Ciberseguridad Práctica 2

**Escaneo de Red**

Daniel Varela Sánchez & Guillermo Martín-Coello Juárez

# 

# **Introducción**

Una de las principales formas de proteger un sistema es conocer las tácticas y pasos que utilizan los atacantes para explotar los defectos en la seguridad. En este sentido, la práctica de escaneo de red es una herramienta fundamental para identificar las posibles vulnerabilidades en una red y poder proteger el contenido sensible adecuadamente.

En esta práctica se llevará a cabo un escaneo con la herramienta “nmap” desde una máquina atacante “Kali-Linux”, con el objetivo de identificar la topología de red, los servicios activos y las vulnerabilidades más significativas que puedan afectar a los sistemas identificados.

El presente informe detalla las metas de la práctica, los pasos a seguir y los resultados obtenidos, con el fin de conocer y evaluar los problemas de seguridad existentes en una red local.

# 

# Desarrollo

## Cuestión 1, Encontrar IP objetivo:

En primer lugar, tenemos que encontrar la dirección IP que tiene la máquina objetivo. Para esto, ya que estamos en la misma red NAT, simplemente nos basta con escanear todas las redes conectadas a dicha red NAT para encontrar aquellas de interés, utilizando el comando nmap -sn. También tenemos que conocer la IP de nuestra propia máquina (para ello en este caso hemos utilizado hostname -I).

|  |
| --- |
| Imagen 1: utilización del comando nmap para encontrar hosts interesantes en la red NAT. |

Como podemos observar, aunque no nos haya devuelto el hostname al hacer el escaneo (debido a la configuración DNS), gracias a la dirección MAC podemos obtener información sobre cada uno de los host conectados a la NAT. En este caso, ya que nuestra máquina es el dispositivo 5, sabemos que la máquina objetivo es el dispositivo 4 (IP 10.0.2.4).

## 

## Cuestión 2, Identificar puertos TCP abiertos en objetivo:

Para identificar los puertos abiertos utilizamos el comando nmap sobre la ip objetivo, obteniendo de vuelta todos sus puertos abiertos, con información sobre cada uno de ellos.

|  |
| --- |
| Imagen 2: utilización del comando nmap para encontrar los puertos abiertos de la máquina objetivo. |

## 

## Cuestión 3, Señalar puertos UDP abiertos más frecuentes:

Continuando con la identificación de la topología de red de la máquina objetivo, escaneamos los puertos UDP más frecuentes (en este caso hemos escogido los 10 primeros), de nuevo utilizando nmap pero con la especificación -sU para obtener los UDP.

|  |
| --- |
| Imagen 3: Escaneo del top 10 puertos UDP abiertos de la máquina objetivo. |

## 

## Cuestión 4, Indicar la versión de los servicios ejecutándose en diversos puertos:

Para obtener la versión de los servicios ejecutándose en un puerto determinado, utilizaremos el comando nmap -sV -p, indicando el puerto objetivo y la ip de la máquina objetivo

|  |
| --- |
| Imagen 4.1: utilización del comando nmap para obtener la versión de los servicios ejecutándose en el puerto 22. |

|  |
| --- |
| Imagen 4.2: utilización del comando nmap para obtener la versión de los servicios ejecutándose en el puerto 23. |

|  |
| --- |
| Imagen 4.3: utilización del comando nmap para obtener la versión de los servicios ejecutándose en el puerto 80. |

En el caso de los puertos UDP, cambiaremos el comando que utilizamos a nmap -sUV -PU, pero con los mismos parámetros. Durante nuestro escaneo no hemos obtenido resultados. Esto se debe a que ningún paquete UDP ha llegado al objetivo. Esto podría cambiar si se escanea durante más tiempo o se ejecutan programas en la máquina.

|  |
| --- |
| Imagen 4.4: utilización del comando nmap para obtener la versión de los servicios ejecutándose en el puerto UDP 2049. |

|  |
| --- |
| Imagen 4.5: utilización del comando nmap para obtener la versión de los servicios ejecutándose en el puerto 5432. |

|  |
| --- |
| Imagen 4.6: utilización del comando nmap para obtener la versión de los servicios ejecutándose en el puerto 3306. |

## Cuestión 5, Averiguar la versión de Sistema Operativo instalado en la máquina objetivo:

Utilizando nmap -O podemos obtener información sobre el sistema operativo de la máquina objetivo.

|  |
| --- |
| Imagen 5: Obtener versión del SO de la máquina objetivo. |

Como podemos observar, la máquina objetivo presenta una versión de Linux que ronda entre la 2.6.9 y la 2.6.33.

## 

## 

## Cuestión 6, Capturar bandera flag1.txt:

Como ya hemos podido observar tras el análisis que hemos hecho, la máquina objetivo tiene ciertas posibles vulnerabilidades que podemos utilizar para entrar en ella. Una de ellas se encuentra en el puerto 2049, RFS, que nos puede permitir acceder a sus archivos sin tener que hacer login. Con esto bastaría para encontrar la flag que buscamos, pero vamos a ir un paso más allá y entrar en el sistema, para poder buscarla directamente desde dentro. Usar la vulnerabilidad de RFS nos permite acceder a los archivos del objetivo y guardar nuestra clave pública como usuario registrado y así acceder sin problema.

Para ello primero creamos un par de claves RSA pública-privada. A continuación volcamos los archivos de la máquina objetivo usando nfs para poder editarlos.

|  |
| --- |
| Imagen 6.1: Creación de claves y volcado de archivos. |

Una vez tenemos las claves y los archivos, copiamos la clave pública en el archivo de claves autorizadas para iniciar sesión de la máquina objetivo.

|  |
| --- |
| Imagen 6.2: Copia de clave pública para autorización de login en máquina objetivo. |

Finalmente, ejecutamos el comando ssh usando la clave privada generada para acceder al usuario root de la máquina objetivo.

|  |
| --- |
| Imagen 6.3: Acceso a usuario root utilizando ssh y clave privada. |

Desde el sistema basta con hacer una sencilla búsqueda del archivo con el comando find para encontrar la flag que buscábamos. Además podemos modificar los permisos de ésta para que solo el administrador tenga acceso a ella.

|  |
| --- |
| Imagen 6.4: Búsqueda de flag y cambio de permisos. |

## Cuestión 7, Conectar al servidor SQL y obtener hash del admin:

Como ya hemos accedido al sistema como usuario root, simplemente utilizamos los comandos de mysql para acceder a las bases de datos. En el caso de que no hubiésemos accedido al sistema, podríamos haber aprovechado la vulnerabilidad del puerto 3306 (tcp).

|  |
| --- |
| Imagen 7.1: Utilización de comandos de mysql para obtener acceso a base de datos. |

Accedemos a la base de datos tikiwiki, donde existen diferentes tablas. Buscamos la tabla de usuarios (en este caso users\_users) Y hacemos una query para obtener el hash del admin. Además, hemos podido comprobar que la base de datos también guarda las contraseñas sin cifrar (poco seguro).

|  |
| --- |
| Imagen 7.2: Obtención del hash del administrador de la base de datos tikiwiki. |

## 

## Cuestión 8, Explicación documentada, siguiente paso:

La importancia que tienen los puntos 5, 6 y 7 desde el punto de vista de un atacante es que en ellos se utilizan las vulnerabilidades del sistema para acceder a datos sensibles que no deberían de ser accesibles para un usuario no autorizado. Como ya hemos comentado en el punto 6, el paso siguiente (que ya hemos ejecutado y documentado en dicho punto) sería obtener acceso al inicio de sesión del ordenador objetivo y acceder completamente a su sistema sin ninguna restricción. Esto, para un atacante maligno significa el completo acceso y capacidad de uso de todos los datos y facultades del sistema. A partir de aquí el atacante podría robar los datos, eliminarlos, secuestrarlos, eliminar el acceso al resto de usuarios, etc.

## 

## Cuestión 9, Tabla con herramientas y órdenes utilizadas:

Órdenes y herramientas del ejercicio 1)

| hostname -I | Muestra la IP de la máquina. |
| --- | --- |
| sudo nmap -sn 10.0.2.0/24 | Encuentra los hosts interesantes en la red NAT. |

# Órdenes y herramientas del ejercicio 2)

| nmap 10.0.2.4 | Escaneo puertos TCP del objetivo. |
| --- | --- |

# Órdenes y herramientas del ejercicio 3)

| sudo nmap -sU --top-sports 10 10.0.2.4 | Escaneo puertos UDP del objetivo (10 más usados). |
| --- | --- |

# Órdenes y herramientas del ejercicio 4)

| sudo nmap -sV -p 22 10.0.2.4 | Escaneo puerto TCP del objetivo. |
| --- | --- |
| sudo nmap -sV -p 23 10.0.2.4 | Escaneo puerto TCP del objetivo. |
| sudo nmap -sV -p 80 10.0.2.4 | Escaneo puerto TCP del objetivo. |
| sudo nmap -sUV -PU 2049 10.0.2.4 | Escaneo puerto TCP del objetivo. |
| sudo nmap -sV -p 5432 10.0.2.4 | Escaneo puerto TCP del objetivo. |
| sudo nmap -sV -p 3306 10.0.2.4 | Escaneo puerto TCP del objetivo. |

# Órdenes y herramientas del ejercicio 5)

| sudo nmap -O 10.0.2.4 | Obtención de detalles del Sistema Operativo del objetivo. |
| --- | --- |

# Órdenes y herramientas del ejercicio 6)

| ssh-keygen | Generador de claves público-privadas. |
| --- | --- |
| cat .ssh/id\_rsa.pub >> /mnt/root/.ssh/authorized\_keys | Copia clave pública en claves autorizadas para inicio de sesión del objetivo |
| ssh -i .ssh/id\_rsa root@10.0.2.4 | Comando ssh para iniciar sesión en el servidor objetivo |
| find / -name flag1.txt | Comando de búsqueda de archivo por nombre |

# Órdenes y herramientas del ejercicio 7)

| mysql -u root -p | Accede a mySQL como usuario root. |
| --- | --- |
| SHOW databases; | Muestra todas las bases de datos. |
| USE tikiwiki | Establece tikiwiki como la base de datos a usar. |
| SELECT login, password, hash FROM users\_users; | Selecciona los campos login, password y hash de la tabla users\_users |

# 

# Conclusiones

La realización de esta práctica nos ha permitido conocer de manera más profunda las técnicas de escaneo de red y su importancia en la aplicación de métodos de seguridad informática.

Hemos aprendido que el escaneo de red, cuyo propósito es identificar un objetivo y recopilar toda la información posible sobre el mismo, es un proceso crucial a la hora de llevar a cabo un ataque informático.

Este proceso es llevado a cabo mediante la identificación de varios elementos que consisten en: las direcciones de red de los sistemas accesibles, la topología de red, los servicios que se encuentran activos en cada objetivo identificado, la determinación del sistema operativo y la versión, el tipo de sistema al que corresponde, y las vulnerabilidades más significativas que puedan afectar a los servicios y sistemas identificados.

Asimismo, esta práctica nos ha permitido familiarizarnos con la herramienta “nmap” y su capacidad para realizar escaneos de red de manera efectiva.

También hemos aprendido cómo utilizar “Kali-Linux” como una herramienta de “pentesting” para evaluar las carencias de seguridad existentes en una red local y recuperar datos acerca de la misma.

En resumen, la elaboración de este proyecto nos ha permitido adquirir habilidades relevantes y de gran utilidad en el campo de la ciberseguridad. En especial cabe destacar la capacidad de analizar, sintetizar y organizar datos dentro del área de seguridad informática, lo que nos permitirá aplicar estos conocimientos en futuros proyectos y situaciones en el mundo laboral.