CSI2450 – IoT and OT Security

Assessment 2: Case Study

Assessment: Case Study
Weighting: 40% of the final mark of the unit
Due Date: See Blackboard *(under Assignments> Assessment Overview)*

Before you proceed, make sure you have read the Video-based Assessment Common Guidelines.

Assignment Overview:

This assessment is aligned to the following learning outcome of this unit:

ULO3: Propose security countermeasures and threat mitigation strategies for IoT and OT.

The knowledge and skills you learnt through Modules 1 to 5 will be required for this assessment. You may use your own virtual environment; however, the Azure virtual lab is the recommended environment for this assessment.

Scenario:

Ports are critical components of a country's economy and play a vital role in its international relations and global competitiveness. They are important for several reasons such as: trade, economic growth, strategic importance and infrastructure development. Port security is vital to protect against terrorism, prevent illegal activities, protection of national borders, protection of economic interests, and compliance with international regulations. Ports are identified as one of the critical infrastructure sectors covered by the Security of Critical Infrastructure Act (SOCI), along with sectors such as energy, telecommunications, and water. As such, owners and operators of ports in Australia are required to comply with the security obligations set out in the Act, and to report any security incidents or threats to the government.

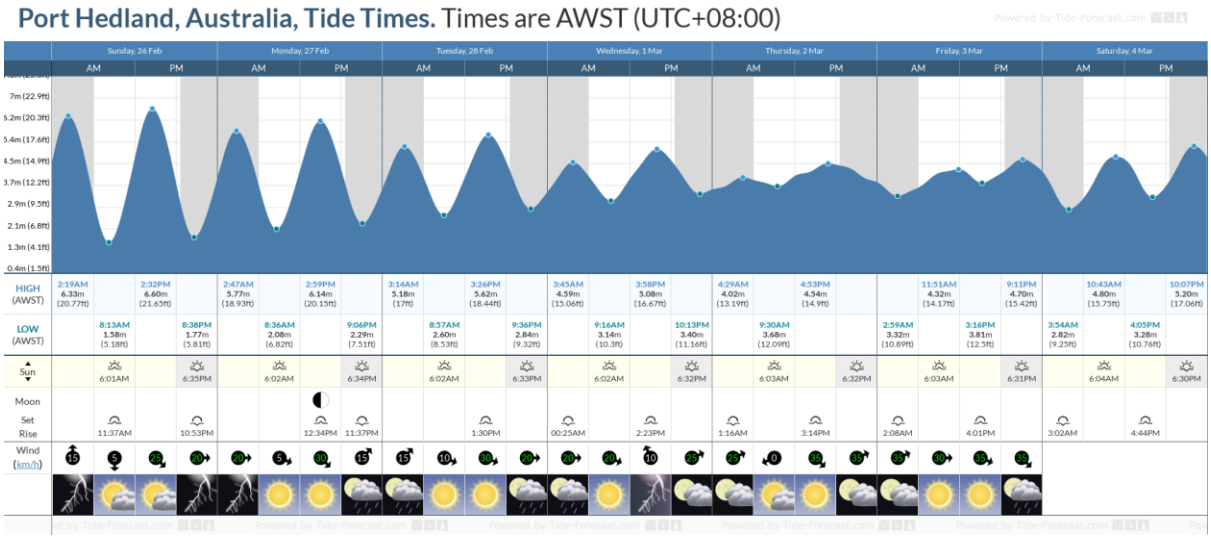
Ports rely heavily on technology and computer systems to manage their operations, including cargo tracking, vessel scheduling, and communications. This reliance on technology makes them vulnerable to cyber attacks, which can cause significant disruptions to their operations, compromise sensitive data, and pose risks to the safety and security of personnel and cargo.

Accurate and up-to-date tide data is essential for port authorities and ship captains to make informed decisions about navigation, berthing, and safety within the port. The following are some reasons why tidal data is important:

1. Navigation: Tides can have a significant impact on the depth of water at a port, and therefore on the ability of ships to navigate safely. For example, low tides can cause problems for ships with deep drafts, while high tides can make it easier for ships to enter or leave a port.
2. Berthing: Ports also need to know the tide data to determine the best times for ships to enter and leave the port, and for berthing at docks. If the tide is too low, ships may not be able to dock, while if the tide is too high, the ship may not have enough clearance under bridges or other structures.

3. Safety: Tides can also affect the safety of navigation within the port. For example, strong tidal currents can make it difficult for ships to move or can cause them to drift off course, potentially leading to collisions or other accidents.
4. Environmental concerns: Tides can also play a role in environmental concerns at ports, such as in the case of tidal energy projects or the management of pollutants or other waste materials.

The following is an example of tidal data for Port Hedland in Australia. You can more information from tide-forecast.com



Source: https://www.tide-forecast.com/locations/Port-Hedland-Australia/tides/latest

Tasks:

You are recommended to use the Azure Virtual Lab environment provided to you in the course. Alternatively, you may use another virtualisation setup on your own machine. In the latter case, supporting you by the lecturer/facilitator to troubleshoot technical difficulties related to your setup such as VMware/VirtualBox will be limited. If you are using the Azure lab, please make sure you maintain a backup of your work outside the Azure lab. If a reset of the lab is required, all data in the Azure lab will be lost.

You are required to use the following three VMs provided to you in Azure.

1. Client VM
2. Server VM
3. Monitor VM

Configure your environment based on the following requirements:

Client VM Requirements

- The purpose of this VM is to act as a MQTT Publisher to publish tide values to the MQTT Broker
- Based on the scenario provided above, determine a tide range. (Hint: use high and low tide values that are reasonable based on the tide data from tide-forecast.com website).
- The publish topic must be “port-tide”.
- Do not use authentication.
- Create a script to publish the tide values every 5 seconds.

Server VM Requirements

- The purpose of this VM is to act as the MQTT Broker as well as the MQTT Subscriber.
- Ensure the MQTT Broker is configured to provide the required functionality for the MQTT Publisher (Client VM).

Monitor VM Requirements

- The purpose of this VM is to investigate the traffic between the Client VM and Server VM.

Note: This VM on Azure is already configured to be on promiscuous mode to detect network traffic in the subnet. If you are using your own environment, ensure you have configured your virtual machines appropriately.

- Configure the IDS to alert if any MQTT traffic is from other sources except the Server VM and Client VM.

Video Recording (Submission)

You are required to complete the following tasks and submit in the form of a video recording.

1. Give an introduction of yourself and overview of your setup. You can give an overview of the setup by showing each VM, explaining its purpose, and displaying its IP address.
2. Show evidence that the MQTT Broker service is running and conjured as required in the above requirements.
3. Show evidence that the MQTT Publisher is publishing the tide values using the required script. Additionally, run the MQTT subscriber command on the MQTT Broker and show that the tide values are being received as expected. Keep the publisher and subscriber running for the rest of the tasks.
4. Capture network traffic from the Monitor VM. Identify and explain the publish and subscribe traffic. Your explanation should include: TCP/IP handshake, the source and destination information, ports, protocols, and MQTT payload.
5. Perform an FDI attack on the MQTT broker using the Host machine. You are required to inject an out-of-range tide value to the MQTT broker. Verify from the MQTT Broker to check whether the attack was successful. Was the attack successful? Explain the outcome.
6. Did the IDS alert this attack? Explain the outcome.
7. Implement authentication on the MQTT Broker and MQTT Publisher.

Note: You do not need to record when you are making these configuration changes, however, you need to show the relevant configuration files to show that you have implemented authentication.

8. Repeat the FDI attack again (assume the attacker does not have valid credentials). Was the attack successful? Explain the outcome.
9. Implement one additional security control to further strengthen the security of the MQTT Broker. Justify your solution.