Ecole Supérieure
d'Informatique et du Numérique
COLLEGE OF ENGINEERING & ARCHITECTURE

Lab 03: Fundamental Security
Instructor: Prof. Anass Sebbar
Level: Engineering - 3rd Year

Lab 03: Network Attacks and System Security

Objectives

The purpose of this lab is to illustrate various **flood attack techniques** and penetration testing strategies. You will learn how to launch **Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks**, analyze their impact, and test network resilience using different tools.

In this lab, we will focus on:

- Simulating HTTP Flood and DDoS attacks using HULK.
- Executing Ping Flood attacks to assess network resilience.
- Using Nmap to scan for open ports and detect vulnerabilities.
- ARP Spoofing attacks
- Man In The Middle attacks (MITM)
- Hijacking DNS queries with DnsSpoof to manipulate network traffic.

Instructions

- The lab report must be submitted one week after the lab session on the Moodle platform, respecting the deadline mentioned there.
- The lab must be performed individually in class, but the report should be submitted in groups of up to 2 students.
- Lab groups must remain the same for all reports throughout the semester.

Legal and Ethical Precautions:

DoS and DDoS attacks, as well as other penetration tests, are illegal if they are carried out without explicit permission. Please ensure that these tests are conducted in a controlled and ethical environment (e.g., on systems for which you have permission to test for security). This lab must be carried out in a laboratory setting or with dedicated testing machines.

This lab will be carried out on two machines: a virtual machine running **Kali Linux**, used to perform network attacks and security analyses, and a machine running **Windows 7**, which will be used as a target to test resilience to attacks. Kali Linux offers many tools such as *Nmap* , which are essential for this type of testing. Windows 7 will make it possible to simulate a vulnerable system and observe the impact of attacks on a real environment.

Part 1: Security and Penetration Testing

1. **Hping3 Resiliency Testing (Ping Flood):**
   Use *Hping3* to send a large number of ICMP requests (ping) to the target, rendering their network unusable.

   ```
   $ sudo --flood --icmp [target IP]

   Ex: $sudo ping -f 192.168.179.129
   ```

2. **Port Scanner with Nmap:**
   Use *Nmap* to scan open ports on the target machine, identify vulnerable services, and scan operating systems.

   ```
   $ sudo  nmap -sS @ip (SYN scan for DoS)

   $ nmap -sU @ip (scan des ports UDP)

   Or : sudo nmap -sU -v <IP>
   ```

Part 2: MiTM Attack on FTP and Telnet Protocols

In the following exercise, we will use the Ettercap software to perform an ARP Poisoning attack. A “man in the middle” attack—literally meaning “person in the middle”—is a type of attack in which an attacker positions their machine between two communicating hosts, as shown in the diagram below. Once in this position, the attacker can launch a variety of dangerous attacks because they intercept all traffic between the two hosts. There are several methods to become a "man in the middle"; in this lab, we will perform an attack based on the ARP protocol.

a. Description of the ARP Poisoning Attack

This attack occurs when a machine requests the MAC address associated with an IP address. The attacker responds to the requester with packets that falsely indicate that the IP address is associated with the attacker’s own MAC address. In doing so, the attacker bypasses the legitimate IP-MAC mapping response from the actual host. This attack is known as ARP poisoning (or ARP spoofing). Note that this attack is only possible if the attacker and the victim hosts are on the same broadcast domain (defined by an IP address and subnet mask on each host).

b. Steps to Perform the Attack

1. **Select Sniffing Mode:**
   - In Ettercap, choose the "Unified sniffing" mode by navigating to:
     `Sniff -> Unified sniffing.`
2. **Scan for Hosts on Your Subnet:**
   - Go to:
     `Hosts -> Scan for hosts`
     This will scan your subnet to discover available hosts.
3. **List the Discovered Hosts:**
   - Navigate to:
     `Hosts -> List Hosts`
     Verify that your machines are detected by Ettercap.
4. **Select the Victim Machines:**
   - Choose the target machine (Target 1) by clicking the “Add to Target 1” button.
   - Choose the machine whose identity will be spoofed (Target 2) by clicking the “Add to Target 2” button.
5. **Start tcpdump:**
   - Open a terminal and launch the `tcpdump` command to capture network traffic before initiating the attack.
6. **Initiate the Man in the Middle Attack:**
   - With the targets selected, launch the “Man in the Middle” attack by choosing “ARP Poisoning” from the MITM section in the menu bar.
   - Do not check any additional options.
7. **Verify the Attack:**
   - Examine the output from the `tcpdump` command as well as the ARP tables on the victim machines.
   - What do you observe?
8. **Restoring Normal State:**
   - How would you return the network to its normal state after this attack?
9. **Mitigation Measures:**
   - What countermeasures could be implemented to defend against such attacks?

c. Diagram Task

- **Provide a Diagram:**
  Create an explanatory diagram that shows the progression of the attack. Your diagram should include the different messages sent by the attacker, the target, and the impersonated machine.

Homework: MITM Attack Using BetterCAP

BetterCAP is a powerful, extensible, and portable framework written in Go. It provides an all-in-one solution for performing reconnaissance and attacks on WiFi networks, Bluetooth Low Energy devices, wireless HID devices, and Ethernet networks.

1. **Initiate BetterCAP and Start Sniffing**
   Launch BetterCAP on your Kali Linux VM. Use its interactive console to start network sniffing. BetterCAP will display available commands to manage network attacks.

2. **Perform ARP Poisoning**
   Use BetterCAP's ARP poisoning module to redirect traffic between the target devices. This will cause the victim machines to send their data through your machine.
3. **Execute the MITM Attack**
   With ARP poisoning in place, BetterCAP will intercept and relay communications between the targeted hosts. Monitor the session to capture network traffic, including potential sensitive data like passwords.
4. **Capture and Analyze Traffic**
   Observe the network packets captured by BetterCAP. Pay particular attention to any transmitted credentials or other sensitive information that the attack might reveal.

Download last version of Bettercap

```
wget https://github.com/bettercap/bettercap/releases/download/v2.23/bettercap_linux_amd64_2.23.zip
```

unpack, move, do cleaning and checking:

```
unzip bettercap_linux_amd64_*zip sudo mv bettercap /usr/local/bin/ rm README.md LICENSE.md bettercap_linux_amd64_*.zip bettercap -h
```