

## 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 mascheines . . . . .	5
4.2 scanning the network . . . . .	6
4.3 exploring the websites . . . . .	6
4.4 breaking the http authtication . . . . .	6
4.5 sshing into the server . . . . .	6
4.6 exploring the system . . . . .	6
4.7 procces flag . . . . .	6
4.8 comment flag . . . . .	6
4.9 sudo flag . . . . .	6
4.10 history flag . . . . .	6
4.11 tmp flag . . . . .	6
4.12 it's over but actually not . . . . .	6
4.13 trying to escalate privaledgs . . . . .	6
4.13.1 smart enumeration . . . . .	6
4.13.2 trying a kernel level exploit . . . . .	6
4.13.3 checking suid binarys . . . . .	6
4.13.4 checking root proccses . . . . .	6
4.13.5 trying metasploit . . . . .	6
4.13.6 trying other common ctf priv escalation ways . . . . .	6
4.14 reseting the root password and exploring the vm . . . . .	6
4.15 7 flags . . . . .	6
4.16 talking abt the setup etc or sum idk :shruge: . . . . .	6
<b>5 References</b>	<b>7</b>
<b>6 List of figures</b>	<b>8</b>

## **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, which can be seen in Figure 3.

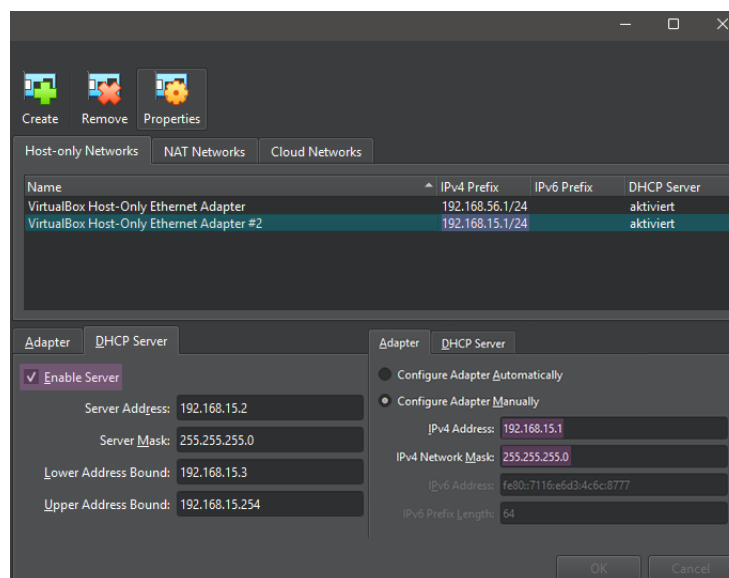


Figure 3: Showing the IP settings for the new Host-only network

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.

- 4.2 scanning the network
- 4.3 exploring the websites
- 4.4 breaking the http authentication
- 4.5 sshing into the server
- 4.6 exploring the system
- 4.7 process 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 privileges
  - 4.13.1 smart enumeration
  - 4.13.2 trying a kernel level exploit
  - 4.13.3 checking suid binaries
  - 4.13.4 checking root processes
  - 4.13.5 trying metasploit
  - 4.13.6 trying other common ctf privilege escalation ways
- 4.14 resetting the root password and exploring the vm
- 4.15 7 flags
- 4.16 talking about the setup etc or sum idk :shrug:

## 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