htl donaustadt
Donaustadtstraße 45
1220 Wien

Abteilung: Informationstechnologie
Schwerpunkt: Netzwerktechnik

Ethical hacking of a CTF-VM

Laboratory protocol Exercise 7: Ethical hacking of a CTF-VM

Figure 1: Grouplogo

Subject: ITSI
Class: 3AHITN
Name: Stefan Fürst, Justin Tremurici
Groupname/number Name here/12
Supervisor: SPAC, ZIVK
Exercise dates:
Submission date:

htl donaustadt
Donaustadtstraße 45
1220 Wien

Abteilung: Informationstechnologie
Schwerpunkt: Netzwerktechnik

Contents

1 Task definition

2 Summary

3 Complete network topology of the exercise

4 Exercise Execution

4.1 Setting up the virtual machines.

To get started with this CTF, make sure that VirtualBox version 7.1.4 is used. The VM to attack must be imported by double-clicking the provided `.ova` file. After the import is complete, the network settings must be changed to use Host-only Adapter mode. Since using the default Host-only network did not work, we had to create a new Host-only network. To do this, either press `<C-h>` or click on `File` > `Tools` > `Network Manager`, as shown in Figure 2.

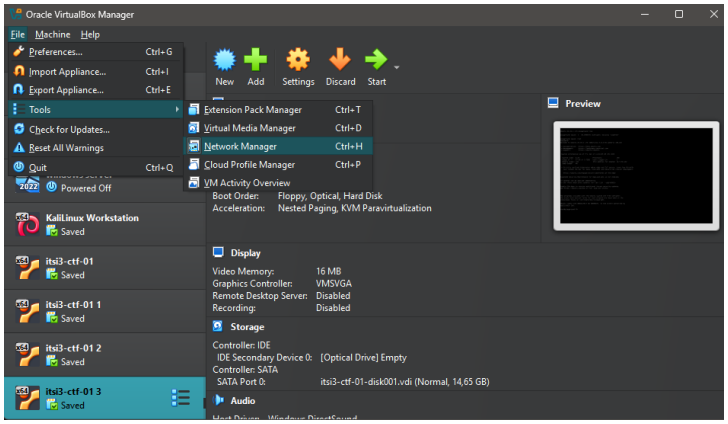


Figure 2: Opening VirtualBox Network Manager settings

In this menu, click on `Create`, then check the `Enable Server` box to enable the DHCP server so the target VM will receive an IP address. Then, click on `Adapter` to view the IP range of the network, which in our case is `192.168.15.0/24`, which can be seen in Figure 3.

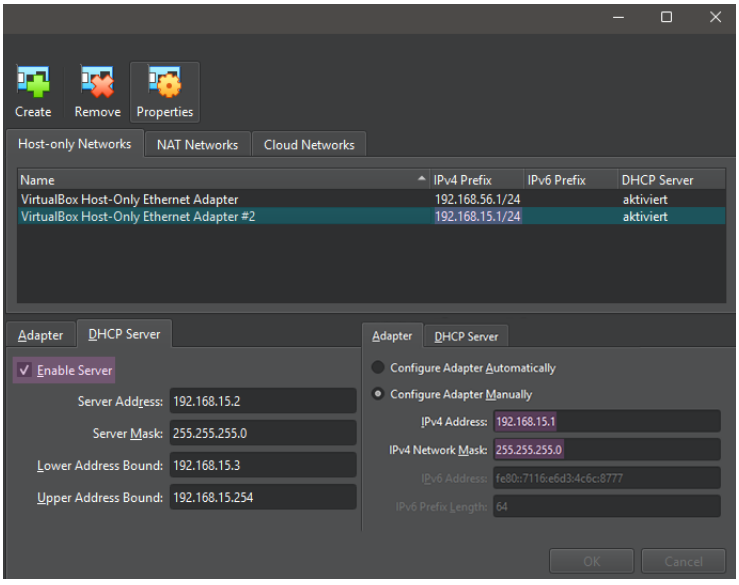


Figure 3: Showing the IP settings for the new Host-only network

Next, open the virtual machine settings by selecting the VM in the list and pressing `<C-s>`. Under the `Network` section, change the network adapter to use the Host-only Adapter and select the VirtualBox Host-only Ethernet Adapter #2, which was just created. Perform this step for both the target VM and the Kali VM, as detailed in Figure 4.

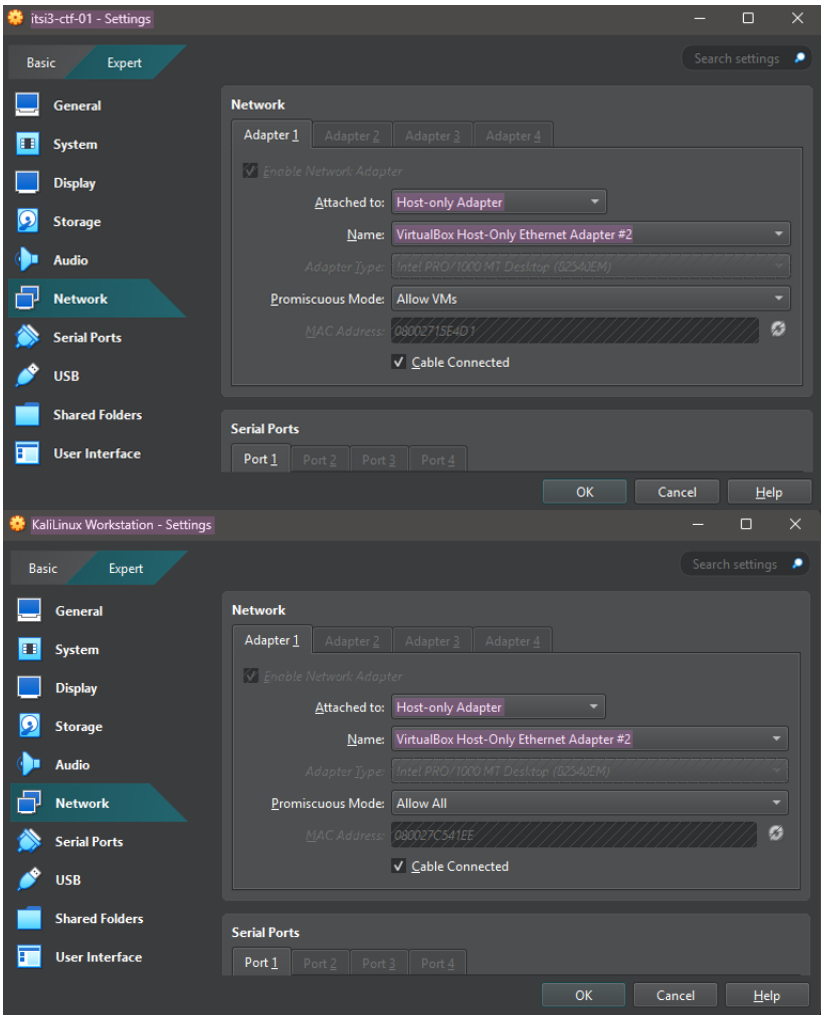


Figure 4: Showing the network configuration of the virtual machines

4.2 Reconnaissance: Scanning the Network

Any attack starts with reconnaissance, which in this case means scanning the network with `nmap`. Since we don't know the IP address of the target server yet, we need to scan the network to find it. For this, the command `nmap 192.168.15.0/24` is used to scan the entire network for open ports, as illustrated in Figure 5.

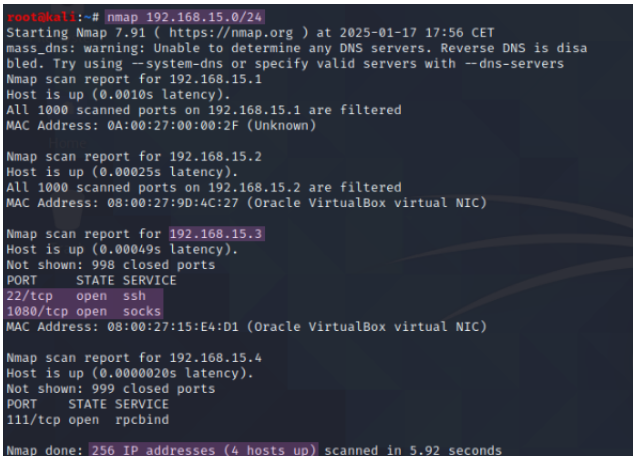
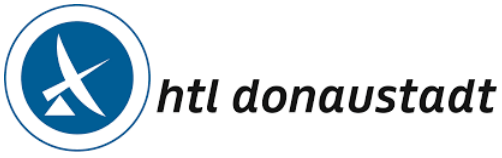


Figure 5: Results of the nmap scan

We can detirme that the target has the ip address `192.168.15.3` since as seen in Figure 3



5 References

References

6 List of figures

List of Figures