University of Piraeus
Department of Digital Systems
Postgraduate Programme " Digital Systems Security "

Development of a cyber range platform

Vasileios Linardos

Supervisor: Dr. Konstantinos Labrinoudakis

February 2021

Acknowledgments

I would like to thank my supervisor Dr Konstantinos Labrinoudakis, my supervisors Gregory Blanc and Olivier Levillain at Telecom SudParis where all the lab tests took place, it was a great experience working with them all. Also I would like to thank my fellow partner and classmate during our master studies, Evi Dimou, for her precious help. Last but not least, a big thank you to my parents and Ioanna for their incredible support.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου Δρ Κωνσταντίνο Λαμπρινουδάκη και τους επιβλέποντες μου Gregory Blanc και Olivier Levillain στο πανεπιστήμιο Telecom SudParis όπου πραγματοποιήθηκαν όλες οι εργαστηριακές δοκιμές. Επίσης θα ήθελα να ευχαριστήσω την συνεργάτιδα και συμφοιτήτρια μου Εύη Δήμου για την πολύτιμη βοήθεια της. Τέλος θα ήθελα να πω ένα μεγάλο ευχαριστώ στους γονείς μου και την Ιωάννα για την υπέροχη συμπαράστασή τους.

Table of Contents

Περίληψη

Σήμερα, οι απειλές στον κυβερνοχώρο είναι παντού και νέες επιθέσεις συμβαίνουν καθημερινά. Είτε μιλάμε για παραβιάσεις δεδομένων, κλοπές μεμονωμένων αναγνωριστικών, διακοπές συστημάτων από επιθέσεις χάκερ ή ευπάθειες που εντοπίζονται σε κρίσιμες υποδομές, ο αυξανόμενος αριθμός είναι συγκλονιστικός. Ως εκ τούτου, η συνεχής εκπαίδευση και κατάρτιση σε νέες τεχνολογίες / λογισμικό είναι ζωτικής σημασίας τόσο για μηχανικούς ασφαλείας και προσωπικό μηχανοργάνωσης όσο και για τους οργανισμούς γενικότερα. Η τεχνολογία Cyber Range (CR) τα τελευταία χρόνια ήρθε ως εργαλείο με στόχο τη μείωση του χάσματος δεξιοτήτων μεταξύ των οργανισμών και των υποδομών τους. Για όλο και περισσότερα πανεπιστήμια, επιχειρήσεις, μη κερδοσκοπικούς οργανισμούς και κυβερνήσεις ανά τον κόσμο, η απάντηση είναι η δημιουργία, ένταξη ή επέκταση ενός Cyber Range. Η ιδέα δεν είναι καινούργια, αλλά η έκρηξη ενδιαφέροντος για τα Cyber Ranges είναι σαφής. Στην παρούσα διατριβή, θα παρουσιάσουμε μερικές από τις βασικές περιπτώσεις χρήσης των CR και θα επικεντρωθούμε στην εκπαιδευτική εφαρμογή τους και θα παραθέσουμε την εμπειρία μας στην ανάπτυξη και τον έλεγχο του CyTrONE, ενός ολοκληρωμένου συστήματος ανοικτού κώδικα για την εκπαίδευση στην ασφάλεια του κυβερνοχώρου.

"Τα Cyber Ranges είναι καλά καθορισμένα ελεγχόμενα εικονικά περιβάλλοντα που χρησιμοποιούνται στην εκπαίδευση στην κυβερνοασφάλεια ως ένας αποτελεσματικός τρόπος για τους εκπαιδευόμενους να αποκτήσουν πρακτικές γνώσεις μέσω πρακτικών δραστηριοτήτων."

Λέξεις κλειδιά

Cybersecurity, cyber range, cybersecurity training, cybersecurity education, cybersecurity practice, CyTrONE

Abstract

Nowadays cyberthreats are everywhere and new cyber-attacks occur on a daily basis. Whether counting data breaches, individual ID thefts, system outages from hacker attacks or vulnerabilities detected to critical infrastructure, the growing numbers are staggering. As such, continuous education and training upon new technologies/software are vital either for cyber-security and IT personnel and for organizations in general. Cyber Range (CR) technology in the last few years came as a key tool for reducing the skills gap between organizations and their infrastructure .For more and more universities, enterprises, nonprofit groups and governments around the globe, the answer is to build, join or expand a cyber range. The concept is not new, but the explosion in interest in Cyber Ranges is clear. In the present dissertation, we will present some of the key use-cases of CRs and we will focus on the educational application and we will state our experience deploying and testing CyTrONE, a complete open-source integrated Cybersecurity Training Framework.

"Cyber ranges are well-defined controlled virtual environments used in cybersecurity training as an efficient way for trainees to gain practical knowledge through hands-on activities."[1]

Keywords

Cybersecurity, cyber range, cybersecurity training, cybersecurity education, cybersecurity practice, CyTrONE

[1] https://www.researchgate.net/publication/311621279_CyRIS_a_cyber_range_instantiation_system_for_facilitating_security_training

Acronyms

CR - Cyber Range

CyTrONE - Cybersecurity Training and Operation Network Environment

CyRIS - Cyber Range Instantiation System

CTF - Capture The Flag

DevOps - Development Operations

IT - Information Technology

KVM - Kernel-based Virtual Machine

LMS - Learning Management System

OS - Operating System

VM - Virtual Machine

1. Introduction

Cyber security is the process of protecting networks, devices, programs and data from attack, damage, or unauthorized access. Driven by global connectivity, governments, corporations, financial and medical organizations and universities collect, process, and store unprecedented amounts of data on computers and other devices and transmit it across the internet everyday. As the volume and sophistication of cyber attacks and threat actors grow, cyber security attention is required to protect companies and organizations that are tasked with safeguarding information relating to critical infrastructure (national security, health and public services) and the enterprise.

In most companies, it's common that the bulk of cybersecurity training rests within IT and security teams. While this makes sense to most company leaders, it's important for all employees to engage in protecting an organization from outside intruders. Therefore, a lot of courses about cyber security are available not only for advanced learners but also for beginners. The cyber security training seminars for beginners, help them to recognise and react to cyber threats and to improve their skills in protecting themselves and their businesses. On the other hand, the objective of the advanced courses is to provide IT personnel with deep knowledge and sharpen their skills on security and give learners hands-on exposure to real-world incidents.

According to NIST[2], cyber ranges are interactive, simulated representations of an organization's local network, system, tools, and applications that are connected to a simulated Internet level environment. They provide a safe, legal environment to gain hands-on cyber skills and a secure environment for product development and security posture testing. A cyber range may include actual hardware and software or may be a combination of actual and virtual components. Ranges may be interoperable with other cyber range environments. The Internet level piece of the range environment includes not only simulated traffic, but also replicates network services such as webpages, browsers, and email.

1.1 Scope and Objectives

The scope of this report is to analyze cyber ranges and focus on how they can be used to provide knowledge and skills to security practitioners. It also discusses the main use-cases, as well as raises the key asset of cyber ranges in education.

In particular, the objective of the thesis is to present how cyber ranges can be a useful tool for security practitioners, but also to present the CyTrONE as a complete cybersecurity training framework.

[2] The Cyber Range: A Guide - Guidance Document for the Use Cases, Features, and Types of Cyber Ranges in Cybersecurity Education, Certification and Training - Prepared by the NationalInitiative for Cybersecurity Education (NICE) Cyber Range Project Team

1.2 Outline

The structure of the report is as follows:

- Chapter 2 provides an overview of cyber ranges, beginning from their definition and insights into the how of cyber range technology.
- Chapter 3 focuses on the necessity of cyber ranges for education and training purposes and it explains why it's a key asset in the training of cybersecurity.
- Chapter 4 presents the CyTrONE implementation and testing in detail and ends with conclusions and future work.
- Chapter 5 provides a summarization of key findings.
- Annex provides the code that is used for the implementation of the thesis.

2. Cyber Ranges: Design and Use-cases

Cyber ranges are virtual environments that use actual network equipment, as required. They can range from single stand-alone ranges in a single schoolhouse or an organization to internet replicating ranges that are accessible from around the world. Cyber ranges may be used internally by private and public organizations, or by students in the classroom or online from training and education providers. Cyber ranges are in use and provided by organizations across the Government, Private Industry, and Academia.

2.1 Types of cyber ranges

Cyber ranges have developed into a variety of types with each type holding a different set of features and capabilities. In general, we are going to apoose four main types of cyber ranges which are described below:

1. **Simulation Ranges**: The objective of simulation ranges is the recreation of a network environment based on the behavior of real network components. Simulations run in virtual instances and do not require any physical network gear. In a typical simulation environment, VMs replicate specific server, network, and storage of a particular IT infrastructure. These VM templates are standardized and thus, somewhat limited in how closely they simulate real IT infrastructure. Though quick to spin-up, the closer the cyber range matches the target exercise infrastructure, the higher the fidelity of the exercise. So, the granularity with which the simulation can match the target environment is directly proportional to the successful simulation outcome. For this reason, cyber ranges should require a strong orchestration layer. The upside of a simulation environment is the speed of reconfiguration and the ability to use generic server and storage equipment. The primary downside of a simulated network is unpredictable and unrealistic latency and jitter of network performance.

2. **Overlay Range**: Overlay ranges are cyber ranges running on top of real networks, servers and storage. Overlay cyber ranges have a significant fidelity advantage over simulation ranges, but they come at a considerable cost of hardware and the cost of potential compromise of the underlying network infrastructure. Typically, overlay networks are set up as global testbeds, one of the largest being the Global Environment for Network Innovations (GENI), sponsored by the National Science Foundation.

3. **Emulation Ranges**: Emulation is running the cyber range on dedicated network infrastructure, mapping as-built network/server/storage infrastructure onto physical infrastructure: a physical infrastructure that becomes the cyber range. An emulation provides closed-network experiences with multiple interconnected environments. Emulation includes traffic generation that emulates

numerous protocols, source patterns, traffic flows, attacks, and underlying internet connectivity. When done right, emulation creates true-to-life experiences, rather than pre-programmed actions and response. A key differentiator for accurate emulation has URLs that resolve to the cyber range's DNS and virtualized Internet IP addresses using real-world geo-IP addresses. The National Cyber Range (NCR)[3] is probably the most significant emulation initiative.

4. **Hybrid Ranges**: As the name suggests, hybrid ranges emerge from a customized combination of any of the above types. The Virginia Cyber Range[4] is an example of range that utilizes multiple features above. Another hybrid range is the European Future Internet Research & Experimentation[5], started in 2008.

2.2 Cyber ranges classification

Being virtual environments, they are not only restricted to an organization's local network but also range from single standalone ranges in an organization to internet replicating ranges which could be accessed from around the world such that they can be used by private as well as public organizations along with students, researchers, trainers, and education providers. Based on their purpose of utilization, cyber ranges may be classified as follows:

2.2.1 Education

The idea of 'Cyber Range for education' came up in 2015. The idea was to provide training on cyber-attack, defense, and detection, for developing certifications, to collaborate with industries, carry out research, and to offer training for military and veterans. The Virginia Cyber Range offers cyber range for Education. Certain Cloud based cyber ranges boost the number of trained cyber professionals. The Michigan Cyber Range[6] encourages teaching, testing and training. Apart from being digital playgrounds, these cyber ranges offer a repository of course materials that the educators and students can benefit from. These ranges offer defensive trainings primarily such that students can imitate to be network administrators and study simulated attacks.

2.2.2 Military, Defense and Intelligence

Military organizations and government agencies require cyber warriors with befitting skills to counter cyber terrorism. Weaknesses and vulnerabilities are critical to the nation's infrastructure. Hence the Military and Defense implement large scale cyber ranges like Defense Advanced Research Projects

[3] https://ieeexplore.ieee.org/document/6956748
[4] https://www.virginiacyberrange.org/
[5] https://www.sciencedirect.com/science/article/abs/pii/S1389128613004362
[6] https://en.wikipedia.org/wiki/Michigan_Cyber_Range

Agency (DARPA)'s National Cyber Range (NCR). DARPA's primary aim is to replicate large networks for the Department of Defense (DOD) weapon systems and operations. A realistic testing facility is provided for research. Apart from enabling the development and deployment of state-of-art cyber testing capabilities, it could also facilitate scientific use of cyber testing methods. DARPA also sees to it that a virtual environment is provided for qualitative, quantitative and realistic assessment of cyber technologies for research and development. U.S. Army Communications-Electronics Command, or CECOM,has proposed a cyber range that is capable of developing configurations for supporting multiple environments through the cyber range. It has also been observed to incorporate features like Cyber Threat characterization and dynamic threat capability.

2.2.3 Enterprise and Commercial

A cyber defense center is effective if people can operate it and defend enterprises. Enterprises and commercial organizations deploy cyber ranges to conduct games and simulations in order to strengthen cyber security capabilities. These commercial organizations need a superior way to develop ranges so that they are at par with the rapid growing applications, threats and traffic volumes. They provide cyber range solutions to create an operationally relevant environment that mirrors Global Information Grid[7] (GIG) and enables sophisticated simulations and manages a distributed network of cyber ranges. The Pinecone Cyber range is one such Commercial Cyber range. The IBM X Force Command Centre[8] is the first ever commercial cyber simulator and uses live malware to test security.

2.2.4 Service Providers

Either through cloud or through in-house infrastructure the market share of Cyber Range technologies are ever-growing. There are services that offer online cyber ranges, so a business can get started with them as quickly as possible without installing their own in-house server equipment. These companies operate what is known as "cyber ranges as a service".

2.2.5 Open Source

Security professionals need practical real-world experience. However, performing dangerous activities on production, personal or work networks may lead to serious consequences. There are some approaches to open-source solutions around Cyber Range technologies with CyTrONE being, at the time writing this report, the only complete framework. Another approach based on open source technologies, had been presented at BSides London 2019[9] [10]

[7] https://en.wikipedia.org/wiki/Global_Information_Grid
[8] https://www.ibm.com/security/services/managed-security-services/security-operations-centers
[9] https://github.com/secdevops-cuse/CyberRange
[10] https://www.youtube.com/watch?v=Ed1ujM3xWNg

2.2.6 Law Enforcement

According to Computer Security Institute (CSI)'s survey[11], thirty four percent of respondents reported intrusions to law enforcement. Applications in military and law enforcement are being developed and tested in cyber ranges. This determines their feasibility and effectiveness in practice. The Michigan Cyber Range is one such cyber range. A cyber range environment makes use of a lot of computing devices and every device used increases the vulnerability of a cybercrime. Law enforcement can respond to the resulting cybercrimes. They also ensure technical help with forensics and investigation along with training, victim services and community education.

2.2.7 Others

Apart from being useful for the domains discussed above, cyber ranges may also offer miscellaneous assistance to Incident Handlers and for Continuity of Operations (e.g. using Cyber Ranges as sandbox environments). As common attack techniques could be analyzed, one can respond to attacks when they occur. Malicious applications and network activity could be monitored. Network vulnerabilities and root causes of incidents become easy to identify as the configuration of cyber ranges can lead to incident response. IBM X-Force Command Centre is one such cyber range. Security incidents can lead to disruption of continuity of operations. Often cyber ranges provide redundant and resilient systems for supplying functions in such scenarios.

[11] http://www.sis.pitt.edu/jjoshi/courses/IS2150/Fall10/CSIsurvey2008.pdf

3. Using Cyber Ranges for Cybersecurity Education

In the current digital world that we live in and as more and more parts of our lives have an "interconnected" part, continuous education is a non going back reality. From the primary school and the family environment, children and pre-school children have their first interaction with the digital world, either through a device (laptop, tablet etc) or through the mainstream media (TV, satellite etc). Nowadays, high school students are increasingly diving into programming and internet technologies. A big part of their education is being more and more based upon the internet and the digital world.

3.1 Cybersecurity in the education system

Taking into account all the above, schools, universities and all the educational institutions need to set cybersecurity training and awareness programs as a high priority. Despite the sector facing major challenges such as a lack of staffing and a lack of funding and resources, cyberattacks are no less frequent or less severe in education. In fact, they seem to be gaining ground in prevalence year-on-year as instances of breaches in schools and higher education are widely reported.The more worrying breaches are where student safety is compromised. Educational institutions are entrusted to safeguard their students, many of whom are minors, but a weak cybersecurity infrastructure can put them at risk. It's an unfortunate fact that, while cybersecurity in Education is necessary to protect against financial loss and prevent disruption, it's also crucial to protect students from harm and also to fortify them as future employees, parents, individuals.

With Education venues varying in size, purpose, and stature, the motives for attack can vary too. For example, what might be a common threat for world-renowned Universities/Colleges might not be an issue for schools or school districts. So, institutions need to evaluate the risk and understand what data is vulnerable to unauthorised access. Distributed Denial of Service, or DDoS attacks are a common type of attack on all levels of Education venues. This is where the attacker's motive is to cause widespread disruption to the institute's network, having a negative effect on productivity. This can be a relatively easy attack for amateur cybercriminals to carry out, especially if the target network is poorly protected. There have been instances of students or teachers successfully carrying out a DDoS attack, with motives ranging from simply wanting a day off, to protesting the way a complaint was handled.

Data theft is another attack affecting all levels of education because all institutions hold student and staff data, including sensitive details like names and addresses. This type of information can be valuable to cybercriminals for several reasons, whether they plan to sell the information to a third party or use it as a bargaining tool and extort money. Another motive for hackers carrying out an attack on an education institution is for financial gain. This might not be as high a risk for public schools, but with private institutions and Universities/Colleges handling a large number of student fees, they're a prime target for cybercriminals. Today, it's usual for students or parents to pay fees via an online portal, often transferring

large sums of money to cover a whole term or year of tuition. Without proper protection or preparation on the part of education institutions, this presents a weak spot for cybercriminals to intercept.

The fourth reason why education is a target for cybercrime is espionage. In the case of higher education institutes like Universities/Colleges, they're often centres for research and hold valuable intellectual property.Universities/Colleges need to be suitably protected, as it's thought that scientific, engineering and medical research by UK Universities has been previously compromised by hackers, and with plenty of time and money to fund them professionals are often at the helm of these attacks. With these four motives in mind, the way in which hackers carry out an attack on Education networks can further help us understand how to protect them and create appropriate content for the Cybersecurity educational programs.

According to a 2018 survey conducted by JISC[12] IT professionals from higher education were asked to name the top cyber threats facing their institutions, and the top three answers give us insight into the most common ways Education networks are breached. Phishing campaigns often take the form of an email or instant message and are designed to trick the user into trusting the source in a fraudulent attempt to access their credentials – whether that's sensitive student data or confidential research. This type of attack is highlighted as the top threat facing higher education venues, suggesting hackers regularly target the sector using the method. Also in the top three cyber threats highlighted by the report, ransomware and malware attacks prevent users from accessing the network or files and cause disruption. More advanced forms of this threat can see attackers hold files to ransom. Ransomware or malware typically infects devices using a trojan, a file or attachment disguised to look legitimate. However, some ransomware (like the WannaCry attack) have been shown to travel between devices without user interaction. The third threat listed by professionals in both further and higher education is a lack of awareness or accidents. This could be on the part of staff or students who aren't sufficiently trained to practice good cyber hygiene or accidentally compromise the network. Despite taking on different appearances, human error plays a key part in each of these three Education sector cybersecurity threats. However, with better overall cybersecurity training, and awareness on the motives and method of attackers, education venues could better protect themselves against cyberattacks. However, the sector is also facing challenges which hinder progress.

Finally, another main pillar of cybersecurity education comes along with the rising trend of cyber bullying. As cyber bullying is ever-expanding through various social (and not only) media platforms, educational institutions have another grief to cope.

3.2 Using cyber ranges for educational purposes

Using the below somehow abstract figure, we will try to explain a standardized lifecycle of cyber security training using Cyber Range technologies. When we are talking about trainees we do not only mean IT

[12] Cyber Security Posture Survey 2018Research Findings
https://community.jisc.ac.uk/system/files/288/Cybersecurity_Posture_Survey_2018_Research_Findings_0.pdf

and security personnel but also high school and college/university students. Even primary school children can interact with specialized training through interactive games and LMS platforms.

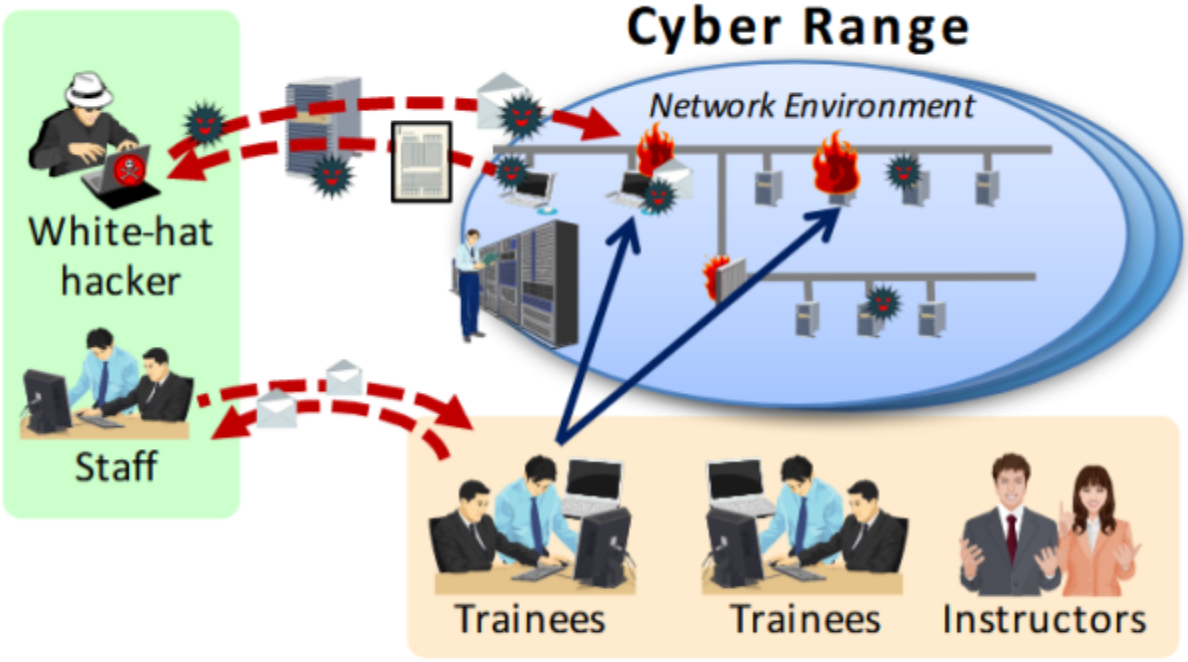


Figure: Cyber Range explanation

In accordance with the academic environment in which the technical part of the present report took place, we will specify a cyber training procedure upon these environments. Starting from a lab environment where we can have our cyber range setup, we can design multiple, tiered and differentially in terms of context cyber security educational programs. Example given, we can imagine a trainee given access to a specific instance from our cyber range. In this specific scenario, the trainee may have to do some certain tasks to find a clue to move forward to the next machine or to solve a riddle or just to answer a question given through an LMS framework. The scenarios that we can design are endless. We can emulate vulnerabilities and specific services, emulate forensics and hardening scenarios and so forth in a mimic of a Capture The Flag game. White-hat hackers can play their part in red and blue teaming scenarios. Supposing that trainees are the administrators of the cyber range and white-hat hackers (also trainees or maybe experts), we can emulate a real life scenario. It's up to the instructors and their experience,capabilities and imagination to design and deploy numerous scenarios. Finally, it's worth mentioning at this point, that the deployment procedure of a new cyber range and the design and testing of new scenarios also pertain to the learning curve that we want to maximize from a DevOps and development perspective respectively.

Having all the above in our minds, the outcome of these training playgrounds should only be one: trainees must learn and gain experience every time they interact with each scenario.

4. CyTrONE

“Cyber ranges as cyber security training platforms. CyTrONE, an open source approach.”

4.1 CyTrONE Overview

CyTrONE (Cybersecurity Training and Operation Network Environment), is a cybersecurity training framework that aims to facilitate training activities by providing an open-source framework that automates the training content generation and environment setup tasks. The advantages of this approach are threefold: (i) improve the accuracy of the training setup; (ii) decrease the setup time and cost; (iii) make training possible repeatedly, for many participants.When using CyTrONE, an instructor provides input regarding the training by selecting the desired scenario, and the framework will retrieve the appropriate content from a training database

CyTrONE has been designed specifically to meet a set of requirements that any effective training program/solution should meet. We can summarize the requirements in a few key points:

- Training content should be easy to meet each target audience’s knowledge and level of expertise
- Training content aims to develop and sharp hands-on skills of the trainees
- Scenarios and content should be as close to real-life incidents and events
- A complete training program should have good cost/performance characteristics so to be easy to scale and maintain on long term

CyTrONE uses a distributed architecture to upload the training content to a Learning Management System (LMS) and to setup the corresponding training environment. For this purpose, CyTrONE makes use of two software packages that are also being developed by CROND at JAIST. Thus, the tool called CyLMS is used for training content to LMS format conversion. Correspondingly, the Cyber Range Instantiation System (CyRIS) is used for training environment setup and the creation of the instances needed.

In addition to the above modules, CyTrONE now includes built-in support for the new module CyPROM that performs progression management for dynamic training scenarios, which is out of the scope of the present report.

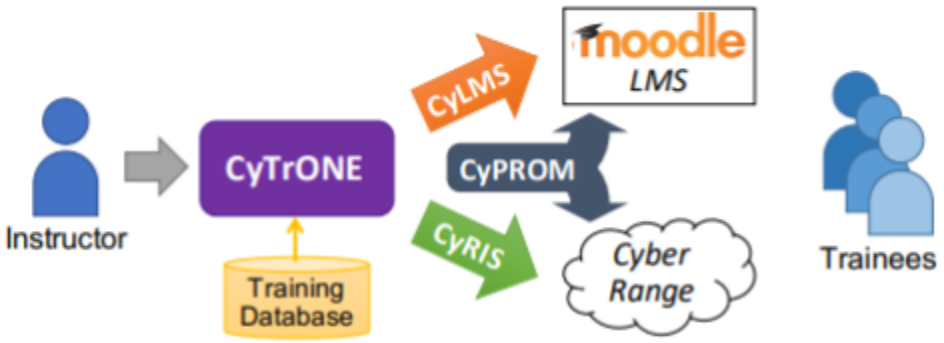
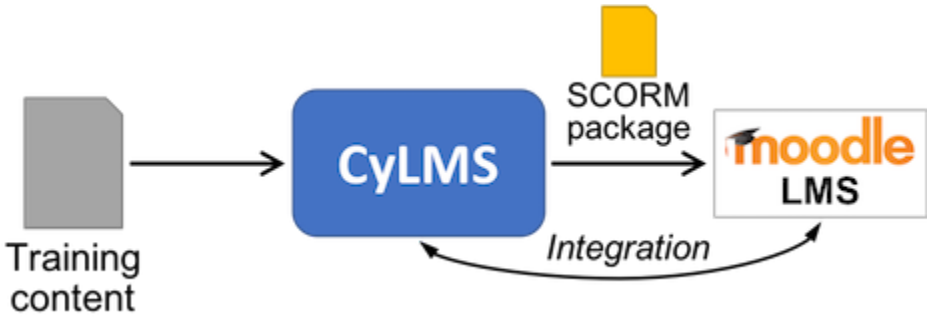


Figure: CyTrONE architecture overview

CyLMS

CyLMS is intended for managing training content in connection with cybersecurity education and training activities conducted via LMSs. Hitherto, it has been tested (and is recommended) only with Moodle LMS.

In the first place,the input file containing the training content representation is converted to a SCORM package. The text-based representation of the training content allows educators to focus on the actual content itself.The conversion to SCORM format makes it possible to import the training content into most LMS software, either manually or automatically. In a second stage, the additional integration functionality with the LMS provided by CyLMS—in particular regarding automated content management and access to the training environment—ensures an improved user experience.



CyLMS uses a hybrid approach for content management. Thus, the input of CyLMS is an original text-based format using the YAML syntax, an easy to manage file format that is also extensible by nature. Then, a converter tool that JAIST implemented produces an equivalent SCORM package by using a

package template to control the presentation style of the training content. In this manner the module is able to combine the flexibility of the input YAML representation with the versatility of the SCORM format to facilitate training content representation. Text-based YAML format has been selected for representing training content in CyLMS because of the following advantages it has:

- Easy to view and modify via any text editor
- Both human and machine readable
- Flexible representation form, allowing inclusion of HTML code (e.g., for changing style or adding figures)
- Straightforward versioning and difference checking
- Small size, easy to archive and transfer in order to share the training content

In the code bloc below we can see an example of a training content representation file for CyLMS. The file includes the following:

- A training activity with the id “Example” for which a title, an overview, and two questions are provided.
- The first question, with the internal id “EX-1”, is a typical question for which the learner needs to fill in the answer; three hints are provided for this question, ranging from somewhat vague to very specific.
- The second question, with the internal id “EX-2”, is a multiple-choice question for which the trainee needs to select the correct answer from the four specified alternatives; this question as well includes three hints.

```
---
- training:
  - id: EXAMPLE
        title: Example questions
        overview:
        These are two example questions that demonstrate how to define training content for CyLMS.
        Please check how the questions are displayed after they are converted to a SCORM package
and uploaded to Moodle.
        questions:
        - id: EXAMPLE-01
        body: What is the name of the Linux distribution used by this server? Indicate only the name,
without version or architecture, e.g., CentOS.
        answer: Ubuntu
        hints:
        - The directory <code>/etc/</code> contains various files with information regarding a Linux
distribution.
```

```
    - One of the most relevant files has a name ending in "release".
    - <code>$ cat /etc/*-release</code>
    - id: EXAMPLE-02
    body: What is the name of the account you are logged in as?
    choices: root, admin, guest01, trainee01
    answer: trainee01
    hints:
    - The account name is typically the same with the name of the user's home directory.
    - "Have you ever asked yourself: Who am I?"
    - <code>$ whoami</code>
```

Although it is possible to import SCORM packages—such as the ones generated by the system—manually into an LMS via its web interface, to facilitate content management CyLMS enabled the import/removal of SCORM packages without any user intervention. While this CyLMS functionality is currently limited to the Moodle LMS, the development team believe that it could be extended to other LMS software if needed. CyLMS uses *moosh (https://moosh-online.com/).* Moosh stands for “Moodle Shell” and makes it possible to perform many Moodle management tasks via the command line. For instance, CyLMS uses the moosh command *course-list* to determine the course id for a given course title, and the command *activity-add* in order to add a SCORM package as a Moodle activity.

```
cytrone@ubuntu:~/Downloads/cylms-1.0$ ./cylms.py -h
################################################################################
CyLMS v1.0: Cybersecurity Training Support for LMS
################################################################################

OVERVIEW: CyLMS set of tools for cybersecurity training support in Learning Manageme
nt Systems (LMS).

USAGE: cylms.py [options]

OPTIONS:
-h, --help                      Display this help message and exit
-c, --convert-content <FILE>    Convert training content file to SCORM package
-f, --config-file <CONFIG>      Set configuration file for LMS integration tasks
                                NOTE: Required for all the operations below
-a, --add-to-lms <SESSION_NO>   Add converted package to LMS using session number
                                NOTE: Usable only together with 'convert-content'
-r, --remove-from-lms <NO,ID>   Remove session with given number and activity id
```

CyLMS help page

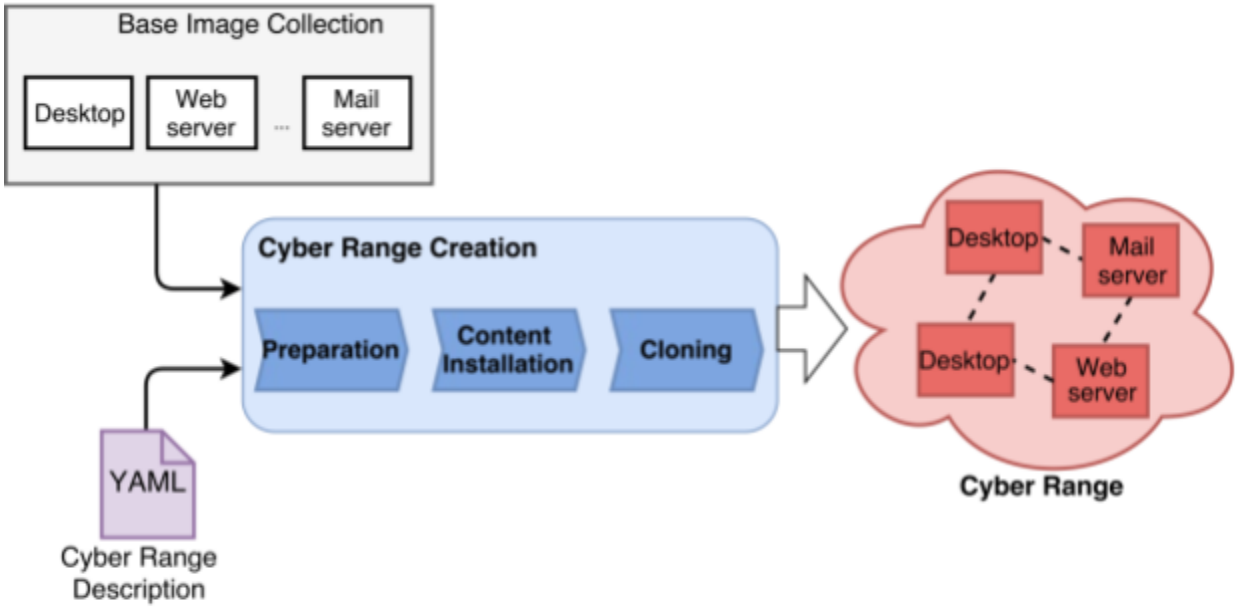
FInally in the above screenshot we can see the CyLMS’s help page with the available options.

CyRIS

CyRIS is the core component of the integrated cybersecurity training framework CyTrONE that is also being developed by CROND (JAIST).The workflow of CyRIS is described in Figure below. The two main inputs that the system takes to create the desired cyber range are:

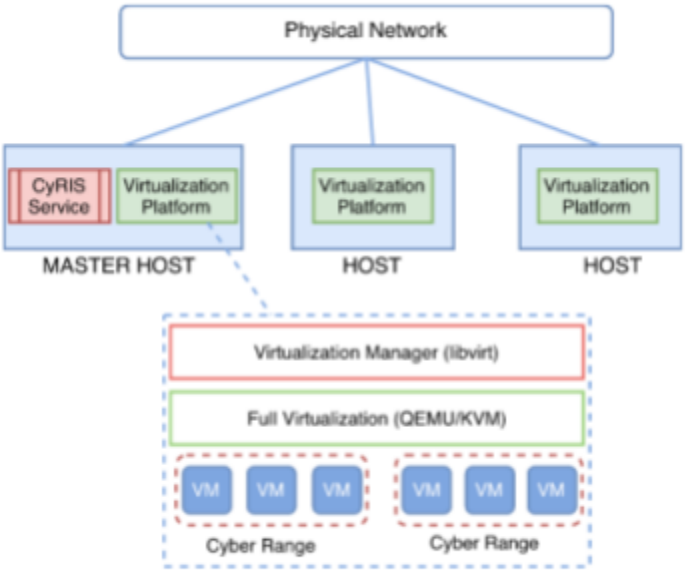
- A cyber range description file
- A set of virtual machine base images

The cyber range description file is for instructors/admins to describe the composition and content of the cyber range. It can be created manually or generated from a template. This Description is written in YAML, a text-based file format, and defines all the necessary information for creating a given cyber range.The base images are used via the KVM virtualization system, and they contain a pre-installed operating system and several basic system configurations (e.g., IP address, etc.).



CyRIS architecture workflow

The execution infrastructure is represented by a collection of hosts, each of them equipped with a virtualization platform (currently working on QEMU/KVM), which are connected to a LAN network. One of the CyRIS hosts is designated as a master host, and manages the entire execution, performing tasks such as processing the input description file, preparing the base images and installing security content into them, and cloning the virtual machines to other hosts.



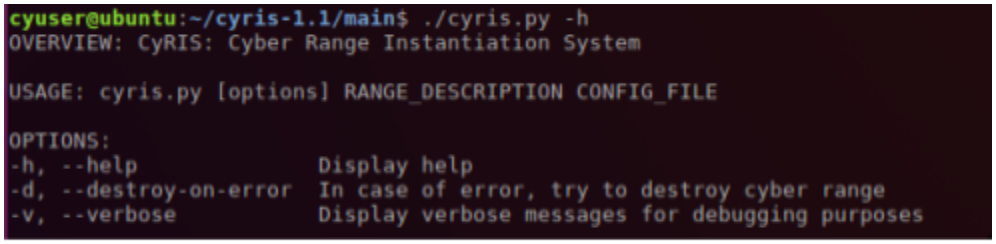
Cyber Range deployment using CyRIS with KVM virtualization

In order to create security-related content in the cyber range, CyRIS offers a wide range of functions. These functions are divided into two categories, as basic functions and security functions. The first group includes functions that are commonly found in other well-known automated environment configuration tools (Ansible, Chef, etc.), such as installing packages, copying data, configuring network services, add/manage accounts and users, execute scripts/commands and so forth. The security functions is the novelty and the big difference in CyRIS compared to other tools. These functions include the capability for reproducing actual security-related incidents, such as emulate attacks, traffic capturing, emulate malware, modify firewall ruleset and so on, in order to generate corresponding content

In the code block below you can see a sample script which can be used unde the instantiation process in order to emulate a ddos attack. The instances in which the attack will take place is defined under the main instantiation configuration yaml file.

```
#!/bin/bash
attack_addr=$1
bash -c "exec -a ddos_attack hping3 -c 10000 -d 120 -S -w 64 -p 80 --flood --rand-source
${attack_addr} &";
sleep 2;
pkill -f ddos_attack;
```

Finally, in the the screenshot below we can see the help page of CyRIS module with the available running options.



CyRIS help page

4.2 Implementation and Testing

4.2.1 Introduction

The main objectives of the current technical part of the report is to provide our results and findings of the tests and the research that had been conducted in the CyTrONE Integrated Cybersecurity Training Framework and mostly focused on the Cyber Range Instantiation System (CyRIS).

This is the first version (v1.0) of the report. We will enrich the current report with more findings, results, benchmarks and proposals as we deep dive into the details of the CyTrONE framework, always in consultation with the development team.

4.2.2 Summary

By using CyTrONE, with automatic environment setup and content generation based on YAML descriptions, it becomes possible for practically anyone to conduct security training anytime and anywhere (given that host servers are available for the cyberrange creation), thus leading to the democratization of cybersecurity training. The flexibility of the framework, in association with the use of a Learning Management System, means that not only classical CTFs, but any other kind of training can be conducted, for instance by leveraging the advances of modern education methodologies, such as adaptive learning, etc. The framework currently uses a classical training paradigm of scenario-based and topic-based questions that are prepared in advance.

We managed under a short period of time to deploy the whole framework in a lab environment, without a basic DevOps background. The learning curve for us as Security Engineer was impressive not only in the architecture and the infrastructure part but also in the educational aspect of the Cyber Ranges. CyTrONE was our base tool but the research went far from this. New topics in the way that cyber security trainings and educational programs should be conducted revealed to us. After all, we must ensure that cyber security education is for all. Spreading and producing knowledge in every way we can must be our first priority.

4.2.3 Details

Our findings and proposals came up after our testing creating cyber ranges using various configurations (see in the appendices some of our yaml configuration files). We focused our examples creating a network scenario based on most common real life networks, a star network with 3 hosts (desktop-user, file server, dns mail server) with all the traffic being routed through a CentOS host which acts as a firewall/router. During the examples, we have also tested the “security features” of CyRIS software, by emulating attacks, capturing traffic and emulating malware effects.

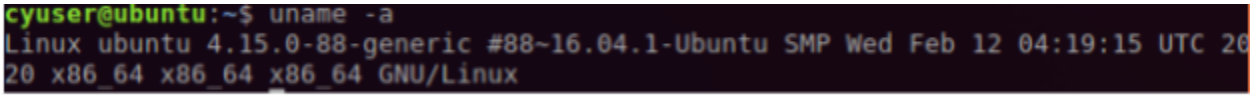
We manage to solve most of the problems that we encounter (most of them occurred from misconfigurations or outdated operating systems). We also mention some findings that we didn’t manage to solve or that we couldn’t find/describe the origin of the problem.

Finally, we have created a table which contains the creation time of some cyber range tests. That helps us to test the stability of the software and how it operates in our testing server.

Important notice here is that all the report and all the testing is from the administrative perspective and we assume that all that findings may help everyone that wants to deploy the whole software.

4.2.4 Server host specifications

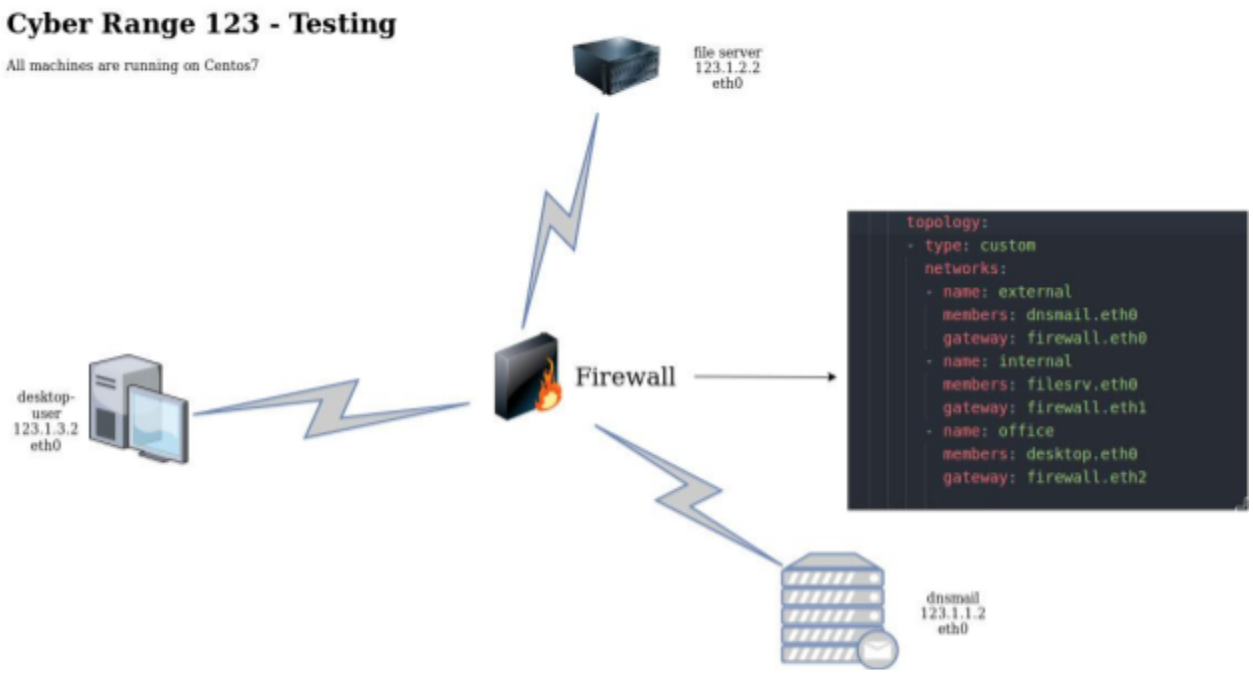
In the screenshot below you can see the system information of our host server. Our machine in which we run all our tests is equipped with 8 cores (version: Intel(R) Xeon(R) CPU E5-2665 0 @ 2.40GHz) and 16Gb of RAM.



Server host specifications

4.2.5 Cyber range network topology

The following figure shows our cyber range network topology, which we use for all our complete tests. All the machines share the same CentOS image.



Cyber Range network topology

In our scenario, all the traffic of the 3 machines should be routed through the firewall machine. Although in the cyber range's logs (screenshots 2,3) we can see the forwarding rule to allow routing through firewall, when we ssh into our entry point (desktop-user) we were unable to reach (either through ICMP or TCP packets) the other hosts (screenshot 4).

```
firewall_rule:
  rule0: sysctl -w net.ipv4.ip_forward=1; sysctl -p
```

Forwarding rule inside the yaml configuration (2)

setup_fwrule.sh

```
ssh -o UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no root@123.1.1.3 "sysctl -w net.ipv4.ip_forward=1;
```

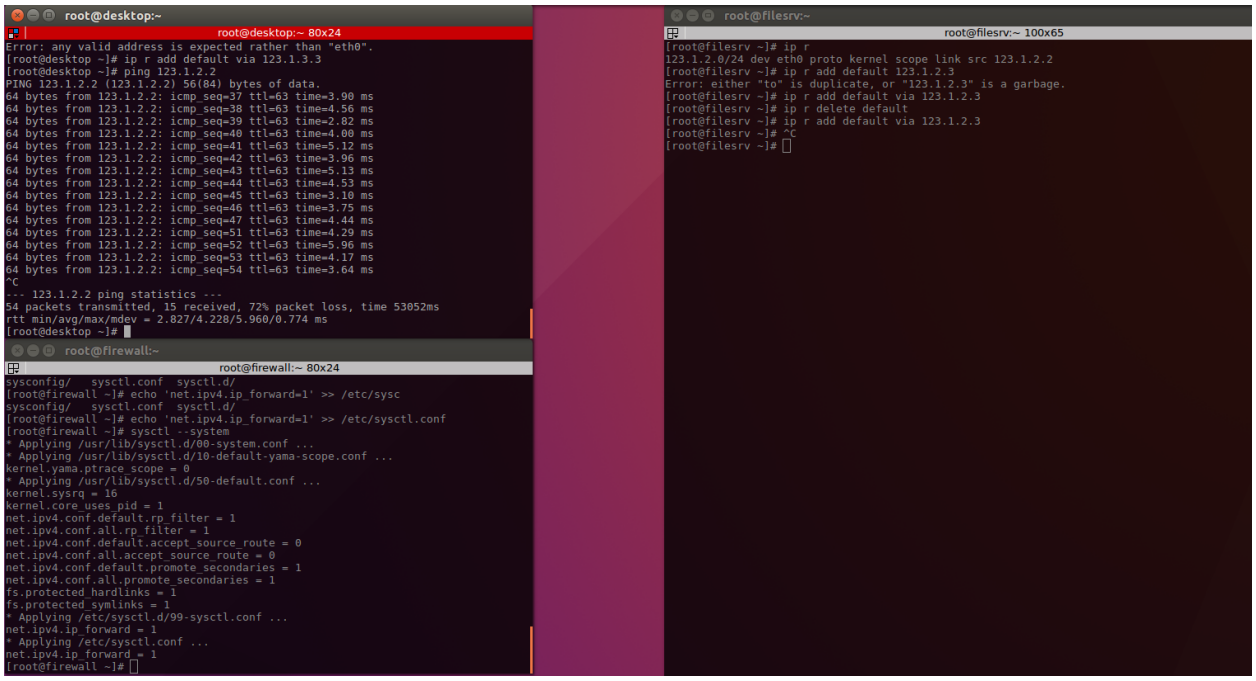
The sysctl command that enables ip forwarding rule in the machine (3)

```
[daniel@desktop ~]$ ping 123.1.2.2
PING 123.1.2.2 (123.1.2.2) 56(84) bytes of data.
^C
--- 123.1.2.2 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2001ms
```

Host unreachable (4)

After investigating the issue, we saw that the *ip_forward (ing)* in the firewall machine was set to 0. We destroy the range and recreate it using the same yaml configuration and again the same misconfiguration occured. In the screenshot below, we can see the fixing of this finding. One persistent solution, without having to manually fix it every time that we create a new cyber range, is to make use of the *execute_program* task that CyRIS supports. We can write a simple shell/bash script so that every time that we create a new range to change the *ip_forward* value.

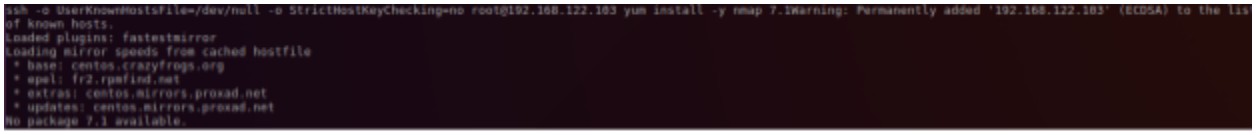
As a general rule, the *execute_program* feature is more than helpful as it helps us automate and execute commands during the instantiation phase. Nevertheless, we shall mention that we don't know why this misconfiguration comes up as even in the verbose mode we see the logs without any error messages.



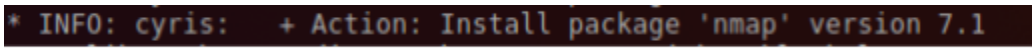
Screenshot 5

4.2.6 Specify software version

Following up, we faced a problem when we tried to specify the version inside the install_package task. By specifying the version of the package that we want to install, in this particular example the package we wanted to install is nmap, we saw the following messages in the verbose mode and also in the creation log (screenshots 6,7).



We can see from the logs that CyRIS's searching for the wrong version of the software. (6)



(7)

CyRIS tried to install nmap version 7.1 despite the fact that in the configuration file we had specified the version 7.10 (see appendix). Somehow the last number in the version was being stripped, leading to an error message as there is no valid 7.1 version in the nmap tool. We tried to code review by finding where the code handles the version parameter without any success as we couldn't find something that prima facie could strip or mis-handle the parameter.

4.2.7 Range notification txt

Every time we create a new cyber range, CyRIS at the end of a successful creation, produces a *range_notification.txt* (screenshot 8) file in which we can find all the information (ssh login credentials) needed by a trainee to access the CR's entry point. It's worth mentioning that we can automatically import this notification txt to the Moodle LMS where the trainee has the first interaction with the whole

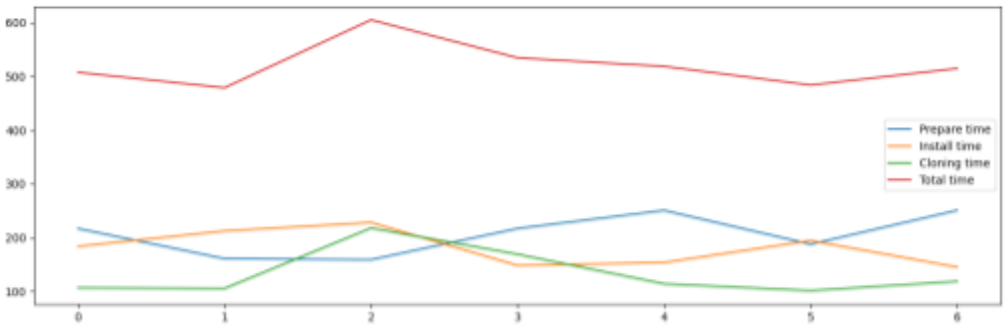
training.

```
cyuser@ubuntu:~/cyris-1.1/cyber_range/123$ cat range_notification-cr123.txt
Dear user,

Thank you very much for using our cybersecurity training framework.
We would like to inform you that Training Session #123 is ready to
use. Please find below detailed information about how to access the
created cyber range instances:

- Total number of cyber range instances: 1

- Cyber range instance #1:
  Login: ssh trainee01@127.0.0.1 -p 62941
  Password: 1b2k8pyfua

We hope you will gain valuable knowledge about cybersecurity through
this training. Feel free to contact us if you want to share with us
what you think about our training framework.

Best of luck,
The Administration Team
```

Screenshot 8

4.2.8 Cyber range creation time

Finally in the following chart we randomly choose the durations of seven different times that we create a cyber range with the same yaml configuration. As we can see the variation is subtle and the software performs with remarkable stability in terms of the creation and the cloning process.

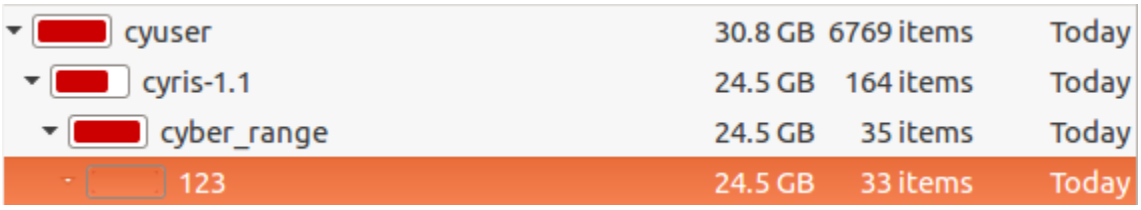


Cyber Range creation time

$T_{total} = T_{preparation} + T_{installation} + T_{cloning}$

Comments for the disk usage

CyRIS uses QEMU-KVM as the backend hypervisor technology in order to deploy and manage the instances. In our scenario, we have deployed 4 machines: desktop, firewall, file server and dns mail. All of them are copies of our base CentOS image and as you can see in the following image, the testing range named '123' needs a total number of 24,5GB of disk space. Now, if we want to clone this particular range for lets say 10 different trainees, the number of disk space will remain (almost) the same as the new ranges are being built from snapshots of this particular first range.



4.3 Recommendations

After all our experience with the implementation and through our everyday usage of the CyTrONE framework, we came to the conclusion that expressing our recommendations would be helpful both for us, to put our experience on paper, and also for the development team with whom we worked closely.

In terms of the documentation, a change to the structure may be useful from the administrative perspective. Specifically, we consider that the documentation is quite large (although detailed) and may be difficult for a single engineer to deploy the whole project at once. The aforementioned admission is also part of the paper that CyTrONE firsts presented: "Relatively advanced technical skills are required to install manually CyTrONE and the related tools of the framework..". As a proposal here, we consider that a step-by-step installation guide following the correct order in which each module should be deployed, would be more than welcome from everyone that would like to explore the framework.

Another proposal that should be included in the future work is the OS compatibility for all the modules of CyTrONE. At the time that this report is being written, CyRIS runs on Ubuntu 16.4 and CyLMS on Ubuntu 18.04. Although we are exponents of the distributed architectural approach of the framework, it may be a barrier for some. With our eyes and vision towards a platform agnostic CyTrONE which will run under all OS.

Considering the open source nature of CyTrONE, all the above are also addressed to the open source community and to all those who are interested in Cyber Ranges as cybersecurity training platforms.

5. Conclusions

Realistic cybersecurity training using cyber ranges is currently mainly conducted in military environments, in critical infrastructure and from private companies when the want to test specific networks and assets. The proprietary systems that are available publicly (from private companies as a product) are expensive. To the best of our knowledge CyTrONE is the first open-source cybersecurity training framework that is fully configurable and flexible.

We have presented our findings and we came up with our recommendations concerning the integrated cybersecurity training framework named CyTrONE and mostly focused on the instantiation part of the software, CyRIS. We have also evaluated the framework performance regarding cyber ranges instantiation, and we have demonstrated that it meets reasonable targettimes for cyber range creation Through this report, we aim to contribute to the improvement of the software, having in mind that many features, bugs and improvements are under construction as the framework is under heavy development. We also choose to research the specific software as we want to contribute and support such large scale open source projects. As more training content is added to the framework, we shall also conduct tests and surveys regarding the training quality improvement ensuing from the use of CyTrONE, which is another measure of train-ing effectiveness.

Our future work includes more testings for the security features of the CyRIS as we would like to create some CTFs for undergraduate students in order to conduct trials for the overall framework.We will also be in open discussion with the JAIST development team with more testing outcomes in direction to improve the performance of the current system.

6. Appendices

```
---
- host_settings:
  - id: host_1
          mgmt_addr: 127.0.0.1
          virbr_addr: 192.168.122.1
          account: cyuser

- guest_settings:
  - id: firewall
          basevm_host: host_1
          basevm_config_file: /home/cyuser/images/basevm_x.xml
          basevm_type: kvm
          tasks:
          - add_account:
          - account: robot.abc
          passwd: abcrb1357
          - modify_account:
          - account: root
          new_passwd: abcd.1234
          - install_package:
          - package_manager: yum
          name: net-tools
  - id: dnsmail
          basevm_host: host_1
          basevm_config_file: /home/cyuser/images/basevm_x.xml
          basevm_type: kvm
          tasks:
          - add_account:
          - account: robot.abc
          passwd: abcrb1357
          - modify_account:
          - account: root
          new_passwd: abcd.1234
          - install_package:
          - package_manager: yum
          name: wget
```

```
        - package_manager: yum
          name: net-tools
  - id: filesrv
          basevm_host: host_1
          basevm_config_file: /home/cyuser/images/basevm_x.xml
          basevm_type: kvm
          tasks:
          - add_account:
          - account: robot.abc
          passwd: abcrb1357
          - modify_account:
          - account: root
          new_passwd: abcd.1234
          - install_package:
          - package_manager: yum
          name: samba samba-client samba-common
          - package_manager: yum
          name: wget
  - id: desktop
          basevm_host: host_1
          basevm_config_file: /home/cyuser/images/basevm_x.xml
          basevm_type: kvm
          tasks:
          - add_account:
          - account: daniel
          passwd: blake
          - install_package:
          - package_manager: yum
          name: net-tools
          - package_manager: yum
          name: nmap
          version: 7.10

- clone_settings:
  - range_id: 123
          hosts:
          - host_id: host_1
          instance_number: 1
          guests:
          - guest_id: firewall
          number: 1
```

```
forwarding_rules:
- rule: src=office,external dst=internal.dbsrv dport=3306
- rule: src=office,external dst=internal.filesrv dport=139,445
- rule: src=office dst=external dport=25,53
- guest_id: dnsmail
number: 1
- guest_id: filesrv
number: 1
- guest_id: desktop
number: 1
entry_point: yes
topology:
- type: custom
networks:
- name: external
members: dnsmail.eth0
gateway: firewall.eth0
- name: internal
members: filesrv.eth0
gateway: firewall.eth1
- name: office
members: desktop.eth0
gateway: firewall.eth2
```

Bibliography

[1] CyTrONE: An Integrated Cybersecurity Training FrameworkRazvan Beuran, Cuong Pham, Dat Tang, Ken-ichi Chinen, Yasuo Tan and Yoichi ShinodaJapan Advanced Institute of Science and Technology, Nomi, Ishikawa, Japan https://www.jaist.ac.jp/~razvan/publications/cytrone_integrated_framework.pdf

[2] https://github.com/crond-jaist/cytrone/

[3] https://github.com/crond-jaist/cyris

[4] https://github.com/crond-jaist/cylms

[5] A Survey of Cyber Ranges and Testbeds, Jon Davis and Shane Magrath
https://apps.dtic.mil/sti/pdfs/ADA594524.pdf

[6] The Cyber Range: A Guide - Guidance Document for the Use Cases, Features, and Types of Cyber Ranges in Cybersecurity Education, Certification and Training - Prepared by the NationalInitiative for Cybersecurity Education (NICE) Cyber Range Project Team

[7] Understanding Cyber Ranges: From Hype to Reality (March 2020) -
https://ecs-org.eu/documents/publications/5fdb291cdf5e7.pdf

[8] CyRIS: a cyber range instantiation system for facilitating security training
https://www.researchgate.net/publication/311621279_CyRIS_a_cyber_range_instantiation_system_for_facilitating_security_training

[9] KYPO Cyber Range: Design and Use Cases
https://is.muni.cz/publication/1386573/2017-ICSOFT-kypo-cyber-range-design-paper.pdf

[10] CyTrONE: An Integrated Cybersecurity Training Framework
https://www.jaist.ac.jp/~razvan/publications/cytrone_integrated_framework.pdf

[11] Cyber Range: Who, What, When, Where, How and Why?
https://www.govtech.com/blogs/lohrmann-on-cybersecurity/cyber-range-who-what-when-where-how-and-why.html

[12] https://github.com/secdevops-cuse/CyberRange

[13] The Cyber Range: A Guide Guidance Document for the Use Cases, Features, and Types of Cyber Ranges in Cybersecurity Education, Certification and Training
https://www.nist.gov/system/files/documents/2020/06/25/The%20Cyber%20Range%20-%20A%20Guide%20%28NIST-NICE%29%20%28Draft%29%20-%20062420_1315.pdf

[14] Using Cyber Ranges forCybersecurity Education
https://csrc.nist.gov/CSRC/media/Events/Federal-Information-Systems-Security-Educators-As/documents/24.pdf

[15] Cybersecurity education for the next generation – Emerging best practices
https://www.nist.gov/system/files/documents/2017/01/19/d1_trk3_viveros_cybersecurity_education_next_generation.pdf

[16] AWS Cyber Range — The Ultimate Cyber Lab Overview
https://medium.com/aws-cyber-range/aws-cyber-range-the-ultimate-cyber-lab-overview-3affcca1c842

[17] A Comparison of Network Simulation and Emulation Virtualization Tools, Dr. Te-Shun Chou, Mr. Steve Keith Baker, Miguel Vega-Herrera, ASEE's 123rd Annual Conference & Exposition, New Orleans Jazzed about Engineering Education

[18] National Cyber Range Overview
https://ieeexplore.ieee.org/document/6956748