A purple triangle with a white tree and a red circle

Description automatically generated

**UNIVERSITI MALAYSIA TERENGGANU**

**SEMESTER 1 2023/2024**

**CYBER SECURITY CSF3233**

**LAB 5**

**PREPARED FOR:**

**MUHAMMAD ABDUL AALIM AHMAD ROSLI**

**PREPARED BY:**

**ARUN MUGILAN A/L SARGUNAN S63746**

REFLECTION QUESTIONS - TASK 2

1. In your own words, explain ARP poisoning.

* ARP poisoning is a cyber attack where an intruder sends fake messages to a local network, tricking devices into sending their data to the attacker. This allows them to intercept, modify, or block communications between devices on the network.

1. How can we prevent the ARP poisoning attack?

* Use detection tools, static ARP entries, network segmentation, ARP spoofing prevention protocols

1. Why do you think telnrt is not a safe way to connect to a remote machine? What is the safer way to do it?

* Telnet exposes data, including login details, making it insecure for transmitting sensitive information. Use SSH for secure remote connections. It encrypts the entire session, providing protection against unauthorized access and data interception.

REFLECTION QUESTIONS - TASK 3

1. Based on your understanding, what is network security and what are the basic objectives of network security?

* Network security means protecting computer networks from unauthorized access or harm. The main goals are keeping information safe, making sure data is accurate, and ensuring networks are available when needed.

1. Differentiate between Intrusion Detection System (IDS) and Intrusion Prevention System (IPS).

* IDS watches for suspicious activity and raises alerts but doesn't actively block threats. IPS actively identifies and stops potential threats, going beyond just alerting.

1. Why Virtual Private Network (VPN) is important for network security?

* VPNs are crucial for security because they create a secure, encrypted connection over untrusted networks, like the internet, ensuring that data remains confidential.

1. In what situation you might want to install a Demilitarized Zone (DMZ) on your network?

* A DMZ is used when you want controlled access to services from the internet, like web servers. It adds security by separating these servers from the internal network.

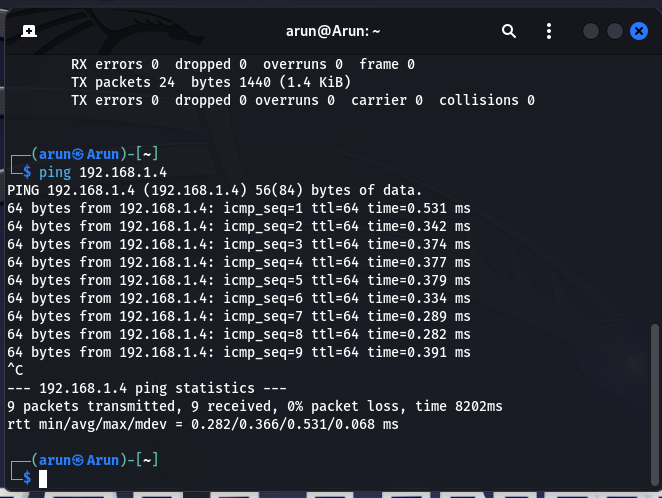
1. What is the role of Network Address Translation (NAT) on a network?

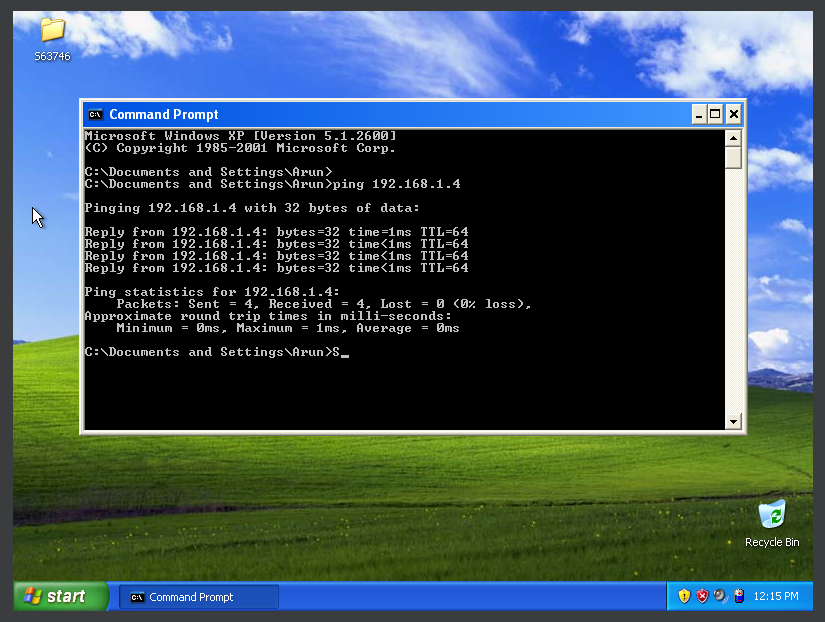
* NAT hides internal device details by mapping private IP addresses to a single public IP address, improving security and providing some anonymity.

1. To apply 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.

* A proxy server acts as a middleman between users and the internet, enhancing security by filtering content, anonymizing traffic, caching for speed, logging user activities, controlling access, and inspecting encrypted traffic. Understanding these functions helps in effectively managing network security.

**Task 1 – Setting up the virtual lab network**

****

****

**Task 2 – MITM Attack using ARP Poisoning**

**A computer screen shot of a spider

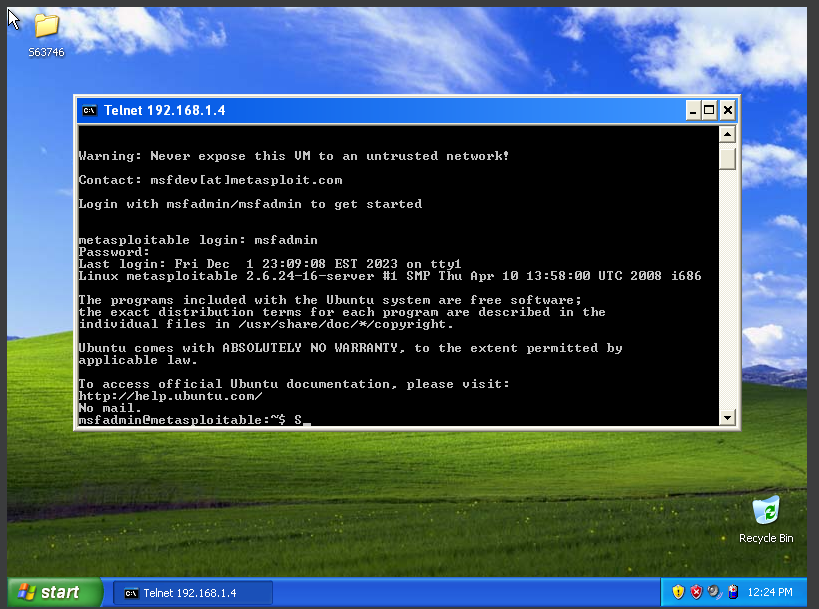
Description automatically generated**

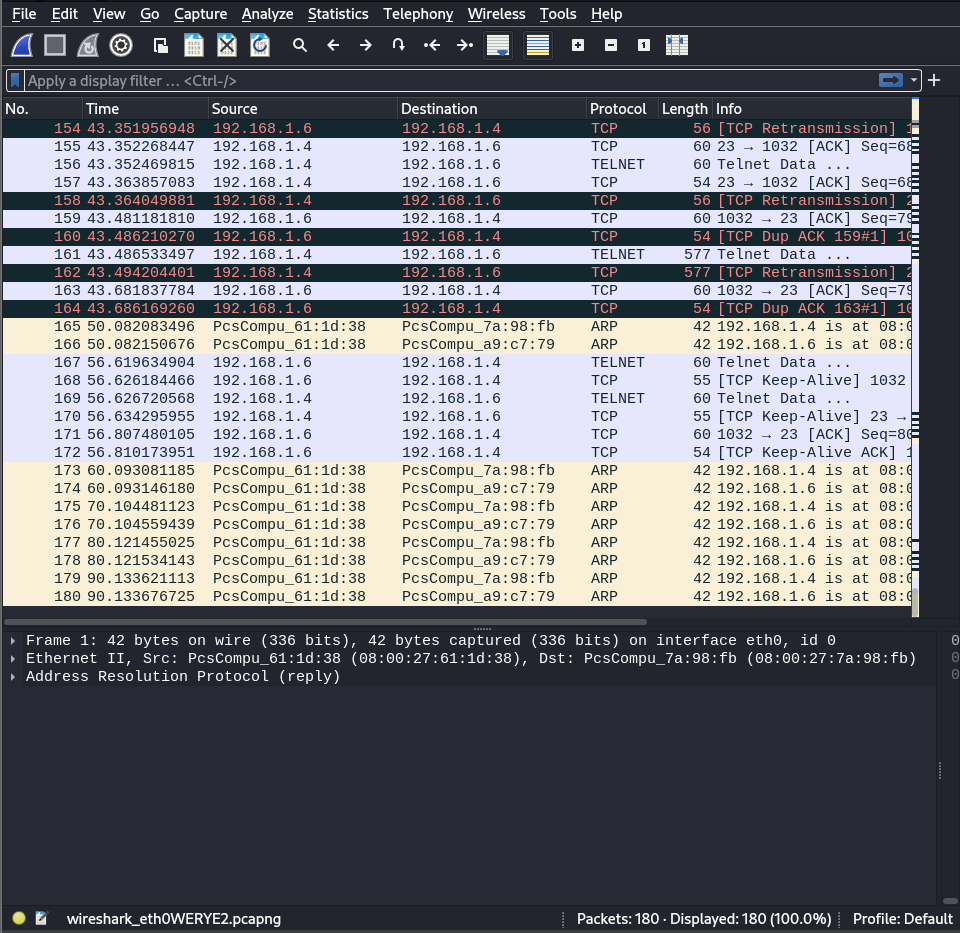
**A screenshot of a computer

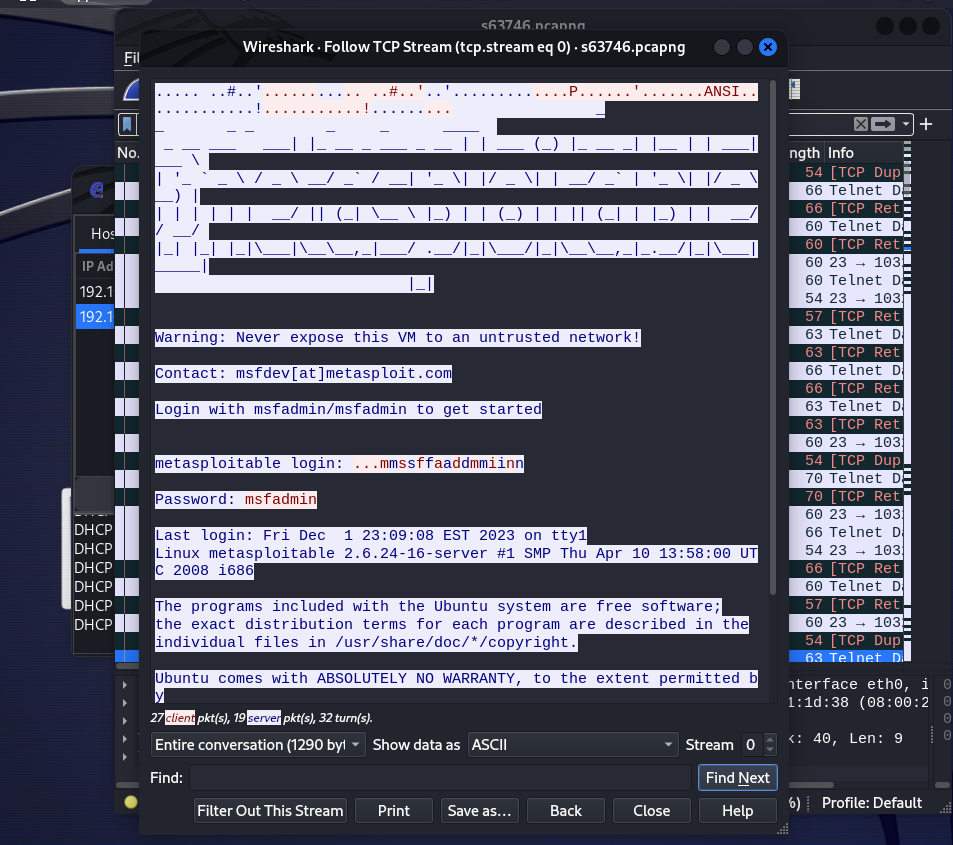
Description automatically generated**

**A screenshot of a computer

Description automatically generated**

****

****

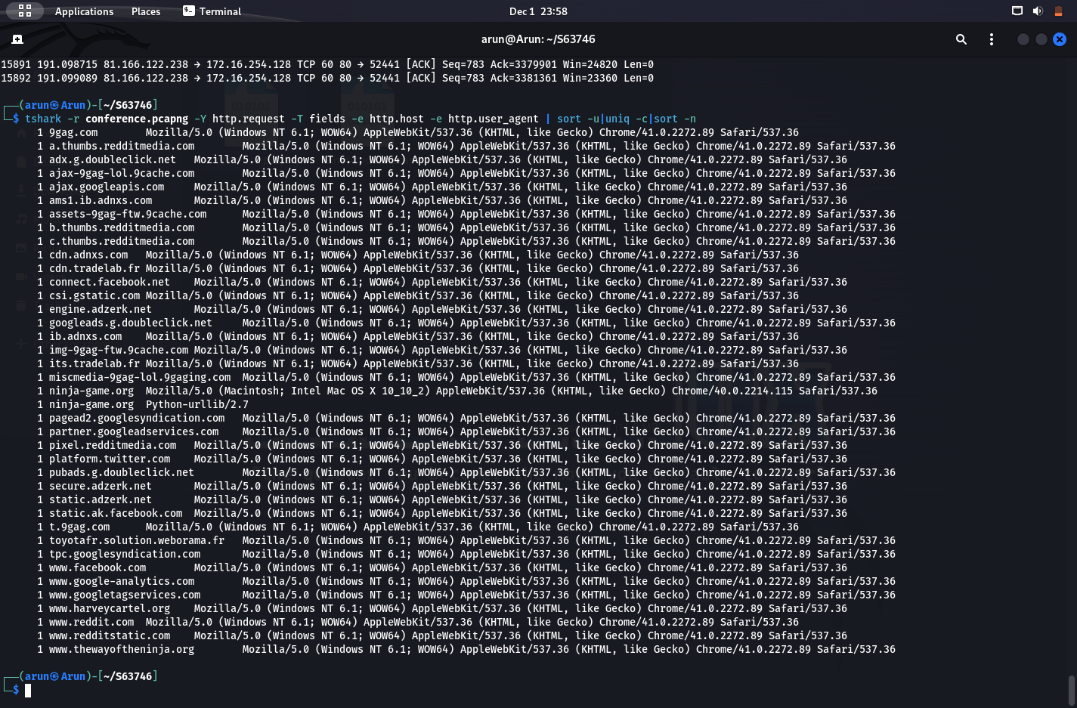
****

**Task 3 – Analysing the network packet**

**A screenshot of a computer

Description automatically generated**

****

****

**A screenshot of a computer program

Description automatically generated**

**A screenshot of a computer program

Description automatically generated**

**A screen shot of a computer

Description automatically generated**

**A screen shot of a computer

Description automatically generated**