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

Lab 01: Network Analysis

Instructor: Prof. Anass Sebbar
Level: Engineering - 3rd Year

Lab 01: Security Properties - CIA Triad

Objectives

The objective of this lab is to set up a network between different machines and analyze the network traffic and client-server connections.

In this lab, we will focus on:

- Capturing and analyzing FTP protocol traffic.
- Capturing and analyzing Telnet protocol traffic.
- Capturing and analyzing SSH protocol 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.

Security Properties (Reminder)

Identify which security property (Confidentiality, Integrity, Availability) is violated in each of the following cases:

1. A hacker attacks a pharmaceutical factory and alters the chemical formula of the produced medicines.
2. A hacker steals the chemical formula of a particular drug.
3. A hacker performs a DDoS attack on a mail server.
4. A hacker executes a data breach on a data server.
5. A media company suffers a ransomware attack.

Hands-on Practice: Understanding the Importance of Confidentiality in Communications

We will be working with two virtual machines:

- One machine with the Linux operating system.
- One machine with the Windows operating system.

Capture and Analysis of FTP Protocol Traffic

Capture Process:

1. On the Windows machine, launch **Wireshark** and start capturing packets.
2. On the Linux machine, start the FTP service by executing the following command:

```
# sudo service vsftpd start
```

If not installed :
Install ftp server using :

```
#sudo apt update
#sudo apt install vsftpd -y
```

To check :

```
# service vsftpd status
```

3. What layer of the OSI model does the FTP protocol belong to? What is the port number used by FTP?
4. From another machine, establish an FTP connection to the Linux server by executing:

   ```
   # ftp "@ip_ftp_server
   ```

5. Enter the ubuntu machine credentials to connect:

   User : ubuntu

   Psswd : @)@)

6. List the contents of the directory.
7. Stop the capture.

Analysis:

- Which transport layer protocol does FTP use?
- Identify the messages exchanged between the FTP client and server. What messages are used to establish the initial TCP connection?
- What are the source and destination port values? What is their purpose?
- If you open a new FTP connection, do the port numbers change? Test and observe.

netstat -an | grep :20

- Analyze the other exchanged messages, particularly TCP messages.

Capture and Analysis of Telnet Protocol Traffic

Capture Process:

1. On the Windows machine, launch **Wireshark** and start capturing packets.
2. On the Linux machine @ip, start the Telnet service

```
# service telnetd start
```

3. What layer of the OSI model does the Telnet protocol belong to? What is its port number?
4. From another machine, establish a Telnet connection to the Linux server:

```
# telnet @ip
```

5. Use the following credentials:
   - User : ubuntu
   - Psswd : @)@)
6. Stop the capture.

Analysis:

- Which transport layer protocol does Telnet use?
- Identify the messages exchanged between the Telnet client and server. What messages are used to establish the initial TCP connection?
- What are the source and destination port values? What is their purpose?
- If you open a new Telnet connection, do the port numbers change? Test and observe.
- Analyze the other exchanged messages, particularly TCP messages.

Capture and Analysis of SSH Protocol Traffic

Capture Process:

1. On the Windows machine, launch **Wireshark** and start capturing packets.
2. On the Linux machine (@ip), start the SSH service:

```
# service sshd start
```

3. What layer of the OSI model does the SSH protocol belong to? What is its port number?
4. From another machine, establish an SSH connection to the Linux server using **PuTTY**.

5. Use the following credentials:

    - User : ubuntu
    - Psswd : @)@)

6. Stop the capture.

Analysis:

- Which transport layer protocol does SSH use?
- Identify the messages exchanged between the SSH client and server. What messages are used to establish the initial TCP connection?
- What are the source and destination port values? What is their purpose?
- If you open a new SSH connection, do the port numbers change? Test and observe.
- Analyze the other exchanged messages, particularly TCP messages. What do you notice?