Network Penetration Testing

Laboratory 02: Wireshark

First name: Jakub Last name: Oźmina

Index number: 156158 Exercise date: 16.10.2025

Used Lab equipment:

Group members:

Report submission

The document containing the exercise instructions includes active text fields where answers to the provided questions must be entered. As a result, once all answers are filled in (along with personal information of the individual completing the exercise), the document transforms into a report. It's recommended to open the file using Adobe Acrobat, or browsers such as Firefox or Chrome.

If you wish to maintain the functionality of the text fields after saving the file (allowing for future changes), avoid selecting the 'print to PDF' option when saving the file to your disk. For added safety against potential loss of entered data due to system crashes, save the file periodically.

Final report should be composed of the following files:

000000_NPT_02.pdf (student ID: 000000, Lab number 02) - main report file (this file)

The report should be uploaded to Moodle no later than the fifth day after the end of the exercise.

Introduction

The objective of this exercise is to familiarize students with Wireshark [1]. Wireshark functions as a packet analyzer. This entails its capability to intercept and analyze packets that are sent and received by a network card (both incoming and outgoing frames). This software is compatible with a wide range of commonly used protocols (such as IP, TCP, UDP, ARP, ...). It boasts a user-friendly graphical interface that is straightforward to navigate. Wireshark proves to be a convenient utility for dissecting protocols and pinpointing network issues. It serves as an ideal instrument for supporting penetration testing endeavors. It is crucial to emphasize that employing Wireshark to surreptitiously monitor network traffic produced by other users, outside of scheduled testing scenarios, is a **VIOLATION of the law!!!**

Wireshark is freely available and can be accessed within the Kali Linux virtual machine that was set up in the preceding exercise. Furthermore, Wireshark is compatible with Windows as well as a variety of Unix platforms.

Lab scenario

1 Run lab enviroment

The exercise will use the virtual test environment prepared during the first exercise consisting of four virtual machines: Kali Linux (KL) [2], Metasploitable 3 (MST3) [3], Metasploitable 2 (MST2) [4] and Jangow (J) [5]. These machines

The project "Cyber Security for the European University EUNICE", implemented under the National Academic Exchange Agency's Strategic Partnerships Programme. Implemented in cooperation between the Poznan University of Technology and the University of Catania, University of Mons, and Brandenburg University of Technology.

are connected in an internal network according to the diagram shown in Figure 1. The machines use an automatic TCP/IP configuration and the Virtual Box acts as the DHCP server. The Wiershark will be run on machine KL.

For PCs with less computing power, you can only run two machines: Kali Linux and a test machine of your choice (preferably running Metasploitable 3).

Once the virtual machines have started, the test environment is ready to run.

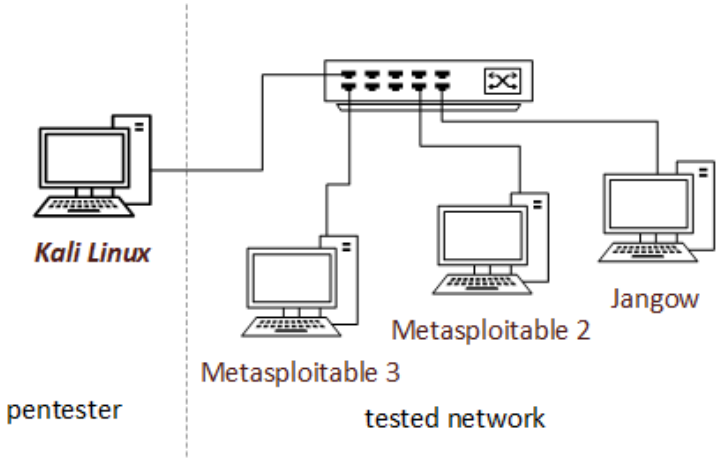

Figure 1: Virtula netwtowk

2 Kali Linux network configuration

Log in to Kali Linux (login: kali, password: kali), start the terminal (command line) and use the `ifconfig` command to check the IP address of this machine. In the text box below, write down the IP address, mask and gateway address of the default Kali Linux machine:

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.100.10  netmask 255.255.255.0  broadcast 15
```

3 Start Wireshark

Run the Wireshark programme (search for Wireshark from the list of available programmes lb also run a terminal, type Wireshark and then click the Enter key). When you start the program, you will see the window shown in Figure 2. In the main part of the programme window, you can select:

A the capture filter (so that only packets meeting the specified condition will be captured by Wireshark);

B interface from which packets will be captured (physical and virtual interfaces are available). It is important to select the interface through which the computer connects to the tested network.

The meaning of the individual icons (see Fig. 3) is as follows:

1. start capture (Start),
2. stop capture (Stop),
3. restart capture,
4. capture options,
5. open the file with the captured packets,

The project "Cyber Security for the European University EUNICE", implemented under the National Academic Exchange Agency's Strategic Partnerships Programme. Implemented in cooperation between the Poznan University of Technology and the University of Catania, University of Mons, and Brandenburg University of Technology.

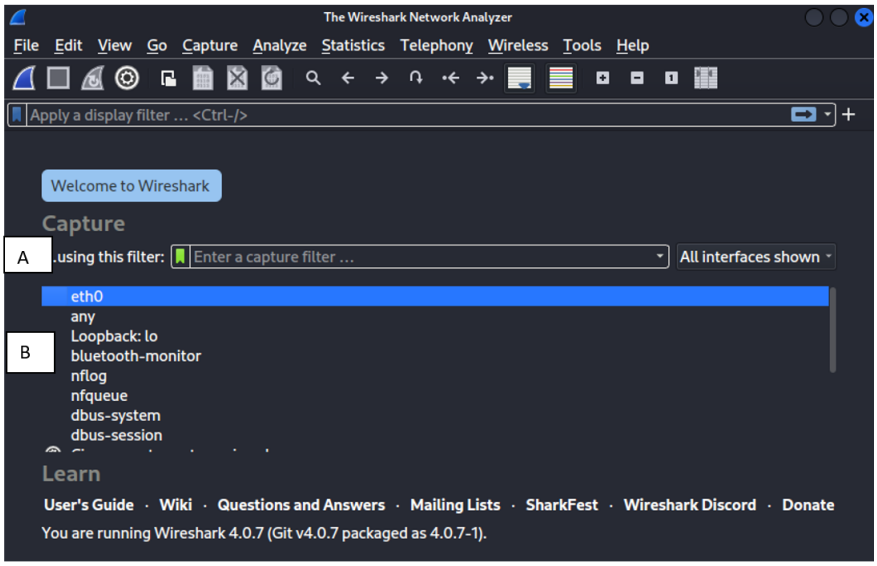

Figure 2: Wireshark mian window

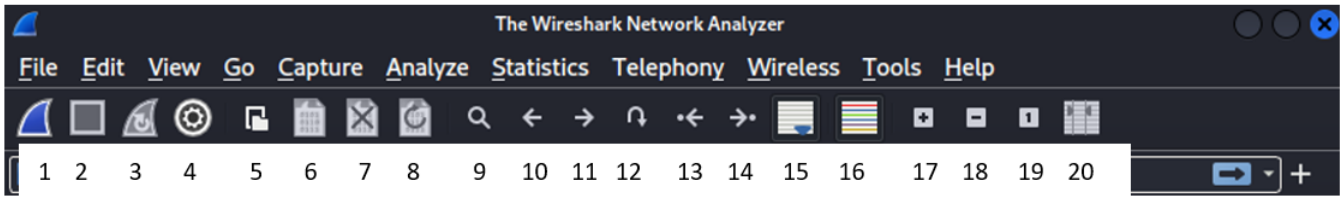

Figure 3: Wireshark - toolbar

6. save captured packets to file,
7. erase captured packets (close file) - restores the program startup window,
8. refresh,
9. find package,
10. go to previously viewed package (in viewing history),
11. navigate to next (in browsing history) viewed package,
12. navigate to package number ...,
13. go to the first package,
14. go to the last package,
15. autopropagate captured packages,
16. colour the packets (depending on protocol),
17. enlarge font,
18. reduce font,
19. initial settings,
20. adjust width of columns to current font size.

The project "Cyber Security for the European University EUNICE", implemented under the National Academic Exchange Agency's Strategic Partnerships Programme. Implemented in cooperation between the Poznan University of Technology and the University of Catania, University of Mons, and Brandenburg University of Technology.

To start capturing packets, after starting Wireshark, select the interface (or interfaces) from which packets will be captured. You can also select an interface by clicking on icon 4 (Figure 3). After clicking, a window with a list of available interfaces will appear, from which you must select the one on which traffic is to be analysed (Figure 4).

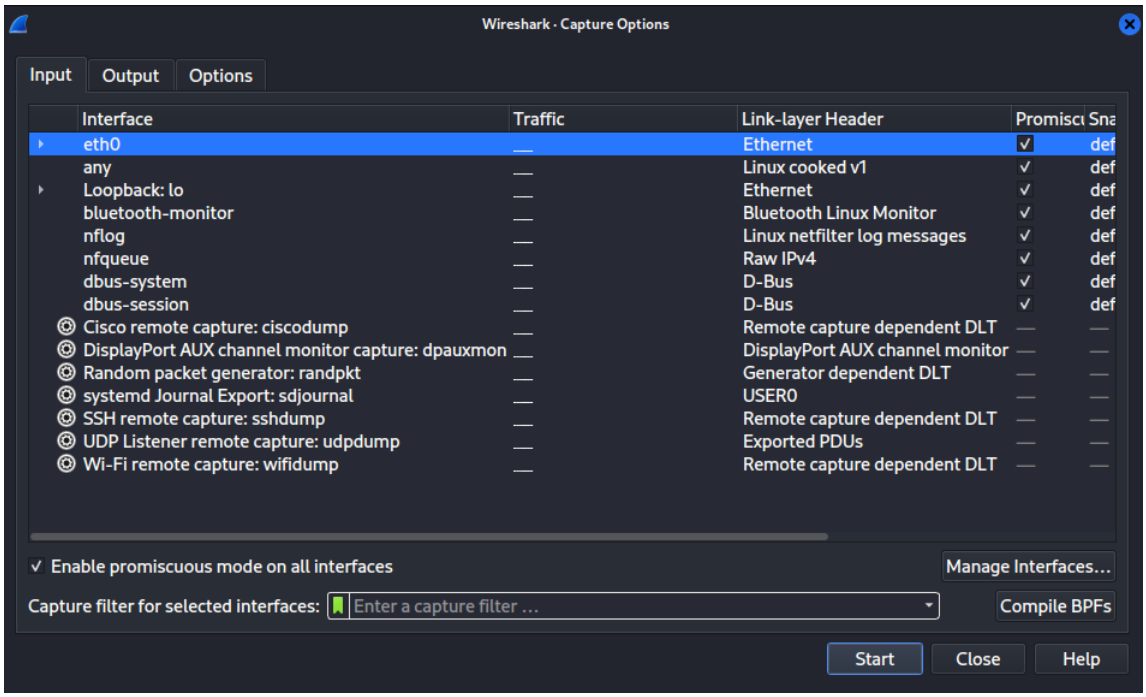

Figure 4: Interface selection window

By clicking on the Start button (icon 1, Figure 3), you can start capturing immediately. It is worth noting that the interfaces from which packets will be captured only need to be selected once. If the user chooses not to start the packet capture from the interface list window, he/she can do so using, for example, icon 1 (Figure 3). The capture can be stopped by clicking on icon 2 (Figure 3) or by selecting the Capture menu and choosing the appropriate option. When the capture is running, the programme window changes appearance (see Figure 5). The Wireshark window is devided into four parts:

1. display filter field - indicates the criterion for displaying packets (if the background of the field is green, the criterion is correct, e.g. to display only ICMP protocol messages, enter icmp and click on the arrow at the end of the filter field; if the filter is correct, the field will turn green),
2. list of intercepted packets,
3. content of the selected package,
4. the packet field - indicates by highlighting the 2 elements of the packet selected in the window (presented in hexadecimal system).

4 Analysis of captured packets

Once the capture has stopped, you can start analysing packets. In order to display only those packets which you want to view, enter the appropriate filter rule in the display filter field, e.g. if you want to display packets sent as a result of a ping command call, enter icmp in the filter field. Figure 6 shows a packet with an ICMP protocol message. Analysing the data presented in Figure 6, we can easily see that the data packets were transmitted according to the IP v4 protocol, the TTL parameter (specifying the packet lifetime expressed in number of hops) is equal to 64, while the type of message transmitted is Echo request.

The project "Cyber Security for the European University EUNICE", implemented under the National Academic Exchange Agency's Strategic Partnerships Programme. Implemented in cooperation between the Poznan University of Technology and the University of Catania, University of Mons, and Brandenburg University of Technology.

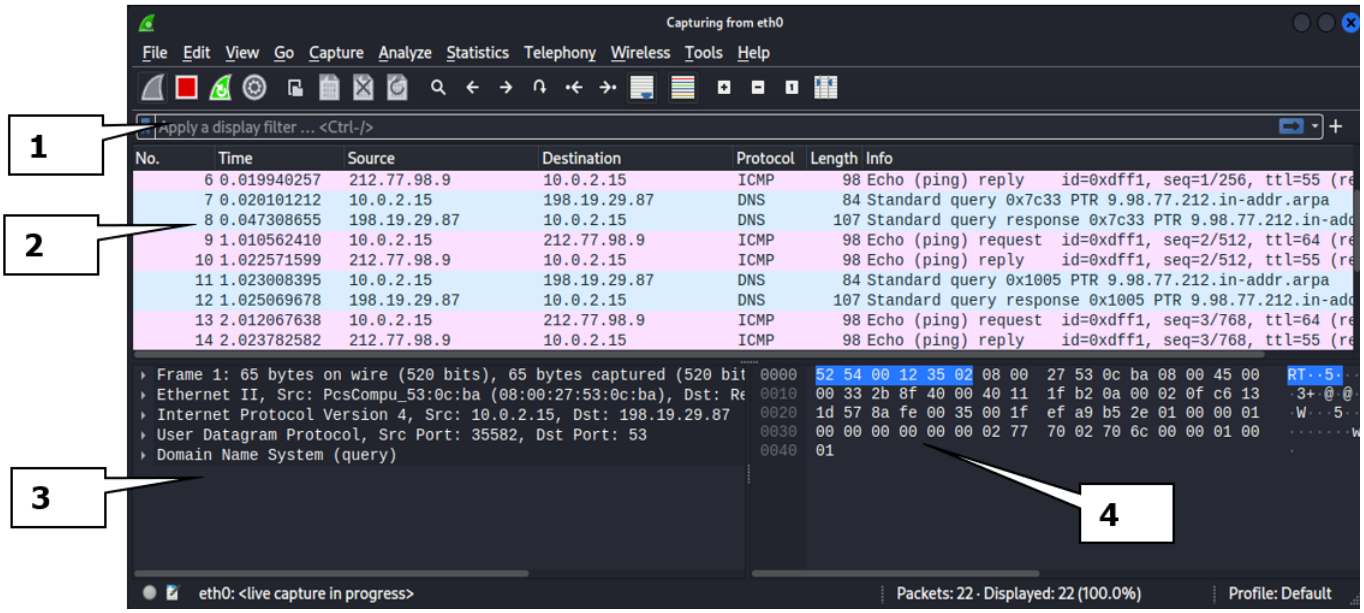

Figure 5: Wireshark – captured packets

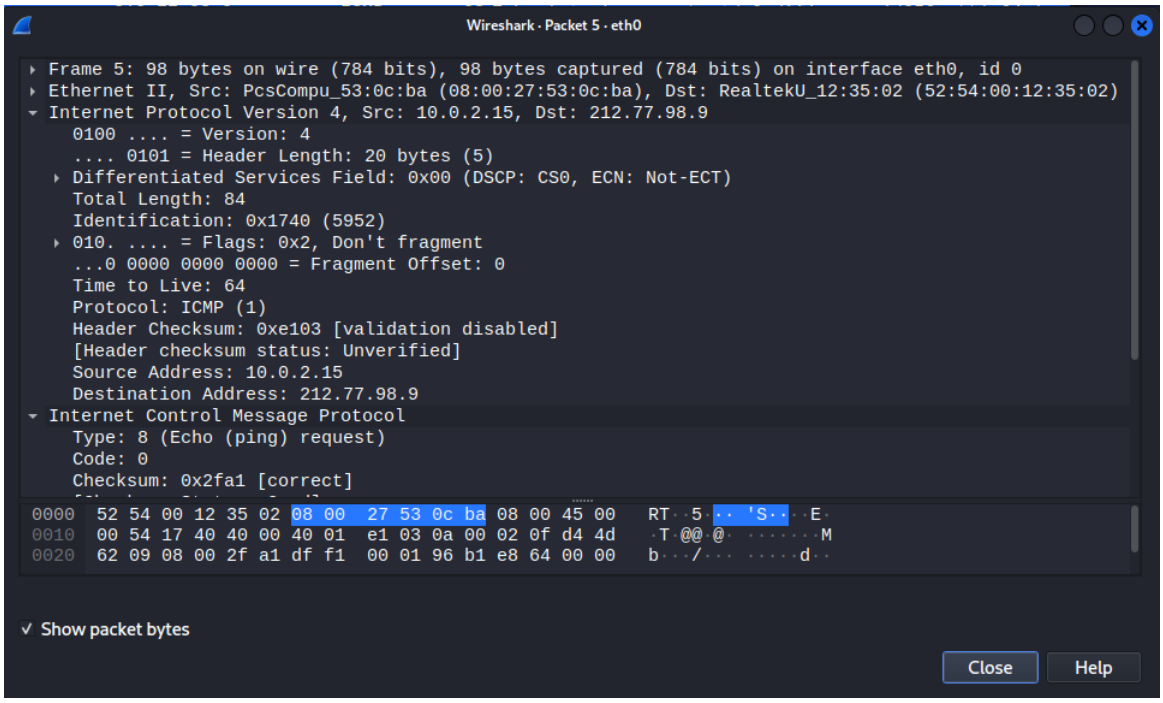

Figure 6: packet analysed

Wireshark generates a number of statistics (Statistics menu). This program can also present packet exchange between the host on which it is installed and the remote host in graphical form (Statistics->Flow graph menu). A graphical representation of ICMP message exchange (ping command) is shown in Figure 7. Figure 8, in turn, shows information on the length of the intercepted packets.

The project "Cyber Security for the European University EUNICE", implemented under the National Academic Exchange Agency's Strategic Partnerships Programme. Implemented in cooperation between the Poznan University of Technology and the University of Catania, University of Mons, and Brandenburg University of Technology.

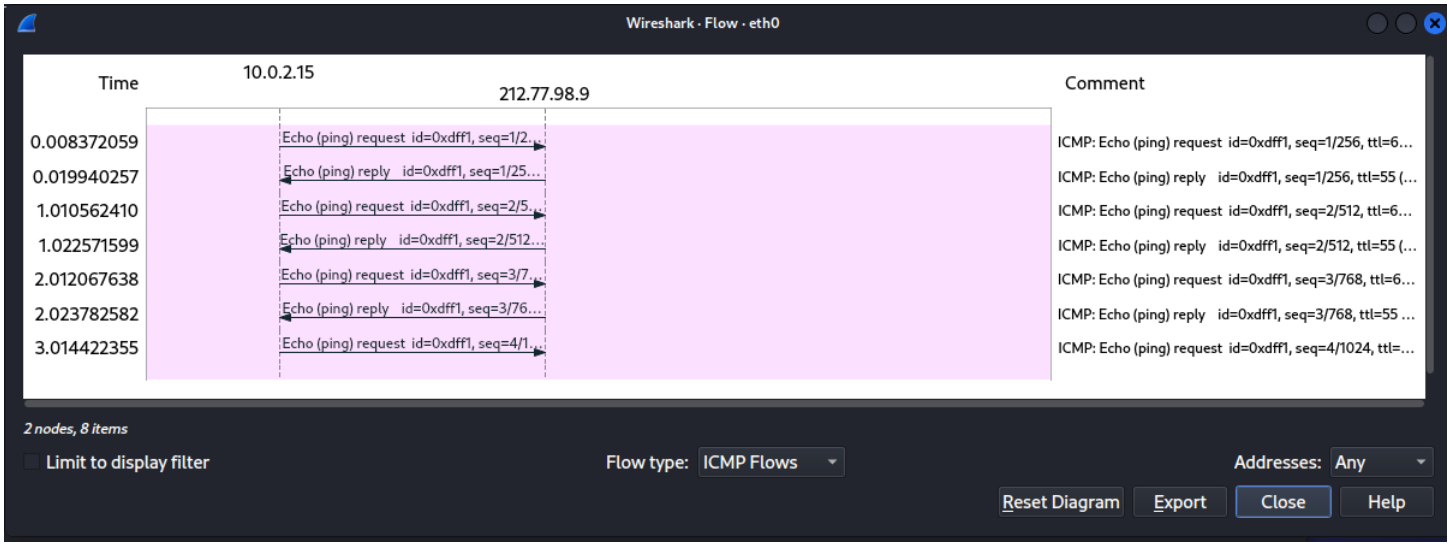

Figure 7: Flow graph

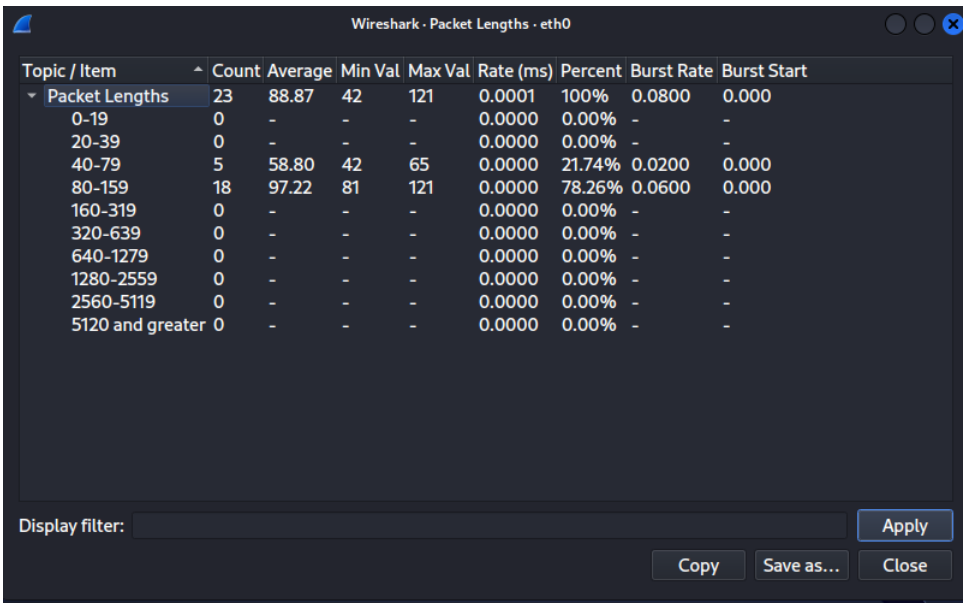

Figure 8: Packet lengths

5 Exercise 1 - Analysis of the operation of the netdicover command

Start packet capture on the interface that connects the KL machine to the virtual test network. Restart the netdiscover program. When all devices are detected, disable the capture and analyse the captured packets. Is it possible to determine the method that netdiscover uses to detect devices from the captured packets?

The project "Cyber Security for the European University EUNICE", implemented under the National Academic Exchange Agency's Strategic Partnerships Programme. Implemented in cooperation between the Poznan University of Technology and the University of Catania, University of Mons, and Brandenburg University of Technology.

Yes it is possible it uses ARP packets

6 Exercise 2 - Analysis of the operation of the ping command

Start packets capture and enter icmp in the capture filter field. In a terminal window, type the command ping address_IP (where IP address is the address of one of the detected virtual machines). After capturing several icmp messages, stop capture and abort the ping command. Answer the questions:
What ICMP protocol messages were received?
Do the TTL parameter values in the sent and received packets differ. Explain the situation that occurred.

What ICMP protocol messages were received?
reply, request
Do the TTL parameter values in the sent and received packets differ. Explain the situation that occurred.
yes dhcp sent max ttl while pcs use default 64 ttl

7 Exercise 3 - Offline analysis

Load the captured packets stored in the traceroute.pcapng file into the programme. What protocol do these packets relate to? Can you determine from the packets what program/network tool was the source of these packets. If not then the answer is traceroute (tracert on Windows family systems). As you can easily see, this command uses an echo request message in a similar way. Why, then, does the ping command not know the nodes through which the packets pass, but traceroute does? Analyse the captured packets against the TTL parameter (it will be helpful to display a packet flow graph). Based on the captured packets, present the idea of how the traceroute command works

The project "Cyber Security for the European University EUNICE", implemented under the National Academic Exchange Agency's Strategic Partnerships Programme. Implemented in cooperation between the Poznan University of Technology and the University of Catania, University of Mons, and Brandenburg University of Technology.

The TTL value starts low for the first packet and increases incrementally for each subsequent packet.

For each router that the packet passes through, an ICMP Time Exceeded message is returned with the TTL value from the router.

The destination sends back an ICMP Echo Reply when the TTL reaches the correct value for the final hop.

This is how traceroute maps out the entire path to the destination. Each hop's router responds with a "Time Exceeded" message, showing the intermediate node.

References

[1] "Wireshark, project webside," https://www.wireshark.org/, accessed: 2023-06-15.

[2] "Kali Linux, project webside," https://www.kali.org/, accessed: 2023-06-15.

[3] "Metasploitable 3, project webside," https://www.rapid7.com/blog/post/2016/11/15/test-your-might-with-the-shiny-new-metasploitable3/, accessed: 2023-06-15.

[4] "Metasploitable 2, project webside," https://docs.rapid7.com/metasploit/metasploitable-2/.

[5] "Jangow, project webside," https://www.vulnhub.com/entry/jangow-101,754/, accessed: 2023-06-15.

The project "Cyber Security for the European University EUNICE", implemented under the National Academic Exchange Agency's Strategic Partnerships Programme. Implemented in cooperation between the Poznan University of Technology and the University of Catania, University of Mons, and Brandenburg University of Technology.

Additional notes

If provided space for an answer is insufficient, use this additional space.

The project "Cyber Security for the European University EUNICE", implemented under the National Academic Exchange Agency's Strategic Partnerships Programme. Implemented in cooperation between the Poznan University of Technology and the University of Catania, University of Mons, and Brandenburg University of Technology.

The project "Cyber Security for the European University EUNICE", implemented under the National Academic Exchange Agency's Strategic Partnerships Programme. Implemented in cooperation between the Poznan University of Technology and the University of Catania, University of Mons, and Brandenburg University of Technology.