Secure Solution: Implementation

ICS Semester 4 - Group G
Secure Solution Results

Nick Blom Jorn Kosterman Ryan Smith
Aleksandar Penev Mihai Glodici

June 17, 2023

Contents

1 Introduction

This document describes the results and implementation details of the project Secure Solution executed in CS4, as defined by our project plan. In the project plan, a problem around using RDP securely was defined. A machine connected to from the outside through RDP, that was used to operate/manage physical machinery, got comprised and via this infected machine the whole network got infiltrated and compromised. To understand how this can be prevented or mitigated, a secure network design was realized to be simulated and implemented on netlab. For this, various principles of network security should have been of relevance. These topics of relevance are introduced in the Scope section.

In regards to the described breach in the project plan, it was not difficult to make this network more secure than the original network the client used. Once a client was connected to the RDP accessible machine, they had full administrator rights, to enhance working capabilities from home. There was no further network security present, not even monitoring solutions. However, this does not mean we put in the least effort to enhance security. When using network security principles, such as VPN or a monitoring server, one needs to realize these need to be secured as well, should they be taken advantage of in a malicious way.

2 Scope

The pre-defined scope was mostly adhered to, though slightly expanded since the start of the implementation phase. The reason for this was already stated in the introduction, to further secure VPN, RDP, and monitoring servers. The following network security principles were applied in the implementation:

- Applying justified network segmentation,
- Controlling traffic between subnets with custom firewall rules,
- Applying a Network Intrusion Detection System on a choke point (router), specifically to monitor RDP traffic on the relevant subnet,
- Applying a Host Intrusion Detection System on the user/employee net to detect suspicious behaviour on workstations,
- Creating a Domain Controller with Active Directory to set up permission and password policies for the VPN accessible subnet,
- Creating a VPN subnet through which the machinery monitoring system can be accessed with RDP *only*.

3 Implementation

3.1 Network structure/segmentation

On netlab, on a shared account (PRO22), the implementation of the designed network was done. Originally, it was planned to have 3 subnets. These subnets were as follows:

- **WAN:** Mimics the outside world, the internet, though in this simulation it is just a subnet with static IPs for our class in CS4. From here, we attached a Windows 10 client to simulate an employee working from home.
- **VLANA (RDP monitor subnet):** Should hold the machinery monitoring system only, so that when something happens with this machine, it is isolated. An employee can connect with this system by first connected to the subnet through a virtual tunnel (VPN), and than RDP to connect to the machinery monitoring system specifically.
- **VLANB (User LAN):** Simulates the network where the employees work from. It should really only hold workstation for employees. Of course, employees and people in general can do stupid things with computers. That is why these workstations will be monitored part of our HIDS (Wazuh agents).

Additionally, we chose to add another subnet (**VLANC**), hosting the AD server for the Domain Controller and a server for the Wazuh Manager. The reason for this, is that these systems should not be discoverable and accessible on VLANB, which will be accessible through VPN. These systems hold important configurations to ensure the working of our HIDS and Domain Controller. By having these in their own subnet, they are harder to access for malicious users trying to infiltrate the network. A network diagram is provided on the next page.

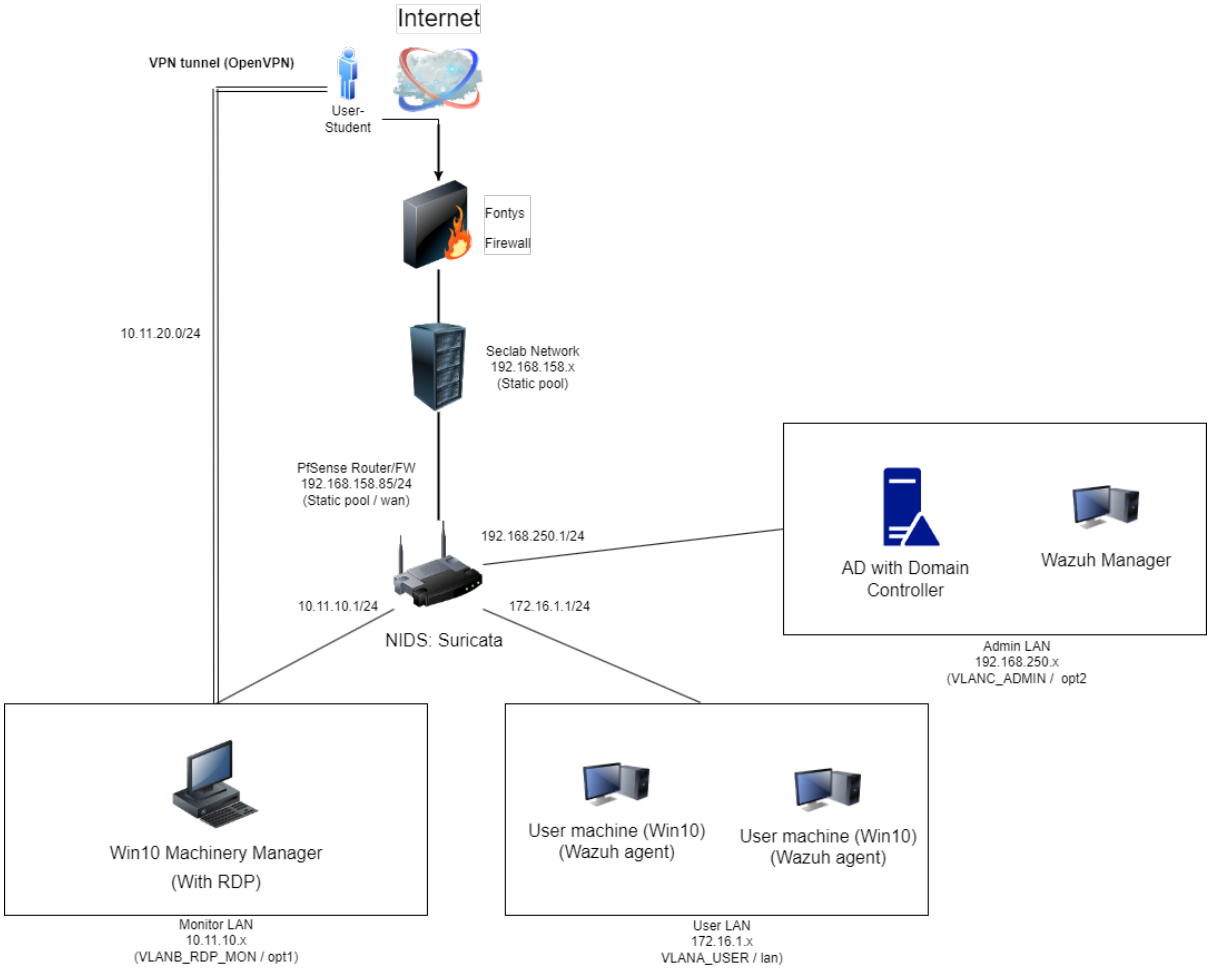

Figure 1: Network diagram with details

However, the AD server was still placed in **VLANB**. This poses a security risk, but we ran into issues with our strict firewall rules we want to adhere to. Placing the AD server in **VLANB** to directly enforce the domain controller there also eased the process of understanding and using the AD server, since some of us were new to this.

All internal subnets have a DHCP service available from the router, so that IPs are assigned dynamically. That is why they are not specified for specific machines in the network diagram.

3.2 Firewall rules

When it comes to the firewall configuration on the VLANs, the objective was to establish stringent rules aimed at minimizing potential attack vectors in the event that an intruder gains access to an internal machine or network. The focus was on enhancing overall network security.

To achieve this, dedicated rules were assigned to each VLAN to enforce access control and filter network traffic. The provided diagram illustrates the implemented rules, highlighting those that are forbidden and those that are permitted. This diagram representation serves as a guide to understand the restrictions and allowances imposed by the firewall configuration.

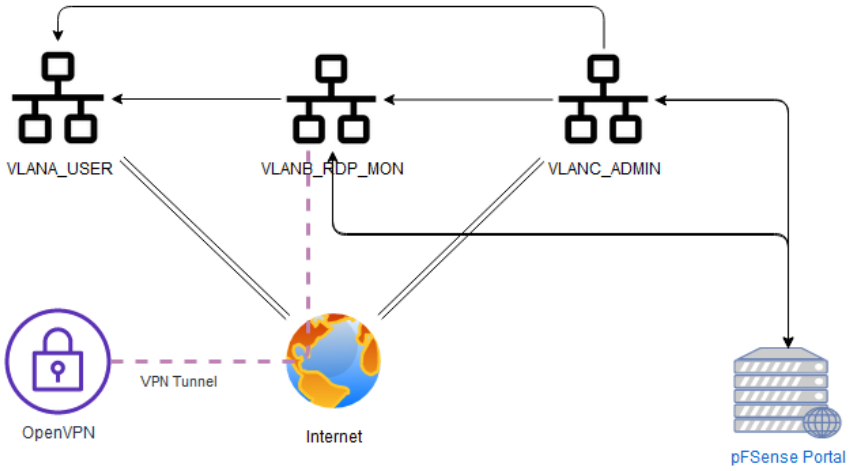

Figure 2: The arrow directions show which connections are possible.

- **VLANA (User LAN):** Considering the user LAN and the potential risks associated with employee workstations, we wanted to implement as stringent firewall rules here as possible. To ensure maximum security, the configuration restricts this VLAN from accessing any other VLAN or the pFSense Portal page. The only exceptions to these rules are the allowance for data transmission related to the RDP connection and the WAZUH manager.
- **VLANB (RDP monitor subnet):** To minimize the potential attack surface of this subnet, we decided to implement rules that allow it only to connect to VLAN A and the pFSense portal. Access to the internet has been disabled for this VLAN, with the exception of the VPN tunnel. This approach aims to restrict external access while maintaining secure communication within the designated VLAN and allowing secure remote connections via the VPN tunnel.

- **VLANC (Admin subnet):** Considering the specific functionalities that the ADMIN role must be able to perform, a decision was made to impose fewer restrictions on the VLAN assigned to this role. This VLAN is granted access to any other VLAN within the network, including the Portal page, as well as unrestricted internet access. This approach allows the ADMIN to configure and troubleshoot various VLANs, ensuring efficient management in case of any issues or complications.

3.3 NIDS

Following the principles of the network segmentation and the strict nature of the firewall rules we implemented. We decided to deploy a NIDS that monitors and logs network traffic and blocks potential threats. So we decided to implement Suricata, due to its advanced features and our previous experience with it during the cyber security semester.

For starters, we decided to use the Maximum Security modern SNORT rule set on VLANs A and B so we could monitor and log for the following:

- **Network traffic patterns:** The NIDS software would monitor network traffic patterns, looking for traffic that is abnormal or suspicious. Examples include: large amounts of traffic, traffic with unusual destinations, and traffic that violates network policies.
- **Protocol analysis:** NIDS software would monitor network protocols, looking for anomalies or unusual behavior. For example, it might detect attempts to exploit vulnerabilities in a protocol or attempts to bypass security measures.
- **Known attack signatures:** NIDS software would be configured to detect specific attack signatures that are known to be associated with certain types of attacks. For example, it might detect a specific pattern of network traffic that is associated with DDOS.

But having the most popular SNORT rule sets only, would not be enough to keep a log and monitor Remote Desktop Protocol traffic and login attempts. That is why we implemented the following rules (see net page):

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 3389 (msg:"Suspicious RDP Connection Attempt";
flow:to_server,established; content:"|03 00 00|"; depth:3; offset:5;
content:"|e0 00 00 00 00 00|"; distance:2; within:6;
threshold: type limit, track by_src, count 1, seconds 60;
classtype:attempted-admin; sid:1000001; rev:1;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 3389 (msg:"RDP Failed Login Attempt";
flow:to_server,established; content:"|03 00 00|"; depth:3; offset:5;
content:"|2e 00 00 00|"; distance:2; within:4;
threshold: type limit, track by_src, count 1, seconds 60;
classtype:attempted-admin; sid:1000002; rev:1;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 3389 (msg:"RDP Successful Login";
flow:to_server,established; content:"|03 00 00|"; depth:3; offset:5;
content:"|fb 00 00 00|"; distance:2; within:4;
classtype:successful-admin; sid:1000003; rev:1;)

alert tcp $HOME_NET 3389 -> $EXTERNAL_NET any (msg:"RDP Login Attempt from Internal Host";
flow:to_server,established; content:"|03 00 00|"; depth:3; offset:5;
content:"|00 00 00 00 00 00|"; distance:2; within:6;
threshold: type limit, track by_src, count 1, seconds 60;
classtype:attempted-admin; sid:1000004; rev:1;)
```

The custom rules implemented are meant to keep a log of all of the RDP traffic and alert on specific occasions. Here's what the custom rules do respectively:

- Suspicious RDP Connection Attempt: This rule alerts when an IP outside of the network tries to connect to a Desktop in VLANB.
- Failed RDP Login Attempt: This will alert when someone attempts to login multiple times with no success.
- Successful Login: The aim of this alert is to log the IP of every computer that established connection via RDP.
- RDP Login Attempt from an Internal Host: The aim of this rule is to log every login Attempt from inside the network.

Conclusion: By implementing these custom rules, we have ensured thorough monitoring and logging of RDP traffic, allowing us to stay aware and respond effectively to any potential security incidents. Our proactive approach to network security, complemented by the NIDS and custom rules, strengthens our overall security and enables us to better protect and react to events happening in our network and therefore protect access from outside threats.

3.4 HIDS

3.4.1 Introduction

The objective of this task was to implement the Wazuh Host Intrusion Detection System (HIDS) on an Ubuntu machine tasked with monitoring two employee machines. The value proposition of implementing an HIDS is that it provides a robust mechanism for detecting and reporting potential security incidents. It does this by analyzing system behavior and configuration status, thereby enhancing the organization's security posture by providing visibility into internal network activities.

3.4.2 Network Configuration

The network was configured such that the Ubuntu machine (dubbed 'C_ADMIN_Wazuh') was in Subnet C, and the two monitored machines, 'A_USER_Employee_Machine' and 'A_WindowsWorkstation', were positioned in Subnet A.

3.4.3 Wazuh Installation and Configuration

The Wazuh server was successfully installed on the 'C_ADMIN_Wazuh' machine. This includes the Wazuh manager and API. A key part of this process was configuring the firewall on the Ubuntu machine to allow traffic on port 1514, where the Wazuh manager listens for incoming connections. Subsequently, the Wazuh agent was installed on both employee machines, with care taken to choose the correct agent based on the operating system of the respective employee machines. To complete the setup, these agents were registered with the Wazuh manager using the 'manage_agents' utility.

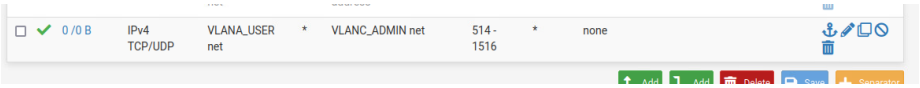

Figure 3: Firewall rule necessary for communication between Agents and the Manager

3.4.4 Wazuh Agent Configuration

Specific files, logs, and processes that are deemed critical to the organization's security were selected for monitoring on 'A_USER_Employee_Machine' and 'A_WindowsWorkstation' machines. This was accomplished by modifying the ossec.conf file, located at /var/ossec/etc/ossec.conf, on each machine.

3.4.5 Data Analysis and Visualization

The Wazuh web interface provided an interactive platform for visualizing and analyzing the data collected by the Wazuh agents. Screenshots of the Wazuh

dashboard displayed the analysis of the data, revealing patterns and potential security incidents.

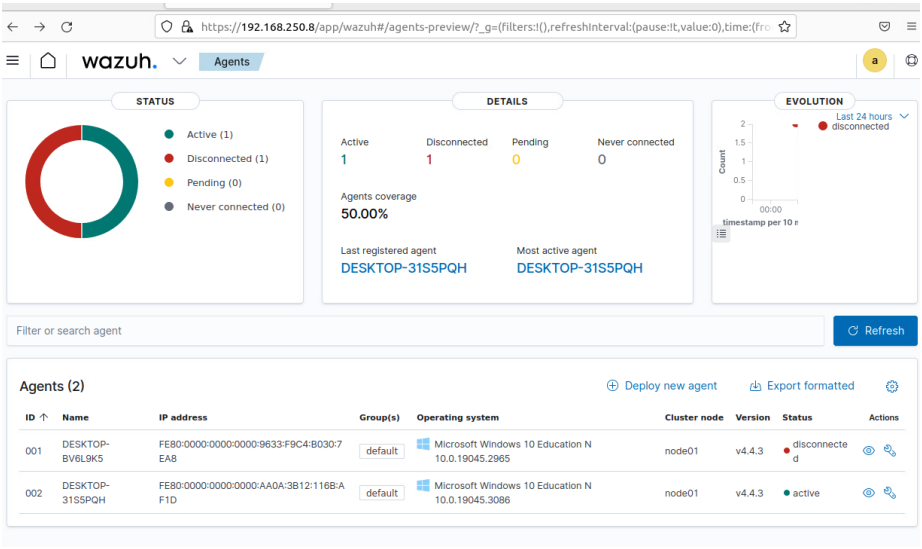

Figure 4: Wazuh Manager dashboard accessed from VLANA

3.4.6 Testing and Validation

The implementation was tested by simulating various events and verifying if they were detected and reported correctly in the dashboard. The tests confirmed that the system was functioning as expected, with all alerts being correctly generated and visualized.

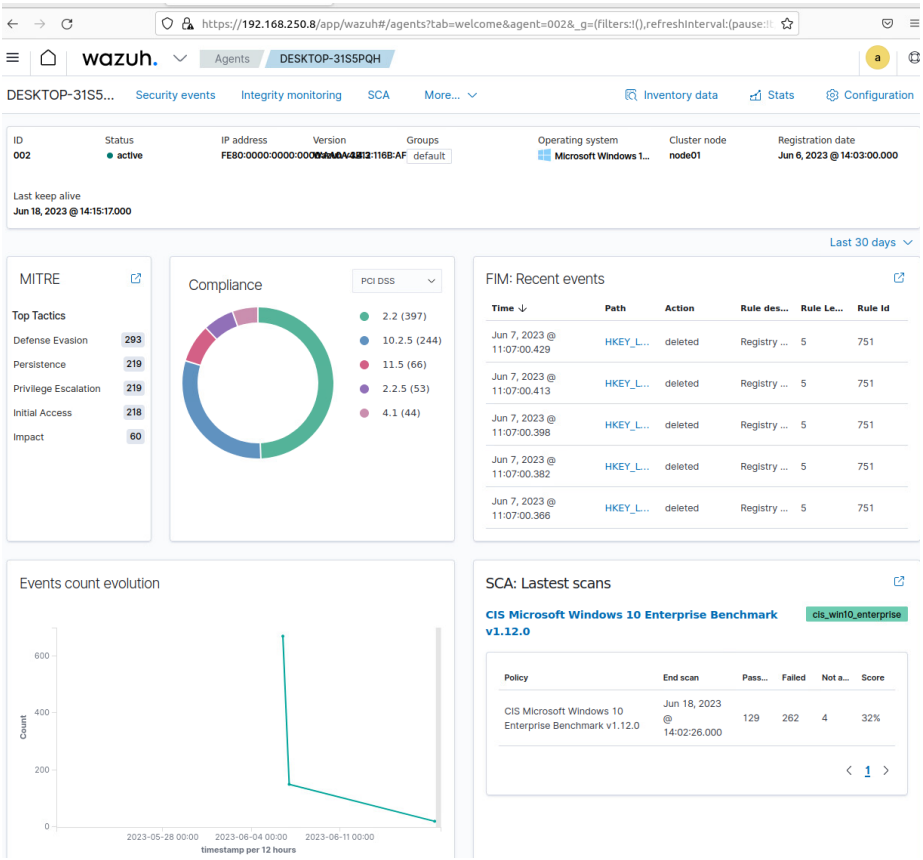

Figure 5: Wazuh Manager monitoring one of the employee workstations in VLANA

3.4.7 Conclusion

The successful implementation of the Wazuh Host Intrusion Detection System on our hosts has significantly enhanced our visibility into system activities and improved our security posture. Despite the challenges faced during the implementation - notably, firewall configuration and agent registration - these were effectively managed and resolved. Finally, the implementation of Network Intrusion Detection Systems (NIDS) was integrated to complement our current HIDS, providing a more comprehensive network security framework.

3.5 AD/policies

The reason why our group decided to make an Active Directory (AD) was to control and limit the employees rights for the RDP target computer, which controls most heavy machinery in the workplace.

This got done by firstly installing a new copy of Windows server 2022 on the dedicated AD machine. After installation, the Active Directory got selected in the windows server manager. At this point the domain name got made 'securesolution.com'.

After the domain controller was created, we had to make a policy that limited access for employees connecting through RDP. We started by creating a user for employees to use and then we began on the policies. We created a new security group for restricted RDP access and added the employee user to it, and then we made a group policy object in the domain and named it "RDP Access Restriction". We added the security group we created to the "allow log on through Remote Desktop Services" under the user rights assignment section. We then configured restricted RDP access to specific machines by adding the restricted RDP group to the restricted groups section, and then applied the group policy to the domain by linking it to our domain.

3.6 RDP via VPN

The reason why we setup a VPN, is to use it together with RDP, for a secure tunnel connection for outside employees into the network. The tunnel ensures that all RDP traffic is encrypted and secured. RDP is a remote access protocol developed by Microsoft. RDP is typically used for remote administration and accessing virtual desktops, as is the case for our simulation. RDP needs to be enabled on the machine that will be accessed via RDP, which is not the case by default. What needs to be considered as well is that RDP traffic should be allowed through the firewall rules. After enabling RDP on the machinery monitoring system, the VPN got setup. This is done using OpenVPN on the PfSense router. Firstly, the OpenVPN server got configured on PfSense, which is available as a package. In this setup, an VPN server certificate was made, and the VPN was set to the 10.11.20.0/24 subnet.

Next a user could be made in the User Manager in Pfsense. This was VPNemployee. While creating this user, it also got an own user certificate.

Now it was time to install the OpenVPN client export plugin on Pfsense. This was easy, as it was downloadable from the package manager in Pfsense. After installing this, a VPN config file could be extracted from the Pfsense router.

Now on a client machine, the Pfsense client could be installed. After installation the config file from the OpenVPN server could be added, whereafter could be logged in with the use of the aforementioned created user. This resulted in a working connection.

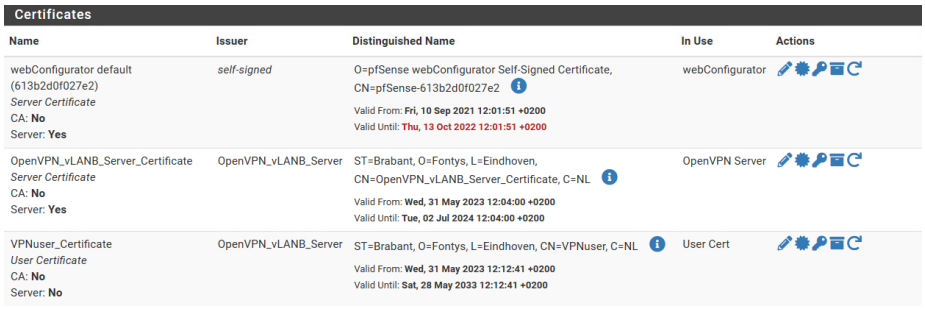

Figure 6: VPN certificates on pfSense router (self-signed)

4 Security Incident Response

In the event of a similar future attack of this degree happening, as described by the project plan, a comprehensive security incident response is vital. This security response outlines the steps that should be taken if this attack happens again in order to reduce the impact and stop the spread of malicious software as fast as possible.

4.1 Alert Reception

The IT team responsible for incident response receive an alert from the IDS/NIDS systems alerting them to a potentially severe security incident involving a compromised network and encrypted systems. The alert contains details that indicate it was caused by an employee that used RDP to connect to the remote server during their off hours at home. The response team documents the alert and details that come with it, such as the source, time of receipt, and initial information provided. The affected employee and IT team are also interviewed to get as much information as they can about the incidents scope and impact.

4.2 Triage

- Categorisation: The incident is categorised as a targeted ransomware attack that is a result of unauthorised access via compromised RDP credentials. Since the severity and impact are quite high, this incident is considered high-priority due to the compromised data, financial impact and the possibility of further attacks, all of which are of immediate concern. This greatly disrupts the working capabilities and employees, with the possibility of affecting external users should other systems get compromised.

- Prioritisation: The response team responsible for this incident prioritise their response efforts based on the criticality of any compromised systems, the importance of their encrypted data, and the possibility of backdoors or residual threats left by an attacker. Immediate effort is put towards containing the incident in order to prevent further damage as well as minimising the potential for any future attacks.

- Assignment: A team of specialised personnel are assigned to handle all the different aspects of the incident response such as the technical response, management response, and legal response. A leader of the incident response effort is assigned to monitor and coordinate the response teams and their activities. This leader must ensure effective communication and collaboration across all of the response teams.

4.3 Response

Technical Response:

- The initially compromised home PC is isolated from the network in an attempt to prevent further spread to other systems.
- All servers accessed remotely by RDP will be thoroughly analysed in an attempt to find any vulnerabilities that were exploited by the attacker, such as weak configurations or software left unpatched.
- Forensic experts conduct a thorough investigation of the employee's home PC in order to identify the cause and origin of the keylogger used, assess the potential data exfiltration, and determine the attack vector.
- A thorough remediation plan is created to remove the keylogger or any other malware in order to restore system integrity and guarantee the confidentiality and availability of data.
- There is a network wide scan of all systems to find any malware infection or indicators of compromise, with the focus being on systems that have gone critical.
- Careful restoration is carried out on the backup data in order to recover encrypted systems and guarantee the integrity and accuracy of the information stored in the backup.

Management Response:

- A communication guide is put in place to keep all management, employees, stakeholders, customers, and external parties informed about the status of the incident and the impact of it.
- The incident response team works with all of the relevant departments such as IT, HR, and finance to keep operational disruptions to a minimum while the incident is ongoing.
- Senior management is given regular updates that focus on the progress of the response effort, status of the restoration process, and addressing any concerns that upper management may have.

Legal Response:

- A legal council is formed to assess any legal ramifications that may arise due to the incident, such as contractual obligations, data protection laws, and any mandatory notifications to clients.
- The forensic evidence from earlier analysis is collected and stored in case it is needed to support possible legal proceedings, such as a criminal investigation or possible litigation.

- The incident response team works in collaboration with the legal council to evaluate the ransom payment, any involvement from law enforcement, and any legal actions against the attackers if they are caught.

4.4 Review

During the review stages, further actions are to be considered and review of the incident response takes place. Once the incident is contained, systems are restored, and operations are stabilised, an in-depth post-incident review is conducted. The incident response teams analysis the root causes of the incident and look for any weaknesses in the security controls or policies and advises new measures to protect against these attacks in future.

5 Conclusion

In this section, we would like to discuss the outcome of an event that would test the resilience of our secure solution and the secure solutions of other groups in our class, but this event did not occur. It is therefore hard to argue whether our secure solution is really safe, since it has not been properly tested, as was originally the plan from the setup of CS4. Alternatively, as suggested by Canvas, the solution was thoroughly tested to show the alerting from the HIDS and NIDS, ensure RDP works only over VPN, VPN connected users are restricted in VLANB by the domain controller, and that the flow of traffic is as expected by the defined firewall rules. Of course, it would be even more interesting to push this design to some production form, where our design would be actually physically tested, as right now all systems are virtual machines on netlab. Best practice is to have an external part test your network simulation by the means of a pentest, for example. Though, our solution does not have any servers facing publicly to the WAN side, which makes it already very hard to break in.

Overall, we were successful in implementing the secure solution as imagined and designed. We tested its main functionalities and features, although more rigorous testing by a third party would have been preferred, such as during a blue team red team event with our class. It was a bumpy road, as a lot had to be learned, but you only really succeed with trial and error, which was definitely the case in this project.

Appendix A: Assignments

This table does not depict exclusivity to one's topic per se, but does indicate one's main involvement per defined Secure Solution topic. A lot of things, like network setup (segmentation) and firewall configuration were mostly done collaboratively with all group members.

Topic	**Implementation**	**Documentation**
Network segmentation	Nick Blom	Nick Blom
Firewall configuration	Aleksander Penev	Aleksander Penev
NIDS	Aleksander Penev, Nick Blom	Aleksander Penev
HIDS	Mihai Glodici	Mihai Glodici
AD and Domain Controller	Ryan Smith, Jorn Kosterman	Jorn Kosterman
OpenVPN configuration	Jorn Kosterman	Jorn Kosterman
Security Incident Response	-	Ryan Smith
Scope definition	All	Nick Blom