Práctica de laboratorio: Análisis de vulnerabilidades con Kali Tools

Objetivos

En esta práctica de laboratorio, explorará las herramientas de escaneo de vulnerabilidades de la red y las utilizará para realizar un escaneo de vulnerabilidades en un host de destino.

- Realizar escaneos de red con Nmap
- Utilice la administración de vulnerabilidades de Greenbone para realizar un escaneo de vulnerabilidades.

Aspectos básicos/Situación

En una práctica de laboratorio anterior, utilizó Nmap para enumerar una computadora host que estaba creando un tráfico inusual en la red. En esta práctica de laboratorio, utilizará Nmap y Greenbone Vulnerability Management (GVM) para escanear el sistema e identificar posibles vulnerabilidades.

Recursos necesarios

- Kali VM personalizada para el curso de Ethical Hacker
- Acceso a Internet

Instrucciones

Parte 1: Ejecutar un escaneo de Nmap en una computadora de destino

En esta parte, utilizará los scripts de Nmap y NSE para descubrir posibles vulnerabilidades en un host de destino.

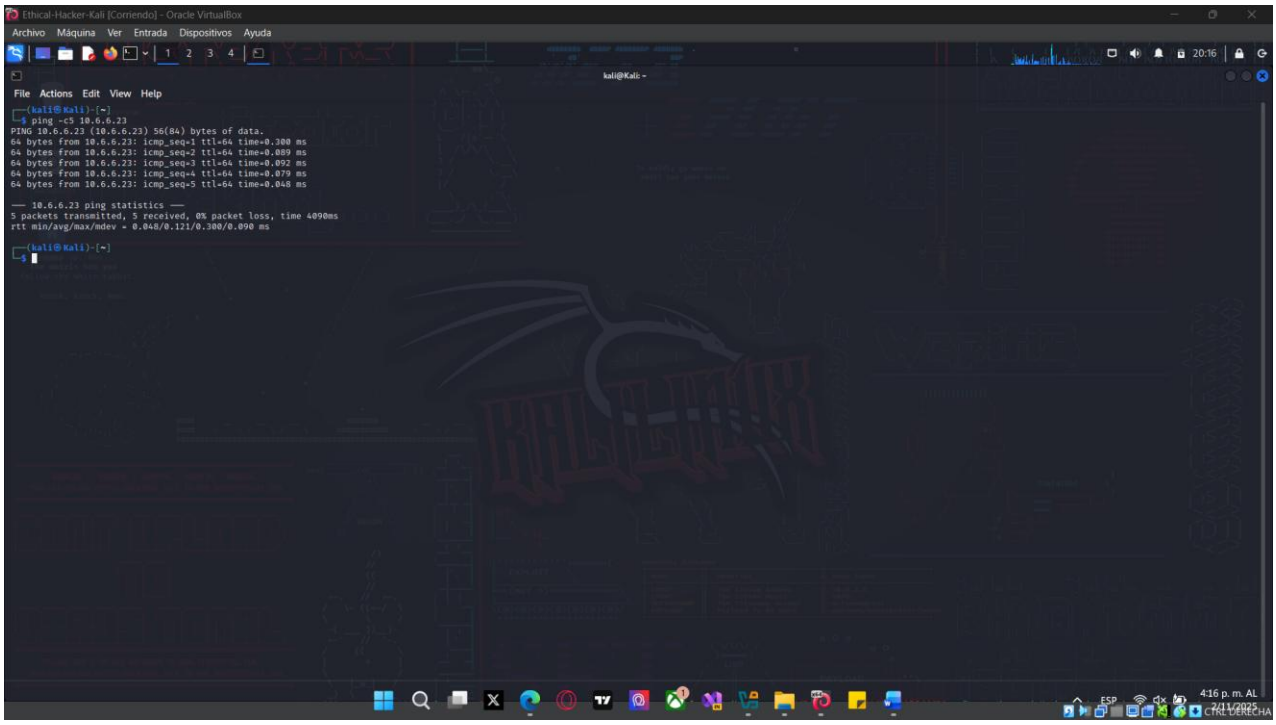
Paso 1: Inicie e inicie sesión en la máquina virtual Kali.

a. Inicie y comience la sesión en la máquina virtual Kali.

b. Inicie una sesión de terminal. Expanda la ventana del terminal a pantalla completa. Utilice el comando **ping** para determinar si se puede acceder a la computadora con la dirección **10.6.6.23** o **gravemind.vm** a través de la red.

```
┌──(kali㉿Kali)-[~]
└─$ ping -c5 10.6.6.23
```

La opción **-c5** le indica al comando ping que se detenga después de cinco intentos. En Linux, cuando no se especifica la opción a **-c**, el comando **ping** continuará indefinidamente hasta que se emita **CTRL-C**.



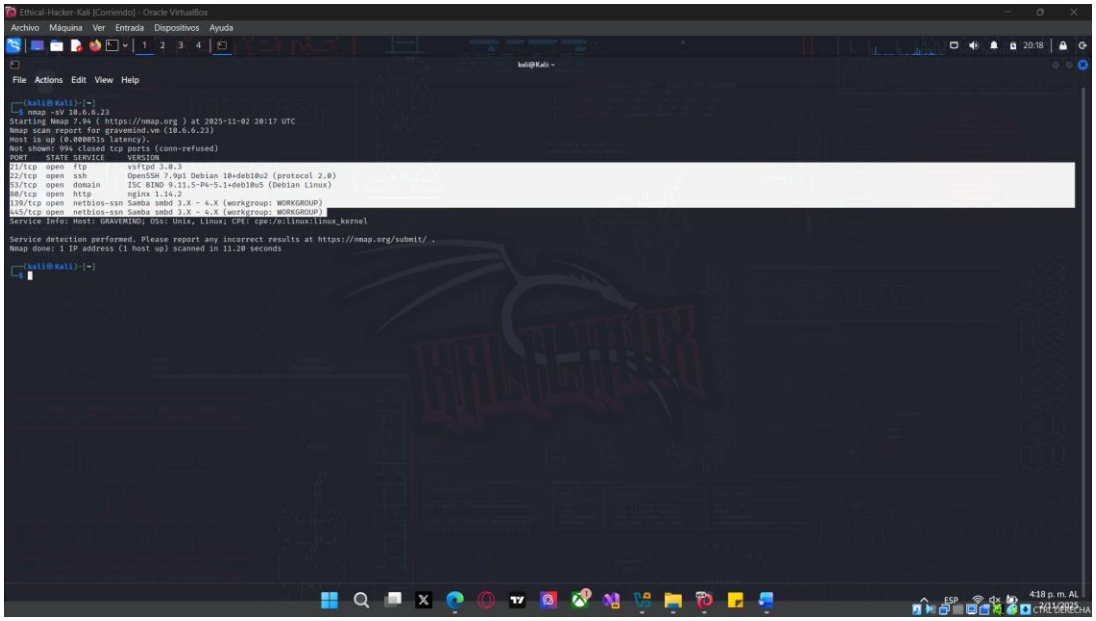
Paso 2: Identifique puertos y servicios abiertos.

Revise los resultados de un escaneo de Nmap en el host con la dirección IP 10.6.6.23.

a. Ejecute un escaneo de ping del host de destino con el comando **nmap -sV** . Tenga en cuenta la lista de puertos y aplicaciones que se detectan en el host.

```
┌──(kali㉿Kali)-[~]
└─$ nmap -sV 10.6.6.23
```

¿Qué puertos están abiertos actualmente en la computadora de destino?



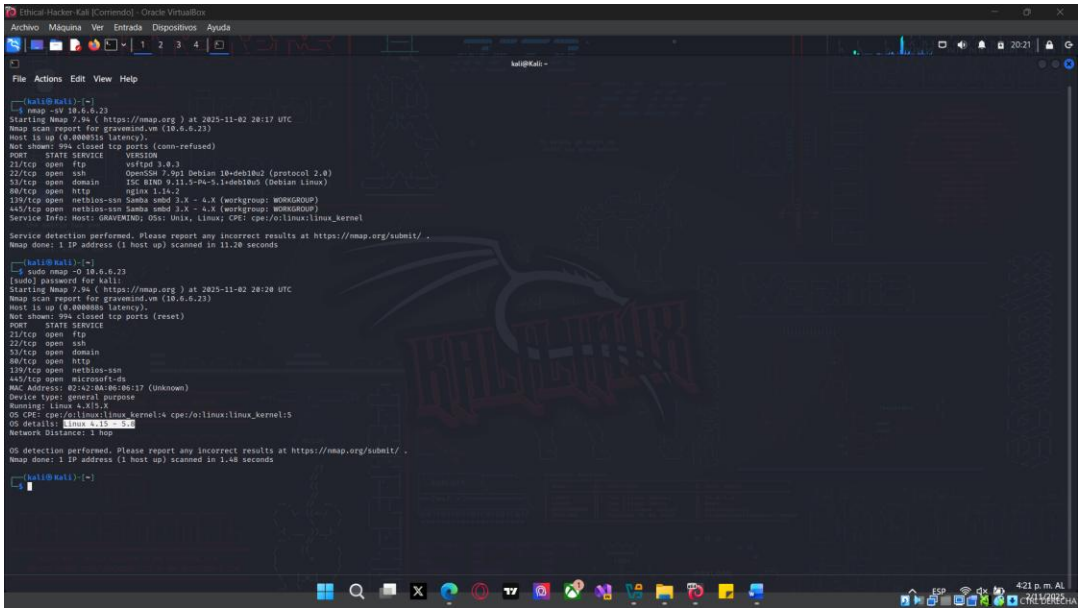
21, 22, 53, 80, 139 y 445

b. Identifique el sistema operativo que se ejecuta en el equipo de destino mediante el comando **nmap -O**.

```
┌──(kali㉿Kali)-[~]
└─$ sudo nmap -O 10.6.6.23
```

¿Qué sistema operativo ejecuta el equipo de destino?

MOSTRAR CAPTURA



Linux 4.15 - 5.6 al momento de escribir este artículo

Paso 3: Utilice el guion de Nmap Vulners para buscar vulnerabilidades.

El guion de Vulners muestra las vulnerabilidades conocidas y la CVE correspondiente. El guion de Vulners utiliza la información de versión de software y puerto abierto para buscar nombres de enumeración de plataforma común (CPE) que se relacionan con el servicio identificado. Luego realiza una solicitud a un servidor remoto para averiguar si existe alguna vulnerabilidad conocida para ese CPE.

a. Utilice el comando **nmap –script** para iniciar el guion de **Vulners**. La sintaxis del comando es **nmap -sV --script vulners [--script-args mincvss =** <arg_val>]<target> donde el argumento de guion **mincvss** restringe la salida solo a aquellas CVE que tienen una puntuación de CVSS más alta que la especificada en el argumento.

Las vulnerabilidades informadas serán aquellas con una puntuación CVE igual o superior a 4. La salida del comando debe ser similar a la que se muestra a continuación.

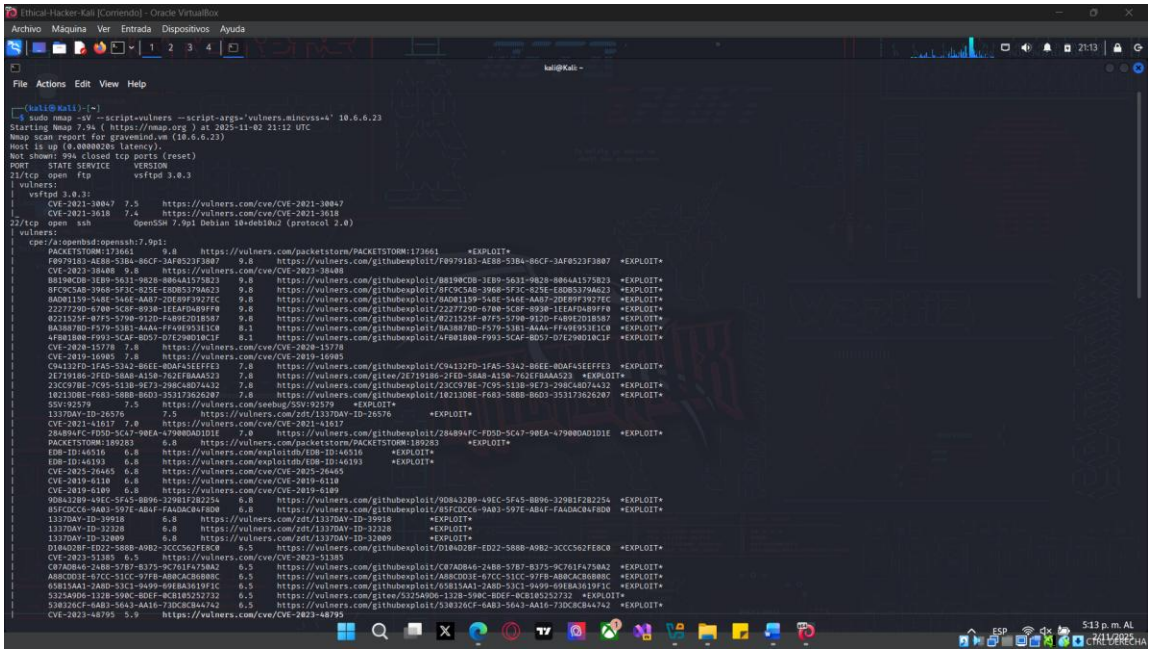
```
┌──(kali㉿Kali)-[~]
└─$ nmap -sV --script vulners --script-args mincvss=4 10.6.6.23

Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-15 14:01 MST
Nmap scan report for 10.6.6.23
Host is up (0.0000040s latency).
No se muestra: 994 puertos tcp cerrados (restablecimiento)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 3.0.3
22/tcp open ssh OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
```

```
| vulners:
| cpe:/a:openbsd:openssh:7.9p1:
| EXPLOITPACK:98FE96309F9524B8C84C508837551A19 5.8
https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F9524B8C84C508837551A19 *EXPLOIT*
| EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97 5.8
https://vulners.com/exploitpack/EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97 *EXPLOIT*
| EDB-ID:46516 5.8 https://vulners.com/exploitdb/EDB-ID:46516 *EXPLOIT*
| EDB-ID:46193 5.8 https://vulners.com/exploitdb/EDB-ID:46193 *EXPLOIT*
| CVE-2019-6111 5.8 https://vulners.com/cve/CVE-2019-6111
| 1337DAY-ID-32328 5.8 https://vulners.com/zdt/1337DAY-ID-32328 *EXPLOIT*
| 1337DAY-ID-32009 5.8 https://vulners.com/zdt/1337DAY-ID-32009 *EXPLOIT*
| CVE-2021-41617 4.4 https://vulners.com/cve/CVE-2021-41617
| CVE-2019-16905 4.4 https://vulners.com/cve/CVE-2019-16905
| CVE-2020-14145 4.3 https://vulners.com/cve/CVE-2020-14145
| CVE-2019-6110 4.0 https://vulners.com/cve/CVE-2019-6110
| CVE-2019-6109 4.0 https://vulners.com/cve/CVE-2019-6109
|_ PACKETSTORM:151227 0.0 https://vulners.com/packetstorm/PACKETSTORM:151227 *EXPLOIT*
53/tcp open domain ISC BIND 9.11.5-P4-5.1+deb10u5 (Debian Linux)
80/tcp open http nginx 1.14.2
|_http-server-header: nginx/1.14.2
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 02:42:0A:06:06:17 (Unknown)
Service Info: Host: 868CF29B394C; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.15 seconds
```

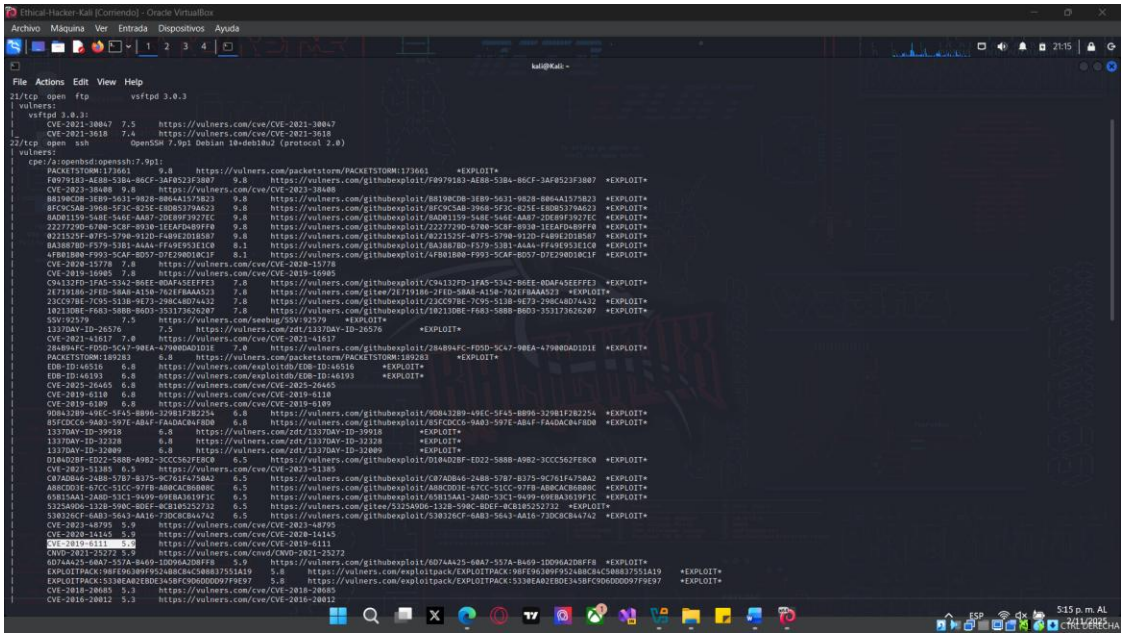
¿Qué servicio se identifica por tener vulnerabilidades conocidas asociadas?



OpenSSH

MOSTRAR CAPTURA

¿Qué CVE está asociada con la vulnerabilidad conocida de nivel 5 o superior?

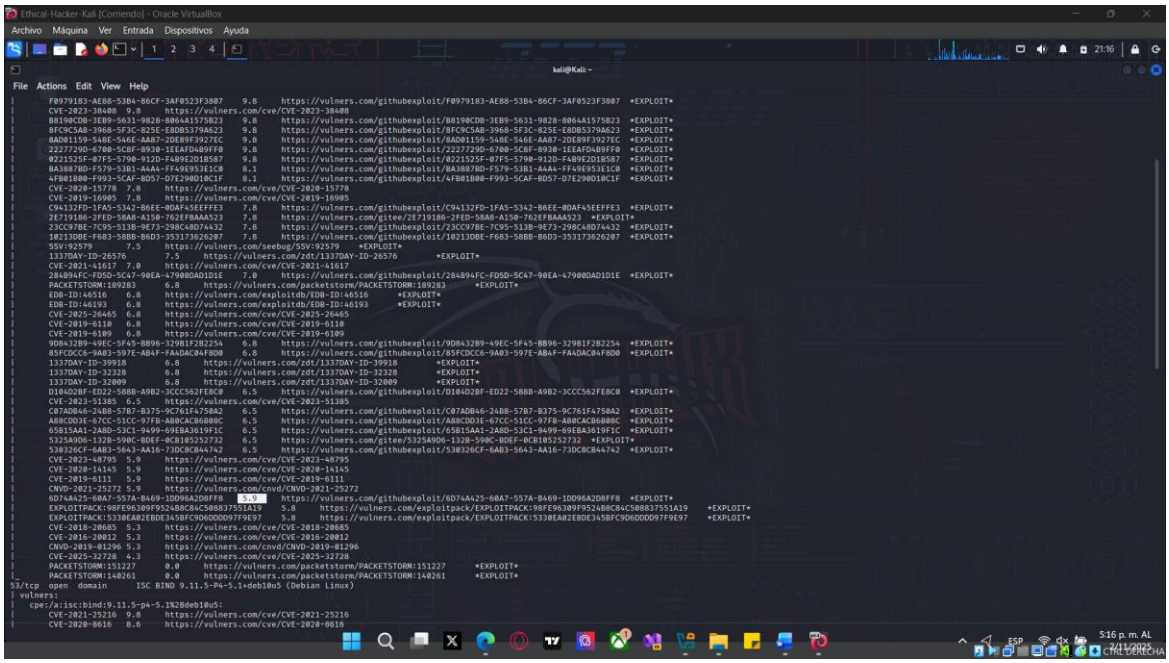


CVE-2019-6111

MOSTRAR CAPTURA

b. Utilice la Base de datos nacional de vulnerabilidades del NIST para obtener más información sobre la vulnerabilidad identificada y cómo puede aprovecharse. **https://nvd.nist.gov / vuln / search**.

¿Qué nivel de gravedad se asigna a la CVE en la base de datos del NIST?



5,9 Mediano

MOSTRAR CAPTURA