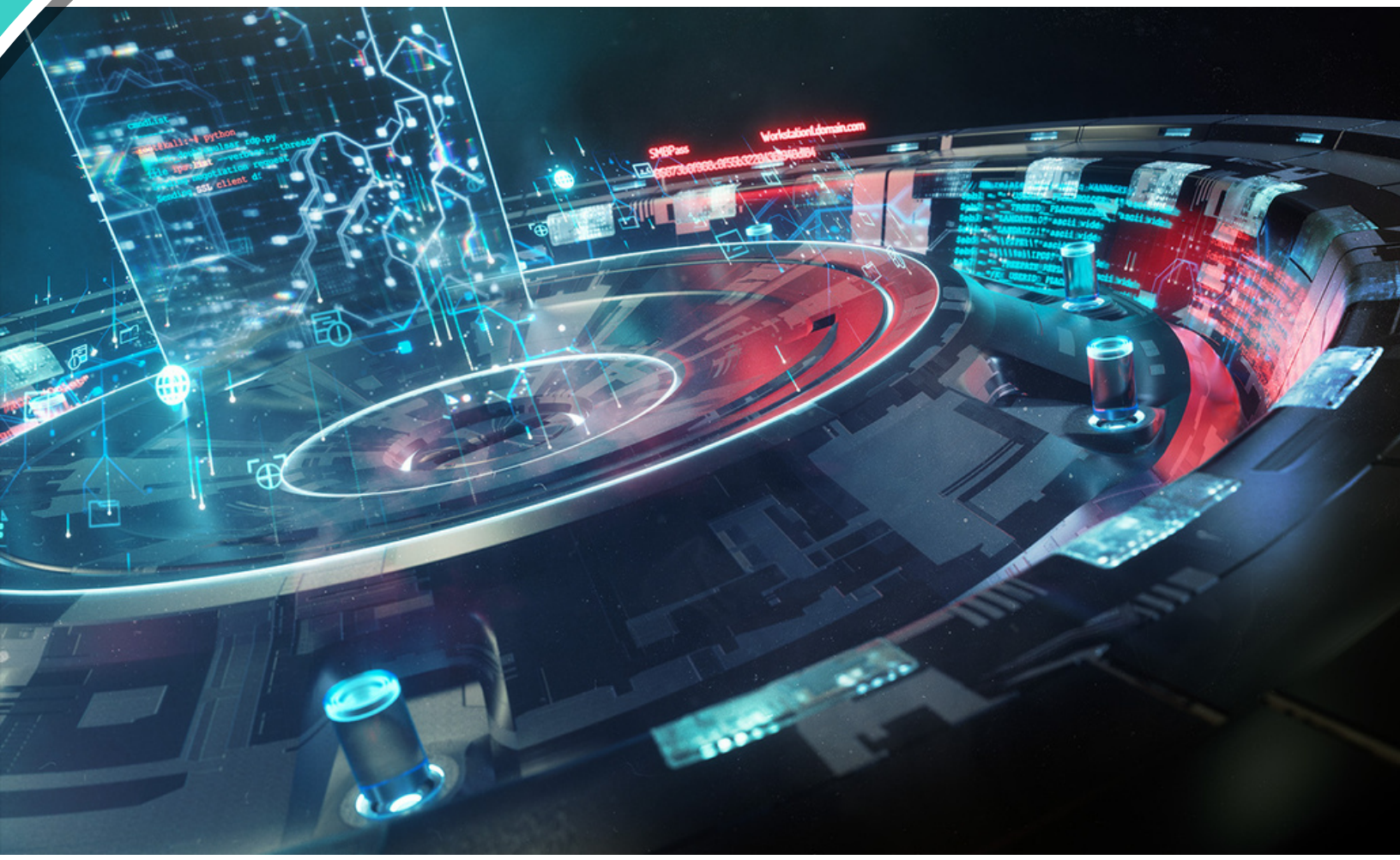
Project Ares®
BY CIRCADENCE

Scenario Catalog



Immersive
Hands-on
On-demand

Project Ares is a hands-on and on-demand learning platform that is offered through a SaaS subscription model. The cyber range and the learning content are integrated.

Try it for Free Here →

Learning scenarios cover:

- All stages of the kill chain
- Offensive and defensive perspectives
- General and specialized networks (e.g. ICS/SCADA, finance, etc.)
- Threat emulations for phishing, botnets, ransomware, malware, and more

Why hands-on cyber security training is Important

- Re-enforce traditional lecture with realistic labs
- On-demand empowering remote learning
- More competent professionals equals better job placement and increased brand recognition for your learning programs

COMBATING THE FORGETTING CURVE

BATTLE ROOMS

- Scenarios designed to help instructors train and assess skills of their learners on a set of fundamental tasks specific to a topic
- Foundational building blocks that all cyber security professionals must be proficient to participate in modern day offensive and defensive operations
- Played individually and allow instructors the choice to enable or disable hints to tailor the learning experience
- Users enter the environment and are provided a simple network environment, instructions and a list of task to complete

Battle Room 1 - Systems Integrator
Battle Room 2 - Network Analyst
Battle Room 5 - Intel Analyst
Battle Room 6 - Linux Basics
Battle Room 8 - Traffic Analyst
Battle Room 9 - Forensics
Battle Room 10 - Scripting Fundamentals
Battle Room 11 - System Security Analyst
Battle Room 21 - Powershell Fundamentals
Battle Room 1001 - Windows Fundamentals 1
Windows Command Shell – Filesystem
Battle Room 1002 - Windows Fundamentals 2
Windows Processes, Services and Applications
Battle Room 1003 - Windows Fundamentals 3
Windows Registry
Battle Room 1004 - Windows Fundamentals 4
Networking

MISSIONS

- Scenarios designed to help instructors train and assess skill levels of their learners within a realistic story that is either offensive or defensive (i.e ransomware attack on a hospital)
- The network environment is more complex than a Battle Room scenario and requires the learner(s) to combine multiple skill sets to complete the learning objectives
- Played individually, or instructors can allow teams to learn together
- Instructors can choose to enable or disable hints and enter the scenario to tailor the learning experience
- Users enter an environment and are given mission orders, rules of engagement and must use their skills to compete objectives

Offensive:

Mission 1 - Disable Botnet – Operation Goatherd
Mission 2 - Stop Terrorist Financing – Operation Bear Treat
Mission 3 - Intercept Attack Plans – Operation Desert Whale
Mission 9 - Manipulate Industrial Control System – Operation Mongoose

Defensive:

Mission 4 - Stop Malicious Process – Operation Artic Cobra
Mission 5 - Protect Financial Institution – Operation Wounded Bear
Mission 8 - Defend ICS/SCADA System – Operation Ocean View
Mission 10 - Stop Ransomware Attack – Crimson Wolf

Load time: 7-8 minutes

Time limit: 12 hours

Number of tasks: 51

Hints: yes

Save session: yes

Team-based: no

BATTLE ROOM 1 - SYSTEMS INTEGRATOR

Scenario overview

The learner is given a Kali 2019 virtual machine accessible through an SSH or VNC terminal which is provided within the scenario. In this environment, the learner conducts a series of specific tasks against a router and a Windows 2008 server.

How to be successful

The learner demonstrates understanding of network and host discovery, network analysis and configuration, host analysis and firewall configuration.

What you should know prior

The learner should be familiar with basic Linux CLI, ports and protocols, data encryption, and network device configuration.

Load time: 4-5 minutes

Time limit: 12 hours

Number of tasks: 57

Hints: yes

Save session: yes

Team-based: no

BATTLE ROOM 2 - NETWORK ANALYST

Scenario overview

The learner is given a Security Onion 14.04 network security monitoring console accessible through an SSH or VNC terminal which is provided within the scenario. In this environment, the learner conducts a series of specific tasks as an entry level network analyst.

How to be successful

The learner demonstrates understanding of cyber defense analysis, patch and release management, as well as signature development, implementation, and impact.

What you should know prior

The learner should be familiar with the basics of intrusion detection, host analysis, systems administration, and network traffic analysis, including the use of tools such as Snort, Wireshark and a command line interface (CLI).

← List of Scenarios

Load time: 4-5 minutes

Time limit: 12 hours

Number of tasks: 7

Hints: yes

Save session: yes

Team-based: no

BATTLE ROOM 5 - INTEL ANALYST

Scenario overview

The learner is given a Windows virtual machine accessible through an SSH or VNC terminal which is provided within the scenario. In this environment, the learner conducts trials in reconnaissance, information gathering, and analysis using open source intelligence tools (OSINT).

How to be successful

The learner demonstrates the ability to identify and connect information from a variety of sources to enhance threat detection.

What you should know prior

The learner should be familiar with basic intelligence gathering and analysis using open source tools such as Maltego.

Load time: 3-4 minutes

Time limit: 12 hours

Number of tasks: 15

Hints: yes

Save session: yes

Team-based: no

BATTLE ROOM 6 - LINUX BASICS

Scenario overview

The learner is given a Kali 2019 virtual machine accessible through an SSH or VNC terminal which is provided within the scenario. In this environment, the learner conducts entry level tasks in system administration, troubleshooting, and access control.

How to be successful

The learner demonstrates the ability to conduct Linux-based network operations through the command line.

What you should know prior

The learner should be familiar with the basics of a command line interface.

← List of Scenarios

Load time: 3-4 minutes

Time limit: 12 hours

Number of tasks: 30

Hints: yes

Save session: yes

Team-based: no

BATTLE ROOM 8 - TRAFFIC ANALYSIS

Scenario overview

The learner is given a Kali 2019 virtual machine accessible through an SSH or VNC terminal which is provided within the scenario. The environment includes multiple pre-installed network analysis tools for the learner to use as they conduct network forensics through analysis of packet capture (or PCAP).

How to be successful

The learner demonstrates the ability to analyze a file and answer questions related to origins of traffic, identification of credentials in the clear, sensitive document exfiltration, and database activity.

What you should know prior

The learner should be familiar with basic intrusion detection and packet capture analysis.

Load time: 4-5 minutes

Time limit: 12 hours

Number of tasks: 39

Hints: yes

Save session: yes

Team-based: no

BATTLE ROOM 9 - FORENSICS

Scenario overview

The learner is given a Windows 10 virtual machine accessible through an SSH or VNC terminal which is provided within the scenario. In this environment, the learner uses forensic tools to research and provide the necessary evidence needed to support a case of an intrusion.

How to be successful

The learner demonstrates the ability to conduct data recovery, disc image analysis, and forensic analysis.

What you should know prior

The learner should be familiar with the basics of host discovery, data archives gathering, and analysis.

← List of Scenarios

Load time: 4-5 minutes

Time limit: 12 hours

Number of tasks: 18

Hints: yes

Save session: yes

Team-based: no

BATTLE ROOM 10 - SCRIPTING FUNDAMENTALS

Scenario overview

The learner is given a Kali 2019 virtual machine accessible through an SSH or VNC terminal which is provided within the scenario. In this environment, the learner conducts a series of tasks using Python 2.7 to become familiar with programming and scripting fundamentals.

How to be successful

The learner demonstrates understanding of how to use data structures, functions, loops, and classes plus basic scripting skills such as string manipulation, file manipulation, conditional statements, and exception handling.

What you should know prior

The learner should be familiar with general programing concepts.

Load time: 6-7 minutes

Time limit: 12 hours

Number of tasks: 65

Hints: yes

Save session: yes

Team-based: no

BATTLE ROOM 11 - SYSTEM SECURITY ANALYST

Scenario overview

The learner is given a Windows 10 virtual machine accessible through an SSH or VNC terminal which is provided within the scenario. Network access to Kali Linux, Splunk, and Windows 2012 is also provided. In this environment, the learner conducts a series of specific tasks common to a System Security Analyst work role.

How to be successful

The learner demonstrates the ability to conduct reconnaissance, administer a domain, and collect and analyze logs.

What you should know prior

The learner should be familiar with the basics of host discovery and analysis, gathering data archives, and forensics analysis.

← List of Scenarios

Load time: 4 minutes

Time limit: 12 hours

Number of tasks: 18

Hints: yes

Save session: yes

Team-based: no

BATTLE ROOM 21 - POWERSHELL FUNDAMENTALS

Scenario overview

The learner is given a Windows 10 virtual machine accessible through an SSH or VNC terminal which is provided within the scenario. In this environment, the learner conducts a series of specific tasks essential to system administration.

How to be successful

The learner demonstrates an understanding of the PowerShell command syntax and is able to use several PowerShell cmdlets and their various options to navigate file systems and the Windows Registry as well as automate repeatable tasks.

What you should know prior

The learner should be familiar with the Windows operating system, basic concepts of system administration, plus scripting and programming structure.

← List of Scenarios

Load time: 10 minutes

Time limit: 12 hours

Number of tasks: 39

Hints: yes

Save session: yes

Team-based: no

BATTLE ROOM 1001 - WINDOWS FUNDAMENTALS 1 WINDOWS COMMAND SHELL – FILESYSTEM

Scenario overview

The player is given a Windows 10 virtual machine accessible through a VNC terminal which is provided within the Project Ares lab. In this environment, the player conducts a series of specific tasks to learn about the native Windows command shell and about key Windows commands to explore and manipulate the Windows filesystem.

How to be successful

The player will be able to perform basic Windows filesystem functions from the command prompt including:

- How to access the command line in user and administrator modes
- How to use the HELP command to display a list of the available commands or detailed syntax information on a specified command
- How to use commands like dir, cd, mkdir, copy con, type, sort, replace, rename, move, findstr, tree, and more to interact with the Windows filesystem
- How to access the notepad app from the command line

What you should know prior

The player should be familiar with the Windows operating system and a basic understanding of filesystem structure. The player should understand the difference between a command line and a graphical user interface.

← List of Scenarios

Load time: 10 minutes

Time limit: 12 hours

Number of tasks: 28

Hints: yes

Save session: yes

Team-based: no

BATTLE ROOM 1002 - WINDOWS FUNDAMENTALS 2 WINDOWS PROCESSES AND SERVICES

Scenario overview

The player is given a Windows 10 virtual machine accessible through a VNC terminal which is provided within the Project Ares lab. In this environment, the player conducts a series of specific tasks to learn how to manipulate applications, services, and processes using the Windows command prompt and PowerShell.

PowerShell is a task automation and configuration management program from Microsoft, consisting of a command-line shell and the associated scripting language.

How to be successful

The player will be able to perform Windows functions including:

- Display running processes and/or services associated with a process using tasklist.exe, PowerShell, or Windows Management Instrumentation Command-line (WMIC)
- Demonstrate how to run a process in the background
- as well as how to kill single or all processes.
- Use the command line to create, start, check status,
- list, stop, and delete running/active services
- Use the command line to display, schedule, modify
- and delete tasks
- View startup applications and/or verify if an application is running
- Run a dynamic-link library (dll) function and create lists of dll files used by startup and other applications

What you should know prior

The player should be familiar with the Windows operating system and a basic understanding of filesystem structure and how to use the command shell.

Project Ares scenario *Windows Fundamentals 1: Windows Command Shell – Filesystem* may be a beneficial (but not required) pre-requisite for this second Project Ares Windows Fundamentals scenario.

← List of Scenarios

Load time: 10 minutes

Time limit: 12 hours

Number of tasks: 20

Hints: yes

Save session: yes

Team-based: no

BATTLE ROOM 1003 - WINDOWS FUNDAMENTALS 3 WINDOWS REGISTRY

Scenario overview

The player is given a Windows 10 virtual machine accessible through a VNC terminal which is provided within the Project Ares lab. In this environment, the player conducts a series of specific tasks to learn basic Windows registry commands and functions from the command prompt.

How to be successful

The player will be able to perform Windows Registry functions from the command prompt including:

- Display a list of registry command operation types and help information
- List the root hives and export root level hives to a .reg file
- Add a registry key or add a value to a key at a specific registry location
- Save, restore, compare, unload, and delete registry keys
- View and import a registry (.reg) file
- Connect to a remote system's registry and copy a registry key
- Use reg query to search the registry for current user settings and modify settings without logging in as that user

What you should know prior

The player should be familiar with the Windows operating system and a basic understanding of filesystem structure, how to use the command shell, and how to work with processes and services.

Project Ares scenarios *Windows Fundamentals 1: Windows Command Shell – Filesystem* and *Windows Fundamentals 2: Processes, Services, and Applications* may be beneficial (but not required) pre-requisites for this third Project Ares Windows Fundamentals scenario.

← List of Scenarios

Load time: 10 minutes

Time limit: 12 hours

Number of tasks: 20

Hints: yes

Save session: yes

Team-based: no

BATTLE ROOM 1004 - WINDOWS FUNDAMENTALS 4 NETWORKING

Scenario overview

The player is given a Windows 10 virtual machine accessible through a VNC terminal which is provided within the Project Ares lab. In this environment, the player conducts a series of specific tasks to learn basic Windows networking administration from the command prompt.

How to be successful

The player will be able to perform Windows networking functions from the command prompt including:

- Common connectivity validation and troubleshooting, such as `ipconfig`, `ping`, and `traceroute`
- Basic firewall management with `netsh`
- Subnet translation based on binary
- DNS management and troubleshooting with `nslookup`
- Route assessment with `route` and `traceroute`
- File server and asset management with `net` commands

What you should know prior

The player should be familiar with the Windows operating system and have a basic understanding of networking, how to use the command line, and how to work with processes and services.

Project Ares scenarios Windows Fundamentals 1: Windows Command Shell – Filesystems, Windows Fundamentals 2: Processes, Services, and Applications, and Windows Fundamentals 3: Registry may be beneficial (but not required) prerequisites for this Project Ares Windows Fundamentals scenario.

← List of Scenarios

OFFENSIVE

Load time: 8-9 minutes

Time limit: 8 hours

Number of tasks: 3

Hints: yes

Save session: yes

Team-based: yes

MISSION 1
DISABLE BOTNET – OPERATION GOATHERD

Scenario overview

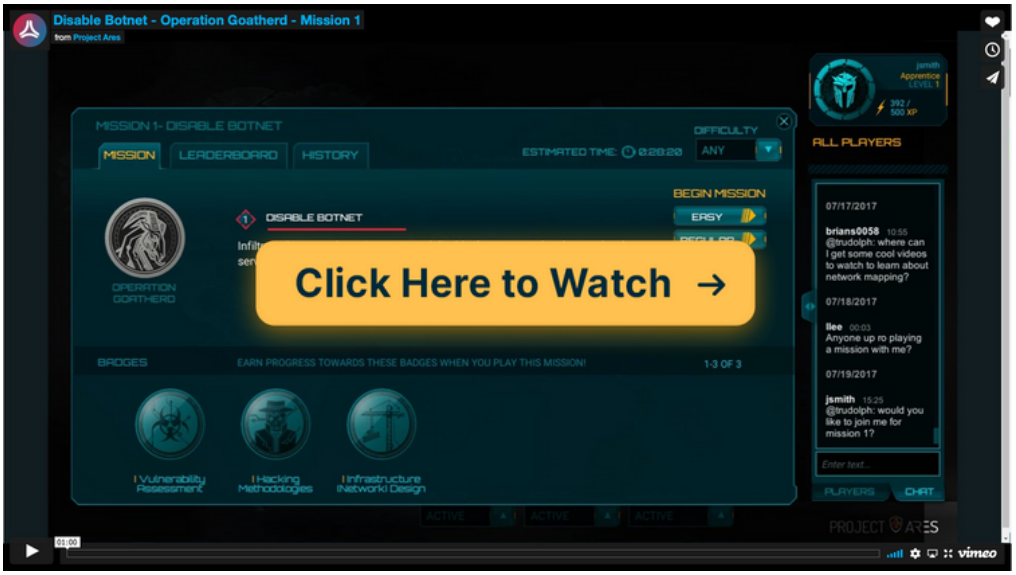
A group of hackers has been running a widespread financial scam using a botnet network. Their activities have triggered a collapse at a National Bank, with thousands of defrauded account holders demanding their deposits from local branches. Intelligence has identified the hacker command and control (C2) server and shown that this server is a single point of failure for the botnet. The goal of this scenario is to take down the C2 server and prevent the scam from claiming more innocent victims.

How to be successful

The learner or team conducts a scan of the C2 server for running services, identifies a vulnerability, performs a brute force attack to obtain credentials and then, acting as the CR orchestrator, kills the web server.

What you should know prior

Learners should be familiar with basic Linux command line interface (CLI), network protocols, password cracking and exploration, and remote administration.



← List of Scenarios

OFFENSIVE

Load time: 7-8 minutes

Time limit: 8 hours

Number of tasks: 6

Hints: yes

Save session: yes

Team-based: yes

MISSION 2
STOP TERRORIST FINANCING – OPERATION BEAR TREAT

Scenario overview

A foreign Arms Dealer has been financing terrorist attacks to help acquire the last components necessary to build a nuclear fission bomb. The latest attack was on a French power plant where the terrorists successfully stole a nuclear centrifuge which will most likely be used to create a nuclear weapon. The goal of this scenario is to retrieve a list of the Arm Dealer's recent banking activity and transactions and use it to identify and locate the terrorist organization before they are able to complete the weapon.

How to be successful

The learner or team infiltrates a corporate web server used by a shell company. Through that server, they should be able to access the Arms Dealer's personal system and retrieve the records needed. The scenario is set to purge all transaction records every 10 minutes so the learners must complete the retrieval within that time.

What you should know prior

Learners should be familiar with basic Linux command line interface (CLI), network protocols, password cracking, webserver exploits, intrusion detection alerts, and reverse scripting.

← List of Scenarios

OFFENSIVE

MISSION 3
INTERCEPT ATTACK PLANS – OPERATION DESERT WHALE

Load time: 5-6 minutes

Time limit: 8 hours

Number of tasks: 4

Hints: yes

Save session: yes

Team-based: yes

Scenario overview

Russia has deployed their new stealth fighter in the middle east. Intelligence suggests that this deployment is a prelude to an imminent strike against U.S. assets in the region. Before taking retaliatory measures, it is critical to verify the Russian squadron's mission objectives. Their hardened cyber infrastructure makes it unlikely that an existing exploit will work; however, intelligence reports indicate that there are known vulnerabilities in the Base Camp network. The goal of this scenario is to find the areas that can exploited and gain access through buffer overflow type attacks.

How to be successful

The learner or team uses a low privilege account located on the Russian Base Commanders' workstation, escalates privileges to root by building a buffer overflow exploit, and attains access to his mission objectives file. If the Russians detect an outside presence, they'll likely disconnect and air gap their system, so there is one chance to get this right.

What you should know prior

Learners should be familiar with shell code injection, non-executable (NX) stack or address-space layout randomization (ASLR), and stack return oriented programming (ROP).

← List of Scenarios

OFFENSIVE

Load time: 5-6 minutes

Time limit: 40 hours

Number of tasks: 5

Hints: yes

Save session: yes

Team-based: yes

MISSION 9
MANIPULATE INDUSTRIAL CONTROL SYSTEM – OPERATION MONGOOSE

Scenario overview

A video produced by the Taliban shows active camps training more fighters. According to satellite imagery, there is a single water treatment facility providing drinking water to the camps. Without a reliable source of potable drinking water, the Taliban would need to find alternate locations for their camps which would interrupt their training processes. Initial reconnaissance has identified the internal network of the water treatment facility and the goal of this scenario is to gain access to the controllers.

How to be successful

The learner or team uses the foothold provided by the reconnaissance team to access the desktop network, analyze the communications to the plant's control systems, and attempt to disrupt the water processing system.

What you should know prior

Learners should be familiar with network infrastructure, management, and defense, as well as vulnerability assessment and incident response processes.

← List of Scenarios

DEFENSIVE

Load time: 4-5 minutes

Time limit: 8 hours

Number of tasks: 4

Hints: yes

Save session: yes

Team-based: yes

MISSION 4
STOP MALICIOUS PROCESS – OPERATION ARTIC COBRA

Scenario overview

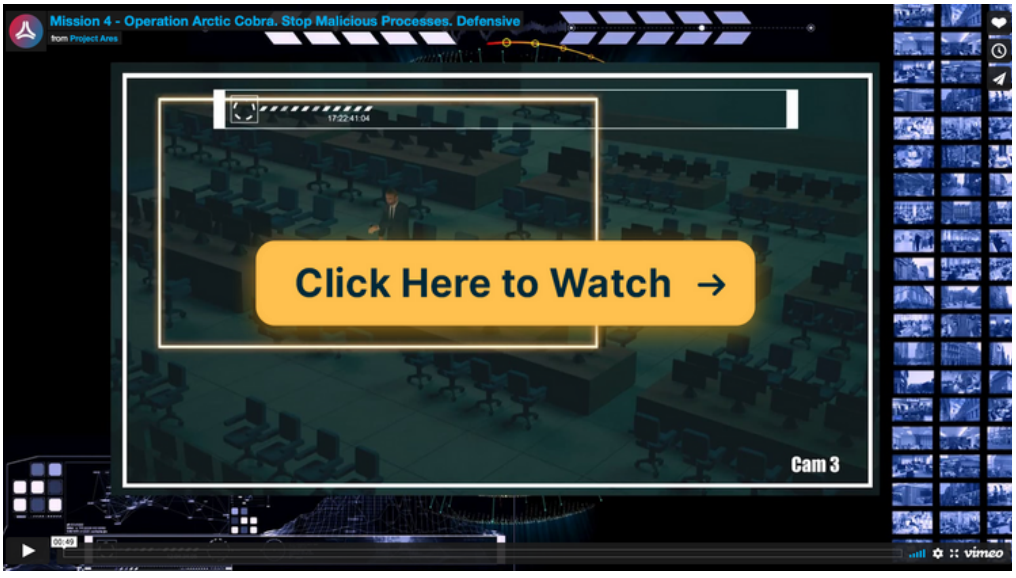
A family of Trojan malware (i.e. ZeuS, Dyre, Dridex, SpyEye) stealing identities has attacked institutions on a global scale. Due to the potentially destabilizing economic impact, the International Cyber Defense Organization (ICDO) has been called upon for assistance. The goal of this scenario is to find and remove any trace of this infection that has exfiltrated identity information from the headquarters of Rahatalo Regional Bank in southern Finland.

How to be successful

The learner or team analyzes network traffic to find and stop all malicious processes attacking this financial institution. They stop exfiltration, analyze the extent of the data loss, and eradicate all aspects of the Trojan to ensure that no further infections can occur.

What you should know prior

Learners should be have a basic understanding of application layer networking, Linux command line interface (CLI), packet capture and analysis, and best practices for containing and eradicating malware.



← List of Scenarios

DEFENSIVE

Load time: 5-6 minutes

Time limit: 8 hours

Number of tasks: 5

Hints: yes

Save session: yes

Team-based: yes

MISSION 5
PROTECT FINANCIAL INSTITUTION – OPERATION WOUNDED BEAR

Scenario overview

A new virus has been detected and is spreading through global financial institutions. The International Cyber Defense Organization (ICDO) has been deployed to all major banks to eradicate this infection. This virus is designed to infiltrate the banking systems, take over financial applications, and collect credentials from unsuspecting users. The goal of this scenario is to investigate, identify, and remove the malware responsible for identity theft.

How to be successful

With bank-provided access to all workstations, the learner or team uses the bank's intrusion detection system to find the current infection and create rules to prevent future infections. Once the rules are established, the team kills the malicious processes and removes the malware from infected machines. Obviously, the bank is still operating so there must not be any negative to bank customers during this investigation and mitigation.

What you should know prior

Learners should be familiar with basic malware analysis, containment, and eradication and also rules development within intrusion detection and prevention systems using Snort.

← List of Scenarios

DEFENSIVE

Load time: 15 minutes

Time limit: 40 hours

Number of tasks: 4

Hints: yes

Save session: yes

Team-based: yes

MISSION 8
DEFEND ICS/SCADA SYSTEM – OPERATION OCEAN VIEW

Scenario overview

There are reports that the local water authority has just been compromised, putting delivery of clean water for the city at risk. Readings from the water treatment plant's SCADA systems are showing that the chlorine level is 10 times above the amount deemed safe for consumption. It's just possible that someone inside the organization gained access to the plant's SCADA system to override all safety functions. The goal of this scenario is to conduct an incident response mission of the water treatment plant's infrastructure and SCADA systems to understand the threat attack vectors used, report attribution, and restore operations.

How to be successful

The learner or team uses network and service analysis to find a programmable logic controller (PLC) that is actively being attacked by an adversary. Through service monitoring, network analysis, and firewall management, they identify and report the adversary to the intelligence community, implement firewall rules to stop the access to the PLC, and monitor the service post firewall configuration to ensure the services remain running.

What you should know prior

Learners should be familiar with network infrastructure, management, and defense, as well as vulnerability assessment and incident response processes.

← List of Scenarios

DEFENSIVE

Load time: 15 minutes

Time limit: 40 hours

Number of tasks: 7

Hints: yes

Save session: yes

Team-based: yes

MISSION 10
STOP RANSOMWARE ATTACK – CRIMSON WOLF

Scenario overview

A hospital in the United Kingdom is in a state of emergency, having fallen victim to a sophisticated ransomware attack. Records affecting thousands of patients have been encrypted, including some who are receiving ongoing treatment. The goal of this scenario is to develop situational awareness of the hospital networks and eradicate any active threats.

How to be successful

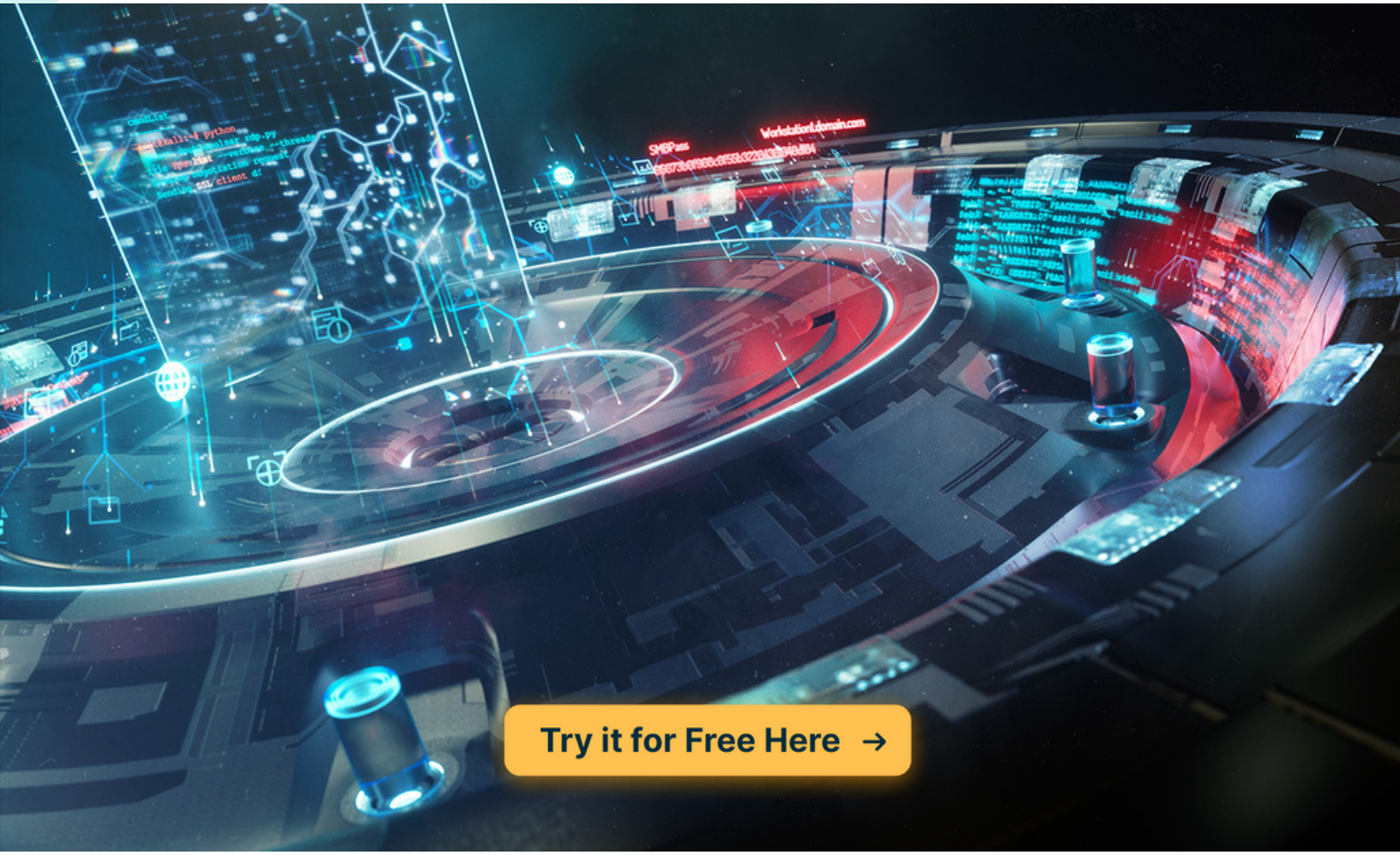
The learner or team uses network monitoring tools to derive accurate network maps, identify risk in email and domain policies, assess hosts for risk and identify abnormalities. With this intel in hand, the learner or team stops threat actions and removes any malicious artifacts.

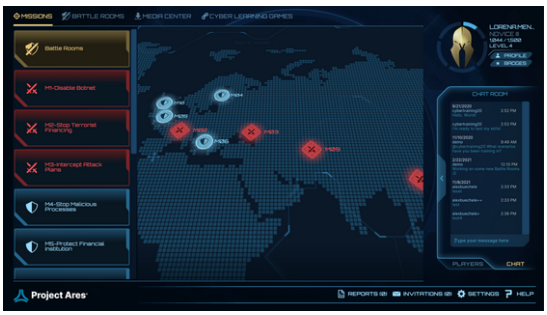
What you should know prior

Learners should be familiar with basic network management, vulnerability assessment, data forensics, and incident response management.

← List of Scenarios

Project Ares®
BY CIRCADENCE





303.413.8800 • https://circadence.com
©2022 Circadence Corporation. All rights reserved.