Metropolitan State University
CYBR 490 – Cybersecurity for Medical Devices
Lab 3: – Main in the middle lab

Overview

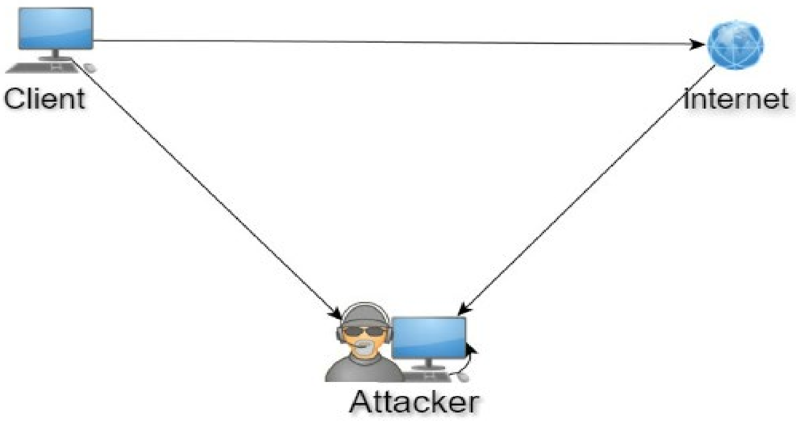
In this lab, Students will learn about the Man in the Middle (MIM) attack. An eavesdropping attack known as a "man-in-the-middle" occurs when an attacker intercepts a data transfer or communication that is already in progress. The attackers place themselves in the "middle" of the transfer and then pose as both authorized participants. This enables an attacker to send malicious links or other material to both legitimate participants in a way that might not be discovered until it is too late. The attacker is also able to intercept information and data from either party.

1.0 Lab Environment

This lab runs in the Labtainer framework, the lab includes links to a pre-built virtual machine that has Labtainers installed, however, Labtainers can be run on any Linux host that supports Docker containers.
From your labtainer-student directory start the lab using:

```
labtainer mitm2
```

A link to this lab manual will be displayed.
This lab consists of three virtual machines: a client computer, a server, and an attacker computer. These computers are all connected to the same network.



2.0 Lab tasks

jane is an administrator at the hospital, when she comes to her desk first in the morning, she always opens a browser to access the EHR system. Attack the hospital system using the Ettercap tool installed in the attacker's machine and prevent jane from accessing the HER system from her computer.

Ettercap is installed in the attacker's machine. Ettercap is a network security tool for Man in the middle attacks. It includes live connection sniffing, real-time content screening, and many more intriguing techniques. It provides various tools for network and host investigation and allows both active and passive dissection of a wide range of protocols.

run the Ettercap tool using this command on one of the attacker's machines sudo Ettercap -G to conduct the ARP poisoning attack.

***Take screenshots of the ettercap interface and save them to a Word document.

Also, a Wireshark tool is installed in the attacker's machine. Run the Wireshark tool to analyze the traffic on jane's computer.

Sudo Wireshark &. Analyze the traffic on ethernet 0

***Take screenshots of the Wireshark traffic and save them to a Word document.

The goal of this lab is to prevent jane from accessing the HER system.

conduct an ARP Poisoning attack using the Ettercap tool. After conducting the attack, the firefox browser should be down.

***Take screenshots of the steps you took on the Ettercap GUI while conducting this attack and save them to a Word document.

To demonstrate the successful attack, Firefox is installed on jane's computer. Run this command
Firefox &
then browse https://www.charmhealth.com/
ssh the server using this command ssh server from Jene's computer and watch the traffic on the Wireshark

***Take screenshots of the Wireshark traffic and save them to a Word document.

Submission

After finishing the lab, go to the terminal on your Linux system that was used to start the lab and type:
stoplab mintm2