Project Ares®

CYBERSECURITY CURRICULUM REFERENCE GUIDE

A use case from a public research instituion in the Western U.S.

Dedicated to **empowering the instructor**

We know you're ready to equip, educate, and empower yourselves to become the best cybersecurity instructors you can be. Therefore, we created this curriculum reference guide, based on a real-life curriculum program from a public research institution in the Western U.S., to inspire you as you start exploring the power of hands-on cybersecurity labs for your classroom.

Encourage your students to build skills for the workforce! Project Ares is an award-winning, immersive, gamified learning platform that helps students of all cyber competency levels apply learned concepts to real-world scenarios.

Our hands-on labs deliver persistent, true-to-life experiences that match and adapt to current threats. Project Ares uniquely combines single- and multi-player exercises and offensive and defensive scenarios that mirror real-life cyber incidents and situations.

Project Ares®

Project Ares Perks

Project Ares provides:

- In-game advisor adds scenario support to help students through activities.
- Trainer View allows for real-time instructor engagement and ability to monitor student progress against established objectives.
- Functional virtual machines simulate Windows, Linux, and Industrial Control System devices for comprehensive preparation on any system.
- The Microsoft Azure cloud enables cyber range learning capacity for classes, clubs, and competitive events of all sizes.

A real-life classroom reference:

An adjunct professor taught a graduate level cybersecurity course using the platform at a public research institution in the Western U.S. To complement classroom taught concepts in the course focused on immersive cybersecurity defense, the professor holistically incorporated the Project Ares platform into the course curriculum.

Lectures coupled with the Project Ares lab environment allowed students to learn cyber theory and immediately apply it to real-world scenarios.

The following course syllabus is a sample to help fellow academic instructors visualize and conceptualize how a cyber range environment can be used to enhance student learning objectives within a cybersecurity course.

Course: Immersive Cyber Defense

WHAT DID STUDENTS LEARN?

Students practice offensive skills in password cracking and exploit development to understand vulnerabilities and then focus on defensive tactics to reduce cyber risk and respond to cyber attacks. At the conclusion of the course, students will have experience using several real-world tools against actual threat attacks.

WHAT WERE THE UNITS OF STUDY?

Unit 1: Adversary tools and tactics
Unit 2: Cybersecurity work roles: Harden, Monitor, Pursue, Coordinate (Lead/Intelligence)
Unit 3: Defense teams tactics and procedures following the NIST Cybersecurity Framework

Students successfully completing this course should have an understanding of pathways to building expertise in the field of cybersecurity and the types of technical careers available.

WHAT WERE THE LEARNING GOALS?

Understand how an adversary develops a campaign to attack a network, including the types of motivations, tactics, and the kill chain pathway. These concepts help defenders understand the data points that are present in an attack and where indicators of compromise can be found.

Understand the different types of work roles and technical competencies involved in cybersecurity defense. Students will be exposed to multiple work roles and then choose the one that interests them for concentration during the course. Their selected work role will also be the basis of their specific midterm exam.

Apply cybersecurity defense knowledge across the full scope of the NIST Cybersecurity Framework to understand what defenders should do before, during and after a breach.

Textbooks, Materials, Mechanics, Oh My!

TEXTBOOK AND MATERIALS

Required: None
Recommended: Project Ares Media Center materials (or other sources on-line) on Linux System administration, Windows System Administration, Wireshark, Nmap, Snort/ SecurityOnion, Metasploit Basic
Tools: Command line tools, Nmap, Wireshark, Snort (Security Onion), Metasploit

ASSIGNMENTS

Weekly homework will be assigned as an activity in the Project Ares environment.

EXAMPLE GRADING MECHANICS

Grading: Midterm (20%) Final Exam (20%), Weekly homework (60%)

To do well in this course, students need to use the Project Ares environment to practice the concepts discussed in the classroom. Students are expected to explore the concepts and research the necessary topics and tools to be used. All homework will be assigned as an activity in the online lab environment. The exams will also be activities in Project Ares to be 3 completed during the exam period.

Sample Course **Outline**

Week	Primary Topic	Objectives	Homework
1	Course Introduction	• Course overview • Project Ares intro • Cyber defense roles (NICE/NIST and careers in defense applicable to the course) • CIA Triad and Adversary thinking • Kill Chain Methodology	• Player profiles in Project Ares • Battle Room (BR) 6 Basic Linux and Cyber Learning • Game -Cylitaire
2	Adversary Tools and Techniques	• Project Ares variability and scoring • Intro to Kali/Metasploit tools • Reconnaissance tactics (Nmap, Dig) • Common Ports (SSH, telnet, VNC, Http) • Password Cracking techniques/tools • M1 Easy walk through	• Cyber Learning Game - PortFlow • Mission 1 - Easy + Medium (for extra credit)
3	Adversary Planning	• Using Nmap, hping3, Burp, etc. to understand network, fingerprinting, protocols • Attack Surface/ATT&CK Framework • Weaponization and Exploitation with Metasploit • Mission 2 Easy walk through	• Mission 3 (Easy or Medium)
4	Individual Work Role: Harden	• NIST/NICE and Work Roles for Teams • Review Harden tasks and contrast with BR1 • Software Assurance and other common issues, OWASP • Importance of Active Directory, OU/GPOs • Firewalls	• Cyber Learning Game - CyQual (Either Host, Net, Sys) Assessment • Battle Room 1 - System Integrator
5	Individual Work Role: Monitor	• Review Monitor tasks and contrast with BR 2 • IDS/IPS with Snort and Bro (Security Onion) • Host and Network Monitoring • Log Aggregation Techniques	• Cyber Learning Game - Regexile • Battle Room 2 - Network Analyst
6	Individual Work Role: Harden	• Review Pursue tasks and contrast with BR 11 • Network Analysis with Wireshark • System Integrity Checking • Forensics	• Cyber Learning Game - CyberVault • Battle Room 11 - Host Analyst
7	MID-TERM	• Assessment in class (hints disabled)	• Battle Room 1, 2, or 11: Network Analyst, Host Analyst or System Integrator

Sample Course Outline (Continued)

Week	Primary Topic	Objectives	Homework
8	NIST CSF: Identify	• Criticial assets and Key Terrain • Mission Impact Model (MIM) • Vulnerability Assessment (Nmap, Nesses) • Understand Risk Management	• Occam Analysis
9	NIST CSF: Protect	• Security Architecture • Tailored Defense • Lockdown Key Terrain (services) • Mission 5 Walk through (malware analysis, alert, prevent malware)	• Mission 5 (Easy)
10	NIST CSF: Detect	• IDS/IPS Rule Review • Log Aggregation • Mission 4 walk through (packet capture, process analysis)	• Mission 4 (Easy)
11		**SPRING BREAK**	
12	NIST CSF: Respond	• Incident Response Process • Workflow and hand off • Role of Intel (and tension of rapid response)	• Mission 10 (Easy) or team play
13	NIST CSF: Recover	• Reporting • Forensics • BR 9 Walk through	• Battle Room 9 (Forensics)
14	Team Tactics	• SOC Operations and Team Play • A look at famous attacks (ransomware) and groups like Lazarus	• Battle Room 10 (Scripting)
15	Review Course Q&A	• Trivia Loot Review • Mission walk through • Prep for final exam	• Mission 2 (Easy) individual or teams

Benefitting the Student: Features and Value

- Instantaneously spin up 3-50+ virtual machines to support classroom exercises
- Modify the Media Center to support course concepts and exercises
- Cyber learning games provide fundamental concept learning via consistent repetition
- Battle rooms (Foundational scenarios) help users practice foundational skills and explore cyber tools
- Missions (Specialized scenarios) offer individual or team-play
- Cloud deployment makes on-demand access flexible from a browser, available 24/7

Let's Stay in Touch!

We’re so happy you’re ready to take the next steps to enrich your teaching approach with hands-on labs in Project Ares!

We hope this reference guide was helpful for you as you plan out or optimize your course or program structure. We are dedicated to making sure that teaching cybersecurity is within reach for you and enjoyable for your students. With the right guidance from our curriculum experts, you can rest assured together, your cyber education needs to be met.

Let us know when you're ready to talk further about specific labs, teaching topics, schedule, and budget.