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, numero de procesadores, cantidad de memoria RAM asignada, velocidad de transmisión del adaptador de red.*

Características de Alice:
- Sistema operativo: Ubuntu de 32 bit
- N.º procesadores: 1
- Memoria RAM: 512 MB
- Velocidad de transmisión del adaptador de red: 1000 Mbit/s

Características de Bob:
- Sistema operativo: Debian de 32 bit
- N.º procesadores: 1
- Memoria RAM: 384 MB
- Velocidad de transmisión del adaptador de red: 1000 Mbit/s

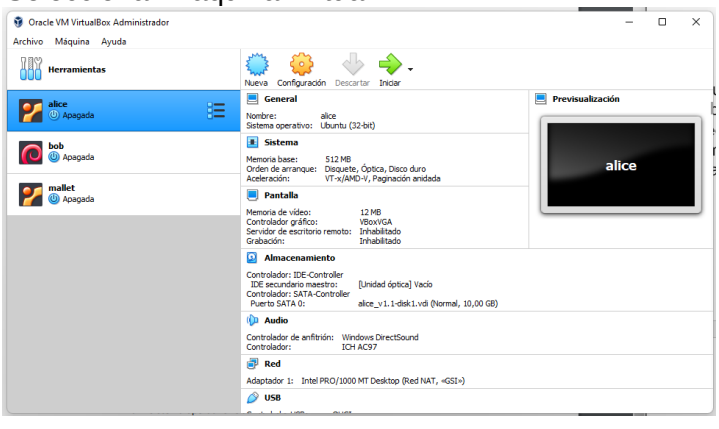
Características de Mallet:
- Sistema operativo: Ubuntu de 32 bit
- N.º procesadores: 1
- Memoria RAM: 512 MB
- Velocidad de transmisión del adaptador de red: 1000 Mbit/s

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

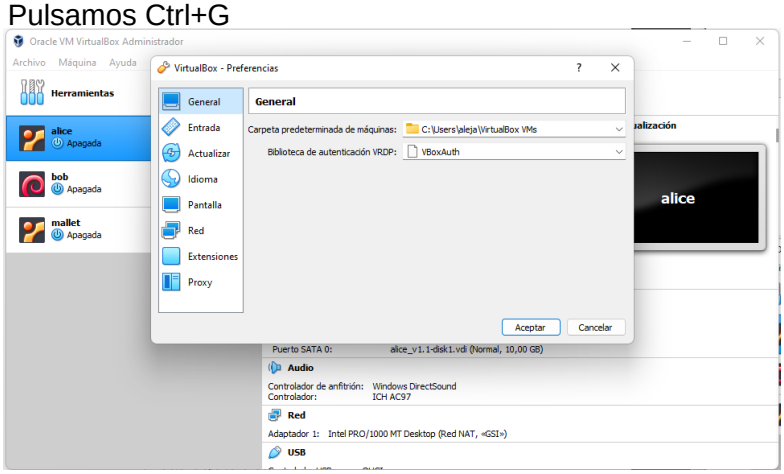
Para la instalación de las 3 máquinas virtuales lo primero es ir a Archivo>Importar servicio virtualizado y después seleccionar en el explorador de archivos cada uno de los archivos .ova que teníamos que tener descargados previamente.

Para configurar la red NAT seleccionamos una máquina virtual y pulsamos Ctrl+G. Nos aparecerá una ventana con distintas opciones, pulsaremos en "Red". En el lateral derecho de la ventana tendremos 3 emoticonos de color verde, pulsaremos al primero (añadir red NAT). Se nos desplegará otra ventana con la configuración de la red, en este caso dejaremos la que viene por defecto. Realizaremos estos pasos con las otras dos máquinas virtuales restantes.

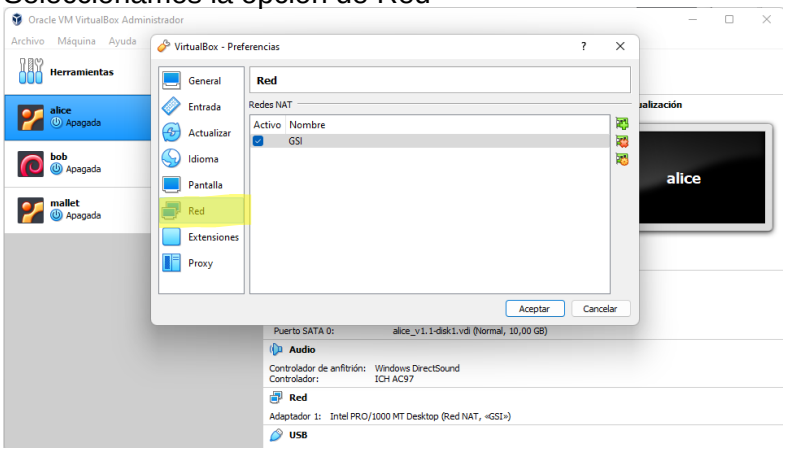
Seleccionar Máquina Virtual



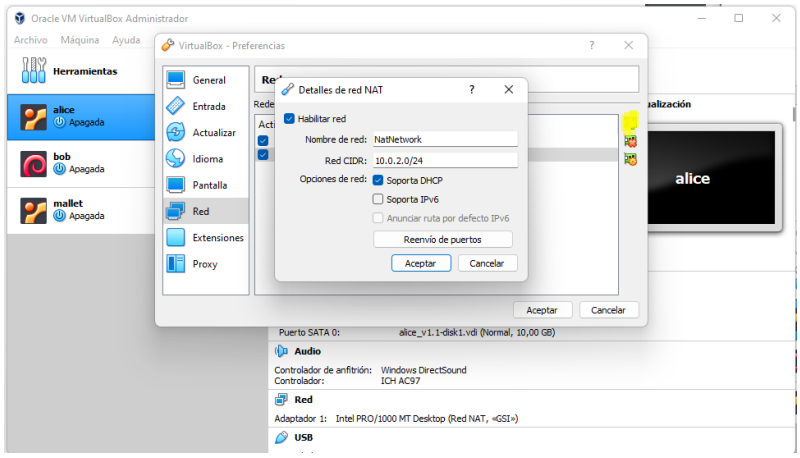
Pulsamos Ctrl+G



Seleccionamos la opción de Red



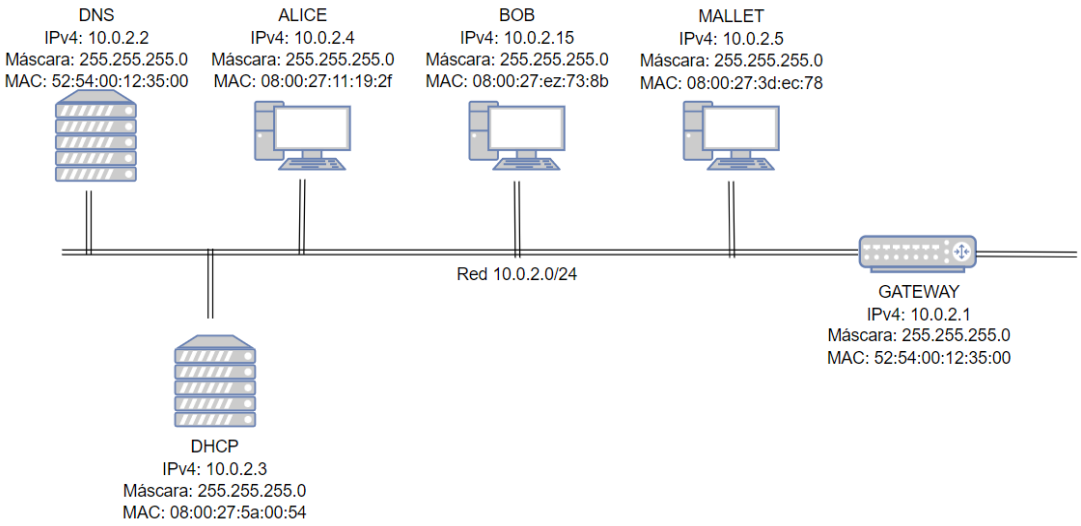
Añadimos una red NAT clicando en el icono de la derecha



Si no nos apareciera la ventana de configuración de la red, se puede modificar la configuración de una red ya creada pulsando en el tercer icono del lateral derecho.

3. *Dibuja un diagrama de 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*

   La puerta de enlace es la misma para todas las maquinas ya que se encuentran todas bajo la misma red NAT. Al diagrama he añadido el servidor DNS que añade virtualbox por defecto.



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.*

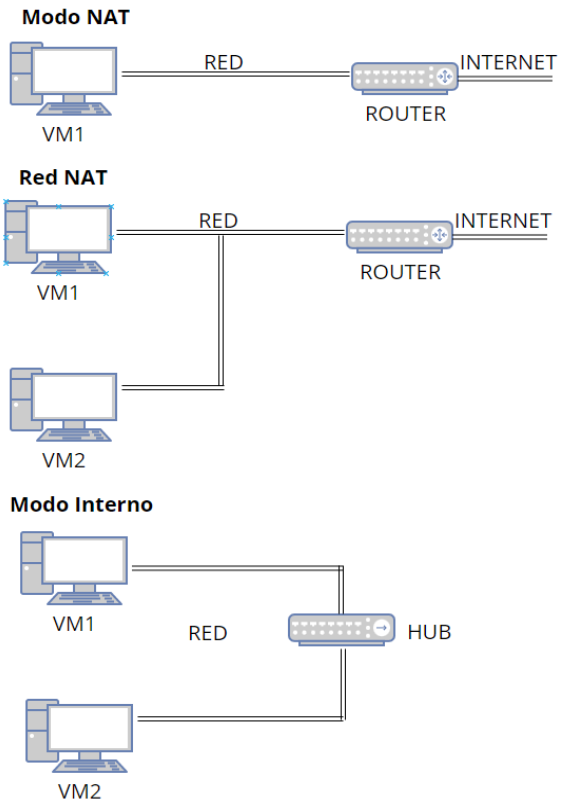
   Modo NAT: Las máquinas virtuales podrían conectarse a internet, pero no comunicarse entre ellas. Para conectarse desde internet a una máquina habría que mapear puertos a través de NAT. No es posible la comunicación con el Host

   Red NAT: Es exactamente lo mismo que el modo NAT añadiendo la posibilidad de conectarse entre las máquinas virtuales

   Modo Interno: En este modo solo hay posibilidad de conexión entre las máquinas, es decir, estas no podrían comunicarse con internet, ni con el host... Solo entre ellas.

	VM ↔ HOST	**VM1 ↔ VM2**	**VM → INTERNET**	**VM ← INTERNET**
Interna	no	si	no	no
NAT	no	no	si	mapeo de puertos
Red NAT	no	si	si	mapeo de puertos

Este ejemplo muestra las posibles comunicaciones que puede tener la máquina virtual llamada VM1 en los tres modos comentados anteriormente.



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, puedes utilizar el comando ping. Documenta la información necesaria que justifique que las máquinas tienen comunicación a nivel de red.*

   Desde la máquina de Bob he realizado un ping a la máquina de Alice y otro a la de Mallet viendo como Bob si que tiene conexión con Alice y con Mallet. Como ping requiere una respuesta también se puede ver que Mallet y Alice se pueden comunicar con Bob.

```
bob:~# ping 10.0.2.4 -c 3
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=0.518 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=2.38 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=1.30 ms

--- 10.0.2.4 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 0.518/1.404/2.385/0.765 ms
bob:~# ping 10.0.2.5 -c 3
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=3.91 ms
64 bytes from 10.0.2.5: icmp_seq=2 ttl=64 time=1.84 ms
64 bytes from 10.0.2.5: icmp_seq=3 ttl=64 time=1.93 ms

--- 10.0.2.5 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 1.849/2.564/3.910/0.953 ms
bob:~# _
```

Tras realizar ping desde Alice a Mallet podemos ver que también tienen conexión entre sí, es decir, que ya queda comprobado que todos tienen conexión con todos a nivel de red.

```
root@alice:~# ping 10.0.2.5 -c 3
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=3.97 ms
64 bytes from 10.0.2.5: icmp_seq=2 ttl=64 time=1.31 ms
64 bytes from 10.0.2.5: icmp_seq=3 ttl=64 time=0.991 ms

--- 10.0.2.5 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 0.991/2.094/3.977/1.337 ms
```

6. *¿Es posible inferir el sistema operativo de cada una de las máquinas a través del valor del TTL (Time To Live) del paquete que devuelven las máquinas después de recibir una petición de tipo ICMP(8)? Justifica tu respuesta.*

   Si que es posible como podemos ver en el enlace recomendado, ya que cada SO tiene valores distintos para los TTL(Tiempo de vida de los paquetes que envía la maquina).

```
root@alice:~# ping 10.0.2.5
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=4.24 ms
64 bytes from 10.0.2.5: icmp_seq=2 ttl=64 time=1.29 ms
64 bytes from 10.0.2.5: icmp_seq=3 ttl=64 time=1.20 ms
64 bytes from 10.0.2.5: icmp_seq=4 ttl=64 time=1.23 ms
```

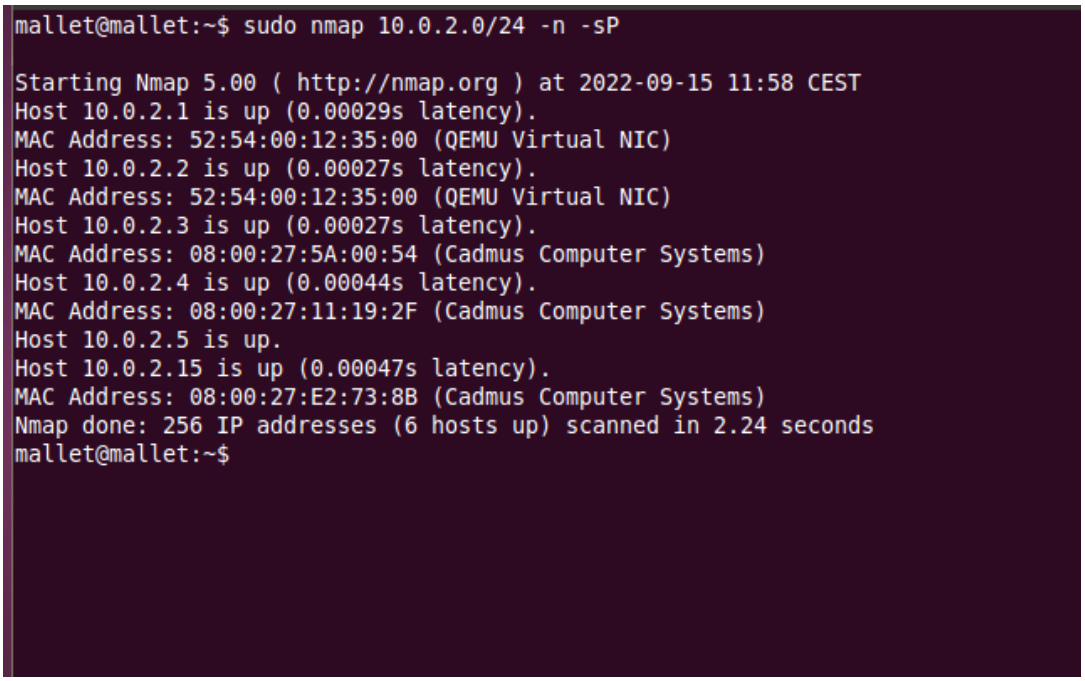
   Por tanto, realizando un ping podemos ver el TTL de los paquetes y en la página del enlace ver a que SO corresponde. En nuestro caso realizamos ping desde Alice hasta Mallet y vemos como el TTL es 64, lo que correspondería a un SO Linux cosa que es cierta como vemos en las especificaciones de la máquina.

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 más adecuado para ello, ARP o ICMP? Justifica tu respuesta.*

   Mediante la instrucción "nmap" con argumentos la IP de la red NAT, -n para que no haga resoluciones DNS y -sP para que haga el escaneo por ACK sin escanear servicios TCP/UDP obtenemos que son 6 los hosts que se encuentran en la red.

   Diría que es más adecuado utilizar el protocolo ARP ya que este es protocolo de la capa de enlace que se encarga de obtener las direcciones físicas de las máquinas que están bajo una misma red.
   Si las máquinas estuvieran en distinta red sería más conveniente usar el protocolo ICMP.

Imagen de los hosts encontrados.



Los host corresponden a las máquinas de Bob, Mallet, Allice, el servidor DNS y el Router de VirtualBox y el servidor DHCP.

8. *Indica los problemas que te has encontrado y cómo los has resuelto.*

   El problema principal es la falta de conocimiento de los comandos utilizados y la falta de costumbre a la hora de trabajar con redes ya que soy de la mención de computación. Los problemas con los comandos han sido resueltos con las explicaciones y las guías dadas por el profesor.

   Otras dudas como los argumentos que debía usar en según qué comandos (por ejemplo, los argumentos de nmap) los he resuelto mediante el libro de prácticas (basin) o en búsquedas por internet.

9. *Bibliografía:*

Apuntes Lab: 2011-Basin-AppliedInfSec-Springer.pdf
Herramienta modelado: *https://online.visualparadigm.com/es/diagrams/features/network-diagram-software/*
Nmap arguments: *https://nmap.org/book/man-briefoptions.html*
Red NAT, modo NAT y modo Interno: https://danitic.wordpress.com/2018/10/24/diferencias-entre-nat-red-nat-adaptador-puente-internal-y-solo-anfitrion-en-virtualbox/