Journal of Cybersecurity Education, Research and Practice

Volume 2021 | Number 1 Article 4

July 2021

Observations, Evaluations, and Recommendations for DETERLab from an Educational Perspective

Ahmed Ibrahim
University of Pittsburgh, aibrahim@pitt.edu

Vitaly Ford
Arcadia University, fordv@arcadia.edu

Observations, Evaluations, and Recommendations for DETERLab from an Educational Perspective

Abstract

DETERLab is a cluster environment that provides a set of virtual machines that can be used by researchers and teachers to run cybersecurity experiments and competitions, and where it is possible to deploy different network configurations to research attack and defense mechanisms in the cyber world. While we were working to develop a pathway for producing more usable and effective cybersecurity educational resources by investigating and examining several projects, we examined DETERLab as a prospective platform to use in the classroom. Throughout our experimentation, we faced challenges that we decided to document in order to help other educators use the environment effectively. In this article, we reflect on the application process, available resources, getting started, and running experiments. We also include an analysis of experiments that have a step-by-step guide, sample solution, grading criteria, network diagram, and teacher manual. In addition, we reflect on the environment for usage in a classroom setting and list all available materials as of the time of writing this article. We believe that DETERLab has the potential to be widely adopted in cybersecurity courses to develop the necessary skills if the key user experience and technical challenges mentioned in this article are addressed. As part of our future work, the findings in this article will be compared to other projects in a much larger research study aiming to develop a pathway for producing more usable and effective cybersecurity educational resources.

Keywords

Cybersecurity, Hands-on Education, DETERLab, Recommendations

INTRODUCTION

Presently, there are numerous unfilled cybersecurity positions advertised by many different sources (Cybercrime Magazine, 2019; Perhach, 2018). A major problem in this area is filling the gap between knowledge and skills. Cybersecurity education is an essential player in producing students that can fill this gap (Winick, 2018; University of San Diego, 2018). An essential element in cybersecurity education is exposing students to hands-on scenarios where they can exercise and put into practice the theory they learn about in the classroom. However, cybersecurity educators face the challenge of offering labs and exercises for their students that simulate real-world scenarios. Developing such labs and exercises is a time-consuming task with many technical challenges, and therefore, it is typical that instructors will look for existing ones that can be easily adopted in their classroom.

Today, several educational platforms offer hands-on cybersecurity instructional labs and exercises (National Initiative for Cybersecurity Education, 2020; SEED Labs, 2020; Siraj & Ghafoor, 2014; DETER Project, 2021). Some of these platforms are easier to use than others and they typically present different types of exercises. In all cases, instructors would prefer to use platforms that are in their simplest form (usable), easy to set up (if needed) and use, well supported, provide enough directions to learners, list expected outcomes, include grading criteria, and offer teacher manuals. Based on these preferences, we assess one such platform called "DETERLab" as part of a larger research study we are working on to develop a pathway for producing more usable and effective cybersecurity educational resources.

DETERLab (DETER Project, 2021; Mirkovic & Benzel, 2012), part of the DETER Project (Benzel, 2011), is a cluster environment that focuses on providing researchers and instructors with a set of virtual machines to run cybersecurity experiments and competitions as well as deploying different network configurations to research attack and defense mechanisms in the cyber world. We decided to evaluate DETERLab's usability and effectiveness in educational settings, providing practical recommendations for improvement because we believe that the platform has the uncovered potential and clear direction if it is made more adoptable.

In this article, we provide our observations and evaluations for the DETERLab project from an instructional perspective. We used a qualitative approach to evaluate the usability and adoptability characteristics of the DETERLab project. We began by creating a class/project, then launched many of the available experiments, and went through all of them as students and instructors. Additionally, we used a quantitative approach in the "Teacher Manuals" subsection to determine

which DETERLab exercises include a network diagram, list the number of machines required, and whether exercises have a corresponding teacher manual. We also identified Teacher Manuals that have a step-by-step guide, sample solution, grading, criteria, and a grade sheet.

All the challenges we faced are documented and shared in this article to help other educators use the environment effectively. Although the DETERLab project has the potential to be used while teaching cybersecurity courses to develop students' skills, this article lists key user experience and technical challenges that moved us away from using it. Our future plan includes polling the broader cybersecurity education community as part of a larger research that will involve evaluating other hands-on cybersecurity education platforms (NICE Challenge, SEED Project, etc.).

Since we could not find any related work on evaluating DETERLab, we provide a quick background on it in the Background on DETERLab section. In the next section, we go over the application process and beginning an experiment. In the Testbed Educational Experiments section, we reflect on our experience with a homework exercise, a "Capture the Flag" (CCTFs), and inspecting teacher manuals. We discuss the challenges we faced as well as our recommendations in the Observations and Recommendations section. Finally, we conclude the article with an overview of future work.

BACKGROUND ON DETERLAB

DETERLab is introduced in (Mirkovic & Benzel, 2012) as an educational facility to help teach cybersecurity topics. It is based on the DETER Project which allows users to reserve physical machines and access them via Secure Shell (SSH). The machines run Linux-based OS and applications of the user's choice and can be organized into a user-specified topology. The DETER Project provides the necessary hardware resources to allow simultaneous classes to run on DETERLab.

The project was developed specifically for easy adoption in educational settings. As mentioned in (Mirkovic & Benzel, 2012), instructors will have detailed guidelines on using DETERLab, managing classes, offering educational exercises, and contributing to available material. In addition, a student manual and an instructor manual should be available for each exercise offered on DETERLab. In the Testbed Educational Experiments section, we discuss these and other related issues.

DETERLab was designed to provide an active learning, beginner-friendly environment (a gradual increase of difficulty level) with a large number of computing resources limiting risk for live malware analysis and automating exercise setup, as well as providing access to reusable, rigorous, and modular

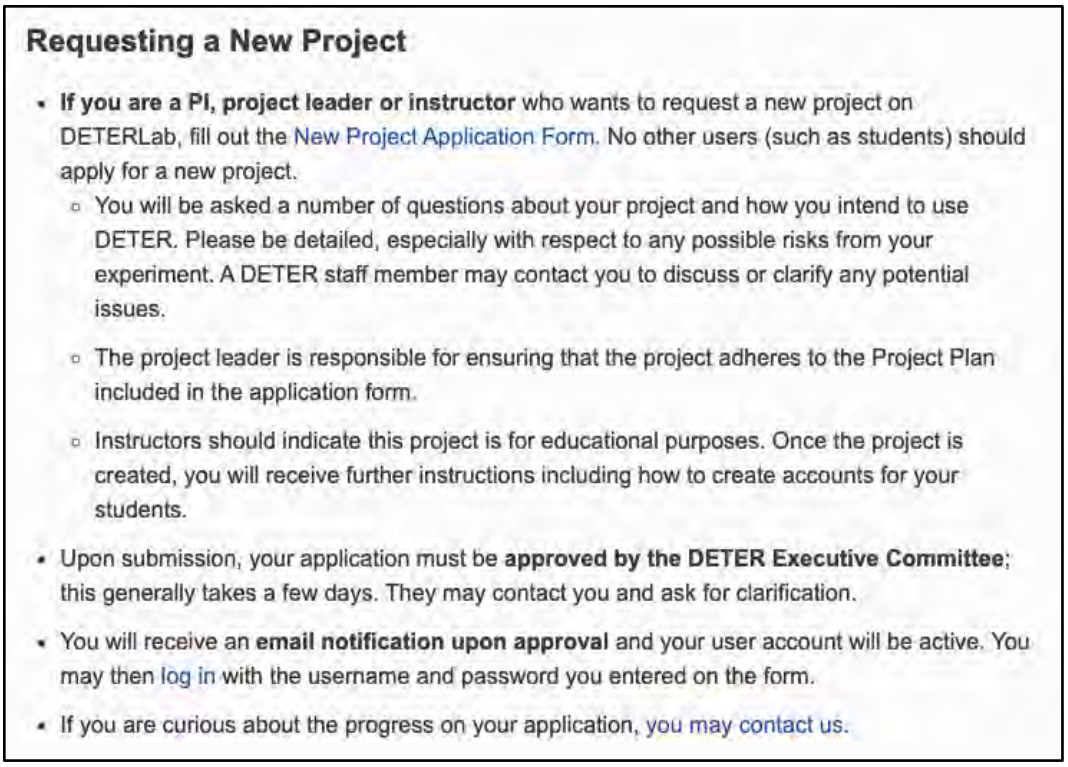
experiments at any time. According to (Mirkovic & Benzel, 2012), in 2012, DETERLab was used by over 47 universities and colleges, and had more than 400 general-purpose computing nodes. As of December 2016, DETERLab users have created 192 projects for their classes and DETERLab has served 13,000 students (DETERLab: User Projects, 2016). However, we could not find any feedback data from students or instructors about their experiences using the platform, and there was no study addressing the areas for improvement.

APPLICATION PROCESS AND BEGINNING AN EXPERIMENT

The DETERLab website mentions that it offers a variety of exercises that cover a wide range of topics including buffer overflows, code/command injection attacks, man-in-the-middle attacks, worm modeling and detection, botnets, and DDoS attacks.

If the user begins researching DETERLab (DETER Project, 2021) by first visiting the DETER Project (Mirkovic et al., 2010) site, they will find that the page they are directed to has a description about DETERLab and a hyperlink in the menu on the right called "Apply for an account" (DETERLab: Application, 2021). The link does nothing but brings the user to the same page they are already on. If they click on the hyperlink called "Registering to Use DETERLab" (DETERLab: Register, 2021) in the body of the page, they will be directed to a page (from a WiKi) including information on how to "Request a New Project" as shown in figure 1.

The "New Project Application Form" (DETERLab: New Project, 2021) is simple. After our registration was approved, our biggest problem was the login process. The first thing we noticed when visiting the DETERLab site is that there is no visible "Register" or "Log in" buttons. But when we looked again into the "Request a New Project" section (figure 1), we noticed a hyperlink called "log in" (DETERLab: Login, 2021). Users should bookmark it because we did not find any other way to log in except by following that inconspicuous link on the "Request a New Project" page. Once users log in as an instructor for the first time, they will land on a page (shown in figure 2) showing their profile. This page includes information about (a) the number of available PCs, (b) tabs, (c) options, and (d) three dropdown menu items. New users should be aware that they are missing an "Experiments" tab until they create an experiment.



Requesting a New Project

- **If you are a PI, project leader or instructor** who wants to request a new project on DETERLab, fill out the New Project Application Form. No other users (such as students) should apply for a new project.
  - You will be asked a number of questions about your project and how you intend to use DETER. Please be detailed, especially with respect to any possible risks from your experiment. A DETER staff member may contact you to discuss or clarify any potential issues.
  - The project leader is responsible for ensuring that the project adheres to the Project Plan included in the application form.
  - Instructors should indicate this project is for educational purposes. Once the project is created, you will receive further instructions including how to create accounts for your students.
- Upon submission, your application must be **approved by the DETER Executive Committee**; this generally takes a few days. They may contact you and ask for clarification.
- You will receive an **email notification upon approval** and your user account will be active. You may then log in with the username and password you entered on the form.
- If you are curious about the progress on your application, you may contact us.

Figure 1: DETERLab -Requesting a New Project

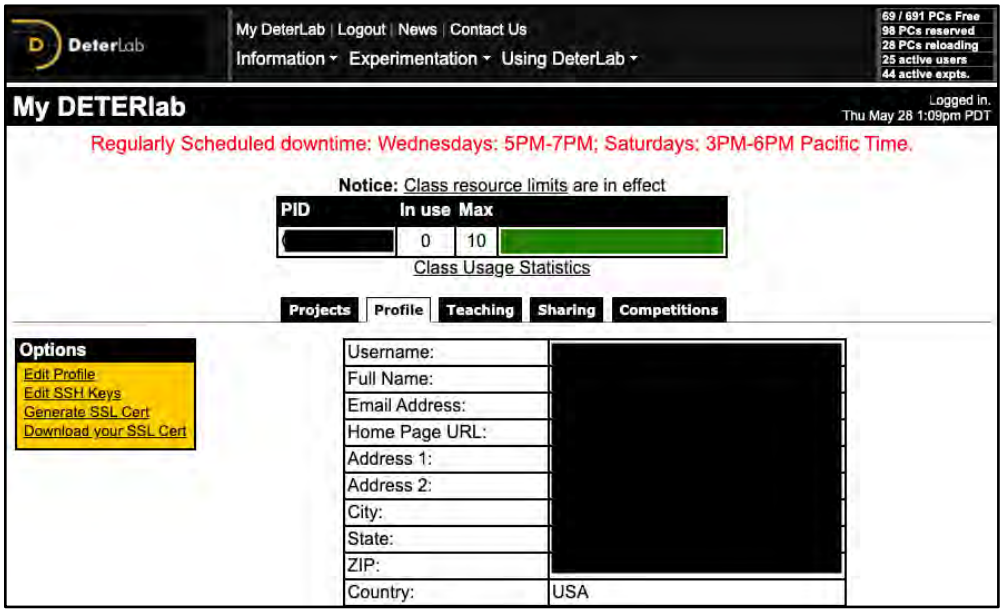


Figure 2: DETERLab Landing Page When Logged In

To create an experiment, users must click on the "Experimentation" dropdown menu and then choose "Begin an Experiment." However, with this, users are presented with a page (shown in figure 3) that asks them for information they do not know. Thus, we recommend that new users check all available experiments first.

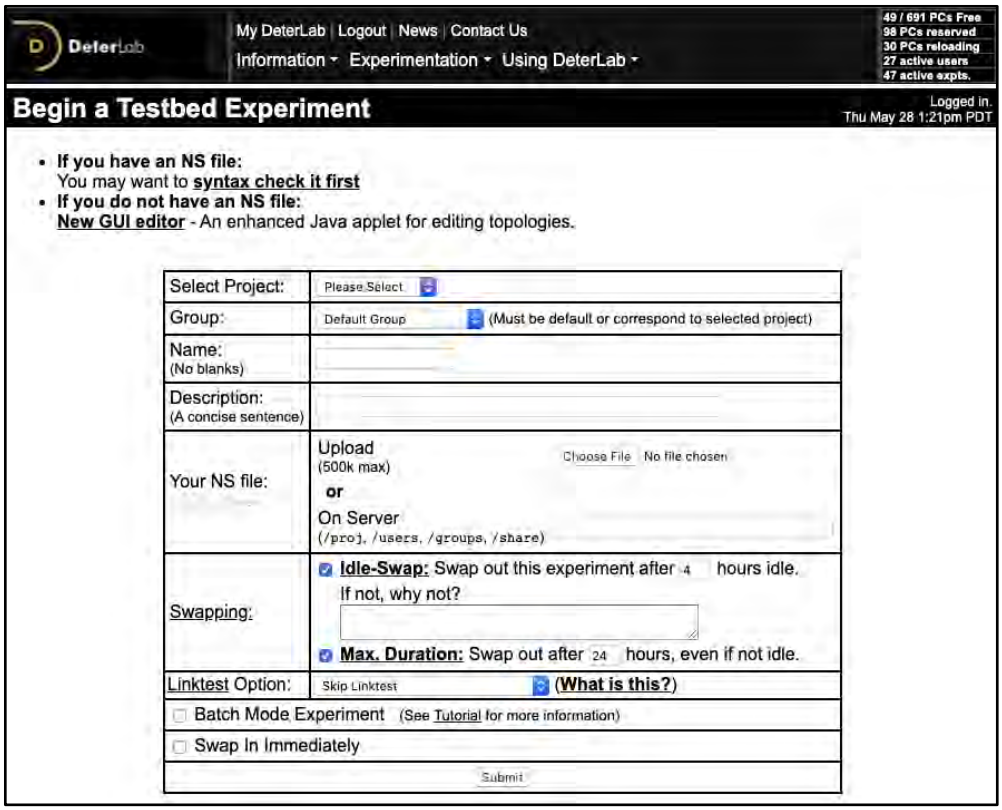


Figure 3: Beginning an Experiment

To see available experiments, they should click on the "Sharing" tab from the homepage and then click on the "Search" button under the "Find shared materials" section (shown in figure 4). This will show them the shared materials available publicly through the DETERLab project. The materials are divided into the following categories/criteria:

- Homework: 23 entries
- CCTF: 4 entries
- Teacher Manual: 17 entries
- Toolkits: 2 entries
- Experiment: 6 entries
- Dataset: 1 entry

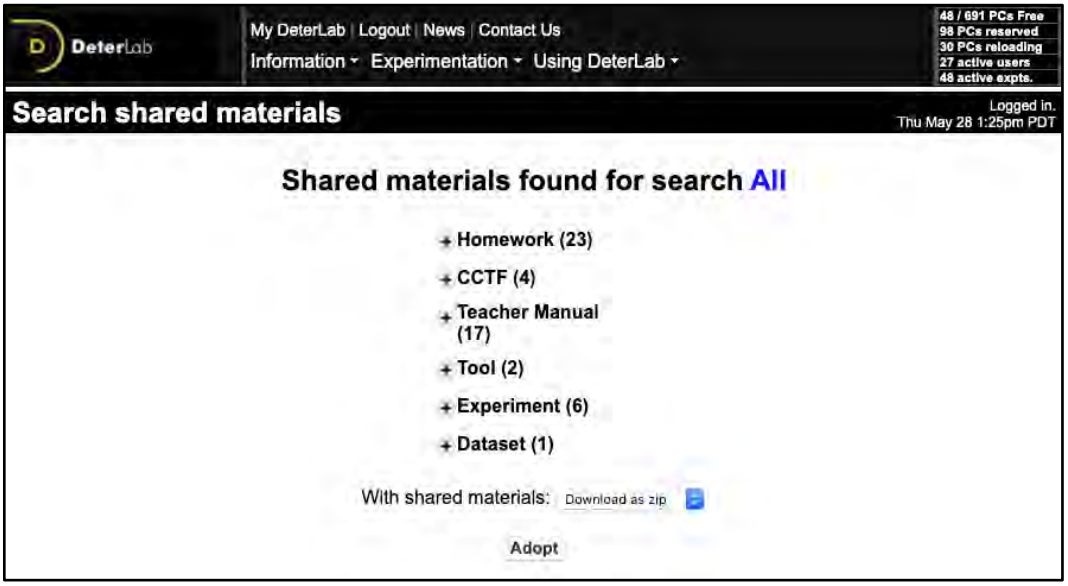


Figure 4: Searching for Shared Material

TESTBED EDUCATIONAL EXPERIMENTS

It was challenging for us to get started because the materials do not follow any kind of standards or consistent formatting. New users should expect to spend several hours trying to find what may work for them. In DETERLab, there are 23 homework assignments and 4 CCTF materials to choose from. In this section, we will go over one homework exercise, one CCTF, then we will discuss each of the respective teacher manuals.

Homework Experiment Experience

To begin the "Linux and DETERLab intro" homework experiment, users can select the "checkbox" under the "Adopt?" column for the "Linux and DETERLab intro" homework entry, then go to the bottom of the page, and change the dropbox from "Download as zip" to "Adopt to my class" then click the "Adopt" button. Users will then be directed to a page listing their class material, which may be difficult to return to in the future. If they lose that page, they can get back to it from their home page by following the sequence: Teaching Tab, click on the project name, and then click on "Manage Materials" from the menu on the left.

Adding material simply makes it available in the user's class menu. The user must still create the experiment to do the homework. Somewhere in the homework, the user will find the information about the NS file which is needed for that homework. For example, in the "Linux and DETERLab intro" homework, the NS

file is located in the `/share/education/LinuxDETERIntro_UCLA/intro.ns` path. Now, if the user goes to the "Begin an Experiment" page (shown in figure 3 previously), they can populate the form with all needed information and use the NS file path they got from the homework in the "Your NS file" textbox. Then, the user should make sure to mark the "Swap In Immediately" box and click the "Submit" button. The user must then wait for 10 minutes or less (per DETERLab instructions) until the experiment is configured for them as shown in figure 5.

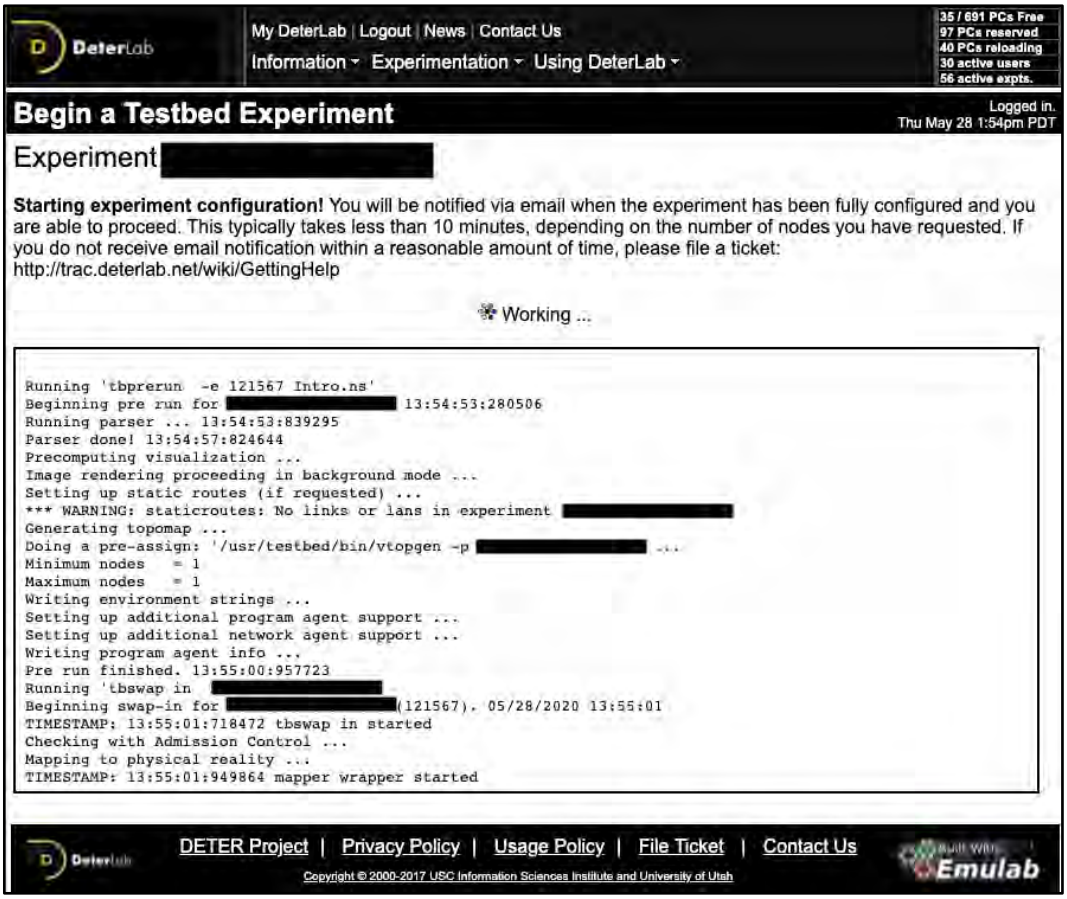


Figure 5: Log Output When Starting an Experiment

In our experiment, it took about 7.5 minutes for the experiment to be created and ready to use. Then the user must consider how to actually use it. The user should now be able to see the "Experiments" tab on their homepage. Once the "Experiments" tab is clicked, the user can click on the experiment name under the "EID" to view its configuration. Clicking on the experiment will direct the user to a page with lots of information as shown in figure 6.

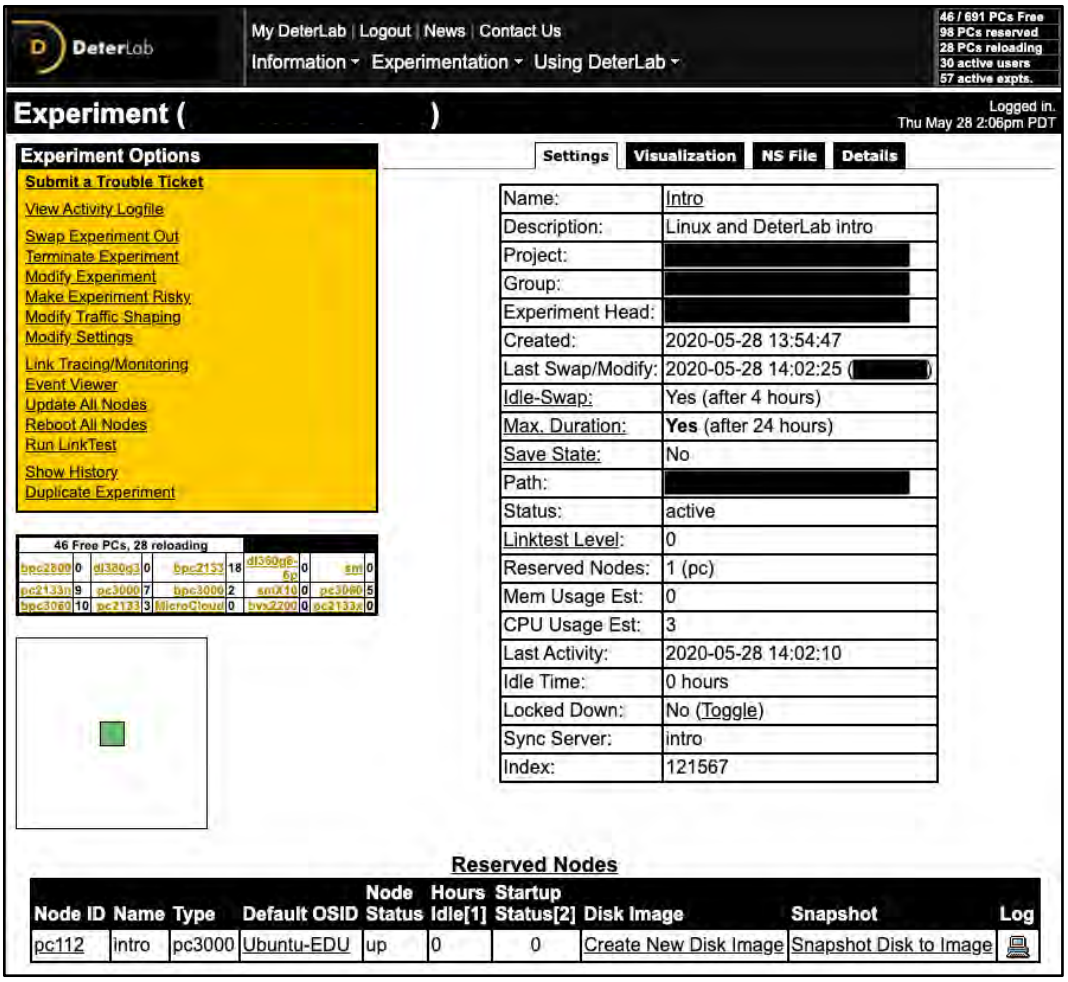
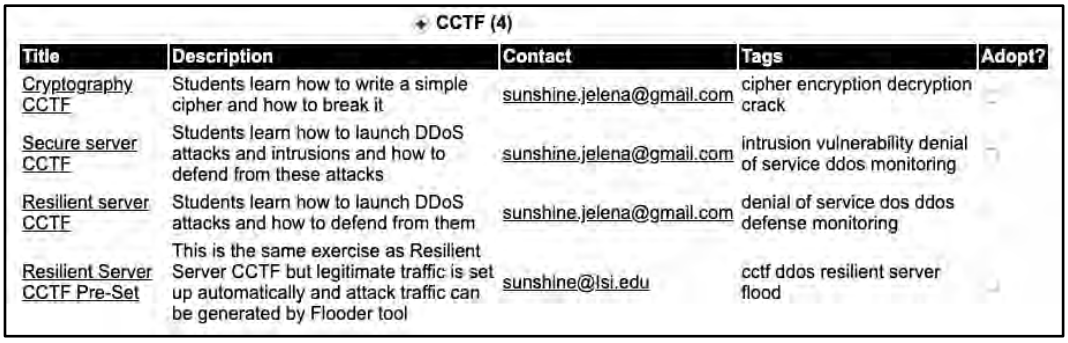


Figure 6: Main Experiment Page After Deployment

We chose the "Intro" experiment because it is simple and uses only one node (computer). Users may now wonder how to access this node (computer). Users must SSH into `users.deterlab.net` using their username and password, then SSH into any node (computer) they want to connect to (nested SSH). In our example, we had to locate the "Qualified Name" of the node (computer) we wanted to SSH into. We did this by clicking on the visualization box showing our nodes (the green box on the lower left in figure 6). For example, if the "Qualified Name" of the node is `intro.Intro.ProjName.isi.deterlab.net`, then users must SSH into `users.deterlab.net` using their username and password, followed by another SSH connection into the qualified node `ssh intro.Intro.ProjName.isi.deterlab.net` without any credentials.

CCTF Experiment Experience

The CCTF resources represent Capture the Flag (CTF) competitions, in which students are split into blue and red teams with the corresponding cyber defense and offense goals. At the time this article was written, there were 4 CTFs, namely: Cryptography CCTF, Secure server CCTF, Resilient Server CCTF, and Resilient Server CCTF Pre-Set (as shown in figure 7). In this subsection, we summarize the "Cryptography CCTF".



+ CCTF (4)

Title	Description	Contact	Tags	Adopt?
Cryptography CCTF	Students learn how to write a simple cipher and how to break it	sunshine.jelena@gmail.com	cipher encryption decryption crack	
Secure server CCTF	Students learn how to launch DDoS attacks and intrusions and how to defend from these attacks	sunshine.jelena@gmail.com	intrusion vulnerability denial of service ddos monitoring	
Resilient server CCTF	Students learn how to launch DDoS attacks and how to defend from them	sunshine.jelena@gmail.com	denial of service dos ddos defense monitoring	
Resilient Server CCTF Pre-Set	This is the same exercise as Resilient Server CCTF but legitimate traffic is set up automatically and attack traffic can be generated by Flooder tool	sunshine@isi.edu	cctf ddos resilient server flood	

Figure 7: List of Available CCTF Competitions

In the Cryptography CCTF, the instructor divides the students into teams and gives each team a file with 10 unique messages (in spoken English) to be exchanged between a client machine and a server machine. Student teams will play as both a Blue Team and a Red Team during the exercise. While playing as a Blue team, the students must create a client program that reads each message from the 10 unique messages, encrypts the message using monoalphabetic, polyalphabetic, homophonic, and polygram ciphers. The client program should then send encrypted messages to the server machine. The server program should be able to successfully decrypt the messages to retrieve the original unique messages. This process can be repeated multiple times. The instructions mention that the encryption/decryption key can be static and stored on the client and server machines.

While playing as a Red Team, the students have access to another team's middle box (sitting between the other team's client and server machines) that allows them to sniff the encrypted messages exchanged by the other team. The Red Team's tasks include implementing a cracking code for all possible ciphers (monoalphabetic, polyalphabetic, homophonic, and polygram) and storing the deciphered messages in a file that will be scored later.

The exercise mentions that the student teams will have to act as the Blue Team and Red Team simultaneously over 2 hours. However, it does not explicitly define the time frame needed for learning, configuring, and deploying the necessary applications on DETERLab. On the other hand, the teacher manual for this CTF (DETERLab: CCTF, 2021) mentions that teachers should break down student tasks

into milestones with appropriately assigned deadlines. The teacher manual also lists a few responsibilities for teachers within the experiment. For example, the teachers must access each team's environment (experiment) to set up access for the Blue Team's and Red Team's machine(s). Also, they may need to reboot a team's machine if a team gets locked out due to using incorrect `iptables` commands.

Although the exercise has the potential to engage students in active learning of cryptographic concepts from both defensive and offensive perspectives, it does not list any learning outcomes, prerequisite knowledge, or the level of difficulty. On the students' side, there were no explicit specifications or examples of ciphers that teams could implement (when using the standard `NS` file specifications and configuration scripts). Additionally, it does not seem feasible for the Red Team to brute-force all kinds of ciphers within a reasonable amount of time. Also, the scope of the required tasks is too large for any team. On the instructors' side, they would need to spend a significant amount of time familiarizing themselves with the system, configuring the necessary settings, and ensuring that everything will work properly for all teams.

The grading rubric provided with the exercises is too vague, making it challenging to grade the submissions. For exercises that have a teacher manual (discussed in the subsequent section, Teacher Manuals), an answer guide (solution) may be included but it provides little instruction on how to reach the solution. We think that these challenges will make this CCTF unlikely to be adopted by a large number of instructors.

As shown in figure 7, there are three more CCTFs. The "Secure Server CCTF" also divides students into teams where each team has defense (Blue) and attack (Red) responsibilities. The Blue side of each team should develop a banking application with a database (behavior and actions are specified in the exercise) and configure a DNS server that allows access to the machine hosting the banking application.

The Red side of each team should try to attack the banking application (gain unauthorized access to legitimate users' banking information or perform unauthorized actions on the banking application). The Red Team can accomplish this by using SQL injections, URL manipulations, exploiting backdoors, or cracking passwords. All the pros and cons we mentioned for the "Cryptography CCTF" apply to the "Secure Server CCTF" as well.

The two other items, "Resilient Server CCTF" and "Resilient Server Preset CCTF", are almost identical with a few rewrites in some sections. The "Secure Server CCTF" has a teacher manual whereas "Resilient Server CCTF" and "Resilient Server Preset CCTF" do not.

Teacher Manuals

When this article was written, there were 23 homework assignments and 4 CCTFs in DETERLab as shared materials, but only 19 teacher manuals (a cropped snapshot is shown in figure 8). All of the manuals are divided into the following sections:

- Place in the Curriculum
- Setup, Solutions, and Grading Suggestions
- Time Burden
- Known Problems and Experiences

Teacher Manual (17)

Title	Description	Contact	Tags	Adopt?
Secure server CCTF - teacher manual	Tools for setup and scoring	sunshine.jelena@gmail.com	secure server CCTF denial of service intrusions vulnerability	☐
Cryptography CCTF - teacher manual	Tools for setup and scoring	sunshine.jelena@gmail.com	encryption decryption cipher crack manual	☐
Linux and DeterLab intro - teacher manual	Teacher manual for this lab	pahp@d.umn.edu	intro linux deterlab teacher manual	☐
DNS man in the middle attack - teacher manual	Teacher manual for this lab	sunshine@isi.edu	dns mitm arp spoofing teacher manual	☐
Internetworking - teacher manual	Teacher manual for this lab	dmorgan@world.oberlin.edu	internet linux teacher manual internetworking network setup	☐
Man in the middle attack - UCLA - teacher manual	Teacher manual for this lab	pahp@d.umn.edu	mitm arp spoofing teacher manual	☐
Computer forensics - teacher manual	Teacher manual for this lab	pahp@d.umn.edu	computer forensics teacher manual	☐
BGP hijacking - teacher manual	Teacher manual for this lab	sunshine.jelena@gmail.com	bgp prefix hijack teacher manual	☐
Comparing UNIX environments - teacher manual	Teacher manual for this lab	dmorgan@world.oberlin.edu	comparing unix environments teacher manual	☐
Software exploits - teacher manual	Teacher manual for this lab	pahp@d.umn.edu	software exploits buffer overflow path traversal sql injection teacher manual	☐

Figure 8: Teacher Manuals

We examined each of the 23 homework assignments and 4 CCTFs to determine which ones include a network diagram, list the number of machines required, and whether they have a corresponding teacher manual. Table 1 shows that only 3 homework assignments (HW) have a network diagram, and 17 out of 23 HW and 2 out of 4 CCTFs have a teacher manual.

We believe the teacher manuals should help instructors navigate through the exercises (step-by-step) and provide clear answers such that they can feel confident in offering such exercises in their classes. We found that only some of the teacher manuals are well-written and provide step-by-step instructions, others lack an explanation of how to reach the solution. None of them provide screenshots or any other visual aids to help guide the instructors while walking through the teacher manual.

ID	Type	Topic name	Has a network diagram?	# of machines required	Has a manual?
1	HW	Worm modeling exercise	Not needed	0	Yes
2	HW	TCP SYN flood exercise	No	4	Yes
3	HW	Software exploits exercise	No more supported - divided into 14, 15, and 16		
4	HW	Securing legacy systems w/ Snort	No	7	Yes
5	HW	OS hardening	No	1	Yes
6	HW	Man in the middle attack - USC	Yes	5	Yes
7	HW	Man in the middle attack - UCLA	No	3	Yes
8	HW	Linux and DETERLab intro	No	1	Yes
9	HW	Internetworking	Yes	5	Yes
10	HW	DNS man in the middle attack	No	5	Yes
11	HW	Computer forensics	No	1	Yes
12	HW	Comparing UNIX environments	No	3	Yes
13	HW	BGP hijacking	Yes	7	Yes
14	HW	Buffer Overflows - UCLA	No	1	Yes - shared manual
15	HW	Pathname Attacks - UCLA	No	1	
16	HW	SQL injection	No	1	
17	HW	POSIX Permissions	No	2	No
18	HW	Firewalls - UCLA	No	2	No
19	HW	Password cracking	No	1	No
20	HW	Intro-Lab-UKY	No	1	No Need
21	HW	Intro-Lab-UKY1	No	1	No Need
22	HW	IPSec	No	5	No
23	HW	IPv6 Internetworking	No	4	No
24	CCTF	Cryptography CCTF	Yes	3	Yes
25	CCTF	Secure server CCTF	No	Not needed	Yes
26	CCTF	Resilient server CCTF	No	Not needed	No
27	CCTF	Resilient Server CCTF Pre-Set	No	Not needed	No

Table 1: Homework materials and corresponding teacher manuals

Table 2 shows which Teacher Manuals have a step-by-step guide, sample solution, grading, criteria, and a grade sheet. We noticed that the sample solution file provided in the "Computer Forensics" teacher manual is corrupted and the "Network Intrusion Detection Systems" teacher manual does not correspond to any existing homework or CCTF and is very lengthy in terms of the number of tasks. Additionally, almost all of the teacher manuals lack a set of grading criteria.

Teacher manual	Step-by-step guide	Sample solution	Grading criteria	Grade sheet
Worm modeling			x	
TCP SYN flood	x			
Buffer Overflows, Pathname Attacks, & SQL Injections		x		x
Securing Legacy Systems		x		
OS Hardening		x		
Network Intrusion Detection Systems		x		x
MITM ARP Poisoning		x		
MITM Lab	x	x		x
Intro to DETER and Unix		x		
Internetworking				
DNS and MITM Attacks	x	x		
Computer Forensics		Corrupted		x
Comparing UNIX environments		x		
BGP Prefix Hijack Attacks	x	x		
POSIX Permissions	x	x		x
CCTF Secure Communication				
CCTF Secure Server				

Table 2: DETERLab materials with corresponding teacher manuals

OBSERVATIONS AND RECOMMENDATIONS

In this section, we will share what we observed throughout our experience trying to use DETERLab for our classrooms. We divide the set of challenges we faced into user experience challenges and technical challenges. Additionally, we will include recommendations that we think could make DETERLab more adoptable.

User Experience Challenges

User Interface: The first major struggle we faced was related to a confusing, outdated user interface (UI). It was challenging to navigate the platform, find where and how to start, and figure out how to add experiments to our project/class. We strongly recommend a major UI overhaul to make it simple, easy to use and navigate, and mobile-friendly.

Navigation-wise, it was difficult to remember how we reached certain pages. There were no "Back" buttons and breadcrumb navigation. The left-menu does not have clear, meaningful names. And more importantly, there is no clear "Sign in" page reachable from the DETER Project site. We had to sign in by adding the link, which we found through an external search engine outside of the DETER Project site, to our bookmarks.

In addition, tabs on the homepage were not consistent. We did not see an "Experiments" tab until we figured out how to add our first experiment -- and only then did a new tab called "Experiments" appear on the instructor's page. We certainly think it would have been better if the tab was always available and once it was clicked, users could have an option to create a new experiment.

Wiki: To learn about the platform, we were directed to the site's Wiki which was complex, overcrowded with text, and not well organized. It was difficult to find an answer to our questions as the search feature was not giving the correct results. Eventually, we had to use an external search engine to actually look things up on the Wiki but even with that, it required an unreasonable amount of time to learn how to use the platform and connect it with the existing and new experiments.

Overall, the Wiki did not seem to be written with the end-user in mind. There are some very useful tips and guidance but they need to be reorganized to allow for a better flow of information as well as include sample screenshots and video tutorials.

Getting Started: Although the above-mentioned two challenges make it difficult to use the platform, we found the platform to be even more challenging for newcomers. We felt that the Wiki and UI are made for people who are very familiar with DETERLab. Thus, new users may face a big learning curve and a lot of challenges, discouraging them from using the platform in their curriculums.

We recommend offering an online training module to use DETERLab for all new users. The module could include videos and sample exercises to walk instructors (and students) through the process of acclimating themselves to the platform.

Technical Challenges

There were several technical challenges that we encountered while working with DETERLab.

Computing Resource Availability: The upper right corner of the DETERLab website showed the number of available PCs out of 691 PCs in total. The number of PCs freely available for deployment varies from day to day, but overall, it has been very low in spring 2020 (under 100), meaning that there is no guarantee instructors will have enough computing resources for students to run experiments at a given time or day. This poses a serious scalability challenge.

Also, instructors must find out the maximum number of machines the students may use at any given time and set their project's "Resource Limit Max" to that number. To figure out how many machines an exercise needs, instructors must swap in that exercise. They can then multiply the number of machines the exercise uses by the number of students in the course.

For example, when the MITM Lab is swapped in, the instructor can see that it requires three PCs. For a 50-student class, the worst-case scenario is that all students will perform the lab at the same time which means that DETERLab must have 150 available PCs. However, assuming that only 15 students will be performing the lab just before the due date, DETERLab must have 45 PCs available at that time. We recommend that instructors have a policy in their syllabus to handle a situation where no PCs are available for students to run their exercise.

Complex Technical Interaction: First, nested SSH connections are required to connect to the remote hosts and they can make the navigation between the hosts on the network confusing. Also, while setting up the experiments/labs, instructors and students may encounter problems with the software versions since some of the labs have not been tested for the past several years. To solve the problem of software version changes, the developers can get the software needed directly on the DETERLab repository or use containers such as Docker (2021).

Additionally, complex experiments/labs like the Secure Server CCTF will require a significant amount of management work by the instructor to prepare the students' Blue/Red Team access to each team's environment/experiment. Since the preparation and management effort by the instructor significantly varies from experiment to experiment, we recommend that DETERLab provides instructors with technical training.

CONCLUSION & FUTURE WORK

In this article, we reviewed DETERLab as an instructional tool that can offer hands-on cybersecurity training in higher education. We reflected on the application

process, available resources, getting started, and running experiments. We critically examined the environment for usage in a classroom setting and listed all available materials as of the time this article was written. Some of the labs were well-written and provided structured educational content whereas others needed an instructional review to make them adoptable. As new users of DETERLab, we encountered multiple challenges that we summarized in the Observations and Recommendations section. We believe that the major challenges include the learning curve to get started, inconsistent material, and limited availability of computing resources.

Our recommendation to those who are looking to use DETERLab is simple: the core of the experiments is great and could be used successfully in the classrooms but expect to put in significant effort and spend a considerable amount of time familiarizing yourself with how things work. Our recommendation to the DETERLab team is to: restructure and redo the Wiki, make the website usable and user-friendly, make homework and teacher manuals consistent, and provide training videos/classes for instructors. Besides, we think that publishing user reviews provides transparency and makes the material reliable, hence improving the material over time.

The findings in this article will be compared to similar projects (NICE Challenge, SEED Labs, U.S. Cyber Range, CLARK, etc.) to develop criteria that can categorize and evaluate existing cybersecurity education resources. For example, the NICE Challenge offers on-demand challenges to practice different "operate", "maintain", "protect", and "defend" scenarios. The challenges are well designed, mapped to the NICE Framework KSAs (National Initiative for Cybersecurity Education, 2020) and CAE Knowledge Units (National IA Education & Training Programs, 2019), include a network map, and present a realistic narrative to students. However, it does not provide a teacher manual and has a 2-day reservation period, limiting the participation and practical adoption in a classroom. As part of our future work, we look forward to conducting a critical review of each of the available cybersecurity educational resources to assess their usability and effectiveness. The ultimate outcome of our research aims to develop a pathway for offering more usable and effective evidence-based cybersecurity educational resources.

REFERENCES

Benzel, T. (2011). The science of cyber security experimentation: the DETER project. In *Proceedings of the 27th Annual Computer Security Applications Conference* (pp. 137-148). Association for Computing Machinery. https://doi.org/10.1145/2076732.2076752

Cybercrime Magazine. (2019). Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021. Cybersecurity Ventures. https://cybersecurityventures.com/jobs/

DETERLab: Application. (2021). DETERLab Application Process. DETERLab Application Process. https://deter-project.org/deterlab_application_process

DETERLab: CCTF. (2021). Cryptography CCTF Teacher Manual. CCTF Teacher Manuals (requires login). https://www.isi.deterlab.net/file.php?file=/proj/teachers/22
DETERLab: Login. (2021). DETERLab Login Page. DETERLab. https://www.isi.deterlab.net
DETERLab: New Project. (2021). New project application form. Create a new project on DETERLab. https://www.isi.deterlab.net/newproject.php
DETERLab: Register. (2021). Registering to use DETERLab. Registration at DETERLab. https://docs.deterlab.net/support/registering/
DETERLab: User Projects. (2016). DETERLab: Table of DETERLab User Projects as of December 2016. DETERLab. https://deter-project.org/table_deterlab_user_projects_december_2016
DETER Project. (2021). DETERLab: Cyber-Defense Technology Experimental Research Laboratory. DETERLab. https://deterlab.net
Docker. (2021). What is a Container? A standardized unit of software. Docker containers. https://www.docker.com/resources/what-container
Mirkovic, J., & Benzel, T. (2012). Teaching cybersecurity with DeterLab. IEEE Security & Privacy, 10(1), 73-76. https://doi.org/10.1109/MSP.2012.23
Mirkovic, J., Benzel, T., Faber, T., Braden, R., Wroclawski, J., & Schwab, S. (2010). The DETER project: Advancing the science of cyber security experimentation and test. In 2010 IEEE International Conference on Technologies for Homeland Security (HST) (pp. 1-7). Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/THS.2010.5655108
National IA Education & Training Programs. (2019). CAE-CD Knowledge Units. 2019 Knowledge Units. https://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2019_Knowledge_Units.pdf
National Initiative for Cybersecurity Education. (2020). Cybersecurity Workforce Framework (1st ed.). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-181r1
National Initiative for Cybersecurity Education. (2020). The NICE Challenge Project develops real-world cybersecurity challenges within virtualized business environments that bring students the workforce experience before the workforce. *NICE Challenge*. https://nice-challenge.com/
Perhach, P. (2018). The Mad Dash to Find a Cybersecurity Force. *New York Times*. https://www.nytimes.com/2018/11/07/business/the-mad-dash-to-find-a-cybersecurity-force.html
SEED Labs. (2020). Hands-on Labs for Security Education. SEED Labs. https://seedsecuritylabs.org/
Siraj, A., & Ghafoor, S. (2014). Integrating Security in Traditional Computer Science Courses. SecKnitKit. http://blogs.cae.tntech.edu/secknitkit/
University of San Diego. (2018). The Cyber Security Talent Shortage: What's Academia Got to Do With It? Master of Science in Cybersecurity at the University of San Diego. https://onlinedegrees.sandiego.edu/education-and-cyber-security-talent-shortage/
Winick, E. (2018). A cyber-skills shortage means students are being recruited to fight off hackers. Technology Review. https://www.technologyreview.com/2018/10/18/139708/a-cyber-skills-shortage-means-students-are-being-recruited-to-fight-off-hackers