ISEC 2077 Security Auditing
Assignment 2 – Netflow Collector Part 2 (In-Class)
(Large Assignment)

Issued Date: September 23, 2025
Due date: October 7, 2025 (In-class demonstration)

Preamble

Note: This assignment has two parts. Part 1 may be done as a team of two. Part 2 will involve individual work.

Objective: The purpose of this assignment is to demonstrate the collection and logging of Netflow records. Now that you have configured your router to capture and export Netflow, your next task was to send those records to a collector so that you can examine the traffic in your network.

In this Part 2, you will establish collectors on separate network segments, vlans and router interfaces. Note Step 1, which requires you to model the system in packet tracer first. You may wish to review your networking assignments from last year.

Requirements

You will need:

1. The router you configured in assignment 1 and 2;

2. Two computers at your pod, each of which will have a bridged VM;

3. A copy of Manage Engine Netflow Analyzer flow collector software on the bridged VM on each of your two machines. Once again, You may download a free 30-day trial edition of this software from the Netflow Analyzer website.
https://www.manageengine.com/products/netflow/

Step 1: Review the steps below and each person in your group should model the entire system in packet tracer, without the netflow collector, first. Verify with your instructor that you model is working before proceeding to the physical implementation. This is an individual evaluation step.

Step 2: Cable your computers to the switch and then to the router to create two separate private 192 networks implemented as vlans. You may use static IP's for your computers, the bridged VM's and the router interfaces**. (4 points)**

Step 3: Sub-divide your router interface into two sub-interfaces and give each a separate network address and ip number. Create two vlans on your switch, one for each desktop and VM pair. You will have to convert your cable to the router to a trunk line to carry both VMs. During the physical implementation, you may do this step together with your partner.

Step 2: Create (New) separate monitors and Exporters for both In and Out traffic on your two router sub-interfaces. Make the Monitors collect netflow version 5**. (3 points)**

Step 3: Modify the Exporters on your router to send traffic from both new Monitors to the Netflow collectors (NetFlow Analyzer) on each of your two VMs. **(2 points)**

Step 4: Send traffic from each vlan to the other and Collect any traffic you can. Display this traffic in Netflow Analyzer **(1 point)**

Step 4: Show your configuration and the captured flows to your instructor to receive credit for this assignment.

Rubric

Part 1 of this assignment is worth 10% (a total of 10 points). Part 2 will also be worth 10% bringing the total value of this assignment to 20% of your final mark and will be evaluated based on in-class demonstration to your instructor and an individual comprehension test.