

## REQUERIMIENTOS DE LABORATORIO

- 1) Windows 10, 90 días de prueba -> <https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise>
- 2) Ubuntu or Kali Linux, recomendamos Kali pero cualquier distro de linux debería funcionar-> Ubuntu <http://old-releases.ubuntu.com/releases/18.04.2/>  
Kali Linux -> <https://www.kali.org/downloads/>
- 3) Virtual Box -> <https://www.virtualbox.org/wiki/Downloads>
- 4) Inetsim software -> <https://www.inetsim.org/downloads.html>.
- 5) Inetsim instrucciones -> <https://www.inetsim.org/packages.html>.
- 6) Microsoft Visual studio con C# y C++.

Nota: Recomendamos instalar solo la partición C: en tu Windows 10 virtual machine.

## GUIA PARA INSTALAR INETSIM

Esta guía es solo un apoyo, tienes todo este material en video en la sección Configurando el Laboratorio.

**Instalando Inetsim en Linux virtual machine.-** Escribe estas instrucciones una por una en la consola de Linux:

- 1) `echo "deb http://www.inetsim.org/debian/ binary/" > /etc/apt/sources.list.d/inetsim.list`
- 2) `echo "deb-src http://www.inetsim.org/debian/ source/" >> /etc/apt/sources.list.d/inetsim.list`
- 3) `wget -O - https://www.inetsim.org/inetsim-archive-signing-key.asc | apt-key add -`
- 4) `apt update`
- 5) `apt install inetsim`
- 6) `sudo gedit /etc/network/interfaces`
- 7) Ahora que está abierto el editor escribe esto al final del mismo:

**auto eth0 -> esto es el nombre de tu interface**

**iface eth0 inet static**

**address 10.0.5.4 -> esto es la dirección ip de tu Linux virtual machine**

**netmask 255.255.255.0**

Ahora debería lucir así

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 10.0.5.4
netmask 255.255.255.0
```

Nota: Usa el comando “ifconfig” en la consola de Linux para averiguar el nombre de tu interface y tu dirección ip (si no sabes como, mira el video “Configurando Inetsim en Kali Linux virtual machine”)

- 8) Ahora escribe esto en la consola de Linux: `sudo gedit /etc/inetsim/inetsim.conf`
- 9) Busca esta línea en el editor que se ha abierto: `#service_bind_address 10.10.10.1`
- 10) Debajo de esta línea añade el mismo comando sin el # y tu dirección ip como se muestra en la figura de abajo:

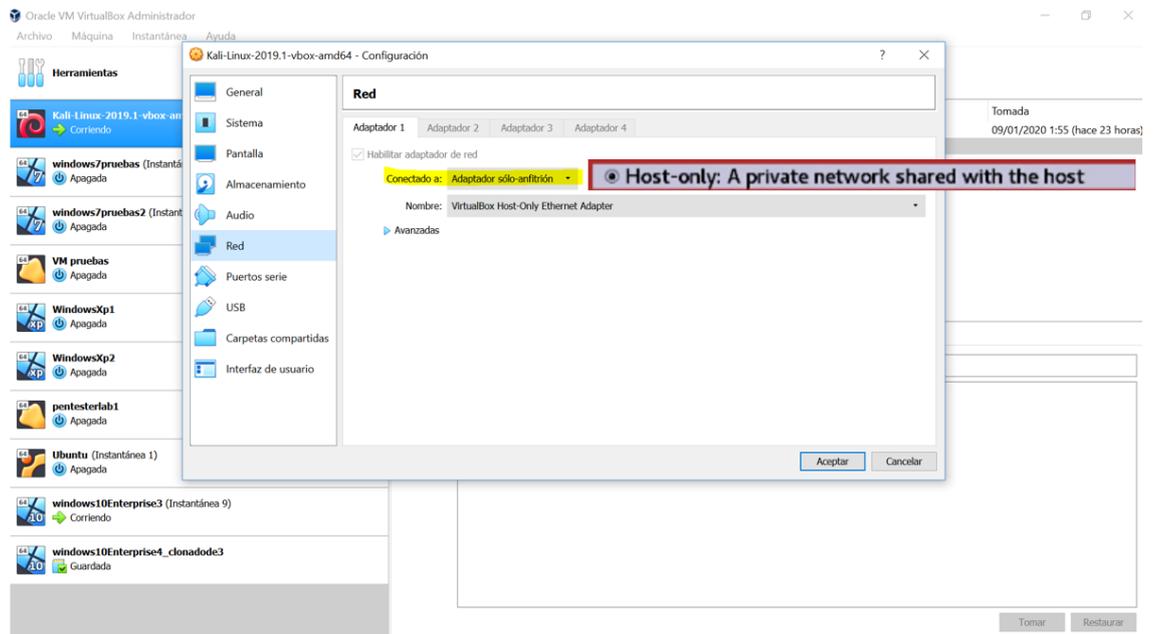
```
#####  
# service_bind_address  
#  
# IP address to bind services to  
#  
# Syntax: service_bind_address <IP address>  
#  
# Default: 127.0.0.1  
#  
#service_bind_address 10.10.10.1  
service_bind_address 10.0.5.4  
#####
```

- 11) Ahora busca esta línea: `#dns_default_ip 10.10.10.1`. Repetimos el procedimiento de arriba, debe quedar así:

```
#####  
# dns_default_ip  
#  
# Default IP address to return with DNS replies  
#  
# Syntax: dns_default_ip <IP address>  
#  
# Default: 127.0.0.1  
#  
#dns_default_ip 10.10.10.1  
dns_default_ip 10.0.5.4  
#####
```

Eso es todo, escribe “inetsim” en la consola de Linux y la simulación empezará a ejecutarse. A continuación se debe configurar Virtual Box:

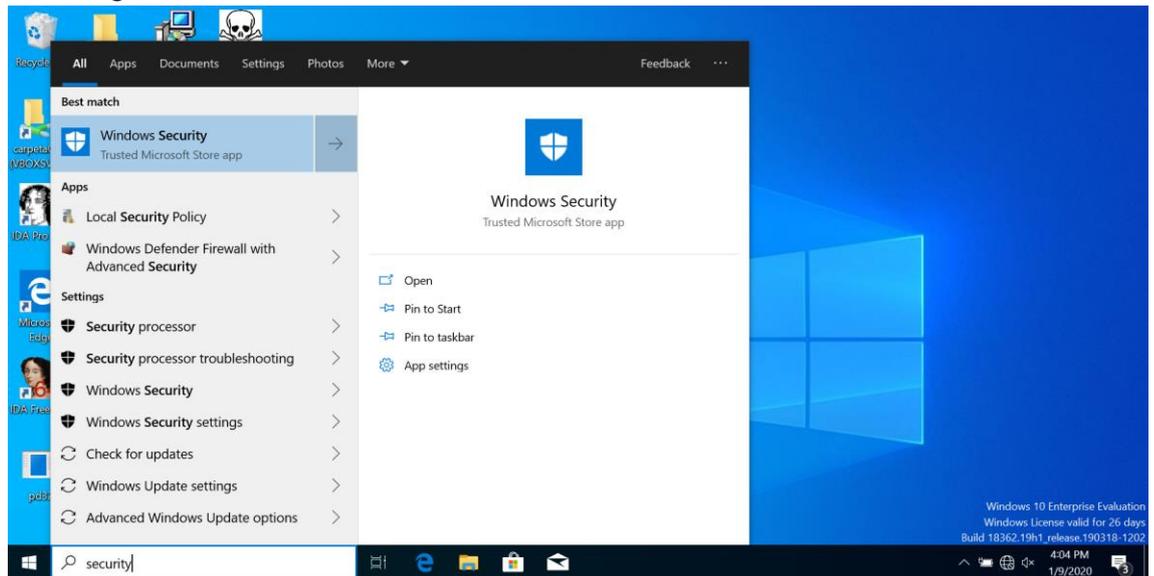
**Configurando Virtual Box.-** Debes configurar la opción de Red de Linux virtual machine y de Windows virtual machine. Las opciones pueden variar un poco de acuerdo a la versión pero debes poner: “Adaptador solo anfitrión” o “Host only adapter”



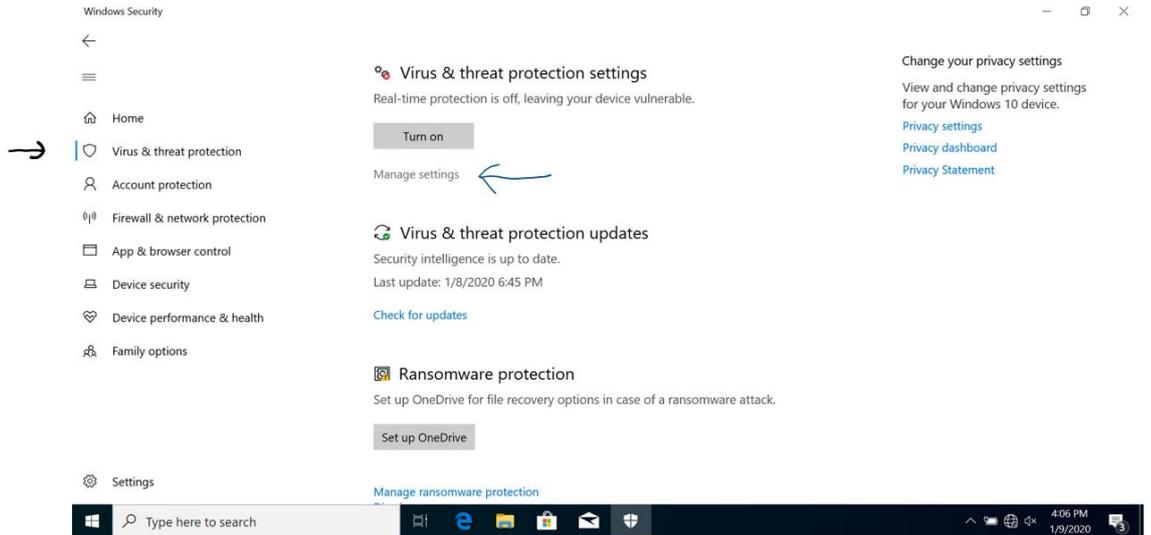
## Desactivar características de seguridad de Windows 10 virtual machine

Es importante desactivarlas porque de lo contrario podrían detectar nuestras muestras de malware e incluso eliminarlas.

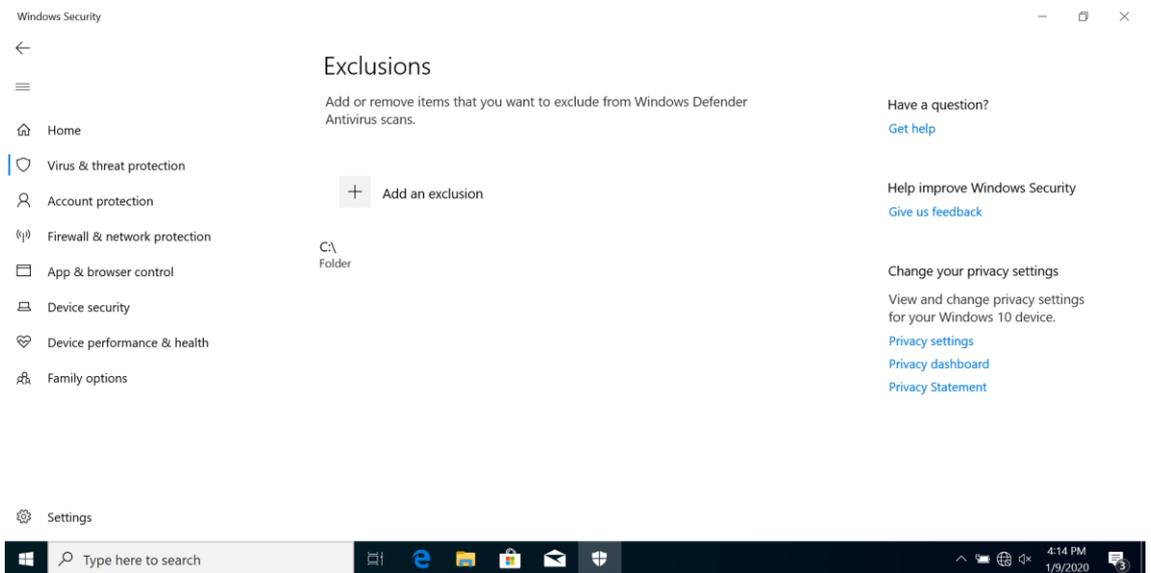
### 1) Busca seguridad de Windows



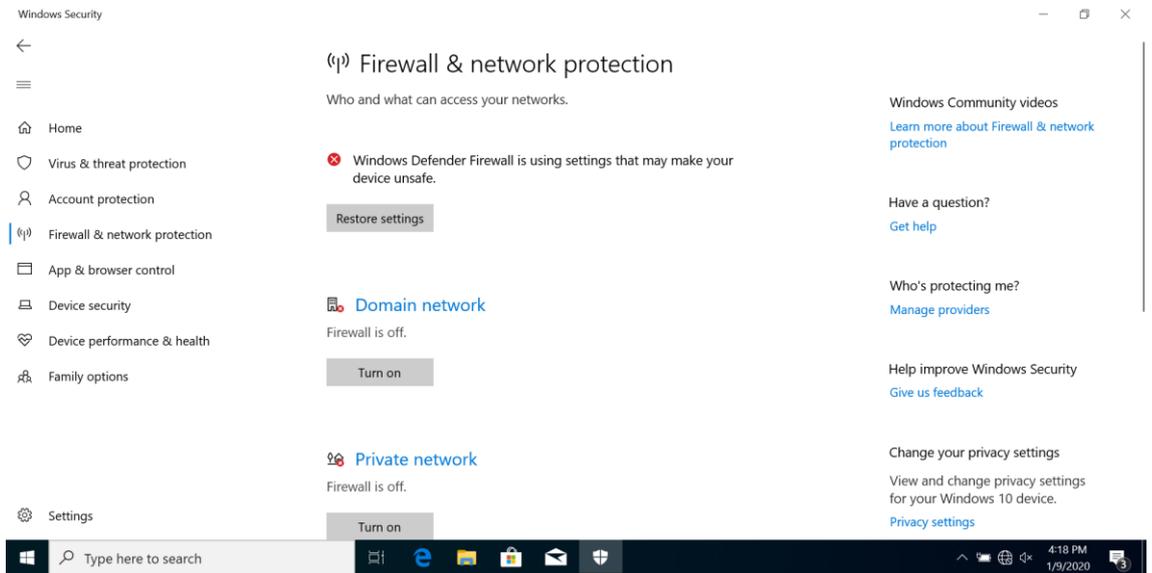
### 2) Busca protección contra virus y amenazas.



- 3) Desactiva toda la protección de virus y amenazas.
- 4) **Aquí un truco.** Aunque desactives la protección en tiempo real, Windows volverá a activarla cuando menos lo esperes, haz esto: Busca exclusiones y añade el drive C: esto ayudará a que Windows Defender ignore este directorio.



- 5) Desactiva todas las protecciones de firewall.



Eso es todo, recuerda que tienes todo esto en video en la sección Configurando el Laboratorio.