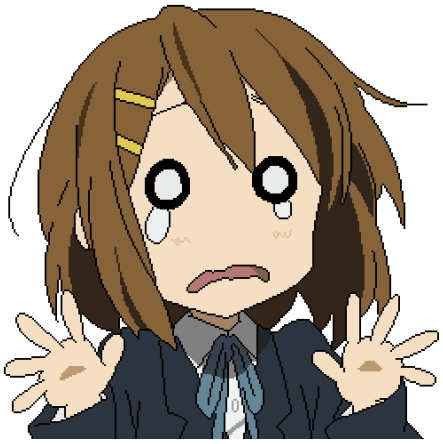
INCS 4810

Culminating Project

Project Proposal

Effects of Ransomware on an Industrial Organization



Students:
Gian Gravela
Scott Zheng
Kevin Chou

Instructor:
Victor Mendez

Tables of Content

Introduction

Overview

In the modern era, cybersecurity has become crucial for organizations and individuals. This is due to society's dependency on various industrial control systems that help our world function. These include the workstations in business operations to the PLCs in plant operations. Therefore, we must implement security in these systems to allow continuous operation in our world. Our project consists of detailing the effects of ransomware on an industrial organization, specifically using the WannaCry malware.

This project represents the culmination of our two years of study in INCS. This project will be completed for INCS 4810 as a showcase of our skills. In this project, we will show off skills that we have gained from classes such as advanced networking and ethical hacking. This project will consist of three main parts:

- Creation of Network
- Vulnerability Testing and Scanning
- Security Implementation

We will be creating a vulnerable network to test, and scan for vulnerabilities, then implement security in the network.

The following project proposal consist of the following sections:

- Introduction
- Project Overview
- Schedule
- Team Coordination

Background Information

The WannaCry ransomware attack was a major security incident that occurred in May 2017. The attack was able to effect over 200,000 computers in over 150 countries, attacking organizations such as hospitals, businesses, plants and various other businesses. The reason WannaCry was observed on a large scale was due to it being a ransomware worm. This enabled it to spread itself rapidly across computer networks using the EternalBlue exploit. WannaCry would encrypt the infected hosts files, leaving the computer inoperable. The majority of organizations had to shut down operations due to their files being encrypted. The organizations that shut down all had one thing in common: they all used legacy systems. One example of this is the Colonial Pipeline, which had to shut down operations due to its business operations network getting infected. Industrial organizations that potentially would pay the ransom to decrypt their files were highly favored targets. Highly targeted organizations often find it challenging to suspend their operations due to the expenses in doing so. Thus, these organizations would pay the ransom to continue their operations. Colonial Pipeline paid an estimate of 5 million USD to the threat actors for the decryption key.

Main elements

Our project will be based on an oil refinery plant, as this particular plant has numerous experiences of ransomware attacks. We will be designing and building virtual test network vulnerabilities using VMware. On this virtual test network, we will be launching a ransomware attack using the WannaCry malware to detail the effects. Upon completion of penetration-testing and vulnerability assessment, we will be designing and building a new virtual test network with security implementations.

Benefits

By conducting this project, we wish to outline the effects of ransomware on an industrial organization. Industrial organizations face operational constraints that prevent system updates without disrupting ongoing processes. Therefore, security measures that don't impede routine operations are necessary. The outcome benefits will include:

- Cost savings
- Maintaining business continuity
- Preventing cyberattacks
- Protection of data

Project Overview

Scope

Industrial organizations are more susceptible to cyberattacks due to a variety of factors. One factor that stands out is the use of legacy systems. Industrial organizations continue to use legacy systems because they're heavily integrated with existing systems. This causes problems as systems may not be supported by the vendor and may have known vulnerabilities that can be exploited. Furthermore, these legacy systems are integrated with existing systems, which further complicates the replacement due to upgrades being time-consuming. Upgrading legacy systems will halt current business operations, which may not always feasible for the business. In our project, we plan to do this. We will be simulating a ransomware attack on our oil refinery plant using the WannaCry malware. Throughout the duration of this project, we have two objectives:

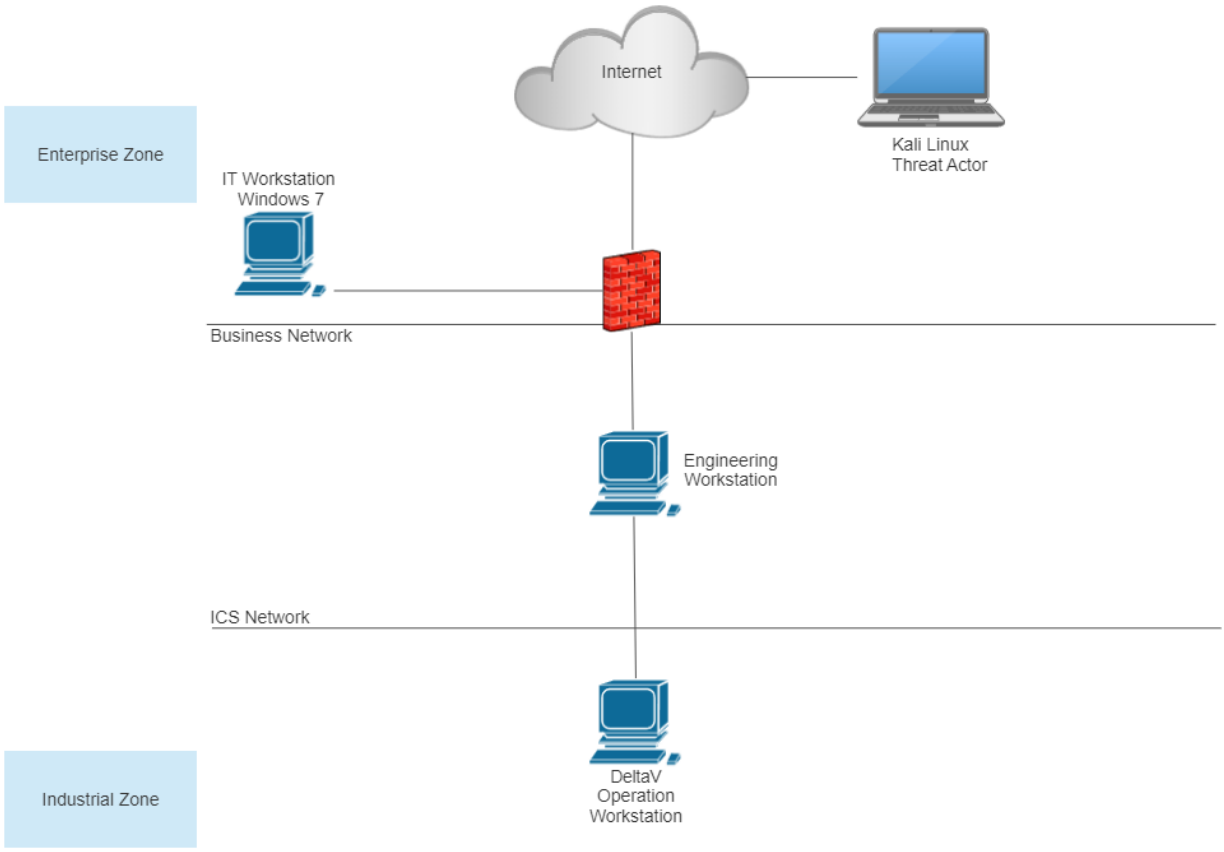
- Detail the effects of ransomware on an industrial organization
- Implement security that does not halt operations

Virtual Test Network

In this project, we will design and build a virtual test network with vulnerabilities in place, for penetration-testing purposes and vulnerability assessment. The first virtual test network will be called V1 and will include the following networks and devices:

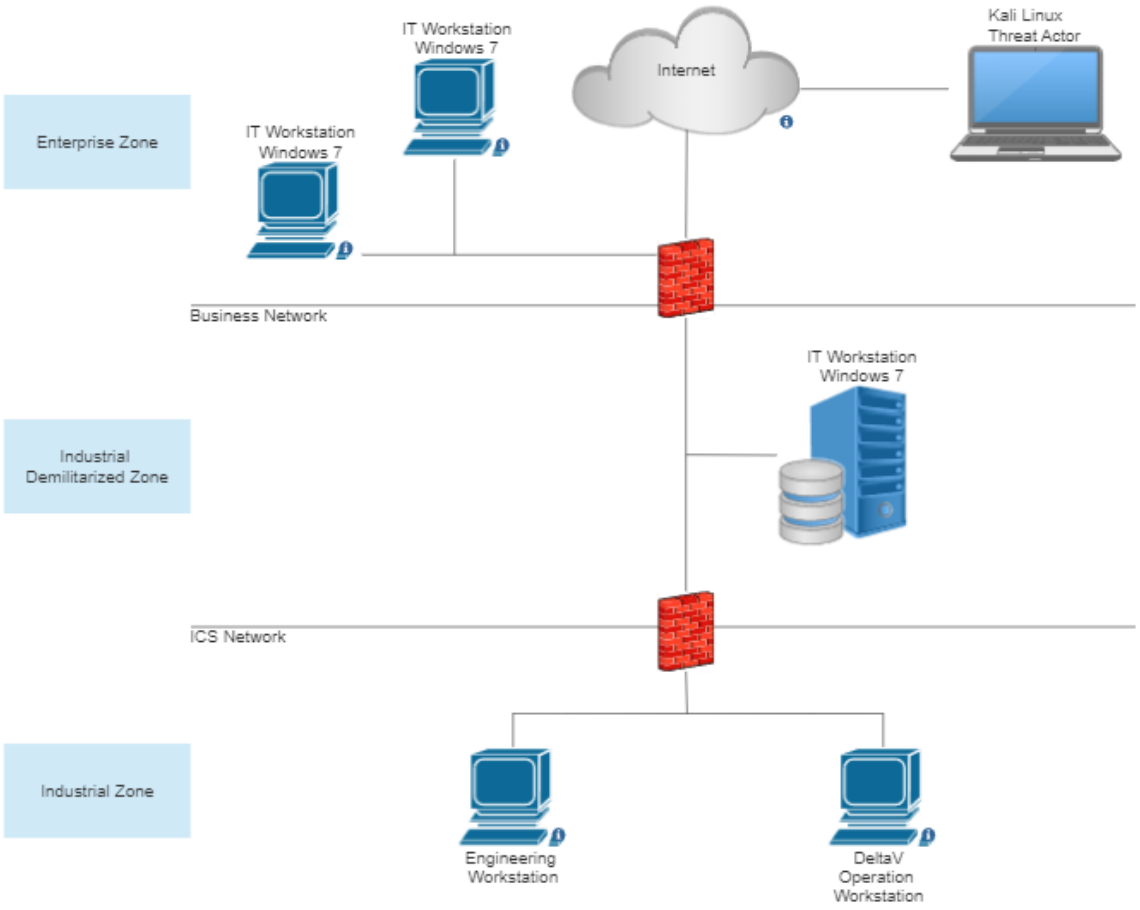
- Public Network
- Business Operations Network
- Plant Operations Network

- Kali Linux VM - Represents the threat actor
- Sophos XG Firewall - Separating outside network and inside network
- Windows 7 VM - Represents an IT workstation is the business operations network
- Windows 7 VM - Represents an engineering workstation
- DeltaV Operator Workstation VM - Represents a device working in the ICS network



Upon completion of penetration-testing and vulnerability assessment of V1, we will be designing and building another virtual test network called V2 that includes security implementations. The improved virtual test network will consist of the following networks and devices:

- Public Network
- Business Operations Network
- Plant Operations Network
- IDMZ
- 2x Sophos XG Firewall - Separating the business operations network from the ICS network.
- Windows Server - Represents a server in the IDMZ
- Kali Linux VM - Represents the threat actor
- 2x Windows 7 VM - Represents an IT workstation in the business operations network
- 1x Windows 7 VM - Represents an engineering workstation
- DeltaV Operator Workstation - Representing a device working in the ICS network



The listed devices may be subject to change as the project progresses. Potential devices that may be used in the future:

- Pfsense firewall

Potential Vulnerabilities

As instructed, our virtual test network was designed with vulnerabilities. One of these vulnerabilities lies within the VM's running on Windows 7. Windows 7 has a vulnerability in its SMB protocol that allows remote code execution. The vulnerability is named MS17-010 and allows a threat actor to remotely execute code over the internet by exploiting it. Upon exploiting the vulnerability, the threat actor is able to gain access and control over the host. The threat actor is able to access data, install malware or try to attempt lateral escalation. In our project, we will be using the EternalBlue exploit on MS17-010. Upon exploitation, we plan to install the WannaCry malware and attempt lateral escalation. Lateral escalation will be accomplished by the malware. WannaCry uses the EternalBlue exploit to spread itself across the network, which also makes it a malware worm. The malware is able to propagate by scanning for hosts that have port 445 (SMB) open, and infect them using this port.

Vulnerabilities can also be observed in our firewall. Although we are using a next-gen firewall, we will not be following best practices when configuring it. This is to allow the exploit and malware to enter the virtual test network. Furthermore, as we won't be following best practices, we will not be defining proper rules for communication between networks. In a secure network, communication between the ICS network and business operations network should not happen. Certain criteria must be met for communication to occur, such as authentication of a user, but we will not be defining this in our firewall for now.

We will not be hardening our devices, which is another glaring vulnerability. This means we will not be disabling unnecessary services and ports, installing up-to-date patches and installing endpoint protection. Device hardening is a crucial part of securing a network, as a threat actor's main goal is to gain access to a device. Simple device hardening can stop threat actors and malware from entering the network. Having a host-based IDS/IPS can harden devices greatly, as they're able to detect and mitigate threat actors and malware almost immediately.

Security Implementations Draft

Our virtual test network with security implementations will be based on the Purdue model. In accordance with the Purdue model, we plan to add an IDMZ to our virtual test network. This is to isolate network traffic, as the ICS network and business operations network shouldn't be able to communicate directly. The IDMZ will also serve the purpose of an additional layer of security. As the server placed in the IDMZ is not directly connected to both networks, the server cannot be used as a point of entry. In all, the IDMZ will be used so that availability of plant operations won't be compromised.

Two Sophos next-gen firewalls will be used in our virtual test network. The sandbox feature in particular will be valuable to the security of the network. If a file enters the network that doesn't match a signature or hash, the file will then be placed in the sandbox. The file is then opened in the sandbox to analyze the characteristics and behaviour of the file. This will be useful for any disguised malicious traffic entering the network. Furthermore, the firewall has deep packet inspection. The deep packet inspection feature will come in handy if our network is faced with any zero-day attacks. This also allows protection from any sophisticated attacks. The firewalls will also be used to define access-control rules. These access-control rules will define communication between different zones and networks. For example, we don't want our users accessing any sketchy sites, so we would block the domains or IP addresses.

Our primary concern of the project is implementing security that doesn't halt the operations of industrial organizations. Therefore, when making decisions on security implementations, it is important to consider solutions that do not require system replacement. Hence, some type of endpoint protection may be used. The endpoint protection will be used to detect and mitigate any malware that comes into contact with the device. If the device is infected with malware, the endpoint protection will isolate the device from the network. This will stop the propagation of the malware.

The listed security implementations are general and subject to change as the project progresses.

Schedule

The project will approximately take a month to complete. A Gantt chart will be used to ensure efficient use of time, track progress, set deadlines, and distribute the workload. The schedule consists of the proposal, creation of network, penetration testing and security implementation, presentation, and report. The final deliverables will contain a presentation, final report, and a virtual network with security implementations that can detect malware and isolate compromised devices.

Milestone

The first milestone will be the creation of our first virtual test network V1. It will include a Kali Linux VM, Sophos XG Firewall, Windows 7 VM IT Workstation, Windows 7 VM Engineering Workstation, and a DeltaV Operator Workstation VM. To achieve our first milestone, the virtual test network will need to have connectivity between all VMs and the ransomware attack must be functioning correctly. To ensure we accomplish this milestone, we will break down the creations of each VM, thus making the task seems more feasible. We will stay organized and follow the deadlines set in the Gantt Chart, and take breaks when necessary. This milestone will begin from April 26 and will be completed by May 5.

The second milestone will be our second virtual test network V2 with security implementations. It consists of an IDMZ, 2x Sophos XG Firewall, Windows Server, Kali Linux VM, 2x Windows 7 VM IT Workstation, 1x Windows 7 VM Engineering Workstation, and DeltaV Operator Workstation. For the milestone to be completed, the virtual test network needs to connect to all other VMs and have the new security implementations. The new security implementations will be able to detect malware and prevent propagation of malware by isolating compromised devices. We will break down the creation of each VM again and ensure connectivity between all VMs. Additionally, we need to confirm that our Sophos XG Firewall is permitting and prohibiting the right traffic in our networks. If we stay diligent and follow our schedule, we will begin this milestone on May 5 and hope to complete it by May 11.

Proposal

The proposal will entail 4 main sections: Introduction, Project Overview, Completion Schedule and Team Coordination. The project overview will discuss the problem statement, project scope, limitations, specifications, and a draft proposed solution. The project schedule will include a Gantt chart and a work breakdown structure. The team coordination section will explain individual member's strengths, project responsibilities, project management, and communication. The proposal is to be started on April 26, 2023 and completed by May 2, 2023.

Creation of Network

The creation of the network will be the initial part of the project. We will design a network called V1 that has vulnerabilities in the system. After, we will build the virtual network on VMware and do penetration testing and vulnerability assessment. Additionally, we will create a second virtual network called V2 that has security implementations that will detect and prevent malware from spreading. The creation of the network will start from April 26, 2023 and end on May 11, 2023.

Vulnerability Testing and Scanning

The second step of our project is to scan and test for vulnerabilities. We will identify the target of system that we would like to scan by determining their IP address or hostname. Next, we will choose a vulnerability scanner and configure it to scan the target. Lastly, we will run the scan, analyze the results, and remediate the vulnerabilities. Vulnerability testing and scanning will start on May 3, 2023 to May 5, 2023.

Security Implementation

Security implementation will be the last part where we install an IDMZ, two Sophos next-gen firewall and endpoint protection in our V2 virtual test network. The installation of these components should not halt production of industrial processes. Additional security implementations will be added as the project progresses. This will start from May 5, 2023 to May 11, 2023.

Final Deliverables (Presentation + Report)

Once the project is completed, a PowerPoint will be created to support our presentation. We will use charts, graphs, and images to support our ideas and findings. The making of this PowerPoint will be started on May 12, 2023 and will be completed by May 19, 2023. The presentation will be on May 24, 2023.

The report will include an introduction, project description, schedule, conclusions and recommendations, and references. Also, the report will contain the research we have done to create our two networks and will outline the steps needed to reproduce the same project. The project report will be started on May 12, 2023 and will be completed by May 25, 2023.

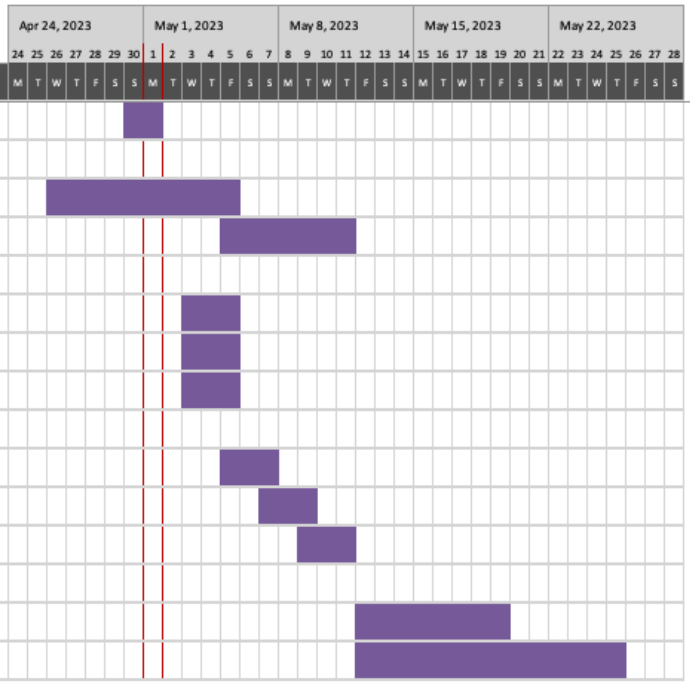
Gantt Chart

Effects of Ransomware on an Industrial Organization

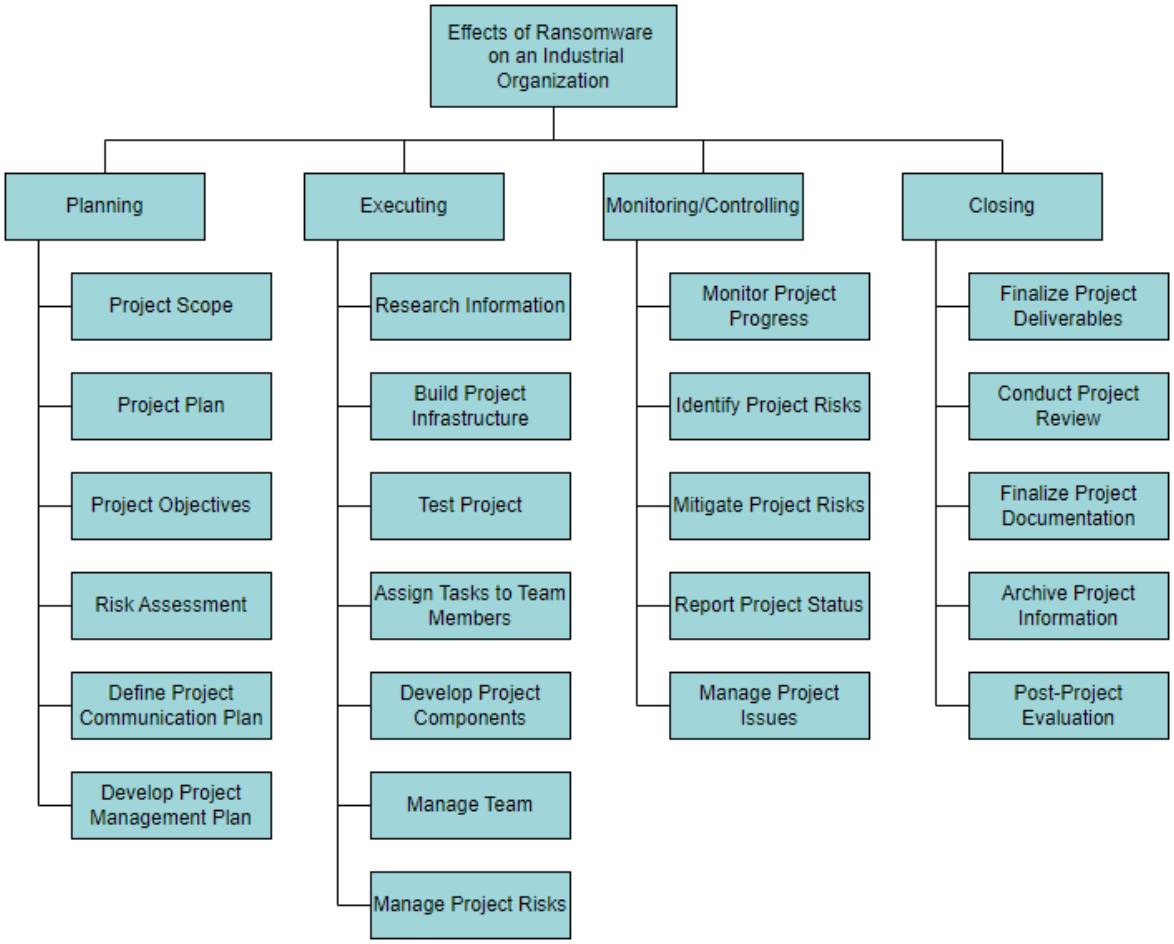
Gravela Network
Kevin Chou

Project Start: Wed, 4-26-2023
Display Week: 1

TASK	ASSIGNED TO	PROGRESS	START	END
WBS	Kevin	0%	4-30-23	5-1-23
Creation of Network				
Create Virtual Test Network V1	Scott	0%	4-26-23	5-5-23
Create Virtual Test Network V2	Kevin	0%	5-5-23	5-11-23
Vulnerability Testing and Scanning				
Identify target	Gian	0%	5-3-23	5-5-23
Choose vulnerability scanner	Kevin	0%	5-3-23	5-5-23
Remediate Vulnerabilities	Scott	0%	5-3-23	5-5-23
Security Implementation				
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	Kevin	0%	5-9-23	5-11-23
Final Deliverables				
Power Point Presentation	Gian	0%	5-12-23	5-19-23
Report	Scott	0%	5-12-23	5-25-23



WBS


Effects of Ransomware on an Industrial Organization
Planning
Executing
Monitoring/Controlling
Closing
Project Scope
Project Plan
Project Objectives
Risk Assessment
Define Project Communication Plan
Develop Project Management Plan
Research Information
Build Project Infrastructure
Test Project
Assign Tasks to Team Members
Develop Project Components
Manage Team
Manage Project Risks
Monitor Project Progress
Identify Project Risks
Mitigate Project Risks
Report Project Status
Manage Project Issues
Finalize Project Deliverables
Conduct Project Review
Finalize Project Documentation
Archive Project Information
Post-Project Evaluation

Team Coordination

Members' Strengths

In this project, we have three members that each bring their own strengths that will ensure the completion of the project.

Gian is a highly effective project manager who possesses several key strengths. His attention to detail allows him to account for every aspect of a project, minimizing the risk of potential issues. Gian also has strong communication skills, which enables him to effectively explain ideas and instructions to his team members. In addition, he possesses strong critical-thinking, which allows him to identify and select the most effective decision for any point of the project. Lastly, Gian is a results-oriented team player who is focused on achieving project objectives and delivering high-quality outcomes.

Scott is a valuable member of the team with a range of strengths that contribute to the success of our project. His strong organizational skills and ability to compile data allows him to structure documents and present data in an easily understandable format. Additionally, Scott's ability to collaborate effectively with others and his adaptability makes him valuable to any team. As a result, this ensures a conducive work environment where he can be assigned any task and work smoothly in a team setting.

Kevin is an essential member of the team with a range of valuable strengths. His technological knowledge makes him our go-to person for any technical issues and challenges. He is able to navigate through complex technical problems with ease, which makes him a valuable asset to the team. Kevin's greatest strength, however, is his drive to complete any task he sets his mind to. He is a persistent and determined individual who is able to overcome obstacles and reach his goals. This trait is invaluable in any project, as it ensures that tasks are completed to the highest standard and that the project progresses efficiently.

Responsibilities

Each member in this project will be given different responsibilities/duties that they will complete within a given deadline. The members in our group are the following: Gian, Scott, and Kevin.

Gian has been designated as the leader of our group. Thus, he is in charge of planning, setting deadlines, and ensuring the end product meets our stakeholders standards. Gian will also be given the responsibility to acquire software, specifically the Sophos XG Firewalls and the malicious ransomware software. In addition, Gian will support Scott in testing the Windows, Linux, DeltaV and Sophos XG Firewall Virtual Machines with the Sophos Firewall. Lastly, Gian will support Kevin and Scott in creating the project proposal and final report.

Scott's responsibilities will be to create the virtual machines, assist Gian in testing the firewalls, ensuring the ransomware attack is successful and document the results of the attack for our final report. Scott will also be in charge of creating and configuring the virtual machines. In addition, Scott will document the

instructions to recreate the attack and the outcomes of the ransomware software WannaCry being used against the virtual test network.

Kevin will be in charge of supporting Gian in the creation of a schedule for our project proposal. The schedule created will consist of a Gantt chart and a work breakdown structure (WBS) set by Gian's deadlines of the project. This schedule will ensure the WannaCry ransomware attack project is completed on time and to our stakeholders standards. In addition, Kevin will support Scott and Gian in the testing and documentation phase of the ransomware attack on the Windows and Linux Virtual Machines.

Challenges

While working on the complex project, we expect to face many difficulties. One of the challenges we expect to encounter is the time the project will require. We may have schedule conflicts between group members. Thus, it will delay our time to complete tasks together as a group. The major challenge we may experience is our equipment not functioning as we expect it to. If our virtual machine, firewalls, and ransomware attack are not operating as anticipated, we will need to find an alternate solution and the project completion may be delayed.

Possible Solutions

These challenges have multiple possible solutions. In order to minimize the possibility of scheduling conflicts among members, we will schedule our meetings two weeks in advance, allowing sufficient time to identify a suitable time for everyone to collaborate. Furthermore, we will assign tasks to each team member that can be completely independently without requiring assistance of other members. We will also create a Gantt chart to ensure all aspects of the project are complete and delivered on schedule. To address our main challenge of equipment malfunctioning, our team will utilize software and hardware that we are familiar with.

Tools

To accomplish the project successfully, a variety of tools will be utilized to aid in the completion of the project. Each tool will serve their own purpose such as communication, collaboration, and virtualization.

To communicate with each other, we plan to use Discord. Discord will provide us with various different methods of communication, for example text chat, screen sharing, voice call and video call. In addition, we will commentate to our stakeholders through email. Email allows us to send updates, questions, and attachments to our stakeholders that ensure the outcome of the project is sufficient.

For collaboration, our group will use Google Docs and Google Drive to work together on word documents and share files. Google Docs will allow us to all simultaneously work on a Word document in different locations. We will also be able to leave feedback in the way of comments and suggestions to each of the others designated parts to improve the report. To share large files across vast distances, Google Drive is an excellent choice. Google Drive enables us to upload large files to the cloud and access them using a shareable link from anywhere in the world with internet access.

Lastly, the most important tool is VMware. VMware will allow us to virtually emulate multiple devices with different operating systems on one host device. For example, two Windows PCs, three Linux Devices, Industrial Equipment and Next Gen Firewalls will be all virtually emulated on one device. VMware will allow us to test potentially malicious software in a secure and isolated environment without it causing permanent damage to our actual hardware/software. In addition, we will be able to create and test different network configurations between multiple virtual machines.

Bibliography

[1] "Ransomware attack leads to shutdown of major U.S. pipeline system," *The Washington Post*, 08-May-2021. [Online]. Available: https://www.washingtonpost.com/business/2021/05/08/cyber-attack-colonial-pipeline/. [Accessed: 01-May-2023].

[2] "Utility companies among those impacted by ransomware attack." [Online]. Available: https://www.tdworld.com/smart-utility/grid-security/article/20969707/utility-companies-among-those-impacted-by-ransomware-attack. [Accessed: 02-May-2023].

[3] "Why was the WannaCry attack such a big deal?," *YouTube*, 26-May-2017. [Online]. Available: https://www.youtube.com/watch?v=etPizFNPupk. [Accessed: 01-May-2023].

[4] "Trojan.ransom.wannacrypt (WANACRYPT0R 2.0/WannaCry, NHS ransomware)," *YouTube*, 14-May-2017. [Online]. Available: https://www.youtube.com/watch?v=Zy4G30kSPnY. [Accessed: 01-May-2023].

[5] "Wannacry Demo (propagation and killswitch)," *YouTube*, 25-Dec-2017. [Online]. Available: https://www.youtube.com/watch?v=Bc8o5jrL2_g. [Accessed: 01-May-2023].

[6] "How wannacry ransomware works," *YouTube*, 15-May-2017. [Online]. Available: https://www.youtube.com/watch?v=agFgibQydzg&t=56s. [Accessed: 01-May-2023].

[7] "Hacking windows with Kali (eternalblue)," *YouTube*, 27-May-2021. [Online]. Available: https://www.youtube.com/watch?v=AGYO2RmXQ10. [Accessed: 01-May-2023].

[8] "EternalBlue exploit against windows 7 (MS17-010)," *YouTube*, 05-Jul-2017. [Online]. Available: https://www.youtube.com/watch?v=_yOkfS21hbw. [Accessed: 01-May-2023].

[9] “Wannacry: The world's largest ransomware attack (documentary),” *YouTube*, 09-Jun-2021. [Online]. Available: https://www.youtube.com/watch?v=PKHH_gvJ_hA. [Accessed: 01-May-2023].

[10] “How wannacry ransomware works,” *YouTube*, 15-May-2017. [Online]. Available: https://www.youtube.com/watch?v=agFgibQydzg. [Accessed: 01-May-2023].

[11]“ICS Purdue model architecture. | download scientific diagram - Researchgate,” *researchgate.net*. [Online]. Available: https://www.researchgate.net/figure/ICS-Purdue-Model-architecture_fig1_349195440. [Accessed: 02-May-2023].