



BOOTCAMP

Ciberseguridad en formato online

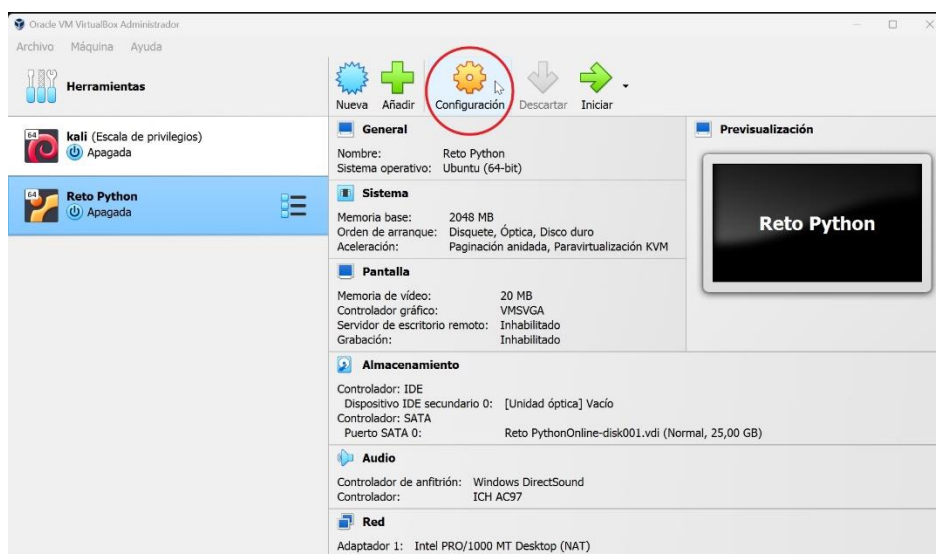


CONEXIÓN POR SSH DE UNA MÁQUINA A OTRA

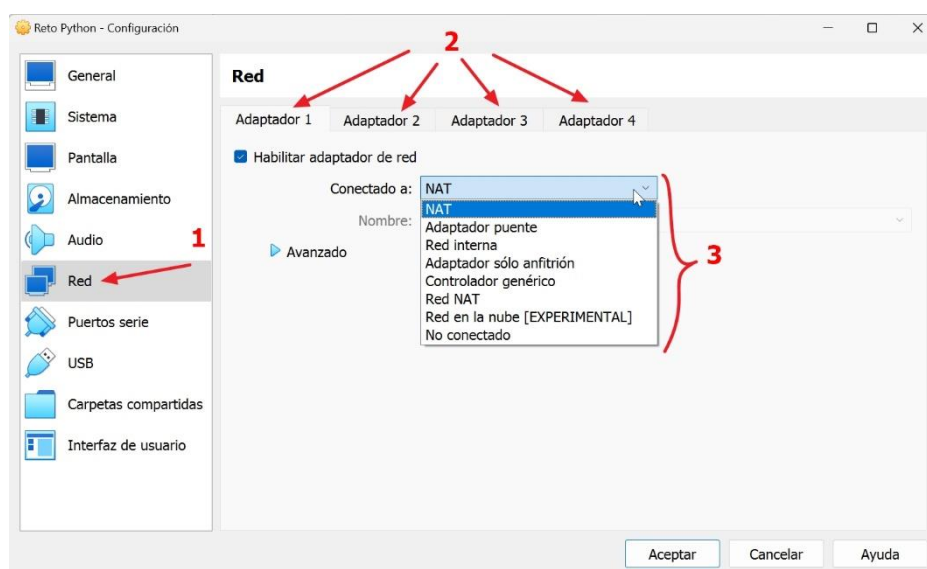
Para la realización de los distintos retos del bootcamp, en numerosos casos nos encontraremos con la necesidad de conectarnos de manera remota a esas máquinas virtuales. Para poder hacer esta conexión debe cumplirse que el puerto 22 esté abierto en la máquina receptora, o sea, la maquina donde vamos a conectarnos de manera remota.

Para poder llevar a cabo esta conexión, antes de iniciar nuestras máquinas virtuales debemos revisar los adaptadores de red para comprobar que las máquinas consiguen verse, ya no solo que tengan la misma máscara de subred, sino que compartan la misma conexión de red.

1º Con VirtualBox arrancado vamos a la pestaña **Configuración**.



2º Creamos la configuración del adaptador/es de red que necesites tener levantados. Puede darse el caso de que necesites tener varios adaptadores para conectar varias máquinas a la vez.

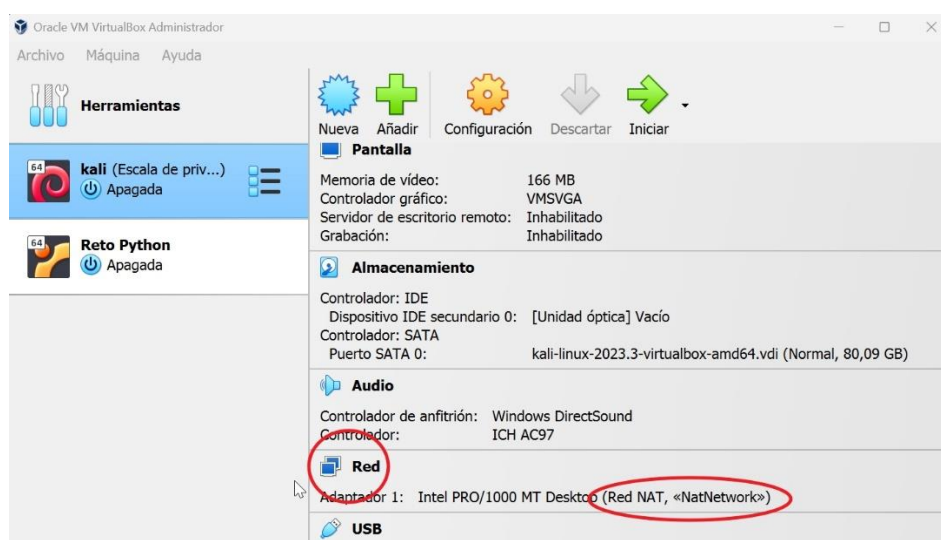


En esta ocasión solo vamos a necesitar un adaptador por lo que seleccionamos el **Adaptador 1** y lo habilitamos. Después seleccionamos el tipo de conexión de red.

Por si no lo sabes todavía hay distintos tipos de conexiones que se pueden efectuar entre dos máquinas, o más.

- **NAT:** La máquina virtual dispone de salida a internet, pero no consigue verse con el resto de máquinas virtuales, ni con el host.
- **Adaptador puente (Bridge):** Conecta a la máquina virtual a la misma red que el host. Para entenderlo de manera más sencilla; creamos un nuevo equipo en la misma red de nuestro ordenador.
- **Red interna:** Conecta las máquinas que tengamos entre sí, pero no cuentan con salida a internet ni a la red donde está situada el host. Creamos una VPN entre las máquinas virtuales y el host. Es una red aislada.
- **Adaptador solo anfitrión (Host-only):** Crea una VPN entre el host y las máquinas virtuales, por lo que solo se mantiene una conexión siempre y cuando la máquina virtual tenga conexión al host. Su diferencia respecto con la red interna, es que con la red interna no nos haría falta tener al host como intermediario, mientras que en Host-only sí.
- **Controlador genérico:** Nos otorga una función muy básica de conexión entre distintas máquinas virtuales y el host. En ningún caso usaremos este tipo de conexión, ya que tiene funciones muy básicas frente a los tipos de conexión que nos brindan los distintos tipos de redes.
- **Red Nat:** Es un tipo de conexión donde nos permite crear una red entre varias máquinas virtuales, con salida a internet.
- **No conectado:** Nos sirve para no tener conexión con ninguna máquina virtual, ni host, ni acceso a internet.
- **Red en la nube:** A día de hoy está en fase de experimentación, por lo que todavía no se hace uso de ella.

3º Para esta ocasión vamos a usar la conexión **Red NAT -> NatNetwork**

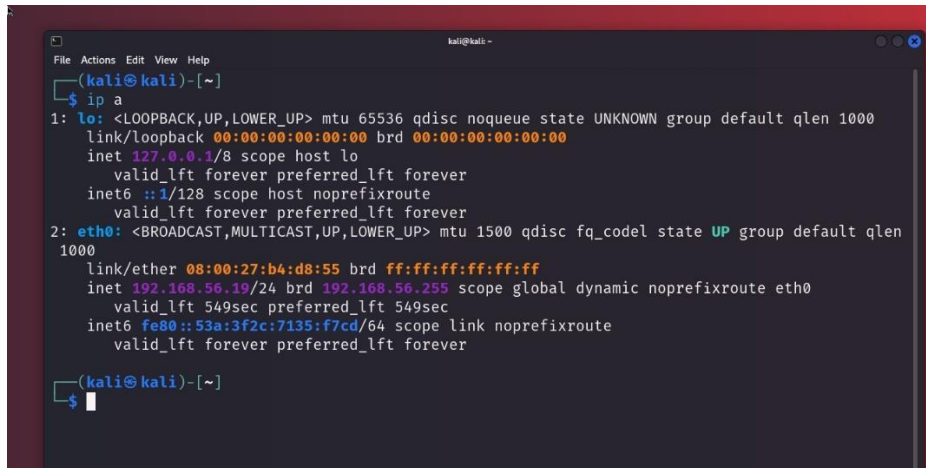


4º Repetimos el mismo proceso con Reto Python.

5º Iniciamos las dos máquinas virtuales.

6º Como la conexión que queremos realizar es desde nuestra Kali a la máquina de Reto Python ya solo debes trabajar desde tu Kali. Dentro de tu Kali abre una terminal y escribe lo siguiente

ip a y pulsa el enter.



```

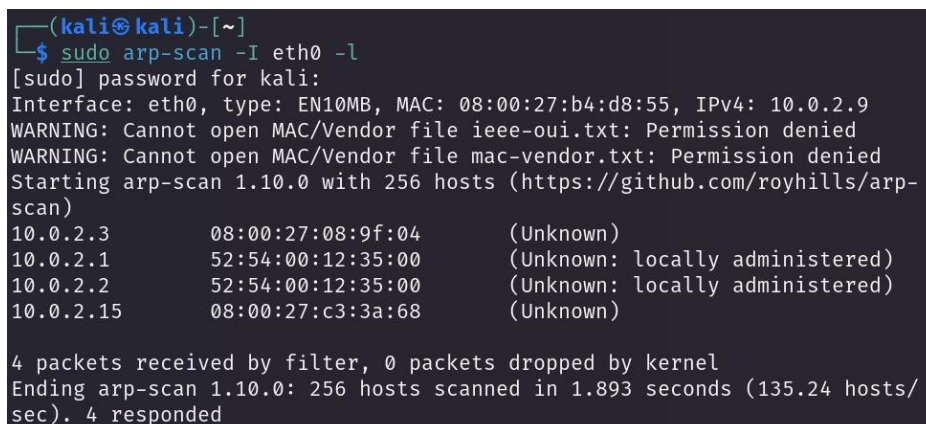
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:b4:d8:55 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.19/24 brd 192.168.56.255 scope global dynamic noprefixroute eth0
        valid_lft 549sec preferred_lft 549sec
    inet6 fe80::53a:3f2c:7135:f7cd/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
(kali㉿kali)-[~]
$
  
```

RECUERDA: Las IP's en este caso que estamos barajando son las mías, no tiene porqué salirte a ti iguales. Lo importante es que entiendas qué es cada aspecto para que puedas realizar la conexión por SSH.

De esta manera te saldrán las opciones de adaptadores de red que hayas creado anteriormente en la configuración de red de la máquina virtual. En este caso hemos seleccionado el adaptador 1 con una conexión de Red NAT; por lo que en este caso nuestro adaptador se corresponde con el **eth0** con una IP en nuestra Kali que es **10.0.2.15**

7º Ahora que ya sabemos cuál es nuestro adaptador vamos a listar el resto de IP's que estén conectados a este mismo adaptador con el siguiente comando:

sudo arp-scan -I eth0 -l



```

(kali㉿kali)-[~]
$ sudo arp-scan -I eth0 -l
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:b4:d8:55, IPv4: 10.0.2.9
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
10.0.2.3          08:00:27:08:9f:04      (Unknown)
10.0.2.1          52:54:00:12:35:00      (Unknown: locally administered)
10.0.2.2          52:54:00:12:35:00      (Unknown: locally administered)
10.0.2.15         08:00:27:c3:3a:68      (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.893 seconds (135.24 hosts/sec). 4 responded
  
```

De esta manera conseguimos listar las distintas IP. Las primeras IP's que aparecen son interfaces de red virtuales de VirtualBox que crea para poder llevar a cabo el enrutamiento de las conexiones. En este caso, la última es la de nuestra máquina Reto Python.

RECUERDA: Las IP's en este caso que estamos barajando son las mías, no tiene porqué salirte a ti iguales.

8º para conectarnos a una máquina por SSH siempre vamos a necesitar dos cosas, saber su usuario y conocer la contraseña. Sin las credenciales nos va a ser imposible conectarnos a través de este protocolo.

Para este primer reto, **Reto Python**, las credenciales son:

Usuario: **user1**

Password: **St@rt1ng**

Sabiendo las credenciales y la IP a la que nos queremos conectar (en mi caso, 10.0.2.15), vamos a realizar la conexión.

9º Volvemos a la terminal de nuestra Kali y escribimos:

user1@10.0.2.15 sean las direcciones IP asignadas a las interfaces de red virtuales de VirtualBox en tu máquina anfitriona.

Después nos pedirá la contraseña: **St@rt1ng**.

Tras esto estaremos conectados al reto para poder iniciar el **TEAM CHALLENGE**.

```
(kali㉿kali)-[~]
$ ssh user1@10.0.2.15
The authenticity of host '10.0.2.15 (10.0.2.15)' can't be established.
ED25519 key fingerprint is SHA256:HkyjvIvLqRiz0qjlfLrfHaHUmKRRKMcRhYtkxwu
6N9Q.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:16: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.15' (ED25519) to the list of known hos
ts.
user1@10.0.2.15's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 6.5.0-28-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Se pueden aplicar 294 actualizaciones de forma inmediata.
88 de estas son actualizaciones de seguridad estándares.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradabl
e

Last login: Thu May  9 12:11:07 2024 from 10.0.2.9
user1@ubuntu-VirtualBox:~$
```

RECUERDA: Cuando nos conectamos por primera vez con unas credenciales a una nueva máquina virtual nos sale un mensaje como este.

```
$ ssh user1@10.0.2.15
The authenticity of host '10.0.2.15 (10.0.2.15)' can't be established.
ED25519 key fingerprint is SHA256:HkyjvIvLqRiz0qjlfLrfHaHUmKRRKMcRhYtkxwu
6N9Q.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:16: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

Este mensaje de fingerprint no deja de ser más que un aviso por si confiamos en la conexión a esa máquina y así ejecutar la conexión por primera vez.



**THE
BRIDGE**

