Hands-on Educational Labs for Cyber Defense Competition Training

Animesh Pattanayak, Stu Steiner, Daniel Conte de Leon

Center for Network Computing & Cybersecurity
and Department of Computer Science
Eastern Washington University

Center for Secure & Dependable Systems
and Department of Computer Science
University of Idaho

CISSE 2021

University of Idaho

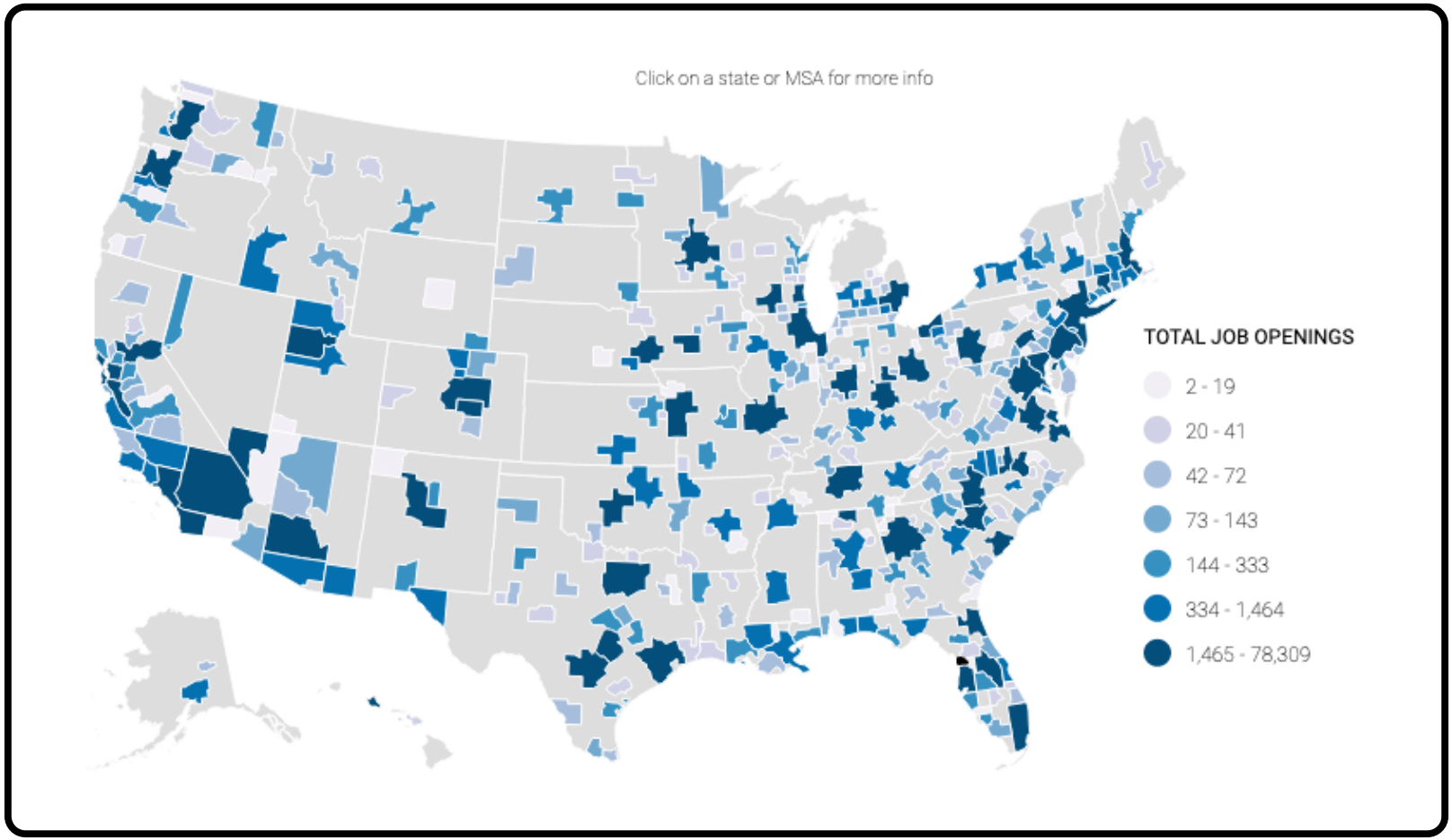
EASTERN WASHINGTON UNIVERSITY

Overview

Background

Open Cybersecurity Positions

All Open Positions by Metro Area [1]



Cyber Defense Competitions

Cyber Defense Competitions Mission

- Provide an educational venue in which students are able to apply the theory and practical skills they have learned in their course work.
- Foster a spirit of teamwork, ethical behavior, and effective communication both within and across teams.
- Provide higher educational institutions a practical mechanism to evaluate their cybersecurity educational programs.

Cyber Defense Competitions

There is a large variety of Cybersecurity Competitions that are Red/Blue Team style

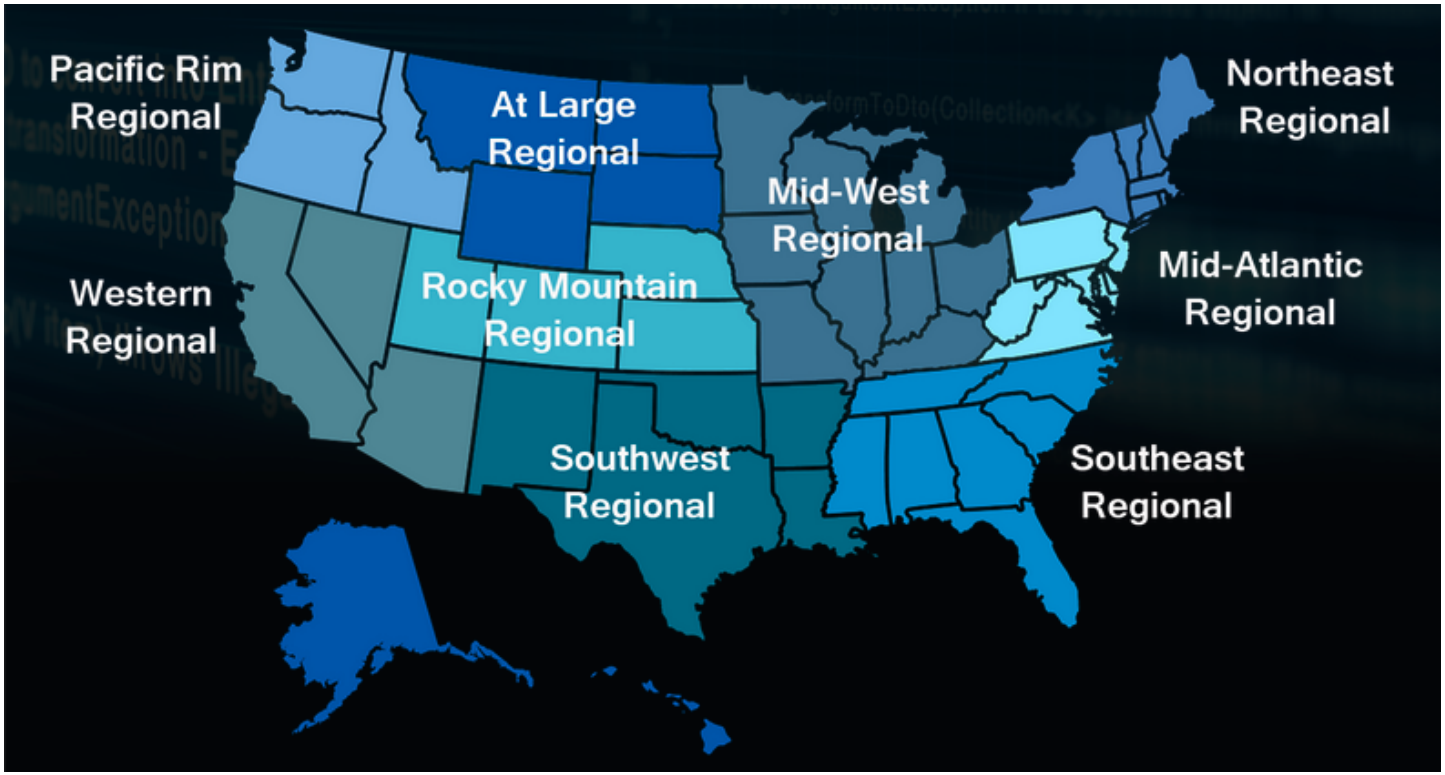
Competitions

- National Collegiate Cyber Defense
- DOE CyberForce
- US Cyber Challenge
- Panoply

This is a small list highlighting some of the major competitions.

Cyber Defense Competitions

This talk is about preparing for the Regional Collegiate Cyber Defense Competition



Cyber Defense Competitions

A typical Cyber Defense Competition is constructed around the concept that the students are brought in as a cybersecurity company to assume administrative/ protective duties for an existing business network.

Students as the Blue Team typical scenario:

- Small to medium business of 50+ employees/users
- 7 to 10 servers
- Traditional Information Technology (IT) services
- Monitoring the system for Red Team attacks
- Small teams 8 maximum competitors

Cyber Defense Competitions

Scoring for a Cyber Defense Competition is based on multiple metrics. Two of those metrics are uptime and business tasks.

- A score bot checks to see if the service is up, running and accessible.
  - Yes, the service is running uptime points are awarded
  - No, the service is down. The team needs to identify, detect and remove whatever is compromising the system. Return the service to running
- Business tasks include answering the phone, responding to emails, reporting incidents, and responding to requests from corporate.

Teaching Cybersecurity

Teaching to compete in a Cyber Defense Competition is different than teaching traditional cybersecurity courses (Network Security, Secure Code, etc.).

Cyber Defense Categories

- Blue Team
- Red Team
- Orange Team
- White/Gold/Black

Skill set includes knowledge from traditional cybersecurity courses; however, the more important skill sets are soft skills, communication skills and teamwork skills.

Proposed Solution: CYOTEE

CYOTEE: Features

CYbersecurity **O**riented **T**raining **E**nvironment and **E**xercises (CYOTEE)

CYOTEE features include:

- Open Source laboratory exercises for common Cyber Defense Competition tasks.
- Semi-automated scripts to aid in setup.
- Laboratory exercises are mapped to NIST NICE framework.
- Holistic approach to learning.
- Student challenges to ensure the concepts are understood.

CYOTEE: Lab Structure

The current structure for each lab

1. **Lab Specifications:** Provides the necessary VMs and configuration/setup scripts for the lab.
2. **NIST NICE Mapping:** The mapping of the KSAs to the NIST NICE Framework
3. **Background:** Provides the necessary required student knowledge to complete the lab
4. **Task and Challenges:** The required tasks and challenges students need to complete.
5. **Completion Time:** Provides the expected completion time for the lab based on the student skills.

CYOTEE: Labs

Current List of Labs

1. Linux Terminal Basics
2. **Linux Hardening**
3. MySQL Usage and Hardening
4. Creating a Vulnerable Web Application
5. Web Application Hardening
6. **Active Directory Usage and Hardening**
7. Customer Service Tasks
8. Organization Management Tasks
9. Incident Management and Response

CYOTEE: Lab 2 Linux Hardening Example

Hardening Tasks include:

1. Default, Weak or Common Passwords
2. Unused Additional Accounts
3. Disabled Automatic Updates
4. SSH
5. Cron and Cronjobs

Challenges include:

1. Changing the Password
2. Remove/Disable Unnecessary Accounts
3. Enable Automatic Update Alerts
4. Hardening SSH via certificates
5. Remove Unnecessary Cronjobs

CYOTEE: Preliminary Feedback

CYOTEE Student Feedback

1. "Progression of labs helped improve my skills and prepare me for the competition"
2. "Without the labs we would have done so much worse"
3. "Can't wait to use the labs to improve and come back next year"

CYOTEE: Features

CYOTEE's Lab Availability

GitHub site:
https://github.com/CenterForSecureAndDependableSystems/CYOTEE

YouTube videos: Coming Soon

Conclusions

Conclusions

CYOTEE labs are a viable solution for training for a Cyber Defense Competition

- Current labs emulate a competition.
- Labs are good for training club students for future competitions.
- Labs are updated after being taught, assessed and after a competition.

Conclusion

CYOTEE labs developed under consortium of EWU and University of Idaho

- Consortium is used to collaboratively train students
- Open source and available from https://github.com/CenterForSecureAndDependableSystems/CYOTEE

Thank You and Questions

Questions?

References

References I


C. Seek, "Cybersecurity Supply/Demand Heat Map," 2021. [Online]. Available: https://www.cyberseek.org/heatmap.html