# **MIST 400– Advanced Information Security**

# Capture the Flag (CTF) Assignment #2 (Team-BASED/ 100 points)

# Network Inspection Forensics: UnknownTrace

**Target:** UnknownTrace.pcapng

**Background** : We have got informed that a hacker managed to get into our internal network after pivoting through the web platform that runs in public internet. The hacker managed to bypass our small product stocks logging platform and then they got our customer database file. We believe that only one of our customers was targeted. Can you find out who the customer was?

**Deliverables:** Provide your answers in the template page named CTF2\_Answers\_Sheet.docx, maintain the same format please. In the first page, provide your group number and group members names. Your answer A minimum 1-page walkthrough report on how your team was able to gain access to Hack the Box and set up an account. Include a detailed description of your methods (even failed ones) and some screenshots of your progress along the way.

**In this CTF, the flag will be a string beginning with HTB{ }.**

**Requirements: You will likely need to access to the following software:**

* **Wireshark**

**HINTS:**

* **Remember how to use Wireshark**
* **Research advanced methods to string together network conversations in Wireshark.**