Educational Challenge:

Contestant Packet B

21-23 SEPTEMBER 2018

Last Updated: 09/13/2018

POINTS AVAILABLE: 0

Challenge 1: Establish Your Battle Station

Situation: To effectively navigate this event, you will need a capable and properly configured computer. You will be asked to complete tasks such as network mapping, packet capture, and vulnerability scanning, among others.

Mission: Properly configure your laptop to be able to complete challenges. To begin challenges, have at least Nmap and Wireshark installed.

Linux-Recommended Distributions

Ubuntu 18.04 LTS-https://tutorials.ubuntu.com/tutorial/tutorial-install-ubuntu-desktop

Kali Linux 2018.2-https://docs.kali.org/category/installation

Notes:

- One of the simplest ways to install these operating systems is by creating a live boot USB drive. If you have at least a 4GB USB drive, follow the documentation provided above.
- Please note the difference in system architecture, or the difference between 32 and 64-bit systems. A 64-bit capable system will run a 32-bit operating system, but not vice versa.

Nmap

Nmap 7.70-https://nmap.org/book/install.html

Notes:

- Operating Systems: Nmap is available for any Unix-based OS as well as Windows. If you have Kali Linux installed, Nmap is a default program. Depending on your OS of choice, follow the Nmap install instructions at the above link.
- Nmap is a command line-based program. Should you desire a simple to use GUI for Nmap, please look into ZenMap-https://nmap.org/zenmap/

Wireshark

Wireshark 2.6.3-https://www.wireshark.org/#download

Notes:

- Wireshark provides a feature-rich GUI to users that wish to monitor traffic. It is available on Windows, macOS, and Linux-based systems. Download and install is straightforward

Actisense NMEA Reader

NMEAReader 1.5.1.7-http://www.actisense.com/media

Notes:

- The Actisense NMEA Reader software provides a simple to use GUI interface for the reading of NMEA2000 messages. While also possible with open source CAN dump software, this software paired with the connected NGT-1 provides a simple interface to familiarize yourself with NMEA2000 message format.

OpenVAS

OpenVAS 9-http://www.openvas.org/news.html#openvas9

Notes:

- OpenVAS is an open source vulnerability scanning forked from Nessus. It provides a GUI interface to perform a vulnerability scan and assessment of a system.

POINTS AVAILABLE: 900

Challenge 2: Map the Network

Situation: After successful recovery of the ship manifest, it has been deemed necessary to further reconnoiter. Target ship is docked in port for an undisclosed amount of time. The crew has been observed preparing for departure, and is expected to depart within the hour.

Mission: Map both the IT and NMEA2000 Networks.

Execution: Fill in the following network worksheets, on the following pages, and return to judges for scoring. Please return open, unfiltered TCP and UDP ports. The first portion of this worksheet involves mapping devices on the IT Network of the ship, of which there are a total of (6). The second portion of this worksheet involves mapping the NMEA2000 devices on the ship, of which there are a total of (10).

Tools: Nmap; Actisense NMEAReader

IT Network Worksheet

Device Name	IPV4 Address	TCP Ports	UDP Ports

NMEA2000 Network Worksheet

Task: Fill in the blank worksheet with information NMEA2000 network to the best of your ability.

Mftr. Model ID	Source ID	Mftr. Product ID	Mftr. Serial ID	Unique ID	ISO Device Function	Device Class	PGN List

POINTS AVAILABLE: 900

Challenge 3: Packet Capture

Mission: Complete a packet capture on the voyage network. Capture and analyze at least three packets containing distinct types of information.

Execution: Utilize packet capture software to sniff the network and extract potentially useful information.

First Packet:

Source IP	Destination IP	Protocol	Information Retrieved

Which TRUDI device was the source of this packet?

Which TRUDI device was the destination of this packet?

What type of information did you find in this packet?

Second Packet:

Source IP	Destination IP	Protocol	Information Retrieved

Which TRUDI device was the source of this packet?

Which TRUDI device was the destination of this packet?

What type of information did you find in this packet?

Third Packet:

Source IP	Destination IP	Protocol	Information Retrieved

Which TRUDI device was the source of this packet?

Which TRUDI device was the destination of this packet?

What type of information did you find in this packet?

POINTS AVAILABLE: 1000

Challenge 4: Vulnerability Detection

Situation: Your initial network analysis has uncovered potential network vulnerabilities.

Mission: Conduct a vulnerability analysis of three devices on the network to determine any possible configuration vulnerabilities.

Execution: Fill out the following:

Device	
Host IP:	

List the discovered vulnerable ports and the associated service (such as HTTP) it provides.

Port Number	Service

Use the following format to submit vulnerabilities:

Port/Service:

Threat Level/CVSS Score:

Vulnerability Description:

Vulnerability Mitigation:

Port/Service:	
Threat Level/CVSS Score:	
Vulnerability Description:	
Vulnerability Mitigation:	

Port/Service:	
Threat Level/CVSS Score:	
Vulnerability Description:	
Vulnerability Mitigation:	

POINTS AVAILABLE: 400

Challenge 5: Decoding AIS Packets

Challenge: Dissect and decode an AIS packet to understand what our ship is broadcasting to vessels around it.

AIS Packet Fields

Sift through your captured packets to find one containing AIS data. AIS data packages contain seven fields separated by commas; fill in each one below to the best of your ability.

Identifier	
Fragment Count	
Fragment Number	
Sequential Message ID	
Radio Channel Code	
Data Payload	
Fill Bytes	

Decoding the Data Payload

Retrieve key information from the data payload you found above and fill in the chart below.

MMSI	
Navigation Status	
AIS Message Type	
Call sign	
Latitude	
Longitude	
Speed	
Heading	
Course Over Ground	
Rate of Turn	

POINTS AVAILABLE: 450

Challenge 6: Identify GPS Components

Challenge: There are several separate components on board that record GPS data. For each component, find where the GPS data is transferred to and identify a GPS data packet to include latitude and longitude information.

Sentence 1:

Information Found

Sentence 2:

Information Found

Sentence 3:

Information Found

POINTS AVAILABLE: 350

Challenge 7: Autopilot

Challenge: The autopilot system works hand-in-hand with the TZ Touch Chart Plotter. Change the destination of TRUDI on the chart plotter and capture the NMEA2000 message sent to the Autopilot system. Determine where the destination's location is with the captured message.

Packet Captured:

Packet information:

POINTS AVAILABLE: 500

Challenge 8: Email Server

Situation: The ship captain has lost his email username and can't even remember the users on the ship. He is desperately trying to get to his ship manifest, as he forgot how many pineapples he has on board.

Mission: Discover all usernames on the email server and submit the following worksheet. Bonus points will be awarded for a successful submission of the ship manifest.

Execution:

Username	Email Address

Ship Manifest

- The ship's manifest is titled TRUDI Manifest
- Please submit the ship manifest in any of the following formats:
    - .xml .xlsx .pdf

POINTS AVAILABLE: 900

Challenge 9 Engineering Network

Challenge: The depth, speed, and temperature sensors are key components of the engineering network, helping to actuate the ship's steering, propulsion, and auxiliary systems. Develop a method to recalibrate a different depth, speed, or temperature offset. **Note:** You must develop the method to recalibrate these fields, you may not have enough time to perform the calibration.

Device:

Water Depth:

Relevant PGN	Field

Speed:

Relevant PGN	Field

Temperature:

Relevant PGN	Field

You will receive 50 points for correctly identifying PGNs and Fields.

POINTS AVAILABLE: 750

Challenge 10: Develop a Defense

Challenge: With the guidance of your mentors, develop a cyber defensive strategy for maritime networks. You will develop a concept on how to better secure systems aboard TRUDI and will be presenting it to a panel of maritime network subject matter experts.

Presentation length: Maximum 7 minutes

Please sign up for a time slot to present with an event judge.

The panel will utilize the following rubric:

Category	Low 0 Points	Adequate 75 Points	High 150 Points
Team communicated a thorough understanding of TRUDI's vulnerabilities			
Team communicated a thorough understanding of how malicious attackers might exploit these vulnerabilities			
Team developed an effective security strategy for defending TRUDI from malicious attackers			
Team developed a creative security strategy for defending TRUDI from malicious attackers			
Quality of team's presentation			