

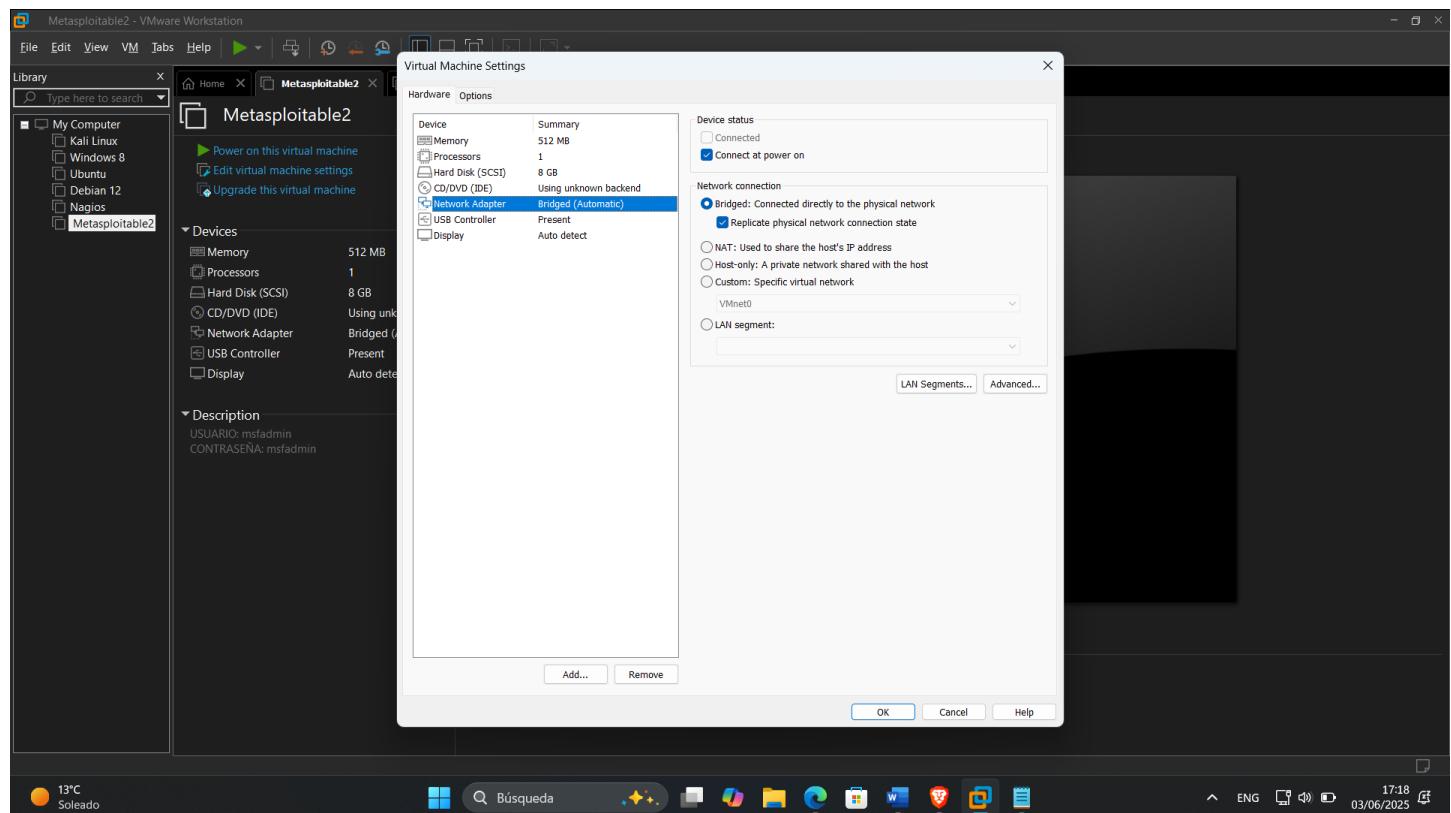
Laboratorio N°11

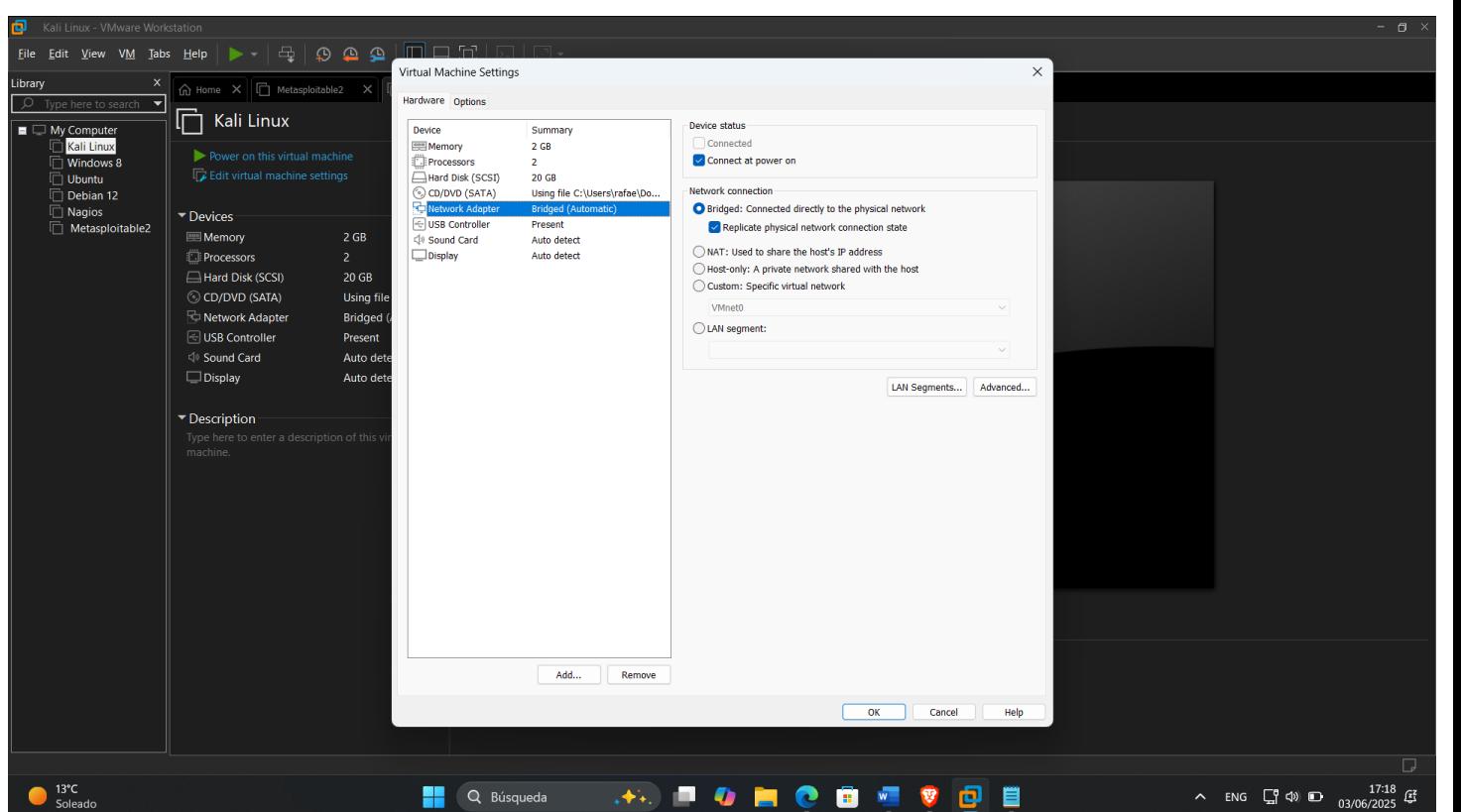
Nombre: Rafael Antonio Patricio Ayllón

CI: 10473854

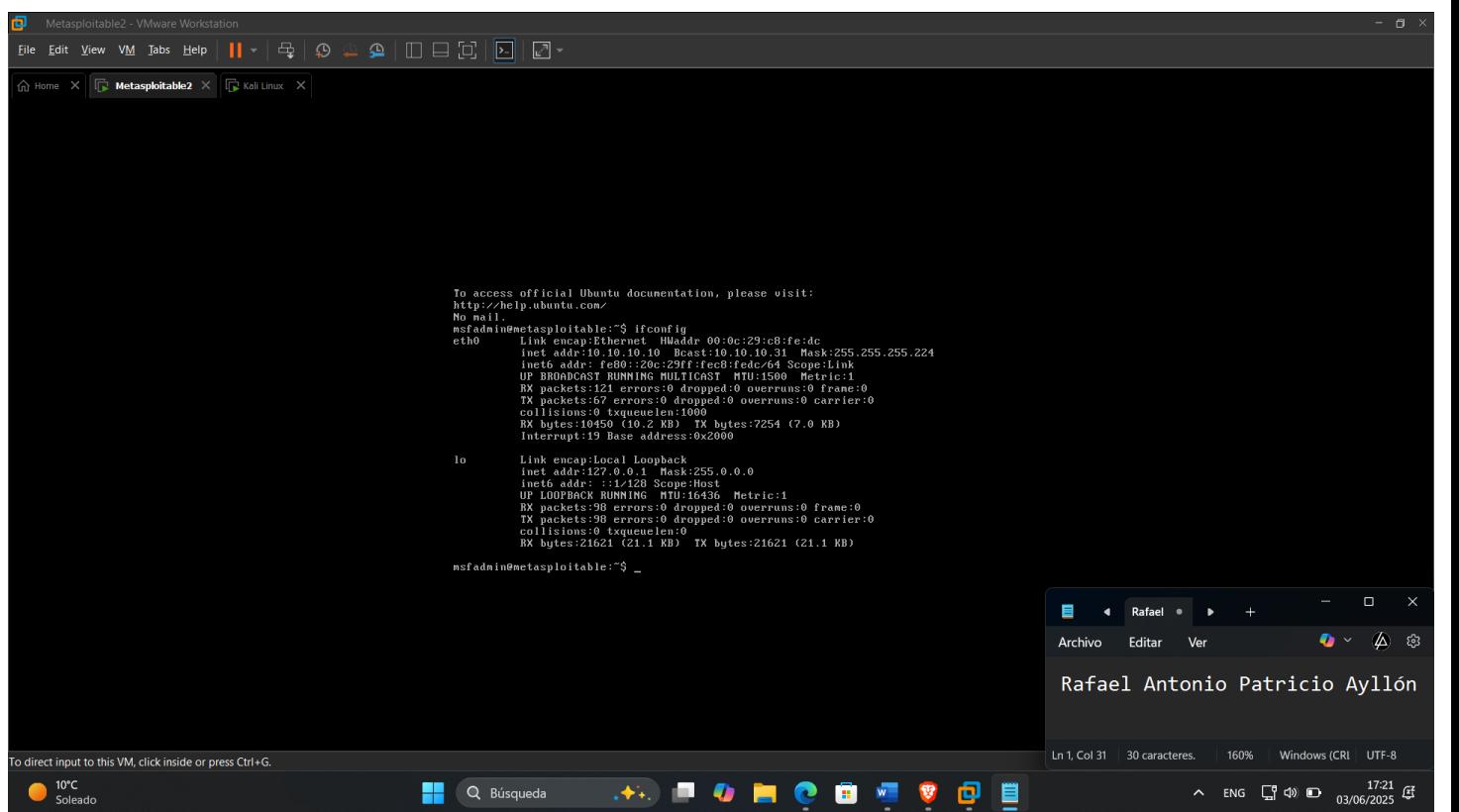
RU: 108771

Se recomienda que el adaptador de red este en el modo "Bridged" como muestra la imagen si es que se está configurando por primera vez la máquina virtual. Si esta utilizando otro modo de tarjeta, verifique que exista conectividad entre Kali y metasploitable2 antes de realizar la práctica.





Inicialmente debemos asegurarnos que ambas máquinas se encuentren en el mismo segmento de red. (Utilice las direcciones IP con las que está configurado su entorno de laboratorio).



```
[root@kali] ~]
# ifconfig
br-a3a8d6f0a26ac: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.18.0.1 netmask 255.255.0.0 broadcast 172.18.255.255
        ether 02:42:c8:09:47:99 txqueuelen 0 (Ethernet)
            RX packets 0 bytes 0 (0.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 0 bytes 0 (0.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
dockeroe: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
        ether 02:42:c0:d0:42:1c txqueuelen 0 (Ethernet)
            RX packets 0 bytes 0 (0.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 0 bytes 0 (0.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.10.1 netmask 255.255.255.252 broadcast 10.10.10.3
        inet6 fe80::2c8:9bf1%4: prefixlen 64 scooped 0x20<link>
            ether 02:42:c8:09:47:99 txqueuelen 1000 (Ethernet)
            RX packets 137 bytes 9708 (9.4 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 35 bytes 3948 (3.8 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        loop txqueuelen 1000 (Local Loopback)
            RX packets 8 bytes 480 (480.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 8 bytes 480 (480.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@kali] ~]
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

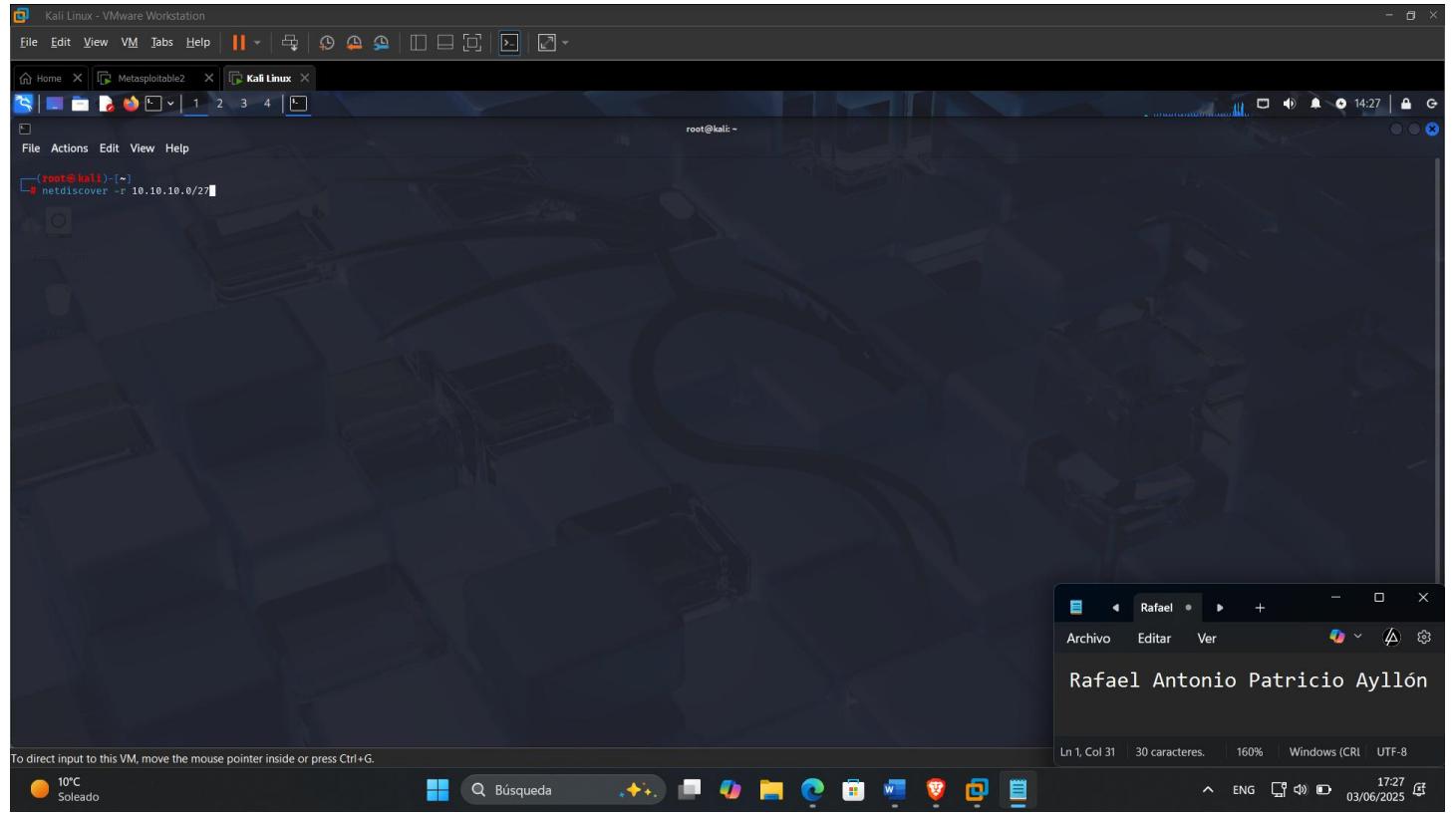
Nos aseguramos que exista conectividad desde la máquina Kali hacia la metasploitable:

```
[root@kali] ~]
# ping 10.10.10.10 (10.10.10.10) 56(84) bytes of data.
64 bytes from 10.10.10.10: icmp_seq=1 ttl=64 time=2.11 ms
64 bytes from 10.10.10.10: icmp_seq=2 ttl=64 time=0.894 ms
64 bytes from 10.10.10.10: icmp_seq=3 ttl=64 time=0.842 ms
64 bytes from 10.10.10.10: icmp_seq=4 ttl=64 time=1.08 ms
^C
--- 10.10.10.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 0.842/1.231/2.112/0.15 ms

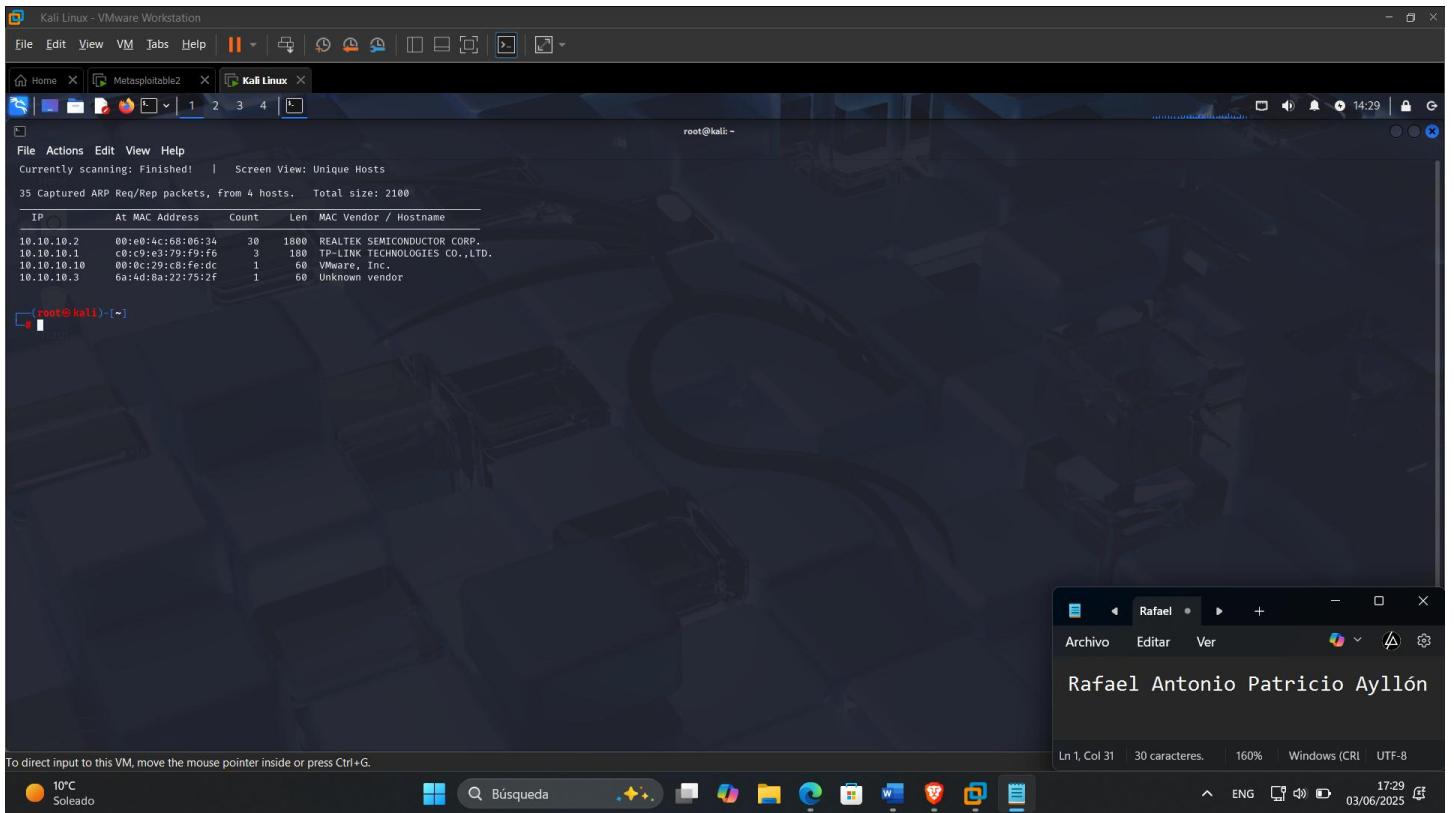
[root@kali] ~]
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Si bien conocemos que existe una máquina a la que tenemos ping, en la etapa de reconocimiento no conocemos a quiénes tenemos en nuestro mismo segmento de red, para ello usamos el siguiente comando para escanear toda la red:

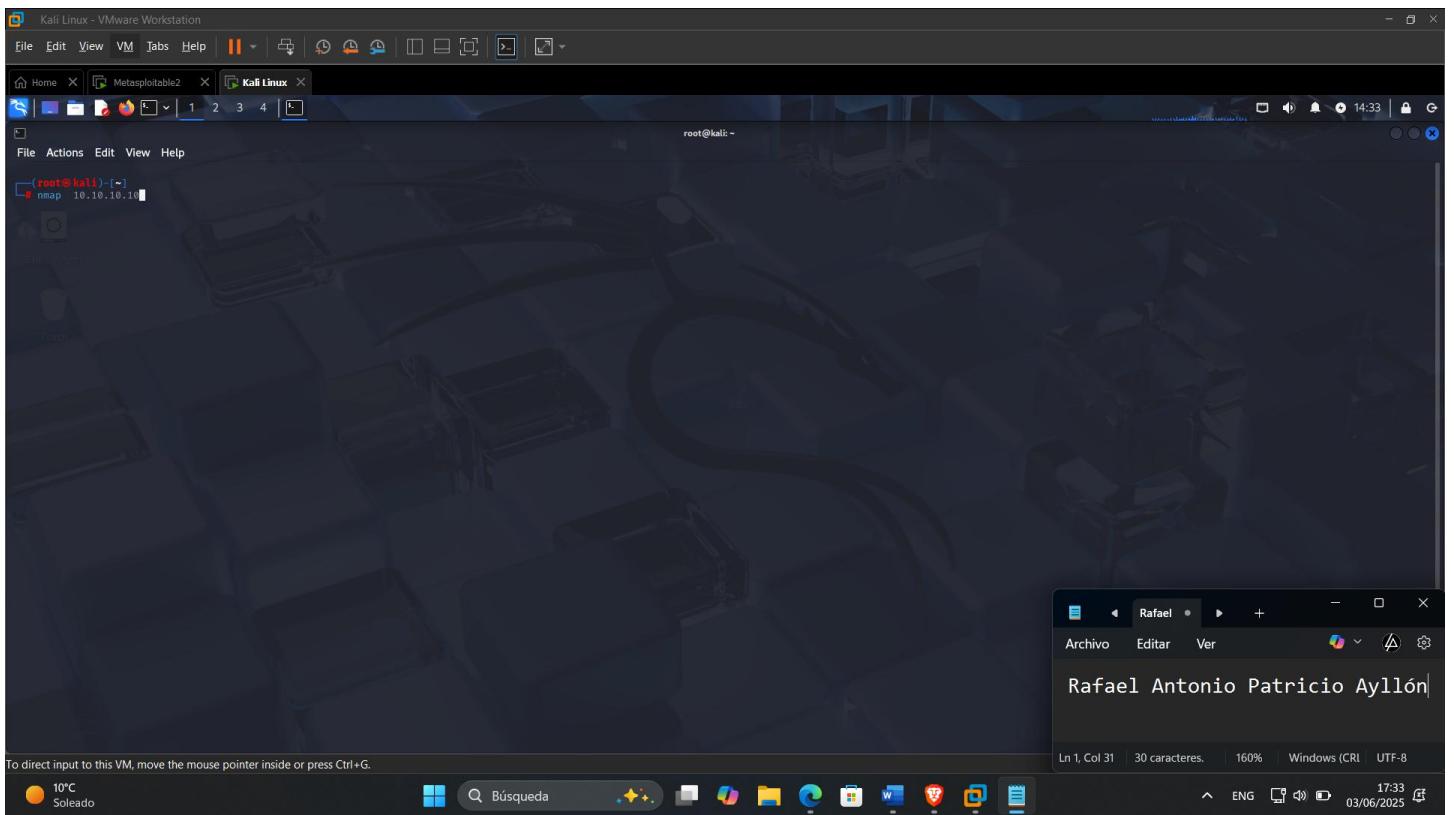


El resultado muestra que hay cuatro máquinas en este segmento de red: 10.10.10.1, 10.10.10.2, 10.10.10.3, 10.10.10.10, de existir más, serían identificadas igualmente.

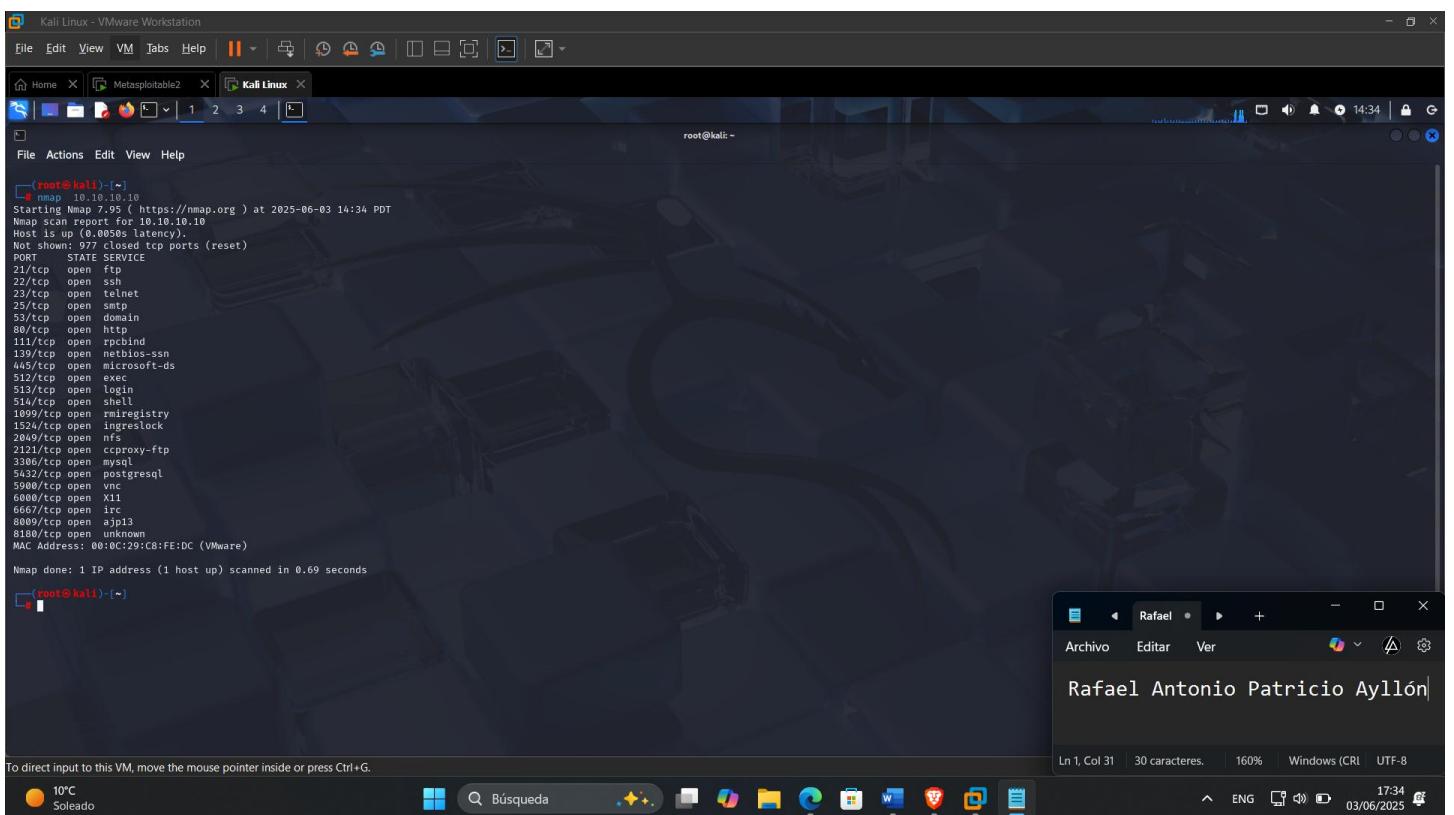


En el caso de que su versión de Kali no cuente con netdiscover, utilice el siguiente comando para descubrir los equipos que son parte de su red: `nmap 10.10.10.0/24`. En este caso se está realizando el escaneo a la dirección de red.

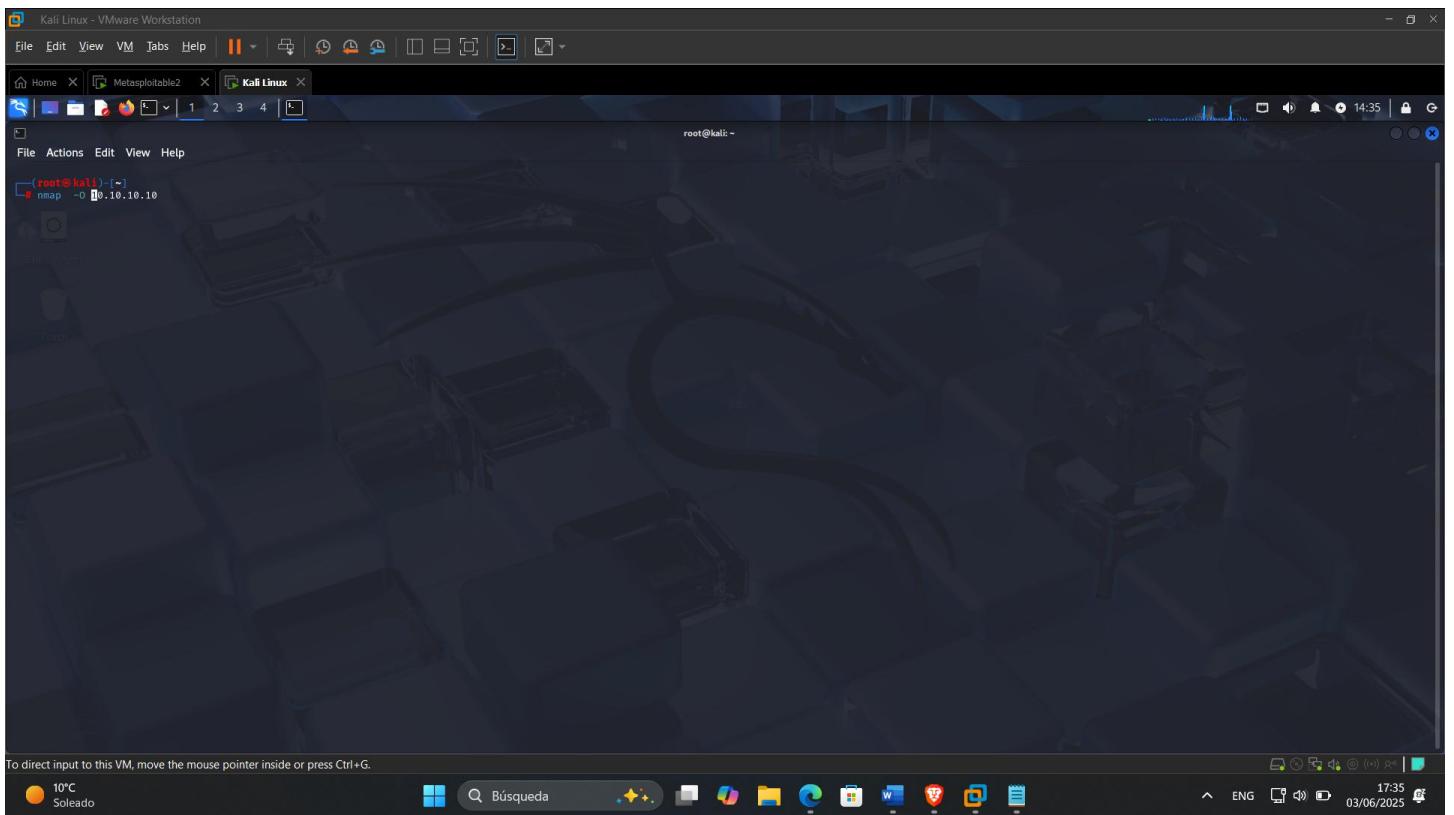
Habiendo identificado a los posibles objetivos, procedemos a realizar el escaneo de la PC metasploitable. Para ello utilizamos el comando:



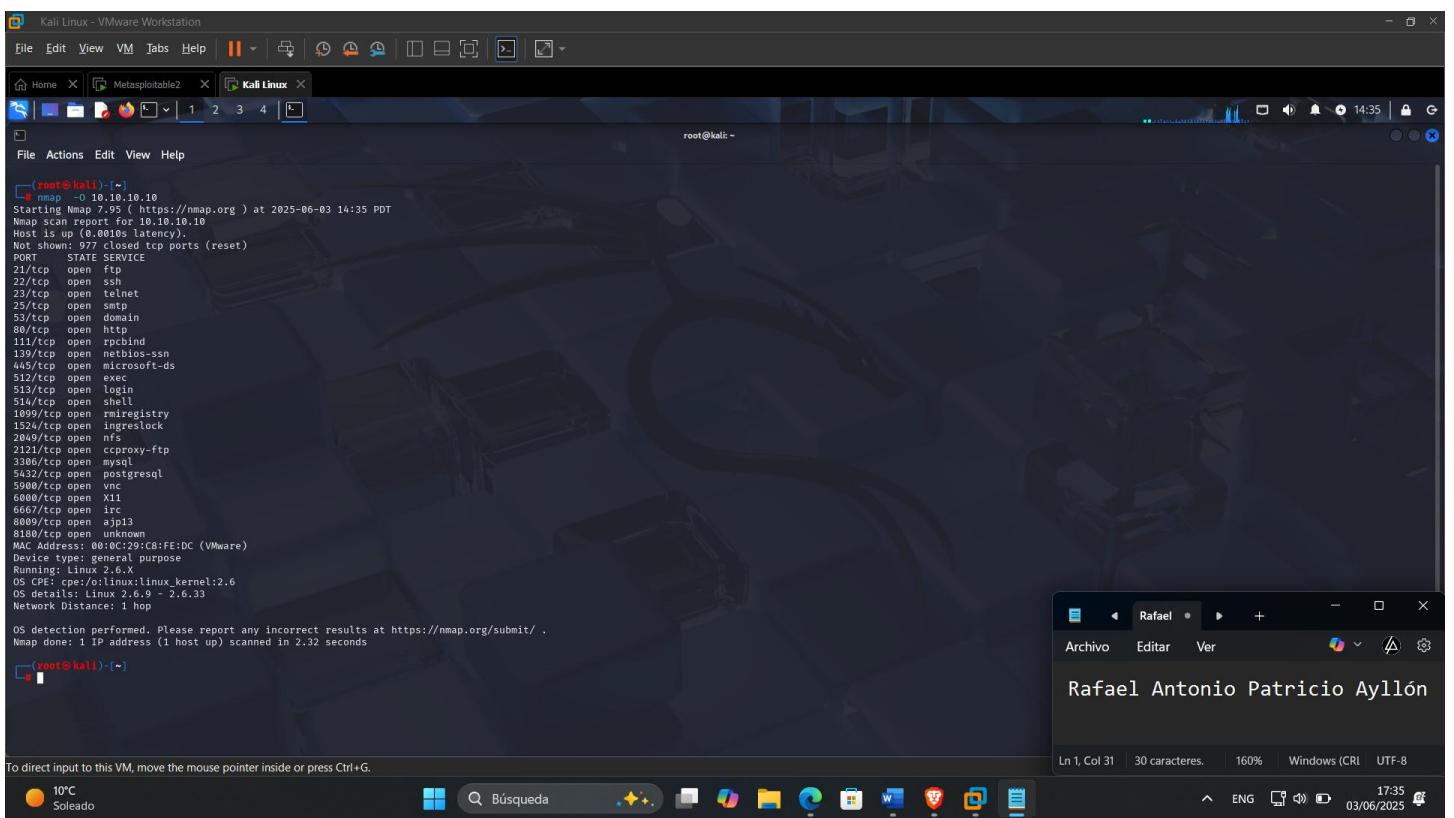
El resultado del mismo arroja que son varios los servicios que se están ejecutando en esa PC.



Sin embargo, no conocemos que sistema operativo es el que utiliza nuestro objetivo, para ello usamos:



Siendo el resultado una distribución en Linux.



Para ver a más detalle los servicios en este caso las versiones que utilizan, usamos el comando:

```
(root@kali: [~]
# nmap -sV 10.10.10.10
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

10°C Soleado

17:36 03/06/2025

Cuyo resultado son las versiones de cada servicio.

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 14:36 PDT
Nmap scan report for 10.10.10.10
Host is up (0.0024s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet  Linux telnetd
25/tcp    open  smtp   Postfix smtpd
53/tcp    open  domain ISC BIND 9.4.2
80/tcp    open  http   Apache httpd 2.2.8 ((Ubuntu) DAV/2)
109/tcp   open  pop3d  vsftpd 2.0.5
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)
512/tcp   open  exec   netkit-rsh rexecd
513/tcp   open  login  OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi  GNU Classpath grmiregistry
115/tcp   open  bindshell  remote root shell
2049/tcp  open  netcat  5.1 (RPC #100003)
2221/tcp  open  rdp   ProFTPD 1.3
3306/tcp  open  mysql  MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc   VNC (protocol 3.3)
6000/tcp  open  x11   (access denied)
6001/tcp  open  x11   (access denied)
8080/tcp  open  http  Apache Jserv (Protocol v1.3)
8180/tcp  open  http  Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:C8:FE:DC (VMware)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Map done: 1 IP address (1 host up) scanned in 12.90 seconds
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

10°C Soleado

17:36 03/06/2025

Si se necesita realizar un escaneo a un solo puerto por ejemplo al puerto 80, usamos el comando:

Kali Linux - VMware Workstation

File Edit View VM Tabs Help ||| Home X Metasploitable2 X Kali Linux X

File Actions Edit View Help

```
[root@kali ~]# nmap 10.10.10.10 -p 80
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 14:38 PDT
Nmap scan report for 10.10.10.10
Host is up (0.00095s latency).

PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:0C:29:C8:FE:DC (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
```

```
[root@kali ~]
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

NYM - LAD Puntuación del p...

Rafael Antonio Patricio Ayllón

Archivo Editar Ver R U C

Ln 1, Col 31 | 30 caracteres. | 160% | Windows (CRI) | UTF-8

17:38 03/06/2025

De igual forma a un rango de puertos:

Kali Linux - VMware Workstation

File Edit View VM Tabs Help ||| Home X Metasploitable2 X Kali Linux X

File Actions Edit View Help

```
[root@kali ~]# nmap 10.10.10.10 -p 21-23
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 14:38 PDT
Nmap scan report for 10.10.10.10
Host is up (0.0012s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
MAC Address: 00:0C:29:C8:FE:DC (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```

```
[root@kali ~]
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

NYM - LAD Puntuación del p...

Rafael Antonio Patricio Ayllón

Archivo Editar Ver R U C

Ln 1, Col 31 | 30 caracteres. | 160% | Windows (CRI) | UTF-8

17:38 03/06/2025

EVALUACIÓN (Capturas de pantalla)

1.- Utilice el comando: nmap -sP x.x.x.x/Z, donde x.x.x.x representa la dirección de red de su segmento y Z representa la máscara de subred. ¿Cuál es el resultado y que significa este?

The screenshot shows a Kali Linux terminal window titled "Kali Linux - VMware Workstation". The terminal is running as root, indicated by the prompt "root@kali: ~". The user has run the command "nmap -sP 10.10.10.0/27" to scan the subnet 10.10.10.0/27. The output shows five hosts up, each with its IP, latency, MAC address, and manufacturer information. The scan took 1.55 seconds. Below the terminal is a Windows taskbar with various icons and a system tray showing the date and time.

```
[root@kali: ~] # nmap -sP 10.10.10.0/27
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 14:40 PDT
Nmap scan report for 10.10.10.1
Host is up (0.0019s latency).
MAC Address: C0:C9:E3:79:F9:F6 (TP-Link Technologies)
Nmap scan report for 10.10.10.2
Host is up (0.0019s latency).
MAC Address: 00:E0:4C:68:06:34 (Realtek Semiconductor)
Nmap scan report for 10.10.10.3
Host is up (0.019s latency).
MAC Address: 6A:4D:8A:22:75:2F (Unknown)
Nmap scan report for 10.10.10.10
Host is up (0.00066s latency).
MAC Address: 00:0C:29:C8:FE:DC (VMware)
Nmap scan report for 10.10.10.8
Host is up.
Nmap done: 32 IP addresses (5 hosts up) scanned in 1.55 seconds
[root@kali: ~] #
```

El resultado muestra las IP activas en el segmento de red indicado. Esto ayuda a identificar cuántas y cuáles máquinas están conectadas.

2.- Realice un escaneo para determinar los puertos abiertos en la máquina virtual Windows 7 o Windows XP (Asegúrese que este en el mismo segmento de red que Kali). De no contar con esas: W7 ni XP, utilice otra máquina o realice el escaneo a su propia PC física. ¿Qué puertos están abiertos?

LAB11-Nmap2025_S1.pdf

PowerShell

```
Máscara de subred . . . . . : 255.255.0.0
Puerta de enlace predeterminada . . . . . : a Copilot

Adaptador de LAN inalámbrica Conexión de área local* 1:
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . . . . : 

Adaptador de LAN inalámbrica Conexión de área local* 2:
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . . . . : comando nmap -sP x.x.x.x/Z, donde x.x.x.x representa la dirección de red de su segmento y Z representa la máscara de subred. ¿Cuál es el resultado y qué significa este?

Adaptador de Ethernet Ethernet:
2.- Realice un escaneo para determinar los puertos abiertos en la máquina virtual Windows 7 o Windows XP (Asegúrese que se encuentre en el mismo segmento de red que Kali). De no contar con esas: W7 ni XP, utilice otra máquina o realice el escaneo a su dirección IP.
Sufijo DNS específico para la conexión. . . . . : ¿Qué puertos están abiertos?
Vínculo: dirección IPv6 local. . . . . : fe80::320f:ef11:15c3:2bcd%17
Dirección IPv4. . . . . : 10.10.10.2
Máscara de subred . . . . . : 255.255.255.224
Puerta de enlace predeterminada . . . . . : 10.10.10.1 (operativo tienen corriendo los siguientes sitios: www.uatf.edu.bo y www.uajms.edu.bo)

Adaptador de Ethernet VMware Network Adapter VMnet1:
Sufijo DNS específico para la conexión. . . . . : siguientes variaciones del comando nmap. El dominio será: https://www.uatf.edu.bo/
Vínculo: dirección IPv6 local. . . . . : fe80::e587:eb42:9647:e230%19
Dirección IPv4. . . . . : 192.168.131.1 [http://192.168.131.1/index.php]
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : Para explicar las diferencias entre cada comando.

Adaptador de Ethernet VMware Network Adapter VMnet8:
nmap -sS dominio

5.- Utilice la variación del comando:
nmap -A dominio -p 80
nmap -A dominio -p 22
```

Rafael Antonio Patricio Ayllón

Ln 1, Col 31 | 30 caracteres. | 160% | Windows (CRI) | UTF-8

10°C Soleado

Kali Linux - VMware Workstation

File Edit View VM Tabs Help

Home Metasploitable2 Kali Linux

File Actions Edit View Help

```
(root@kali:~) [~] # nmap -sS 10.10.10.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 14:42 PDT
Nmap scan report for 10.10.10.2
Host is up (0.0003s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    filtered msrpc
139/tcp    filtered netbios-ssn
445/tcp    filtered microsoft-ds
905/tcp    open  iss-realsecure
912/tcp    open  apex-mesh
3306/tcp   open  mysql
MAC Address: 00:E0:4C:68:06:34 (Realtek Semiconductor)

Nmap done: 1 IP address (1 host up) scanned in 2.68 seconds
(root@kali:~) [~]
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

10°C Soleado

Dirección IP escaneada: 10.10.10.2

Host is up: El equipo objetivo está encendido y responde.

Not shown: 994 closed tcp ports (reset): Nmap escaneó 1000 puertos por defecto. De esos, 994 están cerrados (respondieron con RST).

Puertos abiertos o filtrados:

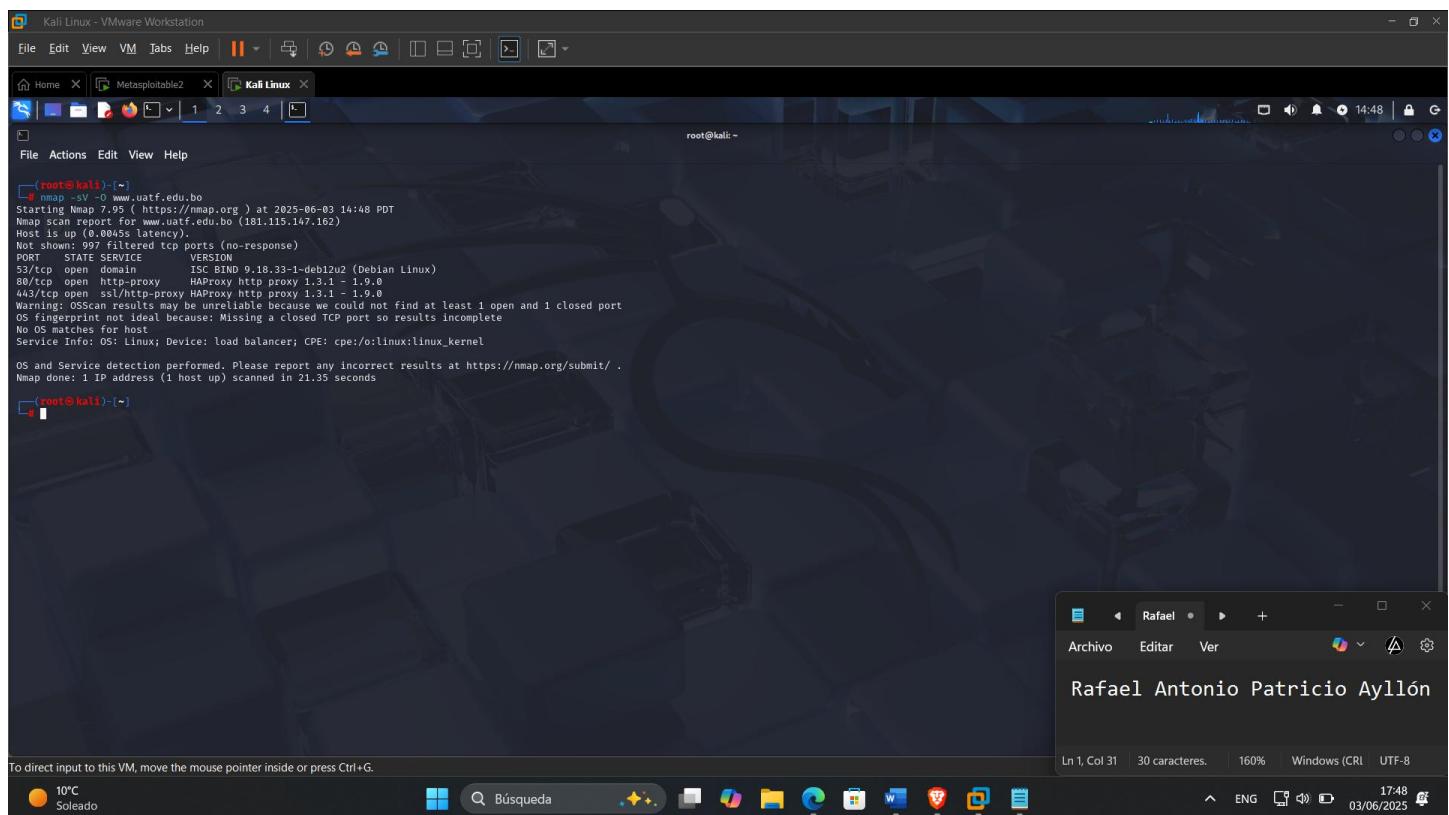
PUERTO	ESTADO	SERVICIO	SIGNIFICADO BREVE
135	filtered	msrpc	Filtrado por firewall, no respondió.
139	filtered	netbios-ssn	Igual que el anterior.
445	filtered	microsoft-ds	También filtrado.
902	open	iss-realsecure	Abierto, puede ser usado por VMware.
912	open	apex-mesh	Abierto, usado por algunas aplicaciones específicas.
3306	open	mysql	Abierto. Servidor de base de datos MySQL accesible.

3.- REQUIERE EL USO DE INTERNET

Qué servicios, versiones y sistema operativo tienen corriendo los siguientes sitios: www.uatf.edu.bo y www.ujams.edu.bo

¿Qué comandos utilizó?

Para la página www.uatf.edu.bo se usó el comando: nmap -sV -O www.uatf.edu.bo



```
root@kali:~# nmap -sV -O www.uatf.edu.bo
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 14:48 PDT
Nmap scan report for www.uatf.edu.bo (181.115.147.162)
Host is up (0.0045s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE          VERSION
53/tcp    open  domain        ISC BIND 9.18.33-1-deb12u2 (Debian Linux)
80/tcp    open  http-proxy    HAProxy http proxy 1.3.1 - 1.9.0
443/tcp   open  ssl/http-proxy HAProxy http proxy 1.3.1 - 1.9.0
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Service info: OS: Linux; Device: load balancer; CPE: cpe:/o:linux:linux_kernel
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 21.35 seconds
root@kali:~#
```

Dirección IP: 181.115.147.162

Puertos abiertos y servicios detectados:

Puerto	Estado	Servicio	Versión
53/tcp	open	domain	ISC BIND 9.18.33-1~deb12u2 (Debian Linux)
80/tcp	open	http-proxy	HAProxy http proxy 1.3.1 - 1.9.0
443/tcp	open	ssl/http-proxy	HAProxy http proxy 1.3.1 - 1.9.0

Sistema operativo estimado: Linux (según los servicios detectados)

Observación: No se identificó con precisión el sistema operativo porque no se detectó al menos 1 puerto cerrado necesario para un fingerprinting más fiable.

Para la página www.uajms.edu.bo se usó el comando: nmap -sV -O www.uajms.edu.bo

```

root@kali: ~] # nmap -sV -O www.uajms.edu.bo
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 14:51 PDT
Nmap scan report for www.uajms.edu.bo (200.87.27.208)
Host is up (0.021s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd
443/tcp   open  ssl/http Apache httpd
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU
No OS matches for host

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.35 seconds

```

Dirección IP: 200.87.27.208

Puertos abiertos y servicios detectados:

Puerto	Estado	Servicio	Versión
80/tcp	open	http	Apache httpd
443/tcp	open	ssl/http	Apache httpd
113/tcp	closed	ident	(no activo)

Sistema operativo: No identificado.

Observación: Aunque no se obtuvo el sistema operativo, se puede inferir que también corre sobre alguna distribución Linux por el servidor Apache.

4.- Utilice las siguientes variaciones del comando nmap. El dominio será: <https://www.uatf.edu.bo/>, <http://infodasa.com/web/index.php> y <http://ubielalto.com.bo/moodle/login/index.php>

Para explicar las diferencias entre cada comando.

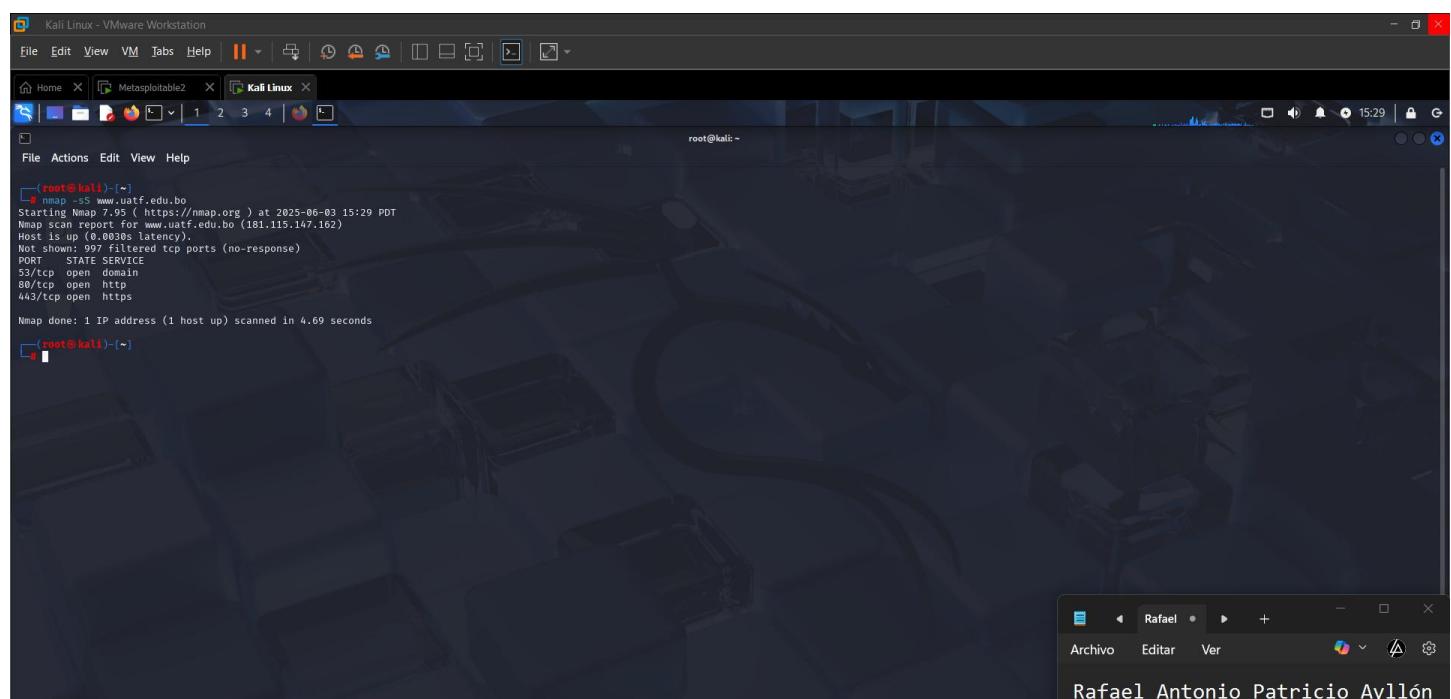
nmap-sS dominio

nmap-sT dominio

nmap-sU dominio

<https://www.uatf.edu.bo/>

nmap -sS www.uatf.edu.bo



```
root@kali:~# nmap -sS www.uatf.edu.bo
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 15:29 PDT
Nmap scan report for www.uatf.edu.bo (181.115.147.162)
Host is up (0.0038s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 4.69 seconds
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Rafael Antonio Patricio Ayllón

Ln 1, Col 31 | 30 caracteres. | 160% | Windows (CRI) | UTF-8

7°C Despejado

Búsqueda

18:29 03/06/2025

nmap -sT www.uatf.edu.bo

```
Kali Linux - VMware Workstation
File Edit View VM Tabs Help ||| Home X Metasploitable2 X Kali Linux X
File Actions Edit View Help
root@kali: ~
# nmap -sU www.uatf.edu.bo
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 15:30 PDT
Nmap scan report for www.uatf.edu.bo (181.115.147.162)
Host is up (0.0044s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 5.04 seconds

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

7°C Despejado

Búsqueda

Archivo Editar Ver

Rafael Antonio Patricio Ayllón

Ln 1, Col 31 | 30 caracteres. | 160% | Windows (CRI) | UTF-8

18:30 03/06/2025

nmap -sU www.uatf.edu.bo

```
Kali Linux - VMware Workstation
File Edit View VM Tabs Help ||| Home X Metasploitable2 X Kali Linux X
File Actions Edit View Help
root@kali: ~
# nmap -sU www.uatf.edu.bo
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 15:30 PDT
Nmap scan report for www.uatf.edu.bo (181.115.147.162)
Host is up (0.0033s latency).
Not shown: 999 open/filtered udp ports (no-response)
PORT      STATE SERVICE
53/udp   open  domain

Nmap done: 1 IP address (1 host up) scanned in 4.76 seconds

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

7°C Despejado

Búsqueda

Archivo Editar Ver

Rafael Antonio Patricio Ayllón

Ln 1, Col 31 | 30 caracteres. | 160% | Windows (CRI) | UTF-8

18:30 03/06/2025

<http://infodasa.com/web/index.php>

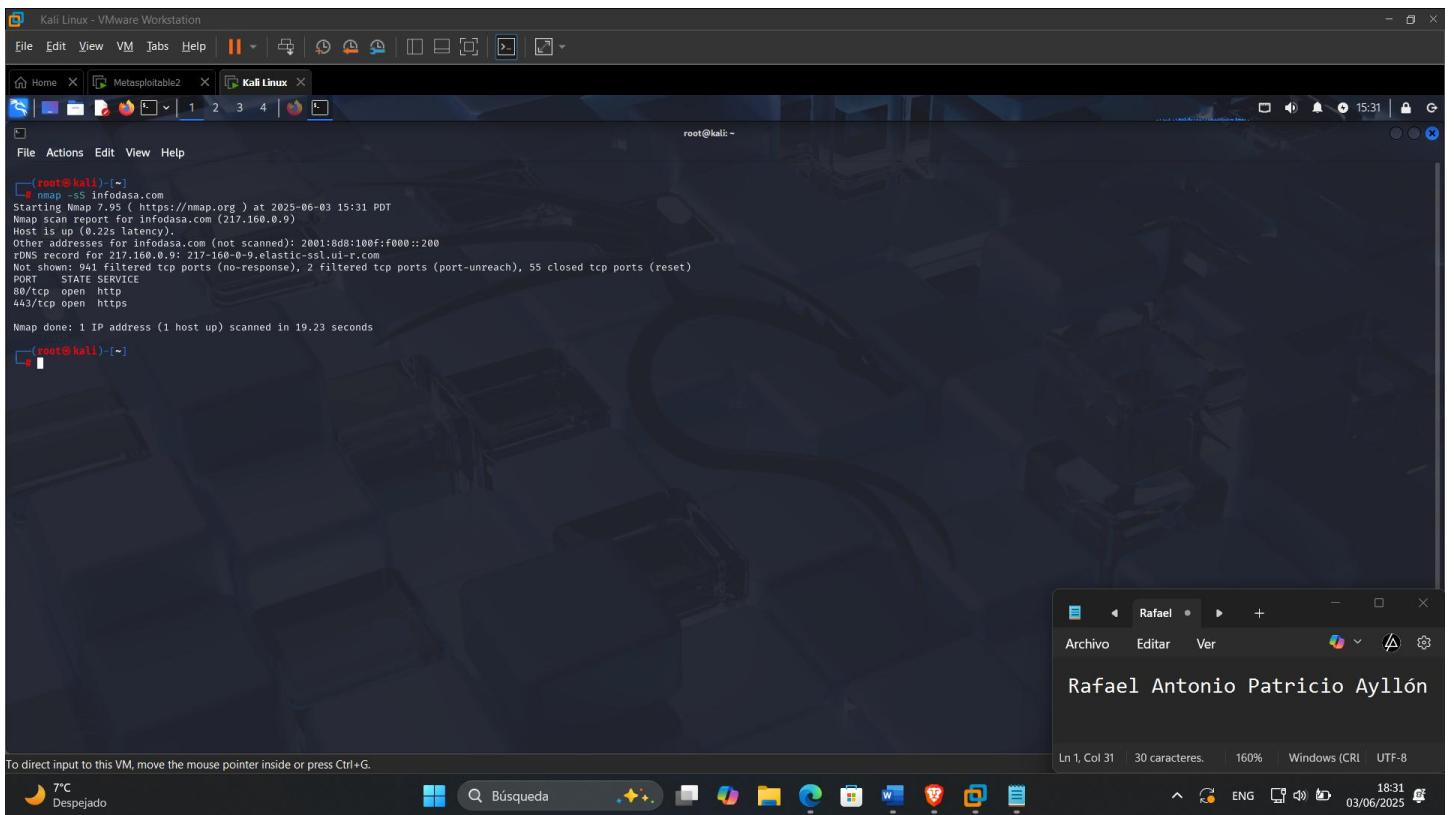
nmap -sS infodasa.com

```
[root@kali ~]# nmap -sS infodasa.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 15:31 PDT
Nmap scan report for infodasa.com (217.160.0.9)
Host is up (0.22s latency).
Other addresses for infodasa.com (not scanned): 2001:8d8:100f:f000::200
rDNS record for 217.160.0.9: 217.160.0.9.elastic-ssl.ui.r.com
Not shown: 941 filtered tcp ports (no-response), 2 filtered tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 19.23 seconds

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



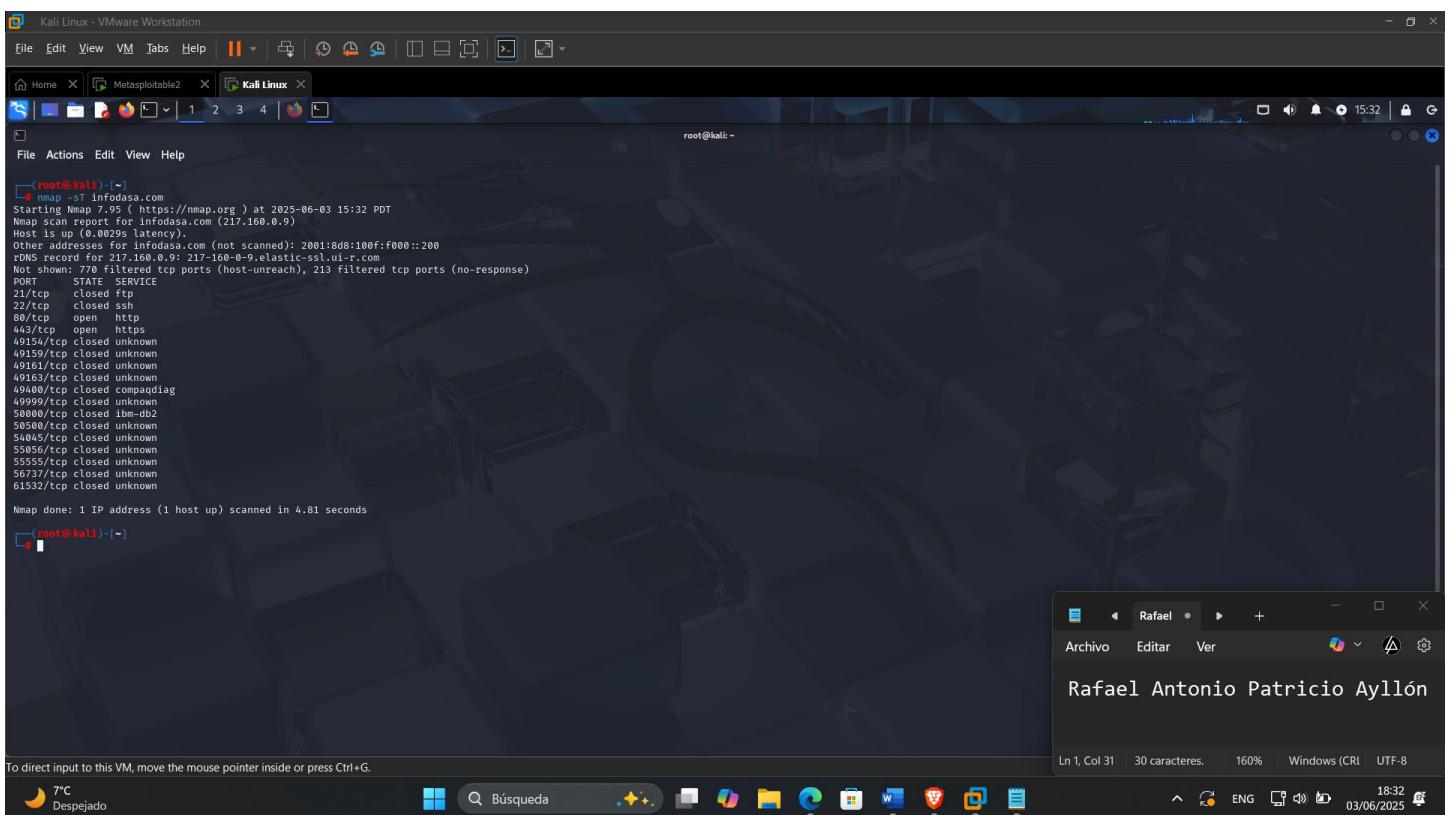
nmap -sT infodasa.com

```
[root@kali ~]# nmap -sT infodasa.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 15:32 PDT
Nmap scan report for infodasa.com (217.160.0.9)
Host is up (0.0029s latency).
Other addresses for infodasa.com (not scanned): 2001:8d8:100f:f000::200
rDNS record for 217.160.0.9: 217.160.0.9.elastic-ssl.ui.r.com
Not shown: 113 filtered tcp ports (host-unreach), 213 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    closed  ftp
22/tcp    closed  ssh
80/tcp    open   http
443/tcp   open   https
4443/tcp  closed unknown
49159/tcp closed unknown
49161/tcp closed unknown
49163/tcp closed unknown
49400/tcp closed compaqdiag
49999/tcp closed unknown
50000/tcp closed ibm-db2
50001/tcp closed unknown
50005/tcp closed unknown
50056/tcp closed unknown
55555/tcp closed unknown
56737/tcp closed unknown
61532/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 4.81 seconds

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



nmap -sU infodasa.com

```
Kali Linux - VMware Workstation
File Edit View VM Tabs Help ||| Home X Metasploitable2 X Kali Linux X
File Actions Edit View Help
root@kali:~#
[+]# nmap -sU infodasa.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 15:32 PDT
Nmap scan report for infodasa.com (217.160.0.9)
Host is up (0.0031s latency).
Other addresses for infodasa.com (not scanned): 2001:8d8:100f:f000::200
rDNS record for 217.160.0.9: 217-160-0-9.elastic-ssl.ui-r.com
All 1000 scanned ports on infodasa.com (217.160.0.9) are in ignored states.
Not shown: 1000 open/filtered udp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 4.54 seconds
[+]#
```



<http://ubielalto.com.bo/moodle/login/index.php>

nmap -sS ubielalto.com.bo

```
Kali Linux - VMware Workstation
File Edit View VM Tabs Help ||| Home X Metasploitable2 X Kali Linux X
File Actions Edit View Help
root@kali:~#
[+]# nmap -sS ubielalto.com.bo
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 15:33 PDT
Nmap scan report for ubielalto.com.bo (190.181.21.110)
Host is up (0.0026s latency).
rDNS record for 190.181.21.110: cooperacion-alemana.org
All 1000 scanned ports on ubielalto.com.bo (190.181.21.110) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 7.36 seconds
[+]#
```



nmap -sT ubielalto.com.bo

```

root@kali:~# nmap -sU ubielalto.com.bo
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 15:34 PDT
Nmap scan report for ubielalto.com.bo (190.181.21.110)
Host is up (0.0036s latency).
rDNS record for 190.181.21.110: cooperacion-alemana.org
All 1000 scanned ports on ubielalto.com.bo (190.181.21.110) are in ignored states.
Not shown: 1000 filtered udp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 26.28 seconds

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

7°C Despejado

Rafael Antonio Patricio Ayllón

Ln 1, Col 31 | 30 caracteres. | 160% | Windows (CRI) | UTF-8

18:34 ENG 03/06/2025

nmap -sU ubielalto.com.bo

```

root@kali:~# nmap -sU ubielalto.com.bo
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 15:34 PDT
Nmap scan report for ubielalto.com.bo (190.181.21.110)
Host is up (0.024s latency).
rDNS record for 190.181.21.110: cooperacion-alemana.org
Not shown: 999 open|filtered udp ports (no-response)
PORT      STATE     SERVICE
53/udp    filtered domain

Nmap done: 1 IP address (1 host up) scanned in 18.77 seconds

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

7°C Despejado

Rafael Antonio Patricio Ayllón

Ln 1, Col 31 | 30 caracteres. | 160% | Windows (CRI) | UTF-8

18:35 ENG 03/06/2025

Comando	Tipo de Escaneo	Características
nmap -sS	TCP SYN (sigiloso)	No completa conexión. Rápido y difícil de detectar.
nmap -sT	TCP connect	Completa la conexión. Más fácil de detectar.

nmap -sU

UDP

Escanea servicios UDP. Más lento, menos fiable.

5.- Utilice la variación del comando:

nmap -A dominio-p 80

nmap -A dominio-p 22

¿Qué tipo de escaneo significa la letra A?

nmap -A uatf.edu.bo -p 80

```
(root@kali:~) # nmap -A uatf.edu.bo -p 80
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 15:41 PDT
Nmap scan report for uatf.edu.bo (181.115.147.162)
Host is up (0.0040s latency).

PORT      STATE SERVICE      VERSION
80/tcp    open  http-proxy  HAProxy http proxy 1.3.1 - 1.9.0
|_http-title: Did not follow redirect to https://uatf.edu.bo/
|_http-open-proxy: Proxy might be redirecting requests
Warning: OSScan results may be unreliable because we did not find at least 1 open and 1 closed port
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.61 seconds

(root@kali:~) #
```

Rafael Antonio Patricio Ayllón

nmap -A uatf.edu.bo -p 22

```

Kali Linux - VMware Workstation
File Edit View VM Tabs Help ||| Home X Metasploitable2 X Kali Linux X
File Actions Edit View Help
root@kali: ~]
# nmap -A uaf.edu.bo -p 22
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 15:43 PDT
Nmap scan report for uaf.edu.bo (181.115.147.162)
Host is up (0.0031s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh
            OS:Running OSScan results: Cisco 3925 router (IOS 12.4) (95%), Dell PowerConnect 2708 switch (94%), Digital Loggers, Inc. power controller (firmware 1.2.7) (94%), Koukaam NETIO-230A power control device or ZyXEL SP-220E thermal printer (94%)
            Aggressive OS guesses: Cisco 3925 router (IOS 12.4) (95%), Dell PowerConnect 2708 switch (94%), Digital Loggers, Inc. power controller (firmware 1.2.7) (94%), Koukaam NETIO-230A power control device or ZyXEL SP-220E thermal printer (94%)
            SMC 8024L2 switch (94%), SunPower solar monitoring device (UIP stack) (94%), Schrack electric meter (94%), Grandstream GXP2000 VoIP phone (93%), Grandstream GXP2020 VoIP phone (93%)
            No exact OS matches for host (test conditions non-ideal).
Network Distance: 5 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1  1.14 ms  10.10.10.1
2  1.79 ms  192.168.100.1
3  3.12 ms  10.11.254.123
4  2.18 ms  10.149.221.238
5  1.91 ms  181.115.147.162

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 8.05 seconds
[~]#

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

7°C Despejado

Búsqueda

Archivo Editor Ver

Rafael Antonio Patricio Ayllón

Ln 1, Col 31 | 30 caracteres. | 160% | Windows (CRI) | UTF-8

18:43 ENG 03/06/2025

nmap -A infodasa.com -p 80

```

Kali Linux - VMware Workstation
File Edit View VM Tabs Help ||| Home X Metasploitable2 X Kali Linux X
File Actions Edit View Help
root@kali: ~]
# nmap -A infodasa.com -p 80
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 15:43 PDT
Nmap scan report for infodasa.com (217.160.0.9)
Host is up (0.0065s latency).
Other addresses for infodasa.com (not scanned): 2001:8d8:100f:f000::200
rDNS record for 217.160.0.9: 217-160-0-9.elastic-ssl.ui-r.com

PORT      STATE SERVICE VERSION
80/tcp    filtered http
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: power-device|firewall|WAP|router|print server|general purpose
Running (JUST GUESSING): APC embedded (96%), Cisco ASA 9.x (96%), Cisco embedded (96%), Synology embedded (96%), HP embedded (93%), D-Link embedded (89%), Microsoft Windows 2000|2003 (87%)
OS:PEP/Windows 2000|2003|cpe:/os:microsoft:windows_2000::sp4 cpe:/os:microsoft:windows_server_2003::sp2
Aggressive OS guesses: APC embedded (96%), Cisco Adaptive Security Appliance (ASA 9.2) (96%), Cisco Aironet 3800-series WAP (96%), Synology RT1900ac router (96%), HP 2101nw wireless print server (93%), D-Link DI-524 wireless broadband router (89%), Microsoft Windows 2000 SP4 (87%), Microsoft Windows Server 2003 SP2 (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 5 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1  1.12 ms  10.10.10.1
2  1.26 ms  192.168.100.1
3  2.88 ms  10.11.254.123
4  2.29 ms  10.149.221.238
5  2.43 ms  217-160-0-9.elastic-ssl.ui-r.com (217.160.0.9)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 8.54 seconds
[~]#

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

7°C Despejado

Búsqueda

Archivo Editor Ver

Rafael Antonio Patricio Ayllón

Ln 1, Col 31 | 30 caracteres. | 160% | Windows (CRI) | UTF-8

18:46 ENG 03/06/2025

nmap -A infodasa.com -p 22

```

root@kali: ~] # nmap -A infodasa.com -p 22
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 15:46 PDT
Nmap scan report for infodasa.com (217.160.0.9)
Host is up (0.00735 latency).
Other addresses for infodasa.com (not scanned): 2001:8d8:100f:f000::200
rDNS record for 217.160.0.9: 217.160.0.9.elastic-ssl.ui-r.com

PORT      STATE SERVICE VERSION
22/tcp    filtered ssh
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: power-device|firewall|WAP|router|print server|general purpose
Running (JUST GUESSING): APC embedded (96%), Cisco ASA 9.X (96%), Cisco embedded (96%), Synology embedded (96%), HP embedded (93%), D-Link embedded (89%), Microsoft Windows 2000|2003 (87%)
OS CPE: {cpe:/cisco:asa:9.2 {cpe:/h:synology:rt1900ac {cpe:/h:hp:101w {cpe:/o:microsoft:windows_2000::sp4 {cpe:/o:microsoft:windows_server_2003::sp2
Aggressive OS guesses: Cisco Network Management Card 3 (9%), Cisco Adaptive Security Appliance (ASA 9.2) (96%), Cisco Aironet 3800-series WAP (96%), Synology RT1900ac router (96%), HP 2101nw wireless print server (93%), D-Link DI-524 wireless router (93%), Microsoft Windows 2000 SP4 (87%), Microsoft Windows Server 2003 SP2 (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 5 hops

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1  1.35 ms  10.10.10.1
2  2.24 ms  192.168.100.1
3  4.68 ms  10.11.254.123
4  2.96 ms  10.149.221.238
5  3.01 ms  217.160.0.9.elastic-ssl.ui-r.com (217.160.0.9)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.45 seconds

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

nmap -A ubielalto.com.bo -p 80

```

root@kali: ~] # nmap -A ubielalto.com.bo -p 80
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 15:46 PDT
Nmap scan report for ubielalto.com.bo (190.181.21.110)
Host is up (0.0066s latency).
rDNS record for 190.181.21.110: cooperacion-alemana.org

PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.6 ((CentOS) PHP/7.4.22)
|_ http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.6 (CentOS) PHP/7.4.22
|_http-title: Construcción - Construcción Html5 Template
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Linux 3.X|4.X (87%)
OS CPE: {cpe:/o:linux:linux_kernel:3 {cpe:/o:linux:linux_kernel:4
Aggressive OS guesses: Linux 3.10 - 4.11 (87%), Linux 3.2 - 4.14 (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 5 hops

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1  1.45 ms  10.10.10.1
2  1.68 ms  192.168.100.1
3  2.88 ms  10.11.254.123
4  2.45 ms  10.149.221.238
5  2.02 ms  cooperacion-alemana.org (190.181.21.110)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.48 seconds

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

nmap -A ubielalto.com.bo -p 22

The screenshot shows a Kali Linux desktop environment within a VMware Workstation window. The terminal window displays an nmap scan command for the host ubielalito.com.bo (190.181.21.110). The output includes information about the host's OS, open ports (22/tcp filtered ssh), and traceroute details. The Notepad window shows a simple text entry: "Rafael Antonio Patricio Ayllón". The taskbar at the bottom shows various application icons.

```

root@kali: ~] # nmap -A ubielalito.com.bo -p 22
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 15:47 PDT
Nmap scan report for ubielalito.com.bo (190.181.21.110)
Host is up (0.00475 latency).
rDNS record for 190.181.21.110: cooperacion-alemana.org
Network Distance: 5 hops

PORT      STATE    SERVICE VERSION
22/tcp    Filtered ssh
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Asus RT-53N WAP (97%), Foundry Networks BigIron 8000 switch (IronWare 07.8.02eT53) (97%), Cisco ACE load balancer (95%), Cisco SLM2008 or HP ProCurve 1800 switch (94%), Cisco SLM2008 switch (94%), Chamberlain myQ garage door opener (93%), Cisco PIX Firewall (PIX OS 6.3(5)) (93%), NetOptics iBypass switch (93%), Sensitronics E4 temperature monitor (93%), Brocade FCX-series switch (89%)
No exact OS matched for host (test conditions non-ideal).

TRACEROUTE (using port 80/htp)
HOP RTT     ADDRESS
1  1.69 ms  10.10.10.1
2  2.40 ms  192.168.100.1
3  3.80 ms  10.11.254.123
4  3.24 ms  10.149.221.238
5  2.70 ms  cooperacion-alemana.org (190.181.21.110)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.00 seconds

```

-A significa

Escaneo agresivo que combina:

- Detección de sistema operativo
- Detección de versiones
- Script scanning
- Traceroute

Es un escaneo completo y detallado.

6.- Que comandos se podría utilizar para realizar una exploración de los puertos TCP y luego UDP en el rango de 22 a 1024. Use como destino los dominios indicados.

nmap -sS -p 22-1024 uatf.edu.bo # TCP

```
Kali Linux - VMware Workstation
File Edit View VM Tabs Help ||| Home X Metasploitable2 X Kali Linux X
File Actions Edit View Help
root@kali: ~]
# nmap -sS -p 22-1024 uatf.edu.bo
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 16:19 PDT
Nmap scan report for uatf.edu.bo (181.115.147.162)
Host is up (0.0032s latency).
Not shown: 1000 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 5.24 seconds
[~] #
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

6°C Despejado Búsqueda 19:19 03/06/2025

Rafael Antonio Patricio Ayllón

Ln 1, Col 31 | 30 caracteres. | 160% | Windows (CRI) | UTF-8

```
nmap -sU -p 22-1024 uatf.edu.bo    # UDP
```

```
Kali Linux - VMware Workstation
File Edit View VM Tabs Help ||| Home X Metasploitable2 X Kali Linux X
File Actions Edit View Help
root@kali: ~]
# nmap -sU -p 22-1024 uatf.edu.bo
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 16:19 PDT
Nmap scan report for uatf.edu.bo (181.115.147.162)
Host is up (0.0041s latency).
Not shown: 1002 open|filtered udp ports (no-response)
PORT      STATE SERVICE
53/udp   open  domain

Nmap done: 1 IP address (1 host up) scanned in 4.49 seconds
[~] #
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

6°C Despejado Búsqueda 19:19 03/06/2025

Rafael Antonio Patricio Ayllón

Ln 1, Col 31 | 30 caracteres. | 160% | Windows (CRI) | UTF-8

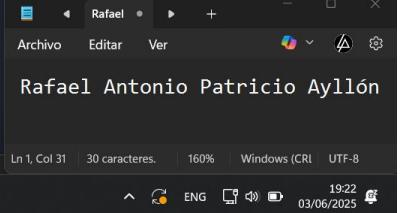
```
nmap -sS -p 22-1024 infodasa.com    # TCP
```

```
Kali Linux - VMware Workstation
File Edit View VM Tabs Help ||| Home X Metasploitable2 X Kali Linux X
File Actions Edit View Help
root@kali:~# nmap -sS -p 22-1024 infodasa.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 16:20 PDT
Nmap scan report for infodasa.com (217.160.0.9)
Host is up (0.031s latency).
Other addresses for infodasa.com (not scanned): 2001:8d8:100f:f000::200
rDNS record for 217.160.0.9: 217.160.0.9.elastic-ssl.ui-r.com
Not shown: 1000 filtered tcp ports (no-response), 1 filtered tcp ports (port-unreach)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
Nmap done: 1 IP address (1 host up) scanned in 11.53 seconds
root@kali:~#
```



nmap -sU -p 22-1024 infodasa.com # UDP

```
Kali Linux - VMware Workstation
File Edit View VM Tabs Help ||| Home X Metasploitable2 X Kali Linux X
File Actions Edit View Help
root@kali:~# nmap -sU -p 22-1024 infodasa.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 16:20 PDT
Nmap scan report for infodasa.com (217.160.0.9)
Host is up (0.037s latency).
Other addresses for infodasa.com (not scanned): 2001:8d8:100f:f000::200
rDNS record for 217.160.0.9: 217.160.0.9.elastic-ssl.ui-r.com
Not shown: 1002 filtered ports (admin-prohibited)
PORT      STATE SERVICE
162/udp  open  smpptrap
Nmap done: 1 IP address (1 host up) scanned in 100.98 seconds
root@kali:~#
```



nmap -sS -p 22-1024 ubielalto.com.bo # TCP

```
Kali Linux - VMware Workstation
File Edit View VM Tabs Help ||| Home X Metasploitable2 X Kali Linux X
File Actions Edit View Help
root@kali: ~
# nmap -sS -p 22-1024 ubielalto.com.bo
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 16:23 PDT
Nmap scan report for ubielalto.com.bo (190.181.21.110)
Host is up (0.0048s latency).
rDNS record for 190.181.21.110: cooperacion-alemana.org
Not shown: 1001 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 5.18 seconds
root@kali: ~
```



```
nmap -sU -p 22-1024 ubielalto.com.bo      # UDP
```

```
Kali Linux - VMware Workstation
File Edit View VM Tabs Help ||| Home X Metasploitable2 X Kali Linux X
File Actions Edit View Help
root@kali: ~
# nmap -sU -p 22-1024 ubielalto.com.bo
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 16:23 PDT
Nmap scan report for ubielalto.com.bo (190.181.21.110)
Host is up (0.029s latency).
rDNS record for 190.181.21.110: cooperacion-alemana.org
Not shown: 1002 filtered udp ports (admin-prohibited)
PORT      STATE SERVICE
162/udp  open  snmptrap

Nmap done: 1 IP address (1 host up) scanned in 1.92 seconds
root@kali: ~
```



7.- ¿Qué otro comando considera necesario en esta fase?

R.- Comando: nmap --script <script> <IP>

Ejemplo: nmap --script vuln 10.10.10.10

Usa scripts NSE (Nmap Scripting Engine) para detectar vulnerabilidades específicas (ej: Heartbleed, Shellshock) durante la fase de escaneo, complementando la identificación de riesgos.