Práctica 2

Jesús Rodríguez Heras
Arantzazu Otal Alberro

27 de marzo de 2019

1. Instalación de máquinas virtuales mediante Vagrant

En esta primera parte vamos a crear el entorno de trabajo, consistente en tres máquinas virtuales pertenecientes a una misma red privada. Las máquinas se tendrán que crear a partir de un mismo fichero Vagrant.

1. VM1, con IP 192.168.2.101
2. VM2, con IP 192.168.2.102
3. VM3, con IP 192.168.2.103

Las máquinas tendrán la siguiente configuración:

- nmap tiene que estar instalado en todos.
- iptables en la máquina VM1.
- ufw en la máquina VM1 (debería estar instalado por defecto).
- fwbuilder.

La instalación de los paquetes se deberá realizar mediante la provisión de Vagrant.

Para inicializar Vagrant usamos `vagrant init debian/jessie64` y luego abrimos y modificamos el archivo `Vagrantfile` de la siguiente forma:

```
Vagrant.configure("2") do |config|

  config.vm.box = "debian/jessie64"
  config.vm.provision :shell, path: "bootstrap.sh"

  config.vm.define :vm1 do |vm1|
   vm1.vm.box="debian/jessie64"
   vm1.vm.hostname="VM1"
   vm1.vm.network "private_network", ip: "192.168.2.101"
  end

  config.vm.define :vm2 do |vm2|
   vm2.vm.box="debian/jessie64"
   vm2.vm.hostname="VM2"
   vm2.vm.network "private_network", ip: "192.168.2.102"
  end

  config.vm.define :vm3 do |vm3|
   vm3.vm.box="debian/jessie64"
   vm3.vm.hostname="VM3"
   vm3.vm.network "private_network", ip: "192.168.2.103"
  end

end
```

A continuación, iniciamos las tres máquinas virtuales en terminales diferentes con `vagrant up vmX` y nos conectamos a ellas mediante `vagrant shh vmX` (siendo "X" el número de la máquina virtual comprendido entre 1 y 3).

Para instalar nmap en todas las máquinas usaremos el aprovisionamiento de Vagrant creando el archivo `bootstrap.sh` siguiente:

```
#!/usr/bin/env bash

apt-get update
apt-get install -y nmap
```

2. Visibilidad de las máquinas

Para los distintos ejercicios, se identifica a las máquinas como VM1, VM2 y VM3. Por comodidad, es recomendable poder usar nombres en las reglas. Para ello, se puede añadir en `/etc/hosts` una línea asociando un nombre y una IP con la siguiente sintáxis: IP NOMBRE ALIAS.

Para hacer esto, entramos en las tres máquinas virtuales y accedemos al archivo mencionado con `sudo nano /etc/hosts` y lo modificamos de la siguiente forma:

```
 192.168.2.101 vm1
 192.168.2.102 vm2
 192.168.2.103 vm3
```

3. Configuraciones IPtables

3.1. Primeras pruebas

En este ejercicio se pide testear VM1 desde VM2, realizando los siguientes ejercicios:

1. **Desde VM2 comprobar los puertos que VM1 tiene abiertos.**
   Para comprobar los puertos usamos: `nmap vm1`.

2. **Prohibir el acceso por ssh.**
   Para ello usaremos: `sudo iptables -A INPUT -p tcp --dport 22 -j DROP`

3. **Responde a las siguientes preguntas:**

   - **¿Qué ha pasado?**
     La consola se queda bloqueada sin poder establecer conexión por ssh.
   - **¿Puedo crear una nueva conexión?**
     Es imposible.
   - **¿La consola sigue funcionando?**
     No, se queda bloqueada y no responde.

3.2. Configuración mínima

En los ejercicios siguientes, siempre debe partir de esta configuración:

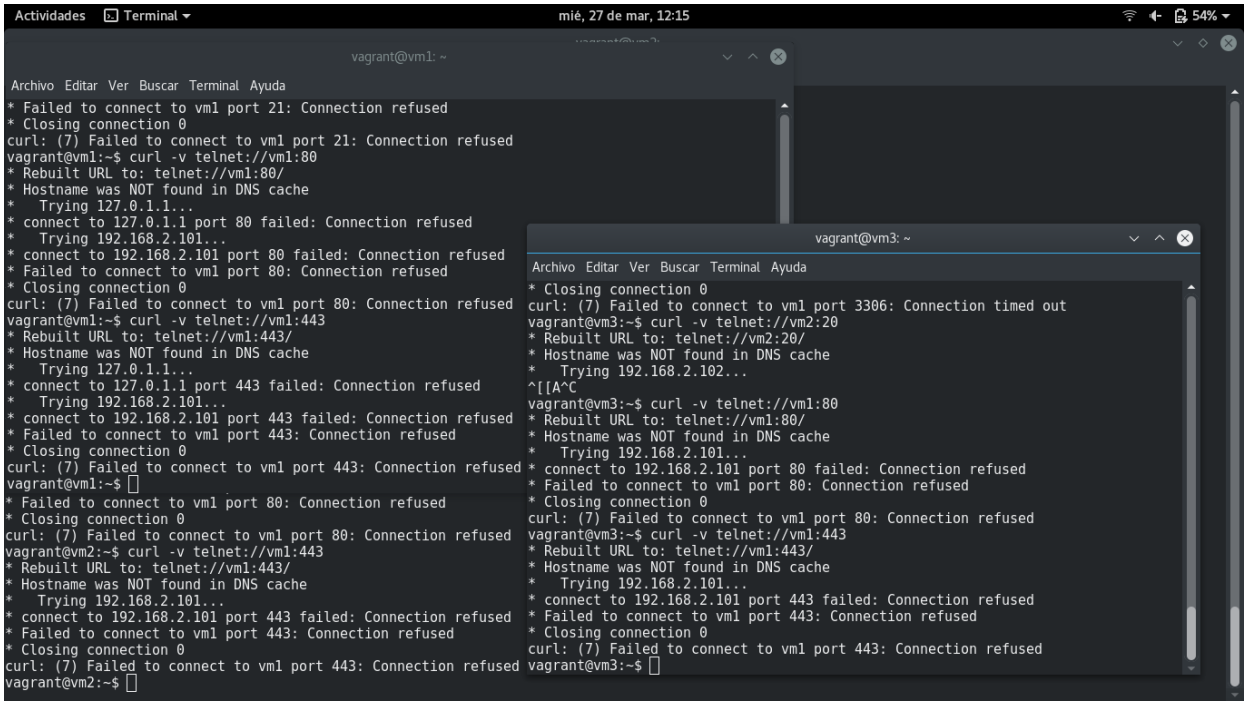
- **Permitir conexiones locales.**
  `sudo iptables -A INPUT -i lo -j ACCEPT`
- **Permitir conexiones ya establecidas.**
  `sudo iptables -A INPUT -m state --state ESTABLISHED -j ACCEPT`
- **Políticas por defecto de rechazar en input.**
  `sudo iptables -A INPUT -j DROP`

Para comprobar estas configuraciones hicimos ping entre las máquinas para ver la conectividad.

3.3. Configurando servidor web completo

Configurar VM1 para que tenga la configuración de un servidor web, permitiendo:

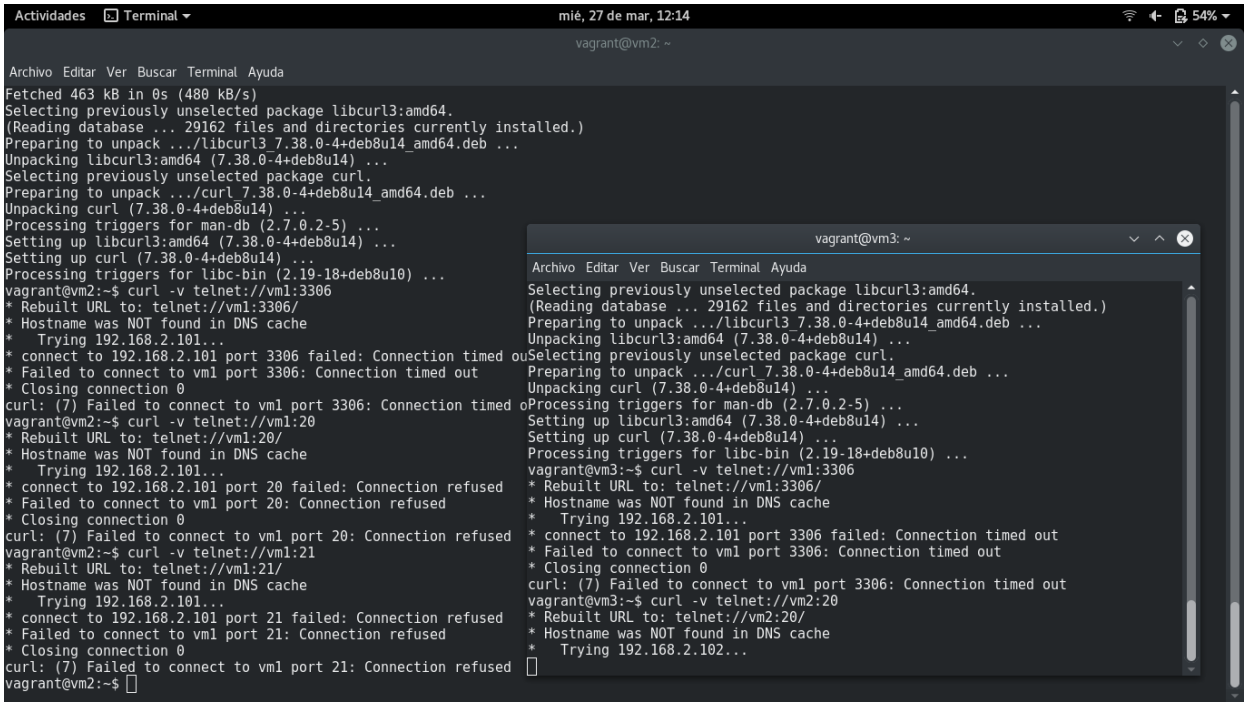
- **Todos se conecten a los puertos http y https.**
  Primero mostramos las iptables con `sudo iptables -L` y, si tenemos la anterior que no permitía conexiones entrantes, usamos `sudo iptables -F` para borrarlas todas[1] (con el inconveniente de que tendremos que reescribir las que queramos).
  Para habilitar http usamos: `sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT`
  Para habilitar https usamos: `sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT`



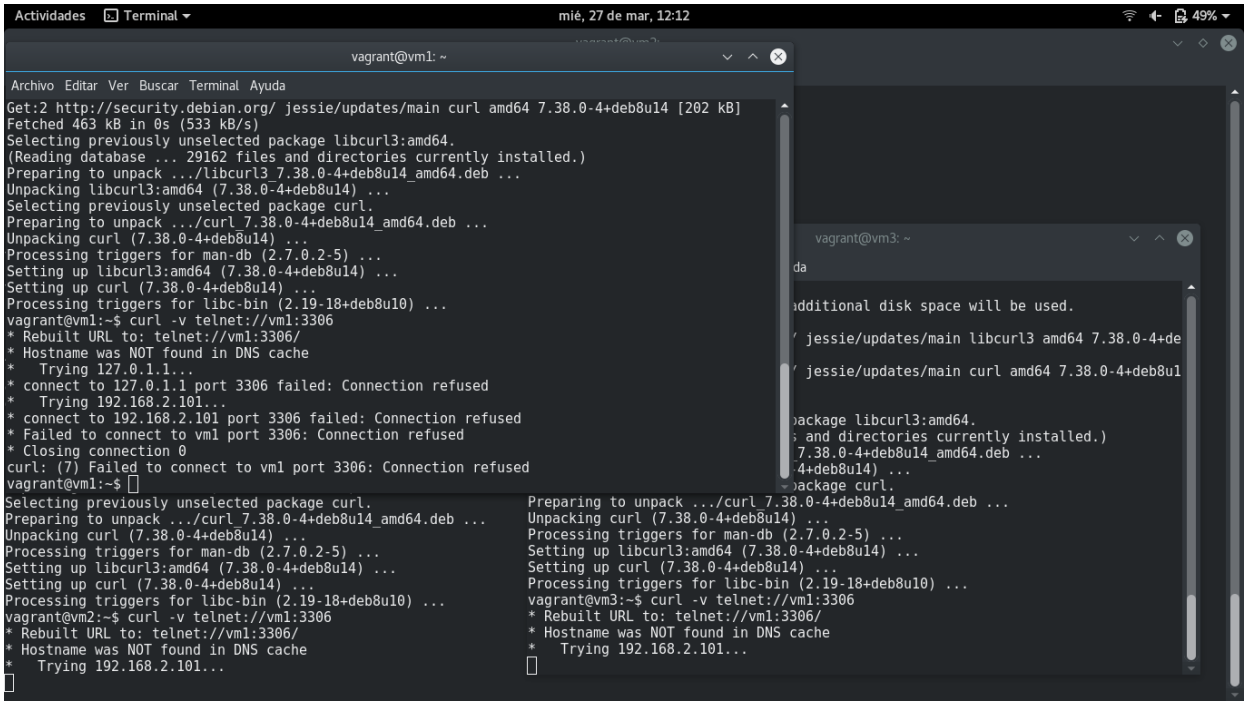
[1] Si queremos borrar solo una regla, mostramos todas las reglas existentes con `sudo iptables -L --line-numbers` y para borrar la que queramos usamos `sudo iptables -D INPUT numeroderegla`

- **Conexión únicamente por parte de VM2 al servidor ftp.**

```
sudo iptables -A INPUT -p tcp --dport 20 -s 192.168.2.102 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 21 -s 192.168.2.102 -j ACCEPT
```



- **Configurar VM1 para que sólo se pueda conectar localmente a mysql.**
  `sudo iptables -A INPUT -p tcp -i lo --dport 3306 -j ACCEPT`



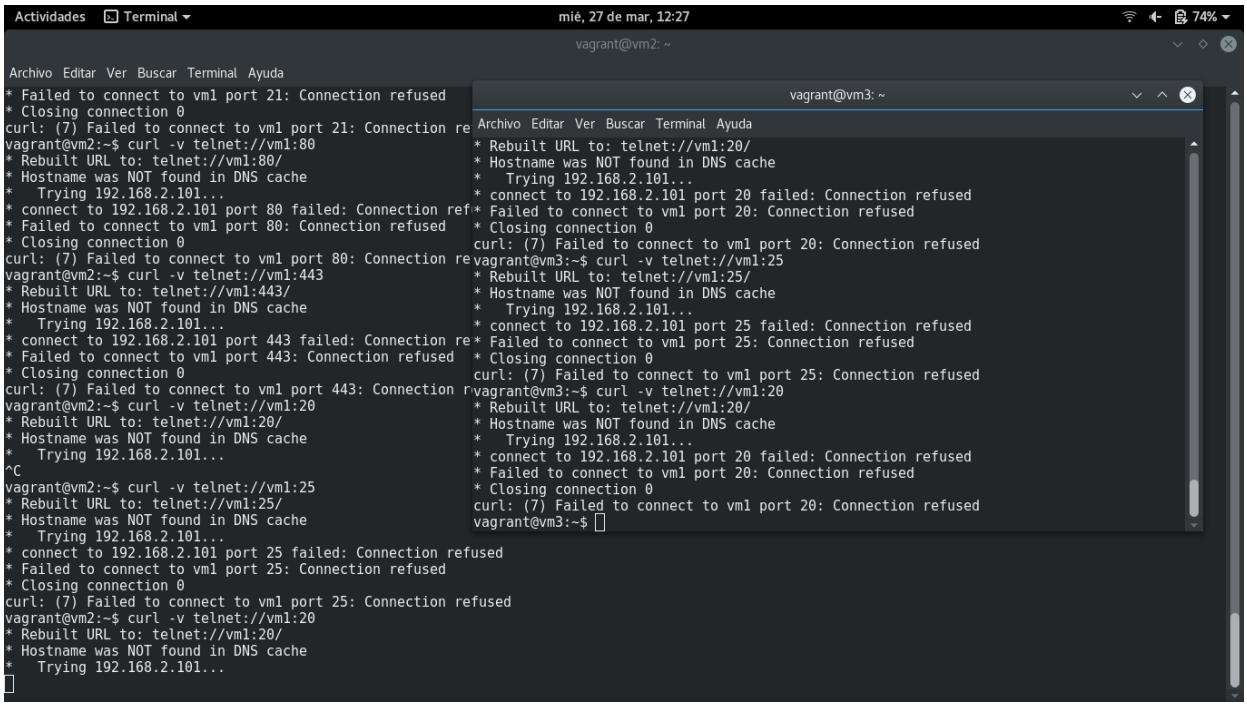
Otra opción para comprobar los puertos abiertos es poner el comando `nc -l numerodepuerto &`. Eso nos abrirá e puerto que queramos y lo mandará a segundo plano con la finalidad de que el nmap o el telnet nos indique que ese puerto está abierto y a la escucha. Para cerrarlo, tendremos que poner el comando `kill -9 PID`, siendo PID el PID del proceso que nos mantiene el puerto abierto (que se nos muestra al mandar a segundo plano el comando `nc`).5

3.4. Poniendo excepciones

Permitir conectar a VM1 desde VM2 y VM3 el acceso a los puertos desde 1:1000, con la excepción de que VM2 no se puede conectar por FTP.

Para VM2: `sudo iptables -A INPUT -p tcp --dport 20:21 -s 192.168.2.102 -j DROP;sudo iptables -A INPUT -p tcp --dport 1:1000 -s 192.168.2.101 -j ACCEPT`

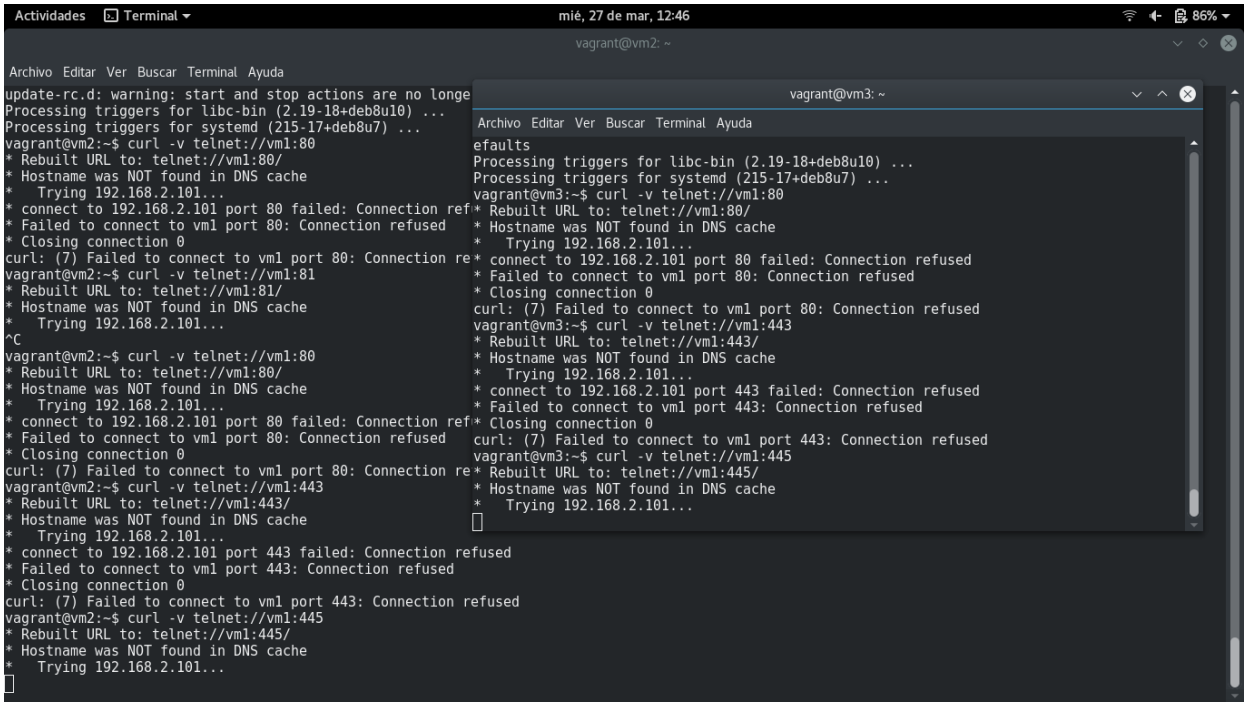
Para VM3: `sudo iptables -A INPUT -p tcp --dport 1:1000 -s 192.168.2.103 -j ACCEPT`



4. UFW

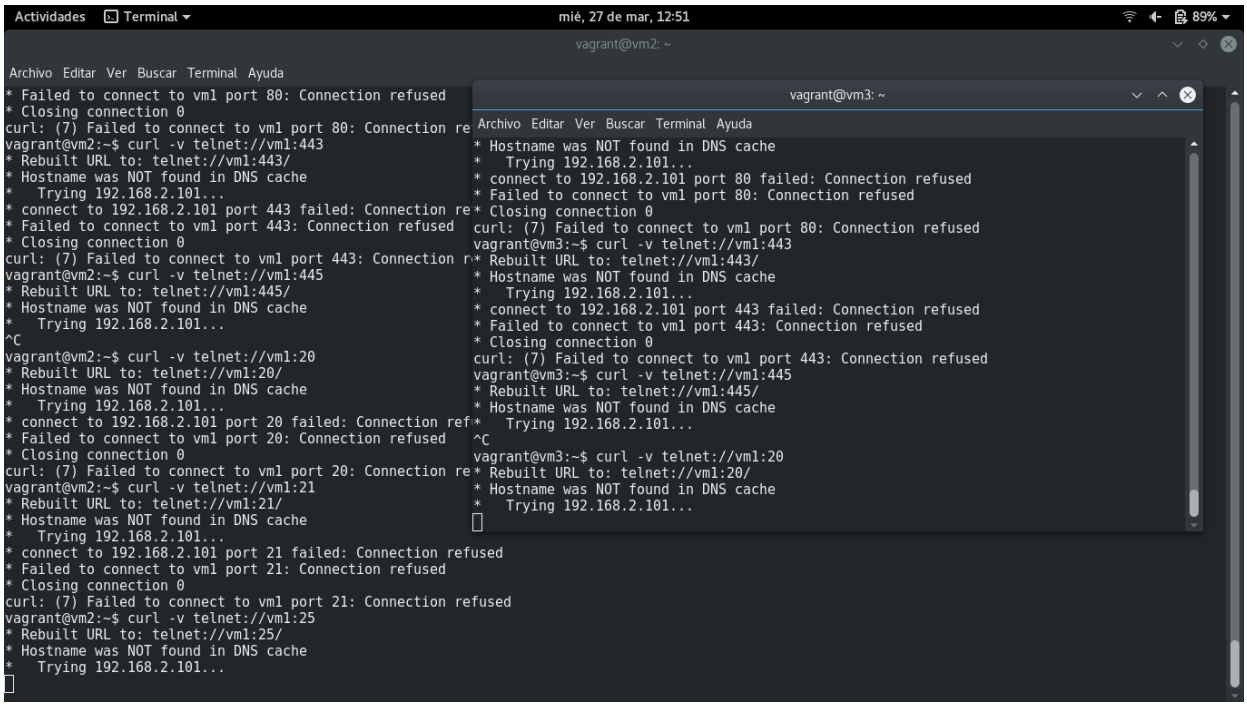
Configurar VM1 para que tenga la configuración de un servidor web, permitiendo:

- **Todos se conecten a los puertos http y https.**
  Para habilitar http usamos: `sudo ufw allow http`
  Para habilitar https usamos: `sudo ufw allow https`



- **Conexión únicamente por parte de VM2 al servidor ftp.**

```
sudo ufw allow from 192.168.2.102 to any port 20
sudo ufw allow from 192.168.2.102 to any port 21
```



- **Configurar VM1 para que sólo se pueda conectar localmente a mysql.**
  `sudo ufw allow from 192.168.2.101 to any port 3306`