# Lab 5 – Traffic Analysis

## Lab Learning Goals

This lab is a challenge to develop your traffic analysis skills. Using the provided pcap file, prepare the answers to the question contained in the lab.

## Required Resources

- **Wireshark 3.2.x** (on your laptop)

## Submission Instructions

- Complete the lab quiz: **Lab 5 – Traffic Analysis**

# Lab Scenario

You are a security analyst for Fanco Inc. working the night shift. At 11:35 PM on Tuesday night, the IDS system alerted you to a potential network attack. It looks as if the intruder is conducting a scanning attack on sections of the network. Some of the hosts in that network segment are running legacy systems that have been scheduled for replacement but may still be vulnerable to attack. You decide to look at the trace files logged on the network sensor to get a better understanding of what is occurring.

The intruder, who accessed the system remotely and pivoted through a compromised server, was not aware that network security monitoring was in place. The organization captures full content data on the network segment that the attack occurred on. Use the **Lab 5.pcap** file, answer the following questions:

1. What is the IP address of the compromised host?

   172.20.34.17

2. What type of port scan did the attacker conduct first?

   Connect scan

3. Identify the hosts that responded to the attacker with open ports.

   172.20.34.152 (MacAddr-70:5a:b6:76:18:d3)

4. What is the MAC address of the Apple device that was discovered?

   00:17:f2:24:8c:dd

5. What is the IP address of the Windows device that was discovered?

   172.20.34.152

6. What TCP ports are exposed on the Windows system?

   60368, 62056