

curso “Experto en Ciberseguridad de Redes y Sistemas”

Paso previo: Instalación de Máquina Virtual Kali.

TEMAS

1. **Fingerprinting**
2. Footprinting
3. IDSs - Snort
4. Nessus
5. Firewalls
6. SGSI
7. Antiphishing
8. MITRE
9. Red Team y Blue Team
10. Principales procesos de Seguridad



Tema 1.Fingerprinting

Desarrollaremos los siguientes sub-temas:

- 1.1 Fingerprinting (parte 1 - Observación)
- 1.2 Fingerprinting (parte 2 - Enumeración)
- 1.3 Fingerprinting (parte 3 - Enumeración Móvil)

Desarrollo

1.1 Fingerprinting (parte 1 - Observación)

Damos los primeros pasos con esta actividad de “**fingerprinting**”, o “Huella digital” de la red que deseamos investigar.

Lo haremos de forma práctica con capturas de tráfico a través de la herramienta “**Wireshark**”, creando nuestra primera base de información de esa red destino.

Finalmente veremos cómo podemos auto asignarnos y configurarnos nuestra interfaz de red, para poder formar parte de la infraestructura sobre la que estamos operando.

Si aún no dominas la herramienta “**Wireshark**”, te recomendamos que hagas un “alto en el camino” y le des una mirada a nuestra serie de videos sobre “Análisis de Tráfico”:



- Análisis de Tráfico - **Tema-01**: Wireshark - **Presentación de la metodología**
<https://youtu.be/L8wA2ro638M>
- Análisis de Trafico - **Tema-02**: Wireshark - **Filtros de Captura**
<https://youtu.be/h72SZI79FEQ>
- Análisis de Trafico - **Tema-03**: Wireshark - **Ajustes de Capturas de Tráfico**
<https://youtu.be/g2QiQf2UtC0>
- Análisis de Tráfico - **Tema-04**: Wireshark - **Seguimiento de flujos**
<https://youtu.be/yTCH7SjK10M>
- Análisis de Tráfico - **Tema-05**: Wireshark - **Filtros de Visualización**
<https://youtu.be/sKU-lvOf3vE>
- Análisis de Tráfico - **Tema-06**: telnet un ejemplo de protocolos inseguros
<https://youtu.be/1FwFKNUFm0E>

Sigamos ahora con nuestro capítulo 1

La actividad de “**fingerprinting**”, un poco como su nombre lo indica, es obtener la huella digital de una infraestructura. Se trata de algo muy interesante y eminentemente técnico, que se inicia con el tema de la charla de hoy “**Observación**”. Esta actividad desarrolla los primeros pasos que debemos dar para comenzar a recolectar información útil para poder ir profundizando “paso a paso” sobre el nivel de detalle.

Como ya venimos haciendo con bastante frecuencia, trabajaremos nuevamente con capturas de tráfico lanzadas desde “**Wireshark**”, y con la misma herramienta gráfica analizaremos lo que ha circulado en esa red.

Iniciamos nuestra práctica, lanzando una captura de tráfico, en la misma red a la que estemos conectados. Recordad que debéis poner la interfaz de red sobre la que deseáis escuchar (observar) en modo “**promisc**” (Promiscuo).



Una vez que comienza la captura, la dejamos hasta que recolecte algunos miles de tramas, luego la detenemos.

En el ejercicio que se presenta en el video, ordenamos la captura desde la columna “**Source**” (podríamos hacerlo también desde la “**Destination**”, sería igual). Esto lo hacemos para analizar de forma ordenada las direcciones IP que aparecen en esta captura en concreto.

En nuestra captura, nos centramos especialmente en el rango de direcciones privadas, pues si estamos tratando de observar una infraestructura, tal cual hemos desarrollado en la **Charla 46**, lo más probable es que se trate de este tipo de rangos.



En nuestra captura de ejemplo, la primera dirección IP privada que aparece es la 192.168.1.1. La experiencia nos indica que, por supuesto sin ser esto una constante, en los extremos de los rangos de red, se encuentran generalmente alojados dispositivos especialmente interesantes, por eso es importante comprender bien los conceptos de máscara de red y de subred, para lo cual os recomendamos que le deis una repasada a la **Charla 45**.

En esta misma captura, vemos que la dirección IP 192.168.1.1, genera un tráfico “**IGMPv2**” (Internet Group Messaging Protocol) hacia la dirección destino 224.0.0.1, que, si volvemos a los videos recientemente recomendados, veremos que se trata de un tráfico “**multicast**”. Este información, ya es un muy buen indicio de que se trata de un dispositivo especial, pues no es normal que un sencillo host genere este tipo de tráfico con tanta frecuencia. En la realidad de esta red, se trata del “Gateway por defecto”, cosa que nuevamente puede intuirse en esta captura. Para poder verificarlo, es tan sencillo como poner esta dirección IP en la configuración e nuestro host, como “Gateway por defecto” y probar si logramos salir a Internet. Si logramos navegar por Internet, acabamos de verificarlo, y ya es un muy buen dato.

Si seguimos avanzando en el orden de las direcciones IP fuente y/o destino, ya podemos ir comenzando a crear nuestro primer inventario de la red que estamos observando, pues esas direcciones IP que generaron tráfico no hay duda que están activas.

Otro detalle que debemos recordar, es que al capturar multicast, este tipo de tráfico, como también el broadcast, todos los switches de esa red LAN tienen la obligación de explotarlo por todas sus bocas, con lo que probablemente, pueda estar escuchando hosts que estén en cualquier ubicación física de esa red. Es decir no necesariamente en nuestro mismo “**Dominio de Colisión**”. Esto también podemos repasarlo en la **Charla 14**.



NOTA: Fijaros la importancia de avanzar “paso a paso” en Ciberseguridad. En menos de una página, hemos avanzado sobre los conocimientos adquiridos en 3 Charlas anteriores.

De no tener la base de estas 3 Charlas, sin lugar a dudas, no se comprendería el detalle de los que estamos tratando aquí.

En esta primer captura de la Charla de hoy, hemos encontrado ya una serie de direcciones IP privadas que sabemos, sin lugar a dudas que están activas.

Con las mismas se puede, comenzar a crear un fichero de texto, sencillo, enumerando las direcciones IP que tenemos hasta ahora.

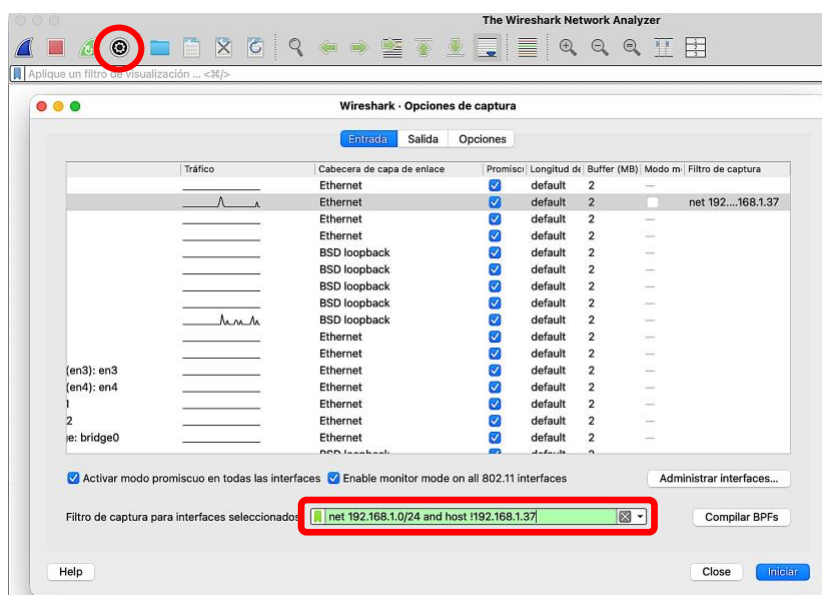
En el caso de nuestra captura de tráfico las direcciones IP fuente que tenemos son:

- 192.168.1.1
- 192.168.1.37 (veremos más abajo que esta es nuestra dirección IP)
- 192.168.1.101
- 192.168.1.134

Para avanzar un poco más en detalle, vamos a lanzar una segunda captura de tráfico, pero ahora con el filtro de captura, especificamos que “**no**” capture nuestra dirección IP.

En el caso de nuestro video, hemos visto cuál es la dirección IP del host, con el comando “**ifconfig**”, esta es: 192.168.1.37, por lo que, tal cual se aprecia en la imagen de la derecha, configuramos:

net 192.168.1.0/24 and host !192.168.1.37



Para cerrar esta primera parte “**Observación**”, debes abrir el video (**Obligatorio**):

 **Fingerprinting (parte 1 - Observación) - Charla 72 -**
Aprendiendo Ciberseguridad paso a paso
<https://youtu.be/2-LG9mi3QqE>



NOTA: Como ya hemos mencionado, todos los videos que forman parte del temario (**Obligatorios**), deberás verlos al completo para poder seguir avanzando en el curso. A medida que transcurren los mismos, te aparecerán las preguntas que deberás responder para tu calificación.

1.2 Fingerprinting (parte 2 - Enumeración)

Numerar no es lo mismo que enumerar. Numerar es contar por el orden de los números.

- La maestra numeró a los estudiantes para verificar si le faltaba alguno: 1, 2, 3, 4, 5,

Enumerar es enunciar sucesivamente las partes de un conjunto.

- Mi hermano enumeró una lista interminable de asuntos pendientes.

Enumeración es la expresión sucesiva de las partes de que consta un todo, ya sea total o parcialmente.

Técnicas de enumeración:

- Extracción de nombres de usuario de correos electrónicos
- Extraer información usando las contraseñas por defecto
- Extraer nombres de usuarios usando SNMP
- Ataque de fuerza bruta al Directorio Activo
- Extraer grupos de usuario de Windows
- Extraer información de DNS usando transferencias de zona

Para comenzar con este tema, emplearemos la herramienta “**nmap**”.

El comando **nmap** (abreviatura de Network Mapper) es una de las herramientas más conocidas y utilizadas en el ámbito de la seguridad informática y la administración de redes. Su función principal es explorar redes, descubrir dispositivos conectados y analizar los servicios que están activos en ellos.

Nmap permite a los administradores de sistemas y a los profesionales de ciberseguridad obtener una visión clara de la estructura de una red. Con él se pueden identificar hosts activos, puertos abiertos, servicios en ejecución e incluso detectar posibles vulnerabilidades. Su potencia y flexibilidad lo convierten en una herramienta fundamental tanto para auditorías de seguridad como para tareas de diagnóstico.

Un poco de historia

Nmap fue creado en 1997 por **Gordon Lyon**, también conocido por su alias Fyodor. Su primera versión apareció publicada en la revista **Phrack**, una conocida publicación dentro del mundo hacker. En sus inicios, nmap era una herramienta relativamente sencilla diseñada para escanear puertos en sistemas Linux.

Con el paso del tiempo, el proyecto creció enormemente gracias a la comunidad de código abierto. Se añadieron nuevas funcionalidades como:

- Detección de sistemas operativos (OS fingerprinting)
- Escaneo de servicios y versiones
- Scripts automatizados mediante el motor NSE (Nmap Scripting Engine)
- Interfaz gráfica (Zenmap)

Hoy en día, nmap es una herramienta multiplataforma que funciona en sistemas como Linux, Windows y macOS, y es considerada un estándar en el sector de la seguridad informática.

Importancia actual

A lo largo de los años, nmap ha pasado de ser una utilidad técnica a convertirse en una pieza clave en pruebas de penetración (pentesting), auditorías de red y tareas de monitorización.

Su desarrollo continuo y su naturaleza abierta han permitido que se adapte a las nuevas necesidades de seguridad en un entorno digital cada vez más complejo.

Su página web oficial es: <https://nmap.org>

Como la parte fundamental de este punto es el empleo de esta herramienta de forma práctica, lo mejor es que no centremos directamente en el siguiente video, donde se presenta todo una serie de ellos a través de nmap.

Para cerrar esta segunda partea parte “Enumeración”, debes abrir el video **(Obligatorio)**:

Video 152. 🌐 Fingerprinting (parte 2 - Enumeración) -
Charla 73 - Aprendiendo Ciberseguridad paso a
paso

<https://youtu.be/CL03n3i2TQI>



1.3 Fingerprinting (parte 3 - Enumeración Móvil)

En esta tercera parte, trabajaremos desde un teléfono móvil, pues es un dispositivo con el que contamos casi las 24 horas, y en alguna oportunidad se nos presentará la necesidad de realizar tareas de fingerprinting, y/o footprinting, desde uno de ellos.

Para poder ejecutar herramientas específicas de enumeración, es necesario en primer lugar **“rootear un teléfono móvil”**

El proceso de **rootear un teléfono móvil** consiste en obtener privilegios de superusuario (o administrador) sobre el sistema operativo del dispositivo, normalmente basado en Android. Esto permite al usuario acceder y modificar partes del sistema que, por defecto, están restringidas por motivos de seguridad.

Consideración importante

Aunque el rooteo ofrece grandes ventajas, también implica riesgos:

- Pérdida de garantía del dispositivo
- Mayor exposición a vulnerabilidades si no se gestiona correctamente
- Posible inestabilidad del sistema

Por ello, es fundamental comprender bien el proceso y sus implicaciones antes de llevarlo a cabo, especialmente si se pretende utilizar el dispositivo en entornos profesionales.

Recomendamos especialmente que esta actividad la lleves a cabo con un teléfono móvil secundario, o que ya no emplees. **NO LO HAGAS CON TU MÓVIL PRINCIPAL.**

Introducción general

En un dispositivo sin root, el usuario opera con permisos limitados para evitar cambios que puedan comprometer la estabilidad o la seguridad del sistema. Sin embargo, al rootear el

teléfono, se eliminan estas restricciones, permitiendo instalar herramientas avanzadas, modificar configuraciones internas o acceder directamente al sistema de archivos completo.

Este nivel de control resulta especialmente útil en entornos técnicos, como la administración de sistemas o la ciberseguridad, donde se requieren capacidades más profundas que las ofrecidas por un dispositivo convencional.

Contexto y evolución

El concepto de “**root**” proviene de los sistemas Unix y Linux, donde el usuario *root* es el administrador con control total del sistema. Con la popularización de Android (basado en el núcleo Linux), la comunidad empezó a desarrollar métodos para obtener estos privilegios en dispositivos móviles.

En sus primeras etapas, rootear un móvil era un proceso complejo y arriesgado, que implicaba explotar vulnerabilidades del sistema. Con el tiempo, surgieron herramientas más accesibles y métodos más estandarizados, aunque los fabricantes han reforzado las medidas de seguridad, dificultando cada vez más este proceso en dispositivos modernos.

Uso en enumeración de redes y sistemas

En el ámbito de la seguridad informática, un dispositivo rooteado puede convertirse en una potente herramienta portátil para tareas de **enumeración**, es decir, la recolección de información sobre redes y sistemas. Algunas ventajas clave incluyen:

- Acceso completo a interfaces de red y configuraciones avanzadas
- Posibilidad de utilizar herramientas especializadas de análisis y escaneo
- Captura de tráfico de red sin restricciones
- Automatización de tareas mediante scripts con permisos elevados

Esto permite transformar un smartphone en una especie de “mini laboratorio” de auditoría, útil para pruebas de penetración, análisis de redes inalámbricas o diagnóstico de sistemas.

En nuestro siguiente ejemplo presentamos los pasos para rootear el móvil Samsung, concretamente un Samsung Galaxy s6 - Versión de firmware SM-G920F - ANDROID 7.

El detalle de cómo hacerlo lo tienes en el video:

Hacking móvil

<https://youtu.be/ZKlqgdbQI9o>



Lo rotearemos empleando la herramienta **ODIN** siguiendo este enlace:

<https://www.techmoviles.com/como-rotear-samsung-galaxy-s6-sm-g920f-con-cf-auto-root/>

Los pasos a seguir, están muy claros en: “**como rotear samsung galaxy s6 con odin**”

<https://miracomohacerlo.com/rootear-samsung-galaxy-s6-galaxy-s6-edge-sin-pc/>

La herramienta Odin, puede descargarse en:

<https://odindownload.com>

A continuación instalaremos: **TERMUX** y el **sshd**:

Una vez instalado Termux, empleando el mismo como una interfaz de comandos Linux, instalaremos:

```
openssh  
nmap  
wget  
coreutils  
tsu  
vi o vim
```

Se creará un nuevo un nuevo servidor ssh (se puede llamar, por ej: "servidor ssh") para conectarnos al servidor ssh:

```
ssh -oHostKeyAlgorithms=+ssh-dss ssh@tu_direccion_IP -p 2222
```

instalaremos **tcpdump** desde termux y solo lo podremos ejecutar desde Termux (en el directorio: /data/data/com.termux/files/home)

Lo podremos ejecutar desde:

```
/data/data/com.termux/files/home # ./tcpdump
```

Termux ya trae también un servidor ssh:

```
lanzarlo: sshd  
detenerlo: pkill sshd
```

Nos podemos conetar al mismo con: `ssh u0_a189@192.168.1.71 -p 8022 (passwd: "la que pusimos")`. Luego nos me dejará hacer "su".

Todos estos pasos, se describen con más detalle en esta tercera parte "Enumeración Móvil", en el video **(Obligatorio)**:

Video 🌐 Fingerprinting (**parte 3 - Enumeración Móvil**) -
Charla 76 - Aprendiendo Ciberseguridad paso a paso
<https://youtu.be/CbdFJ2ORzj4>

