



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

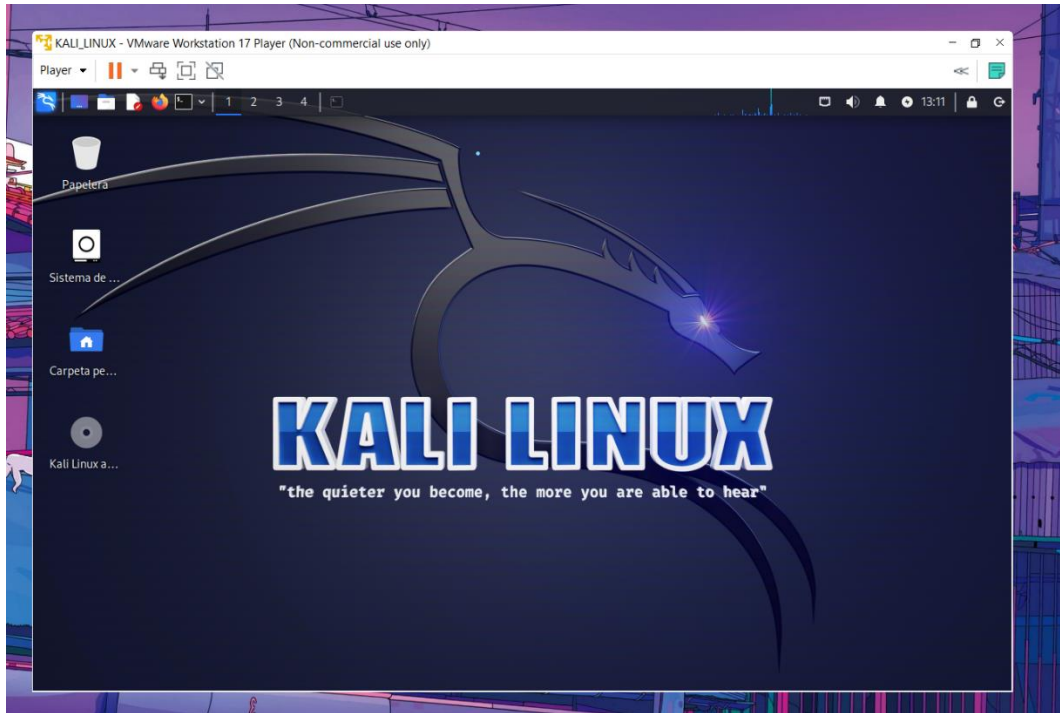
Grupo: 7 M

Fecha: 22/08/23-Tuxtla Gutiérrez Chipas

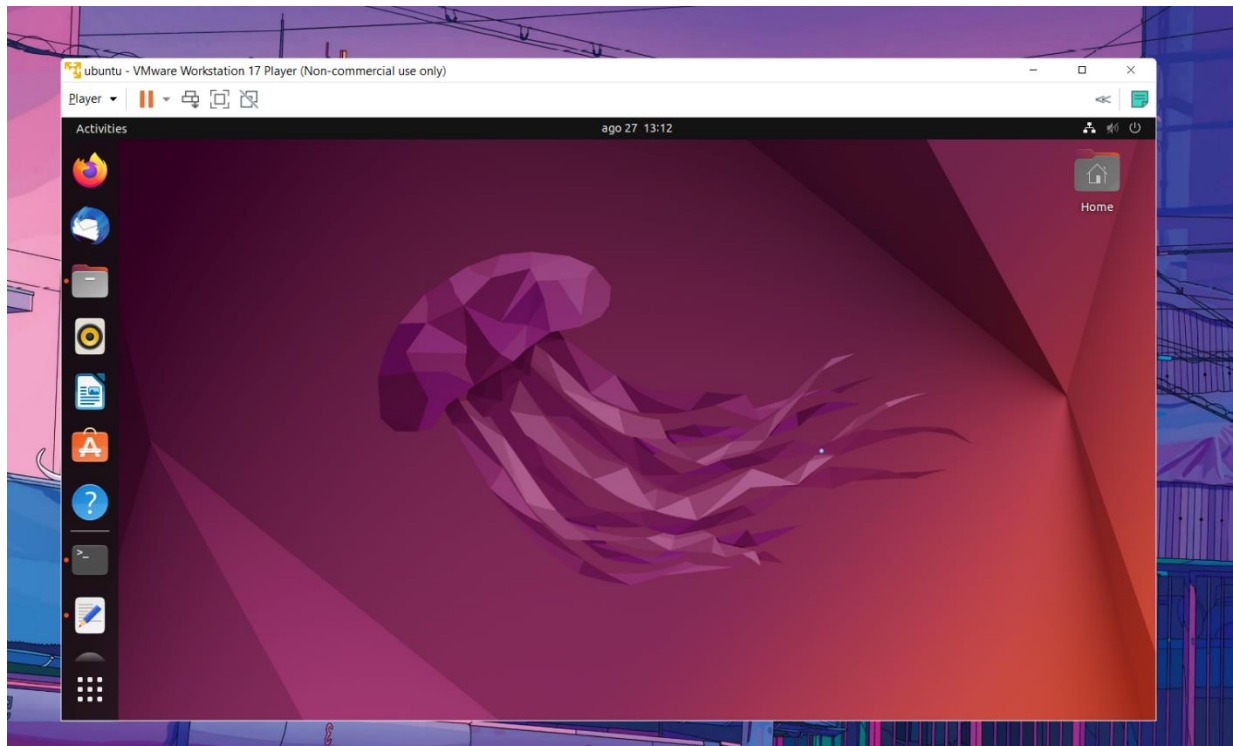
Matricula: A200369

INSTALACIÓN DE MAQUINAS VIRTUALES

Kali Linux



Ubuntu



- Con el comando ip a obtenemos la ip de KALI

```
(alvarez@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 00:0c:29:d2:d2:0e brd ff:ff:ff:ff:ff:ff
    inet 192.168.88.128/24 brd 192.168.88.255 scope global dynamic noprefixro
ute eth0
        valid_lft 1467sec preferred_lft 1467sec
    inet6 fe80::20c:29ff:fed2:d20e/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(alvarez@kali)-[~]
$ ip config
Object "config" is unknown, try "ip help".
```

- 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 192.168.88.128/24

Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-27 12:00 CST
Nmap scan report for 192.168.88.1
Host is up (0.014s 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)

Nmap scan report for 192.168.88.2
Host is up (0.000089s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 00:50:56:E3:E1:E5 (VMware)

Nmap scan report for 192.168.88.129
Host is up (0.00037s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:0C:29:2F:D5:1D (VMware)

Nmap scan report for 192.168.88.254
Host is up (0.00012s 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)

Nmap scan report for 192.168.88.128
Host is up (0.000040s latency).
All 1000 scanned ports on 192.168.88.128 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (5 hosts up) scanned in 8.39 seconds
```

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

```
(root@kali)-[/home/alvarez]
# nmap -O 192.168.88.129

Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-27 12:16 CST
Nmap scan report for 192.168.88.129
Host is up (0.00032s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.47 seconds
```

- 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=7.94XI=7%0=8/27%Time=64EB9547%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,E,"0x0c0x06x81x840000000000");
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-* --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

```
Nmap done: 1 IP address (0 hosts up) scanned in 1.94 seconds

(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.

```
(root@kali)-[/home/alvarez]
# nmap -sS 192.168.88.129
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-27 13:21 CST
Nmap scan report for 192.168.88.129
Host is up (0.000094s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:0C:29:2F:D5:1D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

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 más trazas en el sistema y en logs de firewalls

```
(root@kali)-[/home/alvarez]
# nmap -sV --version-intensity 5 192.168.88.129
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-27 13:25 CST
Nmap scan report for 192.168.88.129
Host is up (0.000080s 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 6.54 seconds
```

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.

```
(root@kali)-[/home/alvarez]
# nmap -sV --version-intensity 0 192.168.88.129
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-27 13:28 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 6.48 seconds
```

4. nmap -sP 192.168.88.0/24

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

```
(root@kali)-[/home/alvarez]
# nmap -sP 192.168.88.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-27 13:33 CST
Nmap scan report for 192.168.88.1
Host is up (0.0011s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.88.2
Host is up (0.00014s latency).
MAC Address: 00:50:56:E3:E1:E5 (VMware)
Nmap scan report for 192.168.88.129
Host is up (0.00019s latency).
MAC Address: 00:0C:29:2F:D5:1D (VMware)
Nmap scan report for 192.168.88.254
Host is up (0.00010s latency).
MAC Address: 00:50:56:F3:86:DB (VMware)
Nmap scan report for 192.168.88.128
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.09 seconds
```

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.

```
(root@kali)-[/home/alvarez]
# nmap -sS -O 192.168.88.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-27 13:39 CST
Nmap scan report for 192.168.88.1
Host is up (0.0051s 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

Nmap scan report for 192.168.88.2
Host is up (0.025s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 00:50:56:E3:E1:E5 (VMware)
Aggressive OS guesses: VMware Player virtual NAT device (98%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 20
4.37) (91%), Microsoft Windows XP SP3 (91%), Actiontec MI424WR-GEN3I WAP (91%), Linux 3.2 (90%), DVTel DVT-9540DW network
NAS device (88%), Linux 4.4 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 192.168.88.129
Host is up (0.00037s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
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

Nmap scan report for 192.168.88.254
Host is up (0.00013s 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
```


6. nmap -help

con este comando podemos consultar todas las opciones disponibles

```
(root@kali)-[/home/alvarez]
# nmap --help
Nmap 7.94 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3], ...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sl: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-P: Never do DNS resolution/Always resolve [default: sometimes]
```

7. nmap --open 192.168.88.129

comando para mostrar solo puertos abiertos

```
(root@kali)-[/home/alvarez]
# nmap --open 192.168.88.129
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-27 14:00 CST
Nmap scan report for 192.168.88.129
Host is up (0.00013s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:0C:29:2F:D5:1D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
```

8. nmap -sV 192.168.88.129

comando para detectar las versiones de los servicios remotos

```
(root@kali)-[/home/alvarez]
# nmap -sV 192.168.88.129
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-27 14:02 CST
Nmap scan report for 192.168.88.129
Host is up (0.00011s 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/submi
Nmap done: 1 IP address (1 host up) scanned in 6.54 seconds
```

9. nmap --packet-trace 192.168.88.129

este comando nos muestra los paquetes enviados y recibidos

```
(root@kali)-[/home/alvarez]
# nmap --packet-trace 192.168.88.129
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-27 14:05 CST
SENT (0.0487s) ARP who-has 192.168.88.129 tell 192.168.88.128
RCVD (0.0490s) ARP reply 192.168.88.129 is-at 00:0C:29:2F:D5:1D
NSOCK INFO [0.1040s] nsock_ioc_new2(): nsock_ioc_new (IOD #1)
NSOCK INFO [0.1040s] nsock_connect_udp(): UDP connection requested to 192.168.88.2:53 (IOD #1) EID 8
NSOCK INFO [0.1040s] nsock_read(): Read request from IOD #1 [192.168.88.2:53] (timeout: -1ms) EID 18
NSOCK INFO [0.1040s] nsock_write(): Write request for 45 bytes to IOD #1 EID 27 [192.168.88.2:53]
NSOCK INFO [0.1050s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [192.168.88.2:53]
NSOCK INFO [0.1050s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 27 [192.168.88.2:53]
NSOCK INFO [0.2210s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 18 [192.168.88.2:53] (45 bytes)
: i.....129.88.168.192.in-addr.arpa.....
NSOCK INFO [0.2210s] nsock_read(): Read request from IOD #1 [192.168.88.2:53] (timeout: -1ms) EID 34
NSOCK INFO [0.2210s] nsock_ioc_delete(): nsock_ioc_delete (IOD #1)
NSOCK INFO [0.2210s] nevent_delete(): nevent_delete on event #34 (type READ)
SENT (0.2329s) TCP 192.168.88.128:41710 > 192.168.88.129:111 S ttl=46 id=23655 iplen=44 seq=1583281399 win=1024 <mss 1460>
SENT (0.2337s) TCP 192.168.88.128:41710 > 192.168.88.129:3389 S ttl=47 id=9006 iplen=44 seq=1583281399 win=1024 <mss 1460>
SENT (0.2343s) TCP 192.168.88.128:41710 > 192.168.88.129:22 S ttl=44 id=3767 iplen=44 seq=1583281399 win=1024 <mss 1460>
SENT (0.2349s) TCP 192.168.88.128:41710 > 192.168.88.129:199 S ttl=47 id=44707 iplen=44 seq=1583281399 win=1024 <mss 1460>
```

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

```
(root@kali)-[/home/alvarez]
# 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"
1 Linux device(s)
0 Window(s) devices
```