Developing cyber security competences using NICE KSAs in cyber ranges

Amir Trent

2020 Laurea

Laurea University of Applied Sciences

Developing cyber security competences using NICE KSAs in cyber ranges

Amir Trent
Business Information Technology
Thesis
December, 2020

Laurea University of Applied Sciences **Abstract**

Business Information Technology

Bachelor of Business Administration

Amir Trent

Developing cyber security competences using NICE KSAs in cyber ranges

Year 2020 Number of pages 37

This Bachelor's thesis delves into the significance of cyber ranges and how they can contribute to university cyber security programs. The goal of the thesis project was twofold: firstly, to bring awareness of the applications of cyber range technology and how it can support cyber security curriculums; and secondly, to suggest how cyber ranges can be used with the NICE framework KSAs to improve cyber security competences in universities.

The thesis report consists of a theoretical framework where the National Initiative for Cybersecurity Education (NICE) competence framework is presented, and the concept of cyber ranges is introduced and defined. The NICE Framework structure and purpose is detailed and the use of it in academia is explored. Furthermore, the NICE Framework is discussed in conjunction with the use of cyber ranges in the past. The theoretical framework will elaborate on the history of cyber ranges, their functions, components, use cases and delivery methods as well as discuss the benefits and challenges in utilizing cyber ranges.

The empirical section compares three cyber ranges in terms of price and usability and presents the selection criteria and justification for selecting one of the three for further review. This section also presents a mapping of a cyber range scenario against a NICE framework work role and corresponding Knowledge, Skills, and Abilities (KSAs) as well as a demonstration of the cyber range application in play. The mapping identifies NICE KSAs that are developed through the simulation exercise, which is showed in the cyber range simulation. The interactive cyber range exercise involves completing an assignment using cyber-related tools in a simulated environment and collecting feedback from the activity.

The concluding section of this thesis presents the findings of the relationship between NICE Framework KSAs and a cyber range activity in relation to the Exploitation Analyst work role. Additionally, it presents other advantages that cyber range exercises provide. The conclusion of the thesis summarizes the importance of cyber ranges and how they can be utilized with the application of NICE KSAs elements to develop competencies required for specific work roles.

Keywords: Cyber range, NICE Framework, Cyber security training, KSAs

Contents

1 **Introduction** 8

2 **Changing cyber environment and growing need of cyber security professionals** .. 9

3 **Theoretical framework: NICE framework and cyber range background** 10

3.1 **NICE Framework** 10

3.1.1 Structure of the NICE framework 11

3.1.2 NICE Framework usage in academia 13

3.2 **Defining cyber ranges** 14

3.2.1 Types of cyber ranges 15

3.2.2 Different cyber range roles 16

3.2.3 Components of cloud based cyber ranges 17

3.2.4 Advantages and disadvantages of cyber ranges 18

3.2.5 NICE Framework in conjunction with cyber ranges 19

3.2.6 ..... The successful use of NICE framework based cyber ranges in higher education 20

4 **Research Methodology** 21

5 **Analysis** 21

5.1 **Selecting and testing a cyber range to illustrate usefulness to cyber security programs** 21

5.1.1 Introducing cyberranges.com 22

5.1.2 Testing cyberranges.com –Selection of scenario for testing and identifying developed NICE KSAs 24

5.2 **Cyber range simulation results** 25

6 **Results** 30

7 **Conclusion** 31

References 33

Figures 37

Tables 38

1 Introduction

Due to globalization advances in technology, the Internet has shaped the way society has developed. As stated by Romero (2019, 3), cyberspace has influenced many facets of modern-day civilization, such as trade and economic systems, governmental infrastructures, health systems, educational institutions, digital business, and other important infrastructures. The Internet has also shaped everyday activities such as entertainment, online shopping, payment applications and social media, among others. As these systems continue to develop due to the advancements within cyberspace, the Internet can also leave these infrastructures exposed to potential malicious threats. (Romero 2019, 2-3) This is why all organizations providing services online must pay increasing attention to the security of their services. This is where cyber security professionals are crucial.

Currently there is an immediate demand for cyber security professionals that possess the capacity to deal with the constant threat of sophisticated attacks. (Topham.et al 2016, 52) The dilemma according to Teoh et al (2017, 137) is that there is an outstanding gap between the wide demands for professionals compared to the shortage of qualified cyber specialist with the competency to mitigate latest threats. This can be attributed to professionals entering the workforce with the lack of security readiness and skills necessary in handling these current sophisticated threats. In order to balance this discrepancy, more universities are incorporating cyber security courses into their curriculums (Topham.et al 2016, 52).

According to Teoh et al (2017, 138), providing a significant amount of practical training supplemented with theoretical knowledge can help produce competent professionals coming into the cyber security workforce with roles including cyber security analysts, incident responders, threat analysts or pentesters, therefore improving the workforce shortage of qualified cyber security specialists. Topham et al (2016, 52) state that many universities that teach cyber security involve a robust concentration on theoretical knowledge with little to no supply of practical hands-on training. Cyber ranges can provide a solution to this. Several universities in the US have already successfully used cyber ranges in their cyber security curriculum to better optimize cyber security training and provide students with a balanced framework of theory and practical application to accurately assess and respond to today's growing cyber threats. (Frankin Jr. 2018)

The goal of this thesis is to focus on how universities can benefit from using cyber ranges to effectively improve their cyber security curriculum in developing today's cyber security professionals. Cyber ranges can be used to develop students' skills in assessing cyber threats and vulnerabilities and mitigate these threats (NIST 2018). By analyzing the applications of cyber

ranges compliant with the National Initiative for Cybersecurity Education (NICE) framework and Knowledge, Skills, and Abilities (KSAs), this thesis will establish how integrating cloud-based cyber ranges can improve the development of cyber security students' skills in universities.

This thesis will be dissected into different sections as follows. The first section will discuss the evolving environment and growing need for cyber security in today's world. The second section is the theoretical framework, which will introduce the NICE framework, and the concept of cyber ranges. The third section presents the research methodology; the fourth section will summarize how cyber ranges have been successfully used in the past by academia. The fifth analysis section will show the selection criteria of three cyber ranges, followed by the mapping of NICE KSAs aligned with the selected cyber range's exercises, ending with an exercise taken from the selected cyber range and its application in NICE KSAs. The last section, discussions and conclusions will finally bring the thesis to a close. As a result, this thesis can provide recommendations on the possibilities and advantages of using cloud-based cyber ranges that are compliant with the NICE work roles and KSAs in the Laurea cyber security curriculum.

2 Changing cyber environment and growing need of cyber security professionals

In today's world the Internet surrounds us both in our working life and in our homes. Digital streaming through Netflix, Hulu, Amazon Prime, personal shopping on Amazon and all other online retailers, social networking with platforms like Facebook, LinkedIn, and WhatsApp. The Internet is now even in our appliances, including refrigerators, alarm systems, washers, and dryers, you name it. The Internet has become essential in the functionality of these infrastructures, as these systems put in place are dependent on cyber networks to develop and flourish. Being so highly reliant on the Internet for our daily lives can make us vulnerable to malicious threats or attacks. These malicious threats can range from hackers who seek to gain access and compromise these networks for financial gain to cyber terrorists who seek to damage and cause disruption to governmental and other critical institutions with catastrophic effect (Romero 2019, 4-6).

Ransomware and DDOS attacks are examples of methods that attackers can use. Ransomware is a malicious malware with which an attacker compromises a network and will demand a fee in exchange of restoring the functionality of their systems. (Kaspersky 2020) This happened to Garmin, a fitness-based tracker company, who recently recovered from a ransomware attack that resulted in their online services being disabled. (BBC 2020) In Finland a recent data breach of Vastaamo psychotherapy services rendered a loss of 40 000 patient records, which are currently being used by attackers to blackmail patients who have used the service (Yle

News 2020). A DDOS attack can be used to flood network servers with traffic, limiting the capacity of its resources until the entire network is rendered inoperable. (Kaspersky, 2020) This recently happened to Amazon Web Services (A10 Networks, 2020). The implications of such attacks can result in financial ruin, irreparable damage of confidence and trust of consumers and other devastating impacts in other domains of modern society.

To combat these threats, the importance of cyber security is increasing. Cyber security is being integrated in digital service infrastructures, constantly being evaluated, and assessed in order to fortify and strengthen defenses against attackers. Security controls may include configuring systems with firewalls, malware defenses or antivirus solutions to help mitigate and fend off common cyber-attacks. As technology in cyberspace becomes more advanced, attackers are also evolving and becoming more sophisticated in their attacks, which makes it more cumbersome to deploy effective countermeasures against these threats (Cisco, n.d). The evolving cyber environment means that the need for cyber security professionals is changing also. Equally, the requirements for learning the profession are evolving too.

Universities have responded to this dilemma according to Bovee and Read (2018, 106) by implementing more hands-on experiential training in the form of labs, capstone projects, and virtual simulated environments such as cyber ranges. Prominent US universities such as the university of Cincinnati and Virginia Tech in addition to international universities like JAMK (Jyväskylä University of Applied Sciences) have participated in building cyber range facilities in order to continually develop the knowledge they are learning in the classrooms through practical application in the form of Capture the Flag (CTF) scenarios, live exercises, team competitions, or lab drills (Dowd 2019, Jyvsectec 2020).

3 Theoretical framework: NICE framework and cyber range background

In this section the NICE competence framework is discussed by delving into the origins of its formation, the components surrounding the framework and its usage in academia. Cyber ranges are also reviewed in this section in relation to their description, cyber range types, roles, components, and advantages and disadvantages. Finally, the chapter discusses how the NICE framework is applied within cyber ranges.

3.1 NICE Framework

The NICE framework was selected as the guiding framework for this thesis as it is widely recognized and has been used by educational providers in improving cyber curriculums (NICCS n.d, Purdue University 2020). The NICE framework could be a viable resource with the intention of improving cyber security education programs also in the future.

The NICE cyber-security workforce framework is a blueprint that was developed through the collaborative efforts of the Office of the Security of Defense (OSD), Department of Homeland Security, and various partners of NIST (National Institute of Space and Technology) to address and define, along with categorizing the cyber security workforce. This framework serves as a rudimentary guideline to help create a workforce whose capabilities are aligned with an organization's needs in cyber security. The NICE framework establishes a common language for educators, employers, future workforce professionals, and casual users in the form of a lexicon structure that elaborates on specific cyber roles and occupations in comprehensive way. This allows for educators to develop their curriculums by covering certain KSAs (Knowledge, Skills, and Abilities needed for respective cyber positions. It also helps employers to reference and identify qualifications and training requirements in developing specific skills for performing cyber security tasks. Lastly, future cyber security professionals can use the framework to explore and gauge different cyber security roles and categories in obtaining certain KSAs or certificates deemed valuable to employers in the workforce (Newhouse et.al 2017, 1-2).

3.1.1 Structure of the NICE framework

As outlined by Figure 1, The NICE structure is composed of components that help identify and define cyber security work in a simplified and structured form. The framework begins with the most essential component, categories. Each category cascades into the specialty areas, followed by work roles, which include a specific list of TKSAs (Tasks, Knowledge, Skills, and Abilities). This section will define more in depth each of these elements that represent the framework. (Newhouse et.al 2017, 6)

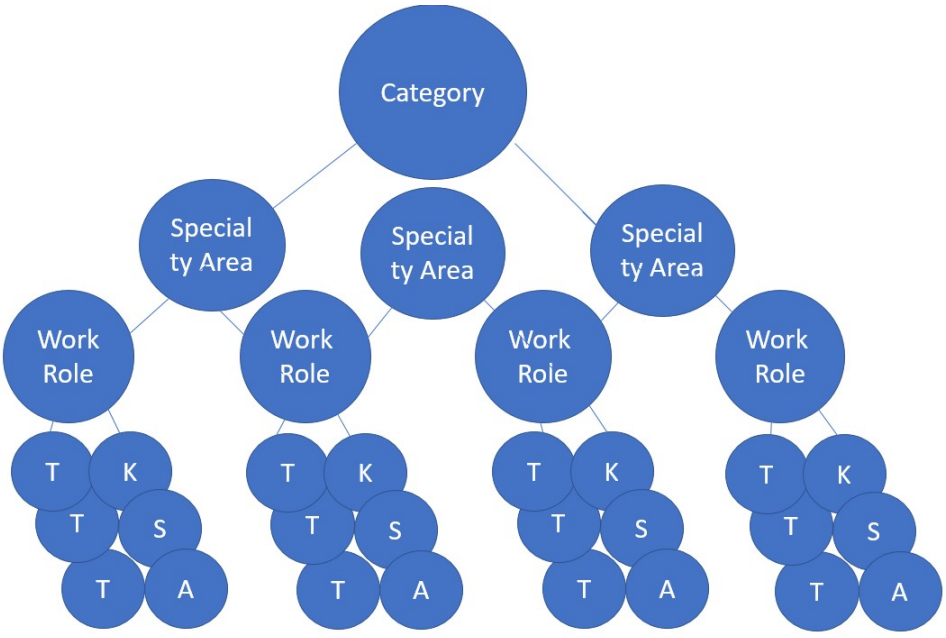

Figure 1: NICE Framework structure. Source: Modified from Newhouse et.al 2017, 6

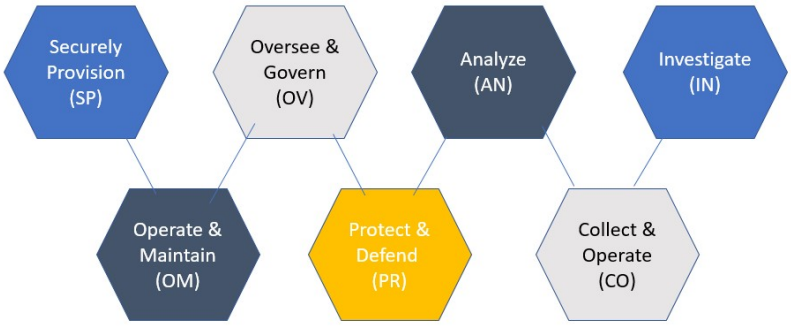

Figure 2. Illustration of NICE categories. Source: Modified from (The Lunarline School of Cybersecurity 2019)

The NICE framework includes seven categories. **Figure 2** illustrates the categories, which serve as the building blocks of the NICE framework. The first category is Securely Provision (SP), which constructs, designs, and conceptualizes secure IT (information technology) systems related to network or system improvement. Some specialty areas pertaining to SP would be risk management and systems development. The second category shown is Operate & Maintain (OM) which is involved in administering support in ensuring IT security and performance efficiency. One of the specialty areas that would aptly describe the OM category would be systems administration. The third category presented is Oversee & Govern (OV), which is responsible for governing, managing, or providing leadership towards conducting effective cyber security work. One of the specialty areas for this category is cyber security management. The fourth category displayed is Protect & Defend (PR) that involves identifying, evaluating, and mitigating threats that can compromise IT systems and networks. One of the specialty areas that explain PR is Cyber Defense Analysis. The fifth category defined is Analyze (AN), which meticulously reviews and assesses cyber security information to establish any value within its data. Threat and exploitation analysis would be two examples of specialty tasks under the Analyze category. Collect & Operate (CO) is the sixth category that provides operations involving deception and denial with the goal of collecting cyber information pertaining to developing intelligence. Cyber Operations and Collections Operations are two specialty areas represented under CO. Lastly the seventh category, Investigate (IN) delves into the investigation of events or cybercrimes related to Information technology systems and networks. Digital Forensics is one of the specialty areas that pertains to IN (NICCS 2020).

Specialty areas are specialized groupings of cyber security established under the seven categories. There are 33 specialty areas, which serve a specified focus of the functions related to cyber security work. In the updated version of the framework publication, the tasks and KSAs have been assigned to the work roles, instead of the specialty areas themselves (Newhouse et.al 2017, 5).

Work roles are introduced as the more comprehensive details behind the cyber security work. These work roles encompass an extensive list of attributes that correlate with the necessary requirements in performing a cyber security function in the form of KSAs and tasks. The NICE work roles are pertinent to both the job position itself and to aid in business processes (Newhouse et.al 2017, 5).

As discussed above, knowledge, skills, and abilities or (KSAs) are the listed attributes that are essential to perform the work roles established from the framework and job occupation. Knowledge would be defined as a foundation of information being utilized towards the performance of a work function. An example of this would be knowledge of cyber threats and vulnerabilities, which would align with the work role of a cyber operator. Skills are described as the technological competence to use processes, frameworks, and utilities related to cyber security functions. An example of skill application would be malware identification and capturing, which would be applied to the work role of a cyber defense incident responder. Then you have abilities, which signify the capacity of performing an action that delivers a specified result or objective. Analyzing malware would classify as an ability that would be applied to the work role of a cyber defense analyst. Lastly there are tasks. Tasks are specific work descriptions that are used to produce the work role associated with specialty areas. Configuring network routers and switches are descriptive tasks related to the work role of network operations specialist under the specialty area of network services (Newhouse et.al 2017, 5).

3.1.2 NICE Framework usage in academia

Educators are able to utilize the NICE Framework as a reference to help students improve current knowledge and skills that they will need when entering the workforce. The NICE framework enables this by establishing tasks within work roles in which cyber security students can further develop particular KSAs. As previously mentioned, educational institutions play an integral role in increasing the quality of professionals heading to the workforce. By integrating the NICE framework within cyber security curriculums, universities are better prepared and develop learners with the necessary skills and knowledge to flourish as competent professionals. This also creates a more streamlined reference for students who are looking for direction as to what skills they need and what courses they should pursue in accordance with the area they are trying to specialize in (Newhouse et.al 2017, 3-9). Universities in

the United States that have successively integrated the NICE framework into their cyber security programs include Virginia Tech, Regent University, ChestNut Hill College, Texas A & M, Augusta University, and other institutions (Frankin Jr 2018).

3.2 Defining cyber ranges

Cyber ranges have numerous definitions and interpretations from different institutions. A general definition by NIST (National Institute of Standards and Education) depicts a cyber range as a virtualized simulated platform of an organizations network environment. This platform includes all the networks, applications, and tools of the organization's real network environment. This allows the user to develop attacks, defend against attacks and holistically train and practice cyber security related skills in a controlled, safe environment isolated from other connected networks that would be vulnerable to malicious activity over the Internet.

Another definition of cyber ranges by Esco (2020) describes it as "a platform for development, delivery and use of interactive simulation environments which includes a combination of core technologies for the realization and use of the simulation environment and of additional components which are, in turn, desirable or required for achieving specific cyber range use cases" (Esco 2020). This definition states that cyber ranges as a resource involves multiple capabilities and functionalities in various focuses of security, depending on its intended specified usage. The type of skills being practiced with cyber ranges often include penetration-testing, system hardening, defending, and responding to attacks (Davis and Magrath 2013, 2). Davis and Magrath (2013, 2) also suggest that the virtualized environment should emulate the network infrastructure in order to reflect real-time situations. This gives the user a realistic interaction with the type of events and problems that occur in today's networks, subsequently improving their readiness. In addition, the cyber range can be also used for cyber security product testing and product development.

Originally cyber ranges were utilized for military purposes in classified security programs, only accessed by authorized top-level personnel, but since then their applications have extended to private and public sectors as well as academia. Several types of people now use cyber ranges, including educators, students, event organizers, researchers, and cyber security professionals.

The purpose behind cyber ranges is to provide a safe interactive environment that allows users to develop and build cyber skills needed in preparation for detecting and mitigating potentially deadly cyber-attacks when they occur (Stone, 2020). These cyber skills are developed through exercises presented in the form of an attack/defend setup where users engage in exercises alternating between launching an attack on a simulated network

environment and trying to safeguard the network and mitigating hostile cyber-attacks. In these scenarios, the users can work individually in these assignments or collectively. The purpose of these attack/defense simulations is to properly gauge current strengths of real-world cyber threats, whilst finding areas of improvement in analyzing and remediating these attacks (Crowdstrike, 2020). The outcome of how these cyber ranges is utilized is determined by its intended application of the respective user (Esco 2020).

Cyber ranges can be used for example for the following purposes:

- Security testing looking for vulnerabilities against security products by attacking the simulated environments.
- Security research to identify and detect new threats and mitigation solutions.
- Competence building using cyber ranges as a cost-effective method in providing hands-on training to personnel.
- Security education, using cyber ranges as a viable pedagogical approach of teaching valuable cyber skills to students pursuing security professions.
- Cyber capabilities development, adopting cyber ranges in building cyber competence efficiently.
- Cyber resiliency development using cyber ranges as a benchmark to assess an organizations capacity to effectively respond to attacks.
- Competence assessment, a method that incorporates cyber ranges in determining one's knowledge through simulation testing.
- Recruitment, listing specific cyber competences to effectively recruit qualified candidates.
- Digital dexterity, an activity to improve an organization's digital development in their business processes, and to facilitate national and international competitions.

3.2.1 Types of cyber ranges

Based on NIST explanations (NIST 2020, 12-13) there are four classifications of cyber ranges dependent on the specific features and capabilities utilized for its intended use case. The four types are simulation, emulation, overlay, and hybrid ranges. Regarding simulation ranges, they are ranges that operate on virtual environments (VMs) that replicate the behavior of a realistic network environment without the necessities of physical network hardware. Overlay ranges or Ad-hoc ranges utilize live networks as their infrastructure, which improves fidelity, adds flexibility with the ability to addition configurations on top of existing networks, but can be unpredictable in managing network control. Emulation cyber ranges are operated on a physical standalone infrastructure that emulates the software and network mapping of the cyber range. This allows a higher fidelity compared to simulation and emulation ranges and because of the physical setup, the network overload, and traffic

performance can be easily monitored in contrast to simulation ranges. The last classified range is a hybrid range, which is a customized combination of the previous ranges (Davis & Macgrath 2013 12-13, NIST 2020, 12-13). The advantage of a hybrid range infrastructure is the scalability with incorporating a physical network infrastructure, whilst having the simplicity of configuring virtual simulations (IXIA 2014, 9).

Cyber ranges can be distributed through two models which come in the shape of a SaaS (Software as a Service) through either a cloud platform, or a physical location; the other delivery model is through a dedicated cyber range which is created onsite by the organization itself. Regarding the first delivery model, cyber ranges are accessed online in the cloud provided by a third-party distributor. If the delivery model were location based the consumer would be required to go to the hosting site of the cyber range, where the customer would receive additional training services (ECS 2020, 26).

3.2.2 Different cyber range roles

Depending on the infrastructure of the cyber range, the participants assume certain roles or teams for the task scenario. The most common teams a cyber range would present are blue teams, red teams, and white teams (Perez 2020, 7).

Blue teams: Blue team roles are designated for participants who are assigned to protecting the targeted network against cyber threats. In this defensive role blue team members are tasked with analyzing threats attackers use to deploy their cyber-attacks. They also develop detection and preventative tactics to further safeguard the network. Exercises conducted as a blue team member can help improve their skills in analyzing and mitigating more sophisticated cyber-attacks as well as increase their cyber defensive skills and knowledge. This role is typically outfitted for users who want to pursue roles indicated by the NICE competence framework such as cyber defense incident responders and improve their preventative, detective, and mitigative skills. (Crowdstrike 2020, NICCS 2020)

Red teams: Red team members assume the role of the attackers who utilize attack techniques to infiltrate target networks. In this role, red team members employ adversarial tactics in form of social engineering, phishing, or elevated privileged access to compromise the network. Exercises performed by red team members help users understand common and future sophisticated attacks threats that may be deployed, along with building skills to better defend against these threats. This role is designed for users who are trying to fulfill NICE work roles as pen testers, cyber analysts, or ethical hackers and want to build on their infiltration skills.

White teams: White team members are responsible for monitoring the activities of the other participants, in addition to managing content and evaluating user performance.

Administrators, instructors, and moderators fill the roles of the White team (Crowdstrike 2020).

3.2.3 Components of cloud based cyber ranges

As depicted by **Figure 3**, a cyber range infrastructure can be comprised of multiple segments depending on the specific cyber range. The foundation of a cloud based cyber range is the orchestration layer; the following layers are underlying layer infrastructure, virtualization layer, and target infrastructure (NIST 2020, 7). The cyber ranges should include an environment that provides scalability in terms of hardware and network configuration to support the infrastructure of the cyber range, real-time feedback of the simulation activities, measures of performance and analytics, and high quality of network data (Urias et.al 2018, 2). These factors are determined by the overall components of the cyber range that will be described in the next sections.

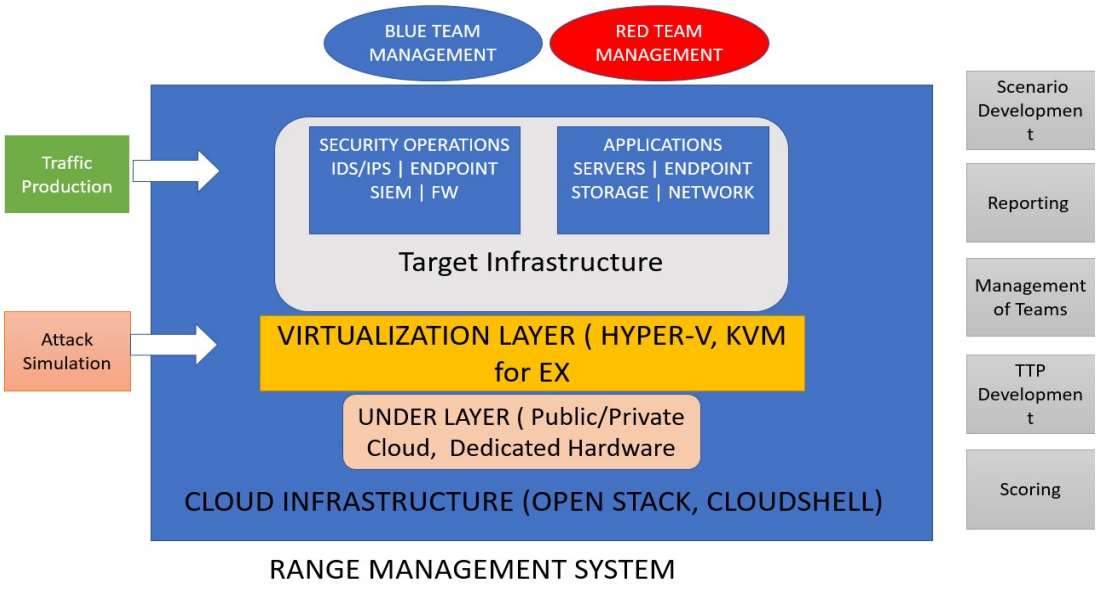

Figure 3. Depiction of the inner workings of a cloud-based cyber range infrastructure. Source: Modified from (NIST 2020, 7)

The cloud orchestration layer is the central technology responsible for controlling all the other functionalities of the cyber range through automation processes not limited to modifying, configuring, and deleting VMs (virtual machines). This administration can be performed through third party services or facilitated in-house with popular products such as Openstack.

The underlying infrastructure or configuration layer pertains to the configuration of the system the cyber range is operating through. This can be implemented through a dedicated physical hardware design comprised of laptops, servers, routers, and other equipment usually set up in a server rack. Other alternative options can also be delivered through cloud models whether through private cloud platforms, public cloud services or hybrid cloud infrastructures, which encompasses both the functions of private and public cloud platforms.

The virtualization layer is comprised of the virtualization technology, which is used for the cyber range applications. The most common method of virtualization is distributed through hypervisor technologies in the form of either bare metal hypervisors like Hyper-V or KVM, which have the hypervisors installed in the hardware, or Type 2 based hypervisors such as VM Workstation Player and Virtual Box that use a host OS to run the virtual machine. The benefit of utilizing a bare metal hypervisor is that the quality and processing power of the hypervisor is enhanced in addition to running multiple virtual machines at one time, whilst the downside is that it requires a specific type of hardware to operate these VMs and is highly costly. The advantage of using a type 2 hypervisor is that it is easy to install, but it is offset by the slow processing power due to the consumption of CPU power and other resources from the host OS.

The target layer depicts the simulated environment of the target that the end user will navigate through. The components inside the environment consist of all the applications that you will normally find in a typical OS, such as servers, networks, firewalls, Internet, storage, IDS systems. This provides the user with a visual realistic representation of a network environment, which they can better analyze and test attack and defense scenarios for familiarity on current setups involving real life network traffic generation and threat simulation.

Lastly the interface that ties all the components together comes in the shape of a range management platform. The online application platform administrates the delivery of the content of the cyber range through utilities such the scoring and reporting of the tasks, participant and role management, description of assignment, management of resources (type of range), instructor tools, and other features (NIST 2020, 6-8).

3.2.4 Advantages and disadvantages of cyber ranges

Cyber ranges can provide a practical method in evaluating human performance and reactional behavior toward making critical decision that impacts the security of a network against potential threats. In addition, the usage of cyber ranges allows institutions to gauge efficiency in current cyber security systems, along with implemented security policies and guidelines. Other benefits include examining the present capabilities of the security team in detecting potential threats and mitigating them effectively. This also becomes useful in scrutinizing any potential qualified candidates in their abilities before they join an

organization. Most importantly, pertaining to this thesis is that cyber ranges can improve the quality of a cyber security education in terms of cyber awareness, readiness, and improving one's capacity to mitigate threats, which would prove beneficial for students entering the workforce.

The overwhelming expense of maintenance is the main disadvantage of cyber ranges that should be considered, especially if the range is constructed in-house. The cost includes maintenance of networks and management of third-party tools alongside modifying and updating network topologies after each cyber range session concludes. Homemade ranges would require constant debugging and updates to ensure consistent quality of performance. Another disadvantage of building a cyber range from the ground is that it would require significant amount of planning in updating, and testing attack scenarios, which would increase overhead, cost substantially. Commercialized ranges provided by third party service providers are tailored to support the constant maintenance of network traffic performance, testing and modification of attack scenarios and virtual machines. Therefore, it is important that an in-house cyber range has all the necessary requirements, such as proper network topology, scenario development, network maintenance, metrics of performance, debriefings, third party tool support, and adaptation of attack scenarios, in order to effectively implement it in a cyber security training program, otherwise a commercial cyber range would be better suited for cyber security curriculums (CyberBit, 2020).

3.2.5 NICE Framework in conjunction with cyber ranges

The NICE framework can be a powerful tool in conjunction with cyber range applications if used effectively. Instructors and administrators could optimize cyber range capabilities by integrating core components within the framework in the design of the cyber range scenarios. This could entail a mapping linking cyber range exercises to the NICE categories involving Collect and Operate, Analyze, Investigate, Oversee and Govern, Operate and Maintain, Protect and Defend, and Securely Provision, in addition to their associated work roles and KSAs. Such KSAs that are focused on in cyber ranges can include the skill to analyze malicious activity in network traffic or knowledge of cyber threats and vulnerabilities or ability to describe techniques used for target exploitation (NICCS 2020). By introducing these types of KSAs in cyber range activities and scenarios, instructors are able to familiarize students with specific KSAs that are being implemented in the workplace, further developing their cyber security training and experience. Due to the flexibilities within a cyber range, the infrastructure could be mapped and tailored to include work roles, and KSAs included in the NICE Framework to help improve current cyber security curriculums with a more focused practical approach (NIST 2020, 11). A handful of prestigious universities that are utilizing cyber ranges aligned with NICE Framework themes include Augusta University, Purdue

University, Miami Dade University, Regent University and Metropolitan State University (Cyberbit Ltd 2019).

3.2.6 The successful use of NICE framework based cyber ranges in higher education

The successful use of NICE framework based cyber ranges in higher education in recent years universities have started to utilize cyber ranges and incorporate them into their cyber education programs. In building these cyber range facilities, students learn to hone their knowledge and skills by immersing in these NICE frameworks based virtual exercises that simulate real life threats. As a result, students are able to apply the skills they have developed in these activities and bring them into the workplace. The following paragraphs will showcase three universities that have successfully introduced cyber ranges in their institution.

Virginia Tech has successfully implemented the usage of cyber ranges in their facilities with the collaboration of Amazon Web Services. The result of this collaboration is a cloud based private infrastructure that provides a practical hands-on laboratory allowing educators to administer coursework and exercises tailored for cyber security students. The distinct types of abilities that students may learn in these exercises are exploiting and assessing vulnerabilities, building secure firewalls, and testing and securing web applications (EdTech, 2019). This laboratory in addition to various Capture the Flag competitions serves as a functional training environment to further develop and strengthen students' cyber security skills (Virginia Tech Daily, 2017).

Wayne State University is a Michigan based university in the United States that is now utilizing a cyber range hub in their facilities provided by the Michigan cyber range. This cyber range hub is a physical infrastructure that includes a multitude of cyber security certification courses and training hands-on simulations that are compliant with various frameworks such as the NICE framework (Johnston 2018).

Regent University is a university based in Virginia in the United States that has employed a cyber range in their school. This cyber range, provided by Cyberbit, is a cloud-based infrastructure that provides practical cyber security exercises and simulation platforms to familiarize students with real world threats such as malware, Man in the Middle attacks etc. In addition to the hands-on training, the cyber range is being assimilated with a specialized cyber program mapped to three tiers of certifications aligned with specific knowledge, skills, and abilities (KSAs) established by the national initiative for cyber security careers and studies. (NICCS, InfoSec Newsflash 2018)

4 Research Methodology

Qualitative research methods were selected for the research methodology of the thesis. The methodology that consists of qualitative analysis can be observed in several ways. One of the qualitive analysis approaches that will be selected for this thesis is pattern coding. This method is defined as codes that are interpreted in order to identify recurring themes, relationships, and patterns (Miles & Huberman 1994, 69).

The pattern coding will be performed by creating a matrix with NICE framework work roles and KSAs, along with one scenario from the cyber range. The aim behind this pattern coding is to determine a connection between NICE KSAs and the scenarios in cyber ranges, and finally illustrate how they are used to improve cyber students' skills and knowledge through a simulation exercise. The methodology aims at displaying how KSAs within NICE framework work roles can be developed through using cyber ranges to improve cyber security skills.

5 Analysis

The analysis section presents the selection of a cyber range for further review, introduces the selected cyber range, maps a scenario from the cyber range against one work role in the NICE framework and shows the use of one of the cyber range’s scenarios in practice.

5.1 Selecting and testing a cyber range to illustrate usefulness to cyber security programs

Three cyber ranges were compared prior to selecting a cyber range for simulation in this thesis. The selection criteria for cyber ranges included NICE framework compliance, accessibility, and cyber range type, see **Table 1**.

Cyber Ranges	**NICE Framework Compliant**	**Cyber Range Service**	**Cyber Range Type**	**Accessibility of Scenarios**
Cyberranges.com	Yes	Free and Subscription	Cloud/Hosted/On Premise/Portable	Easy/Intermediate/Advanced
Cyberbit	Yes	Subscription	Cloud/On Premise	N/A
Immersive Labs	Yes	Subscription	Cloud	Easy/Intermediate

Table 1. Comparison of cyber ranges. Source: Cyberranges.com, cyberbit.com, immersivelabs.com, 2020

All three cyber ranges included in the comparison were NICE Framework compliant. Cyberranges.com was the only one of the three to provide a free option in addition to the subscription-based options. All three cyber ranges in the comparison include a cloud-based option and cyberranges.com and Cyberbit provide additional on-premise options. Cyberranges.com provides the widest array of scenarios out of the three cyber ranges.

Based on the above criteria, cyberranges.com was selected as the cyber range to be further studied in this thesis, due to its versatility on all the selected criteria. Cyberranges.com provides a free service option, which allows users to access the service without the restrictions of a full subscription. The downside to the free option is that the user is limited to a certain number of tokens that get replenished every month from the day the tokens fully deplete. This option can easily be accessed for students and faculty with full functionality of the features cyberranges.com provides. However, it also provides the option of a subscription, which universities could consider purchasing and offering its cyber security students if deemed necessary. Additionally, cyberranges.com provides diverse levels of activities, making it possible to adjust the level of assignments based on the level of courses where cyber range assignments are included. Most importantly the cyber-range exercises in cyberranges.com illustrate the type of tasks that are established through the KSAs in NICE Framework work roles, making cyberranges.com a viable selection for cyber range testing.

5.1.1 Introducing cyberranges.com

Testing cyberranges.com included researching the user interface, its functionalities and ease of use of the site. The platform has a plethora of scenarios involving different type of activities for both individual and team-based simulations relating to real-world situations customized for specific use cases. These types of scenarios are aligned with KSA activities that correspond with certain cyber security positions such as penetration tester, malware analyst, incident responder, and other professions. **Figure 4** highlights some of the numerous activities cyber ranges have to offer related to the highlighted cyber professions.

The cyberranges.com cyber range has the following functionalities:

- Realistic simulations of corporate network infrastructures, real network, and system applications.
- Scouting/reporting of scoring, and statistics of user performance while being NIST/NICE compliant.
- Scenario customizations, orchestration management of virtual processes, attack inject simulations, and team-based scenarios.
- Cyberranges.com can be distributed as a deployment option that is either hosted, subscription-based service, on premise, or portable.

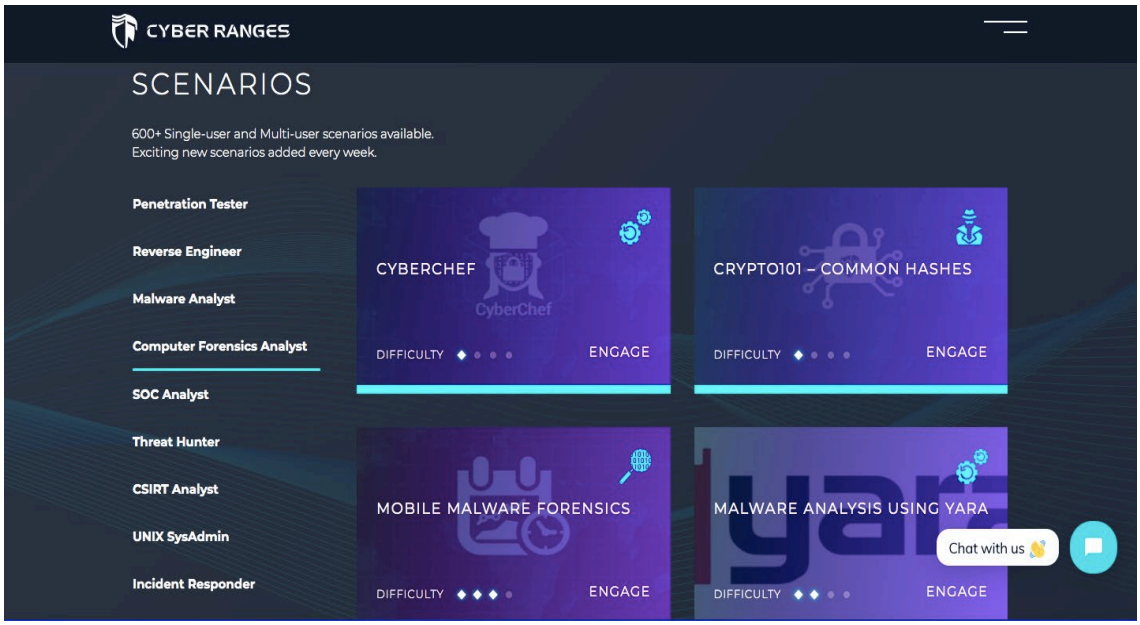

Figure 4. Scenarios of the cyberrange.com cyber range. Source: www.cyberranges.com, 2020

These features give the flexibility and simplicity for customers to utilize the cyber range as they see fit for use cases, whilst giving the learners the accessibility and customization from these features to maximize their learning development.

The user interface of cyberranges.com as depicted by **Figure 5** shows the main options that the user can choose from. The dashboard option outlines real-time statistics of the number of teams, scenarios, accumulated hours, and virtual machines in addition to showing new scenario releases. The library option is where the user will see an extensive list of scenarios, which they can select what they want to perform and is customizable with filter and category options. The complete selection gives the user the option to create competitive events such as CTF (Capture the Flag) scenarios. The playlist option allows the user to either choose a prepackaged collection of several scenarios or create a new playlist from the ground up. The team option gives the choice to either create a new team or join an assembled team to go head-to-head on team-based scenarios. The leaderboard selection provides the user the option to see his or her score rank in comparison to other participants in either an individual or team-based setting. Lastly the help option provides two quick tutorials on how to navigate the platform; other additional options such as configuration settings and account settings can be located on the top-right section of the site.

Figure 5. Illustration of cyberranges.com RLM interface. Source: cyberranges.com, 2020

5.1.2 Testing cyberranges.com –Selection of scenario for testing and identifying developed NICE KSAs

The cyberranges.com range provides more than six hundred scenarios, out of which many can be classified along the NICE framework work roles. Due to the substantial number of exercises included in the range, this thesis focuses on illustrating one cyber range scenario that could be used for developing the KSAs for one specific NICE framework work role. The work role evaluated was Exploitation Analyst, which is one of the various work roles within the NICE competence framework that graduates from cyber security educations may want to pursue. The review of the 600+ scenarios, found a total of 89 scenarios that develop the skillset of Exploitation Analysts on cyberranges.com. The scenario BlueKeep Exploitation was one of these 89 and was selected for further review in this thesis. **Table 2** shows exactly which KSAs the selected cyber range scenario BlueKeep Exploitation develops.

By identifying the specific KSA in relation to the work role, the user will build upon those practical skills through cyber range exercises. In performing the specified cyber range scenario, the activity will familiarize the user with operations that are identified within the NICE framework. The more exercises the user interacts with, the easier it can be for the user to develop relevant NICE KSAs in today's industry to improve their capacity as a cyber security professional.

BlueKeep Exloitation was also used to test the cyberranges.com cyber range in practice. The practical use of the scenario is illustrated in **figures 6-12** below.

The cyber range simulation from the Bluekeep Exploitation scenario demonstrates the activities and methods in which the NICE KSAs pertaining to the exploitation analyst work role can be developed in practice.

Cyberranges.com exercise develops NICE Framework Exploitation Analyst KSAs			
Cyber Range Exercise	NICE Framework Knowledge	NICE Framework Skills	NICE Framework Abilities
BlueeKeep Exploitation	K0005: Knowledge of Application Vulnerabilities.	SS264: Skill in assessing technical information relating to remote operations..ex ip ranges of the target	AA092: Ability to identify target vulnerability
	K0009: Knowledge of Cyber threats and vulnerabilities	SS269: SKill in examining vulnerábilities and exploits utilitized in network traffic.	
	K0608: Knowledge of Linux/and Windows OS system structures and Processes		

Table 2: Mapping of NICE Framework Exploitation Analyst KSAs presented in cyberranges.com exercise

5.2 Cyber range simulation results

The Bluekeep Exploitation simulation was selected to show how NICE framework skills are developed through the use of cyber ranges. As listed in **Table 2** above, the BlueKeep Exploitation simulation improves the following specific NICE framework KSAs: AA092, K0005, K0009, K0608, S0264, and S0269 (NICCS, 2020).

The demonstrated scenario is called BlueKeep Exploitation as depicted in **Figure 6**. In this scenario the user is tasked with infiltrating Microsoft Windows servers in order to obtain a specific flag text inside an administrator's files. The applied method in order to accomplish this objective was to exploit a security weakness in RDP using a CVE (common, vulnerabilities,

and exploits) called BlueKeep. BlueKeep is a CVE that allows you to gain unauthenticated access by exploiting unpatched Windows operating systems ranging from Windows Vista, XP, 7, Server 2003 and 2008 that has RDP services enabled.

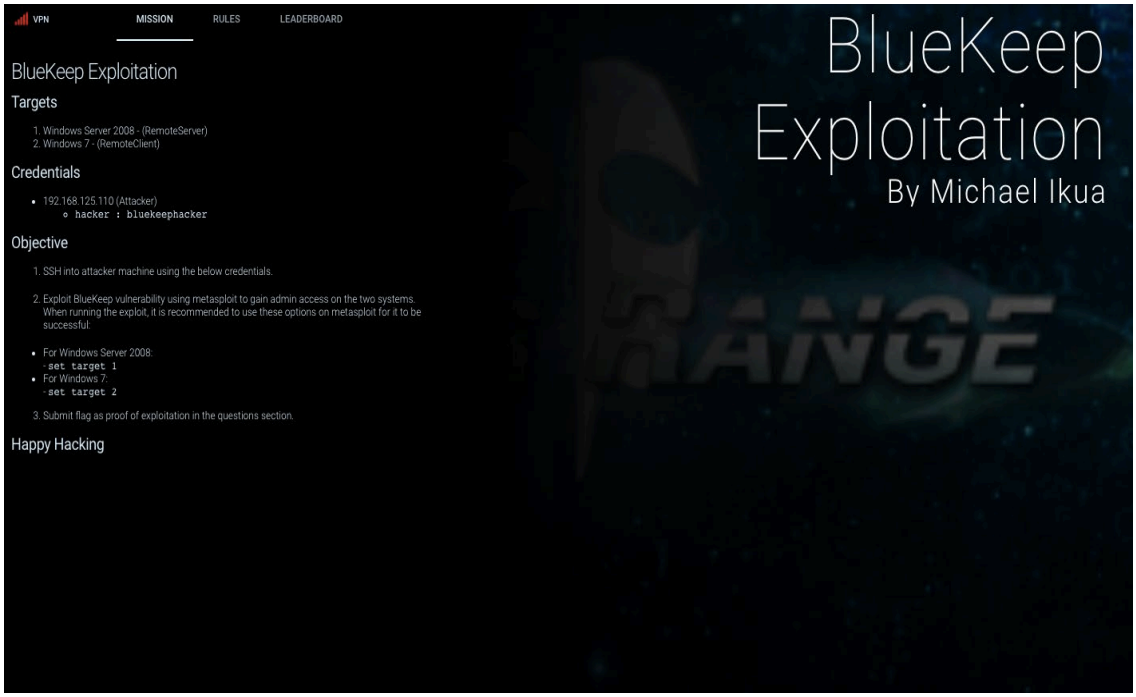

Figure 6: Illustration of BlueKeep scenario objectives. Source: Cyberranges.com, 2020

The infrastructure of this scenario involves using three virtual machines as shown in **Figure 7.** The one used as the primary machine in this simulation is a kali Linux OS named 07, a system typically used for pen-testing and ethical hacking with tools like Metasploit, which will be used for gaining access to the other two window servers named win2012 and windows 7.

Figure 7: Illustration of virtual networks in BlueKeep scenario. Source: cyberranges.com, 2020

As depicted by **Figure 8**, the first action involves gaining access to the kali Linux virtual machine using the provided credentials for the assignment in the command shell/terminal. Once access was gained to the Linux virtual machine, Metasploit was activated. That is a penetration testing software used to identify and exploit vulnerabilities in computer systems.

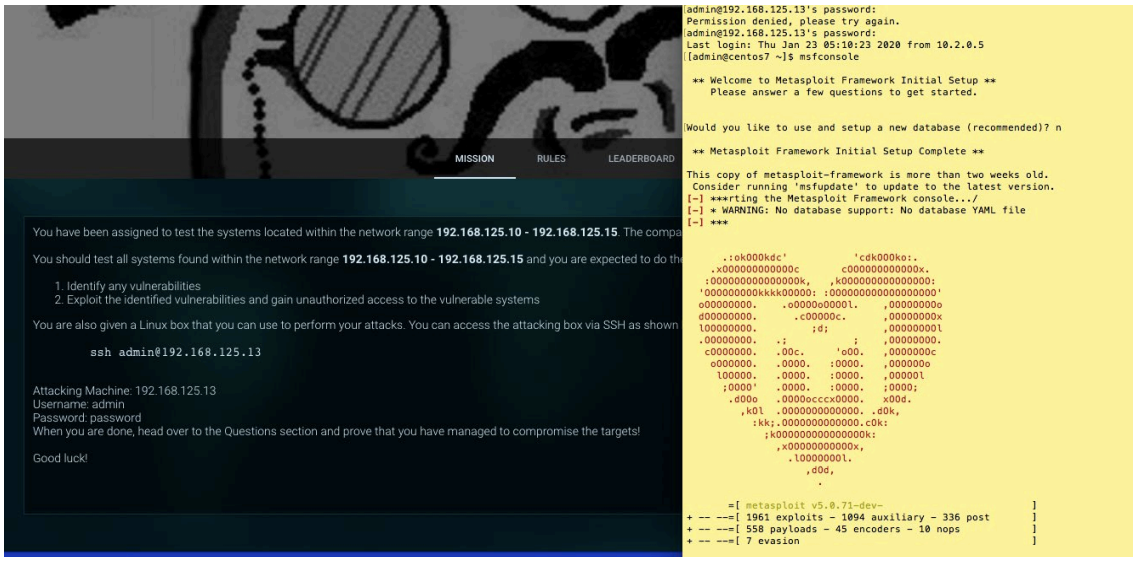

Figure 8: Illustration of accessing Kali Linux and activating Metasplit in BlueKeep scenario. Source: cyberranges.com, 2020

In the metasploit command shell, the search for the BlueKeep exploit provided a list of exploits in relation to Windows systems as shown in **Figure 9.**

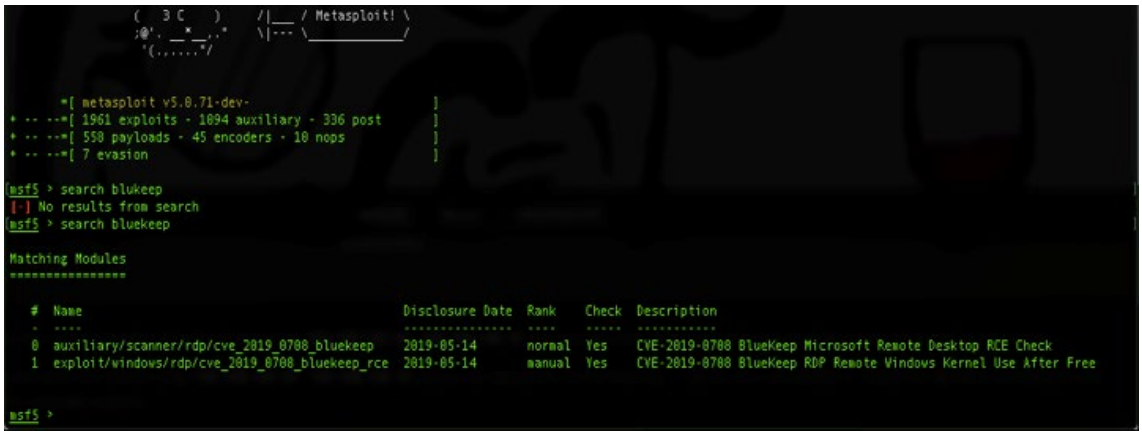

Figure 9: Depiction of using Metasploit in finding BlueKeep exploit for Windows servers. Source: cyberranges.com, 2020

After selecting both exploits to scan for potential vulnerabilities regarding RDP it was possible to exploit and then utilize BlueKeep to gain access to the windows VM as shown in **Figure 10.**

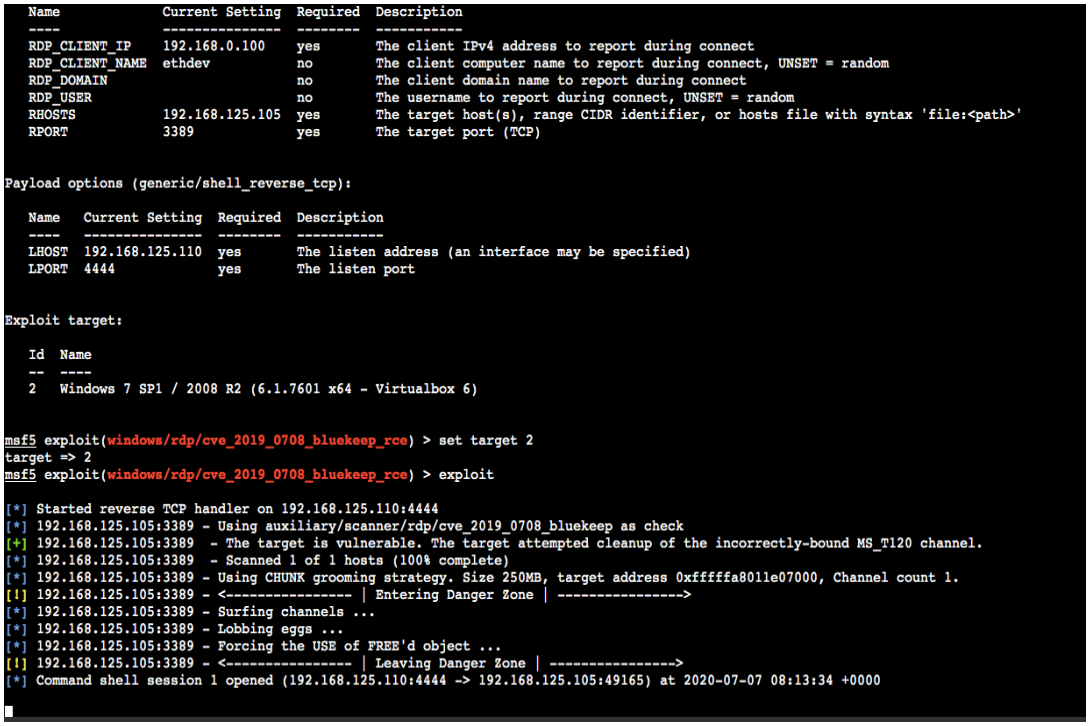

Figure 10 Illustration of performing BlueKeep exploitation for Windows server in Metasploit. Source: Cyberranges.com 2020.

Once accessing the Windows virtual machine, it was possible to easily use some commands to find the administrator's files by traversing into the main drive of OS and the finding the administrator through the user directory folder. Once inside the admin folder it was possible to locate the flag text and paste the flag statement onto the questions box as described in **Figure 11.**

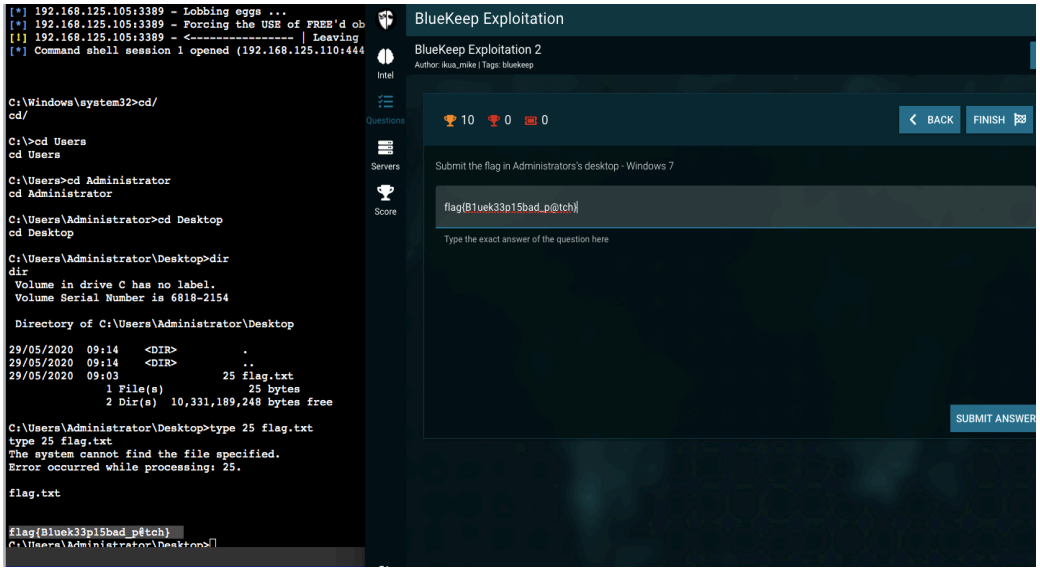

Figure 11. Illustration of accessing Windows server and obtaining flag document.
Source: Cyberranges.com, 2020

Once the same procedure is repeated with the other Windows virtual machine in gaining access to retrieve the flag text, the flag text is copied onto the questions box. After answering the correct statements, the reward was the completion of the scenario, alongside accumulating points toward the rank as shown in **Figure 12**.

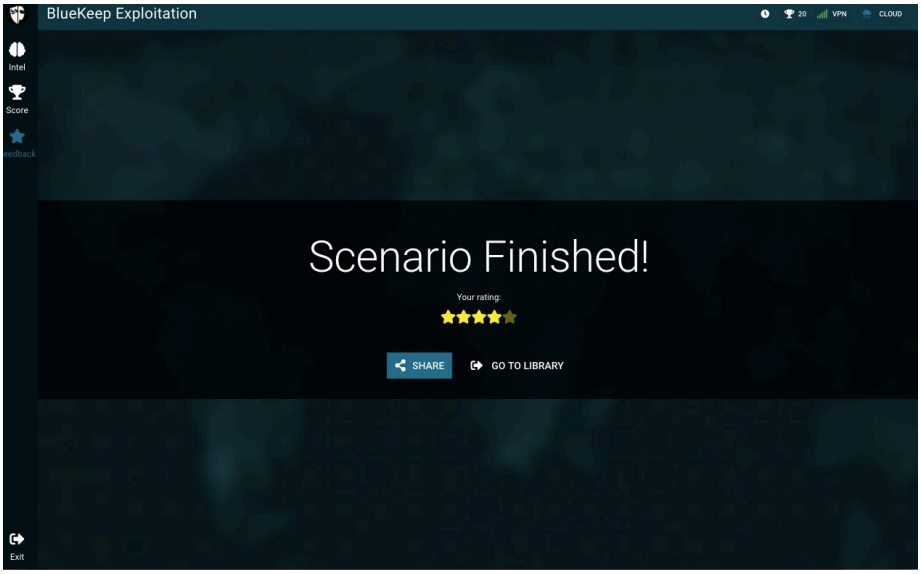

Figure 12. Illustration of completion of BlueKeep Exploitation scenario.
Source: Cyberranges.com, 2020

6 Results

The mapping of the cyberranges.com BlueKeep Exploitation scenario against the NICE framework Exploitation Analyst KSAs in Table 2 indicates that the cyber range can be used to develop the KSAs for that work role. By interacting with NICE based exercises, the user is able to closely analyze the KSAs associated with a work role. As a result, the user is able to apply the same KSAs they developed in these exercises to perform the same work roles in the industry as effective cyber security professionals.

The simulation exercise justifies how cyber ranges that are aligned with NICE work roles can be useful in academia regarding developing cyber security skills. The practicality of the exercises, such as the BlueKeep Exploitation scenario reproduces the type of cyber-attacks that cyber professionals and companies confront every day, helping students better familiarize themselves and learn how to anticipate and respond accordingly to similar situations.

Throughout the BlueKeep Exploitation simulation, six specific NICE KSAs pertaining to the Exploitation Analyst work role were identified as indicated in Table 2. The abilities in describing a vulnerability (AA092) are exhibited by the reading materials on BlueKeep and task instructions provided for the cyber scenario. The knowledge of cyber/application vulnerabilities and Linux / windows systems (K0005, K0009, K0608) are demonstrated by utilizing Linux and windows systems to exploit the BlueKeep vulnerability during the scenario. Lastly, the skills in discerning technical information and reaching vulnerabilities (SS264, SS269) are displayed by using the Metasploit application to analyze vulnerabilities in which the BlueKeep vulnerability is exploited in the cyber range simulation. As a result from the exercise, those KSAs can be further interpreted and developed as the user becomes more familiar with how these KSAs and tasks are related to similar NICE work roles like pentesters or ethical hackers, or malware analysts.

Based on interacting with the cyber range and the scenario, some other benefits identified in using cyber ranges were the following:

- Familiarity with network setups: Every scenario has different network infrastructures, so the user can get accustomed to how certain network topologies are designed that utilizes virtual machines with servers and client PCs.
- Familiarity with industry tools and utilities: The scenarios have prerequisite material such as software and reading documents that are required in order to complete the assignment. In using the tools from these exercises, users are able to get more familiarized with standard industry utilities, along with how these tools function.

- Familiarity in diverse cyber security roles and tasks: Engaging in various scenarios gives the user insight on what other cyber security professions are available and what roles and capabilities they pertain to. Participating in multiple scenarios that incorporate elements from various cyber security positions and work roles as described in the NICE framework can help the user become more versatile in their development and build their technical competence in cyber security.
- Absorption of information: Partaking in these scenarios, I was able to retain the information better compared to standalone theory. These scenarios can reinforce digestion of the knowledge by putting into practice what the user has learned through theoretical teachings. Through these exercises it became easier for me to conceptualize the theory more effectively, resulting in me progressing with practice, gradually turning my development into competence and new skills.

7 Conclusion

In conclusion, this thesis aimed to bring awareness on the applications of cyber ranges in supporting cyber security curriculums while developing cyber security competences. Based on the empirical research with the NICE framework and the applications of cyber ranges, it can be concluded that practical training places a crucial factor in developing cyber security skill competences. The results indicate that cyber ranges are applicable in developing cyber security skills for distinctive work roles and specialty areas established in the NICE framework. By interacting with NICE competence framework-based cyber range exercises, the user can closely analyze and develop certain KSAs ,like the ability to describe a vulnerability, the knowledge of cyber vulnerability and threats, and the skill in analyzing malicious activity as defined by work roles like an exploitation analyst. As a result, the user can apply these same KSAs they developed in these exercises to perform the same work roles in the industry as effective cyber security professionals. This thesis states that cyber ranges are effective in skill development, but also invokes the question of how to effectively incorporate them into a cyber security curriculum.

Based on these conclusions, cyber security programs benefit from using the NICE framework as a reference to highlight what cyber security courses should be introduced and improved on. By using cyber ranges that are compliant with the NICE framework components, the NICE framework can address what KSAs are being taught, and what needs to be implemented in cyber security curriculums in order to further improve the students' cyber security skill competence and flourish into competent cyber security professionals. What separates cyber ranges compared to other traditional methods is that it allows users to interact in real like network environments, which helps improve retaining information and practical training, as opposed to passively learning cyber security concepts through videos and textbook materials

(Murphy 2019). Cyber ranges provide practicality towards developing cyber security skills that are more effective than other theoretical models, which makes them a viable approach in cyber security curriculums.

Cyber security programs could consider utilizing commercial cloud based cyber ranges as a viable delivery model for cyber range implementation. The support of network upkeep, and maintenance of debugs, and added features of cyber ranges would make it a cost-effective model to implement in comparison to an in-house model that requires an adequate network infrastructure with constant maintenance in order to reap the benefits of a cyber range. Cyberranges.com would be a good example of a cost-effective cloud cyber range to incorporate practical exercises to supplement the existing theoretical knowledge provided. The vast array of exercises including the simulation exercises that are aligned with the KSAs from NICE framework and industry certificates like EC-Council CEH and CompTIA's Security+ can make a cyber range like cyberranges.com a feasible and beneficial method towards improving practical training aspects under cyber security curriculums.

By illustrating how effective the applications of cyber ranges in conjunction with a framework like NICE framework can be in developing cyber security skills, the research can serve in explaining how higher education can provide adequate balance of a theoretical knowledge and practical training in a cyber security curriculum that translates into competency in a cyber security workplace.

References

Printed

Bovee, M.W. & Read, H.O.L. 2018, "Cyber-Securing Super Bowl 50: What Can a Live-Fire Football Match Teach Students about Becoming Better Cybersecurity Professionals?", Journal of Information Warfare, vol. 17, no. 4, pp. 106-118, II, IV

Davis, J. and Magrath, S., 2013. A survey of cyber ranges and testbeds (No. DSTO-GD-0771). DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION EDINBURGH (AUSTRALIA) CYBER AND ELECTRONIC WARFARE DIV, pp. 12-13

ECSO, 2020. Understanding Cyber Ranges: From Hype To Reality. [ebook] ECSO, pp.2-31. Available at: <https://www.ecs-org.eu/documents/uploads/understanding-cyber-ranges-from-hype-to-reality.pdf> [Accessed 5 November 2020].

Huezo, R., 2019. Cyberspace Dilemmas. Containment Of Cybersecurity Threats. [online] Academia.edu. Available at: <https://www.academia.edu/41492226/Cyberspace_Dilemmas_Containment_of_Cybersecurity_Threats> [Accessed 4 November 2020].

Miles, M.B, Huberman, A.M. 1994. Qualitative Data Analysis. SAGE Publications. Thousand Oaks California. 2nd edition. pp 67

Newhouse, W., Keith, S., Scribner, B. and Witte, G., 2017. National Initiative For Cybersecurity Education (NICE) Cybersecurity Workforce Framework. [ebook] NIST. Available at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf> [Accessed 5 November 2020].

Shorten, A. Smith, J. 2017. Mixed Methods Research: Expanding the Evidence Base. Evidence Based Nursing.Vol 20, no 3. p.74-75.

Teoh, C. S., & Mahmood, A. K. (2017). Cybersecurity Workforce Development for Digital Economy. The Educational Reviewing, USA,2(1), 136-146.

Topham, L., Kifayat, K., Younis, Y.A., Shi, Q. and Askwith, B., 2016. Cyber security teaching and learning laboratories: A survey. Information & Security, 35(1), p.51

V. E. Urias, W. M. S. Stout, B. Van Leeuwen and H. Lin, "Cyber Range Infrastructure Limitations and Needs of Tomorrow: A Position Paper," 2018 International Carnahan Conference on Security Technology (ICCST), Montreal, QC, 2018, pp. 1-5, doi: 10.1109/CCST.2018.8585460.

Electronic

A10 Networks, 2020. Five Most Famous DDoS Attacks and Then Some. A10 Networks. Available at: https://www.a10networks.com/blog/5-most-famous-ddos-attacks/ [Accessed November 4, 2020].

Cisco, 2020. What Is Cybersecurity? Cisco. Available at: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html [Accessed November 4, 2020].CrowdStrike, 2020. Red Team VS Blue Team In Cybersecurity | Crowdstrike. [online] crowdstrike.com. Available at: <https://www.crowdstrike.com/epp-101/red-team-vs-blue-team/> [Accessed 4 November 2020].

CyberBit, 2018. Cyber Range For Higher Education - Build Or Buy?. [ebook] CyberBit. Available at: <https://storage.googleapis.com/stateless-www-cyberbit-com-liv/2018/10/Cyber-Range-Build-vs.-Buy-White-Paper.pdf> [Accessed 4 November 2020].

Dowd, K., 2019. University Cyber Ranges Immerse Students In Cybersecurity Education. [online] edtechmagazine.com. Available at: <https://edtechmagazine.com/higher/article/2019/10/university-cyber-ranges-immerse-students-cybersecurity-education-perfcon> [Accessed 4 November 2020].

Franklin Jr., C., 2018. 7 University-Connected Cyber Ranges To Know Now. [online] Dark Reading. Available at: <https://www.darkreading.com/cloud/7-university-connected-cyber-ranges-to-knownow/d/d-id/1331224> [Accessed 5 November 2020].

Gonzalez, C., 2020. *Cyber Range The Future Of Cyber Security Training*. [online] Sans.org. Available at: <https://www.sans.org/reading-room/whitepapers/training/cyber-range-future-cyber-security-training-39550> [Accessed 5 November 2020].

InfoSec News Flash, 2018. Immersive Training On Regent University'S Cyber Range Puts Cyber Professionals Ahead Of The Game - Cyber Defense Magazine. [online] Cyber Defense Magazine. Available at: <https://www.cyberdefensemagazine.com/immersive-training-on-regent-universitys-cyber-range-puts-cyber-professionals-ahead-of-the-game/> [Accessed 4 November 2020].

IXIA, 2014. Cyber Range: Improving Network Defence And Security Readiness. [ebook] Phoenix DataCom. Available at: <https://www.phoenixdatacom.com/wp-content/uploads/2015/11/915-6729-01-Cyber-Range-pdl.pdf> [Accessed 5 November 2020].

Kaspersky, 2019. What is a DDoS Attack? - DDoS Meaning. www.kaspersky.com. Available at: https://www.kaspersky.com/resource-center/threats/ddos-attacks [Accessed November 4, 2020].

Kaspersky, 2020. What is Ransomware? www.kaspersky.com. Available at: https://www.kaspersky.com/resource-center/definitions/what-is-ransomware [Accessed November 4, 2020].

NIST, 2018. *Cyber Ranges*. [ebook] Available at: <https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf> [Accessed 6 November 2020].

NIST, 2020. The Cyber Range: A Guide. [ebook] NIST. Available at: <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> [Accessed 5 November 2020].

Purdue University, 2020. IUPUI To Offer Master'S Degree In Cybersecurity For Purdue Cyber Apprenticeship Program. [online] Purdue.edu. Available at: <https://www.purdue.edu/newsroom/releases/2020/Q4/iupui-to-offer-masters-degree-in-cybersecurity-for-purdue-cyber-apprenticeship-program.html> [Accessed 5 November 2020].

Stone, M., 2020. How Cyber Range Training Can Be Effective For All Members In Your Organization. [online] Security Intelligence. Available at: <https://securityintelligence.com/articles/cyber-range-training-effectiveness/> [Accessed 5 November 2020].

JYVSECTEC by Jamk. 2020. Cyber range. https://jyvsectec.fi/. [Accessed 6 December 2020].

Yle Uutiset. 2020. *Vastaamo Board Fires CEO, Says He Kept Data Breach Secret For Year And A Half*. [online] Available at: <https://yle.fi/uutiset/osasto/news/vastaamo_board_fires_ceo_says_he_kept_data_breach_secret_for_year_and_a_half/> [Accessed 8 November 2020].

Vtnews.vt.edu. 2017. Virginia Cyber Range Names Amazon Web Services As Preferred Partner. [online] Available at: <https://vtnews.vt.edu/articles/2017/02/it_cyberrange.html> [Accessed 5 November 2020].

Unpublished

n.d. Using The Nice Framework. [ebook] p.1. Available at: <https://niccs.us-cert.gov/sites/default/files/documents/pdf/using%20the%20nice%20framework_pdf.pdf?trackDocs=using%20the%20nice%20framework_pdf.pdf> [Accessed 5 November 2020].

Figures

Figure 1: NICE Framework structure. Source: Modified from Newhouse et.al 2017, 6 11

Figure 2. Illustration of NICE categories. Source: Modified from (The Lunarline School of Cybersecurity 2019) 12

Figure 3. Depiction of the inner workings of a cloud-based cyber range infrastructure. Source: Modified from (NIST 2020, 7) 17

Figure 4. Scenarios of the cyberrange.com cyber range. Source: www.cyberranges.com, 2020 23

Figure 5. Illustration of cyberranges.com RLM interface. Source: cyberranges.com, 2020 24

Figure 6: Illustration of BlueKeep scenario objectives. Source: Cyberranges.com, 2020 26

Figure 7: Illustration of virtual networks in BlueKeep scenario. Source: cyberranges.com, 2020 26

Figure 8: Illustration of accessing Kali Linux and activating Metasplit in BlueKeep scenario. Source: cyberranges.com, 2020 27

Figure 9: Depiction of using Metasploit in finding BlueKeep exploit for Windows servers. Source: cyberranges.com, 2020 27

Figure 10 Illustration of performing BlueKeep exploitation for Windows server in Metasploit. Source: Cyberranges.com 2020. 28

Figure 11. Illustration of accessing Windows server and obtaining flag document. Source: Cyberranges.com, 2020 29

Figure 12. Illustration of completion of BlueKeep Exploitation scenario. Source: Cyberranges.com, 2020 29

Tables

Table 1. Comparison of cyber ranges. Source: Cyberranges.com, cyberbit.com, immersivelabs.com, 2020 21

Table 2: Mapping of NICE Framework Exploitation Analyst KSAs presented in cyberranges.com exercise 25