NAIT

Edmonton Alberta

CYBR3010

Cybersecurity Foundations

Traffic Capture Lab

Student:____

Traffic Capture Lab

Objectives

This lab is a practical exercise in placing and using a protocol analyzer to capture traffic using different options.

At the end of this activity students will be able to demonstrate their abilities to place and use a protocol analyzer to capture traffic at multiple points in the network, as well as document their work.

Background:

For this lab, students will require a network that includes a minimum of 2 virtual machines.
During the activity, the students will generate and capture different types of network traffic, analyze it with the following instructions.
Screen captures can be used to provide evidence of the desired packets.

Instructions:

You will design, configure, and test a switched network in CML with at least three virtual machines (VMs). You will capture traffic from multiple points in the network simultaneously, using Wireshark, to analyze switched network behavior.

Requirements:

1. **Network Design**
   - Your network must include:
     1. One network switch
     2. One firewall (serving as the gateway for all VMs)
     3. At least three VMs configured as follows:
        a. **Client VM 1**: Has access to other VLAN clients and the internet.
        b. **Client VM 2**: Located in a different VLAN from Client VM 1.
        c. **Client VM 3**: Connected to a SPAN port, capturing traffic on a trunk link.
2. **VM Setup**
   - All client VMs must have Wireshark installed.
   - Use each VM as a packet capture point.
3. **Connectivity & Traffic Generation**
   - Configure VLANs and routing so that Client VM 1 and Client VM 2 can communicate across VLANs.
   - Generate a minimum of 3,000 packets covering different traffic types (e.g., ICMP, TCP, UDP, HTTP).
4. **Traffic Capture**
   - Capture internal traffic at multiple locations in the network **at the same time** (e.g., at the SPAN port, on each client VM).

Deliverables

1- PDF Document with screenshots and explanations

- An introduction to provide an overview of your network build.
- A network diagram of the final network identifying all capture points.
- Packet Analysis: Identify and document the following in your captures:

1. TCP three-way handshake

a. Identify the packets in the complete TCP three-way handshake process.

b. Provide a brief description of the TCP three-way handshake process and explain how you identified the packets captured as being part of the same TCP conversation.

c. List and describe the TCP options used in the conversation.

2. TCP four-way teardown

a. Identify the packets in a complete TCP four-way teardown process.

b. Provide a brief description of the TCP four-way teardown process and explain how you identified the packets captured as being part of the same TCP conversation.

3. TTL

a. Choose an IP packet that is part of communication between the two client VMs.

b. Apply a display filter to isolate that same packet in all three capture points: Source | Network (SPAN) | Destination

c. Provide screenshots from each capture showing:

TTL value | Source MAC | Destination MAC | The display filter used

d. Explain the TTL field and the MAC addresses shown, including why they differ between capture points.

2- Capture files: ***Save all capture files and name them according to the capture point in line with the diagram.***