**TCPDUMP: NETWORK PACKET ANALYSIS**

**1. OBJECTIVE**

The objective of the project is to capture and analyze network traffic using TCPDump.

* Packet Capture: Utilize TCPDump to capture network packets.
* Data Examination: Analyze the content of the captured packets using tools like Wireshark.

**2.TOOLBOX**

**TCPDump:** A command line packet analyzer that allows you to capture and analyze network traffic. It allows precise packet capture according to specific criteria with various filtering options.

**Wireshark:** Allows detailed examination and analysis of captured network packets. It makes it easier to understand the structure of network traffic by providing a visual representation of the data.

**3.THEORETICAL BACKGROUND**

**TCP/IP Protocols:** Allows network administrators and security professionals to monitor, troubleshoot, and analyze network traffic.

**Creating Network Traffic:** It refers to the intentional creation of data packets or network activity for various purposes, such as generating network traffic, testing network performance, simulating user behavior, etc. This can be done using special tools or scripts to simulate different types of network traffic, such as web browsing, file transfers, video streaming, etc.

**Packet Capture Concepts:** TCPDump captures raw data from network interfaces and saves it for later analysis.

**Wireshark and Packet Analysis:** Wireshark is used to visually inspect and analyze captured packets. Interpretation of packet details, protocol analysis, and use of image filters are essential components.

**4. DATA AND ANALYSIS**

**Data Collection:**

* **Capture Network Packets:** Use TCPDump to capture network packets.
* **Save as .pcap File:** Save the captured packets in a .pcap file for further analysis.

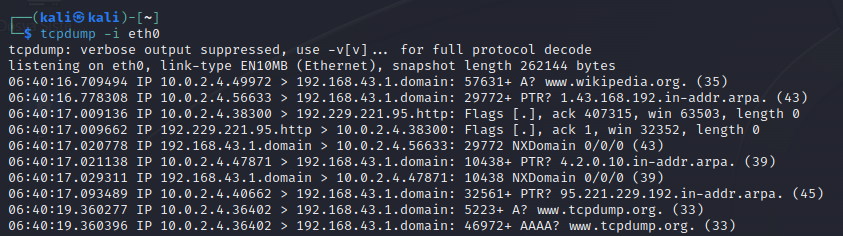
**Data Analysis:**

* **Import into Wireshark:** Open the .pcap file in Wireshark for analyzing of the captured packets.
* **Protocol Analysis:** One aspect of the analysis would involve examining the captured packets to understand the protocols being used, such as TCP, UDP, HTTP, DNS, etc.
* **Traffic Patterns:** Analysis of network traffic patterns, including peak usage times, types of traffic, and identifying any abnormal patterns or spikes in traffic.
* **Abnormalities Detection:** Use Wireshark filters to isolate abnormal patterns. Look for unusual communication, high packet loss, or unexpected protocol behavior.
* **Security Analysis:** Detection of potential security threats, such as unusual network activity, potential malware communication, or attempts at unauthorized access.

**5. PROJECT STEPS**

**a. Creating Network Traffic**

The traffic on which interface will be examined is written on the command line as "tcpdump -i eth0". Websites are surfed to generate network traffic.



**b. Capturing Network Traffic**



**06:40:19.360277 :** timestamp (in hours, minutes, seconds)

**IP 10.0.2.4.36402 > 192.168.43.1.domain :** source ıp (10.0.2.4) and source port (36402)

destination ıp(192.168.43.1) and destination port(domain)

**5223+ A? :** query id and query type

**www.tcpdump.org (33):** queried field and query length



[P.] : PUSH, data transmission

[F.] : FINISH, data transmission finished

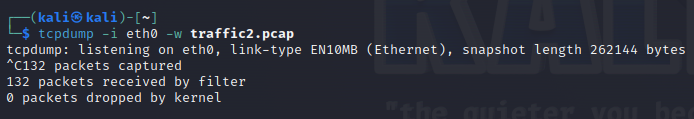
[.] : ACK, packet received and waiting for next one

ack: acknowledgment\_id;

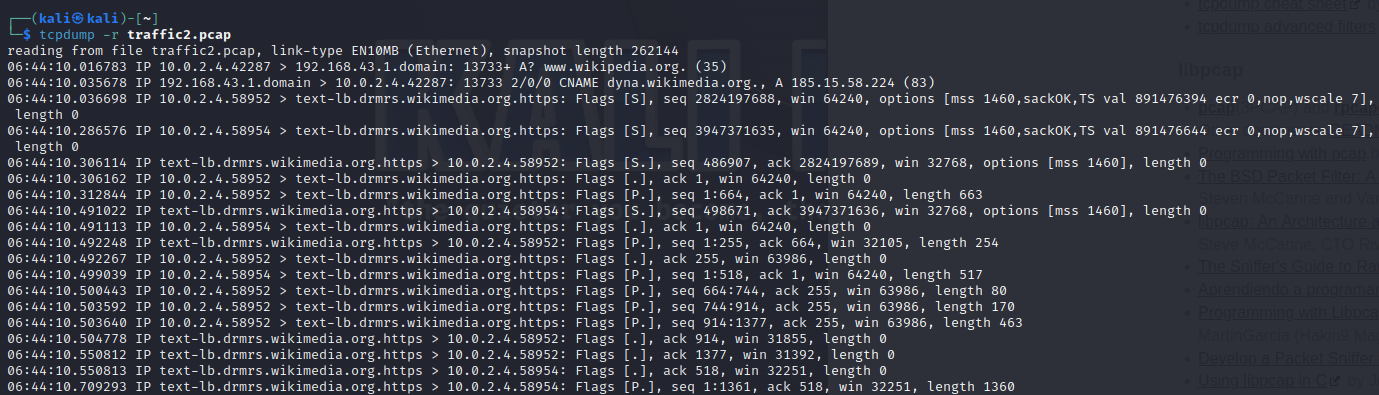
seq: sequence\_id;

win:window\_size.

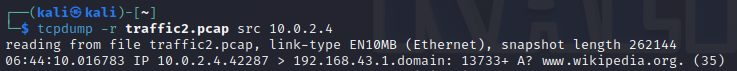
**c. Saving Captured Data**

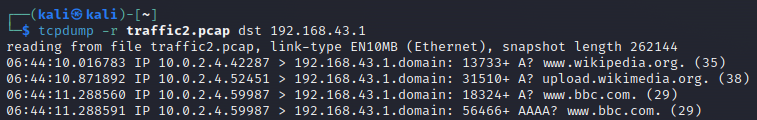
Save captured data to “tcpdump -i eth0 –w traffic2.pcap” file.

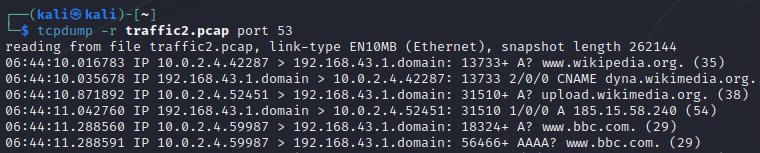
**d. Reading the Saved File**

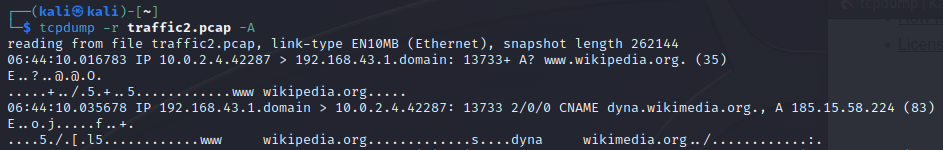
The saved file is read, displayed and filtered for later analysis as "tcpdump -i eth0 –r traffic2.pcap". 

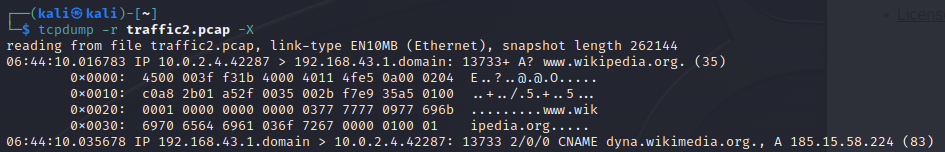
**e. Filtering the Saved File**

Filtering packets where the source IP address is 10.0.2.4 

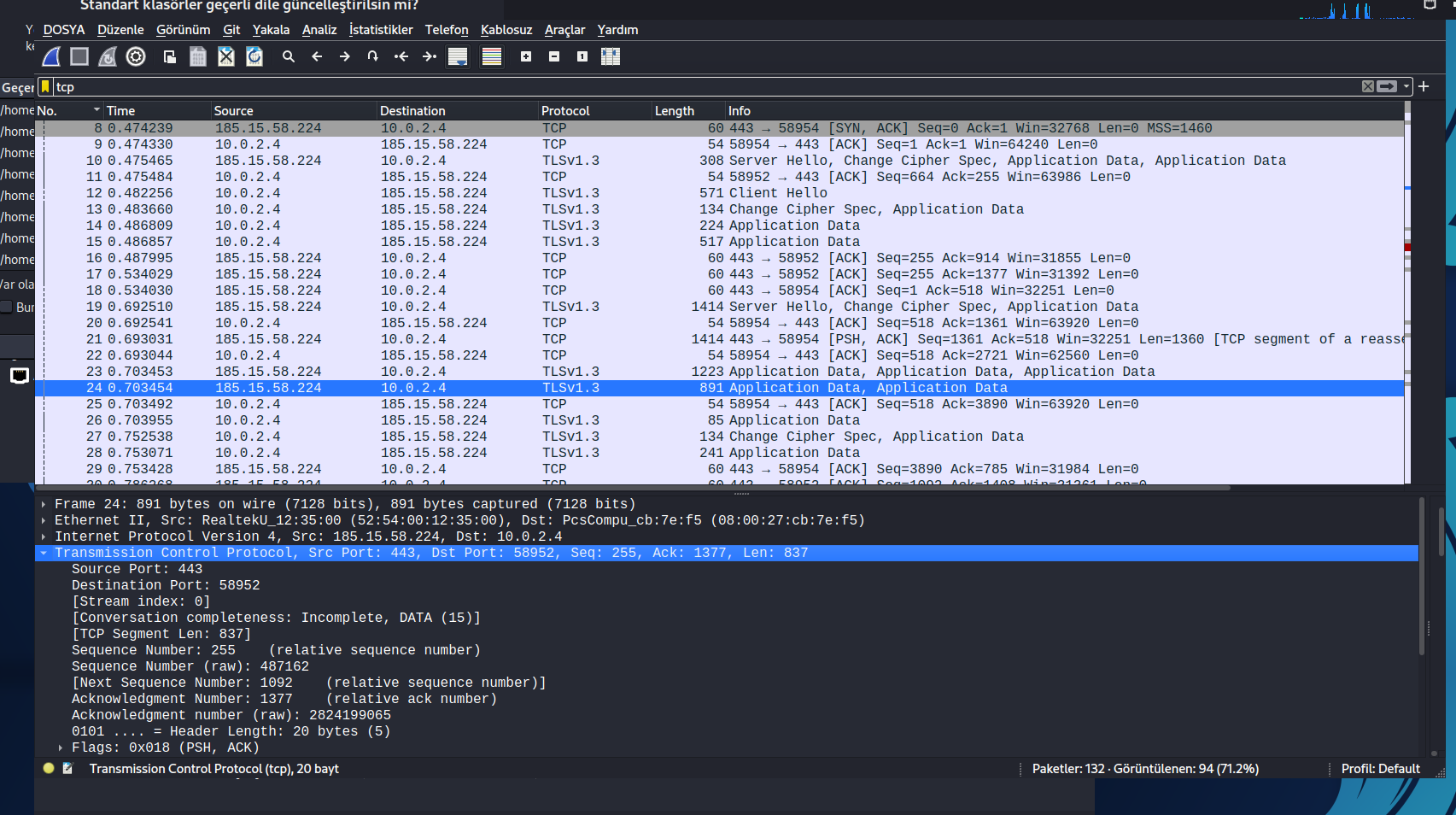
Filtering packets where the destination IP address is 192.168.43.1

Filtering packets where the destination or source port number is 53

Shows the contents of packets in ASCII format

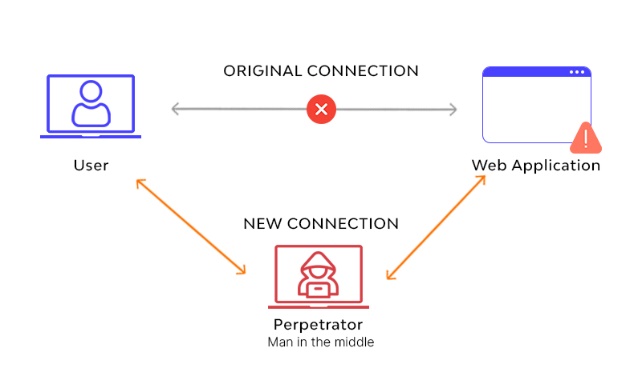
Shows the contents of packets in hexadecimal format

**f. Data Examination**



**g. Attack Detection**

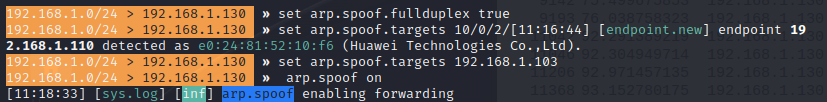
I explained how the login information entered via Wireshark can be obtained when you enter a site and enter an e-mail and password to log in to that site.



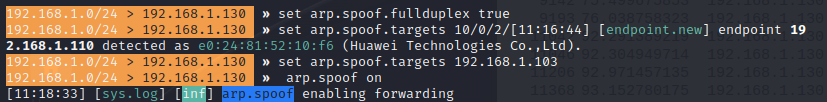
While doing this, he performs the "Man in the Middle (MiTM) Attack". In this attack, the two parties communicating with the Attacker are separated and the transmitted data is viewed, changed or stolen. These types of attacks usually occur on the network and are used to steal users' functionality or open sensitive information.



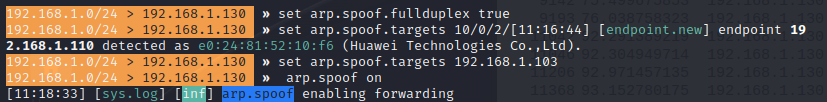
* net.probe on : Shows IP addresses that are actively within the network.



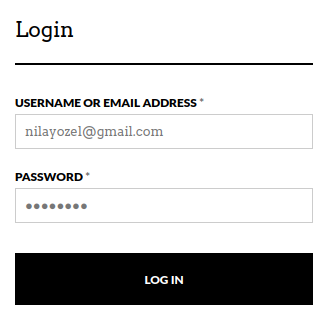
* arp.spoof.fullduplex true : It is necessary to set true to initiate an attack.



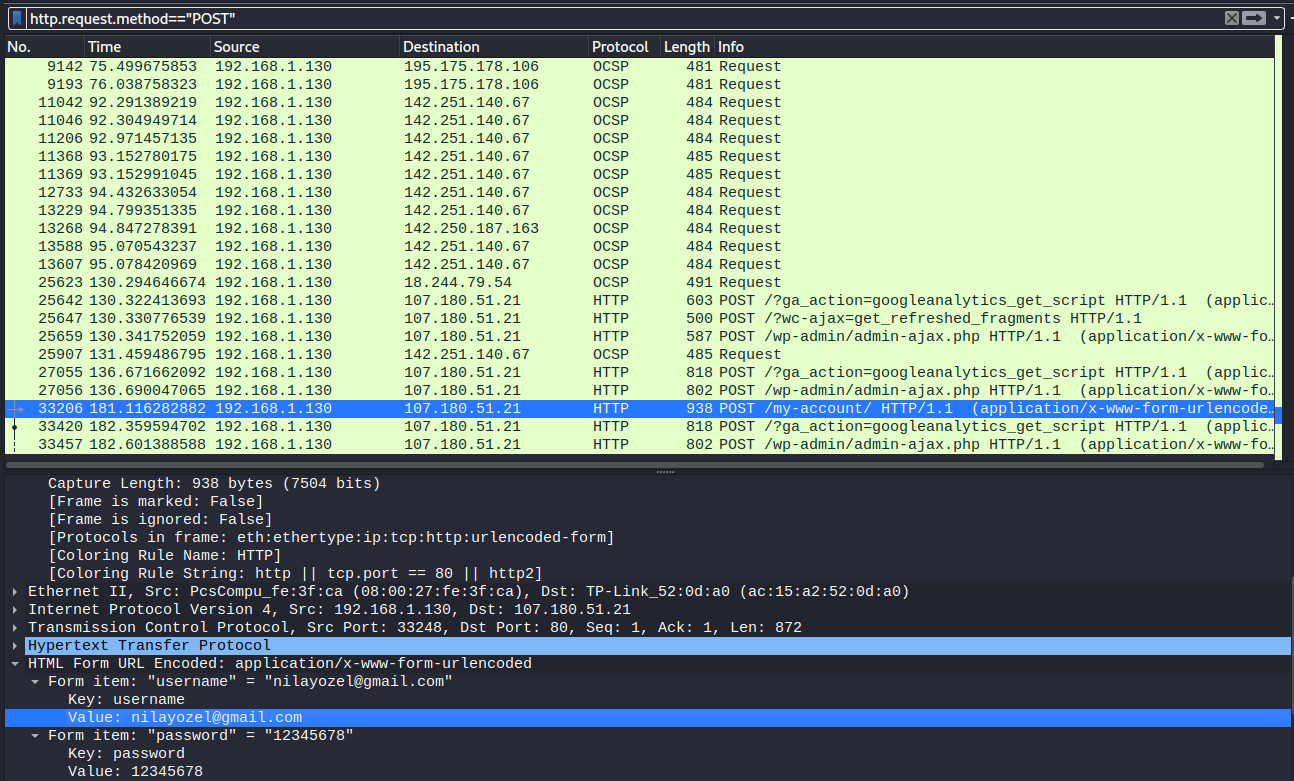
* arp.spoof.targets : The IP address of the target machine is entered, the attack is ready to be launched.

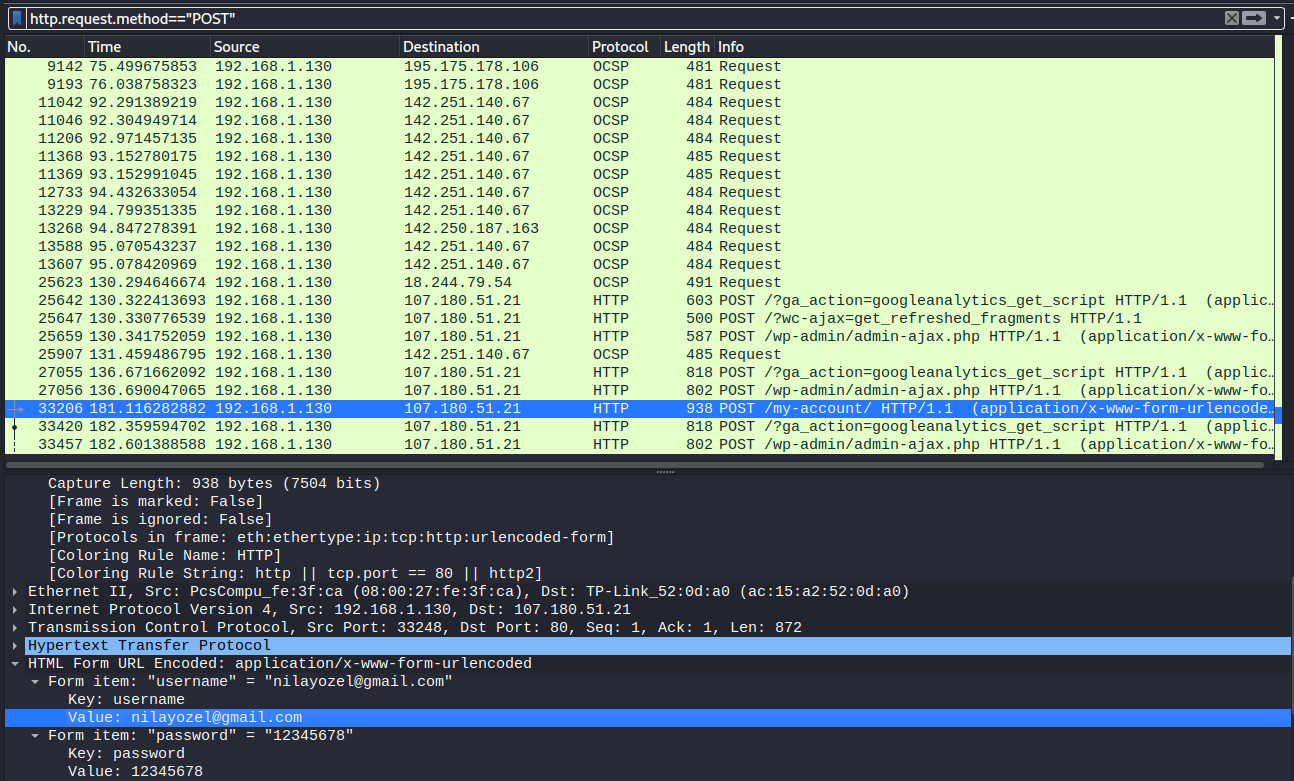


* arp.spoof.on : Attack launched.



After these commands, an unsecured site (eg: http://unicornitems.com) is accessed. Username and password are entered. Afterwards, the traffic capture process in Wireshark is stopped and examined.





The "http.request.method=="POST"" statement is used to filter HTTP requests that contain only the POST method in network traffic captured with TCPDump. So, this expression indicates that a request is used to add or update a specific resource.

**6. CONCLUSION**

As a result of the "TCPDump: Network Packet Analysis" project, it is aimed to capture and analyze network traffic using TCPDump and identify possible threats.

During this project, TCPDump was successfully used to generate network packets and capture packets. Afterwards, the network traffic was recorded in ".pcap" files for analysis of this generated traffic. This recorded data was then subjected to an analysis using tools such as Wireshark. Additionally, Wireshark was leveraged to recognize potential threats and malicious activities, focusing on attack detection.

Potential areas for further research or improvement were highlighted, paving the way for future improvements in network security measures. It provided a basis for future areas of interest, taking into account the evolving environment of network technologies and emerging threats.

**7.DISCLAIMER**

This network analysis project is conducted for security assessment purposes only. The data collected during the project will be used only to achieve the determined goals and analyze network security. It is important to act in full compliance with legal restrictions and ethical standards.

**REFERENCES**

1. https://www.tcpdump.org/

2. https://jvns.ca/tcpdump-zine.pdf

3. https://www.kali.org/tools/tcpdump/

4. https://opensource.com/article/18/10/introduction-tcpdump

5. https://www.linode.com/docs/guides/how-to-use-tcpdump-to-analyze-traffic/

6. https://www.site24x7.com/learn/linux/tcp-dump.html

7. https://www.youtube.com/watch?v=GA3DxA7v11I

8. https://www.youtube.com/watch?v=uN6CSiX8fQQ&list=WL&index=9

9. https://www.youtube.com/watch?v=uN6CSiX8fQQ

10. https://www.youtube.com/watch?v=AIQVNlI\_A20

11. https://www.youtube.com/watch?v=Gdmz3jtqjMM

12. https://www.geeksforgeeks.org/tcp-flags/

13. https://www.hackingarticles.in/network-packet-forensic-using-wireshark/