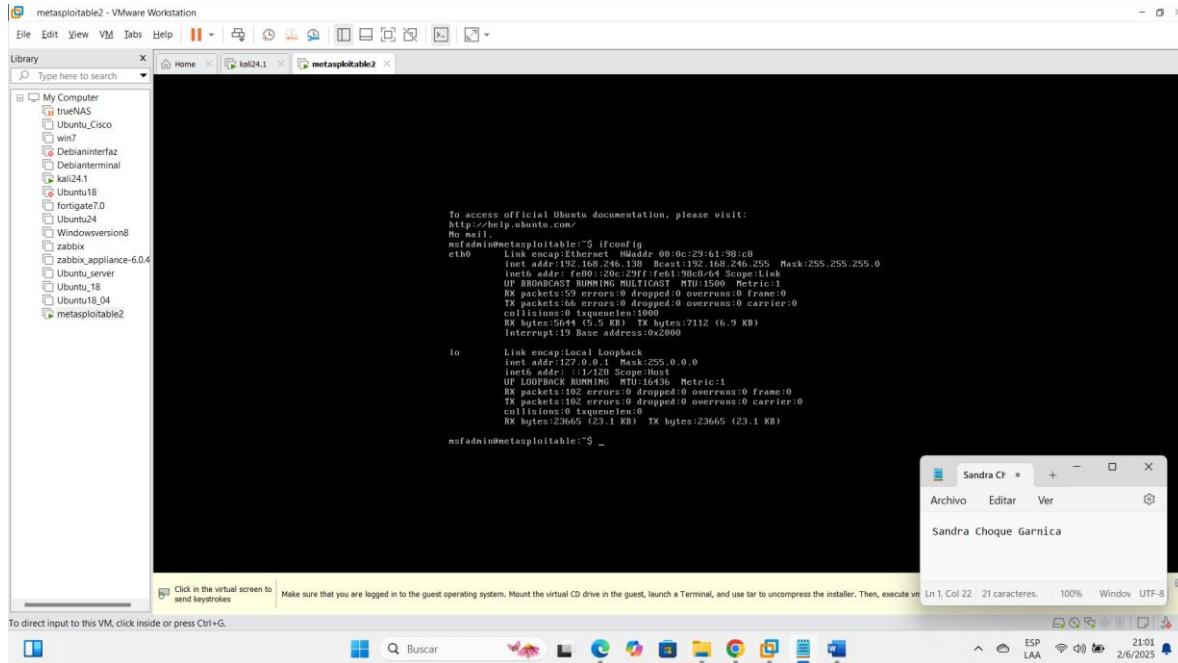


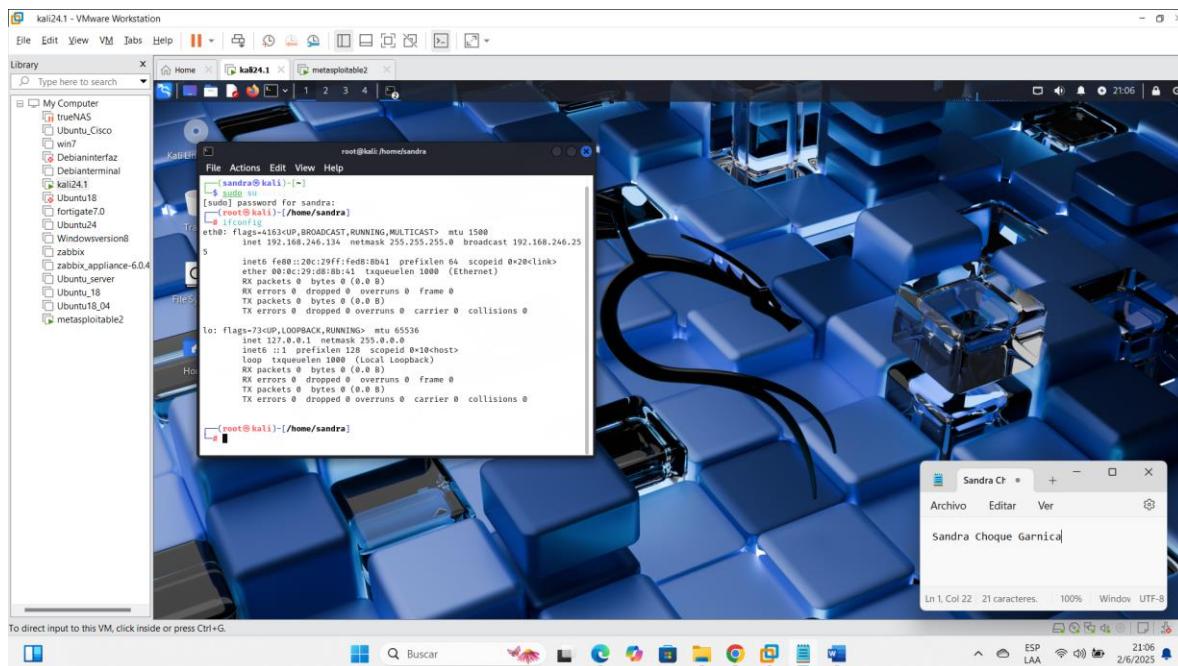
NOMBRE:SANDRA CHOQUE GARNICA

LAB 11 NMAP

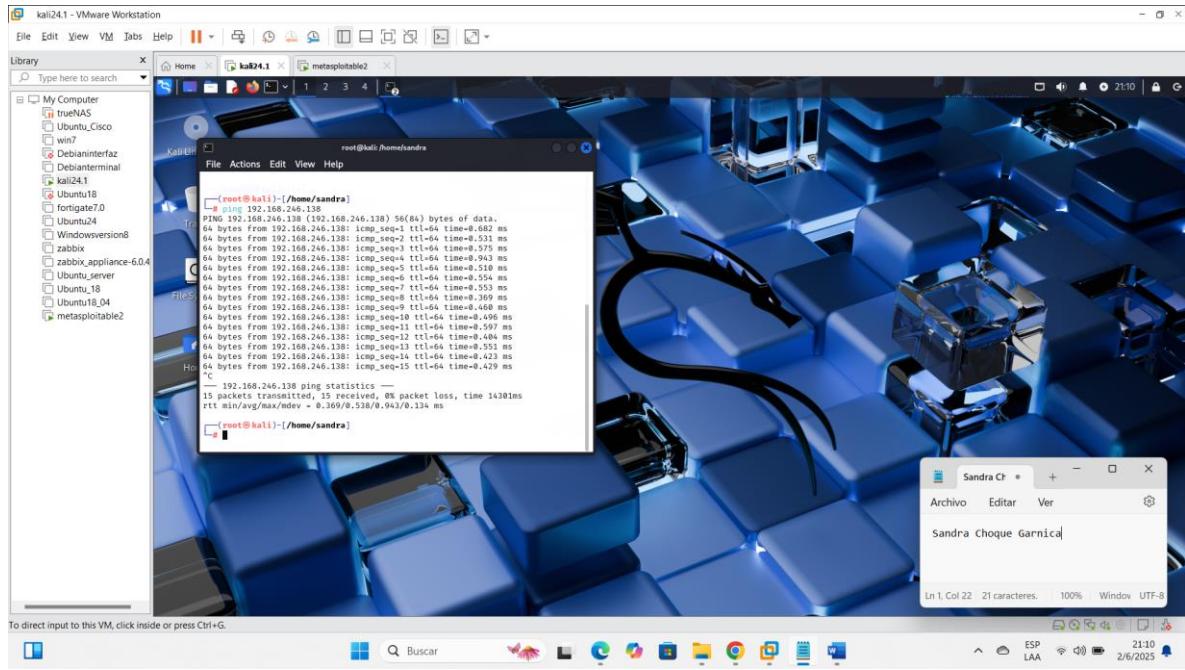
Ip de metasploit



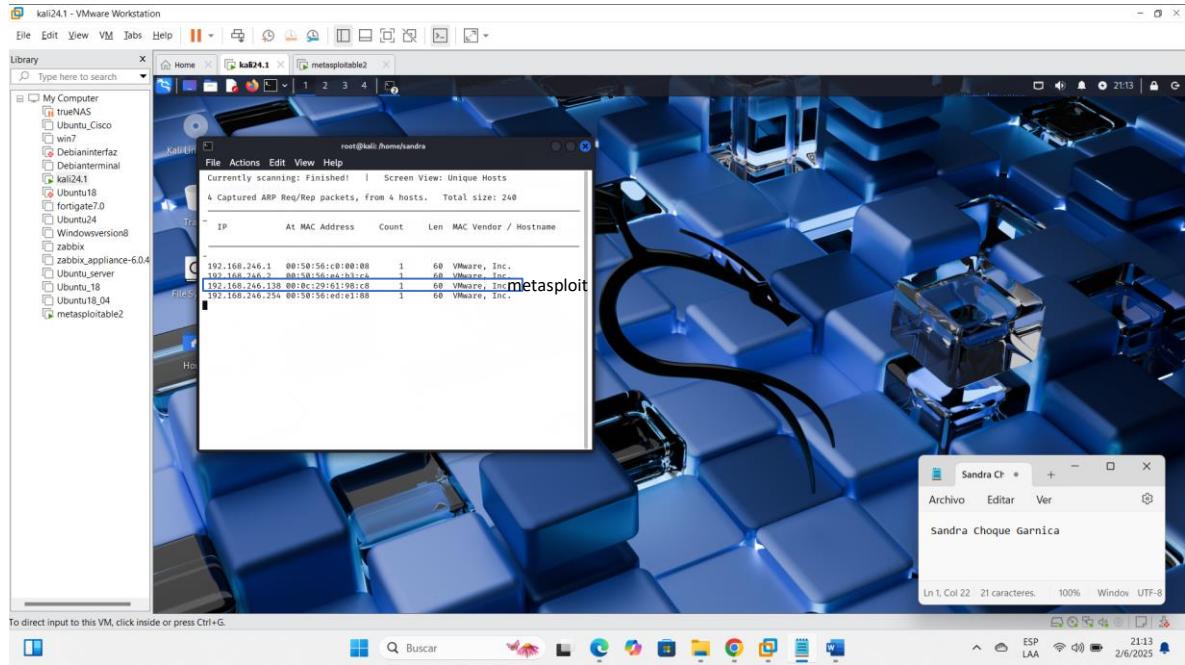
Ip de Kali



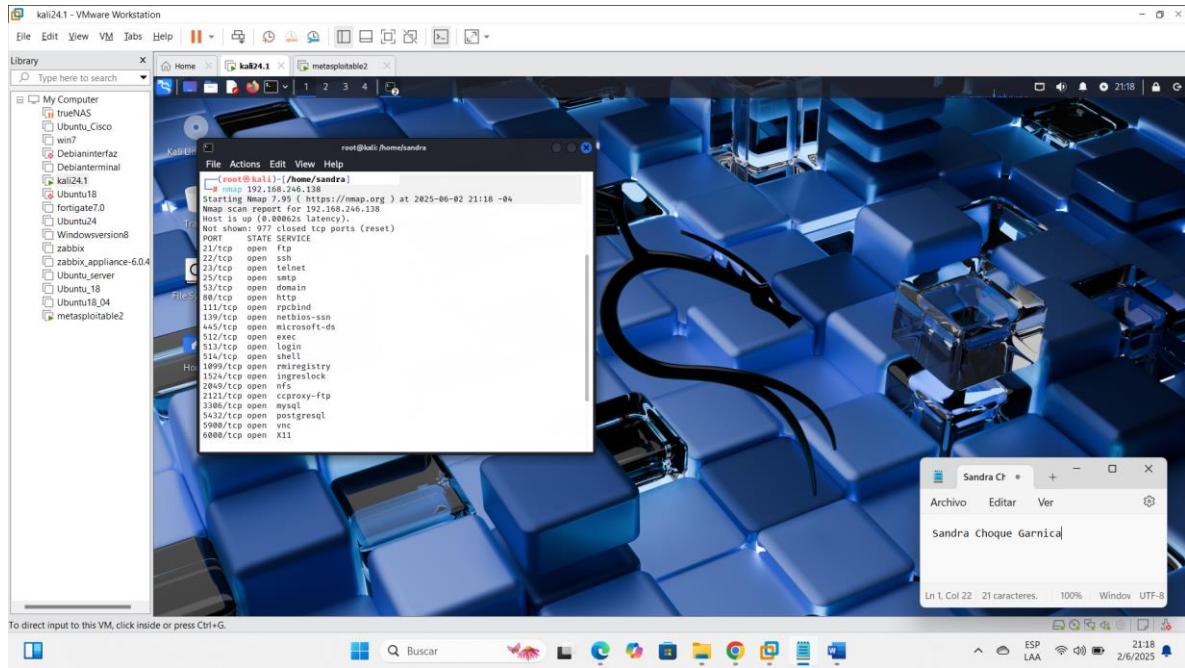
-ping de Kali a metasploit



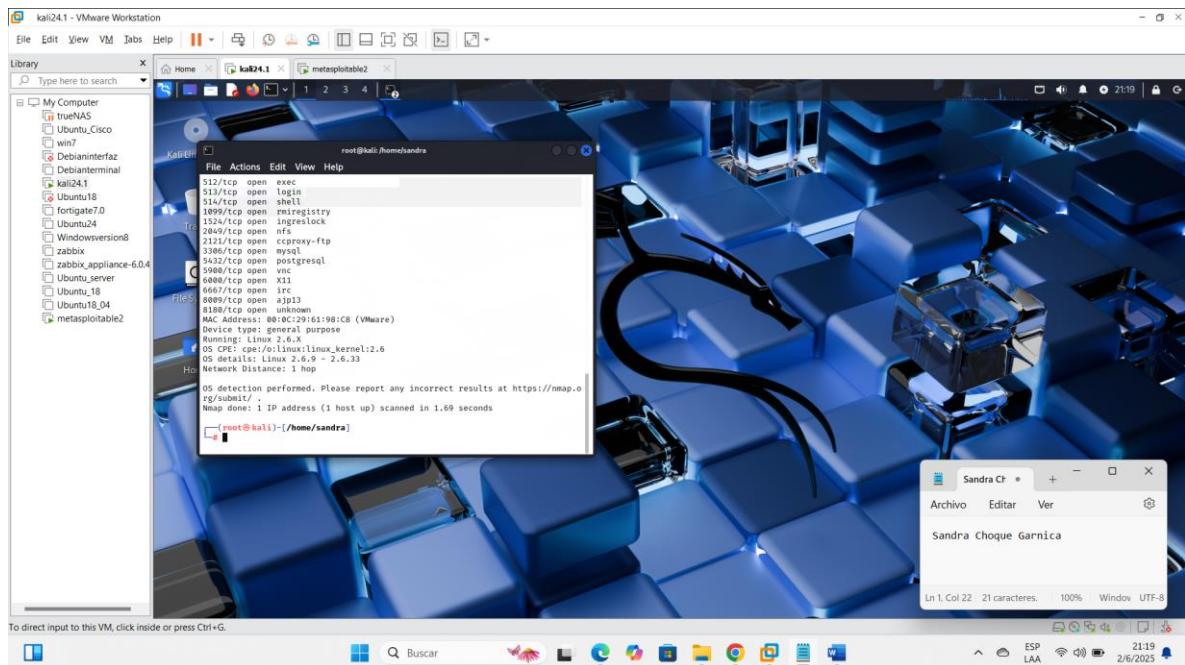
Identificar ip en la misma red



Nmap



-distribución en linux



-las versiones que utilizan

The screenshot shows a Kali Linux desktop environment within a VMware Workstation window. A terminal window titled 'root@kali:[/home/sandra]' is open, displaying the output of a 'nmap -v' scan against host 192.168.246.138. The scan results show various services running on the target host, including Apache, MySQL, PostgreSQL, and VNC. A Notepad window titled 'Sandra C#' is also visible, containing the text 'Sandra Cheque Garnica'.

```

root@kali:[/home/sandra]
nmap -v 192.168.246.138
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-02 21:21 -84
Nmap scan report for 192.168.246.138
Host is up (0.0015s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              vsftpd 2.3.4
22/tcp    open  ssh              OpenSSH 9.4.7p1 Debian Subbu11 (protocol 2.0)
23/tcp    open  telnet           Line 0.9.3
25/tcp    open  smtp             Postfix smtpd
53/tcp    open  domain           ISC BIND 9.4.2
69/tcp    open  domain           Apache DAV/2 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind          2 (RPC #100000)
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)
3128/tcp  open  http             Apache Tomcat/Coyote JSP Engine 1.1
3389/tcp  open  mysql            MySQL 5.0.51a-Ubuntu5
5432/tcp  open  postgresql       PostgreSQL DB 8.3.8 - 8.3.7
5980/tcp  open  vnc              VNC (protocol 3.3)
6000/tcp  open  X11              (access denied)
6067/tcp  open  irc              UnrealIRCd
8080/tcp  open  http             Apache Tomcat/Coyote JSP Engine 1.1
8180/tcp  open  http             Apache Tomcat/Coyote JSP Engine 1.1
MAC Address: 00:0C:29:61:98:C8 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 12.11 seconds

```

-escaneo del puerto 80

The screenshot shows a Kali Linux desktop environment within a VMware Workstation window. A terminal window titled 'root@kali:[/home/sandra]' is open, displaying the output of a 'nmap -v' scan against host 192.168.246.138. The scan results show various services running on the target host, including Apache, MySQL, PostgreSQL, and VNC. A Notepad window titled 'Sandra C#' is also visible, containing the text 'Sandra Cheque Garnica'.

```

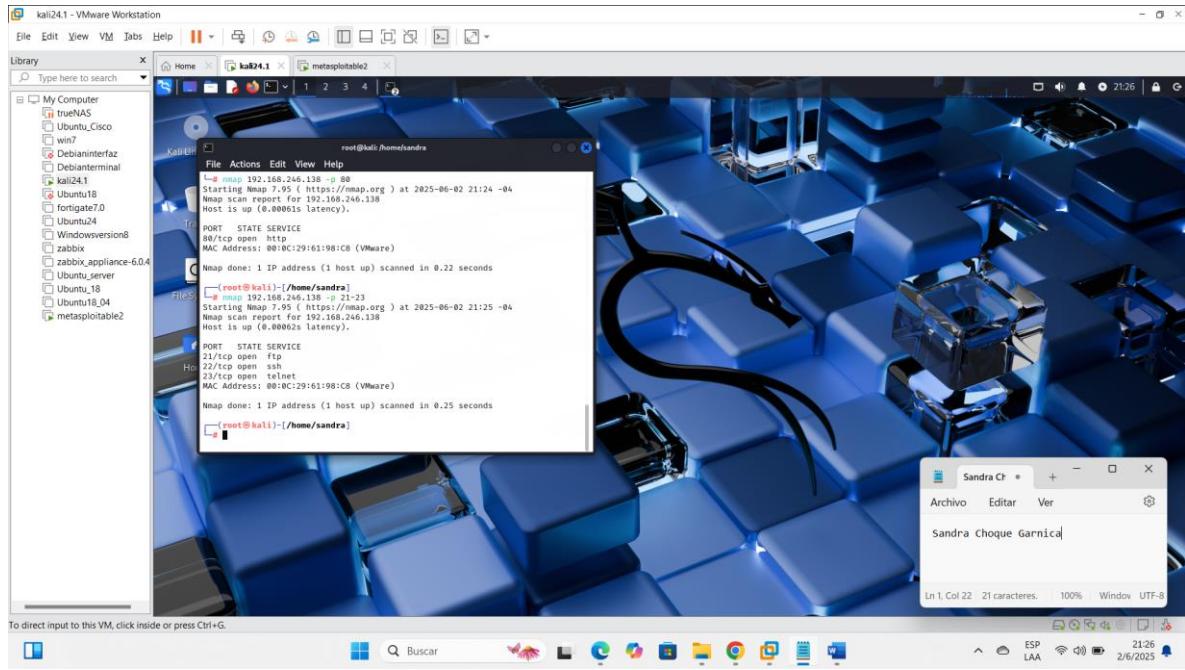
root@kali:[/home/sandra]
nmap -v 192.168.246.138
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-02 21:21 -84
Nmap scan report for 192.168.246.138
Host is up (0.0008s latency).

PORT      STATE SERVICE          VERSION
80/tcp    open  http             Apache Tomcat/Coyote JSP Engine 1.1
MAC Address: 00:0C:29:61:98:C8 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds

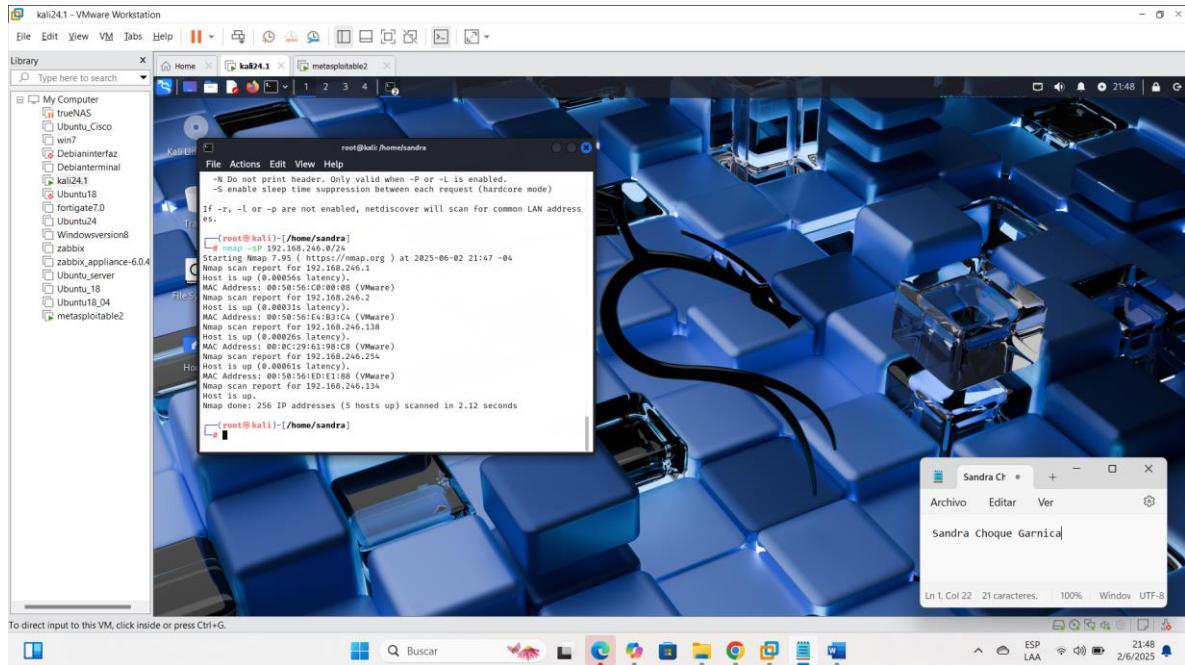
```

-rango de puertos



EVALUACION

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?

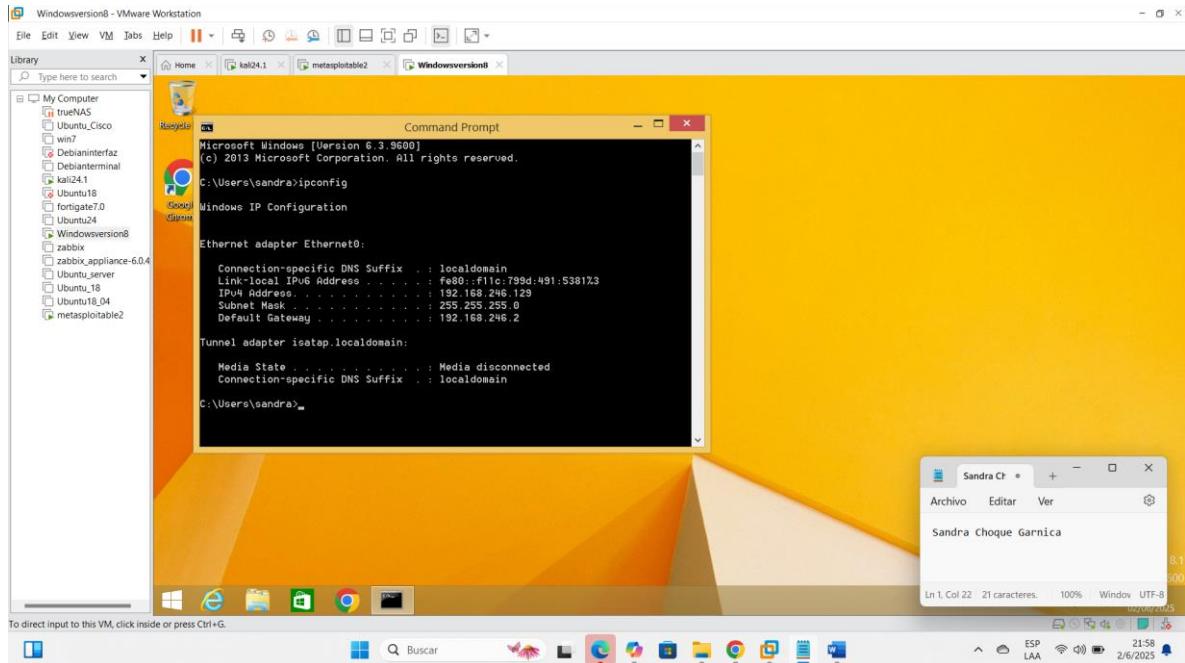
Nmap mostrará una lista de los dispositivos en la red que han respondido al escaneo de ping. Esto significa que los dispositivos 192.168.246.1 y

192.168.246.2, 192.168.246.138, 192.168.246.254, 192.168.246.134 están activos en la red.

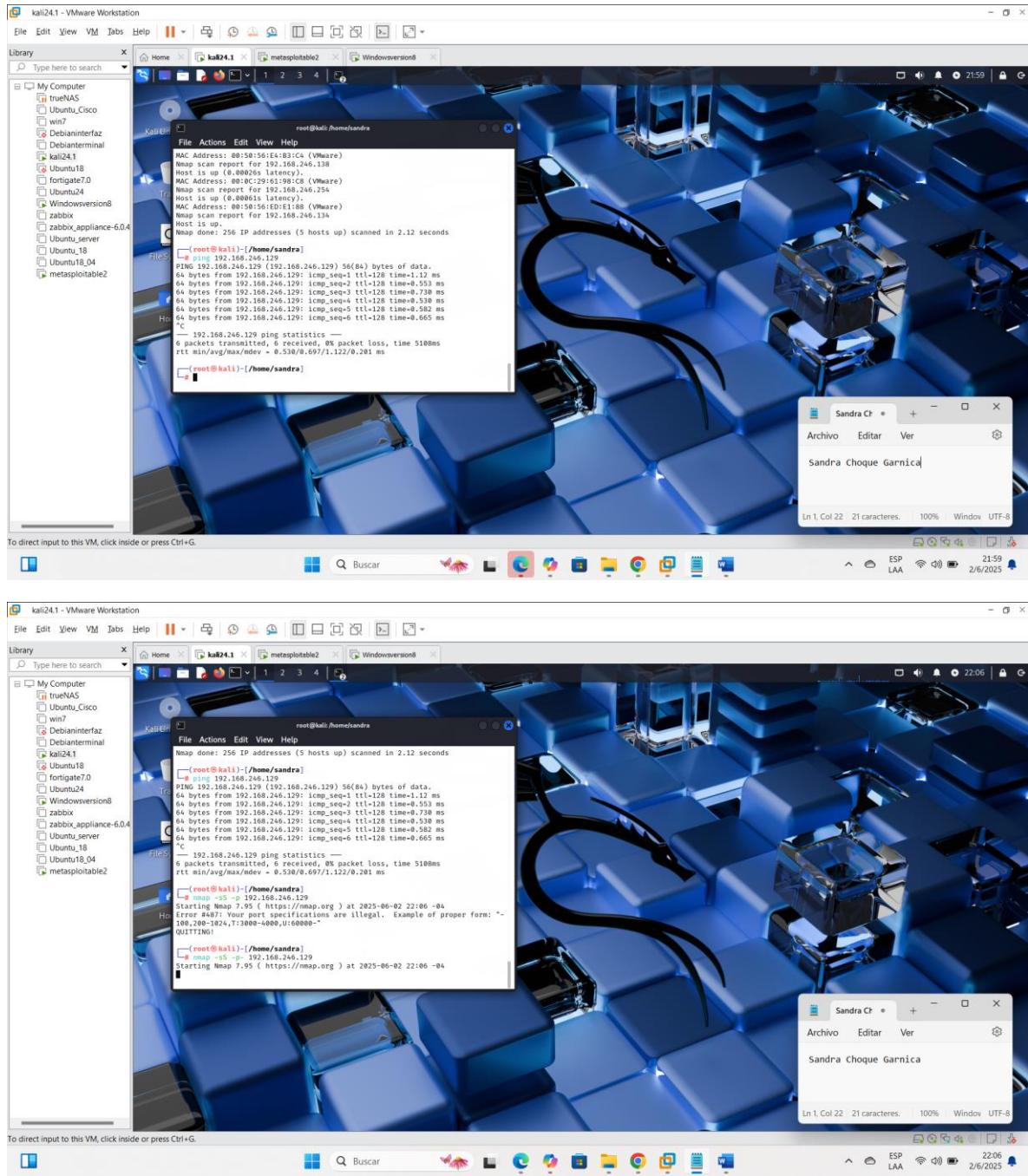
2.- Realice un escaneo para determinar los puertos abiertos en la máquina virtual Windows 7 o Windows XP (Asegúrese que

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

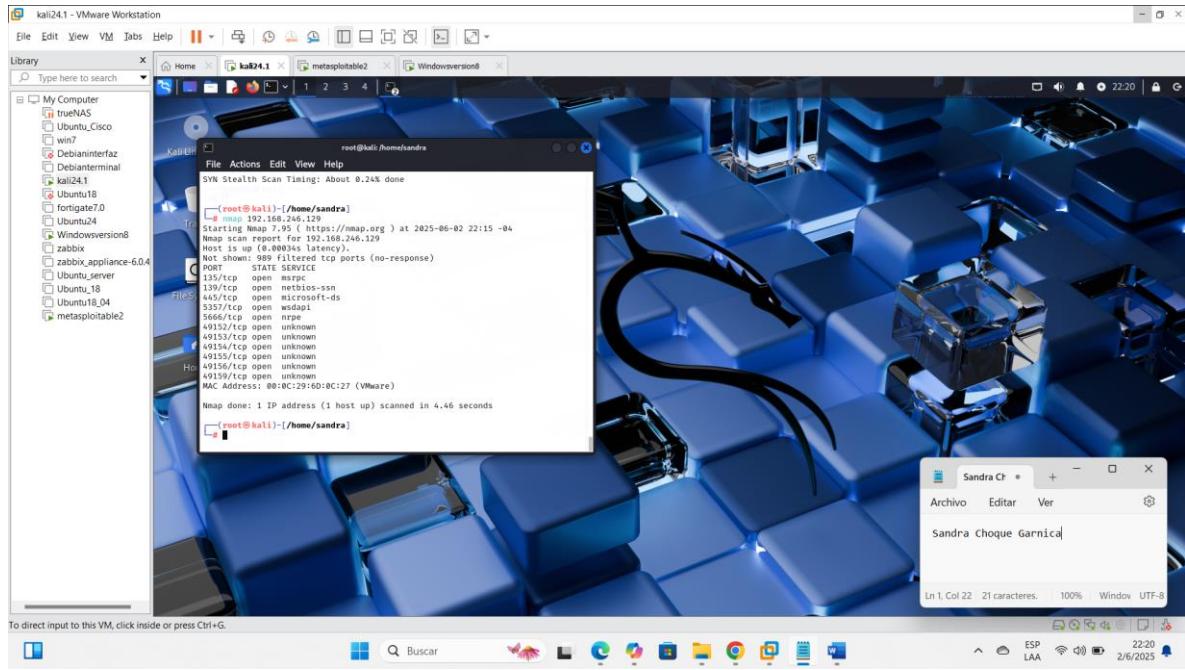
-ip windows 8



-ping de Kali a Windows



propia PC física. ¿Qué puertos están abiertos?



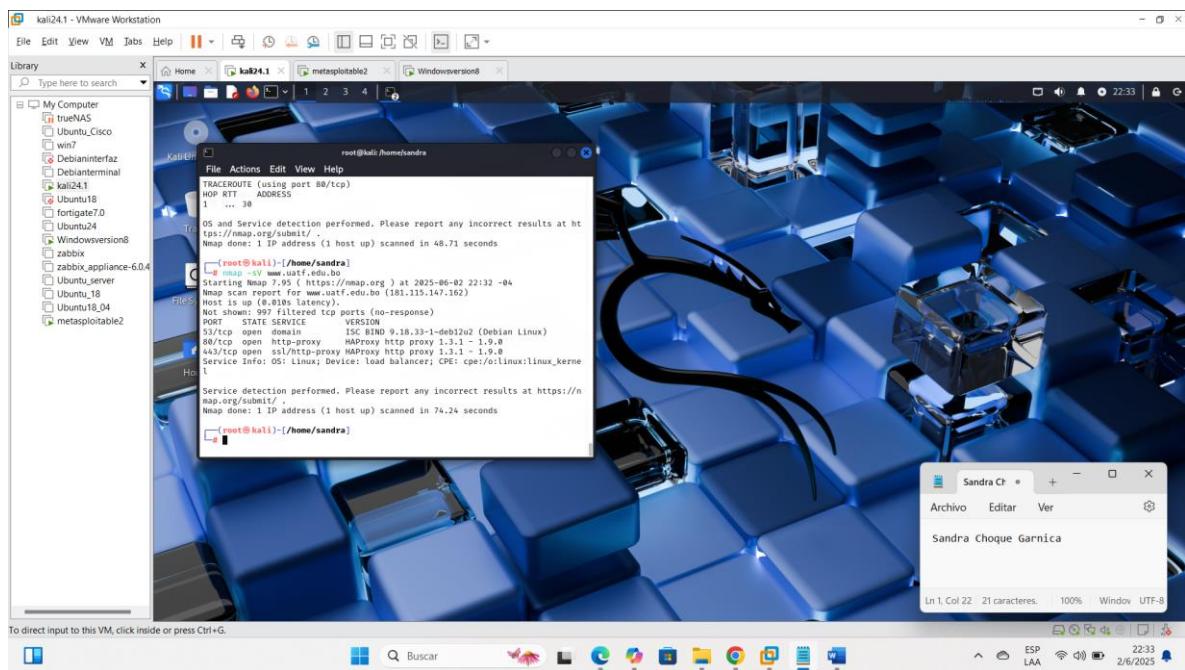
3.- REQUIERE EL USO DE INTERNET

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

¿Qué comandos utilizó?

Servicios y versión

#nmap -sV www.uatf.edu.bo



#nmap -sV www.uajms.edu.bo

```
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 Marproxy http proxy 1.3.1 - 1.9.0
Service Info: OS: Linux; Device: load balancer; CPE: cpe:/o/linux:linux_kernel_1

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 74.24 seconds
[rooth@kali]-[home/sandra]
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-02 22:35 -04
Nmap scan done for www.uajms.edu.bo (200.87.27.208)
Host is up (0.0006s latency).
Not shown: 997 filtered ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd
443/tcp   open  ssl/http-proxy Marproxy http proxy 1.3.1 - 1.9.0

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 105.33 seconds
[rooth@kali]-[home/sandra]
[rooth@kali]-[home/sandra]
```

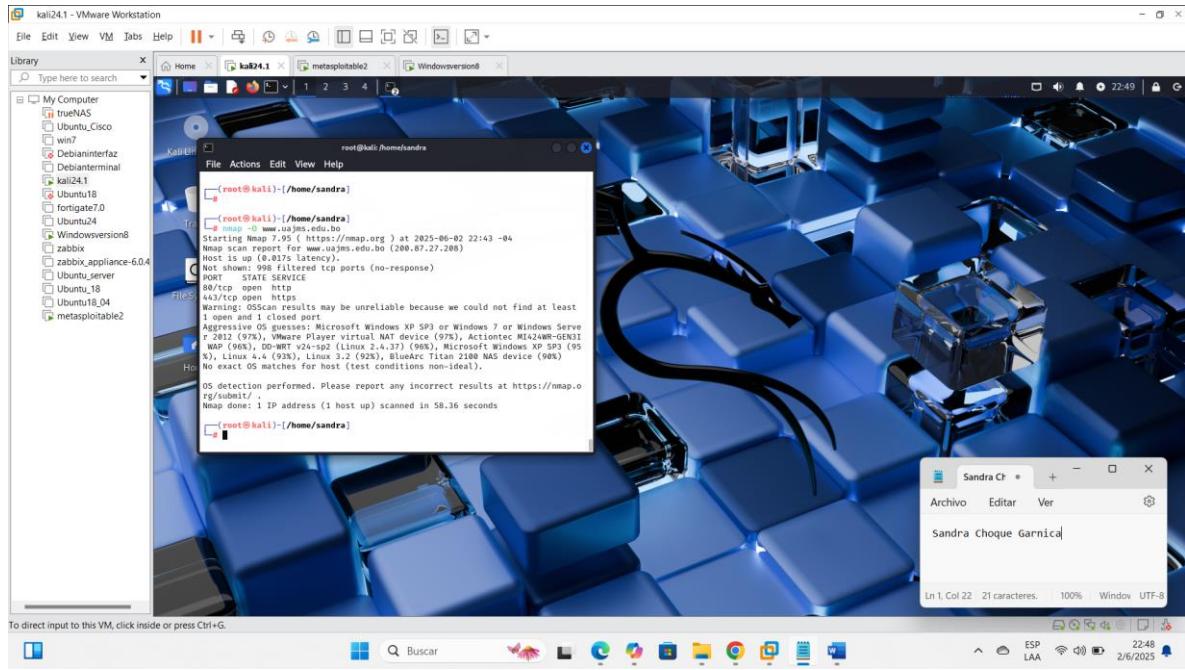
SISTEMA OPERATIVO

#nmap -O www.uatf.edu.bo

```
Nmap done: 1 IP address (1 host up) scanned in 105.33 seconds
[rooth@kali]-[home/sandra]
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-02 22:39 -04
Nmap scan done for www.uatf.edu.bo (181.115.147.162)
Host is up (0.0006s latency).
Not shown: 997 filtered ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd/2.4.42
443/tcp   open  ssl/http-proxy Marproxy http proxy 1.3.1 - 1.9.0

Warning: OSScan results may be unreliable because we could not find at least
one open and one closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.60 seconds
[rooth@kali]-[home/sandra]
[rooth@kali]-[home/sandra]
```

#nmap -O www.uajms.edu.bo



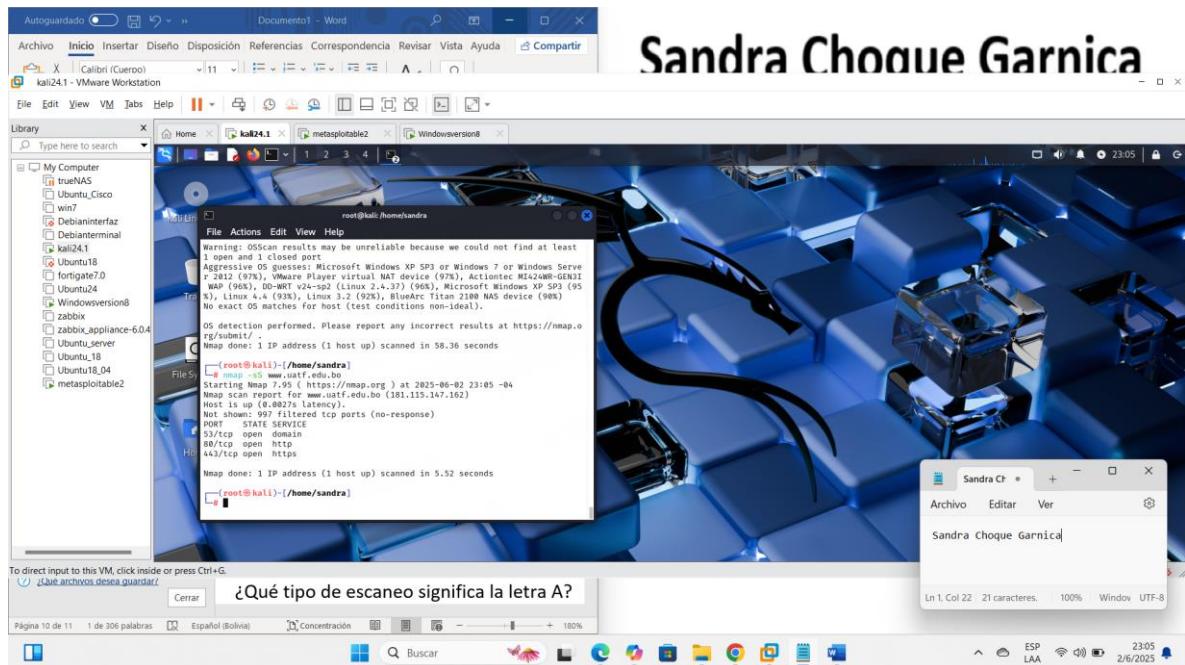
4.- Utilice las siguientes variaciones del comando nmap. El dominio será:
<https://www.uatf.edu.bo/>

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

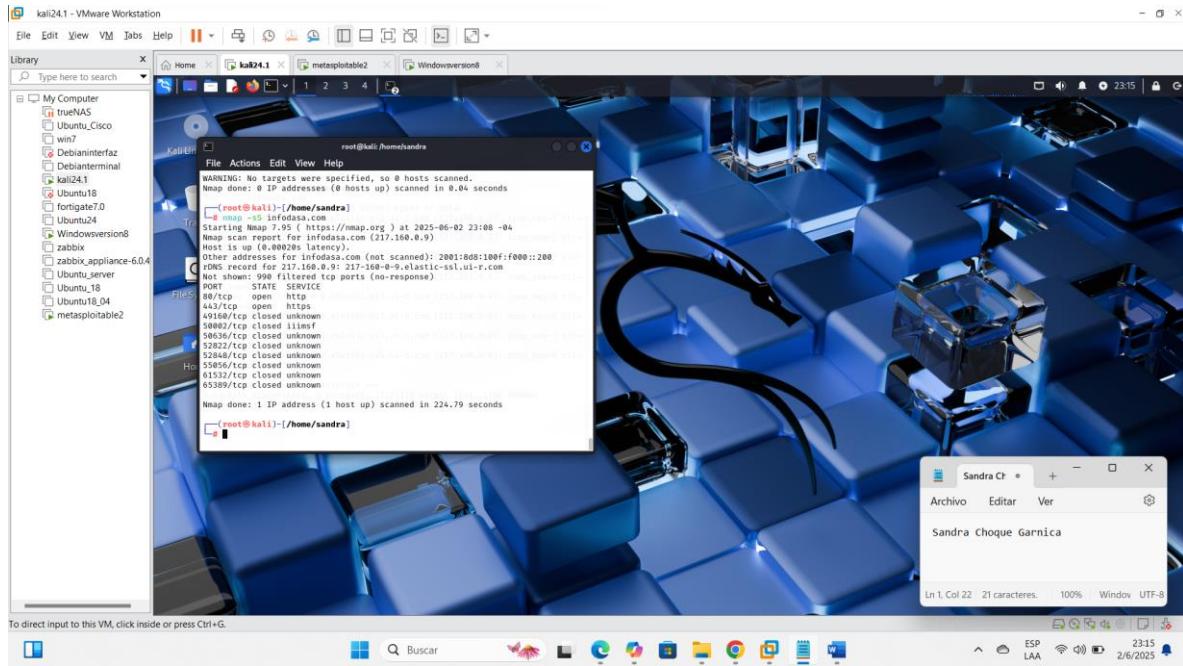
y <http://ubielalto.com.bo/moodle/login/index.php>

Para explicar las diferencias entre cada comando.

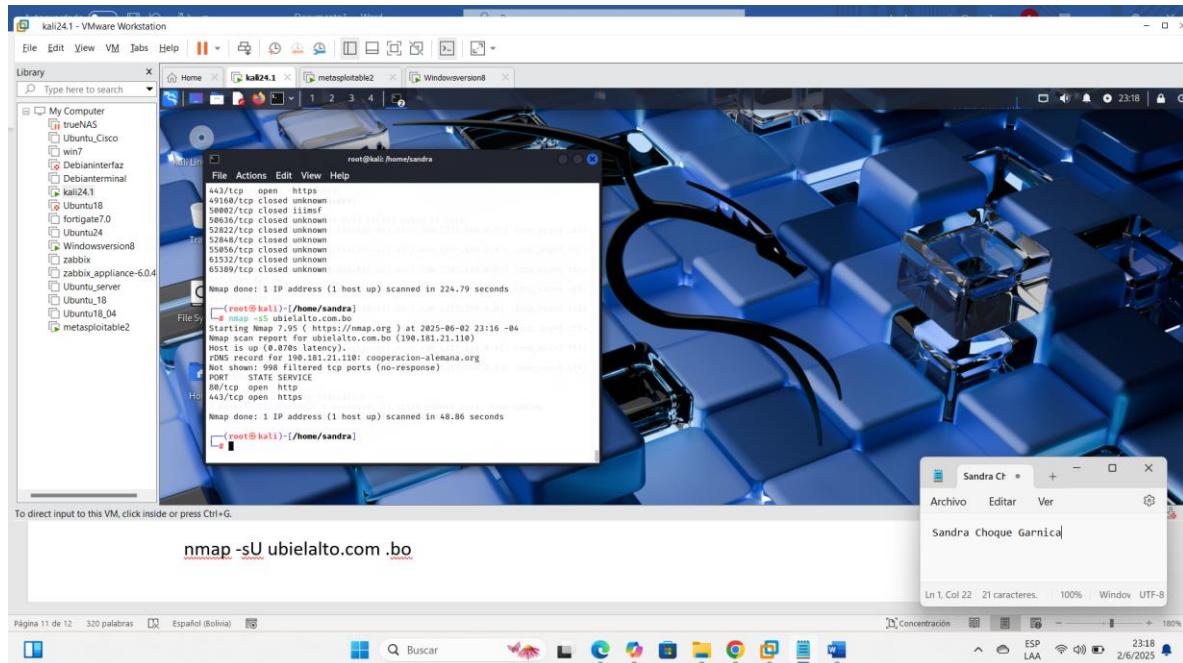
-nmap -sS www.uatf.edu.bo



nmap -sS infodasa.com



nmap -sS ubielalto.com.bo



nmap -sU www.uatf.edu.bo

kali24.1 - VMware Workstation

```

File Edit View VM Tabs Help ||| 
Library Type here to search
My Computer
  trueNAS
  Ubuntu_Cisco
  win7
  DebianInterfaz
  DebiTerminal
  kali24.1
  Ubuntu18
  fortigate7.0
  Ubuntu24
  Windowsversion8
  zabbix
  zabbix_appliance-6.0.4
  Ubuntu_server
  Ubuntu_18
  Ubuntu18.04
  metasploitable2

Home kali24.1 metasploitable2 Windowsversion8

File Actions Edit View Help
└─# nmap -sS ubielalto.com.bo
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-02 23:16 -04
Nmap scan report for ubielalto.com.bo (190.181.21.10)
Host is up (0.07ms latency).
DNS record for 190.181.21.10: cooperacion-alemana.org
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 48.86 seconds
└─# nmap -sT www.uatf.edu.bo
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-02 23:19 -04
Nmap scan report for www.uatf.edu.bo (181.115.147.162)
Host is up (0.012s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 66.69 seconds
└─# Sandra C# -[home/sandra]

```

To direct input to this VM, click inside or press Ctrl+G.

Buscar Buscar

23:20 2/6/2025

nmap -sT infodasa.com

kali24.1 - VMware Workstation

```

File Edit View VM Tabs Help ||| 
Library Type here to search
My Computer
  trueNAS
  Ubuntu_Cisco
  win7
  DebianInterfaz
  DebiTerminal
  kali24.1
  Ubuntu18
  fortigate7.0
  Ubuntu24
  Windowsversion8
  zabbix
  zabbix_appliance-6.0.4
  Ubuntu_server
  Ubuntu_18
  Ubuntu18.04
  metasploitable2

Home kali24.1 metasploitable2 Windowsversion8

File Actions Edit View Help
└─# nmap -sT www.uatf.edu.bo
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-02 23:19 -04
Nmap scan report for www.uatf.edu.bo (181.115.147.162)
Host is up (0.012s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 66.69 seconds
└─# nmap -sT infodasa.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-02 23:21 -04
Nmap scan report for infodasa.com (217.180.8.9)
Host is up (0.00035s latency).
Other addresses for infodasa.com (not scanned): 209.180.100.200
Note: TCP connect() to 217.180.8.9 port 80 failed: Connection refused
A11 100B scans completed. Ignored: infodasa.com (217.180.8.9) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 22.91 seconds
└─# Sandra C# -[home/sandra]

```

To direct input to this VM, click inside or press Ctrl+G.

Buscar Buscar

23:22 2/6/2025

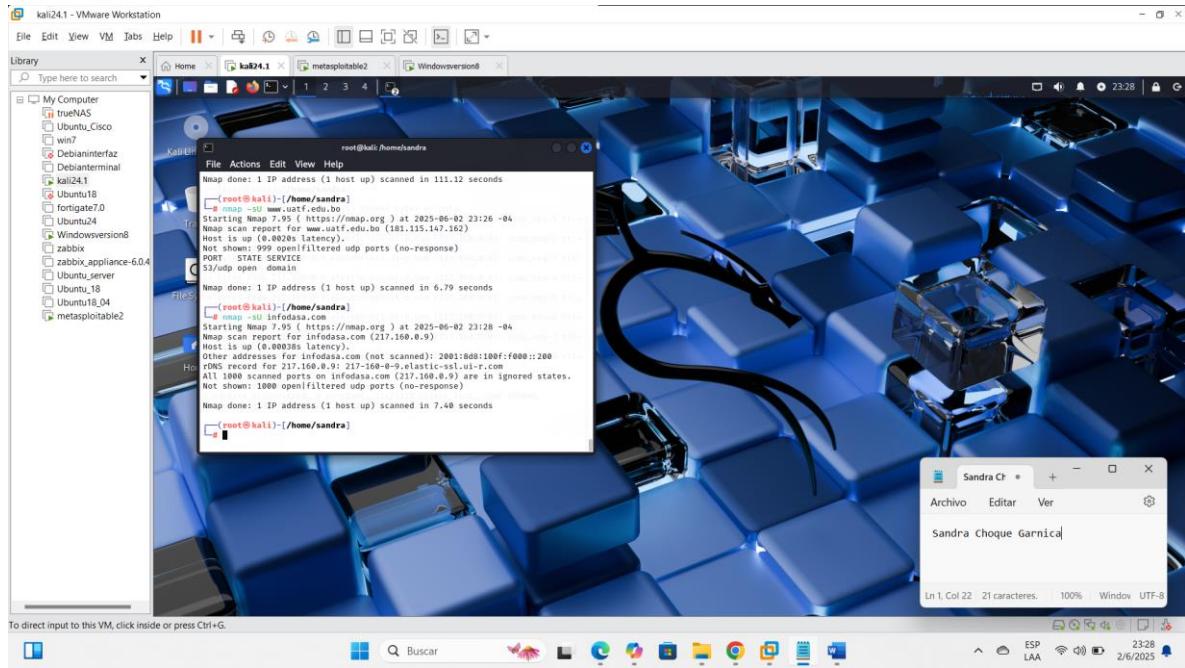
nmap -sT ubielalto.com.bo

The screenshot shows a Kali Linux desktop environment with several windows open. In the foreground, a terminal window titled 'root@sandra' displays two nmap scan reports. The first report is for 'infodasa.com' (217.160.0.9) and the second is for 'ubisalto.com.bo' (198.181.21.110). Both scans show port 80 as open and https as filtered. A Notepad window titled 'Sandra Choque Garnica' is also visible. The desktop background features a blue hexagonal pattern.

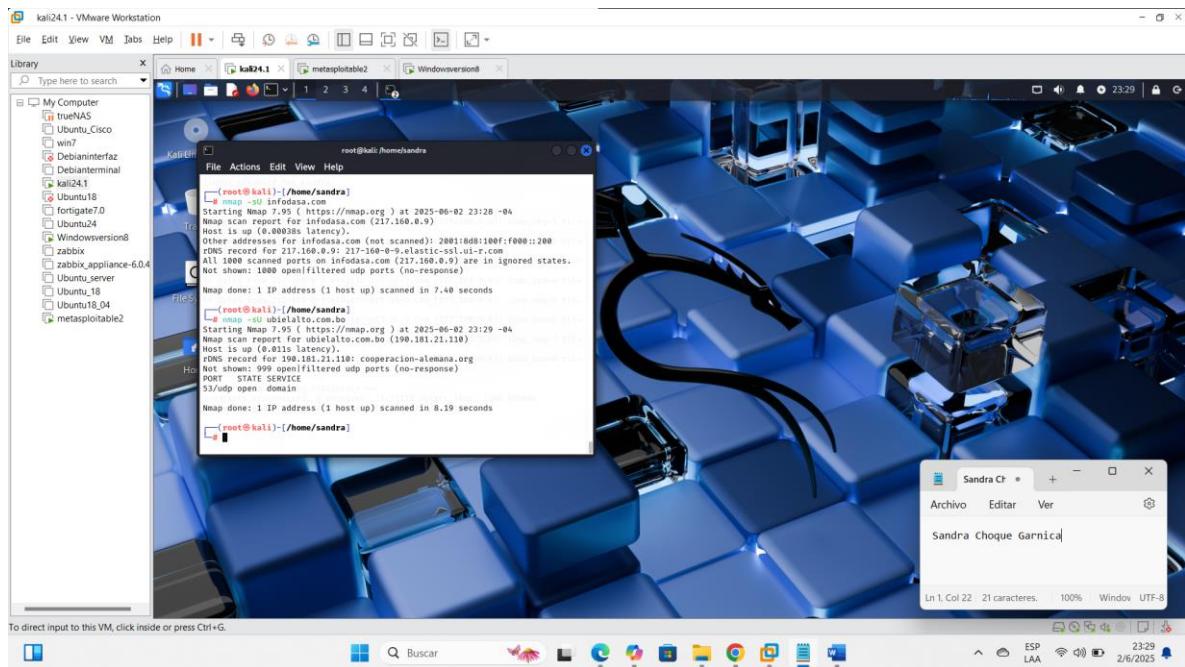
nmap -sU www.uatf.edu.bo

The screenshot shows a Kali Linux desktop environment with several open windows. In the foreground, a terminal window displays the results of an Nmap scan against the IP address 198.181.21.110. The output shows various open ports, including 80/tcp (http), 443/tcp (https), and 53/udp (domain). Another terminal window shows the results of an Nmap scan against the IP address 181.115.147.162, which also lists several open ports. A Notepad window titled 'Sandra' contains the text 'Sandra Choque Garnica'. The desktop background features a blue hexagonal pattern. The taskbar at the bottom includes icons for file operations, search, and system status.

```
nmap -sU infodasa.com
```



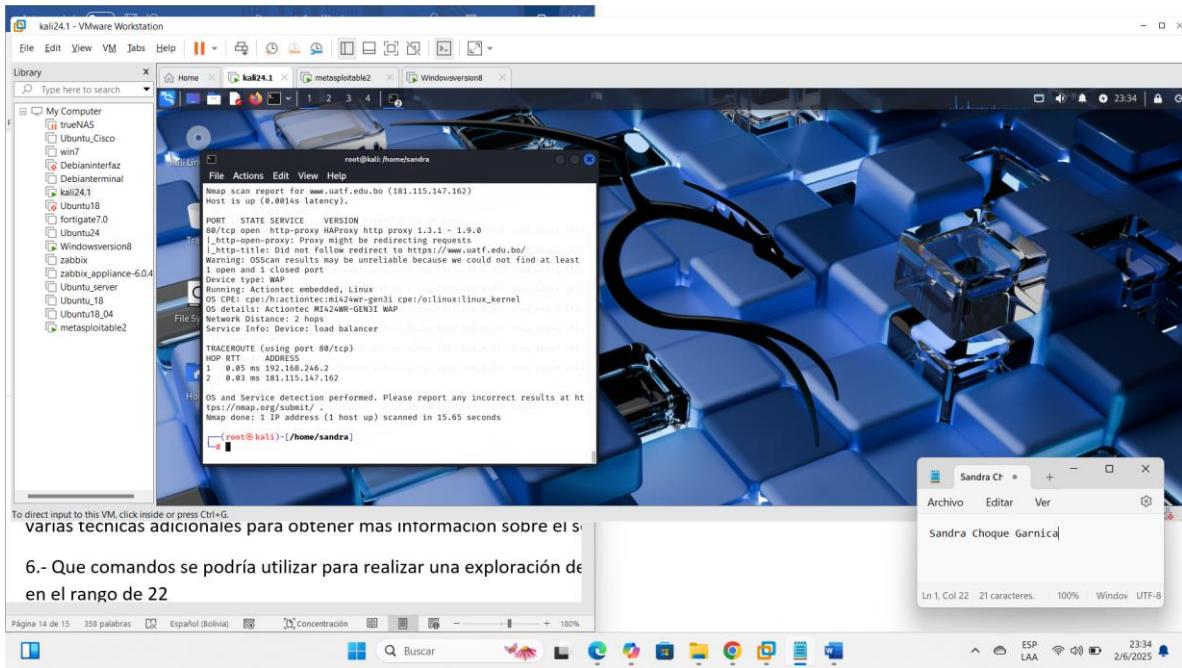
nmap -sU ubielalto.com.bo



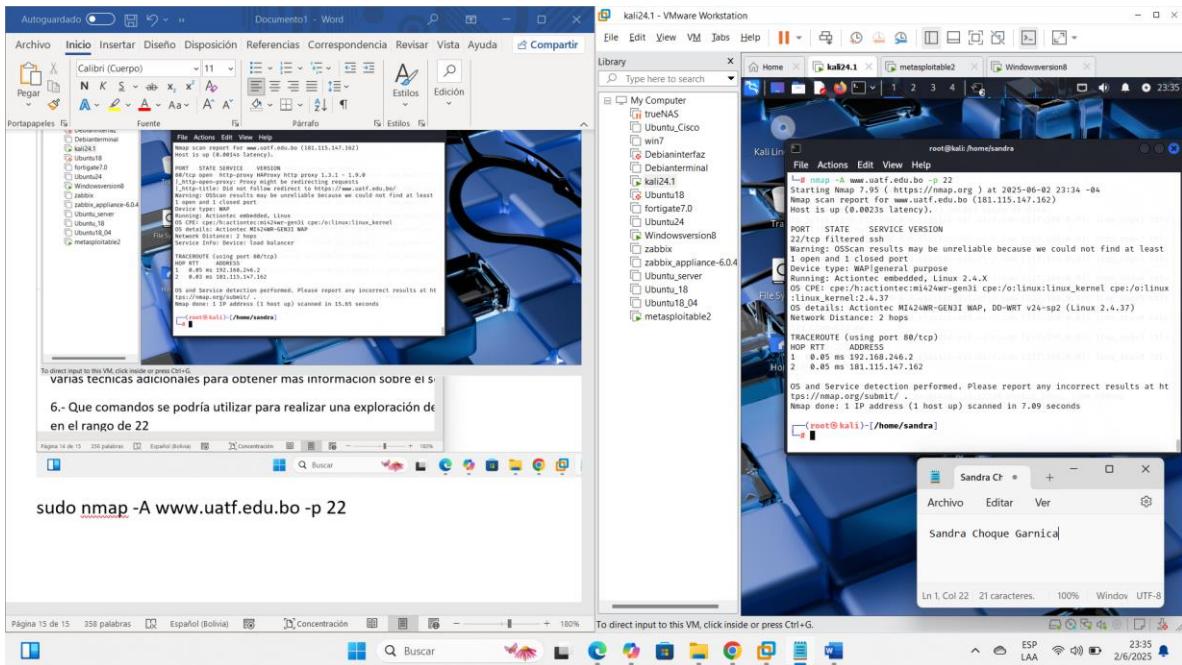
5.- Utilice la variación del comando: nmap -A dominio -p 80

nmap -A dominio -p 22

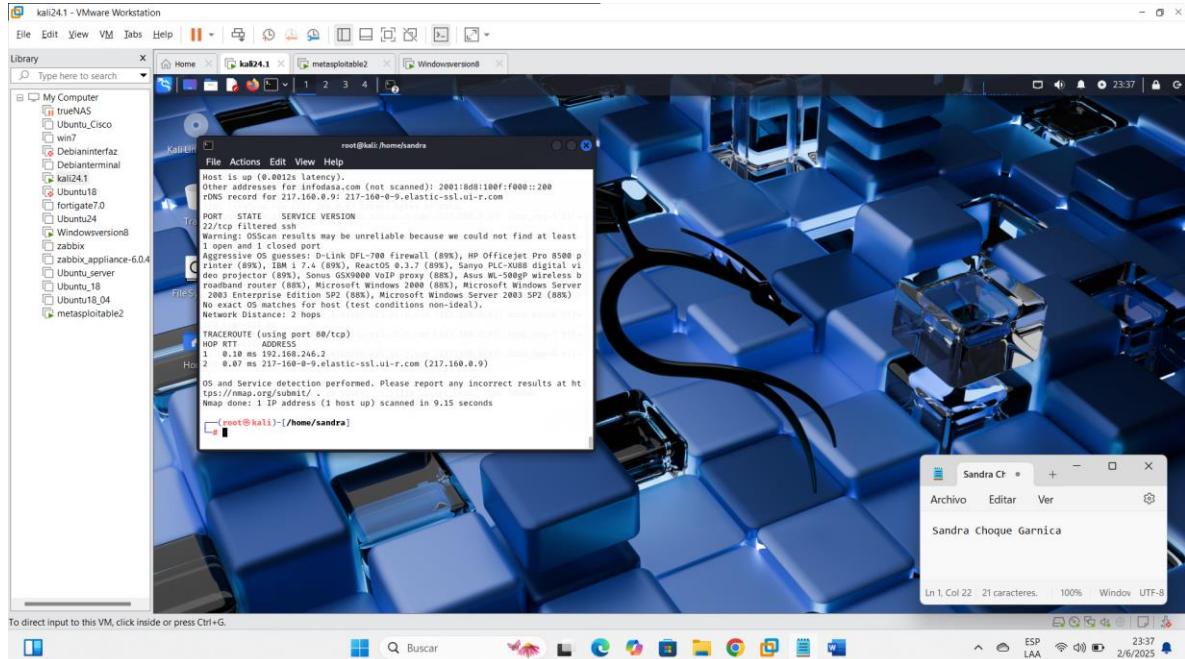
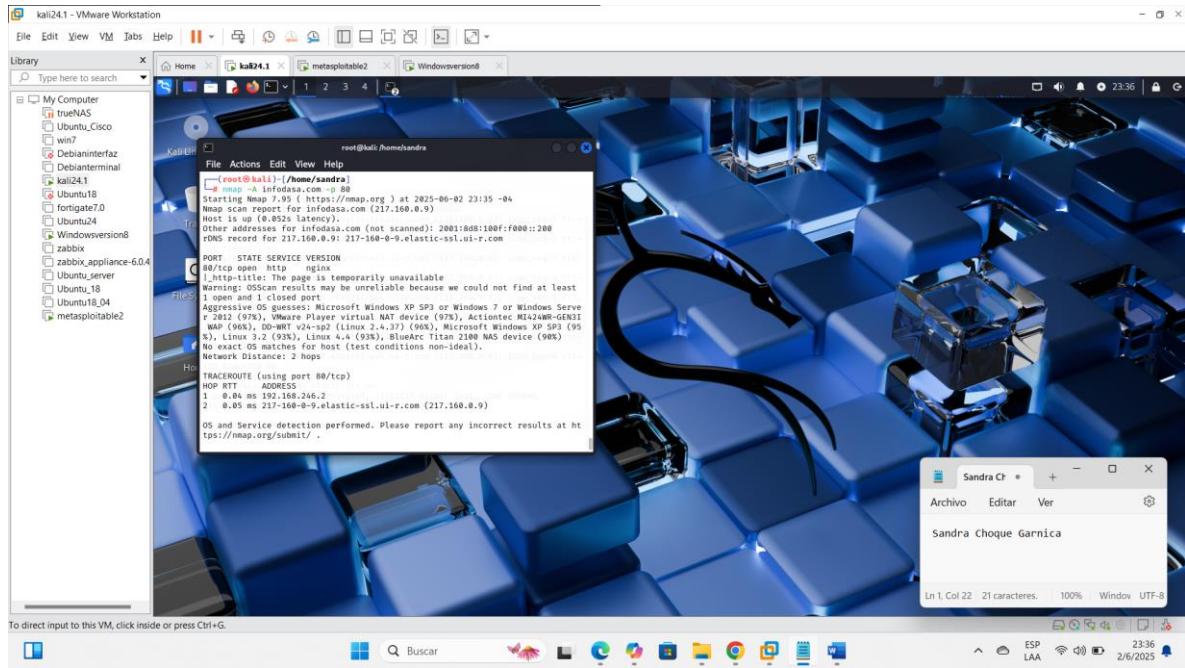
sudo nmap -A www.uatf.edu.bo -p 80



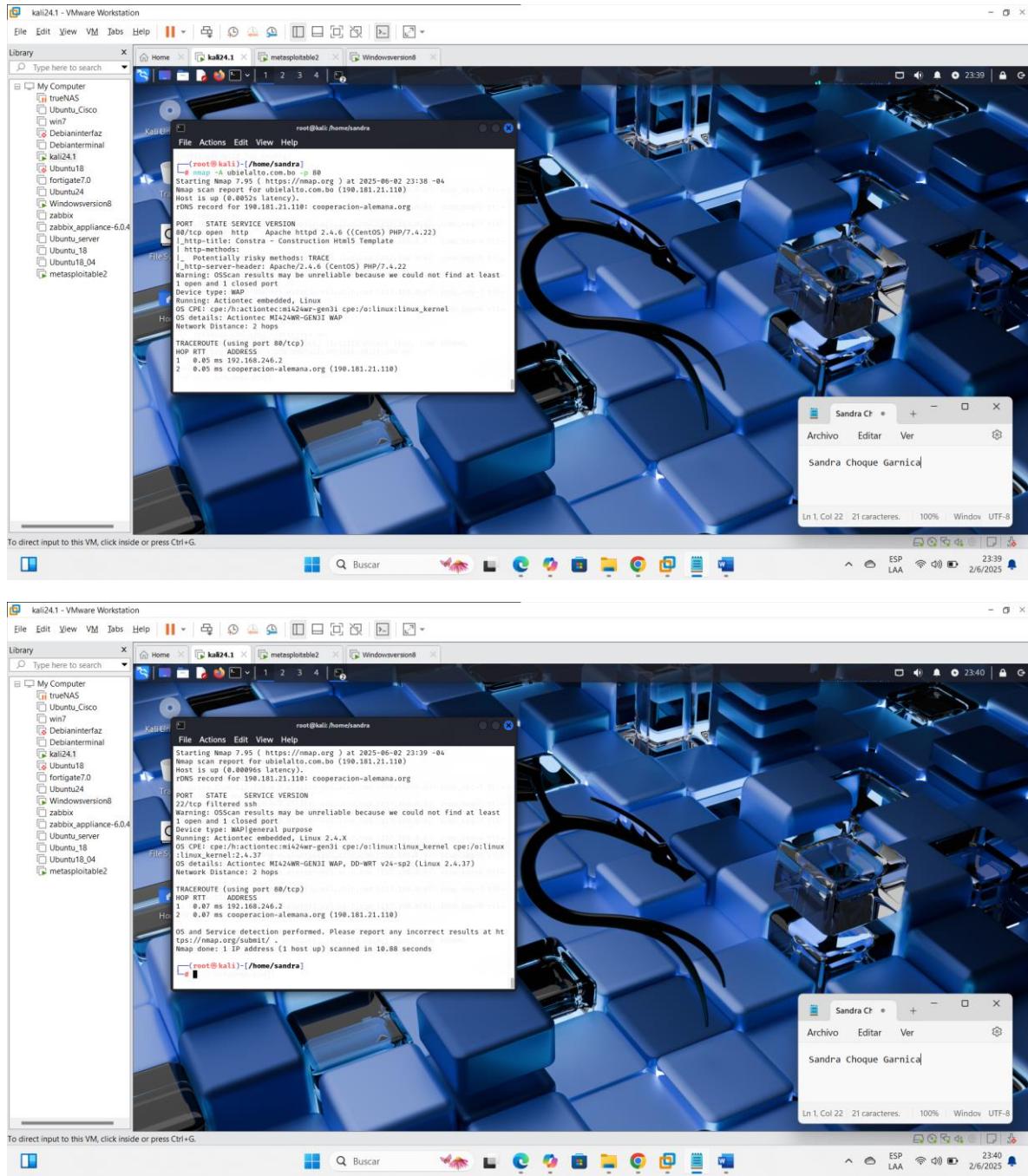
`sudo nmap -A www.uatf.edu.bo -p 22`



Infodasa



Ubielalto



¿Qué tipo de escaneo significa la letra A?

La opción **-A** en Nmap **activa el modo de escaneo avanzado o "agresivo"**. Este escaneo incluye varias técnicas adicionales para obtener más información sobre el servidor.

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.

Puertos TCP

-uutf

kali24.1 - VMware Workstation

File Edit View VM Tabs Help

Library Type here to search

My Computer

- trueNAS
- Ubuntu_Cisco
- win7
- Debianinterfaz
- Debianterminal
- kali24.1
- Ubuntu18
- fortigate7.0
- Ubuntu24
- Windowsversion8
- zabbix
- zabbix_appliance-6.0.4
- Ubuntu_server
- Ubuntu18
- Ubuntu18.04
- metasploitable2

File Actions Edit View Help

```
linus_kernel:2.4.37
OS details: Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37)
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
 1  0.07 ms 192.168.246.2
 2  0.07 ms cooperation-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 10.88 seconds
```

(root@kali)-[~/home/sandra]

To direct input to this VM, click inside or press Ctrl+G.

Sandra Choque Garnica

Ln 1, Col 22 21 caracteres. 100% Window UTF-8

Página 18 de 18 370 palabras Español (Bolivia)

Buscar Buscar

Concentración

ESP LAA 23:45 2/6/2025

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

-infodasa

kali24.1 - VMware Workstation

File Edit View VM Tabs Help

Library Type here to search

My Computer

- trueNAS
- Ubuntu_Cisco
- win7
- Debianinterfaz
- Debianterminal
- kali24.1
- Ubuntu18
- fortigate7.0
- Ubuntu24
- Windowsversion8
- zabbix
- zabbix_appliance-6.0.4
- Ubuntu_server
- Ubuntu18
- Ubuntu18.04
- metasploitable2

File Actions Edit View Help

```
lens -S www.uestf.edu.bo -p 22-1024
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-02 23:43 -04
Host is up (0.0004s latency).
Not shown: 1001 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 96.87 seconds
```

(root@kali)-[~/home/sandra]

To direct input to this VM, click inside or press Ctrl+G.

Sandra Choque Garnica

Ln 1, Col 22 21 caracteres. 100% Window UTF-8

Página 18 de 18 370 palabras Español (Bolivia)

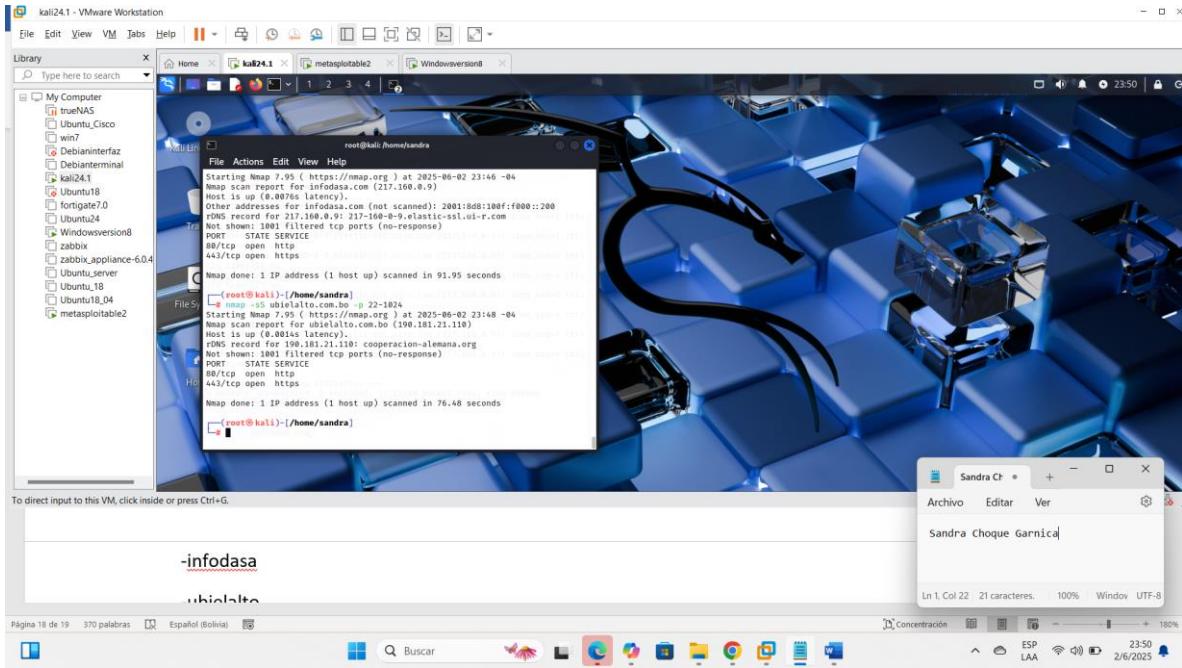
Buscar Buscar

Concentración

ESP LAA 23:47 2/6/2025

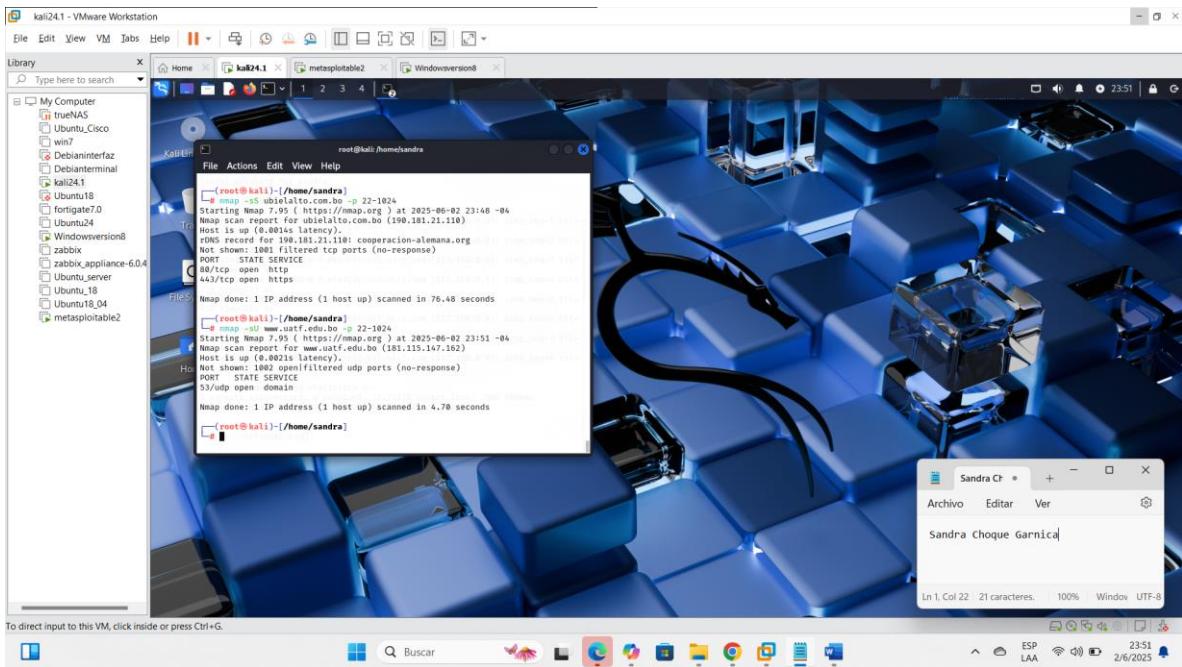
-ubielalto

-ubielalto

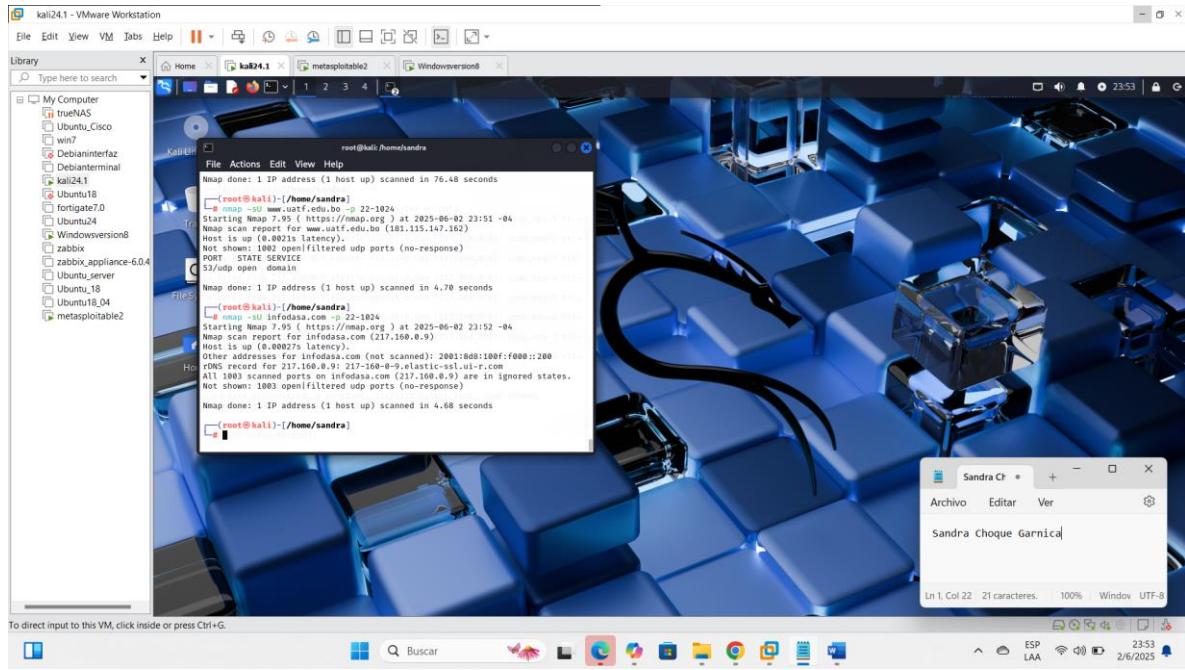


Puertos UDP

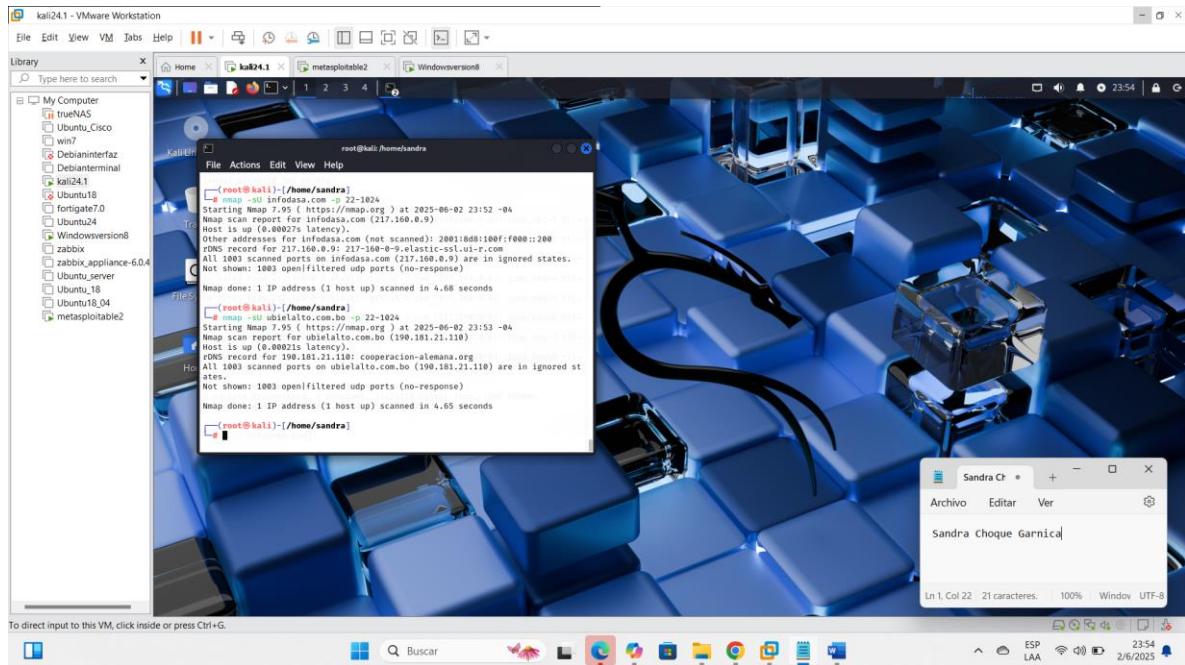
-uatf



-infodasa



-ubielalto



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

R.- sudo nmap --script=firewall www.uatf.edu.bo

Si sospechas que hay un firewall filtrando respuestas, puedes usar este comando