UNIVERSIDAD AUTONOMA DE CHIAPAS

Análisis de Vulnerabilidades

Alumno: Tomás Álvarez Gómez

Actividad: 1.6_Pratica2

Tarea: Practica de Escaneo de puertos

Maestro: Luis Gutiérrez Alfaro

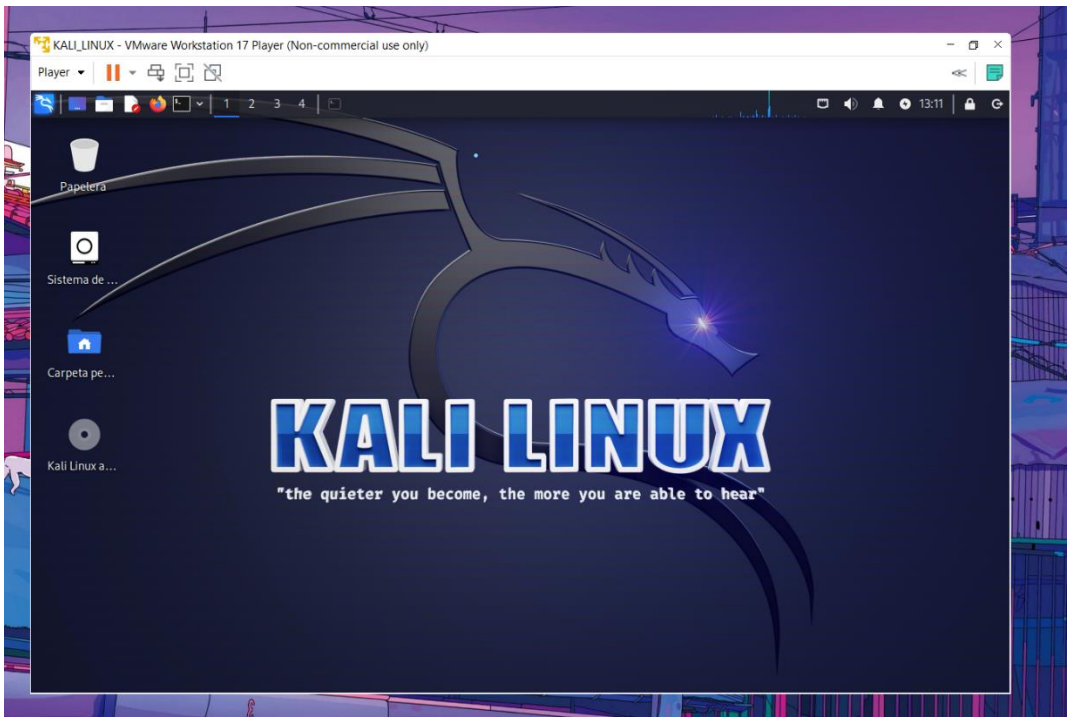
Grupo: 7 M

Fecha: 22/08/23-Tuxtla Gutiérrez Chipas

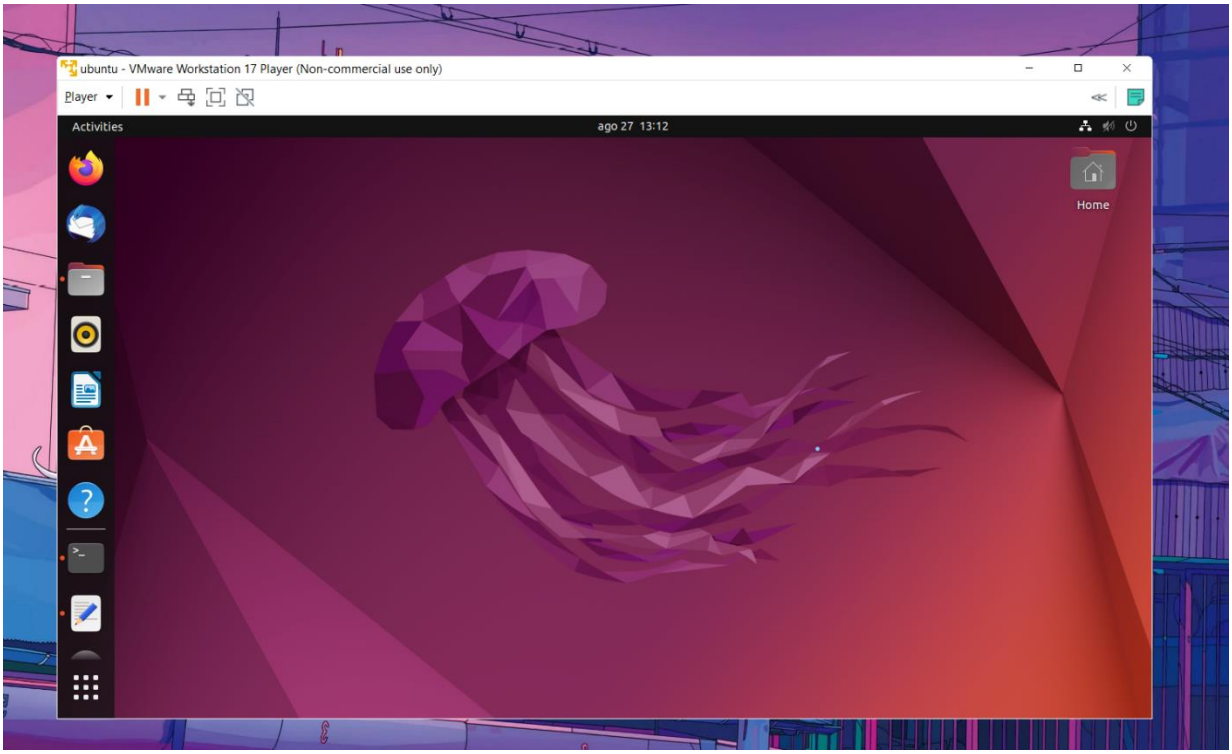
Matricula: A200369

INSTALACIÒN DE MAQUINAS VIRTUALES

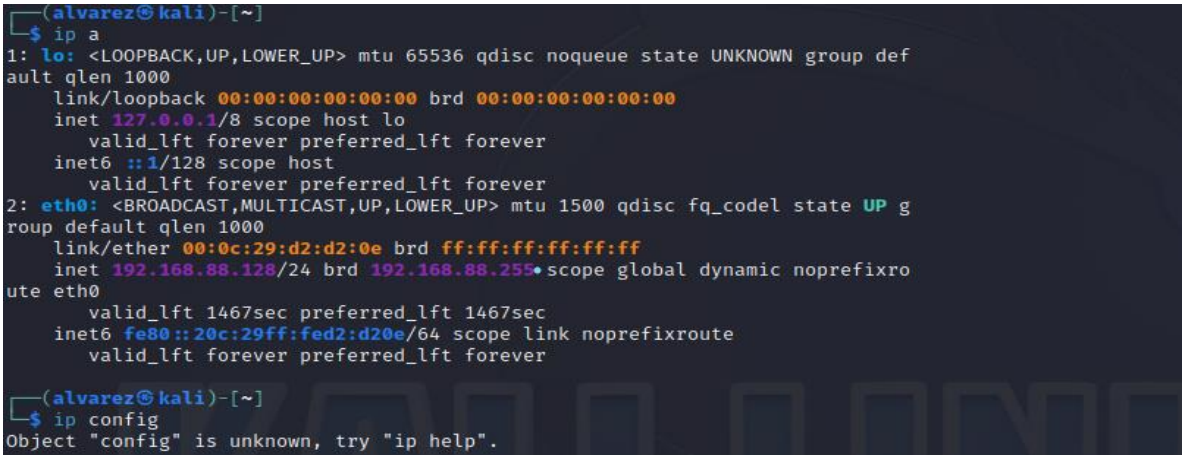
Kali Linux



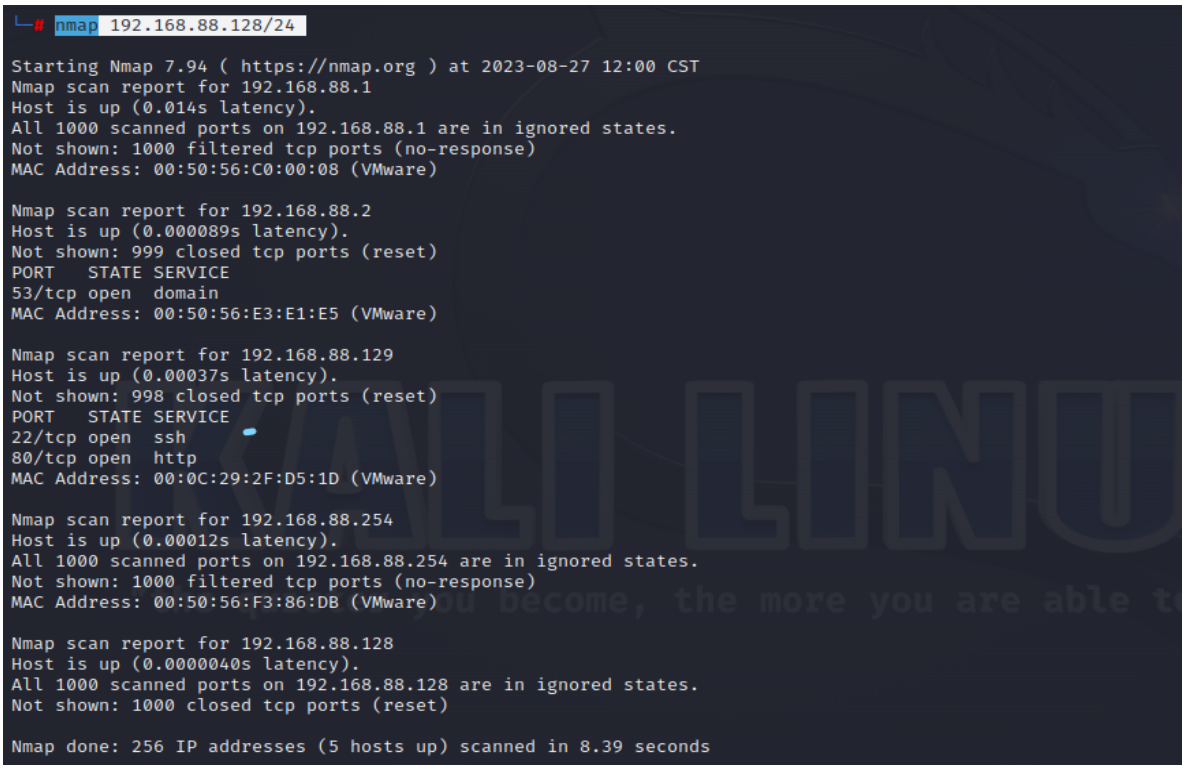
Ubuntu



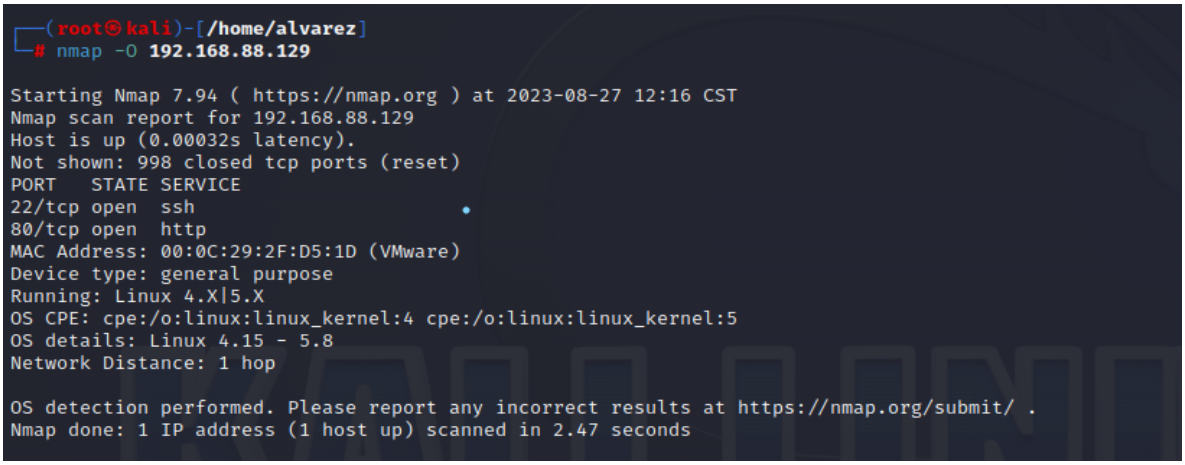
- Con el comando ip a obtenemos la ip de KALI



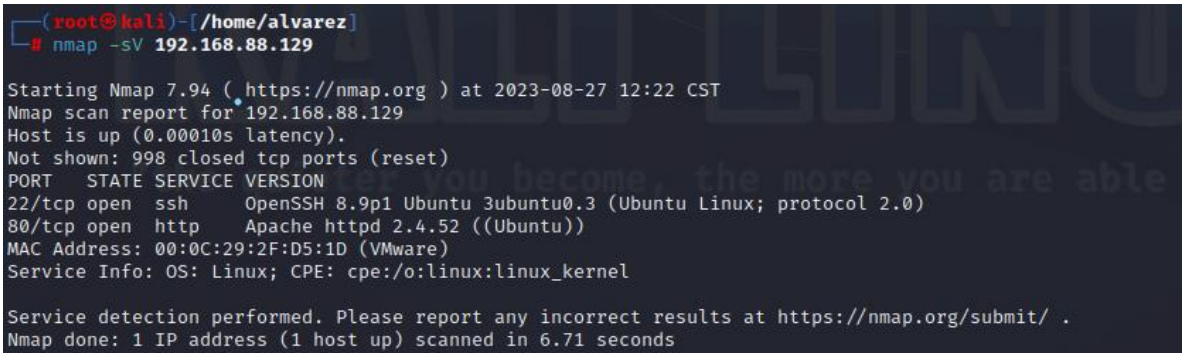
- Se aplica el siguiente comando para escanear el host (nmap 192.168.88.128/24). Dentro de este escaneo identificamos la ip del servidor web.



- nmap -O 192.168.88.192-se escanea la ip y se detecta el sistema operativo

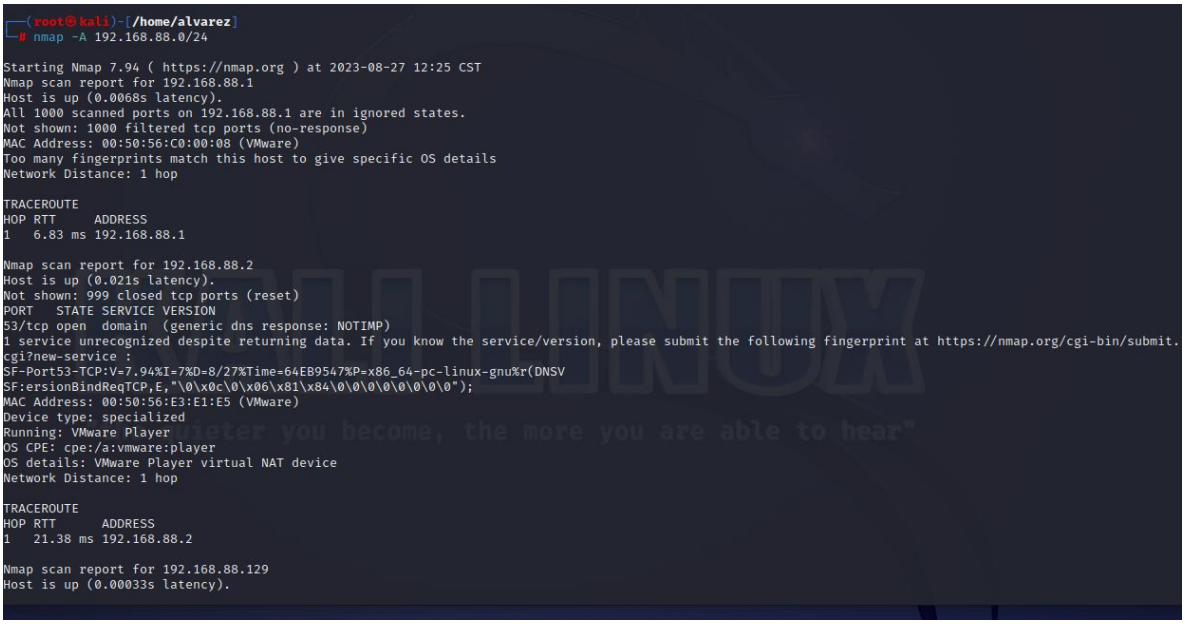


- Nmap -sV 192.168.88.129 se escanea la ip para saber los servicios que se encuentran corriendo en ella.

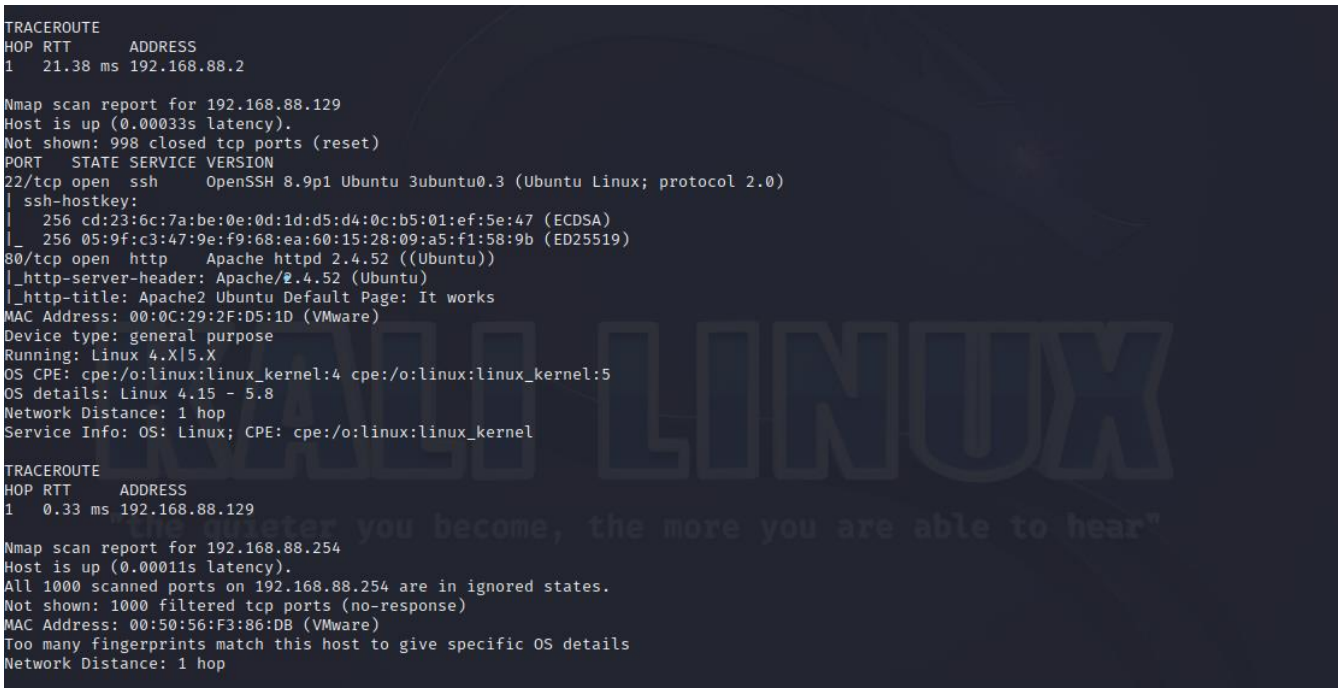


```
┌──(root㉿kali)-[/home/alvarez]
└─# nmap -sV 192.168.88.129

Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-27 12:22 CST
Nmap scan report for 192.168.88.129
Host is up (0.00010s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
MAC Address: 00:0C:29:2F:D5:1D (VMware)
Service Info: OS: 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 6.71 seconds
```

- nmap -A 192.168.88.1 escaneamos la ip para obtener mas información del OS y de los servicios



```
┌──(root㉿kali)-[/home/alvarez]
└─# nmap -A 192.168.88.0/24

Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-27 12:25 CST
Nmap scan report for 192.168.88.1
Host is up (0.0068s latency).
All 1000 scanned ports on 192.168.88.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:C0:00:08 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   6.83 ms 192.168.88.1

Nmap scan report for 192.168.88.2
Host is up (0.021s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
53/tcp open  domain  (generic dns response: NOTIMP)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.
cgi?new-service :
SF-Port53-TCP:V=7.94%I=7%D=8/27%Time=64EB9547%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,E,"\0\x0c\0\x06\x81\x84\0\0\0\0\0\0\0\0");
MAC Address: 00:50:56:E3:E1:E5 (VMware)
Device type: specialized
Running: VMware Player
OS CPE: cpe:/a:vmware:player
OS details: VMware Player virtual NAT device
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   21.38 ms 192.168.88.2

Nmap scan report for 192.168.88.129
Host is up (0.00033s latency).
```



```
TRACEROUTE
HOP RTT      ADDRESS
1   21.38 ms 192.168.88.2

Nmap scan report for 192.168.88.129
Host is up (0.00033s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 cd:23:6c:7a:be:0e:0d:1d:d5:d4:0c:b5:01:ef:5e:47 (ECDSA)
|_  256 05:9f:c3:47:9e:f9:68:ea:60:15:28:09:a5:f1:58:9b (ED25519)
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 00:0C:29:2F:D5:1D (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.33 ms 192.168.88.129

Nmap scan report for 192.168.88.254
Host is up (0.00011s latency).
All 1000 scanned ports on 192.168.88.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F3:86:DB (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT     ADDRESS
1   0.10 ms 192.168.88.254

Nmap scan report for 192.168.88.128
Host is up (0.000047s latency).
All 1000 scanned ports on 192.168.88.128 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 37.88 seconds
```

- nmap -v -p139,445 --script=smb-vuln-*.nse --script-args=unsafe=1 192.168.88.129 escaneo a Ubuntu de puertos cerrados

```
┌──(root㉿kali)-[/home/alvarez]
└─# nmap -v -p139,445 --script=smb-vuln-*.nse --script-args=unsafe=1 192.168.88.129
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-27 13:02 CST
NSE: Loaded 11 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 13:02
Completed NSE at 13:02, 0.00s elapsed
Initiating ARP Ping Scan at 13:02
Scanning 192.168.88.129 [1 port]
Completed ARP Ping Scan at 13:02, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:02
Completed Parallel DNS resolution of 1 host. at 13:02, 0.08s elapsed
Initiating SYN Stealth Scan at 13:02
Scanning 192.168.88.129 [2 ports]
Completed SYN Stealth Scan at 13:02, 0.01s elapsed (2 total ports)
NSE: Script scanning 192.168.88.129.
Initiating NSE at 13:02
Completed NSE at 13:02, 0.00s elapsed
Nmap scan report for 192.168.88.129
Host is up (0.00029s latency).

PORT    STATE  SERVICE
139/tcp closed netbios-ssn
445/tcp closed microsoft-ds
MAC Address: 00:0C:29:2F:D5:1D (VMware)

NSE: Script Post-scanning.
Initiating NSE at 13:02
Completed NSE at 13:02, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
           Raw packets sent: 3 (116B) | Rcvd: 3 (108B)
```

- Escaneo de puertos abiertos

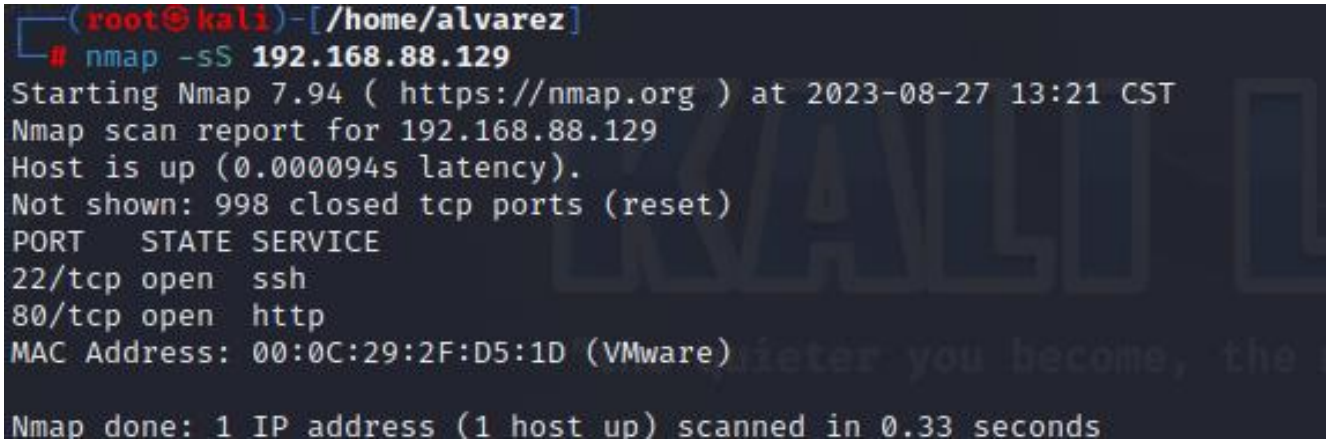
```
┌──(root㉿kali)-[/home/alvarez]
└─# nmap -v -p139,445 --script=smb-vuln-*.nse --script-args=unsafe=1 192.168.88.129
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-27 12:45 CST
NSE: Loaded 11 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 12:45
Completed NSE at 12:45, 0.00s elapsed
Initiating ARP Ping Scan at 12:45
Scanning 192.168.88.129 [1 port]
Completed ARP Ping Scan at 12:45, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:45
Completed Parallel DNS resolution of 1 host. at 12:45, 0.12s elapsed
Initiating SYN Stealth Scan at 12:45
Scanning 192.168.88.129 [2 ports]
Completed SYN Stealth Scan at 12:45, 0.01s elapsed (2 total ports)
NSE: Script scanning 192.168.88.129.
Initiating NSE at 12:45
Completed NSE at 12:45, 0.00s elapsed
Nmap scan report for 192.168.88.129
Host is up (0.00034s latency).

PORT    STATE  SERVICE
139/tcp closed netbios-ssn
445/tcp closed microsoft-ds
MAC Address: 00:0C:29:2F:D5:1D (VMware)

NSE: Script Post-scanning.
Initiating NSE at 12:45
Completed NSE at 12:45, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
           Raw packets sent: 3 (116B) | Rcvd: 3 (108B)
```

- nmap -p445 -Pn --script smb-vuln-ms17-010 192.168.88.2

```
┌──(root㉿kali)-[/home/alvarez]
└─# nmap -p445 -Pn --script smb-vuln-ms17-010 192.168.88.2
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-27 13:07 CST
Nmap scan report for 192.168.88.2
Host is up (0.00020s latency).

PORT    STATE  SERVICE
445/tcp closed microsoft-ds
MAC Address: 00:50:56:E3:E1:E5 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
```

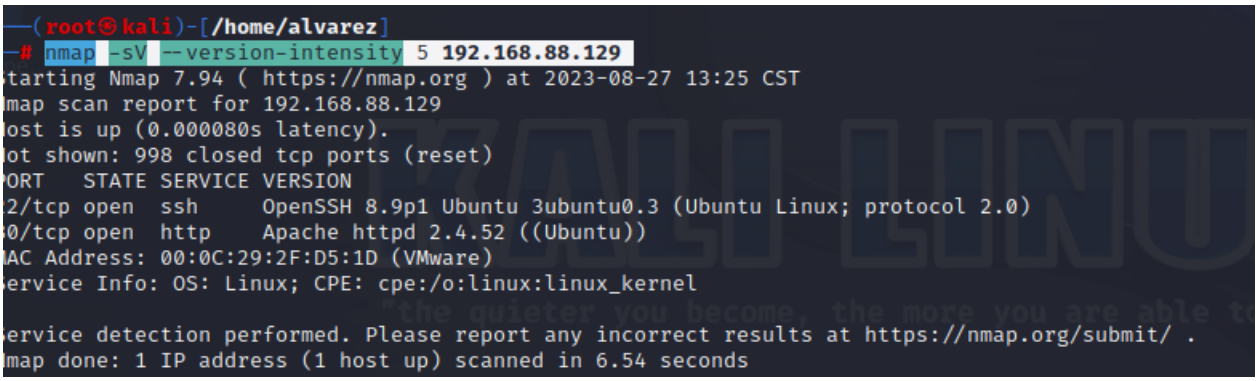
ANEXO DE 10 COMANDOS

1. Nmap -sS este comando determina si el puerto objetivo esta escuchando.



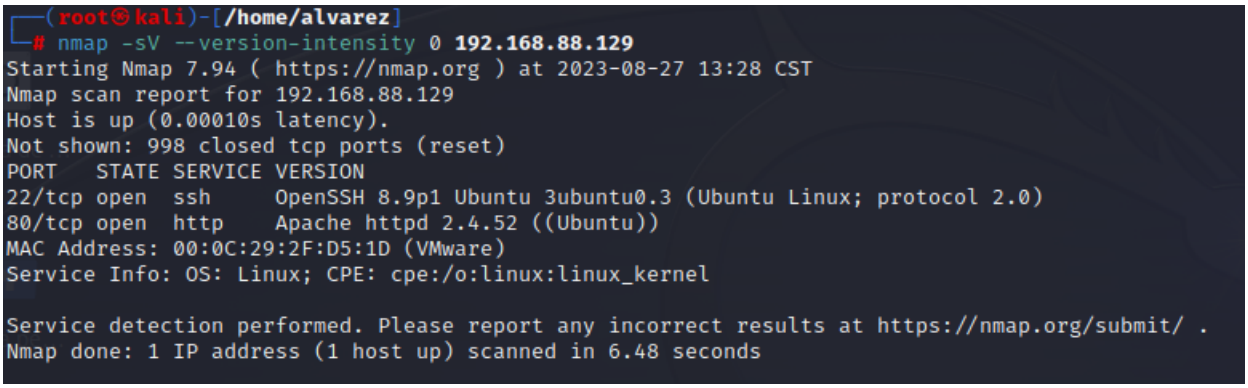
2. nmap -sV --version-intensity 5 192.168.88.129

este comando es útil para detectar servicios que no se están ejecutando en sus puertos definidos, sin embargo este escaneo deja màs trazas en el sistema y en logs de firewalls



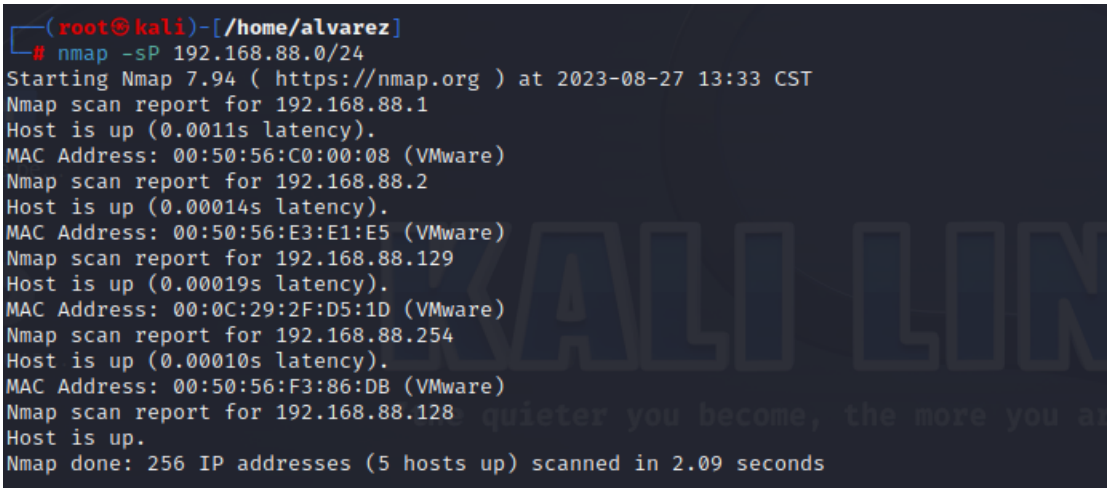
3. map -sV --version-intensity 0 192.168.88.129

Un escaneo ligero, es mucho menos ruidoso que el anterior y permite obtener datos sin llamar la atención.



4. nmap -sP 192.168.88.0/24

comando para descubrir equipos, pero sin mucha información sobre ellos.

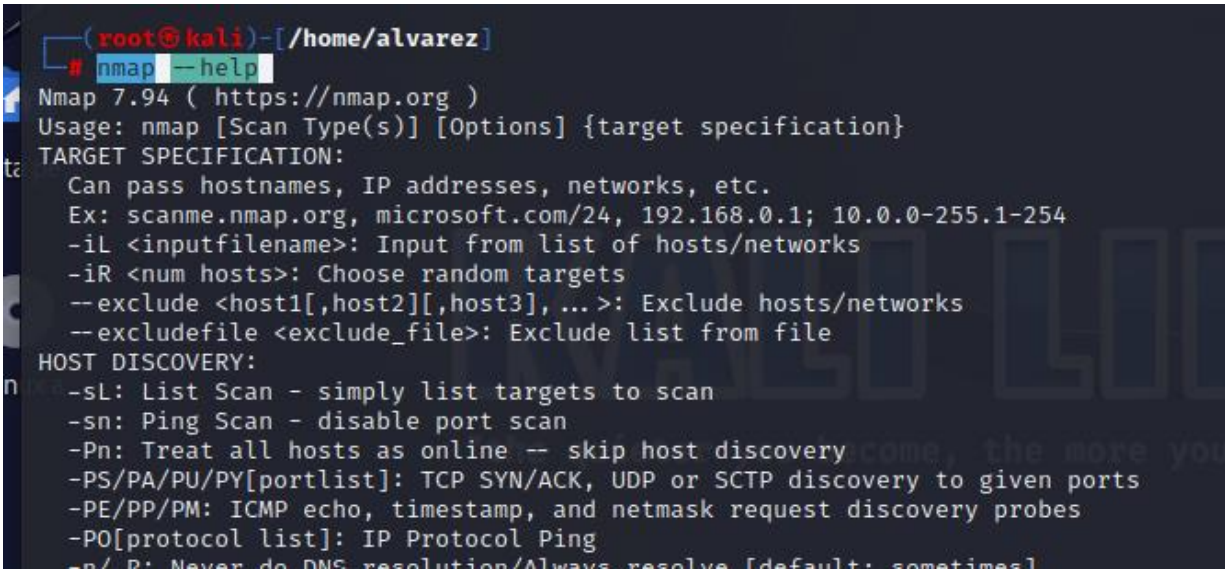


5. nmap -sS -O 192.168.88.0/24

este comando es para escanear una red completa de manera sigilosa con detección del sistema operativo.

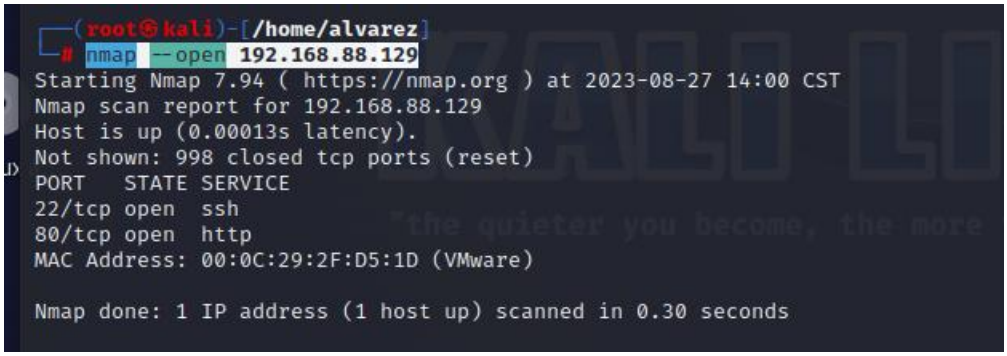
6. nmap –help

con este comando podemos consultar todas las opciones disponibles



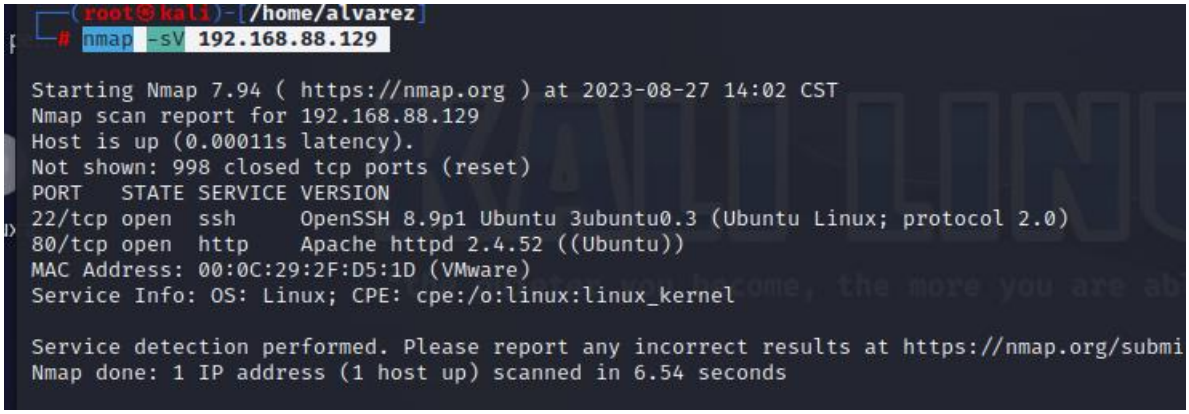
7. nmap --open 192.168.88.129

comando para mostrar solo puertos abiertos



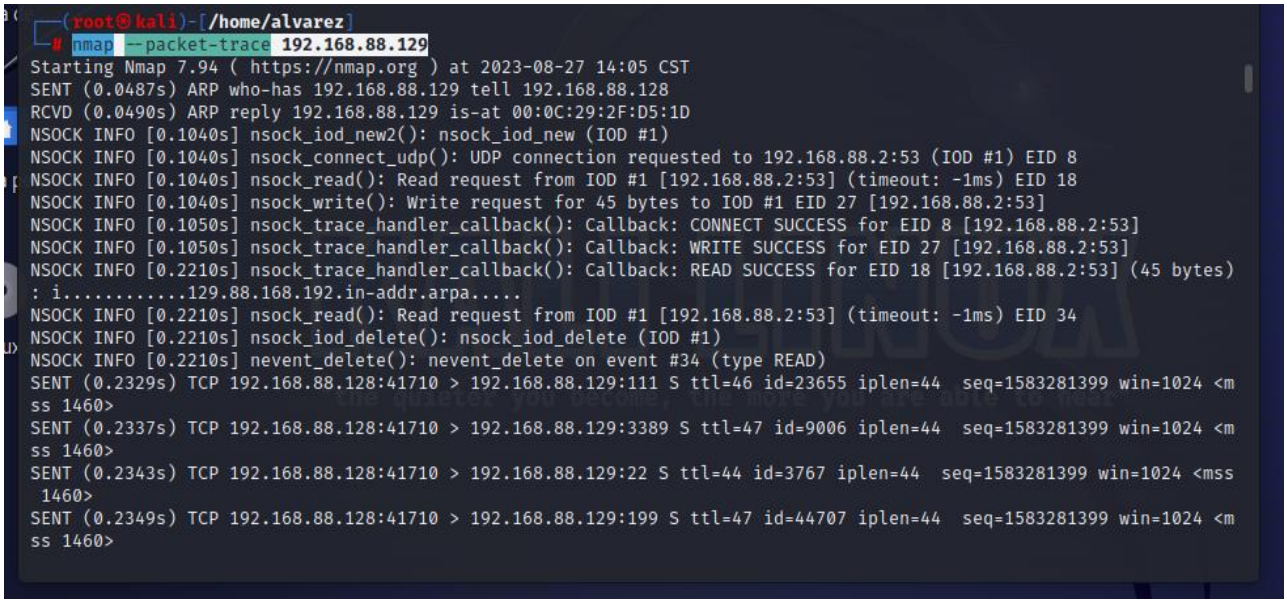
8. nmap -sV 192.168.88.129

comando para detectar las versiones de los servicios remotos



9. nmap --packet-trace 192.168.88.129

este comando nos muestra los paquetes enviados y recibidos



10. nmap -F -O 192.168.88.0/24 | grep "Running: " > /tmp/os; echo "$(cat /tmp/os | grep Linux | wc -l) Linux device(s)"; echo "$(cat /tmp/os | grep Windows | wc -l) Window(s) devices"

comando para ver cuántos dispositivos Linux y Windows están conectados a la red