HERRAMIENTAS DE DIAGNÓSTICO DE FALLOS EN REDES

Para ver errores en la red:

- ping: Utiliza dos mensajes. El de ida sería un ECHO REQUEST (con protocolo ICMP Tipo 8). Como respuesta, el equipo receptor responde con un ECHO REPLY (con protocolo ICMP Tipo 0).
    - ping -R [IPdestino]: Muestra como salida la ruta de ida y vuelta hacia el PC [IPdestino].

- Traceroute: Traza la ruta al destino. Esta herramienta, como ping, nos sirve para ver si dos PC's están conectados entre sí, pero, además, nos sirve para detectar fallos en medio de la conexión. Por defecto, usa paquetes UDP para la solicitud y paquetes ICMP para la respuesta.
    - traceroute -I [IPdestino] : Usa paquetes ICMP para la solicitud, igual que ping.
    - traceroute -T [IPdestino]: Usa paquetes SYNTCP para la solicitud.

Para monitorizar tráfico:

- Netstat: Herramienta que muestra todos los puertos y conexiones en un dispositivo. Nos permite monitorizar los diferentes elementos de la red y poder dar solución a problemas de red.
    - netstat -tl

- Netcat: Herramienta de red que permite abrir puertos TCP/UDP en un host y realizar el rastreo del tráfico en esos puertos. También se puede transferir cualquier tipo de archivo (se usa como complemento a netstat).
    - netcat -l 12345 (lo ejecuta el servidor)
    - netcat [IPservidor] 12345 (lo ejecuta el cliente)

- Tcpdump: Herramienta de red que permite abrir puertos TCP/UDP en un host y realizar el rastreo de tráfico en esos puertos. También se puede transferir cualquier tipo de archivo (se usa como complemento a netstat). Funcionamiento similar a Wireshark. Se ejecuta en la línea de comandos.
    - sudo tcpdump -i [interfaz]

- Wireshark: Software open-source de monitorización y análisis de tráfico de red, que suele usarse como analizador de protocolos. Sirve como una herramienta didáctica para el estudio de las comunicaciones y para la resolución de problemas de red.

En la red dada, hay 9 fallos:

No nos deja hacer ping entre PC_1 y PC_2 (están en la misma red). Esto es por los tres fallos siguientes:

1) No podemos hacer un ping entre dos PC's si uno de los dos PC's está apagado.
2) La tarjeta de red del PC_2 no estaba activada. Para ello, en VirtualBox, PC_2 -> Configuración -> Red -> Adaptador 1 -> Habilitar adaptador de red
3) No hay ningún cable de conexión entre PC_1 y PC_2. Para ello, en VirtualBox, vamos a PC_1 -> Configuración -> Red -> Adaptador 1 -> Avanzadas -> Marcamos la casilla Cable Conectado.
4) En el archivo etc/networks-interfaces siempre se pone la de loopback como mínimo. Si no se pone ninguna más, no se levantará ninguna interfaz más de red. De la misma forma, podemos deshabilitar interfaces en dicho archivo con una serie de comandos.
5) Cambiar la IP del PC_2 porque en vez de ser 33.1.1.3 es 33.8.8.8. Luego, hacemos *sudo nano /etc/netplan/01-network-manager-all.yaml*, y cambiamos la IP 33.8.8.8 por 33.1.1.3. Guardamos y salimos del archivo, y ejecutamos *sudo netplan apply* para que se apliquen los cambios.

No nos deja hacer ping entre PC_1 y PC_3 (están en distinta red). Esto es por los fallos siguientes:

6) SI hacemos ping desde PC_1 hasta PC_3 vemos que es inalcanzable. De hecho el paquete no sale ni de PC_1 (podemos verlo haciendo traceroute). Esto es porque no hay ningún Gateway por defecto en la tabla de rutas de PC_1. Para ello, hacemos *sudo nano /etc/netplan/01-network-manager-all.yaml.* Veremos que la línea del Gateway está comentada. La descomentamos, guardamos y salimos del archivo, y ejecutamos *sudo netplan apply* para que se apliquen los cambios.
7) Si ahora hacemos traceroute desde PC_1 hasta PC_2, vemos que el paquete desde PC_1 si llega al R_1 pero no a R_2. Para ello, usaremos Winbox. Nos conectamos al R_2 y le añadimos la entrada necesaria.

Ahora ya están conectados los tres PC's entre sí. Ahora vamos a intentar acceder remotamente desde PC_1 a PC_3. En todos los PC's está instalado Telnet (usa TCP). Es lo que vamos a usar para conectar los PC's remotamente. Vemos que PC_1 no se conecta remotamente a PC_3 (si se conectase nos pediría las credenciales). Esto es porque:

8) Comenzamos viendo si el puerto 23 (es el que se usa para Telnet) está escuchando en PC_3. Para ello, en PC_3 ejecutamos *sudo netstat -tln* y vemos que sí está escuchando las solicitudes telnet que le llegan. Usaremos Wireshark para ver el tráfico. Vemos que la interfaz enp0s3 no recibe ningún paquete TCP, es decir, los paquetes Telnet no están llegando a PC_3. Esto puede ser por el firewall de los routers. Miramos el firewall de los routers con Winbox. Vemos que el firewall de

R_1 está vacío (no hay problema) pero esto no es así con el R_2 (está restringiendo el tráfico). Ponemos la regla *drop* al final del todo (el orden de las reglas importa). Si, desde PC_1, hacemos telnet 33.1.2.2, vemos que nos sigue sin dejar.

9) Por el Wireshark, vemos que en PC_3 están llegando paquetes SYNTCP desde PC_1 pero vemos que PC_3 no está respondiendo. Esto se debe a que el propio firewall del SO (en Windows es Windows Defender y en LINUX es UFW=Uncomplicated FireWall). Está ocurriendo algo similar al fallo (6). UFW está haciendo que se rechacen los paquetes TCP. Si hacemos *sudo ufw status* vemos las reglas de UFW. Vemos que rechaza los paquetes del puerto 23 (puerto de Telnet). Para modificarlo hacemos *sudo ufw allow 23*. Si ahora hacemos *telnet 33.1.2.2* ya nos pide las credenciales, ponemos *administrador* y *finisterre* y vemos que ya hemos accedido (se nos cambia el prompt y nos pone PC_3).

10) Si intentamos hacer *telnet 33.1.2.2* desde PC_2 (ya no es desde PC_1), vemos que no nos deja. Si filtramos los paquetes TCP desde Wireshark en PC_3, podemos deducir que si se está estableciendo la conexión TCP pero de repente el servicio decide cerrar la conexión (paquete de color rojo). Esto se debe a que en la librería TCPWrappers (librería del sistema que permite conexiones TCP a ciertos usuarios o no). Si hacemos *sudo etc/hosts.deny*, vemos que está denegando todas las conexiones Telnet excepto la de 33.1.1.2 (el PC_1). Comentamos dicha línea, guardamos los cambios y salimos. Ahora si nos deja acceder remotamente desde PC_2 a PC_3 con Telnet.