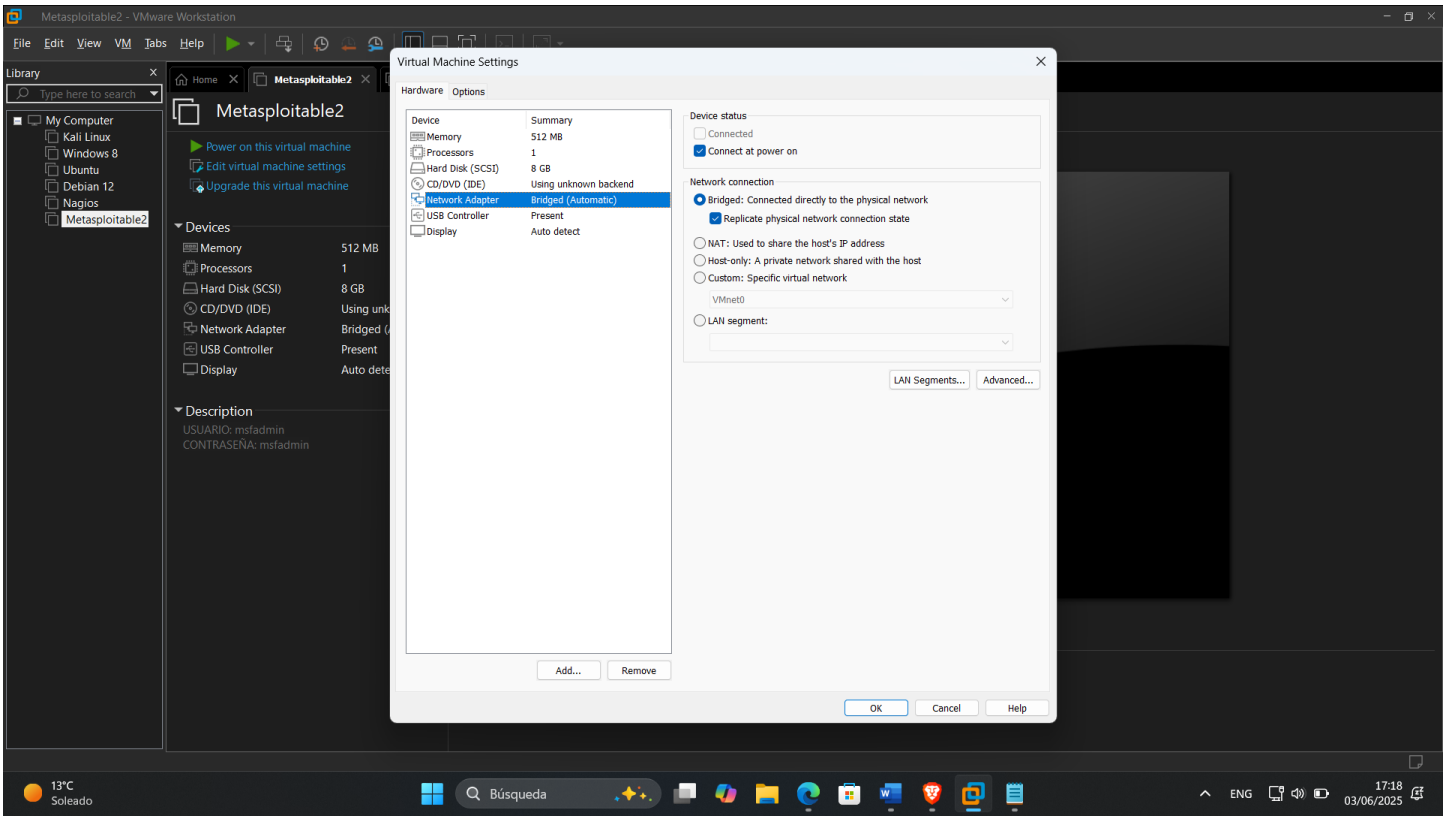
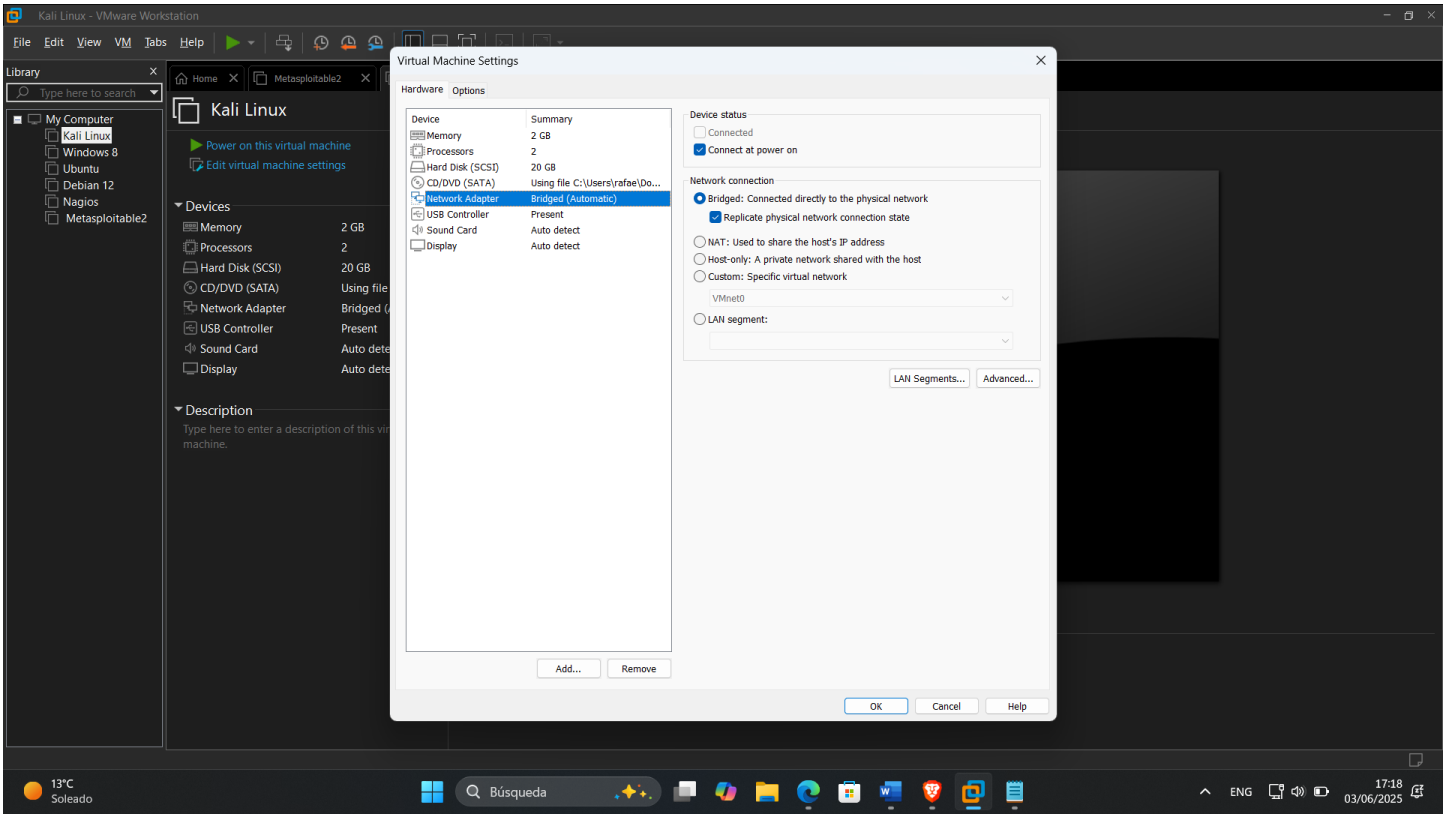
Laboratorio Nº11

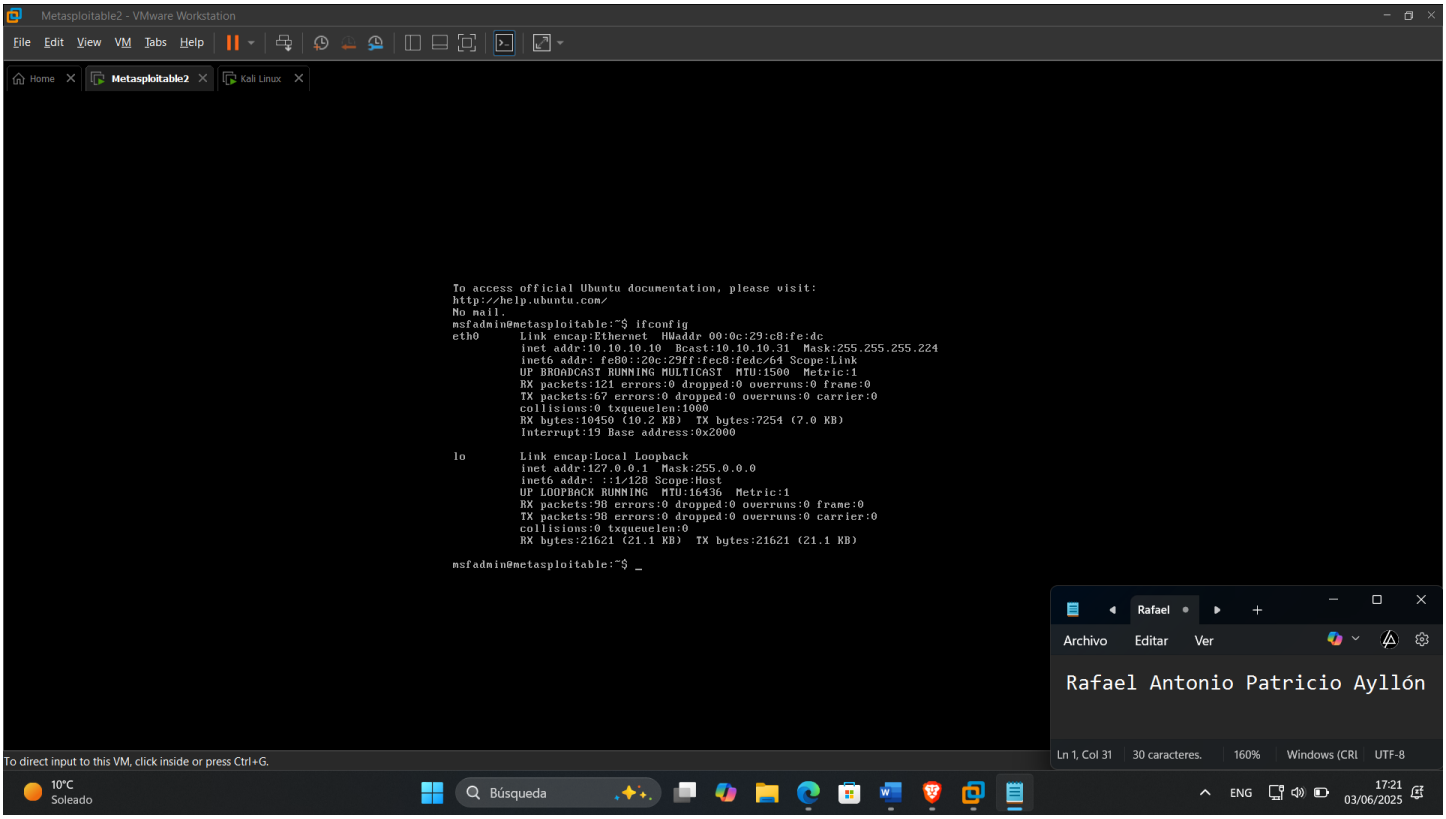
Nombre: Rafael Antonio Patricio Ayllón **CI:** 10473854 **RU:** 108771

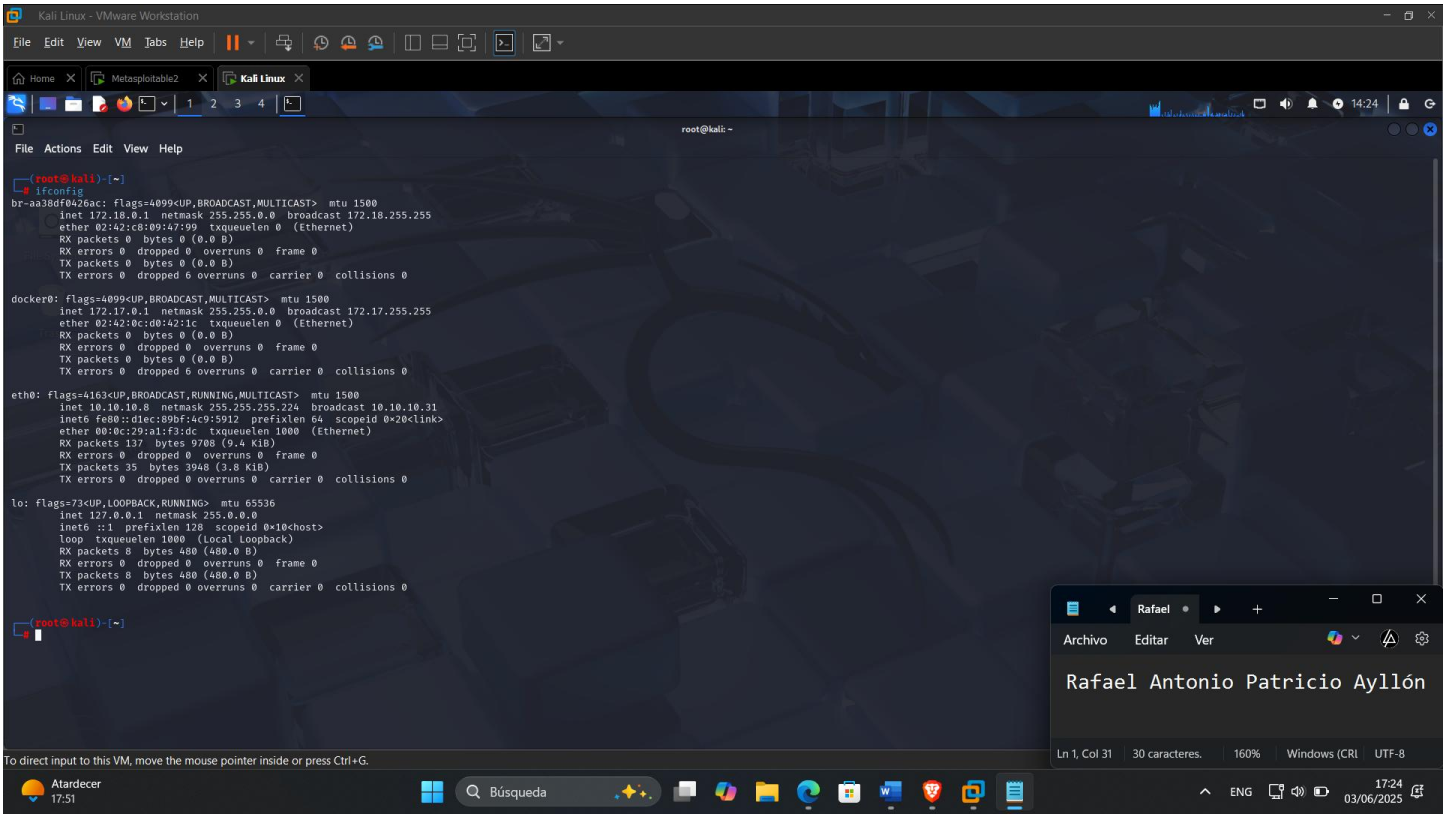
Se recomienda que el adaptador de red este en el modo "Bridged" como muestra la imagen si es que se está configurando por primera vez la máquina virtual. Si esta utilizando otro modo de tarjeta, verifique que exista conectividad entre Kali y metasploitable2 antes de realizar la práctica.



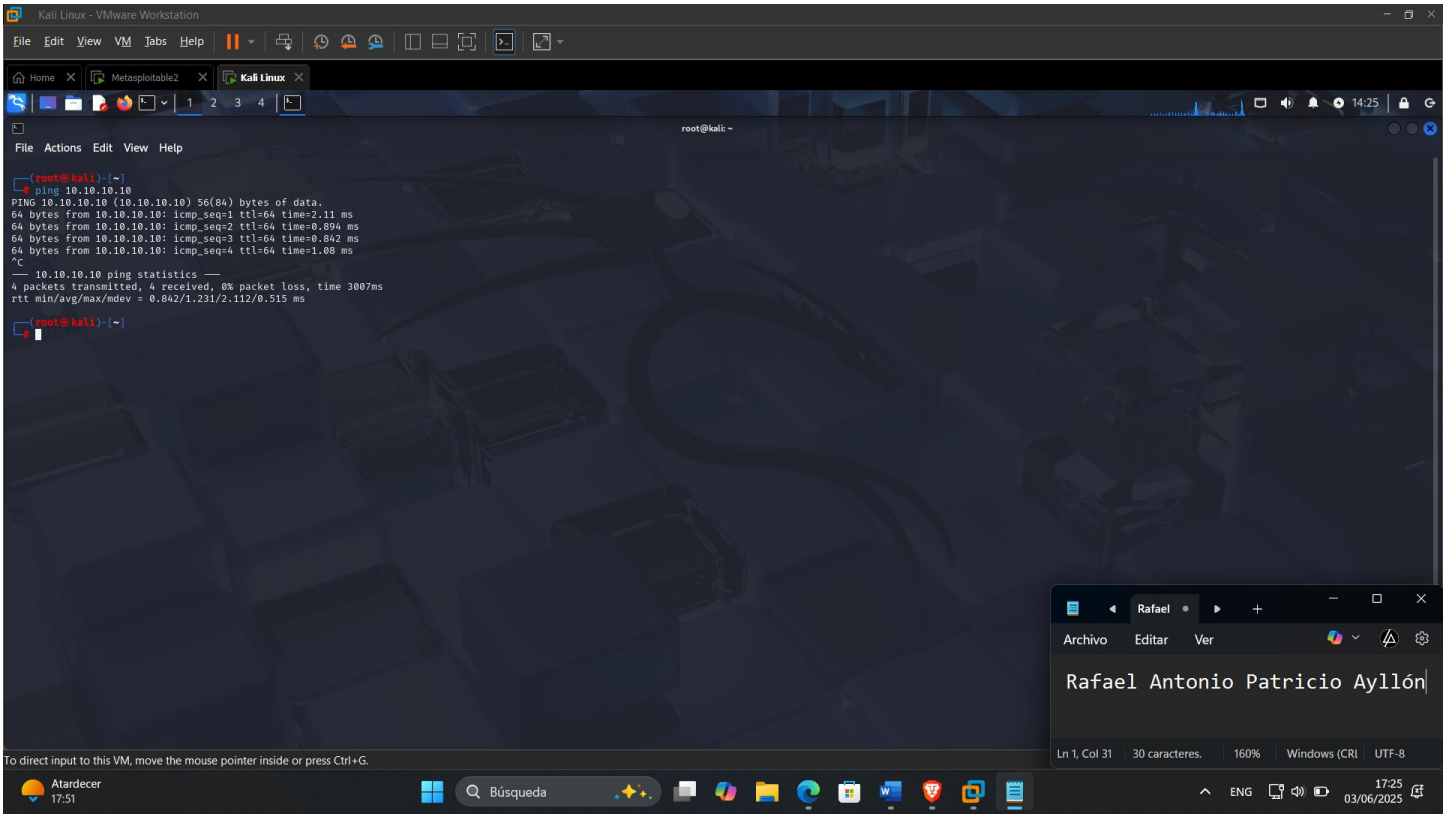


Inicialmente debemos asegurarnos que ambas máquinas se encuentren en el mismo segmento de red. (Utilice las direcciones IP con las que está configurado su entorno de laboratorio).

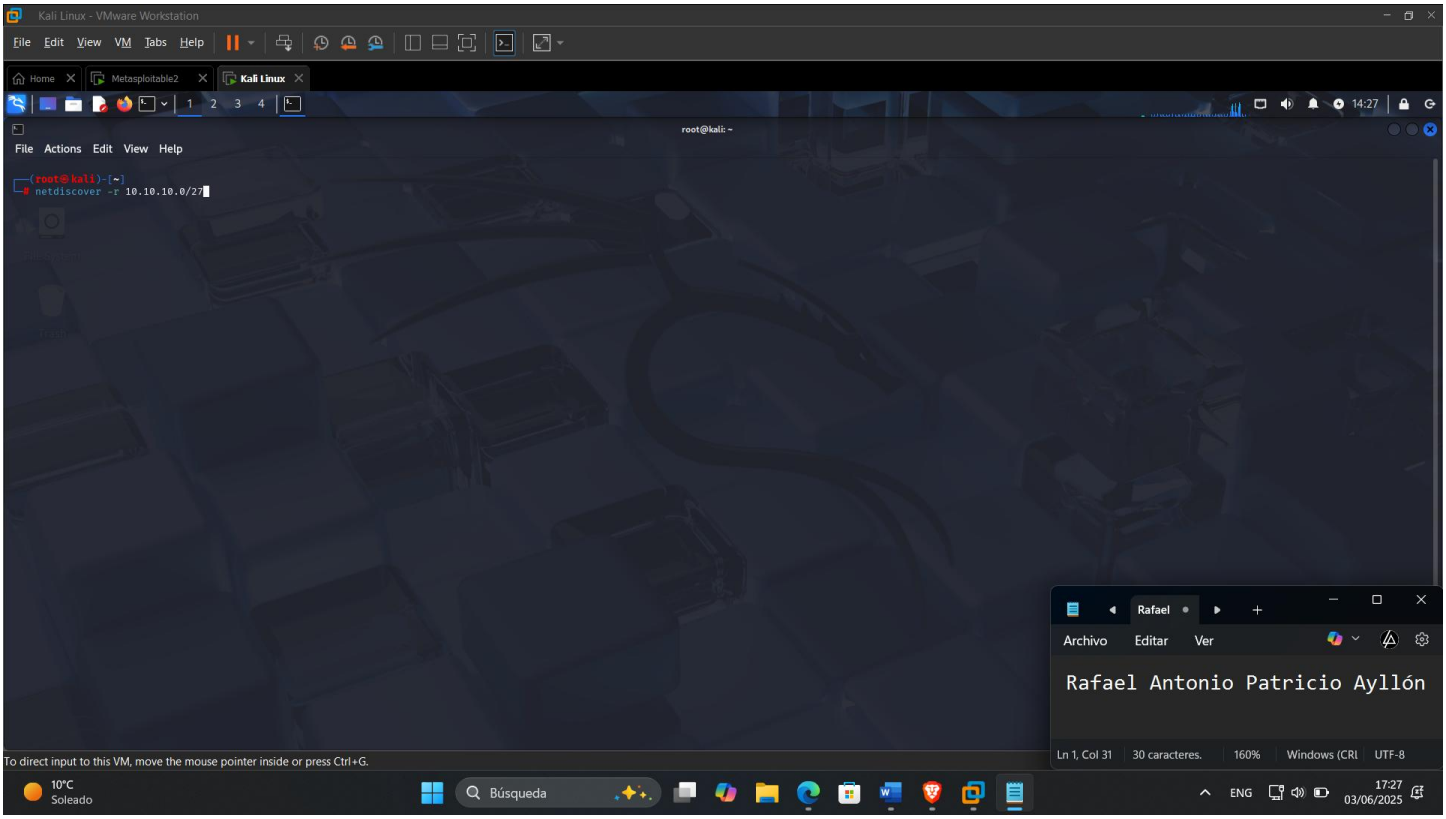




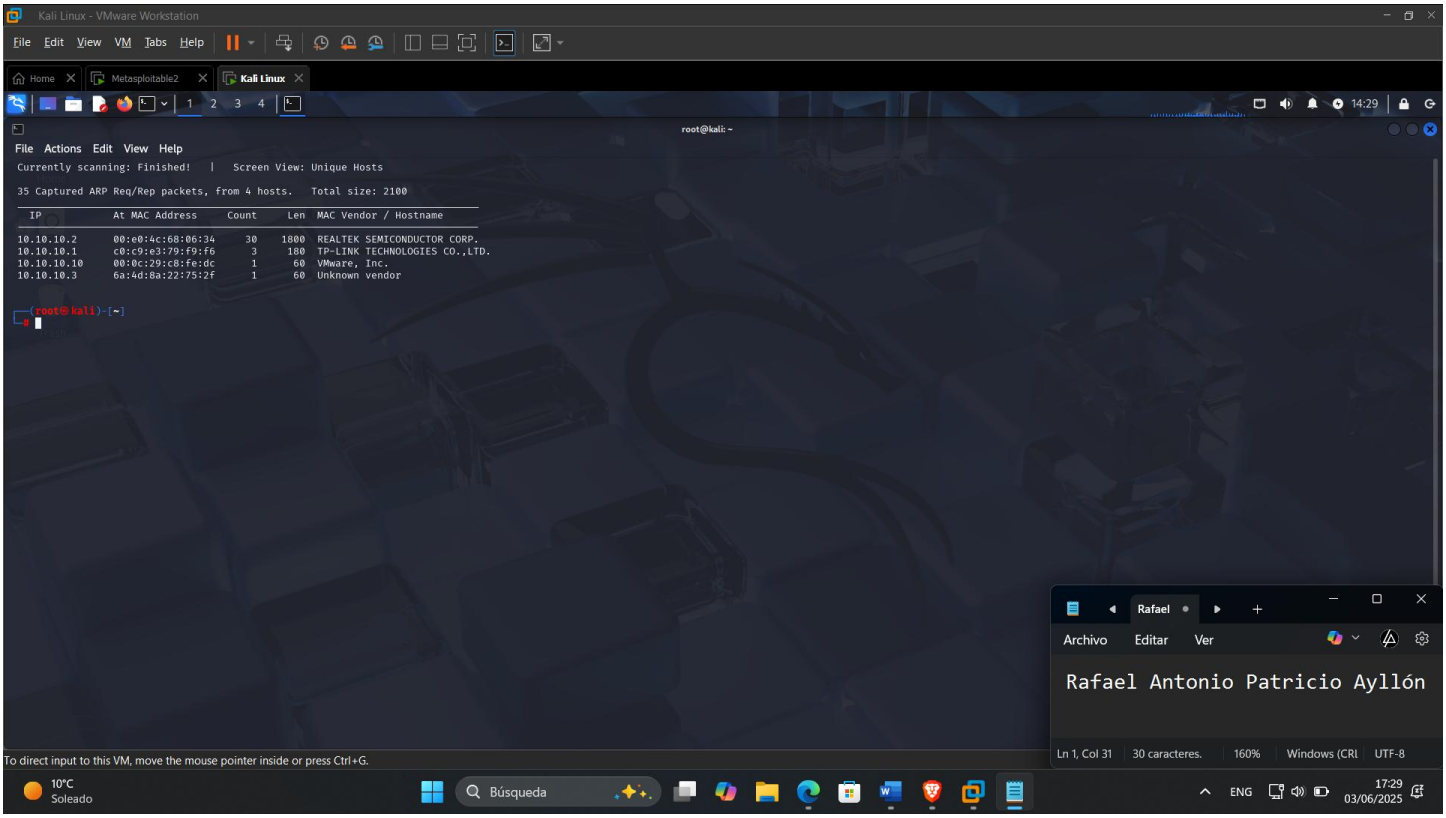
Nos aseguramos que exista conectividad desde la máquina Kali hacia la metasploitable:



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:

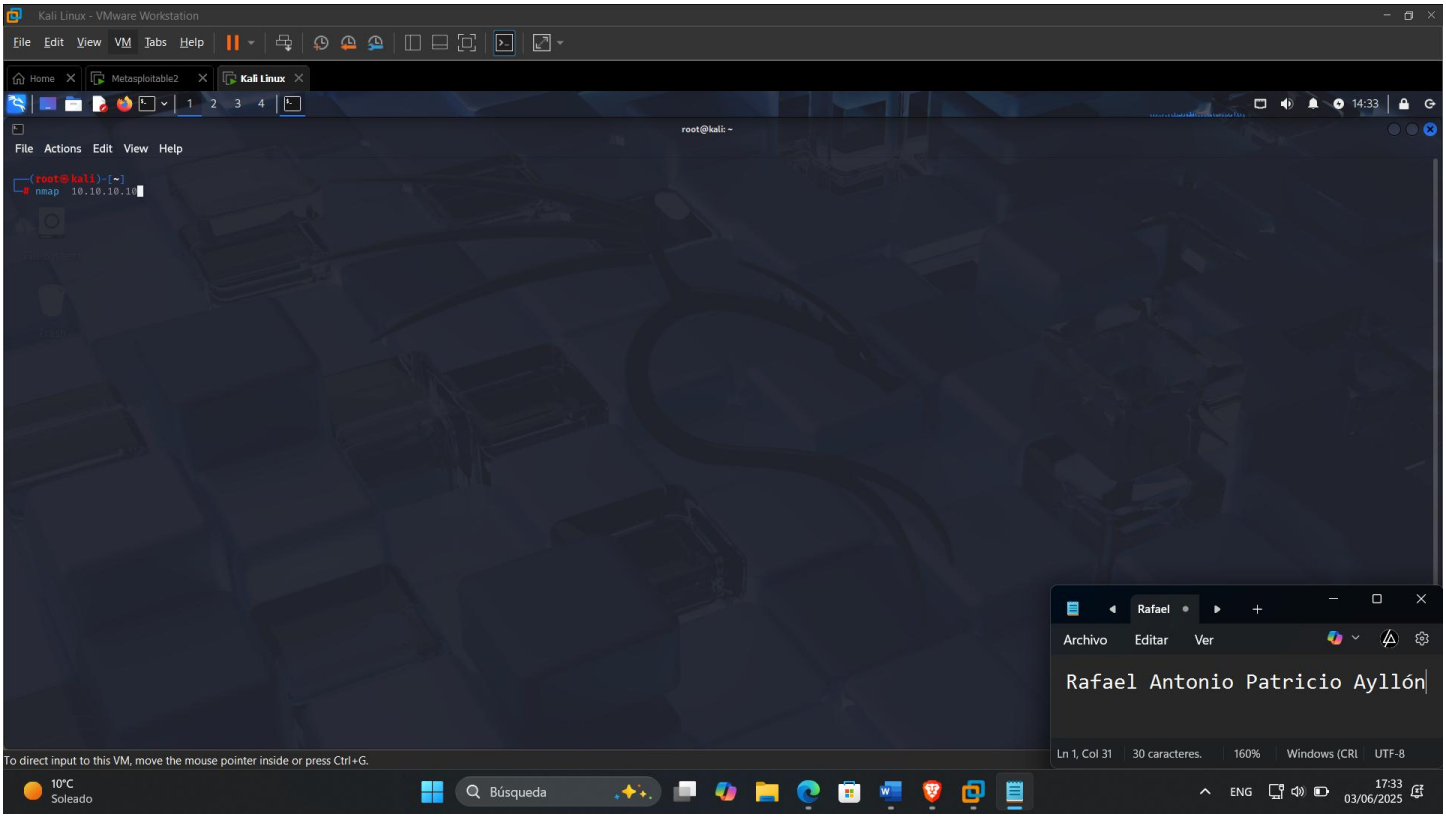


El resultado muestra que hay cuatro máquinas en este segmento de red: 10.10.10.1, 10.10.10.2, 10.10.10.3, 10.10.10.10, de existir más, serían identificadas igualmente.

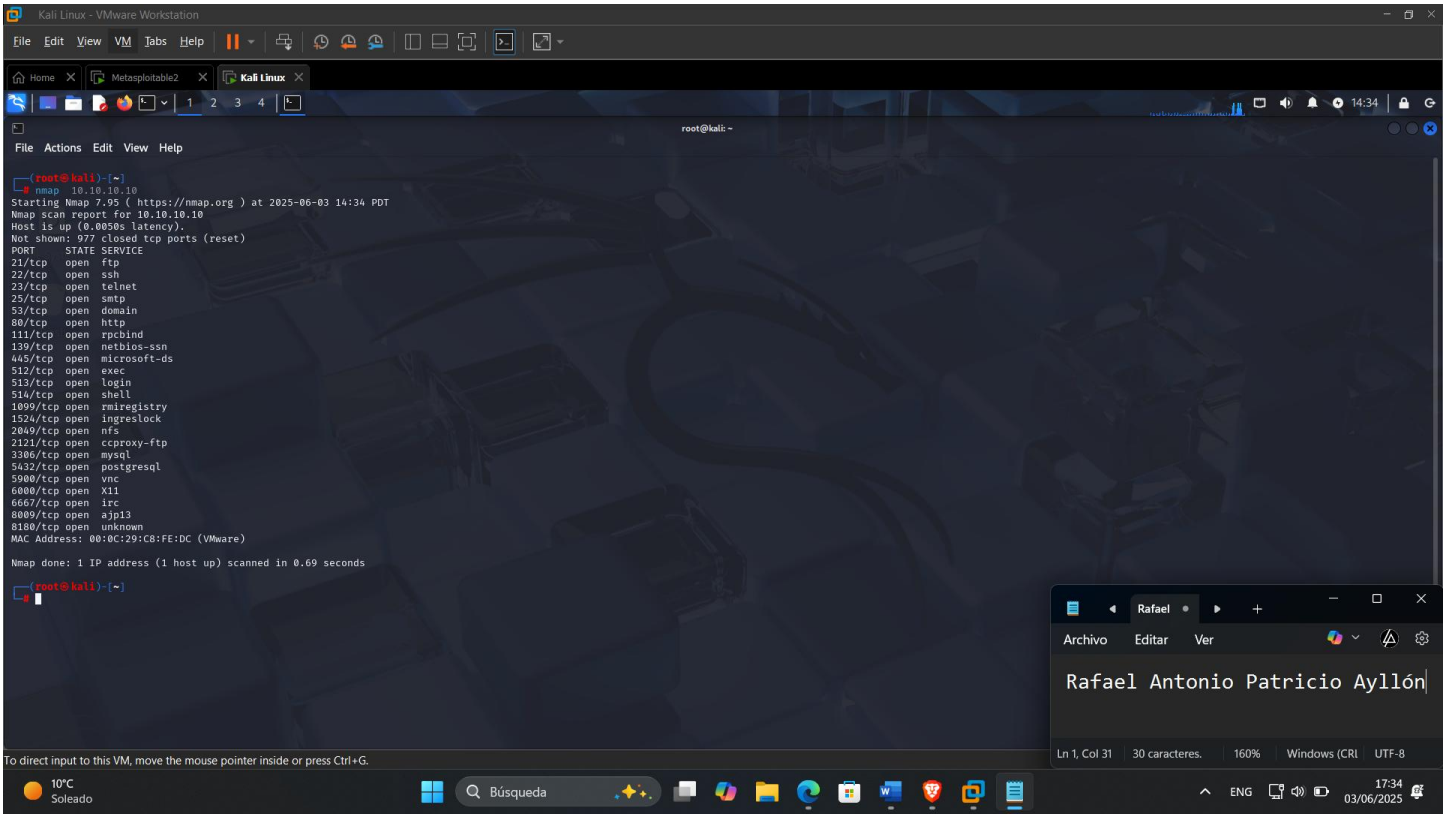


En el caso de que su versión de Kali no cuente con netdiscover, utilice el siguiente comando para descubrir los equipos que son parte de su red: nmap 10.10.10.0/24 . En este caso se esta realizando el escaneo a la dirección de red.

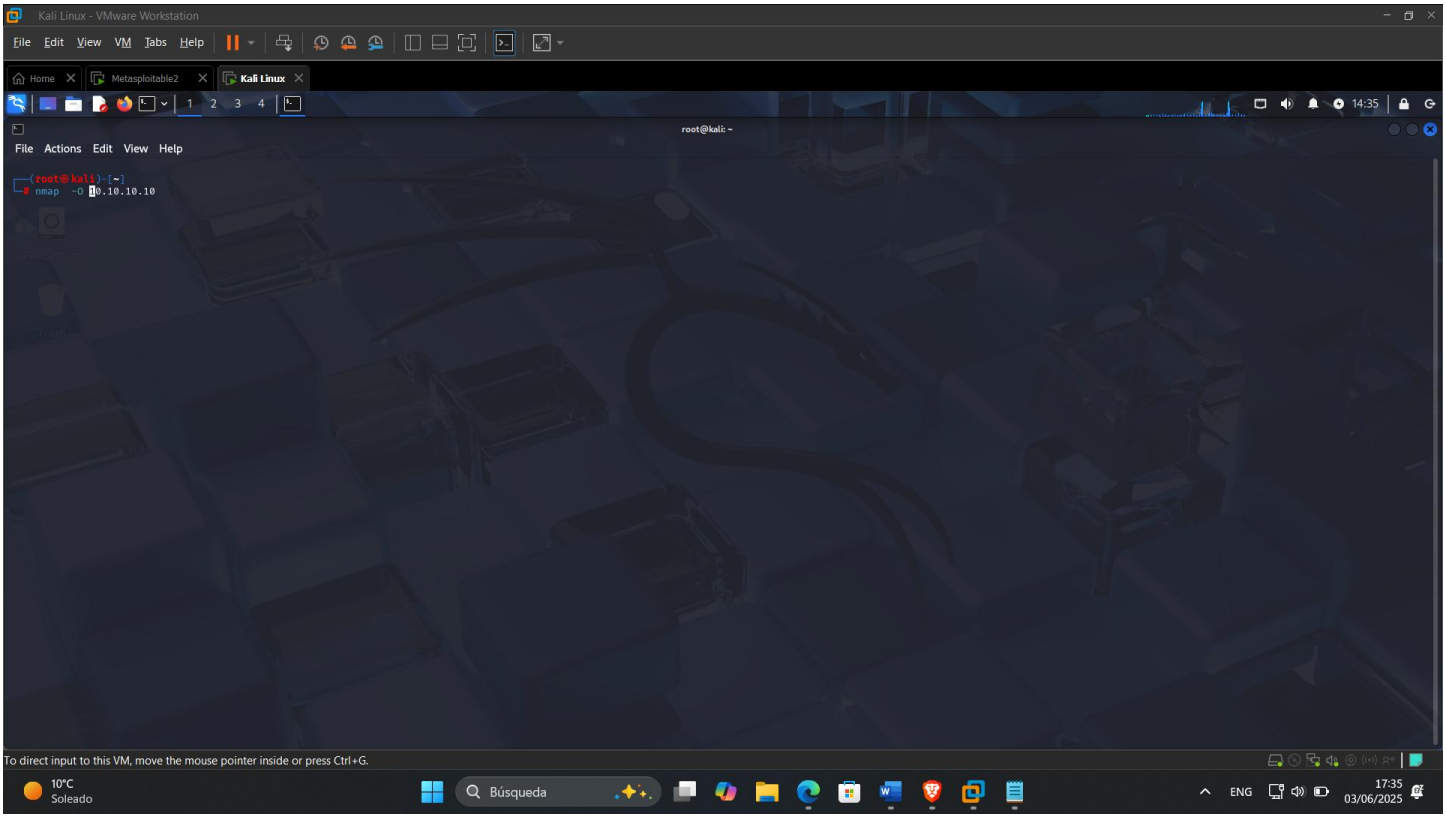
Habiendo identificado a los posibles objetivos, procedemos a realizar el escaneo de la PC metasploitable. Para ello utilizamos el comando:



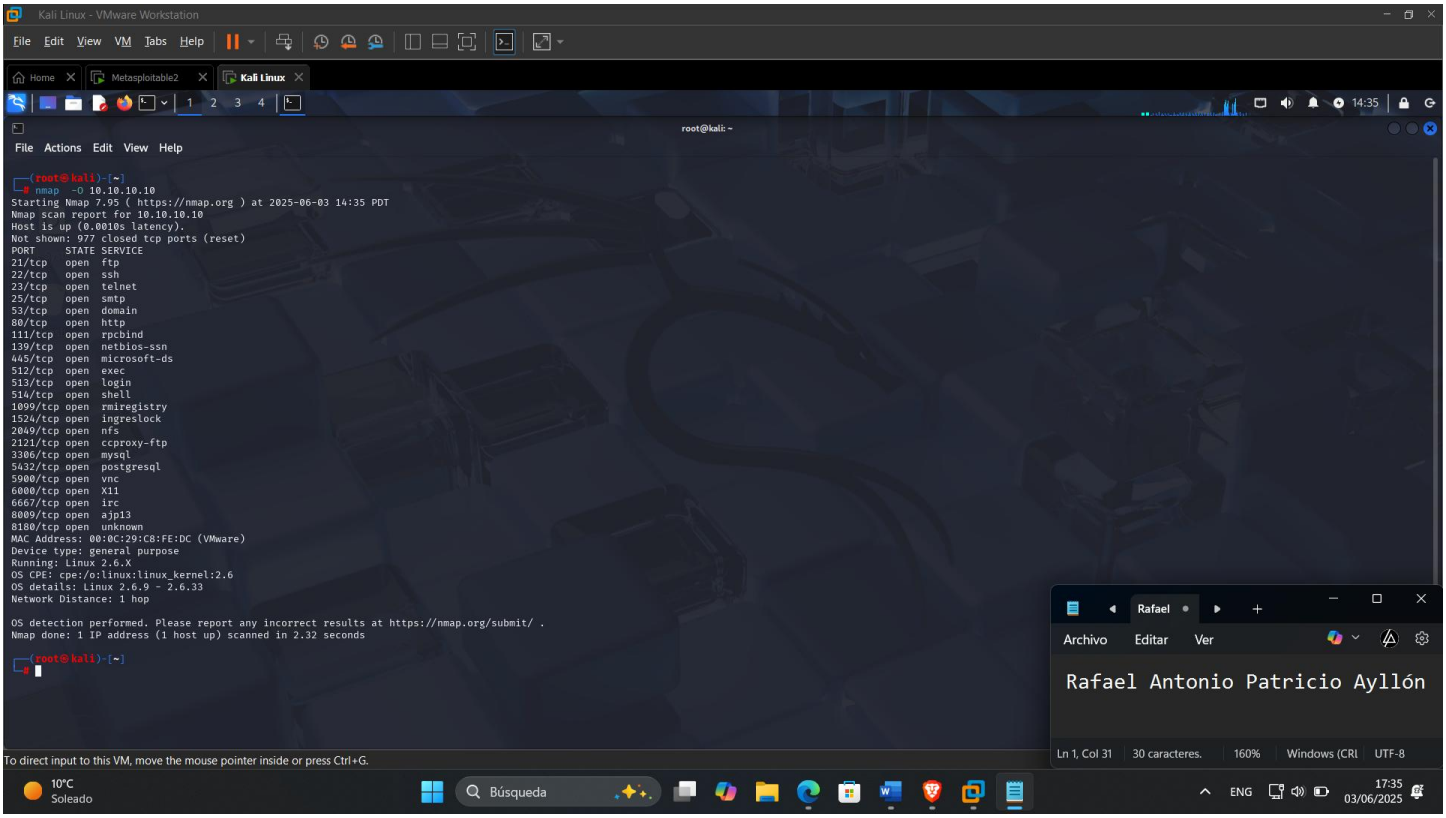
El resultado del mismo arroja que son varios los servicios que se están ejecutando en esa Pc.



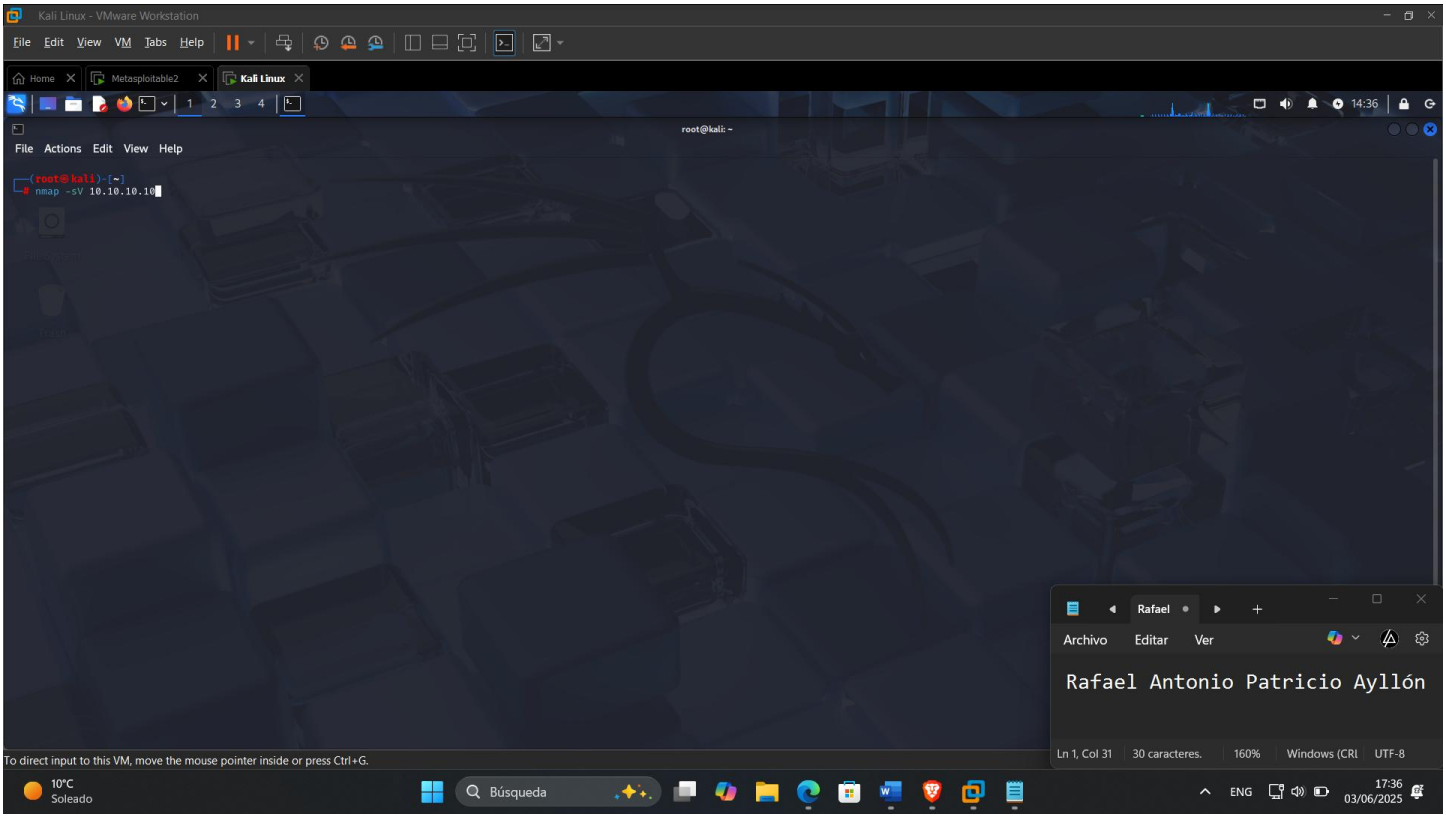
Sin embargo, no conocemos que sistema operativo es el que utiliza nuestro objetivo, para ello usamos:



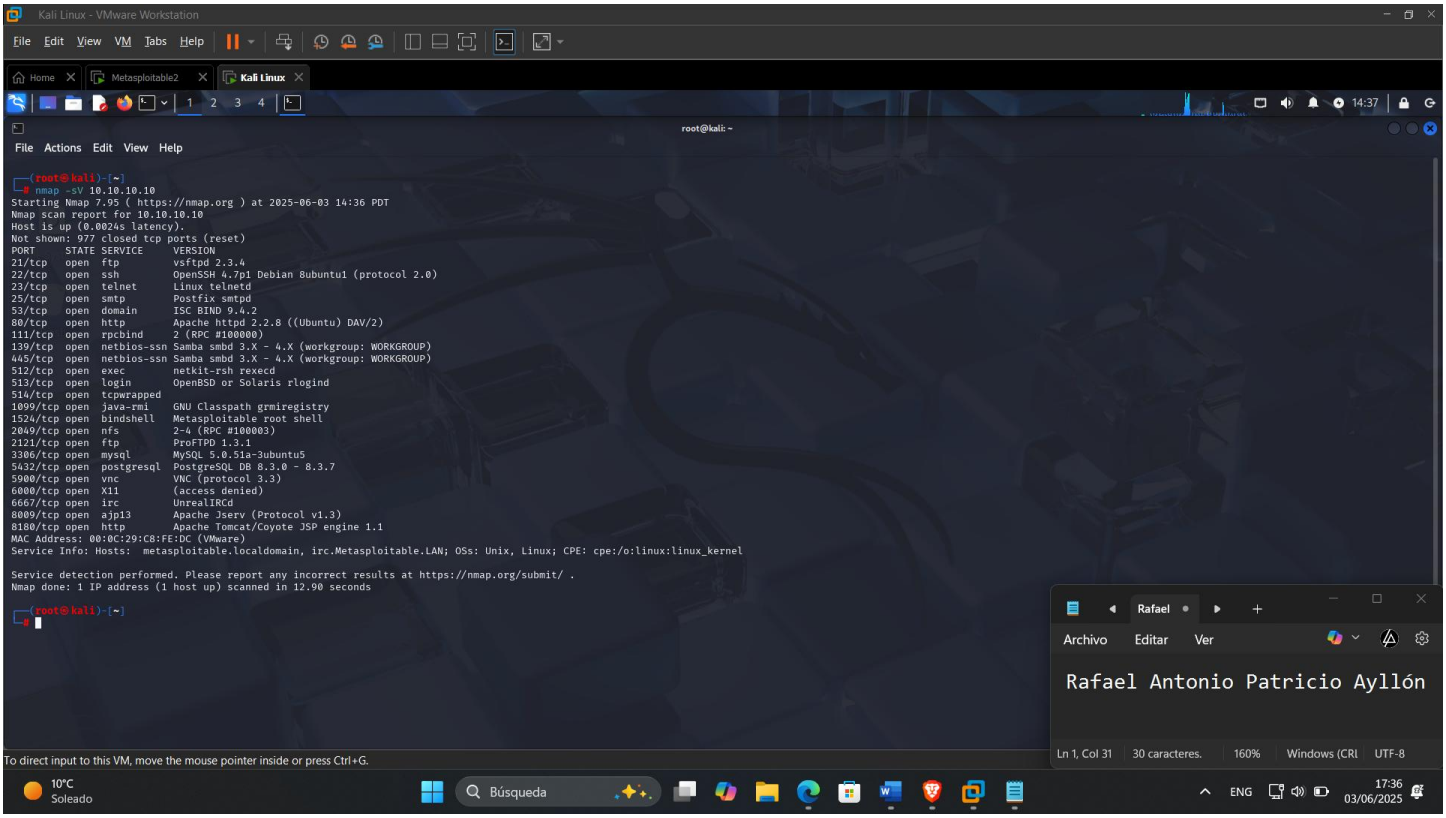
Siendo el resultado una distribución en Linux.



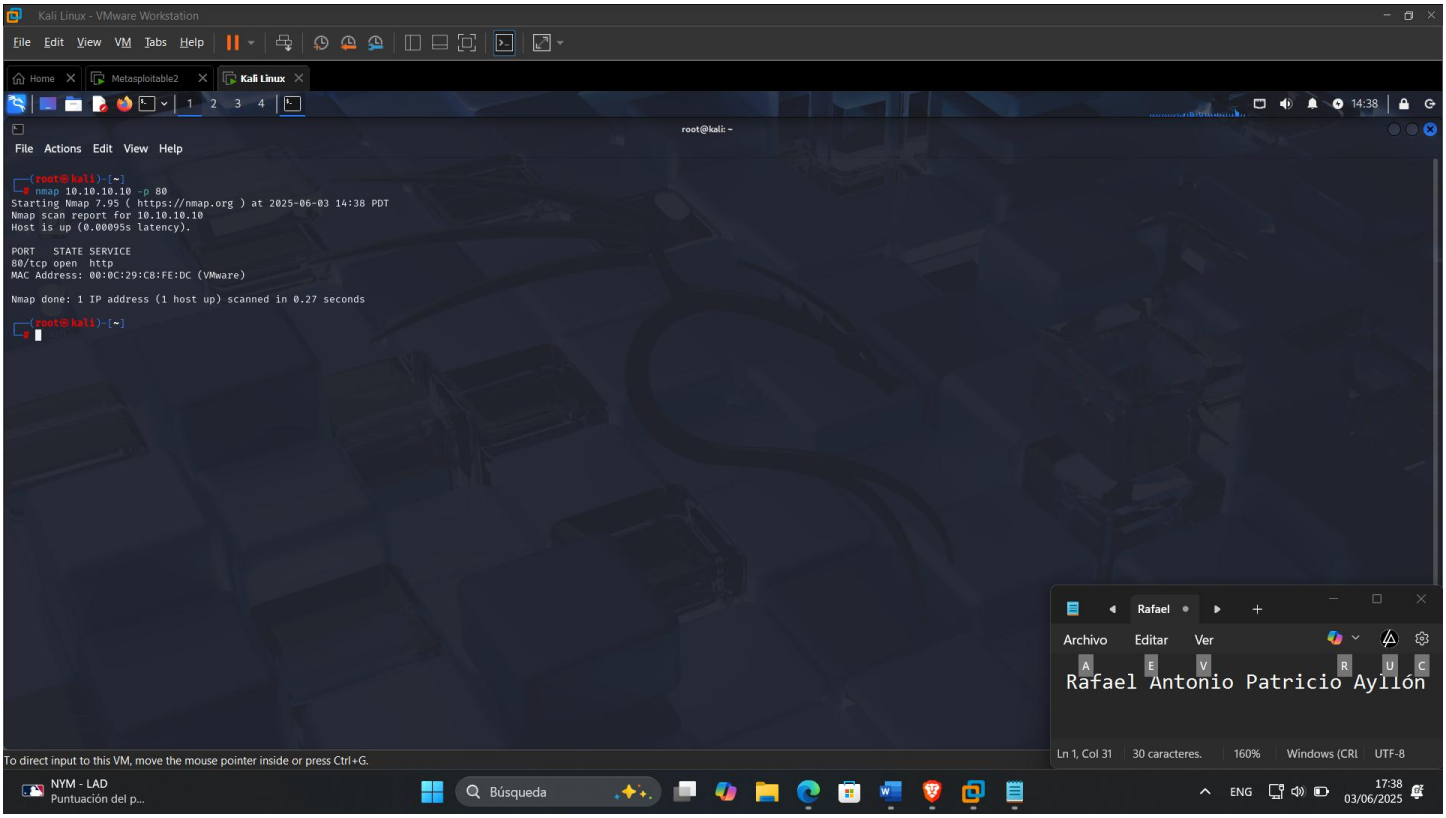
Para ver a más detalle los servicios en este caso las versiones que utilizan, usamos el comando:



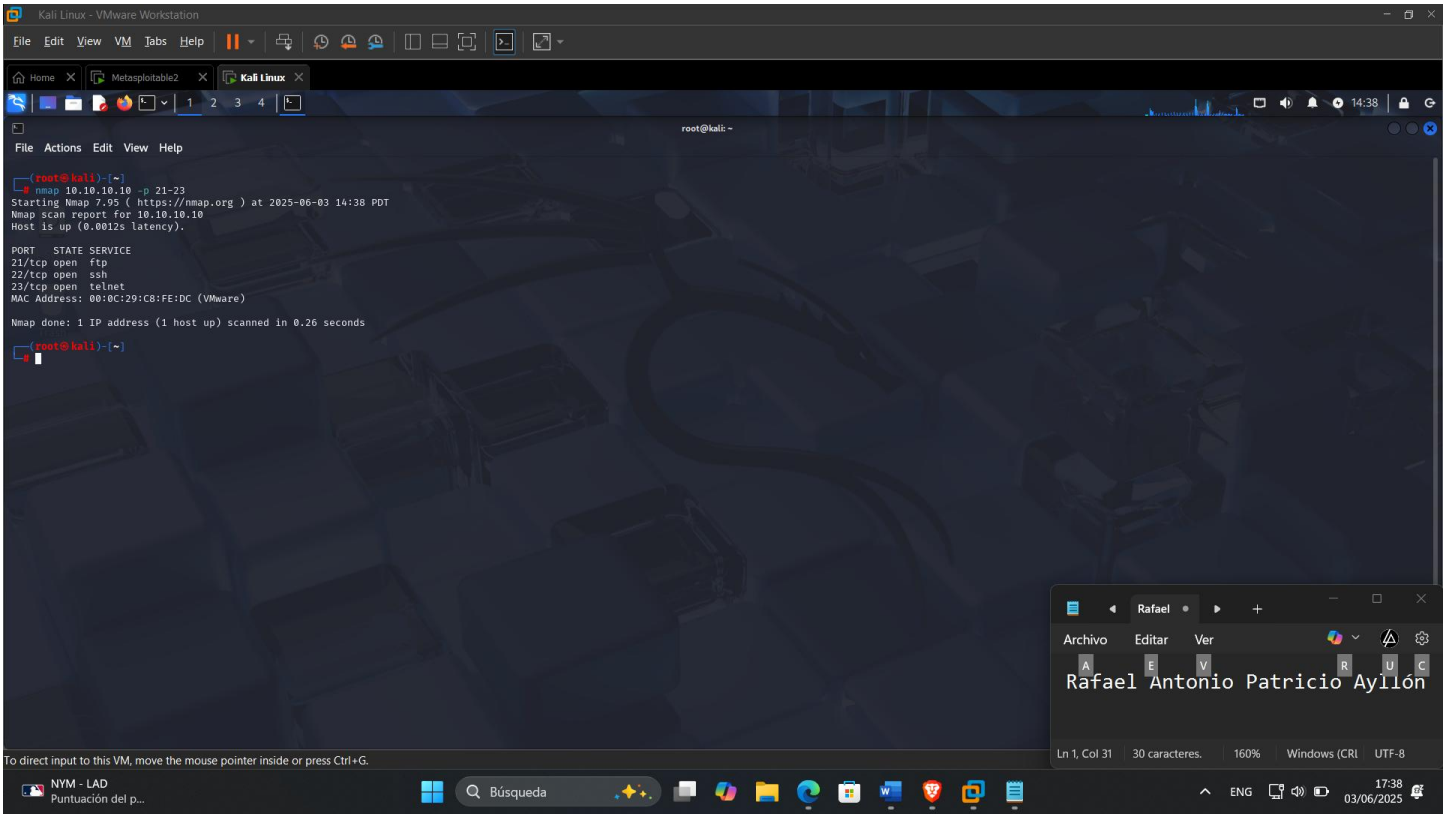
Cuyo resultado son las versiones de cada servicio.



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

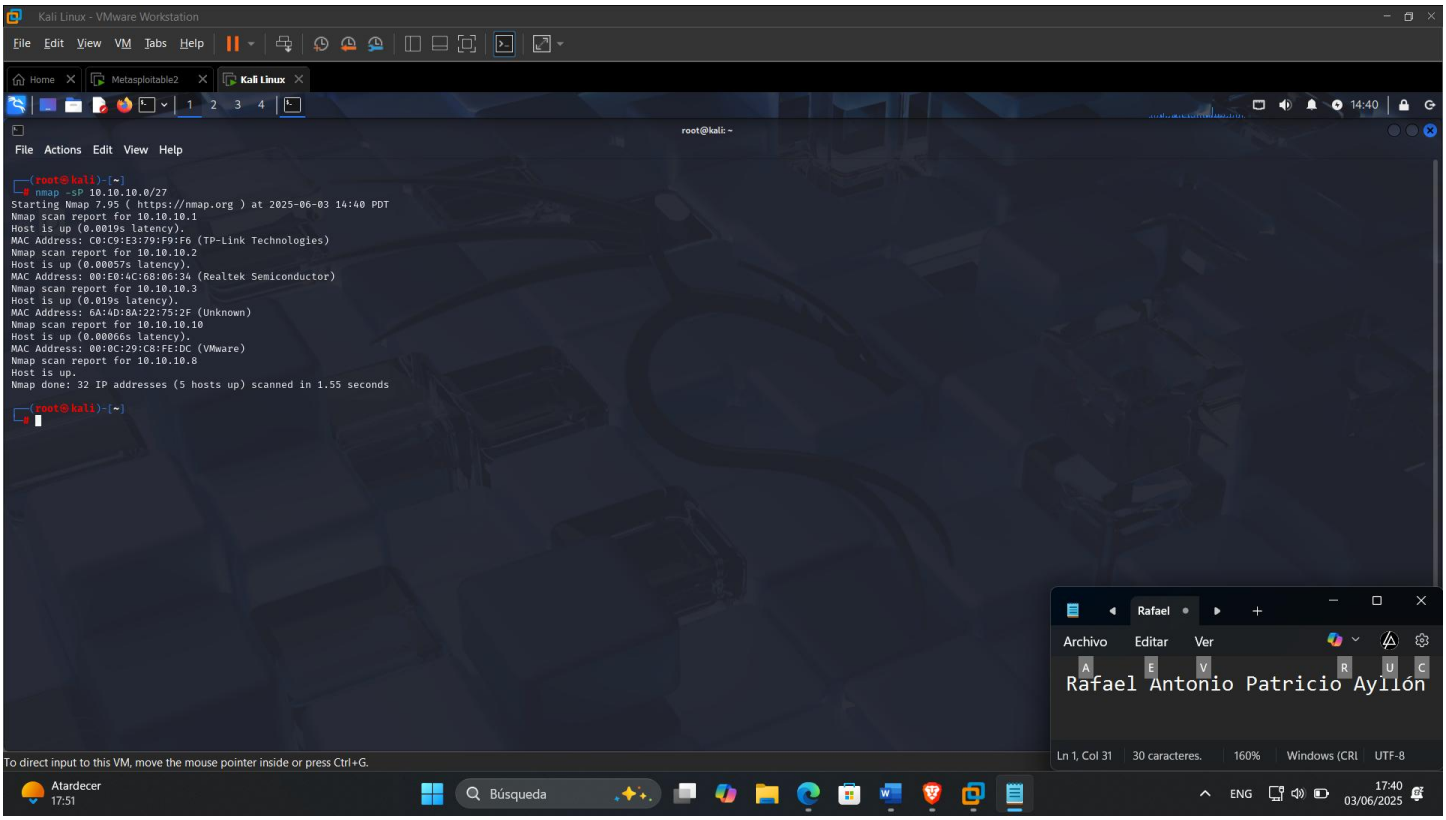


De igual forma a un rango de puertos:



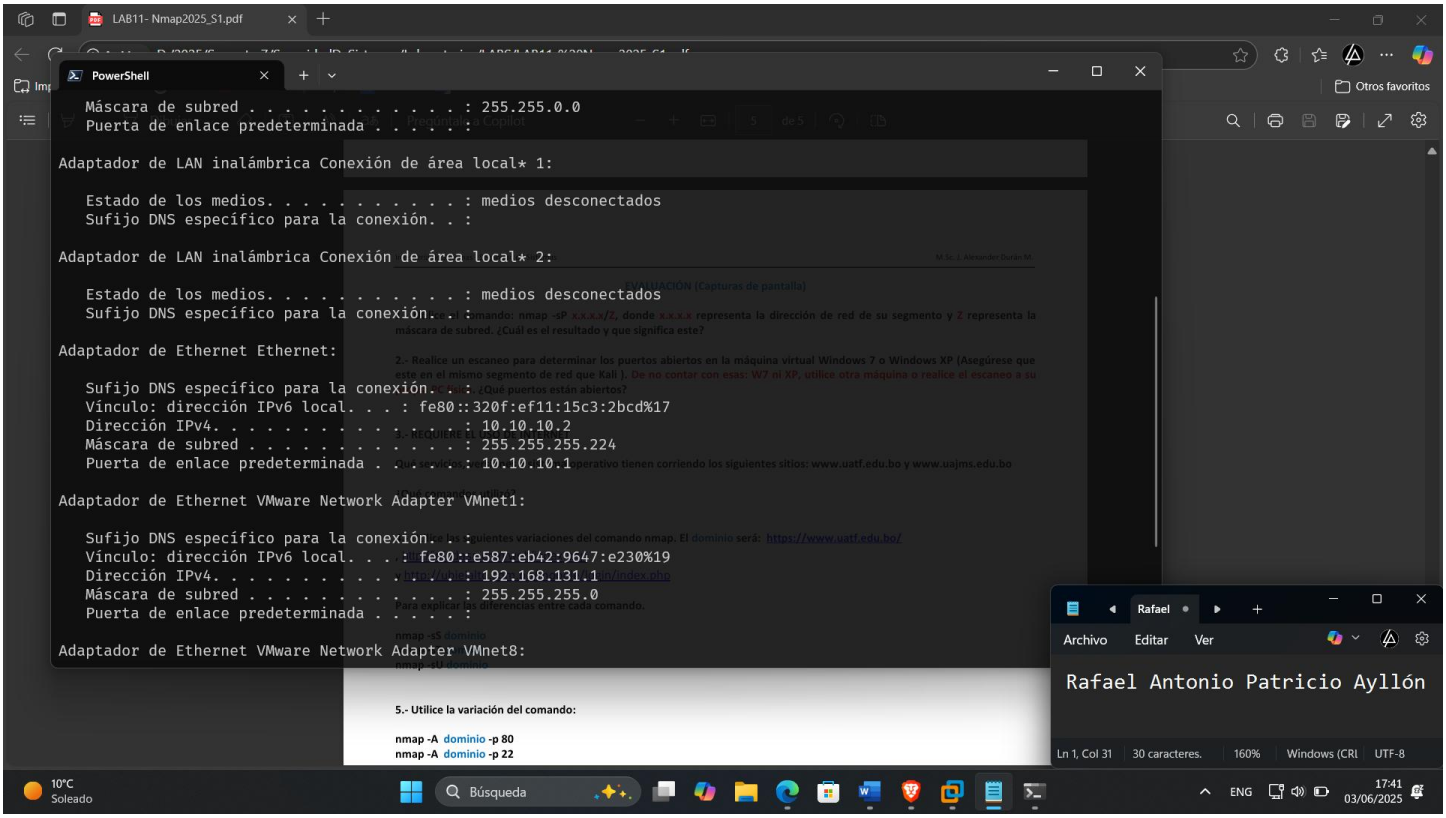
EVALUACIÓN (Capturas de pantalla)

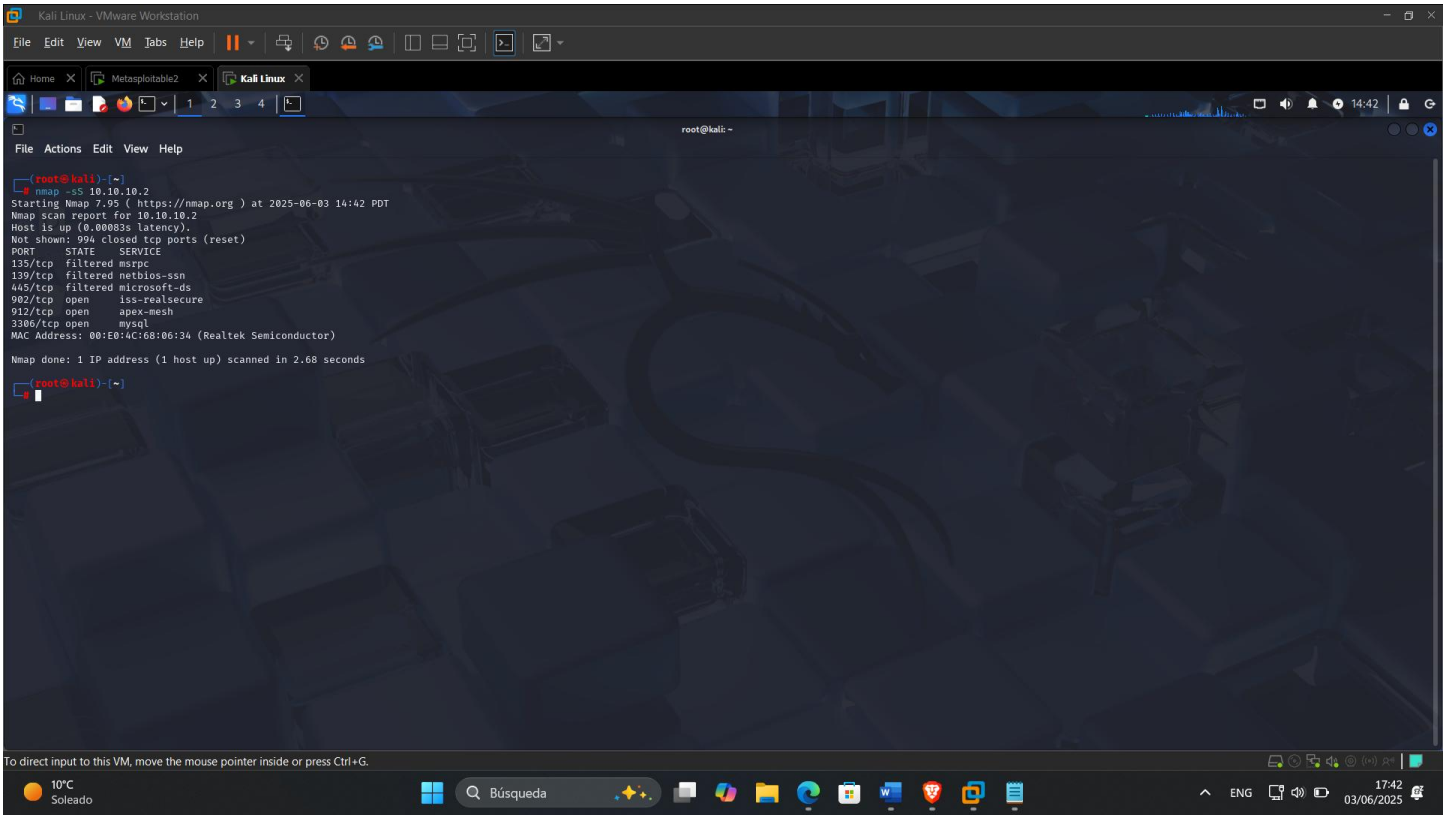
1.- Utilice el comando: nmap-sP x.x.x.x/Z, donde x.x.x.x representa la dirección de red de su segmento y Z representa la máscara de subred. ¿Cuál es el resultado y que significa este?



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?





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:

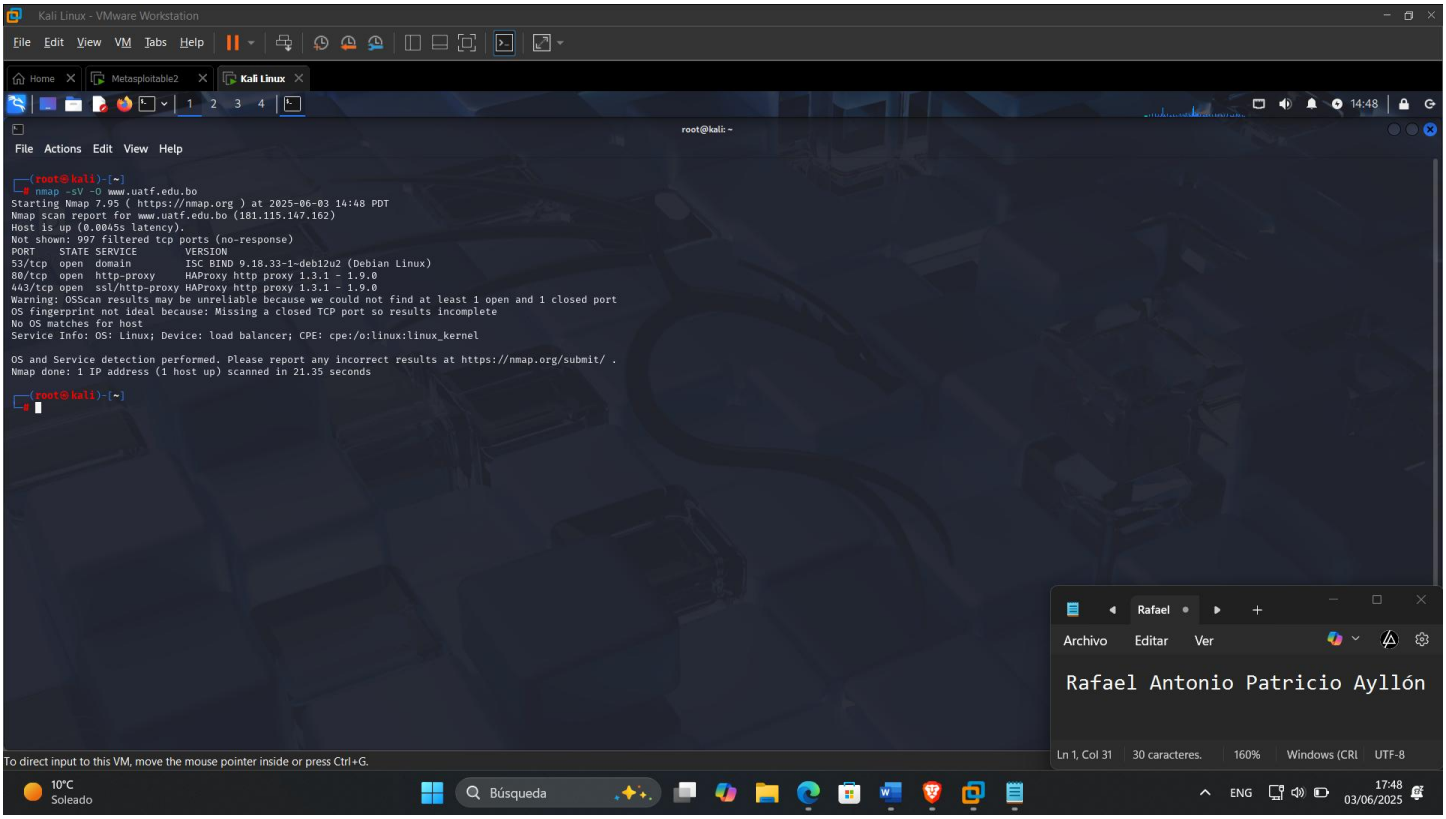
PUERTO	ESTADO	SERVICIO	SIGNIFICADO BREVE
135	filtered	msrpc	Filtrado por firewall, no respondió.
139	filtered	netbios-ssn	Igual que el anterior.
445	filtered	microsoft-ds	También filtrado.
902	open	iss-realsecure	Abierto, puede ser usado por VMware.
912	open	apex-mesh	Abierto, usado por algunas aplicaciones 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.uajms.edu.bo

¿Qué comandos utilizó?

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



Dirección IP: 181.115.147.162

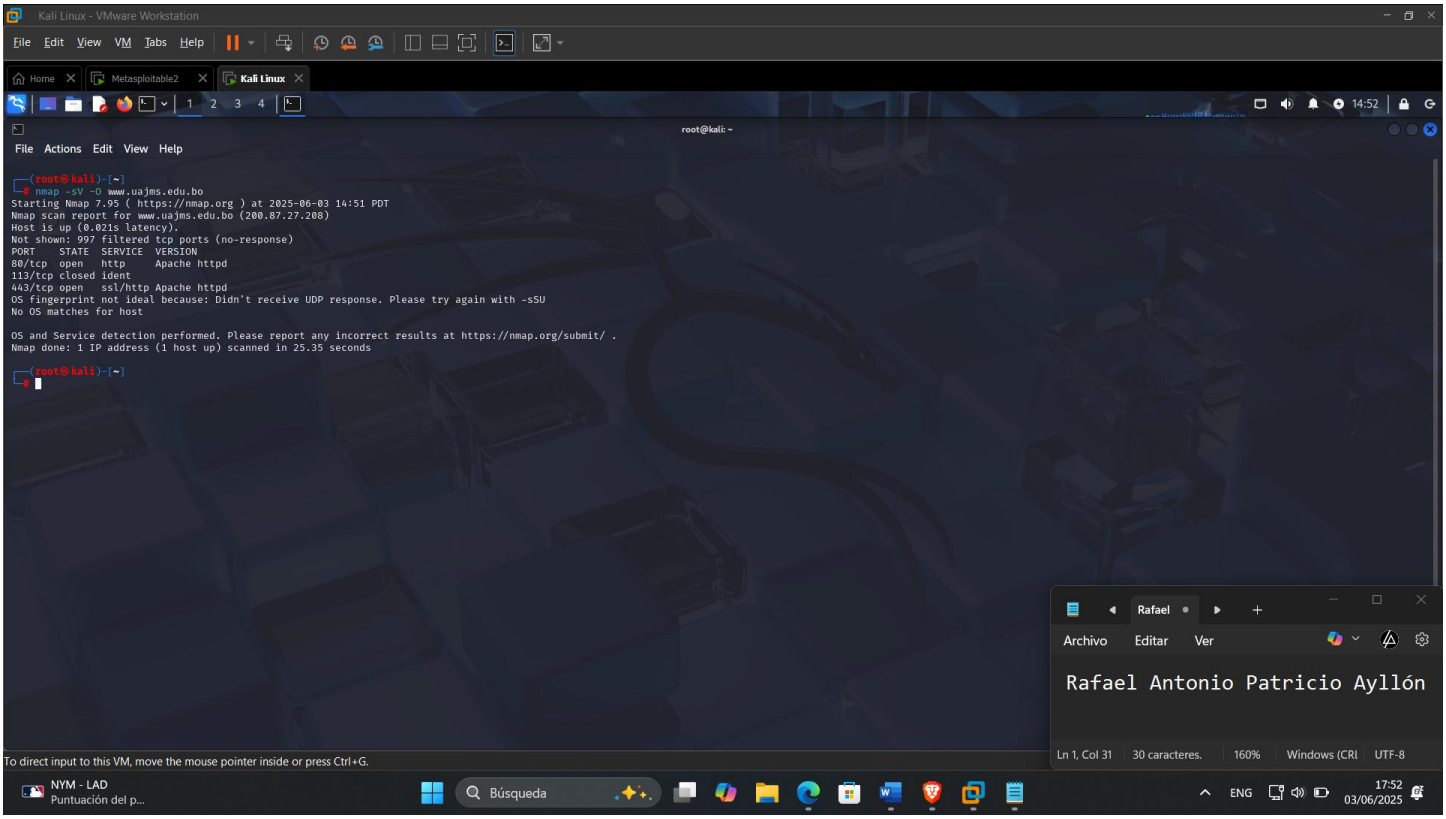
Puertos abiertos y servicios detectados:

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



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.

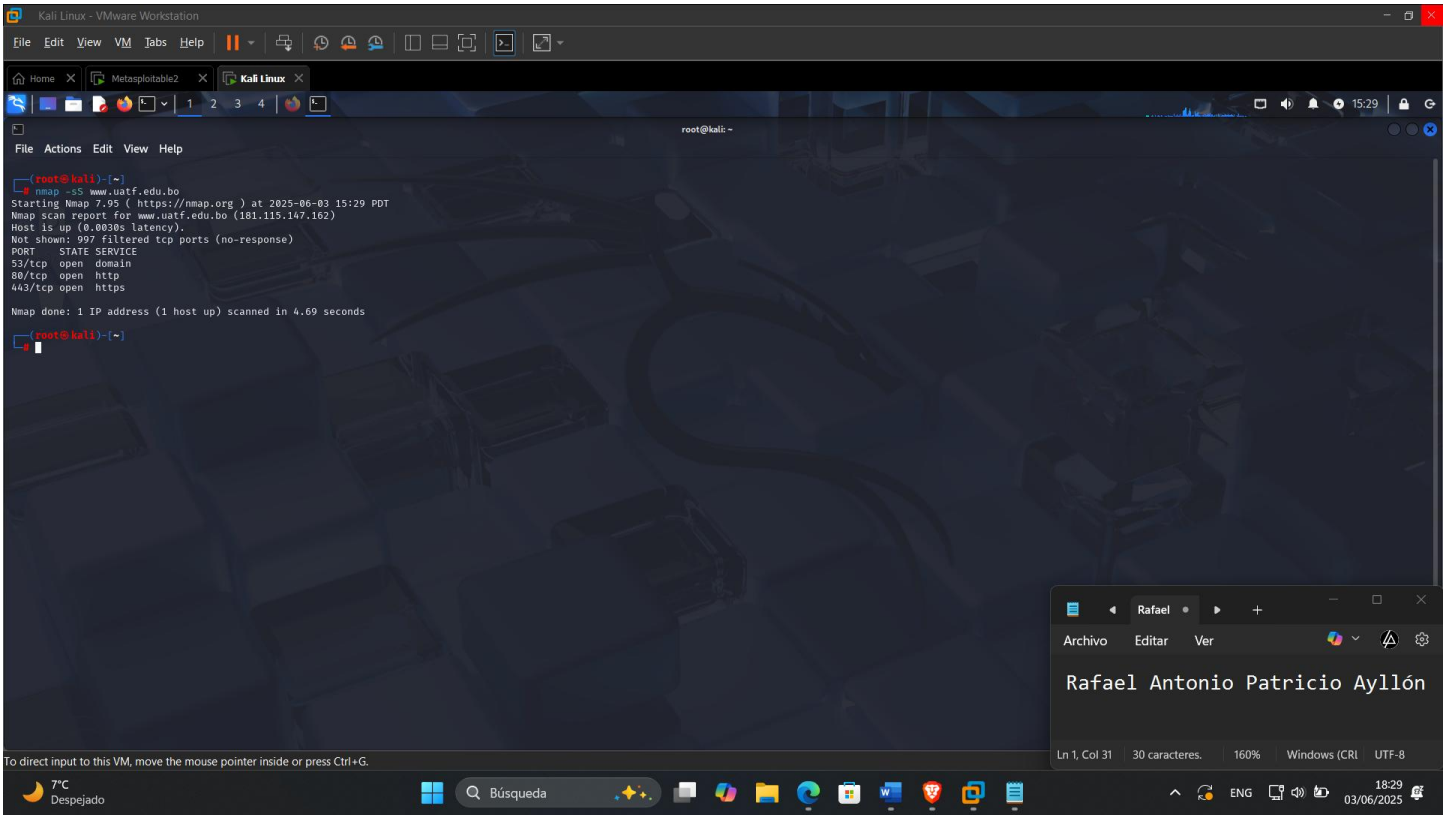
nmap-sS dominio

nmap-sT dominio

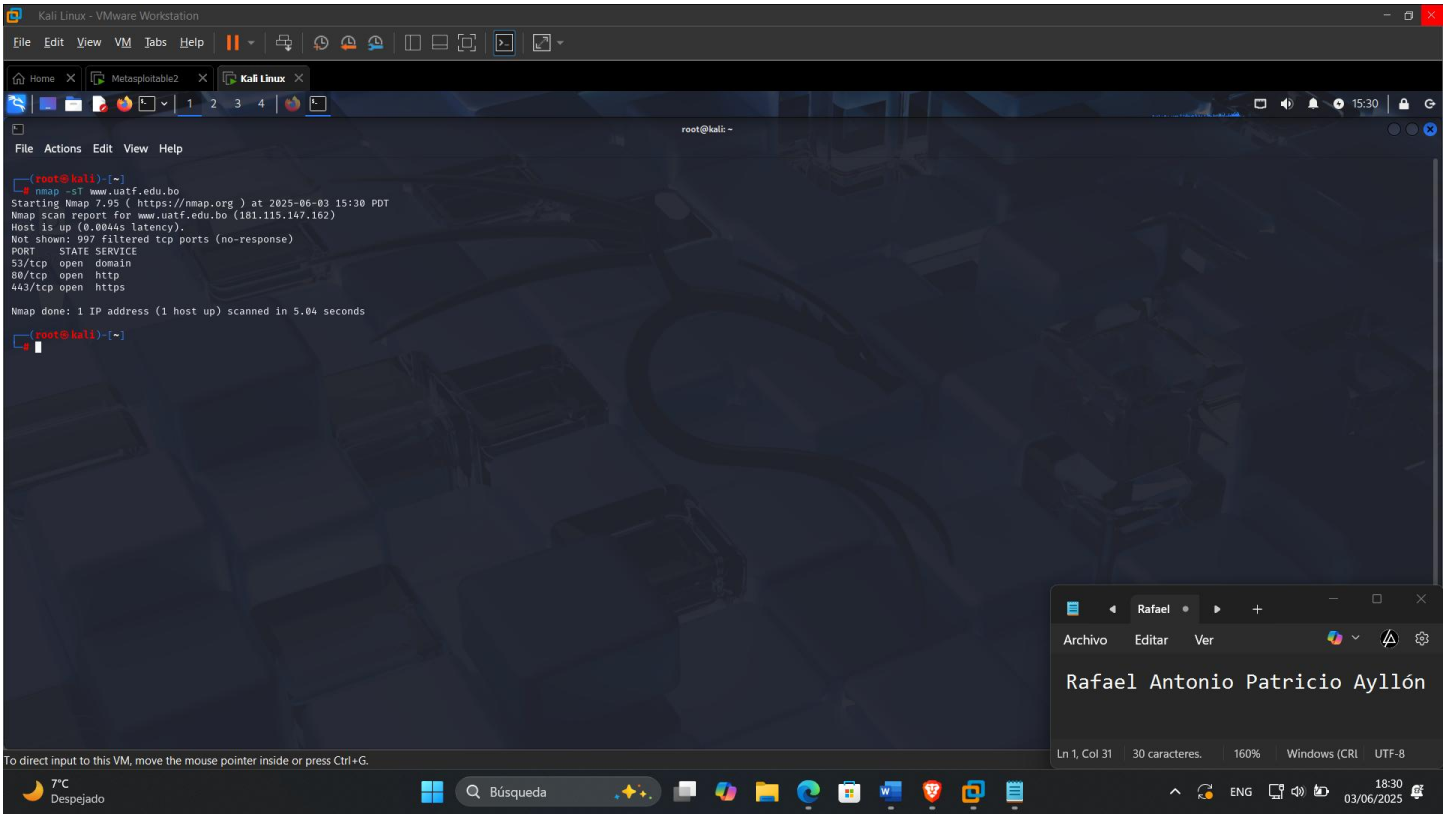
nmap-sU dominio

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

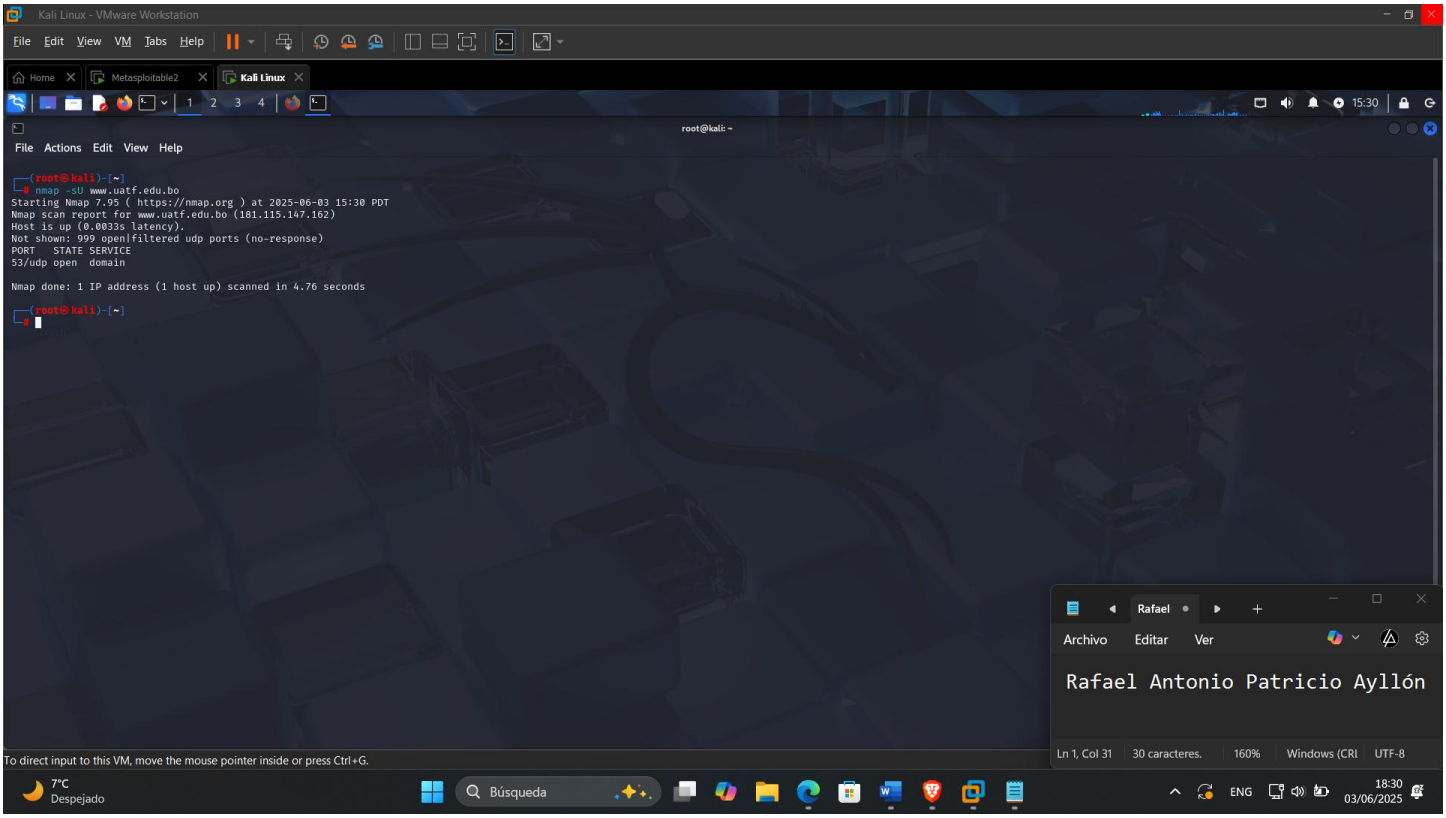
nmap -sS www.uatf.edu.bo



nmap -sT www.uatf.edu.bo

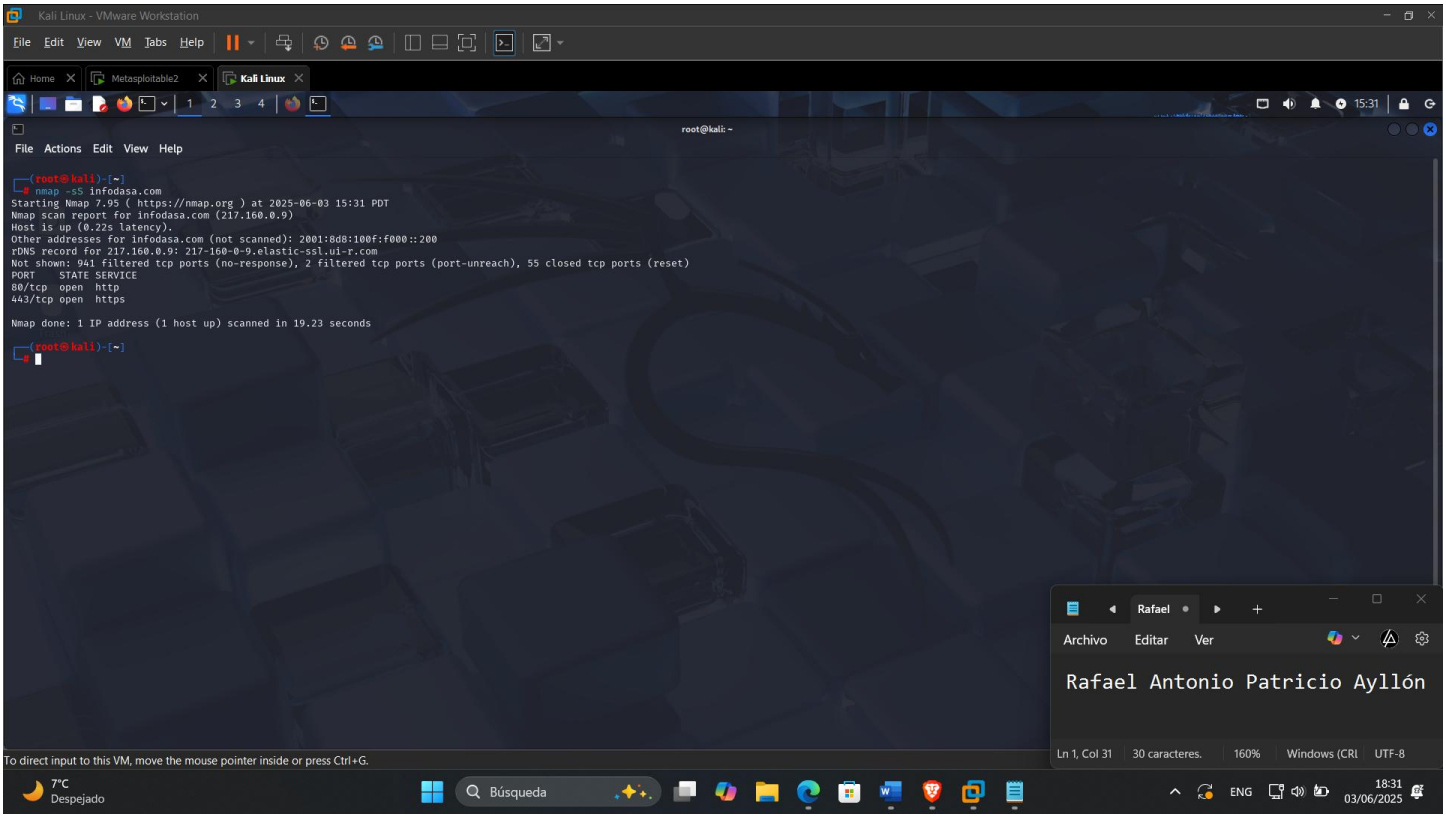


nmap -sU www.uatf.edu.bo

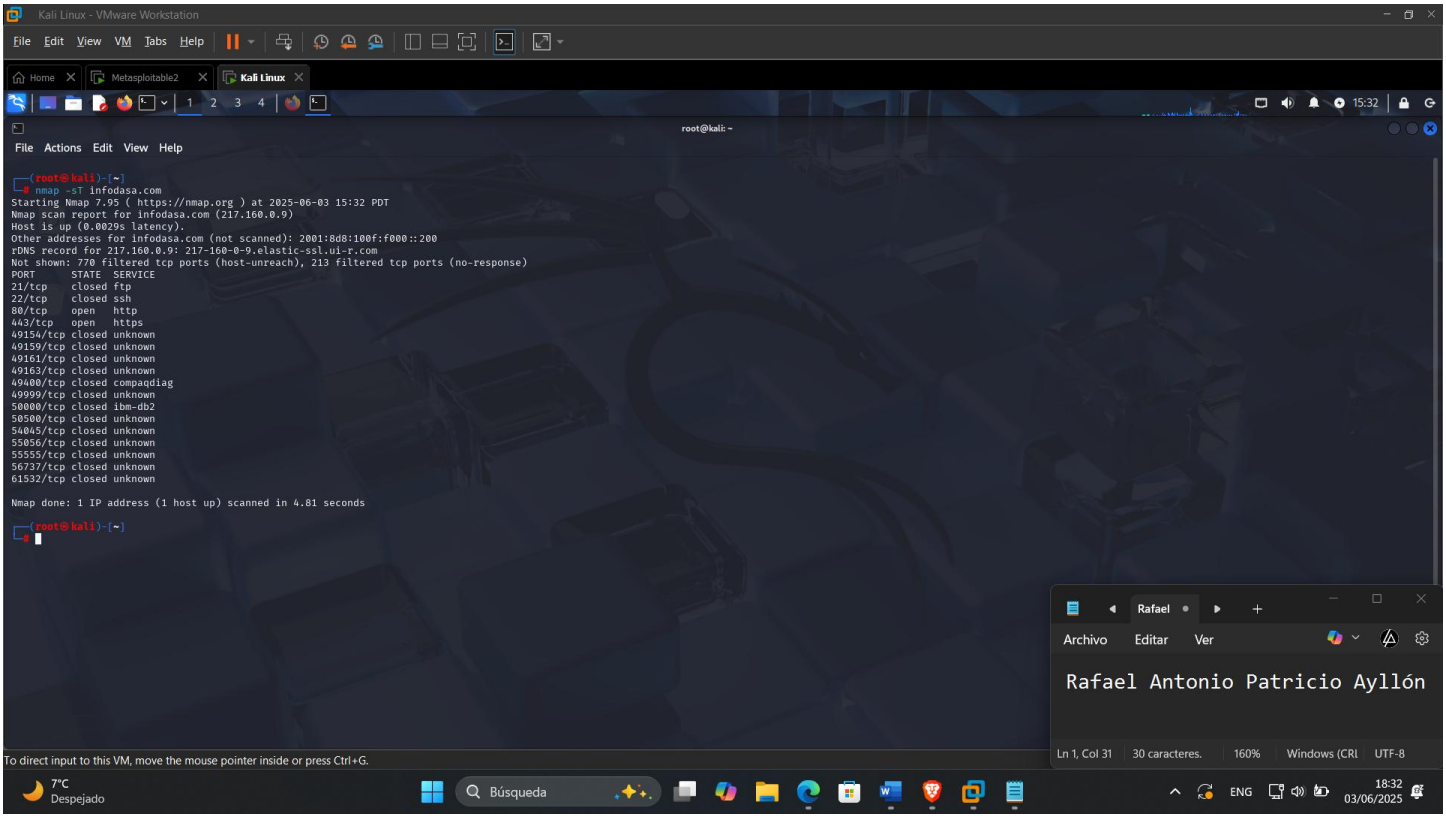


http://infodasa.com/web/index.php

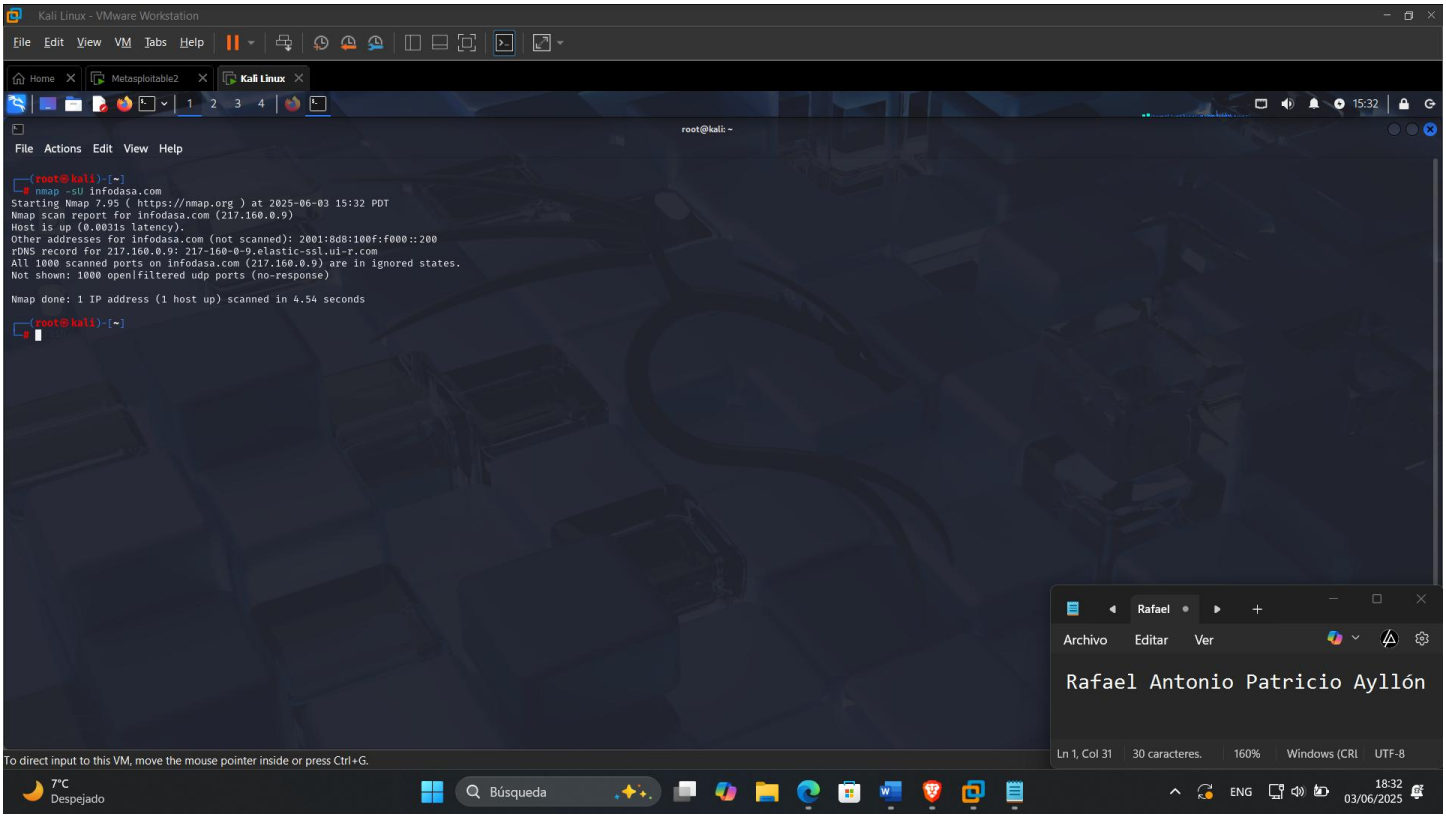
nmap -sS infodasa.com



nmap -sT infodasa.com

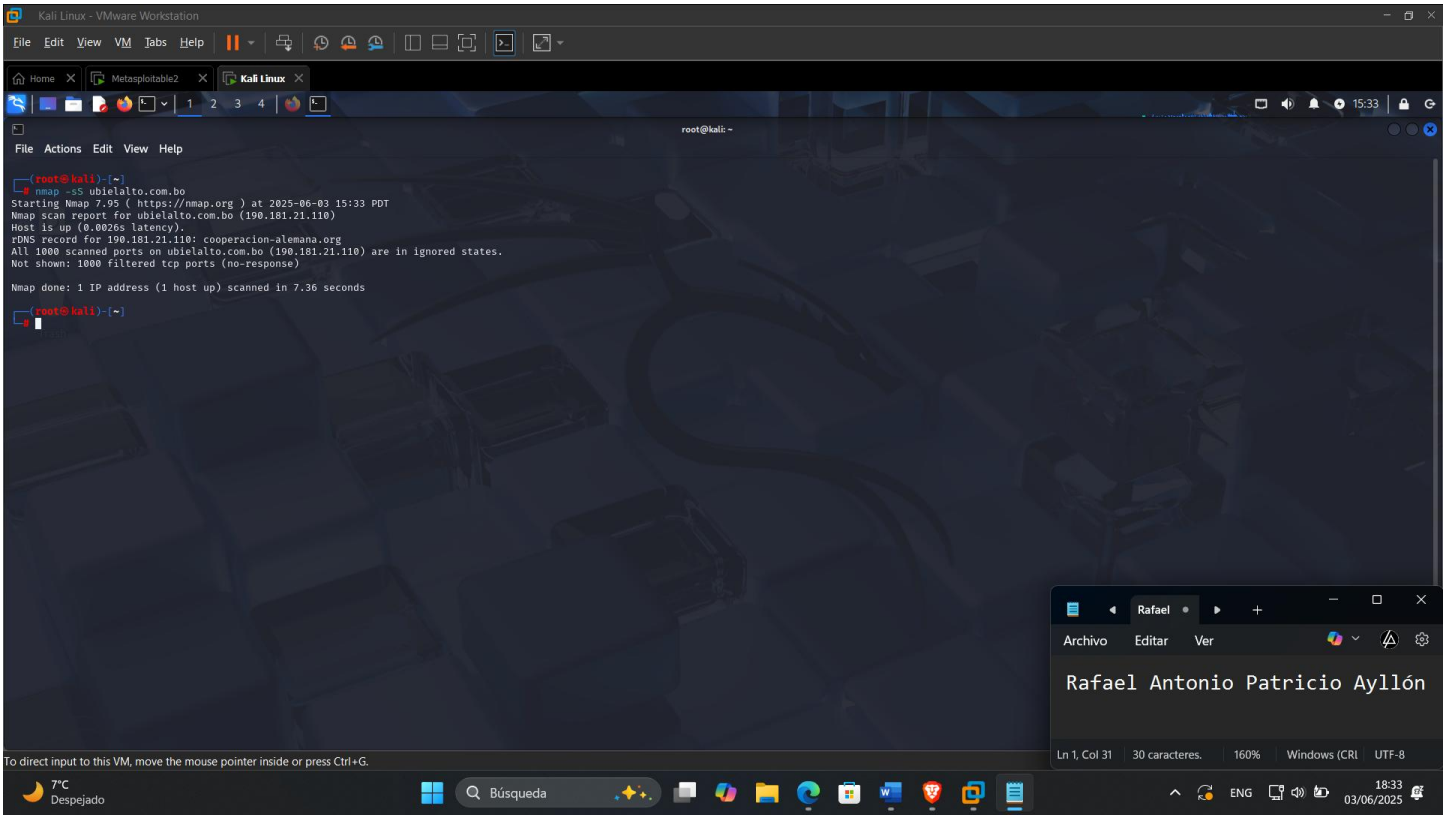


nmap -sU infodasa.com

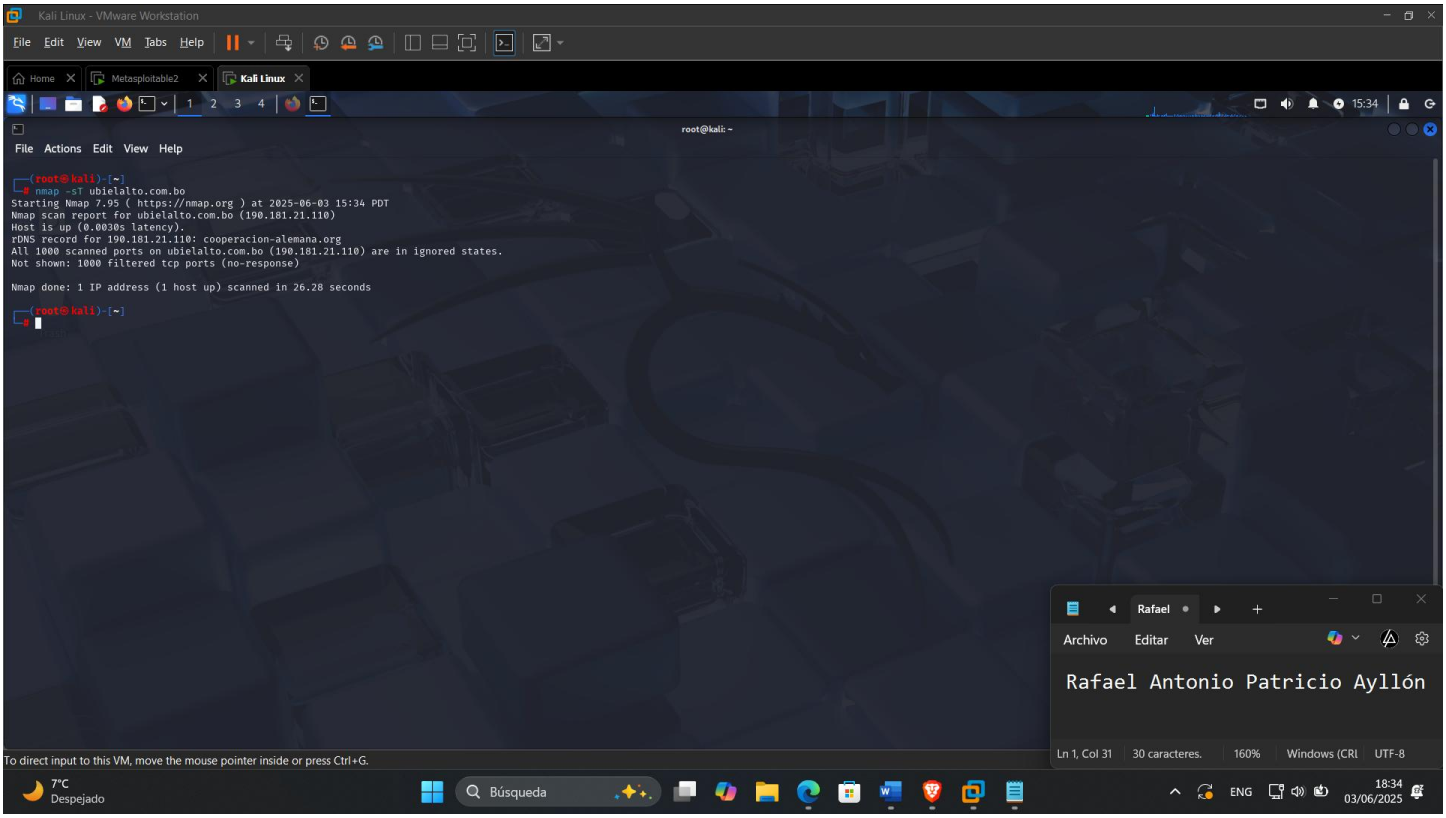


http://ubielalto.com.bo/moodle/login/index.php

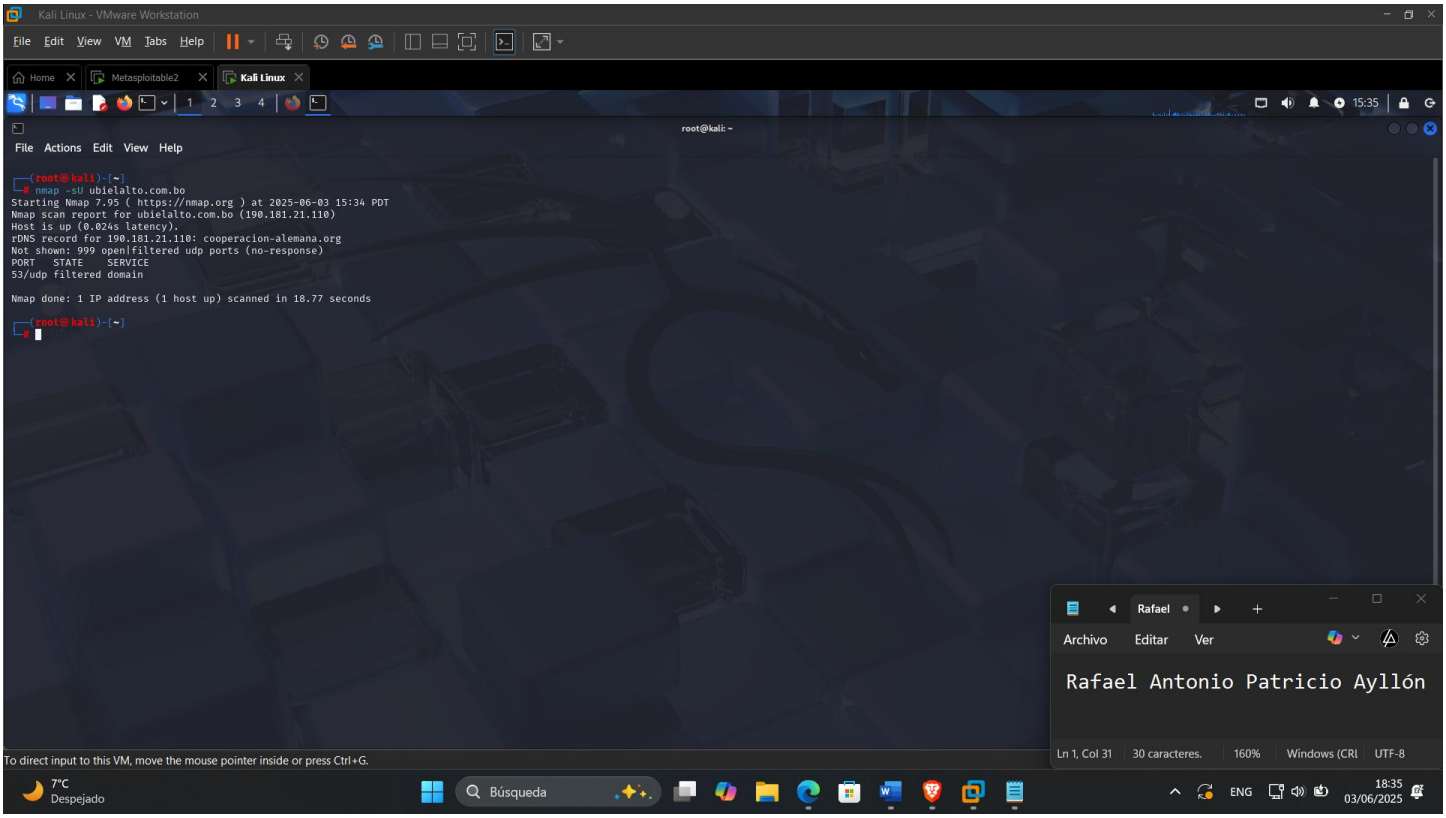
nmap -sS ubielalto.com.bo



nmap -sT ubielalto.com.bo



nmap -sU ubielalto.com.bo



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.

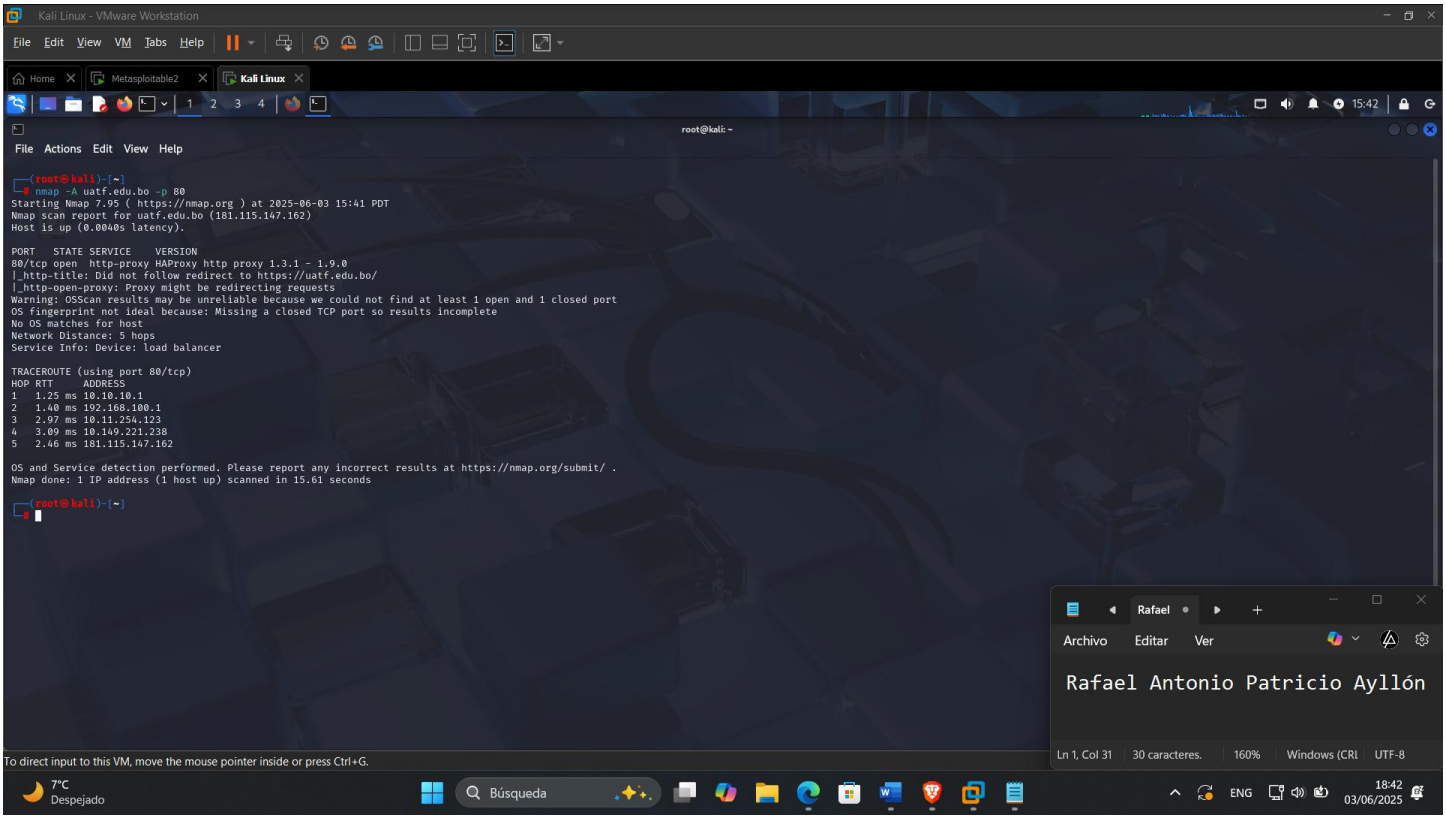
5.- Utilice la variación del comando:

nmap-A dominio-p 80

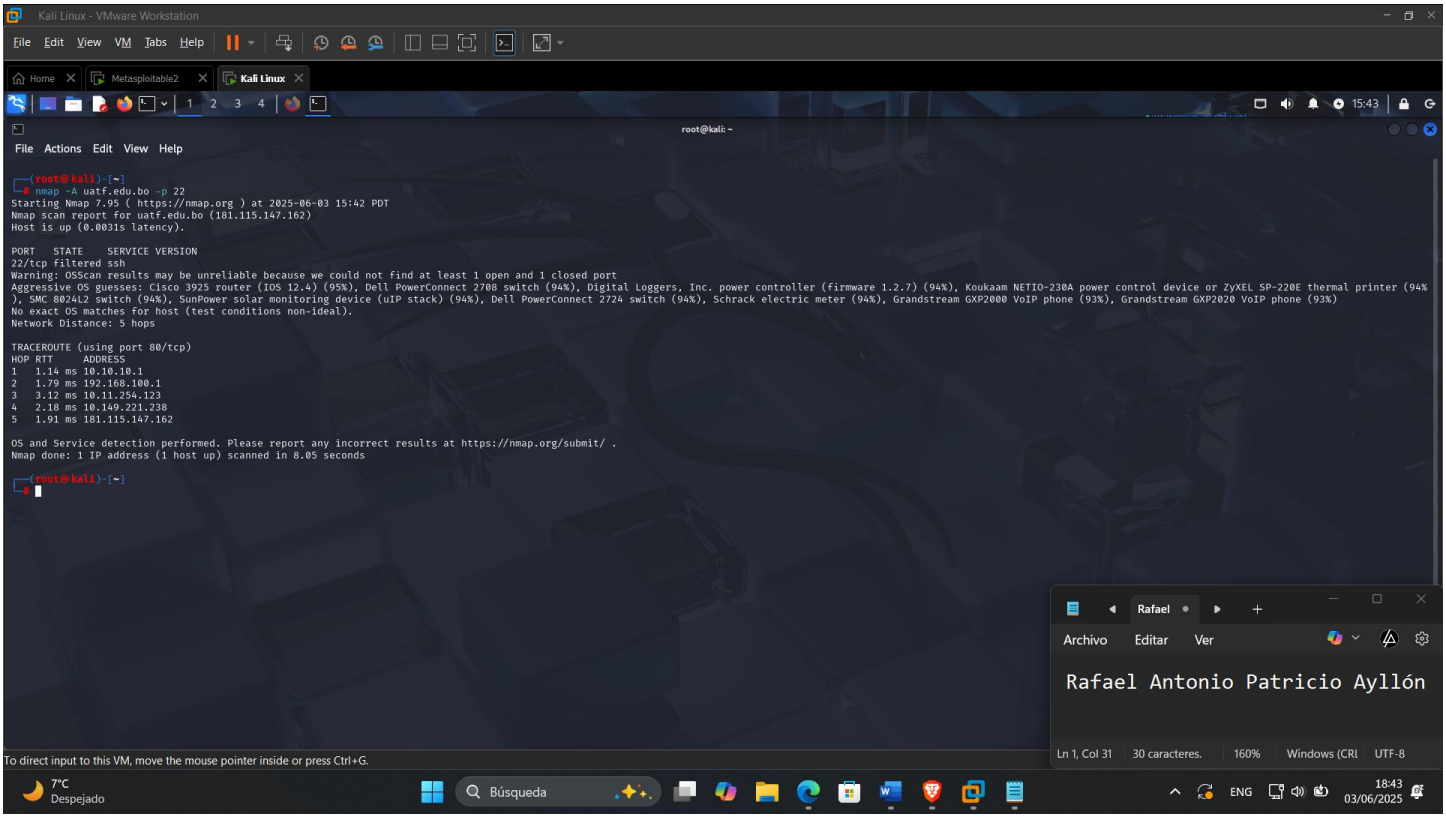
nmap-A dominio-p 22

¿Qué tipo de escaneo significa la letra A?

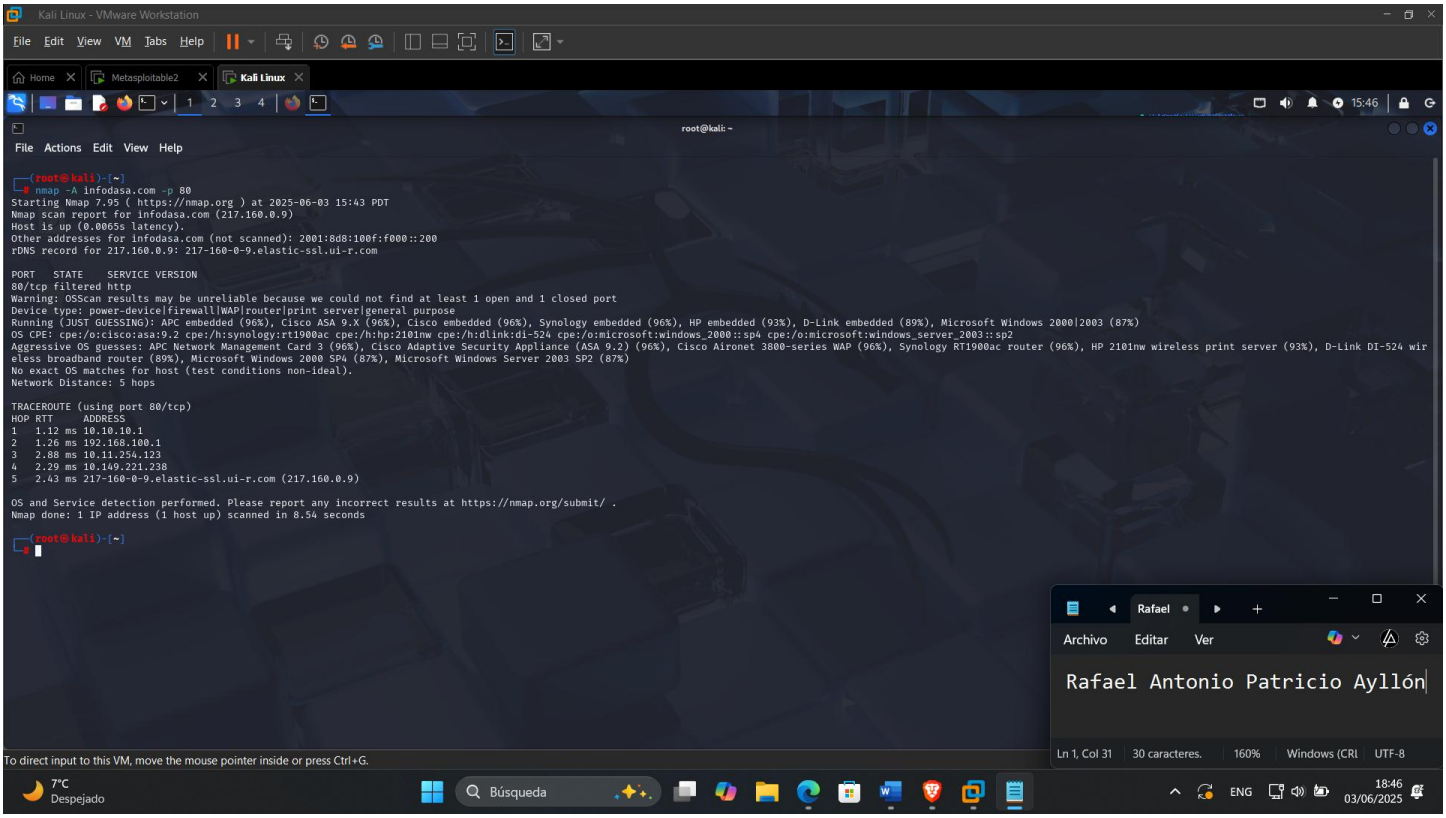
nmap -A uatf.edu.bo -p 80



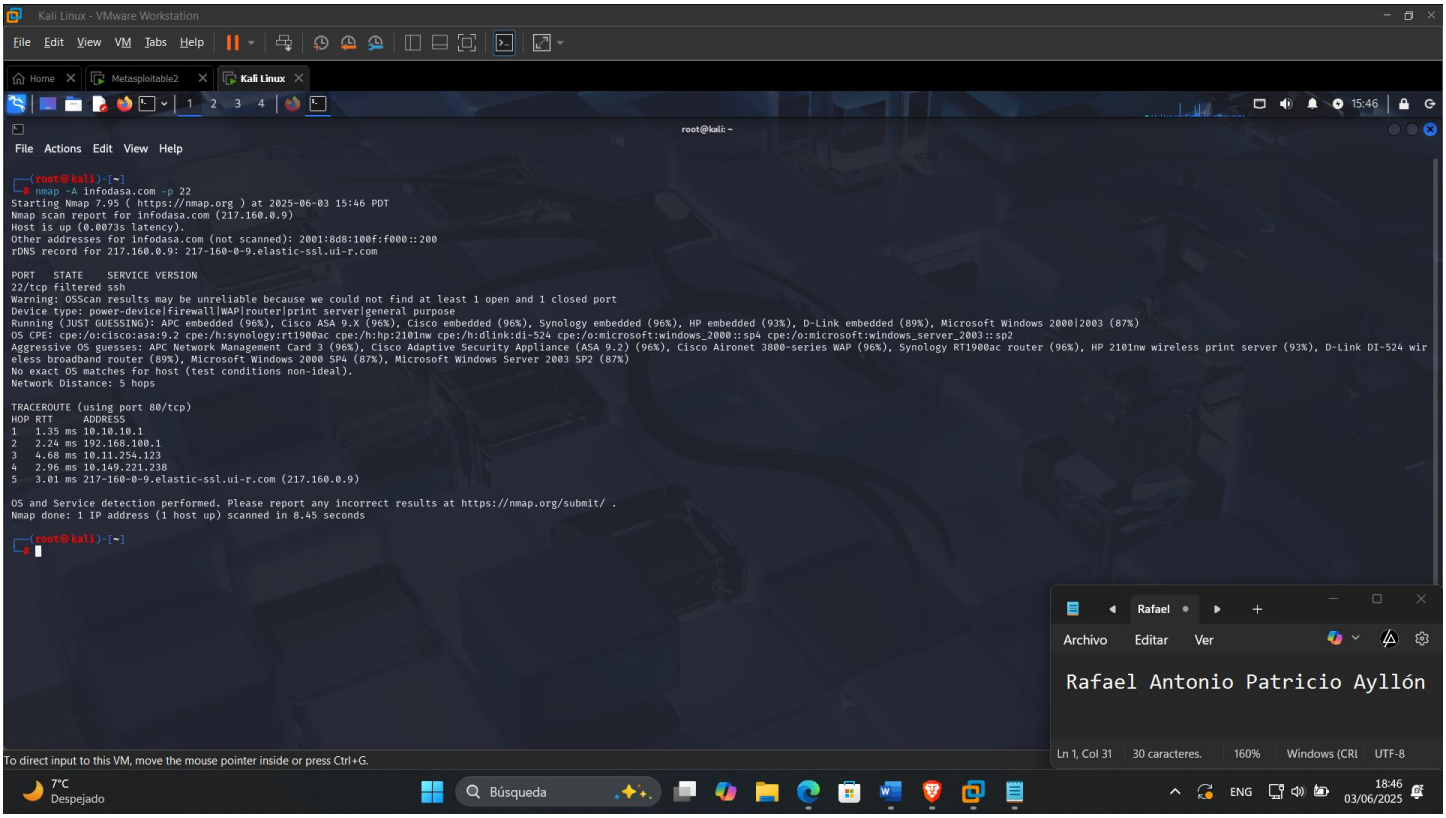
nmap -A uatf.edu.bo -p 22



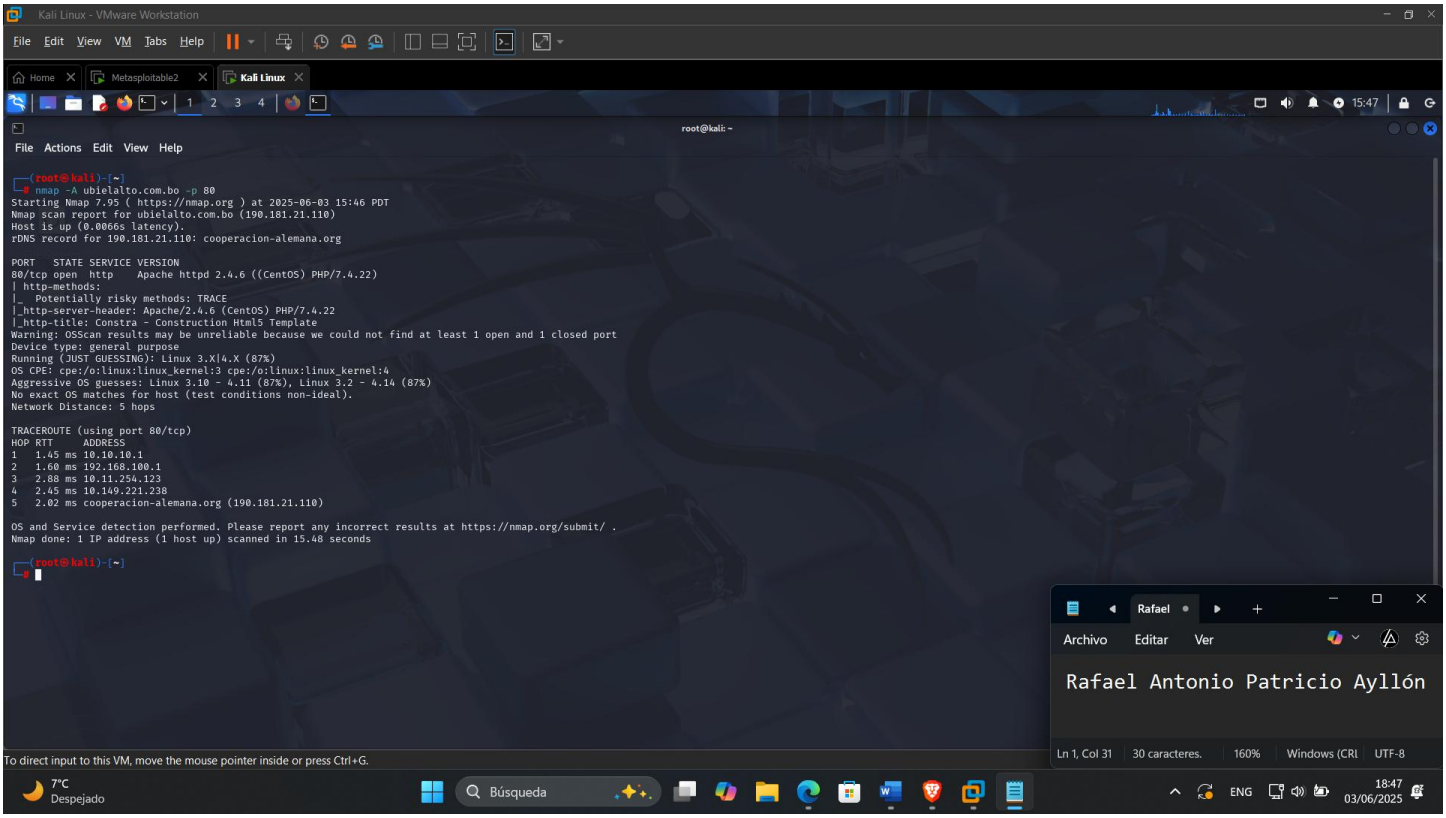
nmap -A infodasa.com -p 80



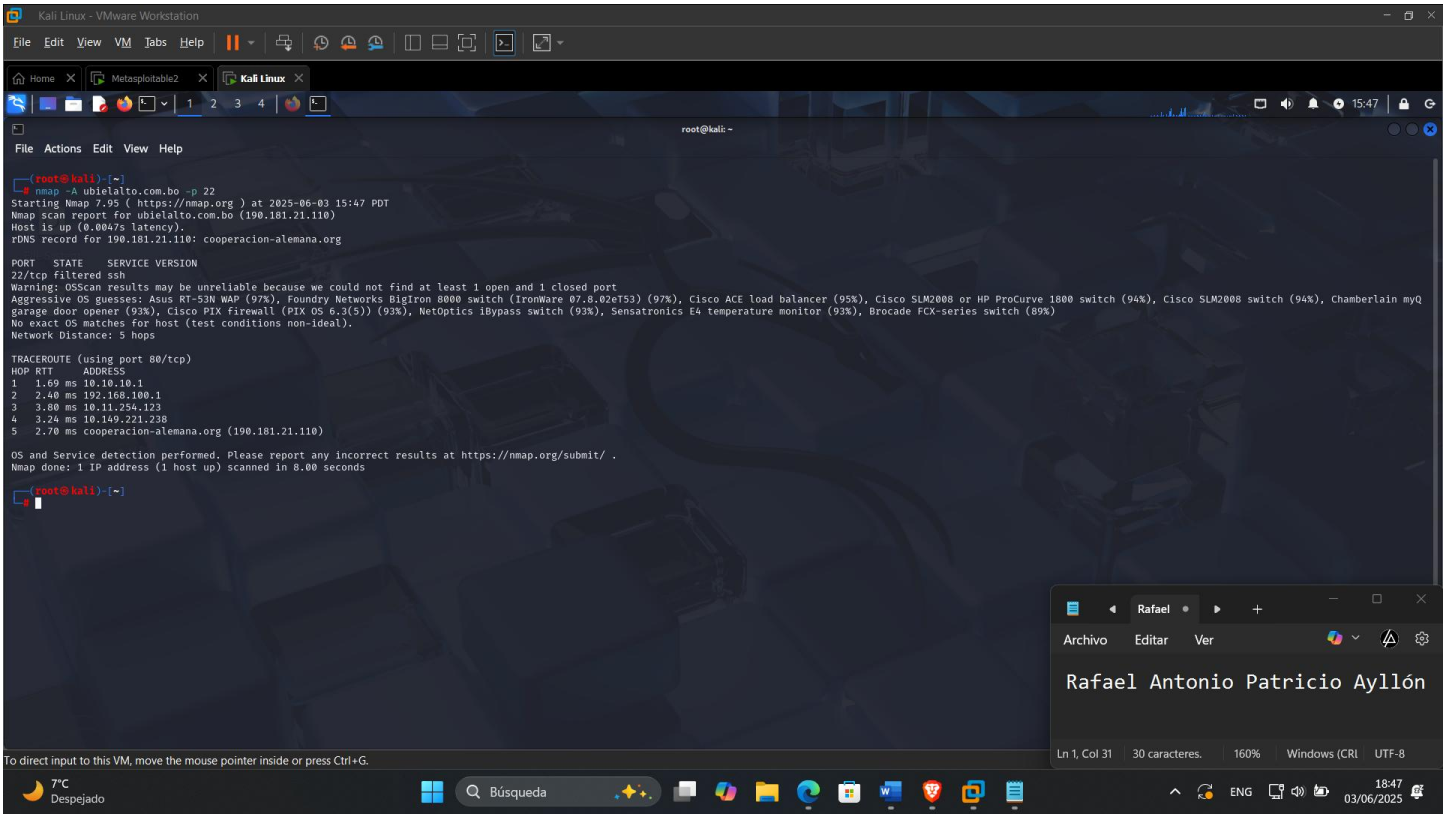
nmap -A infodasa.com -p 22



nmap -A ubielalto.com.bo -p 80



nmap -A ubielalto.com.bo -p 22



-A significa

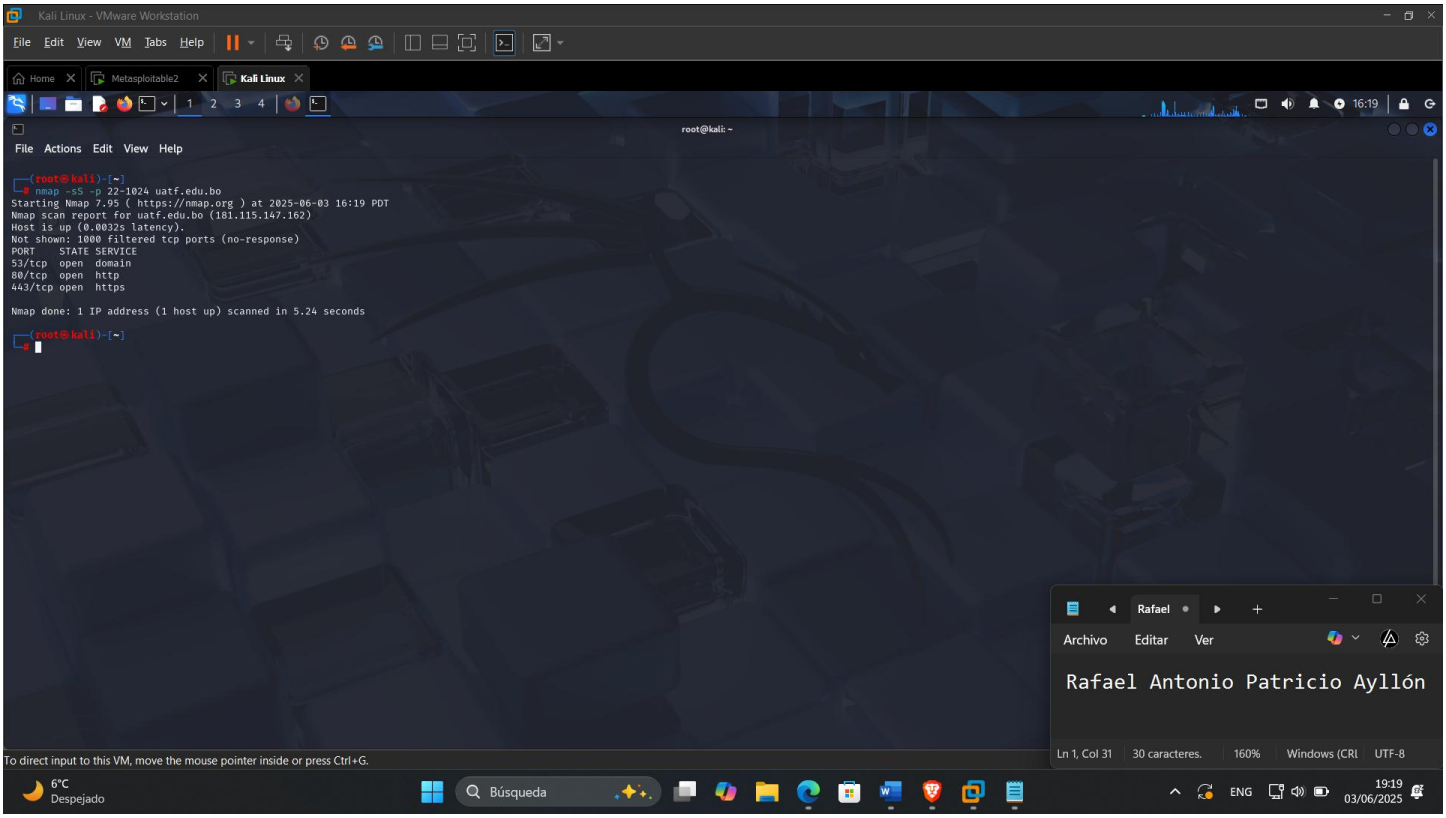
Escaneo agresivo que combina:

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

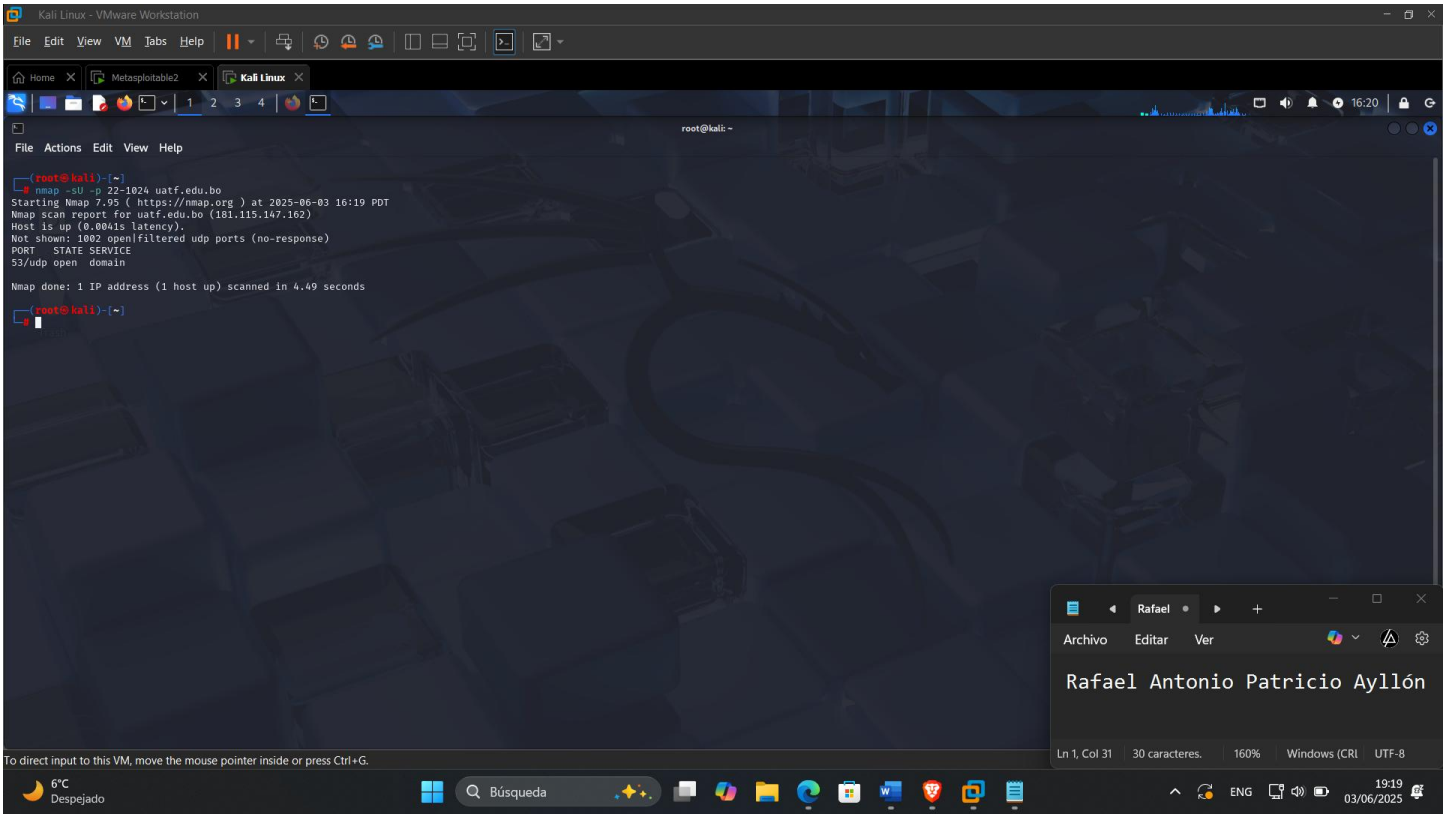
Es un escaneo completo y detallado.

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.

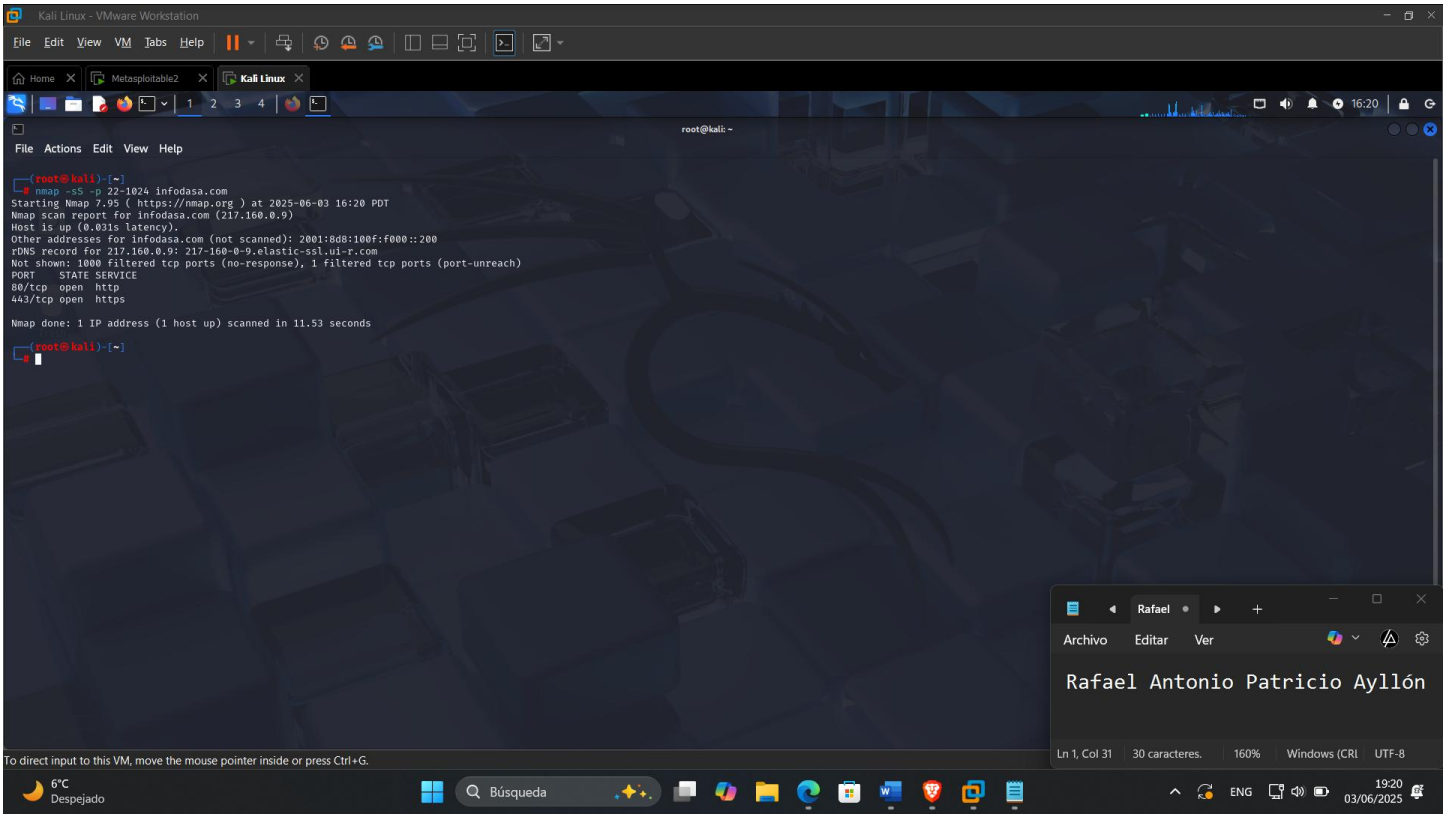
nmap -sS -p 22-1024 uatf.edu.bo # TCP



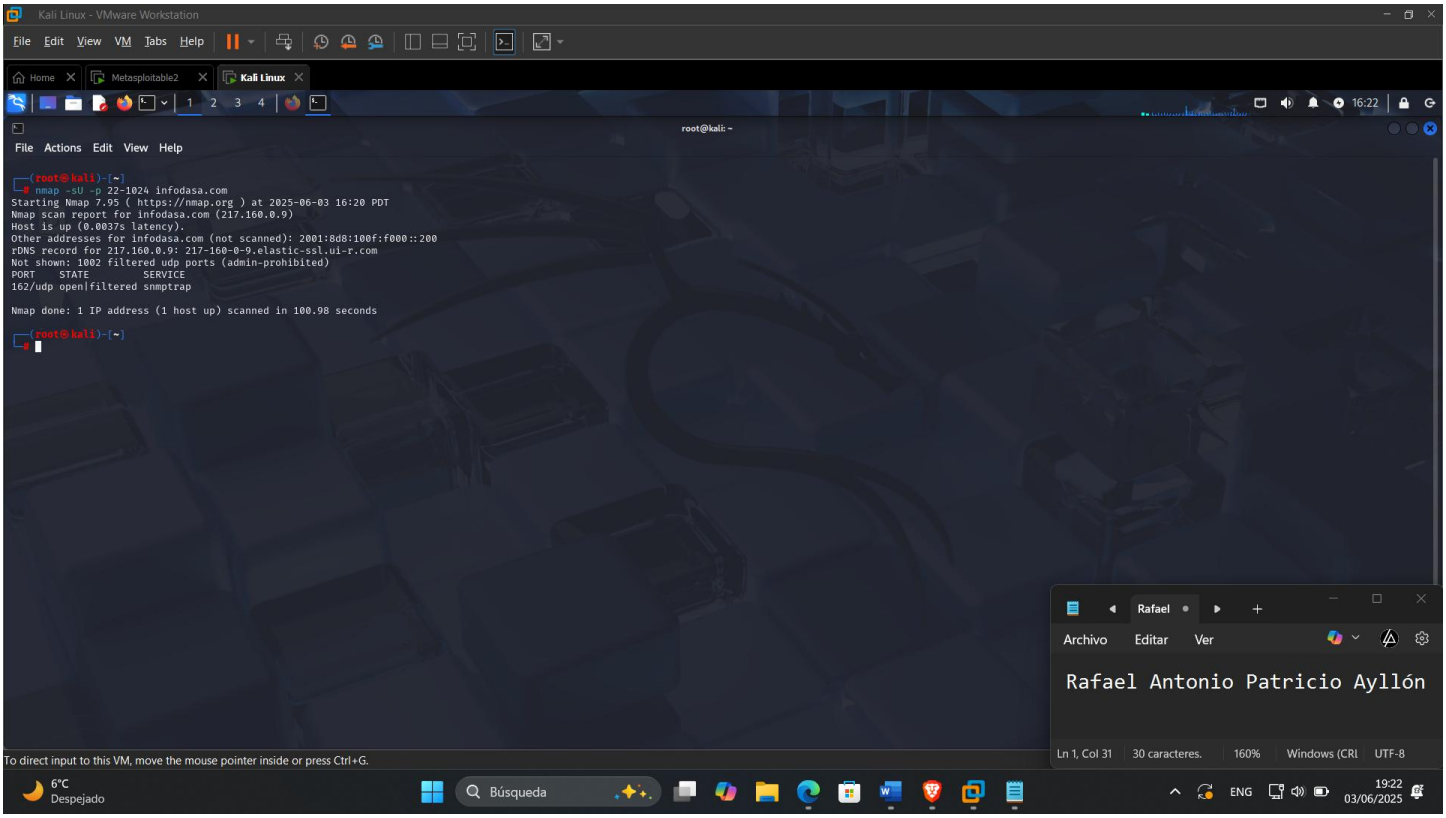
nmap -sU -p 22-1024 uatf.edu.bo # UDP



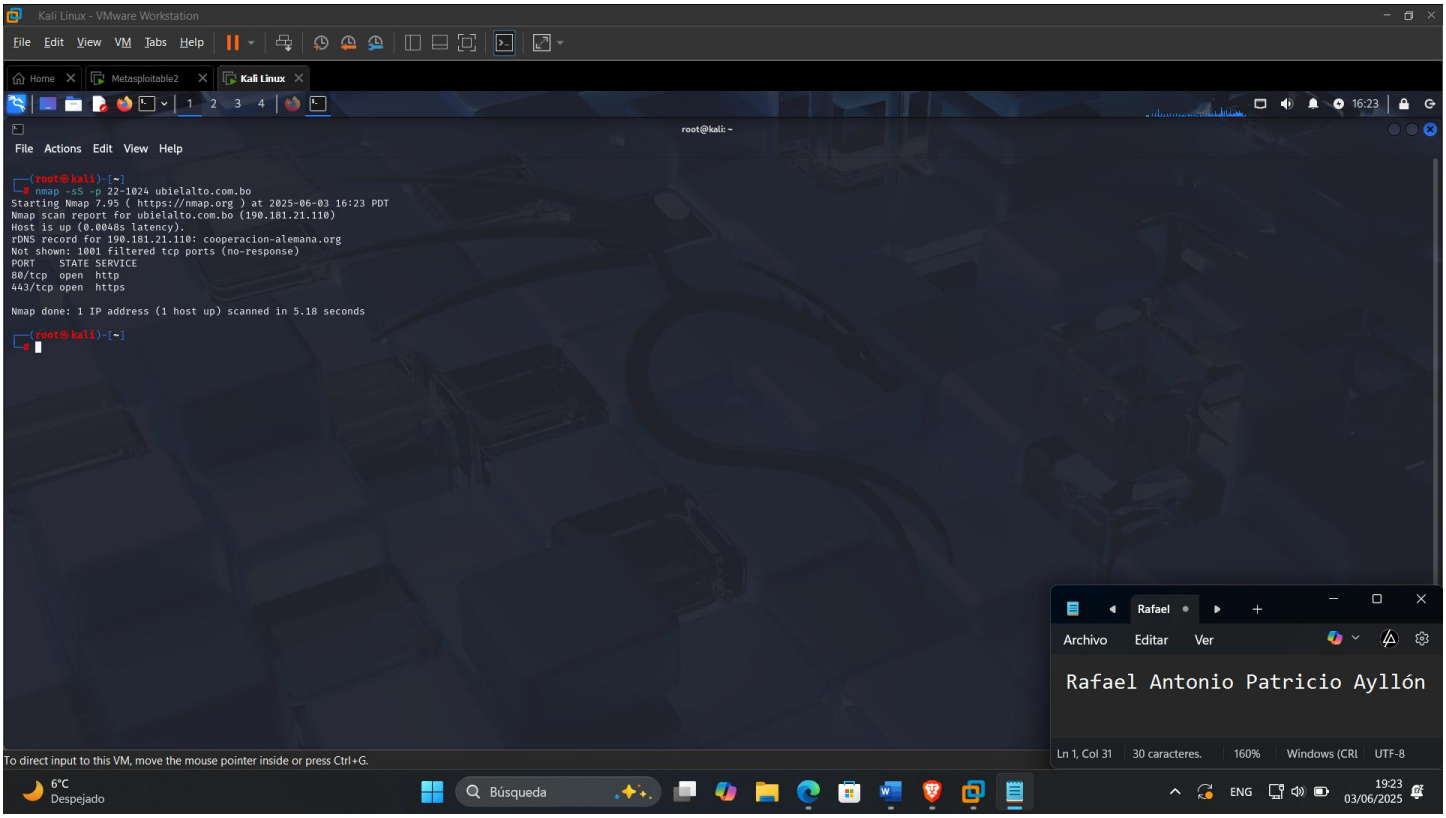
nmap -sS -p 22-1024 infodasa.com # TCP



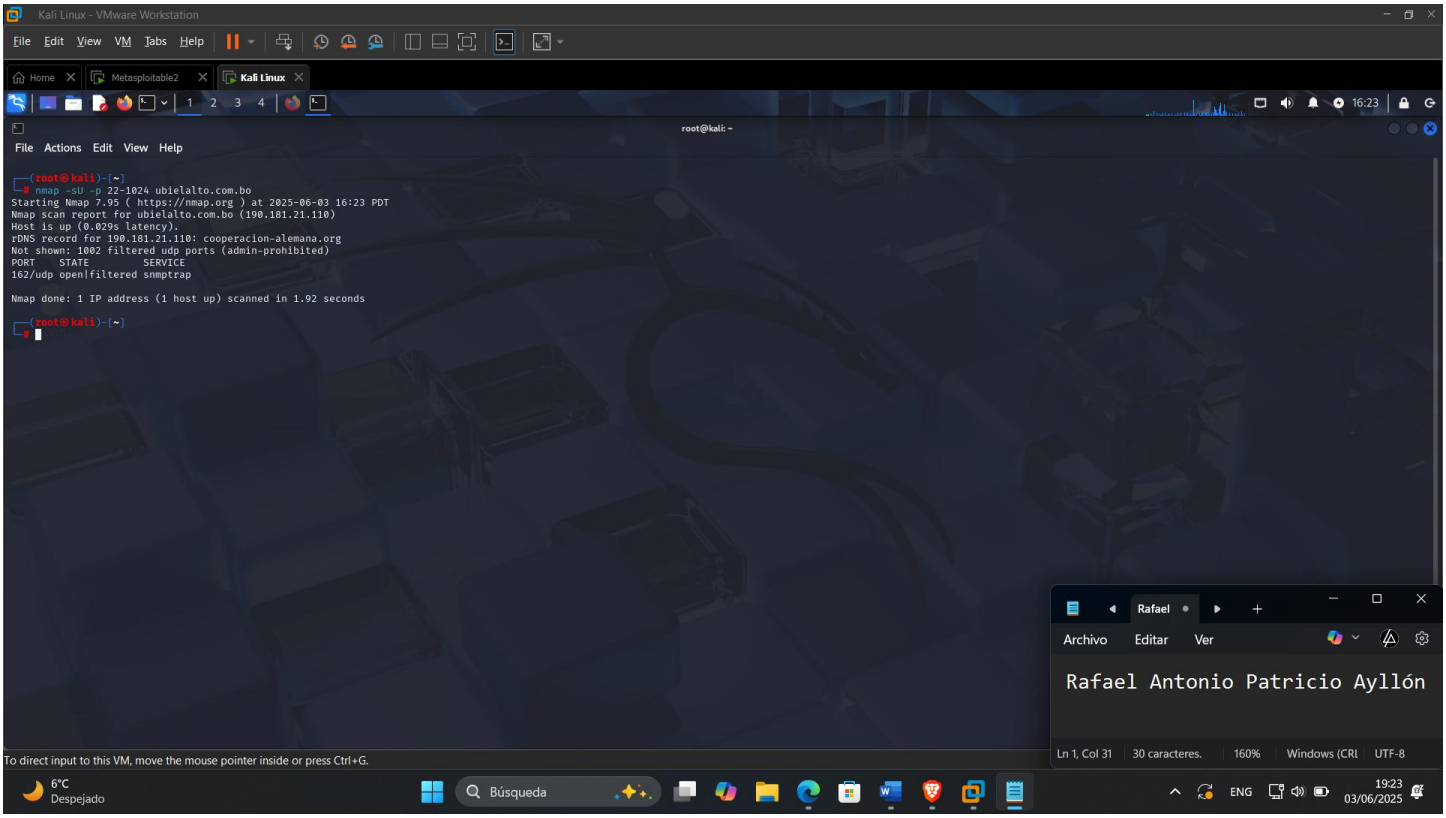
nmap -sU -p 22-1024 infodasa.com # UDP



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



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



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.