**Draft Report**

Project 1: Conducting a Man-in-the-Middle (MITM) Attack and Privilege Escalation

Name: Elif Öztoprak ID: 6715930083

This project demonstrates the process of conducting a Man-in-the-Middle (MITM) attack to intercept sensitive data, followed by privilege escalation on a vulnerable system. Tools like Wireshark, Ettercap, and John the Ripper were used to capture, analyze, and exploit network vulnerabilities. The findings highlight critical security risks and suggest mitigation strategies to secure systems from similar attacks.

Preparation Phase:

The Metasploitable virtual machine was configured as the target system for the penetration testing activities.

* It was started in **host-only** mode to ensure isolation and prevent external network access.
* The machine's IP address was obtained by running the ifconfig command on the Metasploitable terminal:

A screenshot of a computer

Description automatically generated

Kali attacker machine’s IP was obtained to check if machines were set up in the same subnet to facilitate communication. Connectivity was verified by executing the following command from Kali Linux:

A computer screen shot of a program

Description automatically generated

A screenshot of a computer program

Description automatically generated

**Install Essential Tools**  
Kali Linux was updated and necessary tools were installed using the following commands:

apt update && apt upgrade -y

apt install wireshark john ettercap-graphical-y

Each tool was tested to confirm successful installation:

wireshark --version

john --version

ettercap –version

**Start Wireshark**

Wireshark was launched on the Kali Linux machine with using: wireshark

The network interface associated with the target environment (eth0) was selected.

Wireshark filters were applied to isolate specific types of network traffic: http

A screenshot of a computer screen

Description automatically generated

Phase 3: Initiate the MITM Attack

Run Ettercap for ARP Spoofing Open a terminal in Kali Linux and start Ettercap in graphical mode:

sudo ettercap -G

In Ettercap:

Click Sniff > Unified Sniffing.

Select your network interface (eth0).

Click Hosts > Scan for Hosts to scan the network.

Click Hosts > Host List.

Add the Metasploitable IP as Target 1.

Add the Kali IP as Target 2.

Start ARP spoofing:

Click Mitm > ARP Poisoning.

Select Sniff Remote Connections and click OK.

Monitor the intercepted traffic in Wireshark.

A black background with white text

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer screen

Description automatically generated