Lab 1 – Lab set up and Situation awareness

A. Environment set up and getting familiar with Linux/ Ubuntu.

The aim of this practical is to introduce you to the lab environment. You will use the provided virtual machine image on DLE for the upcoming lab. The installed operating system in the virtual image is Ubuntu/ Linux. Please follow the instructions of the following to get familiar with Ubuntu/ Linux.

1. Create or download the virtual machine: you can either
    a. download the provided virtual machine on DLE (see DLE/Day 1 section, find "Lab VM : password "student") (which is an older version of Linux) or
    b. create your own machine by following the instruction "Set up your own VM" (see DLE/ Welcome section). Install Wireshark, Snort on your own VM
2. Watch and follow the steps in the provided video "Help material - Run linux virtual machine", using the downloaded image.
3. Read and follow the steps in "Help material - Intro to Linux"
4. Read and follow the steps in "Help material - Ubuntu manual"
5. Install Splunk: Download and follow the instructions to install SIEM
   https://help.splunk.com/en/splunk-enterprise/get-started/search-tutorial/10.0/part-1-getting-started/install-splunk-enterprise#a686eb97_b6b4_4692_b0db_daeda6df1f98__macOS_installation_instructions

B. Group work: Find 1 recent attack by APT in Sri Lanka or United Kingdom and

1. What is the name of the identified APT and its identification in Mitre ATT&CK
2. In which country is the APT based?
3. Which ATT&CK technique ID maps to their Reconnaissance tactics?
4. Which ID is associated with the identified technique in question 3?
5. Which software/tool is the group known to use for Command and Control (C2)?
6. What Detection Strategy ID would you implement to detect the tool identified in question 5?
7. Present on how you find the answers above