

Práctica 9: Administración de la red

- ▶ Utilizando Virtualbox, añadir a todas las máquinas virtuales creadas en prácticas anteriores una tercera tarjeta red (se supone que la segunda se añadió en la practica 7)
 - a **Las tres máquinas en distinto host:** conectada en modo *bridge* a la interfaz **ethernet** de la maquina host. Uniremos ambos host mediante un cable ethernet
 - b **Las tres máquinas en el mismo host:** conectada a la red interna del virtualbox (la misma red interna en las tres máquinas)
- ▶ De esta manera todas las máquinas han de tener TRES tarjetas de red
 - ▶ primera tarjeta conectada al NAT del virtualbox y configurada mediante dhcp, proporcionando acceso a internet
 - ▶ segunda y tercera tarjetas conectadas conectadas entre sí mediante redes locales

Práctica 9: Administración de la red

- ▶ Para **maquina2** (la de la práctica 2) las tres tarjetas pueden ser
 - ▶ dos de tipo Intel y una de tipo PCnet (en cualquier orden)
 - ▶ una de tipo Intel y dos PCnet (en cualquier orden)
- ▶ Para **maquina1** y **maquina3**, las tres tarjetas han de ser de tipo Intel

Práctica 9: Administración de la red

- ▶ Configurar todas las interfaces de todas las máquinas (para todos los S.O.), de la siguiente manera, de manera que la configuración se mantenga al reiniciar

NIC1 : (**todas las máquinas**) (todos los S.O.) conectada al NAT del VirtualBox) y configurada mediante dhcp

- NIC2**
- ▶ **máquina1** (todos los S.O.) ip 192.168.1.101 con alias 192.168.10.101 y 192.168.100.101
 - ▶ **máquina2** (todos los S.O.) ip 192.168.1.102 con alias 192.168.10.102 y 192.168.100.102
 - ▶ **máquina3** (todos los S.O.) ip 192.168.1.103 con alias 192.168.10.103 y 192.168.100.103

- NIC3**
- ▶ **máquina1** (todos los S.O.) ip 192.168.2.101 con alias 192.168.20.101 y 192.168.200.101
 - ▶ **máquina2** (todos los S.O.) ip 192.168.2.102 con alias 192.168.20.102 y 192.168.200.102
 - ▶ **máquina3** (todos los S.O.) ip 192.168.2.103 con alias 192.168.20.103 y 192.168.200.103

Práctica 9: Administración de la red

1. Comprobar que todas las máquinas virtuales (todos los S.O) tienen acceso a internet a través de la interfaz conectada al NAT del Virtualbox
 2. Comprobar que (simultáneamente al apartado anterior) desde cada máquina se puede acceder a las otras dos utilizando distintas redes locales a las que están conectadas a la segunda y tercera tarjetas. (Comprobar que se accede puede hacerse viendo que responden al ping, o algún otro tipo de conexión)
 3. Rellenar el Cuadro_0 con los detalles de configuración de las NICS en los distintos S.O.
- ▶ En los sistemas linux
- ▶ **devuan:** se configurarán en `/etc/network/interfaces`. Configurar NetworkManager para que respete esa configuración
 - ▶ **ubuntu:** utilizar *netplan*
 - ▶ **fedora:** utilizar *nmcli*

Práctica 9: Control de acceso a nivel de aplicación

- ▶ Comprobaremos el funcionamiento de las `tcpwrappers` en los operativos de `maquina1:DevuanLinux`, `maquina1:Solaris` y `maquina3:FreeBSD` . Es decir, los sistemas Operativos Solaris, FreeBSD y devuan linux recibirán las conexiones de los S.O. de las otras máquinas.
- ▶ **devuan:** Instalar los paquetes `inetutils-inetd`, `inetutils-telnetd`.
Reiniciar

```
#apt-get install inetutils-inetd inetutils-telnetd
```
- ▶ **FreeBSD:** Habilitar `inetd` añadiendo `inetd_enable=YES` a `/etc/rc.conf`. Instalar `telnetd` (`pkg install freebsd-telnetd`).
Reiniciar
- ▶ **solaris:** Habilitar `inetd` (mediante `svcadm` comprobar que `telnetd` está desactivado
- ▶ En alguno de los operativos desde donde hacemos las conexiones puede ser necesario instalar el cliente `telnet`

Práctica 9

- ▶ Comprobar que las conexiones a telnet y a ssh estan desactivadas en devuan, solaris, y FreeBSD
- 1 Comprobar la conectividad para telnet y sshd desde TODOS los operativos de las otras máquinas: Rellenar CUADRO_1 del fichero adjunto
- ▶ Habilitar los servicios *telnet* y *ssh* en Solaris, devuan y FreeBSD
- 2 Comprobar las conexiones para telnet y sshd desde TODOS los operativos de las otras máquinas: Rellenar CUADRO_2 del fichero adjunto
- ▶ Usando los ficheros `/etc/hosts.allow` y/o `/etc/hosts.deny` permitir que se acepten únicamente las siguientes conexiones
 - ▶ telnet en las redes de la NIC2
 - ▶ ssh en las redes de la NIC3
- 3 Comprobar las conexiones: Rellenar el CUADRO_3
- 4 Rellenar el CUADRO_4: Quién está de hecho filtrando las conexiones, `inetd`? `tcpd`? o el programa que proporciona el servicio (`telnetd`, `in.telnetd`...)?

Ayudas

- ▶ los programas que proporcionan los servicios suelen estar en `/usr/sbin`. En los sistemas BSD podemos encontrarlos también en `/usr/libexec`
- ▶ en solaris los ejecutables de `inetd` y `sshd` son `/usr/lib/inet/inetd` y `/usr/lib/ssh/sshd`
- ▶ para reiniciar `inetd` (por ejemplo, después de cambiar su configuración) podemos ejecutar el script correspondiente en `/etc/init.d` (devuan) o en `/etc/rc.d` (sistemas BSD)
- ▶ también se puede reiniciar `inetd` (y que relea su configuración) enviándole la señal `HUP`

Forma de entrega

- ▶ Rellenar los cuadros 0 al 4 del fichero adjunto, junto con los nombres de los miembros del grupo
- ▶ Exportar a pdf con el nombre ASO-P9_ApellidosNombre.pdf, usando solo caracteres ASCII (p.e. si el grupo estuviese formado por Donal Trump Núñez y Bladimir Putin Sánchez, solo se entregaría **UN ARCHIVO**, ASO_P9-TrumpNunezDonal.pdf).
- ▶ Enviar por correo a antonio.yanez@udc.es antes del 19 Mayo con el asunto ASO: practica 9