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 mascheines

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.

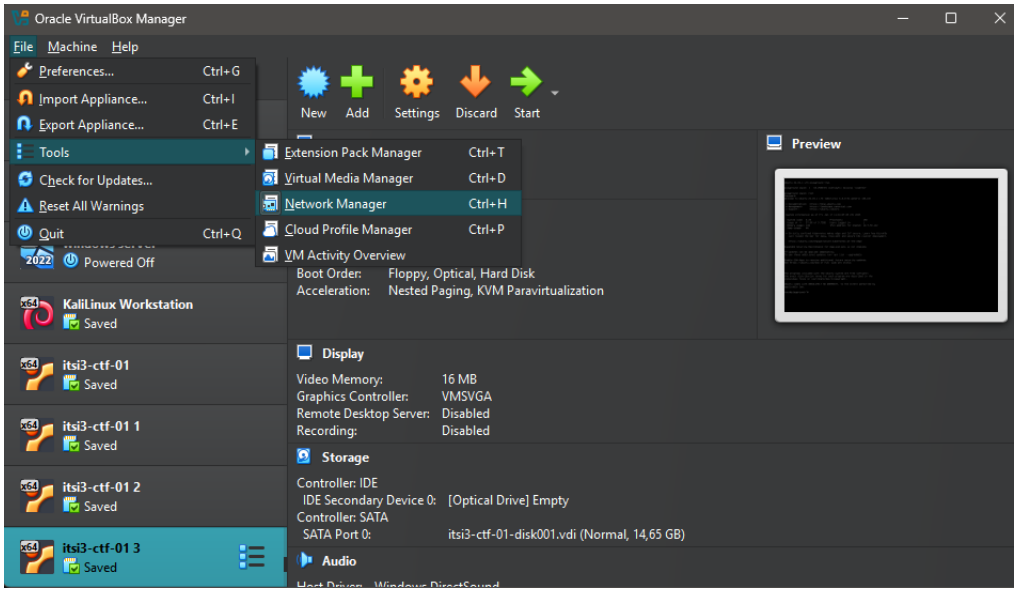

Figure 2: Opening VirtualBox Network Manager settings

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`.

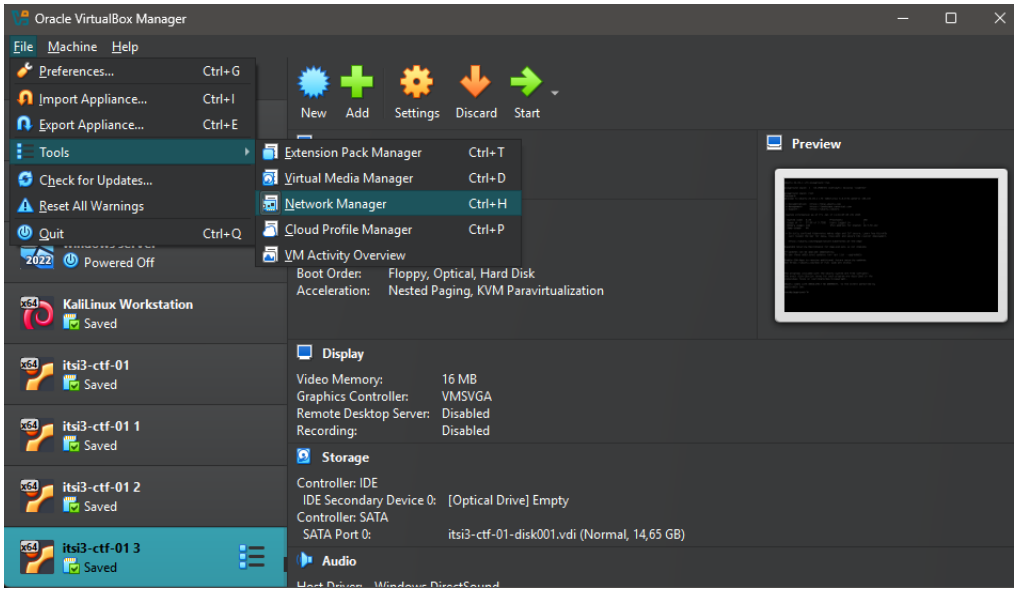

Figure 3: Opening VirtualBox Network Manager settings

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.

4.2 scanning the network

4.3 exploring the websites

4.4 breaking the http authtication

4.5 sshing into the server

4.6 exploring the system

4.7 procces flag

4.8 comment flag

4.9 sudo flag

4.10 history flag

4.11 tmp flag

4.12 it's over but actually not

4.13 trying to escalate privaledgs

4.13.1 smart enumeration

4.13.2 trying a kernel level exploit

4.13.3 checking suid binarys

4.13.4 checking root proccses

4.13.5 trying metasploit

4.13.6 trying other common ctf priv escalation ways

4.14 reseting the root password and exploring the vm

4.15 7 flags

4.16 talking abt the setup etc or sum idk :shruge:

5 References

References

6 List of figures

List of Figures