SECURITY IN THE HEALTHCARE INDUSTRY

A practical cybersecurity approach

Author: Malcom Brandin
Supervisor: Janrik Oberholzer
Noroff Institute of Technology and Digital Media

Table of Contents

1. Introduction

1.1 Background and context

In the digital landscape of the modern world, society has become deeply dependent on technology to support us in our everyday tasks. From communication and scheduling to storing data and conducting research, technology continues to aid us and alter the way we live. In no place is this as prevalent and important as in the healthcare industry where a reliable digital infrastructure often can mean the difference between life and death. It not only helps us store and safekeep critical patient information, it also ensures that medical systems stay available when they are needed which is of huge relevance.

With the accelerating growth in remote doctor appointments and overall digitalisation of healthcare services however, new cyberthreats have emerged because of the growing attack surface.

1.2 Problem Statement

In response to these growing cyberthreats this project concentrates on a fast-growing telemedicine company that in recent time has been faced with security concerns threatening patient confidentiality as well as system availability. Because the company leans heavily on a remote first infrastructure it has become increasingly vulnerable to ransomware attacks, phishing attempts and social engineering as well as unauthorized access which risks often stem from weak passwords and misconfigured Virtual Private Networks (VPNs) or a lack thereof.

Vulnerabilities such as a misconfigured VPN also poses a real threat of non-compliance with regulations like the General Data Protection Regulation (GDPR), which dictates the way in which sensitive data of patients must be handled and maintained.

1.3 Project Aim and Objectives

To address these concerns the CEO of the company has tasked our cybersecurity department with assessing the companies IT infrastructure and develop a set of countermeasures to the security concerns they are faced with. The primary objective of this project consists of

- Analysing and identifying weaknesses in the current IT environment, especially focusing on those affecting remote doctor appointments and data storage.
- Implementing security measures such as VPN, multi-factor authentication, network segmentation along with simulated attacks to monitor and evaluate the system's

ability to detect and withstand intrusions using tools such as Kali-Linux and Windows 10 server and client VM's.

- To educate healthcare staff on cyberthreats by running fake phishing attempts, creating and implementing a security framework to raise awareness and lower the chances of future breaches.
- To test the security measures in a controlled environment and verify their effectiveness.
- To document and summarise the entire process in a final report that demonstrates the necessity of a long-term cyber-security investment.

1.4 Proof-of-concept and value

This project not only aims to demonstrate the importance of cyber-security implementation within a healthcare infrastructure, but it will also serve as a proof-of-concept for how a few security measures substantially can improve an organization's resistance to cyberthreats.

By the simulation of real attacks like phishing attempts and unauthorized access, testing system defences such as VPN, multi-factor authentication, network segmentation and system monitoring this project will show how providers of healthcare can protect important data and ensure system availability.

1.5 Project Structure

The structure of this project will be as follows: an overview of the security challenges we face within modern day healthcare, practical tests and solutions implemented within a testing environment, results from testing security measures and attack simulations as well as a training manual used to educate current and future staff within the healthcare organization.

The results will be provided in a detailed report strengthened by research, practical demonstrations, testing results and a cyber-security training manual catered to the healthcare personnel.

1.6 Introduction conclusion

Above all the goal of this to show why strong cyber-security practices within healthcare is essential. This is not only to ensure that systems and patients stay protected, also to guarantee compliance with modern day regulations such as GDPR.

2. Main part – Security Challenges in Healthcare

Healthcare in today's age has taken significant leaps towards digitalization, spanning from the use of digital tools to remote doctor visits and will most certainly continue to move further in this direction. However, this shift means being faced new challenges within securing these new digital systems, especially since the healthcare industry has become one the most targeted industries by cyber criminals due to the sensitive nature of patient data and the critical need for systems to always be available (Riggi, 2025). Cyber criminals will often try to exploit system vulnerabilities and steal patient information, launch ransomware attacks causing disruptions in healthcare services which puts medical patients' lives at risk (Riggi, 2025; Sarkar et al., 2021). In 2023, healthcare experienced more cyber security attacks than any other vital sector in the EU, with 309 reported major cases (European Commision – Directorate-General for Communication, 2025). A significant example of how serious a matter this is happened in Dusseldorf, Germany during the Covid-19 pandemic, where a hospital was hit with a ransomware attack forcing them to shut down their IT-systems and reroute their emergency patients elsewhere. This led to the death of one of their patients since healthcare was delayed (Sarkar et al., 2021). Another factor to take into consideration is that stolen healthcare records can sell ten times the price of stolen credit card numbers on the dark web, and that the cost to remedy a breach within healthcare costs almost three times that of any other industry which will amount in major financial loss per patient (Riggi, 2025). Failing to properly protect patient data, however, can not only harm the patient and cause significant financial loss, it can also put healthcare providers facing legal risks. Violation of data privacy laws like the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) may result in legal consequences, hefty fines and damage to the organizations reputation (Riggi, 2025).

It is safe to say that poor cybersecurity practices within healthcare not only affects systems but may put lives at risk and cause other serious consequences. Let us now look at the most common threats that health organisations are up against today.

2.1 Digital Transformation and Vulnerabilities

The digital transformation within the healthcare industry has brought with it new appliances like electronic health records (EHRs), cloud-based data storage, and IoT (Internet-of-things) enabled medical devices only to name a few. While this equipment improves things such as operational efficiency and access it also poses new vulnerabilities as before mentioned. As of today, many healthcare institutions still rely on outdated software and unpatched

systems which makes them a prime target for cybercriminals to exploit (CyberArk, 2025). Adding to that, third party applications that do not meet strict security standards and mobile devices used by staff expand the overall attack surface as well. As a by-product this creates a weak infrastructure where even a miniscule vulnerability can cause considerable damage (BD Emerson, 2025). For instance, when medical devices and administrative computers sit on the same network a single breach could allow access to a multitude of highly sensitive systems. This lack of separation gives cyber criminals the ability to move laterally within a system, which means that when they have once gained access to one device, they can navigate quietly across the whole system, reaching more critical entities. These examples are only scratching the surface of what is a much broader picture, however. As healthcare institutions continue to move into a more digitalized infrastructure, new threats will continue to emerge.

As many of these systems were not created with cyber security in mind it also leaves significant gaps in need for us to fill. Without up-to-date security frameworks as well as regular risk assessment and proactive risk management we leave the door open for attacks. This is why it is of great importance to understand what type of threats healthcare organizations are most likely to face today, and how to best protect against them.

2.2 Common Cybersecurity Threats in Healthcare

Unlike other industries, healthcare organizations store a great number of valuable information such as patient health records, insurance, credit card details, medical prescriptions, and even biometric details. This is a main reason for why it is such an attractive industry to cyber criminals. Data like this is of high value on the black market which makes the data vulnerable to exploitation. What follows are some of the most common and dangerous cyber threats facing the healthcare industry today.

2.2.1 Ransomware Attacks

Ransomware is a type of malware which infects systems and files, making them inaccessible until a ransom is paid to the attacker (Center for Internet Security, 2016). When this happens in the healthcare industry it slows down critical processes or in some cases shuts them down completely. This has a trickledown effect of delayed treatments which endanger lives in need of emergency care. The Center for Internet Security (CIS) states that hospitals need for uptime make them an attractive target and that even a minor disruption could

have life threatening consequences, which heightens the likeliness that victims will comply with ransom demands. According to the University of Cincinatti, ransomware attacks on hospitals have seen a rapid increase with 2024 marking some of the most damaging incidents to date (Bishop, 2025). The consequences of ransomware attacks are however not just operational; they may also include legal penalties, violations of patient privacy laws and a damage in reputation.

2.2.2 Phishing and Social Engineering

Phishing and social engineering attacks are common within healthcare today. In this form of attacks the attackers rely on human error and manipulation as opposed to relying on malicious code. The attempt is to trick people into giving away sensitive information by fooling staff with fake emails or calls that seem to be real (HHS, 2023). Phishing emails will often pretend to be from a trusted actor such as IT support or large companies. The email will more times include a link that when pressed downloads malware (malicious software) granting the attacker access. Some messages will even be personalized including staff names and job titles to seem more believable (Avertium, 2024). In special cases attackers will call staff members which is known as vishing (voice over phishing) or even show up in person pretending to be someone else (SecurityMetrics, n.d.). These methods are often very successful. In a report conducted by HHS (U.S. department of health and human services) several real world examples of where these kinds of tactics led to data being stolen and systems being shutdown were displayed. We conducted our own Gophish test where we sent fake emails to your medical staff in a lab environment. Our results showed that many opened the emails, some even entered their passwords showing how easy it is to fall for this form of attacks if there is a lack of training or good methods of protection.

2.2.3 Insider Threats

Insider threats is one of the largest problems within cyber security in healthcare today and is often more common than external threats. These threats come from people within the organization such employees or third party vendors, who either knowingly misuse their access privileges to do harm or unintentionally compromise system data through negligence. Insider threats within healthcare often involve unauthorized access and or sharing of confidential patient data and is often driven by financial motives or lack of

security protocol awareness (Vibert, 2024). Healthcare systems are especially vulnerable since wide access to things like electronical health records are essential for staff members to do their job, which increases the risk of security breaches. Traditional safety measures such as firewalls and anti-virus software often fall short on detecting insider threats because it comes from actors who already have access (CyberArk, 2025), making it less challenging for people with inside access to carry out attacks without triggering any alarms. Adding to what has previously been mentioned by In Lee from the Multidisciplinary Digital Publishing Institute (2022), many insider incidents happen by accident, adding another layer of difficulty to spot them before they can cause any damage. Because of medical staff having wide access and the difficulty of spotting incidents early, insider threats within healthcare are especially hard to combat.

2.2.4 Unsecured IoT Devices

The use of IoT (internet of things) devices within healthcare continues to grow, equipment such as infusion pumps, heart monitors and imaging machines also bring forth a new set of cyber security risks. Since many of these new devices do not have strong security features built-in and often are either un-patched or misconfigured it makes them easy targets for an attacker (Business Wire, 2022). When breached these devices may be used to steal valuable data and even serve as points of entry to larger areas within the healthcare network (Hunter, 2024). Some of the most vulnerable equipment within medicine today include insulin pumps, defibrillators and remote monitoring devices. According to Elliot Anderson from Lumify Cyber (2024), studies have shown that the strong need to always keep this equipment online often outweighs routine security checks, creating gaps that cyber criminals tend to exploit, a situation where lifesaving technology becomes a silent threat (Alzubaidi et al., 2020; Elsayed et al., 2025). These risks are of course made worse by the lack of regulatory security procedures and the long lifespan of medical equipment which may go a long time without regular updates if any updates at all. As the scope of connected IoT devices continues to expand, so does the attack surface. Turning lifesaving equipment into a potential threat.

2.2.5 Third Party and Supply Chain Risks

Third-party and supply chain risks within healthcare as it pertains to cyber security means the threats are brought forth by external partners. This can range from software companies,

equipment suppliers or any other service provider with system access. If any one of these external partners have weak security practices, it creates holes in the security infrastructure which hackers can exploit. It therefore is not enough for the healthcare provider alone to have strong security practices (Censinet, 2024). Often times third-party vendors will not have strong or as strong security practices as their healthcare counterparts and therefore become attractive targets for cyber criminals. Once a third-party vendor has been breached, hackers may steal private information, install malware etc. In certain cases, the vendor may provide important solutions, such as cloud-storage or laboratory software and when attacked it can lead to delays getting test results, treatment cause other complications (Muoio, 2025). In adding, when attackers gain access to a third-party within the supply chain, they have the potential to move laterally within the network reaching more critical areas unnoticed and causing even greater damage (Cedar Rose, 2025). Since outside actors are not in the company's control, it becomes very difficult for healthcare organizations to secure every aspect of the supply chain. As we move towards a more digitalized supply chain with things like remote diagnostic tools and online ordering platforms, every new partner can become a potential security risk.

2.2.6 Weak Authentication and Access Control

Weak authentication and access control are two big issues within cybersecurity in healthcare. Many healthcare institutions today still rely on old systems which are not updated regularly, that do not use multi-factor authentication, that use weak passwords and are granted too much trust (Mahan, 2024). A lack of strong password policies makes systems susceptible to brute force attacks, which is when cyber criminals use automated software to guess the password of users until they have gained access. Frail authentication methods like a single password without extra security steps like biometrics or ID-cards also make it much easier for criminals to gain access. Once inside the system they can cause an array of damage like stealing valuable data or shutting down important systems (Al-Qarni, 2023; Kolbasuk Mcgee, 2024). Having wide access also makes it easier for hackers to move around in the system once it has been breached. When staff members are given more privileges than what is needed for them to do their job a breached account has the potential to cause damage to a larger part of the organization (Dhinakaran et al., 2025).

2.3 Cybersecurity Requirements in Healthcare

Healthcare providers have moral and legal obligation to guarantee confidentiality, integrity and availability of sensitive medical data and patient safety. They are therefore under immense pressure to implement security strategies that ensure the safety of what is known as the CIA triad. This is of course being fuelled by the increase of cyberthreats we are seeing today accompanied by data protection laws being very strict on matters of confidentiality. In this part we will cover the key elements in ensuring that modern day healthcare organisations stay up-to-date, law abiding and most of all secure. Or in other words answering the question, what does a healthcare organization need to stay secure today?

2.3.1 Regulatory Compliance

One of the key elements within modern healthcare today is making sure they stay in compliance with laws and industry regulations. In the EU (European Union) Personal data like medical health records must be stored, shared or used in accordance with the General Data Protection Regulations (GDPR). Providers of healthcare must have strong established technological and organizational protections since they are seen as controllers of data and therefore carry a huge responsibility. If they fail to do this, they may face huge fines of up to 20 million euros or 4% of their worldwide revenue income (GDPR Advisor, 2024).
The Health Insurance Portability and Accountability Act (HIPAA) plays a similar role in the United States, where it demands that healthcare institutions provide protection to personal health information (PHI) using physical, administrative and technical safety methods (Data center Info, 2025). Other initiatives are also moving forward, like the NIS2 Directive in the EU and other frameworks in North America which place more weight on healthcare organizations to improve their overall cyber defence practices (Golani, 2024).

2.3.2 Security Standards

Not only does healthcare organizations have to comply with legal guidelines, but they must also follow well recognized security standards. This is to ensure that the best practices in protecting sensitive data are the ones being used. These security standards provide clear guidelines for managing risks, system security and proactiveness. One of the most known

and commonly used strategies is the NIST (National Institute of Standards and Technology) cybersecurity framework. This specific framework consists of five cybersecurity pillars which are: Identify, protect, detect, respond and recover. This helps organizations have a better understanding of the risks within cybersecurity and what measures to apply in each step of managing any threats (NIST, 2022). Another important standard is **ISO/IEC 27001** which is a framework which purpose is to systematically improve and manage and organizations information security and help implement what is known as an information security management system (ISMS). It includes policies, procedures, and controls that makes it very relevant within the healthcare industry (Ann, 2023). For healthcare providers operating in the U.S. the HIPAA security is a primary standard and contains rules that require physical, administrative and system security. It also a great deal of importance on measures such as access control, logging and encryption to safekeep patient information (HHS Gov, 2024). Other known standards include:

- **HITRUST CSF –** which is a certified framework that combines standards (from ISO, NIST and HIPAA). This framework simplifies meeting security needs for healthcare organizations (Databrackets, 2022).
- **SOC 2 Type II –** A framework based on five service trust criteria which are: security, availability, integrity, confidentiality and privacy. This framework is often used by third-party vendors which manage healthcare data (Sprinto, 2024).
- **CIS Controls –** are a set of sequenced, guided and simplified practices which organizations can use to improve their overall security standings (Center for Internet security, 2016).

It is important to note that most standards are auditable, meaning that they can be certified and checked for compliance which makes it easier to stay within legal boundaries. Frameworks like these help health organizations meet security demands, strengthen security and protect patients' personal safety.

2.3.3 Risk Management

Risk management in healthcare consists of analysing processes and practices within the healthcare organization to identify potential risks, then to assess the likelihood of an incident occurring and the potential damage it could bring. Finally, to implement controls to prevent these risks from manifesting to prevent losses and optimize profits (Adler, 2024).

The risk management process includes five key steps, which are: risk identification, risk assessment, risk evaluation, risk mitigation and risk monitoring which is a systematic approach to dealing with potential threats and a general industry practice (MetricStream, 2024). The overall goal within risk management is of course to minimize them. It is therefore important to question what some of these risks are.

Healthcare establishments face a multitude of risks that include, data breaches and unauthorized access etc. (while only mentioning the cyber related ones). These threats can lead to a breakdown in operations which puts patients at risk and can lead to other consequences as well. Since 2014-2015 and onwards many larger healthcare institutions specifically in the United States began adopting an Enterprise Risk management model, which categorises risks into 8 separate domains, which are:

- Operational
- Clinical & Patient Safety
- Strategic
- Financial
- Legal & Regulatory
- Technological
- Enviromental & Infrastructure Based

This helps institutions with mapping down weaknesses and address them across all areas of the organisation (Nejm Catalyst, 2018).

2.3.4 Access control

Access control is a security measure which helps manage and limit access to assets, systems and facilities within a company's infrastructure (LaViola, 2023). In healthcare it is particularly important to carefully monitor and restrict who has access to certain information due to the high sensitivity of the information and data that is being handled (electronical health records etc.)

Modern day access control tactics usually consists of a combination physical and digital safety measures (like keycards, and multi-factor authentication). These tactics are often outlined from the principle of least privilege which means that staff members get the minimum amount of access they need to do their job (Hameed, 2024). Three basic

components of effective access control are identification, authentication and authorization. Identification is there to determine who an individual is, authentication is there to verify and strengthen that claim and authorization dictates what an individual has overall access to based on rules and roles within the organization. Authentication is done by what is known as a multi-factor authentication, which works by combining two or more components of the following: *something you know* (most often a password), *something you have* (a keycard, smartphone or a USB), *something you are* (biometric fingerprints or a retina scan). This is a layered approach designed to make it much harder for attackers. With this approach an attacker will not get access even if they compromise one factor like cracking a password for example (NIST, 2024; Rublon 2021).
Having well established access control as obligatory company procedure significantly decreases the chances of unauthorized access and data breaches.

2.3.5 Zero Trust Architecture

Zero trust architecture is a cyber security standard which entails that no user, device, or program can be fully trusted by default. On the contrary, it always wants to assume the opposite or the worst, whether it being inside or outside the network. This concept was brought forth by John Kinderwag in 2010, Kinderwag saw holes in traditional perimeter-based security models and argued that organizations would be left vulnerable once a perimeter has been breached without a Zero trust architecture (Kinderwag, 2010). With the increase of online medicine and remote access systems becoming more common, Zero Trust has risen in popularity as one of the safest ways to protect data. Unlike other frameworks, zero trust demands strict verification methods and the application of the principle of least privilege (HHS, 2023).

Some of the key components of zero trust architecture are the following:

- **Continuous verification** – verifying your identity with each new logon.
- **Micro segmentation** – separating networks into smaller sections, minimizing the potential for lateral movement.
- **PolP Access (principle of least privilege)** – users have the smallest amount of access they need.

- **Assume the worst** – designing the infrastructure with the expectation of an attacker already being present in the system.

Security tools like multi-factor authentication (MFA), and strict access controls are strengthened in effectiveness with the zero-trust approach since verification is continuous and nothing is trusted automatically (Rublon 2024; NIST, 2020). Applying these methods is extremely important for healthcare organizations managing remote access and third-party access, especially because of the rise in cyberthreats.

2.3.6 Encryption & Privacy

Encryption is a security method which is used to protect data confidentiality and integrity. With the increase of cyber threats, encryption spearheads security defences against unauthorized access to sensitive data like medical health records and test results (HIPAA Journal, 2020). Encryption transforms data into an unreadable code, meaning that even if a breach occurs, the data being stolen will be of little use without decryption. While delving in to the intricacies of encryption and all it entails is outside of the scope of this project, it is important to recognize the role encryption plays on multiple levels of cybersecurity today, specifically in a defence-in-depth strategy. In this project encryption is incorporated through tools such as Tailscale VPN which makes use of encrypted tunnels to secure remote network connections between end devices (HIPAA Journal, 2020; Intellisoft, 2024).
Together, methods like encryption and multi-factor authentication form a firm foundation for secure healthcare environment practices.

2.3.7 Intrusion Detection & Monitoring

Intrusion detection systems (IDS) play a big role of maintaining security of Internet of Things based networks (IoT-net). With the increase of cyberattacks targeting electronic healthcare, logging and monitoring abnormal behaviour that could signal an attempted attack, or breach is a key factor (Akram et al., 2021). Proactive monitoring makes way for early responses and mitigation, lowering the chances of harming patient safety and operational damage. In this project, we approach this by using Nmap (via Kali-Linux) for reconnaissance purposes and vulnerability testing followed with Windows built in logging tools for activity

auditing. These combined practices will provide insight to penetration attempts, port scans and violations of policies etc. While not being as advanced as mainstream IDS platforms, this approach still aligns with the defence-in-depth principle and demonstrates a solution to monitoring in a real world healthcare work environment (Sharma & Mukherjee, 2023).

3.0 Practical (testing & results)

3.0.1 Virtual environment overview

In order to implement and test the practical methods of this project in a safe and controlled environment, a virtualized space using VMware workstation was created. This setup is meant to imitate a real IT healthcare work environment, which makes it possible to test components such as segmentation, remote access and VPN configuration while not exposing any real threat to systems, networks and data.

The virtual machines that were chosen for this practical step are as follows:

- **Server 1 (Windows server 2022) -** This server will act as our **Domain controller** and **DNS** server, also managing Active Directory and our authentication policies.
- **Server 2 (Windows server 2022) -** will serve as our application server hosting **Tailscale VPN** for secure remote access for clients**.**
- **Windows 10 client –** will be a **domain-joined** client and simulate our healthcare staff computer.
- **Kali Linux –** will be our attacker, used to simulate potential threats like **Phishing** and **Port Scanning**.

These Virtual Machines will all be connected through a manual and isolated (static) connection, apart from Kali-Linux which is meant to sit outside the network for attacking purposes. They have also been set up with a sufficient amount of **CPU**, **RAM**, and storage to facilitate a realistic work environment.

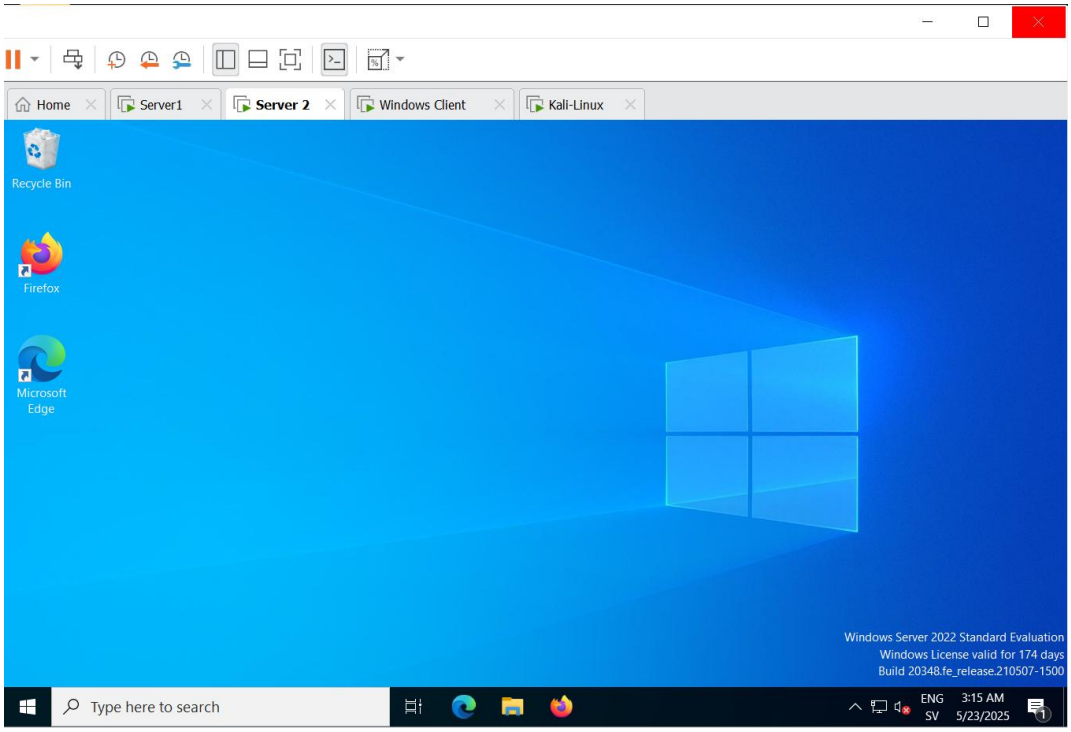

Figure 1: Virtual machine setup in VMware workstation, showing all machines.

3.0.2 Active Directory & DNS Configuration (Server 1)

In this step Active Directory Domain Services (**AD DS**) on Server 1 was configured to handle services such as user authentication and access control from a central point. This is also where users accounts, client devices, and security policies are created, managed and maintained, using tools such as Active Directory Group Policy Management Console (**GPMC**) and Active Directory Users & Computers (**ADUC**).

Server 1 will also manage **DNS** (Domain name system) which is necessary since it allows the virtual machines to find each other on the network with ease. Additionally, a domain which we gave the name **TMedicine.local** was created which will be the central hub for all connected virtual machines and serve as the simulated intranet (internal network). This is also where organizational units (**OUs**) was created using Active Directory Users & Computers (**ADUC**) and placed our medical staff for example.

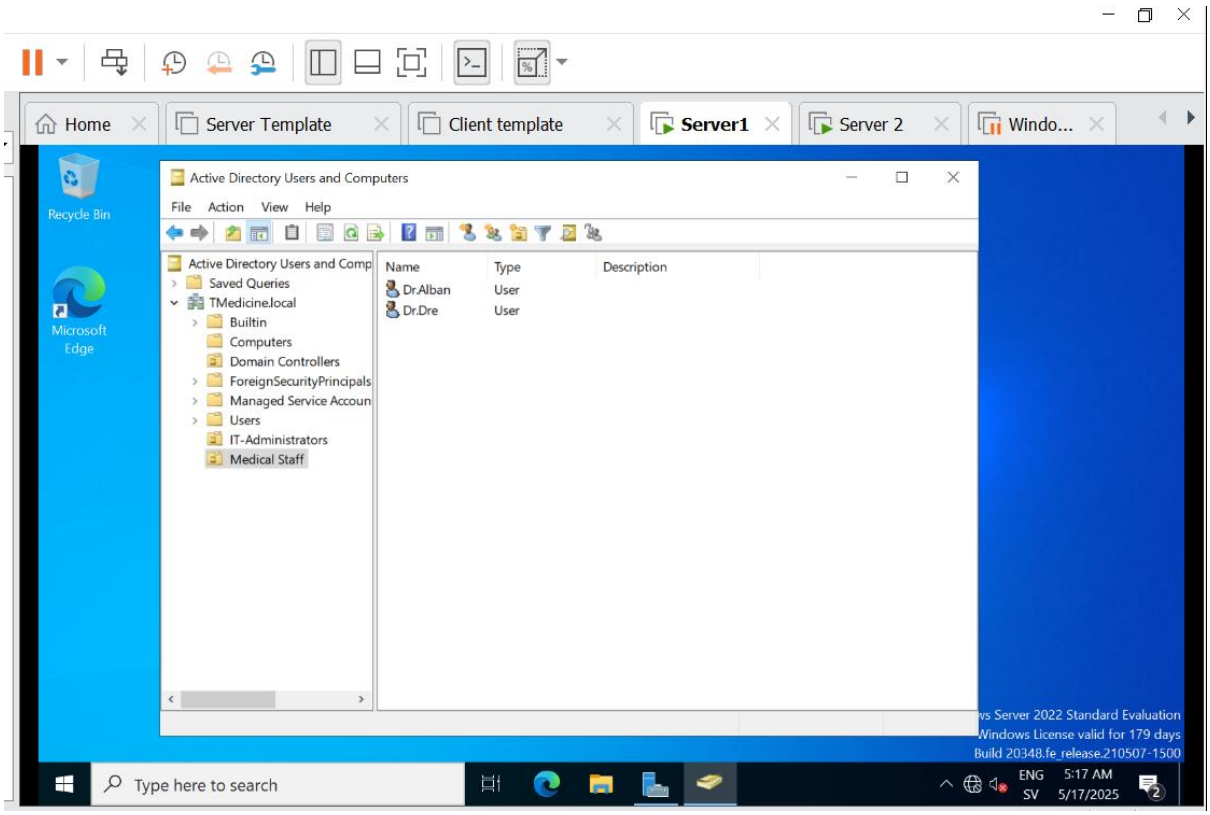

Figure 2: Medical staff members placed in the Organizational Unit.

Configuration steps included:

- Promoting Server 1 to a Domain controller using **AD DS** server roles.
- Adding a new forest (creating a new domain) and naming it **TMedicine.local**
- Adding Organizational Units to our domain (IT & Medical staff).
- Creating client user accounts to represent IT and medical staff within their respective organizational unit (*as shown in figure 2).*
- Setting up a **DNS** so that our Virtual machines can find eachother on the network and pinging them to test connectivity.
- Managing **Group policies** to apply security settings such as:
- Strong password rules
- **RDP** (remote desktop protocol) access for IT personnel only
- Automatic screen lock after a time limit.

These settings will help govern how users may interact with the system and reduce security risks as well as giving us an organized overview of our organization to simplify control.

3.0.3 VPN Configuration (Tailscale) & Remote Access

To enable secure access remotely, a Virtual Private Network (VPN) was configured using an application known as **Tailscale-VPN** on Server 2. As before mentioned, a VPN creates encrypted tunnels for secure access between networks. Fot this project Tailscale was chosen for its simplicity of set up purposes. It is also a low cost and high-quality solution. Tailscale-VPN makes it possible to connect the created Windows 10 client accounts to the virtual test environment (Server 2) remotely as a proof-of-concept. Before downloading and installing Tailscale-VPN however, we made sure to domain-join the Windows client to our **TMedicine** .**local** domain (*as shown below in figure 3*).

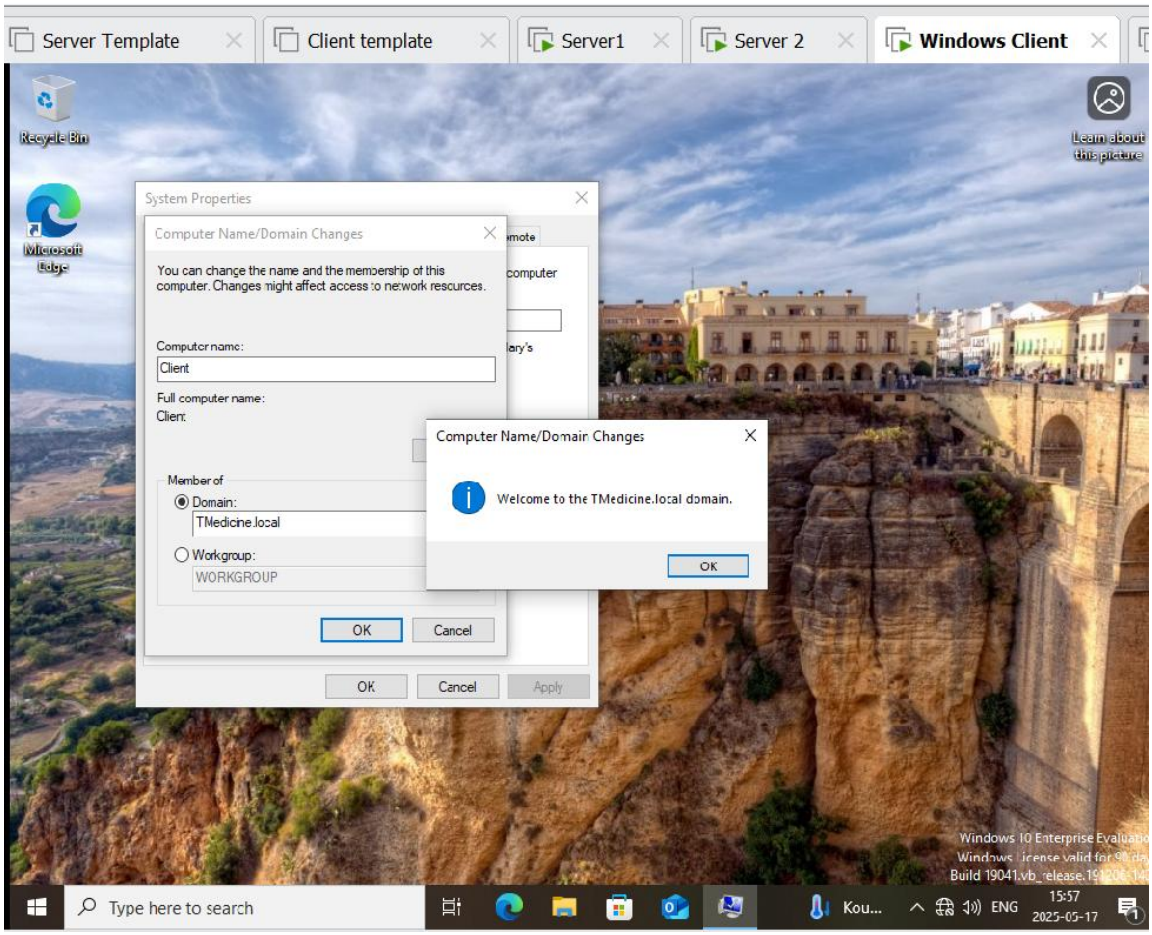

Figure 3: Successfully domain-joining the Windows 10 client to the TMedicine.local domain.

After this step was concluded, we began configuring **Tailscale-VPN**
Configuration steps included:

- Installing **Tailscale-VPN** on **Server 2**.

- Logging in to **Tailscale** on **Server 2** and registering **Server 2** to our **Tailscale network (Tailnet)** *(as shown in figure 4).*
- Authorizing Server 2 using the Tailscale admin console and verifying it being active.
- Installing **Tailscale** on the Windows 10 client and configuring it to create a secure VPN tunnel to Server 2.
- Establishing a **VPN** connection between the Client and Server 2 *(as shown in figure 5)*.
- Testing the **VPN** connection and confirming the connection status between the Windows 10 client and Server 2.

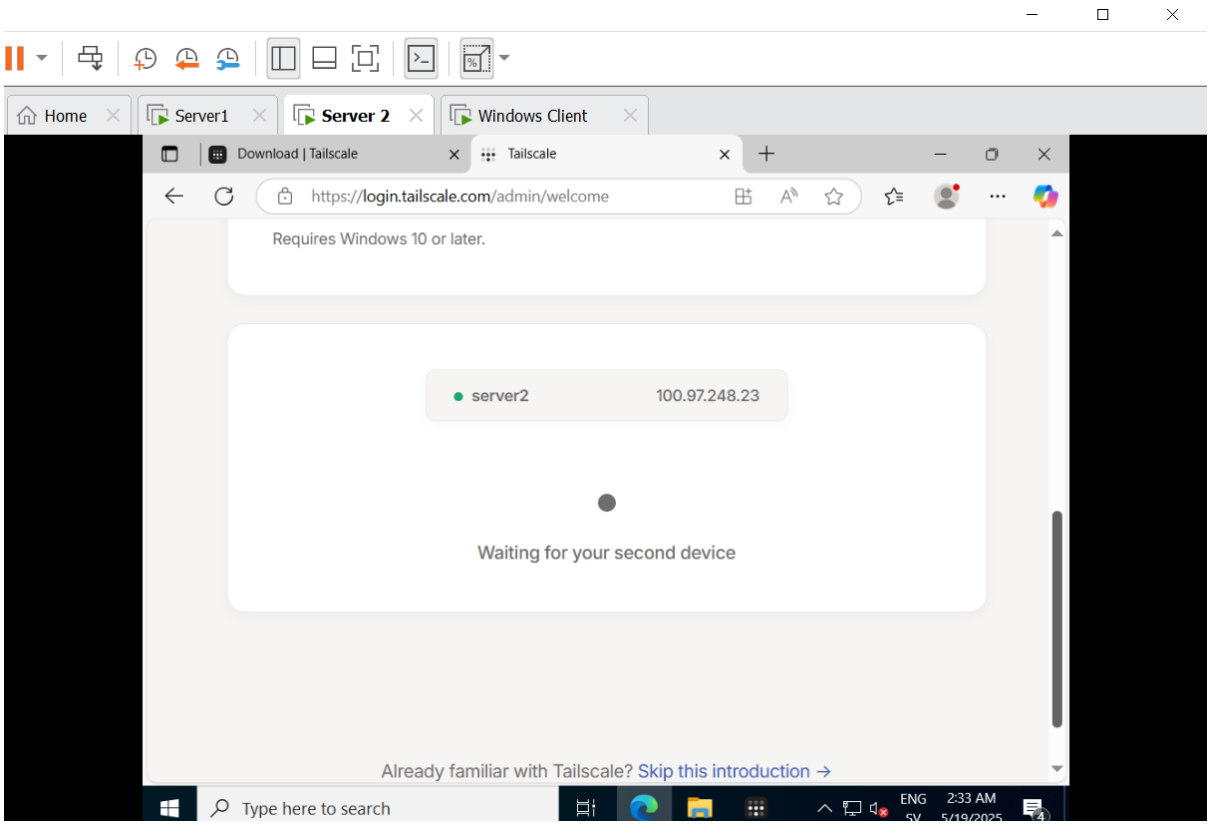

Figure 4: Successfully registering our Server 2 to our Tailscale network (Tailnet).

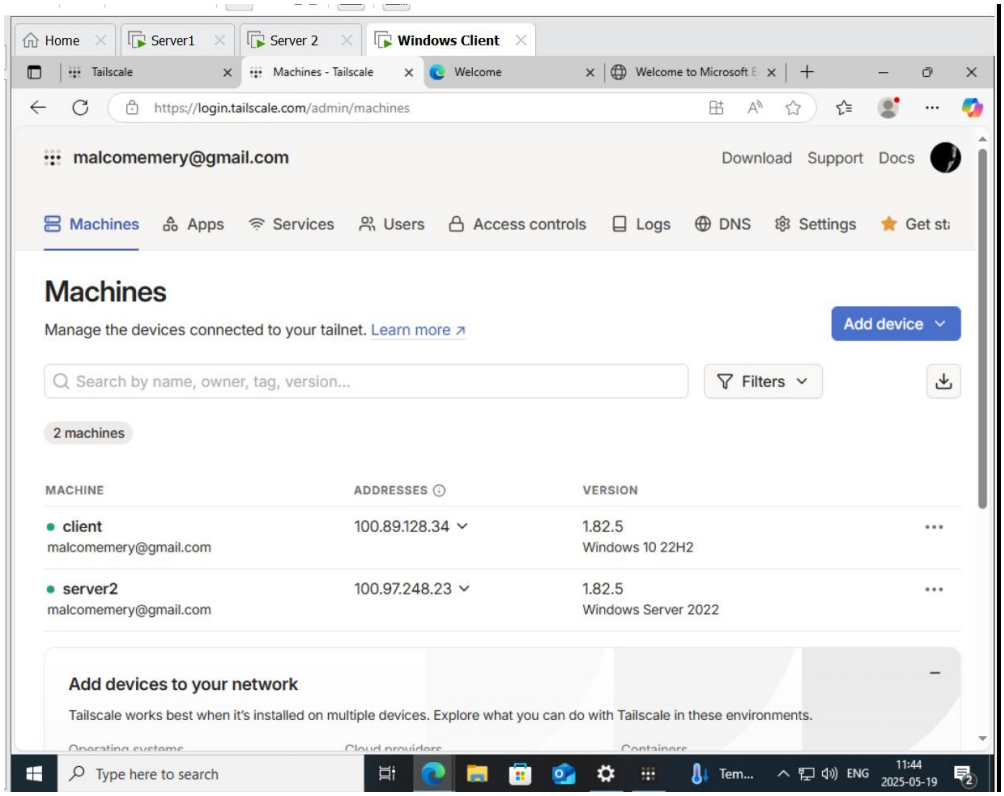

Figure 5: Displays an established VPN network connection between the client and server 2.

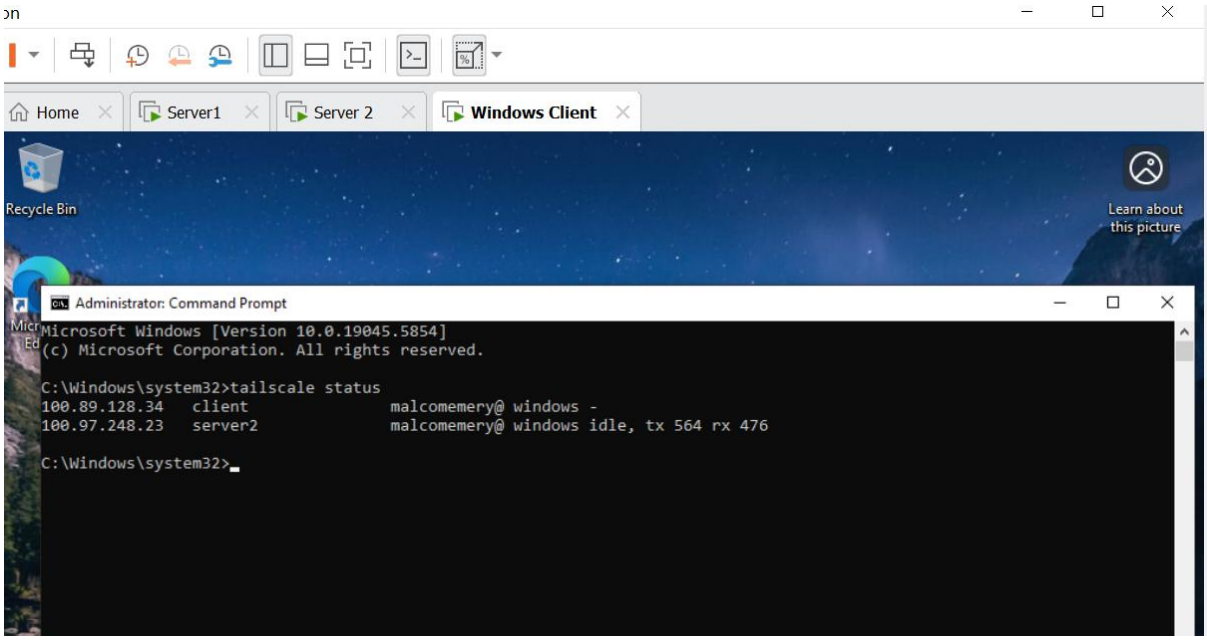

Figure 6: Shows a verified VPN connection status between the client and server 2.

After verifying the established VPN connection (both the client and server 2 were on the same network and communicating), we moved on to testing secure remote access through an encrypted VPN tunnel. By doing this successfully, we displayed **proof-of-concept** on how healthcare staff can access the internal system in a secure way using our simulated test environment.

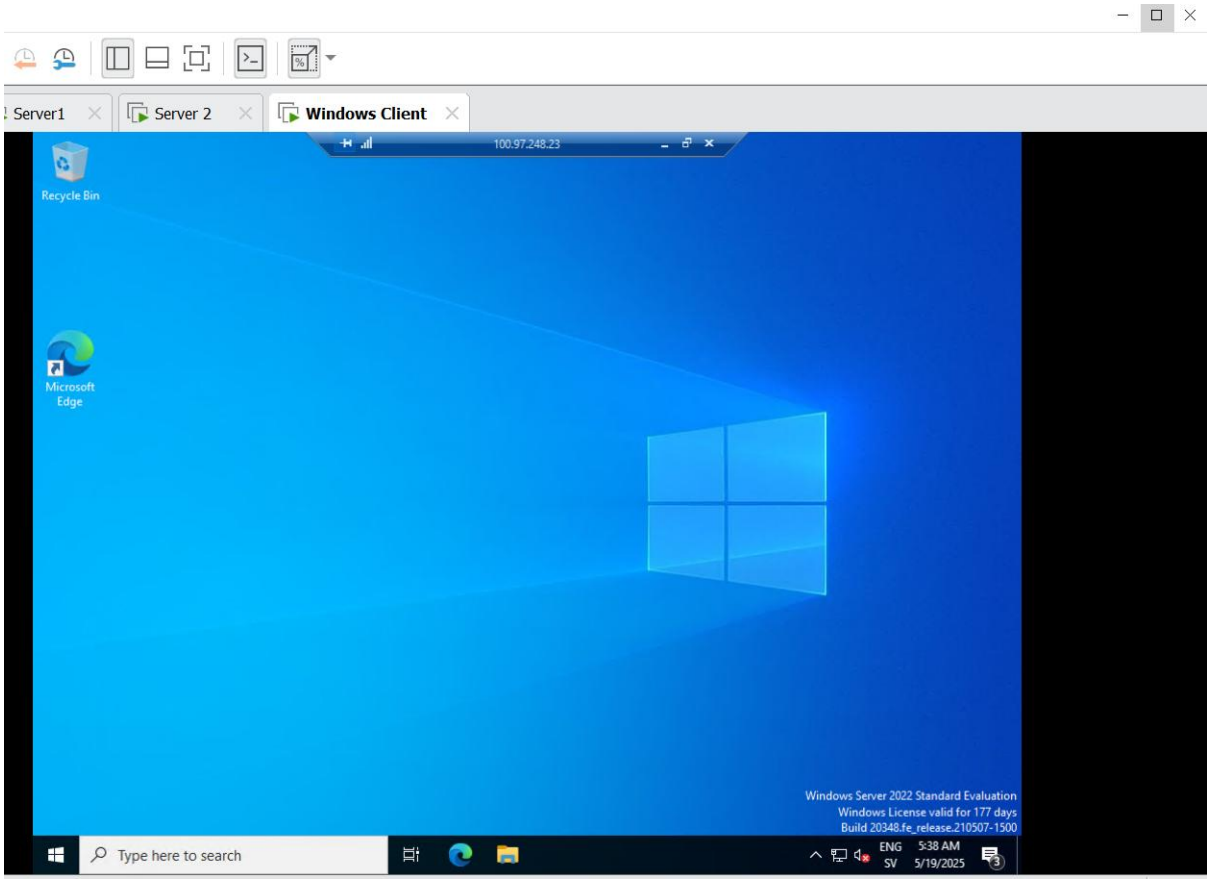

Figure 7: Successful Remote Access login to Server 2 using an encrypted VPN connection.

3.0.4 Multi-Factor Authentication (MFA) Implementation

To further add a layer of security after the previous step, multi-factor authentication was set in place using Google's own 2 step-verification method. This makes sure that just a password is insufficient to login to the system. In our proof-of-concept setup, clients attempting to sign in remotely using the Tailscale-VPN application must approve a login notification sent to a registered mobile phone, adding more certainty that only registered staff members have access to the secure connection (NIST, 2020; Rublon, 2021).

By enabling 2-step verification on our Google account linked to Tailscale-VPN we allowed a push notification to be sent our client mobile device when a login attempt is made on either Server 2 or the Windows 10 client. This ensures that access only is granted once the user confirms their identity using two factors: password and mobile phone.

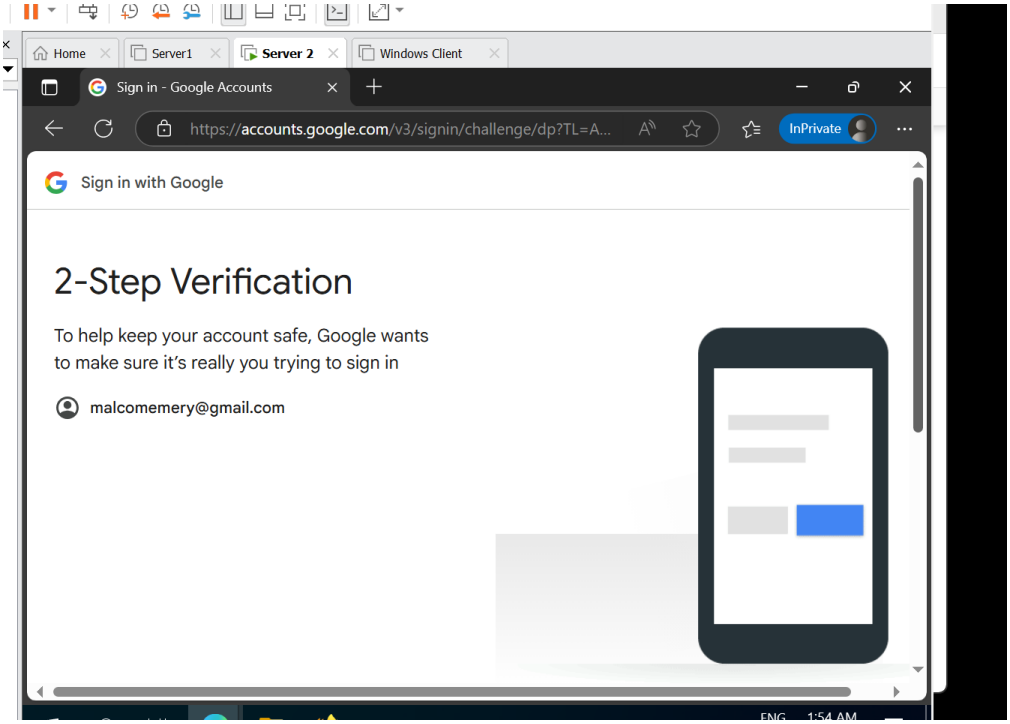

Figure 8: Multi-Factor authentication prompt during our VPN login attempt.

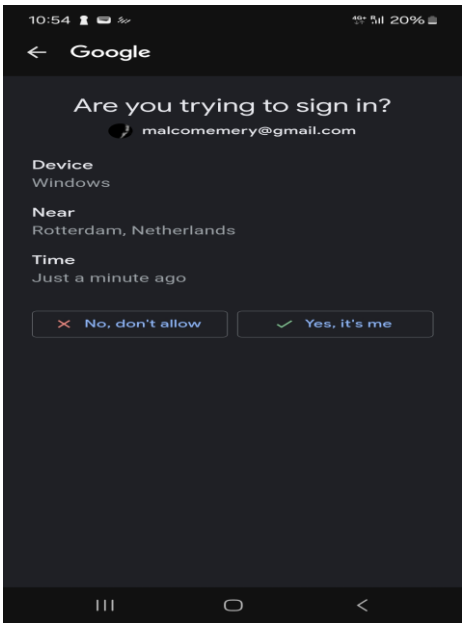

Figure 9: Push notification delivered to the mobile device to allow access.

An encrypted VPN connection combined with our multi-factor authentication improves our test environment strength against unauthorized access, creating strong foundational pillars which we further will improve upon using internal security measures such as network segmentation.

3.0.5 Network Segmentation and Internal Access control

To strengthen internal security and lower the risk of inside threats moving laterally within the network, we implemented strict access control and some basic network segmentation including Windows firewall rules, group policies (GPOs). By applying these methods, we will restrict unwanted access, control communication and enforce measures such as the zero trust architecture and the principle of least privilege. To start things of we implemented a new inbound rule in Windows Defender Firewall on server 2 that only allows the Remote Desktop Protocol (RDP) from trusted IP addresses.

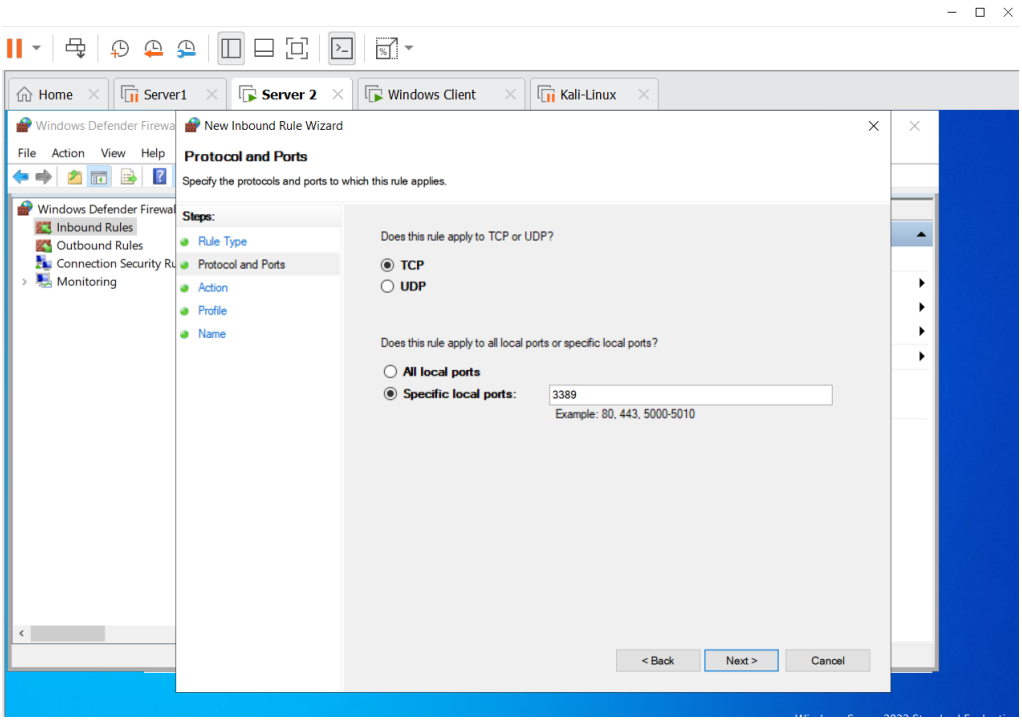

Figure 10: RDP port 3389 inbound rule created in Windows defender firewall.

Moving along, we tailored this rule by scoping it to block out devices that sit outside the internal network, in our simulated setup that specifically meant blocking out our attacker (Kali-Linux 192.168.213.131). while this rule now was implemented in our simulated setup, it is meant to represent blocking out remote access from any IP address sitting outside the internal network, even if the attacker tries to use the right door (RDP over port 3389) the firewall will deny access.

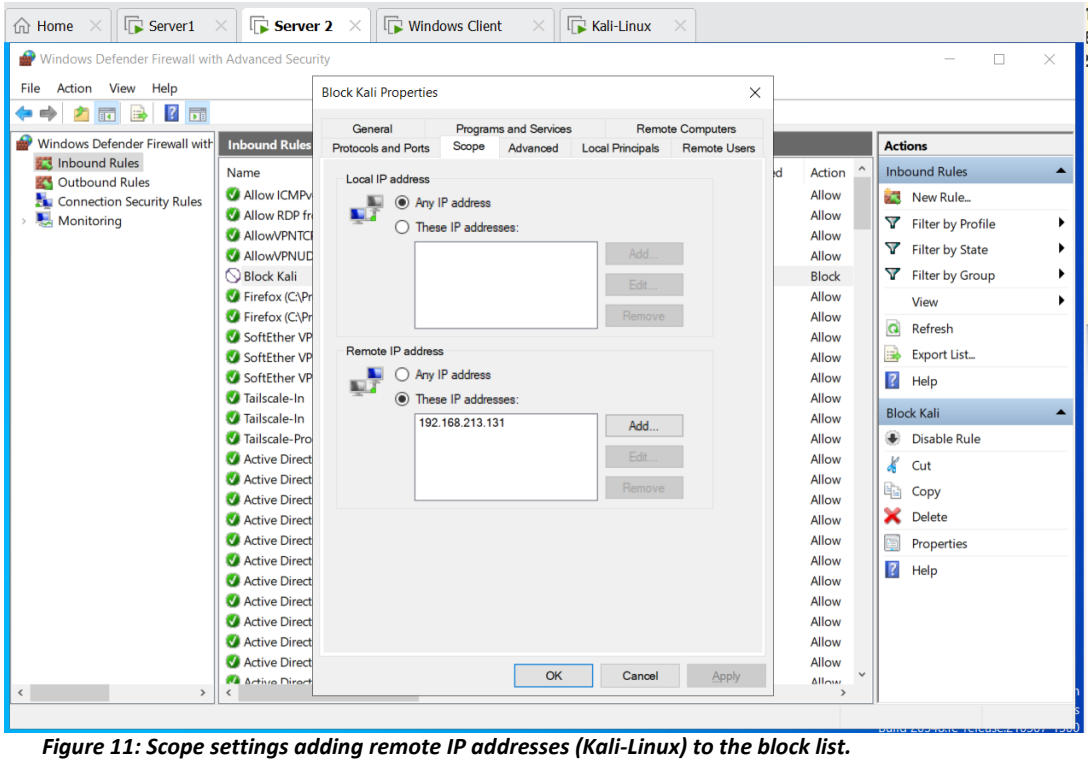

Figure 11: Scope settings adding remote IP addresses (Kali-Linux) to the block list.

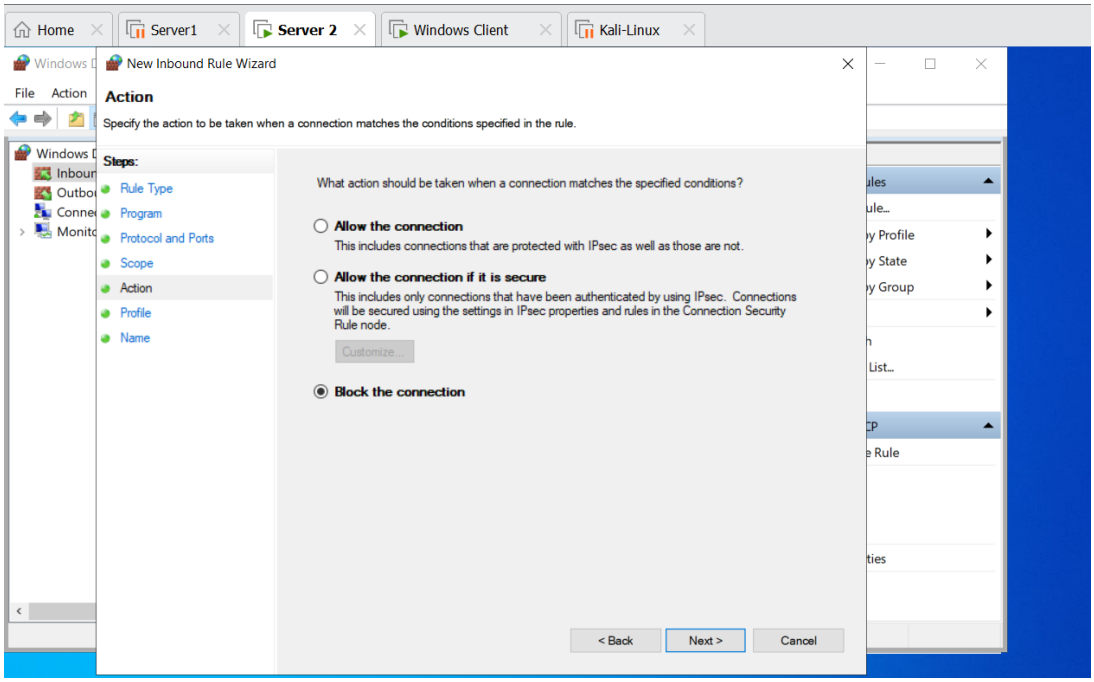

Figure 12: Action to block the connection to remote IP-addresses.

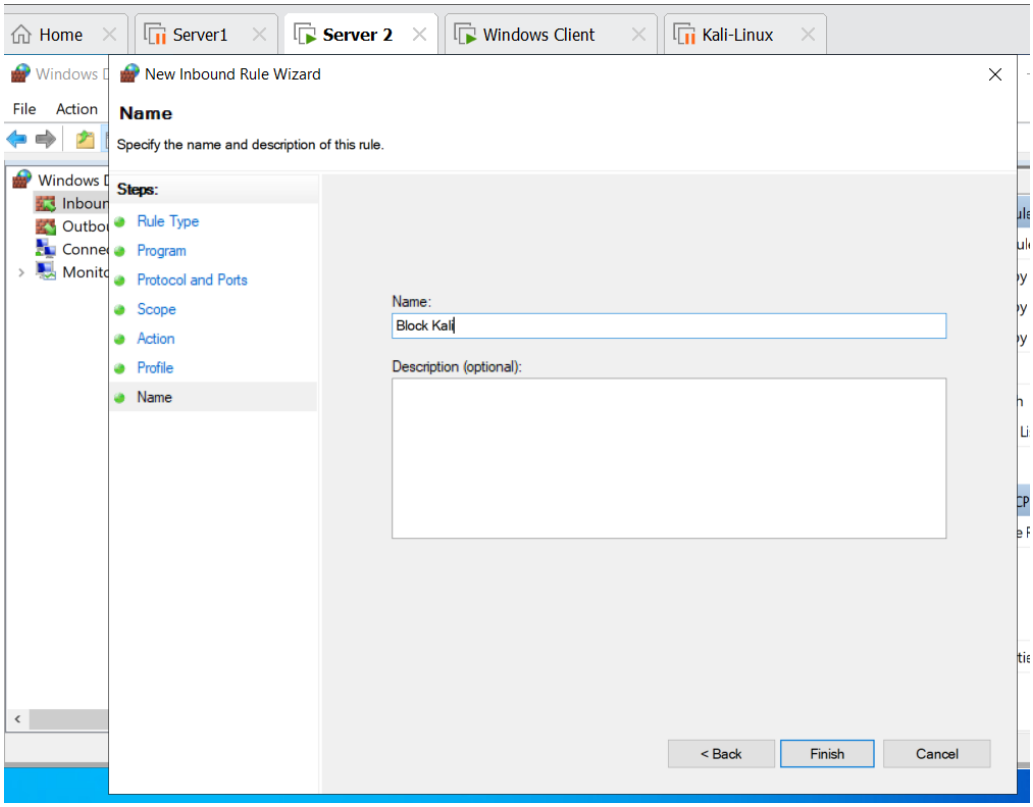

Figure 13: Final step in our inbound rule setup blocking remote IP-addresses.

To add our firewall rules, we also applied Group Policy Objects (GPOs) to create access restrictions internally within the network. An example of this would be that we limited Remote Desktop Protocol logins to our IT-department solely, making sure that medical staff lacks the access to critical parts of the system. This will however not collide with the remote access we implemented via Tailscale-VPN which is the intended way we want our medical staff to remotely access the network.

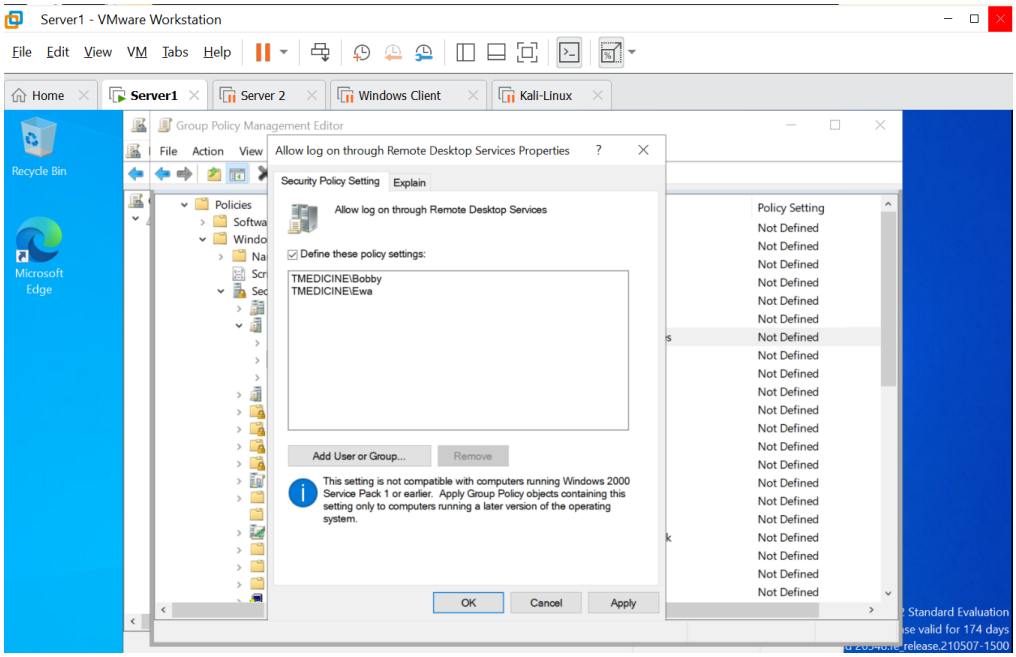

Figure 14: GPO displaying RDP access restricted to our IT-administrators.

As well as Remote Desktop Protocol restrictions, other Group Policy Objects were added to strengthen the overall defences, these policies include strong passwords, account lockout policy and screen lock timers that align with a zero-trust architecture.

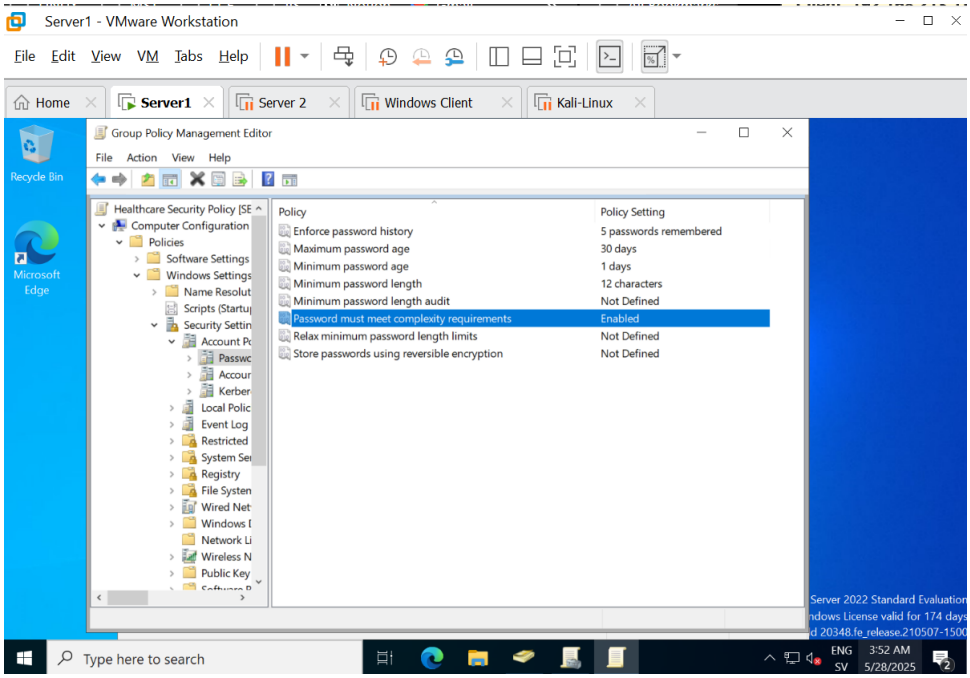

Figure 15: GPO displaying strong password complexity requirements.

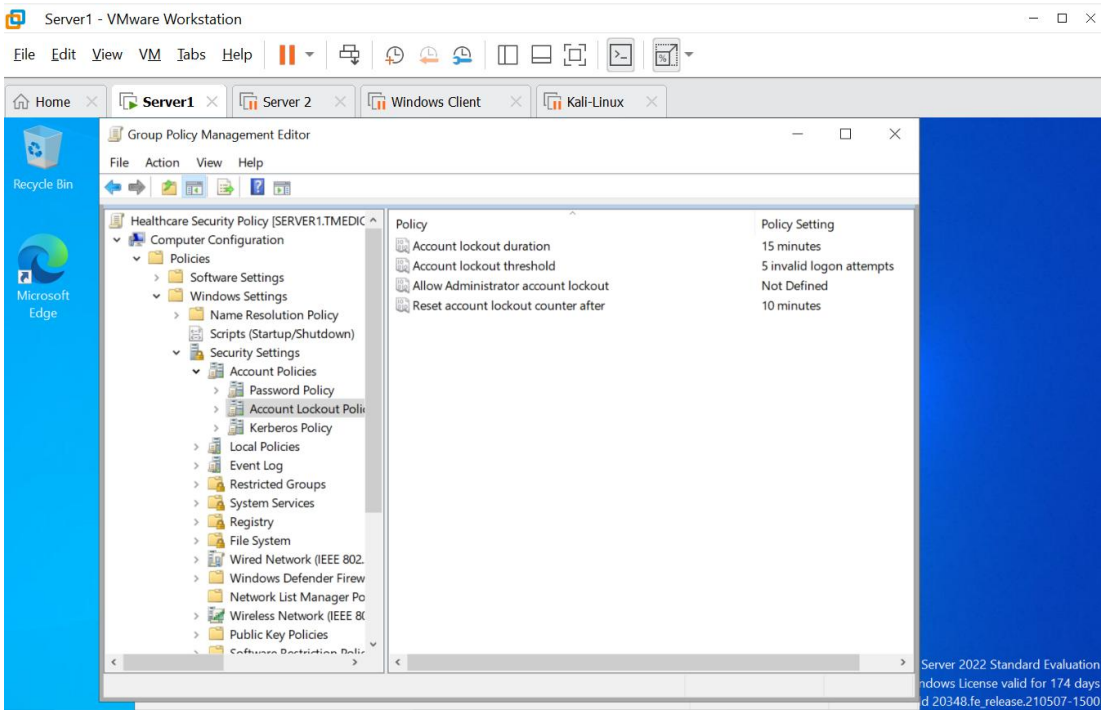

Figure 16: GPO for account lockout policy.

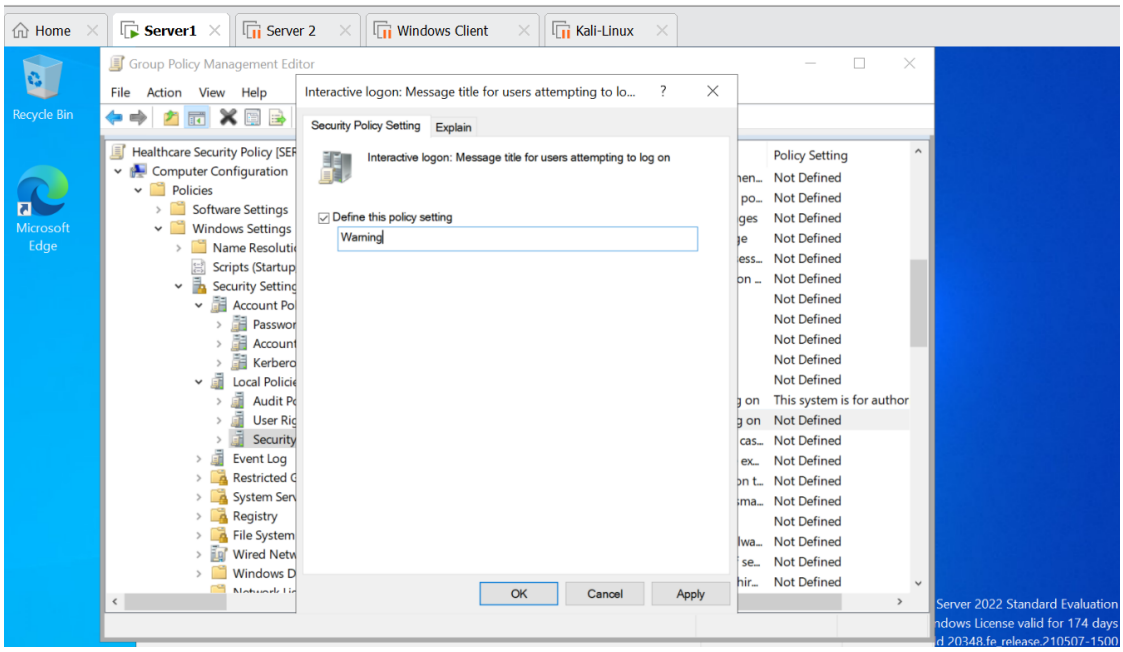

Figure 17: GPO displaying message warning.

The warning message *(as seen above in figure 17)* has the purpose of raising the awareness of cyber security within the healthcare staff, reminding them potential risks and behaviours as well as legally protecting the organization in a way of showing they were warned about monitoring as well as terms of use, etc. While the action may seem small in a grander scheme it does align with a defence-in-depth approach where every layer of added security is an important step. These firewall rules and policy implementations form the groundwork for a solid network segmentation and internal access which reduces our overall attack surface and therefore increases security in our **TMedicine.local** domain.

3.0.6 Security Awareness & Phishing Simulation

In this part of our project the intention is to test the human aspect of our defences by simulating a phishing campaign using **Gophish** from our Kali-Linux VM (virtual machine). Since healthcare organizations are the most targeted sector for cyberattacks such as phishing it is a critical area for staff members to be aware of and know how to deal with in a secure manner. Using **Gophish** we set up a fake phishing campaign that sent out deceptive emails masquerading as being from the IT-department of the healthcare organization. These emails include what is known as a **landing page** that we can use to measure how many staff members clicked on what we masked as a “security update briefing” for healthcare personnel. We can later use these statistics to strengthen our claim as to why it is important

to understand the effectiveness of phishing and why we need to train our staff to counteract it. To complete this we downloaded Gophish on our Kali-Linux VM unzipped the file using our bash terminal, we then launched the application by running the command *sudo ./ gophish.*

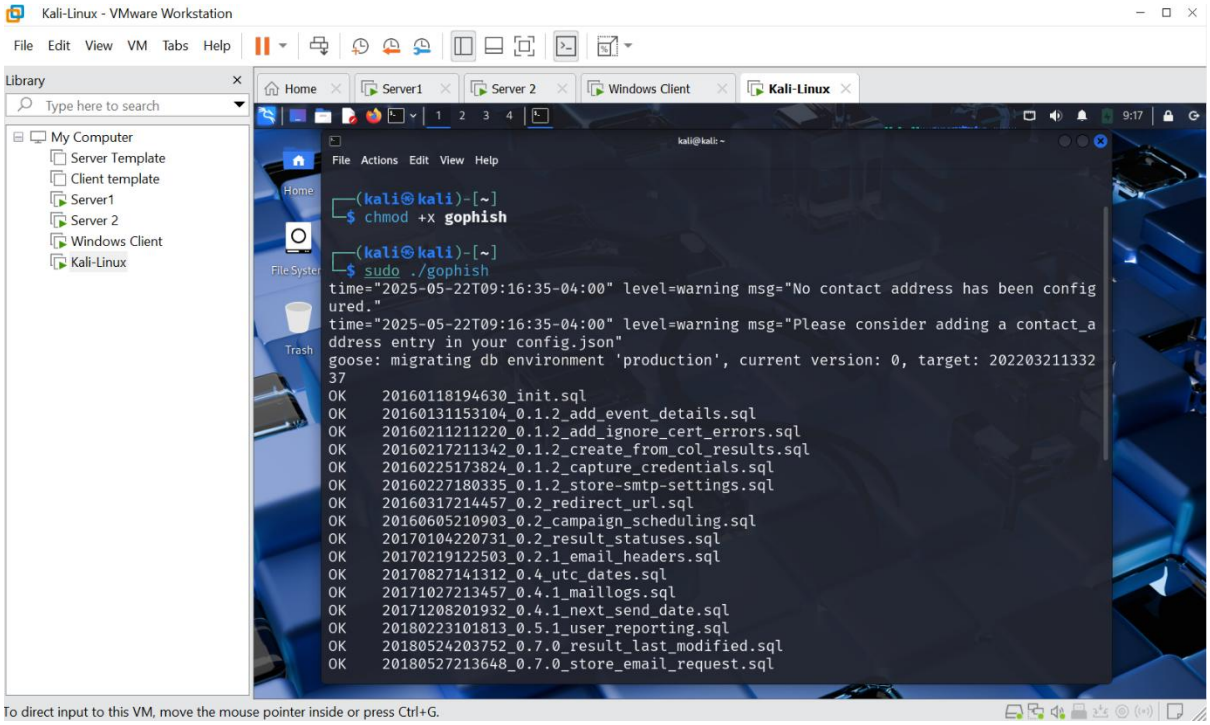

Figure 18: Running the command sudo ./ gophish in the Kali-Linux terminal.

This command will start the administrative panel and the phishing server. Once these services were running, we opened the web browser on our Kali-Linux virtual machine and typed in our localhost IP address **192.168.213.131** followed by **:3333** to take us to our **Gophish** login page. However, this sets up alarm bells for our firewall and were prompted with a URL warning for a potential security risk *(as shown below in figure 19)*. It is important to note that this is prompted for a reason and that in regular cases we should not go beyond this step if we are not certain where it will take us as a safety precaution. In this case we did know that it would be safe and therefore clicked *advanced* followed by *take me there* anyway.

This lands us at the Gophish sign-in page *(as shown below in figure 20),* where our username is admin and the password gets prompted by the terminal.

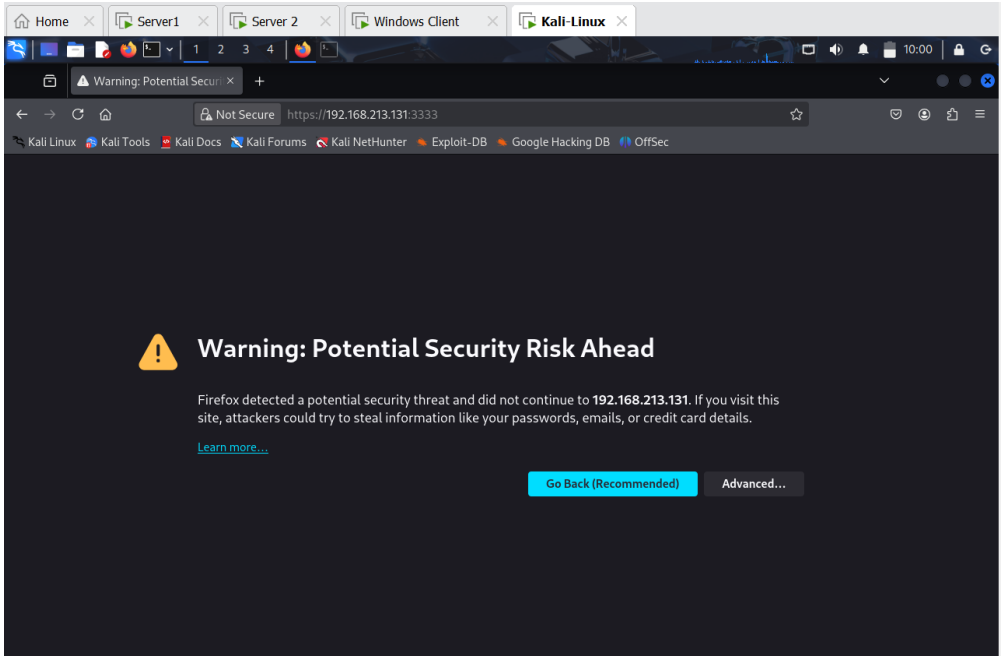

Figure 19: URL warning for potential security risk.

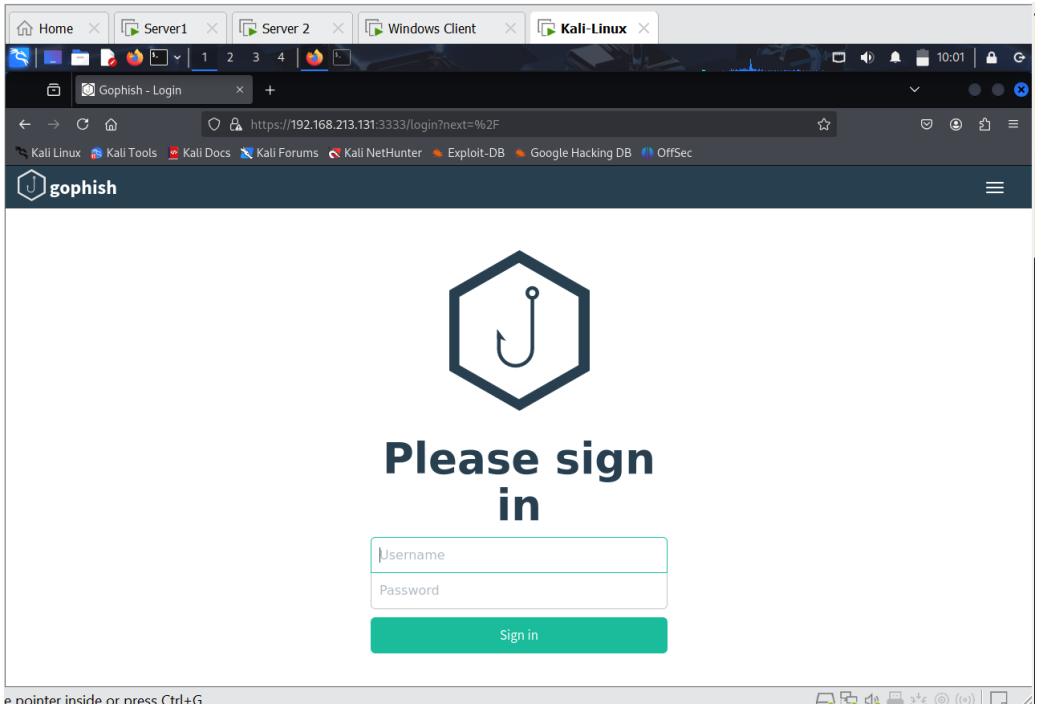

Figure 20: The Gophish sign-in page.

Once we signed in to **Gophish** we began our phishing campaign where the implementation steps included:

- Creating a phishing email template *(as shown below in figure 21)*
- Creating a landing page *(as shown below in figure 22)*

- Creating user group for our medical staff and adding staff members *(as shown below in figure 23).*
- Creating a sending profile *(as shown below in figure 24)*
- Launching our phishing campaign *(as shown below in figure 25)*

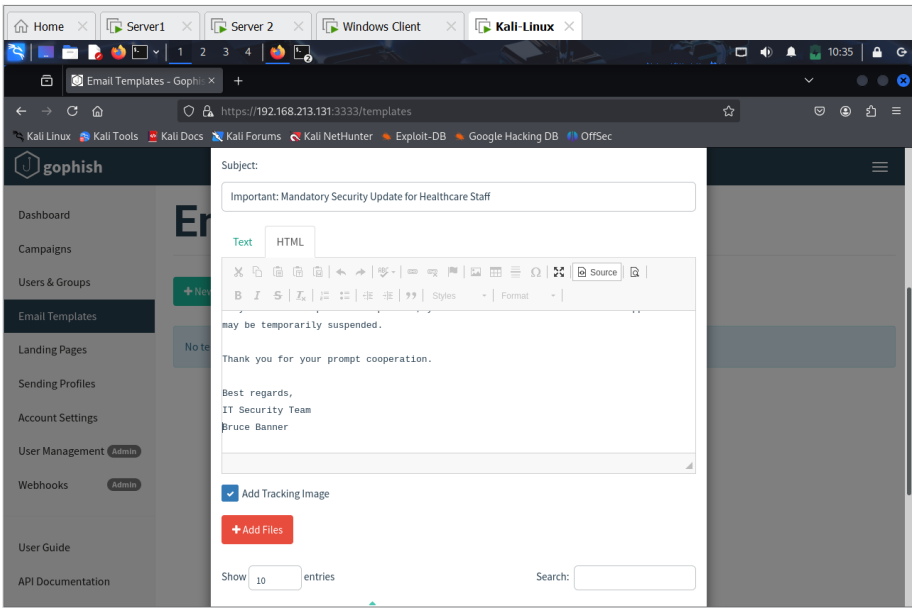

Figure 21: Phishing email template implementation (Gophish).

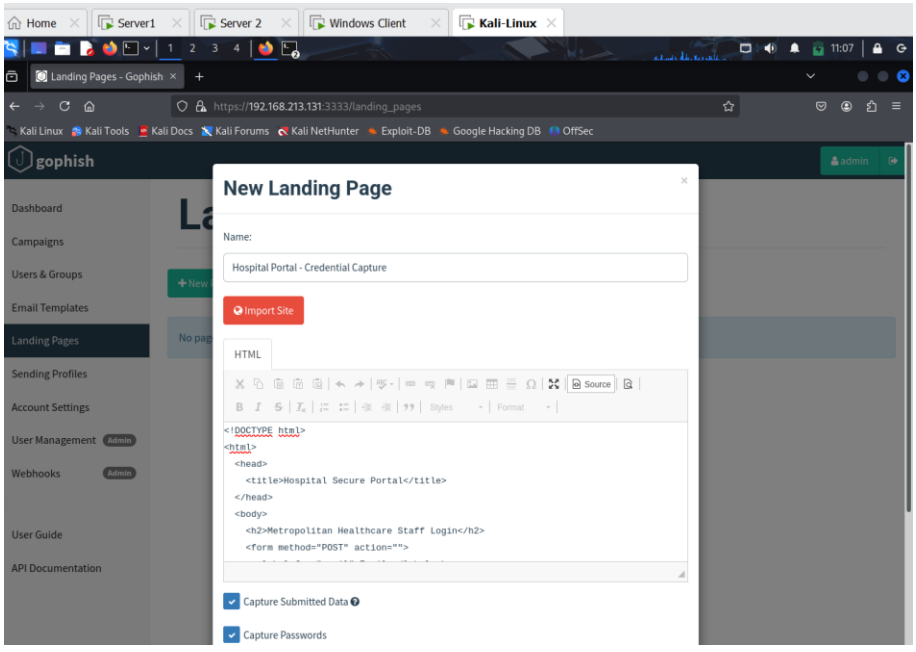

Figure 22: Landing page implementation (Gophish).

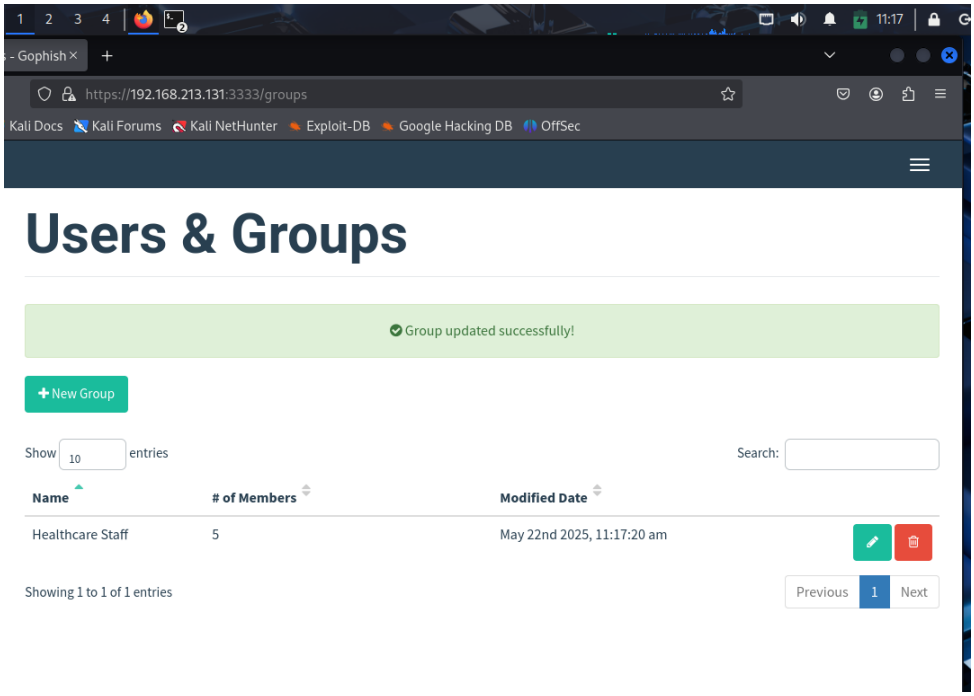

Figure 23: Healthcare staff group creation (Gophish).

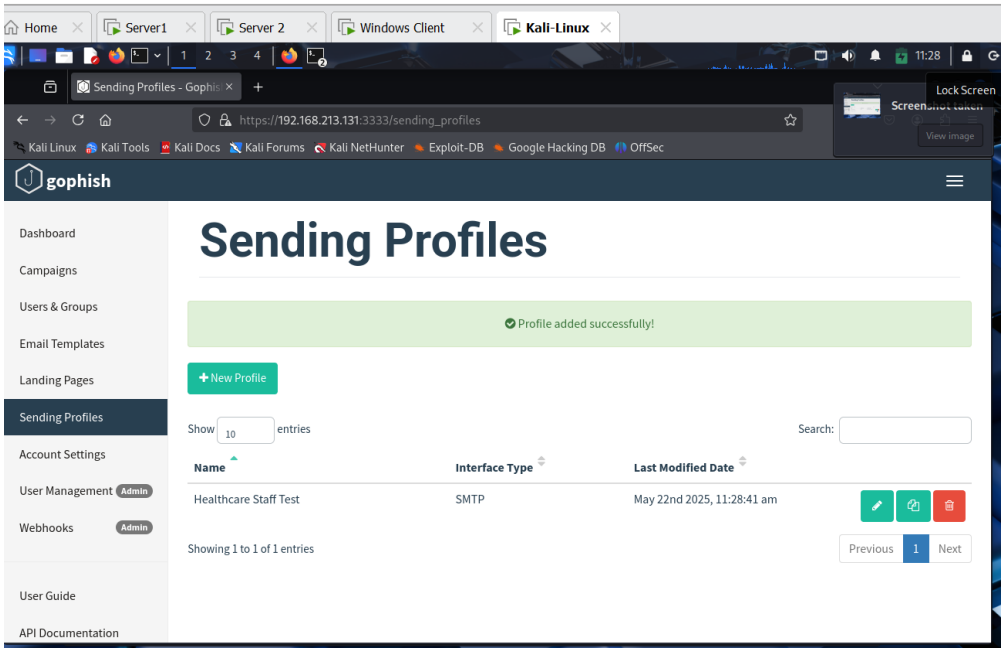

Figure 24: Sending profile implementation (Gophish).

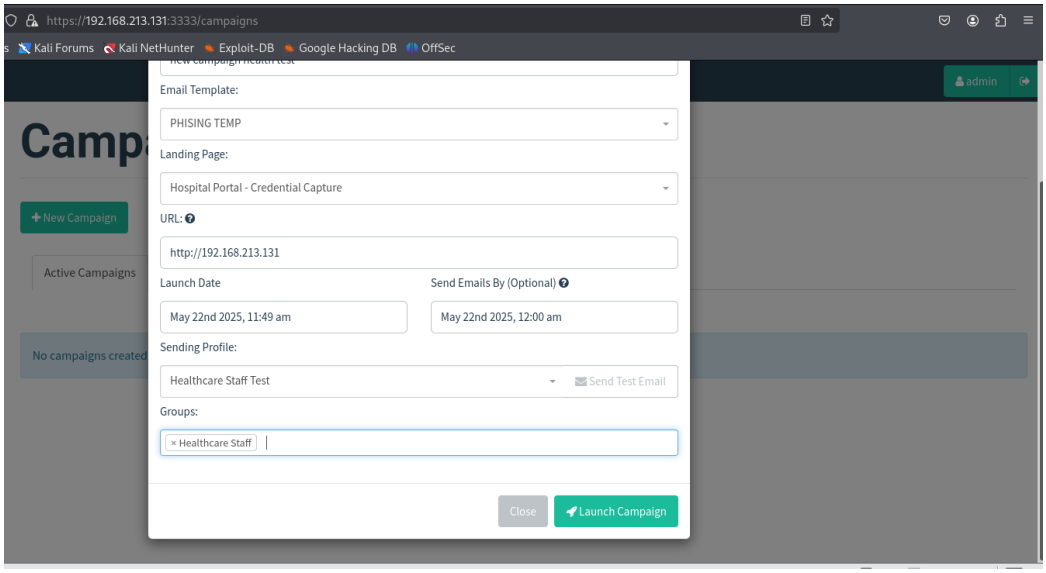

Figure 25: Phishing campaign overview before launch (Gophish)

After launching the campaign, we gave it some time to gather results. When the results were in, they showed that out of the five emails sent only one was reported, three staff members clicked on the link and one staff member submitted their credentials. This strengthens our claim as to why security training regularly must be implemented to healthcare staff to decrease the risk of cyber security breaches occurring via phishing.

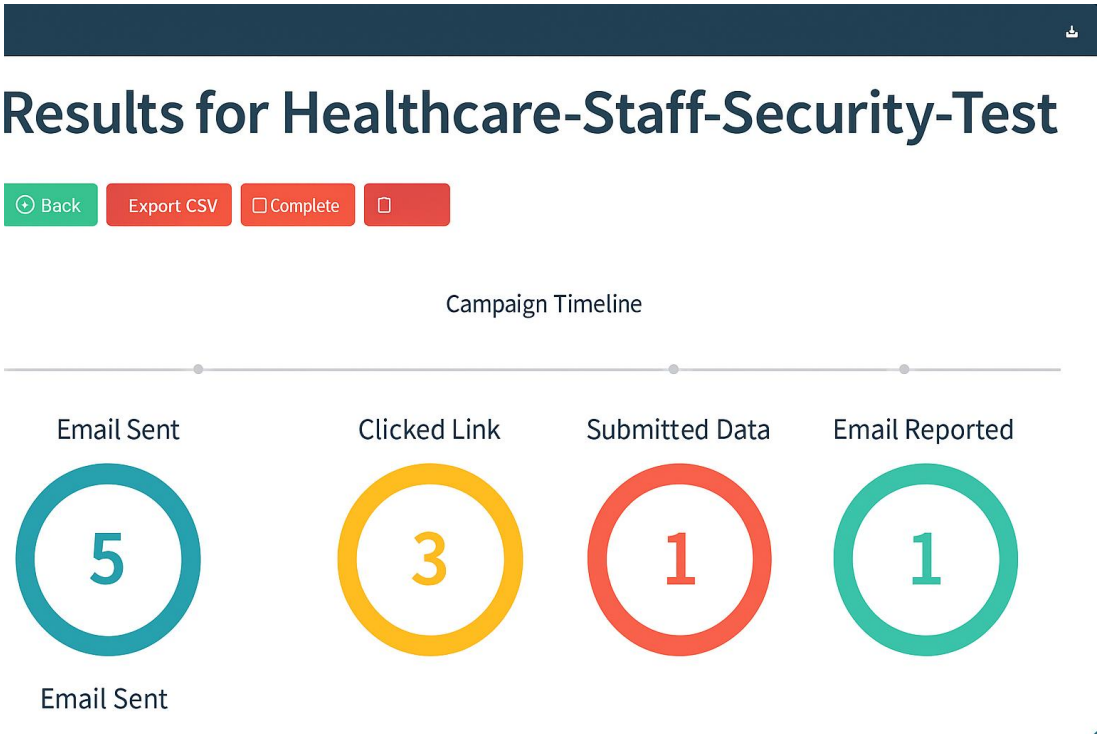

Figure 26: Phishing campaign test results (Gophish).

3.0.7 Intrusion detection and monitoring

Monitoring and detecting potential security threats is a crucial aspect of the cyber security infrastructure. However, incorporating third party SIEM (security management and event management) or IDS (intrusion detection system) platforms was deemed beyond the scope of this project although they can be very effective, there are other basic methods we have chosen for these tasks. In this case, we configured Windows event logs to display events triggering the firewall rules and with Kali-linux Nmap (a port-scanning tool) we simulated the threat of a potential attacker. Port scanning is a method used to discover open or weak ports on a system (Fortinet, 2024). In this case we used Kali-linux Nmap to scan Server 2 for potential vulnerabilities. It is also important to mention that we previously blocked Kali-Linux Ip-address through our windows firewall which means that we at the same time could test that the defences we previously set in place work the way we intended.

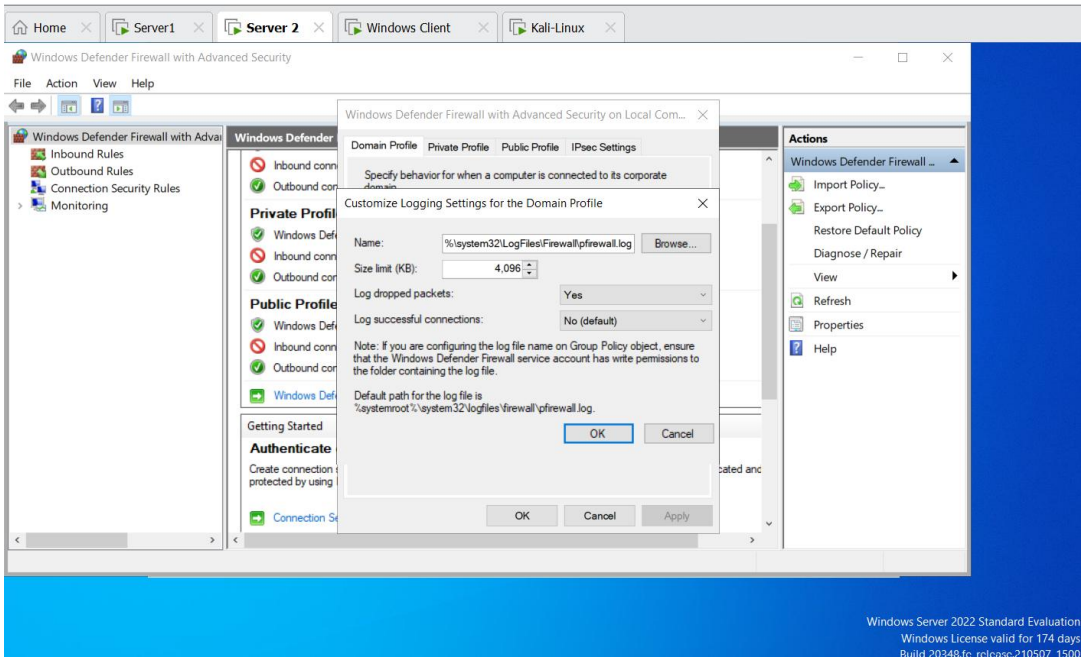

Figure 27: Windows event logs setting configurations.

In Kali-Linux Nmap we typed in the command nmap –p 3389 (port number) followed by the Ip address of server 2 (192.168.213.134) to scan it for potential vulnerabilities. In the mind of an attacker the result one would hope to look for would be that the port would be open.

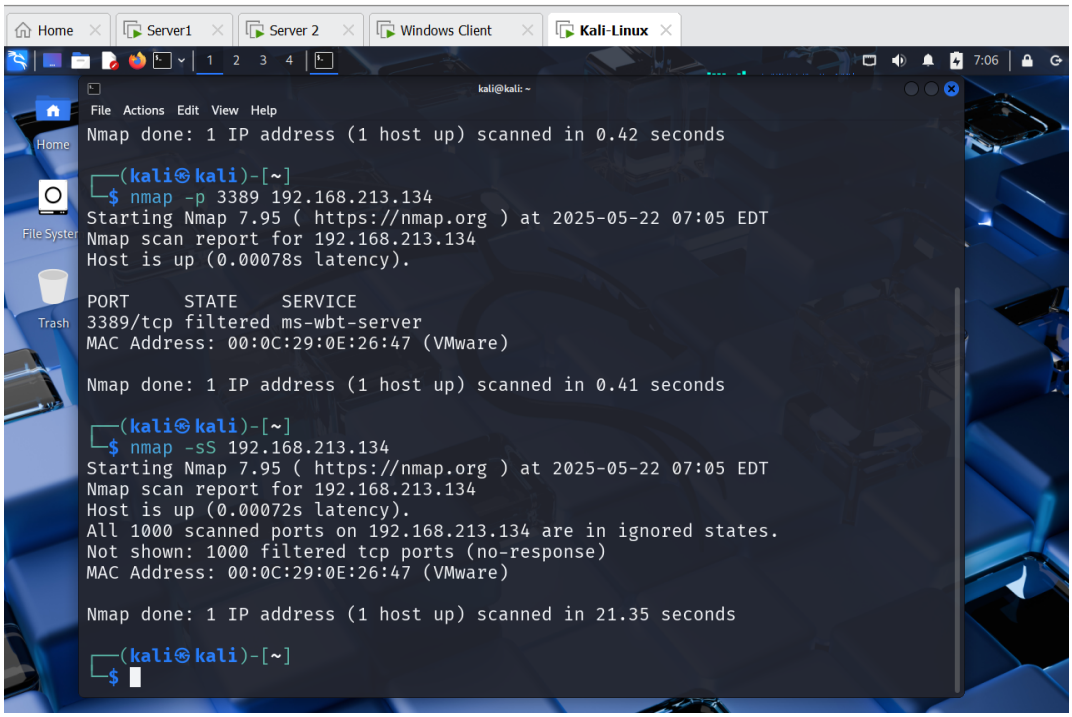

Figure 28: Nmap port scan of Server 2.

The results of the port scan *(as shown above in figure 28)* show that the port state is filtered, which means that the firewall rules we previously set in place to block Kali-Linux IP-address works in the way we intended it to.

Switching over to server 2 we then went to monitor the Windows firewall event logs to see if we discovered any anomalies in network activity.

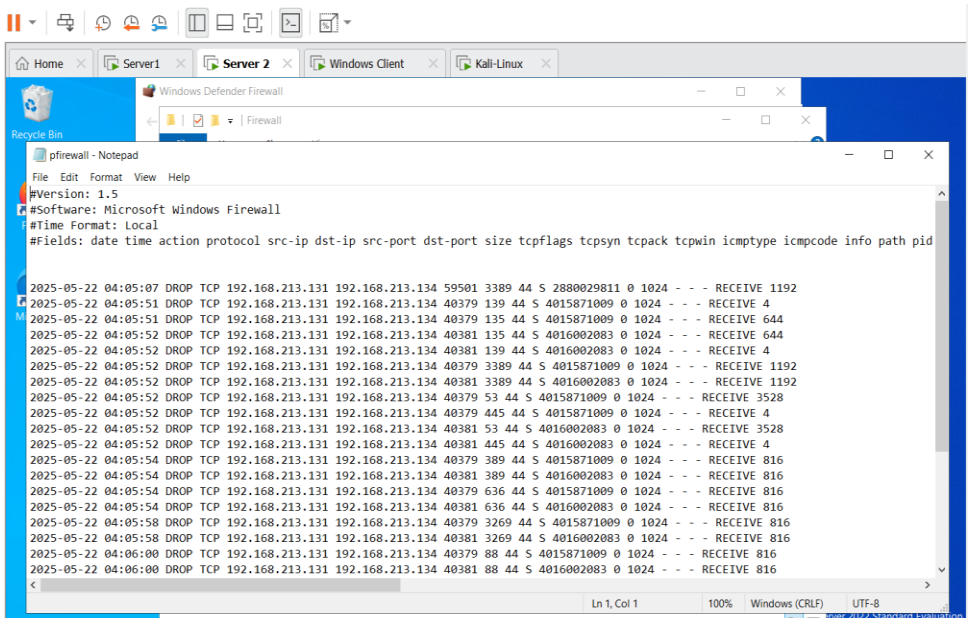

Figure 29: Windows firewall event logs.

Our results reveal dropped TCP (transmission control protocol) packets stemming from the IP address of our Kali-Linux VM. In simpler terms, what this tells us is that our Kali-Linux VM tried to connect to open ports (3389) on our server 2 which is used for remote access, but what was blocked by our firewall since we previously blocked or more specifically denied traffic stemming from our Kali-Linux VM. what this confirms is that our applied firewall rule is working as intended, also that our logs accurately show events that should be deemed suspicious.

3.0.8 Results & Observations

In this project, security measures have been put in place to counteract potential security threats, and tests have been conducted to see the effectiveness of these measures. Other tests like the phishing campaign also helped us get insight into the need for cyberthreat awareness amongst staff members. We will now take a moment to summarize and look at the security measures implemented and the vulnerabilities they cover to share an overview of the work that has been done up until this point to create clarity. It is also important to note that the measures based on research from sources such as NIST (2022), Fortinet (2024), and the U.S department of Health and Human Services (HHS, 2023) et cetera. Paying attention to trends within cyberthreats and best-practice recommendations.

Tailscale VPN

- Creates encrypted network tunnels preventing eavesdropping and data theft (HIPAA Journal, 2020).
- Prevents unauthorized remote connections and man-in-the-middle attacks.
- Protects data in-transit and helps companies follow compliance demands for secure remote access (GDPR Advisor, 2024).

Multifactor Authentication

- Adds an extra layer of verification, strengthening defences to unauthorized logins (Rublon 2021; NIST, 2024).
- Decreases the chances of brute force attacks and credential theft (Mahan, 2024; Al-Qarni, 2023).

Firewall rule for RDP (port 3389)

- Restricts remote access to internal (permitted) IP addresses, blocking out attackers (Fortinet, 2024).
- Protects unfiltered ports from remote exploitation, which is a common tool used for lateral movement (BD Emerson, 2025).

Group Policy Setting (GPOs)

- Strong password complexity enforcement, account lockout after inactivity and auto screen locks lower chances of unauthorized access and aligns with zero-trust (LaViola 2023; Hameed, 2024).
- Restricting system access based on job titles, aligning with principle of least privilege (Junior & Bandiera-Paiva, 2018).

Network Segmentation

- Compartmentalises internal systems into smaller segments preventing lateral movement from potential attackers or viruses (CyberArk, 2025).
- Prevents unauthorized end-devices access to more critical system infrastructure (Anderson, 2024).
- Enforces Zero trust architecture by denying access unknown actors by default (HHS, 2023; Kinderwag, 2010).

Phishing simulation with Gophish (Kali-Linux)

- Results showed that at least 60 percent of medical staff clicked on the landing page, whereas one user gave their credentials. This is consistent with real-world healthcare incidents (Avertium, 2024; HHS, 2022).
- Shows that Phishing and Social Engineering remain two of the biggest threat actors within the healthcare industry (Security Metrics, 2023).
- Proves the strong need for medical staff security training on a continuous basis (Lee, 2022).

Nmap Port Scanning and Windows Firewall log monitoring

- Simulated an outside attacker scanning for open (vulnerable) ports, which showed the port (3389) as being “filtered” revealing that the security firewall measures worked (Fortinet, 2024).

- Windows Firewall logs showed dropped TCP packets from the Kali-Linux (attacker) IP address also validating that the security measures worked as well as proved that logging and detection response was in place (Sharma & Mukherjee, 2023).
- Aligns with fundamental intrusion detection requirements within modern healthcare (Akram et al., 2021).

These security implementations, while significantly increasing the foundational security posture within the healthcare organization as we further evolve into a more digitalized world, also highlights one of our biggest weaknesses within cybersecurity, which is the human factor to consider. While the technical implementations now work effectively, it is time to look at how to implement a framework for how to educate staff on cyberthreats to lower the very alarming statistics shown from the “fake” phishing campaign that was conducted. What follows is a training manual tailored to healthcare professionals on how to better navigate amongst the landscape of cyberthreats.

3.0.9 Cyber Security Training Manual for Healthcare Professionals

The purpose of this manual is to aid healthcare staff in learning how to recognize common potential threats within the field of cybersecurity. The role you play in your organization is crucial protect system security, data security and most of all the confidentiality, integrity and health of your patient's safety. This means instilling a patient safety focused culture of cybersecurity all around (Riggi, 2025).

Recognizing Phishing and Social Engineering

Phishing and Social Engineering are some of the most common threats facing healthcare today. Cyber criminals will use different tactics to fool healthcare staff be it by sending emails with fake links containing malicious software or impersonate someone of authority within the organization, either in person or via phone calls which is a form of phishing known as vishing (HHS, 2022).

Some common warning signals to look for as it pertains to phishing emails are:

- Urgent messages such as: EMERGENCY HEALTHCARE BRIEFING!

- Unknown senders or irregular email addresses
- Emails that impersonate trusted actors (Avertium, 2024)
- File attachments within these emails

Healthcare is a heavily targeted sector because of what cyber criminals stand to gain from breaching the system, the value of patient data such as electronic healthcare records is very high on the dark web (SecurityMetrics, n.d.). While conducting a simulated phishing email campaign on healthcare staff the results showed that 3 out of 5 medical workers clicked on a fake link within the fake emails and one staff member even gave their password. This suggests that the need for staff training is of highest priority moving forward.

Password and Login

Weak passwords and authentication remain one of the leading causes for cyberbreaches (Al-Qarni, 2023). Attackers use software to conduct brute-force attacks cracking their way into the system. A password like “password123” is making the job very easy for cybercriminals which is the opposite of what we aim to achieve.

This is some ways in how we minimize such breaches from occurring:

- Use strong passwords containing letters, numbers and symbols. Stear clear of phrases that are common or dates such as your daughter's birthday perhaps (Mahan, 2024).
- Implement Multi-Factor Authentication such as a password in combination with a digital id card or mobile phone confirmation (NIST, 2024; Rublon, 2021).
- Never share a password
- Change your password and logout if you notice something suspicious

Safe data handling and storage

Healthcare organizations are under legal obligation to comply with GDPR and HIPAA laws referring to patient data and privacy etc. Failing to comply with this can lead to serious consequences legally and financially, not to mention harm your patient safety (GDPR Advisor, 2024; Datacenter Info, 2024). Follow these guidelines:

- Only access the files and data essential to do your job
- Log out before leaving your computer
- Never send personal health records or such over emails or messaging applications
- Never store data on USB drives unless they are approved and encrypted

Report suspicious activity

Among the top risks within healthcare are insider threats, either intentional or accidental (Lee, 2022). If you should notice anything that could be deemed suspicious you are to report it as fast as possible your higher ups or IT-Security team.

Things to report:

- Suspicious emails, phone calls or text messages
- If one of your devices is missing or stolen
- You should notice unauthorized access or system irregularities.
- you click on a suspicious link by mistake
- you notice unauthorized people or staff members acting suspiciously (by your computer etc.)

Acting fast in cases like this can substantially lessen the damage and help the IT personnel to respond quickly (Vibert, 2024).

Foundational Rules for Healthcare Security

Healthcare providers of today make use of principles and architectures known as Zero-trust and least privilege for system protection (HHS, 2022; Kinderwag, 2010). How you conduct yourself should be in alignment with these principles which means to:

- Lock your screen before leaving your system unsupervised (LaViola, 2023).
- Never install unauthorized applications or plug in unknown USB drives.
- Only ever use healthcare approved tools and devices
- Always follow policies for device use and data access

Implementation and maintenance

For this to be as effective as possible, the suggestion is for this security manual to be briefed to every new staff member as a part of their introduction training. Additionally, the manual

should be reviewed quarterly and updated to reflect the current state of cyberthreats and needs within healthcare. The staff members should also be made aware of these new changes when they occur, and refreshment training should take place every season as well.

Final Note

Cyber security is a part of your responsibility as a healthcare provider. A simple mistake like pressing the wrong link or leaving your computer unsupervised can be of great consequence to your patients as well as your organization. By staying aware of these potential threats and following safety guidelines you are doing everybody a great service and saving lives. Your work is valuable and appreciated.

4. Conclusion

In this project the purpose was to assess critical vulnerabilities within the healthcare infrastructure, implement and test security measures that protect patient-doctor interactions and develop a cybersecurity training program for staff members to recognize and mitigate potential threats. Through thorough research on what threats are most ailing to the healthcare industry today and creating a simulated healthcare infrastructure using virtual machines, we were able to implement and test security measures to counter these threats in a safe, test environment. These measures and tests included countermeasures to external attacks like port-scanning and phishing as well as internal threats like lateral movement and privilege misuse, which we addressed by implementing access restrictions and network segmentation. We faced some challenges in this project, especially in the practical phase. When implementing Gophish, for example, the web browser would think our phishing pages were real threats and block them automatically. Our fake emails would also not be delivered because of built-in spam filters. Since we also conducted it using fake email addresses since our clients were not real people, we would face errors, making it challenging to create meaningful metrics on our own. We therefore generated a visual representation based on real statistics. Gophish was useful in showing how easy it is to trick end users with well-crafted phishing emails. To go along with the technical implementations, we created a cyber security manual for training healthcare staff. The manual was written to highlight the security threats

facing healthcare today and how to counter them using our given guidelines following subjects such as safe data handling and recognizing phishing.

Through the writing and researching of this project, AI tools were used as study companions. These tools sometimes helped find appropriate synonyms and simplify complex grammar used by authors. AI was not used to directly write this report, but to support it as a learning tool and improve clarity.

In summary, this project shows us that it is possible to create a simulated setup of a healthcare organization, conduct tests, and implement security measures applicable to real-world scenarios which will reduce the risk of cyber breaches. It also further demonstrates that technology without human knowledge is not enough to create a safe healthcare environment. Education and awareness of these risks are equally important as we move forward within digital healthcare.

5. References

Adler, S., 2024. Risk Management in Healthcare. HIPAA Journal. Available at: https://www.hipaajournal.com/risk-management-in-healthcare/ [Accessed 8 June 2025].

Akram, R., Liu, L., Zhao, Y., Kryvinska, N., Abbas, H., & Rizwan, M. (2021). Trustworthy Intrusion Detection in E-Healthcare Systems. Sensors, 21(24), 8446. https://doi.org/10.3390/s21248446

Anderson, E. (2023) *Top 6 hackable medical IoT devices – and how to safeguard them*. Lumifi Cyber. Available at: https://www.lumificyber.com/blog/top-6-hackable-medical-iot-devices/ (Accessed: 7 June 2025)

Ann N., 2023. *Top 9 Healthcare Cybersecurity Compliance Standards*. Ominext. Published 26 December 2023. Available at: Ominext [Accessed 8 June 2025].

Al-Qarni, E.A. (2023) Cybersecurity in Healthcare: A Review of Recent Attacks and Mitigation Strategies. International Journal of Advanced Computer Science and Applications, 14(5). Available at: https://doi.org/10.14569/IJACSA.2023.0140513

Avertium (2024) Social engineering threats in healthcare. Available at: https://www.avertium.com/resources/threat-reports/social-engineering-threats-in-healthcare (Accessed: 7 June 2025).

BD Emerson (2025) Healthcare Cybersecurity: Regulations & Best Practices. Available at: https://www.bdemerson.com/article/healthcare-cybersecurity-guide (Accessed: 7 June 2025).

Bishop, J. (2025) Cybersecurity experts from University of Cincinnati warn of rising ransomware attacks on healthcare institutions. *Hoodline*, 24 May. Available at: https://hoodline.com/2025/05/cybersecurity-experts-from-university-of-cincinnati-warn-of-rising-ransomware-attacks-on-healthcare-institutions/ (Accessed: 7 June 2025)

Business Wire (2022) Healthcare Under Cyberattack: Unprotected Medical IoT Devices Threaten Patient Care. Available at: https://www.businesswire.com/news/home/20221129005177/en/Healthcare-Under-Cyberattack-Unprotected-Medical-IoT-Devices-Threaten-Patient-Care (Accessed: 7 June 2025)

Cedar Rose (2025) Managing Third-Party Risks in Healthcare: 3 Key Risks & Strategies. Available at: https://www.cedar-rose.com/blog/managing-third-party-risks-in-healthcare-3-key-risks-strategies (Accessed: 7 June 2025).

Censinet (2024) *Pharmaceutical supply chain vulnerabilities & third-party risk: Lessons applicable across industries*. Available at: https://www.censinet.com/perspectives/pharmaceutical-supply-chain-vulnerabilities-third-party-risk-lessons-applicable-across-industries (Accessed: 7 June 2025)

Center for Internet Security (2016) *Ransomware: In the Healthcare Sector*. Available at: https://www.cisecurity.org/insights/blog/ransomware-in-the-healthcare-sector (Accessed: 7 June 2025).

CyberArk (2025) What is Healthcare Cybersecurity? Available at: https://www.cyberark.com/what-is/healthcare-cybersecurity/ (Accessed: 7 June 2025).

DataBrackets, 2022. Comparing Top 5 Security Regulations for Healthcare. Posted 31 October 2022. Available at: DataBrackets [Accessed 8 June 2025]

Data Center Info, 2025. *Healthcare Data Privacy Requirements*. Available at: Data Center Info [Accessed 8 June 2025].

Dhinakaran, B., Abbas, M., Srinivasan, K., & Sundararajan, V., 2025. *Safeguarding confidentiality and privacy in cloud-enabled healthcare systems*. *Expert Systems with Applications*. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0957417425012060 [Accessed 8 June 2025].

ElSayed, Z., Abdelgawad, A. & Elsayed, N. (2025) Cybersecurity and frequent cyber attacks on IoT devices in healthcare: Issues and solutions. arXiv [Preprint]. Available at: https://arxiv.org/abs/2501.11250 (Accessed: 7 June 2025)

European Commission – Directorate-General for Communication (2025) Bolstering the cybersecurity of the healthcare sector. European Commission. Available at:

https://commission.europa.eu/news-and-media/news/bolstering-cybersecurity-healthcare-sector-2025-01-15_en (Accessed: 7 June 2025)

Golani, G., 2024. *New Healthcare Cyber Regulations: What Security Teams Need to Know*. Sentra. Published 28 November 2024. Available at: Sentra blog [Accessed 8 June 2025].

Hunter, M. (2024) IoT Cybersecurity in Healthcare – Mitigating the Risk. CompliancePoint. Available at: https://www.compliancepoint.com/healthcare/iot-cybersecurity-in-healthcare-mitigating-the-risk/ (Accessed: 7 June 2025).

Junior, C., & Bandiera-Paiva, P. (2018). Health Information System Role-Based Access Control Current Security Trends and Challenges. *Journal of Healthcare Engineering*, *2018*, 6510249. https://doi.org/10.1155/2018/6510249

Kolbasuk McGee, M. (2024) *Identity and access management weak in healthcare*. *GovInfoSecurity*, 12 February. Available at: https://www.govinfosecurity.com/identity-access-management-weak-in-healthcare-a-18703 (Accessed: 7 June 2025).

Lee, I. (2022) *Digital Transformation and Cybersecurity in Healthcare*. *Information*, 13(9), p.404. Available at: https://www.mdpi.com/2078-2489/13/9/404 (Accessed: 7 June 2025)

National Institute of Standards and Technology (NIST), 2022. *NIST Updates Guidance for Health Care Cybersecurity*. Published 21 July 2022. Available at: NIST [Accessed 8 June 2025].

NEJM Catalyst, 2018. *What Is Risk Management in Healthcare?* NEJM Catalyst. Published 25 April 2018. Available at: https://catalyst.nejm.org/doi/full/10.1056/CAT.18.0197 [Accessed 8 June 2025].

Mahan, J. (2024) *Why it's crucial to have access control systems in healthcare*. CC Tech Group. Available at: https://cc-techgroup.com/healthcare-access-control/ (Accessed: 7 June 2025).

MetricStream, 2024. *The Risk Management Process Explained: Step-By-Step*. Available at: https://www.metricstream.com/learn/risk-management-process.html [Accessed 8 June 2025].

Muoio, D. (2025) 3rd-party risk and asset management continue to be cybersecurity weak points for healthcare, study finds. *FierceHealthcare*, 15 April. Available at: https://www.fiercehealthcare.com/health-tech/third-party-risk-asset-management-are-cybersecurity-weak-points-healthcare-study-finds (Accessed: 7 June 2025)

Riggi, J**.** (2025) *The importance of cybersecurity in protecting patient safety*. American Hospital Association. Available at: https://www.aha.org/center/cybersecurity-and-risk-advisory-services/importance-cybersecurity-protecting-patient-safety (Accessed: 7 June 2025).

Rublon, 2021. *What Are the Three Authentication Factors?* Rublon Blog. Published approx. 3.5 years ago (cirka 2021). Available at: https://rublon.com/blog/what-are-the-three-authentication-factors/ [Accessed 8 June 2025].

SecurityMetrics (n.d.) 9 Ways to Social Engineer a Hospital. Available at: https://www.securitymetrics.com/blog/healthcare-recognize-social-engineering-techniques (Accessed: 7 June 2025).

Sharma, S., & Mukherjee, S. (2023). Explainable Intrusion Detection for Internet of Medical Things. *KMIS 2023 - 15th International Conference on Knowledge Management and Information Systems*. https://www.scitepress.org/Papers/2023/122103/122103.pdf

Sprinto, 2024. 13 Cybersecurity Standards You Must Know. Sprinto blog. Published ca. December 2024. Available at: Sprinto [Accessed 8 June 2025].

Vibert, R. (2024) Healthcare and Insider Threats: Securing Patient Data from Within. Metomic. *Available at:* https://www.metomic.io/resource-centre/healthcare-and-insider-threats (Accessed: 7 June 2025)