Observación de conexiones TCP y UDP mediante Netstat

# Objetivos de aprendizaje

* Explicar parámetros y resultados de comandos **netstat** comunes.
* Utilizar **netstat** para examinar la información del protocolo en un host.

# Información básica

**netstat** es la abreviatura de la utilidad de estadísticas de red que se encuentra disponible tanto en computadoras Windows como en computadoras Unix / Linux. El paso de parámetros opcionales con el comando cambiará la información de resultado. **netstat** muestra conexiones de red entrantes y salientes (TCP y UDP), información de tabla de enrutamiento del equipo host y estadísticas de la interfaz.

# Situación

En esta práctica de laboratorio el estudiante examinará el comando **netstat** en un equipo host y ajustará las opciones de resultado de **netstat** para analizar y entender el estado del protocolo de la capa de Transporte TCP/IP.

# Explicar parámetros y resultados de comandos netstat comunes.

Abra una ventana terminal haciendo clic en Inicio | Ejecutar. Escriba **cmd** y presione **Aceptar**.

Para mostrar información de ayuda sobre el comando **netstat**, utilice las opciones **/?**, como se muestra:

C:\> **netstat /? <INTRO>**

Utilice el comando de salida **netstat** /? como referencia para completar la opción que mejor se ajuste a la descripción:

| **Opción** | **Descripción** |
| --- | --- |
| **netstat -a** | Muestra todas las conexiones y puertos que escuchan. |
| **netstat -n** | Muestra direcciones y números de puerto en forma  numérica. |
| **netstat -s 5** | Vuelve a mostrar estadísticas cada cinco segundos. Presione CONTROL+C para detener la nueva visualización  de las estadísticas. |
| **netstat -p [nom\_protocol]** | Muestra conexiones para el protocolo especificadas por protocolo. El protocolo puede ser cualquiera de los siguientes: TCP, UDP, TCPv6, o UDPv6. Si se usa con la opción –s para mostrar estadísticas por protocolo, el protocolo puede ser cualquiera de los siguientes:  IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, o UDPv6. |
| **netstat -a 30** | Vuelve a mostrar todas las conexiones y puertos que escuchan cada 30 segundos. |
| **netstat** | Muestra sólo las conexiones abiertas. Éste es un problema complicado. |

Cuando se muestran estadísticas **netstat** para conexiones TCP, también se muestra el estado TCP. Durante la conexión TCP, la conexión atraviesa por una serie de estados. La siguiente tabla es un resumen de los estados TCP desde RFC 793, Transmission Control Protocol, septiembre de 1981, tal como lo informó **netstat**:

| **Estado** | **Descripción de la conexión** |
| --- | --- |
| ESCUCHAR | La conexión local está a la espera de un pedido de conexión de parte de cualquier dispositivo remoto. |
| ESTABLECIDA | La conexión está abierta y se pueden intercambiar datos a través de la conexión. Éste es el estado normal para la fase de transferencia de datos  de la conexión. |
| TIEMPO-ESPERA | La conexión local está esperando un período de tiempo predeterminado después de enviar un pedido de finalización de conexión antes de cerrar la conexión. Ésta es una condición normal y generalmente dura entre 30 y  120 segundos. |
| CERRAR- ESPERAR | La conexión se cerró pero sigue esperando un pedido de finalización por  parte del usuario local. |
| SYN-ENVIADA | La conexión local espera una respuesta después de enviar un pedido de conexión. La conexión debe transitar rápidamente por este estado. |
| SYN\_RECIBIDA | La conexión local espera un acuse de recibo que confirme su pedido de conexión. La conexión debe transitar rápidamente por este estado.  Conexiones múltiples en el estado SYN\_RECIBIDO pueden indicar un ataque TCP SYN. |

Las direcciones IP mostradas por **netstat** entran en varias categorías:

| **Dirección IP** | **Descripción** |
| --- | --- |
| 127.0.0.1 | Esta dirección se refiere al host local o a este equipo. |
| 0.0.0.0 | Una dirección global, lo que significa “CUALQUIERA”. |
| Dirección remota | La dirección del dispositivo remoto que tiene una conexión con este equipo. |

# Tarea: Utilizar netstat para examinar la información del protocolo en un equipo host del módulo.

## Paso 1: Utilice netstat para ver conexiones existentes.

Desde una ventana Terminal, ejecute el comando **netstat –a**:

C:\> **netstat –a <INTRO>**

Se mostrará una tabla que lista el protocolo (TCP y UDP), dirección local, dirección remota e información sobre el estado. Allí también figuran las direcciones y los protocolos que se pueden traducir a nombres. (tarda unos segundos en mostrar toda la información)

La opción –n obliga a netstat a mostrar el resultado en formato bruto. Abra otra ventana Terminal, y ejecute ell comando **netstat –an**:

C:\> **netstat –an <INTRO>**

Utilice la barra de desplazamiento vertical de la ventana para desplazarse hacia atrás y adelante entre los resultados de los dos comandos. Compare los resultados, note la traducción de los puertos bien conocidos por nombres.

Busca y anota tres conexiones TCP y tres UDP del resultado de **netstat –a** y las mismas conexiones con los números de puertos traducidos correspondientes del resultado de **netstat –an**.

| Conexión | Protocolo Dirección Local Dirección remota Estado | |
| --- | --- | --- |
| TCP | TCP | 10.56.135.239:49159 ec2-52-41-114-21:https ESTABLISHED |
| TCP | 10.56.135.239:49243 172.67.70.71:https ESTABLISHED |
| TCP | TCP 10.56.135.239:49708 20.54.37.73:https ESTABLISHED | |
| TCP | 10.56.135.239:54036 52.98.159.2:https ESTABLISHED |
| TCP | TCP | 10.56.135.239:54037 40.101.92.194:https TIME\_WAIT |
| TCP | 10.56.135.239:54043 a104-83-69-234:https LAST\_ACK |
| UDP | UDP | 192.168.56.1:137 \*:\* |
| UDP | 192.168.56.1:138 \*:\* |
| UDP | UDP | 192.168.56.1:1900 \*:\* |
| UDP | 192.168.56.1:61083 \*:\* |
| UDP | UDP | 192.168.56.1:5353 \*:\* |
| UDP | 127.0.0.1:63207 \*:\* |

Consulte el siguiente resultado **netstat**.

| C:\> **netstat –n**  Conexiones activas Protocolo Dirección Local | Dirección remota | Estado |
| --- | --- | --- |
| TCP 127.0.0.1:1070 | 127.0.0.1:1071 | ESTABLISHED |
| TCP 127.0.0.1:1071 | 127.0.0.1:1070 | ESTABLISHED |
| C:\> |  |  |

Un ingeniero de red nuevo sospecha que su equipo host ha sufrido un ataque exterior a los puertos 1070 y 1071. ¿Crees que su sospecha es fundada?

No es un ataque, es una comunicación entre puertos dentro del mismo host.

**Paso 2: Establezca múltiples conexiones TCP simultáneas y grabe el resultado netstat.**

En esta tarea, se realizarán varias conexiones simultáneas a varios servidores. El comando **telnet**

autorizado se utilizará para acceder a los servicios de red de esos servidores, lo que proporcionará varios protocolos para examinar con netstat. (Ejecutar cmd con permisos de administrador para usar el comando telnet. También puedes activar el Cliente Telnet en Windows: ir a Panel de Control – Programas y Características - Hacemos clic en la opción de "Activar o desactivar las características de Windows". En la lista que aparece a continuación activamos la opción de "Cliente Telnet".)

Abra seis ventanas terminales.

Utilizaremos:

* HTTP, servidor web, puerto 80 (telnet osas.atopa.me 80)
* HTTPs, servidor web seguro, puerto 443 (telnet osas.atopa.me 443)
* SMTP, servidor de correo SMTP, puerto 25 (telnet correo.uvigo.es 25)
* DNS, servidor nombre de dominio, puerto 53 (telnet dns.uvigo.es 53)
* FTP, servidor FTP, puerto 21 (telnet ftp.uvigo.es 21)

Ejecuta cada telnet en una ventana terminal y en otra para **netstat –an**. Observa las conexiones que se han establecido con esos cinco servicios y el estado en el que se encuentra cada una de ellas (tendrás que hacer un nslookup para saber las direcciones IP que corresponden a cada servidor y localizarlas en el listado de conexiones).

Rellena la tabla con la información de las conexiones:

| Protocolo | Dirección Local | Dirección remota | Estado |
| --- | --- | --- | --- |
| TCP | 192.168.1.96:26260 | 193.147.85.14:80 | ESTABLISHED |
| TCP | 192.168.1.96:26261 | 193.147.85.14:443 | ESTABLISHED |
| TCP | 192.168.1.96:26262 | 193.147.85.14:25 | ESTABLISHED |
| TCP | 192.168.1.96:26263 | 193.147.85.14:53 | ESTABLISHED |
| TCP | 192.168.1.96:26264 | 193.147.85.14:21 | ESTABLISHED |

¿De qué tipo son los puertos telnet (tcp o udp)?

Tcp porque telnet va sobre tcp.

\* Ejecutar cmd con permisos de administrador para

\* Para cerrar una conexión telnet, presione las teclas <CTRL> ] juntas. Eso mostrará el indicador telnet,

Microsoft Telnet>. Escriba **quit <INTRO>** para cerrar la sesión.