Module 2

Man in the Middle Attack

Contents

[Summary 2](#_Toc130376621)

[Prior Knowledge & Skills Requirements 2](#_Toc130376622)

[Educational Background Requirements 2](#_Toc130376623)

[Hardware Unit and Software 2](#_Toc130376624)

[Activity (Gagne’s Nine Events of Instruction) 3](#_Toc130376625)

[Step 1 3](#_Toc130376626)

[Step 2 3](#_Toc130376627)

[Step 3 3](#_Toc130376628)

[Step 4 3](#_Toc130376629)

[Step 5 4](#_Toc130376630)

[Step 6 5](#_Toc130376631)

[Step 7 5](#_Toc130376632)

[Step 8 5](#_Toc130376633)

[Step 9 5](#_Toc130376634)

[Hardware & Software Specifications 6](#_Toc130376635)

[Hardware 6](#_Toc130376636)

[Software 6](#_Toc130376637)

[Operating System and Setup 6](#_Toc130376638)

[Applications 7](#_Toc130376639)

[References 7](#_Toc130376640)

# Summary

In this module, students will learn what a man in the middle attack is and how it could affect SCADA systems. They will use a computing device to perform this attack within a small network.

# Prior Knowledge & Skills Requirements

* Basic knowledge on how to use a computer system that runs one of the following Operating Systems: Windows, MacOS, or any Linux distribution.
* The ability to search the internet utilizing a web browser.

# Educational Background Requirements

* Undergraduate to graduate level students majoring in a STEM related field.
* Undergraduate to graduate level students majoring in a non-STEM related field but an interest in Cyber Security.

# Hardware Unit and Software

The module uses a Raspberry Pi 4, Keyboard, Monitor, and Mouse. Students will be working on a Linux Operating System called “Kali Linux” and they will learn to use the Linux terminal and other applications such as Wireshark. Specifics on the hardware and software used is described in the [***Hardware & Software Specifications***](#_Hardware_&_Software) section of the module.

|  |
| --- |
| Image of hardware setup here |

# Activity (Gagne’s Nine Events of Instruction)

The activity steps will follow Gagne’s Nine Events of Instruction.

## Step 1

Action: Gain attention.

Administer a pretest that assesses students’ current level of knowledge prior to the activity. This test is meant to prime the students’ attention towards the objectives of the module and does not need to be checked for accuracy. However, have the student hold onto the test to assess their own learning from start to finish. A posttest will be taken at the end of the module.

## Step 2

Action: Inform students of the learning objective.

The following are the Learning Objectives for this module:

* Identify what a “Man in The Middle (MiTM)” attack is and what network protocols are used.
* Utilize software to see “packets” and what takes place during the attack.
* Identify encrypted and unencrypted data.
* Define key terms:
  + Address Resolution Protocol (ARP)
  + ARP Poisoning
  + Domain Name System (DNS) Protocol
  + DNS Poisoning

## Step 3

Action: Stimulate recall of prior learning.

* If this module is performed in succession to the *Wireshark Activity* module, then this would be a good time to remind students about the uses of Wireshark and Kali Linux and transmission how it will be used for this activity.
* Otherwise (or additionally), bring up popular cultural ideas of “hackers” and how they hack “in the movies”. Explain that this activity will seem very similar to the concept of gaining access to another device remotely, like what is portrayed “in the movies” (this can also be used in *Step 1* to “gain attention” as some students might become more interested after hearing this).

## Step 4

Action: Present the content.

* Explain that data is transmitted in the form of packets over the internet and various protocols are required for transmission and retrieval of this data.
* Define the following transfer and application layer protocols:
  + Address Resolution Protocol (ARP)
  + ARP Poisoning
  + Domain Name System (DNS) Protocol
  + DNS Poisoning
* Explain the above terms and how we will use these concepts in the activity.
* Use the “Alice, Bob, and Mallory” analogy to explain how we will “trick” devices into giving us packets meant for another device.

## Step 5

Action: Provide learning guidance.

* Kali Linux Demonstration:
  + Explain what Kali Linux can be and is used for. Kali Linux is an open-source, Debian-based Linux distribution geared towards:
    - Cyber Security Education and Research
    - Penetration Testing
    - Computer Forensics
    - Reverse Engineering
  + Explain the various types of tools it offers and how we will use it for this module. We will use:
    - Linux Command-line Interface – We will use packages and tools on the Linux CLI to perform the actual attack.
    - Ettercap – This module doesn’t utilize Ettercap. However, Ettercap is a tool that can be used for the same task done in this module invite the students to explore this tool after completing the module.
    - Wireshark – This is used to see how the attack happens. Wireshark allows you to see the ARP requests being sent and what ARP requests look like on the network.
* Wireshark demonstration:
  + Explain what Wireshark is.
  + Explain how to use it.
  + Show what a packet looks like and what information we can see about the packets:
    - Packet List:
      * Time
      * Source
      * Destination
      * Protocol
      * Length
      * Information
    - Packet Details:
      * Information pulled from the packet bytes.
    - Packet Bytes: (Brief insight into how the internet works…)
      * The hexadecimal information the device reads.
      * Devices actually only read binary, but hexadecimal representation allows for interpreting 4 binary bits at a time. This makes the representation more compact and take up less space on the screen.
      * Byte information is where the packet details are generated. Due to the use of protocols on the network, seemingly random strings of bytes are meaningful information to a device which can be used to send and receive information over a network channel.
      * Each protocol determines how the bytes are interpreted.

## Step 6

Action: Elicit performance (practice).

Note:

Throughout this process, encourage students to find information on their own but allow students to ask questions and acquire support as needed.

## Step 7

Action: Provide feedback.

Feedback during this module will mostly happen during the practice phase of this module. Performance is determined by whether the student was able to find information using Wireshark. Encourage students to download this tool on their computers at home and experiment with it.

## Step 8

Action: Assess performance.

Administer the post test.

## Step 9

Action: Enhance retention and transfer.

Discuss answers of the posttest with students. Explain the purpose of each question and how it applies to real-life network security.

# Hardware & Software Specifications

This section covers the materials needed to build the Wireshark Activity unit. Variations in the hardware can be used if students can still access the Wireshark application and use the internet.

## Hardware

The module unit requires the following hardware:

* Raspberry Pi 4 Model B
  + 4GB of RAM or greater
* Micro SD card
  + 32GB of memory or greater
* Power supply
  + Input: 100-240V, 50-60Hz, 1.5A
  + Output: 5.0V, 3.6A, 18.0W
* Ethernet Cable
  + Category 6 or greater
* HDMI cable
  + Micro HDMI to HDMI
* Peripherals
  + Monitor
  + Keyboard
  + Mouse

## Software

The software utilized on the Raspberry Pi 4 (RPi4) is listed below. This section also mentions the process of imaging the Micro SD card and links to resources to perform this step. Most RPi4s (units or kits) come with instructions on the setup of process.

### Operating System and Setup

* Information on Raspberry Pi setup can be found at:
  + <https://www.raspberrypi.com/documentation/computers/getting-started.html>
* Before the Raspberry Pi can be used, the SD card must be formatted, and an Operating System (OS) must be written on the card.
* For this module, **Kali Linux** OS is preferred. However, any Linux OS can be used if the software mentioned in the module can be installed. Other possible Operating Systems:
  + Ubuntu
  + Raspberry Pi OS
  + Elementary OS
  + CentOS

### Applications

* Kali Linux comes with most application pre-installed or they are at least recognized by the system and will be installed as needed.
* If another operating system is being used, you will need to download:
  + Wireshark

# References

* <https://www.kali.org/>
* <https://en.wikipedia.org/wiki/Man-in-the-middle_attack>
* [MitM Tutorial Youtube 1](https://youtu.be/GkexkyUbUd4)
* [MitM Tutorial Youtube 2](https://youtu.be/cVTUeEoJgEg)