

Comandos básicos de red para ciberseguridad (Windows y Linux)

1. ping

Verifica la conectividad con otro dispositivo de red.

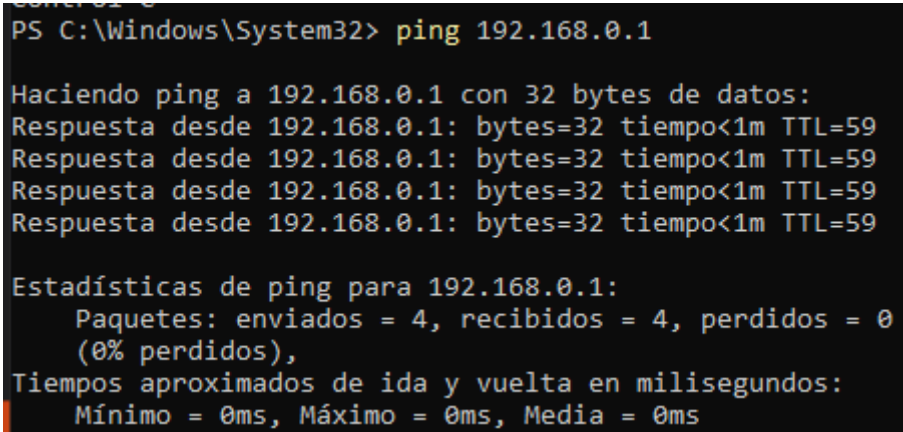
 Utilidad:

- Comprobar si una dirección IP o dominio está accesible.
- Medir latencia de red.

 Ejemplo:

ping 192.168.1.1

ping [google.com](https://www.google.com)




```
PS C:\Windows\System32> ping 192.168.0.1

Haciendo ping a 192.168.0.1 con 32 bytes de datos:
Respuesta desde 192.168.0.1: bytes=32 tiempo<1m TTL=59
Respuesta desde 192.168.0.1: bytes=32 tiempo<1m TTL=59
Respuesta desde 192.168.0.1: bytes=32 tiempo<1m TTL=59
Respuesta desde 192.168.0.1: bytes=32 tiempo<1m TTL=59

Estadísticas de ping para 192.168.0.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

2. ipconfig (Windows) / ifconfig o ip a (Linux)

Muestra la configuración de red del equipo.

 Ejemplo (Windows):

ipconfig /all

```

PS C:\Windows\System32> ipconfig /all

Configuración IP de Windows

Nombre de host. . . . . : DESKTOP-M7CM9BE
Sufijo DNS principal . . . . . :
Tipo de nodo. . . . . : híbrido
Enrutamiento IP habilitado. . . : no
Proxy WINS habilitado . . . . . : no

Adaptador de Ethernet Ethernet 2:

Sufijo DNS específico para la conexión. . :
Descripción . . . . . : VirtualBox Host-Only Ethernet Adapter
Dirección física. . . . . : 0A-00-27-00-00-03
DHCP habilitado . . . . . : no
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::e6bc:3d3a:910e:4b97%3(Preferido)
Dirección IPv4. . . . . : 192.168.56.1(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . :
IAID DHCPv6 . . . . . : 185204775
DUID de cliente DHCPv6. . . . . : 00-01-00-01-30-40-78-F0-48-0F-CF-39-A6-26
Servidores DNS. . . . . : fec0:0:0:ffff::1%1
                           fec0:0:0:ffff::2%1
                           fec0:0:0:ffff::3%1

```

3. hostname

Muestra el nombre del equipo local.

 Ejemplo:

hostname

```

PS C:\Windows\System32> hostname
DESKTOP-M7CM9BE
PS C:\Windows\System32>

```

4. getmac (solo en Windows)

Muestra la dirección MAC de los adaptadores de red.

 Ejemplo:

getmac

```

PS C:\Windows\System32> getmac

Dirección física      Nombre de transporte
=====
0A-00-27-00-00-03     \Device\NPF{22C595A1-103A-495C-930B-7CFC3EBB907A}
D8-43-AE-44-E2-25     \Device\NPF{7DB3B56E-5580-4E9F-AE2D-49D626D0A9B0}
PS C:\Windows\System32>

```

5. arp

Muestra la tabla ARP (asociación entre direcciones IP y MAC).

 Ejemplo:

arp -a

💡 Útil para detectar si hay dispositivos extraños en la red local.

```
Interfaz: 192.168.56.1 --- 0x9
Dirección de Internet      Dirección física      Tipo
192.168.56.255             ff-ff-ff-ff-ff-ff    estático
224.0.0.22                 01-00-5e-00-00-16    estático
224.0.0.251                01-00-5e-00-00-fb    estático
224.0.0.252                01-00-5e-00-00-fc    estático
239.255.255.250            01-00-5e-7f-ff-fa    estático
```

```
Interfaz: 192.168.1.43 --- 0x13
Dirección de Internet      Dirección física      Tipo
192.168.1.1                d8-fb-5e-a8-d8-47    dinámico
192.168.1.40               20-1f-3b-39-e1-29    dinámico
192.168.1.255              ff-ff-ff-ff-ff-ff    estático
224.0.0.2                  01-00-5e-00-00-02    estático
224.0.0.22                 01-00-5e-00-00-16    estático
224.0.0.251                01-00-5e-00-00-fb    estático
224.0.0.252                01-00-5e-00-00-fc    estático
239.255.255.250            01-00-5e-7f-ff-fa    estático
255.255.255.255            ff-ff-ff-ff-ff-ff    estático
```

```
PS C:\Windows\System32> arp -a

Interfaz: 192.168.56.1 --- 0x3
Dirección de Internet      Dirección física      Tipo
192.168.56.255             ff-ff-ff-ff-ff-ff    estático
224.0.0.2                  01-00-5e-00-00-02    estático
224.0.0.22                 01-00-5e-00-00-16    estático
224.0.0.251                01-00-5e-00-00-fb    estático
224.0.0.252                01-00-5e-00-00-fc    estático
224.224.125.119            01-00-5e-60-7d-77    estático

Interfaz: 192.168.0.31 --- 0x5
Dirección de Internet      Dirección física      Tipo
192.168.0.1                00-a0-26-d2-68-9a    dinámico
192.168.0.55               7c-67-a2-de-e8-f6    dinámico
192.168.0.56               cc-28-aa-c9-15-46    dinámico
192.168.0.77               d8-43-ae-44-e2-69    dinámico
192.168.0.90               a4-97-33-4e-9f-c4    dinámico
192.168.1.255              ff-ff-ff-ff-ff-ff    estático
224.0.0.2                  01-00-5e-00-00-02    estático
224.0.0.22                 01-00-5e-00-00-16    estático
224.0.0.251                01-00-5e-00-00-fb    estático
224.0.0.252                01-00-5e-00-00-fc    estático
```

6. nslookup

Diagnóstico de resolución DNS.

📘 Ejemplo:

nslookup google.com

```
Servidor: 250.red-80-58-61.staticip.rima-tde.net
Address: 80.58.61.250

Respuesta no autoritativa:
Nombre: google.com
Addresses: 2a00:1450:4003:803::200e
          142.250.200.142
```

🚩 Permite verificar si un dominio se está resolviendo correctamente o si hay un posible ataque DNS spoofing.

```
PS C:\Windows\System32> nslookup google.com
Servidor: 254.red-80-58-61.staticip.rima-tde.net
Address: 80.58.61.254

Respuesta no autoritativa:
Nombre: google.com
Addresses: 2a00:1450:4003:803::200e
          142.250.201.78

PS C:\Windows\System32>
```

7. netstat

Muestra conexiones activas, puertos abiertos y estadísticas de red.

📘 Ejemplos:

netstat -a # Todas las conexiones y puertos escuchando

```
PS C:\Windows\System32> netstat -a

Conexiones activas

Proto Dirección local Dirección remota Estado
TCP 0.0.0.0:135 DESKTOP-M7CM9BE:0 LISTENING
TCP 0.0.0.0:445 DESKTOP-M7CM9BE:0 LISTENING
TCP 0.0.0.0:5040 DESKTOP-M7CM9BE:0 LISTENING
TCP 0.0.0.0:7070 DESKTOP-M7CM9BE:0 LISTENING
TCP 0.0.0.0:7680 DESKTOP-M7CM9BE:0 LISTENING
TCP 0.0.0.0:49664 DESKTOP-M7CM9BE:0 LISTENING
TCP 0.0.0.0:49665 DESKTOP-M7CM9BE:0 LISTENING
```

netstat -n # En formato numérico

```
PS C:\Windows\System32> netstat -n
```

Conexiones activas

Proto	Dirección local	Dirección remota	Estado
TCP	192.168.0.31:52147	4.207.247.137:443	ESTABLISHED
TCP	192.168.0.31:52443	84.17.62.9:6568	ESTABLISHED
TCP	192.168.0.31:52483	13.107.246.254:443	CLOSE_WAIT
TCP	192.168.0.31:52485	150.171.87.254:443	CLOSE_WAIT
TCP	192.168.0.31:52560	34.107.243.93:443	ESTABLISHED
TCP	192.168.0.31:52615	13.107.226.43:443	CLOSE_WAIT
TCP	192.168.0.31:52619	20.50.88.242:443	ESTABLISHED
TCP	192.168.0.31:52622	51.132.193.104:443	TIME_WAIT
TCP	192.168.0.31:52637	64.233.167.188:5228	ESTABLISHED

netstat -an # Combinado

```
PS C:\Windows\System32> 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	0.0.0.0:7070	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

netstat -b # Muestra qué ejecutable abre cada conexión (Windows)

💡 Útil para detectar conexiones sospechosas o malware que se comunica por red.

```
PS C:\Windows\System32> netstat -b
```

Conexiones activas

Proto	Dirección local	Dirección remota	Estado
TCP	192.168.0.31:52147	4.207.247.137:https	ESTABLISHED
WpnService [svchost.exe]			
TCP	192.168.0.31:52443	relay-0656e159:6568	ESTABLISHED
[AnyDesk.exe]			
TCP	192.168.0.31:52483	13.107.246.254:https	CLOSE_WAIT
[SearchApp.exe]			
TCP	192.168.0.31:52485	150.171.87.254:https	CLOSE_WAIT
[SearchApp.exe]			
TCP	192.168.0.31:52560	93:https	ESTABLISHED
[VirtualBoxVM.exe]			

8. tracert (Windows) / traceroute (Linux)

Muestra la ruta que siguen los paquetes hasta llegar a un destino.

📄 Ejemplo:

tracert google.com

tracert google.com

```
PS C:\Windows\System32> tracert google.es

Traza a la dirección google.es [142.250.201.67]
sobre un máximo de 30 saltos:

  1  <1 ms    <1 ms    <1 ms    192.168.0.1
  2   1 ms     1 ms     1 ms     10.187.4.161
  3  12 ms    11 ms    11 ms    10.143.80.4
  4  37 ms    16 ms    12 ms    33.red-81-45-103.staticip.rima-tde.net [81.45.103.33]
  5   *        *        *        Tiempo de espera agotado para esta solicitud.
  6  13 ms    13 ms    13 ms    17.red-81-46-0.customer.static.ccg.telefonica.net [81.46
  7   *        *        *
```

9. whoami

Muestra el usuario actual en sesión.

 Ejemplo:

whoami

```
PS C:\Windows\System32> whoami
desktop-m7cm9be\admin
PS C:\Windows\System32>
```


10. tasklist (Windows) / ps aux (Linux)

Lista los procesos en ejecución.

 Ejemplo:

tasklist

ps aux

 Útil para detectar procesos maliciosos.

```
PS C:\Windows\System32> 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     1.428 KB
Registry                 148 Services          0    76.036 KB
smss.exe                 556 Services          0     1.248 KB
csrss.exe                 668 Services          0     5.892 KB
wininit.exe              752 Services          0     7.164 KB
csrss.exe                 760 Console           1     6.528 KB
services.exe             828 Services          0    11.044 KB
winlogon.exe             856 Console           1    11.536 KB
```

11. net user

Muestra información sobre los usuarios locales (solo en Windows).

 Ejemplo:

net user

net user nombreusuario

```
PS C:\Windows\System32> net user

Cuentas de usuario de \\DESKTOP-M7CM9BE

-----
2-DAW                Admin                Administrador
DefaultAccount        Invitado            WDAGUtilityAccount
Se ha completado el comando correctamente.
```

```
PS C:\Windows\System32> net user Admin
Nombre de usuario                Admin
Nombre completo
Comentario
Comentario del usuario
Código de país o región          000 (Predeterminado por el equipo)
Cuenta activa                    Sí
La cuenta expira                 Nunca
Último cambio de contraseña      29/08/2025 10:47:05
La contraseña expira             Nunca
Cambio de contraseña             29/08/2025 10:47:05
Contraseña requerida             No
El usuario puede cambiar la contraseña Sí
Estaciones de trabajo autorizadas Todas
Script de inicio de sesión
Perfil de usuario
Directorio principal
Última sesión iniciada           19/09/2025 8:59:16
```

12. net use

Muestra recursos compartidos y unidades conectadas.

 Ejemplo:

net use

```
PS C:\Windows\System32> net use
Se registrarán las nuevas conexiones.

No hay entradas en la lista.
```

13. net view

Muestra equipos compartidos en la red local (Windows).

 Ejemplo:

net view

```
PS C:\Windows\System32> net view
Error de sistema 6118.

La lista de servidores de este grupo de trabajo no se encuentra disponible en este momento.
```

14. route print

Muestra la tabla de enrutamiento del equipo.

 Ejemplo:

route print

```
PS C:\Windows\System32> route print
=====
Lista de interfaces
3...0a 00 27 00 00 03 .....VirtualBox Host-Only Ethernet Adapter
5...d8 43 ae 44 e2 25 .....Realtek PCIe GbE Family Controller
1.....Software Loopback Interface 1
=====
IPv4 Tabla de enrutamiento
=====
Rutas activas:
Destino de red      Máscara de red      Puerta de enlace      Interfaz      Métrica
0.0.0.0             0.0.0.0             192.168.0.1           192.168.0.31   25
127.0.0.0           255.0.0.0           En vínculo            127.0.0.1      331
127.0.0.1           255.255.255.255     En vínculo            127.0.0.1      331
127.255.255.255     255.255.255.255     En vínculo            127.0.0.1      331
192.168.0.0         255.255.254.0       En vínculo            192.168.0.31   281
192.168.0.31        255.255.255.255     En vínculo            192.168.0.31   281
192.168.1.255       255.255.255.255     En vínculo            192.168.0.31   281
```