CIBERSEGURIDAD EN KALI LINUX

PROYECTO FINAL CICLO FORMATIVO DE GRADO SUPERIOR

Josué García Cantos 2ºSTI
IES UNIVERSIDAD LABORAL 2017-2019

Índice

Videotutorial

Nmap y Netdiscover	**00:00 min**
Ettercap	**04:30 min**
Bettercap HTTP	**07:52 min**
Bettercap HTTPS	**10:57 min**
Evil-Droid	**13:23 min**

Presentación

Me llamo Josué García y soy alumno del Ciclo Formativo de Grado Superior de Sistemas de Telecomunicaciones e Informáticos. Mi proyecto está relacionado con la asignatura impartida por Carlos Villora de Redes Telemáticas.

Desde siempre la informática y la ciberseguridad llamaron bastante mi atención, siempre me interesó la forma de poder acceder a cierta información, tener control de accesos o descubrir vulnerabilidades en sistemas operativos o programas. Motivado por ello, me animé a cursar el Grado Medio de Sistemas Microinformáticos y Redes Locales el cual superé con bastante satisfacción, sobre todo en asignaturas como Seguridad Informática.

Es por eso que mi idea de proyecto veía que podía encajar más con la asignatura de Redes Telemáticas, ya que es la asignatura más vinculada a la parte de software.

Mi idea final de proyecto consta de un conjunto de utilidades recogidas en su mayoría en el sistema operativo Kali Linux, para la recopilación de información y acceso mediante ataques Man In The Middle. Con ello trato de mostrar lo simple que puede llegar a ser extraer información privada que usamos a diario mediante Internet como podrían ser accesos redes sociales, usos de cuentas bancarias…

¿Qué es MITM?

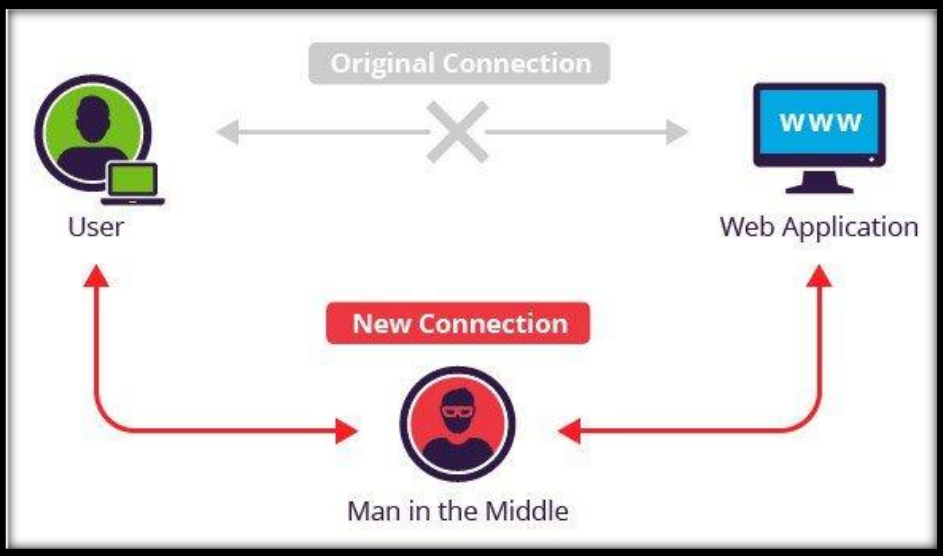
La seguridad es un problema que siempre debemos tener en cuenta, ya que no existe la seguirdad 100% efectiva, la mayor prueba de ello es que las comunicaciones son cada vez más seguras en Internet y a pesar de ello siempre se encuentran fallas a estos sistemas.

Aquí entran en juego los ataques llamados MITM, pero… ¿Qué es un ataque Man In The Middle?

MITM es un método de ataque en el cual se produce un "envenenamiento" de las tablas ARP, que consiste en inundar la red con paquetes ARP indicando que nuestra MAC es la MAC asociada a la IP de la VICTIMA y que nuestra MAC está también asociada a la IP del ROUTER.

De este modo, todas las máquinas actualizaran sus tablas con esta nueva información maliciosa por lo que cada vez que alguien quiera enviar un paquete a través del router, ese paquete no será recogido por el router, sino por nuestra máquina, pues se dirige a nuestra dirección MAC, y cada vez que el router u otra máquina envíe un paquete a nuestra víctima sucederá lo mismo.

Esta parte es fundamental ya que si el envenenamiento solo se produjese en la víctima y no en el router, nos sería imposible enviar la información solicitada, por lo que el ataque fallaría.



Este proceso puede realizarse tanto en redes LAN o WLAN, lo cual lo hace especialmente peligroso en zonas como cafeterías, aeropuertos o más concretamente cualquier punto Wi-Fi gratuito al que nos conectamos sin conocer quien lo gestiona.

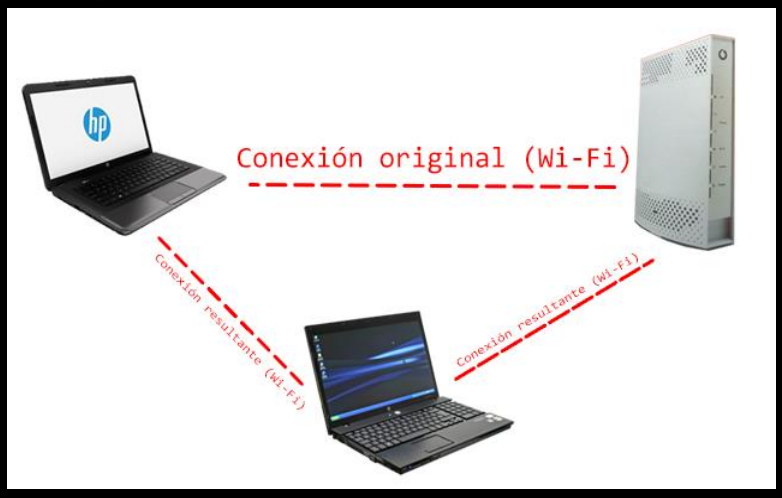
Esquema y Planteamiento

Para este proyecto vamos a usar una red privada Wi-Fi de un domicilio como zona de pruebas, esta red está compuesta por varios dispositivos, teléfonos móviles, videoconsolas y equipos. El ataque se realizará vía Wi-Fi ya que es un método que nos permitirá más fácilmente simular una situación cotidiana. En este caso disponemos de un equipo (HP250) conectado vía Wi-Fi al router (Router Vodafone) al cual trataremos de analizar su tráfico mediante otro equipo (HP ProBook 4510s)

HP 250 G1 — **Equipo Víctima**

HP ProBook 4510S — **Equipo atacante**

Router Avanzado Vodafone — **Dispositivo de interconexión**



Conceptos básicos

Dirección IP	Conjunto de cuatro octetos que identifican a un dispositivo en una red
Dirección MAC	Al igual que la dirección IP, es un identificador de un dispositivo físico, con la diferencia que este es una combinación hexadecimal única.
Apt get-update	Comando de terminal que nos permite actualizar la lista de paquetes disponibles
Apt-get upgrade	Comando de terminal que nos permite instalar las últimas versiones de las aplicaciones encontradas previamente con el comando anterior
Ifconfig	Muestra información vinculada con la tarjeta de red de nuestro dispositivo desde Linux
Ipconfig	Muestra información vinculada con la tarjeta de red de nuestro dispositivo desde Windows
Nmap	Aplicación que nos permite detectar dispositivos asociados a una dirección IP de una red
Netdiscover	Aplicación que nos permite detectar dispositivos asociados a una dirección IP de una red
Sniffing	Método por el cual se analiza el tráfico de paquetes que circula por una red
ARP	Protocolo que permite encontrar la dirección MAC equivalente a una determinada dirección IP, actuando como traductor e intermediario.
ARP-spoofing	Método por el cual se produce un “envenenamiento” de las tablas ARP para acceder a un equipo
Http	Protocolo de transferencia de texto utilizado en las páginas webs, seguridad nula, texto plano sin cifrar.
Ettercap	Aplicación que nos permite realizar ataques MITM
Https	Variante de Http donde la información se encuentra cifrada se encuentra cifrada
Bettercap	Aplicación más actualizada que nos permite realizar ataques MITM
Backdoor	Código parte de un sistema que nos permite acceder a él sin pasar por autentificación previa
APK	Aplicación móvil

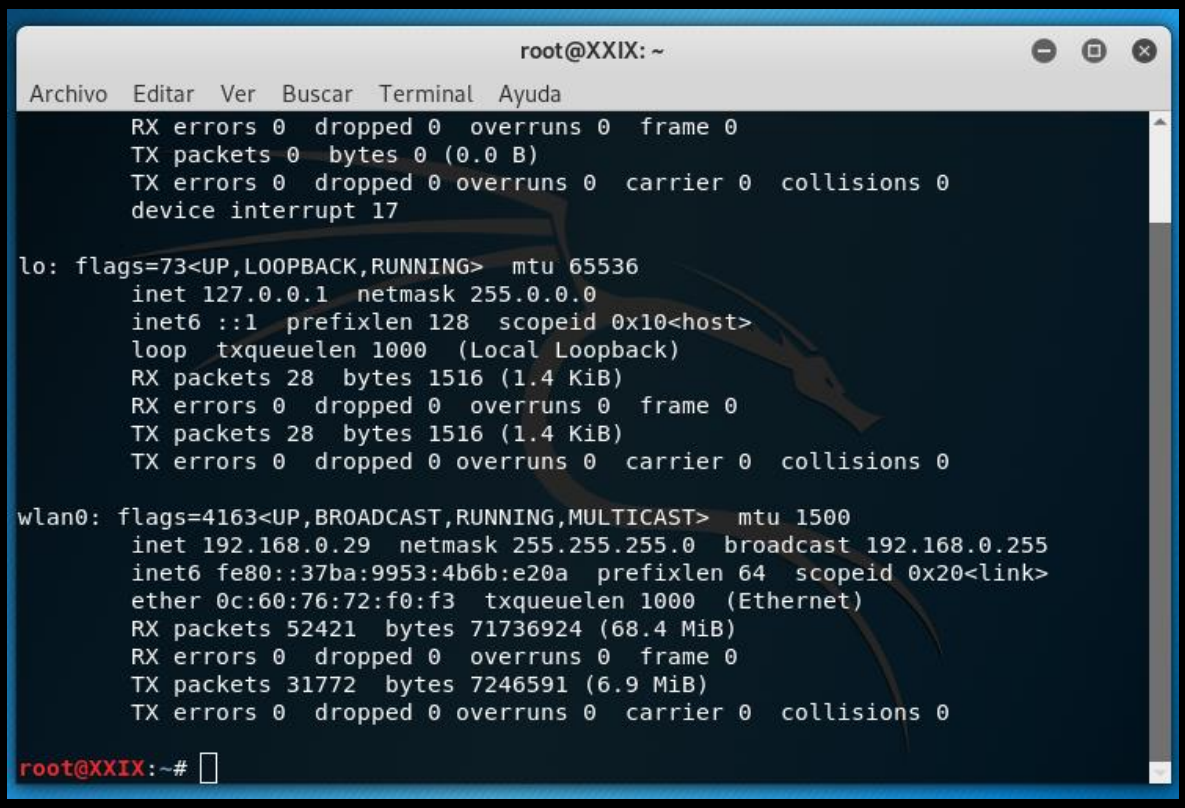
Ataque Man In The Middle

Todos los pasos mostrados se han realizado siendo superusuario

1. Recopilación de información

Una vez que nuestro equipo atacante ha conseguido acceder a la red podemos analizar los dispositivos conectados a ella y recopilar información que puede ser necesaria, como direcciones IP, direcciones MAC, descripción del dispositivo a atacar…

Pero antes debemos saber qué dirección IP se nos ha asignado y en que red nos encontramos para ello nos dirigimos a nuestro termina y tecleamos ***ifconfig***



Ya que estamos utilizando una conexión vía Wi-Fi nos fijamos en la interfaz ***wlan0***, que es nuestra tarjeta wifi, y comprobamos que nos asigna la ***dirección 192.168.0.29*** con una ***máscara de red 255.255.255.0***, esto quiere decir que nos encontramos en una ***red tipo 192.168.0.0/24.***

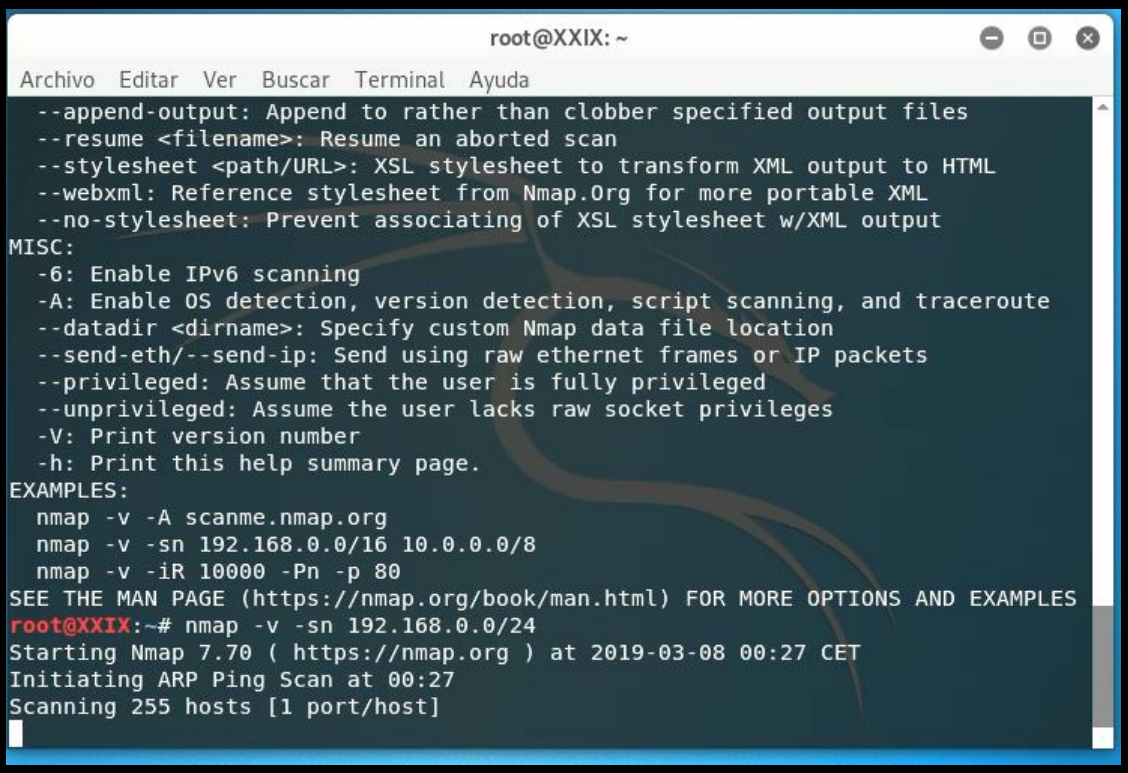
Con esta información ya podemos avanzar y analizar dicha red.

1.1 Nmap

Podemos acceder a la aplicación de dos formas, o bien nos dirigimos a ***Aplicaciones/Análisis de Vulnerabilidad/Nmap*** o bien nos dirigimos a un terminal y tecleamos directamente ***nmap***.

Una vez ahí nos aparecerán todos los parámetros con los que está asociado el comando

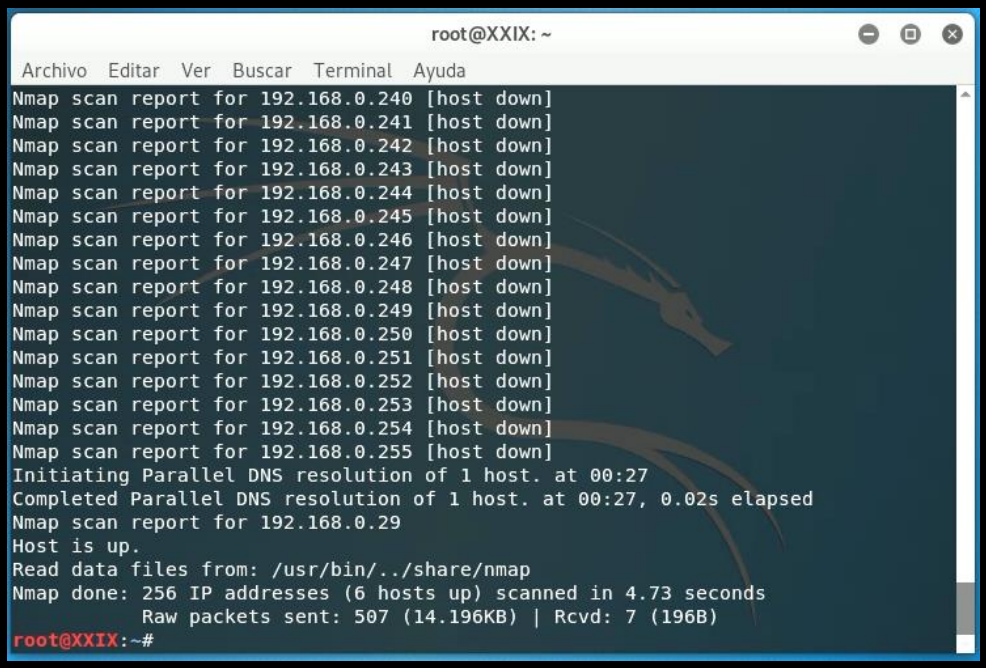
Previamente hemos descubierto que dirección IP se nos ha asignado y por tanto, hemos descubierto que dirección IP tiene la red en la que nos ubicamos.

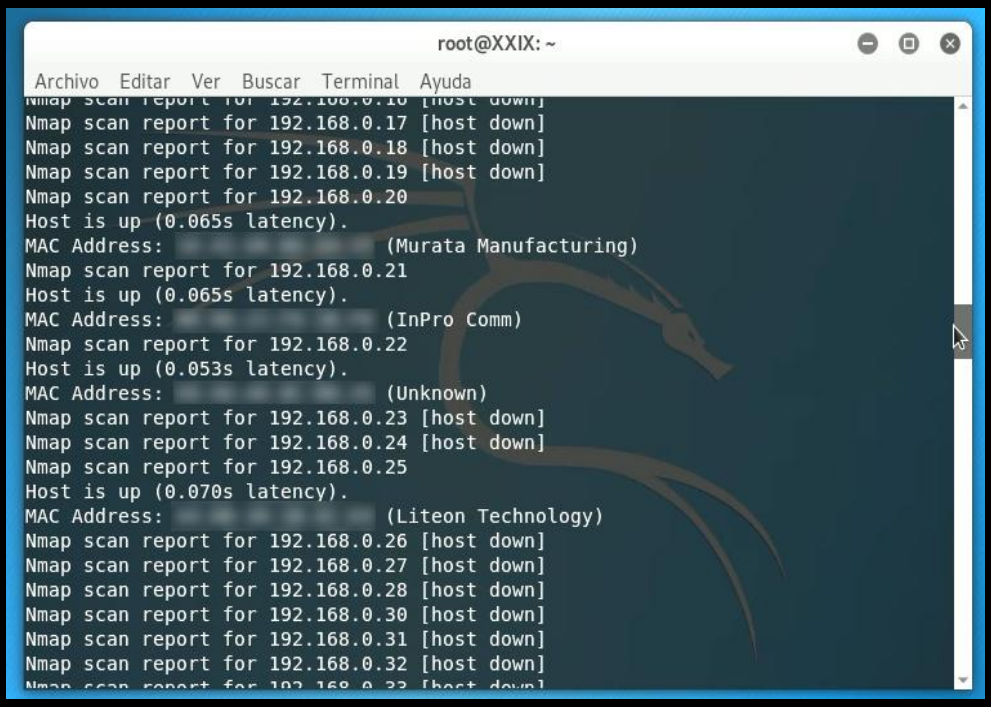


Ahora añadimos el comando ***nmap -v -sn 192.168.0.0/24***

Con -v estamos indicando que nos muestre la información en pantalla

Con -sn indicamos que haga un ping a cada uno de los hosts de esa red para comprobar su conectividad.





Si hacemos scroll hacia la parte superior una vez que ha finalizado podemos encontrarnos con un listado de todas las direcciones IP de la red con el indicativo de si dicho host está activo o fuera de línea.

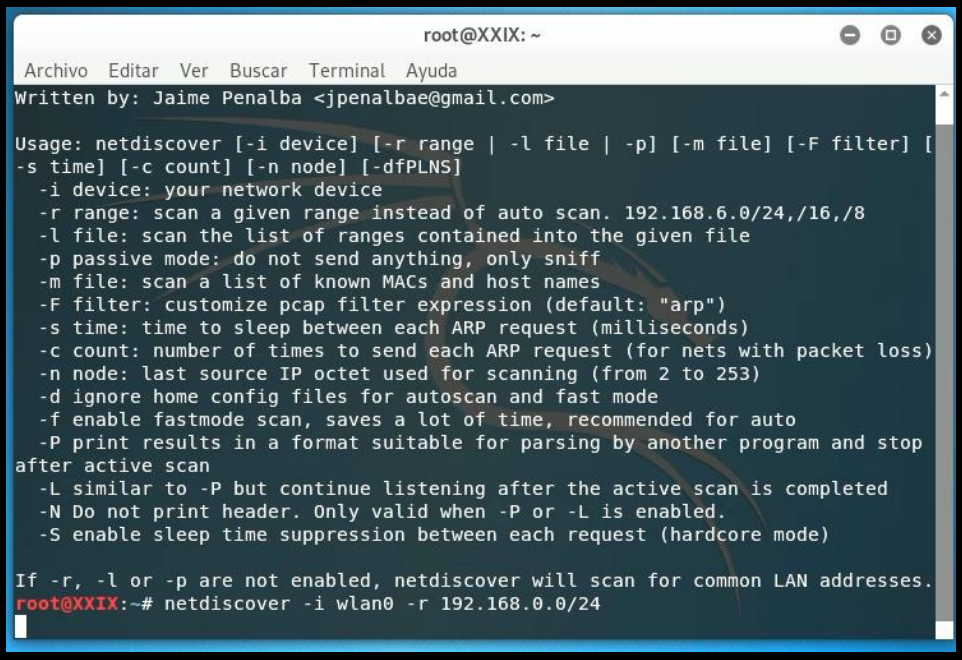
Si está activo además nos muestra información adicional como un nombre descriptivo del dispositivo o incluso su dirección MAC, con algo tan simple como un comando.

Con esta información el atacante solo tendría que elegir una víctima de las mostradas en el listado y proceder al ataque, pero antes vamos a mostrar un método alternativo a nmap.

1.2 netdiscover

La forma de utilizar netdiscover es similar a nmap, necesitamos el comando y los parámetros para mostrar la información.

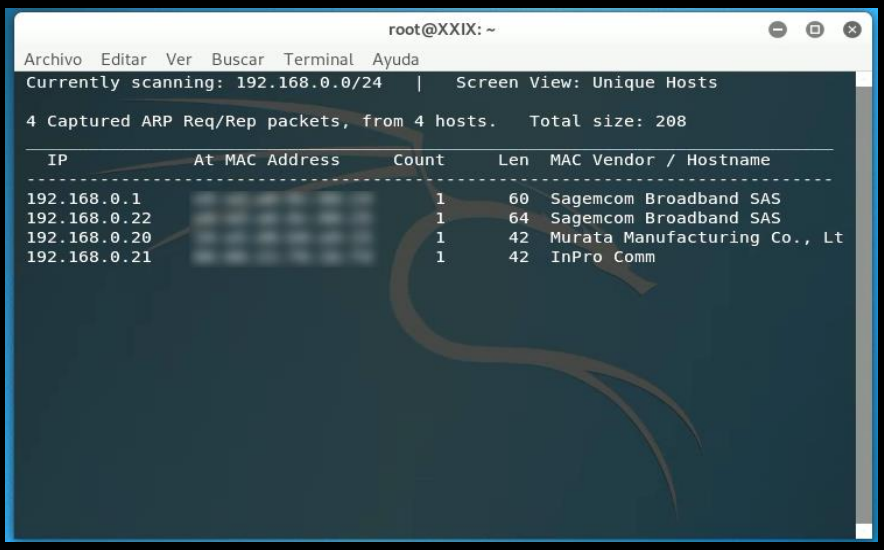
De nuevo accedemos a netdiscover mediante ***Aplicaciones/Recopilación de Información/netdiscover*** o bien abrimos un terminal y tecleamos ***netdiscover***



Tecleamos ***netdiscover -i wlan0 -r 192.168.0.0/24***

Con -i estamos indicando nuestra tarjeta de red

Con -r indicamos el rango de dirección que queremos analizar



Podemos comprobar cómo nos aparecen los dispositivos activos, junto a su IP, dirección MAC y su hostname

2. Sniffing

Una vez que hemos recopilado la información necesaria, podemos pasar a la parte de sniffing o análisis de tráfico. Cabe destacar que el análisis de tráfico que pudiéramos realizar con programas tipo Wireshark, sería únicamente del tráfico existente entre la maquina donde estuviera instalado dicho programa con el resto de equipo, pero no podríamos averiguar el trafico existente entre una máquina adyacente con el router.

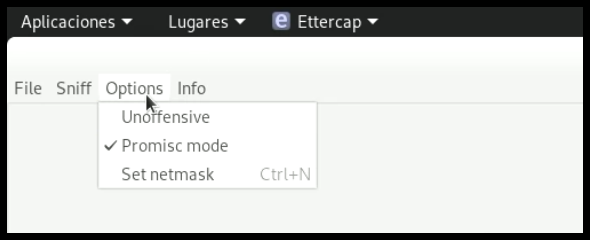
Para ello vamos a comenzar hablando de Ettercap y la forma de utilización

2.1 Ettercap

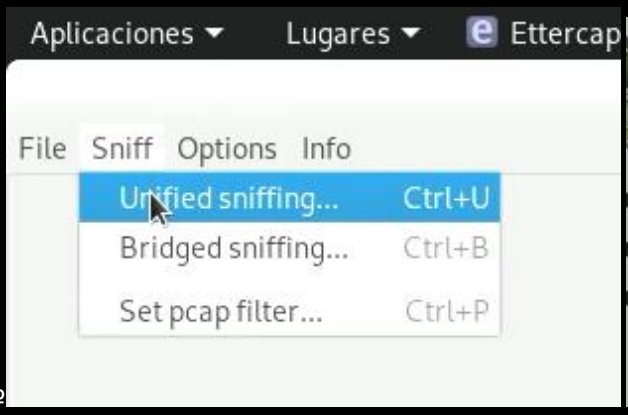
Accedemos a Ettercap mediante ***Lugares/Husmeando y Envenenando/Ettercap***

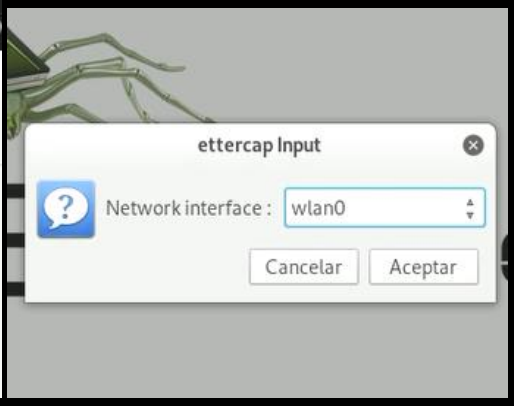
Una vez ahí se nos muestra la siguiente ventana:

Lo primero que debemos tener en cuenta es tener ***activado el Modo Promiscuo***, este viene por defecto activo pero conviene asegurarse que este habilitado.

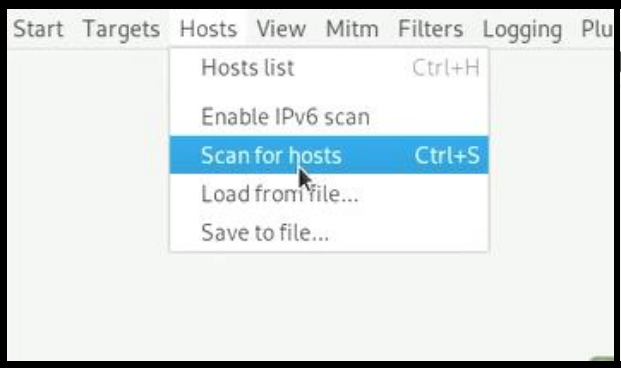


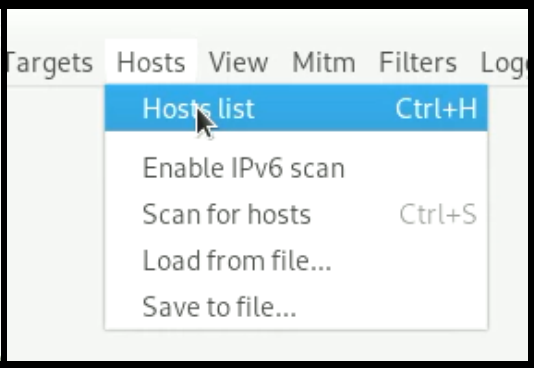
Ahora pasamos a seleccionar la *opción Sniff/Unified sniffing* y seleccionamos la *tarjeta de red wlan0* que estamos utilizando para analizar el trafico y hacemos *click en Aceptar*.

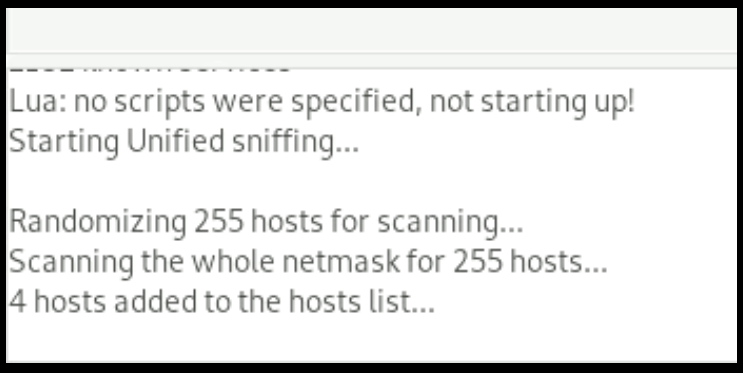




Seguido de esto necesitamos indicarle a Ettercap que máquina queremos seleccionar como víctima del sniffing, por tanto haremos *click en Hosts/Scan for hosts* y tras un par de segundos comprobamos que el escaneo ya *ha detectado 4 hosts* en la red, haremos *click en Host list para visualizarlos*

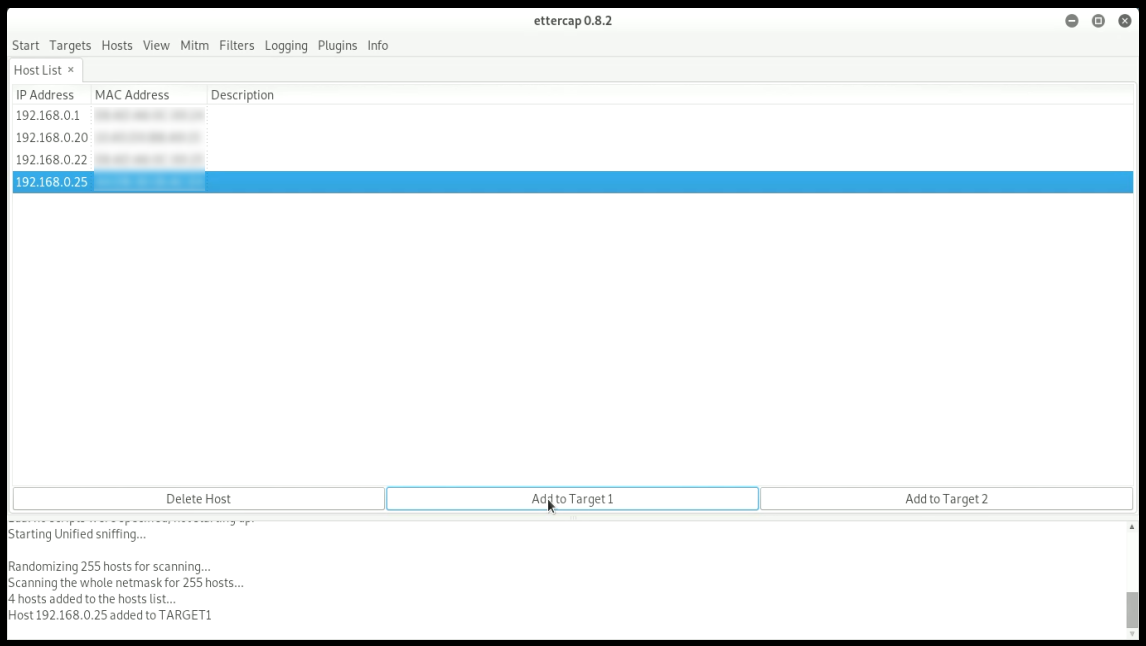




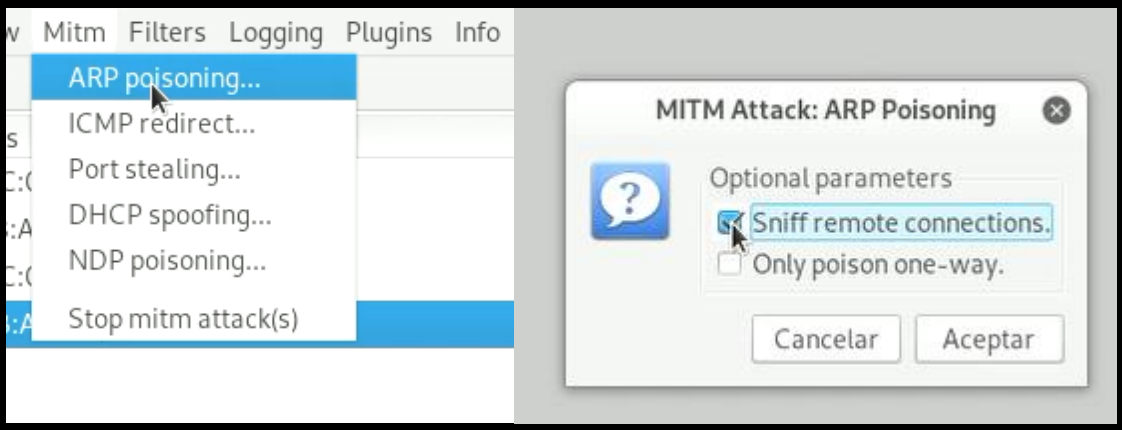


Marcamos este caso la *dirección 192.168.0.25 que hace refrencia al equipo HP250 con un click* y seguido *clickamos sobre la opción Add to Target 1.*

En cuadro de información inferior vemos que se ha confirmado como *TARGET 1*

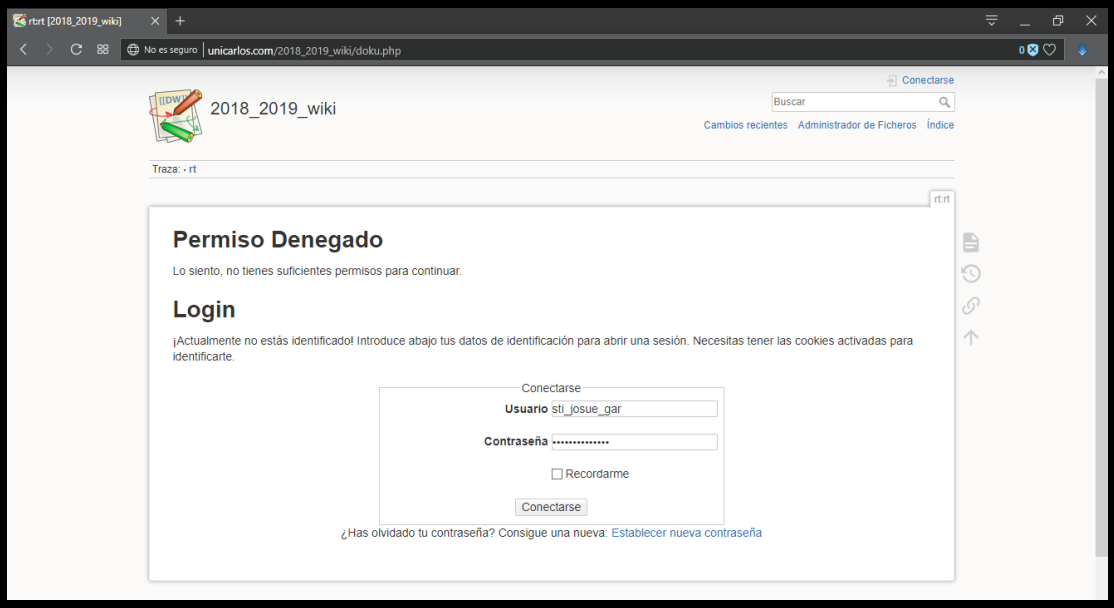


Una vez seleccionado el objetivo, clicamos sobre *Mitm/ARP poisoning* para proceder al envenenamiento de las tablas ARP que hemos mencionado anteriormente y de ahí *marcaremos la casilla Sniff remote connections y Aceptar*



Tras esto Ettercap ya está escuchando el tráfico que existe entre el router y el equipo víctima, gracias al envenenamiento de las tablas de ARP.

Ahora tan solo debemos esperar que la víctima acceda a una web cualquiera con protocolo HTTP, para este ejemplo accedemos a www.unicarlos.com



De forma que en el momento que el usuario se autentifica, nosotros recibimos la notificación en la maquina atacante, mostrándonos toda la información referente a la ***dirección IP del sitio, URL de la web*** y lo más importante, ***login: sti_josue_gar*** y ***password: holaatodoscomoestan***

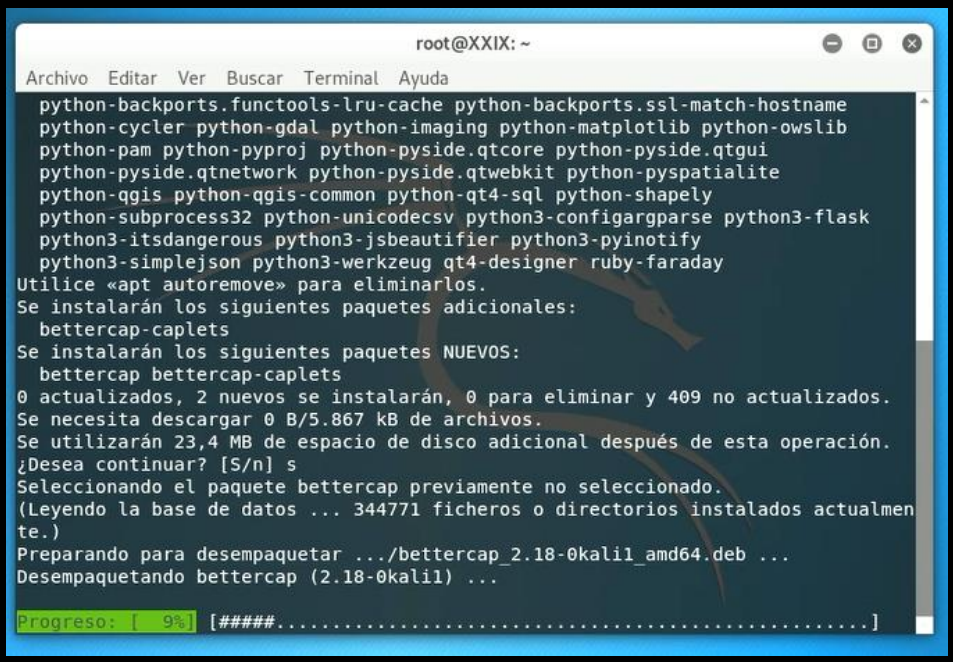
Por ultimo para detener el sniffing, tan solo nos dirigimos a ***Start/Stop Sniffing***

2.2 Bettercap (HTTP)

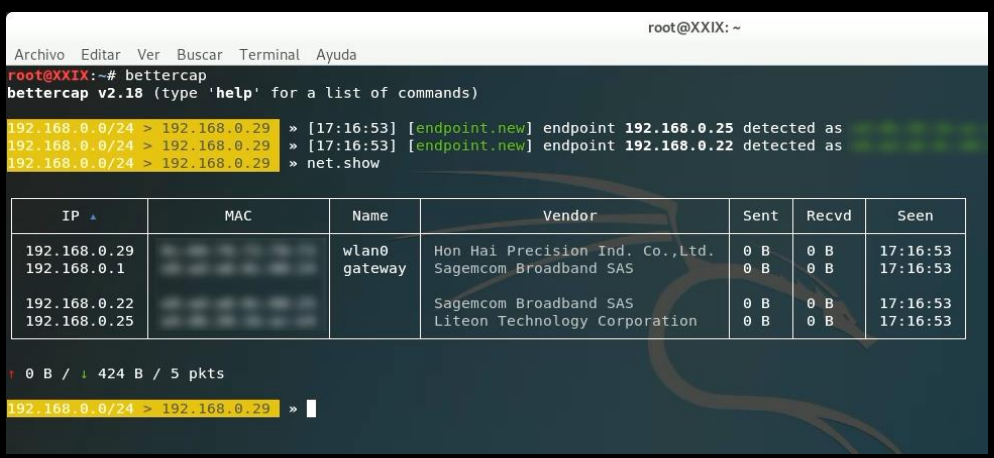
En el caso anterior visto con Ettercap, hemos conseguido extraer el usuario y contraseña que se encontraba en el tráfico de datos que estábamos analizando, pero esta información que apareció tan "facilmente" se debe a que la página carecía de cifrado, es decir utilizaba HTTP.

En el caso actual vamos a trabajar con una herramienta más potente llamada ***Bettercap***, para ello lo primero que debemos hacer es instalarla ya que ***no viene junto a Kali Linux como era el caso de Ettercap.***

Abrimos un nuevo terminal y escribimos ***apt install bettercap***, confirmamos su instalación ***pulsando s*** y esperamos que se descargue e instale

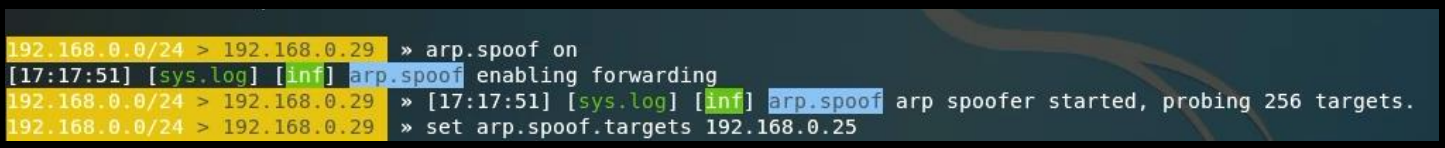


Ahora, iniciamos el programa escribiendo ***bettercap*** en el terminal y se nos mostrará está pantalla



Podemos comprobar que nos aparece una tabla que automáticamente nos detecta los dispositivos conectados a la red actual, lo cual nos ahorra tiempo respecto a métodos anteriores.

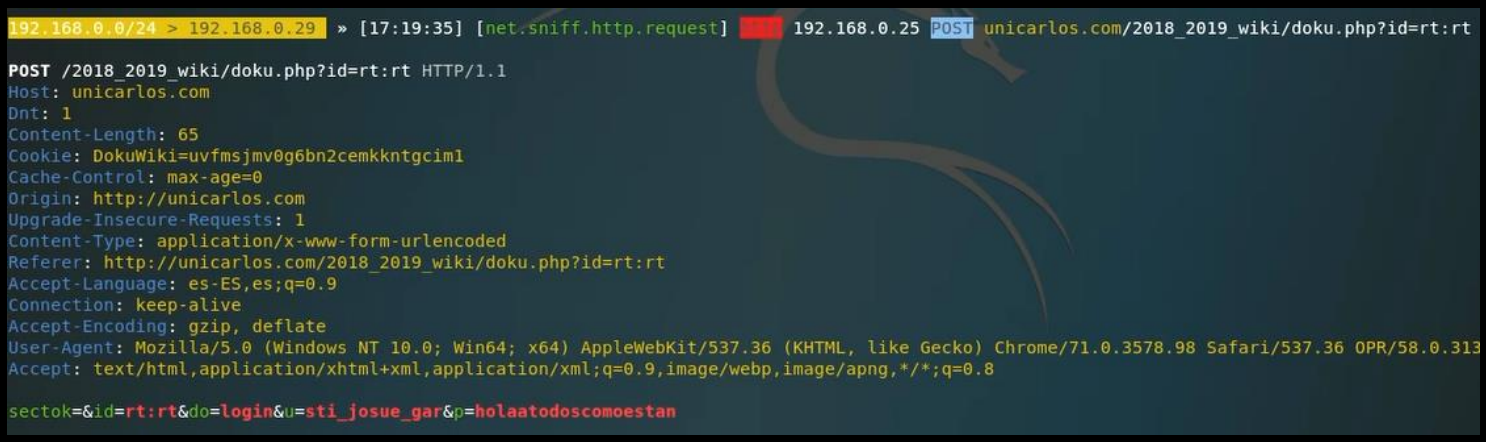
Ahora activamos el envenenamiento de ARP mediante ***arp.spoof on*** y nos aparece un mensaje informándonos que se ha activado y tiene como objetivo cualquier máquina de la red, pero nosotros en este caso tan solo queremos atacar una en concreto, para eso usamos el comando ***set arp.spoof.targets 192.168.0.25***, de esta forma escucha el tráfico de ese único host.



Por ultimo comenzamos el Sniffing con ***net.sniff on***

De nuevo tan solo tenemos que esperar que la víctima inicie en una página web (con http) y en nuestra máquina atacante ***nos mostrará el login y password marcado en rojo*** en la parte inferior.

Login: sti_josue_gar password: holaatodoscomoestan



Podemos comprobar en este método que si la victima navega por una página web ***con un protocolo HTTPS, Bettercap no nos mostrará login o password*** de dicho sitio aunque la victima haya ingresado, para poder acceder a dicha información ***necesitaremos usar caplets***.

¿Qué son caplets?

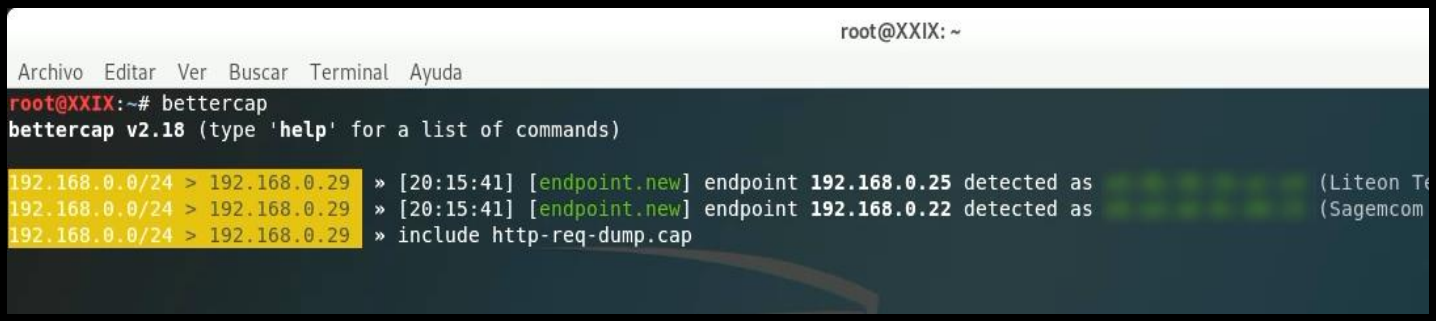
Los caplets podemos calificarlo como conjunto de instrucciones agrupadas en un pequeño programa, algo así como un script.

2.3 Bettercap (HTTPS)

Conociendo ya el programa, abrimos de nuevo el terminal usando el comando ***bettercap*** y una vez dentro para activar escribimos:

include http-req-dump.cap.

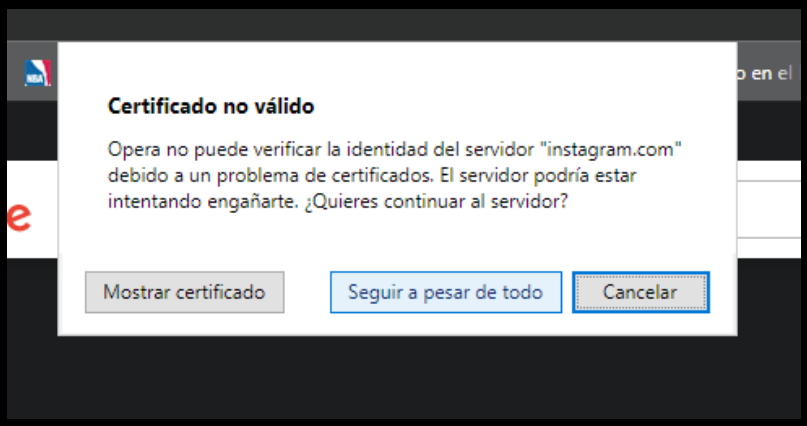
Con esto estamos consiguiendo "convertir" las páginas con protocolo de seguridad HTTPS a HTTP, siendo así texto plano sin ningún cifrado que nos permita extraer la información.



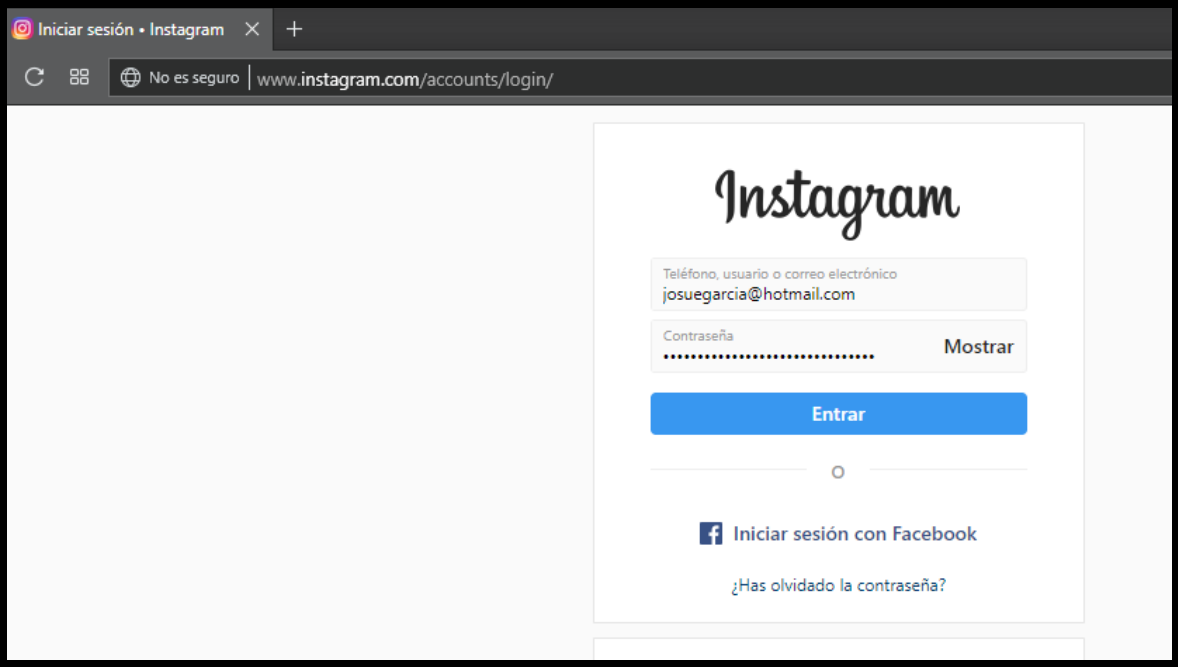
En la imagen anterior está aplicando el cambio a todos los hosts de la red, por lo que escribimos ***set arp.spoof.targets 192.168.0.25*** para que solo lo aplique a un único host vítima.

Hecho esto, cuando la víctima navegue por Internet y entre a una página con seguirdad HTTPS, como en este ejemplo es Instagram, se le mostrará un mensaje diciendo que el sitio no es seguro.

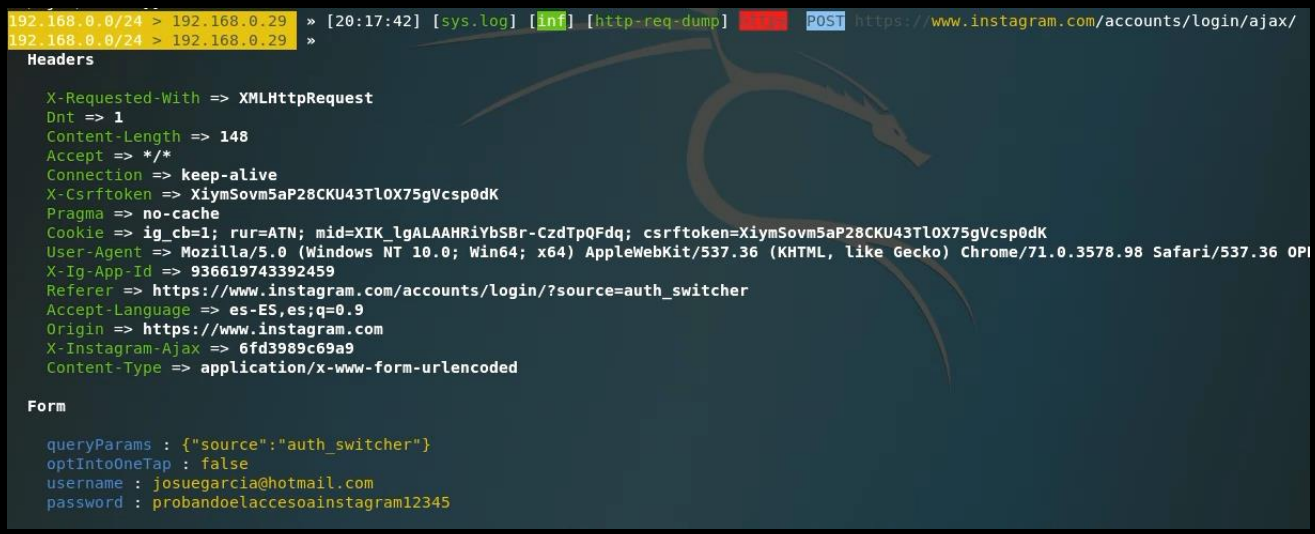
A pesar de eso la gran mayoría es probable que continue clicando en ***"Seguir a pesar de todo"***



A priori la víctima no notará nada extraño, pero si nos fijamos en el detalle, vemos que en la parte superior izquierda el candado verde de ***HTTPS ha desaparecido y ahora se muestra "No es seguro"***



Una vez que el usuario acceda, a nosotros nos llegara la notificación igual que en métodos anteriores:



3. Backdoor en Android

El mercado de las apps móviles va cada vez más en aumento, cualquiera puede crear ya su propia aplicación móvil y tratar de distribuirla libremente o monetizarla, lo cual debe pasar unos controles de calidad en alojamientos como Google Play Store pero… ¿Qué ocurre con esas apps que no pasan un control de calidad?

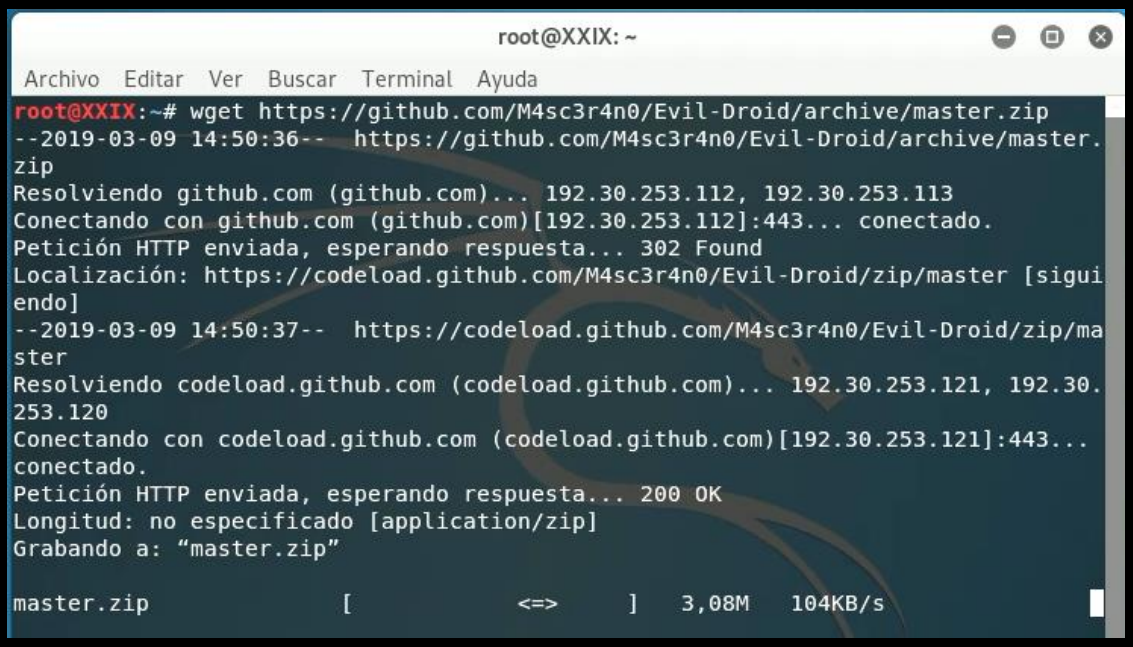
Seguramente tu teléfono móvil te ha advertido de los peligros instalar aplicaciones de origen desconocido, pero en este apartado se quiere concienciar al usuario de lo fácil que puede ser acceder a nuestra información mediante un backdoor en cualquier aplicación instalada en nuestro dispositivo.

En este ejemplo vamos a infectar una aplicación Android llamada SemanaApp, que hemos creado en este mismo Ciclo Formativo mediante AppInventor, para posteriormente instalarla en cualquier dispositivo y comprobar como accedemos al sistema.

3.1 Evil-Droid

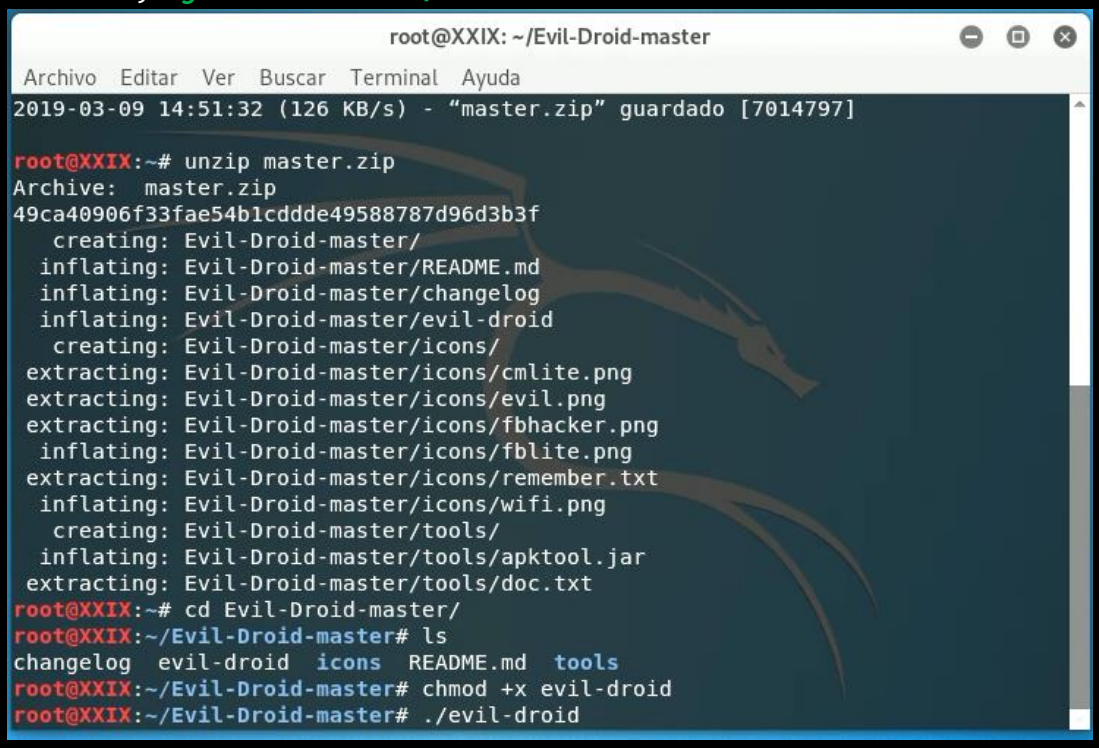
Evil Droid es una herramienta que nos permite infectar el código de una app ya creada con el fin de tomar el control del dispositivo. Vamos a proceder a la descarga:

wget https://github.com/M4sc3r4n0/Evil-Droid/archive/master.zip

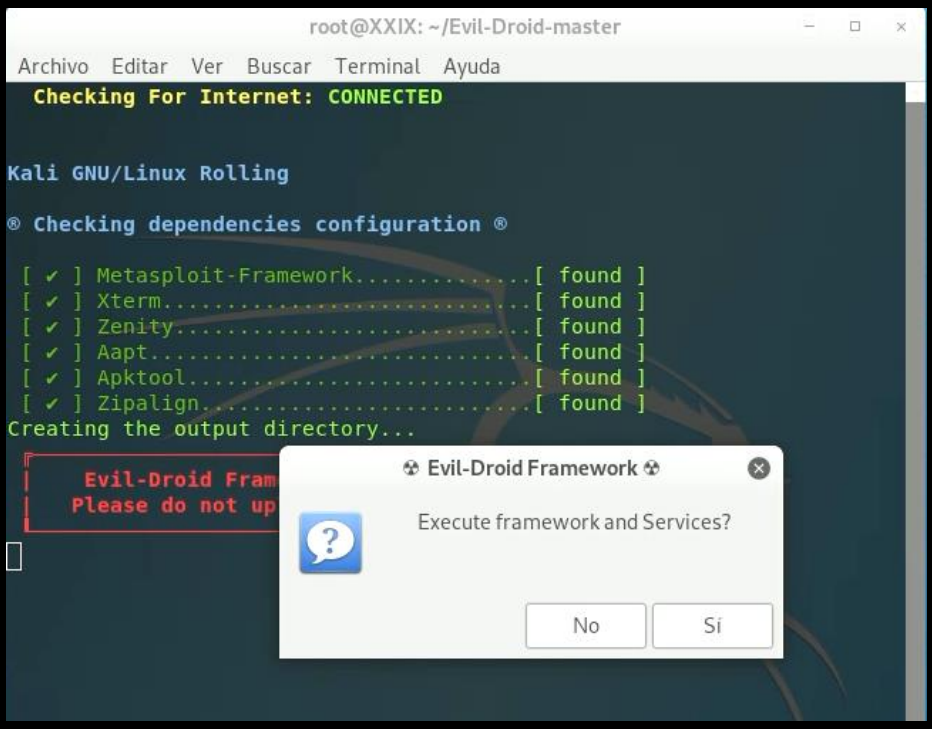


Una vez descargado, ***descomprimimos con unizip master.zip,*** nos dirigimos a la ubicación después de descomprimir con ***cd Evil-Droid-master,*** localizamos el archivo evil-droid y le asignamos permisos de ejecución mediante ***chmod +x evil-droid***.

Tras eso, ***ejecutamos con ./evil-droid***



Tras eso, nos aparece un cuadro de dialogo que ***confirmaremos en SI*** y tendremos el programa en ejecución

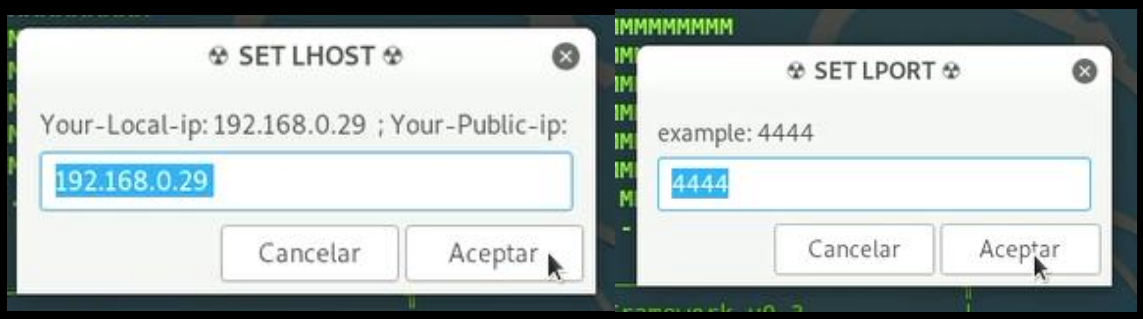


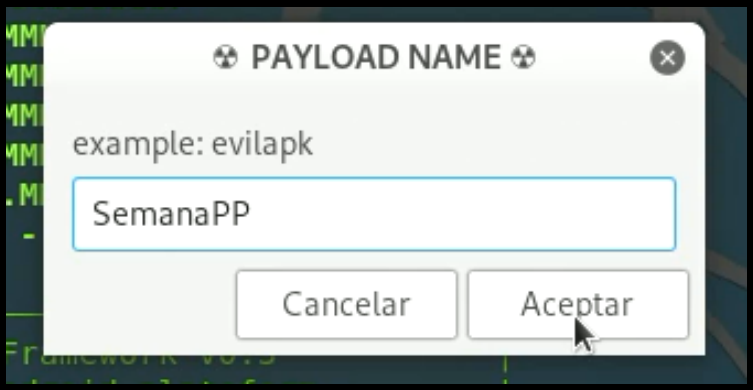
Escribimos 3 e Intro para seleccionar la opción que nos permite crear un backdoor para una apk android

Pasamos a seleccionar nuestra dirección IP desde la cual controlaremos el dispositivo, en este caso, escribiremos ***192.168.0.29***. Tras confirmar, elegiríamos el puerto, por defecto, ***4444***.

En caso de querer realizar ataques fuera de nuestra red, escribiríamos nuestra IP pública o bien, trabajaríamos con ngrok para crear túneles privados hacia un servidor local.

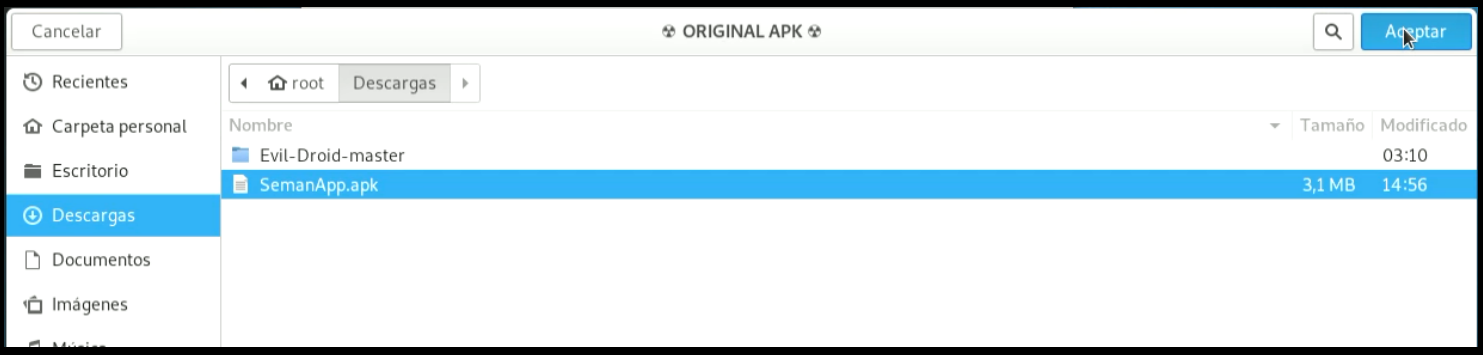
Por último, pasamos a ***renombrar nuestra APK***, en nuestro caso ***SemanaPP***



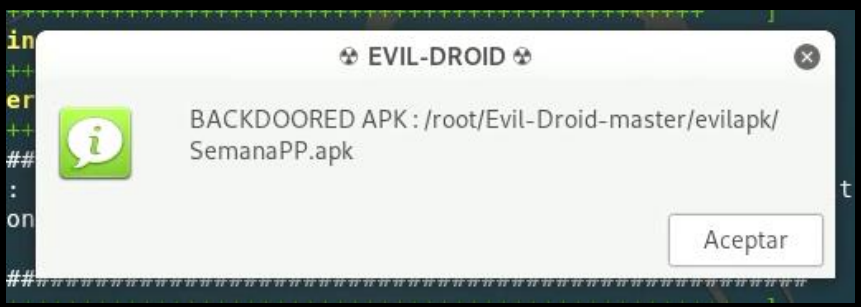


A continuación seleccionamos ***android/meterpreter/reverse_tcp*** y hacemos click en aceptar para comenzar con el proceso de generación del backdoor

Seleccionamos la APK a la cual queremos generarle el Backdoor, en este caso SemanaApp.apk

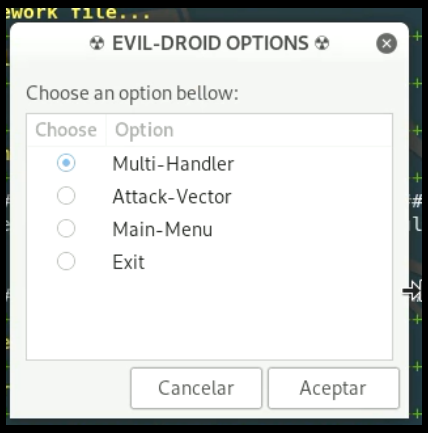


Tras eso el sistema comenzara con el proceso y tras unos minutos nos aparecerá este mensaje, ***indicándonos la ruta de la APK ya modificada***.

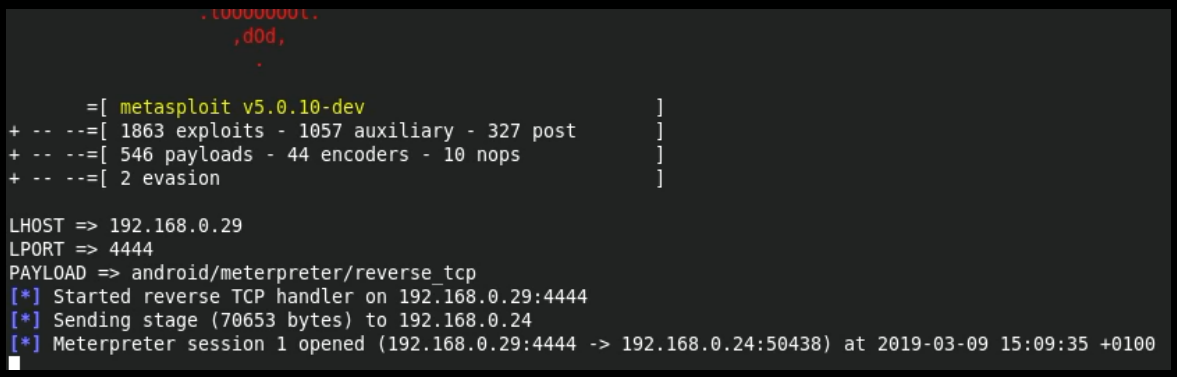


Seleccionamos Multi-Handler y haremos click en siguiente

Desde este apartado podremos mediante comandos establecer los tipos de ataques que realizaremos al dispositivo de la víctima como veremos más adelante.

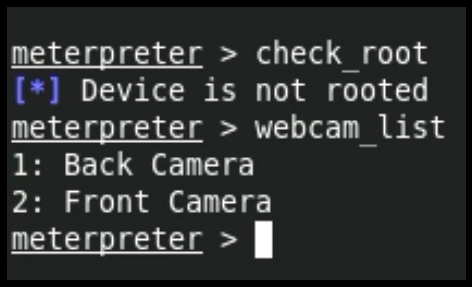


Ahora debemos de hacer que la víctima se instale dicha aplicación, el no notará nada extraño, *el funcionamiento de la APK será completamente normal*, pero tras instalar y abrirla, *Multi-Handler nos informará de que tenemos conexión a la víctima (dirección 192.168.0.24)*



A partir de aquí las posibilidades son varias, para eso *pulsamos ?* para ver todos los tipos de ataque que podemos realizar. Algunas de las cosas que podremos hacer:

- Grabación de micrófono durante X segundos
- Conocer cuantas de cams disponibles tiene el dispositivo
- Video en directo de la cam
- Comprobar si esta roouteado
- Obtener listado de números
- Obtener listado de llamadas
- Obtener SMS
- Geolocalizar



En este otro ejemplo, mediante ***dump_contacts***, hemos extraído un listado de los números de teléfono y nombres que venían en la agenda de la victima

```
meterpreter > dump_calllog
[*] No call log entries were found!
meterpreter > dump_contacts
[*] Fetching 137 contacts into list
[*] Contacts list saved to: contacts_dump_20190309151314.txt
```

Por último solo tenemos que dirigirnos a un nuevo terminal, ***cd Evil-Droid-master*** para movernos hacia dicha carpeta. Hacemos ***ls***, para ver su contenido y encontramos el archivo con los contactos, lo abrimos mediante ***cat contacts_dump_20190309151314.txt***