Indice

[Linux 2](#_Toc158218726)

[Escaneo Pasivo 2](#_Toc158218727)

[Sniffer 2](#_Toc158218728)

[Arp-scan 6](#_Toc158218729)

[NMAP 7](#_Toc158218730)

[Ping 8](#_Toc158218731)

[Escaneo Activo 9](#_Toc158218732)

[HPING3 9](#_Toc158218733)

[NMAP 9](#_Toc158218734)

[Enumeración 10](#_Toc158218735)

# Linux

## Escaneo Pasivo

### Sniffer

El escaneo pasivo tiene como utilidad el conocer un objetivo de ataque sin la necesidad de escanear la red completa de forma activa. En un escenario real, se observa que, al realizar un sniffing de red, se generan numerosas peticiones de conexión a distintos servicios para una o varias IP específicas. Estas conexiones proporcionan información sobre la importancia de ese punto en la red. Sin embargo, es importante tener en cuenta que no necesariamente se trata de un servidor central que debamos considerar como objetivo principal, ya que también podría tratarse de un firewall o un proxy independiente que intercepte estos paquetes en primer lugar.

Para este ejemplo es complicado realizar un sniffing de red óptimo, ya que disponemos de máquinas que realmente no están realizando conexiones reales, no tiene clientes activos, por lo que voy a generar peticiones de conexión a distintos servicios (con éxito o no) a fin de visualizar lo que ocurre a nivel de red.

Pero antes que eso, me gustaría mostrar una información interesante que he encontrado haciendo sniffing de mi propia red local:

Lo primero es que para hacer sniffing con adaptador puente existe una opción avanzada llamada “Modo Promiscuo, que según fuentes que he encontrado en internet (<https://www.pinguytaz.net/index.php/2016/11/20/virtualbox-configurando-la-red/> ) si está desactivado podemos ver los paquetes, pero sin información, se muestran como multicast usando el protocolo mDNS sin otorgar más información. Por lo que yo como quiero analizar mi red lo coloco en “Permitir todo”.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Bien, ya teniendo acceso a mi red observo que constantemente se realizan paquetes con cabeceras PSH desde dos IP públicas concretas (212.145.41.32 y 77.209.227.18) lo que me pareció muy raro, por lo que visité la web de Virustotal para revisar ambas IP, resultando ser direcciones IP limpias pertenecientes a Vodafone, así que tranquilo porque mi conexión a Internet es mediante una red 4G de Vodafone precisamente.

Imagen que contiene Interfaz de usuario gráfica

Descripción generada automáticamente

Patrón de fondo

Descripción generada automáticamente con confianza media

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Patrón de fondo

Descripción generada automáticamente con confianza media

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Como tengo curiosidad decido ejecutar un Whoami desde la máquina Kali con ambas IP, recibiendo el siguiente resultado:

Para la IP 212.145.41.32 obtengo que se trata de un servicio de RIPE Database Quer, que juntándolo con la información de Virustotal sobre Vodafone y una descripción de ChatGPT:

“El servicio de consulta de la base de datos RIPE (RIPE Database Query Service) se refiere a un sistema de consulta que permite acceder a la base de datos mantenida por RIPE NCC (Réseaux IP Européens Network Coordination Centre). RIPE NCC es una organización que se encarga de la asignación y coordinación de recursos de direcciones IP y números de sistemas autónomos en Europa, Oriente Medio y partes de Asia Central.

La base de datos mantenida por RIPE NCC contiene información sobre los recursos de Internet asignados o registrados en su área de responsabilidad, incluyendo direcciones IP, bloques de direcciones IPv4 e IPv6, asignaciones de sistemas autónomos (ASNs), contactos de administración y otros datos relacionados con la infraestructura de Internet en la región que cubre RIPE NCC.

El servicio de consulta de la base de datos RIPE permite a los usuarios realizar consultas y búsquedas en esta base de datos para obtener información sobre recursos específicos de Internet, direcciones IP, nombres de dominio, contactos de administración y otros detalles relevantes. Esto puede ser útil para investigar la propiedad de recursos de Internet, identificar a los responsables de ciertos servicios en línea, diagnosticar problemas de red y realizar análisis de infraestructura de Internet.”

Deduzco por lógica que se trata de un servicio de gestión de recursos de red que usa Vodafone para las conexiones LTE (en este caso), desconozco si para otro tipo de conexiones, dada su distinta naturaleza utiliza este servicio.

Texto

Descripción generada automáticamente

Para el caso de la IP 77.209.227.18 se observa que se trata de otro RIPE de VODAFONE, cuyos atributos descripción es VODAFONE\_SPAIN\_NETWORK y role VODAFONE ESPANA ROLE, dirección completa en Madrid y más información de RIPEs

Captura de pantalla de un celular

Descripción generada automáticamente

Texto

Descripción generada automáticamente

Otra curiosidad es una conexión HTTPS a la IP 104.1.239.159, que resulta ser un servicio de AT&T usado por ARIN (American Registry for Internet Members).

Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente

Entre otras cosas se puede observar cómo mi ordenador de casa realiza conexiones a diferentes servicios externos. Pero. ¿qué pasa si tenemos un servidor? Que será ese servidor quien reciba numerosas conexiones entrantes, por lo que, realizar un sniffing de red en torno a realizar cualquier actividad relacionada con Hacking Ético, se puede determinar de todas las máquinas conectadas dentro de la red local cuál sería el servidor analizando el tráfico de red, y además de eso, podemos averiguar servicios, información de conexiones internas con otros servicios y una serie de actividades para tenerlas en cuenta en los próximos pasos de nuestra labor.

### Arp-scan

La herramienta ARP-SCAN se centra en el descubrimiento, utilizando el protocolo ARP (Address Resolution Protocol), el cual envía solicitudes ARP a todas las direcciones IP en una misma red, registrando las respuestas y enumerando los dispositivos activos en la red, mapeando direcciones IP a direcciones MAC en una red local.

Texto

Descripción generada automáticamente

Si tuviéramos más de una interfaz conectada al equipo y quisiéramos escanear únicamente una de ellas podríamos realizarlo del siguiente modo:

Texto

Descripción generada automáticamente

Como se puede observar, arp-scan nos permite conocer la magnitud de la red, pero no nos otorga mucha más información.

### NMAP

Con NMAP podemos realizar un escaneo basado en paquetes ICMP a toda la red, que, aunque haga un poco de ruido no lo considero un escaneo tan activo.

Texto

Descripción generada automáticamente

Como se puede apreciar NMAP nos da más información, y nos dice que existen dos máquinas de VirtualBox, una con la IP 10.0.2.15 y otra con la 10.0.2.5

Si observamos la IP de nuestra máquina Kali podemos observar que se trata de la 10.0.2.5, por lo que por descarte ya conocemos que la máquina victima es la 10.0.2.15

Texto

Descripción generada automáticamente

Si se desea realizar este proceso sin escanear la red, podemos utilizar la información que nos ha dado arp-scan y escanear un rango de direcciones IP, por ejemplo, desde la 10.0.2.1 hasta la 10.0.2.15

Texto

Descripción generada automáticamente

Para el ejemplo anterior se me ocurre la opción de guardar el resultado de arp-scan en un fichero y generar una lista que contenga solamente la enumeración de las IP a fin de utilizar esa lista para escanear únicamente las IP que hay dentro de la red local.

### Ping

Podemos verificar que tenemos conexión con la víctima realizando un ping:

Texto

Descripción generada automáticamente

## Escaneo Activo

### HPING3

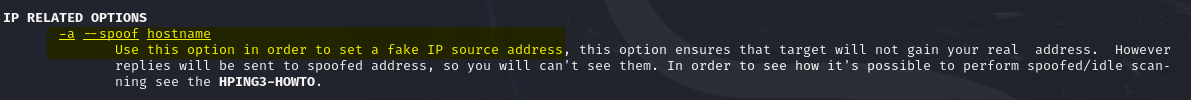
Con HPING3 se pueden realizar escaneos más en profundidad para comprobar los puertos TCP a la escucha mediante el envío de paquetes SYN, paquete que se envía para el proceso de establecer una conexión TCP:

Imagen de la pantalla de un video juego

Descripción generada automáticamente con confianza baja

Donde --scan se especifica el intervalo de puertos, --syn especifica un escaneo basado en paquetes SYS y por último la IP de la víctima

HPING3 tiene opciones interesantes, como utilizar una IP falsa de origen para enviar los paquetes (aprendí sobre Linux con la filosofía RTFM [Read the Fucking Manual])



### NMAP

Con NMAP podemos realizar un escaneo basado en SYS (sin terminar la conexión **-PS**) ACK (terminando la conexión **-PA**), protocolos UDP (**-PU**) o SCTP (es un protocolo orientado a las conexiones, similar a TCP, pero proporciona la transferencia de datos orientada a mensajes, similar a UDP **-PY**):

Texto

Descripción generada automáticamente

Con NMAP además podemos conocer la versión del Daemon utilizado para el servicio utilizando la opción -sV, esta opción es sumamente valiosa para encontrar posibles vulnerabilidades:

Texto

Descripción generada automáticamente

## Enumeración

Para el proceso de enumeración se recolecta la información de los servicios abiertos en la máquina tales como la versión y aparejarlas con las posibles vulnerabilidades conocidas sobre dicha versión con el objetivo de realizar un plan de acción a la hora de explotar la máquina.

Lo que voy a hacer a continuación es una búsqueda de servicios a la escucha, controlando su versión y voy a destinar la salida a un fichero de texto para tener la enumeración de los servicios a mano sin la necesidad de ejecutar nmap cada vez que quiera buscar información sobre los diferentes servicios.

Texto

Descripción generada automáticamente

Adicionalmente también realizo un escaneo que lleva más tiempo aún, como puede ser ejecución de Scripts por defecto y el script vuln, que ya nos da un listado de posibles vulnerabilidades asociadas a un determinado servicio con una determinada versión, aunque puede ser un falso positivo, por lo que debemos comprobarlo más adelante.

nmap -O -sV -vv 10.0.2.15 > TCP\_sV.txtnmap -vv -sC 10.0.2.15 > sC.txt

nmap 10.0.2.15 -vv --script=vuln > vulners.txt

Como el proceso de enumeración puede ser extenso debido a la cantidad de servicios voy a ir de uno en uno.

Bien, analizando el servicio FTP, toda la información que se es que tiene la versión ProFTPD 1.3.5. El escaneo -sC y la ejecución del script vuln de NMAP no arroja ninguna otra información, por lo que toca buscar en fuentes públicas, encontrando un CVE asociado a este servicio FTP: “CVE-2015-3306”.

Fuentes de CVE-2015-3306:

* <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3306>
* <https://www.cvedetails.com/cve/CVE-2015-3306/?q=CVE-2015-3306>