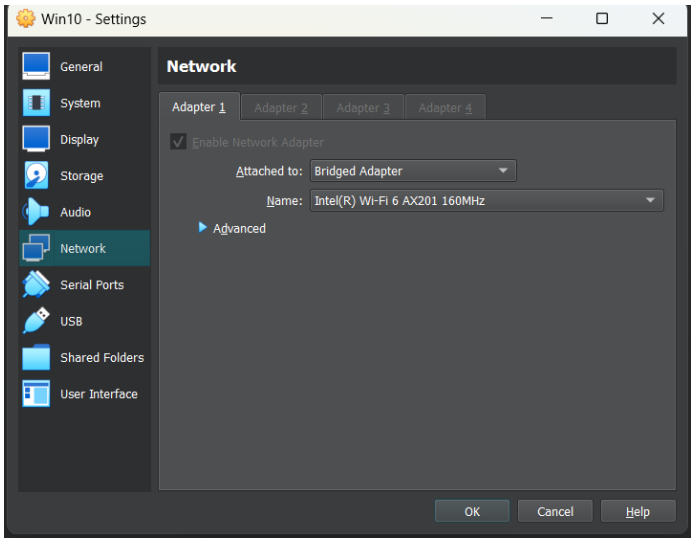
Reporte Shell Inversa en un Entorno de Windows

Se procede a realizar la configuración para establecer una reverse Shell desde una maquina Windows 10 hacia una maquina Kali Linux.

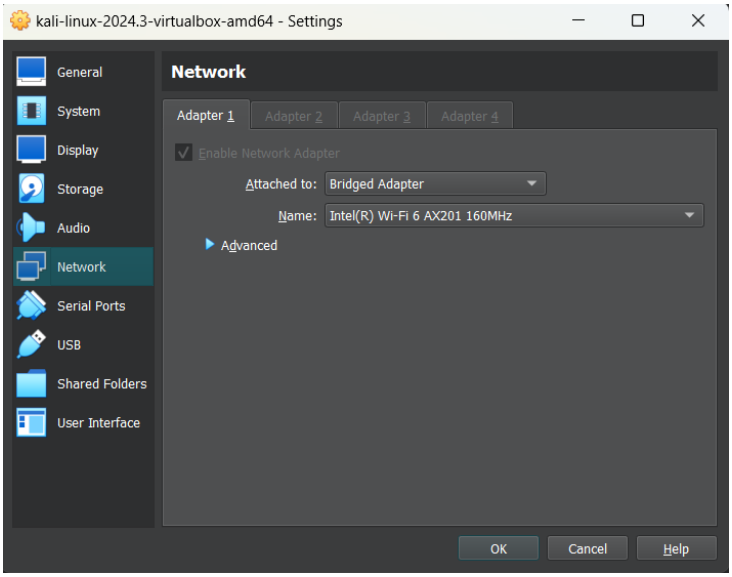
- Maquina atacante (Kali Linux) = M1
- Maquina Objetivo (Windows 10) = M2

Ambas maquinas deben estar configuradas en el adaptador de red en modo **Bridge**

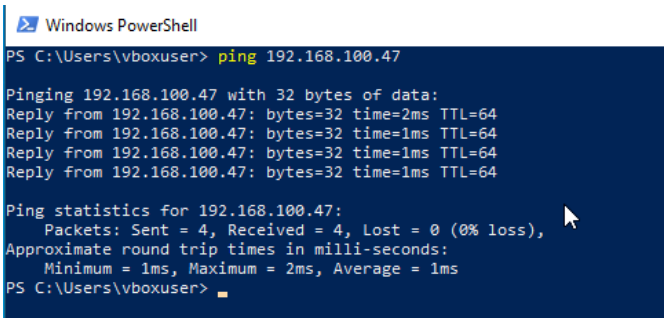
M1

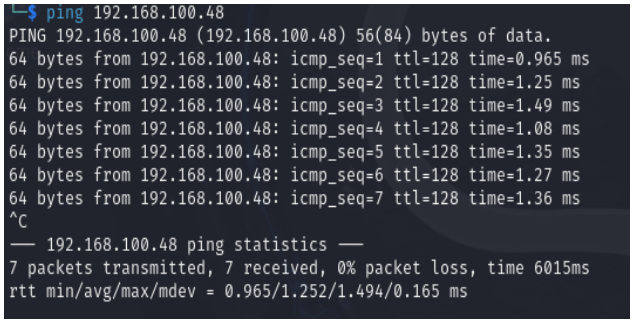


M2



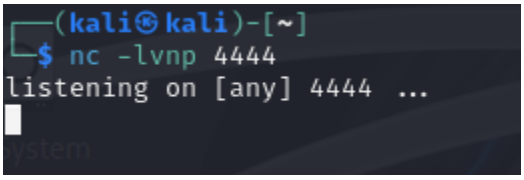
Se verifica que se puedan comunicar entre ambas maquinas





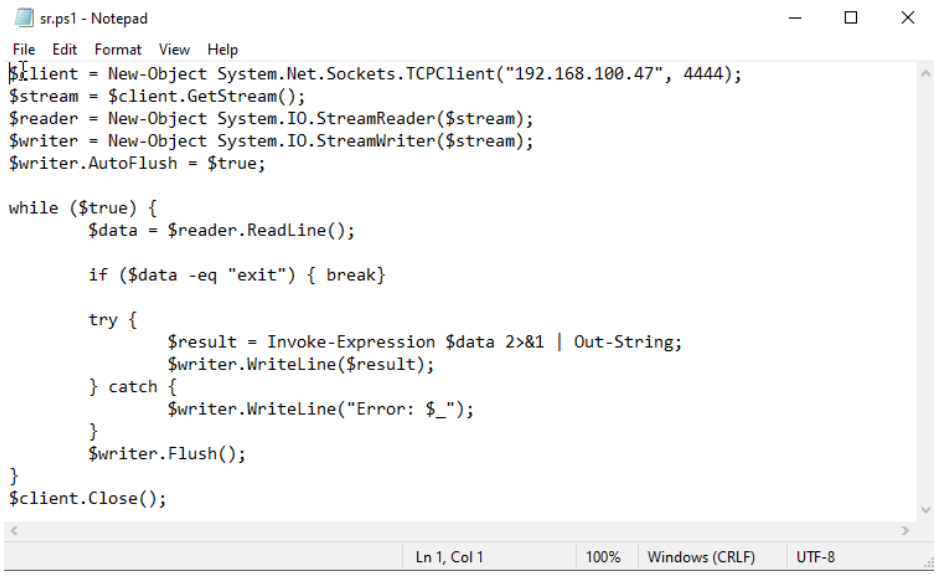
Se procede a establecer la conexión Netcat en la M1, con el comando, lo cual es un listener esperando la conexión desde Windows

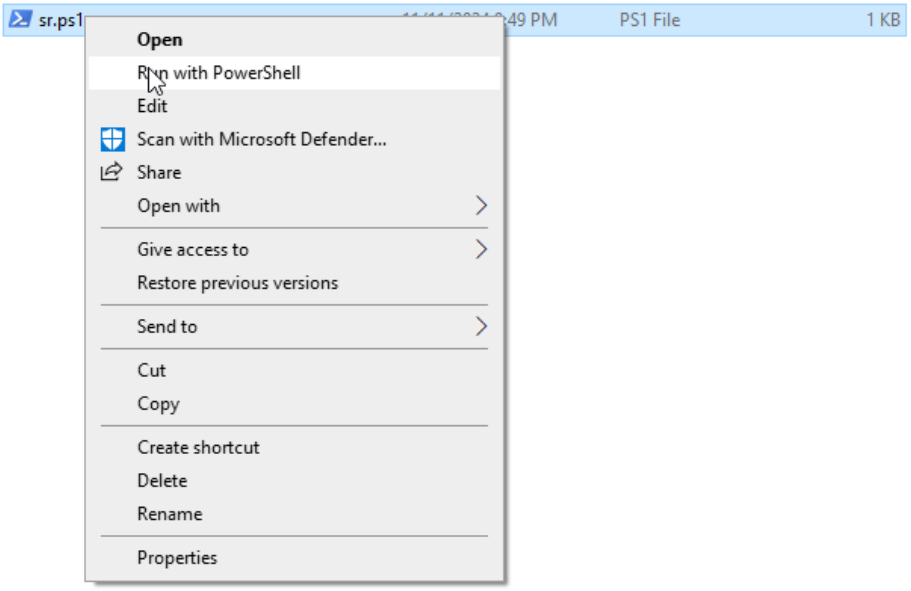
nc -lvnp 4444



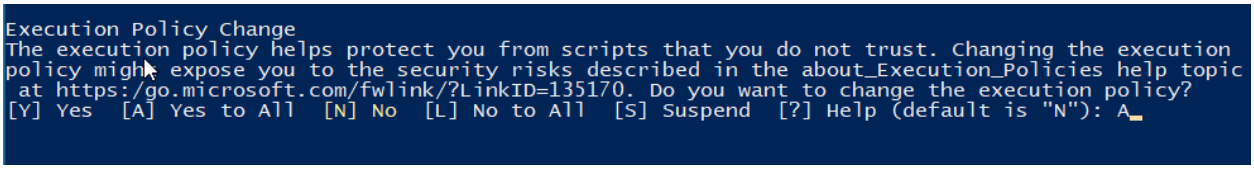
Para establecer la reverse Shell se debe ejecutar el siguiente script en la M2 en la PowerShell

Tener en cuenta que se debe deshabilitar el Firewall en la M2.

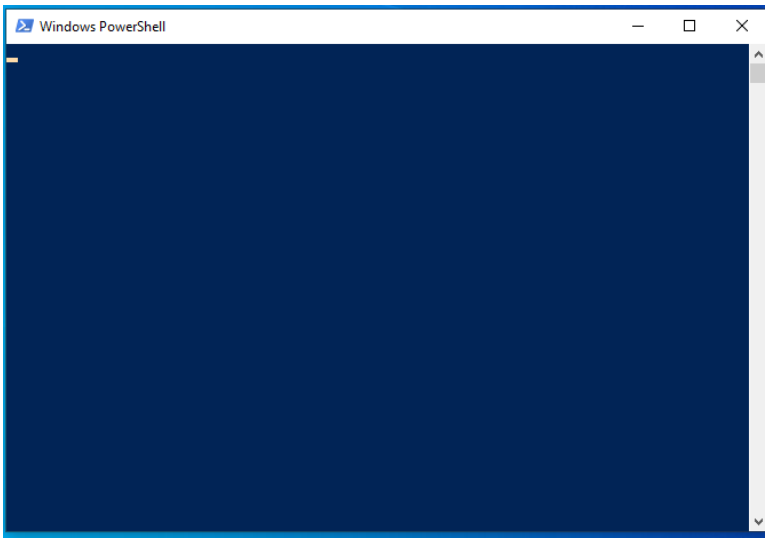




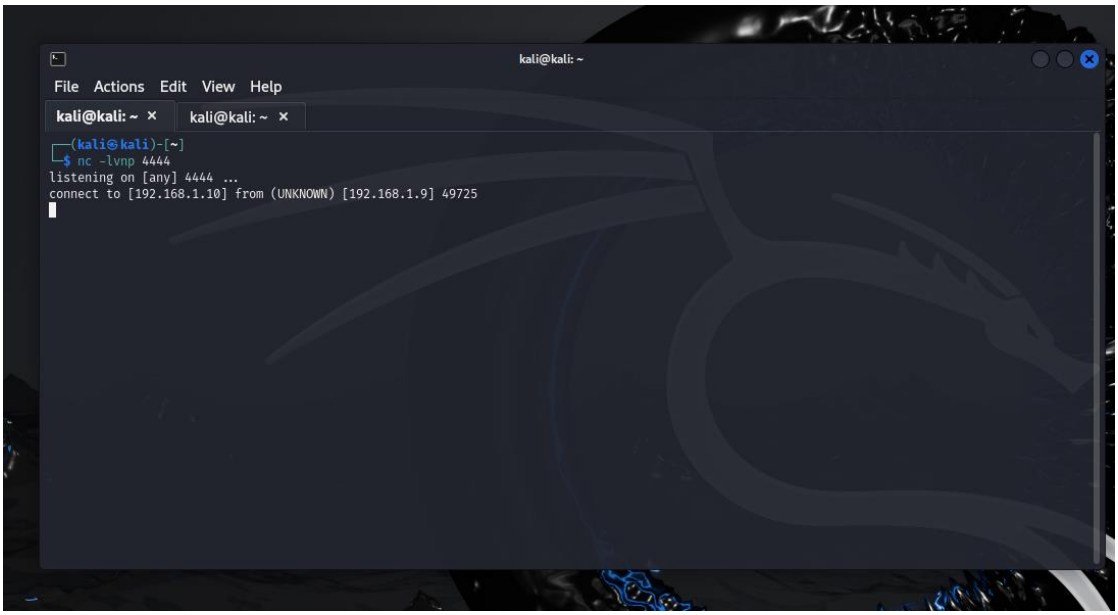
Info: en caso de que se visualice un cambio en las políticas de ejecución, escribir la letas A, indicando que quieres cambiar a todas las políticas.



La ventana de Powershell se mantiene iniciada en la M2



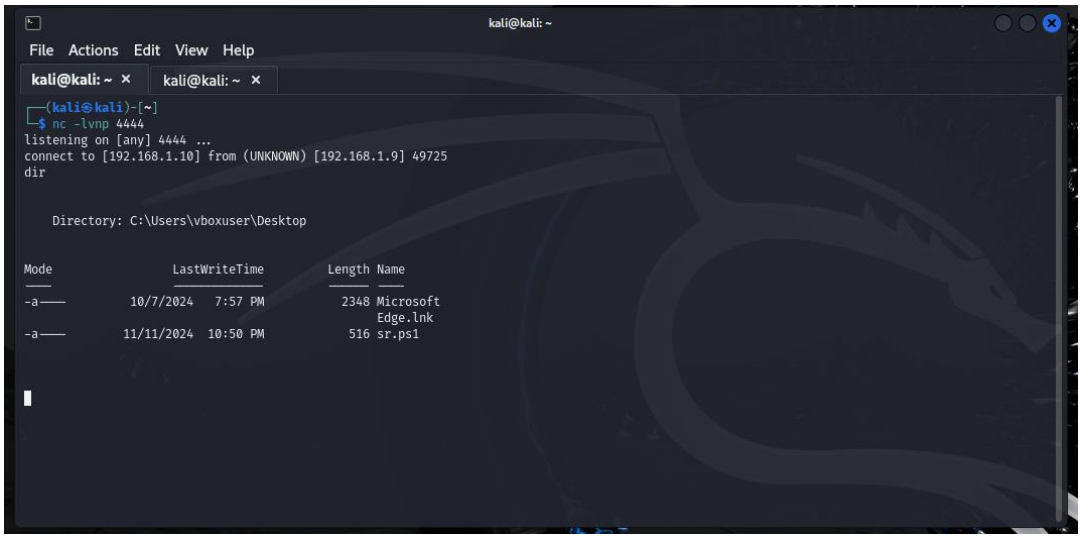
Mientras que en la M1 se visualiza que la conexión ya se ha iniciado



Se procede a ejecutar comandos básicos de Windows:

1. ***dir***

Listar los archivos en el directorio actual

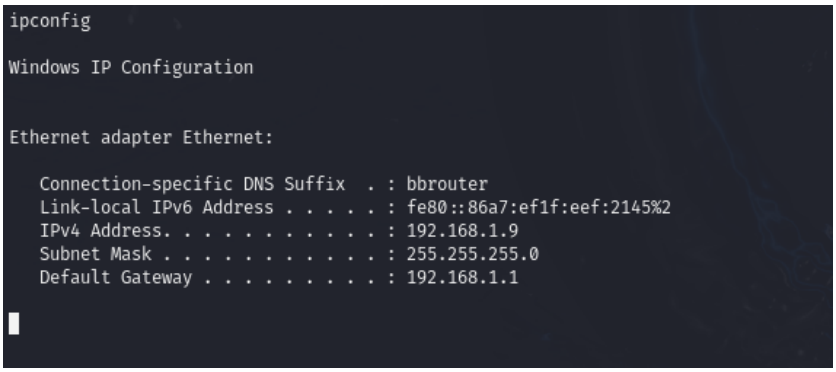


2. *systeminfo*

Obtener información del sistema

3. *ipconfig*

Obtener la configuración de red



4. tasklist

Listar procesos en ejecución

```
tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0        152 K
Registry                        92 Services                   0    108,072 K
smss.exe                       324 Services                   0      1,148 K
csrss.exe                      424 Services                   0      5,392 K
wininit.exe                    500 Services                   0      7,124 K
csrss.exe                      508 Console                    1      5,444 K
winlogon.exe                   600 Console                    1     12,104 K
services.exe                   640 Services                   0      9,908 K
lsass.exe                      656 Services                   0     19,072 K
fontdrvhost.exe                744 Services                   0      3,680 K
fontdrvhost.exe                752 Console                    1      4,840 K
svchost.exe                    764 Services                   0     31,404 K
svchost.exe                    868 Services                   0     13,672 K
svchost.exe                    924 Services                   0      8,192 K
dwm.exe                       1004 Console                    1     60,940 K
svchost.exe                    840 Services                   0      6,256 K
svchost.exe                    884 Services                   0      5,548 K
svchost.exe                   1080 Services                   0     10,044 K
svchost.exe                   1112 Services                   0     21,188 K
svchost.exe                   1124 Services                   0     15,772 K
svchost.exe                   1172 Services                   0     12,024 K
svchost.exe                   1184 Services                   0     13,960 K
svchost.exe                   1268 Services                   0      7,340 K
svchost.exe                   1340 Services                   0     18,808 K
svchost.exe                   1372 Services                   0      8,232 K
svchost.exe                   1428 Services                   0      7,548 K
svchost.exe                   1552 Services                   0     12,284 K
svchost.exe                   1608 Services                   0      7,944 K
svchost.exe                   1620 Services                   0    106,564 K
svchost.exe                   1636 Services                   0      6,040 K
Memory Compression            1692 Services                   0     78,780 K
svchost.exe                   1740 Services                   0      8,252 K
svchost.exe                   1764 Services                   0      8,192 K
svchost.exe                   1772 Services                   0      7,284 K
svchost.exe                   1804 Services                   0      9,996 K
svchost.exe                   1884 Services                   0     13,412 K
svchost.exe                   1928 Services                   0      7,956 K
svchost.exe                   1936 Services                   0     10,724 K
svchost.exe                   1956 Services                   0      9,676 K
svchost.exe                      8 Services                   0     14,024 K
svchost.exe                   1924 Services                   0     13,728 K
svchost.exe                   2108 Services                   0      7,624 K
svchost.exe                   2160 Services                   0     11,692 K
spoolsv.exe                   2188 Services                   0     15,500 K
```

5. hostname

Ver información del equipo

```
hostname
Win10

```

6. *net user*

Listar los usuarios del sistema

```
net user

User accounts for \\WIN10

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
vboxuser                 WDAGUtilityAccount
The command completed successfully.
```

7. *netstast -an*

Ver las conexiones de red activas

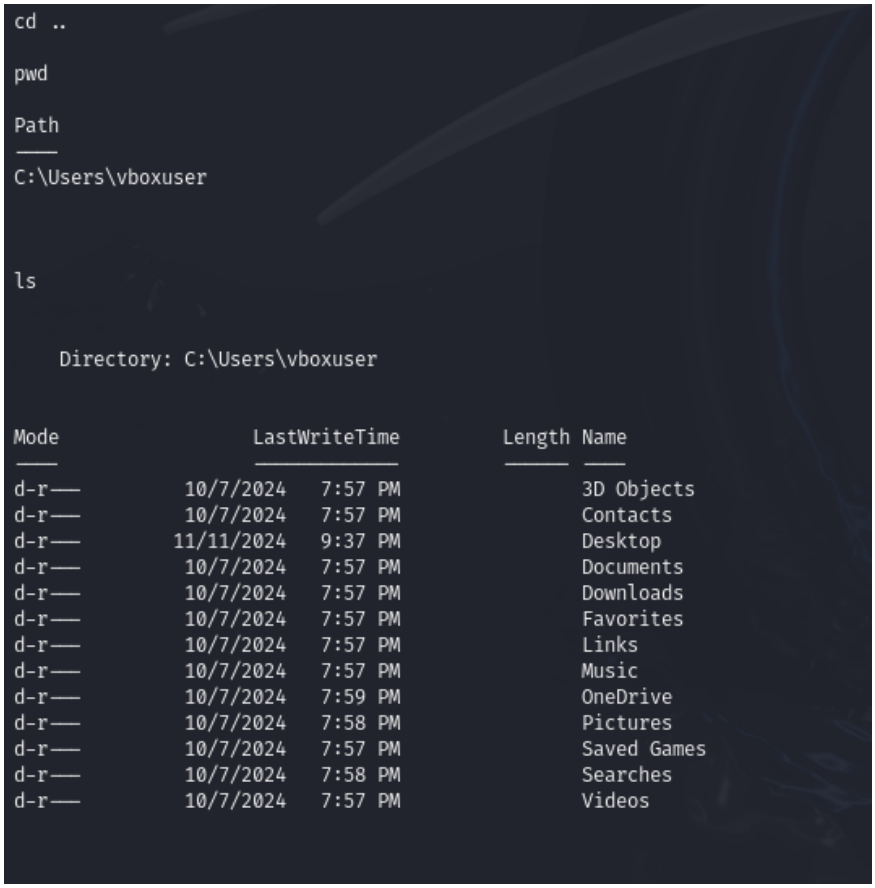
```
netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING
  TCP    192.168.1.9:139        0.0.0.0:0              LISTENING
  TCP    192.168.1.9:49683      52.159.127.243:443     ESTABLISHED
  TCP    192.168.1.9:49717      23.223.28.201:443      CLOSE_WAIT
  TCP    192.168.1.9:49841      52.159.127.243:443     ESTABLISHED
  TCP    192.168.1.9:49847      23.223.28.217:443      CLOSE_WAIT
  TCP    192.168.1.9:49849      23.223.28.204:443      CLOSE_WAIT
  TCP    192.168.1.9:49850      23.223.28.204:443      CLOSE_WAIT
  TCP    192.168.1.9:49851      23.223.28.204:443      CLOSE_WAIT
  TCP    192.168.1.9:49852      23.223.28.204:443      CLOSE_WAIT
  TCP    192.168.1.9:49853      23.223.28.204:443      CLOSE_WAIT
  TCP    192.168.1.9:49854      23.223.28.204:443      CLOSE_WAIT
  TCP    192.168.1.9:49861      52.149.20.212:443      TIME_WAIT
  TCP    192.168.1.9:49862      52.149.20.212:443      TIME_WAIT
  TCP    192.168.1.9:49863      20.97.190.222:443      TIME_WAIT
  TCP    192.168.1.9:49866      40.126.29.13:443       TIME_WAIT
  TCP    192.168.1.9:49867      192.229.211.108:80     TIME_WAIT
  TCP    192.168.1.9:49869      4.152.199.46:443       ESTABLISHED
  TCP    192.168.1.9:49870      192.168.1.10:4444      ESTABLISHED
  TCP    [::]:135               [::]:0                 LISTENING
  TCP    [::]:445               [::]:0                 LISTENING
  TCP    [::]:7680              [::]:0                 LISTENING
  TCP    [::]:49664             [::]:0                 LISTENING
  TCP    [::]:49665             [::]:0                 LISTENING
  TCP    [::]:49666             [::]:0                 LISTENING
  TCP    [::]:49667             [::]:0                 LISTENING
  TCP    [::]:49668             [::]:0                 LISTENING
  TCP    [::]:49669             [::]:0                 LISTENING
  UDP    0.0.0.0:123            *:*
  UDP    0.0.0.0:5050           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5355           *:*
```

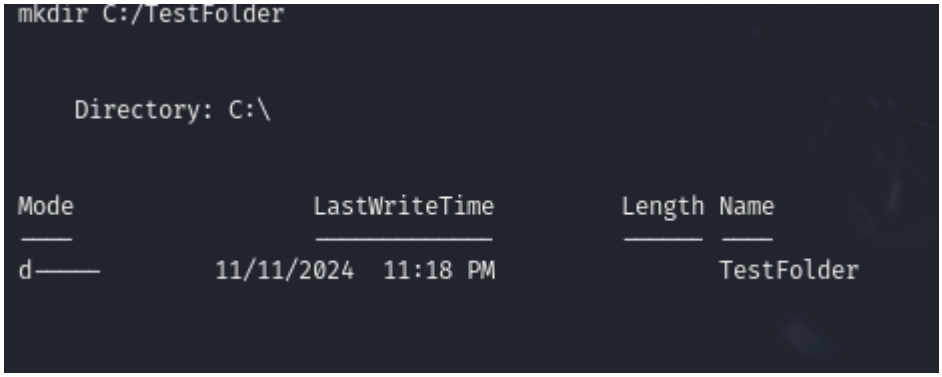
8. ***cd [PATH]***

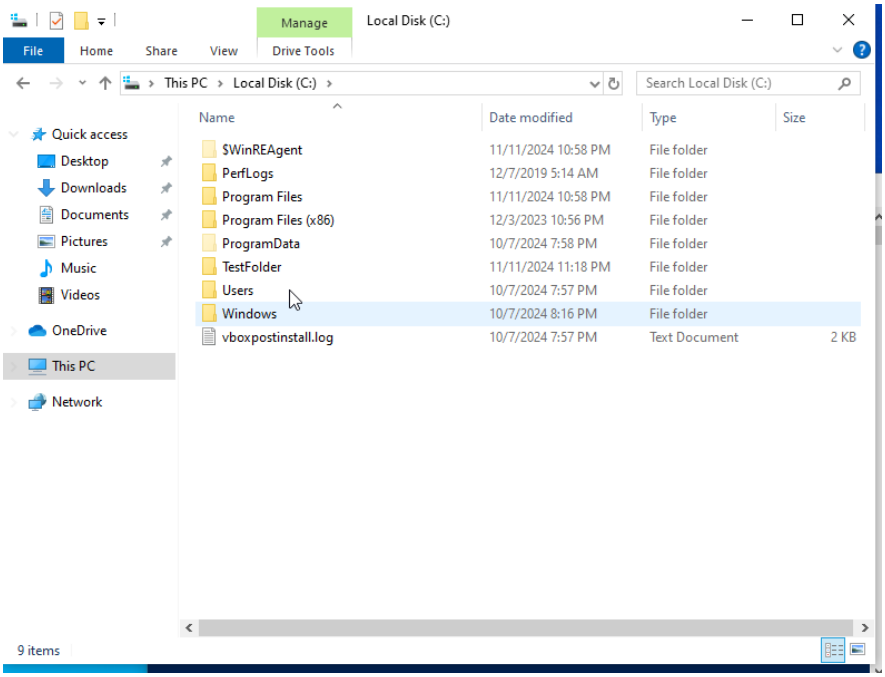
Cambiar de directorio, usar ***pwd*** para verificar el directorio actual. Y ***ls*** para listar los archivos que están en el directorio actual



9. ***mkdir C:/TestFolder***

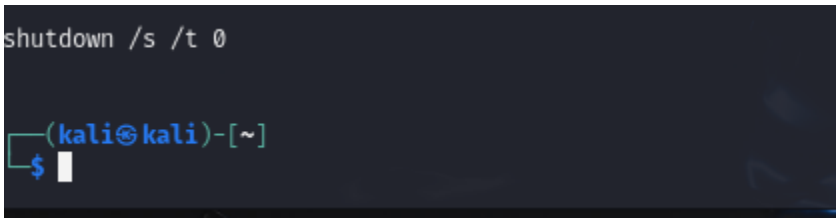
Crear un directorio

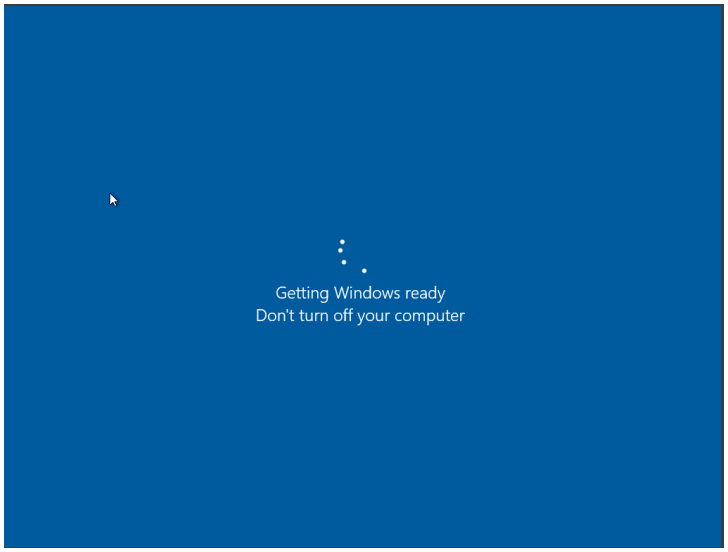




10. shutdown /s /t 0

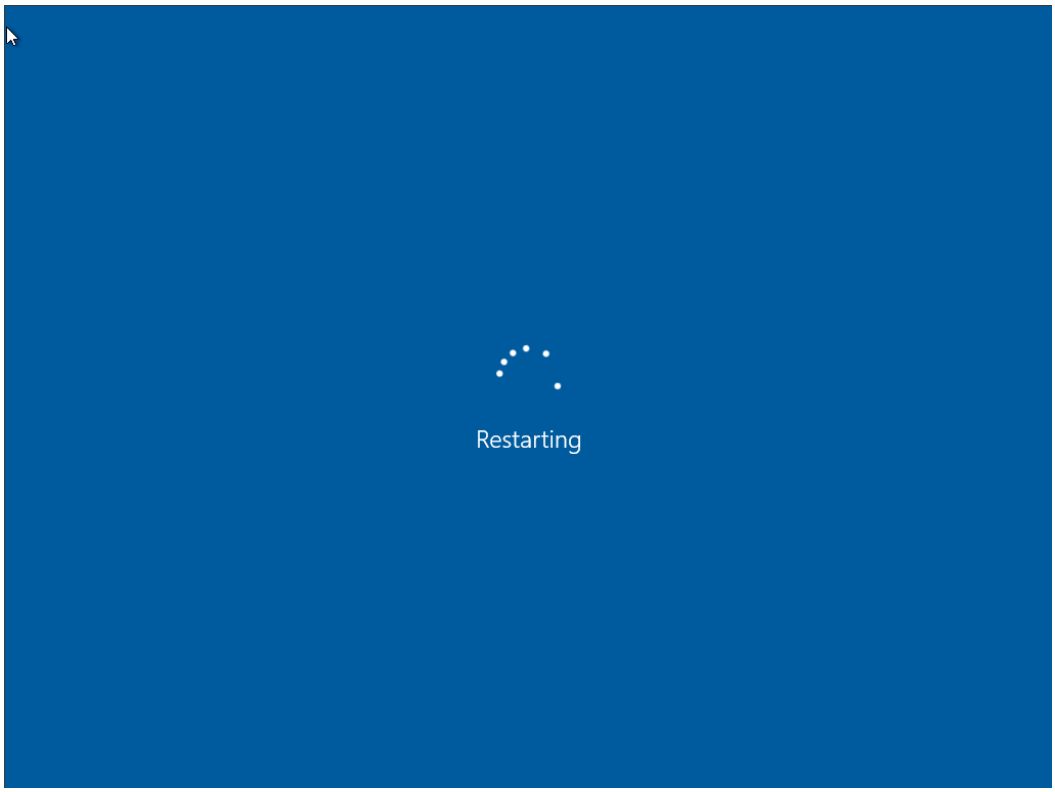
Apagar el sistema





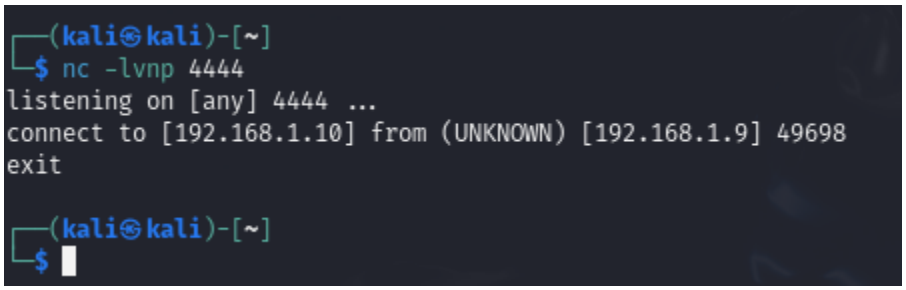
11. shutdown /r /t 0

Reiniciar el sistema



12. exit

Cerrar sesión



Finalizada las ejecuciones de comandos de Windows, se da concluye que al iniciar un reverse Shell, se puede ejecutar los comandos posibles de acuerdo al permiso que tenga habilitado el usuario autenticado.