Security In The Healthcare Industry

Course: Exam Project 1

Project Number: 8

Student Name: Anastassiadis, Alexandros

Class: August-2024-FT-NSA

Startup Date: 12.05.2025

Table Of Contents

1. Introduction

The growth within the remote healthcare services has been a really big and fast-growing sector, especially after the COVID-19 pandemic and also as the technology in the world is expanding and evolves every day when it comes to digitizing everything and making things more comfortable and easier. But it comes with downsides also as people's personal information is transferred across networks e.g. when a doctor is talking to a patient on different locations on a service and sometimes maybe not on the most secure networks, which increases the target for cyberattacks and cybercriminals.

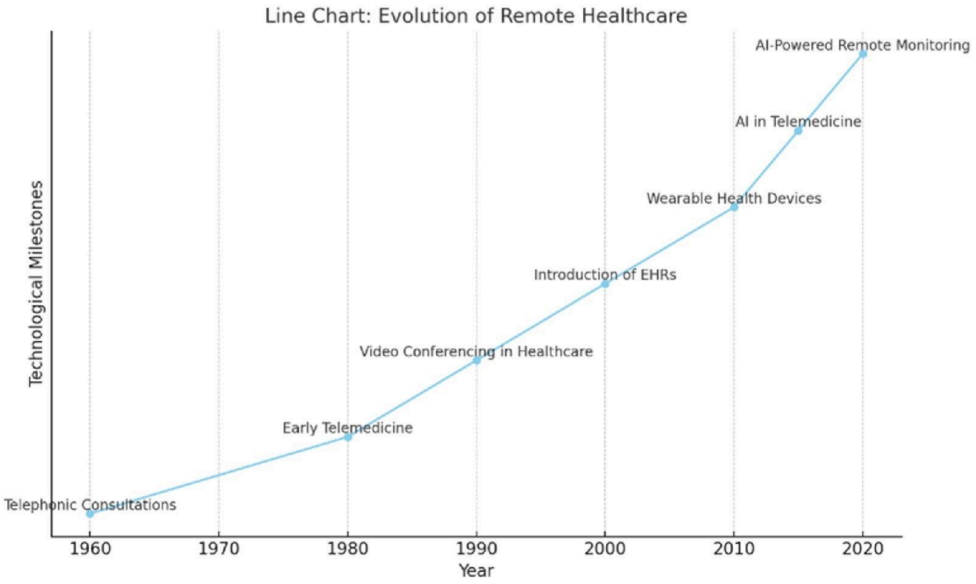


Figure 1.0.0 Displays the growth of remote healthcare (Chaturvedi, Chauhan & Singh, 2025)

This project overall is going to focus on how communication between these remote healthcare services can be more secure by using certain automation and strategies. So, the objective is to create a safe and secure environment that protects personal data and only allows the rightful people to access the content.

It’s going to contain both theoretical and practical parts of this project. It’s going to display the different technologies, tools and ways taken along the way like (MFA) Multi-Factor Authentication, (VPN) Virtual Private Network, Network segmentation, cyberattack simulations and monitoring tools and all of these are going to be runned and tested in a secure environment in VMware in different Virtual Machines. It’s going to simulate a real connection between different parts of these types of healthcare services.

Then there will be a cybersecurity report and tryouts which is going to display results in action, which is going to show that more secure environments are very helpful, important and almost a must these days to know that things are working safely and fine.

1.1 Assignment & Report Structure

This project will announce the most important approaches to keep these remote healthcare services safe and secure. These approaches consist of (MFA) Multi-Factor Authentication, VPNs, network segmentation and access control, and more. These approaches will be explained, how and why they are implemented in remote healthcare environments. Then it will be displayed in practice in virtual machines to show a simulated connection between doctor and patient like a real session between the two parts.

1.2 Subject Introduction

“The average cost for the single most expensive attack was 4.7 million dollars” (Eddy, 2025). As all the technology is getting better and evolving in the world, so are the bad things also and becoming more and more difficult to detect which should tell one how important the security is within IT infrastructures.

Why is healthcare such a big cybersecurity target? One of the bigger vulnerabilities is just that being in the healthcare industry as the data within that is really attractive for attackers such as all the patient records of a lot of things such as names, financial info and more. Very valuable data and also there is a big chance that the attackers are getting paid for letting information go as ransomware is usual towards bigger businesses. Easy things can also be problems that one maybe doesn’t think about such as outdated systems and maybe badly access control or just not enough people with experience within the security sector (Eddy, 2025).

One big issue also is that within the healthcare systems it can go from just an attacker wanting some money to life and death if some life critical equipment is offline. Poorly secured companies can cost them so much “unnecessary” money and time for the clean up after an attack or just rebuild everything sometimes instead of just hiring a security team that has control of everything (Eddy, 2025).

1.3 Measures to Complete Objectives

In order to accomplish the tasks in this project some steps need to be taken, such as:

- Find and establish the threats that remote healthcare systems contain.
- Create and configure a secure network environment with the use of Windows server 2022, along with VPN, (MFA) Multi-Factor Authentication, access control and more.
- The use of Virtual Machines to replicate communication between server and client.
- Creation of imitated cyberattacks, penetration tests and phishing tests to test systems.
- Create a plan for employees to participate in to get more familiar with cyberattacks and detect social engineering attacks.
- Keep records of steps which will evolve in a cybersecurity report followed by a proof-of-concept demo.

1.4 Expected Challenges & Assumptions

The setup within healthcare systems can be complicated and a lot of work. All the different techniques and configurations like the VPN, domain controller and the setups need to be configured rightly for everything to work as it should. So even small mistakes during the setup phase can cause problems and also settings that maybe need to be changed in order for some things to work. Simulating and creating attacks or penetration tests can cause damage, so snapshots are a must which helps to get back to before the problem was caused if it was, that is.

The assumption of this project is that the reader has:

- A stable network connection.
- An efficient and working computer for virtualization.
- Administrative privileges/rights in the test environment.
- A credible and working copy of Windows server 2022.
- A credible and working copy of Windows 10 client or similar operating system.
- Updated operating systems, working software, and tools.

2. Main

This part is going to describe a little bit of information about each topic and the steps taken to deploy a virtual environment to replicate a remote healthcare company. The subtopics will be explained to understand the importance of them and especially within the remote healthcare department and how they will work in a virtual environment. The main goal is to imitate the main field of problems, solutions and configurations as out in the real world.

2.1 Network Setup and Lab Environment

This is an isolated setup which is important for testing practical parts securely.

- Server1 = Windows Server 2022 which is the Domain Controller and a DNS server
- Server2 = Windows Server 2022 used for monitoring, firewall rules and VPN
- Client = Windows 10 workstation which is representing as a doctor's computer
- Kali Linux = Used for phishing simulations as an attacker and for vulnerability scanning

2.2 Identity and Access Management

Identity and access management (IAM) is a structure of different types of technologies and ways for companies to keep control of users/identities within an IT-infrastructure. It contains different things such as username and passwords, and also policies which decide who has access to what data. So, within the healthcare industry that compiles all the people trying to access patient information which includes employees, patients themselves, business partners etc.

Of course, this is not going to stop all the cyberthreats but is a strong start and ground to stand on and begin with before every other risk comes into play.

Within this project, an active directory was set up on server1 which is used for group policies, users, and role-based access. Server1 was then promoted to a domain controller within a domain created and called healthcare.local, then users were implemented to replicate different roles as it would be within a company. So, two users were created, one called dr.alex which was then put into an organizational unit (OU) called Doctors, then itadmin into an OU called IT-Team. These users can be assigned different policies and roles which is like the practice which is used in businesses out in the real world that is called principle of least privilege.

As one client which is going to display as a doctor's computer at work is joined to the domain it displays that the policies etc. can be set up by the IT department.

2.3 Secure Remote Access and VPN Integration

Nowadays, as working remotely is a typical thing, the security of access to the network you're on is a really important thing to keep in mind. So, a remote access VPN lets remote users connect safely to networks via a protected tunnel made through VPN which is the protocol for it and stands for Virtual Private Network. As mentioned earlier, working remotely is a lot more common nowadays, so the companies need to make secure access available and out to the ones working remotely, which remote access VPN does. It makes the internet reachable through a specific dedicated server then the company in this case gives out a VPN client software which is installed on the employee's devices and that client software is connecting to that specific company server (Higgins, 2022). To make sure that everything has not been infected or tampered with the VPN client sets up an encrypted tunnel to the server and all the data which is traveling through the computer and the server is going through the tunnel which makes it unreadable for an attacker which is a key thing in remote work (Higgins, 2022).

And, in this project Tailscale was used as VPN software to simulate the encrypted connection from a doctor's computer to the internal infrastructure. Why Tailscale was used is because it is simple to set up, to use it, and also has strong and stable encryption. So, the risk of Remote Desktop (RDP) is minimized on the public internet. It was installed on both a second windows server (server2) and the client mentioned before, and a VPN connection between both parts was successful. Then RDP connection to server2 from the client was going with the newly assigned Tailscale Ip addresses.

2.4 Multi-Factor Authentication

Multi Factor authentication (MFA) is a security method that wants a user to prove in more than one way who they are and not just one to get access to something like a single password only. So, if an attacker may get their hands on your credentials, they will still have another obstacle they need to overcome. Two-factor authentication (2FA) was more common before and uses two methods but as the technology evolves every single day it was obvious that something stronger and more secure was needed so two-factor authentication is using two factors and MFA is using two or more factors (Bigelow, Yasar & Shacklett, 2025). MFA is a multilayered security measure that helps securing peoples credentials because one single

password isn’t safe anymore as people may trick a person to giving up their passwords such as phishing or even brute force which is a software that tries millions of passwords to get the right one in the end and also stealing peoples credentials is a really big and serious threat and is really important to take serious (Bigelow, Yasar & Shacklett, 2025).

So, to reduce the risk of this happening a software called Duo MFA was installed and configured on server2’s system and login. Then trying to connect via RDP into the server2 from another device shows it has to have another authentication which shows that unauthorized users cannot access as they wish without the right credentials including extra layers of security. This should be a standard procedure for all devices which are going to be used as a remote system.

2.5 Phishing Awareness

The weakest link within cybersecurity is humans and from earlier studies in 2024 it says that 90% of cyberattacks start from a phishing email which should tell you that it is important to be trained and well aware of detecting phishing attacks (Srėbaliūtė, 2024). Phishing is an illegal act as it uses fraud and identity theft. The thing that makes it illegal is that the one sending a phishing email is using techniques/language to trick you into giving out important information as card number information or personal information for the attackers gain which is making it cross the line to illegal (Srėbaliūtė, 2024). So, if you receive an email from maybe “google it-team" you need to double check the sender's information, so the address isn’t a fake one because what seems to be a legit email can be a phishing attempt to harm your personal information.

A phishing attempt was simulated using Gophish from Kali which is acting as the attacker. So, a phishing email was sent to dr.alex as it displays a real attempt to attack the medical staff. Then when dr.alex is following the instructions in the email Gophish logs everything and displays important info like credentials typed in. This shows how important it is for employees to be well trained and aware of phishing attempts especially in a sector as important as healthcare, also that Gophish can be used within companies as a simulator for employees to be more aware of similar attacks.

2.6 Network Segmentation

Network segmentation is like setting up different areas inside your computer network using things like switches, firewalls, routers, which is an important thing to do if you want to keep things more secure. It's like building walls inside your building to keep your data more secure and harder to interrupt. As threats are becoming more and more difficult and sophisticated it's almost essential to have more than one security measure, it's basically extra security measures within your network to help you decide what type of traffic that can pass and who between important zones (Landsberger, 2023). For example, if an employee is hit by a phishing email and clicks a link that is malicious, that attacker has bypassed the main firewall and without segmentation that attacker could move from that first computer to other devices within that same network such as security cameras or even databases with personal information from patients (Landsberger, 2023). It is all made to make it tougher for the attacker to get to its goal with ease. As one can understand, this is really important to set up within a company to not put your data in a vulnerable position.

To demonstrate this within this project, a windows firewall was configured on server2 to block all traffic that comes from the client. This was accomplished by setting up a rule that blocks traffic from the clients IP address. This is mirroring the same type of segmentation as in a company, for example if the client in this case as the doctor shouldn't have access to server2 which can play as IT department where the client should not be, it's helping to separate different areas and positions within a company.

Segmentation is supported by the zero-trust model as it assures even known devices are not able to connect to things that they don't have authorized access to.

2.7 Threat Detection and Monitoring

This is a really important part of security as it helps companies to spot threats before they can expand or take action. In companies threat detection works as security guards constantly look for actions that take place out of the ordinary like weird activities. Keeping an eye on and analyzing the network and all the traffic if something is abnormal it tells you about it before it becomes a serious problem.

There are different types of threat detection tools and software as it may differ from company to company, it can be because of the scale of the company as much as the budget.

To make it easier to understand how it works in this project, the standard built-in monitoring tools in windows are used. Such as Event Viewer which is for keeping track of security happenings. Windows Firewall logs were enabled to keep track of traffic that is blocked or allowed. Then also Resource Monitor to keep track of real-time attempts to connect to the device.

All of the tools mentioned above were used to spot Nmap scans from the Kali attacker machine and detect attempts to connect or access the device. Just to clarify what Nmap is, it stands for network mapper and is a tool that scans networks and tells what ports and services may be open which is a helpful tool for knowing about the vulnerabilities but is also used by people that may want to cause harm with it (Shivanandan, 2020).

2.8 Vulnerability Scanning

Cyberattacks are usually successful because they take advantage of well-known weaknesses and vulnerability scanning is the process to scan for those weaknesses before someone like an attacker can come into play and take advantage of them (Kosinski & Forrest, 2023). It is a way to identify weaknesses in the security matter and actively looking and not only checking around, but today almost everywhere it is tools that check for you and not a person that sits and looks for things so it's automated software. It checks and flags weaknesses, then the IT team can take action thereafter.

So, in this project to simulate the attacker which is the Kali machine Nmap was run from it. Which showed what ports were open etc. like RDP (3389) that is a well-known port in a real-world example. This task showed that applying firewall rules and strictly minimizing the exposure of certain services and ports is important and crucial. The scan was also used as a trigger test as mentioned in the above topic to run monitoring and detection tools.

3. Security Awareness Plan

As one can tell, a cybersecurity awareness plan implemented into a business and a company is almost a must, especially nowadays as the risks are getting more dangerous and harder to detect. The safety of a company is not only about the technical parts and measures but also to

educate users more and to get comfortable spotting a risk before it gets to a serious level of danger. Particularly in healthcare as human errors take the first spot to where the breach is caused. The awareness plan that will be provided below is going to focus on how employees in a telemedicine company can learn to spot and detect risks before they take place.

3.1 Goals

The main goals are to lessen the possibility of phishing and social engineering attacks to complete. Make sure that the employees follow the rules regarding the policies for passwords. Make sure that employees are reporting suspicious activity to the IT department.

3.2 Training Examples

Keep employees updated on new attacks and phishing attempts made by software for testing and sending out fake phishing attempts with Gophish for example, like in this project.

MFA is also important to print into employees heads to always use strong passwords and even real-time MFA applications for enrollments on maybe their phone to keep an extra element to login like Duo Mobile that is going to show later in the practical part.

To remember them to not be on public Wi-Fi without VPN if remote work is the case and, in this project, Tailscale VPN is used to display that. Also, simple things like locking the computer and keeping an extra eye on it if remotely work is in a public space and be careful what to put into the computer such as USB usage like flash drives or file transfers and even sync the cloud so everything is saved regularly (Verizon, 2024).

3.3 Permanent Actions

- Sending out emails about information and reminders to keep things up to date.
- A review of the plan once a while to keep things fresh.
- To get newly hired employees into the cybersecurity plan.

4. Solution / Technical

This part of the report is going to show the construction and technical performance of practical tasks in the project. It’s going to get into the nitty-gritty about all the technical parts

in all of the practical things such as configurations etc. Also, the scope of all the things within the project is going to be covered and how to secure the remote healthcare systems into being less able to get attacked.

Some of the implementation and configurations can be questioned as it may not be the most secure or suitable option for the topic if it was out in the real world, but as it is in a closed secure virtual environment some things may be chosen just because of its ease to use and to get the point out there. It's going to describe how things were made and what to think about when taking the steps. Also, if it is configured in some special way and why.

4.1 Environment Setup

In this project the software VMware was used to set up the isolated environment. All the iso files to put into VMware were downloaded from legit sites straight from the original source. Four machines were created as mentioned before (two windows server 2022, one client windows 10 and one Kali Linux).

After installing go into the machines and update all of them then rename them so it's easier to work with then a good thing to do is to take snapshots if one is working in virtual machines so one can always go back if something unplanned is happening as technology can mess with you sometimes.

4.2 Network Configuration

Before anything we need to make sure that the machines share and are on the same network so firstly turn off the machines and right click on the machines name then press settings → Network Adapter → Choose custom then take VMnet2. Then check if they share the same subnet as each other so on the windows machines go to the command prompt and type ipconfig to see the IP addresses. On the Kali Linux machine go to the terminal and type ip a to display the IP address.
In this project it might be set to NAT to get an internet connection when it's needed as it can be used when downloading certain things online.

4.3 Install Active Directory

Log into server1 as that is going to be the Active Directory. Then open server manager if it doesn't open by itself as it is a standard setting if not changed. After that click add roles and

features then just click next until you arrive at the “server roles”. Then you will see a list of things where DNS Server and Active Directory Domain Services should be selected and marked.

Then go to Next and press Install to finish it. After the installation it will come a warning message that is found after pressing the flag as displayed in the picture below.

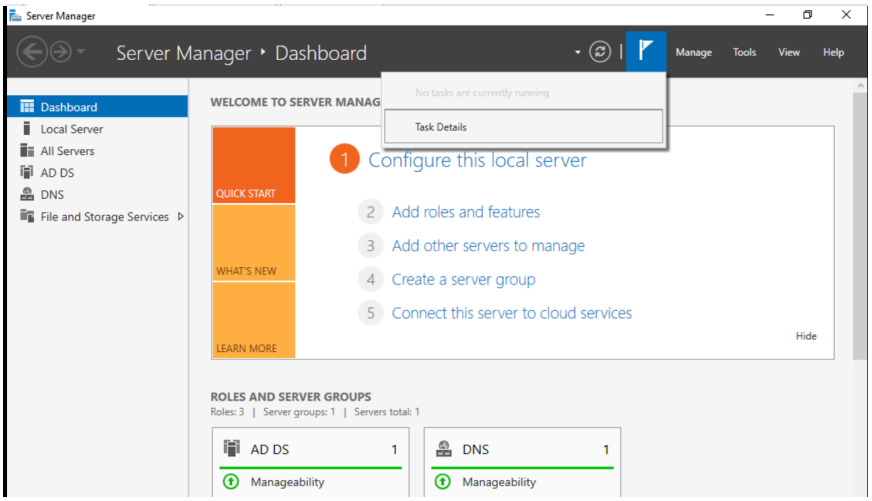


Figure 4.3.0 Showing the button to click for promoting to domain controller (Anastassiadis, 2025)

It will say “Promote this server to a domain controller” where another wizard will start and you should select “Add a new forest” and then choose the domain name which was put as healthcare.local in this project. Put a DSRM password and remember it for extra safety then click next and install. The server will now restart by itself and then you can login as administrator into the newly created domain as shown below.

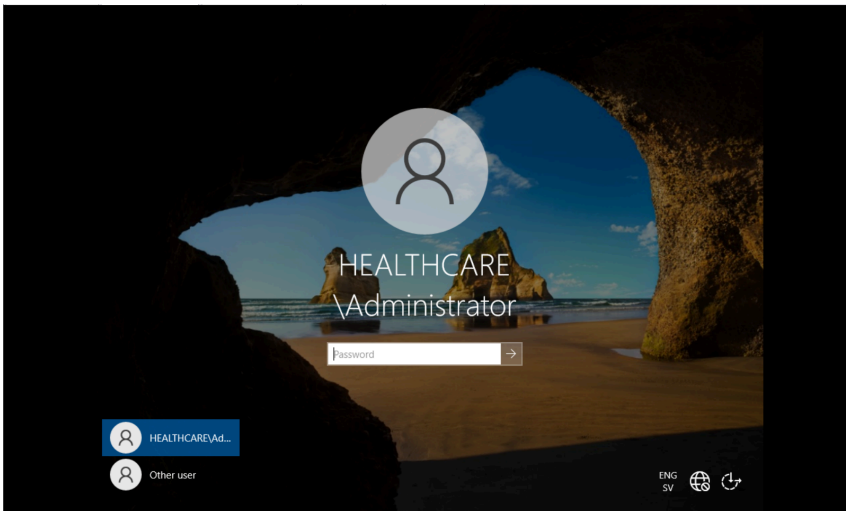


Figure 4.3.1 Displays the domain (Anastassiadis, 2025)

4.4 Creation of Users & Groups

Now after the creation of the domain it's time to log in as the administrator as shown in (*Figure 4.3.1*). Then search in the windows bar for "Active Directory Users and Computer" and go into the settings then right click on the domain name in the left side as shown in the figure below:

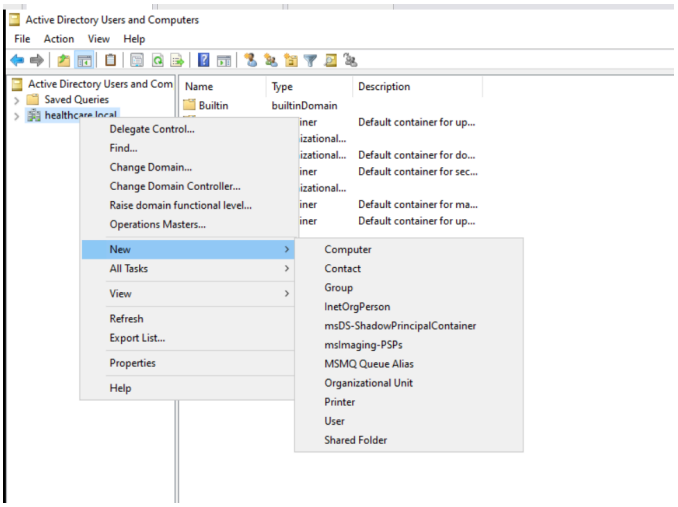


Figure 4.4.0 Shows how to click for making OU (Anastassiadis, 2025)

It will appear a small list of things one can choose from so from there click New → Organizational Unit and choose a name as in this project it was named Doctors and another one called IT-Team. After that users were made called Dr. Alex and itadmin in respective groups and to accomplish that it's needed to right click the newly created OUs → New → User and then fill in the credentials, and also as the password is set make sure to

check the “Password never expires” box as it helps in the environment setup for the simplicity to not have to change at the first login. It will appear as a warning message when doing so but it’s not a problem for the project.

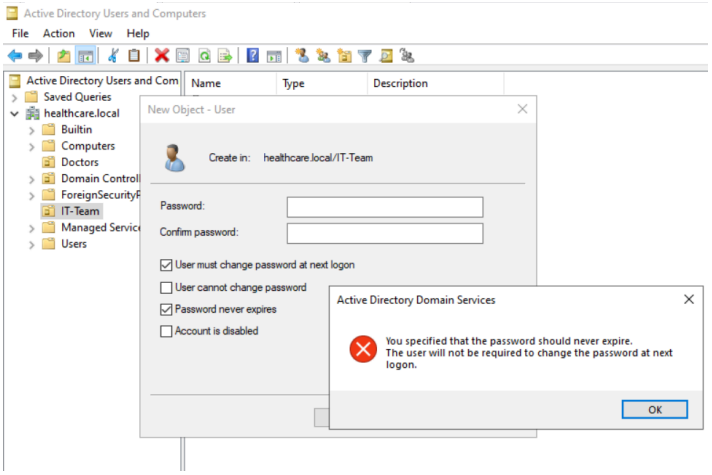


Figure 4.4.1 The warning message to ignore in virtual environment (Anastassiadis, 2025)

4.5 Domain Joining the Client

Login as the domain administrator as shown in (*Figure 4.3.1*) then in the windows search bar search for “This PC” then right click and go into properties. After that scrolling down and under the “Related settings” it should say “Rename this PC (advanced)” after that a popup windows comes up and one thing that is possible to click is where it says “ To rename this computer or change its domain or workgroup, click change” then go into change. Choose the domain and search after the domain name in this case “healthcare.local” everything will show in figure below.

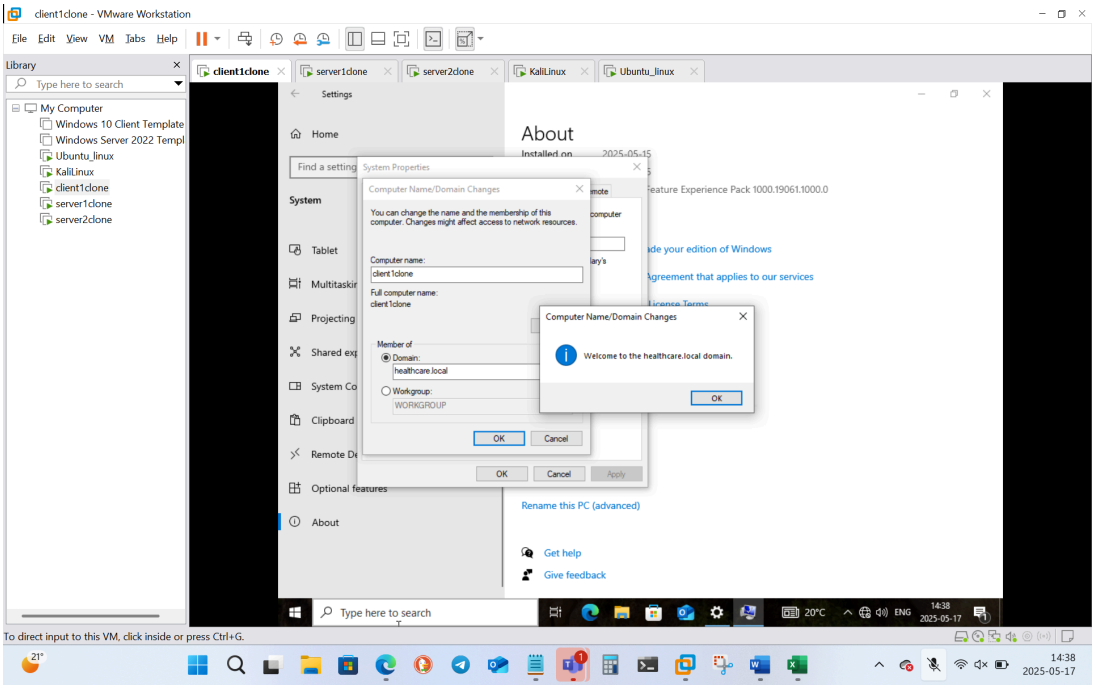


Figure 4.5.0 Showing domain join process (Anastassiadis, 2025)

If asked for credentials type in administrator and the password from server1 to then click ok and restart the computer. After that login as Dr. Alex.

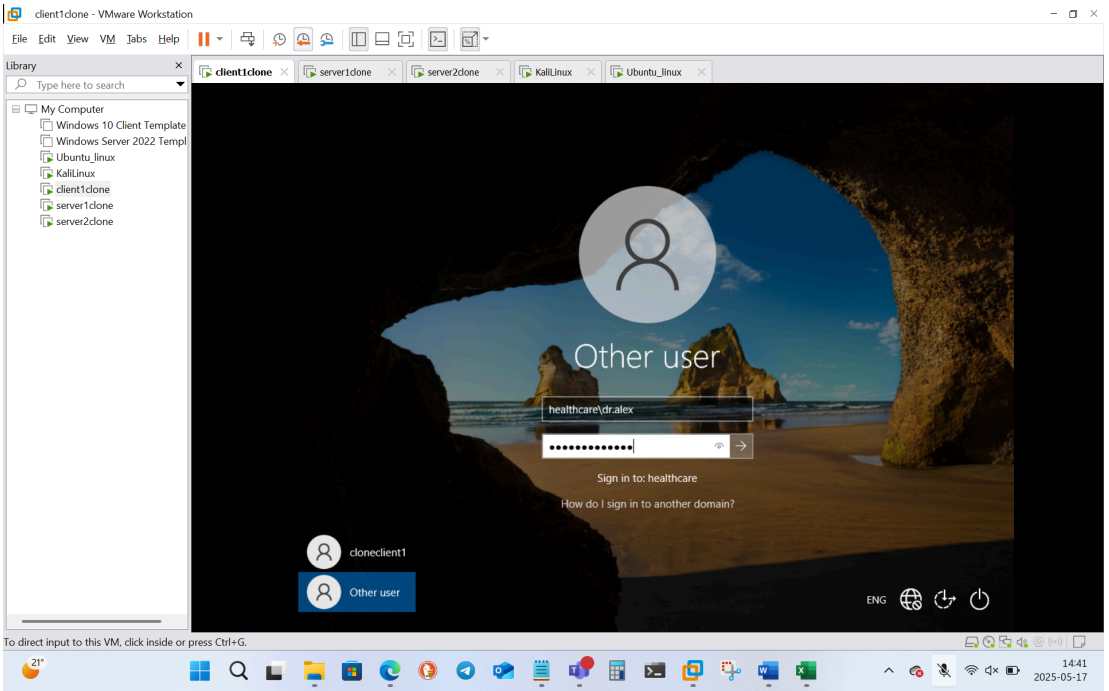


Figure 4.5.1 Login as Dr. Alex (Anastassiadis, 2025)

As it is now domain joined type the domain name then the user name which is dr.alex and it will then login as dr.alex successfully as shown below.

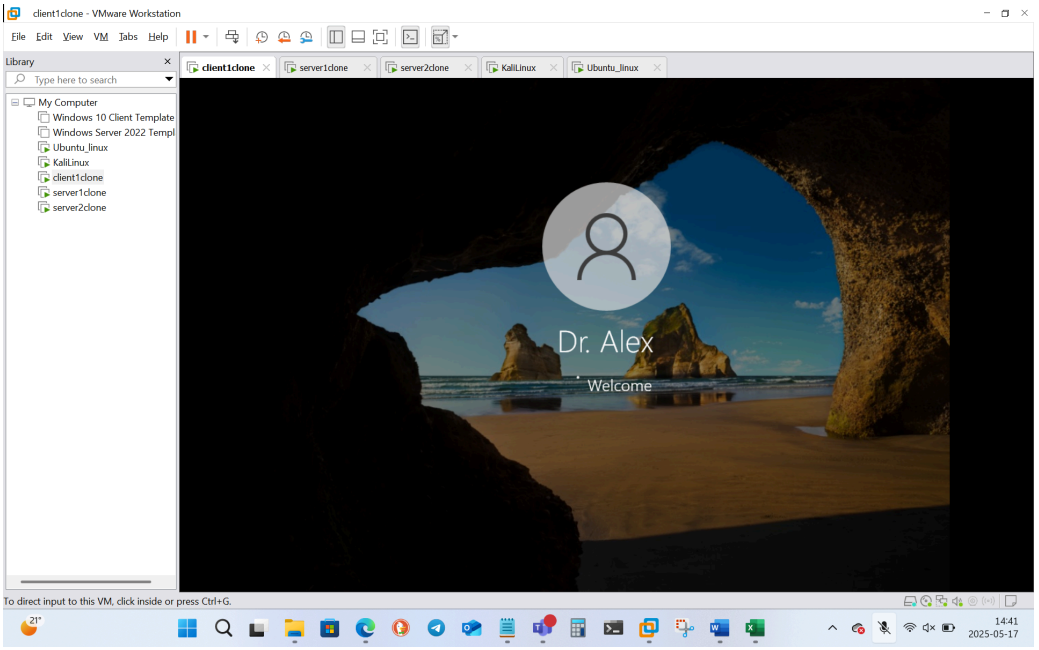


Figure 4.5.2 Displaying that Dr. Alex is logging in (Anastassiadis, 2025)

Server2 was also domain joined in the same domain so it can work with the other devices.

4.6 VPN Server Setup (Tailscale)

From server2 go into a browser and search for tailscales own website and find the download section and then for windows. After the download, start installing the program and after the installation it wants a login method where a personal gmail account was put in. After it's logged into an account it will connect to a private tailscale internet.

Then from the client tailscale is downloaded as before. Also logged into the same account as used on server2 and then it should be displayed in the tailscale menu on both of the devices connected to tailscale VPN services. With their own newly created IP addresses as shown below:

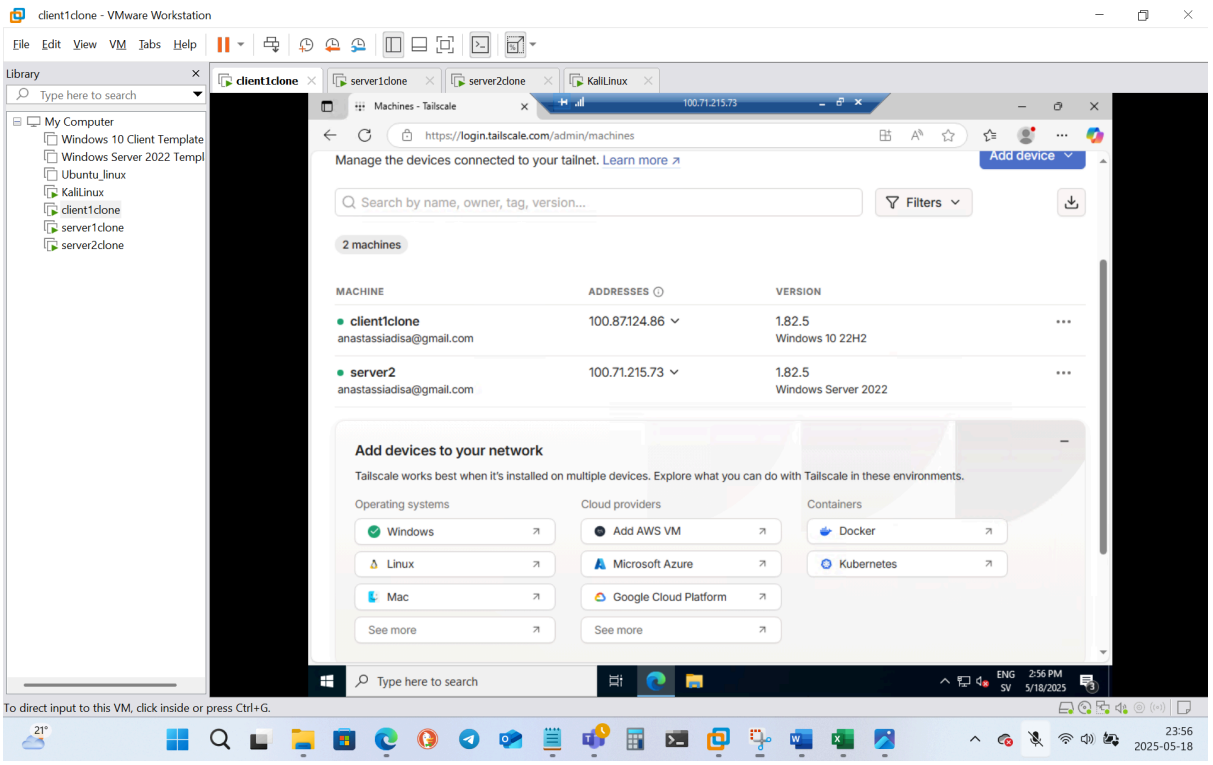


Figure 4.6.0 Shows client & server2 connected to same tailscale internet (Anastassiadis, 2025)

4.7 Connect From Client to VPN

Now it's time to test the connection between the devices connected with both ping and the help of RDP. So in the client go into the command prompt and type in tailscale ip -4 to get the newly given tailscale IP address. Do the same process on server2 to get that IP address also or type in tailscale status to get all the devices connected with its tailscale IP addresses. Then ping the tailscale address of server2 from the client as shown below.

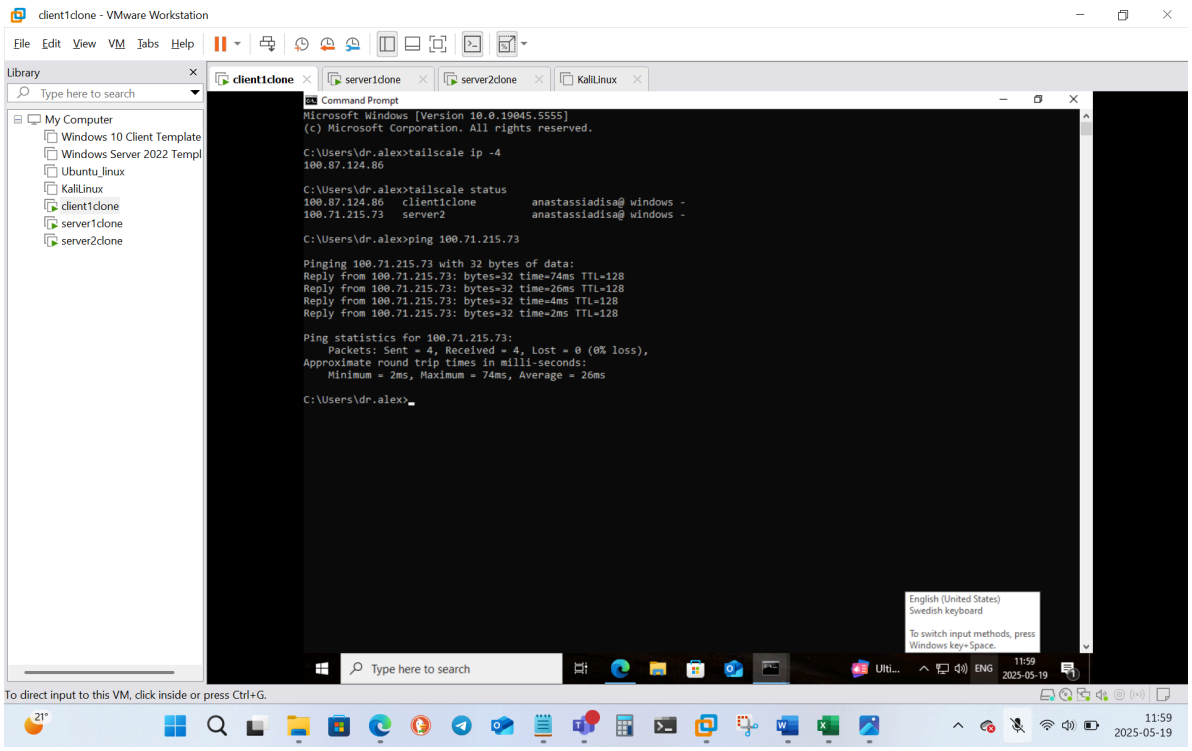


Figure 4.7.0 Commands mentioned earlier (Anastassiadis, 2025)

For the RDP part to connect to server2 from the client but with the tailscale IP address instead. So in the client search in the windows search bar for “Remote Desktop Connection” and click into it and in the computer name field the tailscale IP of server2 is put in there. After that it should be connected remotely to server2 and to show that the connection is going and both devices is connected it shows in (*Figure 4.6.0*) and it displays the IP address of server2 in the top of the picture which means that is the device that's connected through RDP, the picture will follow again for clarity:

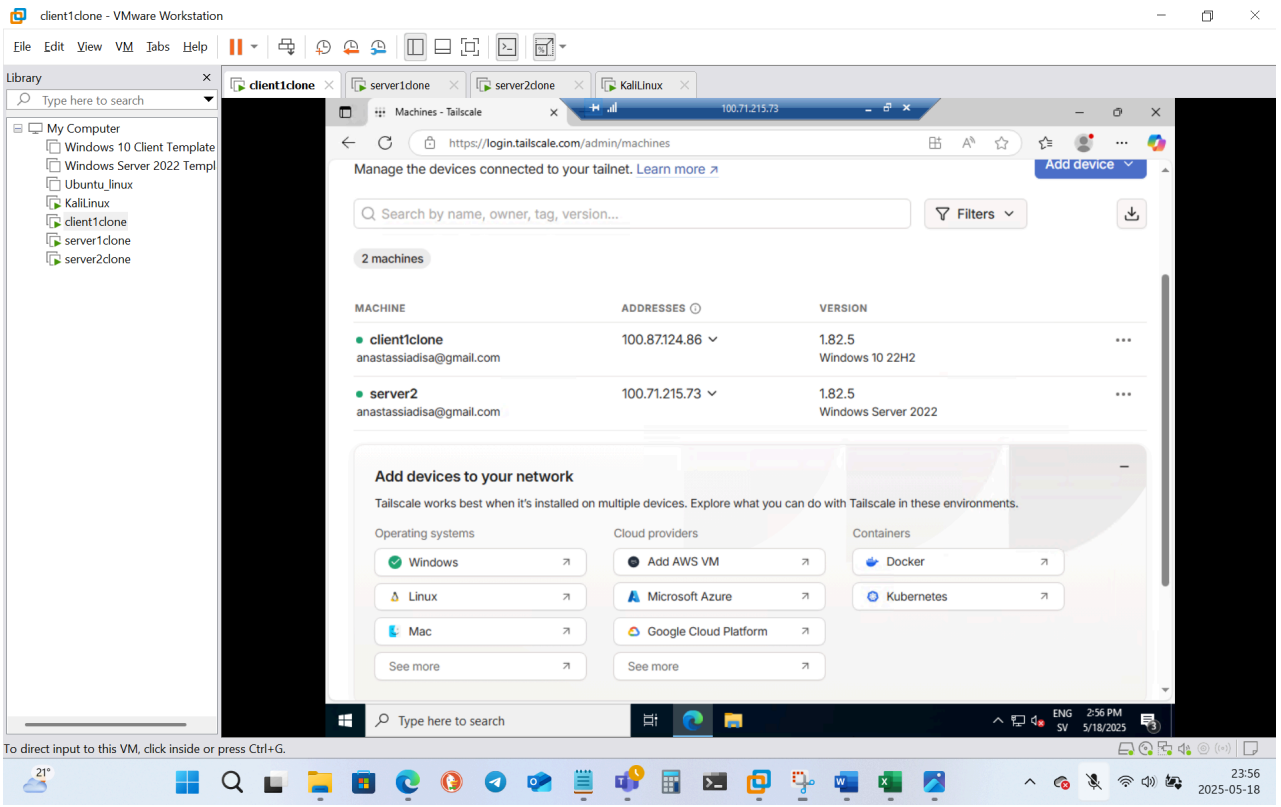


Figure 4.6.0 Referring back for clarity (Anastassiadis, 2025)

If there would be a problem with connecting through RDP because of that server2 where RDP isn't activated. Press the windows button + r then type "SystemPropertiesRemote.exe" then when the popup window is showing go to the Remote option and check the box for "Allow remote connections to this computer". Then it's also possible to choose which users are able to connect through RDP to that device which is also showing a secure and important part for keeping it safe. Both of these options will be shown below.

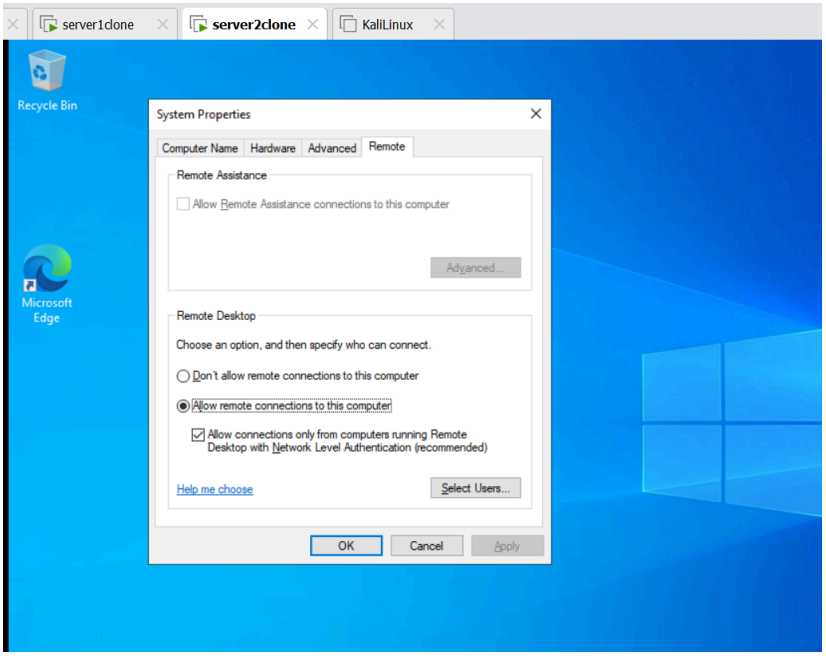


Figure 4.7.1 Displaying the allow RDP connections button (Anastassiadis, 2025)

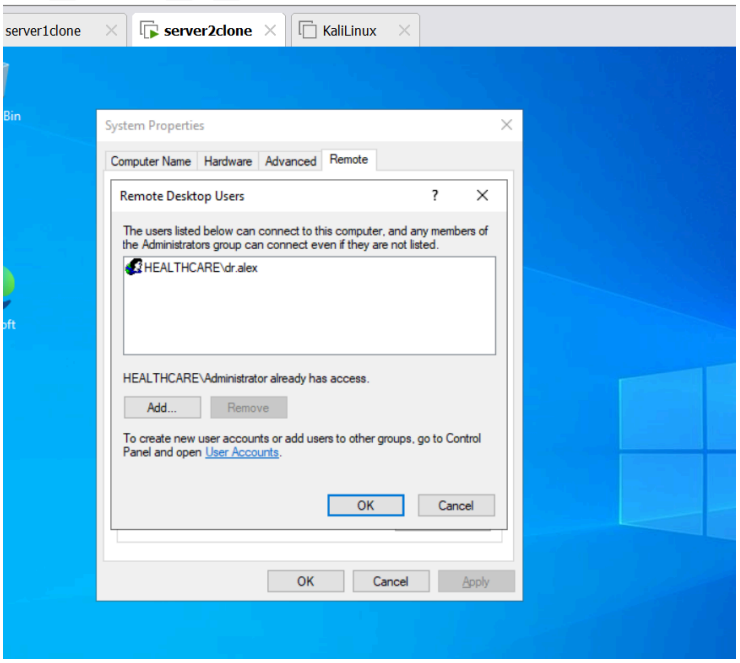


Figure 4.7.2 Shows adding users to RDP (Anastassiadis, 2025)

4.8 Installation of MFA (DUO)

To ensure that remote access is secure to server2 MFA was installed and configured on the device, which is preventing unauthorized users from accessing the device even if they got their hands on the password for some reason there is another step to prove who you are.

First step is to create a Duo account which is made by going into their official website and signup. Then create a free account and start filling the form that is like this picture that follows.

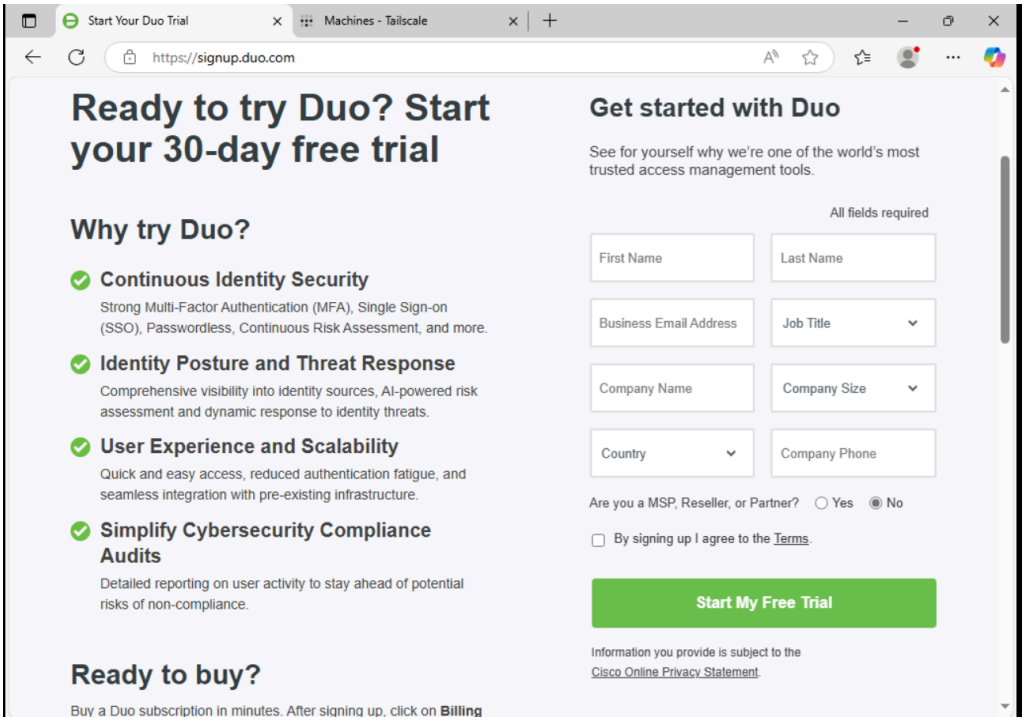


Figure 4.8.0 The form for creating a Duo account (Anastassiadis, 2025)

After the account is created once inside the admin portal go to Applications → Protect an Application and search for “Microsoft RDP”, click at protect besides Microsoft RDP then a site should be provided with following things: Integration key, Secret key, API Hostname which is important to have nearby and remember them because they will be needed later on during the configuration.

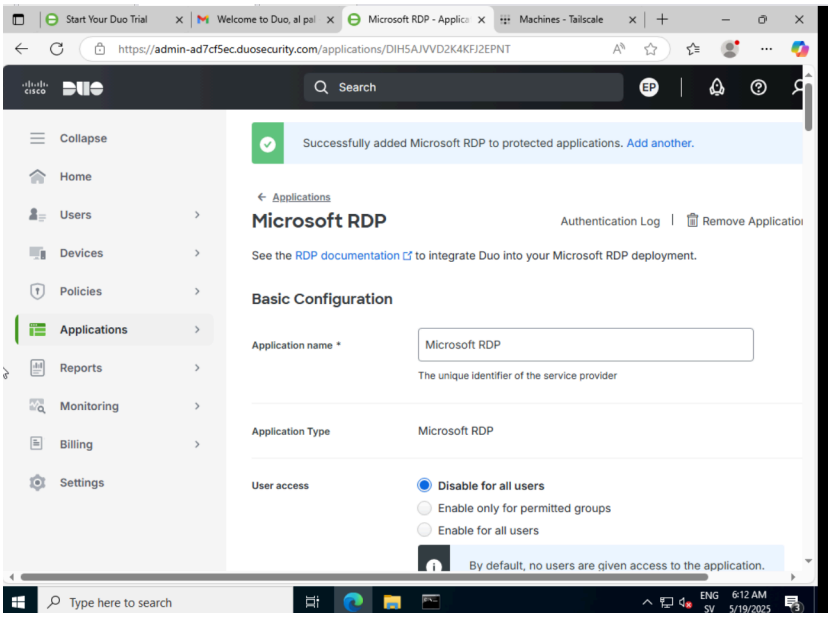


Figure 4.8.1 The application configuration (Anastassiadis, 2025)

Now time for downloading Duo for windows logon so click the sublink “RDP documentation” that is seen in figure 4.8.1 and then scroll down to Step 1: Install Duo and click download the installer. Open up the file on server2 and the configuration wizard will start. Now it's time to fill in the details provided before as mentioned (Integration key, Secret key, API Hostname) like shown below in the following two pictures.

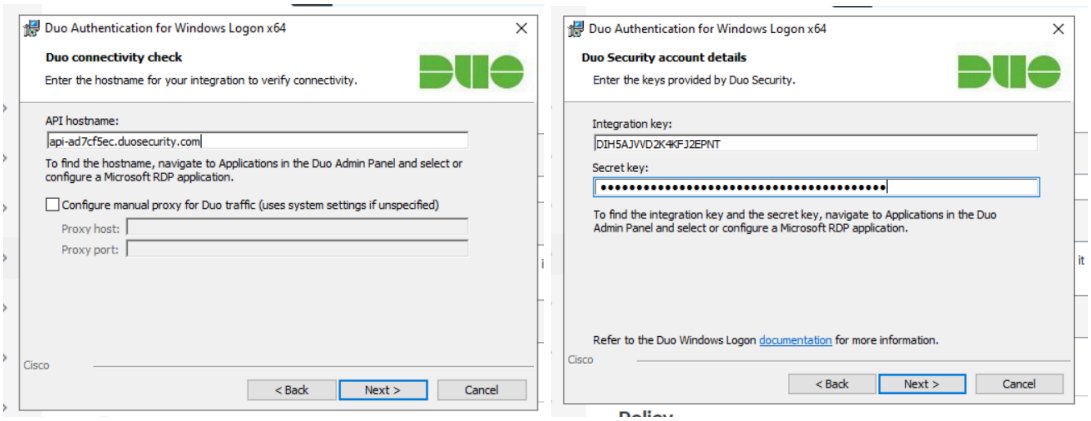


Figure 4.8.2 Show the API hostname, Integration key, Secret key (Anastassiadis, 2025)

When clicking next those pages it will appear three integration options to choose between and here the box for “Only prompt for Duo authentication when logging in via RDP” will be checked as it's helping us to prove that it's working in this project, so it will look like this picture below.

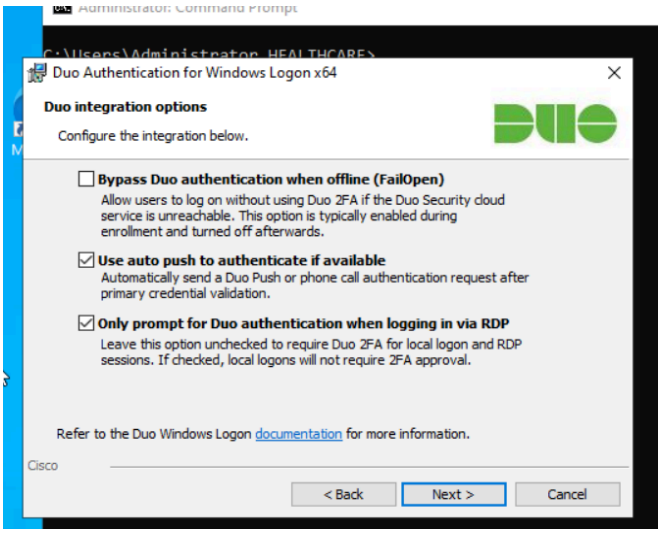


Figure 4.8.3 The configuration of integration options (Anastassiadis, 2025)

If it would appear a bad time request warning when trying to fill in the Secret key etc. it can be because of the time on the device that its not rightfully adjusted to where the location is set and it can look like this:

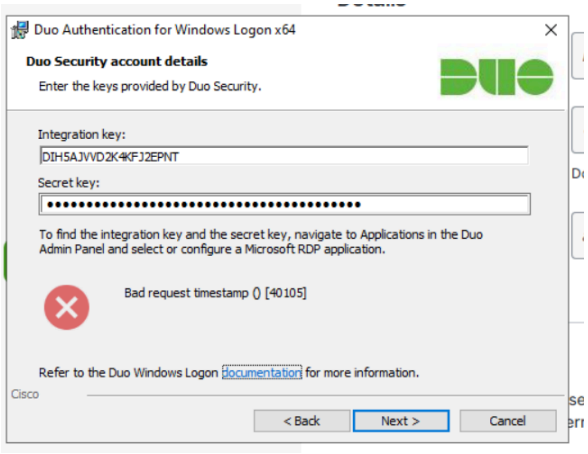


Figure 4.8.4 Displaying error message (Anastassiadis, 2025)

If it would appear it's only that the time needs to be adjusted rightfully and correctly to where you are or what the device location is set as.

Now time to add users so it is located at users in the Duo admin side then click add users and itadmin user is going to be added so that is going into username and then hit save button. Under the user there will be a button where it says add phone and then a phone number is filled in and the method Duo Mobile App is chosen. So in the following picture below is

showing the created user “itadmin” with also a phone and that the status is active and ready to be used:

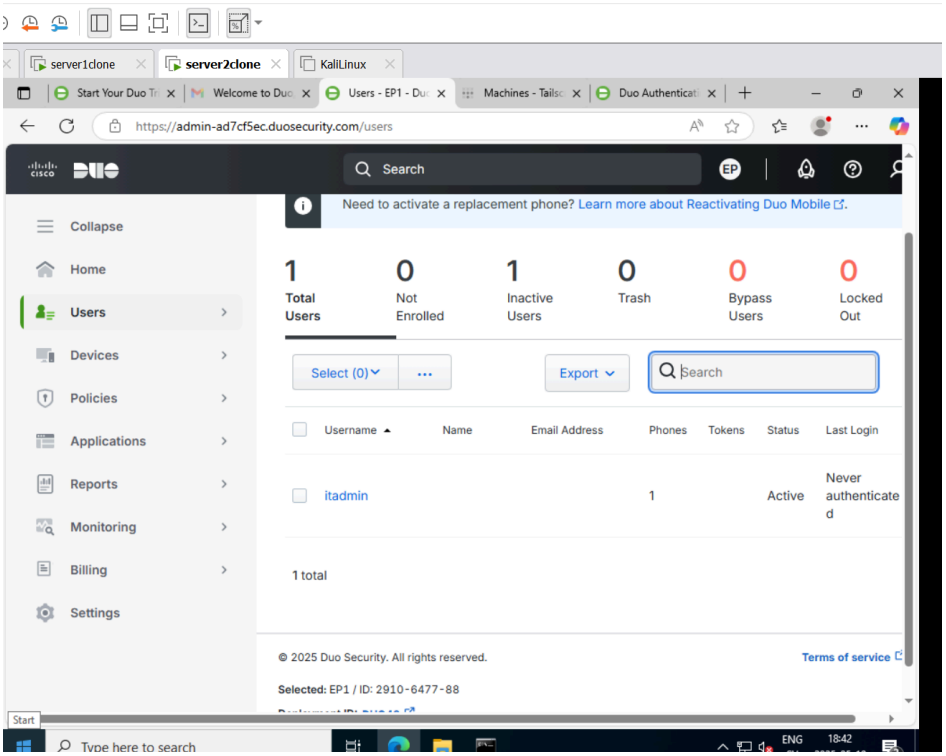


Figure 4.8.5 User added in Duo with phone (Anastassiadis, 2025)

Now it’s time to test that the MFA is working as it should so a RPD connection from the client is going to be made and see if it's needed with a security code as an extra step. So in the client the remote desktop connection is searched in the windows search bar and opened and is going to connect to server2 via it’s tailscale IP as before and is going to show the IP address in the top of the picture and that it’s from the client and also that an authentication is needed to proceed.

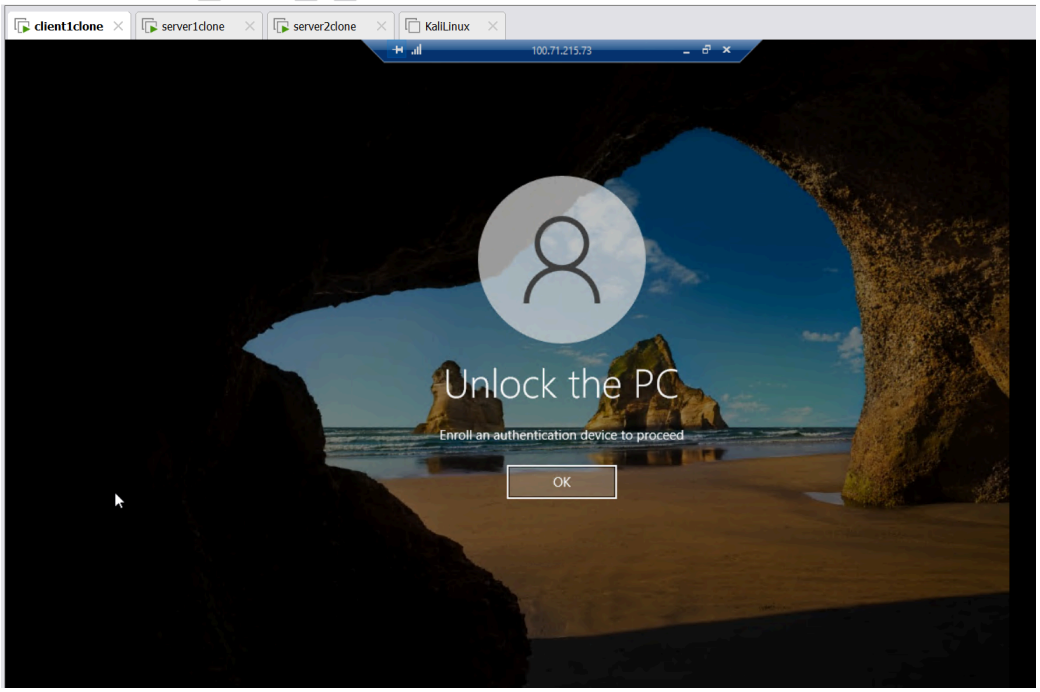


Figure 4.8.6 Login failure because of MFA needed (Anastassiadis, 2025)

Then it sends a three digit code to the phone and lets the user identify itself to succeed with the login.

4.9 Network Segmentation

Network segmentation was equipped on server2 by making a windows firewall rule that is aiming to block out the IP address from the client machine. So the steps now to accomplish this is to be logged in as the administrator on server2.

Then press windows button + r to then search for wf.msc which opens up Windows Defender Firewall with Advanced Security. Now it's time to create a new inbound rule which is seen in the left hand side panel in the window. Then in the new inbound rule wizard first step that is Rule type choose custom then in program side leave as all programs and in protocol and ports side leave as default which is Any then at the scope part which is the important stuff. Here under "Which remote IP addresses does this rule apply to?" select "These IP addresses" box then add the IP address of the client. That is simulating the blocking of a specific device. Then at action choose block the connection and lastly at profile choose Domain, Private, Public and the new rule is named BlockClientFromServer2 which is shown below.

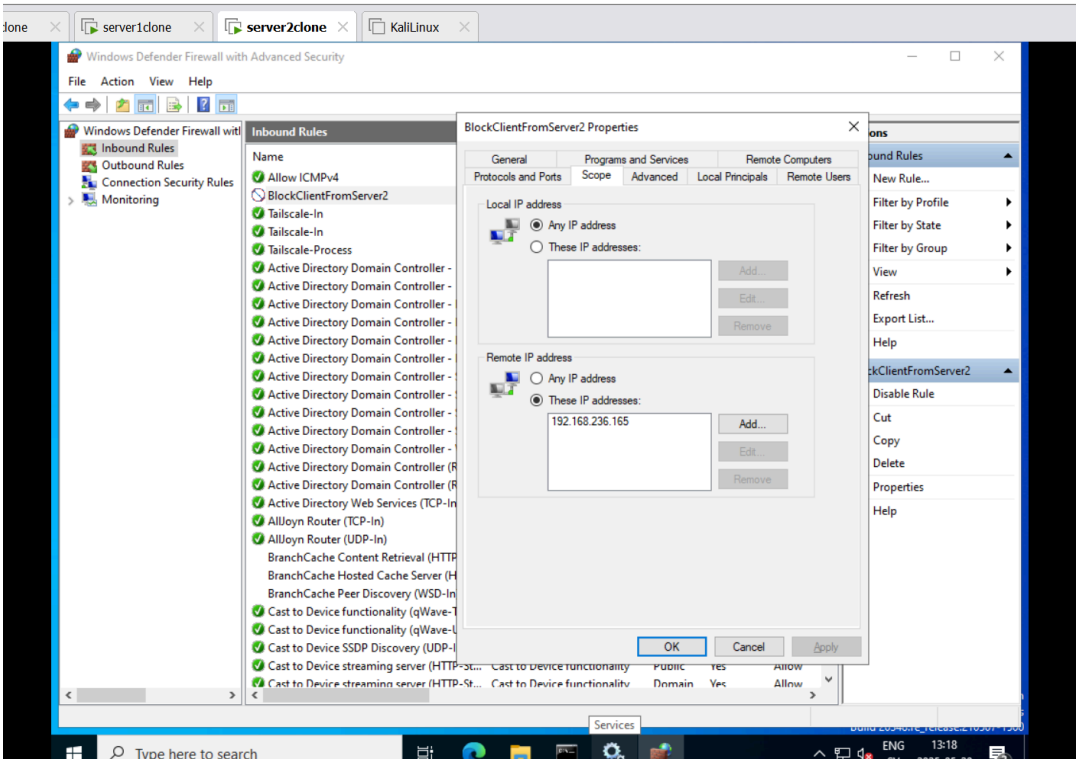


Figure 4.9.0 Newly created firewall rule which shows client IP address blocked (Anastassiadis, 2025)

Now to test the segmentation the client machine needs to be opened and first try to ping the server2's IP address from the command prompt and also try to RDP server2 which is going to show that it's not possible to do either of them as the client is blocked. So the following pictures show the failed connections.

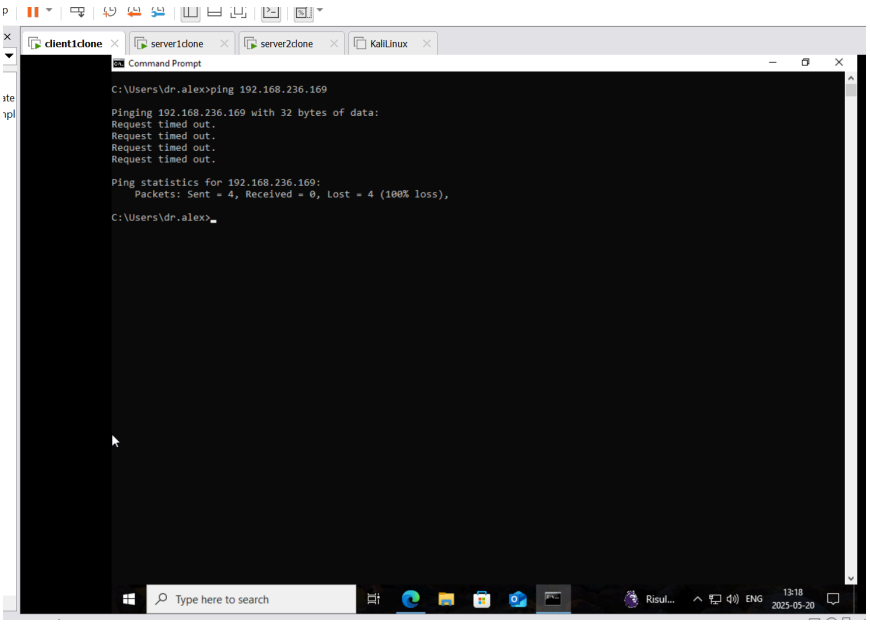


Figure 4.9.1 Showing ping failure (Anastassiadis, 2025)

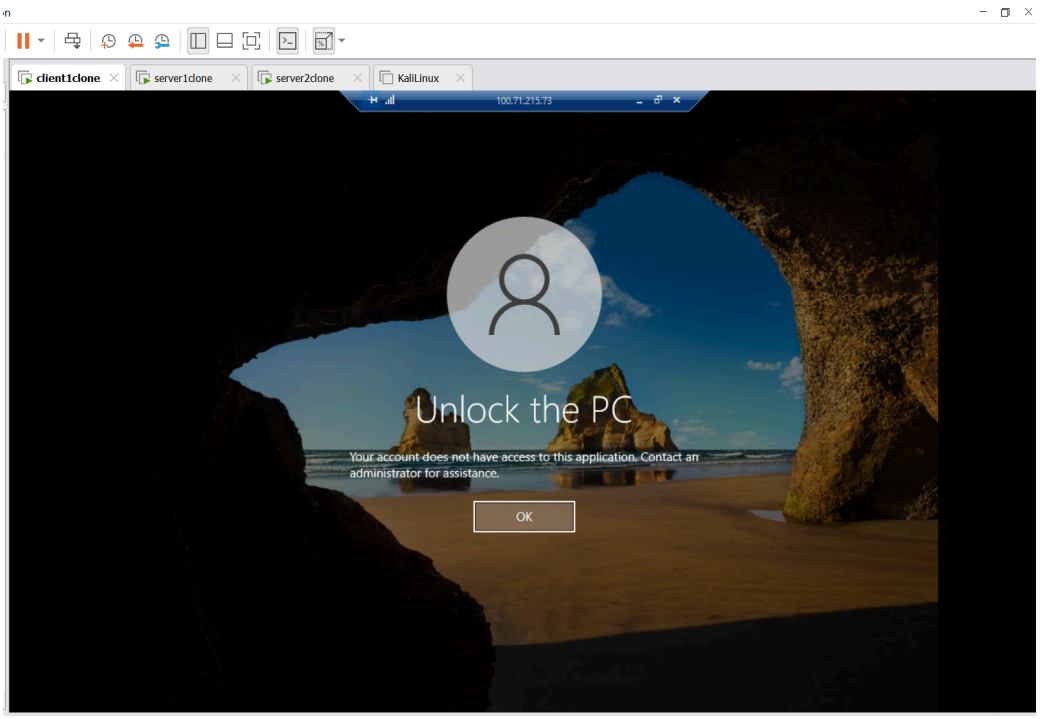


Figure 4.9.2 RDP failure (Anastassiadis, 2025)

This network segmentation can be switched the other way also instead of blocking out one specific device all devices can be blocked from start and then choose those specific devices and users that should have access. So from blocking some to only allowing trusted users which is a much more secure option and more used in real life but this was not in the practical part in this project.

4.10 Vulnerability Scanning (NMAP)

So in this phase a vulnerability scan was made using Nmap from the Linux machine to scan the server2 with its IP address which is revealing open ports and services as mentioned in 2.8 part in this report.

So the first step is to start the Kali Linux machine and make sure it's connected to the same network as the other machines used before. It is always a good option to type in the ip a command to get the ip address of the Kali Linux machine.

Then type in the following command to make a Nmap scan specifically targeted to server2: nmap -sS -sV (IP address of server2) and it will perform its scan. It usually takes a minute or two to get the results and to break down the command -sS stands for stealth SYN scan which

is harder to detect as it is not completing the TCP handshake. -sV is for attempting to detect service versions and then the IP address that is targeted in this case server2.

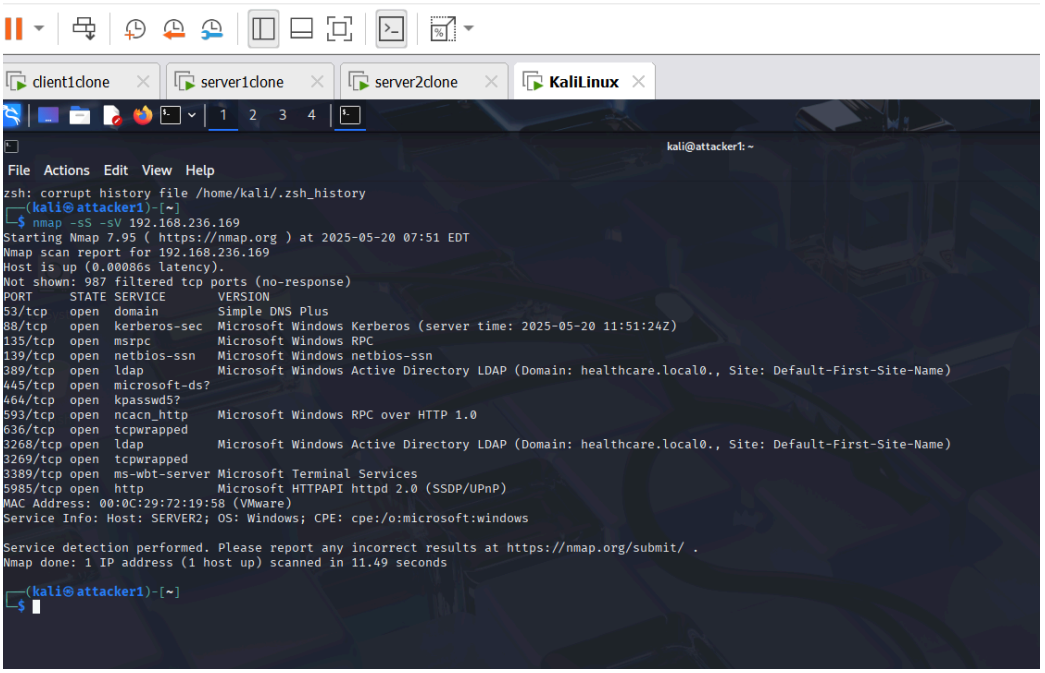


Figure 4.10.0 Nmap scan display (Anastassiadis, 2025)

The scan in the figure above shows all the ports that are open also as services that is running also the domain and the domain name and as it is seen on the picture, also that 3389 port is open which is for RDP and as one can understand it's a security problem for it to be displayed this easy for someone running a scan on a device. This in a real world remote healthcare system could be exposing data that shouldn't be able to be stolen. That's why all these implementations of security are needed.

A Nmap scan can also be targeting the whole network and not just server2 as in this case then it would be for example instead of the IP address of server2 (192.168.50.0/24) which is targeting all the devices on the subnet. Also another option is just a faster and easier scan for maybe lab environments then it is just the command nmap and the IP address after the device which is targeted.

4.11 Phishing Test (Gophish)

Phishing is the most common method for engaging ransomware attacks in hospital environments as well as the rest of the world, where fake emails are being sent to trick

employees and make them think that they are from within the infrastructure such as IT departments and so on. So this step is where a phishing simulation is made using Gophish, so a fake email is sent to a user within the system that is clicking a link within the email and entering its credentials. That is just telling us that implementing MFA and to get the employees to be more aware is important.

Step 1:
Open the terminal in Kali and type in the command: git clone https://github.com/gophish/gophish.git

Step 2:
Now enter the newly created folder with, cd gophish

Step 3:
Then build and launch the gophish with command: go build ./gophish if go is not installed on the machine then run sudo apt install golang.

Step 4:
After the launch is done, get into a browser in Kali and search for https://127.0.0.1:3333 . It can be a SSL warning which is just ignored as this is safe in a test environment. Then login with the credentials that's default which is admin as username and same as password. Down below is how it is supposed to look when logging in.

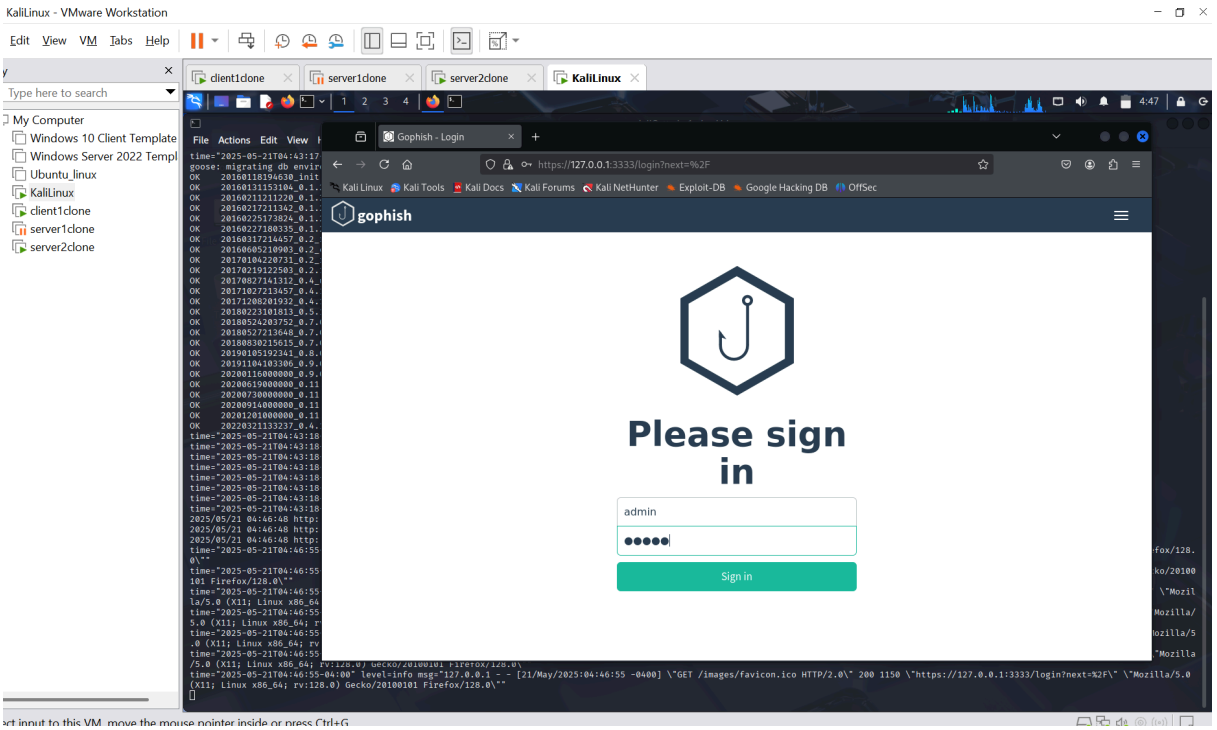


Figure 4.11.0 Login at gophish (Anastassiadis, 2025)

Step 5:

Now time for creating users and groups so in the dashboard in gophish go to the users and groups and click +New group. Add a group called Doctors as the one we created before then add a user with name in this case alex and email, dr.alex@healthcare.local as seen below:

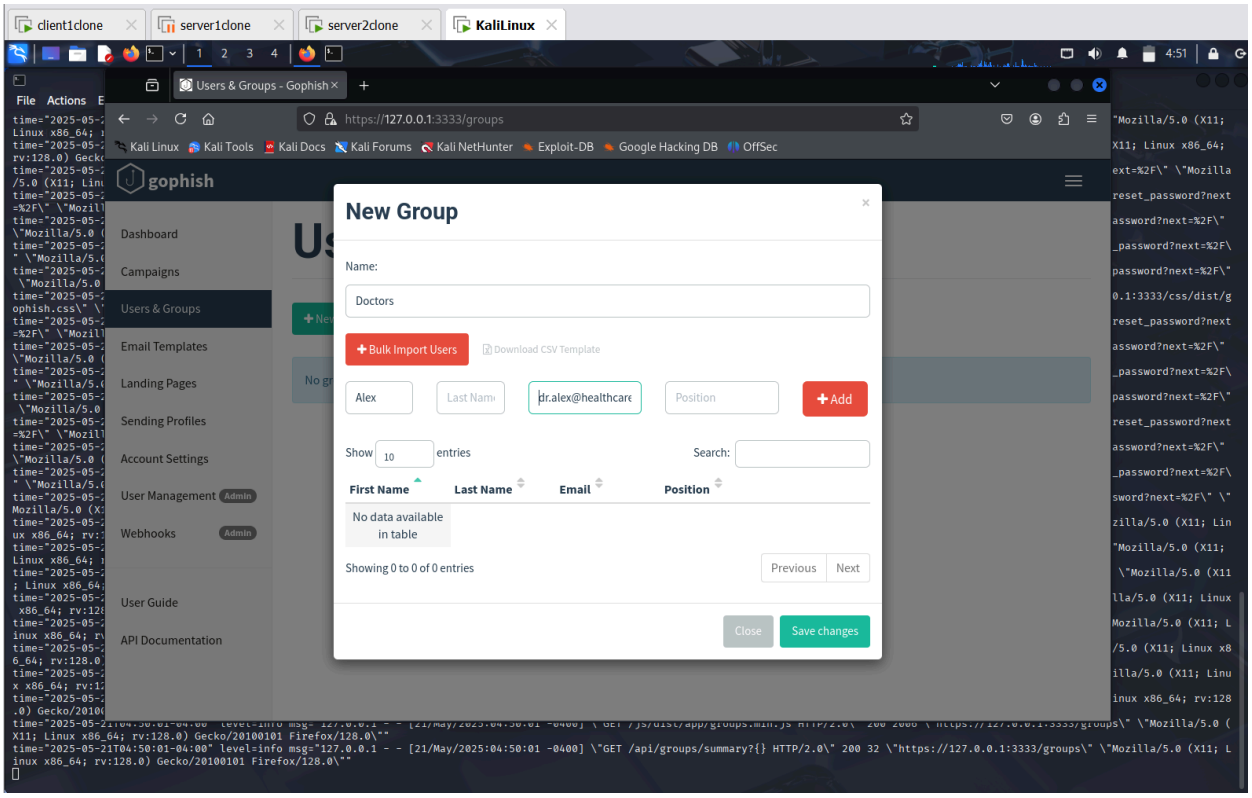


Figure 4.11.1 Showing New group and user (Anastassiadis, 2025)

Step 6:

Now it is time to make the email template for the phishing test. So it is at Email templates → click +New template then choose a title and the subject as one would in a real email and put a text or HTML in the body. Shown below:

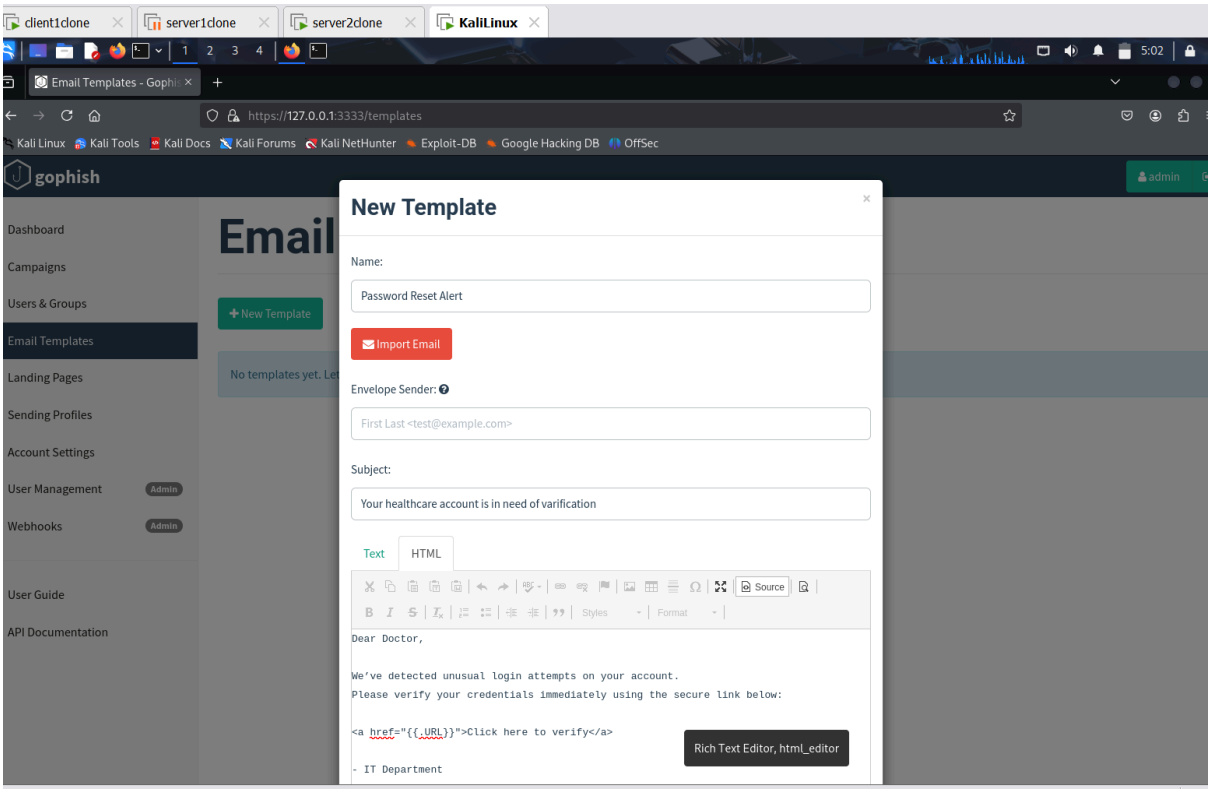


Figure 4.11.2 Email template (Anastassiadis, 2025)

Step 7:

Now time to create a landing page which is made by going to the landing page then click +New Page. Put a name on it but in this project it is named Fake Healthcare Login. Then put in a basic HTML or a Gophish template and check the boxes where it says "Capture

Submitted Data” and “Capture Passwords”.

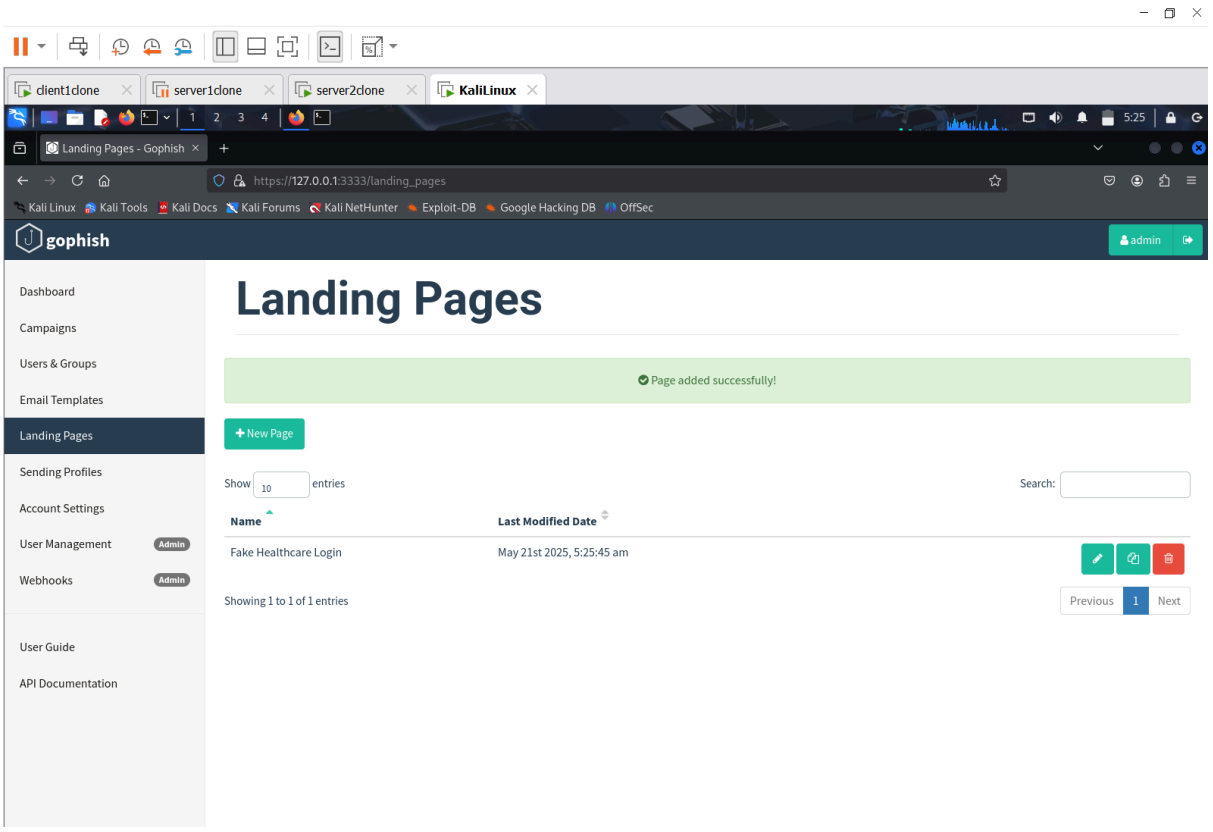


Figure 4.11.3 Landing page created successfully (Anastassiadis, 2025)

Step 8:

This step is where the campaign is created and launched. So as the other creations are by campaign and then click +New Campaign. Now choose the name then the email template and the landing page that were done before. In the URL string put the Kali machine's IP address and :80 after and send it to the doctors group.

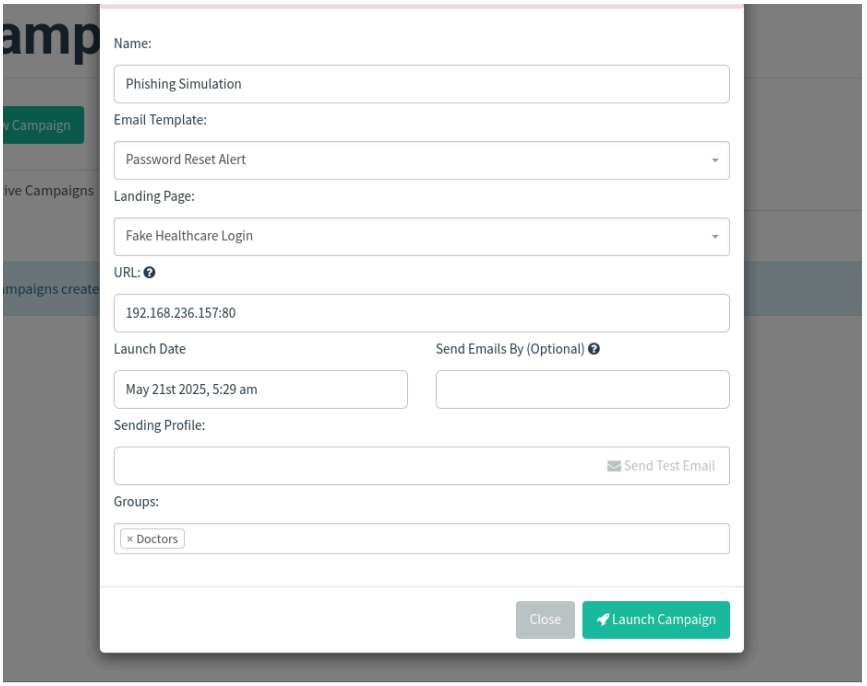
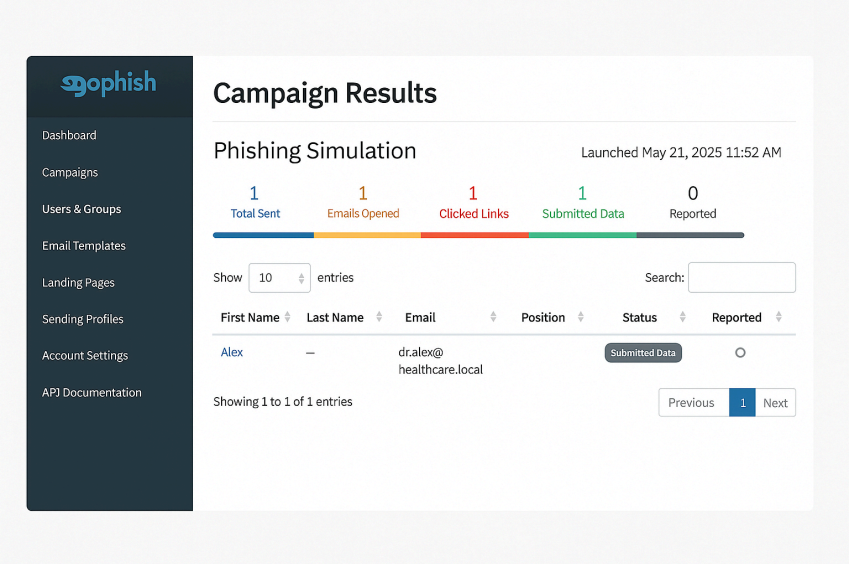


Figure 4.11.4 Campaign launched (Anastassiadis, 2025)

Step 9:

This is the last step in the phishing test, so now it's time to simulate the attack. Logging into the client machine as dr.alex and the email from Gophish is opened via the browser by searching for the Kali IP address and :80 as mentioned in the URL. Click the link in the email and enter some fake credentials. The following pictures are generated by AI because during the tests the software didn't work as it should have, also its going to display that inside the Gophish website it's going to show if the email was sent and if the link in the email was clicked and also the credentials of the user/device that clicked the link.



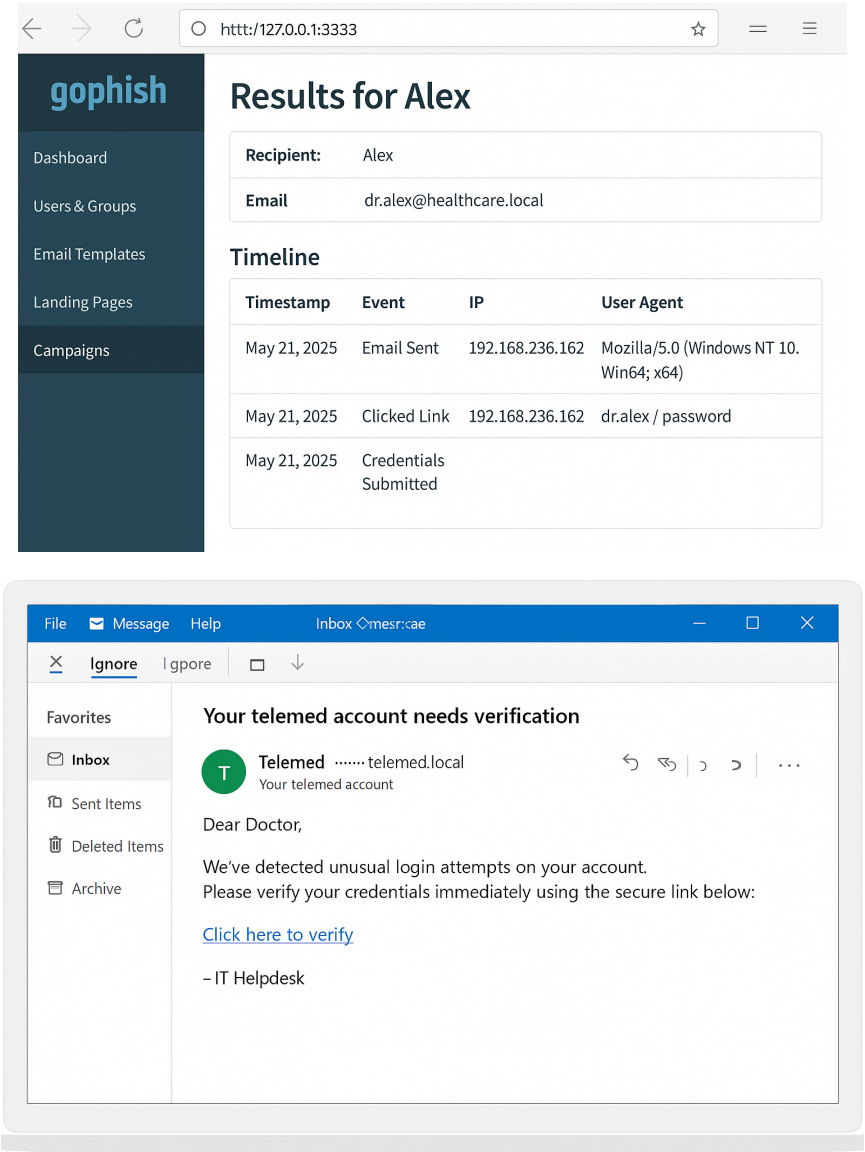


Figure 4.11.5 All three pictures above generated by AI to show practical parts that was mentioned before (ChatGPT OpenAI, 2025)

4.12 Monitoring Using Windows Tools

Instead of installing software to monitor for the device the built in windows tools were used to monitor the behaviour. So here in the last step of this project windows firewall, event viewer and network monitoring will be used to simulate detection tools like other third party applications. Where a Nmap scan is going to be run from the Kali machine and then see how the tools are monitoring and detecting the behaviour.

The first step in this section will be to enable firewall logging so in the windows search bar go into Windows Defender Firewall with Advanced Security, in the middle part there should be a

sublink that says “Windows Defender Firewall Properties”. After going to the private profile tab and down by logging click customize. Now set the Log dropped packets and Log successful connections → yes and keep the name which is the file path to just the basic default setting.

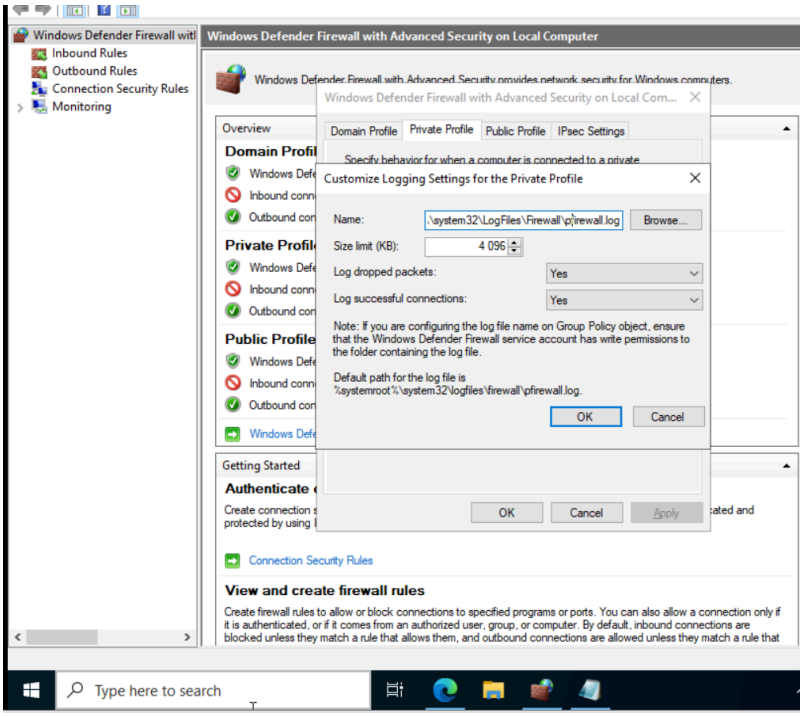


Figure 4.12.0 Firewall logging settings shown (Anastassiadis, 2025)

Second step is to run the resource monitor to keep an eye on connections going on live, where to do it press windows button +r then type resmon and hit enter. After the window opened up go to the network tab and under the network activity tab it will show live connections as shown below:

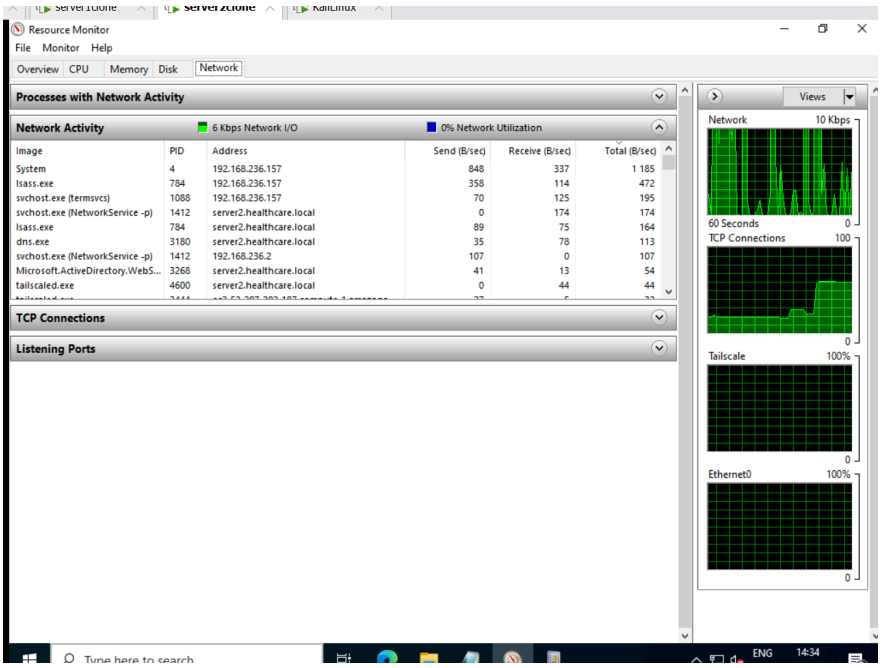


Figure 4.12.1 Showing internet connections in resource monitor (Anastassiadis, 2025)

Now to simulate an attack from the Kali machine the command “nmap -T4 -A (IP address of server2)” where -T4 is standing for timing template and is determining how aggressive the scan is as it ranges from T1 to T5 then the -A is for advanced scan which includes many things such as which OS is in use by the device etc just to make the “attack” as aggressive as possible. The command is trying to scan for open ports on server2 and then using the tools mentioned before to scan and see for warning triangles during the attack.

Before the attack, open up the event viewer and press down Windows logs and take up System and Security, then the ones mentioned before.

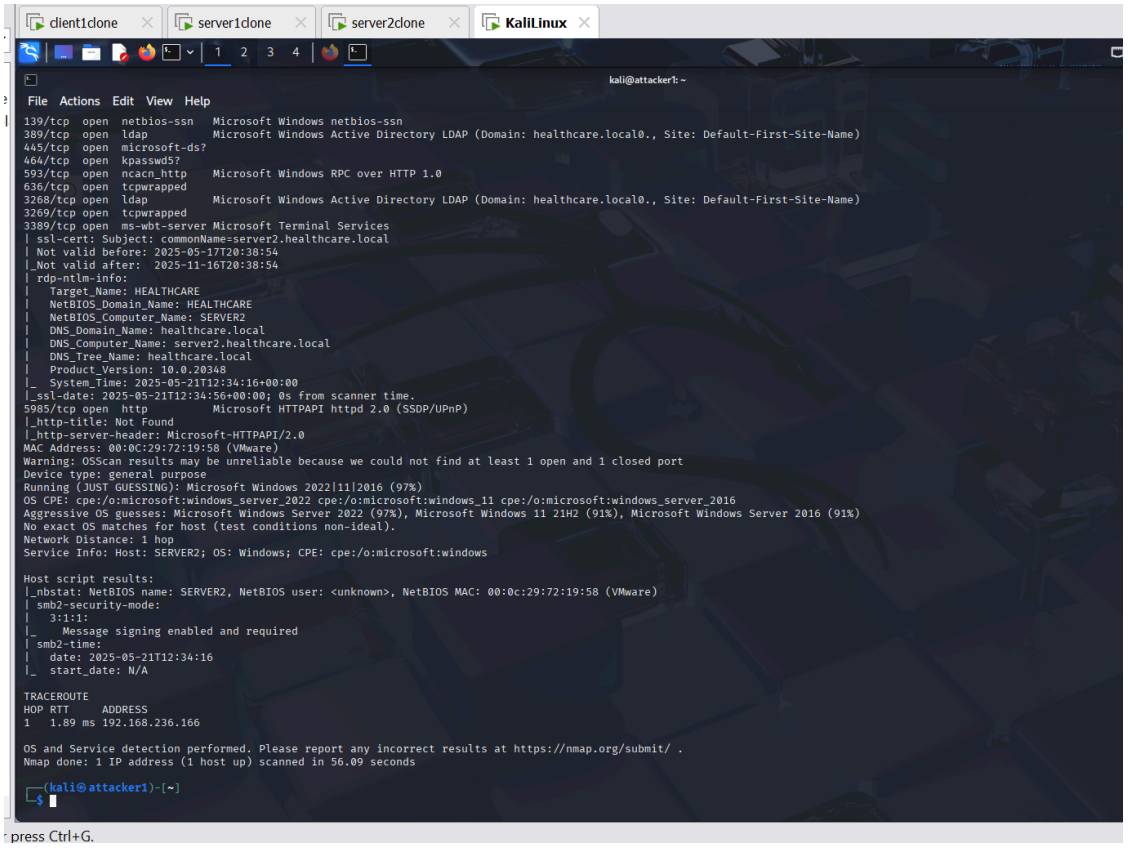


Figure 4.12.2 Nmap simulated attack shown against server2 (Anastassiadis, 2025)

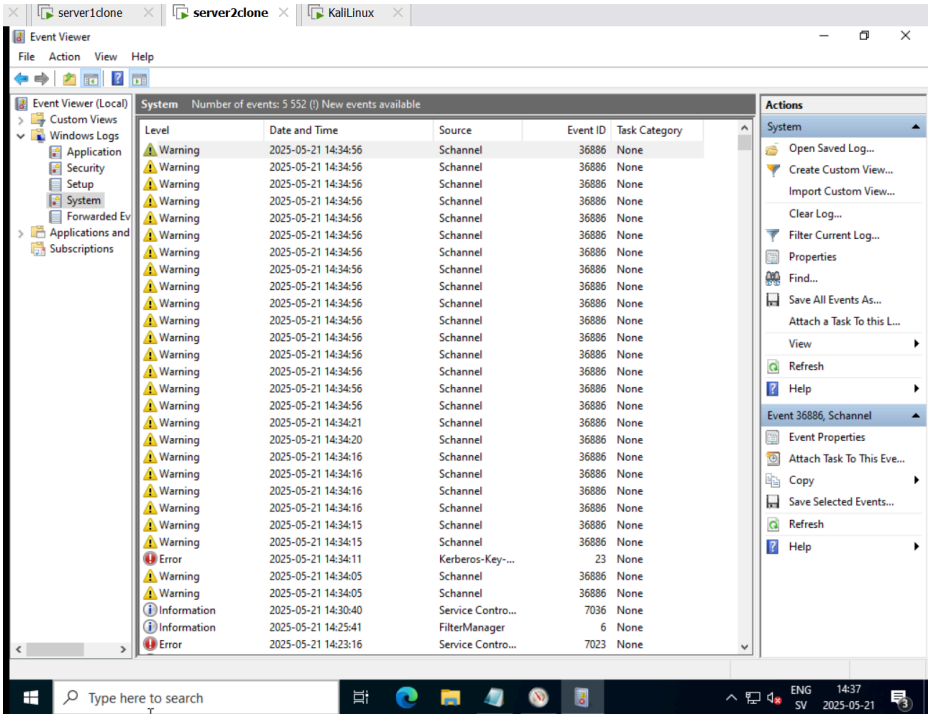


Figure 4.12.3 Event viewer (System) showing schannel warnings that is SSL related tries (Anastassiadis, 2025)

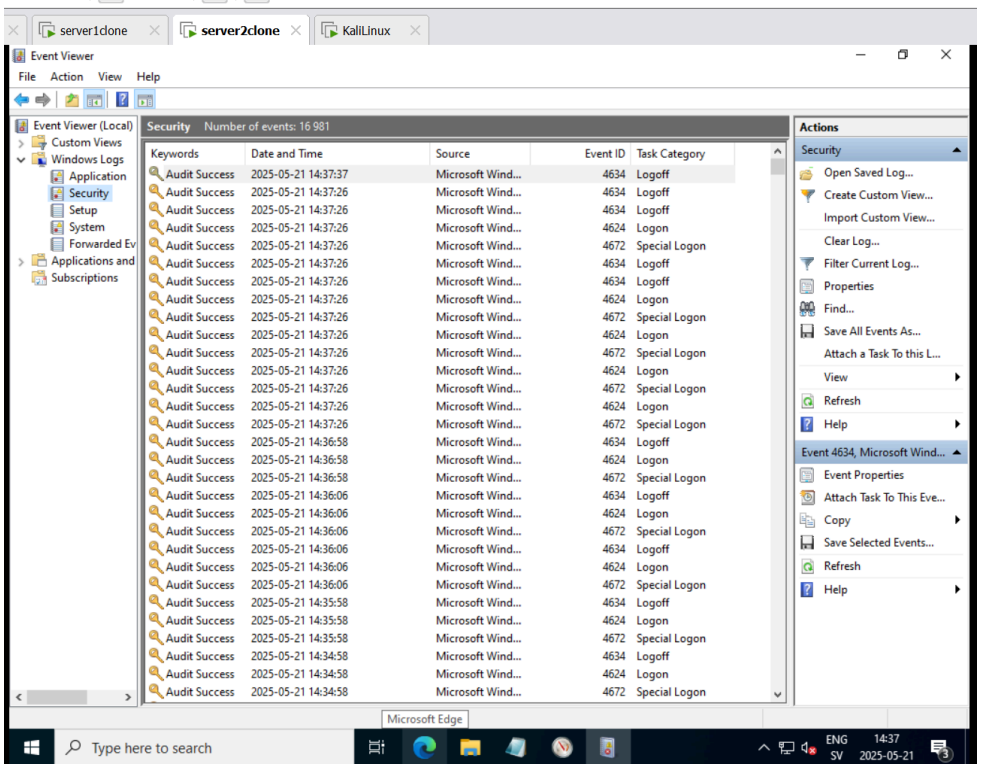


Figure 4.12.4 Showing logons and logoffs which can show brute force attacks or unauthorized access trying (Anastassiadis, 2025)

Then have network activity also on so it's possible to track the activity on there as seen in (*Figure 4.12.1*).

5. Summary & Conclusion

The project was built to simulate and demonstrate a real world healthcare environment with remote cybersecurity threats in mind particularly. Mainly the goal was to make tests and show some strategies to defend the vulnerabilities within healthcare such as data about employees, clients and even the infrastructure of it all.

All of the setup and the infrastructure were created in VMware with four different virtual machines: one Windows client that represented a doctors setup, two Windows servers, and last a Kali Linux machine that was an attacker. Server1 was working as the domain controller and DNS and Server2 provided access remotely, firewall segmentation and logging etc.

This project was using some of the best security practices by implementing role-based access control (RBAC) through Active Directory, making sure that remote access is secure using VPN in this case Tailscale, also setting MFA with Duo Security. These additions made sure that non authorized users couldn't just go in as they would like and only authorized users could access data inside and from outside networks.

An inside phishing test was runned using Gophish which shows that attackers often depend on human beings' own failures to get access. The end results from that test showed the real importance of security awareness training by the staff.

Then the attack surface was more thoroughly looked into using Nmap as a tool where scanning were simulated, those behaviours were logged and monitored using Windows built in tools like Event Viewer and firewall logs that showed plausible attacks.

Some initial thoughts for doing some of the tasks were supposed to be with some other software and tools instead of those used in the project but all the other methods that were used instead showed perfectly fine how they work and the importance of all monitoring and detecting unusual behaviour.

To wrap up everything, this project displayed how important a layered defence strategy, network segmentation, VPN access, phishing awareness and even live monitoring is a must to keep things secure. All of these strategies and tools are improving the cybersecurity aspect of healthcare businesses and even if it was limited tools and so on it shows how important even those easy to use are doing a good job.

6. References, Research & AI Usage

Within this project AI generated pictures can take place as some of the software didn't work as it should, from ChatGPT by OpenAI.

Anastassiadis, A (2025) Screenshots provided by the student mentioned in the text.

Bigelow, S.J., Yasar, K., Shacklett, M.E., (2025) “What is multifactor authentication?” Available at: What is Multifactor Authentication (MFA)? | Definition from TechTarget [Accessed 27 May 2025]

Chaturvedi, U., Chauhan, S.B., Singh, I., (2025) “The impact of artificial intelligence on remote healthcare: Enhancing patient engagement, connectivity, and overcoming challenges”. (Figure 1.0.0). Available at: The impact of artificial intelligence on remote healthcare: Enhancing patient engagement, connectivity, and overcoming challenges - ScienceDirect [Accessed 18 May 2025]

ChatGPT, OpenAI (2025) Generated pictures to back up claims (Figure 4.11.5) [Accessed 21 May 2025]

Eddy, N (2025) “2025’s Biggest Healthcare Cybersecurity Threats” Available at:The Biggest Healthcare Cybersecurity Threats in 2025 | HealthTech [Accessed 6 June 2025]

Higgins, M (2022) “What is a remote access VPN and how does it work?” Available at: What is a remote access VPN and how does it work? | NordVPN [Accessed 27 May 2025]

Kosinski, M., Forrest, A., (2023) “What is vulnerability scanning?” Available at: What is Vulnerability Scanning? | IBM [Accessed 28 May 2025]

Landsberger, D (2023) “What Is Network Segmentation and Why Does It Matter?” Available at: What Is Network Segmentation? | Computer Networking | CompTIA [Accessed 28 May 2025]

Srėbaliūtė, A (2024) “Phishing awareness training: What your employees should know” Available at: Phishing Awareness Training: What Your Employees Should Know [Accessed 28 May 2025]

Shivanandan, M (2020) “What is Nmap and How to Use it – A Tutorial for the Greatest Scanning Tool of All Time” Available at: What is Nmap and How to Use it – A Tutorial for the Greatest Scanning Tool of All Time [Accessed 28 May 2025]

Verizon (2024) “2024 Data Breach Investigations Report” Available at: 2024 Data Breach Investigations Report | Verizon [Accessed 28 May 2025]