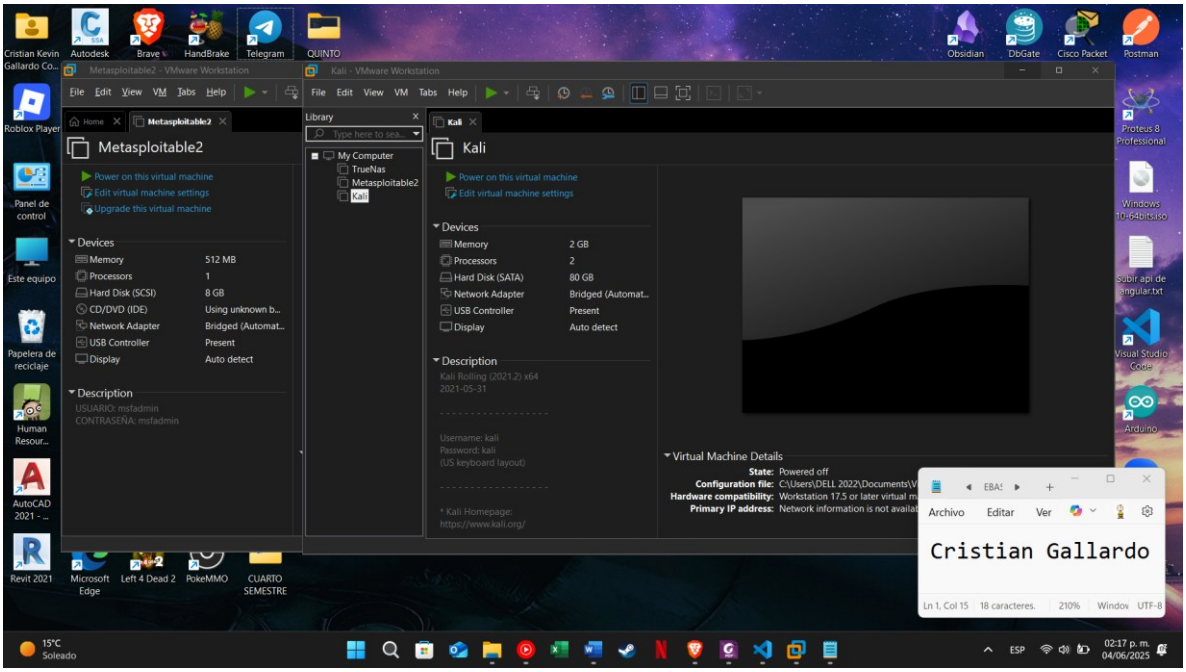
Laboratorio Nro 11

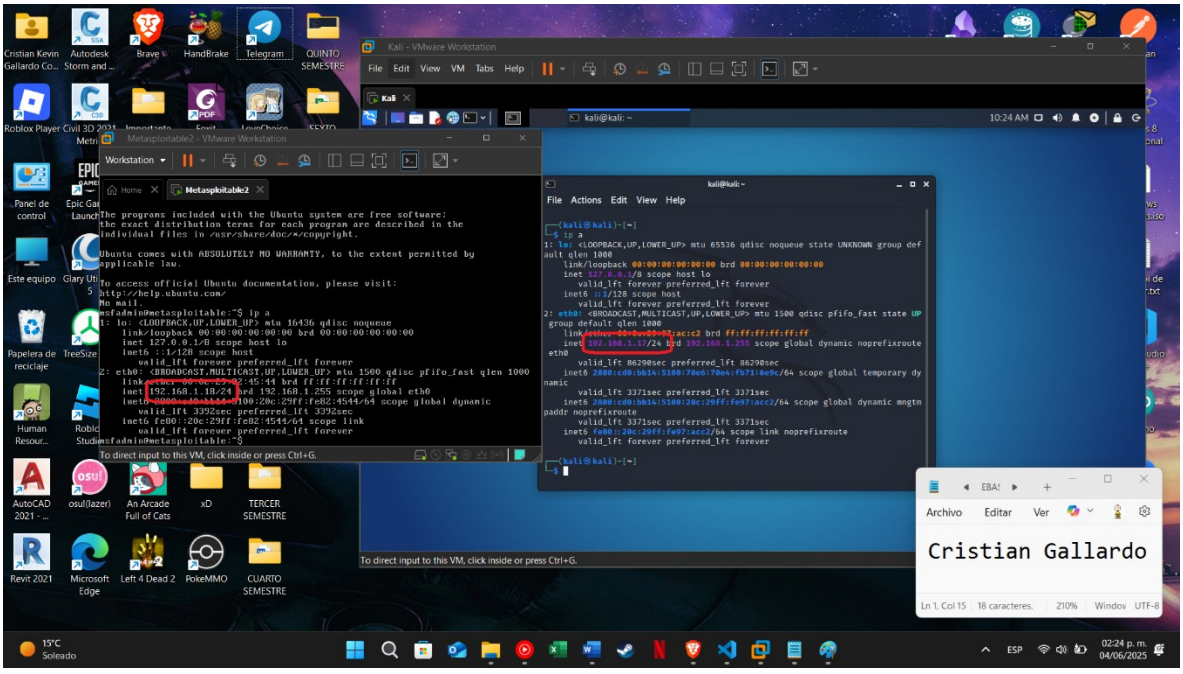
Univ. Cristian Kevin Gallardo Coro

DESARROLLO

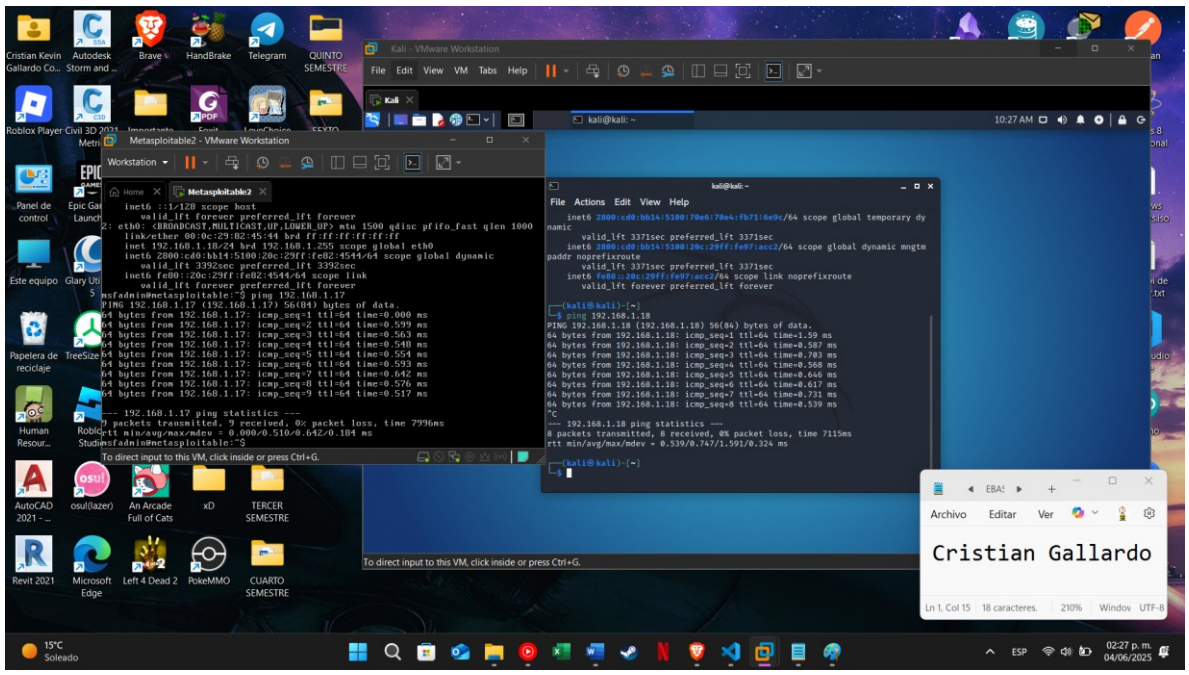
- Nos aseguramos de que nuestras máquinas virtuales estén configuradas en modo bridged



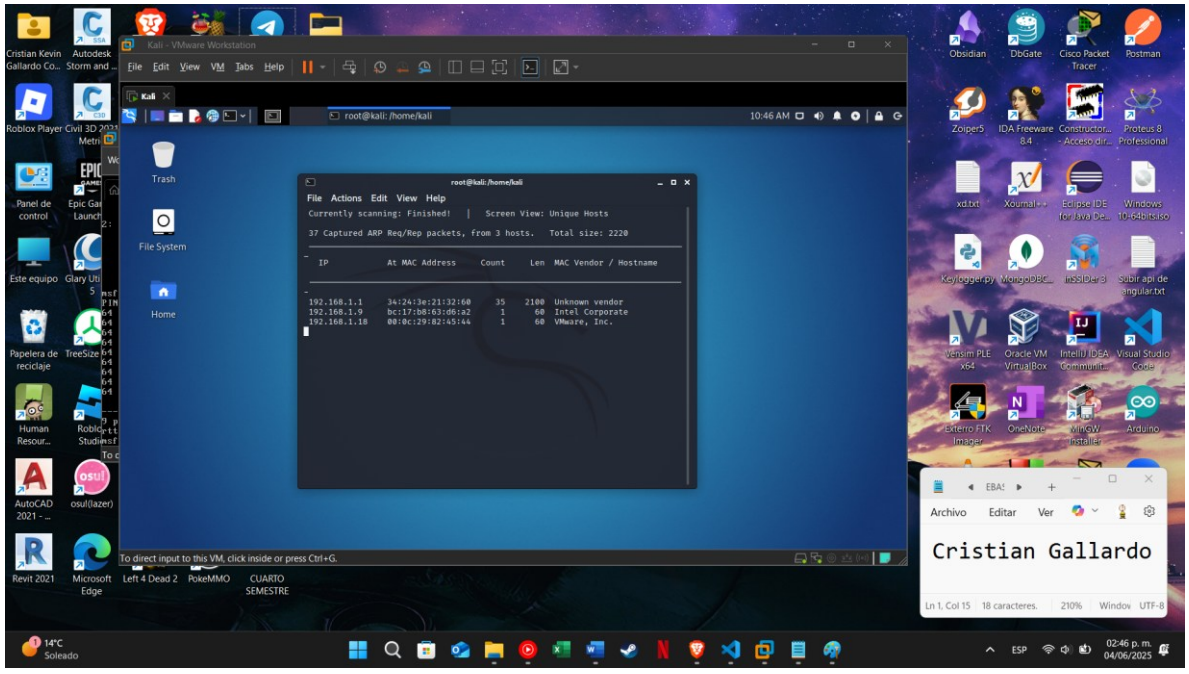
- Verificamos que se encuentren en el mismo segmento de red



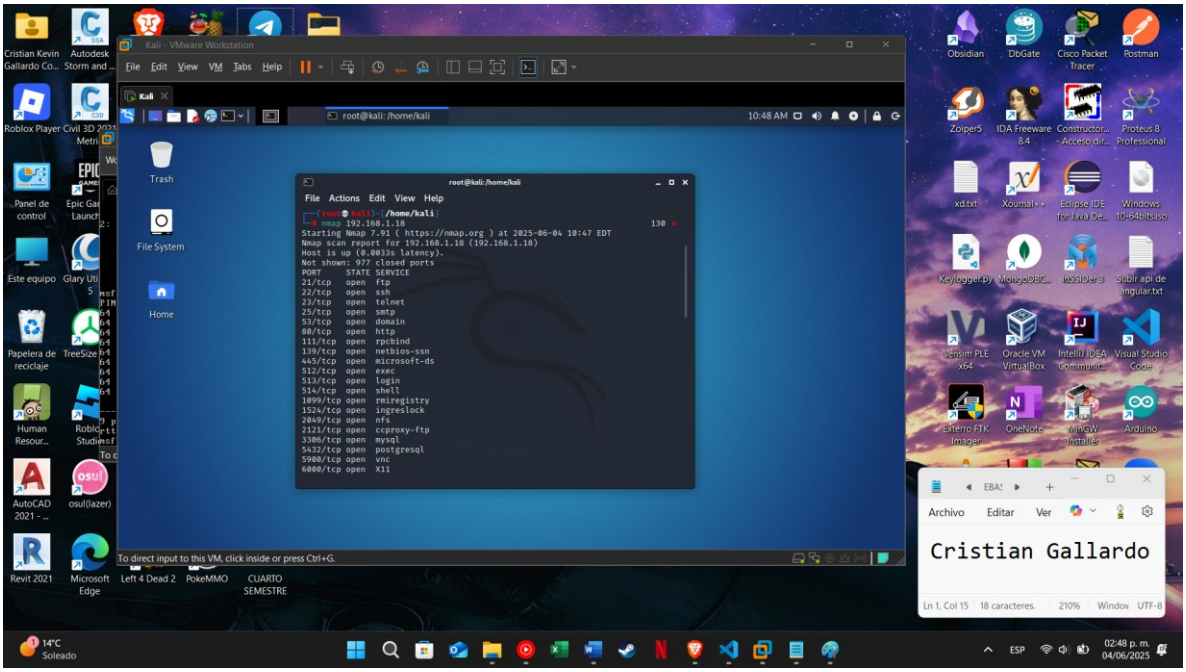
- Verificamos que tengan conexión entre ellas



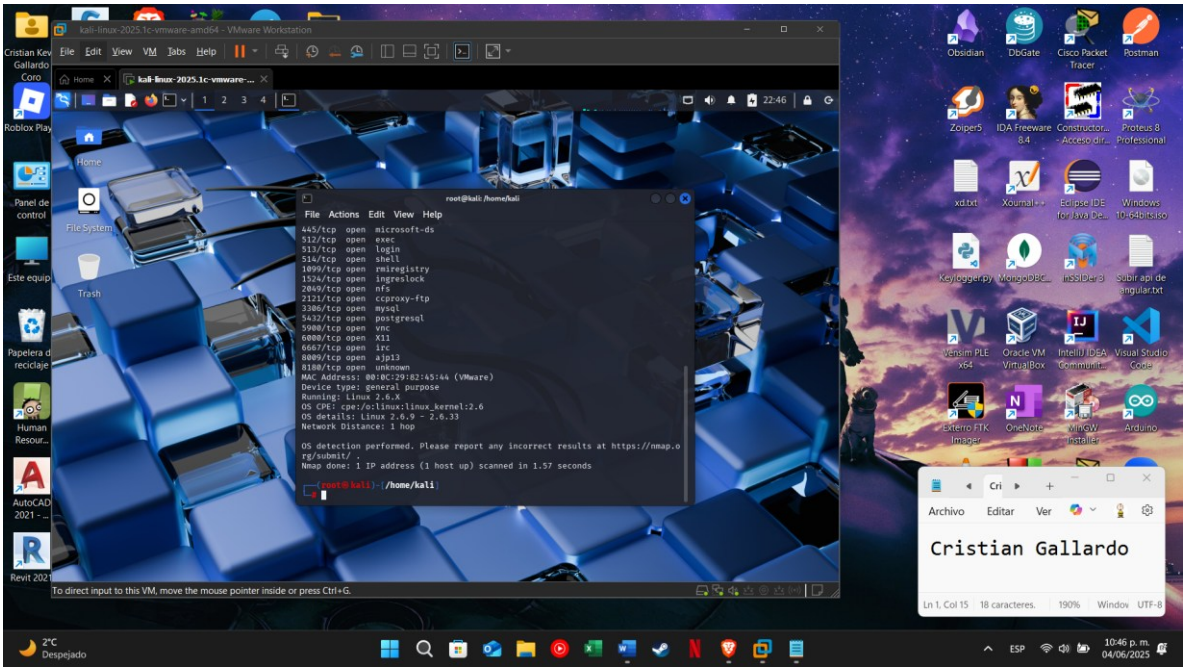
- Aplicamos el comando netdiscover



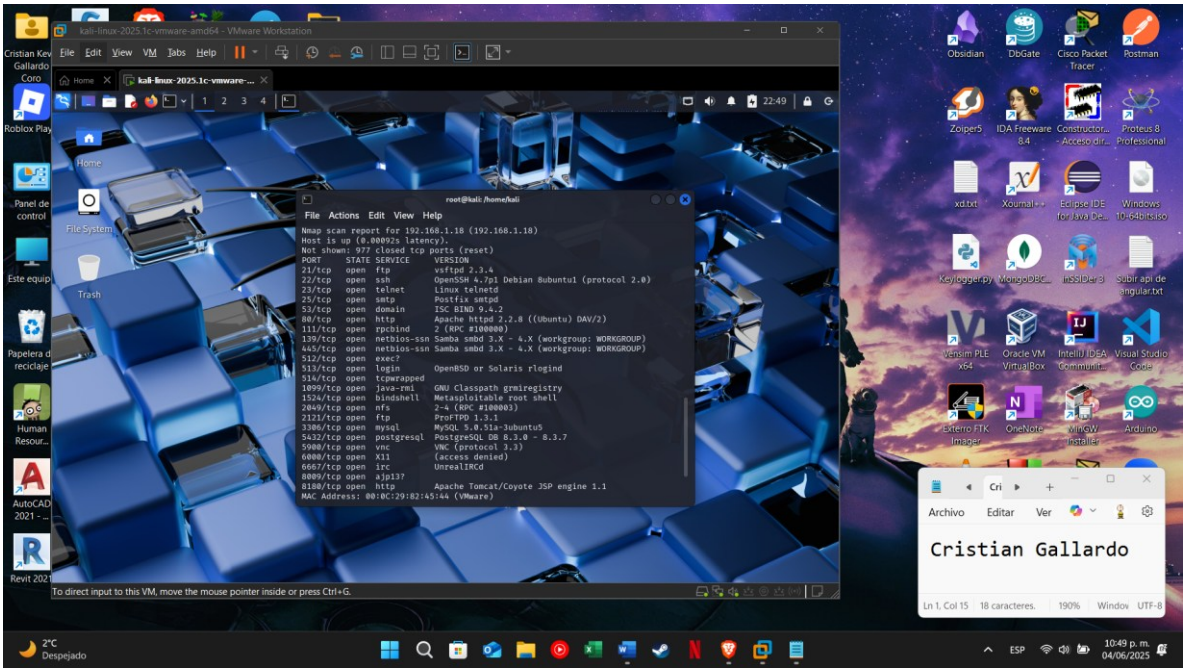
- Ejecutamos el comando nmap



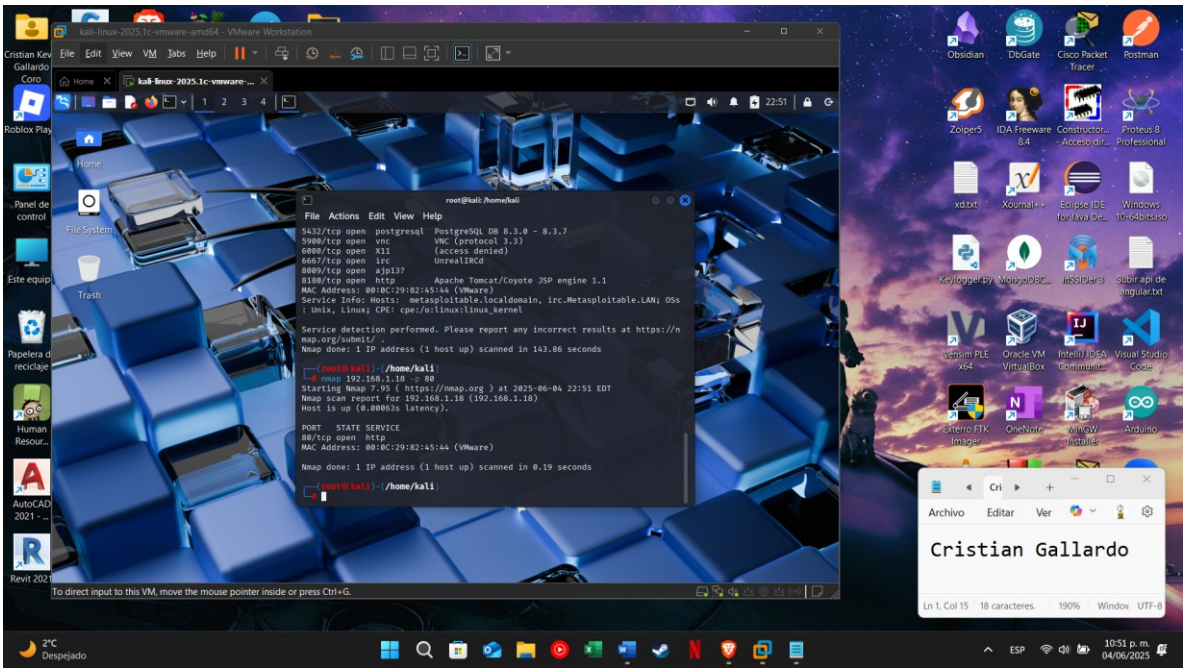
- Revisamos el SO del objetivo



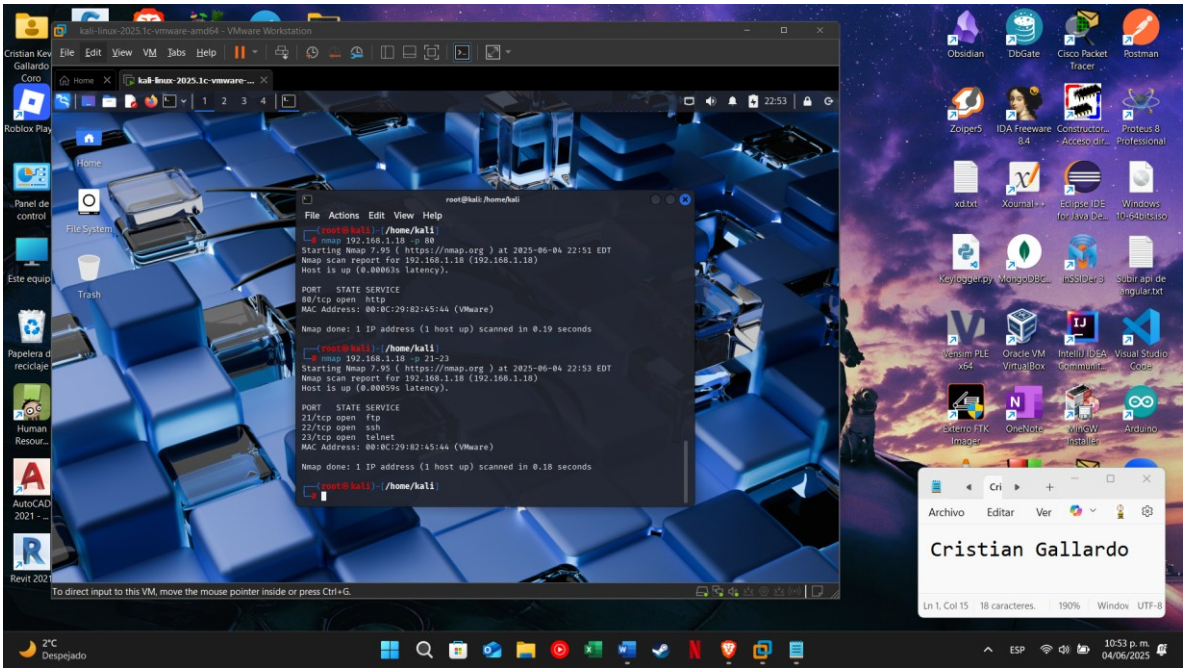
- Revisamos a más detalle los servicios que están en ejecución



- Observamos el comportamiento del puerto 80

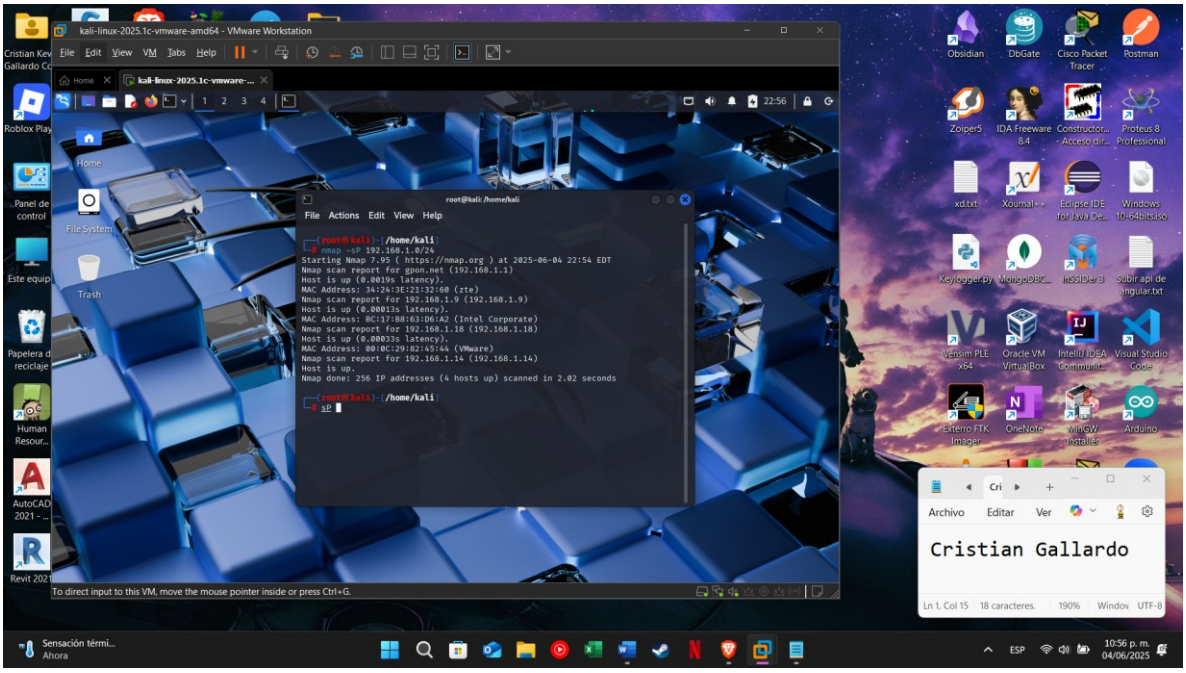


- Observamos el comportamiento de los puertos 21,22 y 23



EVALUACION

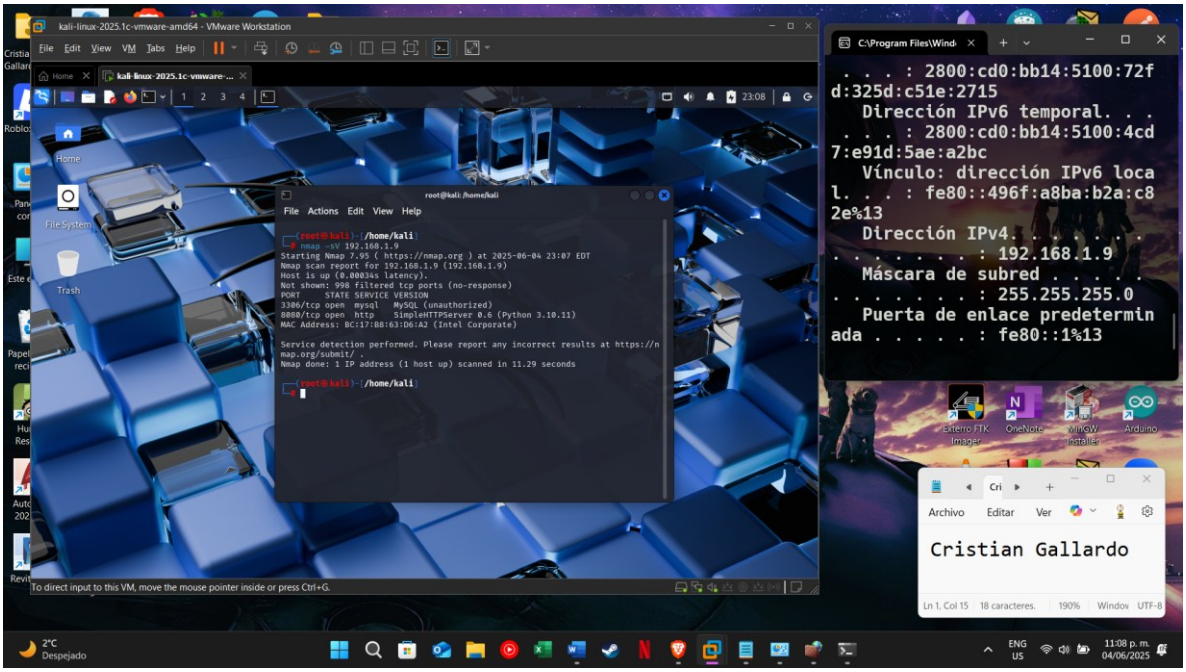
1.



Tiene un funcionamiento similar a netdiscover, ve los hosts dentro de la red los cuales estén activos y nos da su dirección IP y su dirección MAC.

2.

Puertos abiertos en Windows 11 (Máquina local)

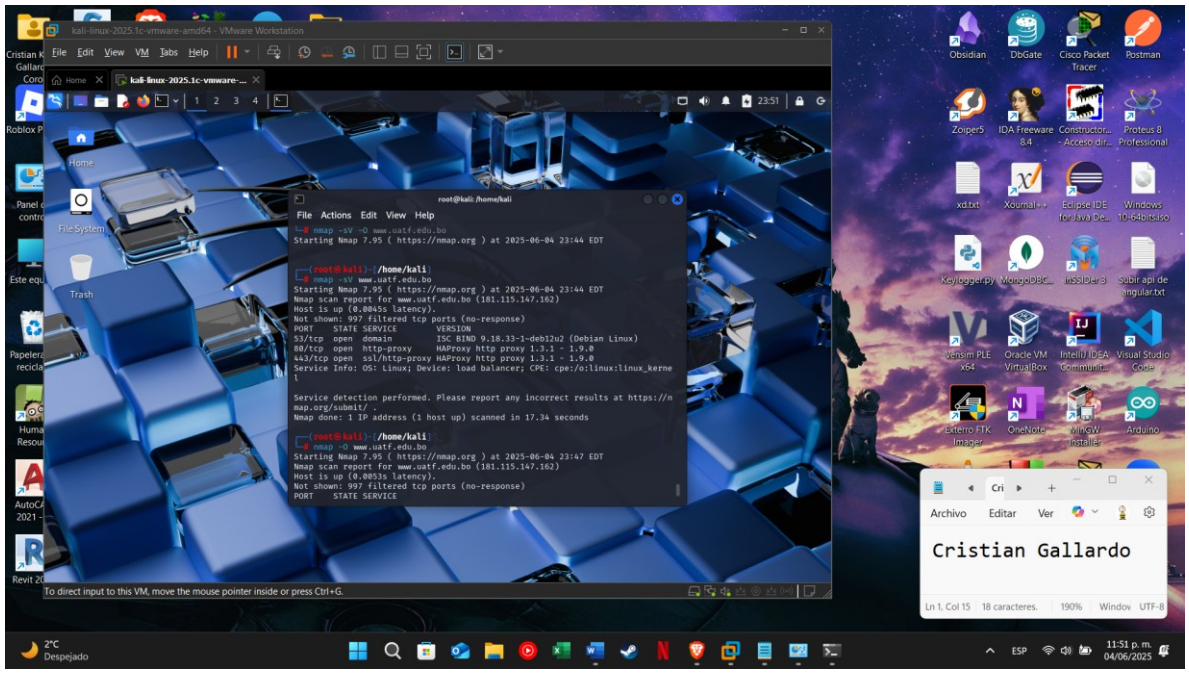


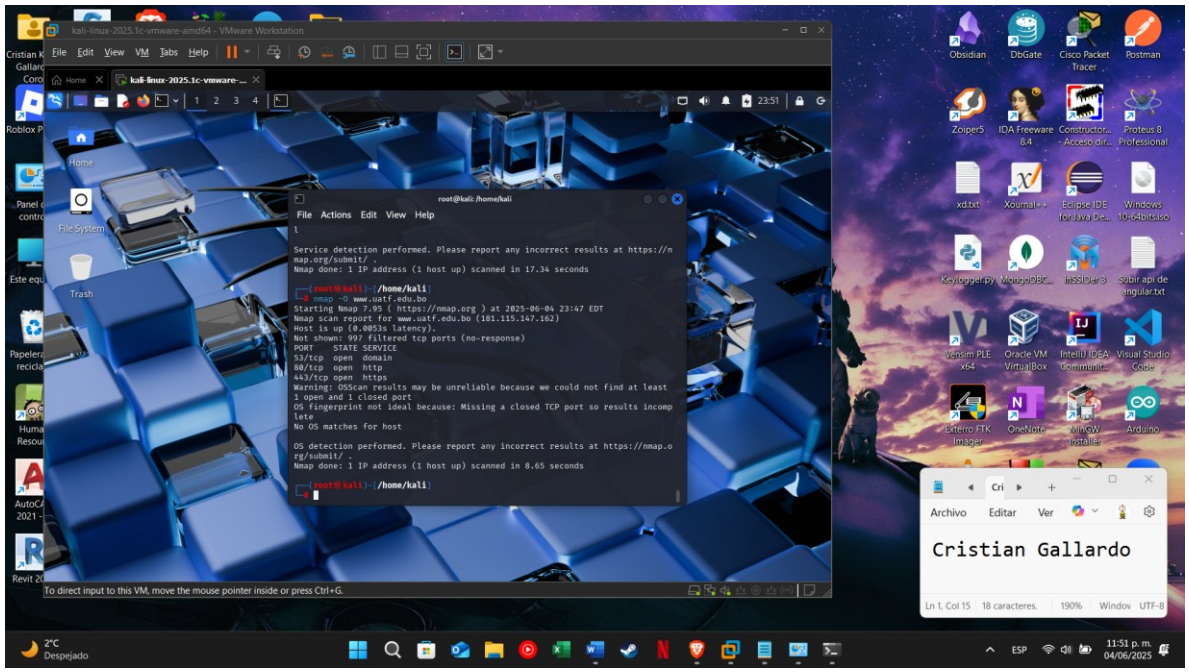
Se puede observar que están abiertos dos puertos, uno de MySQL y otro en http, puerto abierto mediante Python para realizar esta prueba

3.

Sitio UATF

Este tiene 3 servicios activos, el dominio 53 con la version ISC BIND 9.18.33-1-deb12u2 (Debian Linux), http 80 con la versión http proxy 1.3.1- 1.9.0 y https 443 con la versión http proxy 1.3.1-1.9.0, el SO en el que esta corriendo no pudo ser identificado, ya que no cuenta con los puertos suficientes abiertos para poderlo detectar, el único SO, abierto es el de el dominio el cual es Debian Linux


kali-linux-2025.1c-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
root@kali: /home/kali
File Actions Edit View Help
Starting Nmap 7.95 (https://nmap.org) at 2025-06-04 23:44 EDT
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
Service Info: OS: Linux; Device: load balancer; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.34 seconds
Starting Nmap 7.95 (https://nmap.org) at 2025-06-04 23:47 EDT
Nmap scan report for www.uatf.edu.bo (181.115.147.162)
Host is up (0.0053s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Archivo Editar Ver
Cristian Gallardo
Ln 1, Col 15 18 caracteres. 190% Windov UTF-8
2°C Despejado
ESP
11:51 p. m. 04/06/2025


kali-linux-2025.1c-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
root@kali: /home/kali
File Actions Edit View Help
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.34 seconds
Starting Nmap 7.95 (https://nmap.org) at 2025-06-04 23:47 EDT
Nmap scan report for www.uatf.edu.bo (181.115.147.162)
Host is up (0.0053s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE
53/tcp open domain
80/tcp open http
443/tcp open https
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
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.65 seconds
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Archivo Editar Ver
Cristian Gallardo
Ln 1, Col 15 18 caracteres. 190% Windov UTF-8
2°C Despejado
ESP
11:51 p. m. 04/06/2025

Sitio UAJMS

Este tiene 3 servicios activos, el puerto http 80 el cual corre en Apache, el puerto 113 y el puerto 443 https el cual también esta corriendo en apache, el sistema operativo tampoco puede ser observado, ya que tampoco tiene los suficientes puertos abiertos