Síntesis conceptual

Grado: Administración de Sistemas Informáticos en Red
Asignatura: Administración de sistemas operativos
Unidad: 2. Administración de la red en Linux

Resumen

Netplan es desde Ubuntu 17 la herramienta que se usa para configurar la red en estos sistemas. Los ficheros de configuración de *Netplan* se alojan en el directorio */etc/netplan* y llevan la extensión *.yaml*. Si queremos ver la IP de nuestro equipo para poder configurar la red, el comando que debemos usar puede ser **ip a** o **ip addr**. Podemos configurar la IP de manera estática o dinámica, pero cuando hagamos los cambios en los ficheros de configuración, debemos de lanzar el comando **sudo netplan try** para comprobar la sintaxis y **sudo netplan apply** para aplicar los cambios. Hay que tener siempre en cuenta que no se pueden añadir tabulaciones a los ficheros de *Netplan.*

SSH o *Secure Shell* es la principal de las conexiones remotas en los sistemas Linux. Para trabajar con esta herramienta debemos de instalar el paquete *OpenSSH-Server* y configurarlo en el fichero */etc/ssh/sshd_config*. Aquí tenemos que prestar atención a las opciones siguientes:

- *PermitRootLogin*
- *Port*
- *LoginGraceTime*
- *MaxAuthTries*
- *MaxStartups*
- *AllowUsers*
- *DenyUsers*

Los cambios se efectúan reiniciando el servicio **sshd**. Las conexiones las podemos realizar con tres comandos distintos:

- **ssh *usuario@IP***
- **ssh -v -l *usuario IP***
- **ssh *IP***

Para finalizar la sesión usamos el comando **exit**. También podemos acceder a sesiones Linux por SSH desde un cliente Windows con la herramienta *Putty*. La última herramienta que comentamos acerca de las conexiones remotas es VNC, que en nuestro caso se instala como servidor con el paquete *tightvncserver*. Una vez instalado, el comando **vncserver** nos ayuda a configurar la conexión.

Al hablar de seguridad en Linux, debemos referirnos a *Iptables*, que es su *firewall* por defecto, ya que filtra los paquetes entrantes y salientes mediante tablas de filtrado. La principal tabla de *Iptables* es la tabla *filter*, que además cuenta con tres cadenas: *INPUT, FORWARD* y *OUTPUT*. Para ver las reglas que ya hay definidas en *iptables* usamos el comando **iptables -L -v**. Cuando vayamos a añadir reglas debemos de hacerlo con el comando siguiente:

Iptables -A *cadena [opciones]* -j *acción*

Tres opciones muy usadas son: **-s** para IP de origen del paquete, **-i** para la interfaz de salida o entrada del paquete y **-m** para indicar un rango de direcciones. En relación con esta herramienta, para ver los números de las reglas usamos el comando **iptables -L --line-numbers.** Para eliminar las reglas usaremos o bien, **iptables -D *cadena nºregla*** para eliminar una regla en concreto o bien, **iptables -F** para eliminar todas las reglas. Por último, para hacer los cambios de *iptables* persistentes en el tiempo, lanzamos el comando **sudo /sbin/iptables-save**

Conceptos fundamentales

- **Dirección IP:** Dirección de protocolo de internet. Composición de dígitos separados por caracteres que determinan una posición e identidad en la red.
- **Interfaz de red:** dispositivo físico de un equipo que permite la conexión por red a este mismo de manera cableada o inalámbrica.
- **Acceso remoto:** método de acceso a equipos que se encuentran separados físicamente de la posición del usuario.
- ***Firewall:*** dispositivo de red que filtra el tráfico entrante y saliente con la intención de dotar de mayor seguridad a nuestro sistema.
- **Cadena de *iptables*:** conjunto de reglas que indican que debe de hacer el sistema con los paquetes que coincidan con las características que se definen en cada una de las reglas.
- **Dirección *localhost*:** dirección de red local asignada a nuestro propio equipo, por defecto siempre es 127.0.0.1.
- **Memoria volátil:** memoria del equipo que almacena los datos de los programas mientras que esté está encendido, pero cuando se apaga no se registra ningún cambio y toda la información almacenada desaparece.