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

Lab 02: Fundamental Security

Instructor: Prof. Anass Sebbar

Level: Engineering - 3rd Year

Lab 02: Network Attacks and System Security

Objectives

The purpose of this lab is to illustrate network attack techniques such as traffic interception and manipulation, port scanning, as well as Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. You will learn how to use packet capture and analysis tools such as tcpdump, Wireshark, Ettercap, as well as penetration testing tools like Nmap and DnsSpoof. You'll also learn how to divert and analyze network traffic and test your network's resilience to DoS/DDoS attacks.

In this lab, we will focus on:

- Traffic interception and manipulation
- DoS & DDoS Attacks

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* and *Hping3*, 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: Packet Capture and Analysis

1. **Packet Capture with tcpdump:**
   As an administrator, perform packet capture on a network interface with *tcpdump*.

   ```
   $ sudo tcpdump -i eth0 -c 500 -w /tmp/macapture.pcap
   ```

2. **Analyzing Captured Packets:**
   Check the nature of the captured file and view the information using the following commands:

   ```
   $ file /tmp/macapture.pcap
   ```

   ```
   $ sudo tcpdump -r /tmp/macapture.pcap | more
   ```

3. **Advanced Capture:**
   Capture 20 packets without address translation and view the first 1500 bytes of each packet.

   ```
   $ sudo tcpdump -i eth0 -c 20 -n -s 1500 -w /tmp/macapture2.pcap
   ```

   ```
   $ sudo tcpdump -r /tmp/macapture2.pcap –x
   ```

4. **Packet Filtering:**
   Apply filters to observe specific types of traffic, such as TCP packets, ARP packets, or web connections (port 80).

   ⇨ Capturing HTTP Traffic

   ```
   $ sudo  tcpdump 'tcp port 80'
   ```

   ⇨ Capturing ARP (Address Resolution Protocol) Traffic

   ```
   $ tcpdump ether proto 0x806
   ```

   ⇨ Capturing FTP (Port 21) and HTTP (Port 80) Traffic

   ```
   $ sudo tcpdump 'tcp and ( port 21 or 80)'
   ```

5. **Using Wireshark and Ettercap:**
   Use *Wireshark* to analyze packets captured by *tcpdump* or *tshark*, and *Ettercap* to intercept and analyze traffic between a client and a server (FTP, Telnet).
   Wireshark Command:

   ```
   $ wireshark -r macapture.pcap
   ```

Ettercap command:

```
$ ettercap -T -r macapture.pcap | grep TELNET

$ ettercap -T -r /tmp/macapture.pcap | grep TELNET
```

Part 2: DoS and DDoS Attacks

1. **Using Hping3 to Attack in DoS:**
   Hping3 is a powerful tool for generating network packets and performing denial attacks. For example, a SYN flood attack sends SYN packets to overload the target machine.

   ```
   $ sudo hping3 --flood --syn -p 80 [target IP]

   $ sudo  hping3 --flood --udp -p 53 [target IP]
   ```

In your report for each step, **take screenshots, analyze them, and interpret the results.**