



**MARITIME**  
& CONTROL SYSTEMS  
CYBERSECURITY CON

# ACADEMIC VILLAGE PLAYBOOK

**HACK**  
THE PORT 22

Version 1.4.020122



dreamport

Copyright 2022 MISI All Rights Reserved



<b>Who</b>	Students attending Center of Academic Excellence in Cybersecurity accredited colleges, Senior Military colleges, US Cyber Command Academic Engagement Colleges. Students attending other colleges can field teams as well as long as there is space. Key Skills: (Programming/CTF/penetration testing experience encouraged)
<b>What</b>	Hack the Port Academic Village Cyber Exercise and Learning Experience
<b>Where</b>	Ft. Lauderdale Florida, Broward County Convention Center
<b>When</b>	21 – 24 March 2022. Participants need to be ready to engage onsite and virtually 9:00am, March 22, 2022. Badge and other materials should be picked up Monday 03/21/2022.
<b>Why</b>	Increase knowledge, skills and awareness of critical infrastructure cybersecurity and tactics and techniques used to defend and attack maritime and related industrial control, IoT, and IT systems. Learn about the role maritime cybersecurity represents to the nation security and supply chain.



# Introduction



In our Hack-the-Port (HTP) academic village, we have created a hands-on and virtual experience that provides participants with multiple cybersecurity industrial control and related systems, using a maritime transportation sector (MTS) focused theme. The goal is to highlight how the critical infrastructure sectors of the United States intersect at a maritime facility and how attackers may target these sectors to cause harm to the United States through our businesses and infrastructure. Before deciding if you want to participate, we encourage you to read up on the role of maritime cybersecurity and the increased number of cyberattacks to this sector and the descriptions of the critical infrastructure

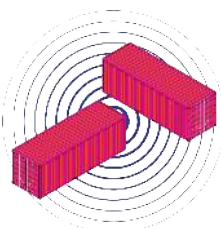
sectors as described by the Cybersecurity & Infrastructure Security Agency (CISA) on the following URL:

<https://www.cisa.gov/critical-infrastructure-sectors>

## What do you do in a village?

Well normally, you visit and take in the sights. In our village it's different. We want some visitors willing to cause trouble and we want others looking to find trouble and stop it. We are looking to award prizes for RED teams who can successfully complete each offensive cyber operational (OCO) scenario without detection and for BLUE team personnel who demonstrate applied knowledge of defensive cyber operations (DCO) to find Red Team attackers without any assistance from MISI personnel.

In this playbook, we introduce our story of Port Cosmar and describe the OCO scenarios we have designed specifically for this Village. We also will discuss how participants will be able to execute defensive cyber operation response actions (DCO-RA) to defend Port Cosmar in real-time. While we aren't giving away the farm here, you will learn all you need to know about participation, and you can determine if you wish to sign-up.



Please be aware, we want to put on best event possible. The actual scenarios we execute are subject to change. We will publish alerts if we change or substitute scenarios prior to the execution of this event.

In this academic village, each scenario will be physically setup in a self-contained section within the convention ground areas or remotely connected facilities if required. All scenarios will be connected via the same physical networks, but you should plan to work on each scenario and amass points to be considered for any awards. We will discuss how participants will be evaluated later. You should plan on being close to the physical scenario if possible and may be offered a chance to interact with the components under strict supervision and for a very limited time window. You will be required to expand access from an initial starting point of low privilege.



## What is Port Cosmar?

To have a realistic event, we need a port to 'hack'. Since we will never interact with live operational port targets on-location, we must create our own port as it is our mission that for any MISI exercise, "it's got to be real". Port Cosmar is the fictitious port story we have created for this event. Your job will be to attack (attempted of course) Port Cosmar by attempting (or stopping) various attacks against Port Cosmar maritime and related interconnected systems. We are exposing various real-life control systems and information technology assets during HTP, and you will interact with these systems either by attacking or defending these assets. Many of these systems are found in real ports around the world. You won't be damaging any property or causing any bodily harm, but you will have a chance to get your hands dirty and you may even get wet. Each scenario will be self-contained on tabletops requiring only wall power and network connectivity.

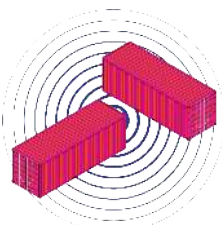


Port Cosmar has a functional network with wireless and wired connectivity running traditional information technology assets and like many port facilities today, will include assets in the cloud. In addition, we will tell you that the simulations of the following types of control systems can also be found within Port Cosmar:

- Gantry Crane
- Liquid Flow Rate Monitoring
- Liquid Storage and Transfer
- Backup Power Monitoring

We know that Port Cosmar does have an online presence it is dedicated to this HTP event only. This includes at least 1 website and online collaboration services. We will release details about the online points of presence as the HTP event gets closer to starting.

To prepare for Hack-The-Port and this competition, we studied laws, requirements, recommendations and even past attacks against MTS and maritime facilities throughout the world. We learned that maritime transportation contributes to one-quarter of US GDP, or some \$5.4 trillion<sup>1</sup>. We learned about the



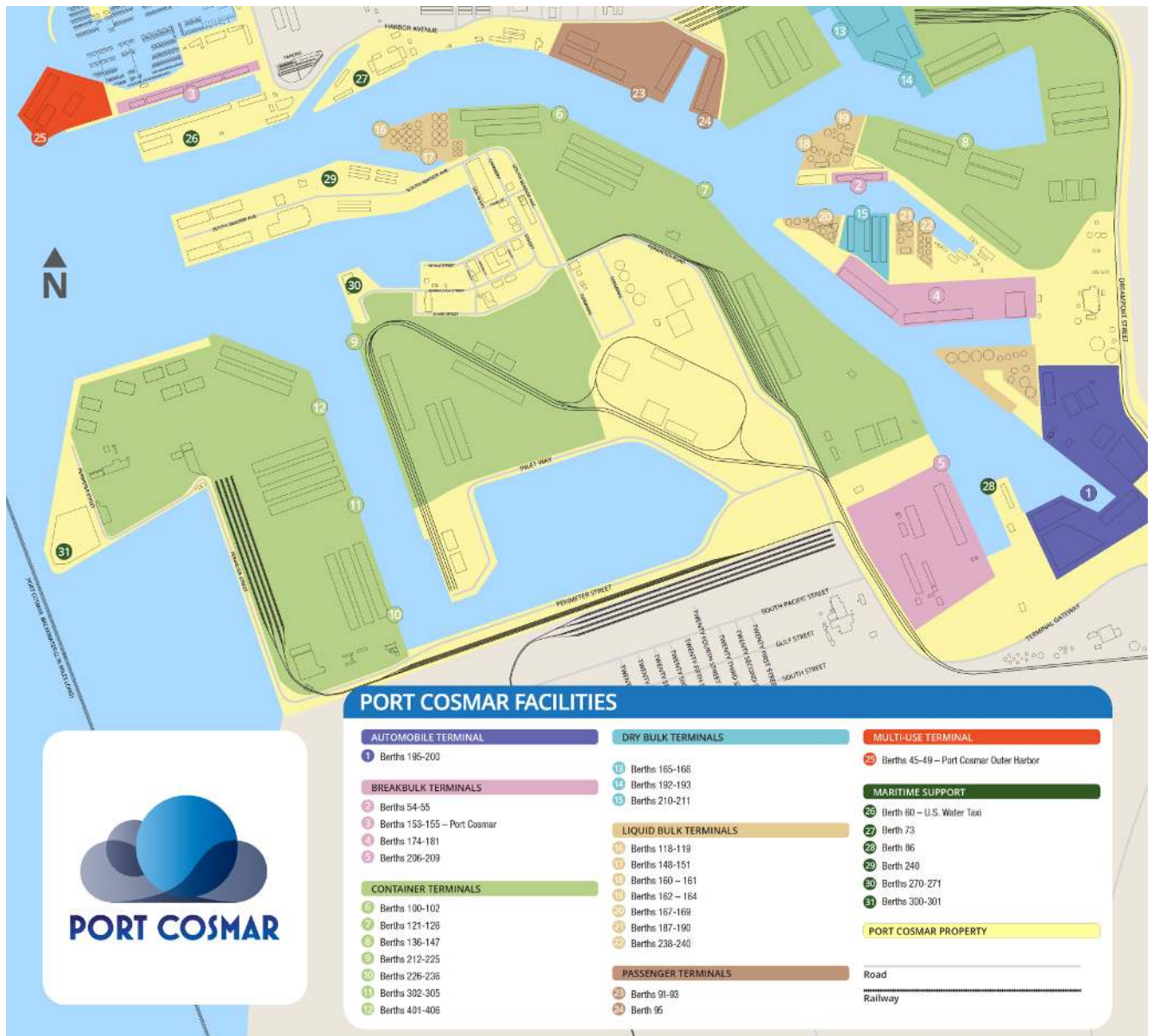
Port Cosmar is fictitious. Any similarity to a real location, person or entity is entirely coincidental. No property or persons will be harmed in the execution of the academic village cyber exercises for Hack-The-Port.

---

<sup>1</sup> <https://www.ttnews.com/articles/ports-shipping-industry-responsible-26-us-gdp-study-says>



The following image is of the map of the fictitious Port Cosmar:



Hack-The-Port, we will be implemented in part in the cloud using Amazon Web Services (AWS).

## Open-Source Intelligence (OSINT) on Port Cosmar

A typical initial task for a RED team member during a penetration test is to learn about their target using publicly available information. This type of information is commonly referred to as open-source intelligence or OSINT. The MITRE ATT&CK framework will call this reconnaissance ([TA0043](#)). OSINT can be leveraged to identify physical locations and assets to target, or even employees that are possible targets for phishing or USB device drops. We are certainly not going to tell the RED team what to look for, but we will reveal that Port Cosmar will have several employees with valid email addresses and will operate a website that may or may not reveal important details for RED team members. We believe the Port Cosmar website will be hosted in AWS and the employees may utilize cloud services for file sharing and communication.

BLUE team be careful. You may want to consider reviewing the same public resources to learn what the RED teams may know about!

## MITRE ATT&CK

Throughout this playbook we will make reference the MITRE ATT&CK knowledge base. We consider this an extremely valuable resource for describing cyber-attacks, but the reader should note that we may be using ATT&CK to reveal a hint or two for our RED teams. If you are interested in participating in Hack-The-Port and the academic village you are urged to familiarize yourself with the ATT&CK Matrices found here:

- <https://attack.mitre.org/>
- [https://collaborate.mitre.org/attackics/index.php/Main\\_Page](https://collaborate.mitre.org/attackics/index.php/Main_Page)

## Scenario Difficulty

When we present a scenario in our playbooks, we provide an estimated level of difficulty associated with it. This difficulty is meant for a Red Team participant only. We use five (5) levels to describe the difficulty of each scenario and we present a description of each level here for your review. Remember, this is our interpretation of the difficulty required to be successful. We have learned to encourage people with no pre-existing skills in Industrial Control Systems and protocols if they are willing to learn on the fly. This is one of the best marks of a successful red or blue team operator. If you can adapt, you will be successful. The difficulties we use to describe our scenarios are:

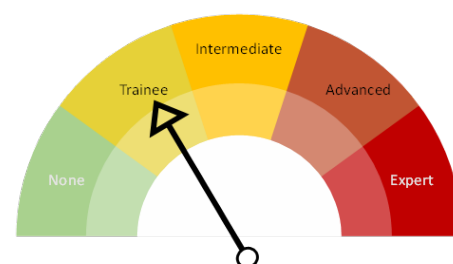
Difficulty	Description
None	A scenario rated as 'None' difficulty means that we consider the answers or actions required as obvious. Usually only one action is required to be successful. Enter a default password, make a single HTTP POST/GET, sniff a value from the network. Crack a key or password which is on a wordlist returning in seconds. We don't expect any coding for scenarios rated as 'None' in difficulty. Scenarios rated as 'None' in terms of difficulty are considered trivial for a blue team defender to identify including the source addresses of the attackers.
Trainee	A scenario rated as 'Trainee' means that someone with less than 1 year of experience should be able to be successful. This will require more than 1 action but examples or descriptions of all the actions required are either provided or can be found with simple Google Searches. These scenarios also will almost never require you to infer a command line argument or determine which tools to use but we may require single line changes to code and scripts for these to be successful (typically changing hard-coded arguments or values that cannot be specified on the command line). We do give hints for scenarios rated as 'Trainee' level of difficulty. Scenarios rated as 'Trainee' in difficulty will be easier for a blue team defender to spot but not as trivial as those rated as 'None'.
Intermediate	A scenario rated as 'Intermediate' may require more than 1 year of experience to complete successfully. This will require multiple steps to achieve success and very few of the follow-on steps or actions will be described in advance. The key with Intermediate Difficulty is the demonstration of applied knowledge. If you are told to achieve an outcome on a target, you first must solve the issue of access to the network, then recon to identify the target followed creation of payloads to achieve your desired outcome. You will have to write code to achieve your goals for a scenario rated 'Intermediate'. This is the first level of difficulty where we consider it equally difficult for a Blue Team member to spot the attack as it is for the Red Team to perpetrate.
Advanced	A scenario rated as 'Advanced' is considered a direct extension of one rated as 'Intermediate'. Here you will have to write more code, work harder for initial access, even perform reverse engineering or use of tools non-standard tools such as software defined radios, programming embedded systems and using programming languages such as C and C++. One concrete example of the difference between an intermediate and advanced scenario will be the injection of industrial control traffic to perform basic functions such as turning off power to an output versus specific traffic to turn off power to some inputs while enabling power to others which means you must understand the input and output states of your target PLC or device.



Difficulty	Description
Expert	The most difficult scenarios we will ever execute. A scenario rated as 'Expert' will require assistance or input from someone with multiple years of experience, more than 5 years and usually more than 10. This will require performing 1 or potentially more actions completely from scratch such as reverse engineering a sample file or constructing your own tool that executes multiple functions. An expert scenario will require difficult work to remain undetected.

NOTE that there is an implicit assumption of existing skill you will bring to Hack-The-Port. The ideal participant in this academic village has some prior exposure to penetration testing, network security assessments, or vulnerability and reconnaissance scanning. If you come to this event understanding industrial protocols such as MODBUS, S7 or EtherNet/IP you will have advantages over your competitors. While we want all interested parties to be involved, you will require some skills to compete.

We will use a simple graphic gauge to indicate our assigned difficulty level for a scenario as follows where an arrow will indicate the difficulty level whose description can be found above in this section.



## Registration

You will be required to register for the academic village to participate. The registration details for the Academic Village at HTP can be found online at:

<https://www.hacktheport.tech/http-academic-village/>

## Execution

We are working on details for the actual execution of the academic village. We strongly encourage you to check-back each week as we establish more details on how the execution of the event will occur. What we can describe now is the following:

- All on-site RED Teams will be positioned in the same physical space at separate tables
- BLUE Teams will be in visual sight of RED Teams but out of earshot.
- The operating hours of each day of our Academic Village will be: 0800 – 1500
- If a BLUE Team member catches a RED Team, they will be able to sever your network access for increasing periods of time
- BLUE Teams will always have visual sight of all stations of the Academic Village whereas RED Teams may not be able to see all stations

## Schedule

Currently the Academic Village is schedule for the following dates:

22 – 25 March 2022, with an estimated end time of 1100 EST, Friday March 25, 2022.

## Controlling Team Access

We reserve the right to schedule each RED team for specific scenarios during the academic village provided you obtain persistence off your ship and on the Port Cosmar networks

successfully. We will NOT inform the BLUE team of any of these details if we choose to implement this strategy. RED team personnel will be required to submit request for exploitation of any resource, and we can use this to inform a team if they are not permitted to attempt an offensive action until a certain time on the clock.

## Exclusion List

We will use an exclusion list (also referred to as a blacklist) during execution of this event to indicate assets which are expressly prohibited from attack or interaction. An asset may represent an IP address, CIDR address, website or even a specific URL on a target on the network. All participants must abide by this list and will receive only 1 warning if they interact with an asset that has been excluded from interaction. Repeated interaction with restricted or excluded assets will result in removal from the event. Participants will need to learn that they must exercise caution when interacting with a control system (e.g., programmable logic controller) or the device may hang or become corrupted.

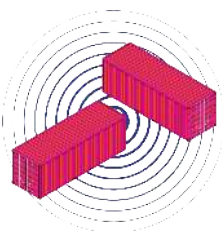
## Scoring

We will be scoring RED team members on their ability to successfully complete the scenarios defined later in this playbook. We utilize [CTFd](#) for tracking team performance and will release a specific site for scoring closer to the event date. Any users with experience with [CTFd](#) should know we are not just looking for a single flag for each scenario. As a RED team member, you should be carefully watching everything to see if there are other flags you can supply to gain points in each scenario. Flags can be almost anywhere.

**To repeat, RED team personnel will be issued a separate invitation to the CTFd server.**

## Network Traffic

Thanks to our partners, we will have full packet capture capabilities for analysis and facilitating execution of an RPE event during the HTP festivities. Several cyber security technologies will be available for BLUE team personnel that utilize this PCAP data for live analysis. This PCAP resource will be available for BLUE team and RPE participants only.



Please be aware, we will not release PCAP from this event to any party that is an active participant (all types of training included), an authorized representative of the United States Government or a MISI partner. RPE participants are considered valid.

## Remote Command and Control

We want to pause for a second and discuss usage of remote command and control (C2) assets during this event. You can assume the Port Cosmar network is connected to the Internet. If you successfully expand access off the 'ship' network (where you started), you may need to control Port Cosmar assets via remote cloud-connected servers. We will not stand up any cloud-connected asset for you during this event. You are responsible for all cloud assets you require for successful operations during this event. You will be required to report on IP addresses used for cloud assets during exploit attempts.

## Awards

We are planning awards for top performing teams within the academic village. We will release further details about the possible awards on the event website.

## Communication

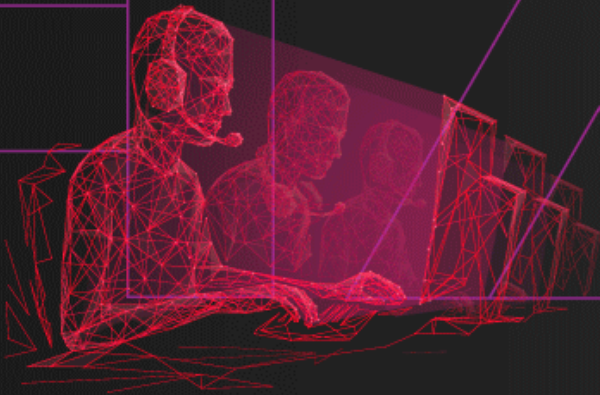
We will utilize a [Discord](#) Server for this event. We will release an invitation link to all registered participant email addresses as the event date comes closer. As with previous events, each team will be separated into different channels. You are strongly encouraged to monitor the Discord Server during normal business hours in the event we need to reach you. If you do not respond to 3 attempts to contact you, your remote access will be immediately terminated until we can discuss whatever issue caused us to reach out to you in the first place.

## Video

We do plan on recording video of each scenario during the academic village. We will not purposefully record any academic teams, but you should be aware that if you cross in-front of cameras recording a scenario you may be inadvertently recorded as well. We reserve the right to stream this video to Twitch or YouTube. Your participation in this event includes a explicit agreement to use your image in any promotional material, video, social media, press releases and websites.



# Teams



## Teams

We discuss the roles you can fill when you participate in the Hack-The-Port academic village here. We need two (2) types of participants in the academic village: RED, and BLUE. We will discuss each team type separately next.

## Remote Participation

With respect to the current COVID-19 pandemic, we have made the decision to allow remote participation in the academic village. We will accept both RED and BLUE remote participants but be forewarned, remote RED team personnel may require additional expertise in networking to achieve success in at least 1 scenario. You need to understand that if you are unable to gain remote access, you may not be able to attempt any of the scenarios we describe in the next section. There will be multiple paths for remote access, do not worry. Remote access adds to the realism of the cyber exercise.

We encourage remote participants to act as OSINT researchers for your team.

Remote RED team participants may be required to connect to the conference networks via a virtual private network (VPN) connection, but you should be fully prepared to use remote attacks to attempt to gain access to the Port Cosmar networks. We will provide a limited number of on-site computers for executing non-standard actions for remote users only which will be accessible through the VPN connection.

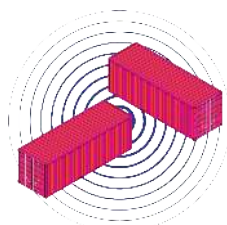
The Blue Team technologies for monitoring Port Cosmar networks are largely network and web-based so there are no expected complications for remote Blue Team personnel if they utilize the VPN connection, they are issued to access village resources.

We will not issue more than five (5) VPN accounts for each remote team.

## Team Rules

We have several rules we must ask you to abide by to participate:

- On-site teams can be no larger than five (5) participants
- Teams can have spectators and supporters that must sit in the spectator area
- Absolutely NO party may execute any action against Port Cosmar online resources until they are given an official start via Discord.
- Each college can field a team five (5) on-site RED team participants and a team of 5 off site (virtual participants).
- Teams must sign and submit an electronic rules of engagement (ROE) PDF prior to the cyber exercise
- Remote Participants must provide source IP address information to MISI
- You must leave any remote code execution vulnerability you find alone but are free to change passwords or create new user accounts unless you are told otherwise.
- Teams agree to leave each other alone, no snooping or spying of screens will be permitted.
- Teams agree to NEVER perform any denial-of-service activities (WIFI actions will be permitted in 1 scenario only)
- Teams agree to report all activities executed and to not engage in any dishonest, illegal or immoral actions up to and during execution of this event.



We cannot stress this enough, if you stray from the approved target list, you will be removed from the competition.

## RED

Offensive or [RED](#) teams are being asked to carry a specific mission for each scenario in the Hack-The-Port Academic village. We strongly urge on-site teams to bring at least three (3) participants for this event, but you may have up to five (5) on a single RED Team. Each mission may require the creation of prototype code to inject, replay or alter traffic to achieve a specific effect. You should be ready to write code (e.g., Python, C or JavaScript), capture network traffic (PCAP), perform network reconnaissance, crack passwords, reverse engineer files and PCAP, and operate remote access programs such as Metasploit, PowerShell Empire, Veil, BEEF, Pupy, and others.

### Expected Skills

We suggest the following skills are required to be a successful RED Team:

- Python (requests, scapy, pymodbus, python-snap7, pyshark, BACpypes)
- Network Recon (nmap, masscan, s7scan)
- Wireless Surveys (Kismet, airodump-ng, hcitool)
- Payload Building (msfvenom, empire, veil)
- PCAP Analysis (Wireshark, tcpdump)
- Vulnerability Scanning (OpenVAS, Nessus, nmap NSE Scripts, openscap, lynis)

## BLUE

We are not only looking for RED teams for our Academic Village. We want to find the group of participants who are eager to defend the facilities of Port Cosmar during our academic village operation. This is commonly referred to as a [BLUE](#) team. You will be granted administrator access to the networks and systems, and if you successfully spot an attacker, you will be granted permission to execute what we call defensive cyberspace operation response actions upon approval from MISI. The center piece of the BLUE team arsenal will be Elasticsearch. BLUE Teams will be granted access to a full Elastic Security Stack for the academic village that will include:

- Syslog
- Windows Log(s)
- Netflow
- PacketBeat

How will BLUE teams compete? A BLUE team member's job is to spot an attack in progress or that has completed and attempt to determine things such as:

- What was the source address of the attack?
- When did it start? When did it stop?
- What was attacked?
- Is it on-going?
- What is the potential impact of the attack?



- What are the TTPs that are being used in this attack?
- Are there any Indicators of Compromise (IoC) that we can capture and share?
- Can we mitigate this attack?
- Can we prevent it from happening again?

As we stated previously, we are using a Discord Server for communication and your job as a BLUE team defender will be to publish a Significant Action or SIGACT alert within the BLUE team channel if you discover an attack. You can then request a DCO-RA to respond which we will discuss shortly.

## Expected Skills

The following skills are required to be a successful BLUE Team:

- Kibana Search/Query
- Kibana Visualization
- Log File Analysis
- PCAP Analysis
- Netflow Analysis
- Cisco IOS

## DCO-RA

A Blue Team can execute defensive cyber operation response actions or DCO-RA to defend a network. We are challenging BLUE Teams to plan to execute DCO-RA for this Academic Village. While we have multiple DCO-RA actions planned, we will reveal now that BLUE team personnel will be permitted to request any of the following actions:

- Block MAC address from Port Cosmar WIFI
- Kick MAC address from Port Cosmar WIFI
- Change WIFI passwords on Port Cosmar WIFI
- Change User Passwords
- Revert/Reinstall Hosts
- Disable Network Ports
- QoS Network Ports

Team members will be permitted to request these actions through Discord, and we will rule on the action and assist in the execution if sufficient evidence is provided. We will not inform RED teams of any DCO-RA actions that are executed against them.

## Vendor Interaction

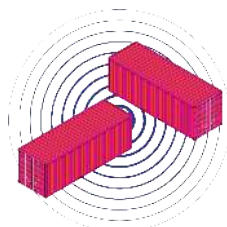
One of the most interesting aspects of the BLUE team is that you will be able to interact with vendors of advanced cyber security technology who are donating their solutions for the HTP event. We already have multiple vendor commitments, and you should leverage this opportunity as free training on some of the most advanced ICS security platforms in the market place.

## Initial Story

The initial story for the Academic Village depends on the participant. For RED teams we may have on-site or remote participants. If you are an on-site RED team participant, each team will be considered a separate ship that has docked in Port Cosmar. Before anything happens to an

on-site RED team, you will be required to connect to the appropriate WIFI network and complete and turn-in a Shippers Declaration for Hazardous Goods (HAZDEC) form. The Port Cosmar harbor facility must open this form on their Microsoft Windows 7 workstations so they can determine if there are hazardous goods on-board your vessel. Each team must specify a ship name and fictitious country that they hail from. In addition, you must drop off goods that you have shipped from your home countries into the port before anything else can happen.

Remote RED team personnel may also turn-in a HAZDEC form, but they must work harder to find and expand access into Port Cosmar networks. There will be at least 1 remote access vector for remote attackers to access the internal Port Cosmar networks. You must find it.



**Throughout the remainder of this playbook, we discuss each scenario separately. You are encouraged to review each scenario so you understand the process(es) you are targeting.**



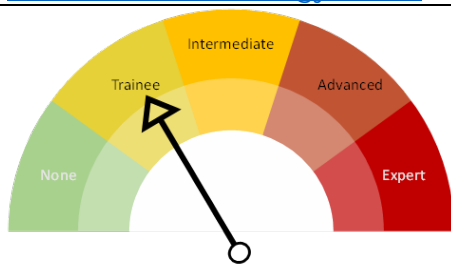
# Scenarios

We discuss the specific scenarios which will count overall scoring in this section. Each scenario will have a stated goal that you should attempt to achieve without detection by the blue team. Each scenario will be under video broadcast during live village hours. MISI may re-stream this video to Internet sources such as YouTube or Twitch but at the very least, all participants will be able to view all video streams while on-site.



# Defense Industrial Base Supply Chain Security



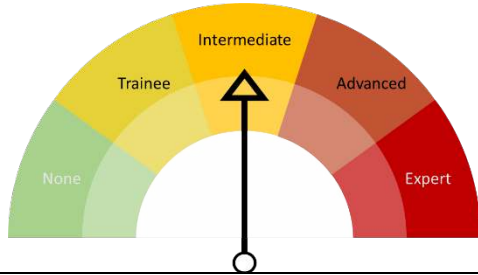
Scenario	Defense Industrial Base Supply Chain Security
Critical Sector	<a href="#">Information Technology Sector</a>
Difficulty	
Suggestions	<ul style="list-style-type: none"> <li>- Metasploit</li> <li>- Veil Framework</li> <li>- PowerShell Empire</li> <li>- Pupy</li> <li>- BEEF</li> <li>- Veil</li> <li>- SSH</li> <li>- IOS</li> </ul>
Technologies Faced	<ul style="list-style-type: none"> <li>- Windows 10</li> <li>- Windows 7</li> </ul>

	<ul style="list-style-type: none"> <li>- Adobe Acrobat/Microsoft Edge</li> <li>- Cisco/Aruba/Ubiquiti</li> </ul>
Description	<p>In this scenario, there are two (2) potential avenues for on-site RED team participants. First you are attempting to subvert the supply chain for Port Cosmar. They have ordered new desktops to be shipped directly to the port facilities and during shipment, the packages have not been secured properly. When you arrive at the Academic Village, you will be given a PC that has been shipped from your home country (still in the original box). You must determine a method to compromise this host and return it to its original wrapping. No BLUE Team personnel will watch your modifications. For the sake of this event, you can safely ignore the fact that the initial startup sequence of the box will have been changed by your alterations, but you must try to reseal the boxes (we will provide tape, scissors, etc.) Read this carefully, you cannot alter or remove existing software, ONLY EXISTING. What happens when a device arrives at a customer location with malicious alterations already made? If you are successful, you will have access to the Port Cosmar network.</p> <p>Second, you must complete and turn-in the HAZDEC form as we mentioned previously. You know (because we told you) that the harbor personnel must personally open and inspect the HAZDEC form so you shouldn't really waste this opportunity. When we publish this form, we strongly urge you to download this template and use it wisely. If you do not complete the fields of the form, you cannot be certain the employee will open it properly.</p> <p>Remote RED team personnel must utilize traditional remote recon TTP to identify the online presence of Port Cosmar and port employees. You are free to supply a HAZDEC form remotely via email. You are strongly encouraged to look for additional remote access vectors as you will need them to even attempt the follow-on scenarios.</p>



# Never Spill A Drop



Scenario	Never Spill a Drop
Critical Sector	<a href="#">Chemical Sector</a>
Difficulty	
Suggestions	<ul style="list-style-type: none"> <li>- Python</li> <li>- nmap/masscan</li> <li>- Wireshark/tcpdump/tshark</li> </ul>
Technologies Faced	<ul style="list-style-type: none"> <li>- Programmable Logic Controller</li> <li>- Human Machine Interface</li> <li>- 12v Diaphragm Pumps</li> <li>- 12v Solenoid Valve</li> <li>- Level Sensors</li> </ul>
Description	In this scenario you are trying to locate the controls for stations that handles the offloading of chemicals of Division 6.1, Class 3 and Class 8 chemicals (by United States DoT standards) within Port Cosmar. In



preparation for this attack, you have already reviewed research on chemical transport and chemical tanker offloading including an eye opening [article](#) from 2014 from the International Journal on Marine Navigation and Safety of Sea Transportation which states “spill risks and chemical incidents are not as well defined than those concerning oils”.

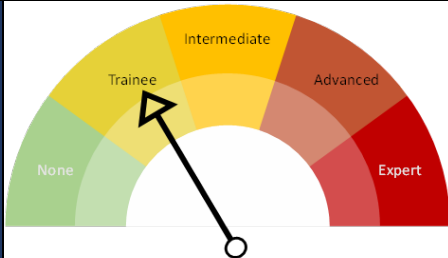
The process offloading chemical stowage involves the controlled transfer of the chemicals through special valves that pressurize the transfer with an inert chemical like nitrogen designed to prevent spills or mixing with ambient air. You must locate the equipment that pumps the chemicals into storage and holding tanks and attempt to remotely open the valves to allow the chemicals to spill. You should assume that there are at least two control system elements in play. Valves to the holding tanks are electronically controlled and the pumps to offload the chemicals are controlled by a human machine interface (HMI). There are liquid level monitors within the holding tanks that report the amount of stored chemical in each tank back to the HMI system.

This system will be operational during your time in the academic village and may be transferring **chemicals** live. For our purposes, the chemicals in this control system will be harmless colored water. Your job as an attacker is to spill these chemicals just as one might do opening the valves and venting inert chemicals or allowing the liquids to spill into the surrounding water and land. This is an unfortunately all too plausible of a danger that is not well understood yet.

This control system will be broadcast on live stream so that any spillage should be immediately visible. You should keep this in mind as it will tip your hand as an attacker. Your presence will be immediately known.

# Go With The Flow



Scenario	Go With the Flow
Critical Sector	<a href="#">Information Technology Sector</a>
Difficulty	
Suggestions	<ul style="list-style-type: none"> <li>- Python</li> <li>- scapy</li> </ul>
Technologies Faced	<ul style="list-style-type: none"> <li>- Windows 10</li> <li>- OPC/MODBUS/IOLink</li> </ul>
Description	<p>We have created a scenario specifically designed for participants with little to no experience in controls systems and control system network protocols. Do not be fooled, just because it's simple does not mean it will be easy to subvert. This scenario models a liquified natural gas (LNG) plant offloading fuel from LNG carrier ships and can also apply to general liquid processing systems that measure flow rate and temperature. This process will also contain sensors</p>

monitoring the surrounding ambient temperature and air quality for volatile organic compounds (VoC).

At a minimum, this station will contain:

- Pump controlled by PLC
- PLC programmed by Engineering Workstation
- OPC Server
- Flow Rate & Temperature Monitor
- IOLink Hub & Master
- Ambient Temperature Monitor
- Human Machine Interface for displaying live data

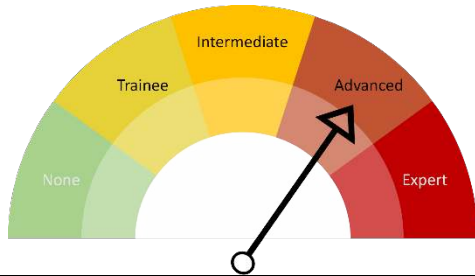
As an attacker, your job will be to interrupt this process and to alter the information displayed to the Port Cosmar employees. If you were able to expand access in previous scenarios you must locate this industrial process. How will you leverage your access and intelligence you may be able to gather to find the subnet(s) where these devices are connected? If you can interrupt the process, you can ensure that the wrong amounts of LNG are transferred while if you can alter the information displayed you could create a situation where environmental factors contribute to fuel spillage or even more hazardous conditions.

It is important to understand that you can attack a control system overtly and covertly. An overt attack can be to open valves or prevent expected operation. This can have temporary effects like work stoppage or loss of revenue/reputation but there are frequently tell-tale signs that an overt attack has taken place.

A covert attack on the other hand is far more dangerous. By simply altering telemetry data you can prevent subsequent elements of the control system from functioning. Alter a sensor reading in a human machine interface and a human operator may fail to enact their portion of the system. This could have disastrous effects and there may never be a sign that you the attacker were ever present.

# Trains-A-Comin

HACK  
THE PORT 22

Scenario	Trains-A-Comin
Critical Sector	<a href="#">Transportation Systems</a>
Difficulty	
Suggestions	<ul style="list-style-type: none"> <li>- Python</li> <li>- Kismet (but not WIFI)</li> <li>- 802.15.x</li> </ul>
Technologies Faced	<ul style="list-style-type: none"> <li>- DCC</li> <li>- HTTP(S)</li> <li>- TELNET</li> </ul>
Description	Port Cosmar has a railyard on-site with multiple train lines active that connect the port to the outside world. Your job as an attacker is to find the train control systems and activate the track switching in time to cause trains to collide in a derailment. You will need to be



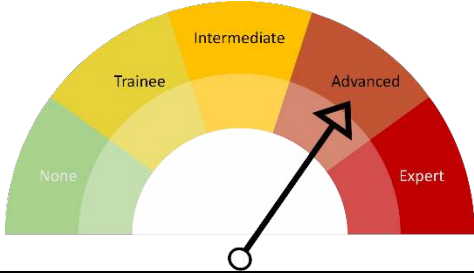
creative here. Due to the sensitivity of train controls, this automated train control network is not connected to the same Port Cosmar networks you experienced at the start of the village scenarios. It is simply located nearby. You will need to exercise ingenuity to find the train control systems. You are not going to find this network with a simple WIFI survey, you will have to work harder than that. This is especially true for remote participants.

Once located, you need to understand how to connect to this separate rail control network and identify the systems that are controlling the trains.

You should attempt to find the actual devices operating track switching control and gain remote access. You won't simply be able to knock on the front door. From here you have only one (1) final challenge. Just because you can see the interface that displays the track switch controls doesn't mean you should activate the switch immediately. First what methods are available to activate the switch controls? Graphical? Command Line? Both?

If you can identify how to control the track switching, you will have to leverage a real-time view of the trains to determine the appropriate times to perform your actions to attempt the derailment. You may only get one chance to cause the derailment before your remote access is discovered. Are you able to gain persistence in the network prior to attempting your derailment?



Scenario	Healthcare Sector
Critical Sector	<a href="#">Emergency Services</a>
Difficulty	
Suggestions	<ul style="list-style-type: none"> <li>- Python</li> <li>- AWS cli</li> </ul>
Technologies Faced	<ul style="list-style-type: none"> <li>- PHP</li> <li>- AWS S3</li> <li>- AWS EC2</li> <li>- Email</li> </ul>
Description	<p>If you reach this scenario in the Hack-The-Port academic village story, there will have been substantial property and even personal damage to employees in and around Port Cosmar. This means the local hospital may potentially be overwhelmed with patients. The hospital in question in our story is called Cosmar General and like the</p>

train control system from the previous scenario, is not connected to the same network as the rest of Port Cosmar. You must discover alternate methods of connecting to this hospital.

If you can identify an access vector into Cosmar General, you must determine a method to gain remote unauthorized access to the hospital networks. There will be more than one (1) access vector into Cosmar General. From here, you must do several things to gain total control over hospital power and devices. Your primary task is to launch a ransomware attack on the hospital demonstrating control over power (lights, even some medical devices), and then prove you can also control backup power. When we say 'backup power' we mean an actual system you must subvert to disable the secondary power source. You will be able to see Cosmar General on camera and we expect visual outcomes for each stage of control.

You should exercise caution in your access vectors into Cosmar general. If another ship finds your vector, nothing stops them from closing that hole behind them and preventing you from achieving your goal. You may want to consider alternate access vectors in case you lose your primary method.

We will tell you that power to the hospital systems will be controlled by a programmable logic controller and this may include a medical device that will be visible on camera the entire time. The backup power system will be controlled via separate means. You must subvert both to gain the full points possible for this event.



**MARITIME**  
**& CONTROL SYSTEMS**  
CYBERSECURITY CON

**Register for Hack The Port 22 Professional Village at**

**HACKTHEPORT.TECH**

**HACK**  
THE PORT 22



**dreamport**

Copyright 2022 MISI All Rights Reserved