Carlos Martín Sanz

4º - Mención en Computación

Práctica 1. Configuración de Laboratorio Virtual de Seguridad.

1. ***Indica las características de cada una de las máquinas virtuales utilizadas para montar el entorno de trabajo virtual: sistema operativo y arquitectura, número de procesadores, cantidad de memoria RAM asignada, velocidad de transmisión del adaptador de red.***

   - **Características de Alice:**

     Sistema operativo: Ubuntu

     Arquitectura: 32 bits

     Numero de procesadores: 1

     RAM: 512 MB

     Velocidad de transmisión del adaptador de red: 1000 Mbit/s

   - **Características de Bob:**

     Sistema operativo: Debian

     Arquitectura: 32 bits

     Numero de procesadores: 1

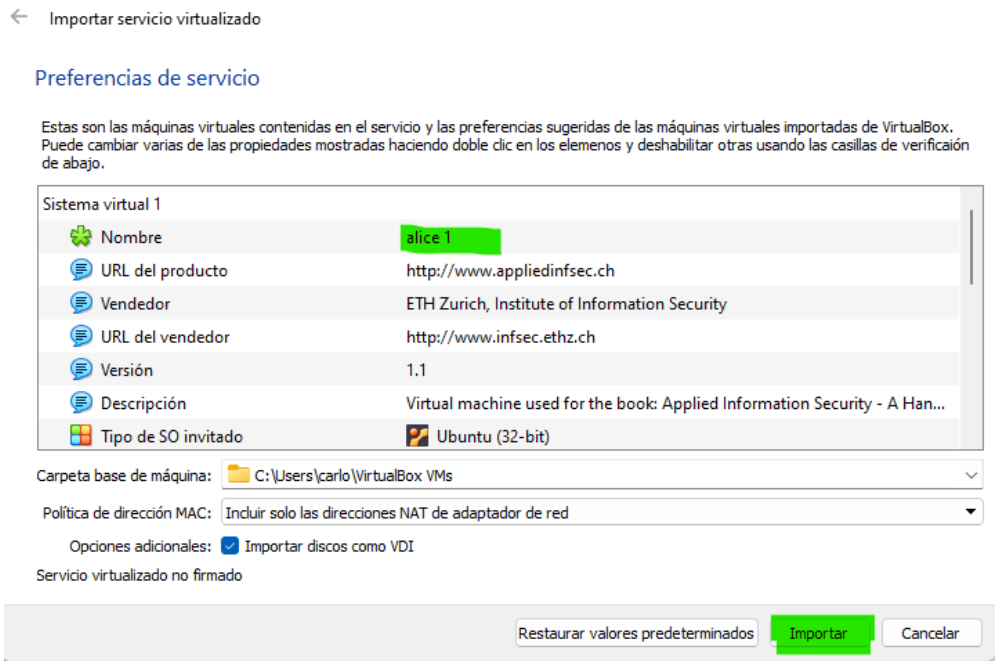
     RAM: 384 MB

     Velocidad de transmisión del adaptador de red: 1000 Mbit/s

   - **Características de Mallet:**
     Sistema operativo: Ubuntu
     Arquitectura: 32 bits
     Numero de procesadores: 1
     RAM: 512 MB
     Velocidad de transmisión del adaptador de red: 1000 Mbit/s

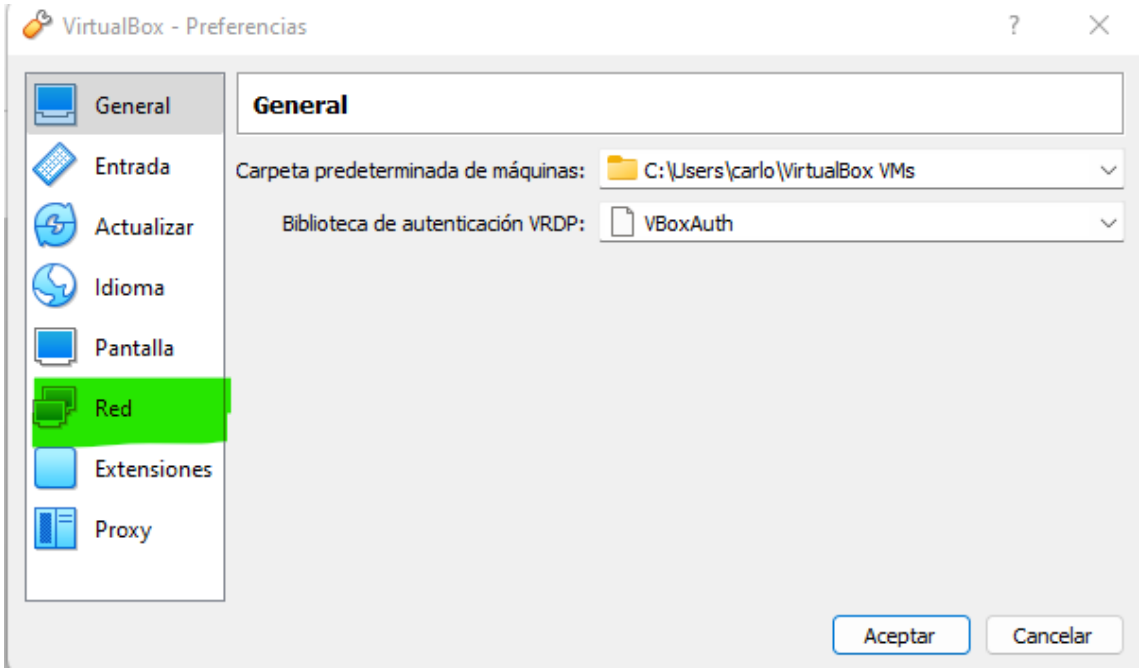
2. ***Configura el entorno de virtualización y las maquinas virtuales para que las tres maquinas se encuentren dentro de la Red NAT 10.0.2.0/24 de nombre "GSI". Documenta todos los pasos realizados***

Primero he importado cada una de las máquinas dentro del VirtualBox, esto lo he hecho haciendo doble click sobre los archivos .OVA que he descargado y se abre una ventana como esta



Y clicando en importar con el VirtualBox (previamente instalado) me ha añadido la máquina automáticamente a la aplicación. Hice esto con las tres.

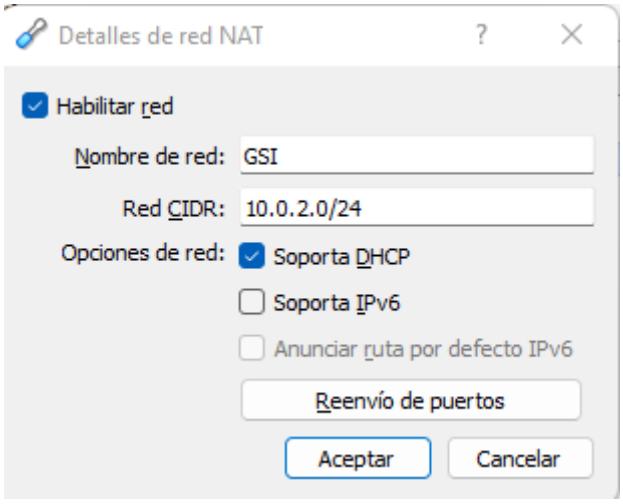
Una vez que ya están importadas, dentro de VirtualBox he clicado en Archivo (parte superior izquierda) y en Preferencias, donde se abre una ventana como esta:



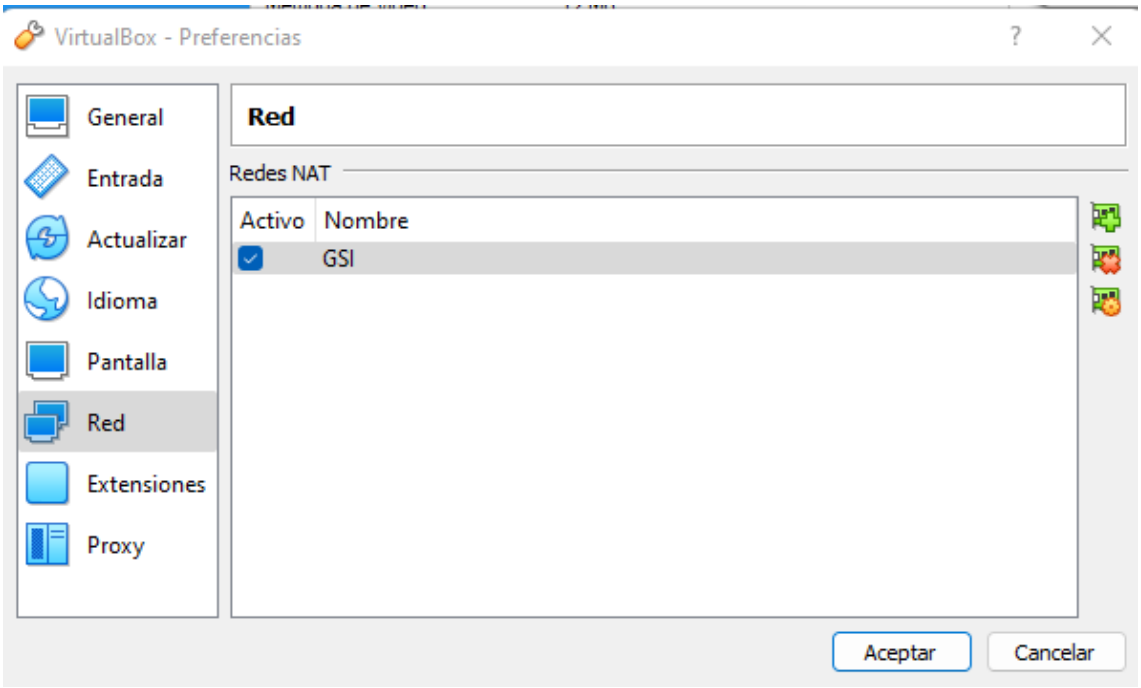
Y después en el apartado Red ya que es lo que nos interesa cambiar de la máquina.

En la derecha de esa ventana aparecen tres iconos, y para crear una nueva red clico en este:

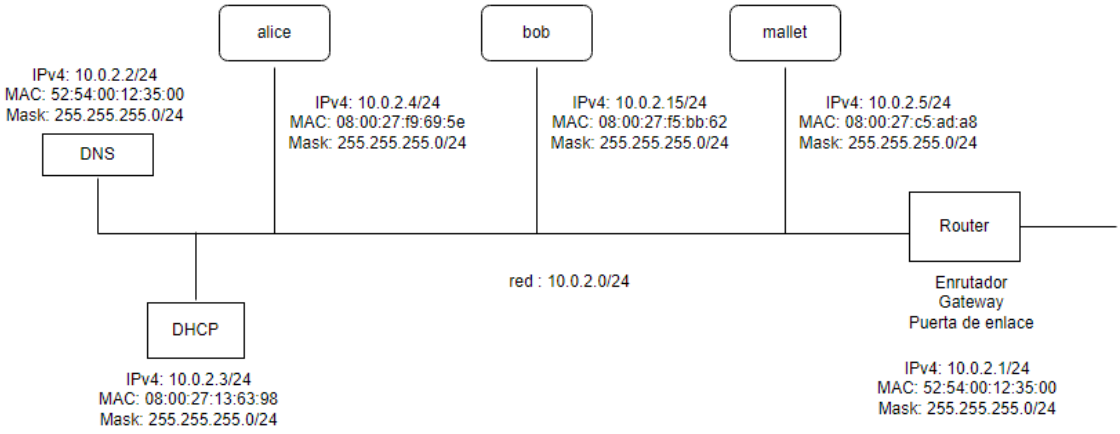
Una vez creada la red NAT, click derecho sobre esta y le cambio el nombre en este caso a GSI y en el apartado Red CIDR escribo la dirección del enunciado 10, como se ve en esta captura:



Aquí ya estaría creada, estos mismos pasos habría que repetirlos en las tres máquinas de la misma forma.



3. ***Dibuja un diagrama de la red lo más detallado posible de la red que forman las tres máquinas virtuales: alice, bob, mallet. Para cada máquina proporciona su dirección MAC, dirección IPv4 y máscara de red. Indica la dirección de red en formato IPv4 de la red en la que se encuentran las máquinas y la puerta de enlace (Gateway) de cada una de ellas. ¿Es la misma? Justifica tu respuesta.***

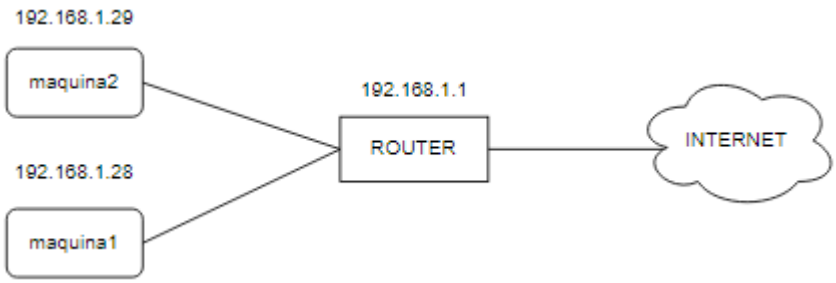


El Gateway o también conocido como router, es el mismo para las tres máquinas ya que se encuentran todas en la misma red, en este caso NAT.

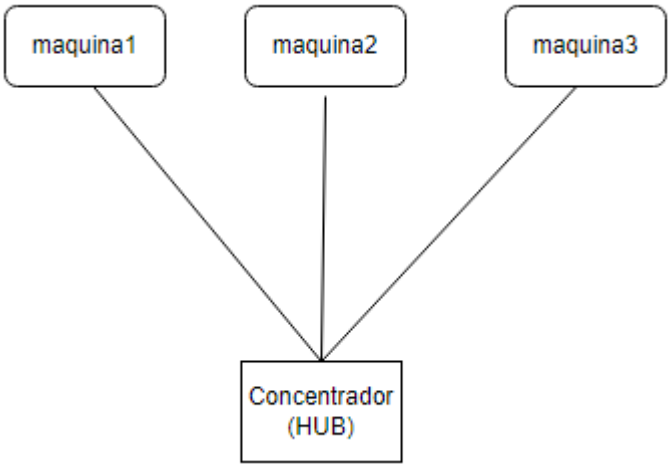
4. ***Indica con tus palabras cuál es la diferencia, en el sistema de virtualización utilizado, entre el modo NAT, red NAT y red interna; para entenderlo mejor, proporciona un ejemplo gráfico de cada uno de los modos de funcionamiento.***

Modo NAT: las máquinas virtuales se pueden conectar a internet, pero para ello se mapean puertos mediante NAT, y no se podrían conectar entre las distintas máquinas virtuales.

Red NAT: incorpora las mismas características que el Modo NAT, pero aquí las máquinas virtuales se pueden conectar entre ellas.



Red interna: las máquinas virtuales se van a poder comunicar entre ellas, que estén en esa misma red, pero no con máquinas que se encuentren en redes externas a esta, puesto que no puede conectarse a internet, y tampoco desde el equipo anfitrión conectarse a las máquinas virtuales.



5. ***Realiza pruebas para comprobar que las máquinas virtuales se comunican entre sí a nivel de red (capa 3 del modelo de referencia OSI). Para ello, puede utilizar el comando ping. Documenta la información necesaria que justifique que las máquinas tienen comunicación a nivel de red.***

Para ello levanto las tres máquinas virtuales, y realizo un ping desde una de ellas a las otras dos, en este caso he elegido de bob a alice y mallet.

```
bob:/home/bob# ping 10.0.2.4 -c 5
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=1.11 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=1.31 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=1.03 ms
64 bytes from 10.0.2.4: icmp_seq=4 ttl=64 time=2.04 ms
64 bytes from 10.0.2.4: icmp_seq=5 ttl=64 time=2.24 ms

--- 10.0.2.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 1.030/1.550/2.245/0.499 ms
bob:/home/bob# ping 10.0.2.5 -c 5
PING 10.0.2.5 (10.0.2.5) 56(84) bytes of data.
64 bytes from 10.0.2.5: icmp_seq=1 ttl=64 time=1.38 ms
64 bytes from 10.0.2.5: icmp_seq=2 ttl=64 time=1.75 ms
64 bytes from 10.0.2.5: icmp_seq=3 ttl=64 time=2.60 ms
64 bytes from 10.0.2.5: icmp_seq=4 ttl=64 time=1.80 ms
64 bytes from 10.0.2.5: icmp_seq=5 ttl=64 time=6.68 ms

--- 10.0.2.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4016ms
rtt min/avg/max/mdev = 1.386/2.847/6.680/1.957 ms
bob:/home/bob#
```

El primer ping es de bob a alice y el segundo de bob a mallet, para evitar que envíe continuamente paquetes hasta que yo lo cancele con la opción “-c 5” hago que solo se

envíen 5, y lo subrayado en rosa indica que se han enviado 5 y el receptor ha recibido todos.

Un ping no solo es envío, sino que también respuesta, por tanto, alice y mallet también se comunican con bob.

Lo único que nos faltaría seria comprobar la comunicación de mallet con alice, para ello, ahora hago otro ping,

```
mallet@mallet:~$ ping 10.0.2.4 -c 5
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.845 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.843 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=0.780 ms
64 bytes from 10.0.2.4: icmp_seq=4 ttl=64 time=0.669 ms
64 bytes from 10.0.2.4: icmp_seq=5 ttl=64 time=0.920 ms

--- 10.0.2.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3998ms
```

Con estos dos pings queda demostrado que las tres máquinas tienen conexión todas con todas en esta red.

6. ***¿Es posible inferir el sistema operativo de cada una de las maquinas a través del valor del TTL (Time To Live) del paquete que devuelven las maquinas después de recibir una petición del tipo ICMP? Justifica tu respuesta.***

Si es posible inferir el sistema operativo a través del TTL. TTL es un temporizador que va incluido en los paquetes que se envían a través de las redes y se encarga de decirle al receptor cuanto tiempo debe retener o usar el paquete antes de caducar los datos de este.

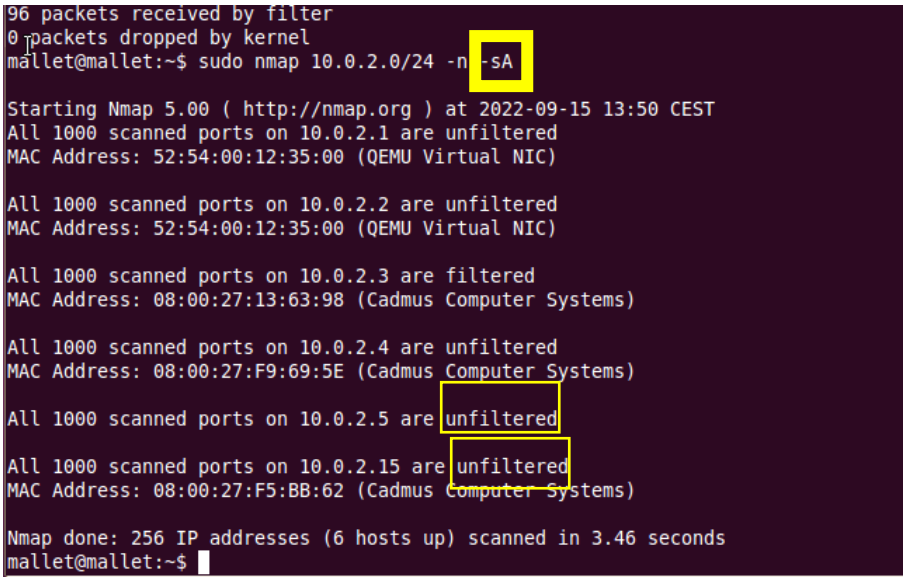
Cada sistema operativo tiene un valor diferente de TTL, por tanto, realizando un ping uno de los campos de información que nos aporta, es el propio valor de este TTL, según el valor que tenga, la máquina tendrá un sistema operativo u otro.

```
64 bytes from 10.0.2.5: icmp_seq=2 ttl=64 time=1.75 ms
```

En este caso (ping de bob a mallet) el valor del TTL = 64, y el valor TTL predeterminado para Linux/Unix es 64, lo cual es correcto puesto que mallet esta montada sobre un sistema operativo Linux (Ubuntu).

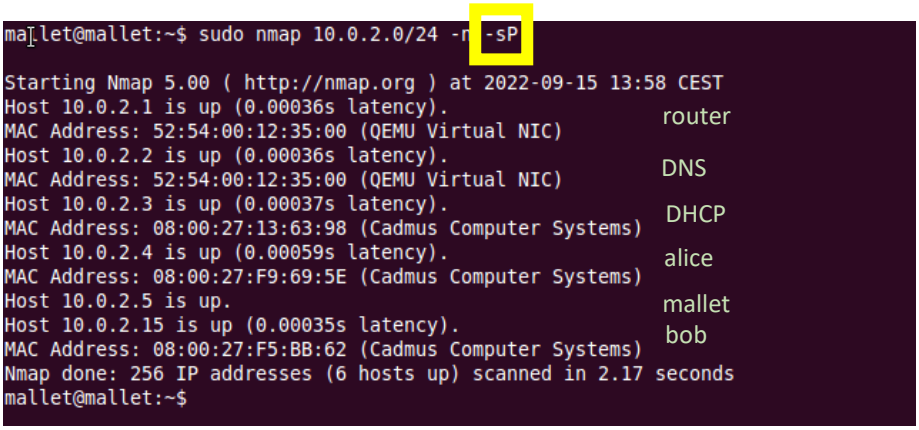
7. ***Desde la máquina "mallet", utiliza la herramienta "nmap" para realizar un descubrimiento de los host que se encuentren en su mismo segmento de red pero sin escanear ningún servicio TCP/UDP. ¿Qué protocolo te parece mas adecuado para ello, ARP o ICMP? Justifica tu respuesta.***

Escaneado con ICMP:



Ya que ICMP determina a través de TCP ACK si un puerto esta o no filtrado, enviando un ACK vacío, y los clasifica como “filtered” o “unfiltered”.

Y escaneado con ARP:



Con ARP podemos ver que nos aporta las direcciones únicamente, de los 6 host.

El escaneado realizado con nmap encuentra 6 hosts activos, donde 3 de ellos son las máquinas virtuales (bob, alice y la propia mallet) y los otros 3 son el servidor DNS, DHCP y el Router de la red NAT.

ARP es un protocolo que solo sirve para las máquinas virtuales que estén en el mismo segmento de red, mientras que ICMP vale para varios segmentos de red. Por tanto, en este caso yo creo que ARP es más adecuado, puesto que las tres máquinas virtuales están dentro de la misma red, y además este escaneo nos proporciona las direcciones MAC de cada uno de ellos ya que pertenecen a la misma red.

Sin embargo, si estuviésemos ante un sistema mucho más grande con varias redes que necesitasen comunicarse errores o datos del estado las redes entre sí, el protocolo ICMP sería el adecuado.

8. Indica los problemas que te has encontrado y como los has resuelto.

La mayoría de los problemas con los que me he encontrado han sido resueltos por el profesor durante la sesión de laboratorio puesto que la mayoría de los comandos o rutas que hemos necesitado no las conocía, por tanto, la realización de los pasos simultáneamente al profesor me ha resuelto la mayoría de los problemas.

De forma resumida en una lista los principales:

- Para editar el fichero de interfaces seria necesario el editor nano
- La ruta /etc/network/interfaces, la cual desconocía, y con ello también la modificación a realizar dentro de este fichero
- Activar la interfaz de red con ifup eth? (? El numero correspondiente)
- Una vez modificado el fichero, como reiniciar de nuevo la red /etc/init.d/networking stop y luego start
- La realización de ciertos comandos como nmap, necesitan permisos de super usuario y por ello necesitan sudo previamente, así como algunos de los parámetros de este como -n (no realice DNS), -sP (escaneo tipo ARP) o -sA (tipo ICMP).