

## 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.

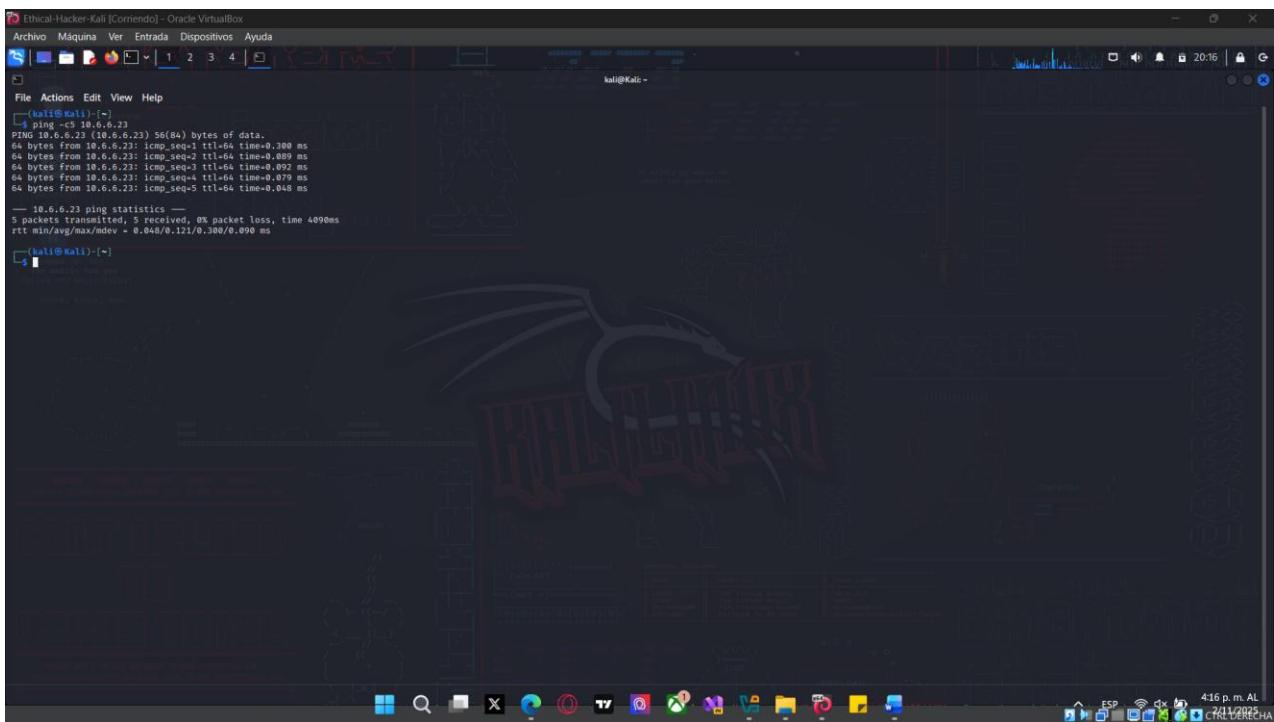
##### Paso 1: Inicie e inicie sesión en la máquina virtual Kali.

- 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**.

## Práctica de laboratorio: Análisis de vulnerabilidades con Kali Tools



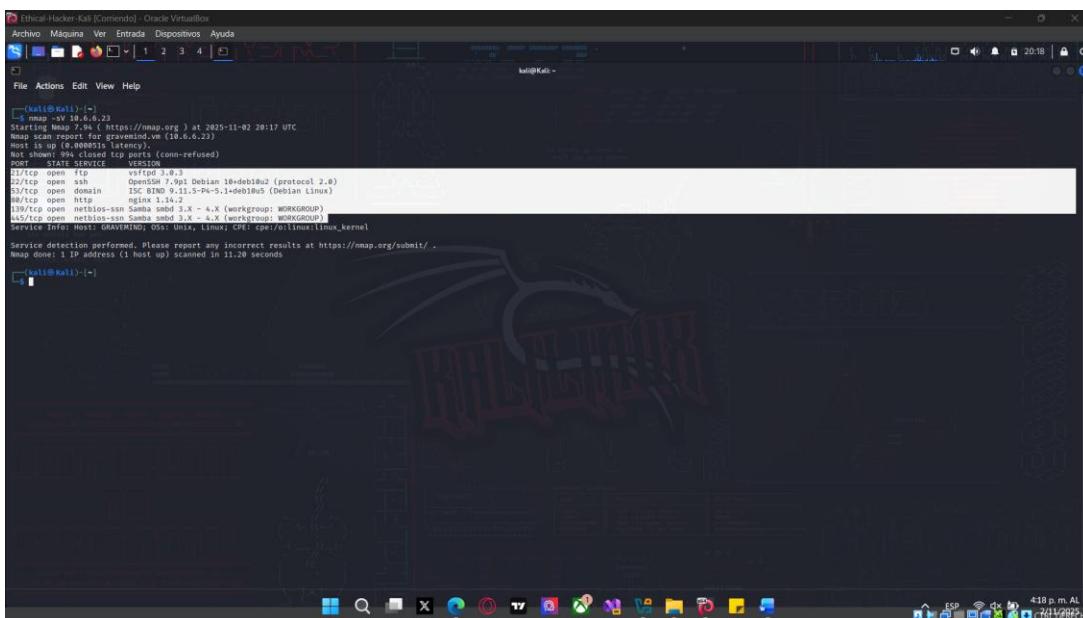
### Paso 2: Identifique puertos y servicios abiertos.

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

- 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?



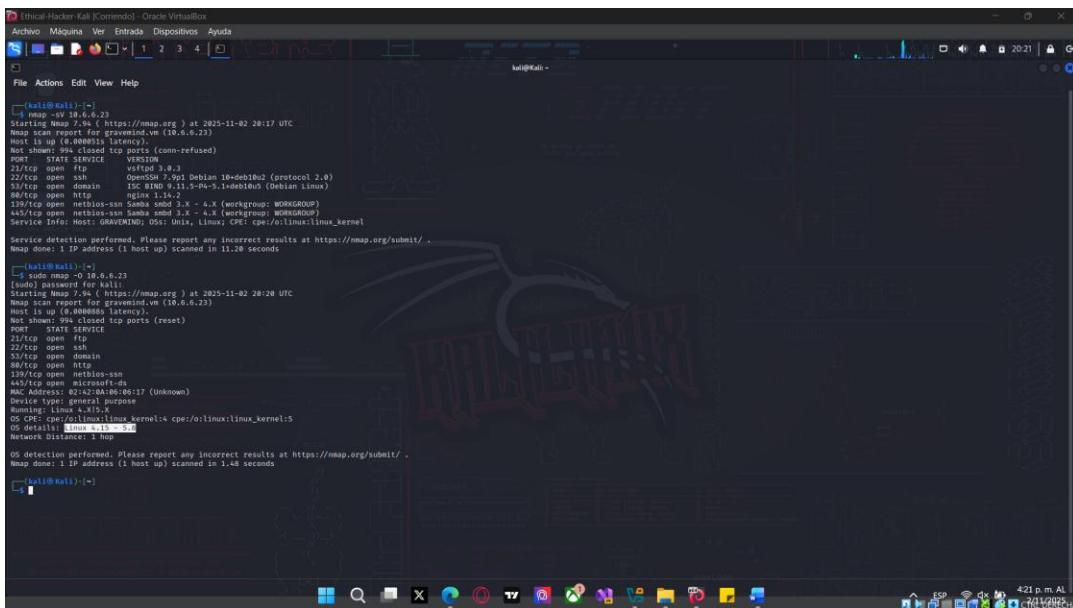
**21, 22, 53, 80, 139 y 445**

- 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



```
(kali㉿Kali)-[~]
$ nmap -sv 10.6.6.23
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-02 28:17 UTC
Nmap scan report for gravenind.vn (10.6.6.23)
Host is up (0.0000040s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh  OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
23/tcp    open  telnet
53/tcp    open  domain  ISC BIND 9.11.5-0+deb10u1 (Debian Linux)
80/tcp    open  http   nginx 1.14.1
139/tcp   open  netbios-ses 3.x - 4.x (workgroup: WORKGROUP)
445/tcp   open  netbios-smb 3.x - 4.x (workgroup: WORKGROUP)
Service Info: Host: GRAVENIND; OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap done: 1 IP address (1 host up) scanned in 11.20 seconds

(kali㉿Kali)-[~]
$ nmap -sv 10.6.6.23
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-02 28:28 UTC
Nmap scan report for gravenind.vn (10.6.6.23)
Host is up (0.000005s latency).
Not shown: 994 closed ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh  OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
23/tcp    open  telnet
53/tcp    open  domain  ISC BIND 9.11.5-0+deb10u1 (Debian Linux)
80/tcp    open  http   nginx 1.14.1
139/tcp   open  netbios-ses 3.x - 4.x (workgroup: WORKGROUP)
445/tcp   open  netbios-smb 3.x - 4.x (workgroup: WORKGROUP)
4455/tcp  open  microsoft-ds
Device: 02:24:00:00:00:17 (Unknown)
Running: Linux 4.15.0-102-generic
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 1.48 seconds
```

**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?

```

File Actions Edit View Help
2/tcp open  ftp vsftpd 3.0.3
| vulners
|_ CVE-2021-36587 7.5 https://vulners.com/cve/CVE-2021-36587
|_ CVE-2021-36518 7.4 https://vulners.com/cve/CVE-2021-36518
22/tcp open  ssh OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| vulners
|_ GnuPG 2.2.20 2020-05-10 2.2.20 https://vulners.com/openpgp/2.2.20
|_ PACKETSTORM:173661 9.8 https://vulners.com/packetstorm/PACKETSTORM:173661 *EXPLOIT*
|_ F9791893-AE8B-3930-B0C7-CF052530A8D9 9.8 https://vulners.com/githubexploit/F9791893-AE8B-3930-B0C7-CF052530A8D9 *EXPLOIT*
|_ B819BC0B-3E89-5611-9828-0804A2175B23 9.8 https://vulners.com/githubexploit/B819BC0B-3E89-5611-9828-0804A2175B23 *EXPLOIT*
|_ BFC0C5AB-3968-53F6-8226-E808579A623 9.8 https://vulners.com/githubexploit/BFC0C5AB-3968-53F6-8226-E808579A623 *EXPLOIT*
|_ 1A900000-0000-0000-0000-000000000000 9.8 https://vulners.com/githubexploit/1A900000-0000-0000-0000-000000000000 *EXPLOIT*
|_ 222779D0-6780-5C8F-9030-1EEAF049FF8 9.8 https://vulners.com/githubexploit/222779D0-6780-5C8F-9030-1EEAF049FF8 *EXPLOIT*
|_ 92238000-0000-0000-0000-000000000000 9.8 https://vulners.com/githubexploit/92238000-0000-0000-0000-000000000000 *EXPLOIT*
|_ 4F801800-F993-5CAF-B057-D7290018C1P 8.1 https://vulners.com/githubexploit/4F801800-F993-5CAF-B057-D7290018C1P *EXPLOIT*
|_ CVE-2019-16945 7.8 https://vulners.com/cve/CVE-2019-16945
|_ CVE-2019-16945 7.8 https://vulners.com/cve/CVE-2019-16945
|_ C9432FD-1FA5-5342-BEEF-80DA54EEFFEE 7.8 https://vulners.com/githubexploit/C9432FD-1FA5-5342-BEEF-80DA54EEFFEE *EXPLOIT*
|_ 7137040E-F683-5886-B603-351173626207 7.8 https://vulners.com/githubexploit/7137040E-F683-5886-B603-351173626207 *EXPLOIT*
|_ 23C597BE-7C95-5116-9E73-298AC4074422 7.8 https://vulners.com/githubexploit/23C597BE-7C95-5116-9E73-298AC4074422 *EXPLOIT*
|_ 182130BE-F683-5886-B603-351173626207 7.8 https://vulners.com/githubexploit/182130BE-F683-5886-B603-351173626207 *EXPLOIT*
|_ 59595000-0000-0000-0000-000000000000 7.8 https://vulners.com/githubexploit/59595000-0000-0000-0000-000000000000 *EXPLOIT*
|_ 1337DAY-ID-26576 7.5 https://vulners.com/zdt/1337DAY-ID-26576 *EXPLOIT*
|_ CVE-2021-41617 7.0 https://vulners.com/cve/CVE-2021-41617
|_ 28000000-0000-0000-0000-000000000000 7.0 https://vulners.com/githubexploit/28000000-0000-0000-0000-000000000000 *EXPLOIT*
|_ PACKETSTORM:187283 6.8 https://vulners.com/githubexploit/PACKETSTORM:187283 *EXPLOIT*
|_ FDB-ID:146516 6.8 https://vulners.com/exploit/FDB-ID:146516 *EXPLOIT*
|_ 10800000-0000-0000-0000-000000000000 6.8 https://vulners.com/exploit/10800000-0000-0000-0000-000000000000 *EXPLOIT*
|_ CVE-2025-26465 6.8 https://vulners.com/cve/CVE-2025-26465
|_ CVE-2019-6111 6.8 https://vulners.com/cve/CVE-2019-6111
|_ CVE-2019-6111 6.8 https://vulners.com/cve/CVE-2019-6111
|_ 90843280-491C-5445-BB96-32983FB2254 6.8 https://vulners.com/githubexploit/90843280-491C-5445-BB96-32983FB2254 *EXPLOIT*
|_ 857FCDC6-9A63-597E-AB4F-FAADAC04F80B 6.8 https://vulners.com/githubexploit/857FCDC6-9A63-597E-AB4F-FAADAC04F80B *EXPLOIT*
|_ 1337DAY-ID-22308 6.8 https://vulners.com/zdt/1337DAY-ID-22308 *EXPLOIT*
|_ 1337DAY-ID-32328 6.8 https://vulners.com/zdt/1337DAY-ID-32328 *EXPLOIT*
|_ 1337DAY-ID-32889 6.8 https://vulners.com/zdt/1337DAY-ID-32889 *EXPLOIT*
|_ D5000000-0000-0000-0000-000000000000 6.8 https://vulners.com/githubexploit/D5000000-0000-0000-0000-000000000000 *EXPLOIT*
|_ CVE-2023-51385 6.5 https://vulners.com/cve/CVE-2023-51385
|_ C7A0B446-24B8-57B7-B375-9C63F475B82 6.5 https://vulners.com/githubexploit/C7A0B446-24B8-57B7-B375-9C63F475B82 *EXPLOIT*
|_ A8500000-0000-0000-0000-000000000000 6.5 https://vulners.com/exploit/A8500000-0000-0000-0000-000000000000 *EXPLOIT*
|_ 65815AA1-2A00-51C1-9499-69EBA16917C 6.5 https://vulners.com/githubexploit/65815AA1-2A00-51C1-9499-69EBA16917C *EXPLOIT*
|_ 53254906-32A8-59C6-B0EF-9C81B052732 6.5 https://vulners.com/gitre/53254906-32A8-59C6-B0EF-9C81B052732 *EXPLOIT*
|_ 53254906-32A8-59C6-B0EF-9C81B052732 6.5 https://vulners.com/githubexploit/53254906-32A8-59C6-B0EF-9C81B052732 *EXPLOIT*
|_ CVE-2023-48795 5.9 https://vulners.com/cve/CVE-2023-48795
|_ CVE-2028-54145 5.4 https://vulners.com/cve/CVE-2028-54145
|_ CVE-2028-54145 5.4 https://vulners.com/cve/CVE-2028-54145
|_ CNVD-2021-75077 5.9 https://vulners.com/cnv/CNVD-2021-75077
|_ 60744645-6847-557A-8469-10096A20HFB 5.9 https://vulners.com/githubexploit/60744645-6847-557A-8469-10096A20HFB *EXPLOIT*
|_ EXPLOITPACK:5338EAE20DE345BF906000097F9E97 5.8 https://vulners.com/exploit/EXPLOITPACK:5338EAE20DE345BF906000097F9E97 *EXPLOIT*
|_ CVE-2018-20685 5.3 https://vulners.com/cve/CVE-2018-20685
|_ CVE-2016-20612 5.3 https://vulners.com/cve/CVE-2016-20612

```

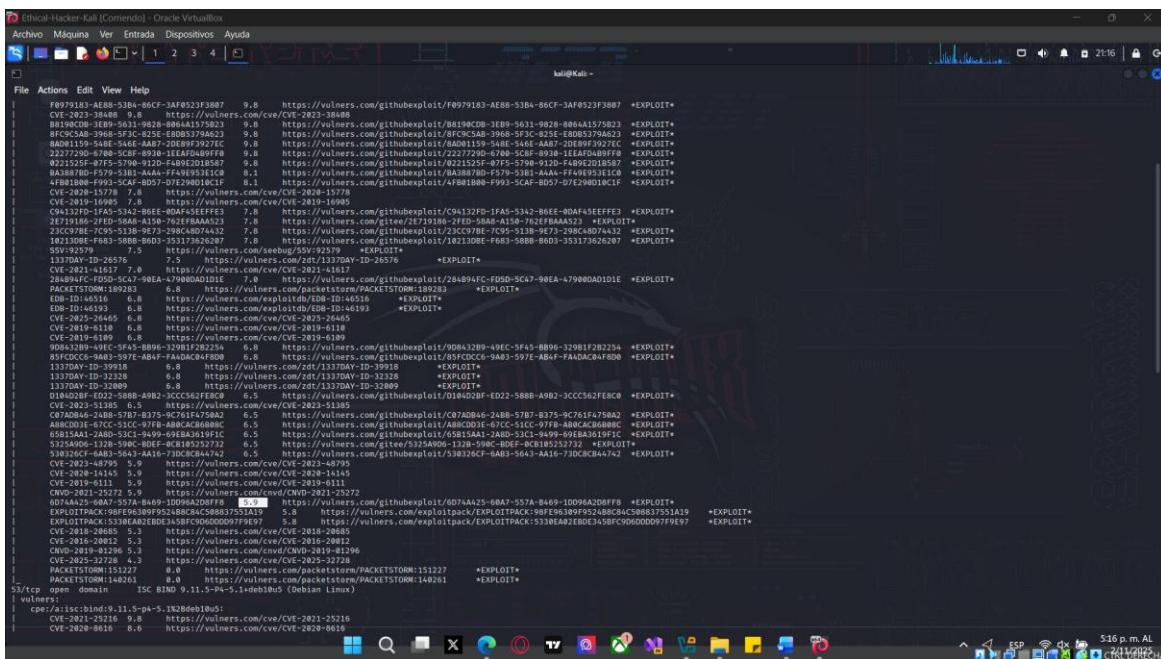
**CVE-2019-6111**

**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?

## Práctica de laboratorio: Análisis de vulnerabilidades con Kali Tools



5,9 Mediano

**MOSTRAR CAPTURA**