Module 1

Wireshark Activity

Contents

Summary

In this module, students will learn about the importance of ensuring they are using secure & encrypted communication channels, especially on public networks. Students will see how applications like Wireshark can be used to watch wired and wireless internet traffic and what encrypted and unencrypted data looks like.

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 an application called Wireshark. Specifics on the hardware and software used is described in the ***Hardware & Software Specifications*** 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 a secure versus an unsecure web communication channel.
- Utilize software to view internet traffic and find an unencrypted password.
- Identify encrypted and unencrypted data.
- Define key terms:
  - ✓ HTTP
  - ✓ HTTPS
  - ✓ TLS
  - ✓ SSL
  - ✓ TCP
  - ✓ UDP

Step 3

Action: Stimulate recall of prior learning.

- Show students an example of an unsecure website.
  - ✓ Websites that don't use HTTPS are not secure.
  - ✓ Most students will probably recall when some internet searches have led them to a page that displayed the statement, "Not secure" or some related message.
  - ✓ Explain why this happens and what it means.

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:
  - ✓ HTTP
  - ✓ HTTPS

- ✓ TLS
- ✓ SSL
- ✓ TCP
- ✓ UDP

- Explain encryption, what encrypted data looks like, and how to encrypt data.
- Introduce Wireshark and explain how the tool is used to view internet traffic and i

Step 5

Action: Provide learning guidance.

- Wireshark demonstration:
  - ✓ Explain what Wireshark is.
  - ✓ Explain how to use it.
  - ✓ Show what a secure and unsecure website looks like on the network using Wireshark.

Step 6

Action: Elicit performance (practice).

- Have students open Wireshark in their workstation.
- Start by walking through the packet capture process with students.
- Have the students capture packets while you (the instructor) make simple searches on in a web browser.
- Help students identify the searches you've made.
- Once familiar with the process, challenge the students to identify another search you make.
- Next, have the students capture packets as you enter "sensitive" information into an unsecured website.
- Students will end their packet capture and search for the packet where your credentials were entered.
- Once students have found the information, the activity is done.

A variation on the activity:

Place students into groups of 2-3. Have one student perform a search to an unsecure website and enter their credentials. The other(s) will attempt to find the victims credentials.

Note:

Inform students to not use any actual passwords or sensitive information but rather a short, non-complex word or phrase.

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 post test 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.
  - Any Linux OS can be used if Wireshark can be installed.
  - Other possible Operating Systems:
    - Ubuntu
    - Raspberry Pi OS
    - Elementary OS
    - CentOS

Wireshark

- Kali Linux comes with Wireshark pre-installed.
- If another operating system is being used, you will need to download the Wireshark application.