Adding A Simple Web Server (WebGOAT)

Introduction of WebGOAT:

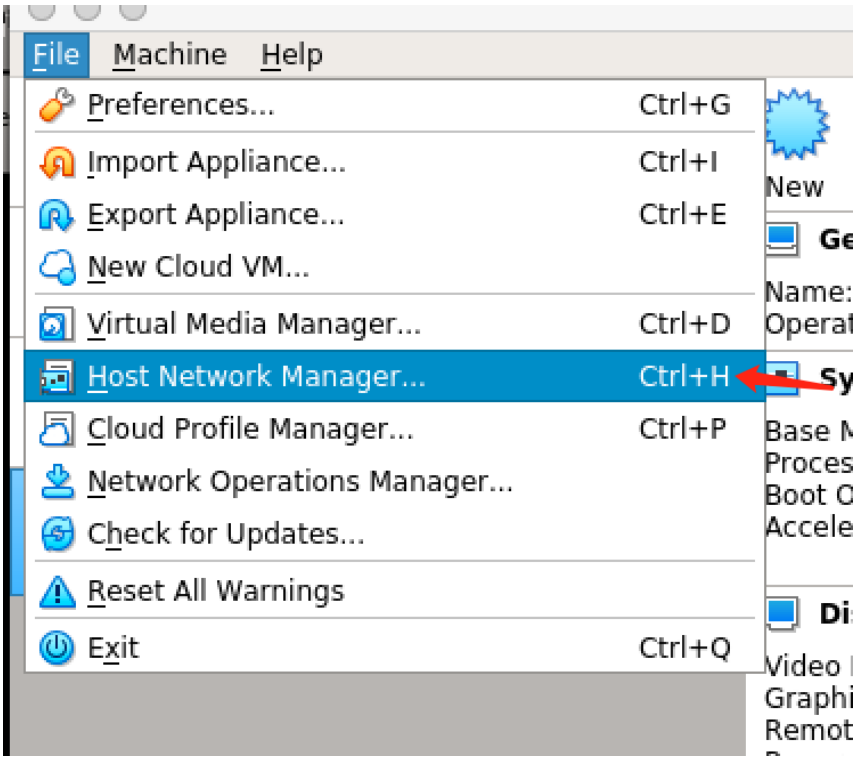
https://owasp.org/www-project-webgoat/#:~:text=WebGoat%20is%20a%20deliberately%20insecure,and%20popular%20open%20source%20components

Part 1: Download and Install the VM

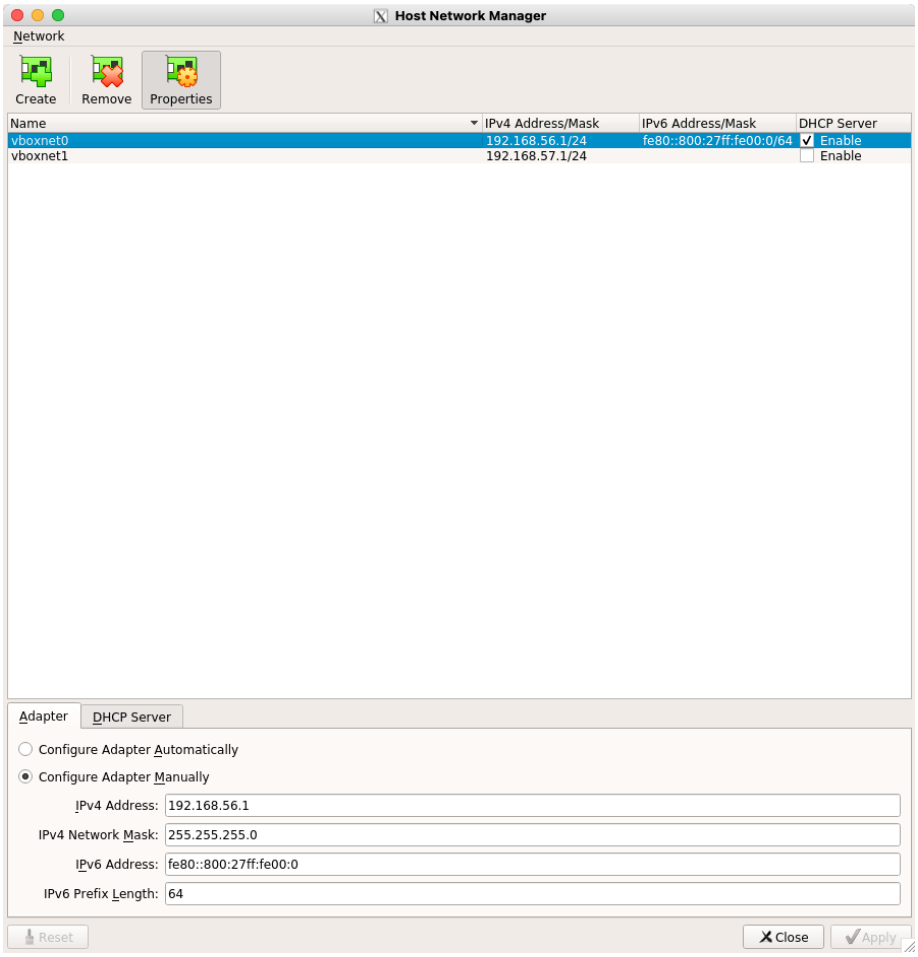
1. Download a pre-configured VirtualBox VM image for WebGOAT, which is available at https://download.vulnhub.com/webgoat/WebGOAT.ova

2. Import and configure the VM:

    1. Open “Host Network Manager”

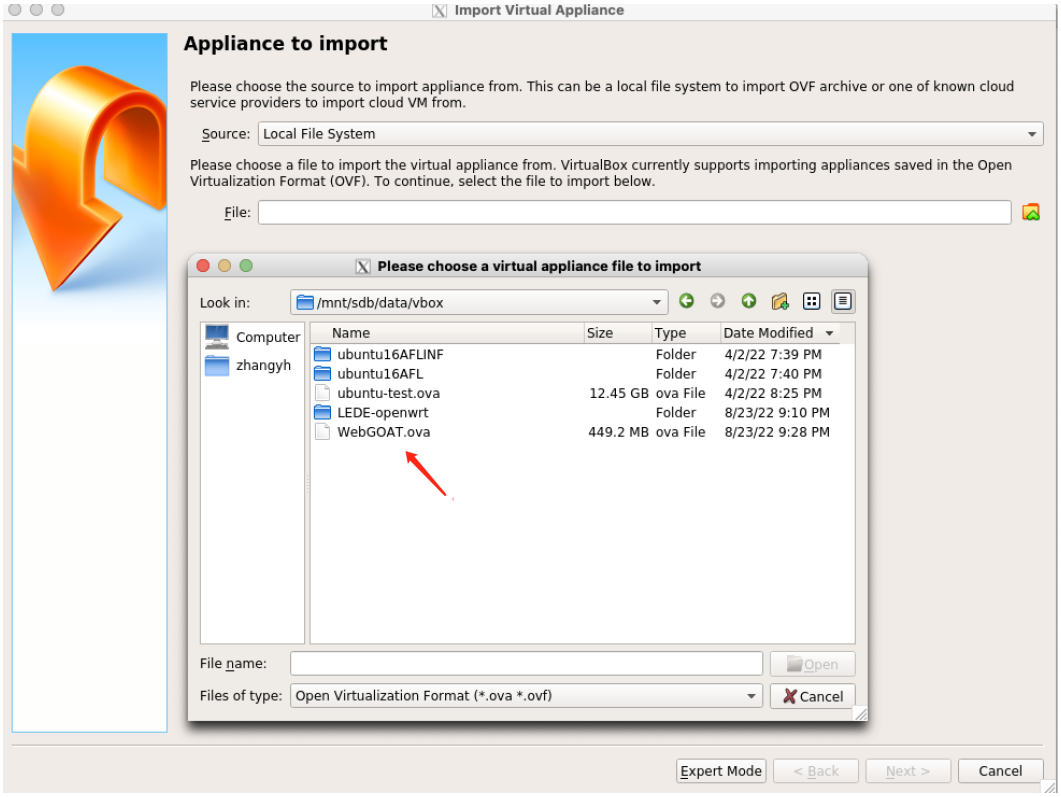


2. Create a new virtual network interface.

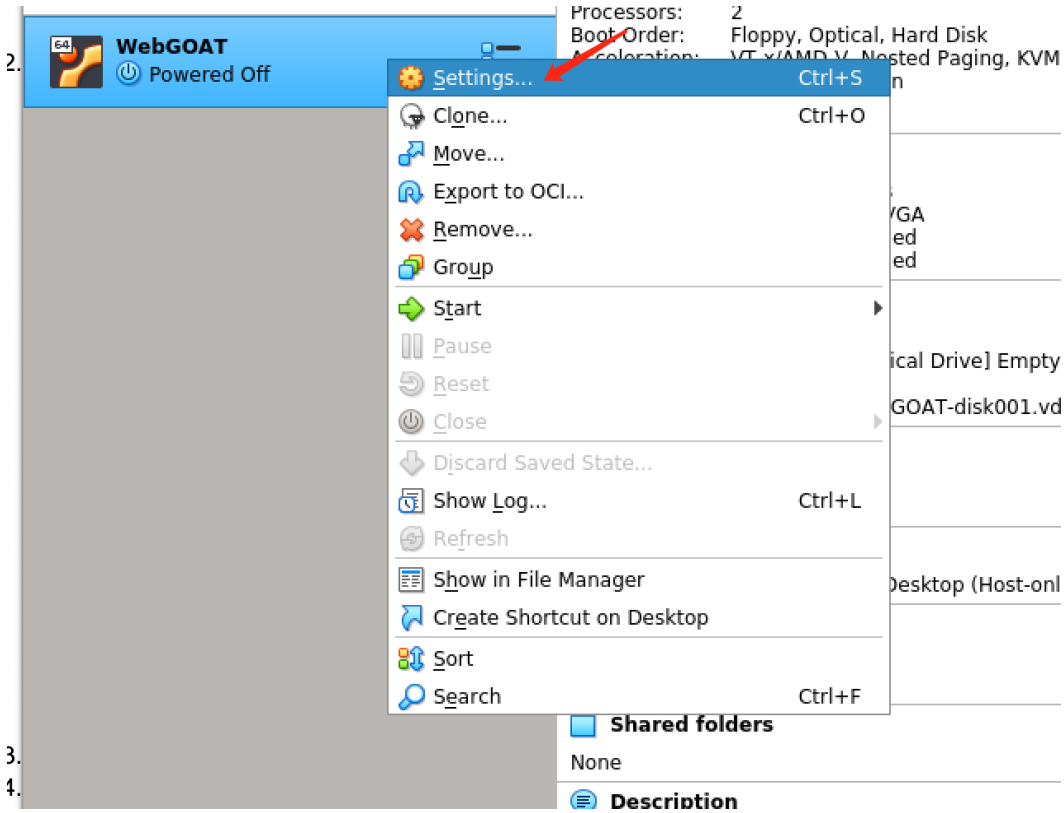


3. Click “Import”

4. Select the WebGOAT.ova and finish the importing process



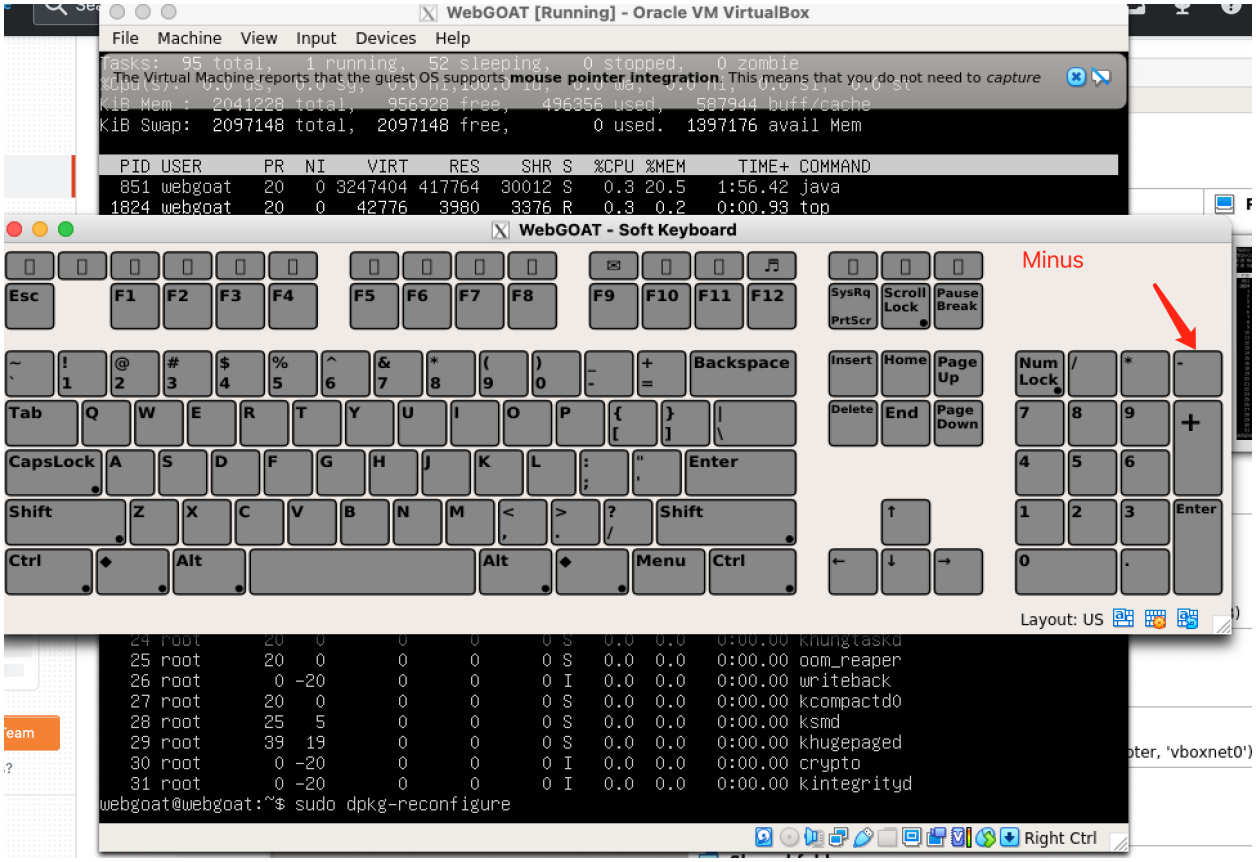
5. Goto settings



6. Change the network adapter to Host-only mode.

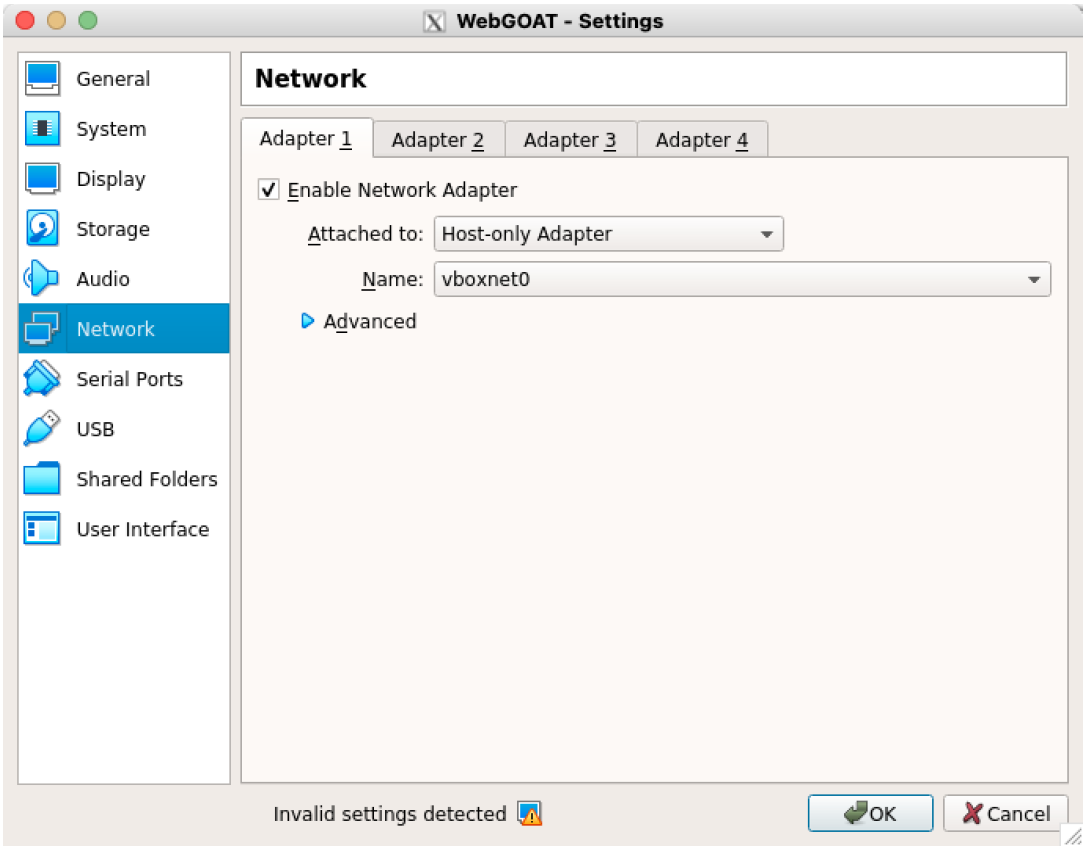
7. Start the VM and log into the machine (both the username and password are both “webgoat”)

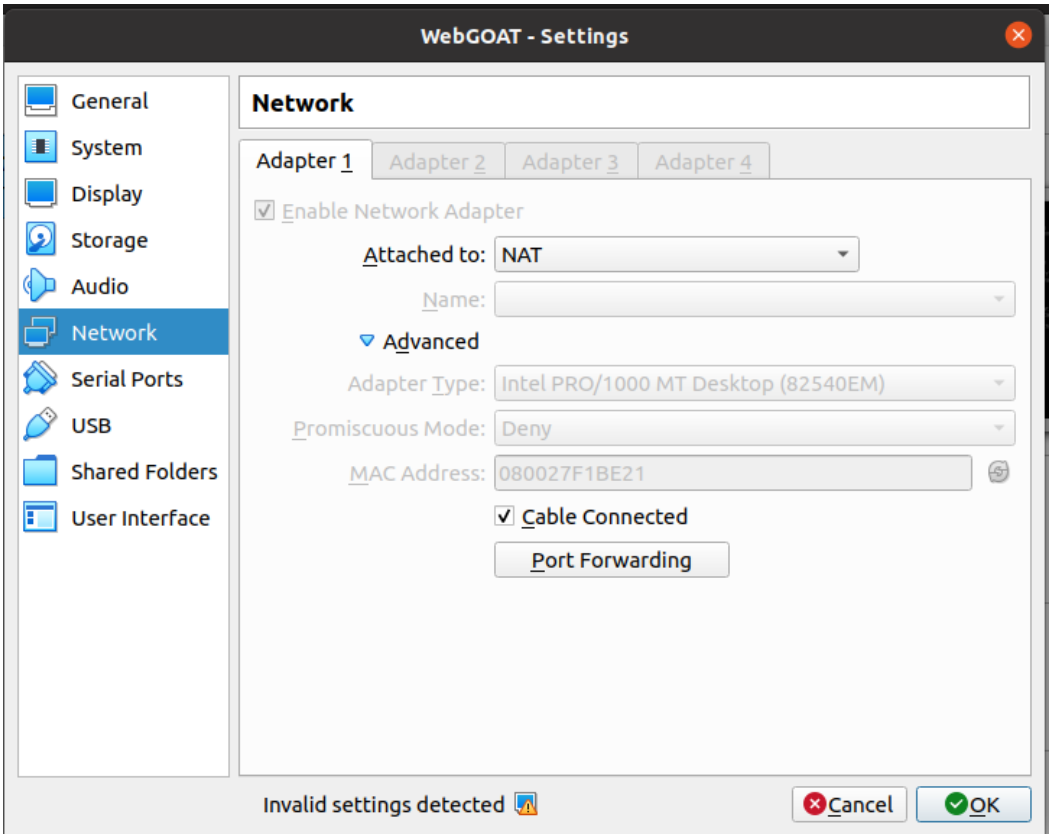
NOTE: You may need to run “`sudo dpkg-reconfigure keyboard-configuration`” to re-configure the keyboard layout with a soft keyboard, and reboot to apply changes.



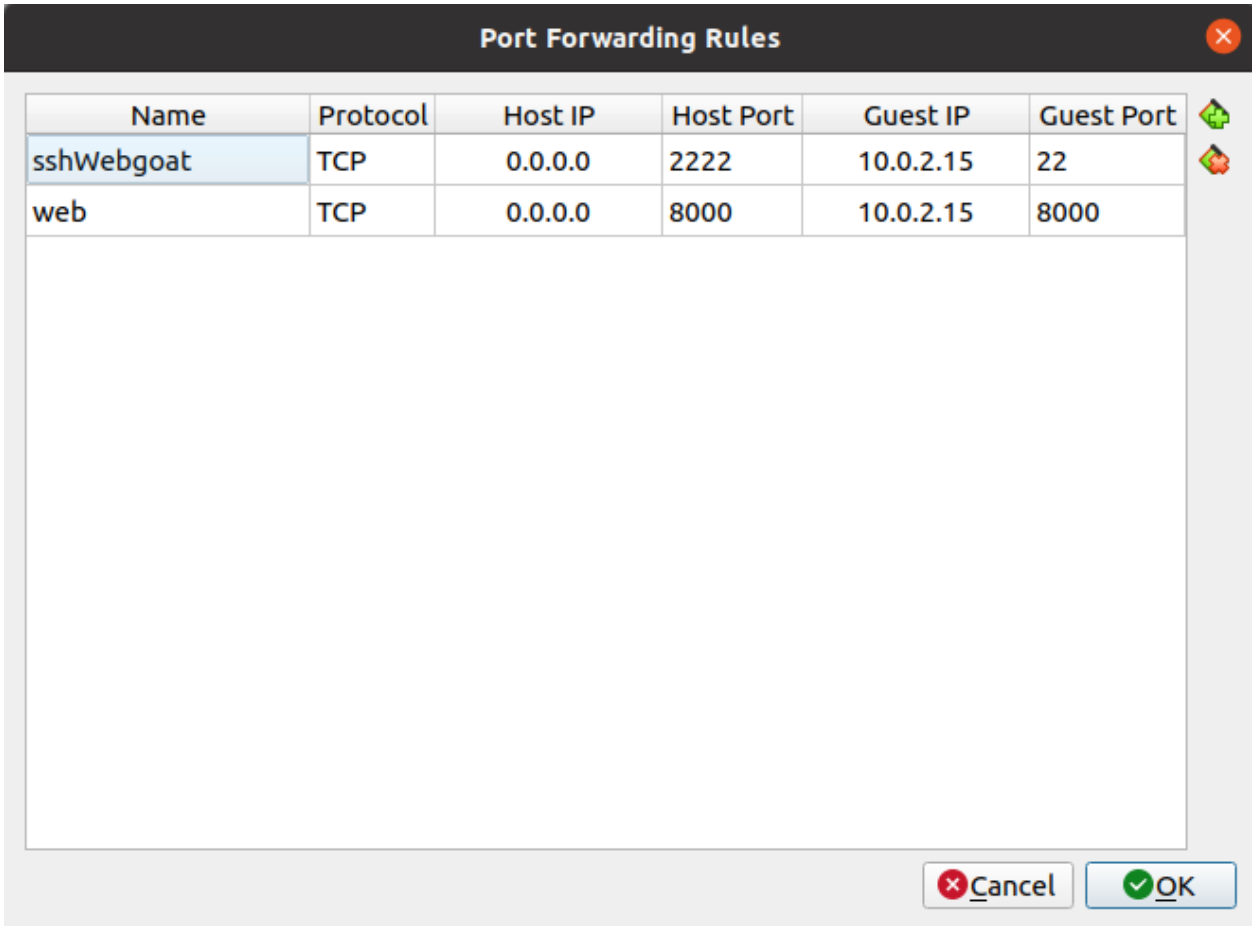
8. Find out the IP address of the VM by running “ifconfig” and look for an IP address similar to “10.0.2.15” (should be this one in most cases)

9. Set port forwarding rules so that you can access the VM from anywhere you can access the host machine. However: “Settings” → “Network” → “Advanced” → “Port Forwarding”


WebGOAT - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Host-only Adapter
Name:
vboxnet0
Advanced
Invalid settings detected
OK
Cancel



10. Setting up port forwarding rules as follows (please replace “10.0.2.15” with the IP address of your VM)



11. **Check the IP address of your host machine. In our case, the IP is** 192.168.56.104. Then you can access the webserver inside your VM with the following URL from anywhere you can access your host machine (e.g., your host machine itself):

    http://192.168.56.104:8000/WebGoat

Add firewall rules by iptables:

and no more traffic from SRC will pass through.

View firewall rules:

sudo iptables -L -v

Show rules with line numbers:

sudo iptables -L --line-numbers

Delete the rule :

sudo iptables -D INPUT 1