

## 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:

## Contents

<b>1 Task definition</b>	<b>3</b>
<b>2 Summary</b>	<b>3</b>
<b>3 Complete network topology of the exercise</b>	<b>4</b>
<b>4 Exercise Execution</b>	<b>5</b>
4.1 Setting up the virtual machines. . . . .	5
4.2 Reconnaissance: Scanning the Network . . . . .	7
4.3 exploring the websites . . . . .	8
4.4 breaking the http authentication . . . . .	8
4.5 sshing into the server . . . . .	8
4.6 exploring the system . . . . .	8
4.7 procces flag . . . . .	8
4.8 comment flag . . . . .	8
4.9 sudo flag . . . . .	8
4.10 history flag . . . . .	8
4.11 tmp flag . . . . .	8
4.12 it's over but actually not . . . . .	8
4.13 trying to escalate privaledds . . . . .	8
4.13.1 smart enumeration . . . . .	8
4.13.2 trying a kernel level exploit . . . . .	8
4.13.3 checking suid binarys . . . . .	8
4.13.4 checking root proccses . . . . .	8
4.13.5 trying metasploit . . . . .	8
4.13.6 trying other common ctf priv escalation ways . . . . .	8
4.14 reseting the root password and exploring the vm . . . . .	8
4.15 7 flags . . . . .	8
4.16 talking abt the setup etc or sum idk :shrug: . . . . .	8
<b>5 References</b>	<b>9</b>
<b>6 List of figures</b>	<b>10</b>

## **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.

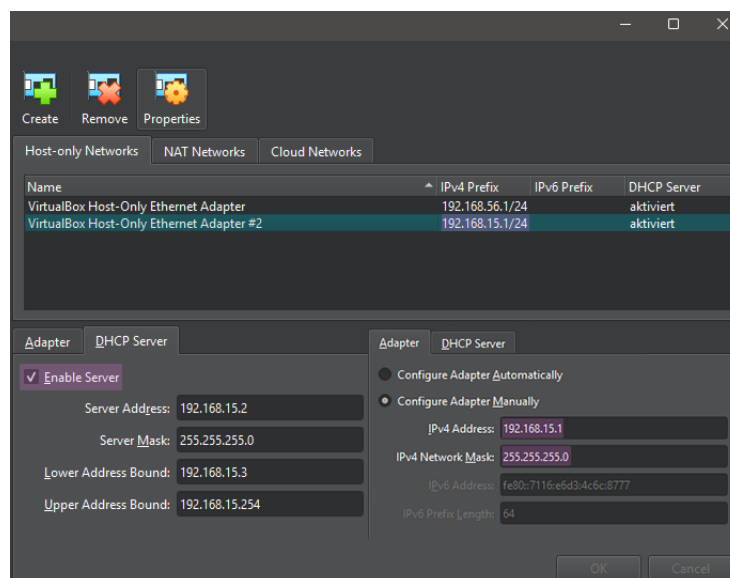


Figure 3: Showing the IP settings for the new Host-only network

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.

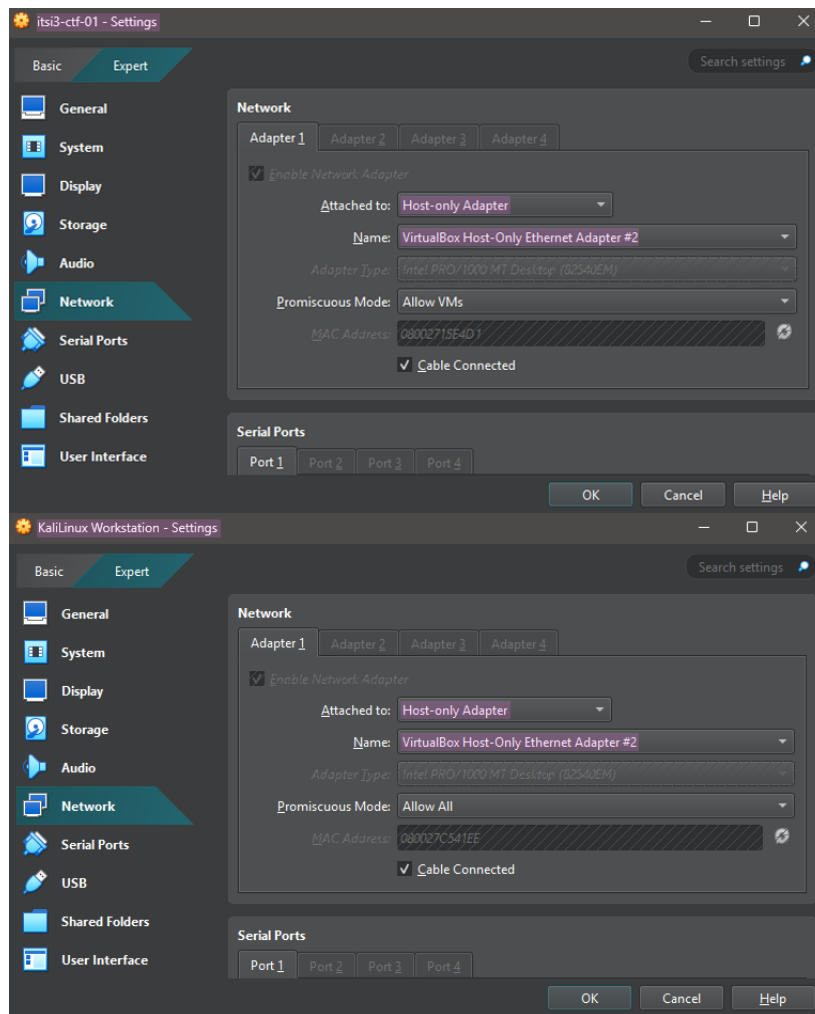


Figure 4: Showing the network configuration of the virtual machines

## 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.

```
root@kali:~# nmap 192.168.15.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2025-01-17 17:56 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.15.1
Host is up (0.0010s latency).
All 1000 scanned ports on 192.168.15.1 are filtered
MAC Address: 0A:00:27:00:00:2F (Unknown)

Nmap scan report for 192.168.15.2
Host is up (0.00025s latency).
All 1000 scanned ports on 192.168.15.2 are filtered
MAC Address: 08:00:27:9D:4C:27 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.15.3
Host is up (0.00049s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
1080/tcp   open  socks
MAC Address: 08:00:27:15:E4:D1 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.15.4
Host is up (0.0000020s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
111/tcp    open  rpcbind

Nmap done: 256 IP addresses (4 hosts up) scanned in 5.92 seconds
```

Figure 5: Results of the nmap scan

We can determine that the target has the IP address 192.168.15.3 since as seen in Figure 3

- 4.3 exploring the websites
- 4.4 breaking the http authentication
- 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

1	Grouplogo . . . . .	1
2	Opening VirtualBox Network Manager settings . . . . .	5
3	Showing the IP settings for the new Host-only network . . . . .	5
4	Showing the network configuration of the virtual machines . . . . .	6
5	Results of the nmap scan . . . . .	7