Open Access License Notice

Hands-on Educational Labs for Cyber Defense Competition Training

Animesh Pattanayak
Ctr. for Secure and Dep. Sys.
& CS dept., Univ. of Idaho
Moscow, ID, USA
animesh@pnnl.gov

Stu Steiner
Computer Science
Eastern Washington Univ.
Spokane, WA, USA
ssteiner@ewu.edu

Daniel Conte de Leon
Ctr. for Secure and Dep. Sys.
& CS dept., Univ. of Idaho
Moscow, ID, USA
dcontedeleon@ieee.org

Abstract—Cyber Defense Competitions provide students with challenging, hands-on, fun, and close to real world opportunities to learn, practice, and perform tasks that they will be expected to complete as cybersecurity professionals. The current availability of training resources focused on Cyber Defense Competitions is limited. We introduce CYOTEE: CYbersecurity Oriented Training Environment and Exercises. CYOTEE provides a set of nine fully modifiable and freely available hands-on laboratory activities intended to help students gain skills needed to be successful at Cyber Defense Competitions. This article provides details for two of those hands-on labs: (1) Linux Hardening and (2) Windows Active Directory Hardening. CYOTEE lab descriptions and setup scripts may be found on the GitHub repository (https://github.com/CenterForSecureAndDependableSystems/CYOTEE).

Keywords—Cyber defense, Cyber defense competitions, Hands-on labs, Windows Active Directory hardening, Linux hardening, NICE Framework

I. Introduction

Attack-Defend, also called Read/Blue team, Cyber Defense Competitions (CDCs) enable students to have a close to real world experience in an enterprise information technology (IT) or operational technology (OT) environment. This experience includes hardening vulnerable machines, maintaining uptime of critical services, providing technical support, documenting and reporting incidents, and responding to user requests, all while under duress from red team attacks.

A. The Problem

To maximize the learning experience of participating in a CDC, students should be adequately prepared in not only the basic concepts of cybersecurity, but also technical and business skills and abilities. However, we found that the current availability of training materials for cyber defense competitions is very limited.

B. Contribution

We present CYOTEE (*CYbersecurity Oriented Training Environment and Exercises*) and we describe two of its hands-on laboratories: Lab 2: Linux Hardening and Lab 6 Windows Active Directory Hardening. CYOTEE's contributions include: (1) Design considerations based on mappings to the NICE framework; and (2) A robust set of hands-on labs based on the knowledge, skills, and abilities needed at CDCs.

C. Overview of this Article

The rest of this article is organized as follows: Section II briefly introduces Cyber Defense Competitions; Section III describes CYOTEE's instructional approach and a mapping to the NICE Framework; Section IV describes the CYOTEE lab environment and lists available hands-on exercises; Section V describes the Linux Hardening lab; Section VI describes the Active Directory Hardening lab; Section VII presents assessment approaches; Section VIII presents the conclusion. Acknowledgements and a complete list of References follow.

II. Cyber Defense Competitions

Red Team - Blue Team Cyber Defense Competitions (CDCs) are training exercises in which a team of penetration testers (Red Team) attempt to exploit vulnerabilities in the infrastructure of the defending team (Blue Team). At or before the start of a CDC, the blue team receives a vulnerable infrastructure, often with an accompanying story. In the story, typically, the blue team has been called in to improve and maintain an IT/OT infrastructure that is vulnerable and/or has been compromised. Vulnerabilities may include weak or default passwords, malicious accounts, back-doors, among many others vulnerabilities. The blue team needs to identify as many vulnerabilities as possible and subsequently harden all services and systems before the Red team exploits them.

The infrastructure at these competitions includes common services and systems, such as databases, web servers, file servers, domain controllers, firewalls, and client workstations. Usually, a Windows domain controller is used to remotely manage policies across the entire domain to ensure that all client machines are appropriately configured. Firewalls provide teams with a tool to systemically control what network traffic is allowed both inbound and outbound using various different filters including, but not limited to, Internet Protocol (IP) addresses and network protocols. Client workstations are the individual employee's computers. These client workstations, typically don't run critical services; however, the workstations may contain sensitive information and they are connected to the systems that run critical services.

In addition to defending the IT/OT systems, the Blue team is expected to perform other technical-and business-oriented tasks. These are called *Injects* in the PRCCDC case and *Anomalies* in the DoE CyberForce case. These intermittently delivered requests ask the Blue team to complete tasks such as adding and/or removing domain users, identifying users that accessed a service in the last hour, or submitting an incident log. In addition to managing *Injects*, the Blue team must respond to emails, maintain logs, report incidents, respond to users requests/issues, and answer the team's telephone. In the CCDC case, a Blue team's member is identified as the business representative and this person is responsible for answering the team's telephone. Telephone calls may include a disgruntled employee trying to file a complaint, or a wrong number asking about heating pizza rolls. Maintaining composure and being respectful while continuing to process *Injects* is critical for the business representative.

The Blue team is scored based on a combination of service up-time, documentation, incident reports, and customer service. At competitions a score-bot periodically and frequently (about once a minute) checks to see if a service is up, running, and accessible, if positive, then the team receives up-time points for that service. If a service is down, the Blue team must work to identify the problem and restore the service. Once the service is restored the blue team will resume earning up-time points. Other points are gained for detailed and well-written hardening documentation, and incident reports, solving customer and infrastructure support tickets, and other technical and business-oriented activities. These activities are intended to simulate the day-to-day operations of the IT and Cyber teams in an organization, albeit in an accelerated manner.

The motivation for CYOTEE originates from a need to prepare students for the National Collegiate Cyber Defense Competition [1] and the US Department of Energy's (DoE) CyberForce Competition [2]. The reason we chose to focus on these two competitions are: (1) They are Red-Blue Team-based rather than Capture-the-Flag-based; (2) Combined, they focus on IT and OT systems; (3) They are likely the biggest and best known in-person and college-level cyber-defense competitions in the US; (4) Teams of students from the University of Idaho (UI) and Eastern Washington University (EWU) have competed on these two competitions for several years and placed well consistently and hence we believe have good knowledge of the skills and abilities needed.

A detailed survey of currently available cyber defense competitions is the out-of-scope of this article; And a detailed, peer-reviewed, and published survey of cyber defense competitions may have yet to be published. For example, a Google Scholar search using the quoted phrase *Cyber Defense Competitions*, performed on 16 November 2021, returned 316 results, and using the quoted phrase *Survey of Cyber Defense Competitions* returned 0 results. A similar number of results is returned by substituting the term *Cyber Defense* by the term *Cybersecurity* in the two search phrases above: 358 1 and 0. Some of the articles that provide some additional information about the topic are: [3], [4].

With respect to related work, we found one publication describing resources focused on preparing for cyber defense competitions: The document *Preparing for the Collegiate Cyber Defense Competition (CCDC): A Guide for New Teams and Recommendations for Experienced Players* published in 2015 [5]. This is an excellent resource describing strategies for: recruiting and managing teams, building knowledge, skills, and abilities, developing competition strategies, and learning to work in teams [5]. Our work, by contrast, focuses on developing and sharing hands-on activities to aid students and instructors when preparing for cyber defense competitions.

The SEED Labs [6] provide a rich collection of excellent hands-on exercises focused on demonstrating vulnerabilities. Our work by contrast focuses on approaches needed to secure vulnerable services when those are embedded within an enterprise infrastructure.

This work was developed with a focus on the in-person competitions. In the last two years (2020 and 2021) these competitions have moved online due to COVID-19 but we hope and expect that these competitions will be back in-person as soon as safe and feasible.

III. CYOTEE'S PEDAGOGICAL APPROACH

A. Pedagogical Approach

Cridlin [7] argued that a holistic approach to learning is needed for adequately understanding and retaining of the learned material. A holistic approach would include reading [8], writing, hands-on coursework, and also continual assessment. Ekwueme et al. [9] state "*The study showed positive improvement on both the students' performance and participation on mathematics and basic science activities and willingness on the part of the teachers to use [a] hands-on-approach in communicating mathematical and scientific concepts to their students*." Although the study was for basic mathematics and science, we believe that the lessons learned also apply to cybersecurity concepts. CYOTEE supports a holistic approach to learning.

CYOTEE supports hands-on learning by tasking students to complete challenges in each laboratory exercise. These challenges require students to mitigate against vulnerabilities, configure machines, utilize applications, and discuss cybersecurity concepts. Students have the opportunity to learn about and practice various cyber defense skills through the laboratory exercises.

To support reading and learning, CYOTEE provides downloadable oratory exercises. The lab exercises include reading tasks, including an explanation of the vulnerabilities associated with each task. Furthermore, each lab exercise includes the rationale, and a guided walk-through on how to complete each challenge.

CYOTEE supports writing and retention of the student's learning by requiring the students submit laboratory reports summarizing vulnerabilities, patches, telephone calls, and

other lab requirements. Students are then assessed approximately two or three days later. These assessments are used to verify the students are retaining the material.

B. Expected Audience

The target audience for the hands-on exercises provided by CYOTEE are college-level students in a variety of majors; For example, Computer Science, Cybersecurity, Information Systems, and Information Technology. The expected level of background needed to best benefit from the materials is basic knowledge of cybersecurity concepts such as those concepts learnt during a first course in Cybersecurity or Information Security.

C. Mapping to NICE Framework

The NIST NICE Cybersecurity Workforce Framework contains seven Categories [10], [11].

1) Analyze
2) Collect and Operate
3) Investigate
4) Operate and Maintain
5) Oversee and Govern
6) Protect and Defend
7) Provision Securely

CYOTEE directly maps to three NICE categories including Protect and Defend, Operate and Maintain, and Provision Securely. Covered cybersecurity specialty areas include:

Protect and Defend noitemsep

1) Cyber Defense Analysis
2) Cyber Defense Infrastructure Support
3) Incident Response
4) Vulnerability Assessment and Management

Operate and Maintain

1) Data Administration
2) Knowledge Management
3) Customer Service and Technical Support
4) Network Services
5) Systems Administrator
6) Systems Analysis

Provision Securely

1) Software Development
2) Test and Evaluation

IV. CYOTEE Laboratory Environment

The laboratory environment needed to support the hands-on exercises is composed of several virtual machines (VMs). These include a mail server, a file server, a domain name service (DNS), and a web server.

A. Initialization Scripts for All Laboratory Exercises

CYOTEE provides scripts to semi-automatically configure the laboratory VMs. Instructors would only need to create the base (vanilla) virtual machines, for example Ubuntu 20.04 and then run the initialization scripts within those VMs. The initialization scripts will then download the needed packages, install the required tools and applications, and perform all needed configuration tasks to setup the hands-on scenario; This includes, creating and modifying configuration files, creating users, creating web applications, and populating application data. For this purpose, the scripts require each VM to have Internet access during the setup process. However, after installation and configuration is complete, the VMs should be fully isolated from the Internet and other non-exercise dedicated networks before running the exercises. This is because a few tasks in some exercises may demonstrate how services are vulnerable before showing how to secure them. For safety and security reasons, such vulnerability demonstration tasks must be performed on an isolated environment only to fully prevent accidental unauthorized scans or access to other systems.

B. CYOTEE Available Labs

The CYOTEE exercises available in the GitHub repository are:

- Lab 1: Basics of the Linux Terminal
- Lab 2: Linux Workstation Hardening
- Lab 3: MySQL Hardening
- Lab 4: Creating a Vulnerable Web Application
- Lab 5: Web Application Hardening
- Lab 6: Windows Active Directory Hardening
- Lab 7: CDC Customer Service
- Lab 8: CDC Organization Management
- Lab 9: CDC Incident Management and Response

Due to space constraints, only Lab 2: Linux Workstation Hardening and Lab 6: Windows Active Directory Hardening are described in this article. The other labs or exercises will be described elsewhere.

V. Lab 2: Linux Workstation Hardening

This lab is intended to increase the student's familiarity with Linux, common Linux vulnerabilities, and how to harden a Linux workstation. Students are asked a series of questions to assess their basic understanding of Linux vulnerabilities [12]. Next, students are asked to read the lab directions before attempting to secure the machine. Completing this lab should take approximately one hour.

A. Learning Objectives

- Basics of Linux Usage
- Basics of Linux Hardening

B. Mapping to NIST Nice Framework

NIST NICE Framework KSAs mappings:

- Cybersecurity and Privacy Principles (K0004)
- Cyber Threats and Vulnerabilities (K0005)
- Basic System and OS Hardening Techniques (K0205)
- Recognizing Types of Vulnerabilities (S0078)
- System, Network, and OS Hardening Techniques (S0121)

C. Configuration and Setup

Listing 1 illustrates the Linux workstation vulnerabilities configuration including: (1) additional users; (2) automatic updates disabled; (3) weak passwords; (4) erroneous cron jobs; and (5) unprotected SSH enabled.

The scripts are provided in the GitHub repository. The instructor will need to: (1) create the VM; (2) clone the specific lab from the GitHub repository; and (3) run the configuration script to build the specific lab's exercises.

Listing 1: Linux Hardening Initialization Script

```
#!/bin/bash
#overhead

sudo dpkg --configure -a
sudo apt-get install git -y
sudo apt-get install openssh-server openssh-
client -y
sudo service ssh start
sudo rm -r CYOTEE

#create users
useradd redteam
useradd guest

#assign passwords to the users
sudo echo -e "redteam\nredteam" | passwd
redteam
sudo echo -e "guest\nguest" | passwd guest

#disable auto-updates
sudo rm /etc/apt/apt.conf.d/20-auto- upgrades
sudo rm /etc/apt/apt.conf.d/20auto- upgrades
sudo cp CYOTEE/CYOTEE_Code_Linux/20-auto-
upgrades /etc/apt/apt.conf.d/20-auto- upgrades

#add a couple of cron jobs
sudo crontab -u thesis -l | { cat; echo "* * *
* * touch ~/Desktop/sensitivefile "; } |
crontab - -u thesis

sudo crontab -u thesis -l | { cat; echo "*/2 *
* * * rm ~/Desktop/sensitivefile "; } |
crontab - -u thesis
```

D. Student Challenges

The learning objectives of these challenges are: (1) Learn to tailor a default Linux Server installation with a focus on security; (2) Learn to audit settings in a Linux Server installation with a focus on system hardening.

- **Task 1: Secure the Password**
  One of the most common vulnerabilities is inadequate password security. Many devices do not come preconfigured with a password, while others have a default password. First, students need to ensure the machine is password protected. Next, the student needs to check if the password is secure. A default password should be changed. Changing the default password does not guarantee your device is secure, because the password may be on a list of common passwords. A secure password should have a long length, varied characters (uppercase / lowercase / special characters / numbers), and not contain personal information such as your pet's name. The default password on this machine is "password".
- **Task 2: Remove / Disable Unnecessary Accounts**
  Multi-user machines are common and often found in shared spaces such as schools, libraries, etc. While additional accounts are not inherently malicious, they may provide an insecure backdoor into the machine. For this reason, unnecessary accounts need to be removed. If one is unsure if the additional account is necessary, then simply disable the account.
- **Task 3: Enable Automatic Updates**
  Updates are a very important element of computing and automatic updates need to be enabled. Computers and their software are often vulnerable. Updates provide patches for these vulnerabilities, helping secure the computer so the vulnerability can no longer be exploited. For security reasons, update sites should be checked daily for new updates, including critical updates. If update sites are not checked frequently, then a patch for a serious vulnerability may accidentally be missed. New vulnerabilities are discovered frequently with exploits developed shortly thereafter. Manually checking for updates can result in missed updates which can leave the user susceptible to exploits. To prevent missing an update automatic updates should be enabled.
- **Task 4: Harden SSH**
  Secure shell (SSH) allows a user to securely log into a remote machine via a terminal; however, it may also pose a security risk if not configured securely. Remote access to a machine potentially allows a malicious actor to bypass password protections and gain full access to the machine. SSH can be hardened by removing passwords and authenticating using SSH keys.

- **Task 5: Remove Unnecessary Cron Jobs**
  Cron is a software utility that schedules tasks to be performed at specified intervals. A Cron job is useful for checking for updates. A Cron job is added to the Crontab file. Crontab uses a specific format, minutes, hours, day of month, month of year, and day of week, to specify the interval for the Cron job. An asterisk (*) for any of the format field means that any value for that field will be accepted. For example, to run the command ls 30 minutes after each hour the corresponding cron configuration line would be: `30 * * * * ls`. Other symbols, such as the step value symbol (/) can be used to provide further control. For example, to create a history backup every thirty minutes the corresponding cron configuration line would be: `*/30 * * * * history > history.txt`.

VI. Lab 6: Windows Active Directory Hardening

This lab is intended to increase the student's familiarity with Active Directory and Group Policy. The tasks in this lab are focused on securing Windows Active Directory running on a Windows server. Completing this lab should take approximately two hours.

Active Directory Domain Services (Active Directory) is a service found on Windows Server operating systems. Active Directory is a suite of configuration tools created by Microsoft which can be used to perform remote administration of systems [13].

Active Directory when used to control and configure a group of machines, is known as a *Domain Controller*. A Domain Controller can be used to remotely push policies, known as *Group Policies*, to all systems on the domain. In the following tasks, you will enable and configure Active Directory on a Windows Server, create Group Policy Objects, and perform a few basic Domain Controller hardening tasks. A base Windows server running Active Directory is configured with numerous common vulnerabilities. students first read the lab directions before attempting to secure the machine.

A. Learning Objectives

- Configure Windows Server
- Configure Active Directory
- Understand Active Directory and Domain Controllers

B. Mapping to NIST Nice Framework

NIST NICE Framework KSAs mappings:

- Cybersecurity and Privacy Principles (K0004)
- Cyber Threats and Vulnerabilities (K0005)
- Test and Evaluation Processes (K0250)
- Recognize Types of Vulnerabilities (S0078)
- Apply Cybersecurity and Privacy Principles to Organizational Requirements (S0367)
- Apply Cybersecurity and Privacy Principles to Organizational Requirements (A0123)

C. Configuration and Setup

This lab requires three virtual machines connected to the same network: (1) A standard Windows Server installation, (2) A DNS Server, (3) A standard Windows Client.

D. Student Challenges

The learning objectives of these challenges are: (1) Learn to tailor a default Windows Server installation with a focus on security; (2) Learn to audit settings in a Windows Server installation with a focus on system hardening.

- **Task 1: Configure Window Server**
  A common hardening task is changing default settings. For Windows Server, there are numerous default settings that students must examine and determine if the default settings are sufficient or if they need to be changed. The following list illustrates some of the Windows Server tasks students should complete.

  1) Configure the hostname `CYOTEE-DC`
  2) Configure an IPv4 address of `192.168.7.20` and a default gateway of `192.168.7.1`.
  3) Configure the preferred DNS Server and no alternate DNS server.
  4) Configure the time zone.
  5) Ensure that the Windows Server is configured as a Global Catalog server.
  6) Ensure that the Windows Server is configured as a DNS Server.
  7) Configure DNS on the Windows Server to use the external DNS server with IPv4 address `192.168.7.30` as a forwarder.
  8) Configure the Windows Server to not allow **root hints**.
  9) Install Active Directory role on the Windows Server.

- **Task 2: Configure Active Directory**
  Using default settings in Active Directory may enable malicious activities to occur. Similar to Windows Server students must examine and determine if the default settings for Active Directory are sufficient or if they need to be changed.

  1) Create a new forest.
  2) Create a `cyotee.local` domain in the forest.
  3) Configure the Forest Functional Level.
  4) Configure the Domain Functional Level.

5) Create Two Organizational Units (OU).
   - Faculty
   - Staff

6) Create the three users for each OU. The username naming convention is `<first-name>.<lastname>@<domain>`. There are no spaces or punctuation within a name. Create a default password for each user (`Password123`), and require a password change at the next login.
   - Faculty
     - Emma Castillo
     - Jeanette Wise
     - Bernadette Rivera
   - Staff
     - Boyd Harmon
     - Jeremiah Houston
     - Adrian Miles

- **Task 3: Security Group and Policies**
  Active Directory default Security Groups (SG) include Account Operators, Administrators, DNS Admins, Domain Admins, Guests, Users, Protected Users, Server Operators, and many more. Understanding how to approach all these groups with a best-practice mindset is key to keeping a system secure. Students must examine and determine if the default security groups are sufficient or if they need to be changed/modified/deleted. The following list illustrates some of the Active Directory Security Group tasks students should complete.

  1) Create Global Security Group for each OU.
  2) Add each OU's user to the respective SG.
  3) Create a Shared Folder for Each OU. The name of the Shared Folder will be the OU name plus the word **Folder** (ex: StaffFolder). Only OU members have access to the folder. The network path will be

     `\\server\share\<foldername>`.

  4) Create a domain linked Group Policy Object (GPO). The GPO Specifications are:
     a) Named `cyotee-pol`.
     b) Create a Folder Redirection Policy. Map the `Documents` folder to a network share on the Windows Server at

        `\\server\share\network-share`.

     c) Remove `Run` from the Start Menu.
     d) Set the Control Panel to only start in icon view.
     e) Block use of `regedit.exe`.
     f) Disable user access to the command prompt.
     g) Disable user ability to change the system time.
     h) Block use of `taskmgr.exe`.
  5) Install the File Server Resource Manager (FSRM). Configuration specification include:
     a) Install FSRM on the Windows Server.
     b) Create a text file in the user's `Desktop` directory containing the word *classified*.
     c) Create a Classification Property called `Classified Property`
     d) Create a Classification Rule called **Classified Files** for files which contain the word *classified*.
     e) Apply the Classified Files rule to the user's Desktop directory.
     f) Verify whether or not the classification rule was applied properly by running the classification.
  6) Create a File Screen. Specifications include:
     a) Block all `.bat` and `.exe` files from running.
     b) Apply the screen to `My Documents` directory.
     c) Generate an appropriate warning message.
     d) Verify that the screen works by attempting to run a `.bat` file in the affected directory.

- **Task 4: Apply Principles of Least Privilege**
  In Active Directory, there are three levels of administrators, namely: Built-In Admins, Domain Admins, and Enterprise Admins. The Built-In Admins group tends to have many users because this group has less privileges than those users in the Domain Admins and Enterprise Admins groups. The privilege levels of each group are actually irrelevant because a member of any of the three groups can modify the membership of the other groups. The ability to modify membership of the other groups allows for a security vulnerability, by effectively gaining administrative control over all systems in the nested group [14]. It is suggested that administrative privileges only be granted to users who absolutely require the role to perform their tasking [15].

- **Task 5**: Remove Browsers
  Microsoft's Windows Server online documentation suggests to improve domain controllers security, one should remove all web browsers [16]. The article states:

  "Browsing the Internet (or an infected intranet) from

one of the most powerful computers in a Windows infrastructure using a highly privileged account (which are the only accounts permitted to log on locally to domain controllers by default) presents an extraordinary risk to an organization's security. Whether via a drive by download or by download of malware-infected "utilities," attackers can gain access to everything they need to completely compromise or destroy the Active Directory environment."

- **Task 6: Hardening Administrator Accounts** Administrator accounts have increased privileges and can often be used to compromise a domain. Securing administrator accounts includes multi-factor authentication and anti-delegation [14].
  1) Require smart card logon for administrators.
  2) Set administrators as sensitive and not delegated.

VII. Assessment

Assessment occurs in two ways. First, students need to submit a lab report explaining the processes for completing the lab tasks. Students also need to explain any discoveries from the lab. The report is graded based on a standard rubric that assesses the completeness of the lab report. Completeness is how well students followed the directions, and how well the report explains the weakness and solution to that weakness. A typical report would contain: (1) an in depth explanation of the weakness, (2) an explanation of the opportunities to exploit the weakness, including activity and impact of the weakness, and (3) an in depth explanation of the tools/methods that are used in mitigating the weakness. Depending on the nature of the lab and its tasks, the report may be centered around a few questions given as part of the lab.

The second form of assessment occurs at the next lab session. Before the next lab is introduced students will complete a small multiple choice/matching quiz based on the previous lab's concepts. These quizzes are meant to continually reinforce concepts and techniques. The idea is that when students attend a Cyber Defense Competition, they are expected to switch between tasks quickly and harden and maintain the security of multiple systems at the same time. These quizzes are not punitive, instead quizzes are meant to remind students of important tasks and concepts and techniques for implementing and maintaining security.

VIII. Conclusion

Cyber Defense Competitions have shown to be effective at preparing participants for integration into the cybersecurity workforce. CYOTEE fills the need for targeted preparation material with respect to Cyber Defense Competitions. By completing the 6 laboratory exercises in CYOTEE, participants will develop knowledge, skills, and abilities which directly map to those indicated in the NIST NICE Cybersecurity Workforce Framework. The laboratory exercises provide students with the opportunity to perform various technical tasks which are motivated by tasks seen at Cyber Defense Competitions, which are in turn motivated by system and network hardening tasks commonly performed at organizations to maintain secure systems.

CYOTEE also includes three discussion-based laboratory exercises. These provide students with the opportunity to discuss other important topics in an IT environment. Topics such as customer service, organizational management, and incident management are critical to the successful operation of an organization and are included at Cyber Defense Competitions. For space reasons, details of these, and other exercises available in the CYOTEE set, will be published elsewhere.

CYOTEE exercise descriptions and all needed laboratory environment setup scripts are freely available in the project GitHub repository at:

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

Acknowledgements

We thank the University of Idaho's (UI) College of Engineering, UI Center for Secure and Dependable Systems, UI Computer Science department, and Eastern Washington University (EWU) Computer Science department's technical and administrative staff for maintaining the infrastructure and support systems which enable our research and instructional programs, including the work presented in this article. We also thank CISSE reviewers and journal editors for their help improving this manuscript.

This research was funded, primarily, by the U.S. National Science Foundation (NSF) under CyberCorps® award 1565572. Mr. Pattanayak was an NSF CyberCorps® scholarship recipient. The infrastructure used to support it was partially funded by NSF, the Idaho Global Entrepreneurial Mission (IGEM17-001), and the M.J. Murdock Foundation. The opinions expressed in this article are the author's and not those of the NSF, the State of Idaho, or the M.J. Murdock Foundation.

References

[1] "National collegiate cyber defense competition," http://nationalccdc.org/index.php/competition/competitors/ccdc-regionals, July 2021.

[2] "Department of energy's cyberforce program," https://cyberforcecompetition.com/, August 2021.

[3] C. La Fleur, B. Hoffman, C. B. Gibson, and N. Buchler, "Team performance in a series of regional and national us cybersecurity defense competitions: Generalizable effects of training and functional role specialization," *Computers Security*, vol. 104, 2021.

[4] D. Conte de Leon, C. E. Goes, M. A. Haney, and A. W. Krings, "Adles: Specifying, deploying, and sharing hands-on cyber-exercises," *Computers Security*, vol. 74, 2018.

[5] "Resource guide: Preparing for the collegiate cyber defense competition (ccdc): A guide for new teams and recommendations for experienced players," https://www.nationalcyberwatch.org/resource/, National CyberWatch Center, 2015.

[6] W. Du, "Seed project," https://seedsecuritylabs.org/, July 2021.

[7] L. Cridlin, "The importance of hands-on learning," *International Laser Safety Conference*, pp. 151–156, 01 2007.

[8] S. Hidi, "Interest, reading, and learning: theoretical and practical considerations," *Educational Psychology Review*, vol. 13, no. 3, pp. 191–209, Sep 2001. [Online]. Available: https://doi.org/10.1023/A:1016667621114

[9] C. O. Ekwueme, E. E. Ekon, and D. C. Ezenwa-Nebife, "The impact of hands-on-approach on student academic performance in basic science and mathematics," *Higher Education Studies*, vol. 5, no. 6, p. 47–51, Nov 2015. [Online]. Available: https://www.ccsenet.org/journal/index.php/hes/article/view/53305

[10] W. Newhouse, "Nice cybersecurity workforce framework: national initiative for cybersecurity education," 2017-08-07 2017.

[11] "National initiative for cybersecurity education," 2019.

[12] G. Avner, "The top 10 linux kernel vulnerabilities you must know," https://www.whitesourcesoftware.com/resources/blog/top-10-linux-kernel-vulnerabilities, March 2020.

[13] A. Jillepalli, D. Conte de Leon, F. Sheldon, and M. Haney, "Enterprise-level hardening of web browsers for microsoft windows," *IJCDS Journal*, vol. 7, pp. 261–274, 09 2018.

[14] B. Mathers, J. Flores, K. Chewie, Y. Shengjin, S. Kumar, E. Ross, K. Nikolaev, L. Poggemeyer, and C. Watson, "Implementing least-privilege administrative models," Aug 2018.

[15] M. Miller, "Active directory security explained and 7 best practices," November 2018.

[16] B. Mathers, J. Flores, L. Poggemeyer, Y. Shengjin, S. Kumar, E. Ross, and A. Rechenberg, "Securing domain controllers against attack," June 2017