**Draft Report**

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

Name: Elif Öztoprak ID: 6715930083

**Introduction**

This report outlines the simulation of a cyberattack using ARP poisoning, credential interception, and privilege escalation techniques. The attack was conducted on a controlled environment to demonstrate the risks posed by unencrypted communications, weak password policies, and outdated system configurations.

**Objectives:**

1. Redirect victim traffic using ARP poisoning.
2. Intercept credentials via a fake login page.
3. Crack captured password hashes using John the Ripper.
4. Escalate privileges and establish persistence on the target system.

**Tools :**

1. Wireshark.
2. Metasploit
3. John The Ripper
4. Ettercap
5. Kali Linux

**Scenario**

Almost everyone of us use café’s not secure Wi-Fi. My aim in this project is to show in which way we can be used to flow traffic through us. Malicious htmls, look alike login pages can be used to steal our credentials.

**Environment Setup**

**Attacker Machine:** Kali Linux 2024.2

* IP Address: 10.10.217.74
* Tools Used: Ettercap, Apache2, PHP, John the Ripper

A computer screen shot of a program

Description automatically generated

**Victim Machine:** Metasploitable 2

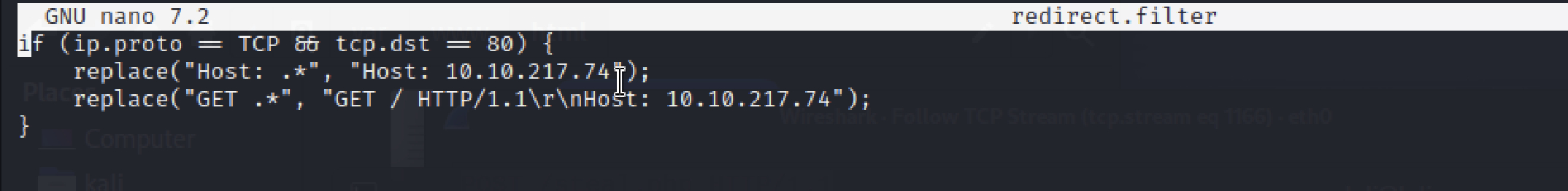
* IP Address: 10.10.217.43
* Vulnerabilities: Unencrypted communication, weak passwords, outdated kernel

A screenshot of a computer

Description automatically generated

**Phase 1: ARP Poisoning and Traffic Redirection**

1. **ARP Spoofing with Ettercap:**
   * Configured Ettercap to perform ARP poisoning between the victim (10.10.217.43) and the gateway (10.10.217.74).
   * Redirected victim HTTP traffic to the attacker's server.



etterfilter redirect.filter -o redirect.ef => Compiled the filter tp be used as a filter in ARP poisoning

A screenshot of a computer screen

Description automatically generated

**Verification:**

* + Checked the victim’s ARP table to confirm the gateway’s MAC address was replaced by the attacker’s MAC.

1. **Setup Fake Login Page:**
   * Deployed a malicious Starbucks login page on the attacker’s Apache server.
   * Configured steal.php to get the captured credentials.

A screen shot of a computer code

Description automatically generated

A screenshot of a computer program

Description automatically generated

**Phase 2: Credential Interception**

1. **Victim Interaction:**
   * Redirected victim to the malicious login page.

A screenshot of a computer

Description automatically generated

* + Simulated the victim entering credentials (e.g., admin:password123).

1. **Captured Credentials:**
   * Verified that credentials were stored in creds.txt on the attacker machine:

Username: elıfoztoprak Password: 12345

A screenshot of a computer screen

Description automatically generated

**Phase 3: Privilege Escalation**

1. **Dumped /etc/shadow File:**
   * Used the captured credentials to log into the victim machine via SSH.
   * Extracted the /etc/shadow file and transferred it to the attacker machine using SCP.

A screenshot of a computer

Description automatically generated

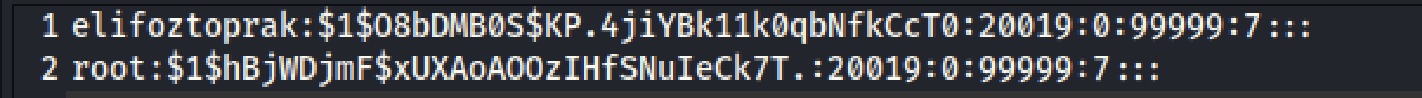
A computer screen shot of a computer code

Description automatically generated

A computer screen shot of white text

Description automatically generated

1. **Cracked Password Hashes:**
   * Used John the Ripper with the rockyou.txt wordlist to crack the hashes.
   * Cracked results:
   * elifoztoprak:12345
   * root:root:20019:0:99999:7:::

****

**A screen shot of a computer

Description automatically generated**

**Phase 4: Post-Exploitation**

1. **Escalated Privileges:**
   * Switched to the root user using the cracked root:toor credentials.
   * Verified root access with whoami.A screenshot of a computer program

     Description automatically generated
2. **Established Persistence:**
   * Added a new backdoor user:
   * useradd -m -s /bin/bash backdoor
   * echo "backdoor:backdoor123" | chpasswd

usermod -aG sudo backdoor

* + Enabled SSH root login for future access.

A black background with white text

Description automatically generated

**Mitigation Recommendations**

1. **Encrypt Communication:**
   * Use HTTPS to prevent credentials from being intercepted during transit.
2. **Regularly Update Systems:**
   * Upgrade the kernel and services to fix known vulnerabilities.
3. Use public Wi-Fi’s carefully:
   * Redirecting and capturing network can be done through public Wi-Fi.
4. **Implement Strong Password Policies:**
   * Enforce complex passwords and periodic changes.
5. **Deploy ARP Spoofing Detection:**
   * Use tools like arpwatch to monitor and detect ARP poisoning attempts.
6. **Restrict Privilege Escalation Paths:**
   * Minimize the use of sudo and limit access to sensitive files.

**Conclusion**

This simulation demonstrated the effectiveness of ARP poisoning, credential interception, and privilege escalation attacks on an outdated system. The results highlight the importance of implementing robust security measures, including encrypted communications, strong password policies, and regular system updates.