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: 17-19.1.2025
Submission date: 20.1.2025

htl donaustadt
Donaustadtstraße 45
1220 Wien

Abteilung: Informationstechnologie
Schwerpunkt: Netzwerktechnik

Contents

1 Task definition

2 Summary

3 Complete network topology of the exercise

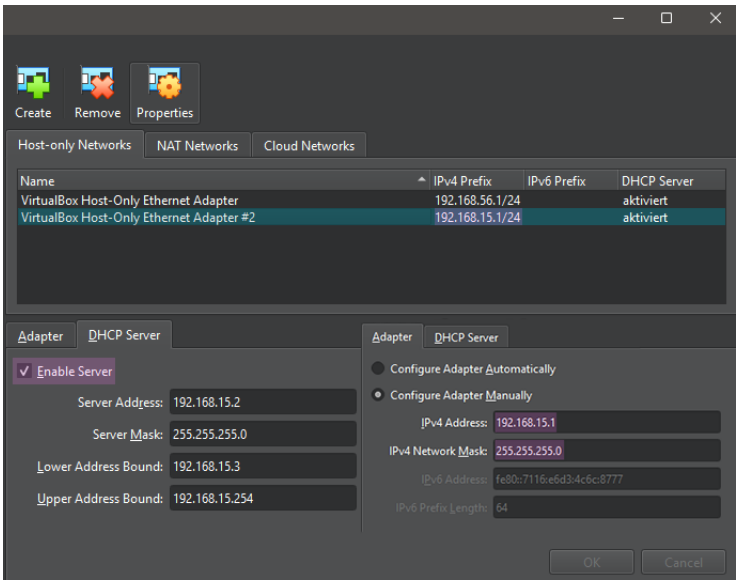


Figure 2: Complete network topology of the exercise

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 3.

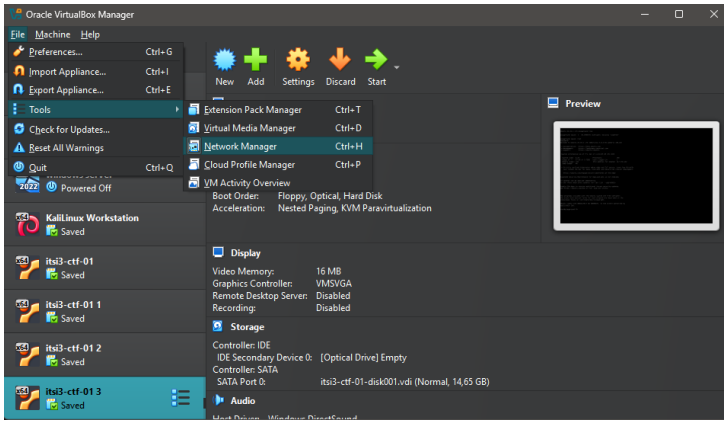


Figure 3: Opening VirtualBox Network Manager settings

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 4.

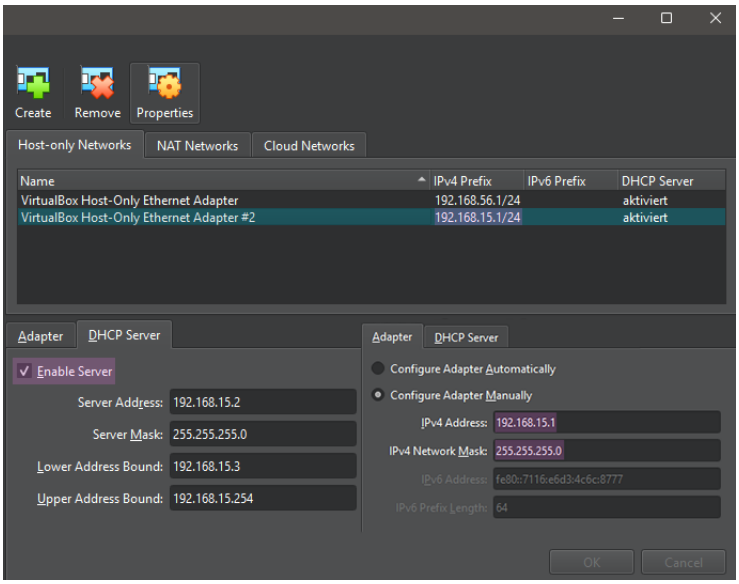


Figure 4: Showing the IP settings for the new Host-only network

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 5.

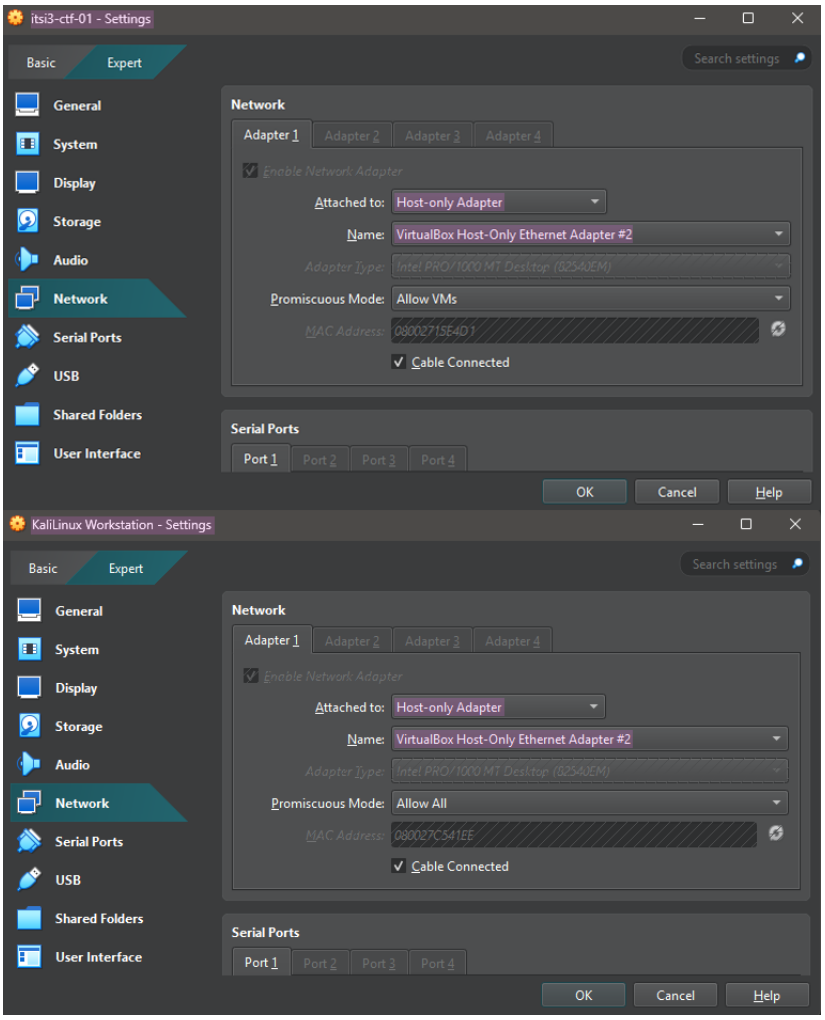


Figure 5: Showing the network configuration of the virtual machines

4.2 Reconnaissance: Scanning the Network

We use the Cyber Kill Chain to structure our steps for completing the CTF, with any attack beginning 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 6.[1]

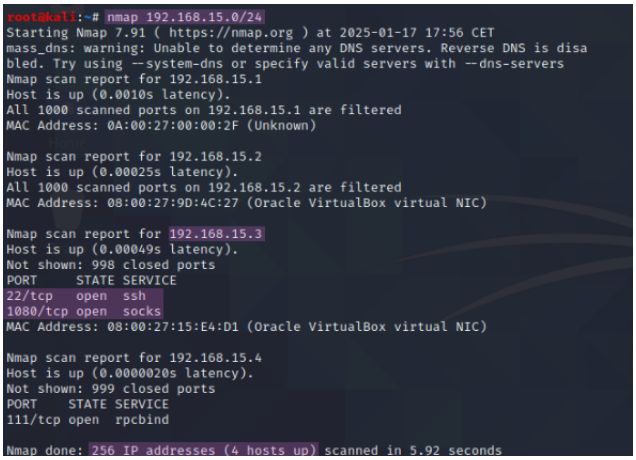


Figure 6: Results of the nmap scan

We can determine that the target has the IP address `192.168.15.3`, since, as seen in Figure 4, `.1` is the network address, `.2` is the `DHCP` server, and `.4` is the IP address of the Kali VM. This can be verified by running `ip a` or by scanning the open ports, since `ssh` is not exposed. Now we can run another `nmap` scan to get fruther information abt the running servives and their version by using the `sV` flag and use the `T4` flag which sets the timing to agressive with the value 4 and the `p` falg with `-` value to scan all ports. The results of the scan can be seen in Figure 7.[2, 3]

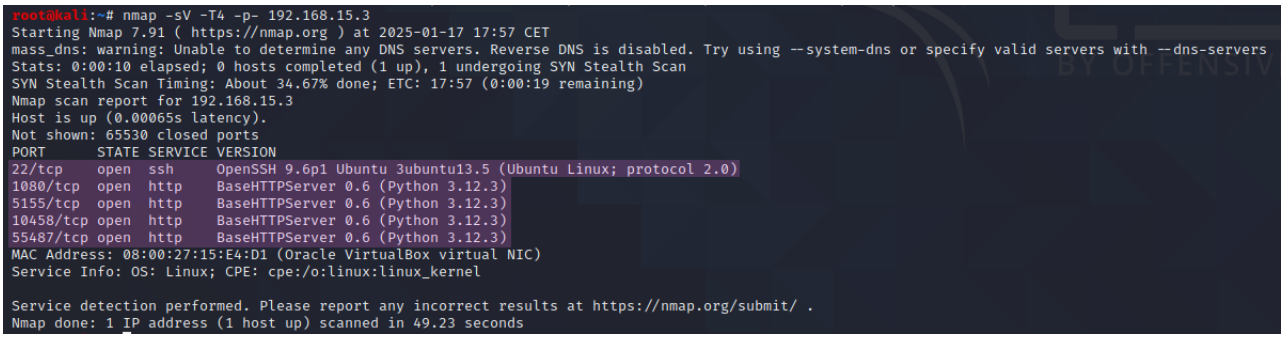


Figure 7: Results of the detailed nmap scan

From this scan, we can see that `ssh` and four `http` servers running `Python 3.12.3` are active on the system.

4.3 Reconnaissance: Exploring the websites

If we open the websites in our web browser of choice, we can see that the one on port `1080` says that to get further, we need to scan deeper, which we already did. The website on port `5155` shows text from foreign languages, which is randomized and always prints out different text on refresh. The site on port `10458` prints out a message in `base64`, and lastly, the one on port `10448` has a basic authentication login prompt for a mini web shell. Figures 8 shows the content of each webpage.

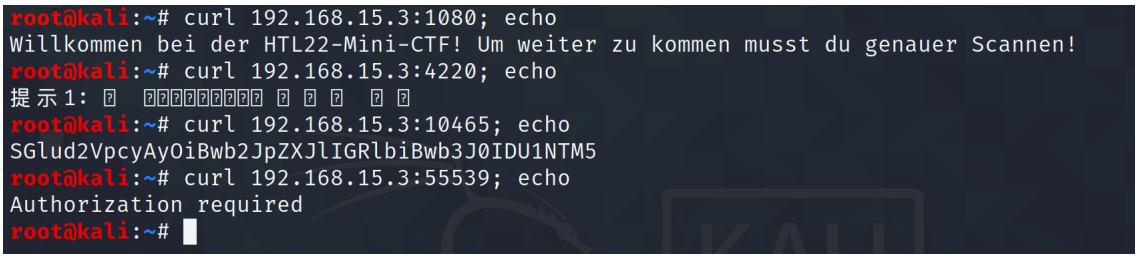


Figure 8: Showing the contents of each page using `curl` [1]

The `base64` message can be decoded by piping the string, using `echo`, into the `base64` command, which gives us the hint to use port `55487`, the site with authentication. This is shown in Figure 9 below.

Figure 9: Decoding the `base64` message

To get all the random variants from the site with the foreign languages, I wrote a quick batch script to recursively relay the website and save the output in a file called `output`, as shown in Figure 10.

```
#!/bin/bash
while true;do
    body=$(curl -s 192.168.15:5155)
    echo "$body" >> output
    echo "$body"
done
```

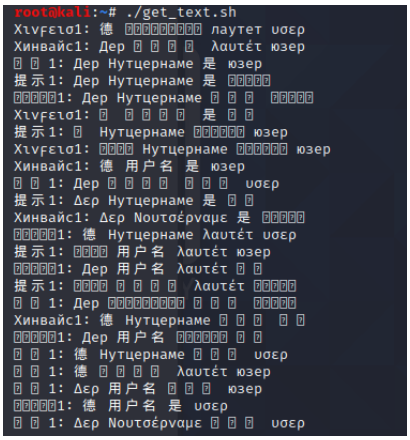


Figure 10: Running the script

After running it for a while, we prompted ChatGPT with the list of outputs to translate, which revealed the following hint, as shown in Figure 11.

[1] The ports are different from those mentioned before, since instead of using screenshots from the browser, we opted to use `curl`. Additionally, on every refresh, the ports are randomized.

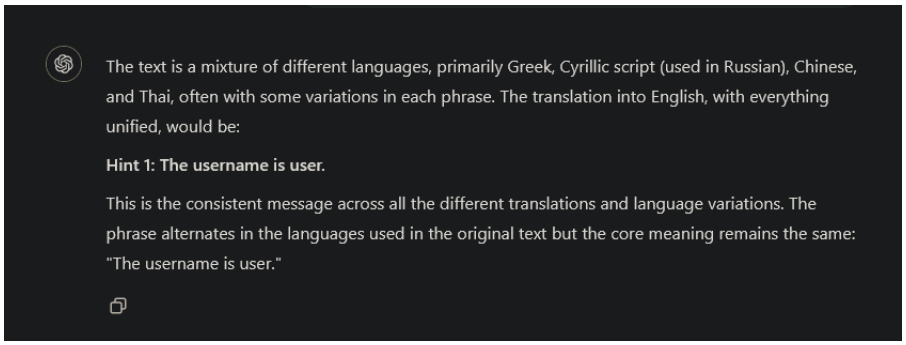


Figure 11: ChatGPT translating the hint

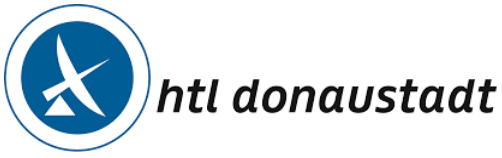
4.4 Weaponization: Evaluating the needed tools

Now that we know the username and that it uses HTTP Basic Authentication, we can use Hydra to brute-force the password. For this, I have chosen the 10-million-password list as our wordlist [4]

4.5 Exploitation: Using Hydra to break HTTP basic authentication

To brute force the password, the following `hydra` command will be used: `hydra -l user -P pw.txt -s 55487 -f 192.168.15.3 http-get /` Here is a breakdown of the options used in the command:

```
-l user
-P pw.txt
-s 55487
-f
192.168.15.3
http-get /
```



5 References

References

[1] “Cyber Kill Chain®,” Jan. 2025, [Online; accessed 19. Jan. 2025]. [Online]. Available: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[2] “Service and Version Detection | Nmap Network Scanning,” Jan. 2025, [Online; accessed 19. Jan. 2025]. [Online]. Available: https://nmap.org/book/man-version-detection.html

[3] “Timing Templates (-T) | Nmap Network Scanning,” Jan. 2025, [Online; accessed 19. Jan. 2025]. [Online]. Available: https://nmap.org/book/performance-timing-templates.html

[4] Jan. 2025, [Online; accessed 19. Jan. 2025]. [Online]. Available: https://raw.githubusercontent.com/danielmiessler/SecLists/refs/heads/master/Passwords/Common-Credentials/10-million-password-list-top-10000.txt

6 List of figures

List of Figures