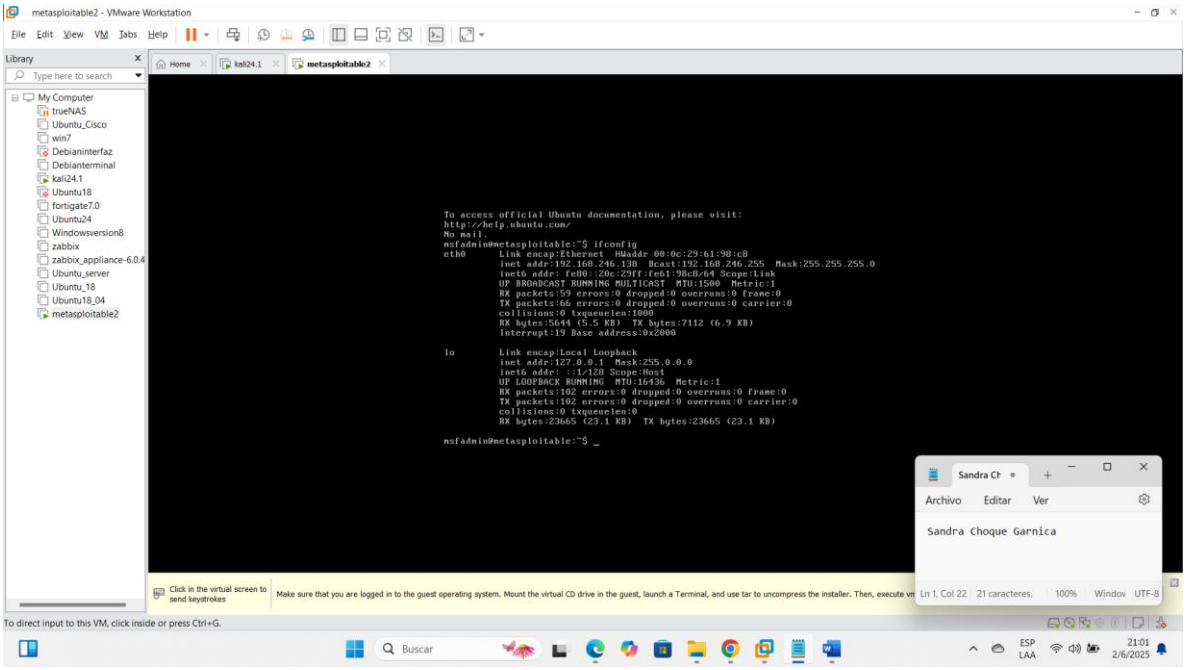
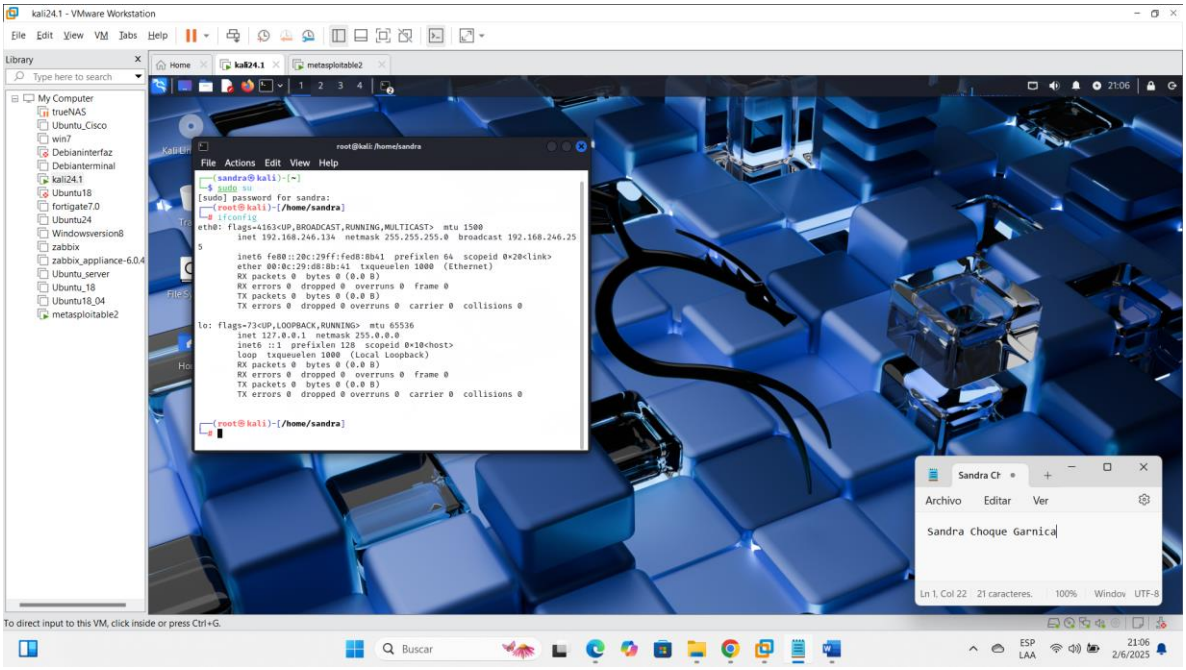
NOMBRE:SANDRA CHOQUE GARNICA

LAB 11 NMAP

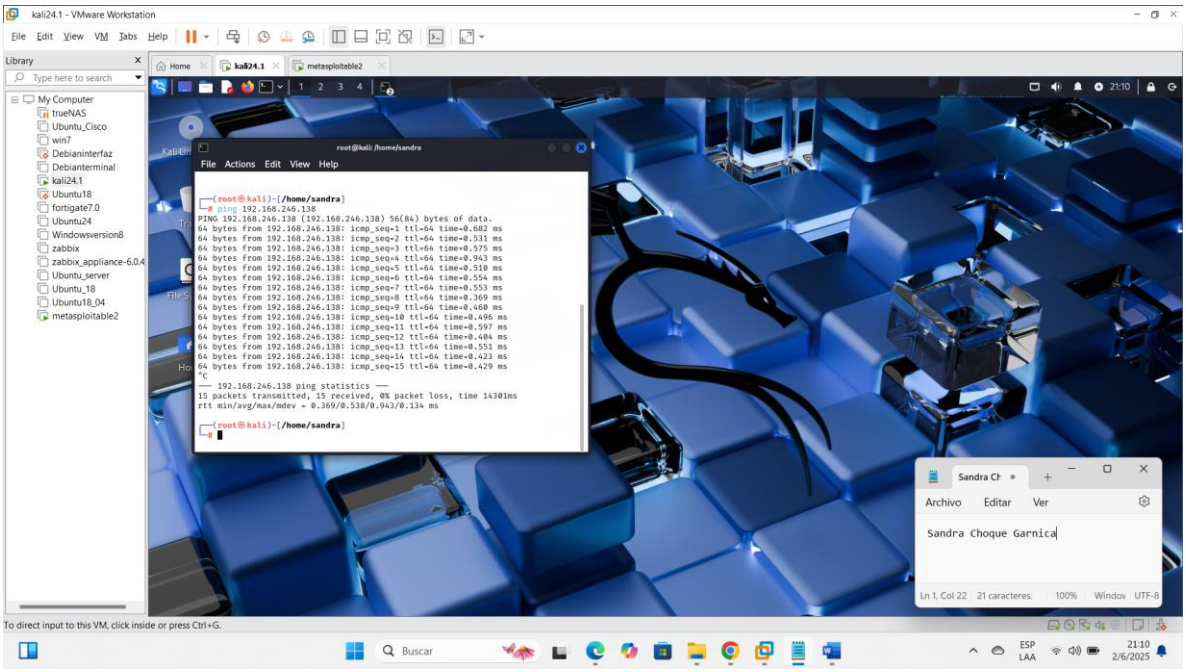
Ip de metasploit



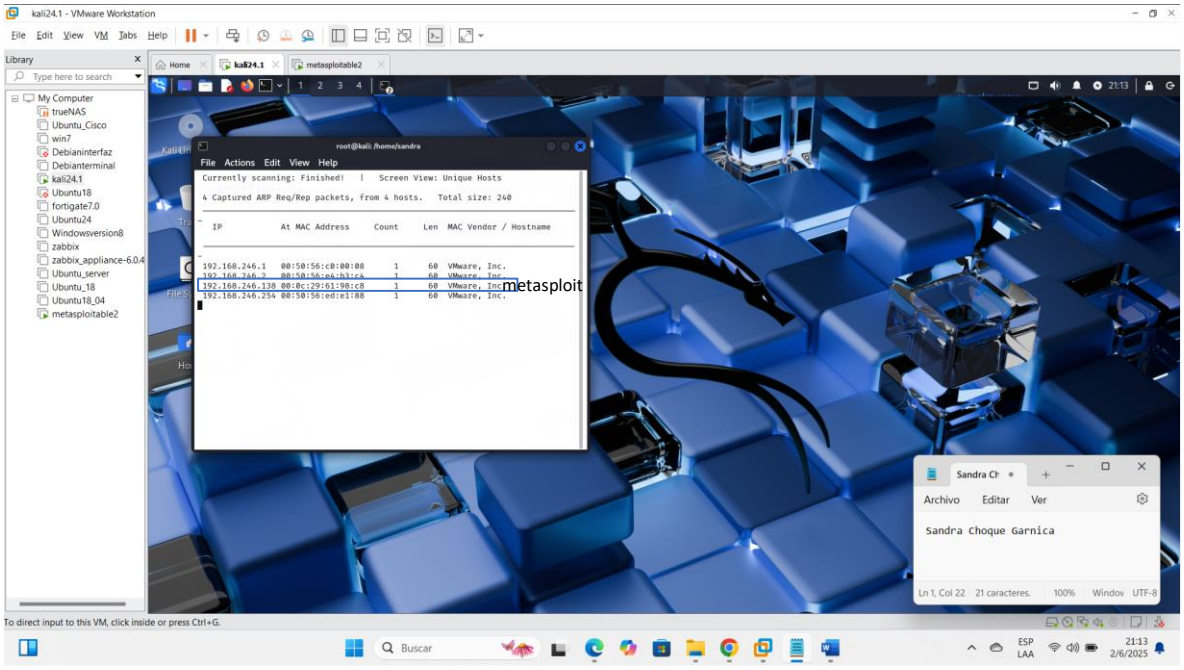
Ip de Kali



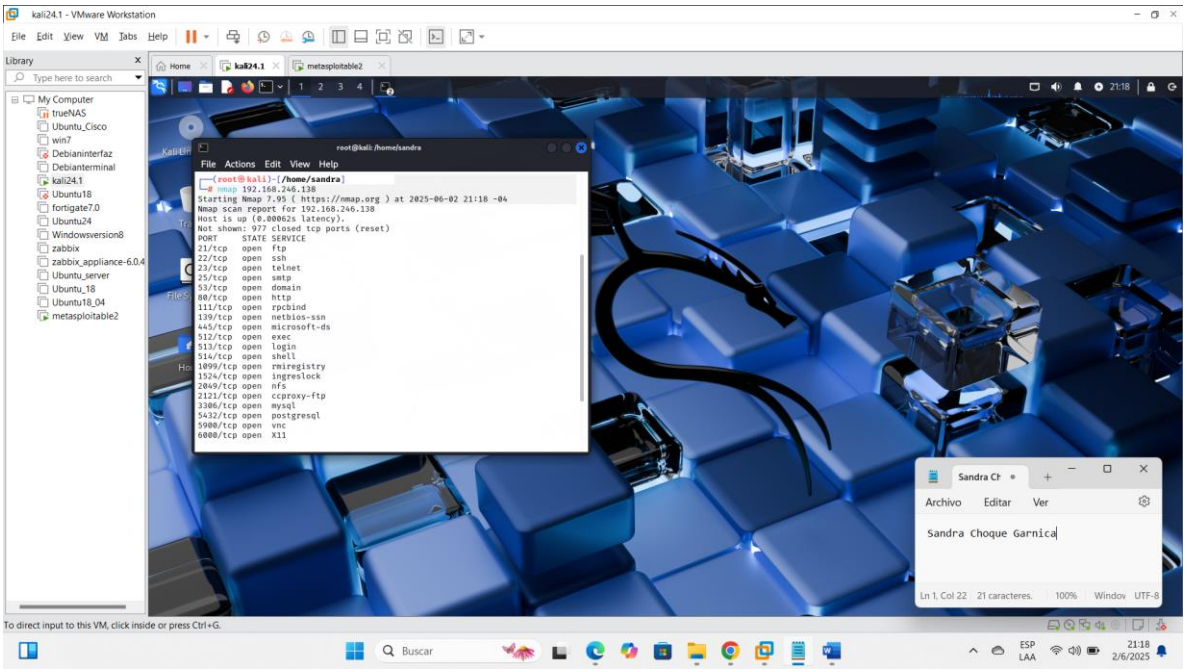
-ping de Kali a metasploit



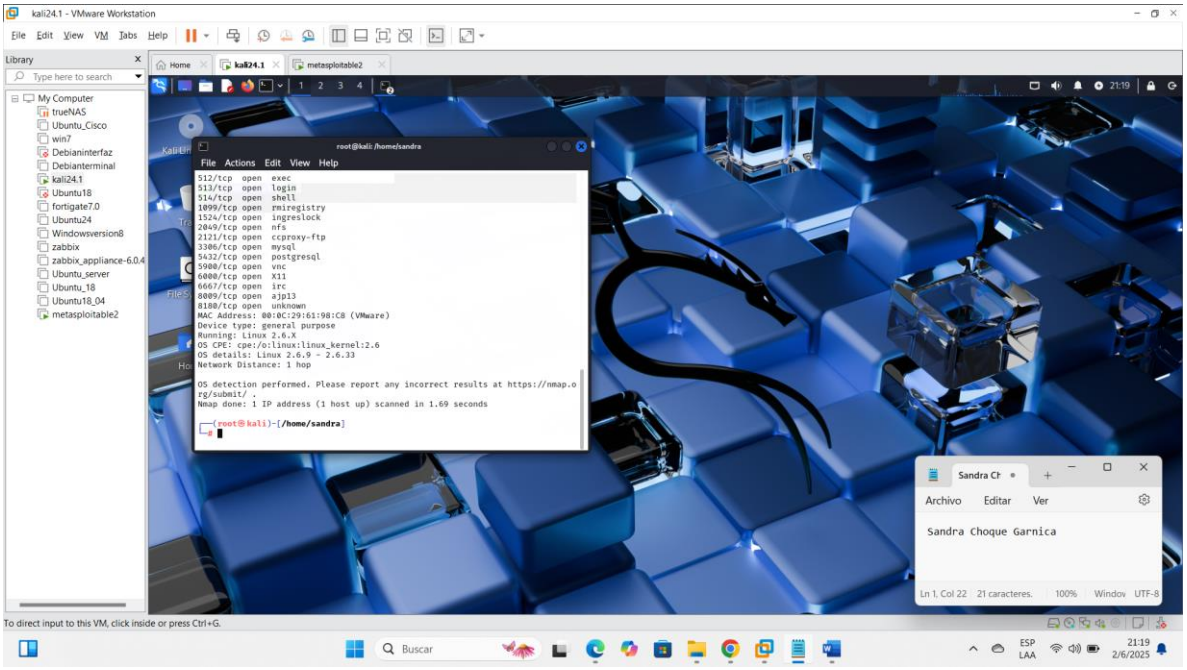
Identificar ip en la misma red



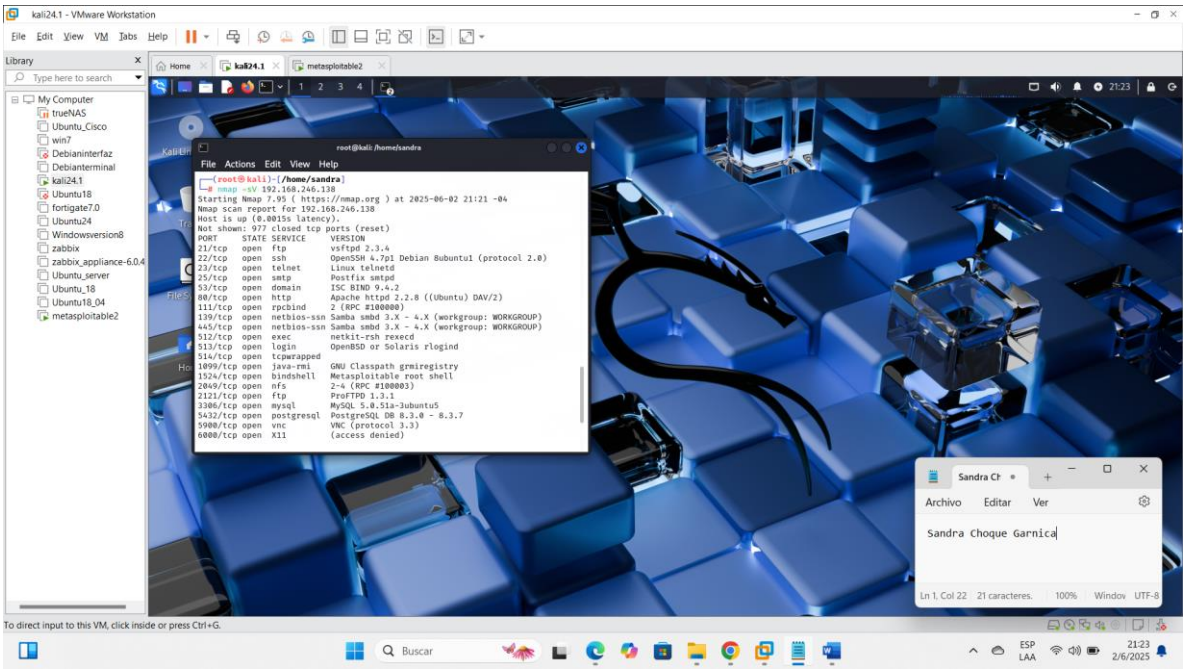
Nmap



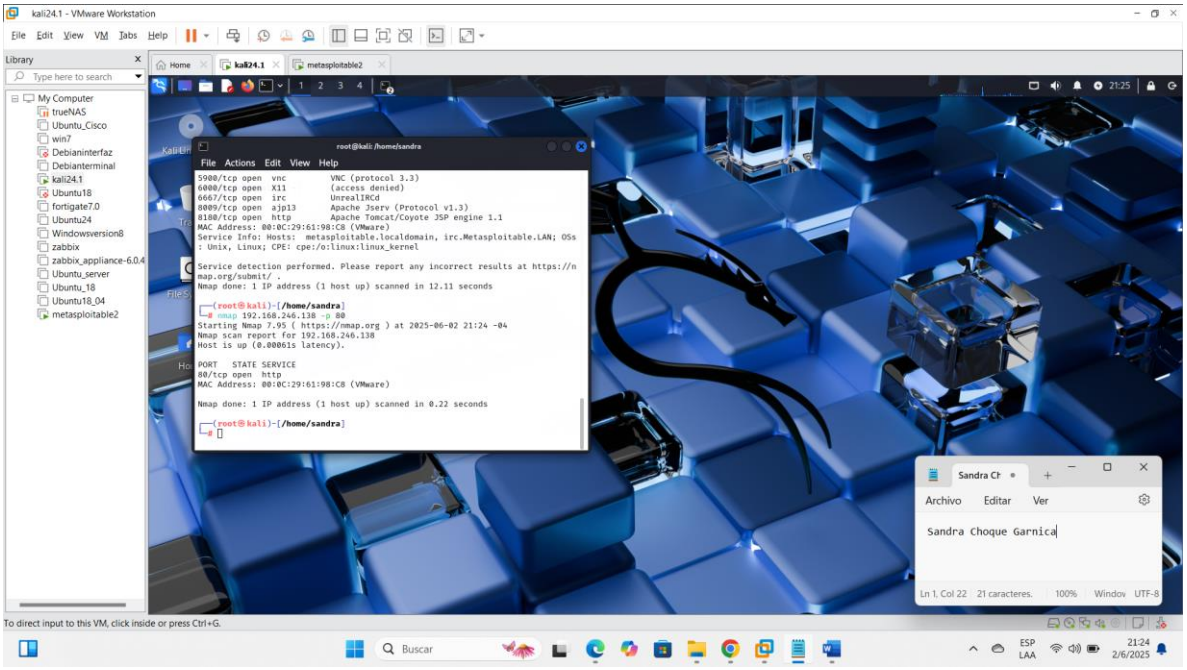
-distribución en linux



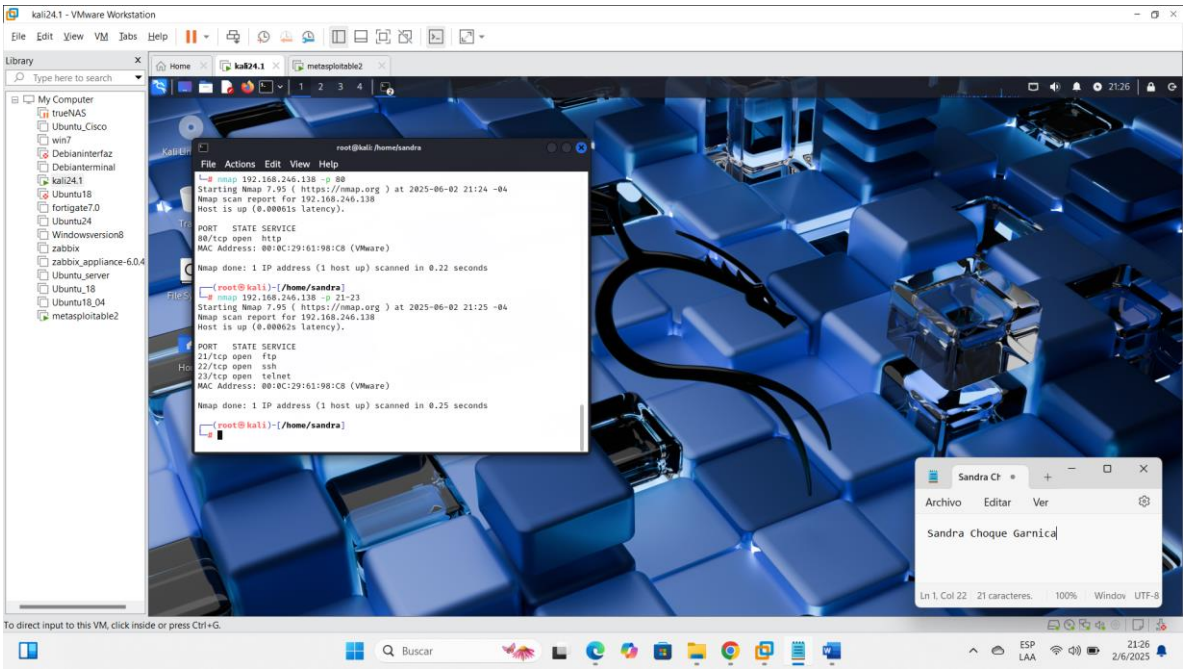
-las versiones que utilizan



-escaneo del puerto 80

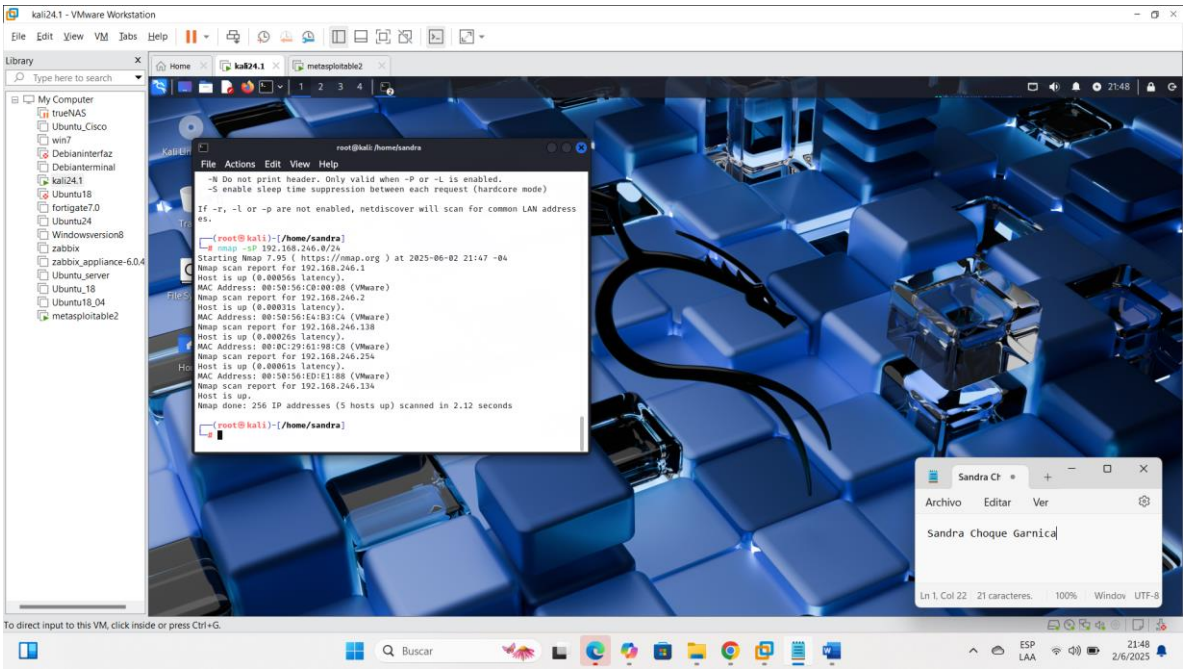


-rango de puertos



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?

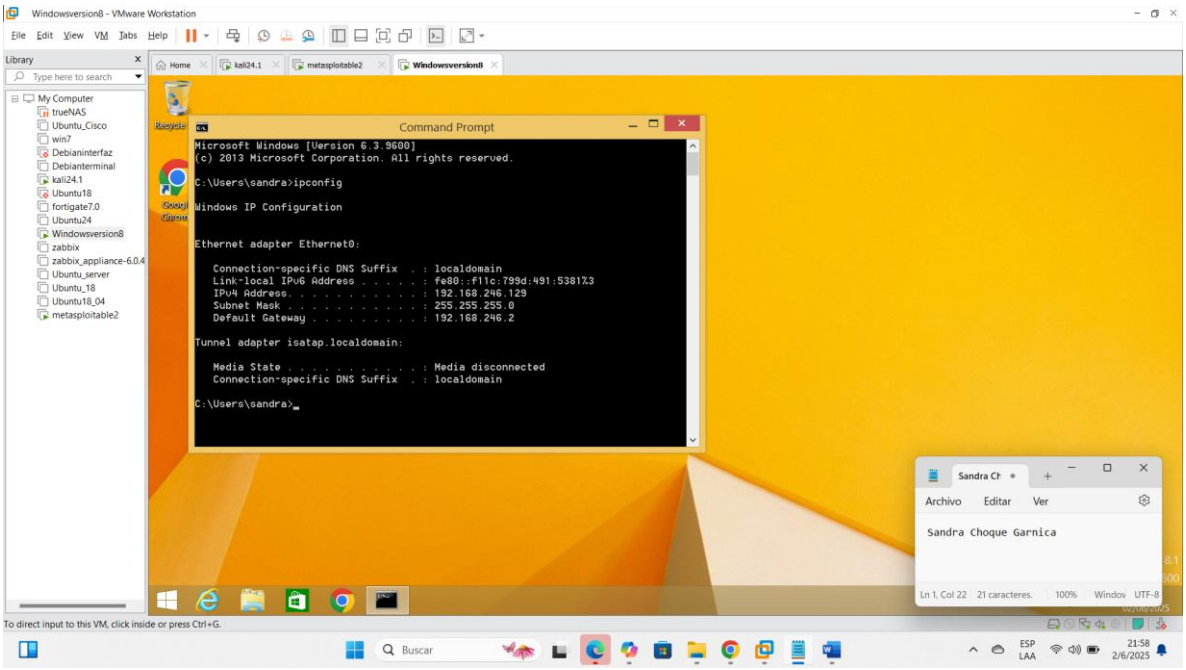
Nmap mostrará una lista de los dispositivos en la red que han respondido al escaneo de ping. Esto significa que los dispositivos `192.168.246.1` y

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

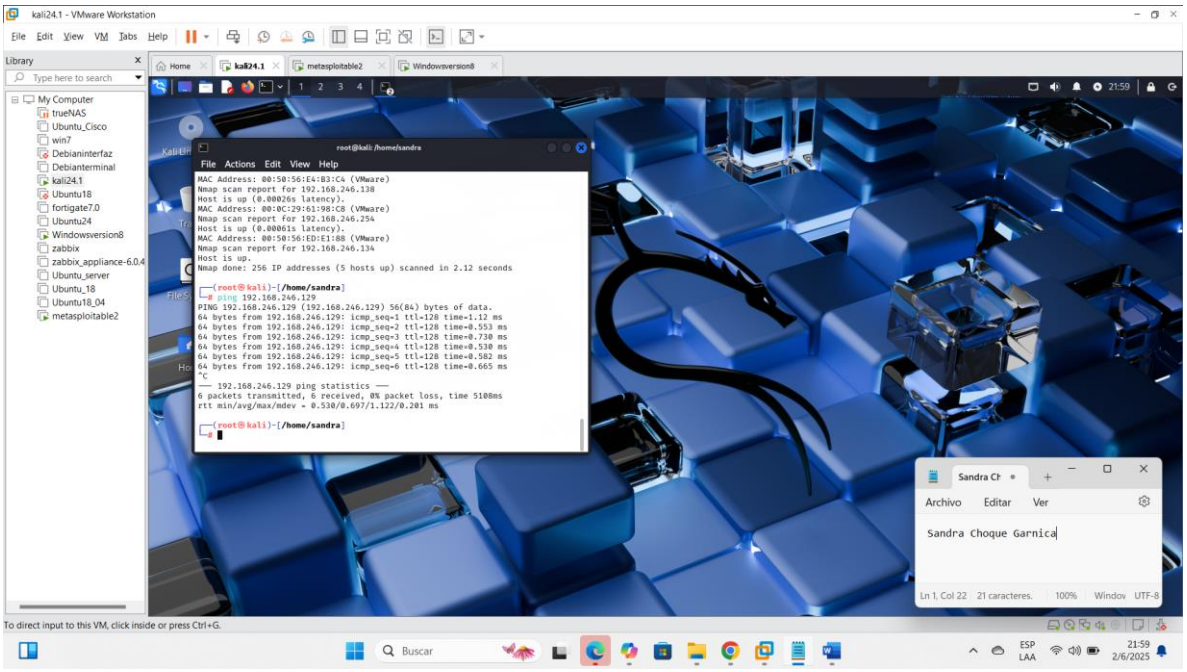
2.- Realice un escaneo para determinar los puertos abiertos en la máquina virtual Windows 7 o Windows XP (Asegúrese que

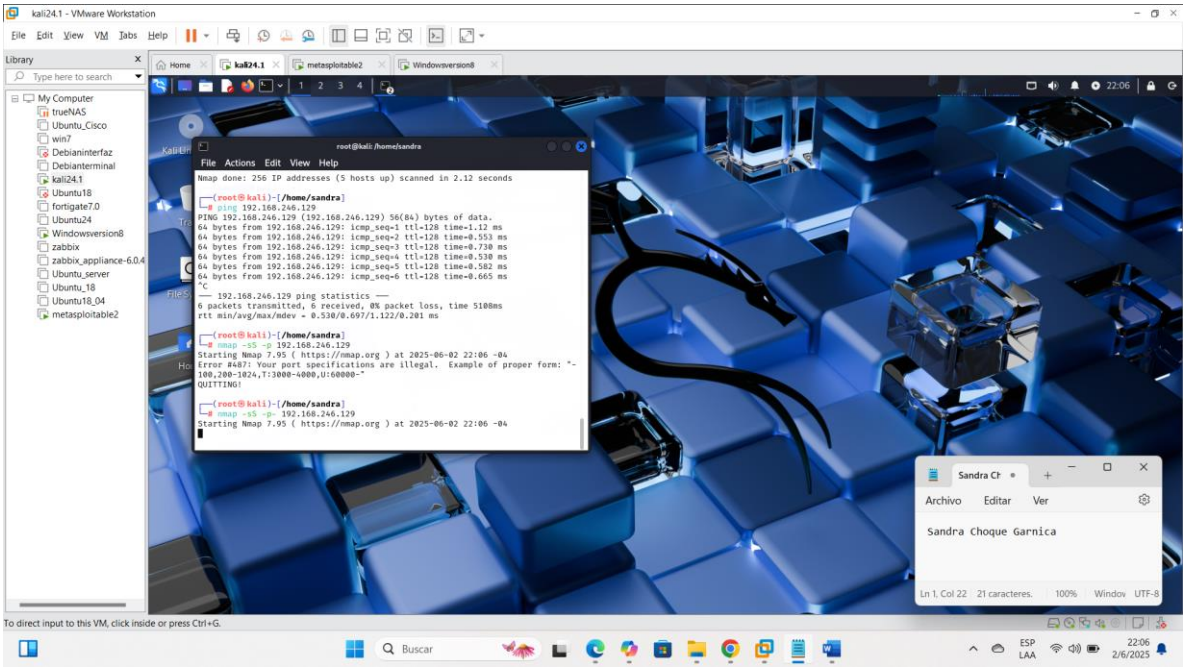
este en el mismo segmento de red que Kali). De no contar con esas: W7 ni XP, utilice otra máquina o realice el escaneo a su

-ip windows 8

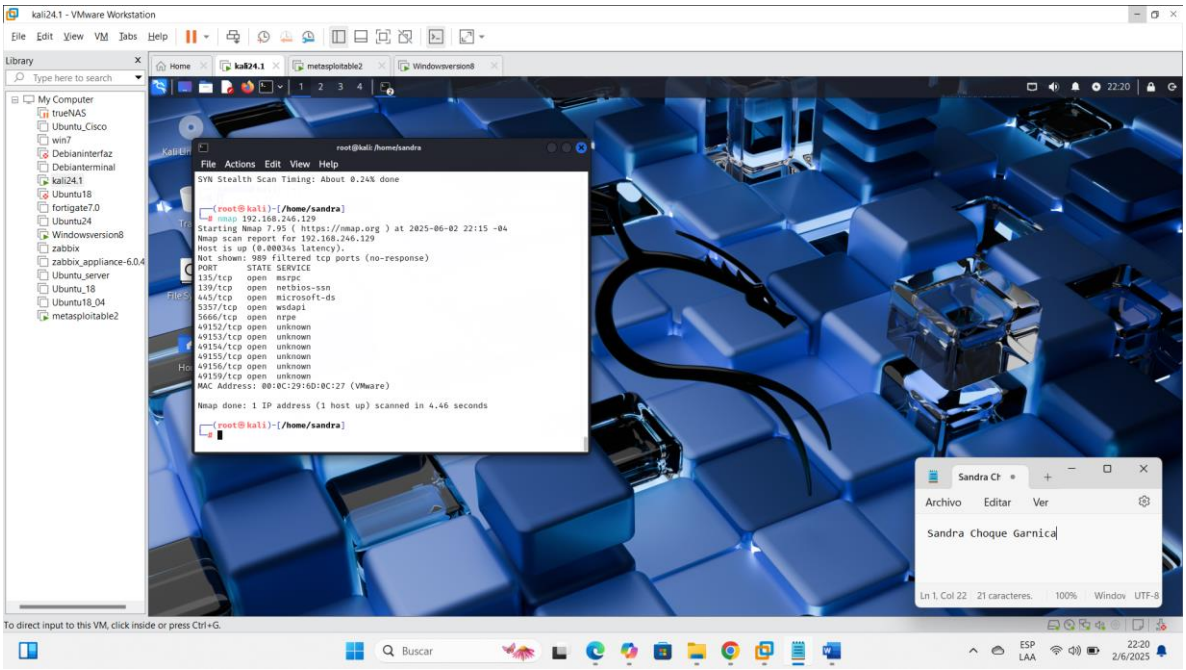


-ping de Kali a Windows





propia PC física. ¿Qué puertos están abiertos?



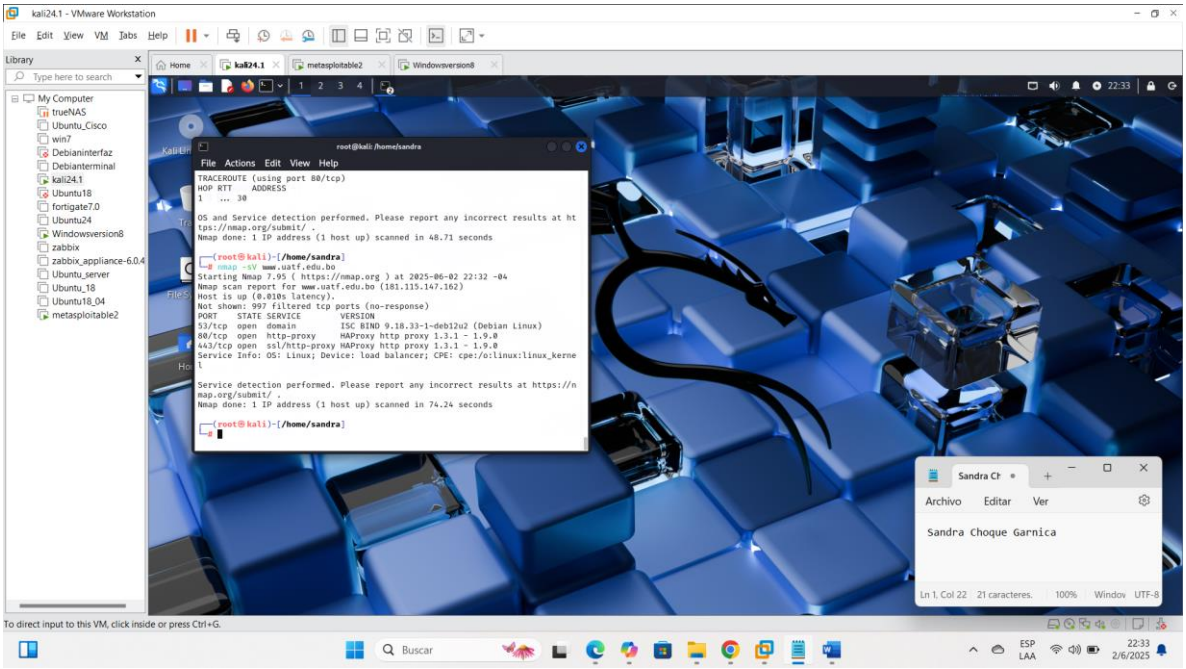
3.- REQUIERE EL USO DE INTERNET

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

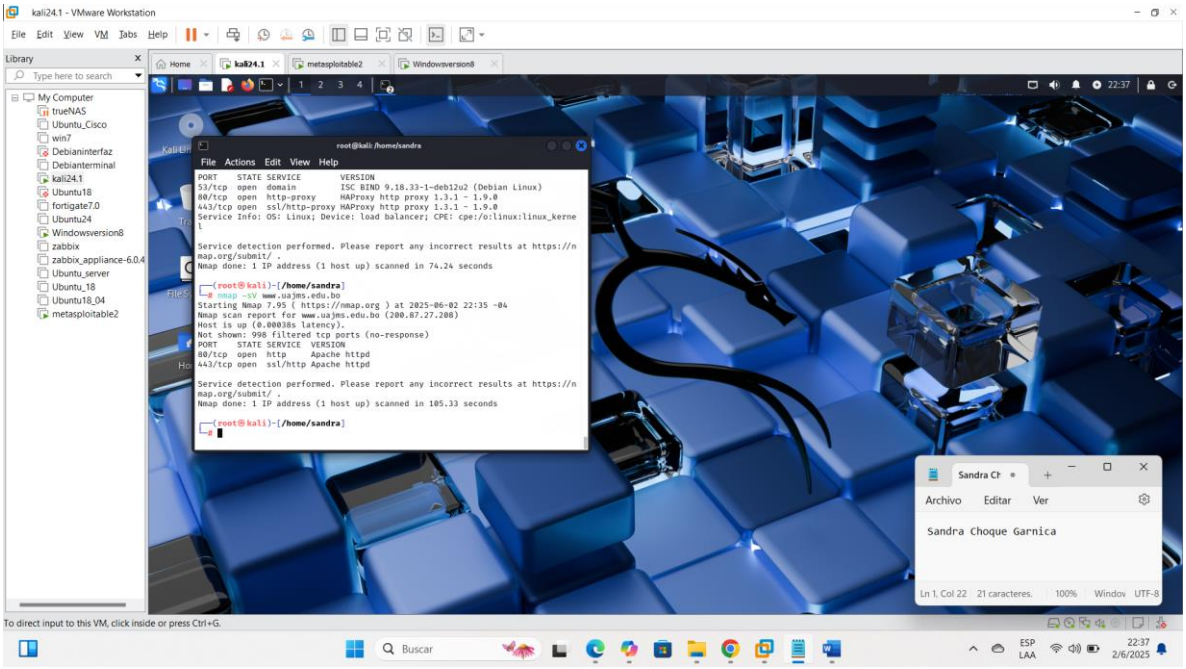
¿Qué comandos utilizó?

Servicios y version

#nmap -sV www.uatf.edu.bo

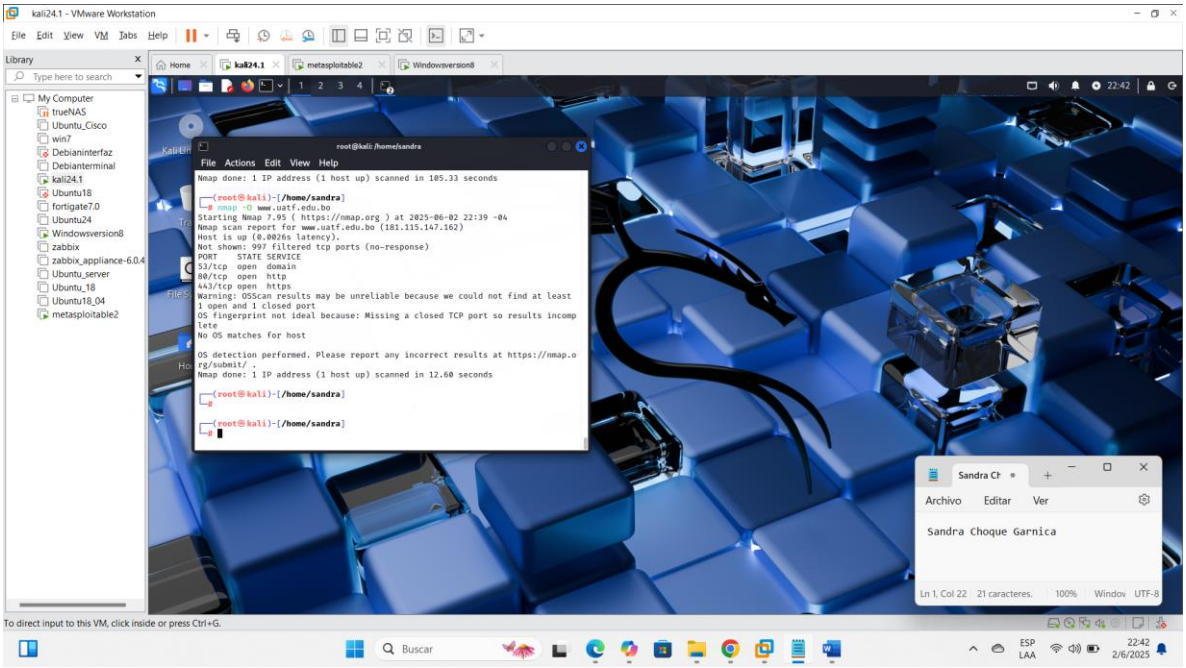


#nmap -sV www.uajms.edu.bo

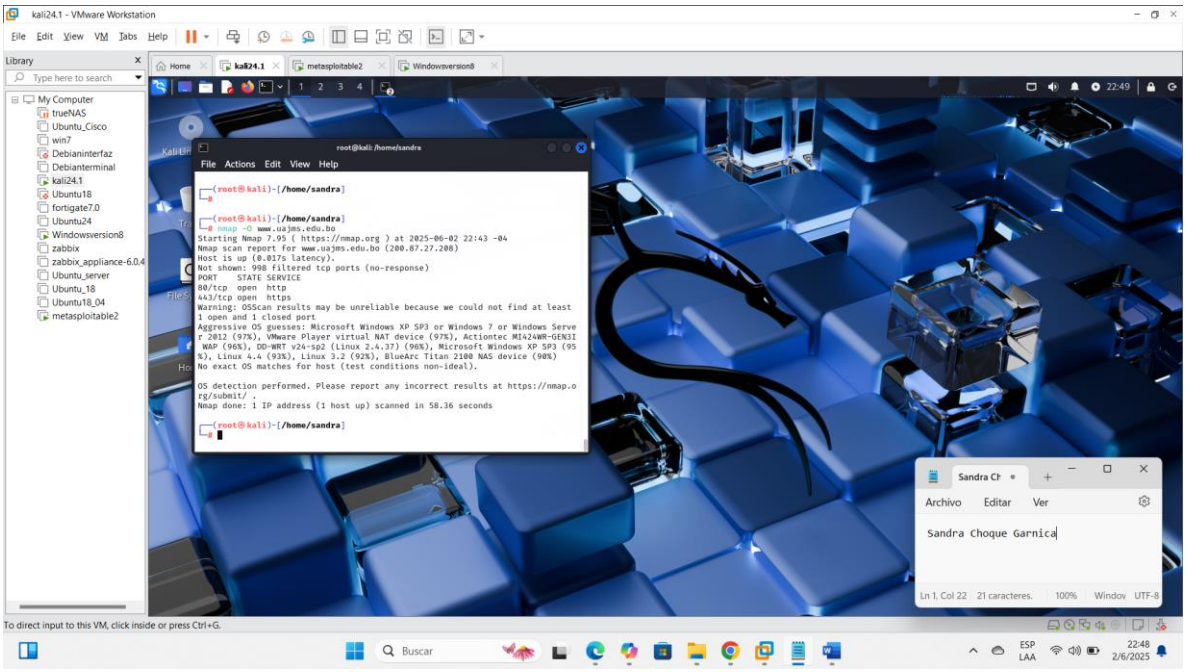


SISTEMA OPERATIVO

#nmap -O www.uatf.edu.bo



#nmap -O www.uajms.edu.bo



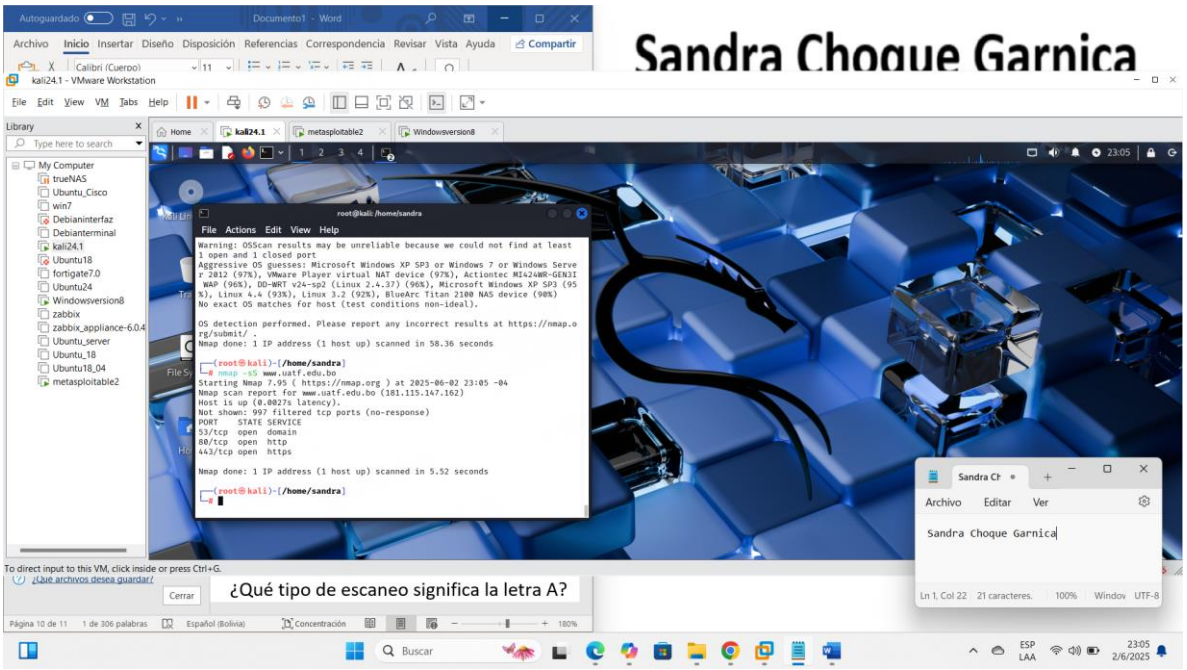
4.- Utilice las siguientes variaciones del comando nmap. El dominio será: https://www.uatf.edu.bo/

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

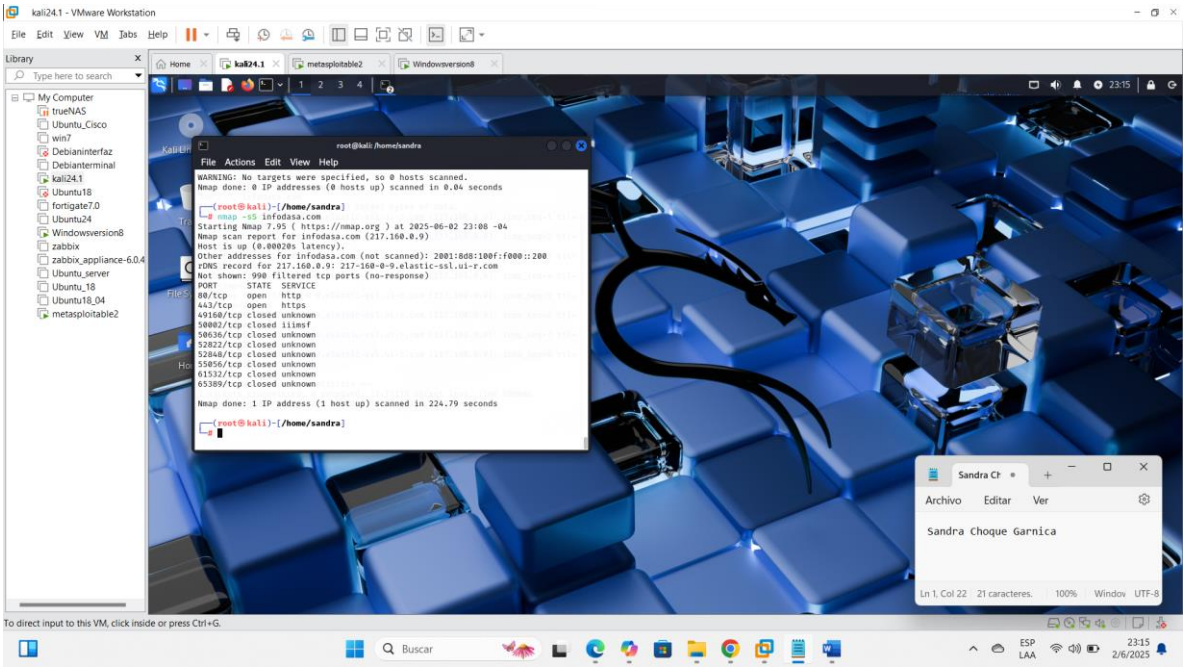
y http://ubielalto.com.bo/moodle/login/index.php

Para explicar las diferencias entre cada comando.

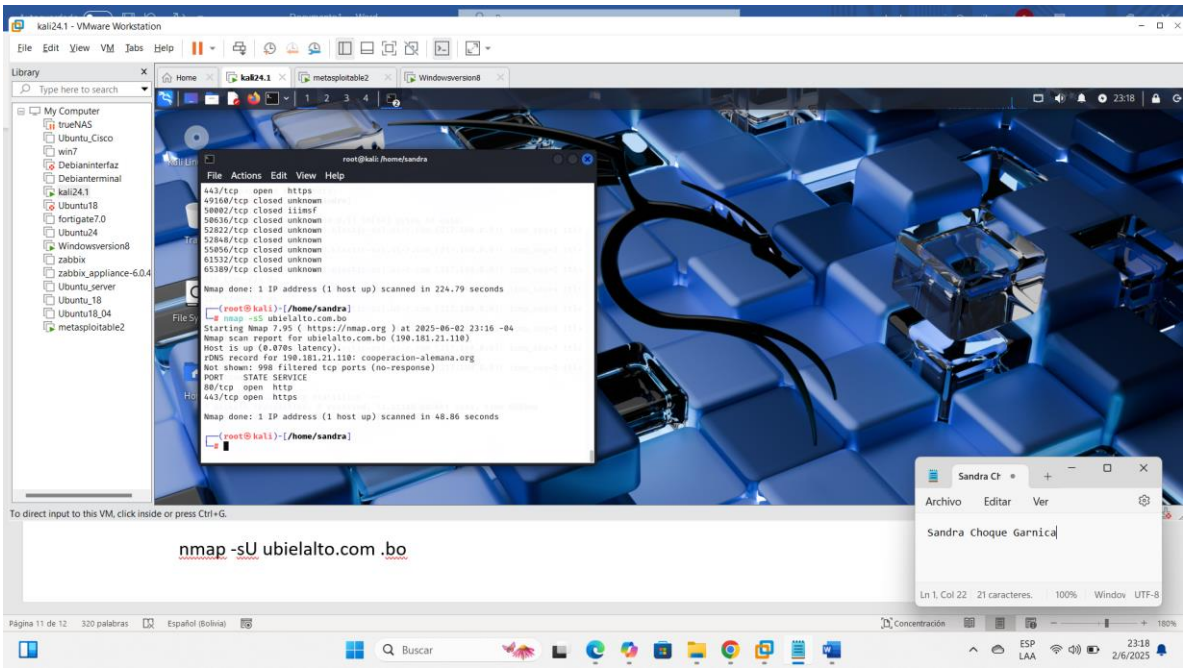
-nmap -sS www.uatf.edu.bo



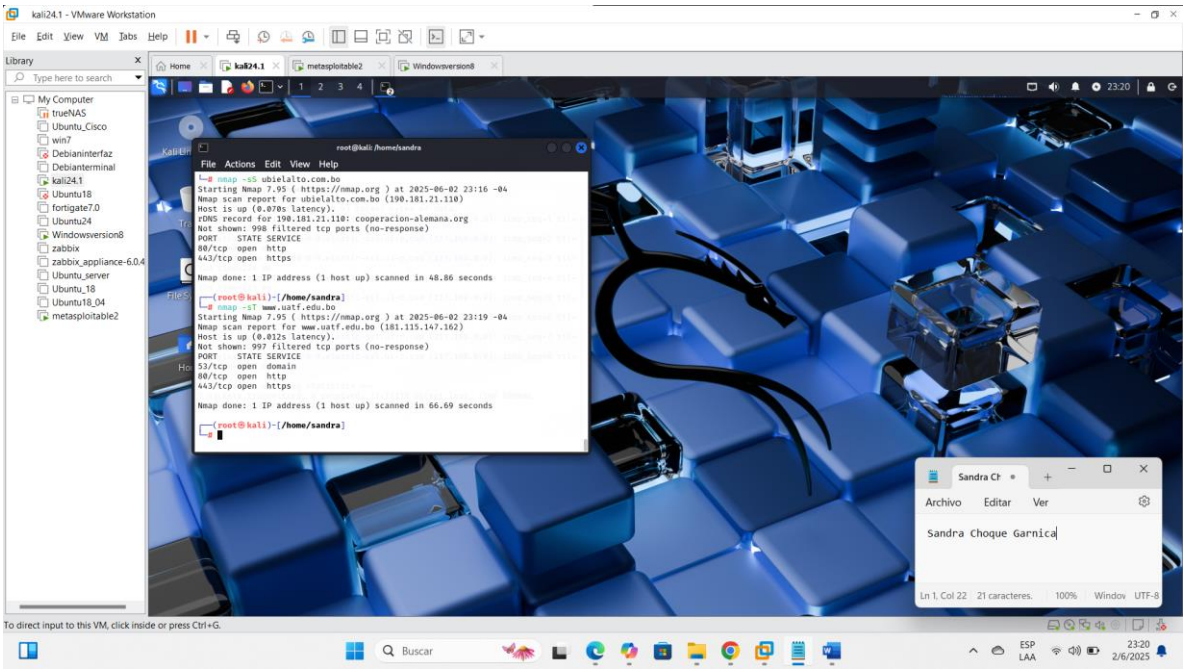
nmap -sS infodasa.com



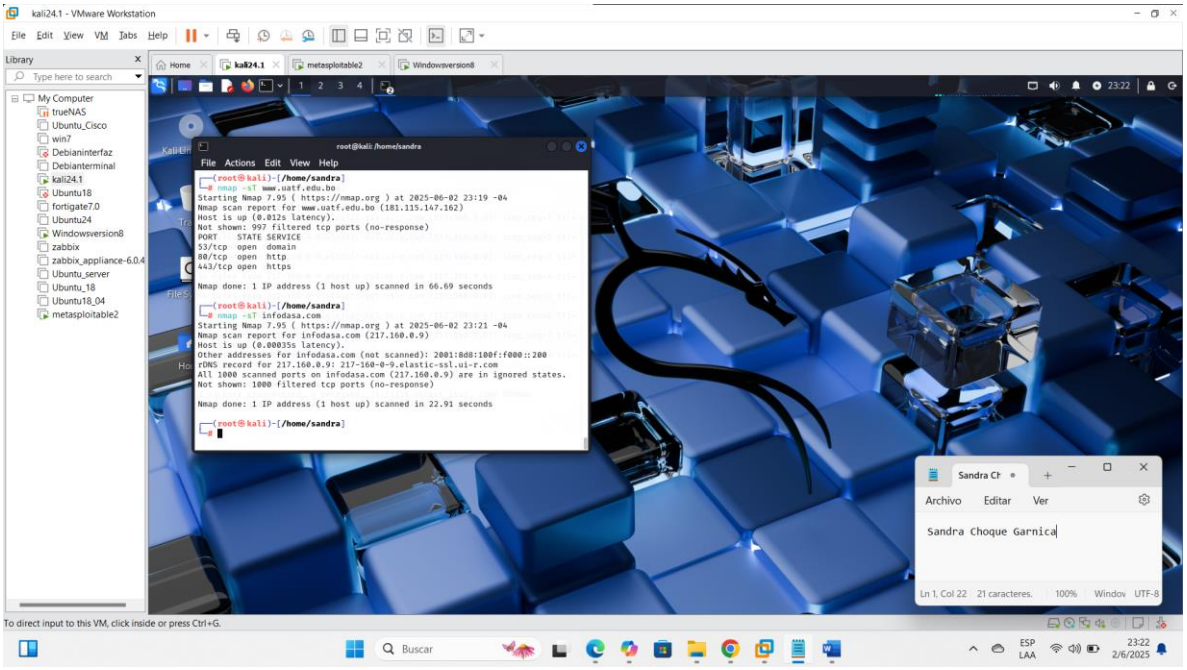
nmap -sS ubielalto.com.bo



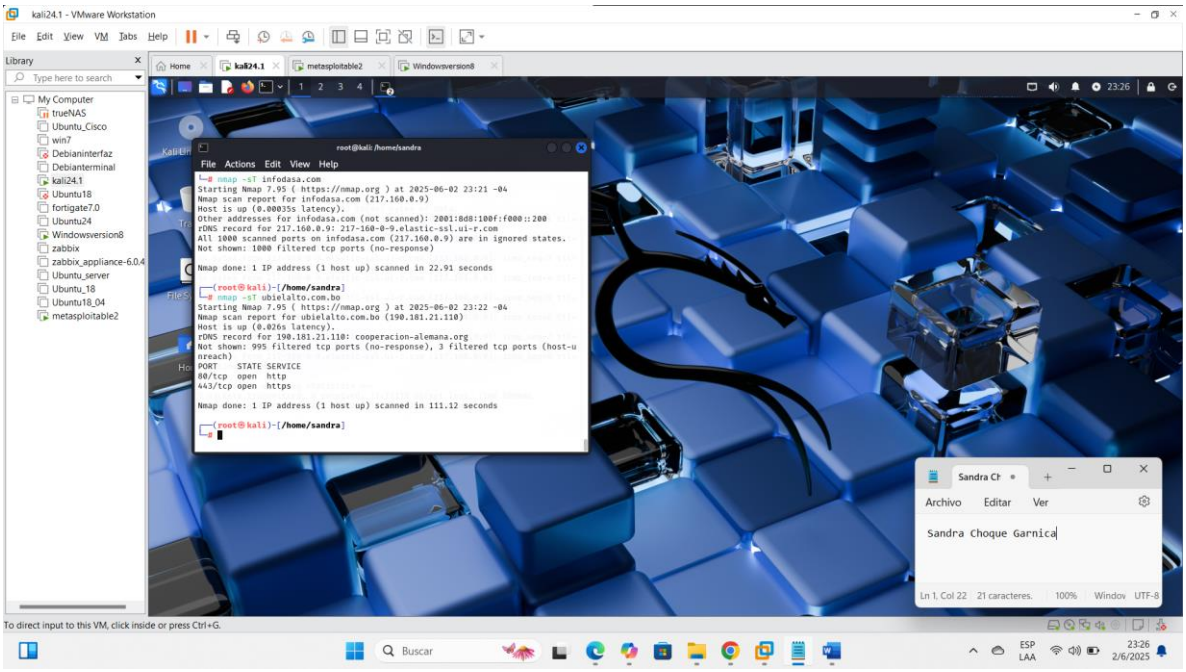
nmap -sT www.uatf.edu.bo



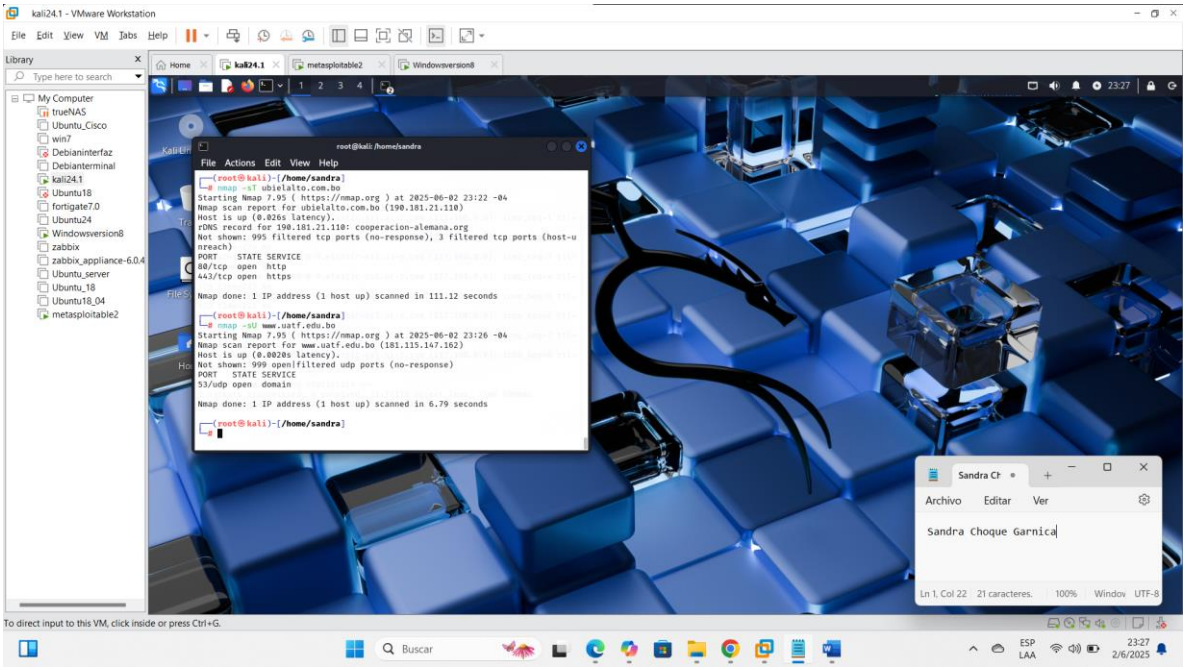
nmap -sT infodasa.com



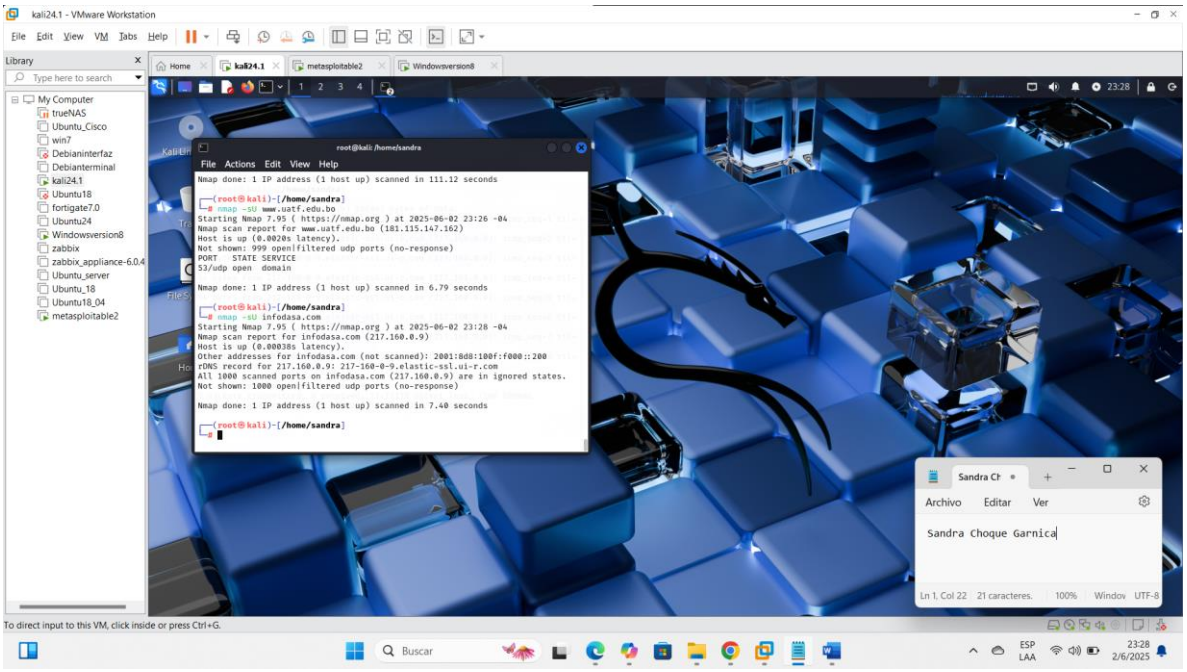
nmap -sT ubielalto.com .bo



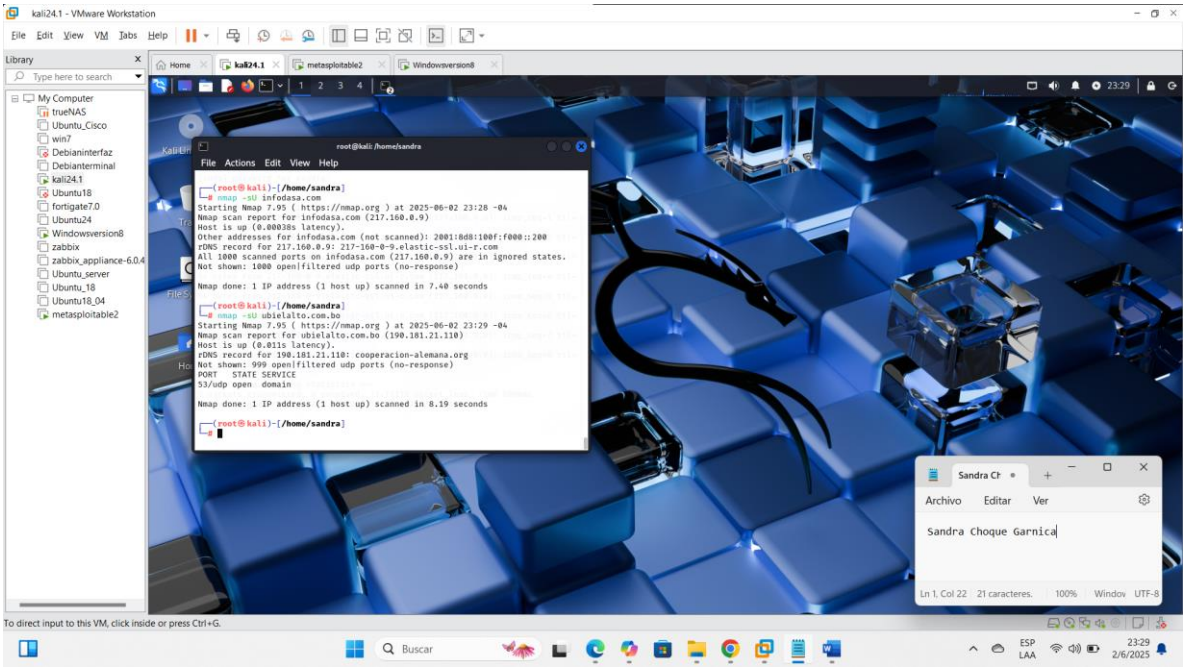
nmap -sU www.uatf.edu.bo



nmap -sU infodasa.com



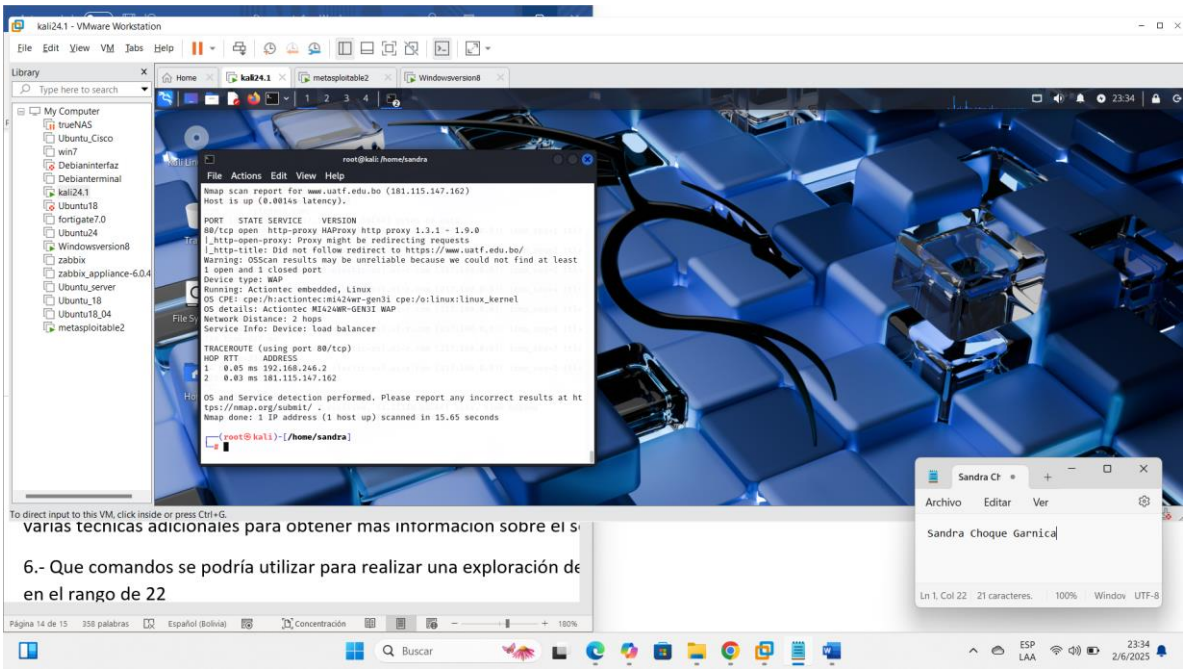
nmap -sU ubielalto.com .bo



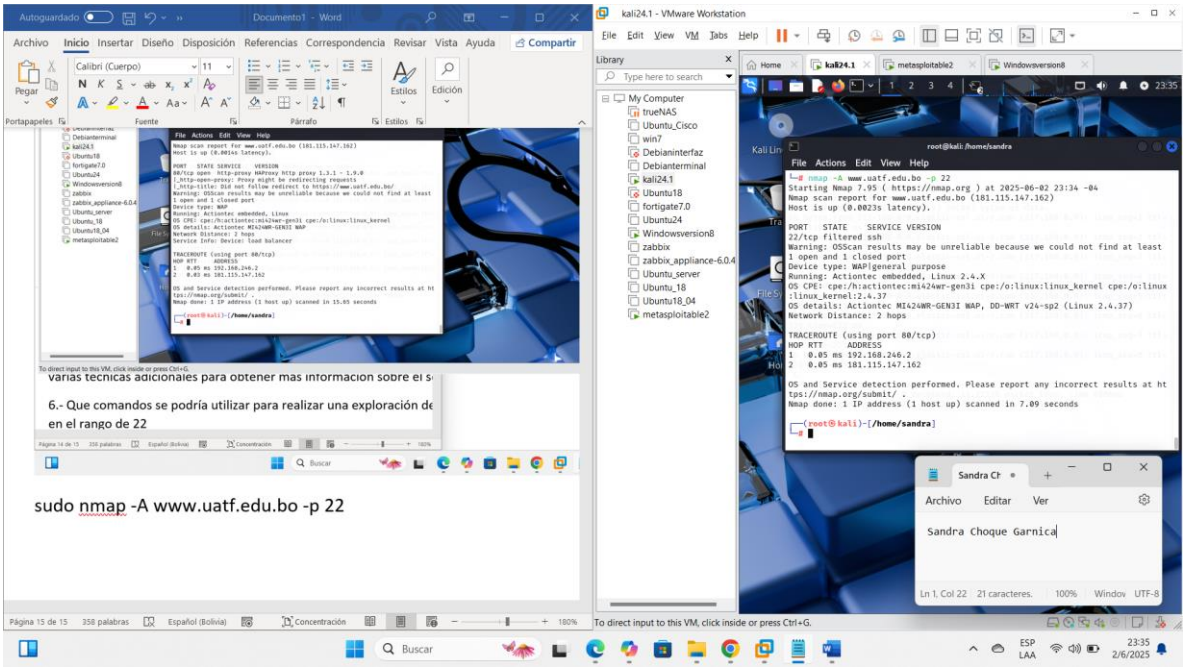
5.- Utilice la variación del comando: nmap -A dominio -p 80

nmap -A dominio -p 22

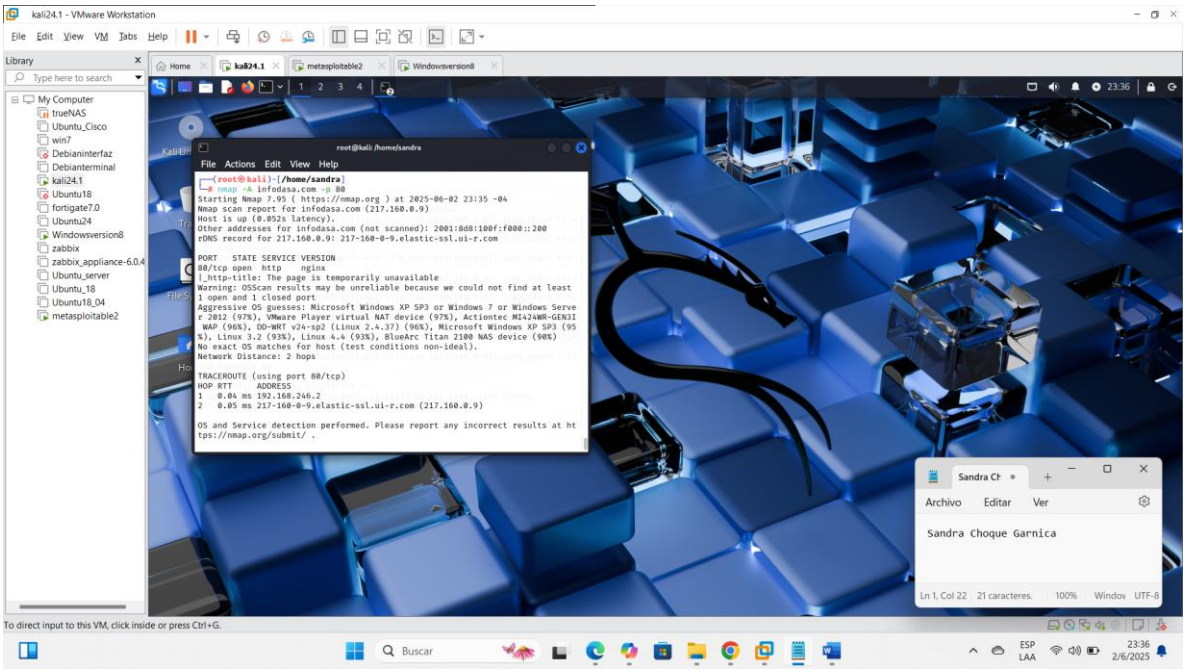
sudo nmap -A www.uatf.edu.bo -p 80

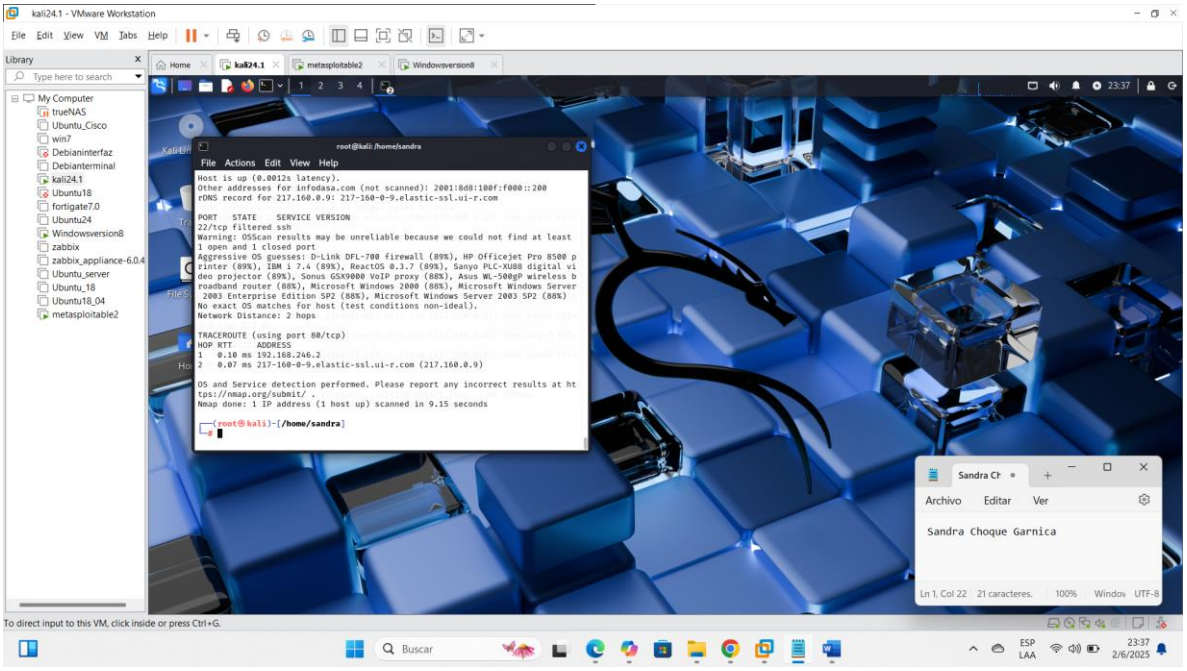


sudo nmap -A www.uatf.edu.bo -p 22

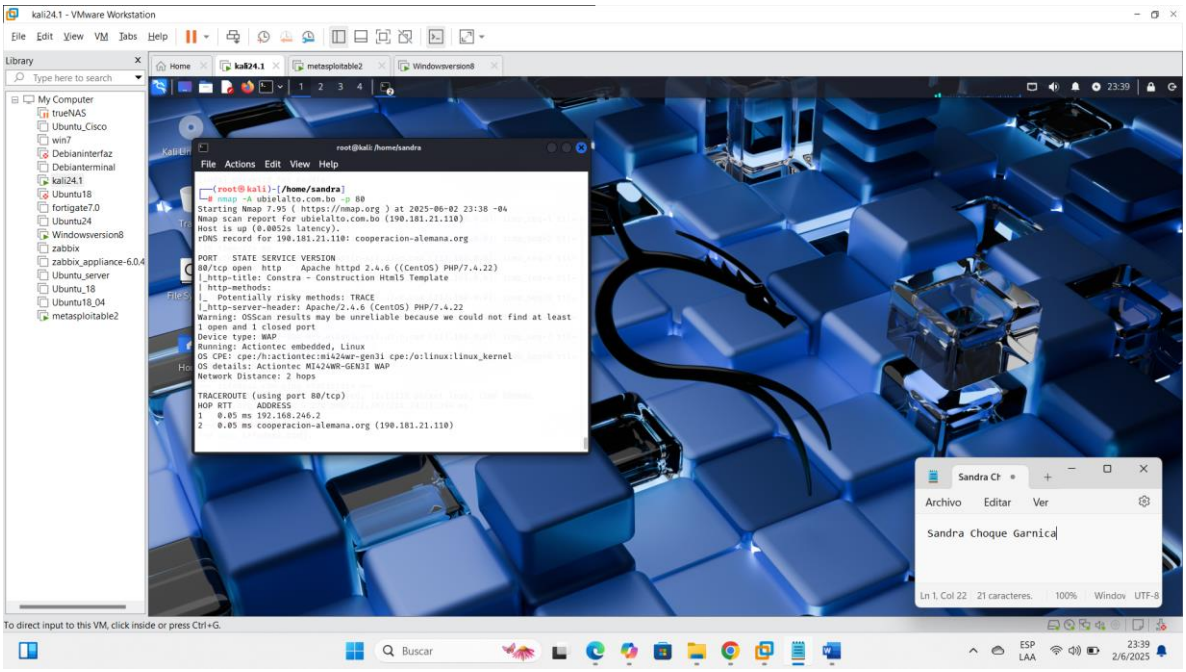


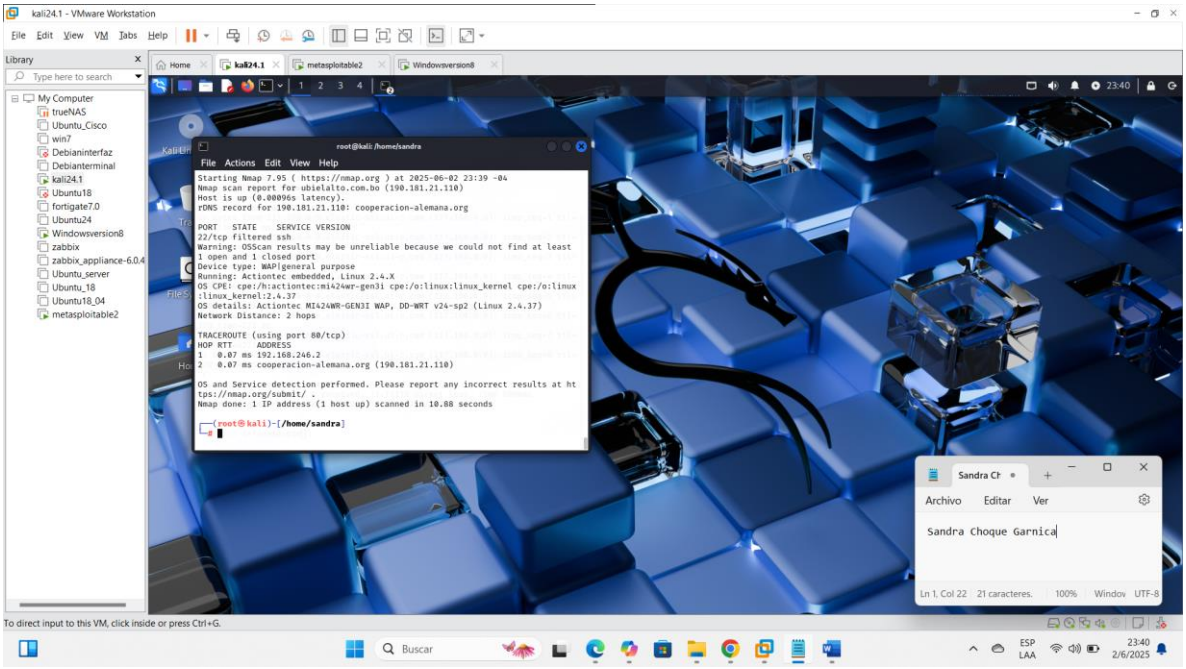
Infodasa


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
Ubuntu_18
Ubuntu18_04
metasploitable2
Home
kali24.1
metasploitable2
Windowsversion8
root@kali: /home/sandra
File Actions Edit View Help
┌──(root㉿kali)-[/home/sandra]
└─# nmap -A infodasa.com -p 80
Starting Nmap 7.95 (https://nmap.org) at 2025-06-02 23:35 -04
Nmap scan report for infodasa.com (217.160.0.9)
Host is up (0.052s 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 open http nginx
|_http-title: The page is temporarily unavailable
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows XP SP3 or Windows 7 or Windows Serve
r 2012 (97%), VMware Player virtual NAT device (97%), Actiontec MI424WR-GEN3I
WAP (96%), DD-WRT v24-sp2 (Linux 2.4.37) (96%), Microsoft Windows XP SP3 (95
%), Linux 3.2 (93%), Linux 4.4 (93%), BlueArc Titan 2100 NAS device (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 0.04 ms 192.168.246.2
2 0.05 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 ht
tps://nmap.org/submit/ .
Sandra Ch
Archivo Editar Ver
Sandra Choque Garnica
Ln 1, Col 22 21 caracteres. 100% Windov UTF-8
To direct input to this VM, click inside or press Ctrl+G.
Buscar
ESP
LAA
23:36
2/6/2025


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
Ubuntu_18
Ubuntu18_04
metasploitable2
Home
kali24.1
metasploitable2
Windowsversion8
root@kali: /home/sandra
File Actions Edit View Help
Host is up (0.0012s 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
Aggressive OS guesses: D-Link DFL-700 firewall (89%), HP Officejet Pro 8500 p
rinter (89%), IBM i 7.4 (89%), ReactOS 0.3.7 (89%), Sanyo PLC-XU88 digital vi
deo projector (89%), Sonus GSX9000 VoIP proxy (88%), Asus WL-500gP wireless b
roadband router (88%), Microsoft Windows 2000 (88%), Microsoft Windows Server
2003 Enterprise Edition SP2 (88%), Microsoft Windows Server 2003 SP2 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 0.10 ms 192.168.246.2
2 0.07 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 ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.15 seconds
┌──(root㉿kali)-[/home/sandra]
└─#
Sandra Ch
Archivo Editar Ver
Sandra Choque Garnica
Ln 1, Col 22 21 caracteres. 100% Windov UTF-8
To direct input to this VM, click inside or press Ctrl+G.
Buscar
ESP
LAA
23:37
2/6/2025

Ubielalto





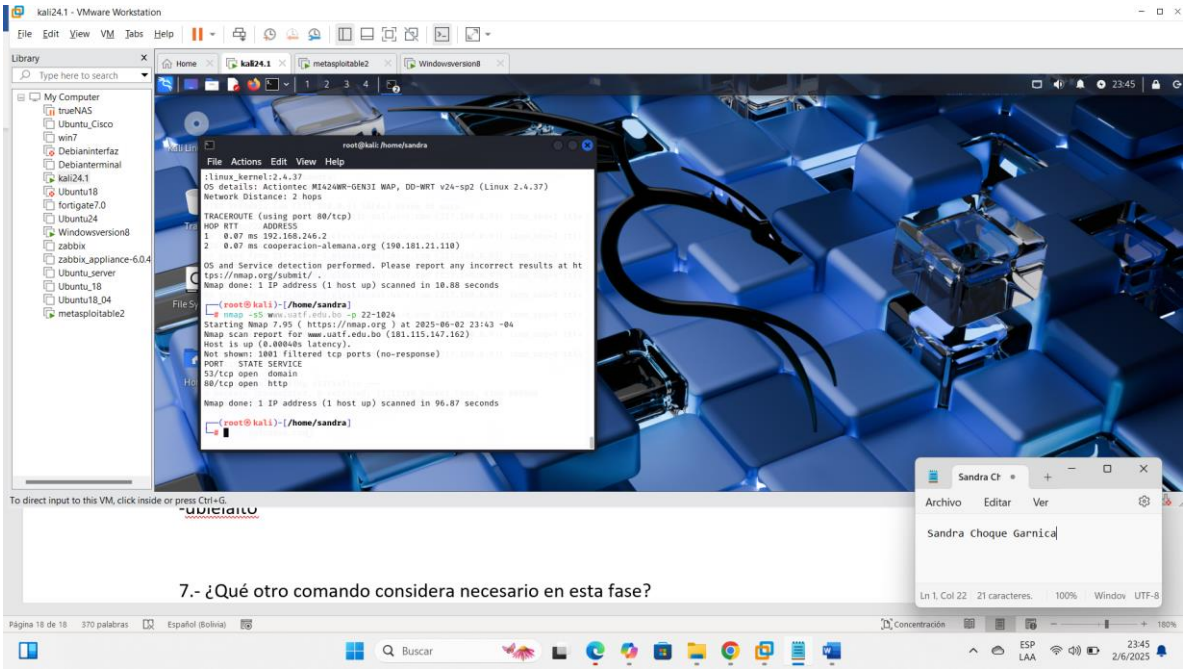
¿Qué tipo de escaneo significa la letra A?

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.

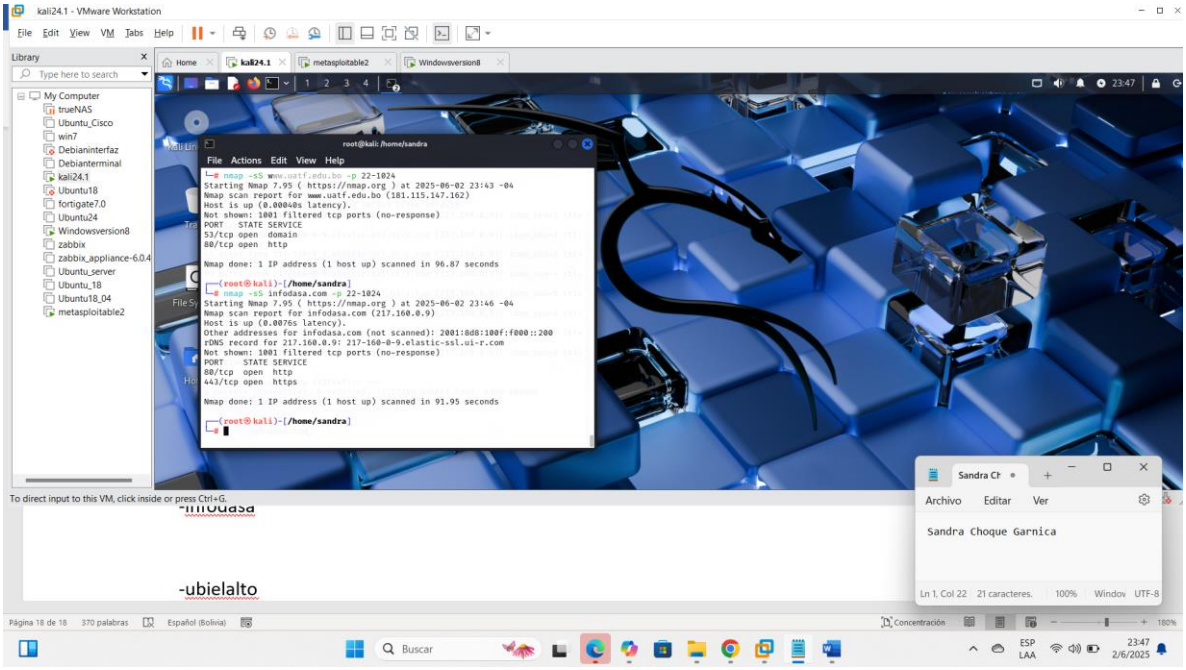
6.- Que comandos se podría utilizar para realizar una exploración de los puertos TCP y luego UDP en el rango de 22 a 1024. Use como destino los dominios indicados.

Puertos TCP

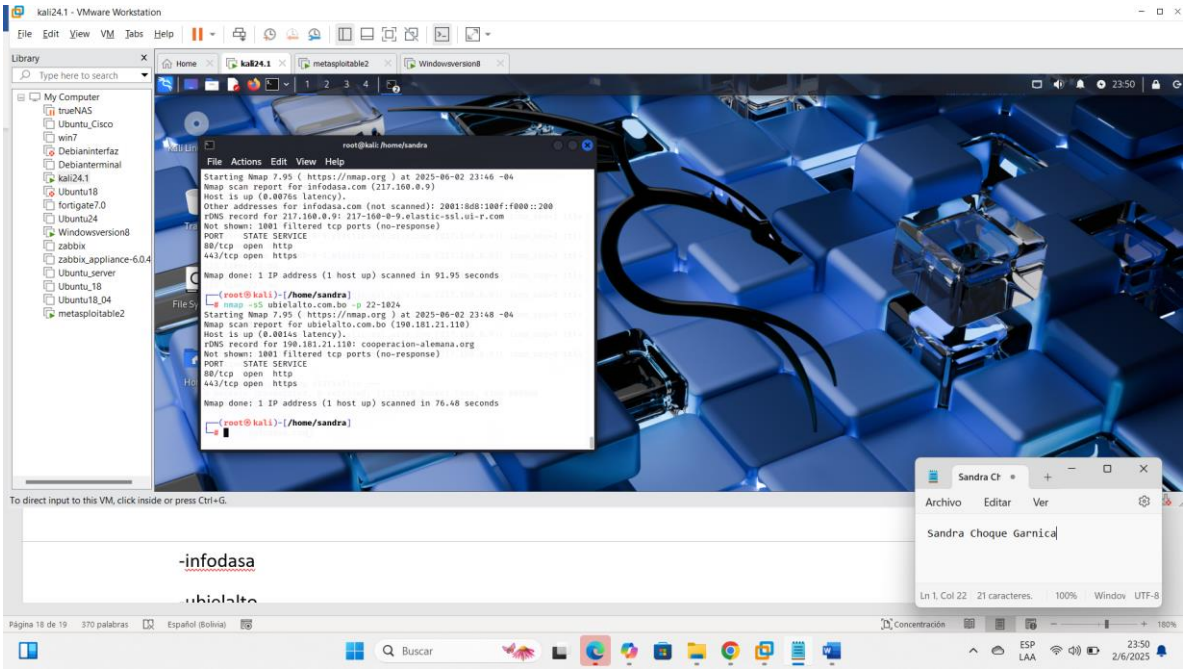
-uatf



-infodasa

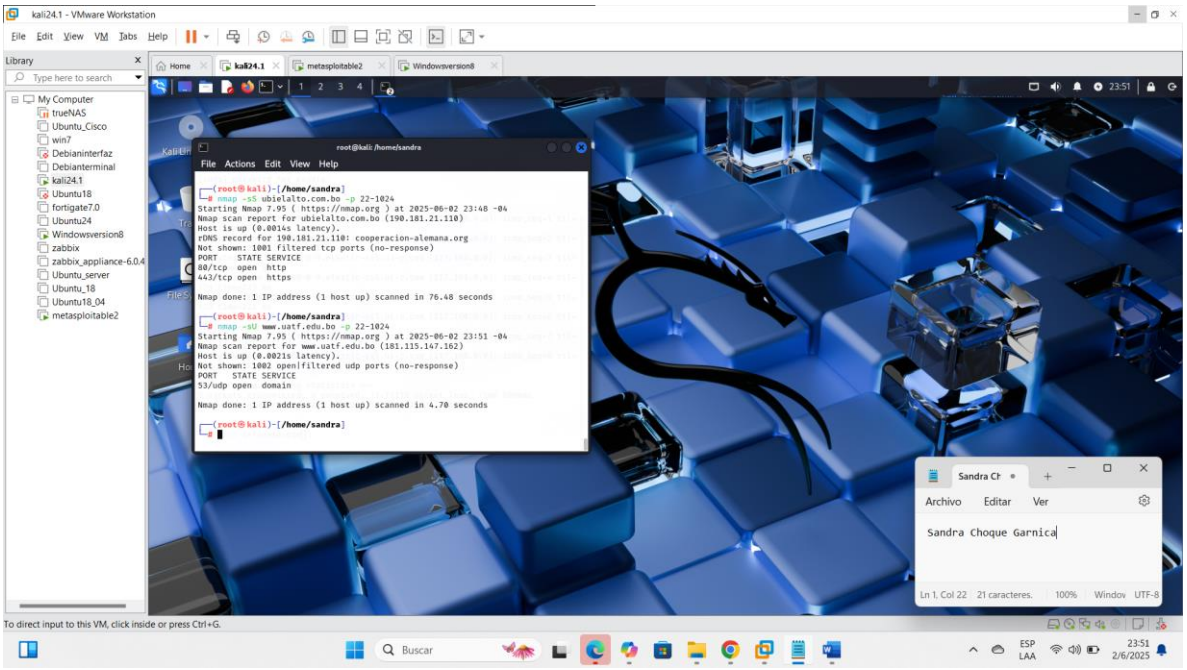


-ubielalto

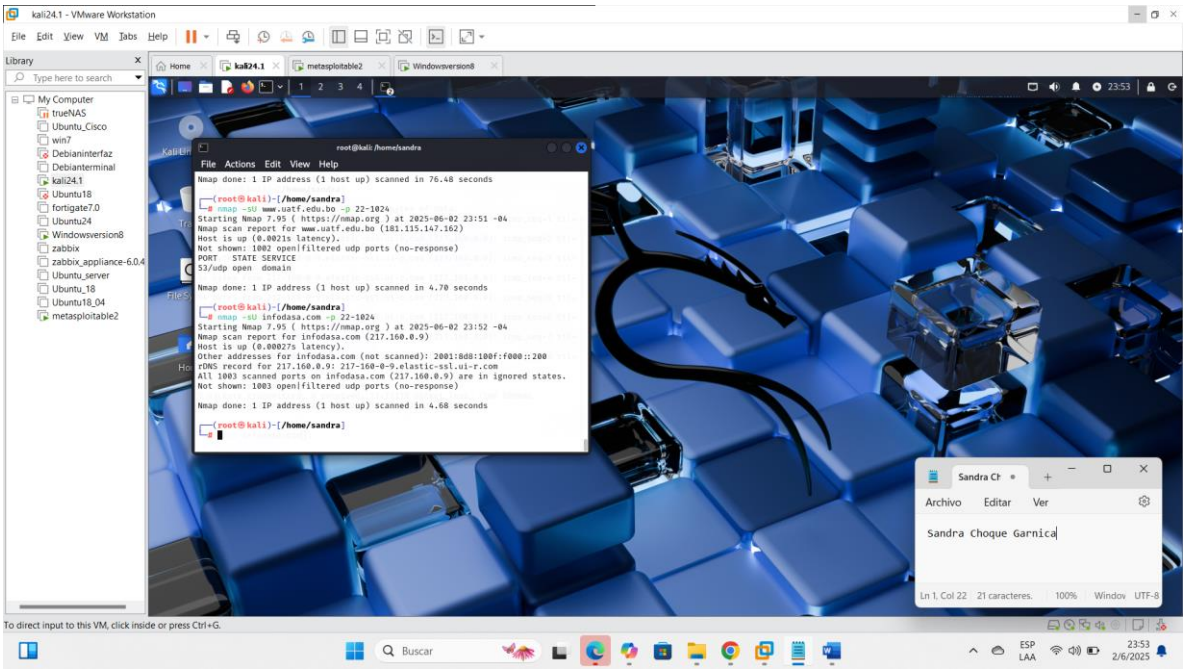


Puertos UDP

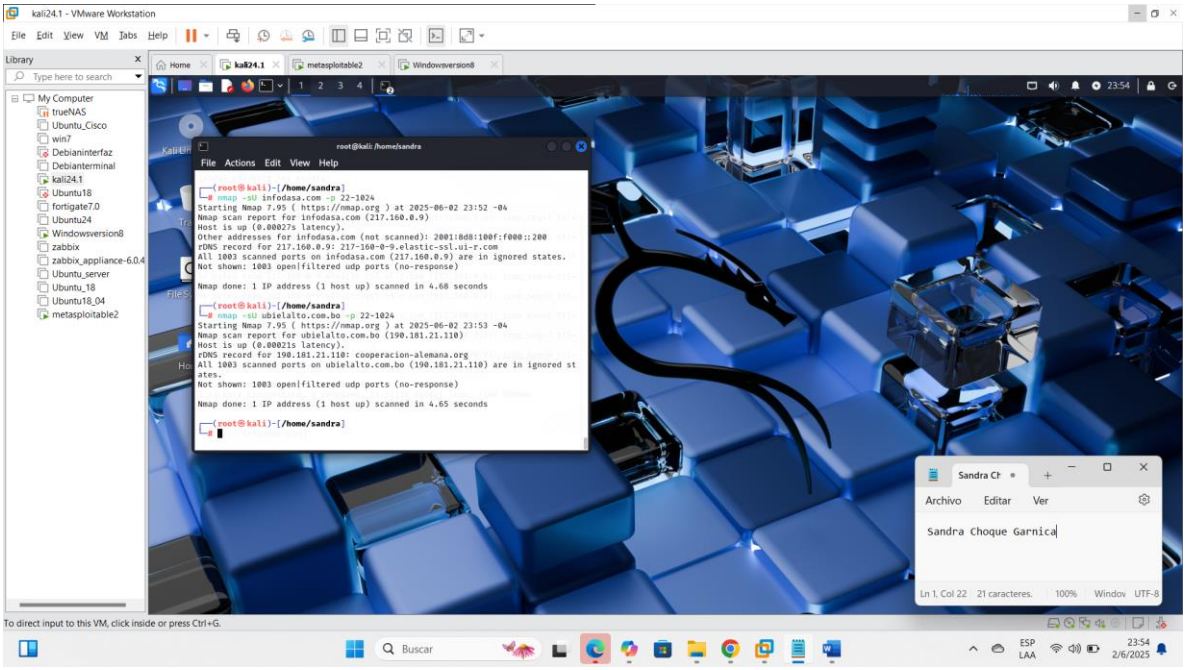
-uatf



-infodasa



-ubielalto



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

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

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