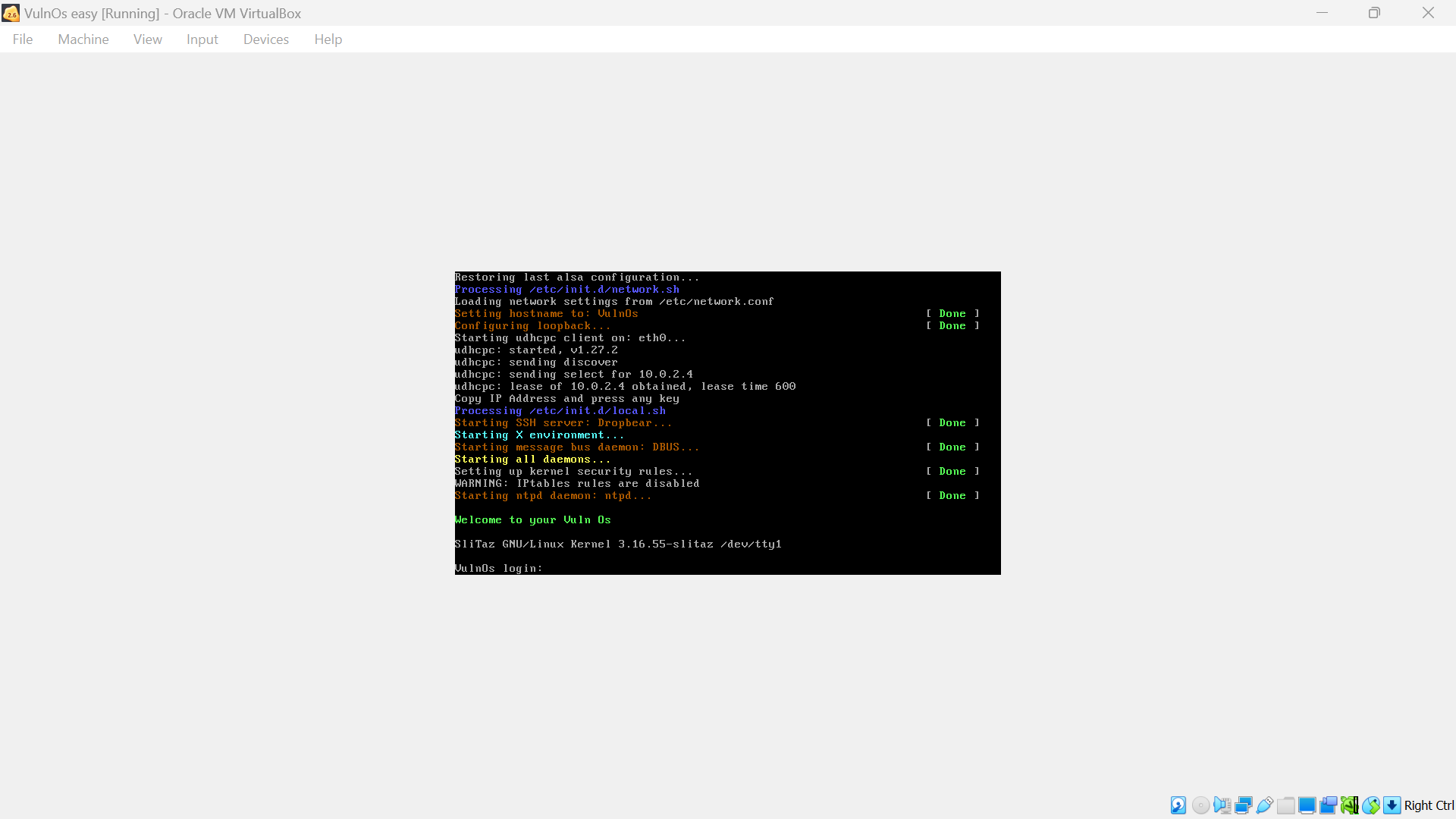
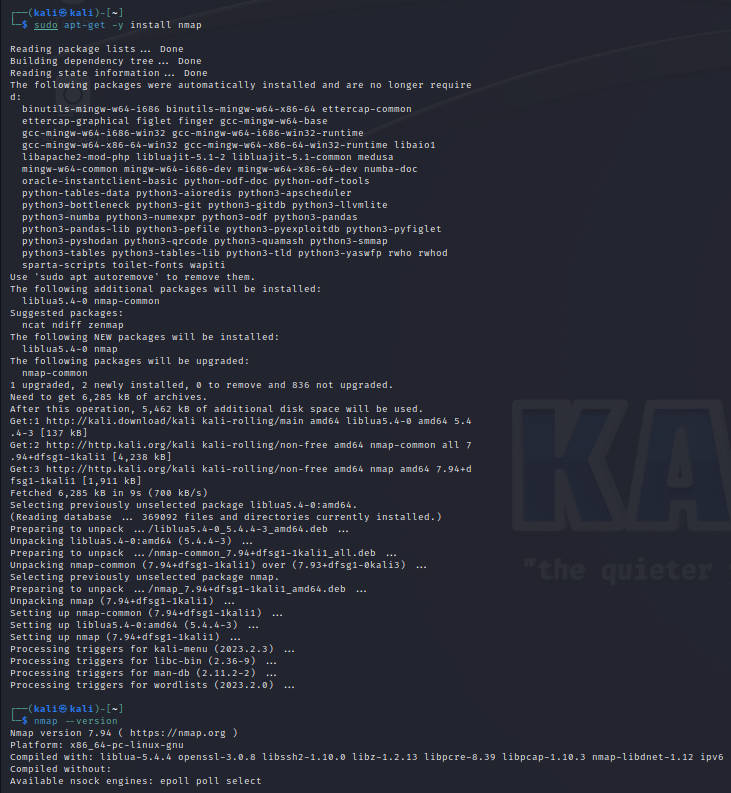
## **Network Security Project**

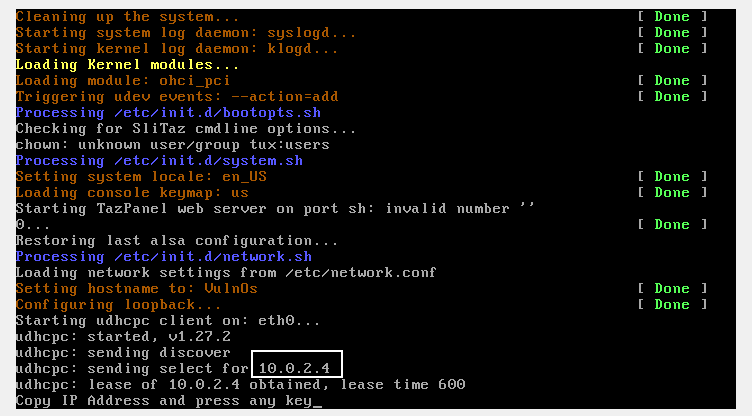
1. **The learner should be able to power on the provided VirtualBox OS** 
   1. VulnOS(Target Machine) is up and running successfully.



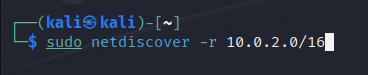
1. **The learner should install Nmap application and target the IP**
   1. Nmap is installed on the Kali machine using the following command -
      1. Sudo apt-get -y install nmap

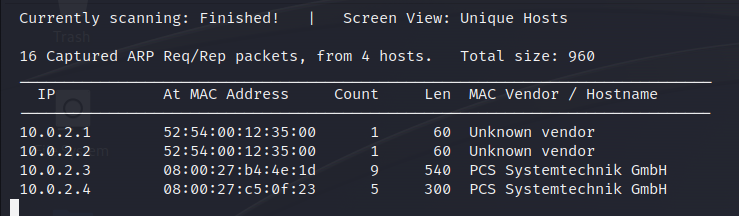


* 1. We can target the IP of the target machine by two ways -
     1. Using the VulnOS Login screen

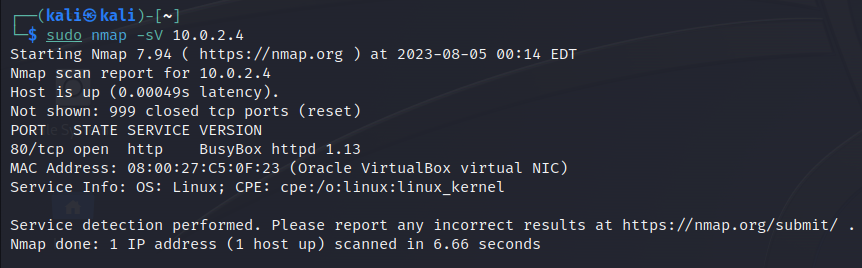


* + 1. Using the netdiscover command in linux
       1. Here we can either use 10.0.2.3 or 10.0.2.4. In our case, we are using 10.0.2.4 as we already know that’s the ip of the target machine.

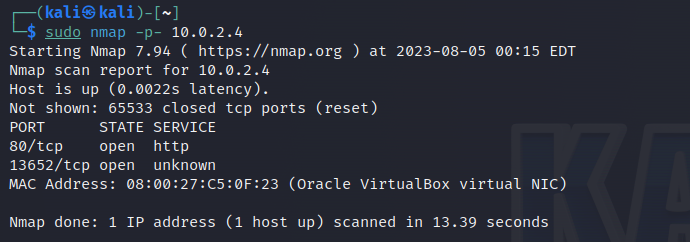




1. **The learner should be able to scan the IP using Nmap**
   1. We should use two commands here to get the ssh port -
      1. nmap -sV 10.0.2.4

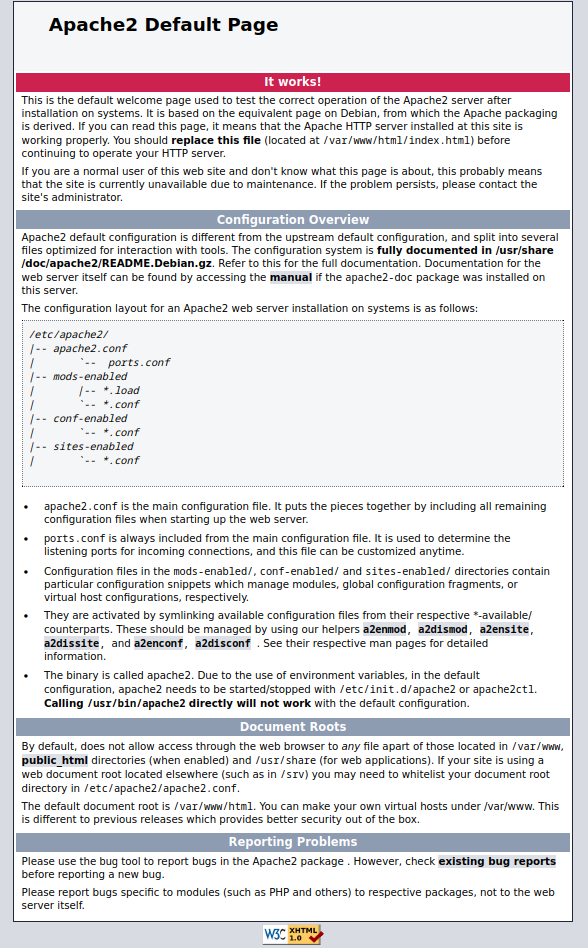


* + 1. nmap -p- 10.0.2.4



Here the reason for using the 2nd command is, the 1st command did not provide us the desired result i.e, the ssh port. Yet the 2nd command too did not provide the desired result but we got an unknown open port which can be used.

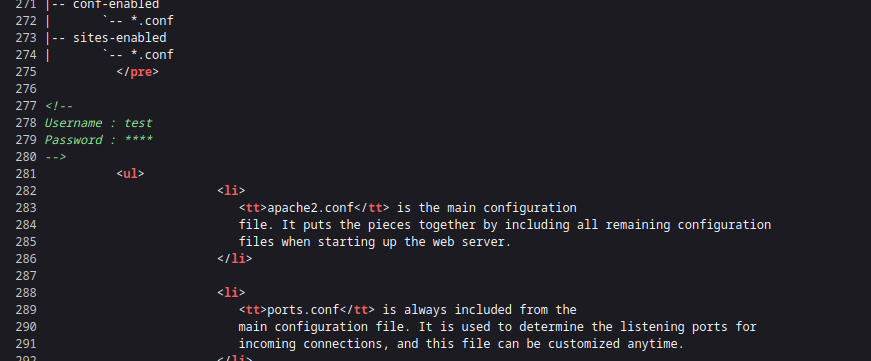
1. **The learner should be able to find out the SSH username**
   1. Go to a browser in Kali and type the IP of the target machine to reach this page.



* 1. Right click on the web page and click on **“View Page Source”**.

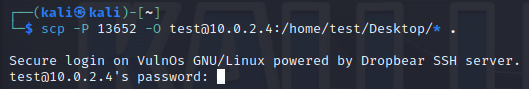


* 1. We will get the HTML code of the web page. Scroll down till you find **“Username”** and **“Password”** in the page.

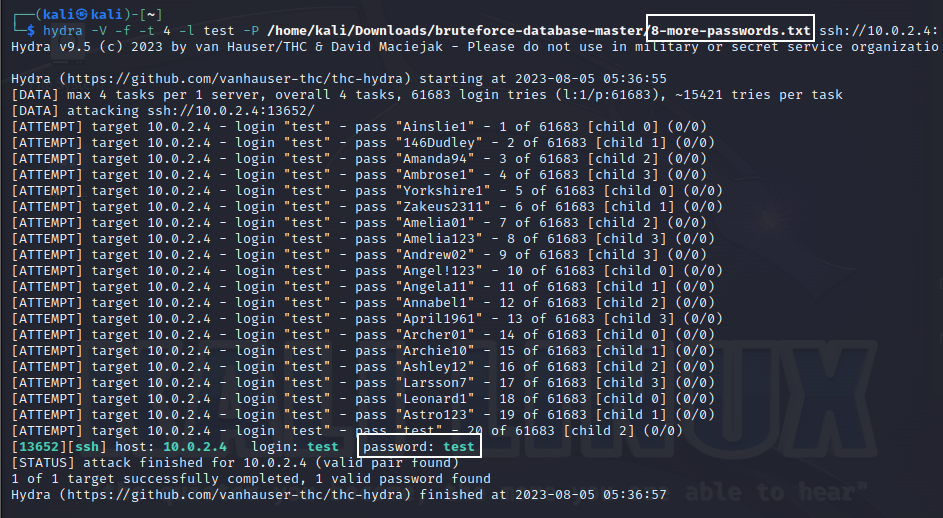


So, the name **“test”** in the **“Username”**  will be our target machine’s Username.

1. **The learner should be able to login via SSH(Three methods were used(a,b,c) Method “a” was successful)**
   1. **Method 1 -**
      1. Using scp command to download file from target machine with port no 13652 -



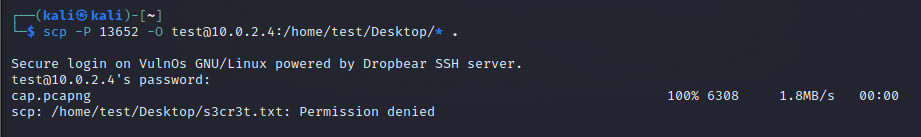
* + - 1. To find password to login to Target machine and download **“cap.pcapng”**the file -
         1. Using Brute-force attack(Hydra) -



For Brute-force, a file named **“8-morepasswords.txt”**(with more than 70,000 passwords)was used.

Password successfully obtained for the target machine and the **“Password = test”**.

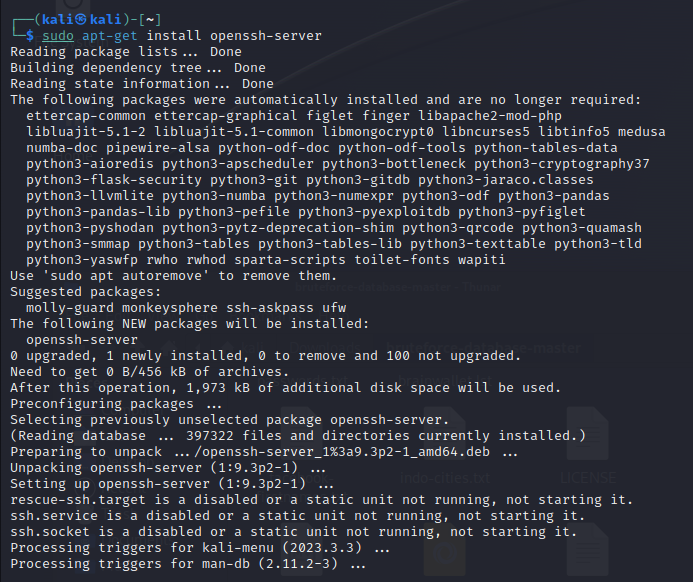
* + 1. Login to download **“cap.pcapng”** file from target machine using the obtained password from Brute-force attack -

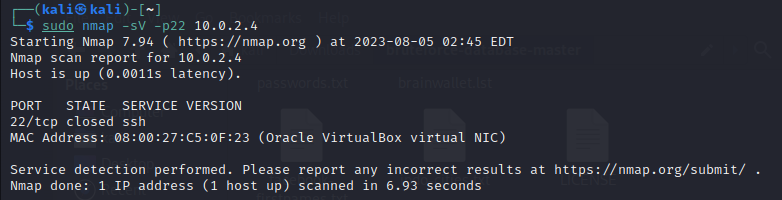


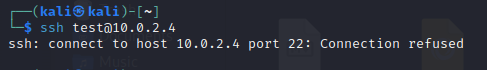
Connection to the target machine was successful and we were also able to download the **“cap.pcapng”** file.

* 1. **Method 2 -**

SSH server is installed to do a port scan for open ssh ports for successful connection.

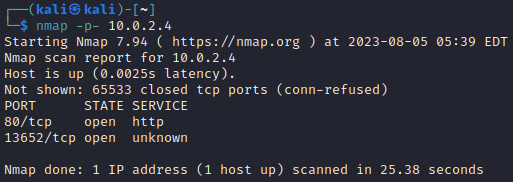






SSH port 22 is closed. So, Connection was refused and login is not possible.

* 1. **Method 3** -
     1. Using “**nmap -p- 10.0.2.4”** to find more open ports -

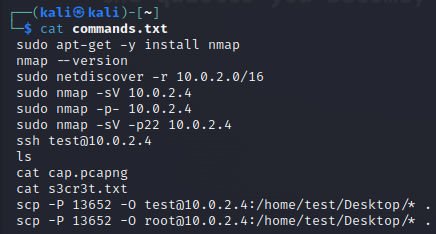


Got an open port with unknown service. So, let us use this port for SSH connection.

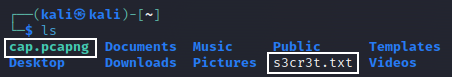
* + 1. Using SSH command with the port no 13652 -

SSH connection failed again due to unknown service.

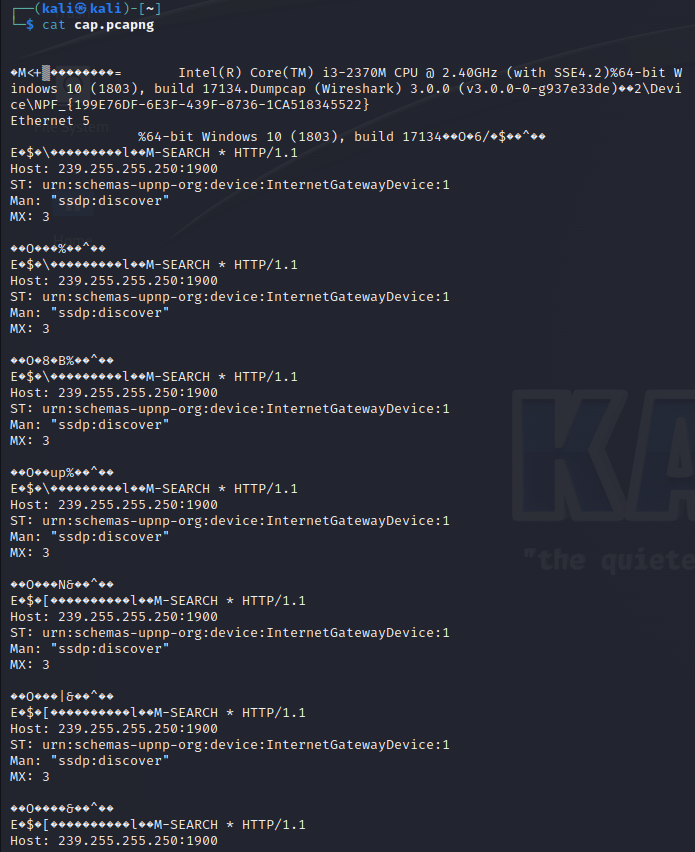
1. **The learner should be able to use the Kali Linux terminal with all proper commands**
   1. All the commands used in Kali linux to successfully run the project -

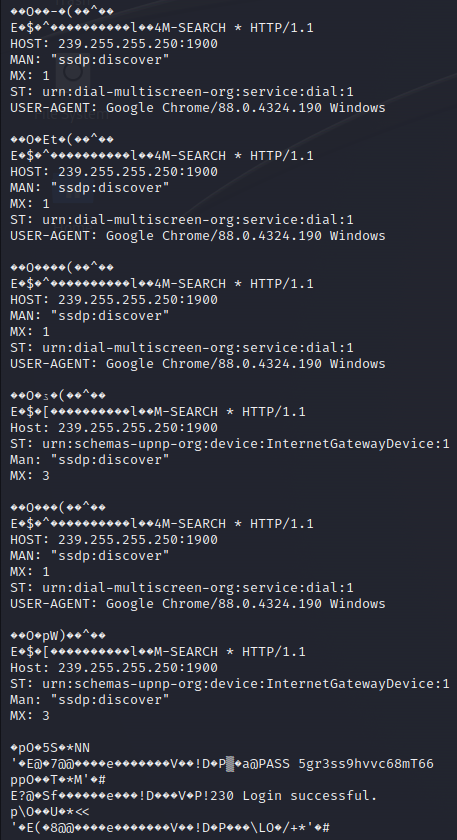


1. **The learner should be able to view the user text file inside the terminal**
2. These are the files downloaded from the target machine.

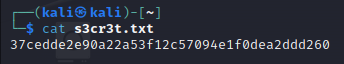
****

1. This is the contents of the cap.pcapng file



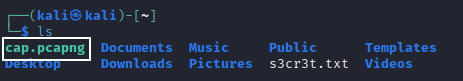


1. This is the contents of s3cr3t.txt

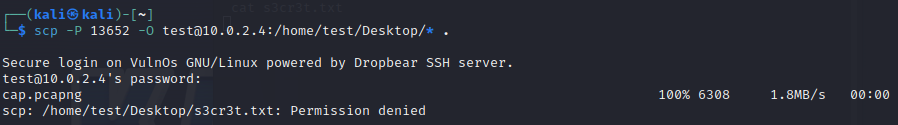


Hence, viewed the content of the files **“cap.pcapng”** and **“s3cr3t.txt”**.

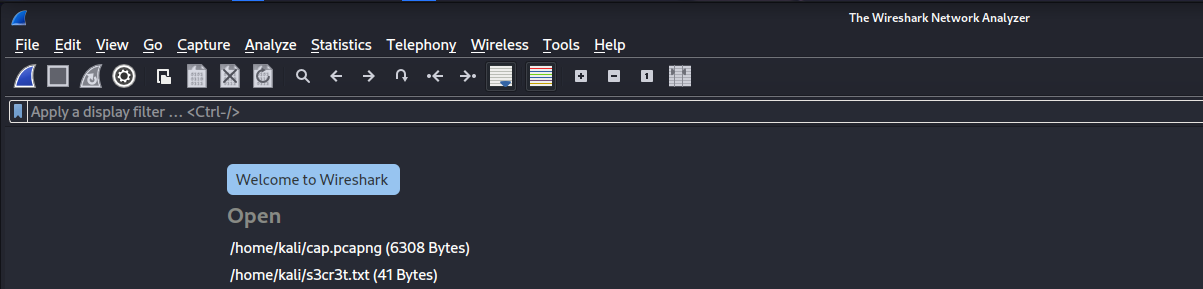
1. **The learner should be able to access the cap.pcapng file to the local disk**
   1. The cap.pcapng file successfully downloaded from target machine to Kali machine -



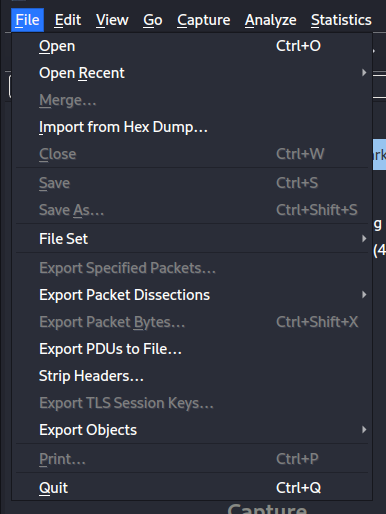
Command used to download file from target machine to Kali machine -

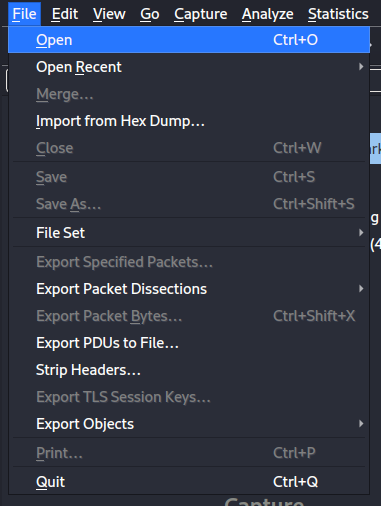


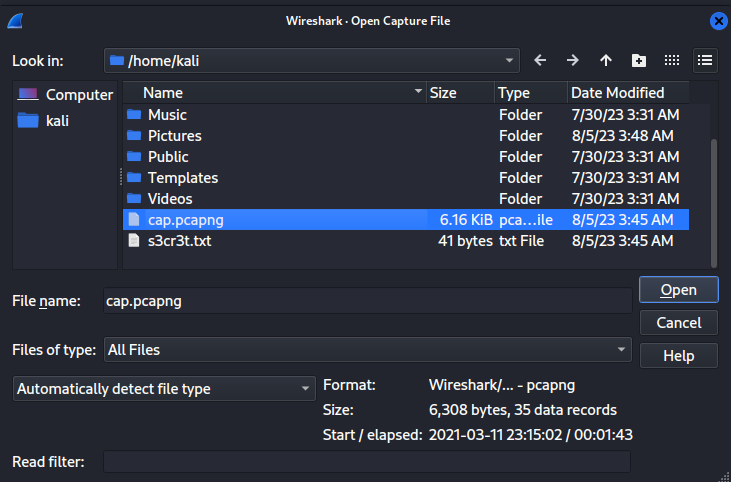
1. **The learner should open the cap.pcapng file in Wireshark and find the PASS from packets table**
2. Wireshark terminal



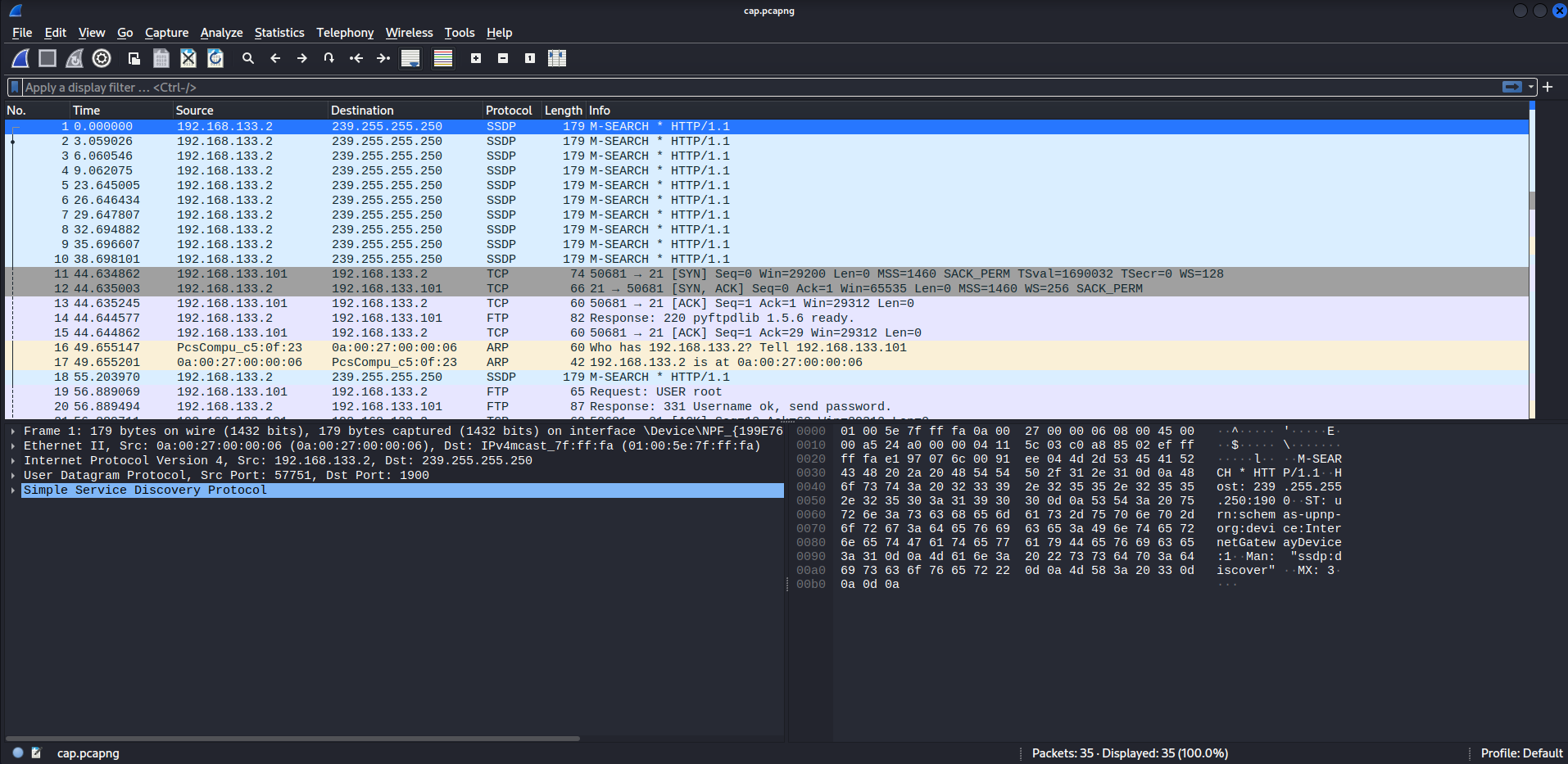
1. Click **“File”** andclick **“Open”** and double click on the **“cap.pcapng”** file -



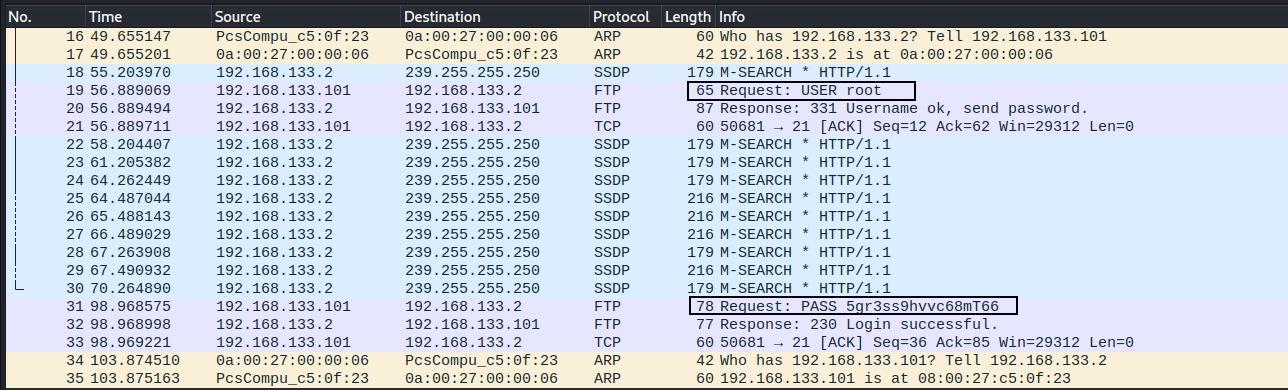




1. Then the **“cap.pcapng”** file will be loaded to wireshark -



1. Scroll down to find **“Password”** of the **root** user -



Use the Password to download the “**s3cr3t.txt”** file from the target machine to Kali machine.

1. **The learner should be able to read the contents in the secretfile.txt**
   1. The contents of the **“s3cr3t.txt”** file is-

