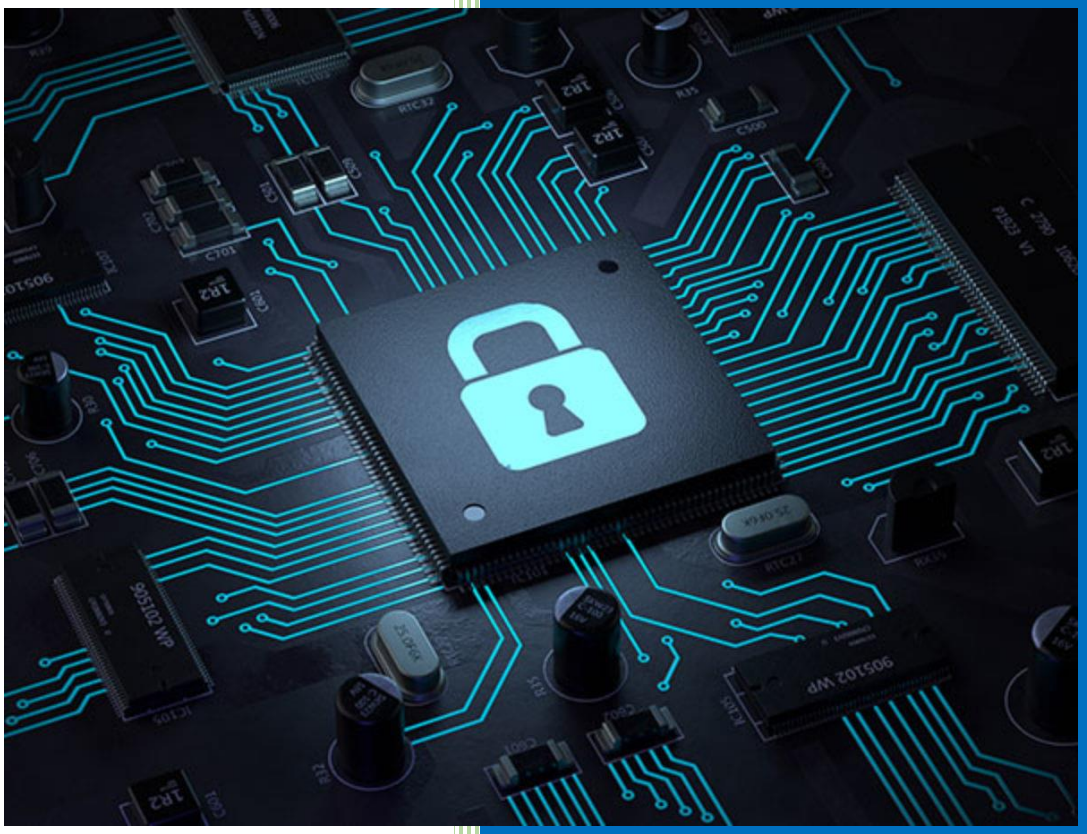
FAKULTI TEKNOLOGI
KEJURUTERAAN KELAUTAN
DAN INFORMATIK

2020/2021

CYBER SECURITY



Lab 5: Network Security

VERSION 1

`

Revision History

Revision Date	Previous Revision Date	Summary of Changes	Changes Marked
30/03/2021		First Issue	Fakhrul Adli Mohd Zaki Dr Farizah Yunus
4/5/2021		-Change the IP Address from 192.168.1.4 to 192.168.1.5 on page 2 -Fixed grammar and spelling mistakes.	

`

CONTENTS

`

INSTRUCTIONS

Manual makmal ini adalah untuk kegunaan pelajar-pelajar Fakulti Teknologi Kejuruteraan Kelautan dan Informatik (FTKKI), Universiti Malaysia Terengganu (UMT) sahaja. Tidak dibenarkan mencetak dan mengedar manual ini tanpa kebenaran rasmi daripada penulis.

Sila ikuti langkah demi langkah sebagaimana yang dinyatakan di dalam manual.

Arahan laporan makmal:

a) Pelajar perlu menyediakan laporan makmal untuk aktiviti makmal.
b) Kandungan laporan makmal mesti terdiri daripada beberapa tangkapan skrin untuk semua tetapan makmal keselamatan maya yang berjaya dengan beberapa penjelasan.
c) Jawab semua soalan refleksi untuk setiap sesi makmal.
d) Pelajar dapat memberikan senarai rujukan untuk rujukan tambahan.
e) Laporan makmal mesti dihantar dalam masa yang diberikan menggunakan pautan yang disediakan di platform eLearning.

This laboratory manual is for use by the students of the Faculty of Ocean Engineering Technology and Informatics, Universiti Malaysia Terengganu (UMT) only. It is not permissible to print and distribute this manual without the official authorisation of the author.

Please follow step by step as described in the manual.

Lab report instructions:

a) Students need to prepare lab report for lab activities.
b) The contents of the lab report must consist of several screenshots for all successful setting of virtual security lab with some explanation.
c) Answer all the reflection questions for every lab sessions.
d) Student can provide the list of references for extra references.
e) *Lab report must be submitted within the time given using the provided link in the eLearning platform.*

`

TASK 1: SETTING UP THE VIRTUAL LAB NETWORK

OBJECTIVE

To set up the network based on the provided topology.

TASK DESCRIPTION

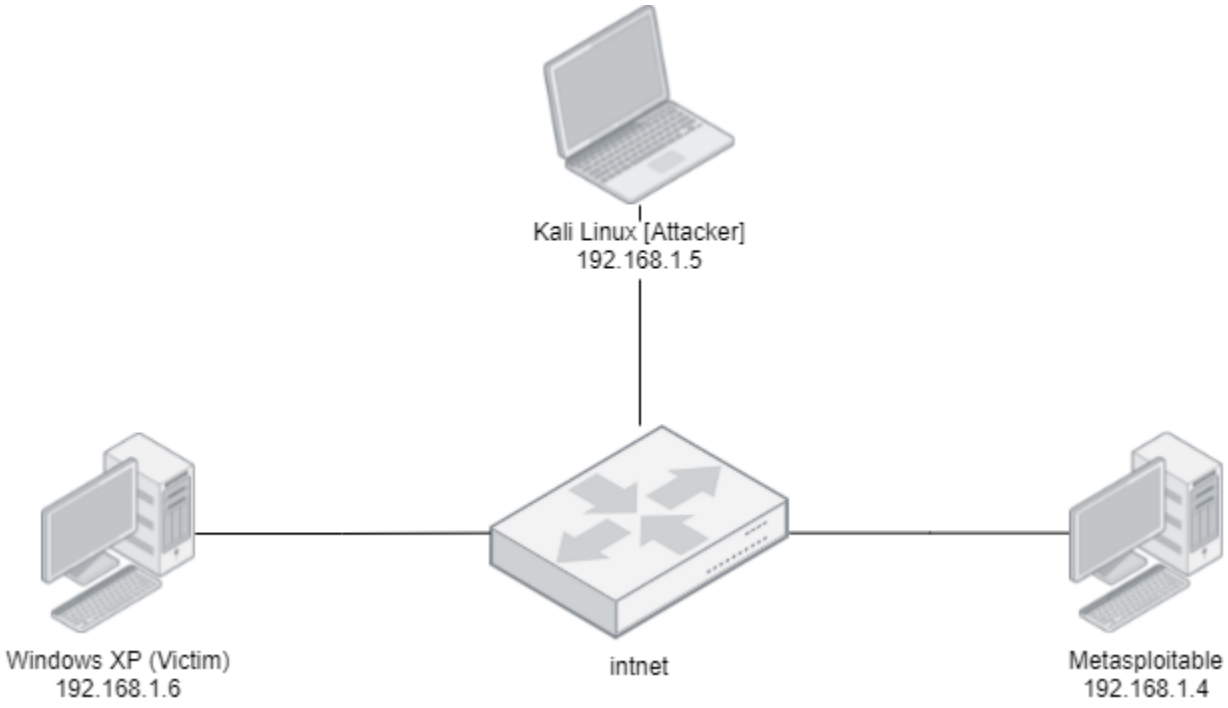
In this task, the student needs to set up the network according to the given topology. This network will be used in the next task.

ESTIMATED TIME

30 Minutes

STEPS:

1. The diagram below shows the network topology that we are going to implement in our virtual lab. For this lab, we are going to connect all the Virtual Machines (Windows XP, Metasploitable and Kali Linux) to the internal network known as **intnet**.



2. Generally, the network configuration of all the virtual machines has been done during the previous lab session.

`

3. You can refer back to all the steps in Lab 2: Social Engineering>Task 4 (page 51) and Lab 4: Host Security>Task 2 (page 5).

4. Make sure the network configuration has been applied correctly. You may use the **ifconfig** command for Kali Linux & Metasploitable and **ipconfig** command for Windows XP to ensure that all the virtual machines assigned with the correct IP Addresses as shown in the above topology.

5. Next, use the **ping** command to test the connection from Kali Linux to Metasploitable and from Windows XP to Metasploitable virtual machines.

6. Take the screenshots of the successful ping operations and put them into your lab report.

7. If all the steps above are successful, then you may proceed to the next task.

`

TASK 2: MAN-IN-THE-MIDDLE ATTACK USING ARP POISONING

OBJECTIVE

To run a man-in-the-middle (MITM) attack simulation using the ARP poisoning technique.

TASK DESCRIPTION

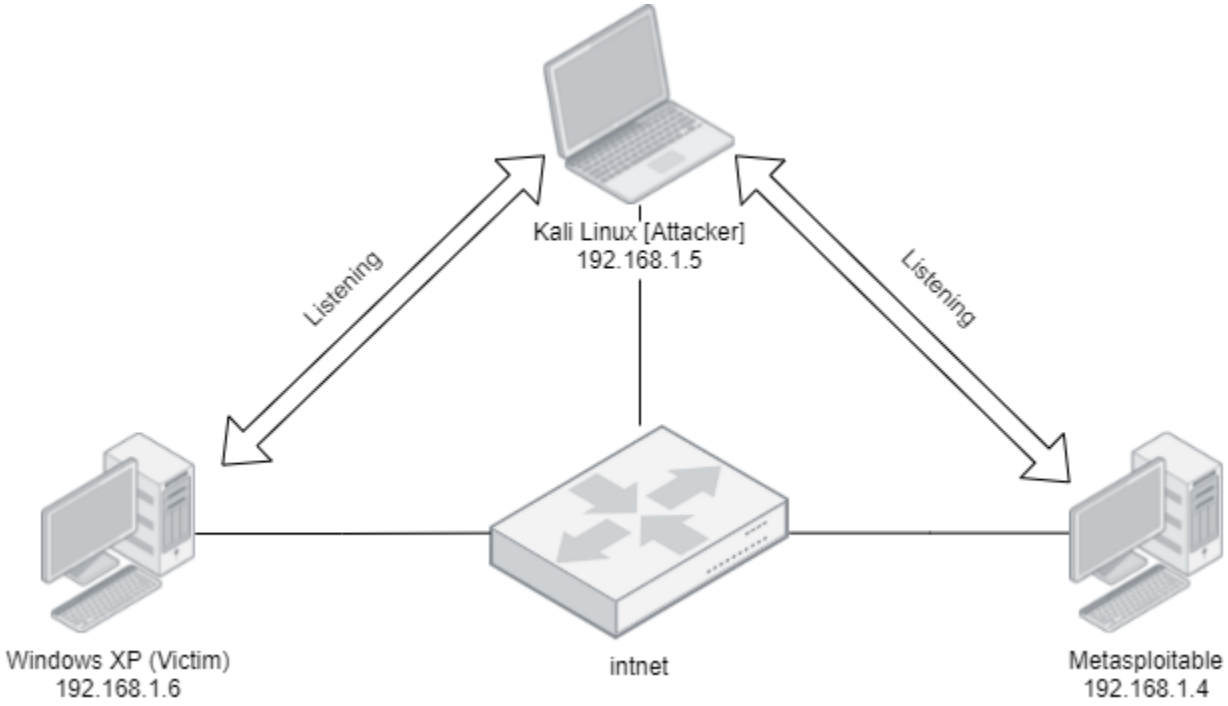
For this task, the student will run a man-in-the-middle attack simulation. This attack will use the ARP poisoning technique where all the network packets from the victim will be captured by using a sniffer software known as Wireshark. Before that, the ARP poisoning/spoofing will be carried out using a special tool in Kali Linux. This tool is known as Ettercap. By using Ettercap, all the packets during the telnet connection between Windows XP (victim) and Metasploitable will be redirected to Kali Linux (attacker) machine as well.

ESTIMATED TIME

90 Minutes

STEPS:

1. Before running the MITM attack simulation, let's review how ARP Poisoning works by referring to the following diagram:



The Address Resolution Protocol (ARP) is a network communication protocol that allows network communications to reach a particular network unit. ARP converts Internet

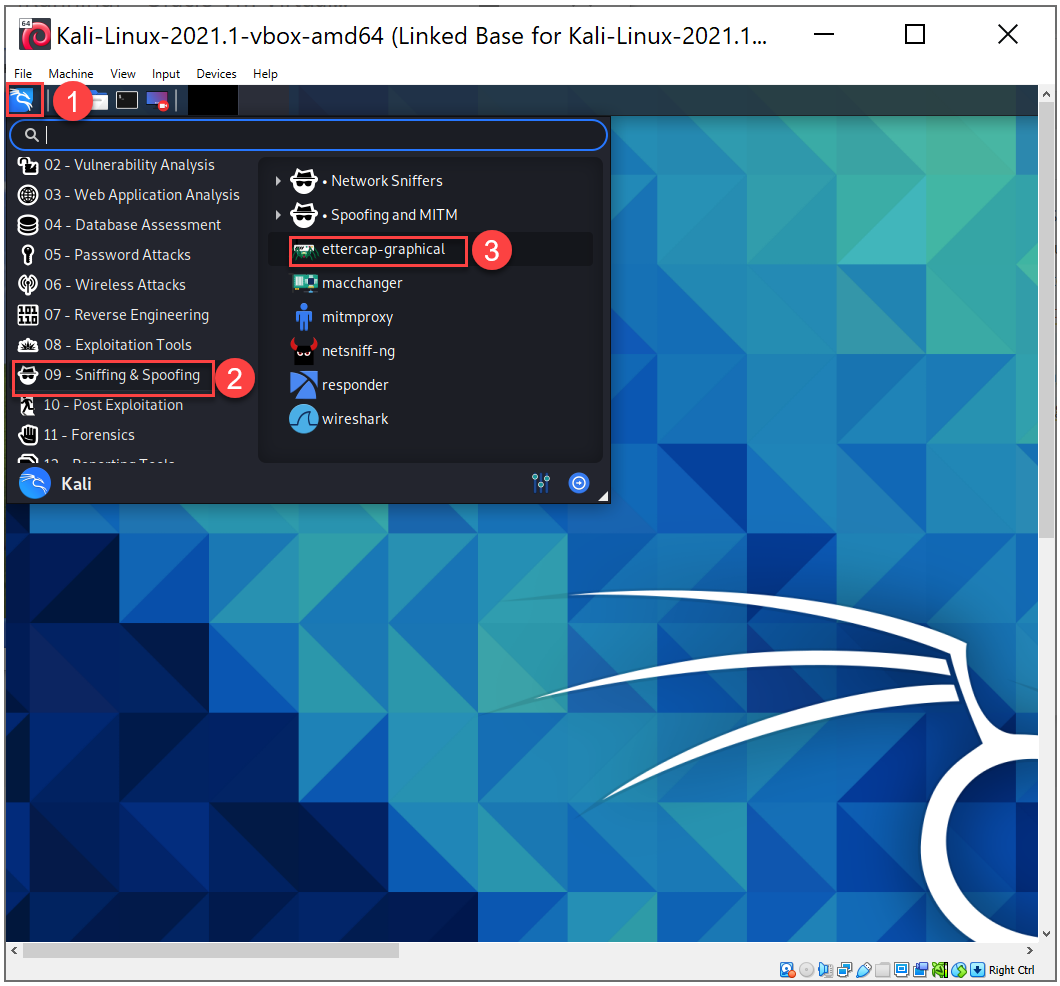
`

Protocol (IP) addresses to Media Access Control (MAC) addresses and the other way around. ARP is most widely used by devices to communicate with the router or gateway that allows them to connect to the Internet. In the older IPv4 standard, ARP only works with 32-bit IP addresses. The Neighbor Discovery Protocol (NDP), which is encrypted and uses cryptographic keys to validate host identities, is used by the newer IPv6 protocol. ARP is still widely used since the majority of the Internet still uses the older IPv4 protocol.
ARP Poisoning (also known as ARP Spoofing) is a form of LAN-based cyber attack that involves sending malicious ARP packets to a LAN's default gateway to alter the pairings in the IP to MAC address table. IP addresses are converted to MAC addresses using the ARP Protocol. Since the ARP protocol was created for productivity rather than security, ARP Poisoning attacks are extremely simple to carry out as long as the attacker has control of or is directly connected to a computer on the target LAN.

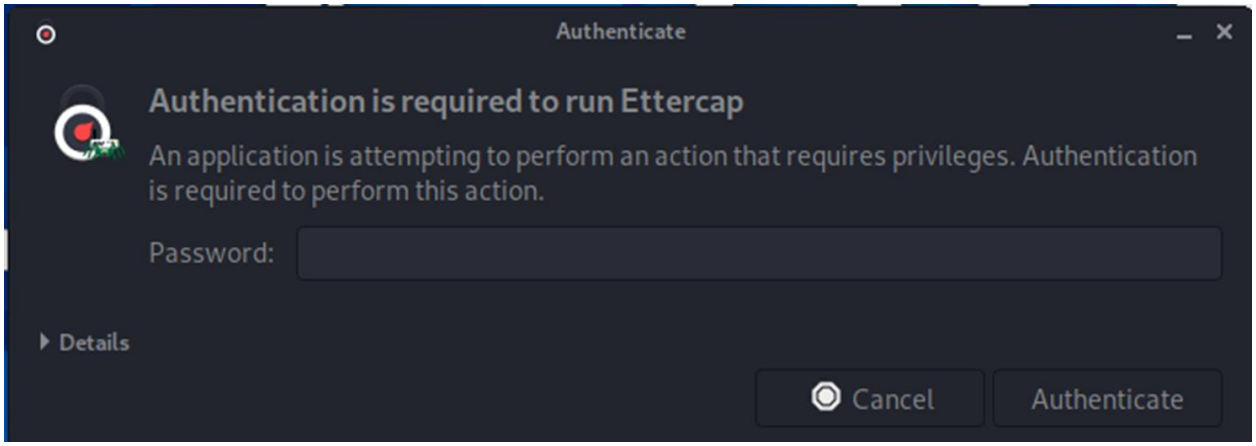
2. First of all, continuing from Task 1, go to the Kali Linux virtual machine and log in to the system. Check the network settings of Kali Linux where it should always hold the IP Address 192.168.1.4.

3. Next, click on the Kali Linux home button. Scroll down until you see **09-Sniffing & Spoofing,** then choose **ettercap-graphical**.

`



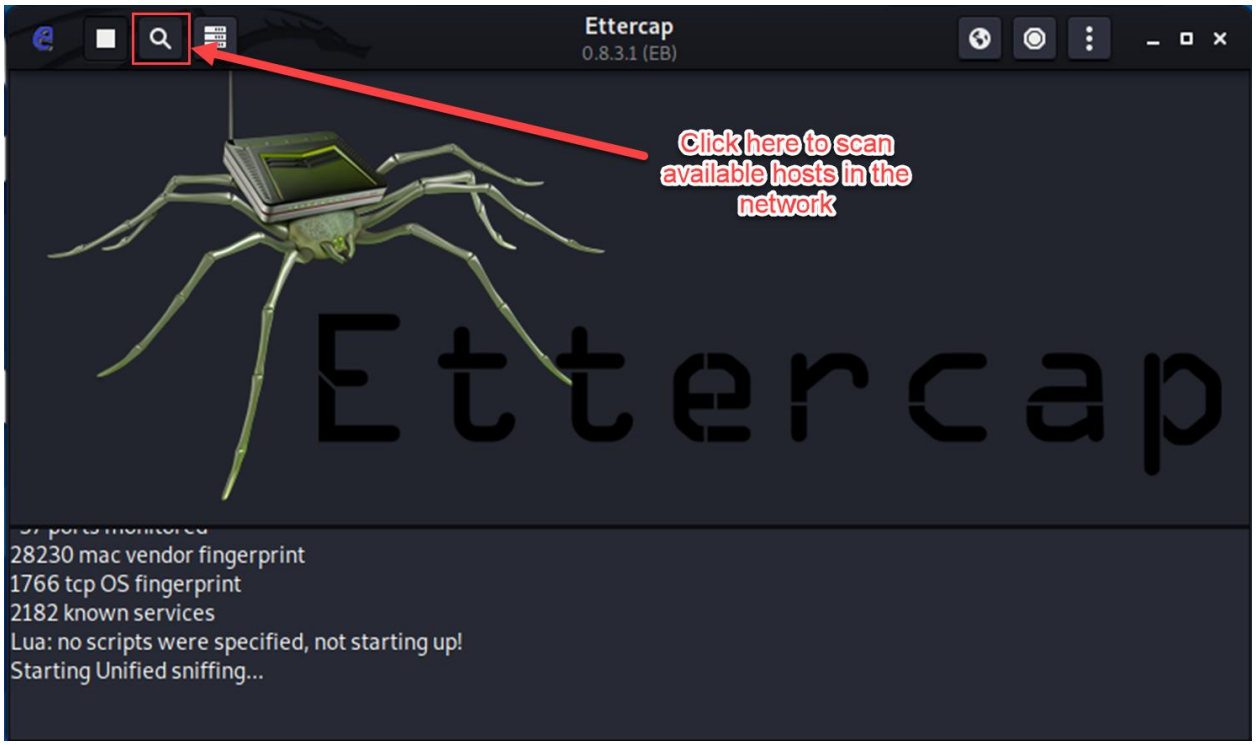
4. To run Ettercap, you need to enter the password for Kali Linux.



`

5. You will a screen below, then click on the tick symbol.

6. Now, we are ready to scan the host in the internal network **intnet**. Click on the magnifying glass symbol.



`

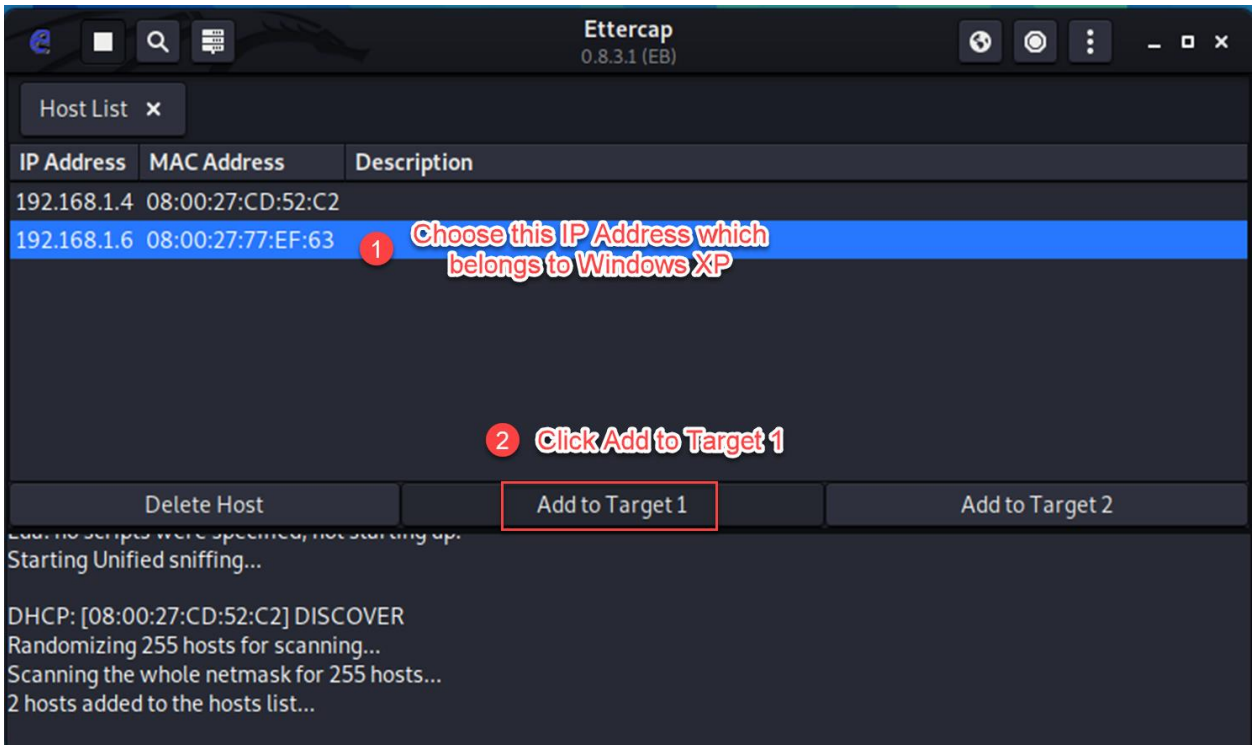
7. Please wait for a few seconds for the scanning to complete. After completion, we can see that Ettercap has detected 2 available hosts in the network.

`

8. Now, click on the icon to view the detected hosts.

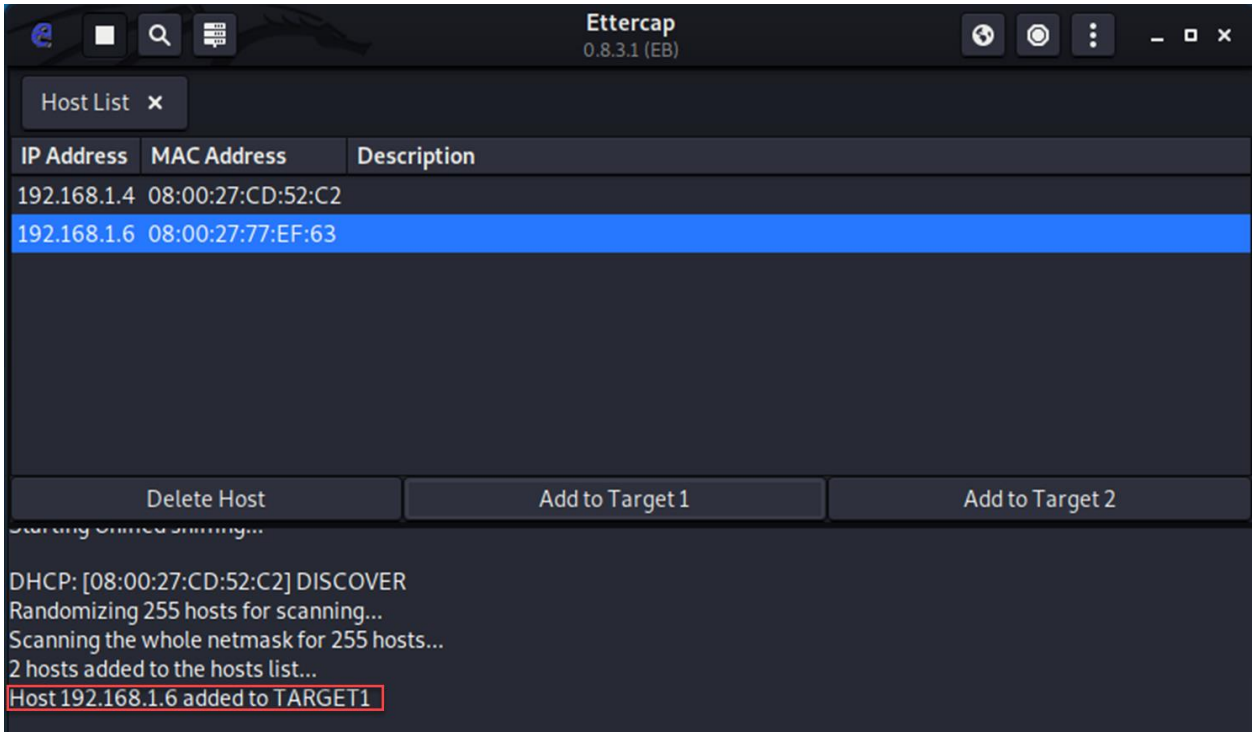
`

9. You will see two IP Addresses in the list. Both belong to Metasploitable and Windows XP virtual machine respectively. Now, we are going to choose **192.168.1.6** which is the IP Address of the victim (Windows XP). Click **Add to Target 1**.

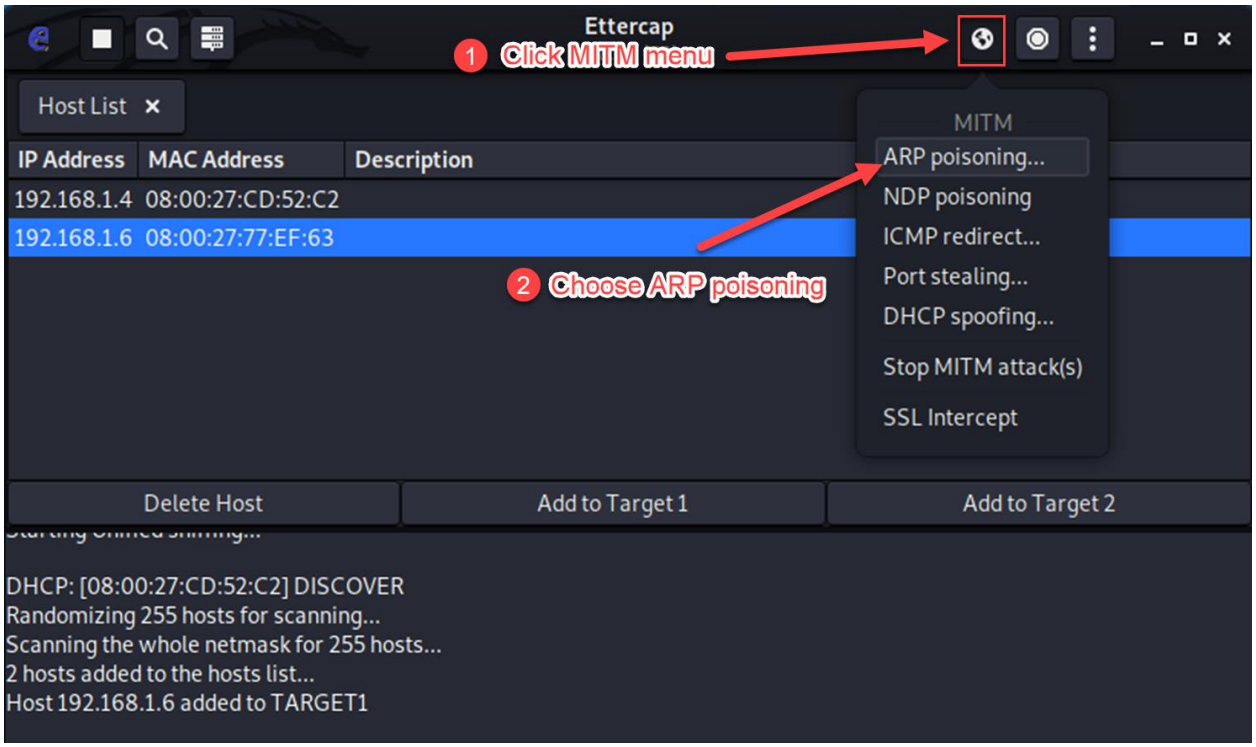


`

10. At the bottom of the console, you will see a confirmation that 192.168.1.6 has been added to Target 1.

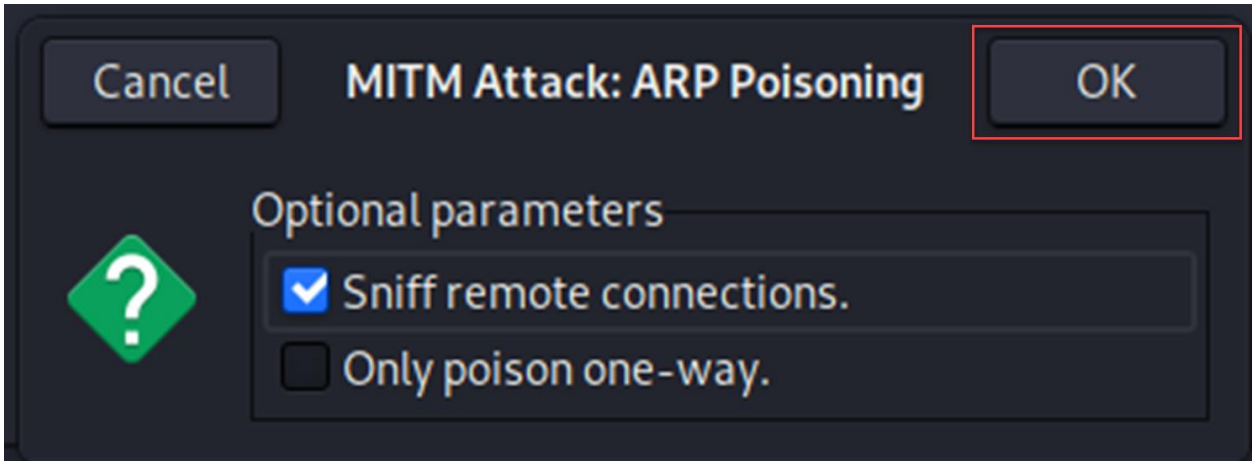


11. Now, go to the MITM menu, then choose ARP poisoning.

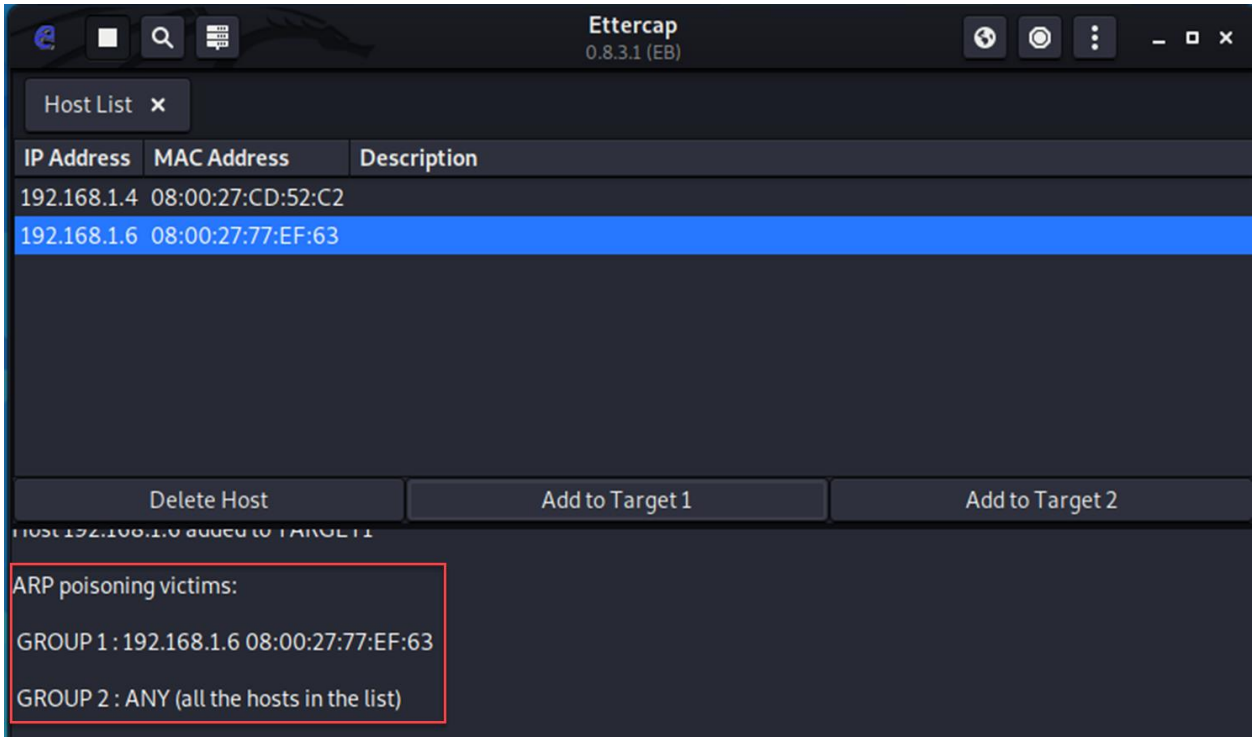


`

12. Click OK to proceed.

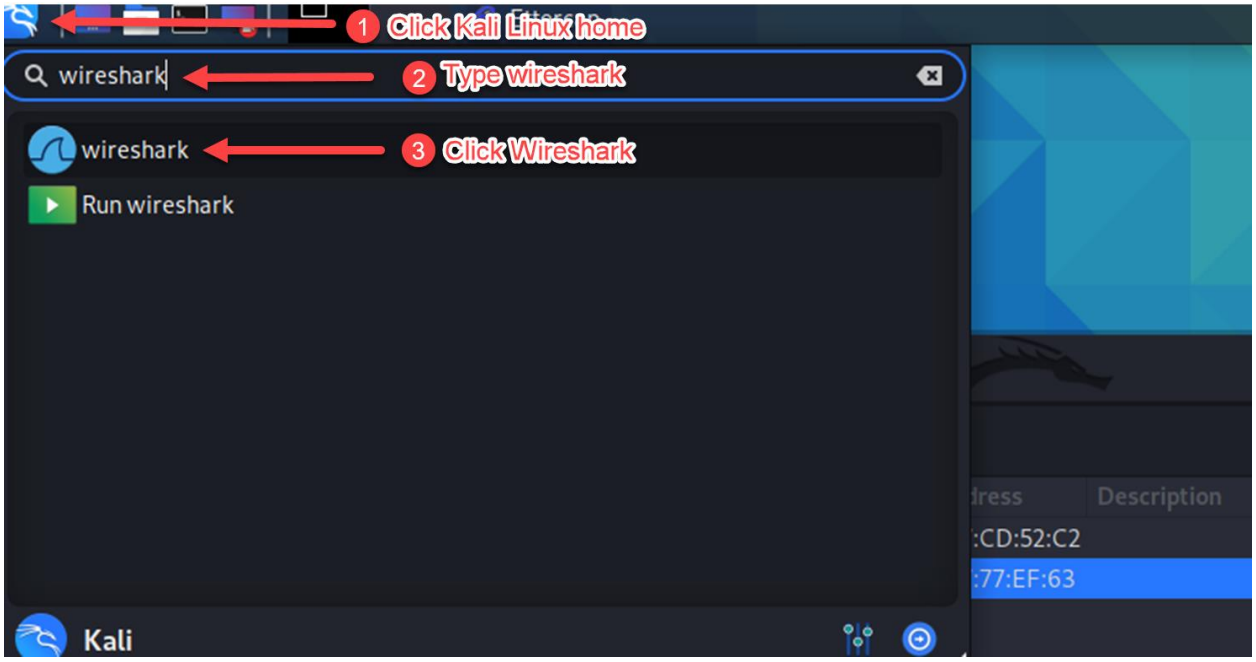


13. You will see **192.168.1.6** now become an ARP poisoning victim.

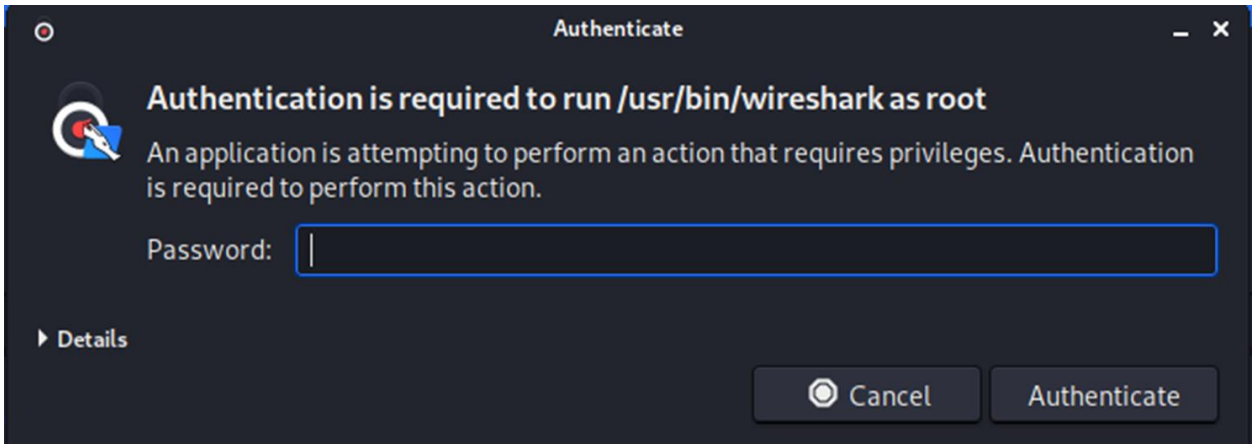


`

14. Next, we are ready to run Wireshark, a packet sniffing software. Do the steps as shown in the screenshot below.

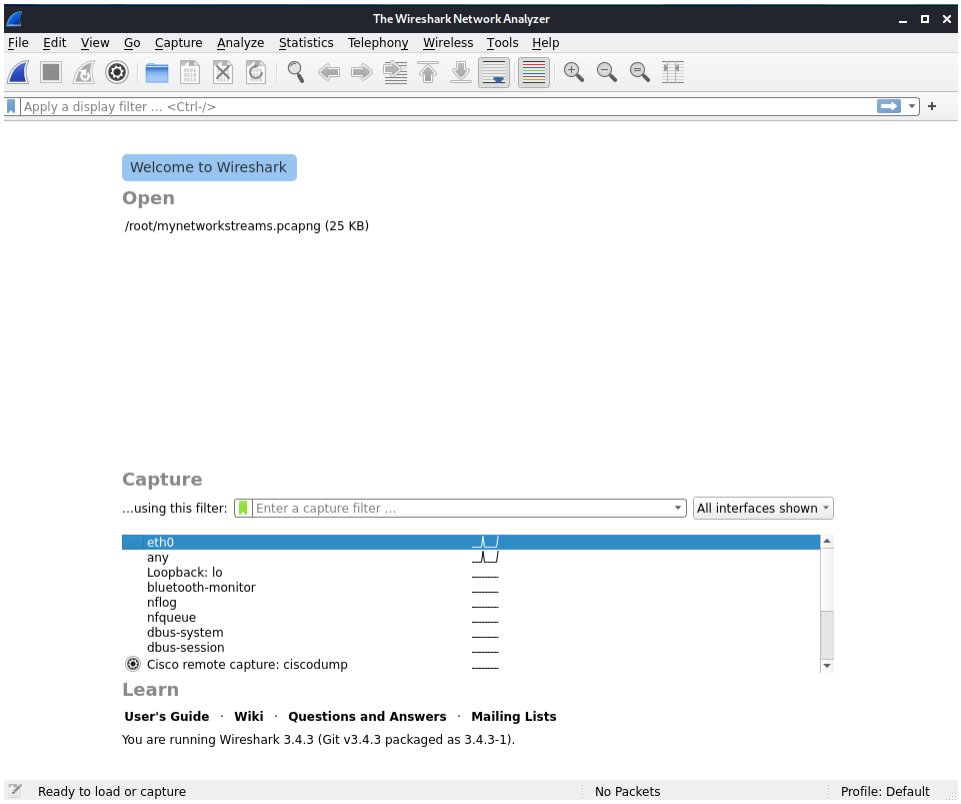


15. To run Wireshark, we also need to supply the password. Click **Authenticate**.



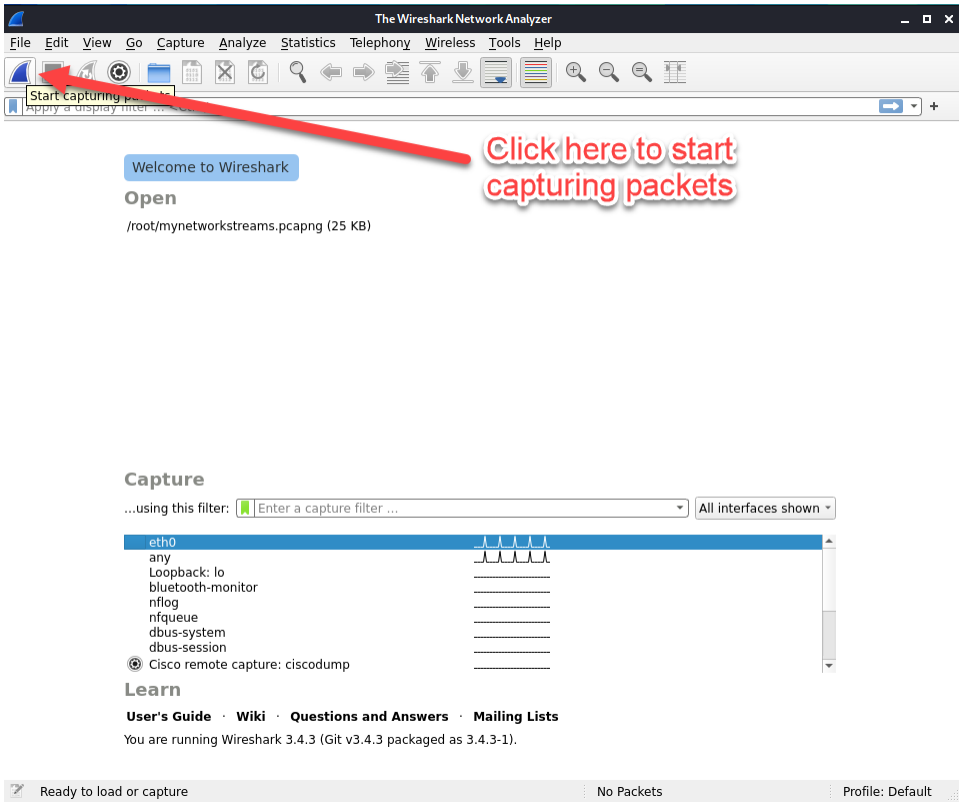
`

16. You will see a home screen of Wireshark as following:



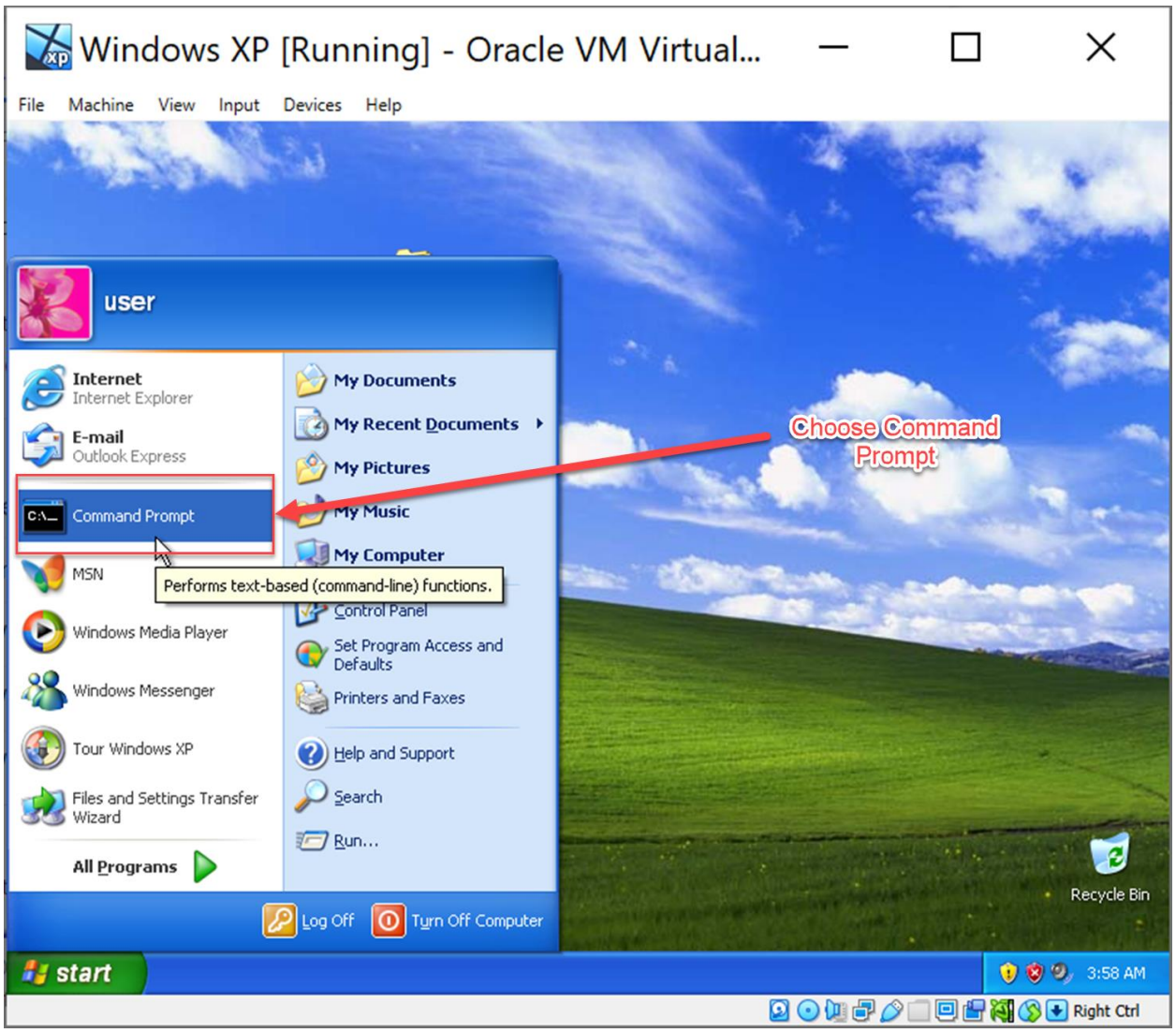
`

17. Now the attacker (Kali Linux) is ready to capture the packet that belongs to the victim (Windows XP). Click the fin icon to start capturing.



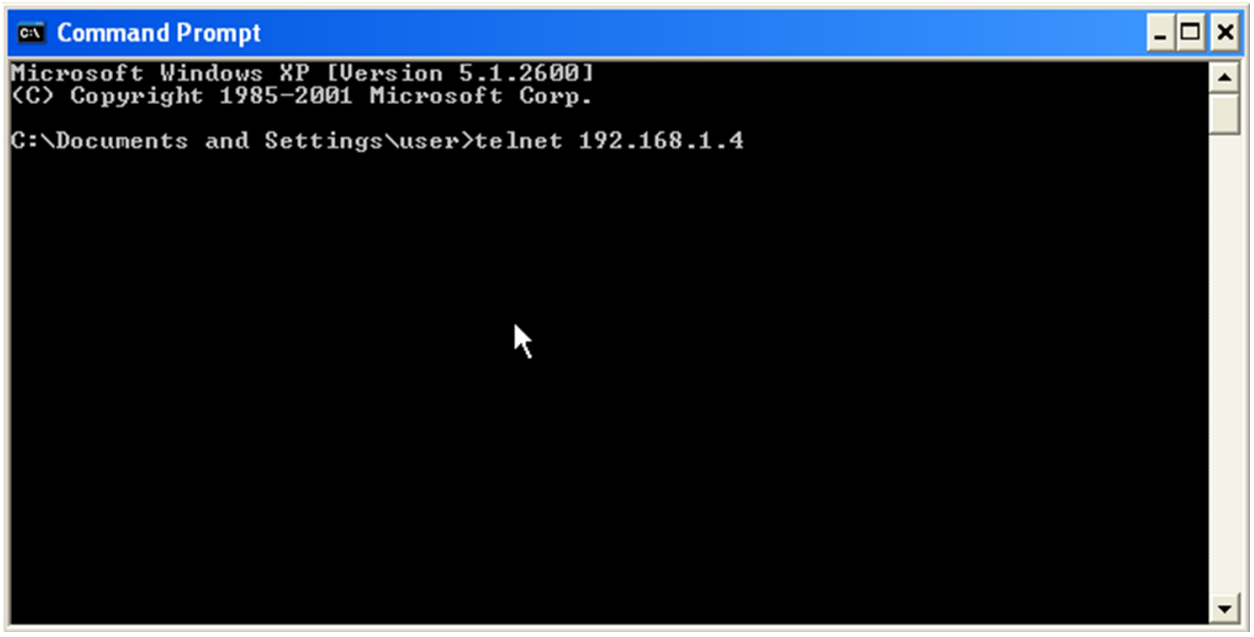
`

18. It's time to switch to the victim's machine. Click on the **Start** button, then choose **Command Prompt**.



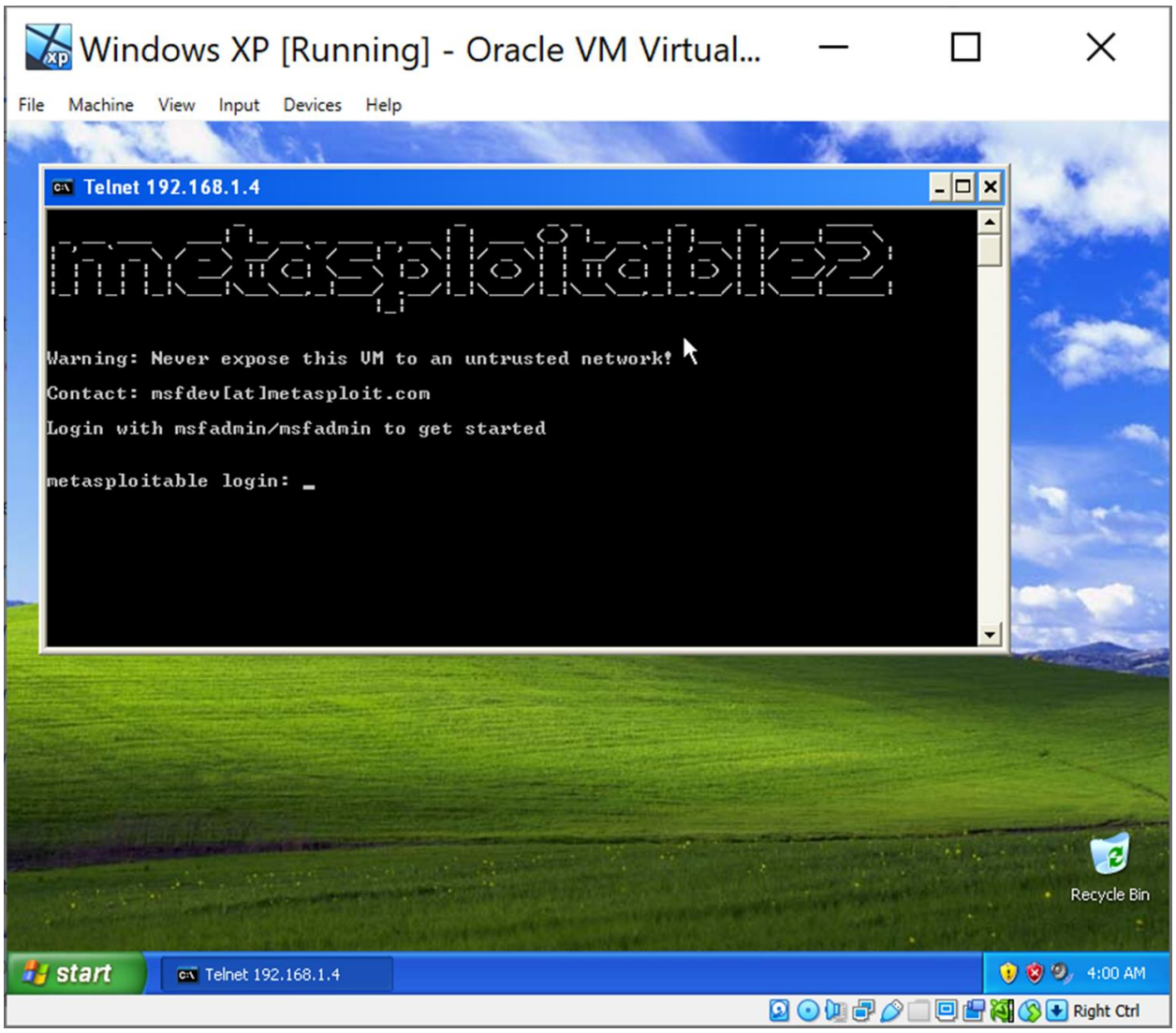
`

19. We open the command prompt to run a telnet program. Telnet will allow us to connect to a remote machine (Metasploitable). Type the command as shown in the screenshot, hit **Enter** when completed.



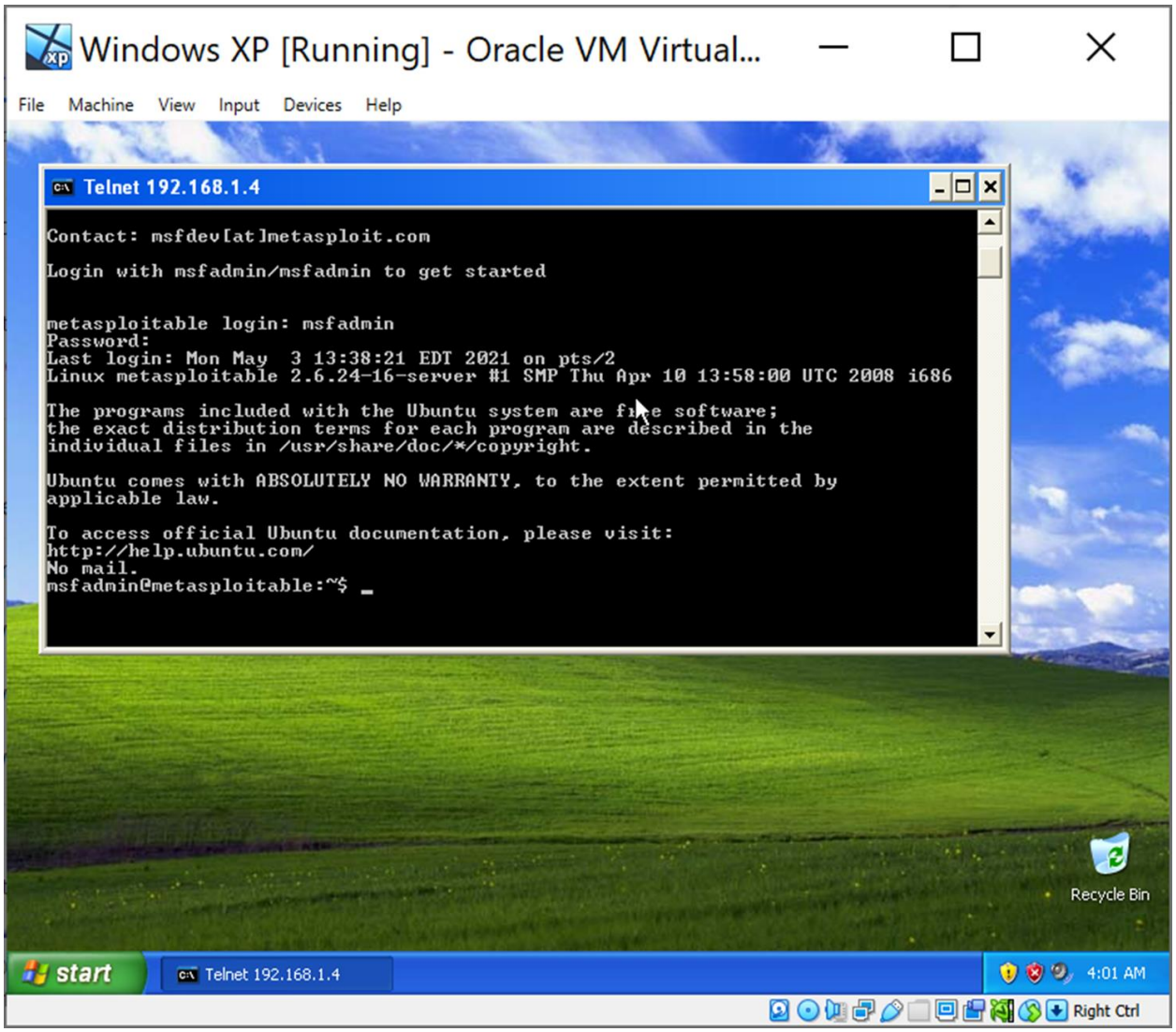
`

20. If the connection is successful, we will see the home screen of the Metasploitable machine. Enter the login and password as **msfadmin**.



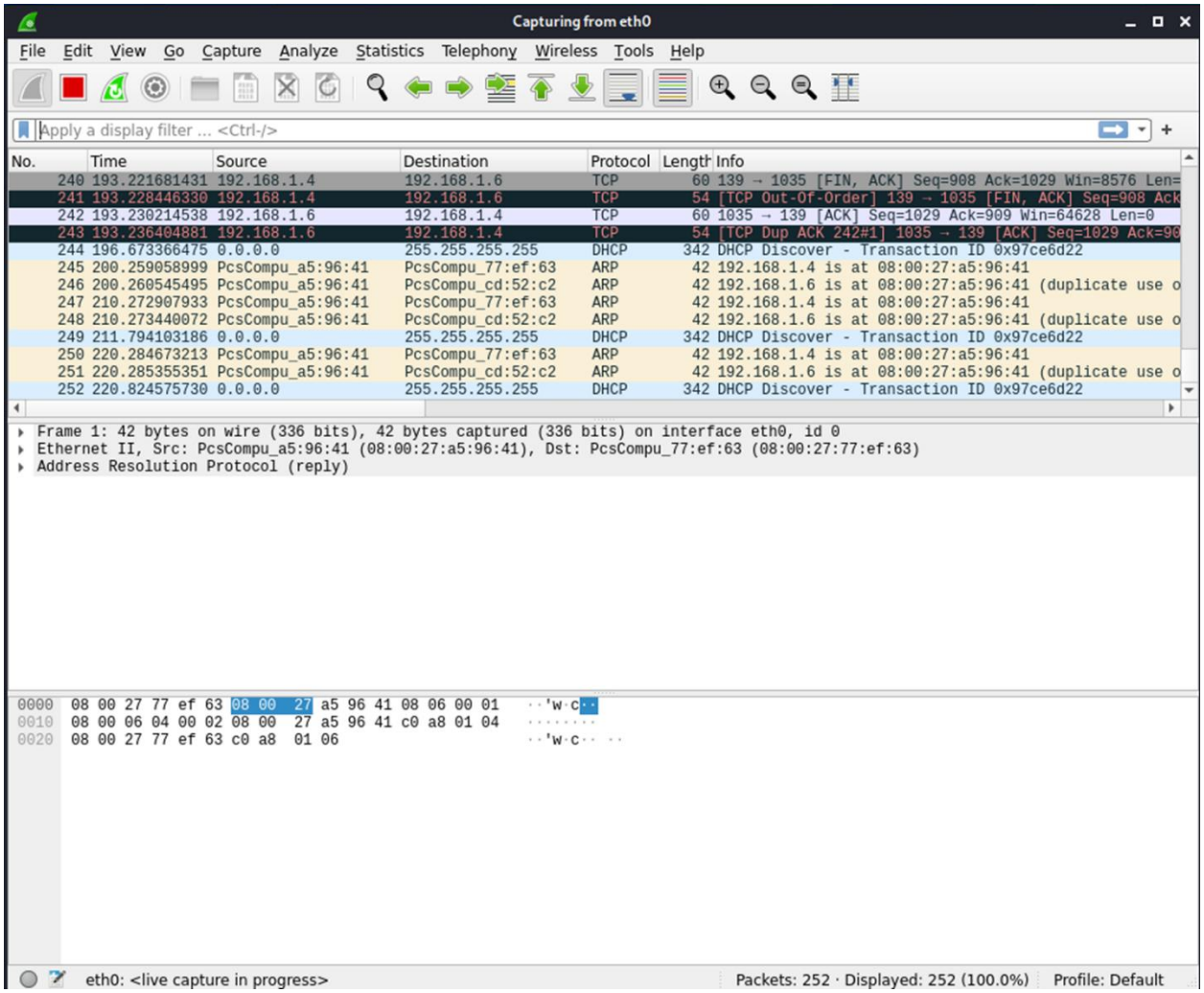
`

21. Now, we have successfully connected to Metaspolitable machine from Windows XP. For confirmation, you will see a line, **msfadmin@metasploitable:~$,** waiting for you to enter any Linux command.



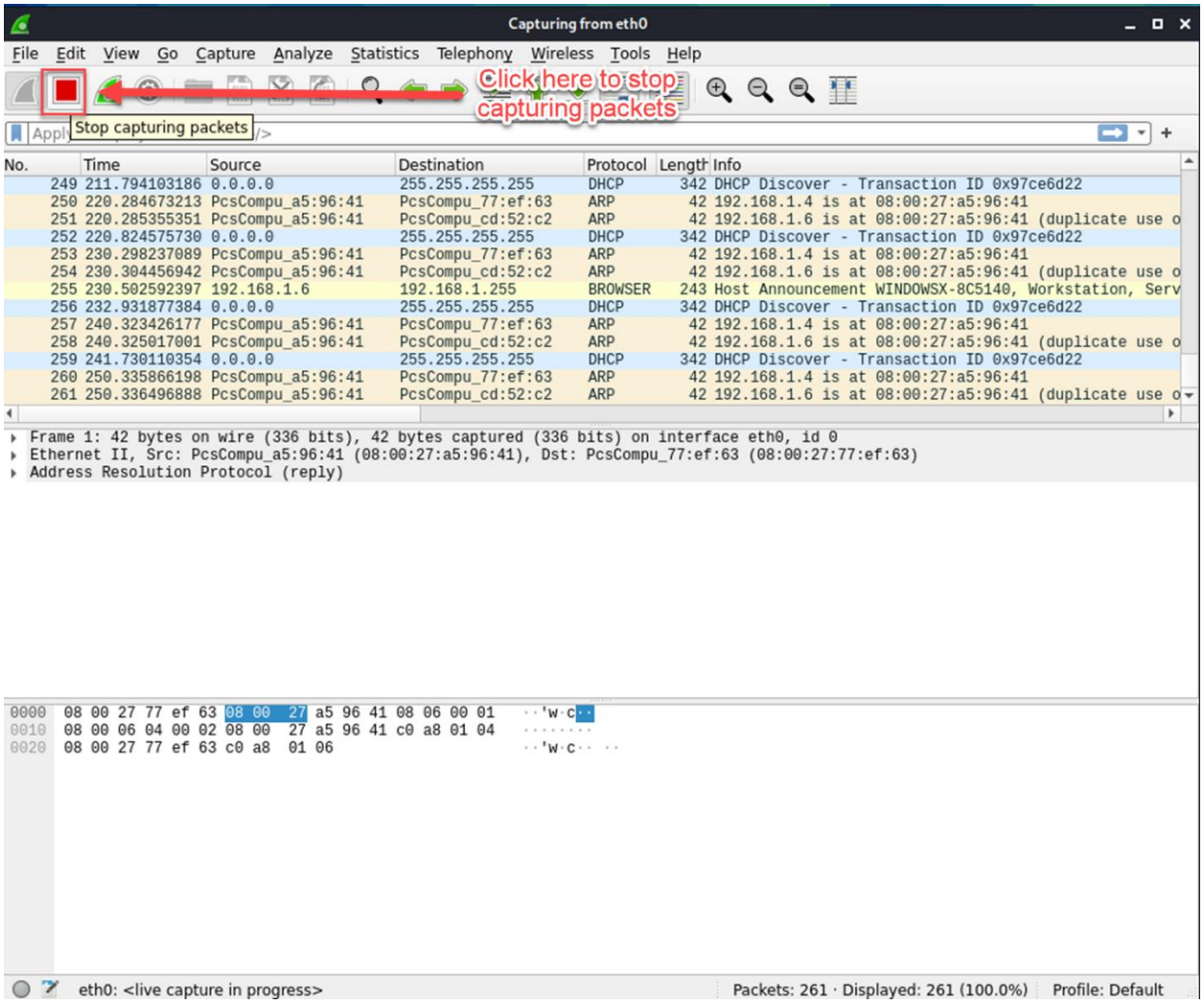
`

22. We are done with the victim machine, now switch back to Kali Linux virtual machine and observe the output of Wireshark. You will see lines of network packet information.



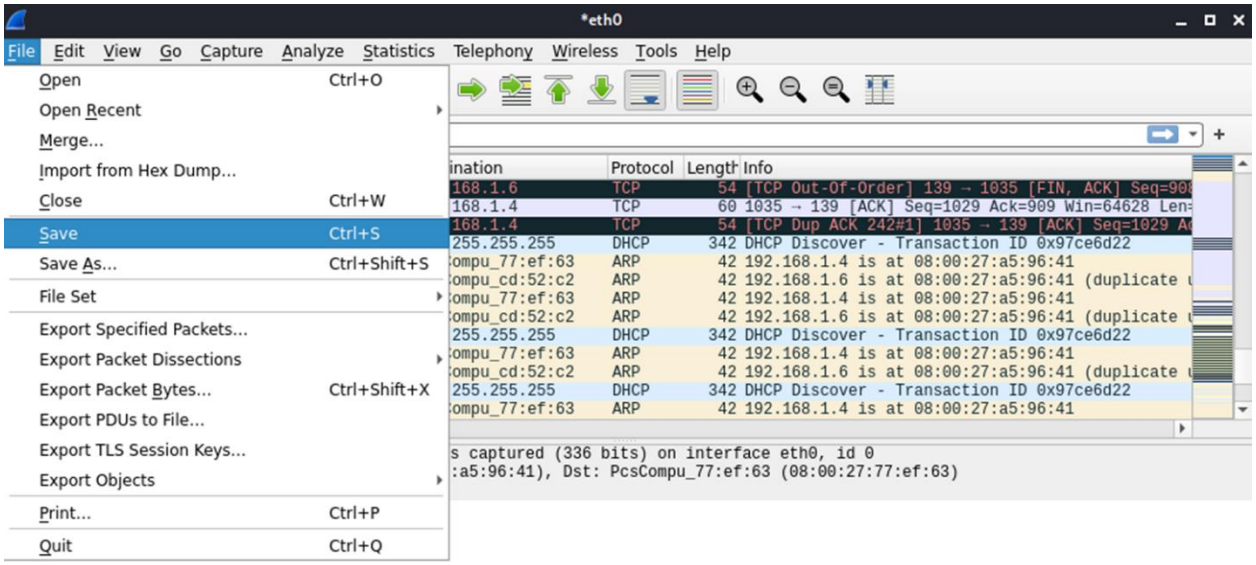
`

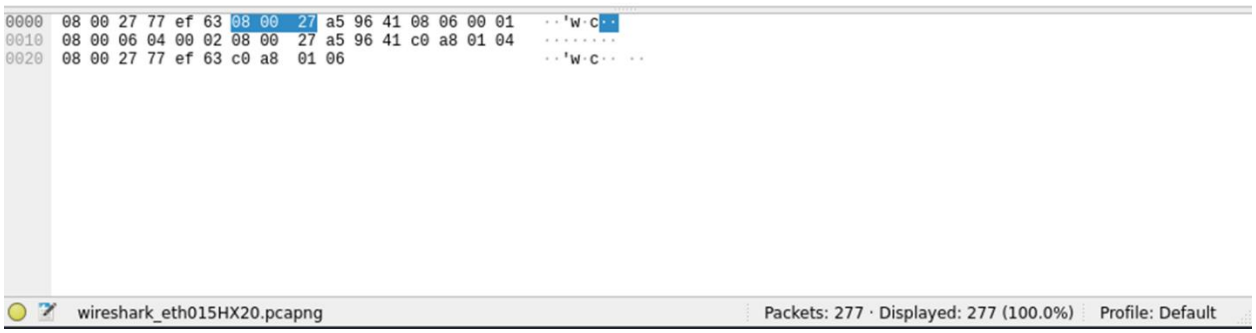
23. Click the stop button to stop capturing packets.



`

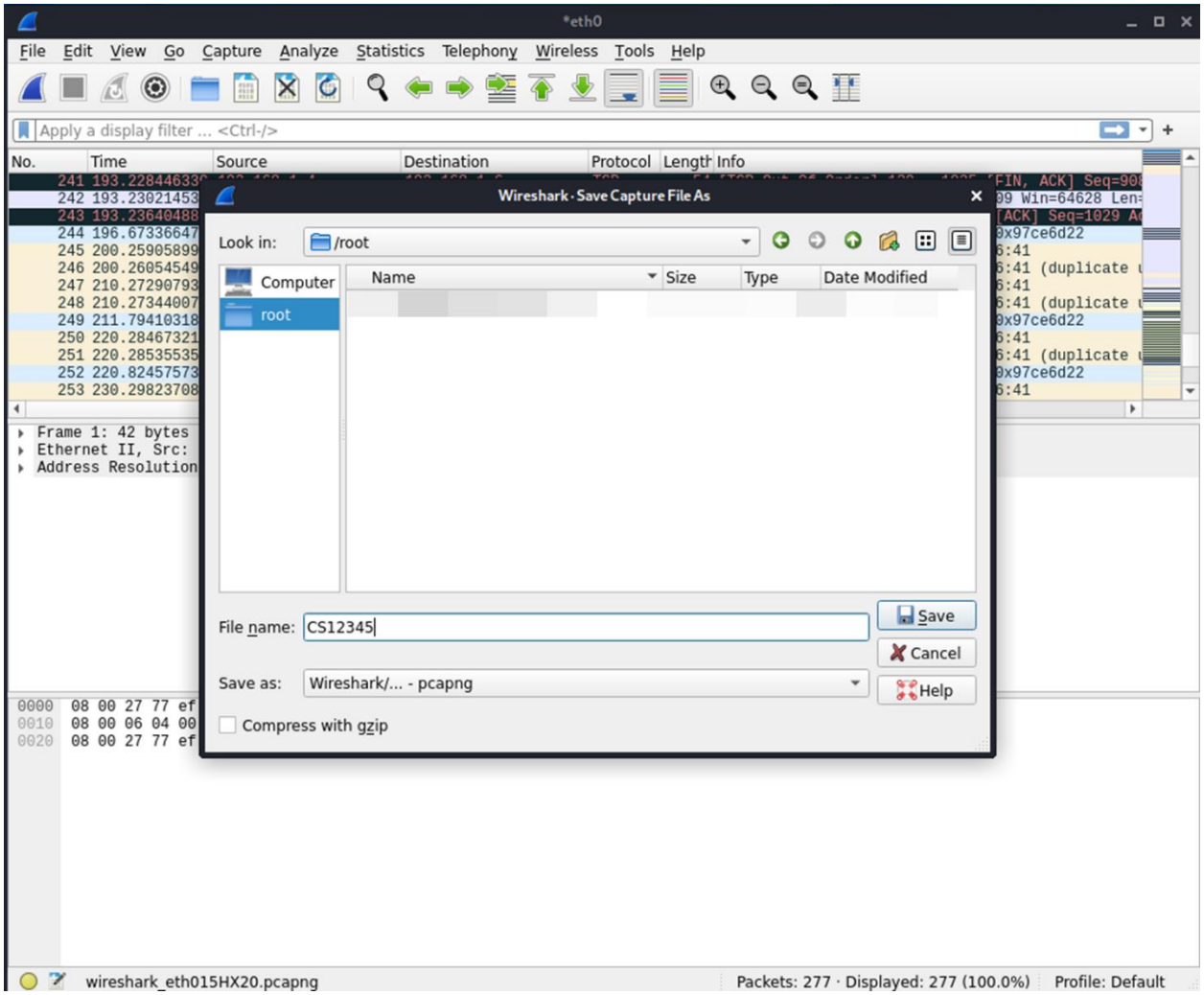
24. We are going to save the output to a file with a **.pcap** extension. Follow the step as shown in the screenshot below:





`

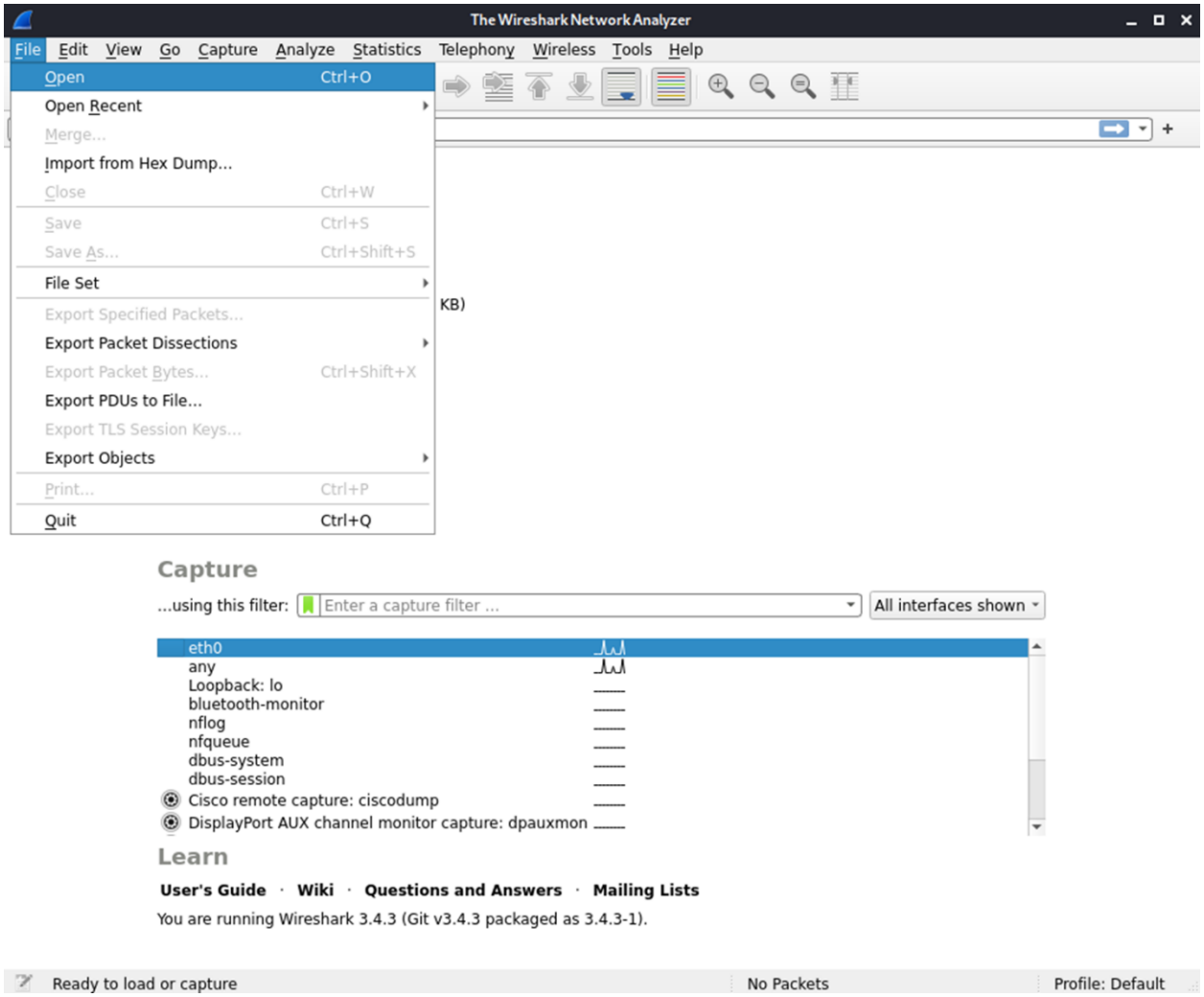
25. Put your matric number as the filename. Take a screenshot of this activity and put it into your lab report. Click **Save**.



26. Now, close and re-run the Wireshark software.

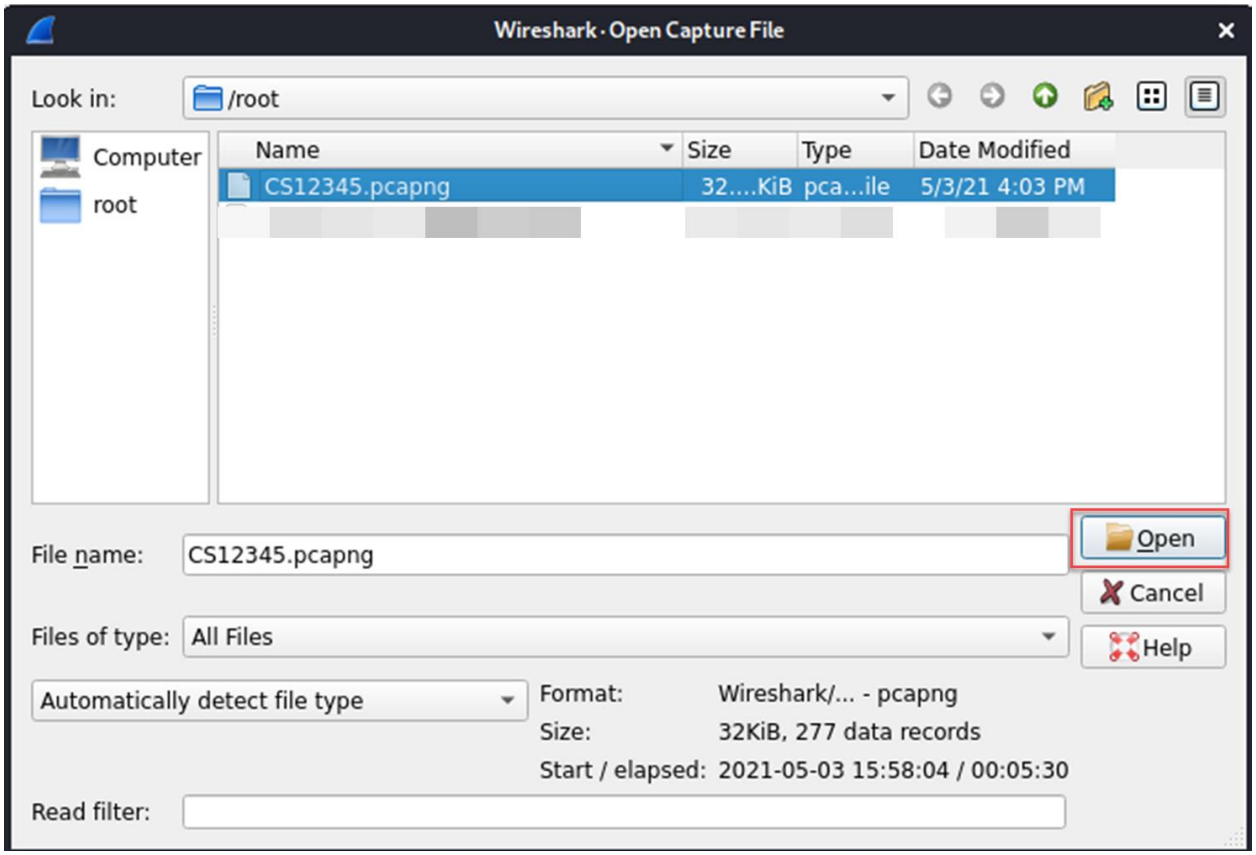
`

27. This time we are going to open the file as we save earlier. Click **File>Open**.



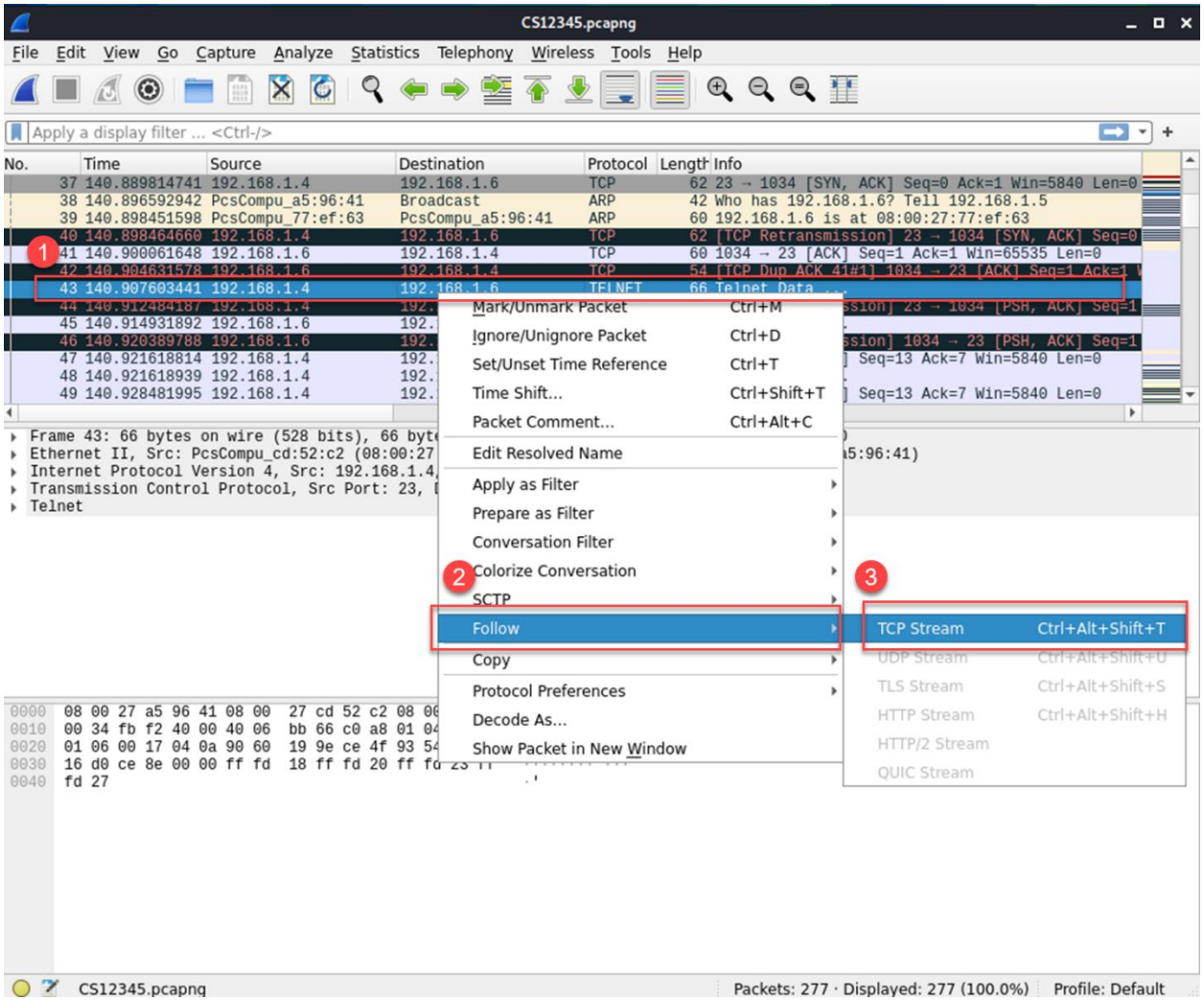
`

28. Select the **.pcap** file that has been saved with your matric number as the file name. Click **Open**.



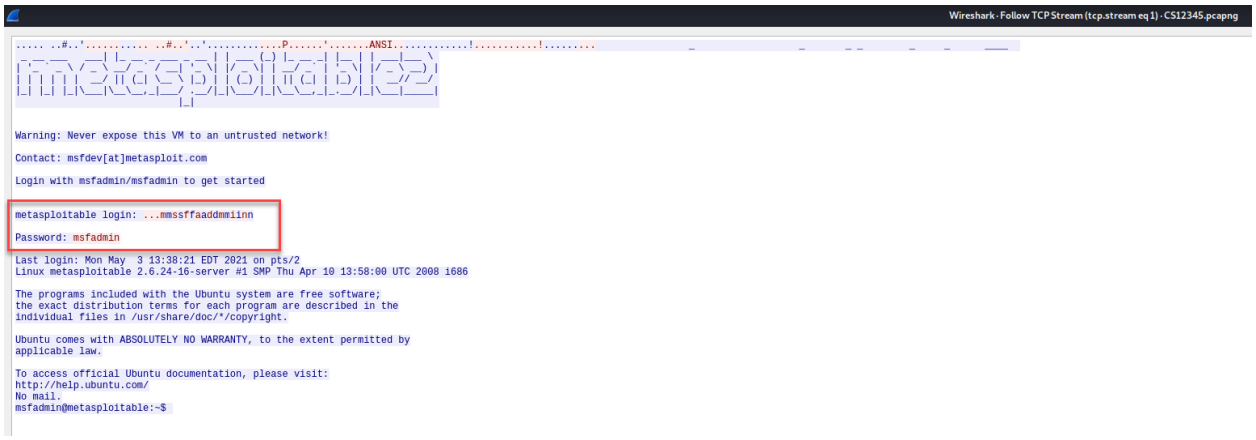
`

29. You will series of output (which is the same as before). Now, execute the steps below to follow the TCP stream of the telnet activity done in the victim's machine before.



`

30. Finally, you will see the result of the TCP streams following. At this moment, the attacker can see the login and password in a clear form. Those input has been inserted during the telnet session from the victim's machine to Metasploitable. The attacker wins!



REFLECTION QUESTIONS

1. In your own words, explain ARP poisoning.
2. How can we prevent the ARP poisoning attack?
3. Why do you think telnet is not a safe way to connect to a remote machine? What is the safer way to do so?

`

TASK 3: ANALYSING THE NETWORK PACKET

OBJECTIVE

To analyse the network packet using multiple tools

TASK DESCRIPTION

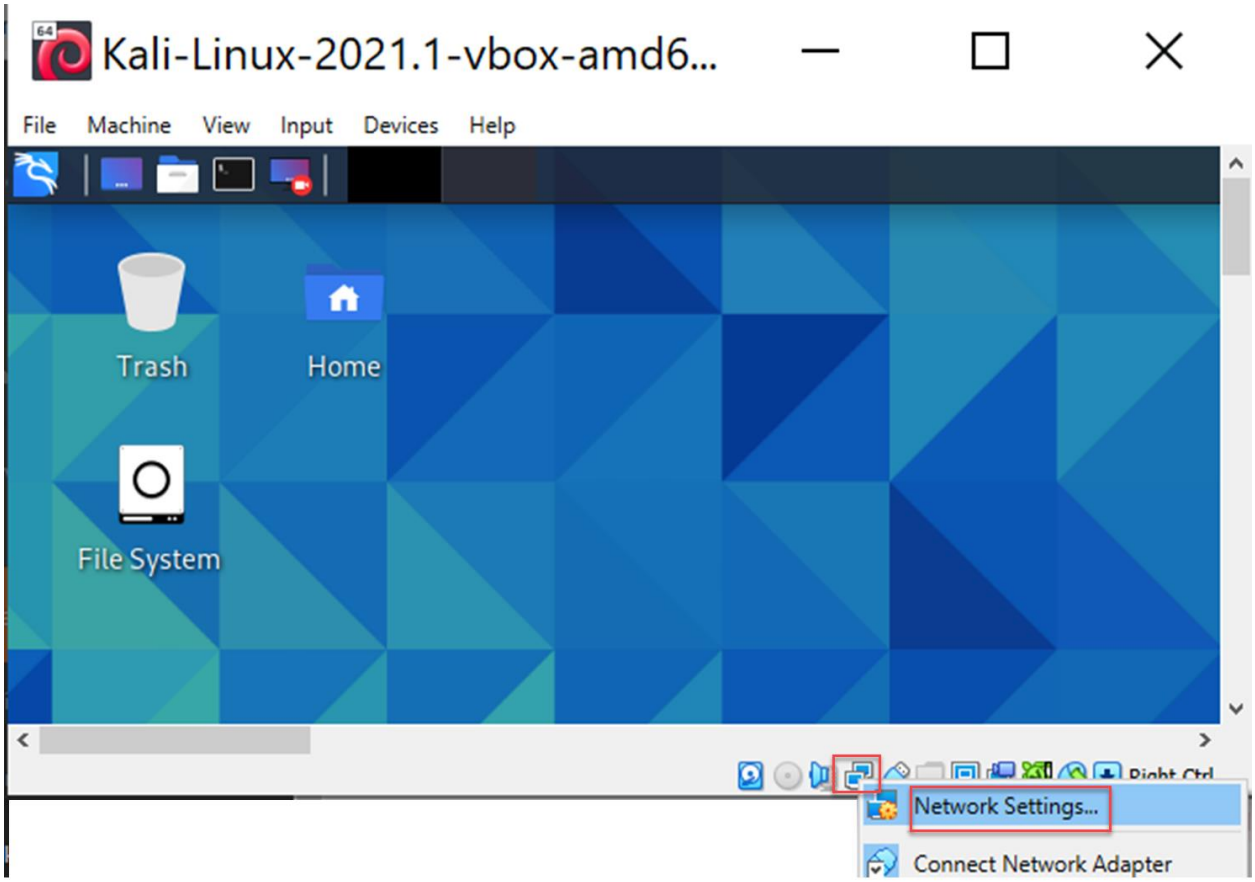
For this task, student needs to run packet analysis tools from various sample taken from the provided website.

ESTIMATED TIME

60 Minutes

STEPS:

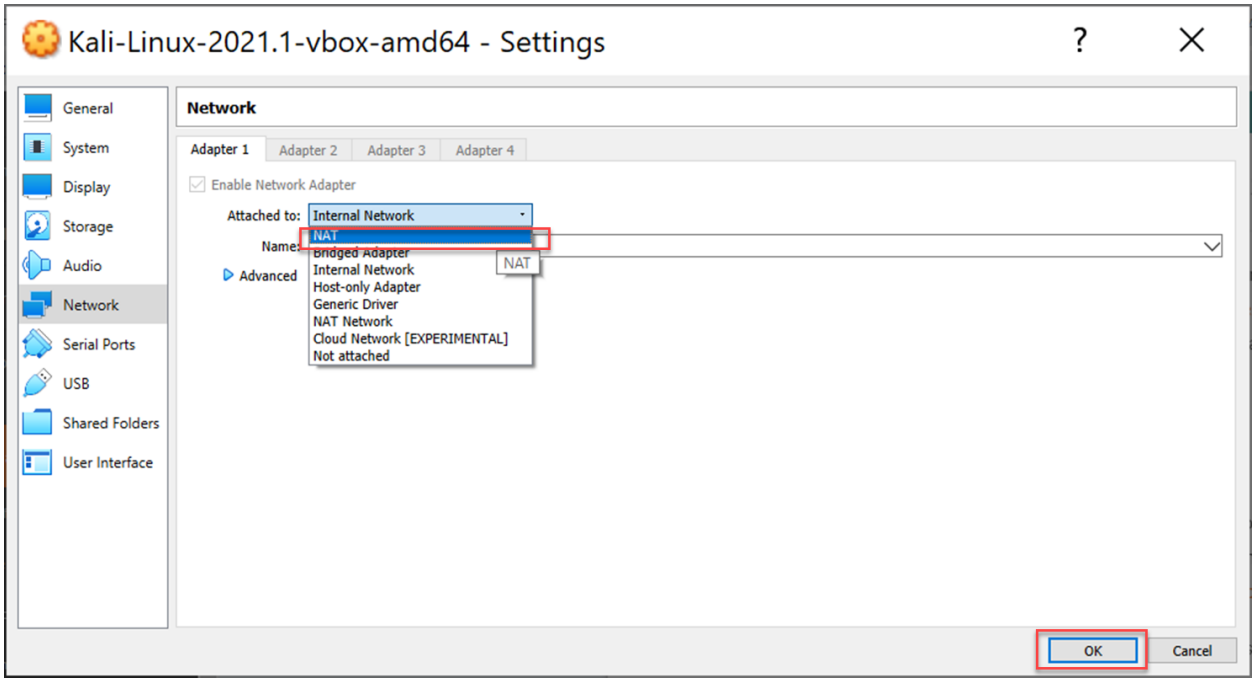
1. At the Kali Linux virtual machine, we are going to change the network from internal to NAT. Click the icon and choose **Network Settings…**



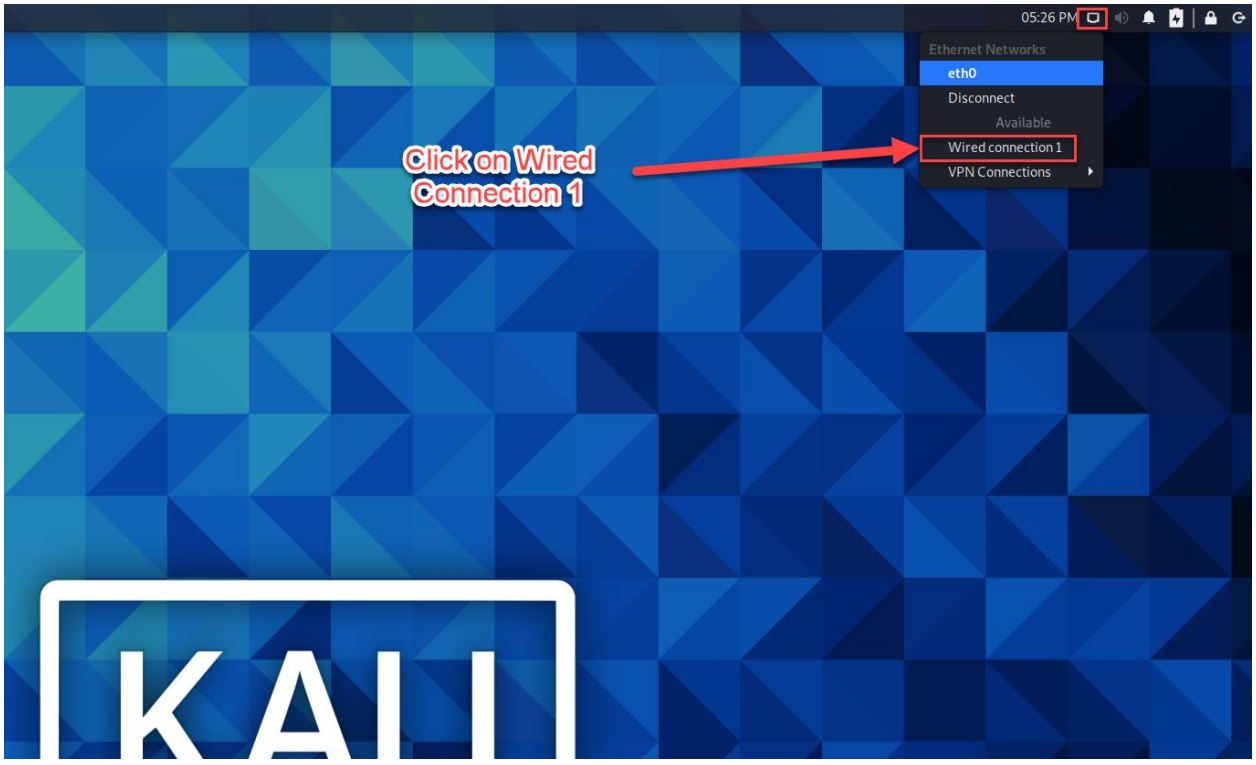
`

`

2. Change the network from internal to NAT. Click **OK**.

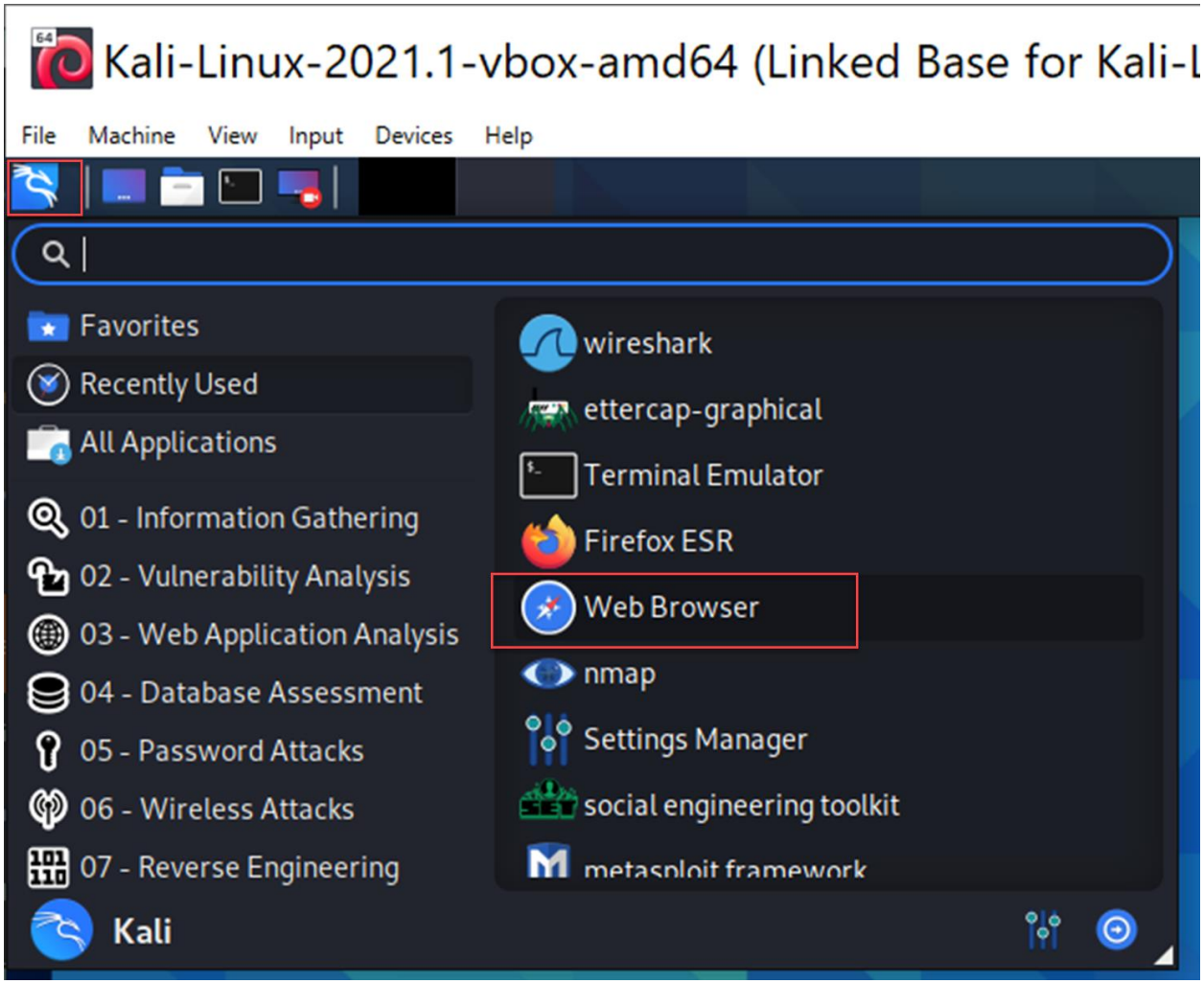


3. Next, click on the network icon in Kali Linux, then choose **Wired connection1**.



`

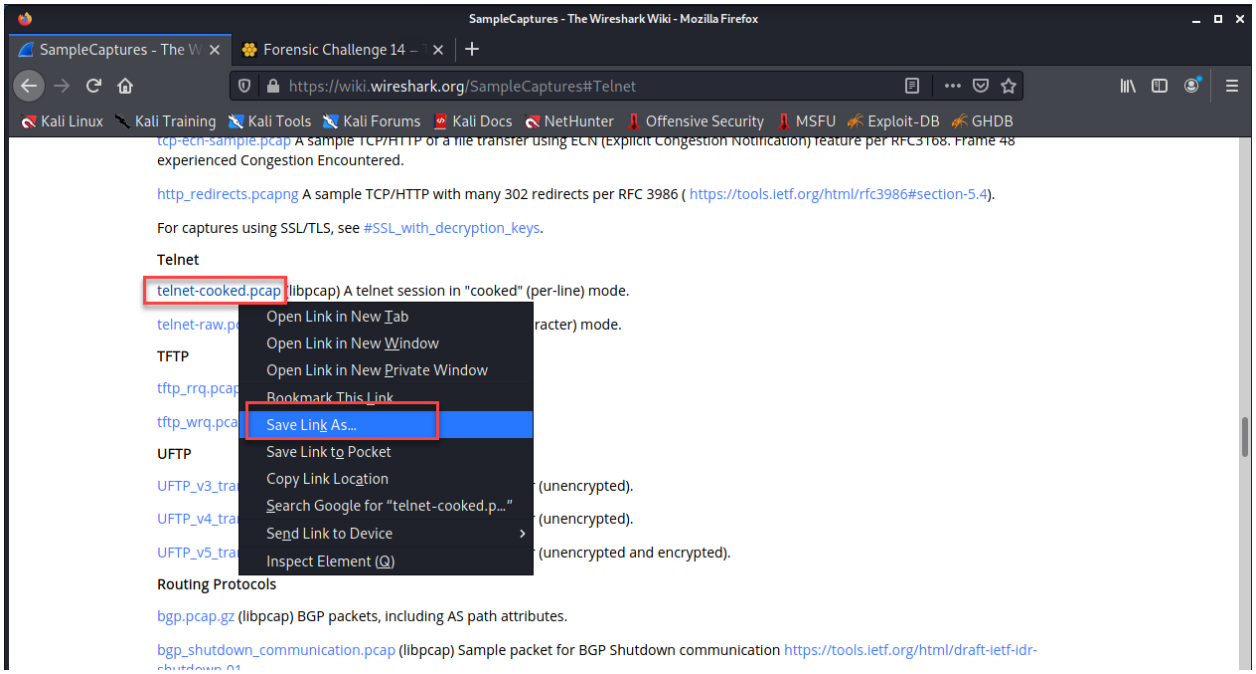
4. Then, open a browser.



5. At the URL bar of the browser, type https://wiki.wireshark.org/SampleCaptures#Telnet and click + sign to open a second tab. On the second tab, type https://www.honeynet.org/challenges/forensic-challenge-14/

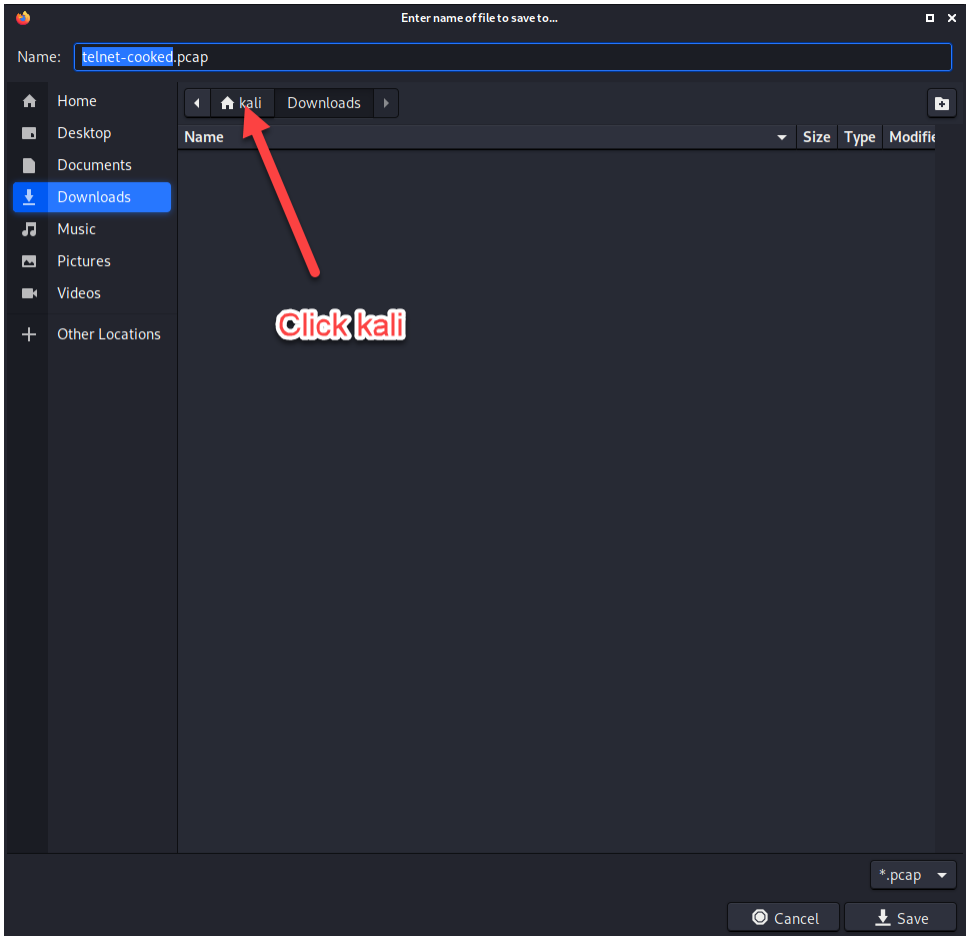
`

6. At the first tab, right-click on **telnet-cooked.pcap** then choose **Save Link As...**

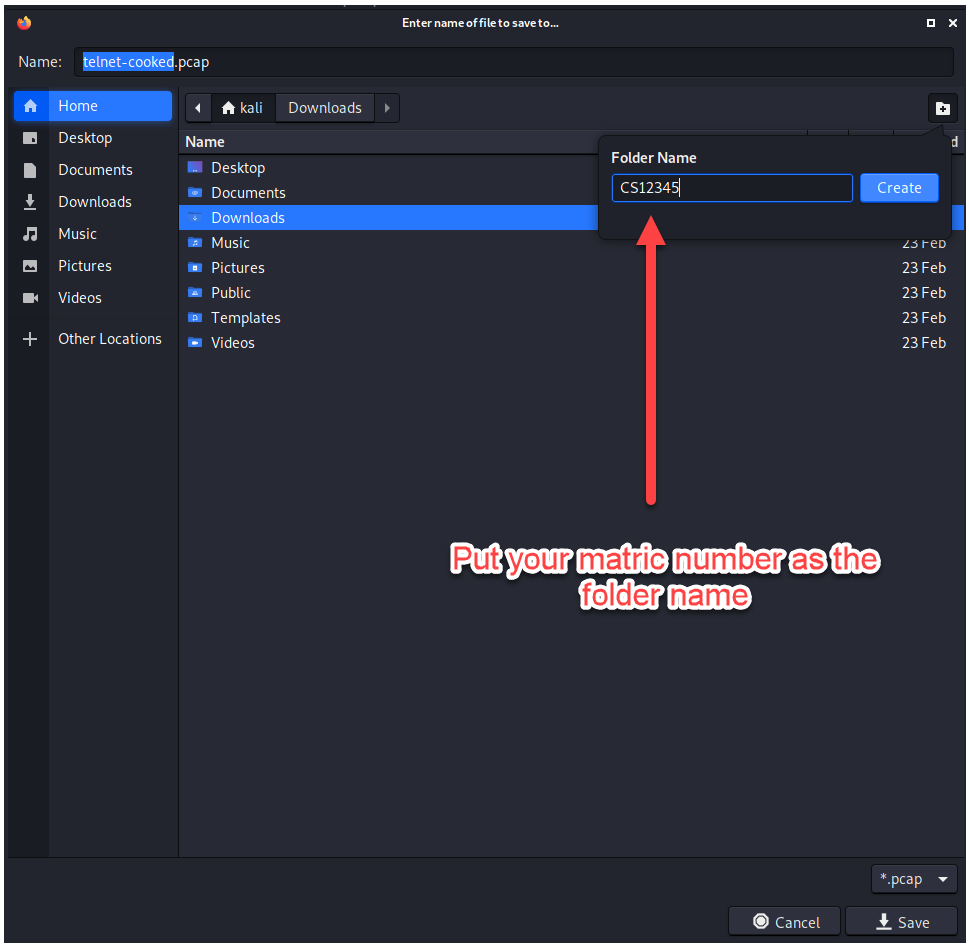


`

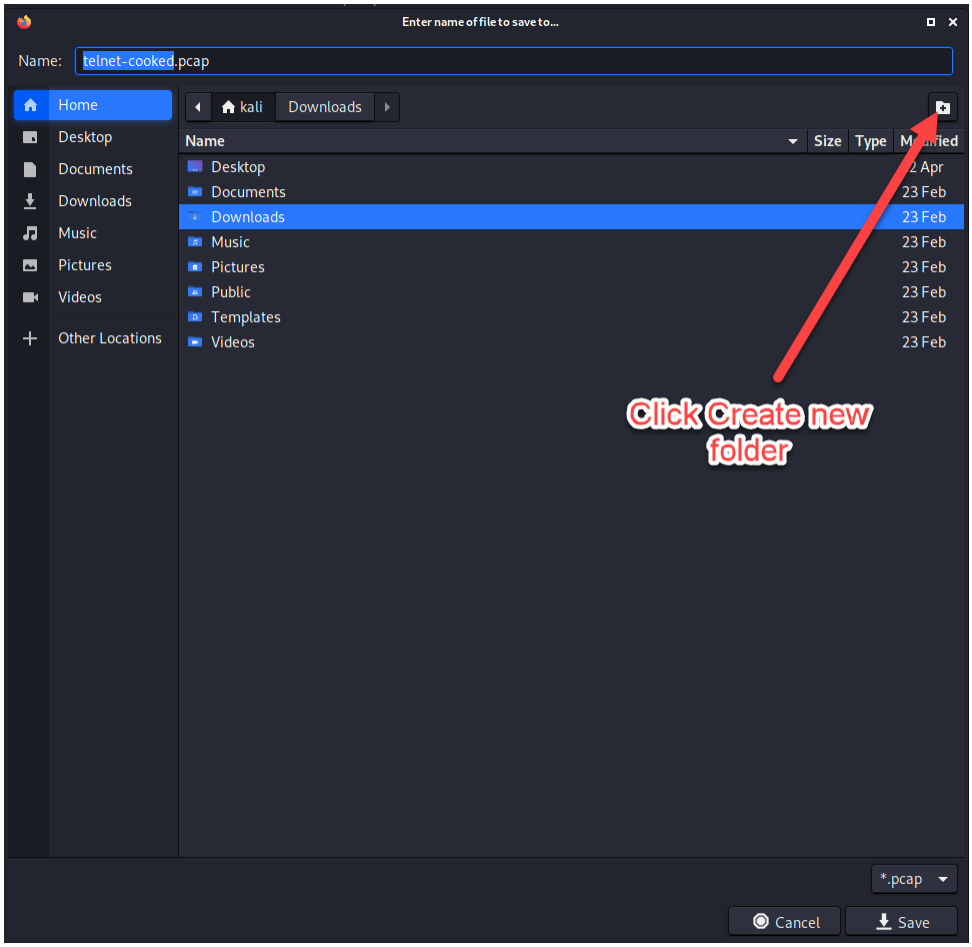
7. Follow the steps below to create a new folder with your matric number as its name and save the above file.



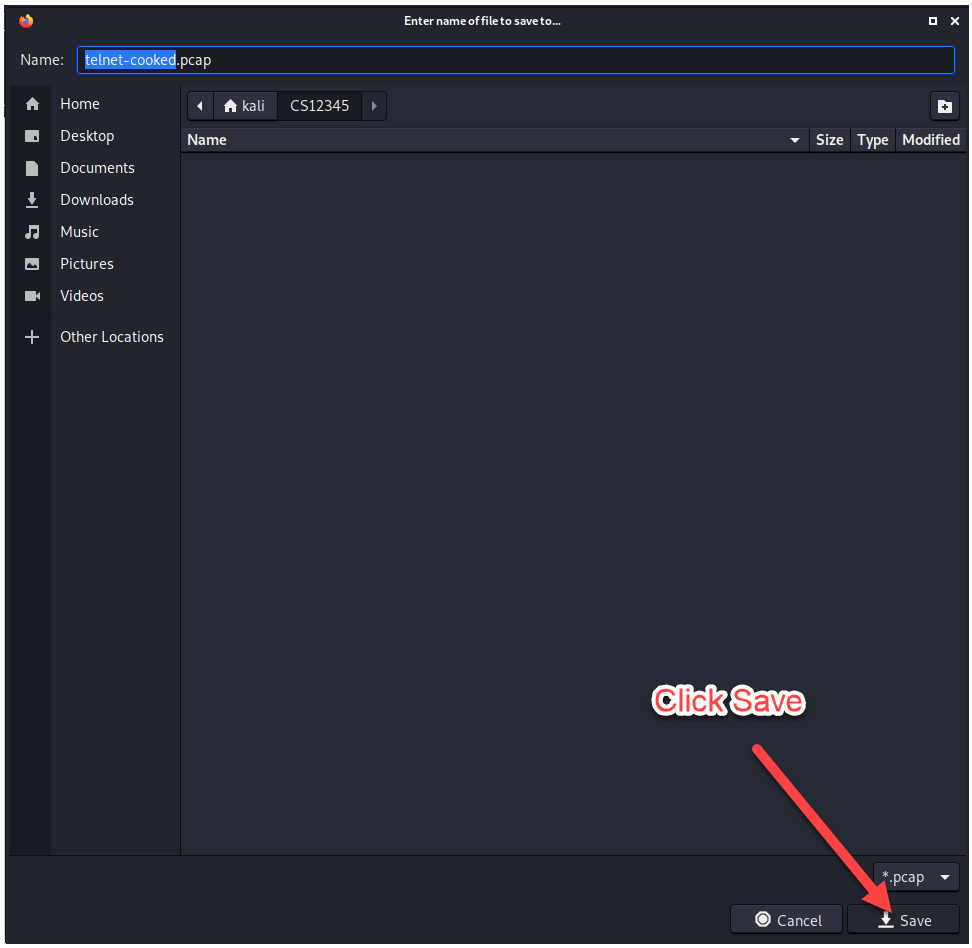
`


Enter name of file to save to...
Name: telnet-cooked.pcap
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Other Locations
kali
Downloads
Name
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
23 Feb
23 Feb
23 Feb
23 Feb
Folder Name
CS12345
Create
Put your matric number as the folder name
*.pcap
Cancel
Save

`

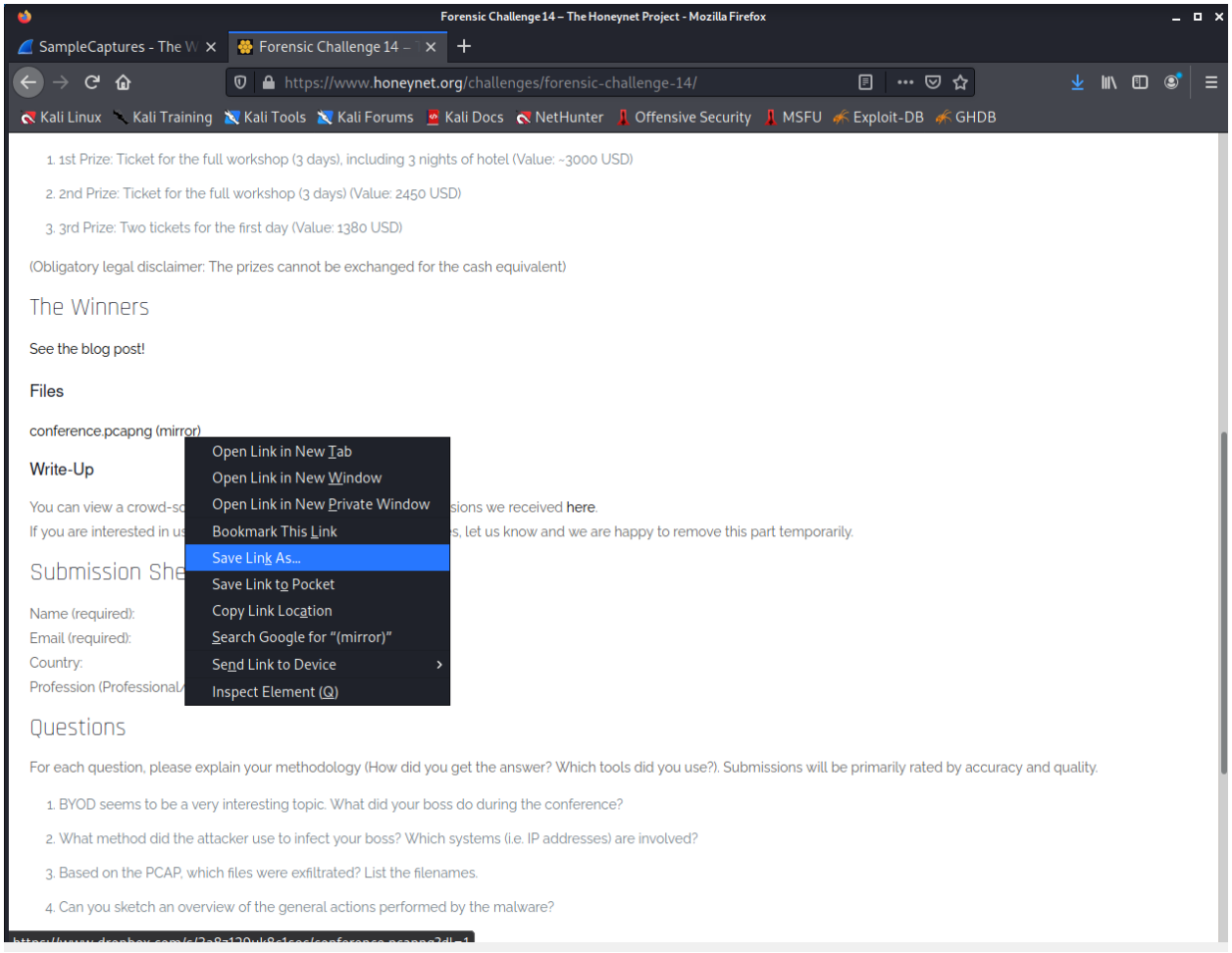

Enter name of file to save to...
Name:
telnet-cooked.pcap
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Other Locations
kali
Downloads
Name
Size
Type
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
23 Feb
Click Create new folder
*.pcap
Cancel
Save

`


Enter name of file to save to...
Name:
telnet-cooked.pcap
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Other Locations
kali
CS12345
Name
Size
Type
Modified
Click Save
*.pcap
Cancel
Save

`

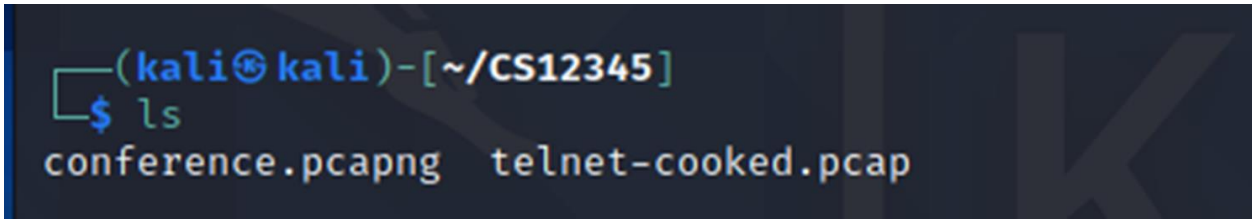
8. Next, we move to the next tab, with the second file. This time use the same folder as created before.



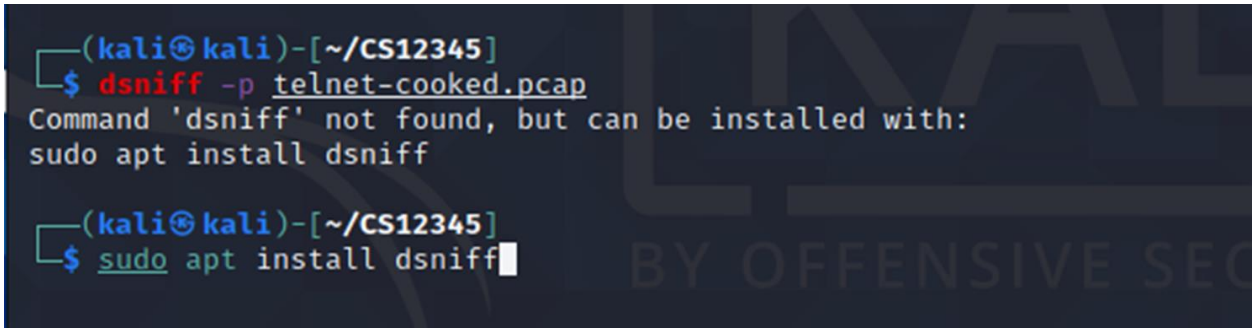
`

9. After finish downloading those file, open the terminal in Kali Linux. Follow the following commands. The second command is to change the current directory to the folder we created to save the downloaded files.

10. When we list the content of the folder, we can confirm two files are available.

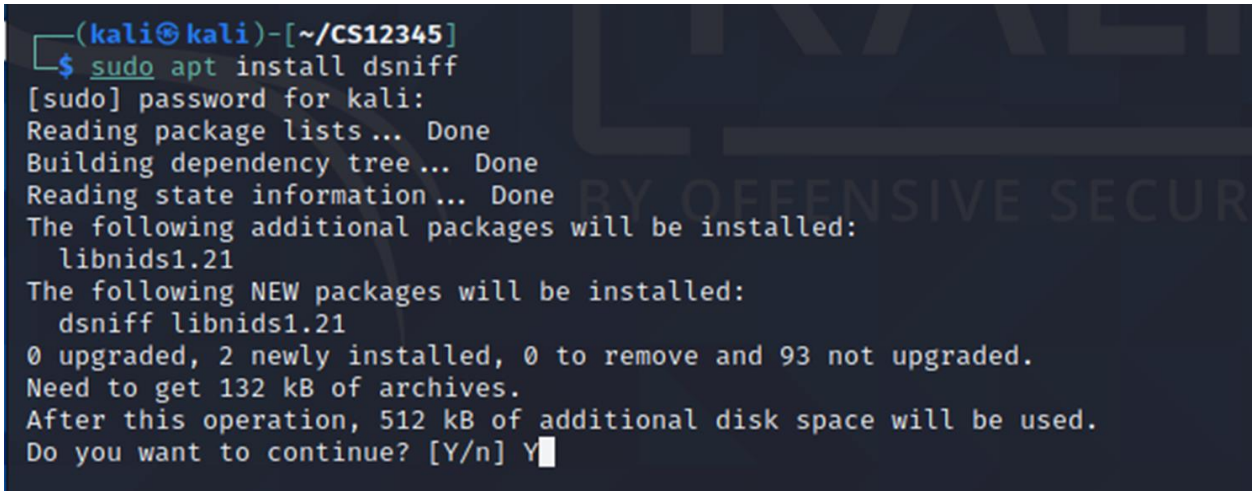


11. Next, we are ready to experiment with the first packet analyser tools known as **dsniff**. Like Wireshark, Dsniff is also used to capture packets and now we are going to use it to reassemble and view the plaintext transactions that took place in an offline PCAP file that we have downloaded before. In the beginning, you may find that some of the tools are not available in Kali Linux by default, so we need to download and install them manually. Follow the command shown in the screenshots.

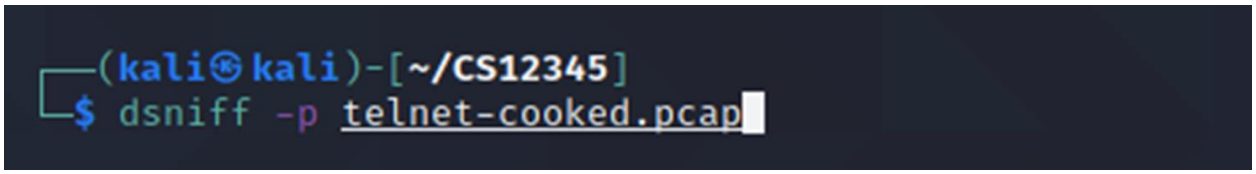


`

12. Choose **Y** to proceed with the installation. Wait until the installation finish.



13. After the installation finish, re-run the command and put the .pcap file as the parameter. As the output, you will see communication between two devices. Save the screenshot of the output and put it into your lab report.



14. Next, we are going to use the second tool known as tshark. The following command will give us a copy of each web browser used to visit per unique website. Again, save the portion of the output screenshot in your lab report.
Note: For the rest of the commands below, take a screenshot of every output.

15. The following command will extract all the files that were transferred using the HTTP protocol. The result will save in a folder named tshark_folder.

`

16. To verify the content of the folder, type the **ls -l** command.

```
┌──(kali㉿kali)-[~/CS12345]
└─$ ls -l tshark folder
```

17. The last tools we are going to experiment with is the **urlsnarf**. Urlsnarf is used to sniff HTTP requests from live network traffic and also offline **.pcap** files. This tool can help us determine which websites were visited by the clients on a network.

```
┌──(kali㉿kali)-[~/CS12345]
└─$ urlsnarf -p conference.pcapng | grep "http://" | cut -d "/" -f 5
```

18. Finally, we can use other options in urlsnarf to determine the user agents (which refer to the client's web browser) that are used during the communications. By using the following command, we can remove duplications and sort our output.

```
┌──(kali㉿kali)-[~/CS12345]
└─$ urlsnarf -p conference.pcapng | grep "http://" | cut -d '"' -f 6 |sort -u
```

REFLECTION QUESTIONS

1. Based on your understanding, what is a network security and what are the basic objectives of network security?
2. Differentiate between Intrusion Detection System (IDS) and Intrusion Prevention System (IPS).
3. Why Virtual Private Network (VPN) is important for network security?
4. In what situation you might want to install a Demilitarized Zone (DMZ) on your network?
5. What is the role of Network Address Translation (NAT) on a network?
6. To applied and manage the security principle, you must understand how the network devices and technologies operate. Explain how the proxy server operates to provide security on the network.