame a un número o que se entre en una web.

Obtener información confidencial, como claves o datos bancarios, pero a veces también para vender productos inexistentes o “infectar” el móvil. Para lograrlo, envían un SMSal usuario con una promoción irresistible, la posibilidad de conseguir un premio o simplemente un aviso de una empresa de mensajería de una entidad bancaria

CARTA NIGERIANA / TIMO 419

- Herencia vacante que la víctima adquirirá.
 - Cuenta bancaria abandonada.
 - Lotería que la víctima ha ganado.
 - Un contrato de obra pública.
 - Una gran fortuna que desean donar generosamente antes de morir.
-

TÉCNICAS DE VISHING

Están divididas en categorías que se caracterizan por el grado de interacción que se tiene con la persona de la que se quiere conseguir información.

Técnicas Pasivas. Observando las acciones de la persona, conocer sus conductas informáticas, obtener datos simples como cumpleaños, nombres de familiares, etc.

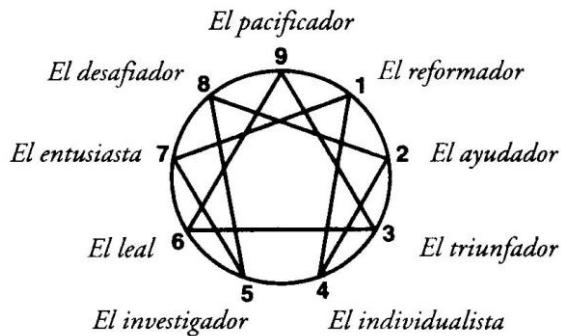
Técnicas No Presenciales. Obtención de información a través de medios de comunicación como Cartas, IRC, email, teléfono... las personas tienden a sobreconfiar datos cuando ven un texto bien escrito y con algún emblema, sello o firma para darle falsa legitimidad.

Técnicas Presenciales No Agresivas. Como seguimiento de personas, vigilancia de domicilios, inmersión en edificios, acceso a agendas y

Dumpster Diving (buscar información como post-it, boletas recibos resúmenes de cuenta, etc. En la basura del investigado).

Técnicas Agresivas. Como la suplantación de identidad (hacerse pasar por IT, servicios técnicos, personal de seguridad, etc.), despersonalización y la más efectiva de las presiones psicológicas. La combinación de estas técnicas junto a la explotación de 3 factores psicológicos antes comentados sobre el afectado, pueden ser altamente efectivos en el trabajo cara a cara entre víctimas.

15. ESTUDIA A TU OPONENTE: ENEATIPO



Descubriendo el eneatipo de la persona a la que quieras atacar puedes adaptar el tipo de phishing que deberías realizar.

ENEATIPO 1: EL REFORMADOR

El tipo idealista de sólidos principios. Las personas tipo Uno son éticas y concienzudas, poseen un fuerte sentido del bien y el mal. Son profesores y cruzados, se esfuerzan siempre por mejorar las cosas, pero temen cometer errores. Bien organizados, ordenados y meticulosos, tratan de mantener valores elevados, pero pueden resultar críticos y perfeccionistas.

Normalmente tienen problemas de rabia e impaciencia reprimidas. En su mejor aspecto, el Uno sano es sabio, perceptivo, realista y noble, a la vez que moralmente heroico.

ENEATIPO 2: EL AYUDADOR

El tipo preocupado, orientado a los demás. Los Dos son comprensivos, sinceros y bondadosos; son amistosos, generosos y abnegados, pero también pueden ser sentimentales, aduladores y obsequiosos. Desean intimar con los demás y suelen hacer cosas por ellos para sentirse necesitados.

Por lo general tienen problemas para cuidar de sí mismos y reconocer sus propias necesidades. En su mejor aspecto, el Dos sano es generoso, altruista y siente un amor incondicional por sí mismo y por los demás.

ENEATIPO 3: EL TRIUNFADOR

El tipo adaptable y orientado al éxito. Las personas tipo Tres son seguras de sí mismas, atractivas y encantadoras. Ambiciosas, competentes y energéticas, también pueden ser muy conscientes de su posición y estar muy motivadas por el progreso personal. Suelen preocuparse por su imagen y por lo que los demás piensan de ellas.

Normalmente tienen problemas de adicción al trabajo y de competitividad. En su mejor aspecto, el Tres sano se acepta a sí mismo, es auténtico, es todo lo que aparenta ser, un modelo que inspira a otras personas.

ENEATIPO 4: EL INDIVIDUALISTA

El tipo romántico e introspectivo. Los tipos Cuatro son conscientes de sí mismos, sensibles, reservados y callados. Son demostrativos, sinceros y personales emocionalmente, pero también pueden ser caprichosos y tímidos. Se ocultan de los demás porque se sienten vulnerables o defectuosos, pero también pueden sentirse desdeñosos y ajenos a las formas normales de vivir.

Normalmente tienen problemas de autocomplacencia y autocompasión. En su mejor aspecto, los tipos Cuatro sanos son inspirados y muy creativos, capaces de renovarse y transformar sus experiencias.

ENEATIPO 5: EL INVESTIGADOR

El tipo vehemente y cerebral. Los Cinco son despabilados, perspicaces y curiosos. Son capaces de concentrarse y enfocar la atención en desarrollar ideas y habilidades complejas. Independientes e innovadores, es posible que se obsesionen con sus pensamientos y elaboraciones imaginarias. Se desligan de las cosas, pero son muy nerviosos y vehementes.

Por lo general tienen problemas de aislamiento, excentricidad y nihilismo. En su mejor aspecto, el Cinco sano es pionero visionario, suele estar en la vanguardia y es capaz de ver el mundo de un modo totalmente nuevo.

ENEATIPO 6: EL LEAL

El tipo comprometido, orientado a la seguridad. Las personas tipo Seis son dignas de confianza, trabajadoras y responsables, pero también pueden adoptar una actitud defensiva, ser evasivas y muy nerviosas; trabajan hasta estresarse al mismo tiempo que se quejan de ello.

Suelen ser cautelosas e indecisas, aunque también reactivas, desafiantes y rebeldes.

Normalmente tienen problemas de inseguridad y desconfianza. En su mejor aspecto, los Seis sanos son estables interiormente, seguros de sí mismos, independientes, y apoyan con valentía a los débiles e incapaces.

ENEATIPO 7: EL ENTUSIASTA

El tipo productivo y ajetreado. Los Siete son versátiles, optimistas y espontáneos; juguetones, animosos y prácticos, también podrían abarcar demasiado, ser desorganizados e indisciplinados. Constantemente buscan experiencias nuevas y estimulantes, pero la actividad continuada los aturde y agota.

Por lo general tienen problemas de superficialidad e impulsividad. En su mejor aspecto, los Siete sanos centran sus dotes en objetivos dignos, son alegres, muy capacitados y muy agradecidos.

ENEATIPO 8: EL DESAFIADOR

El tipo poderoso y dominante. Las personas tipo Ocho son seguras de sí mismas, fuertes y capaces de imponerse. Protectoras, ingeniosas y decididas, también resultan orgullosas y dominantes; piensan que deben estar al mando de su entorno y suelen volverse retadoras e intimidadoras.

Normalmente tienen problemas para intimar con los demás. En su mejor aspecto, los Ocho sanos se controlan, usan su fuerza para mejorar la vida de otras personas, volviéndose heroicos, magnánimos y a veces históricamente grandiosos.

ENEATIPO 9: EL PACIFICADOR

El tipo acomodadizo, humilde. Los tipos Nueve son conformistas, confiados y estables. Son afables, bondadosos, se acomodian con facilidad y ofrecen su apoyo, pero también pueden estar demasiado dispuestos a transigir con los demás para mantener la paz. Desean que todo vaya sobre ruedas, sin conflictos, pero tienden a ser complacientes y a minimizar cualquier cosa inquietante.

Normalmente tienen problemas de pasividad y tozudez. En su mejor aspecto, los Nueve sanos son indómitos y abarcadores; son capaces de unir a las personas y solucionar conflictos.

16. PRINCIPIOS SOCIOLOGICOS DE EFECTIVIDAD

1. *Todos queremos ayudar*, por lo que nos mostramos dispuestos siempre a dar un poco más de lo que se nos pide.
 2. *El primer movimiento es siempre de confianza hacia el otro*, que se explica por sí solo.
 3. *No nos gusta decir NO*, esto lleva a mostrarnos menos reacios a ocultar información y a cuestionarnos si no estaremos siendo muy paranoicos al negar todo y en cómo afectará esto en la idea del otro sobre nosotros.
 4. *A todos nos gusta que nos alaben.*
-

17. CREACIÓN DE PRETEXTOS: COMPORTAMIENTOS Y POSTURAS

La ingeniería social prospera explotando el miedo, la codicia, la amabilidad, la curiosidad, etc., lo que podría llevar a los usuarios a abrir correos electrónicos, hacer clic en enlaces, descargar archivos adjuntos...

- Reclamar autoridad.
 - Generar incomprendión.
 - Voluntad de ayudar: Apelar a la bondad y a la buena fe.
 - Temor a perder un servicio.
 - Respeto social: Miedo que tienen los usuarios a no ser socialmente aceptados o a perder su reputación.
 - Gratis: Ofrecer un producto o servicio gratis a cambio de información privada suele llevarse a cabo por medio de páginas web emergentes de sitios poco legítimos, en mensajes de redes sociales o aplicaciones de mensajería.
-

USO DE PRETEXTOS

1. Personalizar el pretexto.
 2. Simplificar el pretexto para ganar flexibilidad.
 3. Contar con un mapa de ruta.
 - a. Dirigir a una persona pregunta abierta o cerrada.
 - b. Hacer uso de perfil acorde hombre/mujer.
 - c. Usar diferentes habilidades sensoriales (visual, auditivo y cinestésico).
 4. Tener diferentes vías de escape.
-

PYPHISHER

Envía un enlace. Al proporcionar el usuario y la contraseña las guarda.

```
[root@kali]# git clone https://github.com/KasRoudra2/PyPhisher.git  
[root@kali]# pip3 install -r requirements.txt  
[root@kali]# python3 pyphisher.py
```

VIDPHISHER

Igual que el anterior, pero abre la cámara.

```
[root@kali]# git clone https://github.com/KasRoudra/VidPhisher.git
```

Al ser un archivo .sh debe ejecutarse con bash

```
[root@kali]# bash ./vp.sh
```

No tenemos loclx authtoken, damos intro

```
[?] Choose an option:  
[1] Selfie Filter  
[2] Online Meeting  
[d] Change Media Directory (current: /home/kali/tools/VidPhisher)  
[t] Change Type of Media (current: video)  
[p] Change Default Port (current: 8080)  
[s] Change Default Duration (current: 5000)  
[x] About  
[m] More tools  
[0] Exit  
  
Vid@Phisher $ 1
```

```
[✓] URL 1 > https://danny-room-capability-chicago.trycloudflare.com
```

Copiamos enlace y abrimos en chrome (podemos compartir). Cada x tiempo guarda un archivo de video.

Para ver los videos instalamos:

```
(root㉿kali)-[/home/kali/tools/VidPhisher]  
# apt install vlc
```

Para ver el video no podemos actuar como sudo. Con el comando vlc y añadiendo la ruta (mejor arrastrar el archivo) se abriá vlc y se verá el video.

```
(kali㉿kali)-[~]  
$ vlc '/home/kali/tools/VidPhisher/VidPhisher-2023-10-20T10-58-23-143Z.webm'
```

4. ESCANEOS NMAP

18. TIPOS DE ESCANEOS

Las técnicas de escaneo pueden dividirse en dos grupos:

- **Open Scanning** (escaneo abierto). Fiabilidad del 100% en los resultados devueltos, es la que más rastros deja en el log del sistema remoto y la más sencilla de filtrar. Sigue el protocolo TCP. La información es completa y exacta, pero los sistemas de detección de alarmas te pueden detectar.
- **Half Open Scanning** (escaneo a medio abrir).
- **Stealth scanning** (escaneo sigiloso). No termina el protocolo, la información la tienes que interpretar. Lo bueno es que son más sigilosos.

Descubrimiento de la Red

- Ping
- ARP

Descubrimiento de la máquina

- TCP SYN
 - TCP Connect
 - UDP
 - TCP FIN, NULL Xmas
 - ACK
 - Idle (zombie)
-

19. PING SWEEPER -sn / -sP

Nuestro primer objetivo es obtener un “mapa” de la estructura de red o, queremos ver que direcciones IP contienen hosts activos y cuales no. Para ello, hacer un barrido de ping nmap -sn.

Al ejecutar un escaneo por ping puede ser detectado por un IPS.

```
(kali㉿kali)-[~]
└$ nmap -sn 127.0.0.1
```

-sn Manda ping a los equipos y responde si están encendidos o no.

El IDS te detecta y el IPS te detecta y te puede parar. Los sistemas windows tienen el protocolo ICMP desabilitado, por lo que no funciona al hacer ping.

```
(kali㉿kali)-[~]
└$ nmap -sP 127.0.0.1
```

-sP Trata a todos los equipos como si estuvieran encendidos y hace el escaneo (sin ping). Tarda bastante, no se suele utilizar.

-sS solo para cuando se es sudo.

```
(kali㉿kali)-[~]
└$ nmap -Pn 127.0.0.1
```

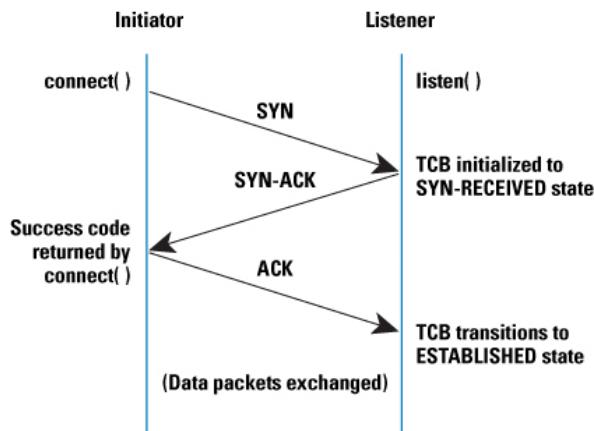
-Pn Hacer un escaneo sigiloso, realizando un escaneo sin ping.

Por defecto, nmap realiza un ping al host antes de realizar un escaneo, nmap al ejecutar un escaneo por ping puede ser detectado por un IPS, si al detectar que el escaneo por ping no fue exitoso hacia el host, nmap envía un mensaje diciendo que el host no se encuentra habilitado y no siempre es así. Tarda más.

20. ESCANEO TCP

ESCANEO TCP connect (-sT)

Análisis de puertos enviando paquetes TCP CONNECT.



Mientras que con el sS (SYN/ACK) dejamos la conexión “a medias”, con este tipo de análisis realizaremos un 3-way-handshake (saludo de 3 direcciones) o lo que es lo mismo, una conexión completa vía TCP.

Usarlo cuando no tenemos acceso root, opción menos eficiente que TCP SYN, ya que requiere más tiempo y paquetes para obtener la misma información.

Problema que tiene es que deja mucho ruido.

```
(kali㉿kali)-[~]
$ nmap -sT 127.0.0.1
```

ESCANEO IDLE SCAN (-sI) Servicios TCP

Utiliza ordenador zombie para hacer el escaneo.

Permite escanear un objetivo sin enviarle un solo paquete utilizando la propia dirección IP origen, por lo que se considera la técnica más avanzada y sigilosa de todas las presentes en Nmap. Para ello es necesario utilizar un tercer equipo, denominado *zombie*, cuya IP tomaremos para que aparezca como fuente de las sondas desde el punto de vista de la máquina objetivo.

La máquina zombie será alcanzable y su implementación TCP/IP genera una secuencia de identificadores IP predecible.

```
[kali㉿kali)-[~]
$ nmap -PO -sN -n -v -p 80 --scanflags SYN,ACT <subred_objetivo>
```

Cualquier objetivo válido debería responder con un paquete RST y por tanto deberá aparecer el puerto 80 como no filtrado.

```
[kali㉿kali)-[~]
$ nmap -sI [IP Zombie][IP víctima].
```

<https://securityhacklabs.net/articulu/hacking-con-nmap-tecnicas-basadas-en-el-escaneo-de-puertos-1>

<https://securityhackslabs.net/articuloo/hacking-con-nmap-tecnicas-basadas-en-el-escaneo-de-puertos-2>

21. DEFINICIÓN DE IP'S

- **nmap target1,target2,etc** Escanear varios objetivos.
 - **nmap target1-target4,etc** Escanear varios objetivos correlativos.
 - **nmap host/mascara** Escanear una subred completa /24.
 - **nmap -iL [list.txt]** Escanear un fichero con hosts.
 - **nmap [10.1.1.1*]** Escanea 10, 11, 12, 13, 14, 15, 16, 17, 18 y 19.
 - **nmap 192.168.1* --exclude 192.168.1.137** Excluir el 137 del mapeado.
-

22. DEFINICIÓN DE PUERTOS

Nmap escanea por defecto los 1000 puertos más “importantes”, consulta estos:

/usr/share/nmap/nmap-services

- **nmap -p [target]** Define los puertos de manera unitaria, conjunta (22, 25), por rango (22-455) o rangos (1*).
 - **nmap -p- [target]** Escanea todos los puertos
 - **nmap –top-ports=10 [target]** Escanea los 10 puertos más importantes.
 - **nmap -F [target]** Escanea los 100 puertos más conocidos.
 - **nmap -sU-sT-p U:[puertos], T:[puertos][target]** Escanea los puertos de protocolo.
 - **nmap -p “*” [target]** Analiza todos los puertos.
 - **nmap -r [target]** Obtiene la lista de puertos ordenados en orden creciente.
 - **nmap –allports [target]** No excluye ningún puerto de la detección de versiones, incluir el 9100 (impresora).
-

23. RESULTADOS DE NMAP

- **Abierto (open)**: Aplicación aceptando conexiones TCP, datagramas UDP o asociaciones SCTP en el puerto.
- **Cerrado (closed)**: El puerto es accesible pero no existe ninguna aplicación escuchando en él. Encontrarlos es frecuentemente el principal objetivo del escaneo de puertos.
- **Filtrado (filtered)**: El paquete que se ha enviado ha sido filtrado por un firewall, reglas del router, etc, y nmap no puede determinar si está abierto o no.

- **Sin filtrar (*unfiltered*):** El puerto es accesible pero nmap no es capaz de determinar si está abierto o cerrado. Este estado solo lo devuelve el tipo de escaneo ACK.
 - **Open | filtered – closed | filtered:** nmap no es capaz de definir si el puerto está abierto/cerrado o filtrado. Ocurre cuando los puertos abiertos no generan respuesta.
 - **Closed | filtered:** Utilizando cuando Nmap no es capaz de determinar si un puerto está cerrado o filtrado. Este es solo utilizado para el escaneo idle IP ID.
-

24. EVASIÓN DE FILTROS DE PAQUETES, IDS, FIREWALL

- **nmap [target] -f:** Fragmentar paquetes, dividir el encabezado TCP en varios paquetes = o < a 8 bytes.
- **nmap [target] --mtu <number>:** Alternativa a -f, pero definiendo el tamaño de los paquetes. El tamaño debe ser múltiplo de 8 (no se puede usar -f y -mtu de forma conjunta).
- **nmap [target] -n:** No hace resolución de dominio.
- **nmap [target] -D d1,d2:** Encubre IPs con análisis con señuelos. Usa ME para poner la posición de tu IP real, en la sexta posición o más tarde para evitar la detección, si no pondrá tu IP de forma aleatoria.
- **nmap [target] -S:** ip, Falsea la dirección origen.
- **nmap [target] -g:** source, Falsea el puerto origen.
- **nmap [target] --source-port:** Falsea el puerto de origen.
- **nmap [target] --randomize-hosts:** nmap aleatorio, no secuencial, lo no predefinido no alerta a los cortafuegos.
- **nmap [target] --spoof-mac mac 00:11:22:33:44:55:** Cambia la MAC de origen; p.e. para filtrado MAC.

- **nmap [target] --scan-delay <time>ms:** Se usa para agregar un retraso entre los paquetes enviados, útil con redes inestables o para evadir cualquier activador de firewall/IDS basado en el tiempo que pueda estar en su lugar.
- **nmap [target] --badsum:** Para detectar la presencia de un cortafuegos/IDS o malas configuraciones. Válido para protocolos TCP, UDP o SCTP.
- **nmap --data-length:** Para enviar una carga aleatoria de Bytes a cada puerto evitando lo predefinido en nmap (el valor de 0 se deshabilita la carga); ralentiza el escaneo pero hace que el escaneo sea menos llamativo.
- **--max-os-tries:** Establecer un número máximo de intentos contra el sistema objetivo.
- **--proxies:** Uno o más servidores proxy HTTP o SOCKS4, expresada como URL en el formato proto://host:port, este comando es solo válido para NSE y el escaneo de versiones (usar proxichains).
- **-T0-5:**
 - **nmap --min-rate [number][target]:** Tasa de paquetes mínimo (5000 es bastante).
 - **nmap --max-rate [number][target]:** Máxima velocidad de paquetes.

EVASIÓN

Cuando se requiere hacer un Pentesting, la forma más optima de realizarlo es siendo sigiloso, de tal manera que cada uno de estos números representan la agresividad con la que se envían los paquetes hacia el (los) host(s).

Rango	Nombre	Detalle
-TO	Paranoico	Muy lento – No recomendable.
-T1	Sigiloso	Útil para la evasión de IDS – Lento.
-T2	Educado	No interfiere con el objetivo – Lento pero recomendable.
-T3	Normal	Escaneo por defecto.
-T4	Agresivo	Escaneo rápido y agresivo – No recomendable.
-T5	Demente	Escaneo muy rápido y muy agresivo – No recomendable.

Otra forma de realizar un escaneo sigiloso es agregar la opción `-f`. Esta opción permite fragmentar los paquetes enviados, de tal manera que esto permitirá regularizar el tráfico enviado hacia el host.

- **-PS n:** envía un TCP SYN al puerto 80 por defecto para descubrir hosts levantados, “n” puede ser otro puerto o puertos a probar.
- **-PA n:** Envía un TCP ACK al puerto 80 por defecto para descubrir hosts levantados, “n” puede ser otro puerto o puertos a probar.
- **-PU n:** Envía un datagrama UDP al puerto 40125 por defecto para descubrir hosts levantados, “n” puede ser otro puerto o puertos a probar.
- **-sL:** No escanea, únicamente lista los objetivos.
- **-PO:** Ping por protocolo.

- **-PN:** No hacer ping.
 - **-n:** No hacer DNS.
 - **-R:** Resolver DNS en todos los sistemas objetivos.
 - **--traceroute:** Trazar ruta al sistema, para topologías de red.
 - **-sP:** Realizar ping, igual que con -PP -PM -PS443 -PA80.
-

GUARDADO

¿Qué pasa cuando hay que analizar un /24 (255 equipos) o un 16 / (65000 equipos) o rangos más grandes no podríamos sacar todo esto por consola?

Nos vamos a las opciones de *nmap*. Añadiendo > doc.txt nos lo guarda en un documento de texto.

```
(root㉿kali)-[~/home/kali]
# nmap
```

Podemos elegir en qué formato guardar los datos de *nmap* con estos comandos.

```
OUTPUT:
-oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt
kIddi3,
      and Grepable format, respectively, to the given filename.
```

-oA va a extraer todos los formatos.

```
-oA <basename>: Output in the three major formats at once
```

Se crean ficheros listos para exportar a herramientas externas.

DESCUBRIMIENTO

- **nmap [target] -v:** Incrementa el nivel de verbosidad (nivel de detalle del escaneo), admite hasta 3 (vvv). **-d (1-9)** para establecer el nivel de depuración.
 - **nmap [target] --packet-trace:** Ruta de paquetes.
 - **nmap [target] --resume file:** Continuar un análisis abortado, tomando formatos de salida con **-oN o -oG**.
 - **nmap -O [target] -6:** Activar análisis IPV6.
 - **nmap –reason [target]:** El motivo por el cual un puerto está marcado como abierto o cerrado y por qué el host está marcado como activo.
-

INFO DEL SISTEMA

- **nmap -O:** Habilitar la detección del sistema operativo fingerprinting.
- **nmap -O --osscan-guess:** Escaneo de sistema operativo. Muy agresivo.
- **nmap -O <target> | grep “OS” | sed -n 1,2p:** Mostrar solo sistema operativo del escaneo.
- **nmap -O --oscan-limit <target>**
- **nmap -sR:** inunda todos los puertos TCP/UDP con órdenes de programa NULL SunRPC para determinar si son puertos RPC y, si es así, los programas y número de versión que están detrás.
- **nmap -sV:** Detección de la versión de servicios, incluye el -sR, por lo que es más usada.
- **nmap --version-intensity <intensidad del 1 al 9>:** Si el número es más alto, el escaneo es más lento y mayor es la probabilidad de identificar el servicio (por defecto el 7).

- **nmap --A [target]**: Detección de la versión de servicios, del sistema operativo, lanzamiento de scripts y traceroute de sus paquetes (incluye -sC, -sO, -sV--traceroute).
 - Es útil para conocer si hay routers intermedios, cuantos saltos damos, comprometer el router...
 - Manda muchos paquetes y nos pueden identificar (IDS).
 - -sC habilita el lanzamiento de scripts para nmap. Intentará interactuar con el servicio para extraer información. Lanza scripts automáticamente sin seleccionarlos en base al servicio, pero no todos los servicios tienen scripts. Podemos generar scripts extensión.nse.
-

25. CATEGORÍA DE LA BIBLIOTECA DE SCRIPTS

- **safe**: No afectará al objetivo.
- **intrusive**: No es seguro. Es probable que afecte al objetivo.
- **vuln**: Explorar en busca de vulnerabilidades.
- **exploit**: Intento de explotar una vulnerabilidad.
- **auth**: Intentar omitir la autenticación para ejecutar servicios (p.e. iniciar sesión en un servidor FTP de forma anónima).
- **brute**: Intento de fuerza bruta de credenciales para ejecutar servicios.
- **discovery**: Intente consultar en ejecución para obtener más información sobre la red (p.e. consultar un servidor SNMP).

Para visualizar los scripts disponibles en bases de datos podemos usar el comando:

- **#locate nse | grep script**: En Linux.
- **#nmap --script-help***: En Windows.

Para obtener información de un script en concreto: **nmap --script-help=<nombre>** -> **nmap --script-help=xmpp-brute**

26. NSE – BÚSQUEDA DE SCRIPTS

OPCIÓN 1

```
(root㉿kali)-[~/home/kali]
└─# locate script.db
    /usr/share/nmap/scripts/script.db

(root㉿kali)-[~/home/kali]
└─# cat /usr/share/nmap/scripts/script.db

Entry { filename = "x11-access.nse", categories = { "auth", "default", "safe", } }
Entry { filename = "xdmcp-discover.nse", categories = { "discovery", "safe", } }
Entry { filename = "xmlrpc-methods.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "xmpp-brute.nse", categories = { "brute", "intrusive", } }
Entry { filename = "xmpp-info.nse", categories = { "default", "discovery", "safe", "version", } }

(root㉿kali)-[~/home/kali]
└─# grep "ftp" /usr/share/nmap/scripts/script.db
Entry { filename = "ftp-anon.nse", categories = { "auth", "default", "safe", } }
Entry { filename = "ftp-bounce.nse", categories = { "default", "safe", } }
Entry { filename = "ftp-brute.nse", categories = { "brute", "intrusive", } }
Entry { filename = "ftp-libopie.nse", categories = { "intrusive", "vuln", } }
Entry { filename = "ftp-proftpd-backdoor.nse", categories = { "exploit", "intrusive", "malware", "vuln", } }
Entry { filename = "ftp-syst.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "ftp-vsftpd-backdoor.nse", categories = { "exploit", "intrusive", "malware", "vuln", } }
Entry { filename = "ftp-vuln-cve2010-4221.nse", categories = { "intrusive", "vuln", } }
Entry { filename = "tftp-enum.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "tftp-version.nse", categories = { "default", "safe", "version", } }
```

OPCIÓN 2

Para buscar categorías:

```
(root㉿kali)-[~/home/kali]
└─# grep "safe" /usr/share/nmap/scripts/script.db

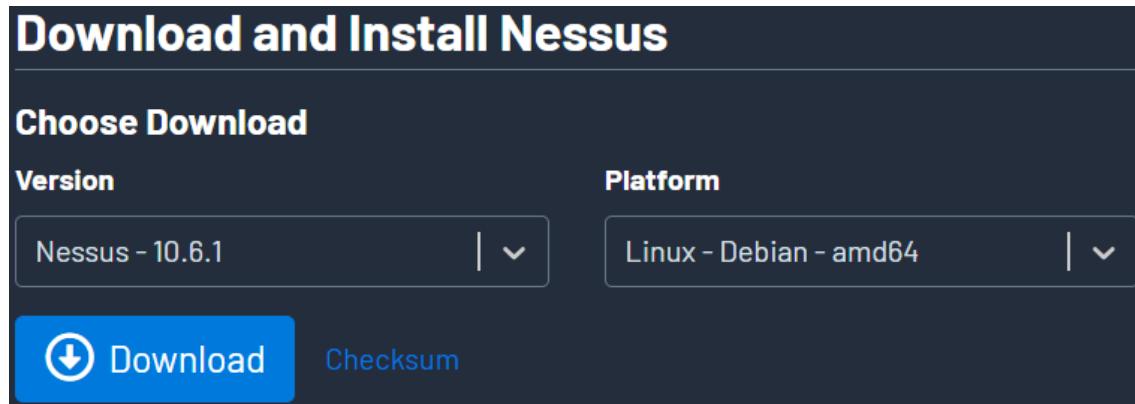
Entry { filename = "acarsd-info.nse", categories = { "discovery", "safe", } }
Entry { filename = "address-info.nse", categories = { "default", "safe", } }
Entry { filename = "afp-ls.nse", categories = { "discovery", "safe", } }
Entry { filename = "afp-serverinfo.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "afp-showmount.nse", categories = { "discovery", "safe", } }
Entry { filename = "ajp-auth.nse", categories = { "auth", "default", "safe", } }
```

27. APLICACIONES PARA NMAP

- Nessus
 - Golismero
 - OpenVAS
 - Nuclei
 - Cariddi
 - Uapití
 - LandGuard
 - Sucubus
 - NeXpose
 - McAfee Vulnerability Manager
 - Acunetix
 - Nikto
 - Cmsmap
 - Wpsan
 - Joomscan
 - Zap
 - Burp suite pro
-

NESSUS

En la web <https://www.tenable.com/downloads/> podemos descargar nessus. Descargamos la versión para Debian10. Permite bajar también las actualizaciones.



Pasamos el archivo .deb a kali y lo abrimos en una terminal.

```
(root㉿kali)-[~/home/kali]
└─# dpkg -i '/home/kali/Desktop/Nessus-10.6.1-debian10_amd64.deb'
```

Creamos un archivo con nano *nessus.txt* y añadimos el siguiente texto para guardar las instrucciones:

```
GNU nano 7.2                         nessus.txt
- You can start Nessus Scanner by typing /bin/systemctl start nessus.service
- Then go to https://kali:8834/ to configure your scanner
```

Podemos ver el estado de Nessus.

```
[root@kali)-[~/home/kali]
# service nessusd status
o nessusd.service - The Nessus Vulnerability Scanner
  Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; preset: disabled)
  Active: inactive (dead)
```

Inicializamos el programa.

```
[root@kali)-[~/home/kali]
# /bin/systemctl start nessusd.service
```

Para arrancar el entorno gráfico nos vamos a linux y buscamos <https://kali:8834/>. Completamos los ajustes para instalarlo. Nos registramos con Nessus Essentials.

OPENVAS

OpenVAS es una herramienta integral de escaneo de vulnerabilidades.

Ofrece pruebas autenticadas y no autenticadas, admite una gama de protocolos industriales y de internet de alto y bajo nivel, proporciona optimización del rendimiento para escaneos a gran escala y presenta un sólido lenguaje de scripting interno para diseñar cualquier prueba de vulnerabilidad.

Se puede descargar de:

<https://github.com/greenbone/openvas-scanner>

NUCLEI

Nuclei es un escáner diseñado para sondear aplicaciones modernas, infraestructura, configuración de nube y redes, ayudando a identificar y corregir vulnerabilidades.

Internamente, Nuclei se basa en el principio de plantillas. Estos archivos YAML detallan cómo identificar, clasificar y corregir amenazas de seguridad específicas.

Una comunidad global de profesionales e investigadores de seguridad contribuye activamente a la biblioteca de plantillas. Este ecosistema, actualizado continuamente dentro de la herramienta Nuclei, ha recibido más de 5000 plantillas

Se puede descargar de:

<https://github.com/projectdiscovery/nuclei>

NIKTO

Nikto es una herramienta de escaneo de servidores web con una base de datos de más de 6700 archivos/programas potencialmente peligrosos, incluidos ciertos archivos o programas, inspecciona las versiones obsoletas de más de 1250 servidores y busca problemas particulares en más de 270 versiones de servidor.

Nikto está diseñado para operaciones discretas.

Su objetivo es evaluar un servidor web lo más rápido posible, dejando rastros evidentes en los archivos de registro o siendo detectable por los sistemas IPS/IDS.

Sin embargo, es compatible con los métodos de *LibBigaining* para contrarrestrar IDS, ya que sea para experimentar o evaluar una configuración IDS.

Se puede descargar de:

<https://github.com/sullo/nikto>

28. WAF

Firewall para aplicaciones web.

Un WAF mantiene el tráfico malicioso fuera de tu sitio web, funciona como una vacuna. Pueden ser físicos o subcontratados, agregar un registro A a tus DNS, o cambiarte a los servidores de nombres del WAF.

Envía una petición estándar, analiza la respuesta y averigua si un WAF está en funcionamiento, si no consigue información, envía varias peticiones maliciosas para tratar de comprender la lógica del WAF y así poder identificarlo.

Si tampoco consigue información, la aplicación compara y analiza todas las respuestas para determinar si hay un WAF activo.

29. EJEMPLOS DE SERVICIOS VULNERABLES

- **SNMP** (*Simple Network Management Protocol*): Utilizado por numerosos dispositivos como routers, impresoras... Permite conectarse al equipo y extraer y modificar la configuración y detalles

del sistema. P.e. puede configurar forward en los routers dejando entrar así los paquetes o no (DoS).

- **SMB (Server Message Block)**: Permite la compartición de información. P.e. carpetas compartidas en Windows, samba para unix, etc.
 - **FTP (Files Transfer Protocol)**: Intercambio de ficheros.
 - **SMTP (Simple Mail Transfer Protocol)**: Permite enviar correos electrónicos.
 - **VPN (Virtual Private Network)**: Permite establecer redes privadas virtuales, punto a punto, donde el tráfico va cifrado.
 - **WebDAV**: Protocolo que nos permite guardar archivos, editarlos, moverlos y compartirlos en un servidor web.
 - **Credenciales por defecto**: Muy normal y con muchas vulnerabilidades.
-

5. CAMPAÑA DE PHISHING

30. GOPHISH

Gophish es kit de herramientas de phishing de código abierto

Gophish es un conjunto de herramientas de phishing de código abierto diseñado para empresas y evaluadores de penetración. Proporciona la capacidad de configurar y ejecutar rápida y fácilmente interacciones de phishing y capacitación en concientización sobre seguridad.

Lo descargamos.

```
—(root㉿kali)-[/home/kali/Desktop]
# unzip gophish-master.zip
```

Borramos la carpeta .zip, ya que no nos va a servir de nada.

```
—(root㉿kali)-[/home/kali/Desktop]
# rm -r gophish-master.zip
```

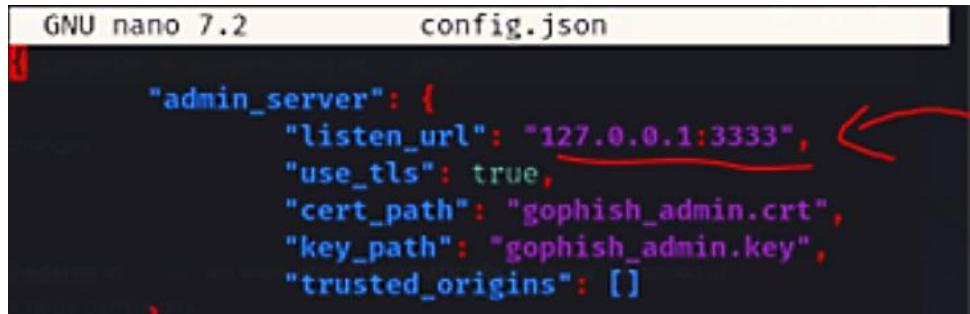
Clonamos de GitHub la versión para Linux y descomprimimos la carpeta.

<https://github.com/gophish/gophish.git>

```
—(root㉿kali)-[/home/kali/Desktop]
# wget https://github.com/gophish/gophish/releases/download/v0.12.1/gophish-v0.12.1-linux-64bit.zip
```

La máquina virtual debe estar en adaptador puente para poder difundir el phishing en la red.

Con *ifconfig* vemos cual es nuestra IP, la cual debemos introducir en el archivo de *config.json* en el apartado de *listen_url*.



```
GNU nano 7.2          config.json

{
    "admin_server": {
        "listen_url": "127.0.0.1:3333",
        "use_tls": true,
        "cert_path": "gophish_admin.crt",
        "key_path": "gophish_admin.key",
        "trusted_origins": []
    }
}
```

A continuación, paramos (si no está parado ya) Apache2.

```
(root㉿kali)-[~/home/kali]
# systemctl stop apache2 && systemctl status apache2
```

Damos permisos de ejecución a Gophish y lo ejecutamos.

```
(root㉿kali)-[~/home/kali/phising/gophish]
# chmod u+x gophish
```

```
(root㉿kali)-[~/home/kali/Desktop]
# ./gophish &
[1] 2532

(root㉿kali)-[~/home/kali/Desktop]
# time="2023-10-20T10:55:44-04:00" level=warning msg="No contact address has been configured."
time="2023-10-20T10:55:44-04:00" level=warning msg="Please consider adding a contact_address entry in your config.json"
goose: no migrations to run. current version: 20220321133237
time="2023-10-20T10:55:44-04:00" level=info msg="Please login with the username admin and the password 560eba0c461d6cdf"
time="2023-10-20T10:55:44-04:00" level=info msg="Starting IMAP monitor manager"
time="2023-10-20T10:55:44-04:00" level=info msg="Creating new self-signed certificates for administration interface"
time="2023-10-20T10:55:44-04:00" level=info msg="Starting new IMAP monitor for user admin"
time="2023-10-20T10:55:44-04:00" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"
time="2023-10-20T10:55:44-04:00" level=info msg="Starting phishing server at http://10.0.2.15:80"
```

Identificamos el usuario y la contraseña. Accedemos a la web local para configurar Gophish como administradores, iniciando sesión con este usuario y contraseña.

The screenshot shows the Gophish web application interface. At the top, the URL is https://192.168.89.143:3333. The main navigation bar includes links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The title bar says "gophish". On the left, a sidebar menu lists: Dashboard, Campaigns, Users & Groups, Email Templates, Landing Pages, Sending Profiles, Account Settings, User Management (with an "Admin" badge), Webhooks (with an "Admin" badge), User Guide, and API Documentation. The main content area is titled "Dashboard" and displays a message: "No campaigns created yet. Let's create one!". A large button labeled "New Campaign" is visible.

En *Sending Profiles* podremos configurar el perfil del envío. Necesitaremos tener un servidor SMTP. También se puede verificar que los mensajes se envían correctamente clicando en el botón de Send Test Email.

LANDING PAGES

Clicando en *Import Site* podemos importar el código de la web que deseamos clonar.

The screenshot shows the "New Landing Page" dialog box. The "Name:" field contains "Paginacionada". A red arrow points to the "Import Site" button. Below it is a WYSIWYG editor toolbar with various HTML and CSS icons. A checkbox at the bottom is labeled "Capture Submitted Data". At the bottom right are "Cancel" and "Save Page" buttons.

OTROS USOS DE GOPHISH

- Crear templates de correo y asegurar que cada correo se dirija a diferentes destinatarios usando la sintaxis del framework integrado.
- Crear grupos de usuarios a los que dirigir el phishing, introduciéndolos manualmente o importándolos de base de datos.
- Configurar diferentes campañas de phishing desde *Campaigns*.
- En *Dashboard* aparecerá un resumen de todas nuestras campañas y sus status.