Syed Himel

CYBER DEFENSE EXERCISES IN XAMK VIRTUAL LABORATORY

Bachelor's thesis

Bachelor of Engineering

Information Technology (B.ENG)

2022

South-Eastern Finland
University of Applied Sciences

South-Eastern Finland University of Applied Sciences

Degree title	Bachelor of Engineering
Author(s)	Syed Himel
Thesis title	Cyber defense exercises in XAMK virtual laboratory
Commissioned by	XAMK Cyberlab
Year	2022
Pages	73 pages and 1 appendix page
Supervisor(s)	Vesa Kankare

ABSTRACT

The purpose of this study was to research the current best practices of cyber defense and the possible ways to implement them in a virtual lab environment. The thesis will add value to the commissioner virtual lab by providing a collection of exercises. To build a cyber defense network, different tools and techniques were studied and implemented.

Research through design approach was chosen as the research approach of this thesis. Design research is suitable for the research problems and the desired solution. Qualitative research methods were used to collect data from different sources, peers, and pilot students. The research process was broken into different stages, which were gathering resources and analyzing the resources to create cyber defense exercises for XAMK virtuallab environments.

The purpose of these cyber defense exercises was to build virtuallab environment exercises to develop participants' skills in cyber operations. The built exercises had various scenarios such as attacking a machine, detecting the attack, and defending and strengthen the security for future attacks. The target group of this study was XAMK students and companies that want to carry out cyber defense exercises in virtual environments. This defensive lab can be used to train individuals in real-time scenarios, and it can be used to practice different operating system (Linux OS or Windows OS) and their properties. The participants in these exercises will gain the required skills and experience in managing situations using different tools and techniques when an incident takes place.

The result of the thesis can be developed further in the future. They can be used to carry out defensive exercises in real events. With the help of the exercises, the cyber security skills of students and external company personnel can be developed in the future.

Keywords: Cyber Security, Cyber Defense, Incident Response, Situational awareness, Log4Shell, Network monitoring, Intrusion detection

CONTENTS

1 INTRODUCTION

Massive amounts of data are being generated every second, which is either stored somewhere or in transfer. Along with the data growth, the number of data leakages is also growing continuously. To protect data from being leaked, security comes as a priority, whether it can be training an individual, strengthening a system, or creating a shield around the infrastructure. Organizations all around the world invest significant amounts of money and effort to protect systems against cyber-attacks. Cyber experts need to invest their time remarkably into improving the security posture of organizations where they always need to defend the system against an attack. To defend a system against cyber-attack, one needs to know how the cyber offensive side of cyber security works. After all, there is always an admission of weakness in systems where it needs to be exposed before patching.

Security plays a key role in protecting our data and privacy. Without security, there is no privacy. Privacy is no more private, and it is because of the internet (Valkama 2018). Keeping our data and information completely private to us is called privacy. Nowadays, Privacy is no more private to us because it is open in the air, and it is done via the Internet. Threat actors take advantage of security vulnerabilities to gain access to our data and losing personal data makes it clear that there is a lack of privacy. Privacy is one of the biggest assets of security. Without proper implementation of security, there is no privacy. In the last ten years, there has been a vast number of cyber-attacks against our data. For example, in the year 2013, USA big box departmental store named Target was hacked and lost up to 40 million of their customers' card details (Washingtonpost 2013). In 2015 Facebook noticed one of the biggest data breaches done by Dr. Kogan and a data farm named Cambridge Analytica (CA). Dr. Aleksandra Kogan builds an application named "thisisyourdigitallife" (Kozlowska 2019). The application was designed to harvest people's data from Facebook and CA was successful to steal around 50 million Facebook users' data (Kozlowska 2019). America faced a big hack in 2015 by a Vietnamese hacker named Ngo Minh Hieu. He has stolen over 200 million Americans' data for selling on the dark web (Ewe 2022). According to Ewe (2022), victims suffered a lot from such attacks

such as one lost her house and was struggling to feed her children. In 2016, hackers took control of up to 500 million Yahoo user accounts (NCSC 2016). According to Bernard et al. (2017), Equifax faced a massive cyber-attack in (the year) 2017, which affected 143 million US consumers. People have lost their personal information such as social security numbers and driving license numbers.

The number of cyber-attacks in recent years has increased dramatically. Attackers are targeting different sectors such as Medical, Bank, Governmental agencies. In 2018 and 2019, one of the Finnish psychotherapy farms named Vastaamo reported a data breach. After taking control of the Vastaamo database, malicious actors started blackmailing the patients by threatening to publish their data on the dark web (YLE 2022a). In 2020, a software company named SolarWinds found out that their Orion software has been compromised by a group of attackers. It was a supply chain attack as it compromised over 18 000 of its customers (Jankowicz 2020). Some of SolarWinds' customer names are Microsoft, Ford, Visa, The Secret Service, The Department of Defense, The US President's office, NASA, and Cisco (Jankowicz 2020). According to YLE 2022b, F-Secure found over 200k personal data of Finnish LinkedIn users in a hacking forum. Attackers mostly use these types of data to run phishing campaigns (YLE 2022b).

Cyber-attacks are not only affecting our systems, but also the humans, our society, and the economy. During the Covid-19 pandemic, there have been ransomware attacks on the hospital sector. According to Wetsman (2021), there has been a ransomware attack On the University of Vermont (UVM) Health Networks. Medical authorities were unable to access the health records over weeks as this malware infected every computer in UVM medical center (Wetsman 2021). Attackers are targeting the biggest sectors which might cause serious problems in our society and eventually can harm human life. In October 2022, there was a ransomware attack in Denmark that forced the train authorities to stop the trains. Attackers targeted a third-party IT service provider named Supeo to gain access through operational technology systems to interrupt train

operations (Paganini 2022). In the last ten years, there have been different malware attacks on nuclear power plants. For example, in the year 2016 German Nuclear power plant was attacked by malicious actors with “W32.Ramnit” and “Conficker” malware (Trendmicro 2016). The attack on the German nuclear power plant did not cause a serious problem as it was not designed to harm the power plant itself. However, cyber warfare weapon like Stuxnet has the capability of destroying critical physical infrastructures. In the year 2010, Stuxnet has been used by USA and Israel to damage Iran's nuclear weapons (Chen et al. 2011). Stuxnet is a type of worm that was designed to target Industrial Control Systems. Nowadays, state-level actors are using different attack techniques such as hybrid operations to defeat opponents. Hybrid war can be very dangerous for a state as these attacks are carried out with the help of Artificial Intelligence (AI) technology such as deepfake. AI deepfake algorithm called Generative Adversarial Network (GAN) is used to clone voices, images, and videos (Mazzucchi 2022). As a result, deepfake technology can be used to manipulate people's minds for disinformation purposes. For example, a deepfake video of President Vladimir Putin was posted on Twitter where he was declaring Peace (Wakefield 2022). On the other hand, another video of President Zelensky was released on the Facebook taking of surrendering to Russia (Wakefield 2022). Deepfake videos are being used by the military for hybrid war e.g., on March 2022, a Russian state-level hacker took control of a Ukraine TV channel, and they were showing a deepfake video of President Zelensky where he was sending a message to his soldiers for surrendering to Russian military (Wakefield 2022). According to Rybski (2021), cyber threat effects, such as hybrid attacks, can be mitigated using the most important tools which are exercises. As a result, to safeguard businesses and our society cyber security students always need to practice real-world scenarios through different exercises to keep updated.

XAMK Cyberlab, the commissioner of this thesis, wanted to train their students of Bachelor and Master of Engineering in the degree programme of Cybersecurity for upcoming cyber challenges. Cyberlab is one of the best cybersecurity innovative platforms where students can specialize themselves, for example, in networking, cyber security, and data centers. Students can practice a large

number of exercises in a virtual laboratory environment to facilitate a hands-on experience with virtual machines. Exercise allows practicing different tools and techniques using various operating systems without breaking physical machines.

The objective of this thesis is to train students in the commissioner organization. In addition, this thesis aims to train individuals to understand cyber defense in a broader view, from penetration to defending a system. Students will be able to learn more about cyber security through the exercises by doing the penetration and defending the system against it. This thesis covers the details of exposing and patching a vulnerability. The tasks are broken into three parts. First, it identifies the target and its flaws. After (successfully) finding a target, it moves on to the attacking phase. In the attacking phase, it describes the steps needed to expose the vulnerability. Finally, it discusses how to defend a system by detecting an attack and strengthening the system to protect it from future attacks.

2 RESEARCH METHODOLOGY

In the following sections, the research problem and the questions of this thesis will be covered. In addition, it will justify a research approach and data-gathering methods.

2.1 Research problem

Billions of devices are getting connected online, which creates a bigger surface for threats like cyberattacks. Attackers are always growing with their tools and techniques, but cyber professionals are still behind in the race. Millions of devices are being hacked and trillions of dollars are being lost, which leads the world to a tremendous need for cybersecurity professionals. According to a June 2022 survey from the world's largest non-profit (ISC)2 association of certified cybersecurity professionals, there is a global cybersecurity staff gap of 2.7 million people (Alexandria 2022).

Preparing for cyber defense is more likely to be affordable than unexpected attacks, which may cost a large-scale of money. To defend a system, organizations need cyber professionals like Blue Team who work towards defending an organization by e.g., detecting attacks, isolating machines, and strengthening the network security. To reach that level of experience of protecting a system from cyber-attacks, cybersecurity students need to do hands-on practice. It is not enough to know how to protect the system because a defender also needs to be familiar with the attacking process. When a defender becomes familiar with an attacking process or acts like an attacker, he or she can better protect the system. For the ongoing race, students need to prepare themselves to gain proper knowledge and expertise in the defensive side of cyber security.

This thesis is planned to help the industry to fill the cyber security skill gap. Through the cyber defense lab exercises, students will be able to practice real-world security threats and possible solutions.

This research paper can be divided into three topics, which are scan, exploit, and defend. The first topic includes the steps that are needed to scan for vulnerabilities in a system. The second topic covers the process of exploiting the vulnerabilities that are found via scanning. Finally, the defense topic will describe the steps needed to prevent this specific attack and other attacks in the near future. These steps are implemented with various tools including Nmap, Netcat, Metasploit, Elasticsearch and Windows Defender.

2.2 Research questions

Based on the present situation in the cybersecurity field, the following research questions were chosen for this thesis.

1. What are the skills required by a cyber defender?
2. How are the required skills exercised?
3. What kind of simple environment can be built to exercise some of these skills?
4. What are the common processes and tools for a defender?

The design of the XAMK virtual cyber defense lab exercises will take shape after successfully answering these questions. The designed lab exercises will also help to develop further exercises based on the attack and defensive scenarios.

2.3 Research approach

The purpose of this study is to build a cyber defense lab exercise for XAMK Cyberlab. According to teachers, the XAMK virtuallab environment is suitable for cybersecurity studies plus its exercises, such as the cyber defense lab. Design research was chosen as the research approach of this thesis. As this thesis works towards constructing cyber defense exercises and there are constant changes and development, design research aligns well with this research (Kananen 2013).

According to Frayling (1993), design research can be categorized in three different ways, which are research for design, research into design, and research through design. Gathering resources to design something is called *research for design*. *Research into design* is when the researcher research about design. This is when the design is the subject rather than the purpose of the design. However, when a researcher is doing design or creating something to learn things by doing hands-on practice, it falls under the category of *research through design*. Research through design takes a problem outside of design and uses that design to address the problem (Frayling 1993). Research through design approach uses design as a research tool, where the design becomes a tool for knowledge creation. The objective of the thesis is to design and create cyber defense exercises in XAMK virtuallab environment. Based on research through design, the exercises will be the tools for students which will be used to learn and gain defensive knowledge in the cyber field.

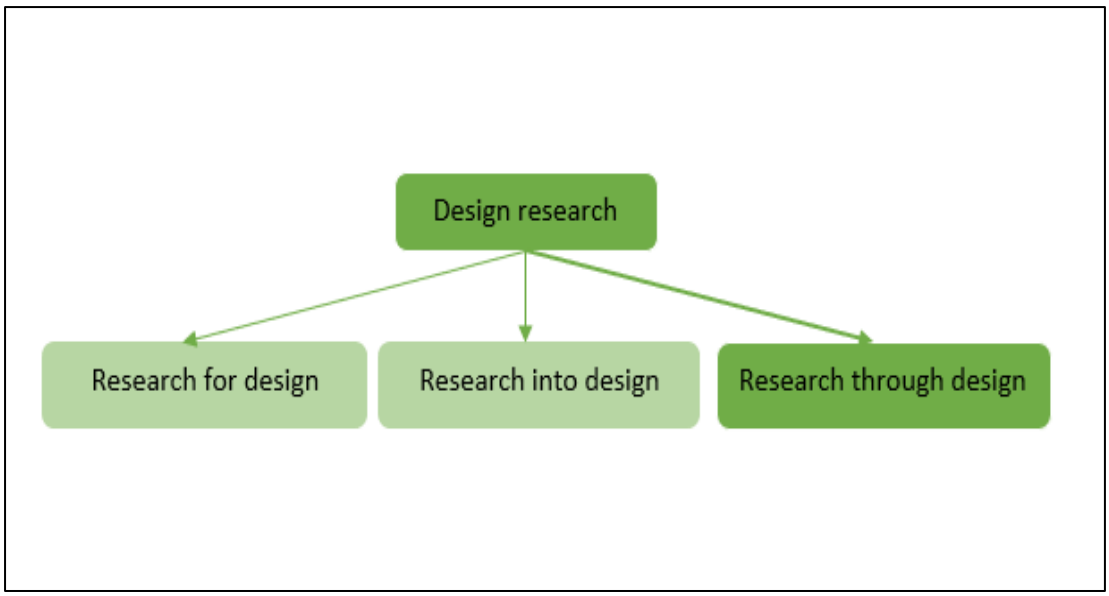

Figure 1. Different types of design research

The above picture (Figure 1) shows the different options in design research and research though the design has been picked for this research. Research through design helps us to write academic papers along with helping to deal with new technologies (Koskinen 2011), as it allows us to research recent technologies to design and create something based on the finding which can be used for learning purposes. For example, while this thesis paper was written, a virtual laboratory

exercise was created for learning cyber defense. The exercises were created based on the findings and practicing the exercises will help students to gain knowledge. This design research will create experiences that matter by ensuring that we solve real problems for real people.

This research will follow a design cyclic approach, which consists of three phases; understand, create, and evaluate. The cycle will start with the understanding phase, where it will be checked if the action will help with creating a solution (Lee et al. 2017). Understanding is counted as the input of the cycle. After understanding the scenarios, the design will be created in a virtual lab environment. Finally, the lab topology will be tested to check if it is working as expected and will help to achieve the desired result. In this phase, most of the testing is done. After ample testing, the cycle starts back from the creation phase to remake something new or maybe even to the resources to do more understanding work to create and test (Lee et al. 2017).

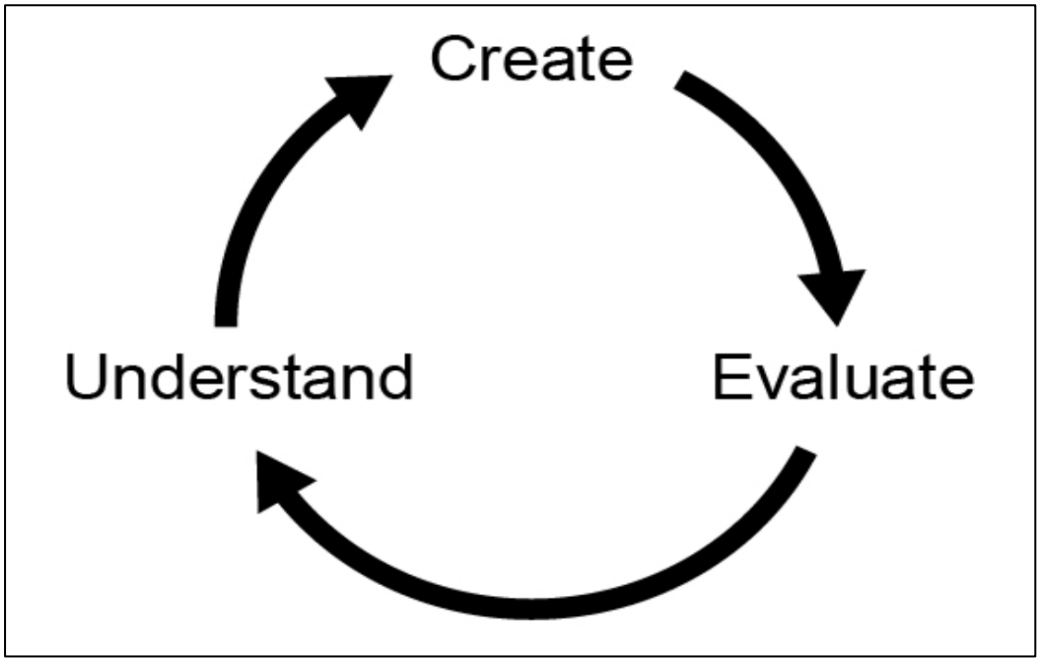

Figure 2. Understand, create, and evaluate the design life cycle

The above picture (Figure 2) shows the cycles that are being discussed. The cyclic approach is chosen to make the design process more efficient. There will be numerous design changes based on the virtual lab environment and what

students need. However, after every change, there will be plenty of testing, which will help to move the research forward.

2.3.1 Research methods

A qualitative research method is used to collect data for this design research. Research that is conducted to find out about people's experiences can be classified as qualitative research (Silverman 2021). The purpose of this qualitative study is to describe the objective of the thesis instead of making a prediction using various references. Scientific research helps qualitative research by serving as background information. It creates an understanding of real-life phenomena where understanding can be summarized into theories and models. Therefore, the cyber defense exercises were designed based on real-life security vulnerabilities using various resources. Business needs this method for developing their operations and decision-making. In qualitative research, different places can be used to search for required data and collected information can be converted into knowledge. For this thesis, data was collected from peers, XAMK personnel, and different internet sources which are then used to design exercises. The real-life security vulnerability in XAMK virtuallab environment exercises will help students to generate knowledge. By keeping all this in mind, the qualitative method was chosen for this thesis as it will provide all the answers to the questions.

2.4 Data collection

Data gathering is the most important part of the research. A qualitative method is used to collect data from different sources. This section will cover different methods of qualitative data gathering, such as keeping a diary and peer review.

2.4.1 Meeting with XAMK personnel

To fulfill the needs of XAMK Cyberlab, it was important to know about the current virtuallab environment. The XAMK virtuallab environment is a virtual training platform for students and staff. After having a couple of successful meetings with the supervisor and commissioner, the required information has been collected

about the virtuallab. During the meeting, a small testing network of devices was built in the XAMK virtuallab environment. However, some useful tips and tricks were shown to make the faster move while building exercises from scratch. After getting an overview of the virtuallab environment, it helped to collect the necessary resources for this study.

2.4.2 Gathering Internet data

The expansion of social networking with a network of computers made qualitative research methods way easier (Silverman 2013). Researchers can use the internet to collect tremendous amounts of data. Most of my data sources are from different books and official sources such as NIST, OWASP, Microsoft and Apache. The main aim of the thesis is finding the best possible ways to defend a system. The literature focused on available research papers that are being used in cyber defense.

2.4.3 Diary to track records

To move back and forth in the developing life cycle of this design research, it is very important to keep a record. Keeping notes of every step helped to fix the error and improve what from it. The most important feature of virtual environments is to save the version after making any major changes to the system, e.g., after successfully implementing the Minecraft server on a Windows 10 machine. It always helps to re-run the original version in the event of any bug or system damage. However, keeping screenshots of major changes and documenting all steps in series helped to track issues faster. For example, if there has been a misconfiguration, it can be fixed easily by checking the diary briefly.

2.4.4 Peer assessment/review

A sample of this study along with a lab demo is being shared with a few friends. After explaining the concept of this thesis, the following feedback was given:

- The topology looks good, but if it is possible to get a reverse shell from a Windows machine, that would be great.
- As Log4shell is one of the worst vulnerabilities in a few decades, it is an excellent choice.
- If the lab works the way it is planned, students will be able to learn a lot of different things.
- Hands-on practices with real-world vulnerability are always a good choice.

The feedback helped to move forward and improve the exercise by implementing a reverse shell connection.

2.5 Data analysis

The first step of the analysis began by reading and screening books along with online resources to find a starting point for my analysis. However, reading various documentation and academic articles from various sources helped to get started. The collected data, which carries tremendous amount of information, can be used efficiently to process new information (Silverman 2013). After the analysis of the data, the collection information and knowledge were ready to be applied for the use of the research. All this information helped to understand the solution to the problem. As a result, the collected data resources helped to create the exercise. However, the exercises are being changed and tested again and again based on different information from the resources.

2.6 Research outline

This study started with a meeting with my supervisor where we discussed the topic. After the topic was approved, the research plan was written, which included an introduction and research methodology. In total, there are six chapters, including the references. The first chapter starts with the introduction of this research, where cyber security and the need for cyber defense are discussed. The second chapter covers the research methodology, which started with a research problem followed by questions. Research approaches are covered in

the second chapter. It also covers the data collection methods and the way it is been analyzed.

The third chapter discusses the theoretical parts of networking and cyber security. It covers the need for cyber security in organizations. The fourth chapter covers the technical details of the Log4Shell vulnerability which was implemented in the XAMK virtual laboratory. The fifth chapter contains most of the practical parts. The building of exercises is discussed here, from vulnerable machines to attacking machines with different tools and techniques that are needed to penetrate and defend a system. However, it shows the way we need to defend our system from an attack like this. The sixth chapter is the concluding chapter where the solution is discussed. It also talks about further development methods of this thesis. The seventh chapter contains the references that are being used during the whole research.

The end product of this thesis is several exercises that are appended to the thesis but will not be published to keep it completely private to the commissioner's organization. The exercises will be practiced by XAMK students and other parties with proper rights of use.

3 WORLD NEEDS CYBER PROFESSIONALS

This chapter will cover the general theories of this study. Starting with a brief history of networking, the need for security for individuals and businesses is covered to demonstrate the importance of cyber defense. It also discusses the topics that fall under the umbrella of security.

3.1 Networking history

A few decades ago, there were no networks, and we did not have the internet (Tarnoff 2016). People used to use stand-alone computers that they controlled in their homes. In 1969, the American Rescue Plan Act (ARPA) introduced a computer network, and it is called ARPANET (Tarnoff 2016). When two or more devices communicate together using communications protocols (e.g., IPv4, IPv6, UDP, TCP, QUIC) to exchange data or share resources is called a computer network. Protocol plays a bigger role in networking, as it is considered the transport medium which allows to transmission of data between devices on the same or different network. For Example, Internet Protocol (IP) is used to connect devices across the network and Transmission Control Protocol (TCP) is used to create a session between the source and destination to transmit data. According to Funet (n.d.), the Finnish University and Research Network, Arpanet was built to communicate for academic and research purposes through a fixed link. To connected two different networks together, ARPA researchers Robert Kahn and Vint Cerf designed a protocol that could carry data from one network to another (Tarnoff 2016). The protocol started working back in 1976, and it made it possible to communicate between two networks which gave us the Internet (Funet n.d.). In short, the internet is a combination of many networks. For example, if we want to visit our well-known service provider LinkedIn, we must pass through different networks (routers) to reach the original server. The router is a networking device that is used to forward data packets between networks.

The picture below (Figure 3) is a demonstration of connectivity from my network to the LinkedIn server through different routers. Ping commands are used to see

if the server is responding to my request and tracert is used to know how many routers it takes to reach the destination.

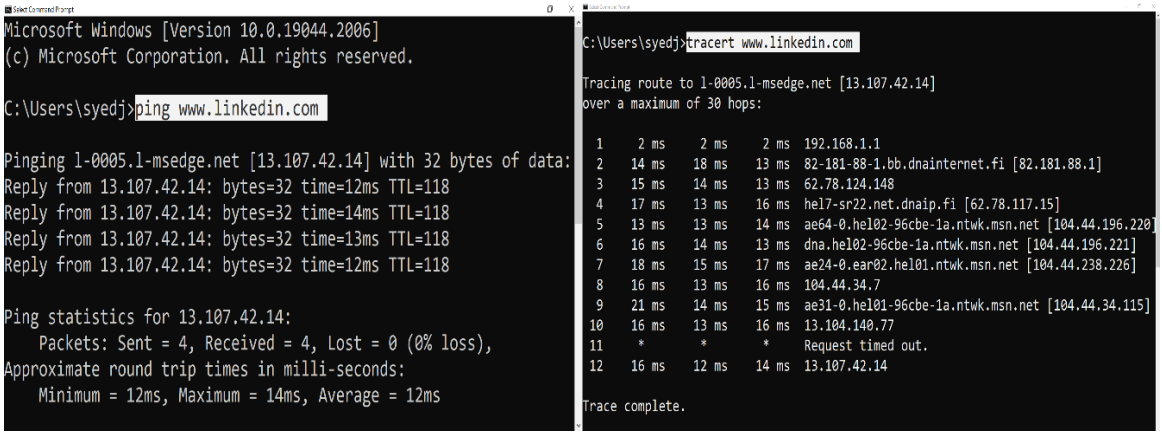

Figure 3. Networking connectivity from a Windows machine to service provider LinkedIn

According to University College London (2022), Professor Peter Kirstein known as the “father of the European Internet” played a role in the invention of the internet. He is the first person to add a computer on the ARPANET which could communicate outside the US (UCL 2022). The architecture of the ARPANET was described by Professor Peter Kirstein which is shown below (Figure 4). The architecture contains some IMPs (Interface Message Processors), which is a type of packet-switching computer which was connected via superfast 56 Kbit/s lines (Funet n.d.).

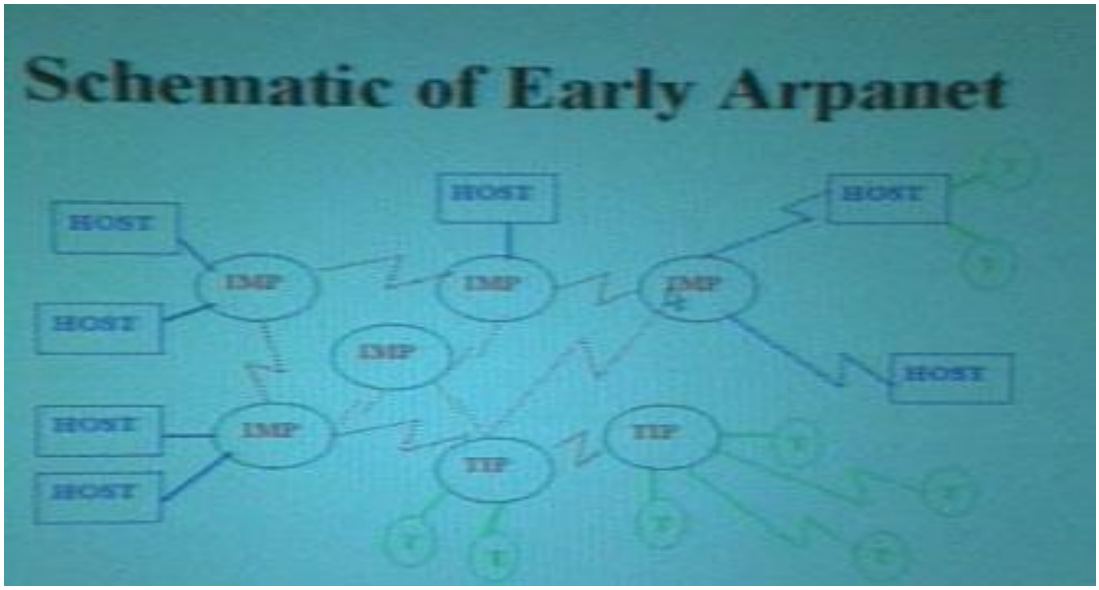

Figure 4. The network architecture of ARPANET (Funet n.d.)

Nowadays, the network is more complex and considerably more extensive than in earlier decades, as billions of devices are getting connected to the internet. In the year 2022, approximately more than 13.1 billion IoT devices connected to the internet (Vailshery 2022). For example, due to ever-expanding networks of devices, there is already an IPv4 address (Internet Protocol version 4) shortage. Internet Protocol address such as IPv4 is used to identify the individual device and it is used to communicate from one network to another. To overcome the shortage of IPv4, Internet Engineering Task Force (IETF) developed a newer version of the Internet Protocol which is IPv6 (Deering et al. 1998). As a consequence of rising the number of devices, there is an increase in cybercrime too.

3.2 Introduction to cyber security

The practice of securing internet-connected components such as CPU, RAM, Hard drives, Software, applications, sensitive data/information, and the network itself, from unauthorized access by a threat actor using various tools and techniques is called cybersecurity. Cybersecurity is not only about responding to attacks, but also about making future-proof systems, applications, users, and networks to protect against threats (Ozkaya 2019). In earlier days, there was not much risk, and that is how computing started, and the internet began (Ozkaya 2019). At the beginning of the internet, it was a trusted network, and most communication was not encrypted (Meier-Hahn 2017). Since the 1970s, the security landscape completely changed as attackers got advanced technology with more tools and techniques (Ozkaya 2019). At the end of the 1970s, the well knows hacker Kevin Mitnick got unauthorized access to the network of Digital Equipment Corp (DEC) (Ozkaya 2019). Nowadays, there are thousands of malicious actors on the internet trying to intercept data, trying to compromise servers, trying to access systems, and generally do bad stuff. There is always a risk of being infected by a virus, compromised by ransomware, or whatever.

“The only truly secure system is one that is powered off, cast in a block of concrete, and sealed in a lead-lined room with armed guards – and even then, I have my doubts.” (Dewdney 1989, 23) This quote was written by A.K. Dewdney

in the year 1989 about the security of computer systems. It was published in Scientific American the popular science magazine and it was written in “Computer Recreations: Of Worms, Viruses and Core war.”

The rise of smart devices like IoT, smartphones, and other devices will never end. With the steady rise of electronic devices, there is always a risk of being compromised. According to AV-TEST (n.d.), there is a remarkable rise in malware infection in recent years which is seven times more, compared between the years 2012 and 2022. As computers are connected via the internet and data are stored on our computers. This data got to be stored securely, it got to be protected, it got to be stored in a way that we can rely upon it and know that information is not going to get compromised. To do that we must take certain measures such as controlling access and securing the data.

The internet is a network made up of numerous entities. They are called autonomous systems that are all kind of glued together and create this friendly type of network (Tarnoff 2016). To access different services from the internet we are using client software such as Google Chrome and Microsoft Edge. When we browse a website, we are passing through several routers that are owned by other companies we do not even know. If we want to access the CNN website, the CNN server will know that we are accessing their service. Beside CNN, there are other parties who might know that we went to CNN website. At the network level, other people do know that we went to CNN. To see the whole process, we can turn on the traceroute as shown in Figure 3 and check how many routers we are passing to reach our destination. The further away the server is the more routers we must pass through. However, the communication between the computer and the CNN server is encrypted but the CNN web page is not made up of just the CNN server but from several other servers.

The picture below (Figure 5), shows the overview of the CNN website and Ghostery report. Client software Google Chrome has been used to visit CNN.com and Ghostry browser extension has been turned on to see different servers that are providing services in the CNN web portal. Ghostery is an open-source privacy

and security browser extension which is used to block unnecessary traffic. Ghostery blocked 22 tracers from the CNN website which are not necessarily important and might be malicious. In these types of scenarios, there is always a risk of compromising privacy. As a result, it is very important to be careful while using the internet, especially when visiting untrusted sites.

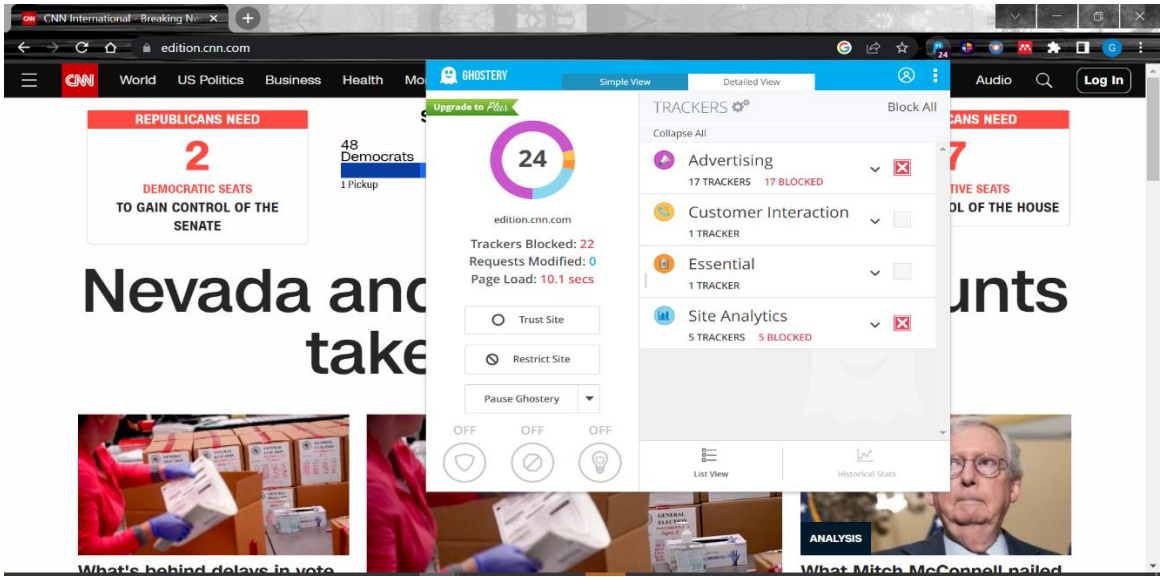

Figure 5. Ghostery report on CNN website

Connecting a computer to a network or the internet itself is giving an opportunity to threat actors. Threat actors can gain access to a system using various methods such as using social engineering techniques or exploiting a vulnerability of the system or applications. At present, we are mostly dependent on software systems such as Microsoft Office, Email, Chrome, web applications, Wolt, Uber rider, SolarWinds Orion, Apache, Minecraft, and billions more. Software is made up of code and there is always a chance of having software defects (McGraw 2004). Software's connected to our system, systems are connected through a network and ultimately the network connects to the internet (McGraw 2004). Giving the best opportunity for attackers to attack easily instead of physical access. Secure programming is very important to prevent defects as early as possible. Threat actors can exploit software defects using various tools and techniques to take control of a system. According to McGraw (2004), security holes in software are common but internet-enabled applications are facing the most intrusion. In this research, an intentionally vulnerable software i.e., Minecraft

Server will be used to demonstrate intrusion against the software defect and the possible ways to detect and defend against such intrusion.

3.2.1 Information security model

Through different security measures, our assets such as data, information, and system are protected. To protect different assets Confidentiality, Integrity, and Availability (CIA) along with a security framework is crucial for information security (Cole 2013). CIA triad helps organizations to develop better security policies that help to protect data from data violation (Andress 2015). Information security is the practice of protecting information against unauthorized access. The term information security is like cybersecurity but not to every extent. As cybersecurity deals with protecting against attacks and information security focus on securing information.

Confidentiality is a component of privacy. It makes sure the assets are not leaked or disclosed to unauthorized parties (Cole 2013). *Integrity* deals with data modification. It makes sure the assets or data is accurate and is not modified by an authorized party (Cole 2013). Assets or information must be available when needed and it is confirmed by a*vailability*. All three components of CIA triad must be guaranteed to make a secured system or application (Andress 2015).

There are different types of attacks that can harm the CIA triad. For example, an eavesdropping attack can harm confidentiality, data poisoning can compromise integrity and denial-of-service can affect availability.

3.2.2 Cybersecurity frameworks

Cybersecurity frameworks provide guidelines for organizations to better manage the security process and reduce cybersecurity risks (NIST 2018). There are some main frameworks such as PCI DSS (Payment Card Data Security Standard), ISO 27001/27002 (Standard Organization for Standardization), CIS Critical Security Controls, NIST (National Institute of Standards and Technology), COBIT, HIPPA and GDPR. It is important to use the framework to improve the critical

infrastructure of an organization (NIST 2018). The framework can be implemented in stages and changed to meet organizational needs (NIST 2018).

3.2.3 Components of the framework

The NIST framework can be broken down into three primary components such as the Core, Implementation Tiers, and Profiles. The NIST framework Core has five different functions such as identify, protect, detect, respond, and recover. Using different functions, Core helps organizations to reduce their effort in finding, managing and fixing security problems easily (NIST 2018). Implementation Tiers help to identify how well organizations are following the rules of the Cyber-Security Framework (CSF) (NIST 2018). Profiles help to distinguish between the current situation and the desired target state of cybersecurity activities of an organization (NIST 2018).

3.2.4 Framework functions

There are five different Core functions in the cybersecurity framework. Each function deal with a specific task such as:

- **Identify**: Helps the organization to identify its assets.
- **Protect**: Helps to protect the identified assets.
- **Detect**: This function helps the organization monitor the assets to detect intrusions.
- **Respond**: Helping the organization to respond when a breach happens.
- **Recover**: Helping organizations to get the business up and running after a cyber incident.

3.3 Protecting data

An enormous amount of data that are being generated are pulling threats. Data are generated by our Phones, computers, Smartwatches, CCTV, Video Surveillance Systems, Information Monitoring Systems and Aircraft. The generated data can be in three different stages: at rest, at transmission, or in use (Hakkala et al. 2022). Malicious intruders are always behind the scenes for

making bad use of our system and ultimately data as systems are admitting to weaknesses. Such as, due to lack of designed-in security in Automatic Dependent Surveillance-Broadcast (ADS-B) technology makes it vulnerable to different attacks (Jamming, spoofing, flooding, coordinated and DoS.) (Wu et al. 2019). ADS-B technology is used in aircraft to find the accurate location. ADS-B Is insecure due to a lack of authentication and less-data-bit (encryption) features (Wu et al. 2019). According to Wu et al. (2019), due to the insecurity of this technology, transmitted aircraft data will be insecure and will affect confidentiality, integrity, and availability. To win against malicious actors and to save businesses from data breaches, protecting data is a must-to-do task.

3.3.1 Data at rest

Improvement of data safety is as important as safeguarding the king from a war. XAMK cyber defense lab exercises have been implemented in a way that students can practice stealing data at rest, in transit, and progress. According to Hakkala et al. (2022), Data that is stored on a system (e.g., hard drive) and not actively used is called data at rest**.** An intruder can break into an information system to access data at rest using different techniques such as exploiting Log4shell vulnerabilities. According to Cole (2013), data at rest can be protected using two different options such as encrypted file or folder and full disk encryption. Strong encryption can be used to protect data at rest but to use data it needs to be decrypted and it will make it vulnerable when data is in use (Hakkala et al. 2022). Data can be protected via homomorphic encryption to make it difficult for adversaries to access (Hakkala et al. 2022). Homomorphic encryption does not necessarily require decrypting data before use as it allows users to make changes to encrypted data without first decrypting it (Fisher 2018).

3.3.2 Data in transit

Data that are actively being moved from one place to another can be classified as data in transit (Hakkala et al. 2022), for example, log in to social media accounts with user details. Attackers can take advantage of different vulnerabilities to gain access to a system or traffic to achieve the goal of capturing data in transfer. In

the year 2022, one of the most dangerous Application Programming Interface (API) vulnerabilities has been reported and it is called ‘Spring4Shell’ (Osborne 2022). Nowadays, APIs are integrated everywhere to transfer data from system to system. According to Knight (2022), hacking APIs can even take down an entire country because most of the countries are being powered by APIs i.e., Industrial Control Systems and modern cars. Such attacks can be used to capture data at rest, in transfer, and even in use. Information that is transferred over an untrusted network is very critical to protect. According to Cole (2013), using a trusted VPN such SSL VPN can help to ensure data protection while it is passing through an untrusted network. Data in the transfer can be protected using secured communication methods such as using modern TLS version 1.3 (Hakkala et al. 2022). There are always vulnerabilities in different protocols, but it is important to use the strongest encryption protocol possible.

3.3.3 Data in use

Data that is actively used for computational needs are considered as data in use e.g., providing user login input for social media accounts (Hakkala et al. 2022). The attacker needs control over the system to check data in use, and it can be achieved via exploiting vulnerable server software or by malware (Hakkala et al. 2022). For example, one of the popular GPS tracking devices made by the Chine-based company MiCODUS had vulnerabilities in their API server, GPS tracer protocol, and web server of MV720 GPS tracker (Bannister 2022). According to Bannister (2022), these types of vulnerability are life-threatening as attackers could use GPS data to monitor a car and can suddenly stop the vehicle on a dangerous highway. As a result, it Is important to safeguard the system and software from an intruder.

3.3.4 Data encryption

Secret writing using mathematical formulas has been used for centuries to protect information and communication. The goal of secret writing is achieved using code and the whole method is called cryptography. The process of hiding or encoding information to protect it from unauthorized access is called

cryptographic encryption (Anderson 2021). According to Anderson (2021), due to strong encryption, cryptography can provide confidentiality, integrity, and authenticity. Nowadays, cryptography is being used almost everywhere such as for Internet communication, Data storage. E-commerce, Blockchains and Mobile systems.

Data encryption can be in different forms such as symmetric, asymmetric, and hash. The symmetric cryptographic algorithm uses only one secret key for both encrypting and decrypting data (Andress 2015). Examples of such symmetric algorithms are AES, DES, 3DES, Twofish and RC4. According to Anderson (2021), the symmetric algorithm is considered fast, and it is mostly used for large data encryption. On the other side, asymmetric algorithms use different keys for both encryption and decryption (Cole 2013). Asymmetric encryption is also called public key encryption. The public key is used to encrypt data and the private key is used for decrypting (Cole 2013). Some examples of asymmetric algorithms are RSA, ElGamal, Diffie-Hellmann and Elliptic curve. This algorithm is used for key exchange, and it is resource intensive with slow performance (Andress 2015). Cryptographic hashing algorithm or hash function uses mathematical formula where it takes data as input to produce a fixed-size string called hash (Andress 2015). Hashing data is one-way and it is mostly used for storing data securely (Andress 2015). After hashing a chunk of data, it can be modified, but the modification can be detected as the signature will not be valid after modification (Anderson 2021). Examples of hashing algorithms are MD5, SHA-1, SHA-256, SHA-384 and SHA-512.

Cryptography does not stop cyber-attacks as threat actors are also tempering cryptographic systems using cryptoanalysis (Cole 2013). Cryptoanalysis is the method that is used to break into systems that are being made using cryptography (Cole 2013). Along with cryptoanalysis, encryption can be tempered using brute force and side-channel attacks (Cole 2013), for example, trying to decrypt all possible keys using various brute-forcing tools to find plaintext.

Practicing cryptology can help in understanding the process of cryptographic encryption and the way it is broken. Cryptology is the combination of cryptography and cryptoanalysis (Andress 2015). As it is important to understand both sides of it to protect systems against adversaries. Implementing modern cryptographic algorithms can be challenging but can secure systems and applications against all adversaries (Anderson 2021).

3.3.5 Detecting outbound traffic

Cyber defense is not easy as a cyber offense. The offensive side of cybersecurity is about finding one or more vulnerabilities. On the defensive side, professionals need to find all possible weaknesses to fix them before some break-ins. Due to modern attack types, there is always a risk of compromising systems. According to Cole (2013), organizations should always train employees along with implementing defense in depth to deal with the advanced persistent threat (APT). As APT is a sophisticated attack where unauthorized actors remain undetected for a long period to steal critical information (Cole 2013). According to Cole (2013), there should be a security boundary between corporate networks and outside networks and organizations should implement outbound detection and inbound prevention.

Network traffic that is generated from an inside host toward the internet or untrusted networks is classified as outbound traffic. According to Cole (2013), an organization can improve its security posture by implanting outbound traffic monitoring and detection. The outbound connection can be monitored by looking into the domain name or destination IP, the length of the connection, the amount of data being sent outside, and the number of packets (Cole 2013). Along with monitoring the traffic, it is important to implement protection on devices (e.g., Anti-Virus software and firewalls) and implement end-point protection on operating systems (e.g., Elasticsearch).

3.3.6 Preventing inbound traffic

Threat actors are mostly running their operations from outside the network. There are many different possible ways to gain access to the internal network and the access can also be seen in the network traffic. Malicious traffic is either transferred through a wireless or wired medium. As a result, it is important to check and drop out malicious traffic before it affects the internal network. Identifying and preventing malicious traffic before it harms the internal system is classified as inbound prevention (Cole 2013). If malicious inbound traffic is not prevented, the adversary will have complete access to the network and ultimately systems. According to Cole (2013), if key tools are not present, traditional defensive technology is not enough to secure the system against APT. New attack types are always changing, and cyber defense tools need to be implemented accordingly to protect against new threats. After all, traditional technologies are still valuable to add an extra layer of security. Some of the earlier prevention technologies that are still being used widely are Network-based firewalls, Intrusion Prevention Systems (IPS) and Data Loss Prevention (DLP).

Some of the modern technologies are based on pattern matching (signature), and rules such as Snort or Anti-Virus software. According to Cole (2013), application-aware systems that check and monitor traffic can reduce the risk of APT. Organizations should invest in behavioral monitoring systems along with application-aware devices and anomaly analysis using various tools (Cole 2013).

3.4 Cyber defense for businesses

People used to use computers peacefully without any worry about security risks. Now it is time to worry about security and understand the risk in the system that we are using. Nowadays, the computer is used for different typs of work, which means all our data is stored in that computer. Unauthorized access to it may result in identity theft, where our personal information gets compromised (Ozkaya 2019). For businesses it is more damaging e.g., if a threat actor gets access to the formula of penetrating strike bomber B-21 Raider, it can become a massive threat against a nation. There are numerous businesses that are based on the

value of their intellectual property. If that value is lost, the company would go out of business. So, companies need to defend that data. As, organizations are surviving on data which can be from customers, employees, or software. To protect business data, it is important to identify critical information. After successfully identifying the information, it needs to be located and checked for access control (Ozkaya 2019). Protecting data is not as easy as creating a large amount of data. Data protection needs various measures to protect data from intruders. According to Ozkaya (2019), an organization needs to create proper segmentation of their network to protect critical information such as creating a DMZ network, Private network, and Middleware tier.

In most cases, human hacking can be the first step before targeting a system (Anderson 2021). Threat actors plan the attack way to make sure the plan goes as expected. Among all the different types of hacking, social engineering is the most common type of hacking and people always fall for this (Ozkaya 2019). For example, tricking a person to click on a malicious link sent via email or text message. Social engineering can be done in various ways such as manipulating humans' minds to plug a malicious cable, USB, and CD. Security was not ignored and cannot be ignored in the future as the cost can be significant. People need to be trained to fight the battle against social engineers (Anderson 2021). Because, due to the rise of different attack techniques, attackers have the capability to apply social engineering techniques against victim in order to get business information. Collected information can be misused to target the business. As a result, training people will help to reduce the problems. The training can be done in different ways such as: doing it on your own, attending university programs, or attending employer training programs.

Along with training people, companies also need to invest in securing their infrastructure both physically and logically. As intruders can access both methods to cause harm. According to Anderson (2021), security engineers are mostly focused on securing electronic devices, but it is not enough as physical access can help attackers to bypass a security device. Examples of security devices are CCTV, security alarms, sensors, and others. Protecting all different types of

electronic components falls under logical security control such as End devices, routers, switches, software, and others (Anderson 2021). Different tools and techniques are being used by security professionals to protect the complete logical security of an organization (Anderson 2021). Due to different security risks, there is always a need for cyber professionals in the business.

3.5 Different types of hackers

There are different types of hackers, and they can be classified predominantly by their goal. Some hackers who hack for their state or nation are called state-sponsored hackers and some hacker groups that are targeting industries or opposite parties for political causes are considered hacktivists. In public, hackers are often known as malicious cyber actors but, there are good and bad hackers (Roberts 2022). Hackers can be classified with different hats (Roberts 2022).

The Picture (Figure 6) below shows six different types of hackers. Some of them are commonly seen such as White hats, Black hats, or red hats but others are not that common.

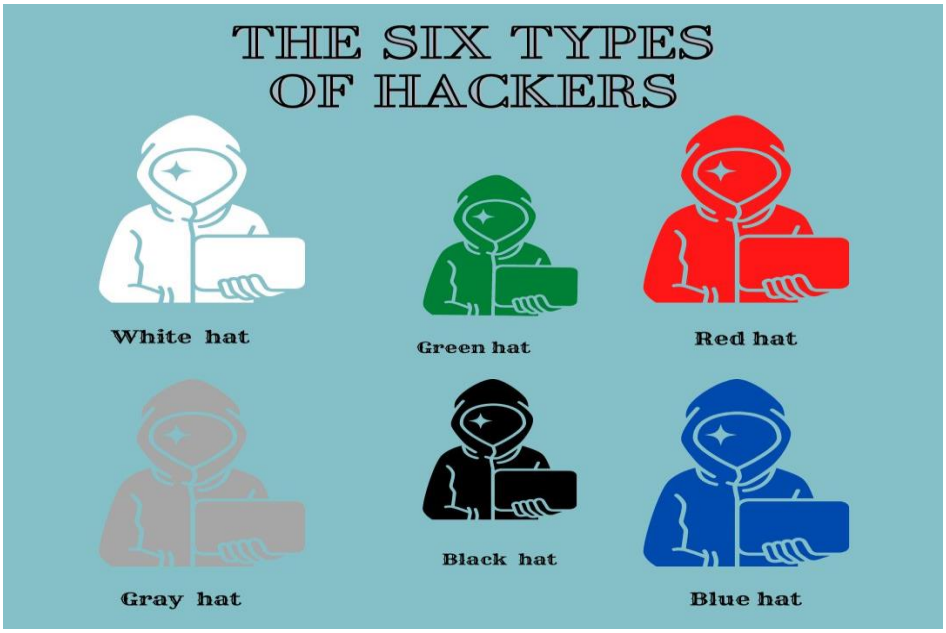

Figure 6. Six different types of hackers

- **White hat hackers**: Those who penetrate the system ethically with permission, to detect vulnerabilities (e.g., zero-day) are called white hat

hackers or ethical hackers. They are the opposite of white hat hackers as they do not exploit for malicious intent. They might work against black hat hackers to protect organizations before or during a cyber incident.

- **Blue hat hackers**: They work for revenge either for personal satisfaction or can be others.

- **Red hat hackers**: Attackers that use cyber-attack toward black hat hackers either for attacking or stopping them are called red hat hackers.

- **Green hat hackers**: They are new to hacking and usually called Newbie hackers who are enthusiastic to learn and become experts. Usually, they are not a threat to anyone.

- **Gray hat hackers**: They are a mix of both black and white hat hackers. They may penetrate the system without permission but normally they do not cause harm.

- **Black hat hackers**: Attackers that are aiming toward their agenda such as earning money are considered black hat hackers. They gain access to the system without permission to exploit known or zero-day vulnerabilities. Cyber-attacks that are happing all around the world are mostly done by black hat hackers.

3.6 Different types of attack

Attackers are not always following the same route to reach their target. There are different types of attacks that are used depending on the end goal. Some common types of attacks are:

- **Phishing**: This is a type of social engineering attack, and it is used to trick people into clicking on a malicious link. After a successful click on a link, an attacker can gain access to the system and do different bad stuff such as stealing sensitive data (Cole 2013).

- **Malware**: This is a type of malicious software especially designed to cause harm to the system. Malware have different capabilities based on its architecture. It has different varieties such as keyloggers, Trojans, spyware, ransomware, viruses, and worms (Tietsort 2022). In general, attackers target users to click on a dangerous link which opens a way for malware to run inside the system and cause harm such as encrypting files and installing files (Cisco 2022).

- **Denial-of-service (DDoS)**: Attack that target systems, servers, or network with a large number of network traffic to burn out bandwidth, and services and ultimately shutting the system (Cisco 2022). After a successful DDoS attack, systems are unable to receive legit traffic. For example, a DDoS attack on websites can harm the server, and users will be unable to access that service (Tietsort 2022).

- **Man-In-the-middle** (MitM): When an attacker resides in between two-person communication or network is counted as a Man-in-the-middle attack. MitM attack is also called an eavesdropping attack (Cisco 2022). An attacker can interrupt the traffic to filter and steal data (Cisco 2022). Mostly happens when someone accesses unsafe public Wi-Fi or after a malware attack on a system (Tietsort 2022).

- **SQL Injection**: Structured Query Language (SQL) injection is a server-based attack where the attacker inserts malicious code as input to find sensitive information (Cisco 2022). For example, after finding a vulnerable website, an attacker can insert malicious code into a search box or as input to get information.

- **Zero-day exploit**: An exploit that is made based on a newly discovered vulnerability is called a zero-day exploit (Cisco 2022). Exploits are made to disclose the vulnerability before a solution comes into the market (Tietsort

2022). For example, a coding error in software might lead to zero-day vulnerability.

- **Drive-by Download**: Cyber-attack that requires user interaction to visit a malicious site or download malicious software to harm the system is called a Drive-by download (Tietsort 2022).

The attack can be based on a system, software, or web application based. Due to the rise of web services, there are many critical security risks to web applications. According to OWASP Foundation Inc (2022), In the year 2021, there has been a list of the ten topmost web applications security risks. Some of the vulnerability types are Broken Access Control, Cryptographic Failures, Injection, Insecure Design and Security Misconfiguration.

3.7 Different phases of hacking

Different types of hackers use different attack types, but they also follow different attack phases. Ethical hackers follow given guidelines to help in their attacking steps which are called cyber kill chains. These rules are not strickle followed but will help to stay on track. According to lockheedmartin (n.d.), there are seven separate phases in the cyber kill chain to enrich a cyber analyst's adversary techniques and procedures.

Seven phases of the cyber skill chain:

1. **Reconnaissance**: This is the phase to research and select a target for moving into the next phase of an attack.
2. **Weaponization**: Preparing exploits and other necessary payloads for delivery using some methods.
3. **Delivery**: A method of sending the weapon or exploit to the target system.
4. **Exploitation**: After successfully delivering the exploit, it will be triggered to exploit the vulnerability.
5. **Installation**: After the installation of the exploit, it will allow a backdoor from the victim’s system.

6. **Command and control**: Providing enough control to the attacker so that he/she can remotely control the system using various commands.
7. **Actions on objectives**: Attacker works to fulfill the objective of the attack which can be from stealing data to damaging a system.

3.8 Security best practices

Securing an organization's data and systems is the responsibility of cyber professionals. Cyber professionals are also working towards securing the data of everyone outside of their organizations by implementing security in devices. For example, securing home routers, securing operating systems (i.e., Windows, macOS), securing applications and websites. But this is not enough to secure our data and privacy unless we become aware of different common security practices.

Some of the common security practices are as follows:

- **Not clicking suspicious links**: Malicious actors are using social engineering techniques to send links via email, text messages, or links that may hide inside website ads. Clicking malicious links might download harmful executables on the system and might give the system access to the threat actor (Tietsort 2022). It is recommended to not click on any links that look suspicious.

- **Using strong passwords**: Strong passwords are not easy to guess or break. Easy passwords can easily be broken using different brute-forcing tools and various password dictionaries. It is not a good practice to use the same passwords in different places. It is recommended to use long passwords using different characters and changing them often (Tietsort 2022). The password manager can be used to remember the password instead of saving it on paper or on the computer itself.

- **Updating system**: Updating your system is very important as OS vendors are always patching and improving the system posture (Tietsort 2022).

Keeping the system backdated by not updating the system might leave the system to attacks (Andress 2015).

- **Updating applications**: There might be vulnerabilities in any specific application, and it might be patched by the vendor. Leaving backdated applications might give a chance to hackers to exploit that existing vulnerability (Tietsort 2022). For example: using a vulnerable version of Minecraft server. As a result, it is important to update applications when latest updates are available.

- **Defender**: it is important to use default defender as it helps to defend the system in many ways (Microsoft 2022). For example, Microsoft defender helps to protect against different cyber threats.

- **Anti-Virus software**: Using antivirus software adds one extra layer of security to the system. Modern anti-virus also helps to protect the system against accidental clicking on harmful links (Tietsort 2022).

- **Unnecessary services**: To reduce the attack surface It is important to not run unnecessary services on a system (Andress 2015).

- **No updates available but vulnerable application**: In case of any zero-day vulnerability, the vendor might be working toward releasing a patch. While waiting for the patch, it is important to disable the software or specific function (Tal 2021). For example: Disabling affected versions of Apache Log4j versions (Tal 2021).

- **Sensitive information in public**: It is not a good idea to share sensitive information in public such as Birthdate, travel details, or others. Leaving useful data in public leaves a point for a hacker (Tietsort 2022). It will be easier for them to target an attack.

- **Unnecessary data**: It is a good practice to delete all unnecessary information and sensitive data when those are not used (Andress 2015).

- **Learning security**: It is a good practice to learn about security and teach family and others. It will help us and our society to become aware of cyber threat actors. According to Andress (2015), companies need to train employees to be aware of cyber incidents.

Humans are the best firewall ever and assigning our security policy will help us to become stronger. Being a strong cyber-aware person will help the organization and society to become safer.

4 LOG4SHELL VULNERABILITY

XAMK Cyberlab virtual exercises were designed to carry Log4Shell vulnerability. The vulnerability was created through a vulnerable Minecraft server to demonstrate the effect it can bring on a game. Due to Log4Shell's easy exploitation techniques, a simple payload sent from client software can harm the vulnerable system. After all, the Log4shell vulnerability was chosen as it is one of the biggest vulnerabilities of the last decades with a CVSS score of 10.

At the beginning of December 2021, a new log4shell vulnerability was found and disclosed. Log4Shell (or CVE-2021-44228) was a zero-day vulnerability that authorize attackers to remotely control servers and possibly install malware (Zugec 2022). According to the CVSSv3 Vulnerability Assessment scale, log4shell received a score of 10 out of 10. The flaws were discovered in the well-known Apache open-source logging library called log4j, which is a portion of the Apache Logging project (Juvonen et al. 2022). Log4j library provides additional features for logging, for example, log levels, mechanisms for writing to different log files, templates for scrolling logs, and more (Apache n.d.b.). The vulnerability has existed since 2013, but it was noticed and began to be used in December 2021 (Jerbi 2021). The Financial Times (give full in-text reference) notes that with the help of log4shell, hackers carry out about 100 attacks per minute on various services and applications around the world. Since December 2021, Log4Shell are still being targeted by malicious actors. According to Villaluna (2022), there are 1,467 Log4Shell vulnerable instances around the world. Due to the high use of this popular Apache library, millions of businesses, government agencies, and cloud services are being affected. For example, between June to mid-July 2022, a U.S. Federal agency found an advanced persistent threat (APT) on their network where Iranian state-level actors used Log4Shell exploit against VMware Horizon servers (CISA 2022).

4.1 Apache open-source project

Apache is one of the most used free & open-source cross-platform web server software (Zugec 2022). It is developed and maintained by an open community of

developers working under the Apache Software Foundation team (Apache n.d.c.). Apache Software Foundation is responsible for all these open-source projects such as Logging Services. Open-source projects are developed by the team and Apache users contribute to the project in the form of bug reports of feature suggestions through the developer form (Apache n.d.c.). However, the Apache Logging Services project deals with the java-based logging facility Apache Log4j, which was originally written by Ceki Gülcü (Founder of several Open-Source projects) (Apache n.d.c.). Log4j was initially released on 8th January 2001 by Apache Software Foundation and kept growing with its versions such as log4j 1 and log4j 2. (Apache n.d.a.). However, Apache Software Foundation is holding the copyrights on Apache code as well as logging services code (Apache n.d.c.).

4.2 The need for Log4j

To log something in Java, there are different options for logging frameworks. The most popular ones are logback, log4j2 and log4j. (Apache n.d.a.). Among all these libraries, Log4j is a common Java logging library that users can use for logging information from their code (Zugec 2022). Log4j is used to log messages to a file. For example, in case of a program malfunction, the logging function will create a log message to a log file which then can be looked up for troubleshooting the problem. The developer just needs something to log messages and headers. For that, an object is needed, which has log methods. To log something, a user just needs to instruct the object for logging.

Figure 7 shows the way we use the logging library to instruct logging messages in the logger file.

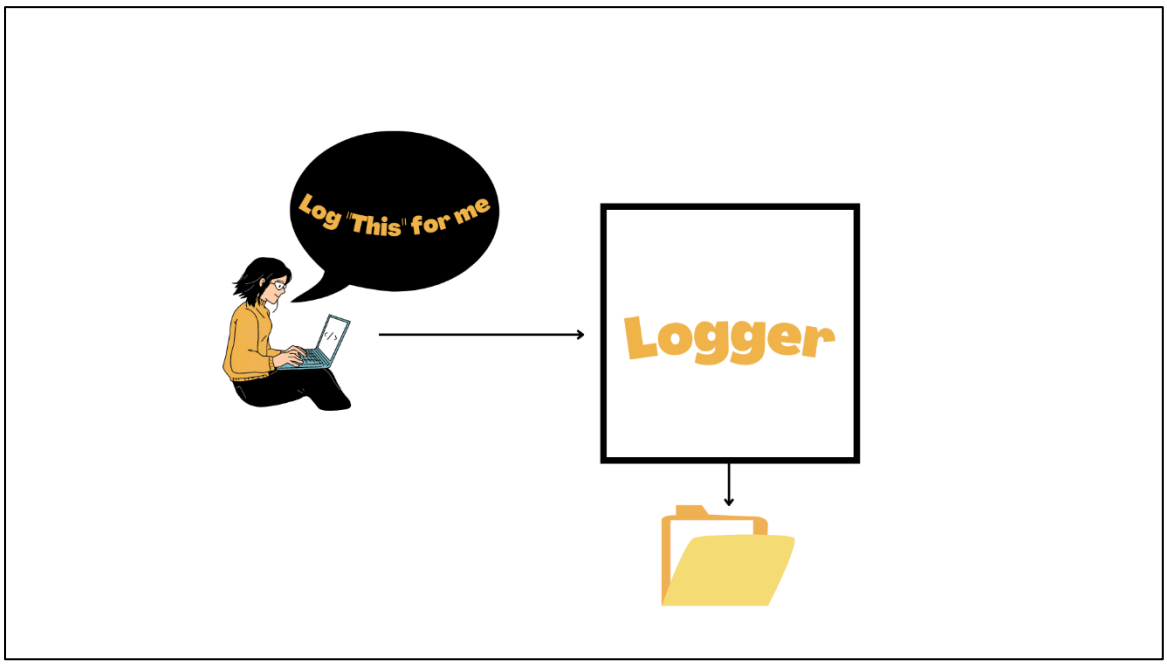

Figure 7. A simple example of a logger to store logging messages in a logger file

Log4j was used without any severe security concern for many years till the end of the year 2021. There was a major vulnerability that was hiding inside the Log4j library. It was and is one of the major security issues for the world, as any Java application that uses Log4j can be compromised unless the patch version is used (Microsoft 2022). From the year 2021 to 2022, different versions of Log4j have been exploited. According to Juvonen et al. (2022), Log4Shell vulnerability can affect different IoT devices, embedded devices, critical infrastructure, and cyber-physical systems. Due to the severity of Log4j, companies had to find and fix their Log4j adaptation and update to the most up-to-date version. On the other hand, adversaries were abusing the vulnerable target before it gets fixed. Companies might check their application and come to the conclusion that the Log4j library is not used anywhere so it is good to use the application. In reality, Log4j is such a prevalent library, that indeed in case of companies might be using it indirectly. For example, companies might not be utilizing Log4j directly but may well be depending on another library that calls Log4j for logging or that library might depend on another library that calls Log4j. According to Tal (2021), more than 60% of java applications that they checked, indirectly call the Log4j library and not depending on it directly.

A program might be using a different logging library rather than Log4j but in many cases, the user logging library may be using Log4j indirectly. Figure 8 shows an example of calling the Lo4j library indirectly.

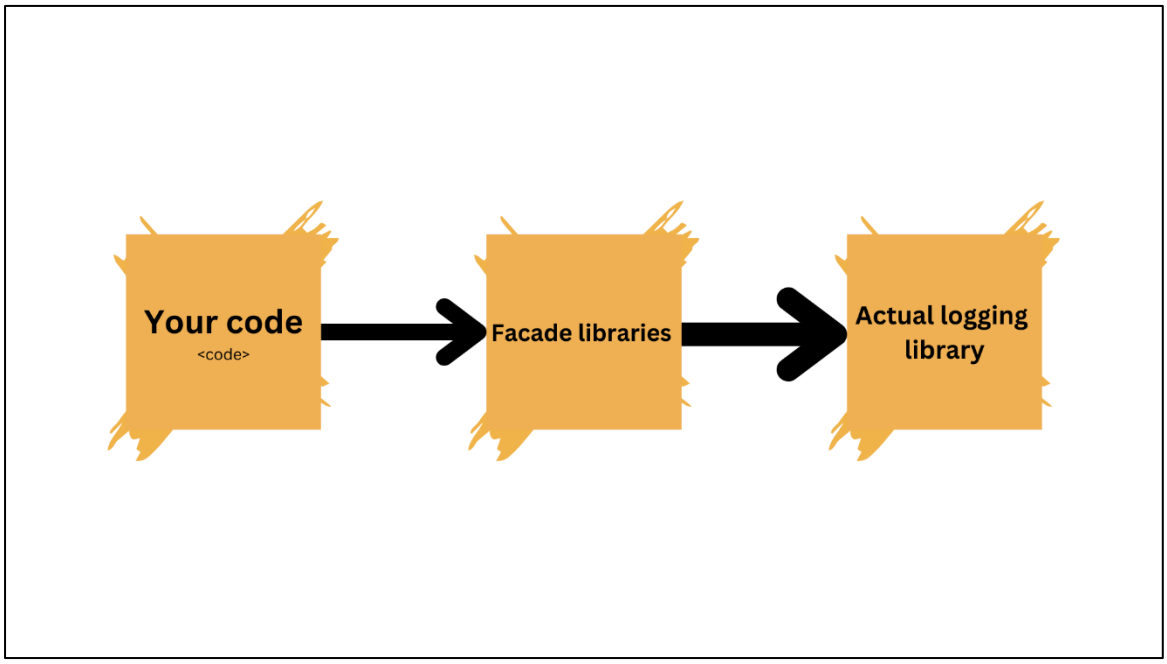

Figure 8. Example use of log4j indirectly

Facade libraries contain no functionality, they just have interfaces. This library provides a standard API that can be used to do logging (Apache 2022). Then these façade libraries call another library to do the actual logging (Apache 2022). While writing programs, the developer does not need to think if log4j or any other logging system is being used or not. The developer simply uses facade library API in their code and then a jar is added that implements the interface which will call log4j underneath and then the actual log4j library is needed that does the actual work.

4.3 Log4j for the developer and security analyst

The entire security industry, basically the whole internet in a frenzy over application security. Information Technology (IT) professionals are always using logging features to debug programs, fix issues, and for many other purposes. As logging features help to improve things in applications and the system itself. For example, the analytics engine Elasticsearch uses Log4j 2 for logging traffic. The

developer will use this logging library for troubleshooting to find problems with the program and security analysts will use this to find anomalies within the traffic. If you are developing an application and you want to do good by logging these kinds of events. That is where Log4j comes in. Instead of implementing all the code to enable that logging feature, Log4j can do it for you. It is an open-source free framework that you can just wrap into code nicely and easily, and it does all the work for you (Tal 2021). Unfortunately, a flaw in this library has resulted in a vulnerability known as Log4Shell. Log4Shell vulnerability allows an aggressor to send a message to the application (Log4Shell vulnerable), permitting them to execute possible malevolent code like RCE. For example, an attacker can easily execute remote code execution (RCE) and denial of service attacks (Juvonen et al. 2022). Developers and security professionals who are responsibly coding by adding custom logging to their applications, that is the vulnerable piece, that came back to bite them.

4.4 Discovery of Log4Shell

Log4Shell vulnerability was found by Alibaba Cloud Security Team.
A member of the Alibaba Cloud Security Team named Chen Zhaojun privately disclosed Log4Shell vulnerability to the Apache Software Foundation on 24th November 2021, which was publicly uncovered on 9th December 2021 (Jerbi 2021). According to Apace (2022), all versions of the library between 2.0-beta7 to 2.17.0 except 2.3.2 and 2.12.4 are considered helpless to remote code execution (RCE) attacks. The use of this vulnerability by attackers can lead to the loss of data, privacy, malware attacks e.g., ransomware. According to Microsoft (2022), attackers like nation-state actors are moreover taking advantage of log4j vulnerability which leads to the deployment of ransomware. For example, in the year 2021 right after the release of Log4Shell, there was a sudden rise in an old inactive ransomware family called “TellYouThePass” (Gatlan 2021). There has been a rise of different malware attacks besides “TellYouThePass”. According to Microsoft (2022), Novel Khonsari ransomware has been deployed as a payload in many different places. To execute the Novel Khonsari attacker, use a java class file via JNDI which then tricks the system to download the real ransomware (Muir 2021). Attackers do not need a lot of experience to execute such attacks. Just

one line of code is enough, as in the situation with the game Minecraft. The main reason for the appearance of Log4Shell is incorrect input validation. In simple words, the server trusts unreliable data coming from users too much, which makes your software accessible to intruders. An attacker can send the string *User-Agent: $ {env: TEMPORARY_SESSION_TOKEN}* instead of, for example, “Google Chrome”, which can cause compliance problems (Ducklin 2021). This tricks the server into saving such a string to disk. Log4shell is a dangerous vulnerability as an exploit can be installed quickly, and remotely and at the same time it might be difficult to detect.

4.5 Affected applications

Log4j is utilized by millions of business applications, and it is now having the worst software vulnerability ever. This includes cloud services, manufacturers, including even IoT devices. Variables just like the vulnerability being so far-reaching, it is troublesome to locate all the places it exists (Tal 2021). As the vulnerability is extremely simple to abuse makes this a perfect storm. All a cybercriminal needs to do is essentially plan a noxious file, host it through a server that they control, and send a few adjusted codes to the field that is being logged by the application server (Tal 2021). Once the payload is delivered to the vulnerable server and malicious code gets executed. An attacker can take control of the application or system to move somewhere else inside the organization. According to Ilascu (2022), a large-scale of vendors use log4j in their applications and patched the vulnerability to protect themselves from Log4Shell attacks. Some of the well-known vendors are Adobe, Amazon, Cisco, Atlassian and Oracle. After all, the well-known gaming company named Minecraft was also using the log4j library in their game server. An attacker can send malicious payload via Minecraft client software which will lead to a compromising system (Microsoft 2022).

4.6 Overview of Log4Shell vulnerability

This vulnerability was nicknamed Log4shell. An attacker can open a shell on the target server by exploiting the vulnerability and issuing commands. There was a

change in log4j back in 2013 that allowed you to do JNDI lookups in log messages (Jerbi 2021).

Below is an example of JNDI code taken from the Apache Software Foundation website (Apache n.d.b.).

JNDI looks like:

final Logger logger = LogManager.getLogger(…);
logger.error("{}: Error {}", "${jndi:ldap://logconfig/prefix}", error.getMessage());

According to Apache (n.d.b.), the code is calling a prefix for the logging message from JNDI, by sending the JNDI URL as a contention. The passed string value is resolved by log4j. After that, Log4j lookup for certain sorts of strings. For example, if you have any string like hello world over here what it does is insert the string in the curly (Apache. n.d.b.).

An example code from the Apache Software Foundation website (Apache n.d.b.):

logger.error("Inserts String here: {}", "Hello World");
logger.error("Looks up value and inserts: {}", "${jndi:ldap://… }");

The characters that are passing as a contention have this syntax which is the dollar curly. At that point, it is usually a clue for log4j to check it up. In this case, the actual string within the dollar curly is JNDI. Log4j can say it's a JNDI lookup, it will now look up the value and will insert that within the twofold wavy for the format string. This is the vulnerability in log4j that can be easily taken under control.

4.7 Use of LDAP

Lightweight Directory Access Protocol (LDAP) is an attack based on the user agents that are being sent along those headers. LDAP is used to access and

manage the directory services as it can be used as the medium to communicate with Active Directory (AD) and AD is a directory services database (Zugec 2021). It plays a significant role as corporations grow, as it helps to organize user data and assets into a tree-like structure. As a result, it is easier to store, manage and secure information about an organization, its users, and its assets. However, attackers who can control log messages or parameters took this way to execute self-assertive code stacked from LDAP servers when message lookup substitution is empowered (Lakshmanan 2021). According to the Apache Foundation advisory, this behavior is disabled by default.

Figure 9 shows the use of an LDAP server between a victim and an attacker machine. When an attacker machine sends LDAP server links to the victims' computer, the Log4j vulnerable computer does not verify the connection. As a result, the computer sends an LDAP query to the attacker machine which allows an attacker to send a malicious payload, resulting in compromising the system.

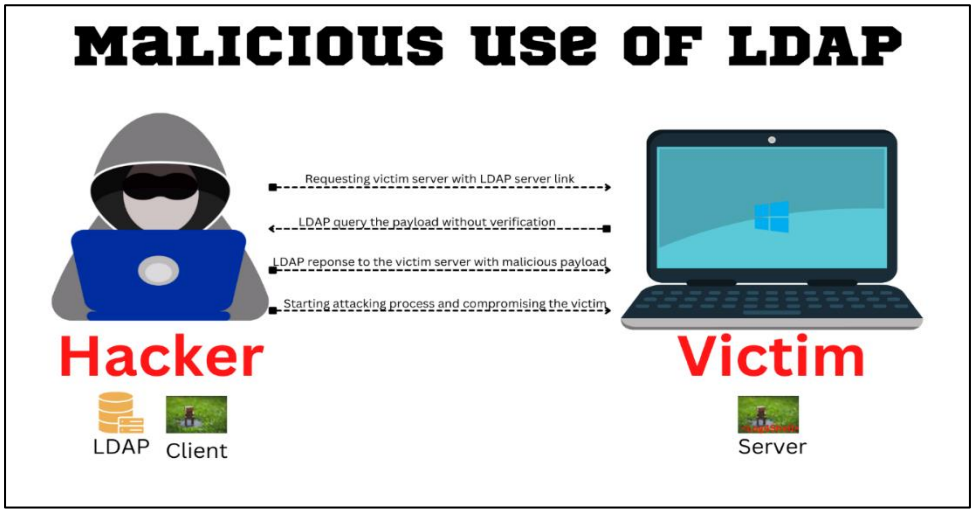

Figure 9. The process of using an LDAP server

5 CYBER DEFENSE EXERCISES IN XAMK VIRTUALLAB

This chapter will cover the design of XAMK virtuallab environment. As this thesis was planned to train students, this chapter will not discuss the technical details to keep it private to the commissioner's organization. The technical details of this exercises were covered in exercise guidelines.

5.1 Virtuallab environment

The testing system in real scenarios is always fun but costly. The cost of infecting a real device for the testing purpose would be significant. Due to testing purposes, a system might need to be infected more than once and there might be a risk of system failure. As a result, virtual environments are always the best choice for doing cyber exercises. XAMK Cyberlab exercises are done via the virtuallab environment, and this is the main reason behind creating the exercises in XAMK virtuallab environment. Students can also access the exercises from remote locations.

5.1.1 Virtual Machines (VM)

The network topology of the cyber defense exercise consists of four different virtual devices. Each device is used for specific purposes such as Kali Linux has been used as an attacker machine, Windows 10 has been chosen as the victim machine, Ubuntu has been picked for monitoring the traffic and the router connects all the devices.

Figure 10 shows a topology an example topology of cyber defense exercises. All the devices are connected to the internet via the router. Devices contain all the necessary tools to run a successful attack on a victim and the tools for detecting such attacks.

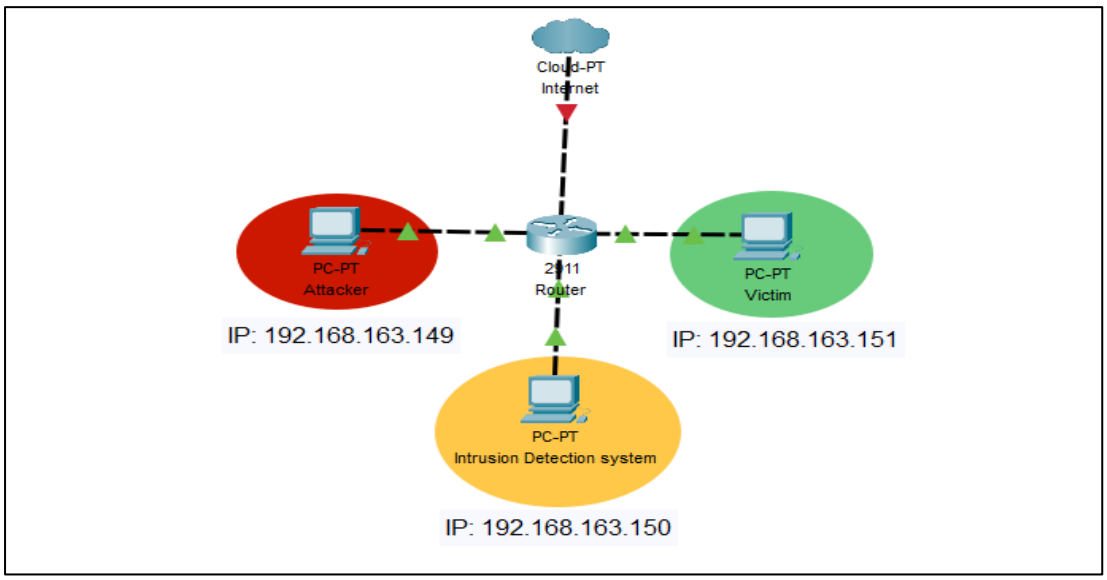

Figure 10. Example Network topology in XAMK virtuallab environment

For the exercise, devices are configured in a single subnet mash. Each device is assigned a specific private IP address from that subnet. For example, the IP address of a Windows machine is 192.168.163.149, and Kali Linux is 192.168.163.151.

5.2 Vulnerable machine (Windows 10 Operating System)

Knowing the attack surface of a system lets an attacker plan well for action. The Attack surface can be a potential vulnerability in hardware, software, network, or the user himself/herself (Human error) (Andress 2015). These attack vectors (vulnerabilities) can be exploited to gain access to a network or the system itself. Reducing the number of attack vectors by reducing the attack surface will reduce the risk of getting compromised (Ozkaya 2019). Intentionally vulnerable Windows 10 machines of this study were designed to provide such attack surface through different attack vectors. As a result, it can be tested against successful attacks.

There are different vulnerabilities in the system such as Log4Shell and RDP vulnerability. The device is not updated, no anti-virus software is installed, nor the defender is turned on, which makes it more vulnerable to different attacks. The user of the windows machine was permitted admin to provide a vulnerable environment with admin rights for an attacker. An intentional Log4Shell

vulnerability has been created using the affected version of the Minecraft server which is 1.15.2. As the Minecraft server has the logging capability using the java Log4j library, an older version of java (Java version 8) has been installed to carry out a successful attack on the server. After fulfilling all the requirements, the Windows machine was ready for executing attacks.

To make the exercise more interesting, an attack scenario was planned. Students can play the role of an attacker to attack an imaginary employee (e.g., Talent acquisitor) where they can capture data at rest, in the move, and progress. A simple employee database was created using Excel where there will be employee names, dates of birth, passport numbers, emails, bank account details, and much more sensitive information. All data from the created database would be stolen using different techniques. Along with the database, there is a demo for stealing victims' social media accounts (e.g., Facebook). Different tools and techniques were used to steal the social media account such as using Keylogger or commands to record victim screens. Students were able to see a phishing technique where a malicious file will be downloaded after clicking a suspicious link. Finally, RDP was used to see the GUI of the victim computer and malware will be executed to show the effect. Malicious actor can stay unnoticeable in a compromised system to cause more harm unless there is enough protection (Cole 2013).

5.3 Attacking machine (Kali Linux Operating System)

Exposing a vulnerability helps to make a stronger system. It is not an easy task to expose a zero-day vulnerability by students. As a result, it is always a good choice to pick an exciting vulnerability to practice exposing and gain experience. For this study, students will be using the Kali Linux machine as an attacking machine as it has a lot of different pre-installed hacking tools. All the tools and different techniques are being used to exploit the intentional Log4Shell vulnerability of Windows 10 machines.

5.3.1 Attacking tools and techniques

Kali Linux has most of the tools pre-installed. Along with the existing tools, some additional tools and services were installed for helping with the exercises. Before installing any tools, the system was updated using the *Sudo apt-get update* and *upgrade* command. As the aim of this exercise was to exploit the Log4Shell vulnerability of the Minecraft server, the basic requirements were fulfilled first. Such as Installing Java versions 8 and 11 along with Minecraft client. After the successful installation of the client software, it was able to connect with the Minecraft game which was running inside the Windows machine.

The connection was successful between the attacker and victim machine. The next step was to prepare a PowerShell payload. PowerShell script was chosen for this exercise as it has been widely used for malicious tactics. According to a Finnish-born company named Nixu, Malicious actors use PowerShell for various steps in hacking such as 61% use for Command-and-Control, 47% for Lateral Movement, 47% for Establishing persistence, 47% for Credential Theft and 37% for Privilege Escalation. (Nixu 2022). The PowerShell script was configured with the Kali Linux IP address and the respective port number that will be listening from Netcat. The script was then compiled using Base64 to add inside java function which was then converted into a Java class using the Java compiler (Javac). The compiled Java class was used as the exploit for this attack which had the capability of providing a reverse shell from a Windows machine.

The exploit for compromising the Log4Shell vulnerability needs to be delivered to victim machine. There are a few other services that need to be running inside Kali Linux i.e., LDAP server, Netcat listener, Apache server, and Minecraft Client. The Marshalsec LDAP server was installed inside Kali Linux with a default port of 1389. As a Netcat listener, the Apache server is pre-installed, and the Minecraft client is already installed inside the Machine. Before delivering the payload through Minecraft client texting facilities, the services need to be up and running. For example, the LDAP server should run with the default port, and when the victim machine request LDAP service, it should direct the traffic to the Apache server port 80. Apache server was hosting different files e.g., Malware, and

PowerShell reverse TCP exploit. When LDAP sends the traffic to the Apache server, it will respond with the payload which will be then executed inside the Windows machine. As the PowerShell script has the Kali Linux IP address and the listening port number. Windows machine will connect with the listening port which will be running in Netcat. For that, it is important to match the Netcat listening port with the port number that was given in the script. If the port number matches, the connection will be established between the Windows machine and Kali Linux, resulting in compromising the system.

After a successful connection, it was possible to check the victims' machine files and there is the possibility to do lots of staff using Netcat. To make the process more interesting, Metasploit was used to gain another excess using the PowerShell script. Using Metasploit the existing database inside a Windows machine can be moved, and it can be deleted and edited. Metasploit also provides the capability of sending a keylogger to a windows machine, which can be used to achieve different objectives such as stealing social media IDs and Passwords. The Metasploit framework can also be used to send Malware inside Windows machines, it can be used to listen to the user, and it can also turn on the camera. Metasploit was used to check the active time of the user and when a user was inactive the RDP session was enabled to use the system graphically.

In real hacking, the attacker steals data and asks for ransom. For demonstrating similar scenarios, the data was stolen, and malware was executed in the victim's machine. To show if victims do not agree to pay the ransom, hackers sell the data in the dark market. To demonstrate a similar approach an onion site was created to show an example scenario of selling data. Tor was used for staying anonymous and the python server was used to host the onion site. As hacker uses “the onion router” (tor) to make the tracing process harder and the dark web is used for illegal activity (Anderson 2021).

5.3.2 Attacking process and results

The attacking process will start with target identification in other words with the reconnaissance phase. Participants of this exercise can use the Nmap tool or

other network scanning tools to discover the target IP. After finding an IP address, it is possible to find more information about the target such as running services, open ports, and OS information. After finding detailed information, participants can also do more research based on the found result.

To make the process easier, the exploits were prepared for the participants. As the weaponization phase is ready, participants need to prepare delivery phases such as LDAP to sever, Apache server, Netcat listener, and the Minecraft client to send the weapon. When the services are ready, participants can start the delivery process using the Minecraft client text method where they text the server with a command such as *${jndi:ldap://Kali-Linux-IP:LDAP-Port/Log4jRCE}*. When the server receives the command the Log4Shell vulnerability will be exploited. The server then requests services from LDAP where LDAP sends the request to the Apache server. The Apache server will replay with the Java class file containing the PowerShell script. The PowerShell script will get executed inside the machine which will result in a reverse Netcat shell.

As the victim's computer will be under the participants' control, participants will be able to Command and Control the machine. The use of the Metasploit tool will help to execute various commands, it also helps to execute further exploit. The participants will fulfill the objective of the attack after gaining the data from the victim's machine.

5.4 Traffic monitoring machine (Ubuntu Operating system)

To detect security events traffic monitoring is a compulsory part. There is not a single product that can make a 100%-secure system or infrastructure (Cole 2013). As a result, implementing security devices along with monitoring traffic must be present to detect attacks. For the thesis few tools were tested to detect and monitor traffic such as Elastic stack, Wazuh, and Wireshark. To reduce the load on the virtual machine, only Elastic stack and Wireshark have been implemented for participants. Besides the detecting phase of the exercise, participants will be able to see and analyze a malicious file using different operating systems such as REMnux. After a successful Log4Shell attack, a

malware sample will be transferred to the Victim machine to demonstrate the effect of malware.

5.4.1 Elastic stack

Elasticsearch is a free, open-source search and analytics engine used for traffic monitoring and security solution (Elastic 2022). It helps to store system data that can be searched and analyzed in real-time (Elastic 2022). Elastic stack is made up of four different components beats, Logstash, Elasticsearch, and Kibana (Elastic 2022). Beats is an agent which is used to collect data from the system such as log sources. Logstash is used for listening on ports for different activities and it also checks on different files. All details collected from an agent will then be passed to the server which is called Elasticsearch. Elasticsearch helps to store system data, it helps to search and analyze data in real-time through the web-based user interface called Kibana. For example, Kibana can be used to query Elasticsearch for the security events of an agent.

Figure 11 shows the web-based interface of the Elastic stack called Kibana. It was configured with a Windows 10 agent which was the victim of a Log4Shell attack. As a result, the security event is showing the detected traffic that was carried out. As the attack was carried out using PowerShell script, figure 11 also shows five different attempts of the attacker.

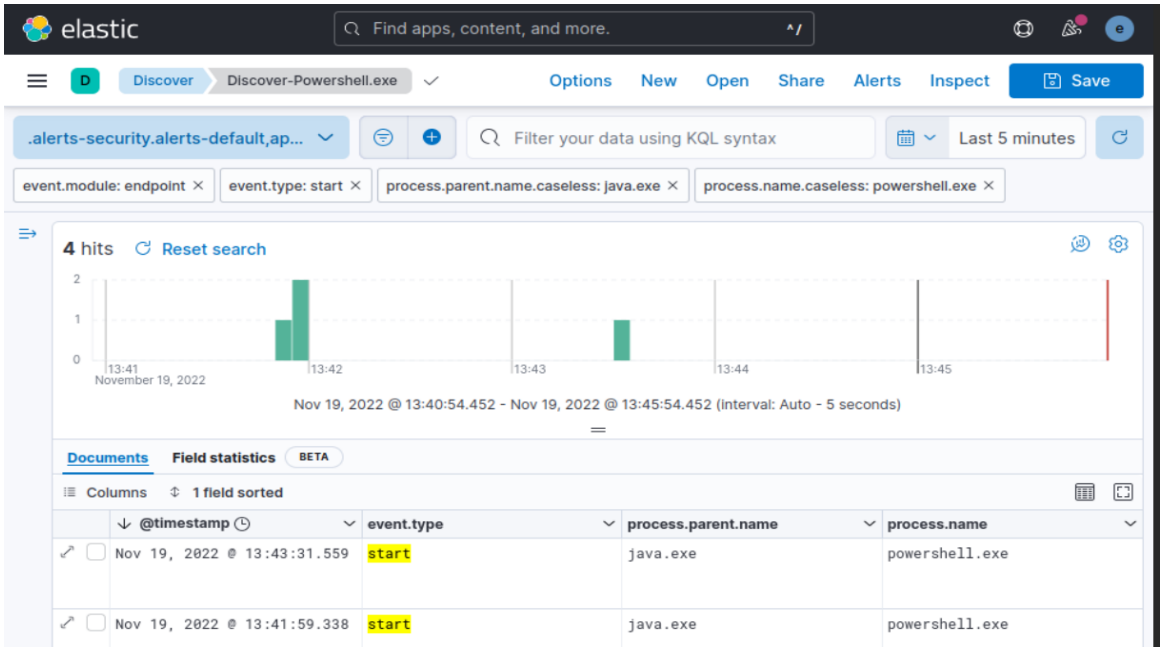

Figure 11. Overview of Kibana web interface

5.4.2 Wireshark

Wireshark Is a well-known free and open-source network traffic analyzer. It can be used for various purposes from troubleshooting the network to analyzing malicious traffic (Sharpe n.d.). Investigating network packets can help professionals to find suspicious traffic on the network as Wireshark is a great sniffing tool (Andress 2015). Wireshark has been implemented for the defensive exercise to detect Log4Shell attacks where different signatures are added to find specific traffic such as JNDI and TCP SYN (Transmission Control Protocol Synchronization) from the victim machine. Analyzing malicious traffic using Wireshark also helps professionals to do threat hunting which is a very important part of cyber security.

Figure 12 shows the captured packets by Wireshark. The packet shows the detection of the Log4Shell exploit which was sent from the Kali Linux machine.

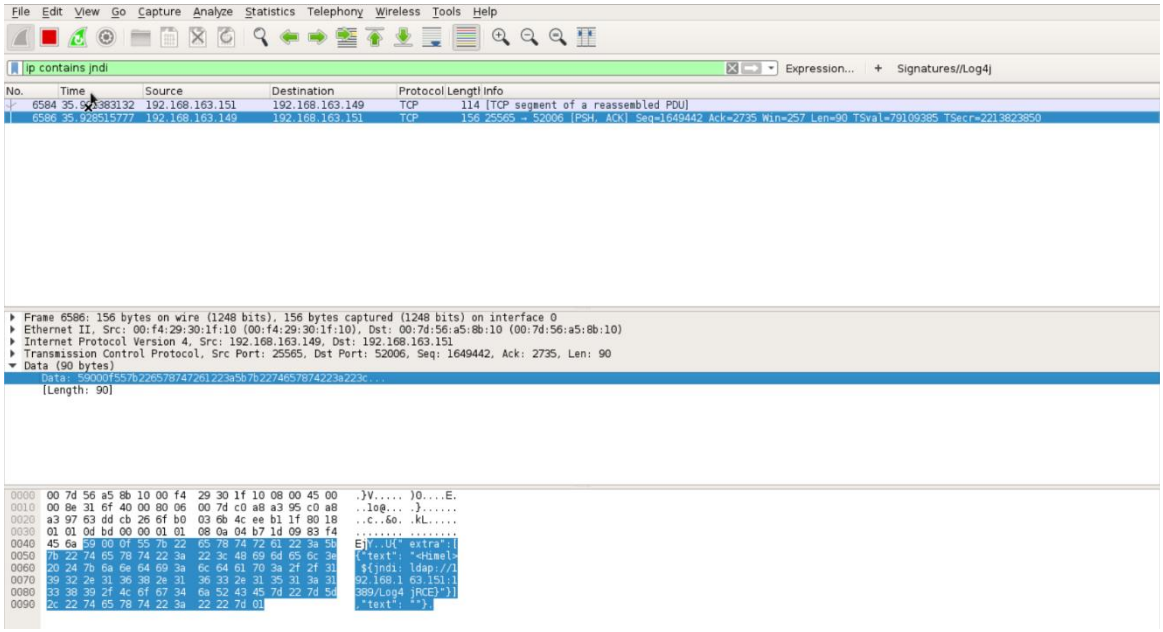

Figure 12. Packet analysis using Wireshark to detect Log4Shell attack

5.4.3 Discover vulnerabilities

Vulnerability scanning helps to find issues in the system which then can be repaired before something goes wrong. Doing a regular vulnerability scan against the system will help to quickly remediate any vulnerability (Cole 2013). As a result, the system can be protected well against adversaries. In the exercise of this thesis, Nessus the vulnerability discovery tool has been used for vulnerability analysis. Nessus can be used for scanning the target system or network. After a successful scan, system risk and network risks can be identified, and they can be fixed at the same time using different security measures (Tenable n.d.).

Figure 13 shows the network scan using the Nessus vulnerability scanning tool. The tool was used to scan the network. In figure 13, there are 68 different vulnerabilities in three different devices which are the router, Windows machine, and the Ubuntu device itself.

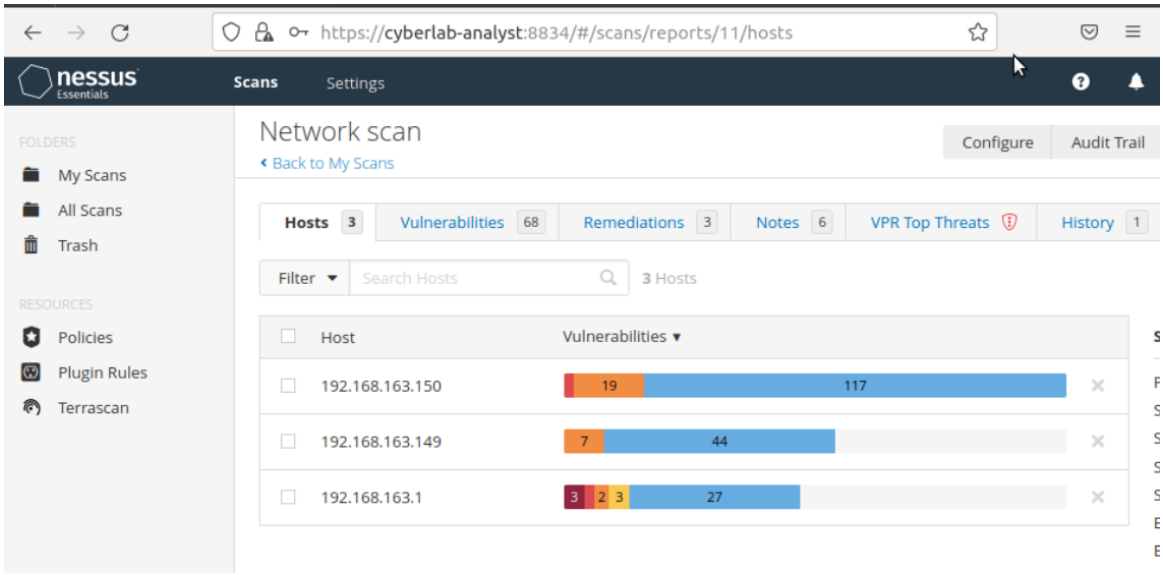

Figure 13. Network vulnerability scan using Nessus

5.5 Defending the system

There is always a chance of getting infected by a malicious party. Detection is always a good choice, but it does not stop harming the system. As a result, defending a system is important. According to Cole (2013), investing in security and implementing security products are the right things to do as they will keep the organizations from the news headline. In this study, Windows 10 machines were picked as victims' computers where there was different intentional vulnerability. Some common security measures can be implemented to help strengthen the security of the vulnerable Windows 10 machine and to defend against Log4Shell attacks. This common security practice can be implemented on any other machines to reduce security risks by defending the system against different cyber-attacks.

Compromising a system is way easier than strengthening security. To defend against attacks like Remote Code Excitation there are various tools on the market. Nowadays, defending tools are built-in with Operating Systems such as Windows Defender. When a system becomes a victim of a cyber-attack, there is always an Indicator of Compromised (IOC) such as suspicious behavior on the system, suspicious tasks in the Task manager and suspicious connection to another IP address. In case a system has been compromised but nothing harmful happened yet, the victim can check the Task manager to end the suspicious task

and the connection IP too. To see the connected IP of the compromised system, a victim can use the netstat command to see all details about IP and ports. If there is anything suspicious found on the system, the connection can be terminated using different ways such as using the “taskkill” command with PID (Process ID), which will kill active connections on a local computer.

Suspicious traffic can be captured in real-time to check detailed information. Wireshark can be used for more details about the connection and data that is moving between the attacker and the victims' system. Elastic stack also helps to defend against attacks besides detecting them. Some defending features have been enabled for the defending part of this exercise except the paid features.

Windows defender firewall plays a big role in defending against the Log4Shell attack. Real-time protection was able to detect the malicious traffic which resulted in dropping the PowerShell script instead of Downloading and executing it. As a result, it is very important to turn on Windows defender to protect against different common attacks. Windows Remote Desktop Protocol was turned on intentionally. It is a vulnerable protocol and can easily allow access to an attacker. As a result, it should be turned off for safety purposes.

The Minecraft server has been patched by the vendor. The used Minecraft server for this thesis was intentionally vulnerable to Log4shell attacks. There were a few security features that were turned off by the Minecraft server but for the exercise, the features were turned on even though the server prompted the feature to be vulnerable. As a result, it provided a vulnerability that was exploited by the Kali Linux machine. To secure our system, it is important to turn off those vulnerable features and upgrade the server to a patched version of Minecraft. In any scenario, it is always a good choice to use the updated version of the software as vendors fix security issues to protect clients from different attacks. The used Java version for this exercise was the compromised version. As a result, it is also important to update the Java version to the latest version.

During the attack scenario, the attacker's machine was able to do various things with the victims' machine. Because the user of the victim machine was having admin rights which made it was possible to do whatever the user wanted. Taking the administrative right of a normal user would help to reduce the access of an attacker by reducing the function of vulnerabilities (Laiho 2022). As removing admin rights is the most important security control as it will protect end users by giving fewer functions to an attacker (Laiho 2022). Defending a system is crucial unless we want a hacker to take control of our system.

6 DISCUSSION AND CONCLUSION

Throughout the research, a different approach was followed to find the answer to the research questions. After analyzing all collected data, a cyber defense exercise has been built to demonstrate the solution to the research problems.

6.1 Solutions to research problems

The thesis started by pointing out some questions to solve the research problem. Due to the rise of computing in our society, the number of cyber-attacks is growing rapidly. Companies become the victims of cyber criminals which results in losing data, reputation, and more. To protect companies from different cyber threats, cyber professionals are needed to build a cyber defense against those attacks. In the race between cyber professionals and cybercriminals, professionals are having skill gap issues. By considering the current industrial problem, this thesis built a cyber defense exercise for XAMK Cyberlab with one of the biggest vulnerabilities of the last decade. To prepare cyber security students for the upcoming cybercrime.

To solve the problem of this thesis four different questions were answered which are:

1) What are the skills required by a cyber defender?

Defending a system against modern attacks is hard. Attackers are using their knowledge to use different tools and techniques to compromise systems. Attackers may target our system to steal data, ask for ransom, or for damaging the system. To withstand such attacks, the cyber defender needs to keep up-to-date information about the current attacks that are going on all around the world. Gaining knowledge from different sources will help to understand how the attackers are attacking but to learn the real effect, it is very important to practice such scenarios to gain enough knowledge to protect the system against those adversaries. Hacking like a hacker will teach the defender the process that a hacker uses or the tools that are used. Knowing about different attacking

processes and tools that attackers use, will help a defender understand what things need to be fixed to make a better-secured system. Even after making a secured system, the defender is always needed to find other weaknesses in the system before a hacker finds it. After all, defenders are required to practice different scanning and defending tools such as Elastic stack, Wazuh, Snort, Nessus, and OpenVAS.

2) How are the skills exercised?

To improve the security experience, it is crucial to do the hands-on practice. Real devices are too expensive to practice hands-on hacking scenarios. As a result, virtual devices are always the best choice as it does not cost much, they can be saved, they can be infected with malware. To practice hacking and defending, different tools needed which are widely available. For example, the installation of Kali Linux provides different hacking tools like Metasploit.

With the help of different vulnerable software, a vulnerability can be created inside a system. This vulnerable system can be attacked from a different machine which then can be detected using various open-source tools.

3) What kind of simple environment can be built to exercise some of these skills?

Based on the first and second questions of this thesis a virtual cyber defense exercise has been built inside XAMK Cyberlab. To demonstrate a simple virtual environment that can be used to practice cyber defense. Using this exercise, cyber professionals will be able to improve their cyber security skills through hacking and defending a system. The exercise aims to teach students all the necessary processes to exploit a vulnerability. Through the exploitation of the vulnerability, students will be able to take control of the system and use different commands to explore the system. At the end of attacking a vulnerable machine, students will be able to detect such attacks in real-time along with defending against those attacks to make a strong system. After all, students will be able to

gain knowledge about different attacking, detecting, and defending processes, tools, and techniques which will help to make a secure system.

4) What are the common processes and tools for a defender?

There are different defensive tools available in the market both free and paid. For practicing cyber defense, open-source, and free tools are sufficient. Some of the open-source tools that have been implemented inside the cyber defense exercise of this study are Elastic stack (Elasticsearch, Kibana), Wireshark, Nessus, and Windows defender. With these tools, vulnerabilities of the system were assessed, and malicious traffic was detected and prevented using defending mechanisms.

While straightening system security, cyber professionals need to actively monitor traffic for malicious activity. In case of any suspicious traffic is noticed, the traffic needs to be analyzed using different tools like Wireshark. Through analyzing malicious traffic, the threat can be detected as possibly finding the malicious files of destination details. For example, if packet analysis shows the attackers were trying to run an exploit Minecraft server, it will give a hint to look for any weakness in that server

6.2 Conclusions

The study plan was to develop a cyber defense exercise for XAMK Cyberlab. To make the research interesting, a well-known vulnerability Log4Shell was chosen. As Log4Shell vulnerability existed inside a popular gaming sever named Minecraft. The Minecraft server was implemented inside the virtuallab environment to demonstrate the effect of Log4Shell vulnerability.

The exercise shows the impact a vulnerability can bring on our life. Through the Log4j vulnerability, an attacker can run code from a remote location. It gives a chance to attacker to do a lot of bad things like stealing data, installing a back door, spying on a victim, or even running ransomware.

Through the attacking phase of this exercise, students will be understanding the way an attacker act. Based on the attacker act, students will be able to add security measures to the compromised system to run a similar attack to detect and defend. Through the different use of different tools and techniques along with different security measure student will be able to learn the way to defend against attacks.

I strongly believe that through exercise students will gain numerous skills. These exercises will help to achieve the basic skills for hacking and defending a system. After the successful creation of these exercises, a demo was created to share with peers and XAMK personnel. Based on the feedback, the outcome of this thesis can be considered successful. These exercises can be improved in many ways such as using Active Directory to connect vulnerable machines or making other intentional vulnerabilities. Conclusively, while practicing these exercises, it is important to improve the exercise as the threat landscape is always changing with different attack types and techniques.

6.3 Further development of the study

The built exercises in XAMK Cyberlab can be rebuilt by anyone to exercise their cyber security skills. It can build in virtual environments like VMware, VirtualBox, or even in cloud environments. The basic requirements for this exercise will be a victim machine with a vulnerable Minecraft server which can be exploited using the attacking machine with the presence of the required tools that were discussed in Chapter 5. After creating a vulnerable environment, the attack can be performed to see the effect. Based on the attack, security tools can be implemented to detect and defend against such attacks. The defending mechanism for these exercises was also discussed in Chapter 5.

There are different hacking and defending tools available online. Most trustable tools can be implemented to learn more about the tools. For example, implementing Wazuh, Snort, Suricata, and many others.

The topology of the exercise can be reconstructed by adding additional Windows server and a few other machines. To make the processes smoother, the server can be infected with Log4Shell vulnerability instead of the Windows 10 machine. In this scenario, the server will be the Active Directory (AD) for all other machines. The AD can be hacked to get complete access to the machine. Through server access, the hacker can use the techniques of APT and lateral movement to move silently from one machine to another. Hackers can command another machine while the AD will be under control. It is also possible to infect others' computers or lock the user out.

In the created exercises Windows defender real-time protection was turned off during the attack. It can be turned on to check different obfuscation techniques. As malware attacks are rising worldwide and malware use different obfuscation techniques to bypass a defender. It will be a good idea to try different hiding techniques to hide from defenders which will result in a better and more secured system.

REFERENCES

Alibabacloud. 2021. Security Advisory on Apache Log4j 2 RCE Vulnerability (CVE-2021-44228). [online] Available at: https://www.alibabacloud.com/notice/log4j2 [Accessed 19 September 2022].

Anderson, R. 2021. Security engineering: A guide to building dependable distributed systems. New York: Wiley.

Andress, J. 2015. The Basics of Information Security: Understanding the fundamentals of infosec in theory and Practice. Waltham, MA: Syngress.

Apache. 2022. Apache Log4j™ 2, Log4j – Apache Log4j 2. Available at: https://logging.apache.org/log4j/2.x/ [Accessed November 26, 2022].

Apache. n.d.a. Apache Log4j security vulnerabilities, Log4j – Apache Log4j Security Vulnerabilities. Available at: https://logging.apache.org/log4j/2.x/security.html [Accessed November 16, 2022].

Apache. n.d.b. Log4j 2 API, Log4j 2 API - apache log4j 2. Available at: https://logging.apache.org/log4j/log4j-2.2/manual/api.html [Accessed November 19, 2022].

Apache. n.d.c. Apache HTTP Server Project , About the Apache HTTP Server Project - The Apache HTTP Server Project. Available at: https://httpd.apache.org/ABOUT_APACHE.html [Accessed November 26, 2022].

AV-TEST. n.d. Malware | AV-TEST. [online] Available at: https://www.av-test.org/de/statistiken/malware/ [Accessed 21 September 2022].

Bannister, A. 2022. Zero-day flaws in GPS tracker pose surveillance, fuel cut-off risks to vehicles, *The Daily Swig* | *Cybersecurity news and views*.. Available at:

https://portswigger.net/daily-swig/zero-day-flaws-in-gps-tracker-pose-surveillance-fuel-cut-off-risks-to-vehicles [Accessed November 11, 2022].

Bernard, T.S. et al. 2017. Equifax says cyberattack may have affected 143 million in the U.S. *The New York Times*, 10 November 2022. Electronic newspaper. Available at: https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html [Accessed November 10, 2022].

Chen, T.M. & Nimeh, S.A. 2011. Lessons from stuxnet, IEEE Xplore. Available at: https://ieeexplore.ieee.org/document/5742014 [Accessed November 10, 2022].

CISA. 2022. Alert (AA22-320A), CISA. Available at: https://www.cisa.gov/uscert/ncas/alerts/aa22-320a [Accessed November 18, 2022].

Cisco. 2022. What is a cyberattack? - most common types, Cisco. Cisco. Available at: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html#~types-of-cyber-attacks [Accessed November 15, 2022].

Cole, E. 2013. Advanced persistent threat understanding the danger and how to protect your organization. Boston: Syngress.

Deering, S. & Hinden, R. 1998. RFC 2460 - internet protocol, version 6 (ipv6) specification. IETF. Available at: https://datatracker.ietf.org/doc/html/rfc2460 [Accessed November 10, 2022].

Ducklin, P. 2021. Log4Shell explained – how it works, why you need to know, and how to fix it, Naked Security. Available at: https://nakedsecurity.sophos.com/2021/12/13/log4shell-explained-how-it-works-why-you-need-to-know-and-how-to-fix-it/ [Accessed November 16, 2022].

Dewdney, A.K. 1989. Computer Recreations, March 1989, Scientific American. 260(3), 10–113. E-journal. Available at: https://doi.org/10.1038/SCIENTIFICAMERICAN0389-110.

Elastic. N.d. Welcome to elastic docs, Elastic. Available at: https://www.elastic.co/guide/index.html [Accessed November 18, 2022].

Ewe, K. 2022. This hacker stole data from 200m Americans. now he's infiltrating scam gangs., VICE. Available at: https://www.vice.com/en/article/3adpky/cambodia-vietnam-scam-operations [Accessed November 10, 2022].

Fisher, D. 2018. Microsoft open sources seal homomorphic encryption library, Decipher. Duo Security. Available at: https://duo.com/decipher/microsoft-open-sources-seal-homomorphic-encryption-library [Accessed November 11, 2022].

Frayling, C. 1993. Research in Art and Design. Royal College of Art Research Paper 1(1) 1-5 Available at: https://researchonline.rca.ac.uk/384/3/frayling_research_in_art_and_design_1993.pdf [Accessed 9 Aug 2022].

Funet. n.d. The ARPANET. [online] Available at: https://researchonline.rca.ac.uk/384/3/frayling_research_in_art_and_design_1993.pdf [Accessed 16 September 2022].

Gatlan, S. 2021. TellYouThePass ransomware revived in linux, Windows Log4j attacks, BleepingComputer. BleepingComputer. Available at: https://www.bleepingcomputer.com/news/security/tellyouthepass-ransomware-revived-in-linux-windows-log4j-attacks/ [Accessed November 16, 2022].

Greig, J., 2021. Second Log4j vulnerability discovered, patch already released. Web page. Available at: https://www.zdnet.com/article/second-log4j-vulnerability-found-apache-log4j-2-16-0-released/ [Accessed 19 September 2022].

Hakkala, A. & Koskinen, J. 2022. Personal data protection in the age of mass surveillance, *Journal of Computer Security*, 30(2), 273–274. Available at: https://doi.org/10.3233/jcs-200033 .

Ilascu, I. 2022. LOG4J: List of vulnerable products and vendor advisories, BleepingComputer. BleepingComputer. Available at: https://www.bleepingcomputer.com/news/security/log4j-list-of-vulnerable-products-and-vendor-advisories/ [Accessed November 16, 2022] .

ISC2. 2022. (ISC)² Research Finds Employer Hiring Practices Must Evolve to Overcome the Cybersecurity Workforce Gap. Web page. Available at: https://www.isc2.org/News-and-Events/Press-Room/Posts/2022/06/16/ISC2-Research-Finds-Employer-Hiring-Practices-Must-Evolve-to-Overcome-the-Workforce-Gap [Accessed 1 July 2022].

Jankowicz, M. & Davis , C.R. 2020. These big firms and US agencies all use software from the company breached in a massive hack being blamed on Russia, *Business Insider.*. Available at: https://www.businessinsider.com/list-of-companies-agencies-at-risk-after-solarwinds-hack-2020-12?r=US&IR=T [Accessed November 10, 2022].

Jerbi, A., 2021. P1 Labs » Remote Code Execution through Signaling Using Log4j (CVE-2021-44228). Web page. Available at: https://labs.p1sec.com/2021/12/22/remote-code-execution-through-signaling-using-log4j-cve-2021-44228/ [Accessed 20 September 2022].

Juvonen, A., Costin, A., Turtiainen, H. & Hämäläinen, T. 2022. On Apache LOG4J2 exploitation in Aeronautical, maritime, and aerospace ... Available at: https://www.researchgate.net/publication/362705683_On_Apache_Log4j2_exploitation_in_aeronautical_maritime_and_aerospace_communication [Accessed November 26, 2022].

Knight, A. 2020. Memoirs of an API hacker: Intercepting encrypted mobile traffic to hack a bank's API server, Alissa Knight. Available at: https://www.alissaknight.com/post/memoirs-of-an-api-hacker-intercepting-encrypted-mobile-traffic-to-hack-a-bank-s-api-server [Accessed November 11, 2022].

Koskinen, I. 2011. Design Research Through Practice: From the Lab, Field, and Showroom. Morgan Kaufmann Publishers.

Kozlowska, I. 2019. Facebook and data privacy in the age of Cambridge Analytica, The Henry M. Jackson School of International Studies. University of Washington. Available at: https://jsis.washington.edu/news/facebook-data-privacy-age-cambridge-analytica/ [Accessed November 10, 2022].

Laiho, S. 2022. Removing admin rights hardens your environmentSami Laiho, Recast Software. Available at: https://www.recastsoftware.com/resources/removing-admin-rights-hardens-your-environment/ [Accessed November 18, 2022].

Lakshmanan, R., 2021a. Extremely Critical Log4J Vulnerability Leaves Much of the Internet at Risk. Web page. Available at: https://thehackernews.com/2021/12/extremely-critical-log4j-vulnerability.html [Accessed 23 September 2022].

Lakshmanan, R., 2021b. Hackers Begin Exploiting Second Log4j Vulnerability as a Third Flaw Emerges. Web page. Available at: https://thehackernews.com/2021/12/hackers-begin-exploiting-second-log4j.html [Accessed 17 September 2022].

Lee, J., Wickens, C., Liu, Y. & Boyle, L., 2017. Designing for people. Charleston, S.C: CreateSpace. Available at: https://www.researchgate.net/publication/319402797_Designing_for_People_An_introduction_to_human_factors_engineering [Accessed 12 Aug 2022].

Lockheedmartin. N.d. Cyber kill chain®, Lockheed Martin. Available at: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html [Accessed November 13, 2022].

Mazzucchi, N. 2022. Hybrid coe, Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats. Available at: https://www.hybridcoe.fi/ [Accessed November 10, 2022].

McGraw, G. 2004. Software security, IEEE Xplore. IEEE. Available at: https://ieeexplore.ieee.org/abstract/document/1281254 [Accessed November 11, 2022].

Meier-Hahn, U., 2017. The Internet was built on trust — but what does it run on? | APNIC Blog. [online] APNIC Blog. Available at: https://blog.apnic.net/2017/07/13/internet-built-trust-run/ [Accessed 21 September 2022].

Microsoft. 2022. Guidance for preventing, detecting, and hunting for exploitation of the LOG4J 2 vulnerability, Microsoft Security Blog. Available at: https://www.microsoft.com/en-us/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/ [Accessed November 16, 2022].

Muir, M. 2021. Analysis of novel Khonsari Ransomware deployed by the Log4Shell vulnerability - cado security: Cloud investigation, Cado Security | Cloud Investigation. Available at: https://www.cadosecurity.com/analysis-of-novel-khonsari-ransomware-deployed-by-the-log4shell-vulnerability/ [Accessed November 16, 2022].

Murphy, H., 2021. Hackers launch more than 1.2m attacks through Log4J flaw. Web page. Available at: https://www.ft.com/content/d3c244f2-eaba-4c46-9a51-b28fc13d9551 [Accessed 10 October 2022].

NCSC. 2016. Data breach of 500m yahoo accounts, NCSC. Available at: https://www.ncsc.gov.uk/news/data-breach-500m-yahoo-accounts [Accessed November 10, 2022].

NIST. 2018. Framework for Improving Critical Infrastructure Cybersecurity. NIST Technical Series Publications. Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [Accessed November 11, 2022].

Nixu. 2022. Nixu Threat Intelligence Threat Landscape Snapshot Q2/2022, Nixu Cybersecurity. Available at: https://www.nixu.com/blog/nixu-threat-intelligence-threat-landscape-snapshot-q22022 [Accessed November 17, 2022].

NVD. N.d. NVD - CVE-2021-44228. Web page. Available at: https://nvd.nist.gov/vuln/detail/CVE-2021-44228 [Accessed 11 October 2022].

Osborne, C. 2022. API security: Broken Access Controls, injection attacks plague the enterprise security landscape in 2022, The Daily Swig | Cybersecurity news and views. The Daily Swig. Available at: https://portswigger.net/daily-swig/api-security-broken-access-controls-injection-attacks-plague-the-enterprise-security-landscape-in-2022 [Accessed November 11, 2022].

OWASP. 2022. Owasp Top Ten, OWASP Top Ten | OWASP Foundation. Available at: https://owasp.org/www-project-top-ten/ [Accessed November 15, 2022].

Ozkaya, E. 2019. Cybersecurity: The Beginner’s Guide. Packt Publishing

Paganini, P. 2022. A cyberattack blocked the trains in Denmark, Security Affairs. Available at: https://securityaffairs.co/wordpress/138127/cyber-crime/cyberattack-blocked-trains-denmark.html [Accessed November 10, 2022].

Roberts, K. 2022. Being aware of the 6 different types of hackers, Bulletproof.co.uk. Available at: https://www.bulletproof.co.uk/blog/different-types-of-hackers [Accessed December 2, 2022].

Rybski, S. 2021. Comprehensive security together #6: The role of exercises in countering hybrid threats, Turvallisuuskomitea. Available at: https://turvallisuuskomitea.fi/en/comprehensive-security-6-the-role-of-exercises/ [Accessed November 11, 2022].

Silverman, D. 2013. Doing qualitative research. 4th ed. Sage Publication Ltd.

Silverman, D. 2021. Qualitative research. 5th ed. Sage Publications Ltd. Available at: https://books.google.nl/books?hl=en&lr=&id=7RwJEAAAQBAJ&oi=fnd&pg=PP1&dq=qualitative+research&ots=LXl2FX_5Yn&sig=yjr-kdyU3PJ97dikjC2jdUi8xec#v=onepage&q&f=false [Accessed 9 Aug 2022].

Sharpe, R., Warnicke, E. and Lamping, U. n.d. Wireshark User's Guide, Wireshark user's guide. Available at: https://www.wireshark.org/docs/wsug_html_chunked/ [Accessed Ngovember 26, 2022].

Tal, L., 2021. The Log4j vulnerability and its impact on software supply chain security. Web page. Available at: https://snyk.io/blog/log4j-vulnerability-software-supply-chain-security-log4shell/ [Accessed 19 September 2022].

Tarnoff, B., 2016. How the internet was invented. The Guardian, [online] Available at: https://www.theguardian.com/technology/2016/jul/15/how-the-internet-was-invented-1976-arpa-kahn-cerf [Accessed 16 September 2022].

Tenable. n.d. Nessus documentation: Tenable™, Tenable. Available at: https://docs.tenable.com/Nessus.htm [Accessed November 26, 2022].

Tietsort, J.R. 2022. 17 most common types of cyber attacks & examples (2022), Aura. Available at: https://www.aura.com/learn/types-of-cyber-attacks [Accessed November 15, 2022].

Trendmicro. 2016. Malware discovered in German Nuclear Power Plant, Malware Discovered in German Nuclear Power Plant - Wiadomości bezpieczeństwa. Available at: https://www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/malware-discovered-in-german-nuclear-power-plant [Accessed November 10, 2022].

UCL Computer Science. 2022. About Peter Kirstein. [online] Available at: https://www.ucl.ac.uk/computer-science/about/about-peter-kirstein#:~:text=Peter%20Thomas%20Kirstein%20CBE%20FREng,Vint%20Cerf%20and%20Bob%20Kahn [Accessed 16 September 2022].

Vailshery, L.S. 2022. IOT connected devices worldwide 2019-2030, Statista. Available at: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ [Accessed November 10, 2022].

Valkama, H. 2018. Heikki Valkama: Teknologiajättien Tarkkailijatontut Ovat olleet Tänäkin Vuonna tuhmia – Menetettyä yksityisyyttä on Vaikea Saada Takaisin, Yle Uutiset. Available at: https://yle.fi/uutiset/3-10565677 [Accessed November 10, 2022].

Villaluna, J. 2022. 2022 trustwave spiderlabs telemetry report, Trustwave. Available at: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/2022-trustwave-spiderlabs-telemetry-report/ [Accessed November 16, 2022].

Wakefield, J. N.d. Deepfake presidents used in Russia-ukraine war, BBC News. BBC. Available at: https://www.bbc.com/news/technology-60780142 [Accessed November 10, 2022].

Washingtonpost. 2013. Target cyberattack by overseas hackers may have compromised up to 40 million cards, The Washington Post. WP Company. Available at: https://www.washingtonpost.com/business/economy/target-cyberattack-by-overseas-hackers-may-have-compromised-up-to-40-million-cards/2013/12/20/2c2943cc-69b5-11e3-a0b9-249bbb34602c_story.html?noredirect=on&utm_term=.2d3d9c763c06 [Accessed November 10, 2022].

Wetsman, N. 2021. The pandemic revealed the Health Risks of hospital ransomware attacks, The Verge. Available at: https://www.theverge.com/2021/8/19/22632378/pandemic-ransomware-health-risks [Accessed November 10, 2022].

Wu, Z., Guo, A., Yue, M., & Liu, L. 2019. An ADS-B message authentication method based on certificateless short signature, IEEE Xplore. IEEE. Available at: https://ieeexplore.ieee.org/document/8792081 [Accessed November 11, 2022].

YLE. 2022a. Probe of psychotherapy firm's data breach finds possible European, employee links, News. Available at: https://yle.fi/news/3-12543823 [Accessed November 10, 2022].

YLE. 2022b. F-Secure: Data of 200k Finnish linkedin users posted on Hacker Forum, News. Available at: https://yle.fi/news/3-12670591 [Accessed November 10, 2022]

Zugec, M. 2022. Technical advisory: Zero-day critical vulnerability in LOG4J2 exploited in the wild, Technical Advisory: Zero-day critical vulnerability in Log4j2 exploited in the wild. Bitdefender SRL. Available at:

https://businessinsights.bitdefender.com/technical-advisory-zero-day-critical-vulnerability-in-log4j2-exploited-in-the-wild [Accessed November 26, 2022].

Appendices