Internship On Cyber Security

BY

Partho Protim Halder

ID: 201-15-13776

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Computer Science and Engineering

Supervised by

MD. Sazzadur Ahamed
Assistant Professor
Department of Computer Science & Engineering
Daffodil International University

Co-Supervised by

Professor Dr. Md. Ismail Jabiullah
Professor
Department of Computer Science & Engineering
Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY

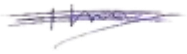
DHAKA, BANGLADESH

JANUARY 2023

APPROVAL

This Project/internship titled **"Internship on Cyber Security"**, submitted by **Partho Protim Halder**, ID No: 201-15-13776 to the Department of Computer Science and Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on January 19, 2023.

BOARD OF EXAMINERS



Chairman

Dr. Touhid Bhuiyan
Professor and Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner

Md. Sadekur Rahman
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner

Fahad Faisal
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

External Examiner

Dr. Mohammad Shorif Uddin
Professor
Department of Computer Science and Engineering
Jahangirnagar University

DECLARATION

We hereby declare that this internship has been done by us under the supervision of Mr. Md. Sazzadur Ahamed**, Assistant Professor, and Department of Computer Science & Engineering** at Daffodil International University. We also declare that neither this internship nor any part of this internship has been submitted elsewhere for the award of any degree or diploma.

Supervised by:

Md. Sazzadur Ahamed

Assistant Professor

Department of Computer Science & Engineering

Daffodil International University

Co-Supervised by:

Professor Dr. Md. Ismail Jabiullah

Professor

Department of Computer Science & Engineering

Daffodil International University

Submitted to:

Partho Protim Halder

ID: 201-15-13776

Department of Computer Science & Engineering

Daffodil International University

ACKNOWLEDGEMENT

First, I begin by expressing our sincere thankfulness to the Almighty God for His divine favor, which has enabled me to successfully finish the internship.

I'm very thankful and want to express my sincere gratitude to **Md. Sazzadur Ahamed, Assistant Professor, Department of CSE** Daffodil International University, Dhaka. Knowledge & Understanding of my supervisor in the sector of “Cyber Security” execute this Internship. His interminable patience, scholarly guidance, constant encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior drafts and correcting them at all stages, and reading many inferior drafts and correcting them at all steps have helped me finish this Internship.

We would like to convey our heartfelt thanks to Professor Dr. Touhid Bhuiyan, Head, Department of CSE, for his kind assist in fulfilling our intern's work, as well as to other academic colleagues and the staff of CSE department of Daffodil International University.

Thank you to all of our Daffodil International University classmates who participating in this forum while completing their course work.

Finally, we must humbly honor our parents constant support and patience.

ABSTRACT

Information security education is currently in great demand due to the ongoing dangers denial-of-service assaults, invasions, & breaches of internet-connected computer networks. Such instruction for future system and network managers, while also information security aficionados would be best provided in a lab setting at a recognized educational institution with world-class academics. It goes further than that. Education, research, and outreach are three ways where the educational institution may make a difference. The ability of students to do survey, receive a study, & share their expertise with the area via a mission of outreach using the baseline environment provided by this internship. To record the daily activities is a common thing nowadays. Even, we also need to record the milestone of the job list of that people who work in different institutions, it does not matter the company is small or big. Otherwise, it would be difficult to monitor the work properly or to get the expected outcome from the team members or staff. We hope that through this internship we can be benefited and improved. Especially for many companies in Bangladesh. Anyone can use this software personally. For this he will need to add the task himself and have to update the work in time. Another one of is multiple use. This is basically for the company or team. Where the team leader will be able to monitor the work of his team members. And, the chairman will be able to monitor every member. Even if he wants, he'll be likely to construct a new team also. Besides additionally, creating new group for the internship or determination of the leader, this kind of features will be available to the chairperson. And, the leader can monitor the members, he can assign tasks according to the priority or necessary and the members will be able to assign their own tasks and update it in time. By this way the work can be monitored personally and can be improved by proper monitoring. And, the company or team will be able to improve their work and easily monitor the condition of the works of all employees. This will reduce the work ethic and everyone will be focused on the work and will try to increase the progress of their work. Which will be beneficial for the company.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Introduction

The internship report which is being written here is called 'Cyber Security'. Information is widely available online, and company owners are both at risk of data stealing. Technological developments year after year, and cyberattacks after that. Cybercrime is a huge area that isn't linked to every single platform including an Internet connection. Yet computers, cellphones & all tablets have some sort of digital protection, but they also have "weak areas" that hacker have learned to exploit.

Thankfully, there are certain digital security solutions and services that work alongside their malicious tech rivals. Even while the complexity of our digital environment hides sophisticated dangers, most can use network-based attacks using digital catastrophe prevention technologies. As we do many works in every day, so if our target is written or if we work according to any schedule, then we will get more motivation and inspiration to do the works fast. And, when we will see our work is being recorded, we will be able to know which work we are doing on time and which we are not doing on time. It will help us to finish our work on time.

Besides, there are many small and big companies, also many business organizations in our country. Any company will be able to know the current working status individually of every employee by using the website. In this way, the staff will be focused on their work more. Even, the group leader will be able to share the tasks with his group members and keep an eye on everyone. Also, the employee of the day or month will be helpful for promotion and it will play a crucial role in this regard. Also, there are attendance systems. Employee gives attendance from dashboard. And CEO monitor time-in, time-out and total work time of an employee. Considering all these features, we are progressing in this internship. This total extension has been created in spite of the fact that they are Virtual Machine.

1.2 Motivation

We are inspired to complete this task internship from the hassle of managing tasks. Every company has many working departments or teams. They need to track their teams or department's progress and similarly, team leaders need to track the progress of every team member. Many companies face difficulties to complete this procedure and many times they could not find the accurate result. And in this pandemic situation, this makes it more difficult. So, the company needs a system to help their working producer.

Similarly, we face the problem of managing personal tasks, so that we think to make a personal and professional section. Also, attendance system, in online it's so difficult to monitor how many times an employee work. So, need a proper system to track work time.

1.3 Objective

Our primary objective is managing and monitoring activities, time tracking and team collaboration made simple. These are useful to individuals, teams, and organizations to assist them perform tasks efficiently and on time.

The main objective of cybersecurity is to keep data safe from theft or compromise. In order to do so, we consider three critical cybersecurity objectives.

1. Maintaining data confidentiality
2. Maintaining data integrity
3. Limiting data access to just authorized users

There are methods to keep these objectives in mind.

1. Sorting the assets based on to their priority & importance. The most major items are always kept safe.
2. Finding potential hazard.
3. Choosing the most of good security guard deployment technique for each hazard.
4. Monitoring any breaches and controlling both data in motion and at rest.
5. Iterative maintenance and problem management.
6. Adapting policies to tackle risk using previous assessments.

These are the primary goals that We want to fulfill.

1.4 Expected Outcome

We will get these results when we begin the internship

i. Secure and defend networks and computer systems from cyberattacks.

1. Describe the legal, ethical, and privacy aspects of information security.
2. Recognize vulnerabilities that are crucial to an organization's information assets.
3. Define the security measures necessary to ensure the networks and computer systems of a company operate with the needed levels of confidentiality, integrity, and availability.

ii. Analyze and look into cybersecurity incidents or crimes involving digital evidence and computer systems.

1. Recognize network and computer system assaults on an organization.
2. Make suggestions for solutions, such as the creation, adjustment, and implementation of incident response plans.
3. Use critical thinking and problem-solving abilities to identify current and upcoming assaults on the computer systems and networks of a business.

iii. Communicate well in a work environment to deal with information security risks.

1. Communicate suggested information security solutions to technical and non-technical decision-makers verbally and in writing.
2. In a context of information security, use business concepts to evaluate and interpret data for planning, decision-making, and problem-solving.

1.5 Report Layout

This is started in the format of the report, how this report format was created?
Basically, we worked on four chapters here and they are...

In “Chapter 1” **Introduction**:1
Chapter number one is mentioned the introduction, motivation, objectives, and expected outcome of the internship have been discussed which was followed by the report layout later.

In “Chapter 2” **Website Working Process**:
Chapter number two is mentioned, how to working a website?

In “Chapter 3” **The Methodology**:
Chapter number three is mentioned my overall implementation at the time of the Intern. Here is what We did to make this whole project.

In “Chapter 4” **Using Software, OS and Tools to attack:**
Chapter number four is mentioned, which software or tools using my Intern.

In “Chapter 5” **Hacker to do hack**:
Chapter number six is mentioned, hacking methodology of hacker and Hacking Process.

In “Chapter 6” **Malware Analysis**:
Chapter number five is mentioned the malware or various analysis.

In “Chapter 7” **Security Driven System Administrator on my work**:
Chapter number seven is mentioned the malware or various analysis of my work.

In “Chapter 8” **Overall Implementation and Testing in my office:**

Chapter number eight is mentioned the working process on Intern.

In “Chapter 9” **Conclusion and Prospects**:

Chapter number nine is mentioned the future work of Cyber Security and the conclusion of this project.

CHAPTER 2

FUNCTIONING OF THE WEBSITE

It's crucial to understand how websites function before starting to build your own website and publish it online. Here are some fundamental words:

Simply said, a website is a collection of web sites carrying codes that explain the style, structure & content per each page.

A request is sent by your browser to the server, an internet-connected computer, for a particular web page. Your machine and the server are linked through an IP address by the browser. The domain name is translated to produce the IP address. (Don't worry, your browser handles all of this automatically; You are not required to look up the IP addresses yourself.)

To put it another way, you will require the following in order for your website to be seen on the internet [3]:

1. Website
2. Domain Name
3. Server

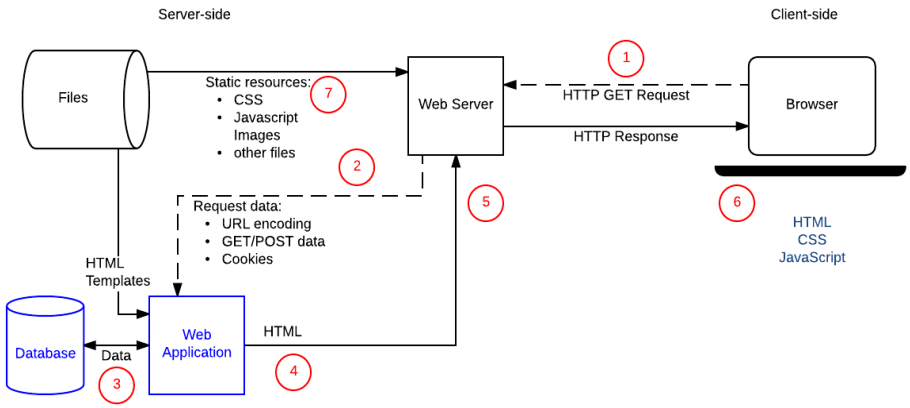


Figure 2.1: Functioning of the website

2.1 Website

Website is a frequently composed by a number of web pages, photos, and other components that are connected together to produce a single, bigger document. Consider a website to be a book, each page serves as a stand-in for a specific web page.

The number of pages on a website might range from one to hundreds. Each page's text, images, and other elements will be distinctive. Then, a folder comprising all of the web pages and components is produced and saved on your website hosting server.

Every website is made of codes that define how it should be organized, styled, and content-wise. The most used coding language for creating web pages is HTML [3].

2.2 Make Website

However, just because the website is programmed does not imply that you must be an IT geek to create one. Nowadays, to design website, you don't even need to know how to code or have any other technical talents or knowledge. The ability to create functioning, attractive websites without much or any technical skills has greatly increased thanks to technological advancements.

The top option is to utilize a website builder to develop your website if you have little to no technical expertise. Most website builders available are made with the non-technical user in mind:

- Everything is based online. Nothing has to be downloaded or installed. Simply launch your web browser, enter the website builder's URL, log in, and begin creating your website.
- No technological expertise is necessary. Since website designers are designed & maintained to experts, you are not need to tinker with the technological intricacies. You can build a fully functional website from scratch without writing a single line of code.

- It is visible. The WYSIWYG (What You See Is What You Get) editor used by website builders normally allows you to design your website by simply dragging and dropping website elements into the appropriate location.
- Templates that have been expertly created. Since the majority of website builders have a sizable library of expert design templates, you would not have to worry about clashing color palettes or an inconsistent layout.

2.3 Domain Name

The address you entered in the address bar of your web browser to access a website is called a domain name. The domain name https://bugsbd.com/ serves as an illustration. A domain name makes a website distinct. In other words, a domain name cannot be used by more than one website.

You do not need a personalized domain name for website, it's true. Some website owners provide free alternatives, such as a free domain name. However, free domain names are really sub-domains. For instance, your free website URL may be http://yourname.example.com if your website builder is "example.com".

There are several issues with this kind of site address:

- Because you don't own example.com or any of its subdomains or subfolder versions, your website is effectively taken "hostage." Any sub-domains and/or sub-folders may be created and/or deleted by the website builder at any time, with or without prior notice.
- Many clients will not do business with a firm that lacks a domain name of its own. You and your company may have the professionalism, integrity, and trust you need with a personalized web domain (custom domain email address).
- Domain names are given prominence by search engines like Google and Bing over Sub-Domains.

Although customized domain names really aren't free, but you may now get one when you sign up for an annual service plan from numerous service providers.

2.4 DNS

The Internet's phonebook is the DNS Server (DNS). People use domain names such as facebook.com or google.com to access information online. Public Ip (IP) addresses may be used to communicate across web browsers. DNS converts domain names into IP addresses, allowing browsers to access Internet resources.

Every Internet-connected device has a distinctive Ip that the other machines may use to locate the device. DNS servers minimize the need for people to learn sophisticated modern alphabetic IPv4 addresses like 192.168.1.1(in IPv6).

DNS resolution entails converting a hostname (for example, www.bugsbd.com) into such a Port number that computer can recognize (such as 192.168.1.1). Every World wide web computer does have an Internet address, which is used to identify the proper Internet device in the same way that somehow a physical address is used to distinguish a certain dwelling. A translation must occur between what a user types into their web page (domain name) as well as the machine-friendly address necessary to locate the example.com site when it is requested.

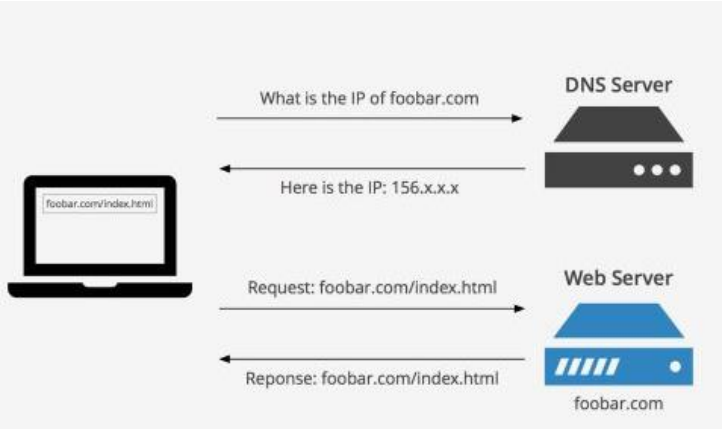


Figure 2.2: DNS Server

2.5 A Website Server

A web server is the computer that accepts a request to the web server from your browser. Imagine you are in charge of drafting the job post for a position that recently became available at your organization. Even if you create the most intriguing advertisement, nobody will see it unless you publish it on a job board.

The same is true for websites. Even if you design the most beautiful website, it won't be available or visible on the Internet unless it is uploaded to a web server.

Users can setup a server at leisure, but it will need a significant amount of experience, time, and resources (power and Internet connection). The most logical option would be to pay a web hosting provider, cost-effective, and useful course of action. Imagine it being similar to leasing space on a web host's server. You may utilize place at their server for your website to be hosted for a monthly price, and since it's their server, they handle all the technical parts of putting it up, maintaining it, and providing all particular resources required to run it for you so that you don't have to.

2.6 Everything Fits Together

If you open a web browser and enter a domain name, the web pages associated with that domain name will be shown in your browser.

However, have you ever questioned how your internet browser works determines what information should be shown?

Every domain name will be assigned to website., also known as a website address, and All domain name is connected to the Internet address of the remote server on which it is hosted. Domain Name Servers used to control & monitor IP addresses (or DNS for short).

You could set up a network at home, but this will necessitate a lot of knowledge, time, and resources to do it (Specifically, electricity and an Internet connection). Having to pay for web hosting company could be the most logical, cost-effective, and useful course of action. Imagine it being similar to leasing space on a web host's server. You may use their server

space to host your webpage for a monthly price, and since it's their server, they handle all the technical parts of putting it up, maintaining it, and providing all available resources necessary to make it work, necessary to make it work.

2.7 Anatomy of a URL

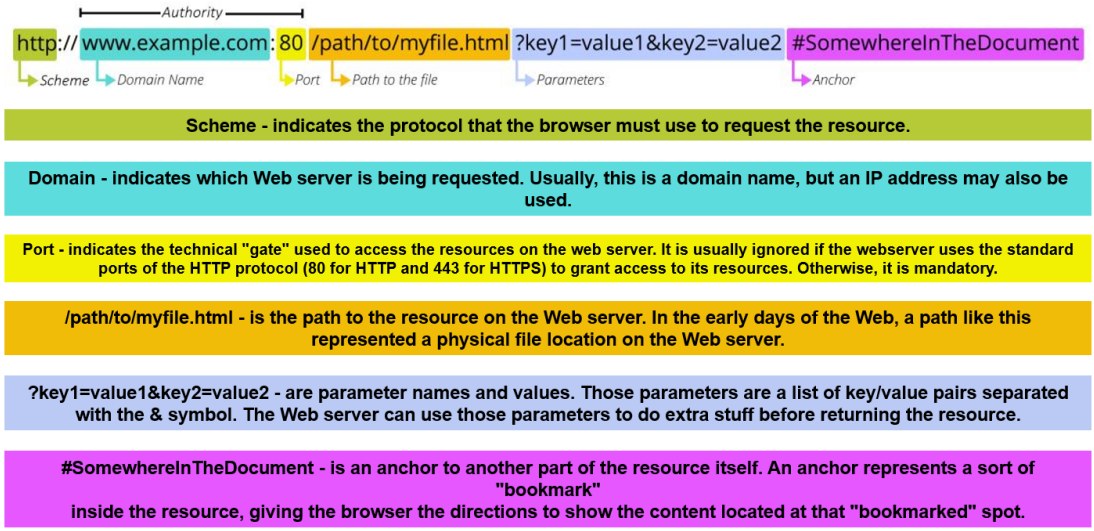


Figure 2.3: Anatomy of a URL

2.8 HTTP Request & Response

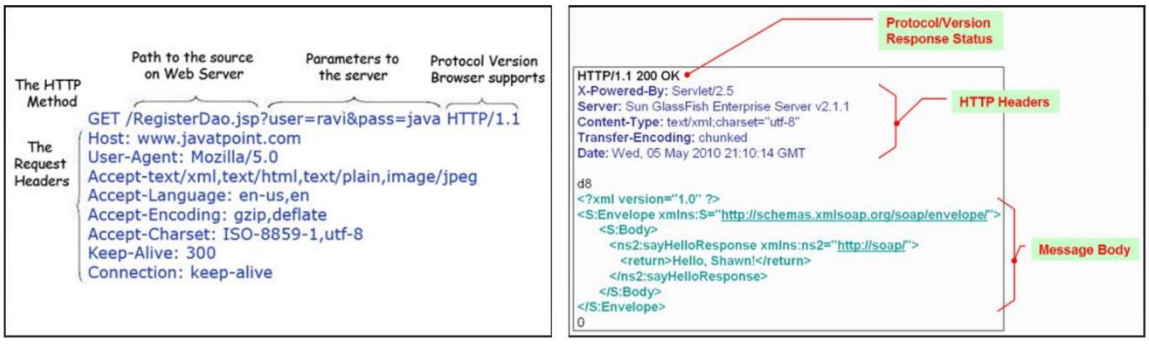


Figure 2.4: HTTP

2.9 HTTP VS HTTPS

HTTPS is equivalent to HTTP with authentication and encryption. The use of TLS (SSL) by HTTPS to encrypt and digitally sign requests and responses sent via normal HTTP is the only difference between the two protocols. As a result, HTTPS is substantially more secure than HTTP. The URL of an HTTP website starts with http://, but the URL of an HTTPS website starts with https://.

HTTP: A web server, which houses a website, uses HTTP to deliver data to a browser (where you view a website, like Chrome). The only issue with HTTP is that anyone might potentially abuse the information that is sent between the server and the browser. You may easily wow your audience and give your Presentations a certain zing and appeal. Simple to alter the text, photographs, and colors.

HTTPS: By using HTTPS, you strengthen that connection's security and prevent data eavesdropping. To prevent unauthorized parties from viewing the data, it is encrypted while it travels back and forth between the server and the browser [1].

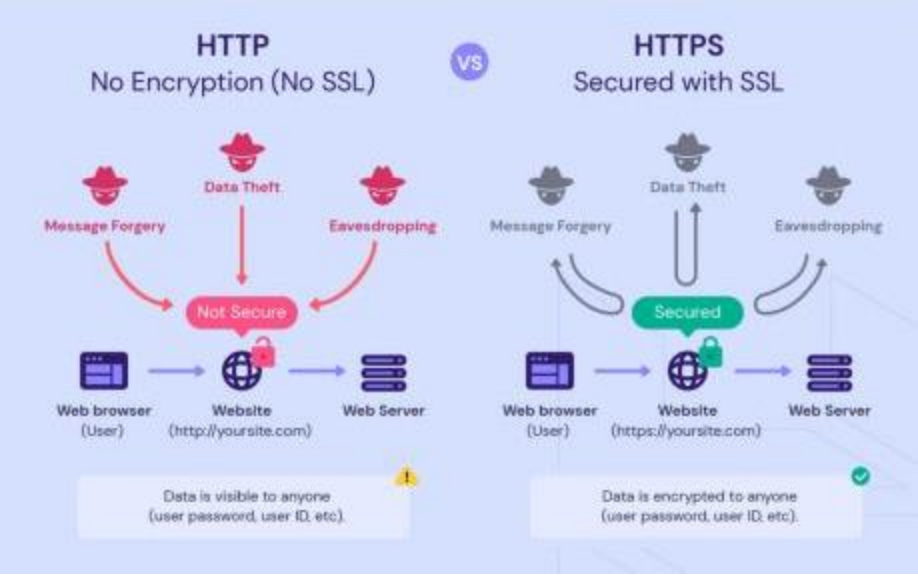


Figure 2.5: HTTP VS HTTPS

CHAPTER 3

THE METHODOLOGY

3.1 OSI Model in Cyber Security

A conceptual framework known as the "Osi Layer" (Open System Interconnection Model) is used to describe how well a networking system operates. The OSI model organizes computer operations into a standardized set of rules and guidelines in order to facilitate interoperability across various objects and applications. The OSI reference model separates computer-to-computer interactions into seven different levels of abstraction: physical, data connection, networking, transports, sessions, presentation, and application.

The International Organization of Standardization released the OSI in 1984, whenever network computing was barely getting started (ISO). The Osi is commonly used today to explain network architecture, despite the fact that it does not always perfectly fit individual systems [13].

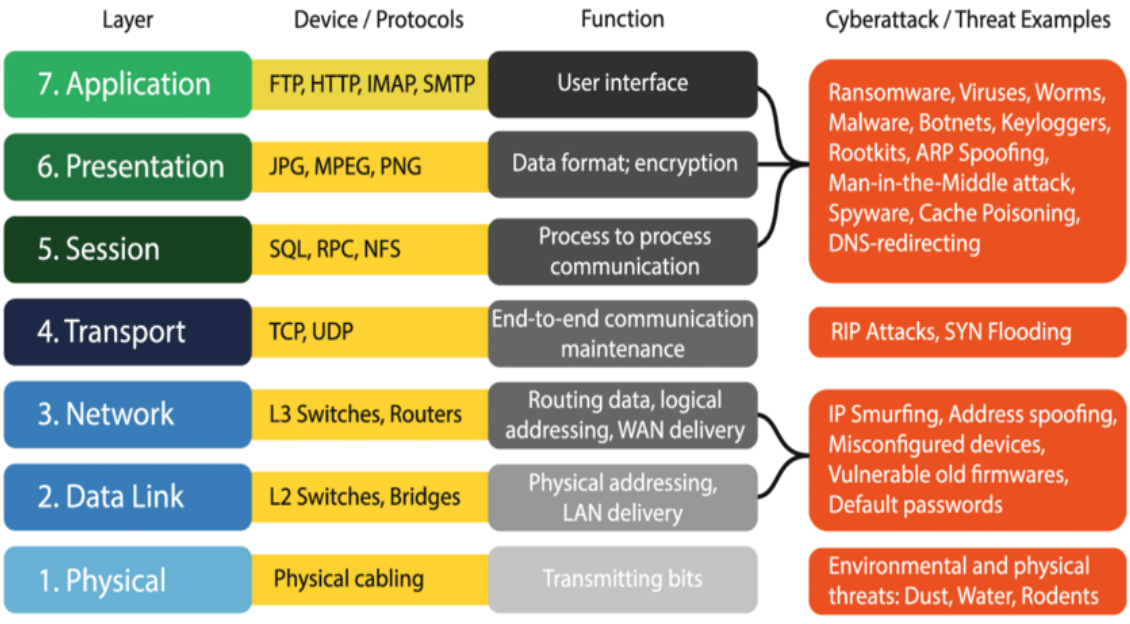


Figure 3.1: Osi Model

3.2 Testing for Penetration

A penetration test, also called as a testing process, mimics a cyberattack on our computer network in order to identify potential weaknesses. Penetration testing is often used in conjunction with a firewall for web applications in the context of internet application security (WAF).

Pen testing comprises trying to log in with any of the application platforms (such as client - side servers, APIs, and so on) in order to find security issues such as un-sanitized input that are vulnerable to code injection attacks.

Using the data from the penetration test, you can enhance your WAF security processes and address any weaknesses [1].

3.3 Hacking Methodology

1. Reconnaissance is the initial stage in hacking. It is also recognized as the information collecting and foot-printing phase. At this step, we collect as much information on the target as possible. Typically, we get information on three groups:

a. Network
b. Host
c. Parties concerned

There are two types of foot-printing:

- Active: Direct interaction with the target to know more about them. Scanning the target, for example, using Nmap
- Passive: Trying to discover as much as possible as possible about the objective without contacting it physically. This comprises acquiring data from publicly accessible websites, social media, and so forth.

2. Scanning: There really are three types of scanning:

- Port scanning: At this step, the target is scanned for information such as open ports, active systems, and other services utilized by the host.

- Vulnerability Scanning is the method of examining a target for exploitable faults or vulnerabilities. Typically, automated tools are used.
- Identifying the topology of the network, routers, firewalls, servers, and host information, and then utilizing that information to construct a network diagram. This map might offer useful information during the hacking process.

3. Get Access: An attacker utilizes a number of tools or tactics to gain entry to the machine or network at this step. He must upgrade his power rating to administrator after login in in order to run the software he needed, change data, or hide data.

4. Get Access: An attacker utilizes a number of tools or tactics to gain entry to the machine or network at this step. He must upgrade his power rating to administrator after login in in order to run the software he needed, change data, or hide data.

5. Cover Tracks or Analysis and WAF Configuration:
Clearing Tracks: Nobody aspires to be caught stealing. An astute hacker constantly erases all signs of his activities so that no one can recognize himself in the future. This requires modifying registry settings, changing Log values, removing all applications he used, and wiping all folders he created.

Analysis: A report outlining the penetration test's findings is subsequently put together.

- Several weaknesses were exploited
- Access to confidential information
- How long did it take the penetration tester to remain concealed in the system?

This data is examined by security personnel in order to aid in adjusting a company's current WAF setting as well as other application security technologies to correct vulnerabilities and fight against impending assaults [14].

3.4 OWASP Vulnerability (2017 Upgrade 2021)

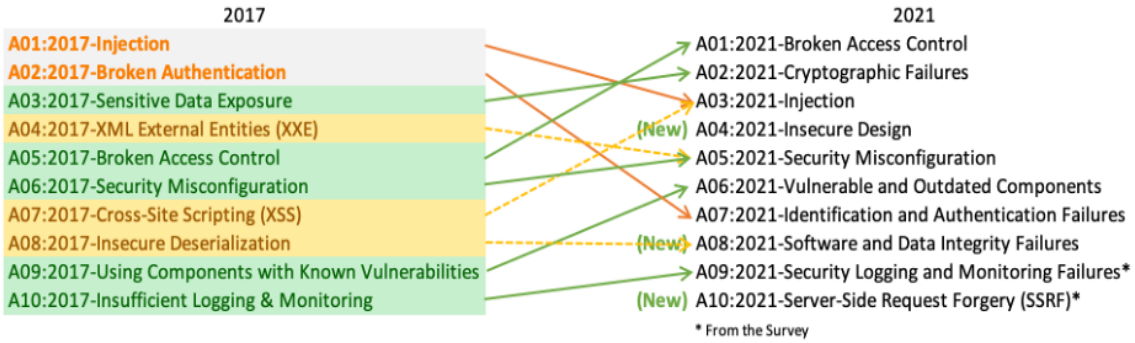


Figure 3.2: OWASP Vulnerability (2017 Upgrade 2021)

This data is examined by security personnel in order to aid in adjusting a company's current WAF setting as well as other application security technologies to correct vulnerabilities and fight against impending assaults [2].

3.5 Risk Residual

I'll let Ed Norton handle this one: "A new automobile made by my business departs someplace at 60 mph. The back differential is locked. The automobile crashes and flames, trapping everyone inside. Should we now issue a recall? Multiply the number of cars in the field, A, by the likely rate of failure, B, and then by the typical out-of-court settlement, C. A multiplied by B multiplied by C equals X. We don't conduct recalls if X is lower than the expense of doing so." Residual risk is what remains after you have done all that is cost viable to strengthen security, but going any farther is a waste of money. The corporation is ready to accept residual risk as a bet in the belief that it will not occur [15][16].

3.6 Network Sniffing

Network sniffing is the use of sniffer programs to monitor and analyze data packets travelling through computer networks in real time. Sniffers may be used for a variety of objectives, including information theft and network management.

Network sniffer is used for both ethical and immoral objectives. These are used by network administrators as network monitoring & analysis tools to identify and avoid network-related issues such as traffic congestion. Cybercriminals employ these technologies for nefarious goals such as identity theft, email hijacking, sensitive data theft, and more [3].

3.7 Poisoning with ARP

ARP poisoning is a type of network intrusion that may be countered by using the following techniques:

Get live, professional coaching from anywhere you are!

- Enroll inside an upcoming online live boot camp to ensure your certification.
- Use packet filtering: Spam filters may detect and stop packets with contradictory source addresses.
- Avoid trust relationships: Organizations should create a process that depends as little as possible on trust relationships.
- Use ARP spoofing software to detect: Some applications check and verify data before transmission and prohibit faked data.

Use cryptographic internet protocol: ARP spoofing attempts may be prevented by using https protocol such as SSH, TLS, and HTTPS, which encrypt data before and after transmission [3].

CHAPTER 4

USING SOFTWARE, OS AND TOOLS

4.1 Cloning

Cloning is a procedure in which an image of one computer's hard drive is created and transferred to as many machines as desired. The following were the issues with this concept:

1. A network failure
2. Process takes too long.
3. Computer updates
4. How often should I update?
5. Hard drive deterioration.

The correct operation of the network depends on a number of variables, which makes network cloning uncertain. This lab shouldn't have to bear the risk of a network outage since research output would decrease. Additionally, a choice about cloning the system must be made if network cloning is taken into account. Users will experience annoyance since cloning time will interfere with their ability to utilize the lab. Only one machine can duplicate an image from another system using nonnetwork cloning. It is not practical for this process to take so long. The lifespan of the hard drive is also shortened by wear and tear, which causes the lab equipment to degrade quickly.

4.2 VMWare

VMWare is a piece of proprietary software that will help with managing the setup of the computer. The virtualization layer it offers transforms the actual machine into a logical resource pool. Any operating system or program can get these resources. VMWare is installed as a guest operating system on top of the operating system. The operating system is the system that runs the operating systems for VMware. Appendix a contains more information regarding the specifics of the VMware installation. The ultimate product is a

setting in which the guest operating system's administrative rights are granted. Any program may be installed on the device with the user's authorization. For a more comprehensive description of how to use VMware, see Appendix B. With administrator privileges, the user is able to make the modifications necessary to install software by altering the machine's configuration files. However, since this operating system is not a document on the host system, VMWare accomplishes the intended goal of keeping the host's file type [7].

4.3 Using Operating System

Here, Using some of operating system in VMWare. That’s are [5][8]:

- Kali Linux
- Ubuntu
- Windows 10
- Windows 7
- Windows Server 2019

4.4 Standard Tools and Burp Suite Tools

Hackers may use a variety of tools such as: to automate certain manual activities & speed up overall hacking process [1].

- Metasploit
- Wireshark
- NMAP
- The Burp Suite
- ZAP OWASP
- Nikto
- SQLmap

Burp Suite is a comprehensive tool for hacking web applications. It includes all of the tools that a hacker could need to exploit an application. Among these functions include, but aren't limited to:

- Proxy
- Spider
- Scanner
- Intruder
- Repeater
- Decoder
- Comparer
- Sequencer

CHAPTER 5

HACKER AND HACKING

5.1 The Elements of Cybersecurity

Major elements of cybersecurity are:

- Information security
- Network security
- Operational security
- Application security
- End-user education
- Business continuity planning

5.2 Pentesting Approaches are Classified into Three Kinds

These are the three types:

- Black-Box Testing
- White-Box Testing
- Gray-Box Testing

Black-Box Testing:

In rare cases, the cyber-attacker may have no knowledge of their targeted target. In order to breach the defenses, the cyber-attacker will launch an all-out attack, also referred as a brute-force assault. In a black-box situation, the pentester has no information of the victim(s) they are about to attack. As a consequence, doing this type of pentest may take a long time, thus automated tools are largely depended upon. This is sometimes referred to as a trial-and-error technique.

White-Box Testing:

This type of pen-test is sometimes referred to as clear-box testing. In some cases, the pen-tester has some advanced knowledge of the Web application being tested and its underlying code editor. When compared to a black-box test, this kind of assault takes less time to initiate.

Gray-Box Testing:

This type of pen-testing combines both black-box & white-box testing. This merely indicates that the pen-tester is familiar with the targets they want to assault. This kind of task necessitates the use of both automatic and manual tools. As compared to alternative tests, this one has the best likelihood of uncovering hidden security flaws and vulnerabilities.

5.3 Do A Pentest

- The Red Team
- The Blue Team
- The Purple Team

These three teams' functions may be summarized as follows:

The Red Team:

This gang of pen-testers simulates a cyber-attack. That is, this team acts as the one who launches the real threat in order to breach the lines of protection of the company or organization and seek to exploit any uncovered holes.

The Blue Team:

These are pen-testers who pose as legitimate IT employees in a company. Their primary goal is to prevent any cyber-attacks conducted by the Red Team. They adopt a proactive approach while also keeping a high sense of security awareness.

The Purple Team:

This is a hybrid of the Red Team as well as the Blue Team. For instance, they have the Blue Team's security arsenal and a working understanding of what the Red Team is intending to attack. The Purple Team's major responsibility is to assist both of these teams. As a result, the Purple team's pen-testers cannot be influenced in any way and must retain a neutral vantage point [14].

5.4 Certifications That are in High Demand for Pen Testing

There is no question that there are an infinite number of certifications available in the cybersecurity area. However, if a pen-tester wants to be acknowledged as the best in their area, the following certifications are required[17]:

- Ethical Hacker Certification (aka CEH – this is administered by the EC Council)
- The Certified Professional in Offensive Security (aka OSCP – this is administered by Offensive Security)

5.5 A White Hat and A Black Hat

This specific topic may spark a huge philosophical argument about information freedom, and whether anything done in a purposefully flawed fashion is truly breaking into it, and so on. The most common example I've heard is the traditional Jedi scenario – identical equipment, different ideas.
Personally, that difference between a black hat or a white hat, according to the folks I know who have worked on the both sides of the line, is who signs the check [17].

5.6 A Vulnerability or An Exploit

Many people would argue they are the exact same thing, and they would be correct in certain ways. However, one is a prospective issue, whilst the other is an ongoing one. Consider this: you have such a shed with such a broken lock that won't latch correctly. In

certain regions, such as big cities, it is a serious issue that must be addressed quickly, however in others, such as rural areas, it is more of an annoyance that can be addressed when the time comes. It would be a weakness in both circumstances, whereas the large cities drain would be an instance of an exploit – there are individuals in the region actively abusing a known flaw [17].

5.7 A Black Box Testing and A White Box Testing

The distinction lies in the information provided by the individual commissioning the test. A white box testing is one in which the ethical hacking team is provided as much knowledge about the environment as feasible, while a black box testing is, well, a black box. They have no idea what's within [17].

5.8 The Three-way Handshake & Launch a Denial-of-service Attack

The 3 handshake is a key component of the TCP protocol: SYN, SYN/ACK, ACK. The outgoing sync from server to client is denoted by SYN. SYN/ACK is the server's acknowledgment to the client, indicating that yes, I hear you, and let's start a connection. The last link, ACK, permits the two to communicate. The issue is that this is a pretty simple form of denial-of-service attack. The client initiates the SYN link, the server answers with the SYN/ACK, but the client then initiates another SYN. The server considers this a new connection request and maintains the prior connection open. As this is performed many times extremely fast, the server soon gets overwhelmed with a massive amount of connection requests, ultimately overwhelming its capacity to connect to real users [17].

5.9 Footprinting

Footprinting is the process of gathering and discovering information about a target network before trying to gain access to it. Among the hacking tactics are [17]:

- Open source footprinting: This approach searches for administrator contact information, which may then be utilized in social engineering to guess the proper password.
- Network enumeration: This occurs when the attacker tries to identify the targeted domain names and network blocks.
- Scanning: Once the network has been identified, the next step is to probe the network's active IP addresses.
- Stack fingerprinting: This technique should be used as the last footprinting step after the port and host have been mapped.

5.10 SQL Injection

When an application fails to sanitize user input, SQL injection happens. As a result, a hostile hacker would insert SQL queries to obtain unauthorized access and perform database management activities. SQL injections may be divided into three types [17]:

- Error-based SQL injection
- Blind SQL injection
- Time-based SQL injection

5.11 Cross-site Scripting

Cross-site scripting (XSS) exploits include injecting malicious code into normally safe and trustworthy websites. When an intruder inserts a malicious payload, typically in the form html JavaScript code, into a web form, XSS occurs. The following are the categories of XSS vulnerabilities [17]:

- Cross-site scripting was reflected.
- Cross-site scripting that is saved
- Cross-site scripting using the DOM

5.12 A Distributed Denial of Service (DDoS) Attack

DOS assaults entail flooding servers, systems, or networks with traffic in order to consume too many resources from the target. This renders genuine users' access to and usage of targeted sites difficult or impossible [17].

- DOS assaults are common.
- Attacks on buffer overflow
- ICMP flooding
- SYN influx
- Teardrop assault
- Smurf assault

5.13 The Most Typical Forms of Cybersecurity Attacks

The most typical forms of cybersecurity assaults are as follows [17]:

- Malware
- SQL Injection Attack
- Cross-Site Scripting (XSS)
- DoS
- Man-in-the-Middle Attacks
- Reusing Credentials
- Phishing
- Session Hijacking

Figure 5.1: Cybersecurity Attacks

5.14 Data Leaking

The illicit sending of data to a whereabouts are or an unauthorized party inside an organization is referred to as data leakage. It can physically or electronically transport data.

It generally happens via the internet, emails, & mobile devices that store data.

Data leaking types include [17]:

- The Unintentional Breach - The vast majority of information leaks instances are unintentional.
- For example, a business may transfer private material to the incorrect recipient.
- Disgruntled or malicious employee - An authorized entity transfers private material to an unauthorised body.
- Electronic Communication with Bad Intentions - The issue is that all electronic media are susceptible of file transmission and external internet access sources.

5.15 CSRF Assaults

Cross-site Request Forgery (CSRF) occurs when an attacker convinces a victim into doing activities on their behalf.

CSRF attacks may be avoided in the following ways [17]:

- Using the most recent antivirus software, which aids in the prevention of harmful scripts.
- Do not visit other websites or read emails while identifying to your bank account or making any financial transactions through any other website, since this aids in the execution of dangerous scripts when connected to a financial site.
- Never store your login/password for financial transactions inside your browser.
- Turn off JavaScript in your browser.

5.16 Port Scanning

A port scanning program is used to locate open services and ports on a host system. Security managers generally use it to exploit holes, but hackers also use it to target victims.

The following are some of the most prevalent port scanning techniques [17]:

- Ping test
- TCP connectivity
- TCP is only half-opened.
- NULL, FIN, and X-MAS stealth scanning
- UDP

5.17 DNS Tracking

- DNS (Domain Name System) is indeed a system that converts human-readable domain names into computer-readable IP addresses. It enables websites to be hosted under a memorable domain name.

- DNS monitoring is simply the monitoring of DNS records to verify that traffic is appropriately routed to your website, digital means, services, and so on.

5.18 Salting and Hashing

- Hashing is a one-way function that converts data to a fixed-length value that is mostly used for authentication.
- Salting is an additional step for hashing that gives extra value to passwords by changing the hash value generated.

5.19 Attack with a Man-in-the-Middle

The following techniques help to avoid "Man-in-the-Middle Attacks" [17]:

- Unauthorized users are avoided by using greater WAP/WEP security on wireless access points.
- To safeguard sensitive information, use a VPN to create a secure environment. It makes use of key-based encryption.
- Public key pair-based verification must be used at several stages of a stack to ensure that you are transmitting the correct stuff.
- HTTPS is required for secure communication over HTTP via the public-private key exchange.

5.20 Assault with Brute Force

It is a court hearing approach for determining the correct password or PIN. Hackers repeatedly attempt all possible credential combinations. In many situations, brute force assaults are automated, with software working to login using credentials. There are methods for preventing Brute Force assaults. They are as follows [17]:

- Password length may be set.
- Password difficulty should be increased.

- Limit the number of login failures. assault with brute force

It is a court hearing approach for determining the correct password or PIN. Hackers repeatedly attempt all possible credential combinations. In many situations, brute force assaults are automated, with software working to login using credentials. There are methods for preventing Brute Force assaults. They are as follows [17]:

- Password length may be set.
- Password difficulty should be increased.
- Limit the number of login failures.

CHAPTER 6

MALWARE ANALYSIS

Malware analysis is the method of determining the behavior and purpose of a suspicious file or URL. The outcome of the study aids in identifying and mitigating potential threats. Malware analysis aids security personnel and security analysts largely by:

- Instances are triaged pragmatically based on severity.
- Detect and avoid occult signs of compromise (IOCs).
- Increase the impact of IOC alerts and warnings.
- When searching for dangers, provide context.

6.1 Malware Analysis Types

The analysis may be completed in a static, dynamic, and hybrid mode.

6.1.1 Static Evaluation

Simple static analysis does not need running the code. Instead, static analysis searches the file for evidence of malicious intent. Detecting rogue infrastructure, libraries, or bundled files might be beneficial. Technical indicators such as files, hashes, strings comprising Ip's and domains, and file headers data may be used to determine if a file is malicious. It is also feasible to observe the virus without running it using tools such as network analyzer and disassemblers to understand more about how it works.

6.1.2 Dynamic Evaluation

During dynamic malware analysis, potentially hazardous code is performed in a "sandbox," a secure environment. Because of this closed environment, security professionals may witness the virus in action without fear of it infecting their machines or getting into the business network.

Deeper visibility enabled by dynamic analysis enables threat analysts and incident responders to determine the true nature of a threat. Additionally, automated sandboxing saves time by eliminating the requirement to debug a file in order to detect harmful code.

6.1.3 Synthesis Evaluation (incorporates both of the preceding strategies)

Complex malicious code might escape scrutiny by sandbox technology on occasion, and basic system analysis is not a dependable solution. Security teams benefit from hybrid analysis, which blends dynamic and static analysis methodologies. This is mostly because it can detect malicious code that is attempting to conceal itself and then extract countless more signs of infection from static or previously unknown code. Hybrid analysis can detect even the most complex malware attacks.

6.2 Malware Analysis Use Case

6.2.1 Malware Identification

Adversaries are utilizing increasingly complex tactics to circumvent detection by existing technologies. In-depth behavioral analysis may be used to uncover common code, malicious functionality, or infrastructure, speeding up the detection of threats. Another outcome of a malware investigation is IOC extraction. The IOCs may then be sent into SEIMs, real-time threat platform, and security orchestrating tools to help teams stay informed about potential threats in the future.

6.2.2 Triage and Threat Alerts

Higher-fidelity alarms are provided by malware analysis tools early in the attack life cycle. Teams can thus save time by giving these warnings' outcomes priority over those from other technologies.

6.2.3 Incident Response

Early in the attack life cycle, malware analysis techniques offer higher-fidelity alarms. Teams may save time by elevating alert findings over those derived from other technologies.

6.2.4 Threat Hunting

Threat hunters can leverage behaviors and artifacts revealed by malware research to identify comparable behavior, access to a specific data connection, port, or domain, for example. Analyzing firewall & proxy log or SIEM data might help teams identify relevant hazards.

6.3 Malware Analysis Stages

6.3.1 Analysis of Static Properties

Static characteristics include things like maliciously encoded strings, header data, hashing, metadata, embedded resources, and so forth. This kind of data might possibly be everything that is required to generate IOCs because there is no obligation to run the application in order to access it. The results of the static properties analysis can be used to determine the next step, which may involve additional research using more thorough techniques.

6.3.2 Analysis of Interactive Behavior

Peer counseling is used to observe and engage with a virus or worm in a lab setting. Understanding how the sample's registry, file system, processes, and networks operate is the aim of analysts. If the analysts believe the infection has a certain capability, they may develop a simulation to put their notion to the test. A talented analyst with exceptional originality and aptitude is necessary for behavioral analysis. Without automated technology, it is impossible to effectively finish the protracted and complicated process.

6.3.3 Analysis That is Completely Automated

Completely automated analysis quickly and simply analyzes questionable files. The study may identify possible effects if the virus penetrates the networks and then present security experts with a report that really is easy to read and provides rapid remedies. Fully automated analysis is the most efficient way to analyze ransomware at scale.

6.3.4 Team Manage

Team management is very important in any company so we have tried to make team management easy & efficient in this project. The team management option is only for the department head or CEO, they can create new teams, add members to the team and hire a team leader from team member. and they can be monitoring all member work progress also team leader from here.

6.3.5 Reversing Codes Manually

In this stage, analysts decode encrypted information using developer tools, disassemblers, compilers, and specific tools to find any hidden skills that the viruses may have that have not yet expressed itself. Code downturns take a long time and a special skill. Because of these circumstances, malware investigations usually skip this step, omitting a plethora of critical information about the virus's structure.

6.4 Traffic Analysis

1. The infected Windows virtual machine's IP address is [9]: [redacted]

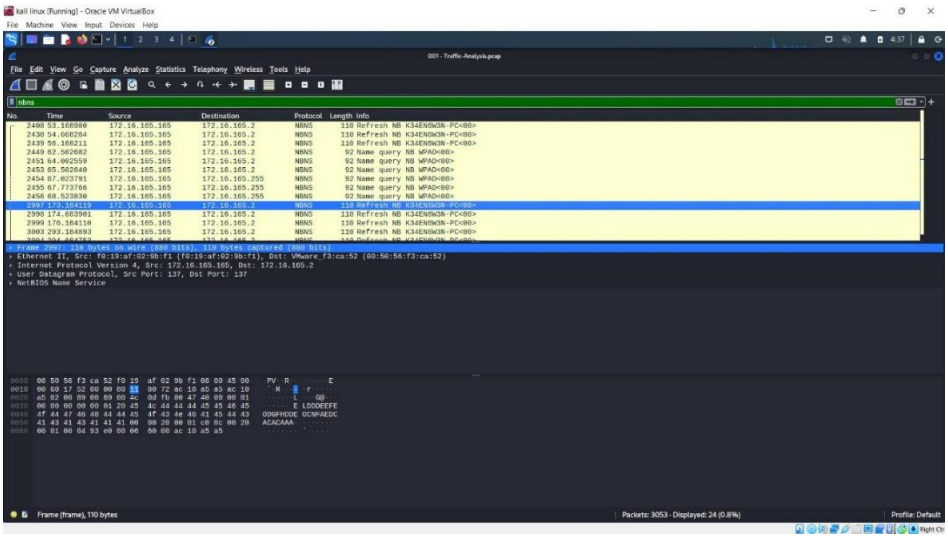


Figure 6.4.1: The infected Windows virtual machine's IP address

2. The address of the infected Windows virtual machine [9]:

[redacted]

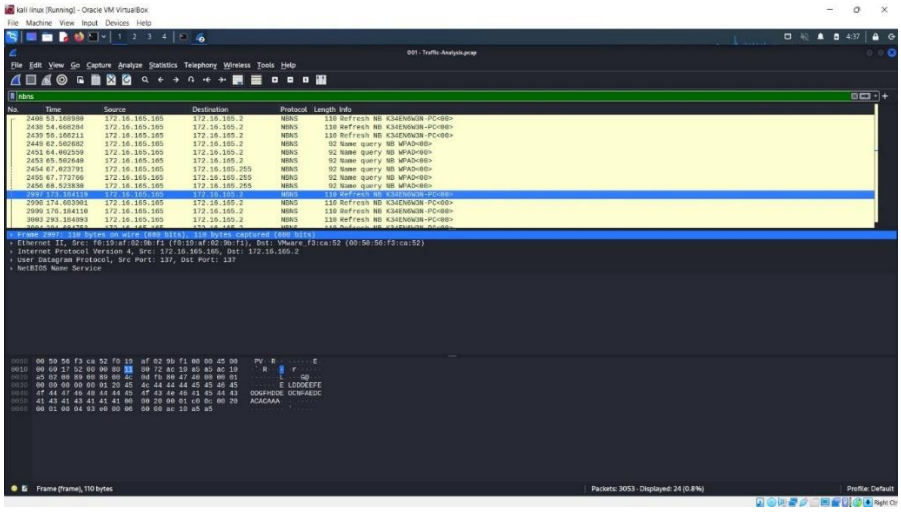


Figure 6.4.2: The address of the infected Windows virtual machine

3. The infected VM's MAC address is [9]:

[redacted]

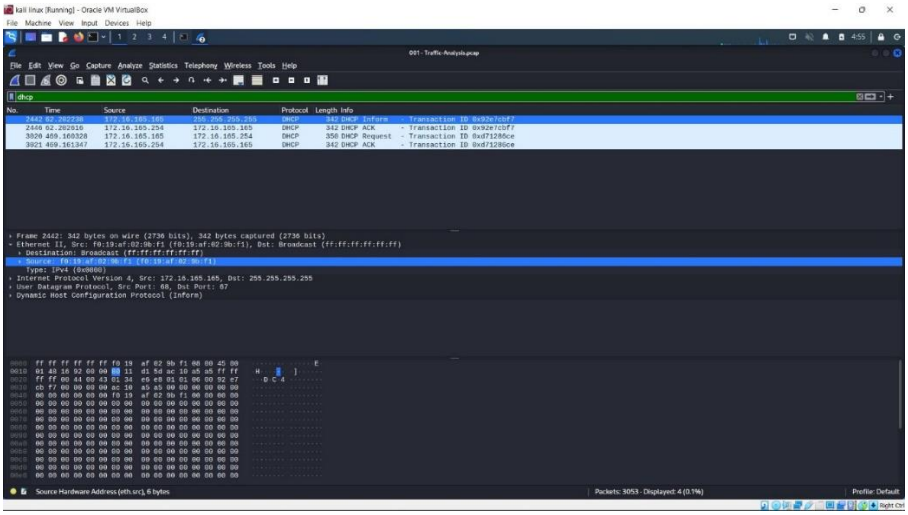


Figure 6.4.3: The infected VM's MAC

4. The IP address of the compromised website is [9]:

[redacted]

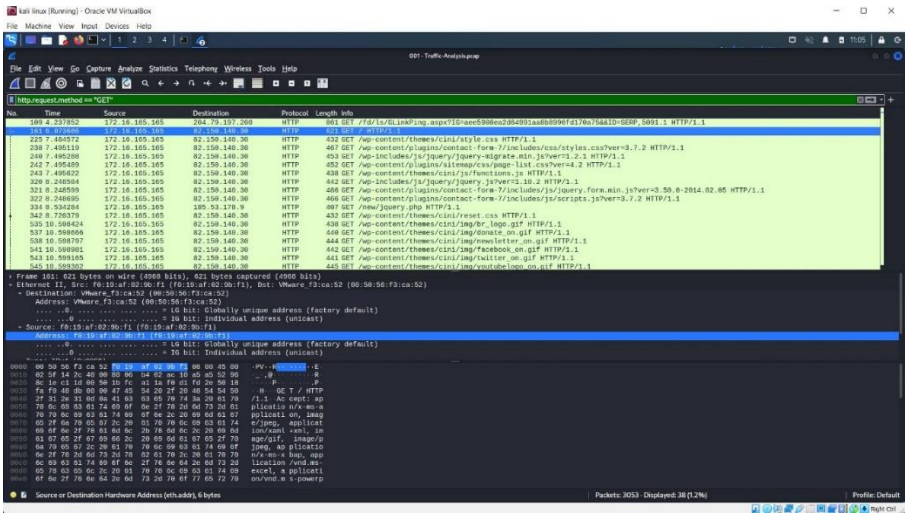


Figure 6.4.4: The IP address of the compromised website

5. The hacked website's domain name is [9]:

Host: [redacted]

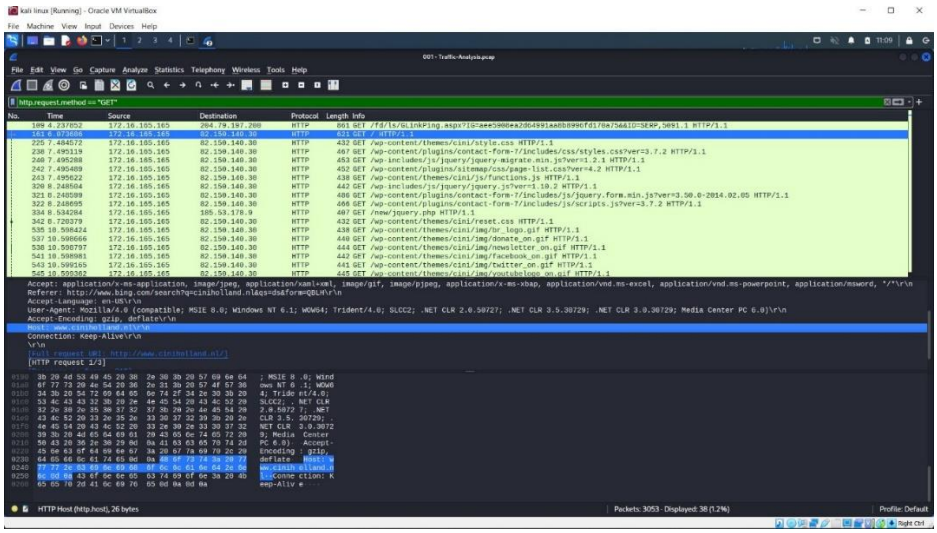


Figure 6.4.5: The hacked website's domain name

6. The exploits kit and virus were supplied using the following IP address & domain name [9]: [redacted]

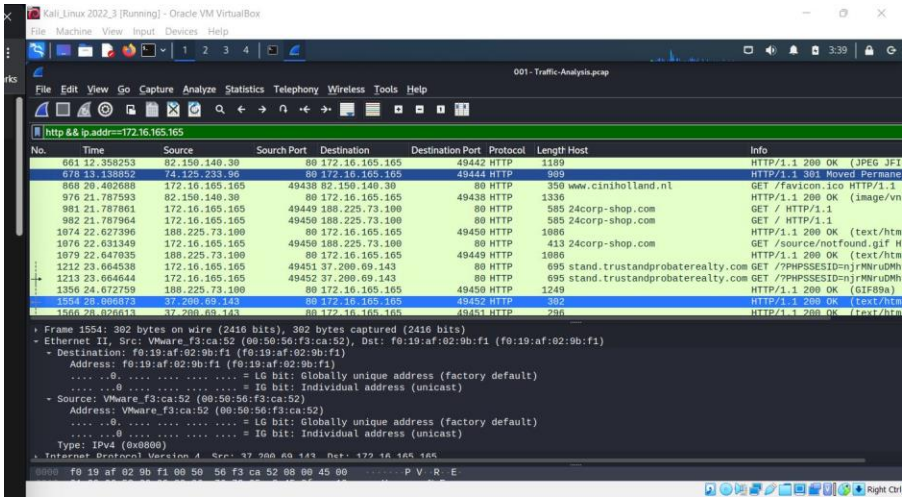


Figure 6.4.6: The exploits kit and virus were supplied using the following IP address & domain name

7. The domain name from which the exploit kit & malware were transmitted was:

Host [9]: [redacted]

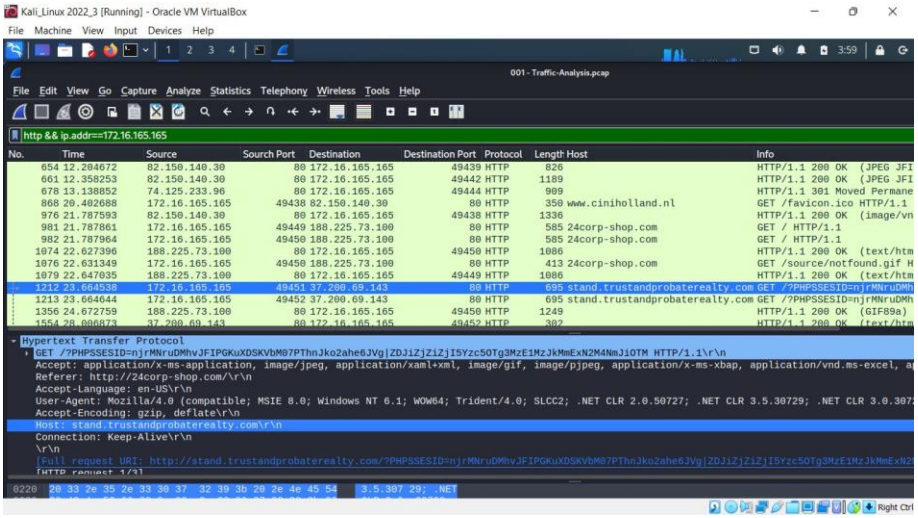


Figure 6.4.7: The domain name from which the exploit kit & malware

6.5 Static Analysis of Malware Analysis

6.5.1 Static Analysis Laboratory

Please keep in mind that the virus samples should only be extracted inside your virtual environment! These documents have the power to reproduce over network drives and could destroy your machine. Furthermore, if you try to extract these documents on a current Windows version, Security Software may quarantine them.

Step 1: After unpacking the Practical Malware Labs Malware to your desktop, browse to the Chapters 1 the first chapter files Lab01-01.dll & Lab01-01.exe. The following are the files that will be tested for this exercise.

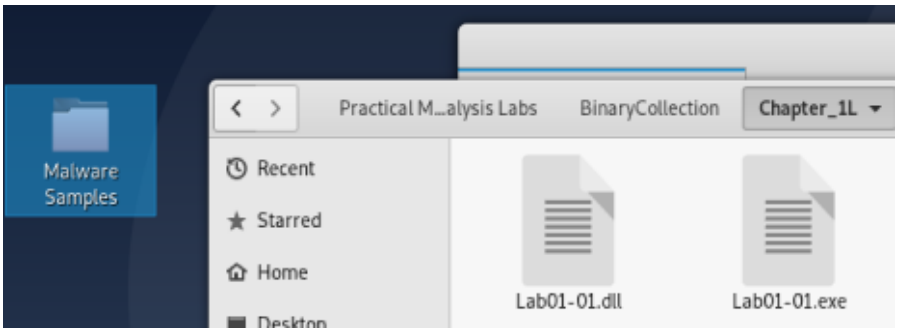


Figure 6.5.1: Malware Practical Malware Labs

Step 2: In the virtual environment, go to https://www.virustotal.com/gui/home/upload. Choose a file by clicking it. Select Lab01-01.dll from of the Chapter 1 contents and save it to your desktop.

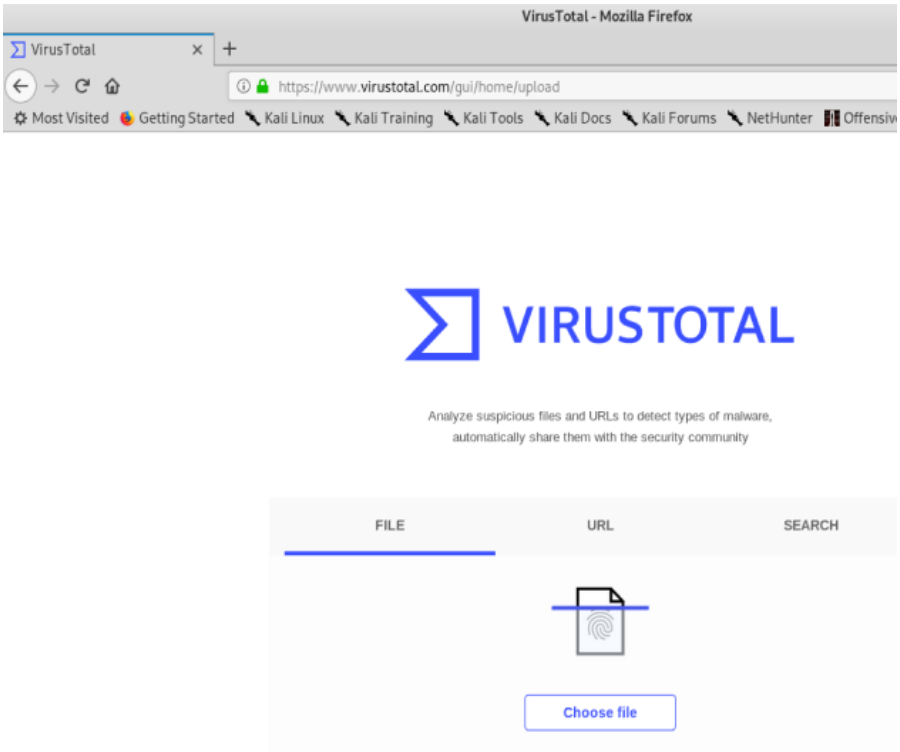


Figure 6.5.2: Malware Practical Malware Labs

Step 3: That once scan is finished, review the information in the tabs below.

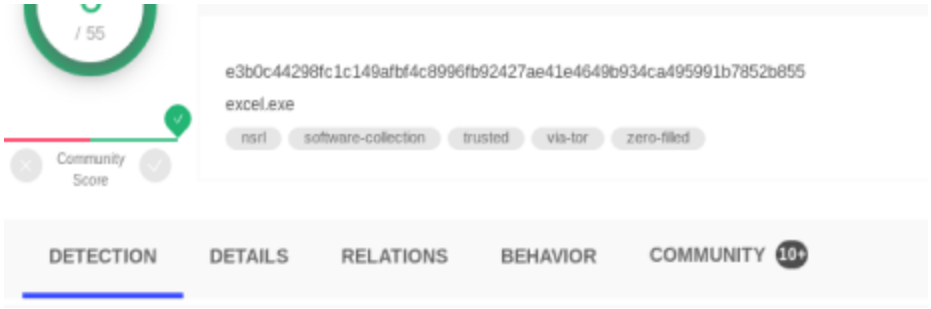


Figure 6.5.3: Malware Practical Malware Labs

Step 4: Repeat for Lab01-02.exe, Lab01-03.exe, and Lab01-04.exe.

Step 5: Include pictures of the tool and its analysis results in a Word document. Then, answer the lab problems below with your results [10].

6.5.2 Fill Out and Submit the Pertinent Lab Questions

1. Lab01-01.dil
   Lab01-01.exe
2. LoadLibrary or GetProcAddress, which are utilized to load and access extra functions, are often included in bloated and obfuscated code.
3. The Internet Traffic section contains network activity caused by the virus, such as opening a monitoring port or making a DNS request.
4. The viroustotal is often used for web application testing. It may be set up to enable malware experts to capture particular server requests and answers in order to modify what is sent to a machine. When viroustotal is configured as a man-in-the-middle, users may change HTTP or HTTPS requests delivered by the virus to the remote server so order to persuade the host to provide you with more information.
5. Static analysis entails deciphering the malware's internals by putting the exe into a debugger and inspecting the program instructions to determine what the program performs. Because the CPU executes the instructions, sophisticated static analysis can tell you precisely whatever the program does. Advanced static analysis, on the

other hand, has a more difficult learning curve that basic static analysis & requires specialist understanding of disassembly, code constructions, or Windows operating system fundamentals.

6. Advantages of static code analysis:
    - It can detect flaws in code at specific locations.
    - It may be carried out by qualified software assurance programmers who have a thorough understanding of the code.
    - It enables for faster turnaround on repairs.
    - When automated tools are employed, it is quite quick.
    - The whole code base may be scanned using automated techniques.
    - Automated technologies may give mitigation suggestions, minimizing the amount of work spent on research.
    - It enables flaws to be discovered earlier in the life cycle, lowering the cost of remediation.

Limitations of static code analysis:

- If done manually, it takes a long time.
- All programming languages are not supported by automated tools.
- False positives & false negatives are produced by automated technologies.
- There are insufficient skilled employees to undertake a comprehensive static code analysis.
- Automated technologies might provide the mistaken impression that everything is taken care of.
- Automated tools can only be as good as that of the rules they scan with.
- It does not detect vulnerabilities introduced during runtime.

Walker Dependency:

Dependency Walker is indeed a static analytical technique that is used to investigate DLLs and routines imported by malware. It supports both x86 & x64 binaries and generates a tree

structure diagram of any and all DLLs that are loaded in memory when the virus is executed. It is available for free download at http://www.dependencywalker.com/.

PEiD:

PEiD is a freeware static code analysis tool for detecting packers and compilers. More than 600 fingerprints are included for identifying packers, industry that deals, and processors in PE file format. PEiD also provides plug-ins, the most helpful among which is Krypto Analysis system (KANAL). KANAL may be used to locate popular cryptographic methods in PE files & export the data to IDA Pro. Although the PEiD initiative has been abandoned, the utility should still be available for download at http://www.peid.info/.

Strings:

Strings is a static analysis tool that may be used to examine ASCII & Unicode strings within binary code. Strings are frequently a rapid method to gain a high-level overview of malware capabilities, although packing and string obfuscation might limit the program's utility. Strings is available as part of the Sysinternals tool suite and may be downloaded at http://www.sysinternals.com/.

7. Static Analysis Best Practices:

There are a few myths to dispel before getting into static code analysis best practices. For instance, static analyzers are not single-use products nor is dynamic analysis better or worse than static analysis. But in general, there are concrete best practices along with emerging best practices developers should adopt when it comes to static analysis for code quality.

- Identify the scope of the problem.
- Make the code readable for other developers.
- Write code with reusability in mind.
- Keep extensibility available if an application needs new features in the future.
- Develop code that uses minimal resources while still executing quickly.

- Utilize dynamic and static analysis [10].

6.5.3 Practices of Static Analysis

1. Use antivirus software to do static malware analysis.

- EDITOR'S CHOICE: CrowdStrike Falcon An endpoint security platform that detects malware activities using AI techniques. This cutting-edge cybersecurity solution combines local data gathering units with a cloud-based analytical engine. Begin a free 15-day trial.
- Security Event Manager by SolarWinds (FREE TRIAL) The ideal protection for enterprises seeking a strong system capable of handling a large quantity of devices or the log data generated by them.
- NextGen SIEM Platform from LogRhythm Complete defensive system that handles threats from beginning to end in a single, integrated design.
- Splunk Enterprise Security Suite SIEM solution with comprehensive security monitoring & threat detection capabilities that keeps up with the complexity of today's complicated threats.
- McAfee Endpoint Security Manager This intelligent SIEM integrates analysis to rich context to identify and prioritize risks, while outstanding, dynamic data displays aid in the tracking of behaviors and settings.
- ArcSight ESM by Micro Focus With real-time log data correlation at a pace of 100,000 events a second, this is the fastest SIEM system possible for organizations.

2. Observe malware behavior

RATs: A remote access tool (RAT) is employed to remotely administer a computer or devices. RATs are often employed in targeted assaults with specified purposes, such as stealing data or moving lateral across a network. The server is operating on a victim's machine that has been infected with malware. The client is operating remotely as the attacker's command and control unit. The servers send out a signal to the clients to initiate

a link, and the client controls them. RAT communication is often accomplished using standard ports such as 80 and 443. This diagram depicts the RAT network.

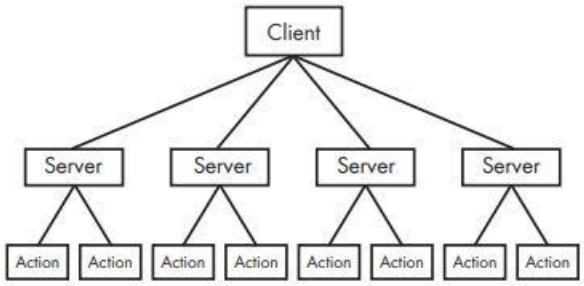


Figure 6.5.4: Observe malware behavior

3. Examine the following static analysis tools, methodologies, and practices:

- Installing antivirus and antimalware software to combat the dangers
- Increasing network users' technological awareness in order to avoid data breaches and theft, whether deliberate or unintentional.
- Putting regulations in place and enforcing them, as well as assuring the safeness of hardware items
- Updating & patching the operational system and the application software on a regular basis

However, just because you've taken each of these precautions does not imply your work is over. You must continue to monitor your network and the protection plan that is defending it. You must keep a close eye out for signals of external dangers and potential flaws. In the event of an immediate danger, you must devise an effective defensive plan based on real-time assessment of behavioral data gathered from your network.

4. Examine compressed and encrypted files:

Malware authors often utilize packing or encryption to make its files harder to identify or analyze. Obfuscated programs are those whose execution has been concealed by the

malware creator. Packed programs are a kind of obfuscated software in which the harmful code has been compacted and cannot be examined. Both strategies will substantially restrict your efforts to examine malware statically. Legitimate programs generally always contain a large number of strings. Malware that has been packed or disguised has relatively few strings. If you search a program using Strings and discover that it only includes a few words, it is presumably obfuscated or packed, implying that it is harmful. To examine further, you'll probably need to do more than static analysis.

CHAPTER 7

SECURITY DRIVEN SYSTEM ADMINISTRATOR

Computer networks are critical to company, and they need a committed professional or multiple individuals to handle the network's day-to-day functioning. System administrators may help with this.

A system administrator (sysadmin) is an IT expert who maintains a company's computer environment and assures the ongoing and optimum functioning of its IT services & support systems. Sysadmins are primarily responsible for "keeping the lights on" for the business, hence reducing work interruptions [6].

7.1 Establish Local Domain and Applications

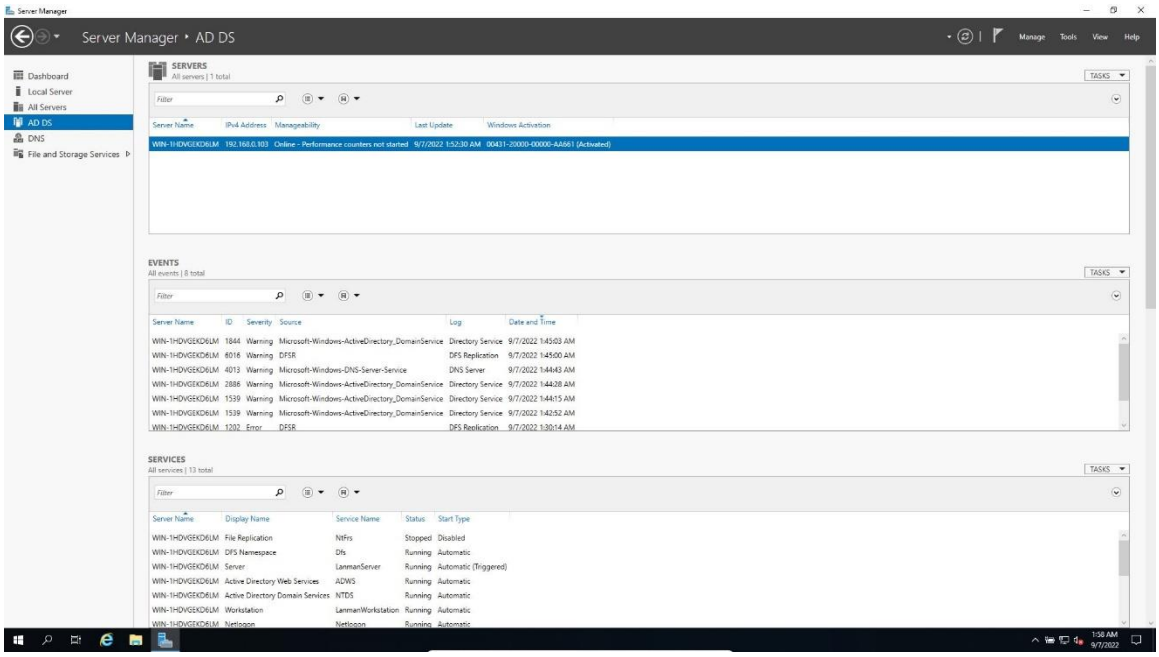


Figure 7.1: Create a Local Domain & Applications

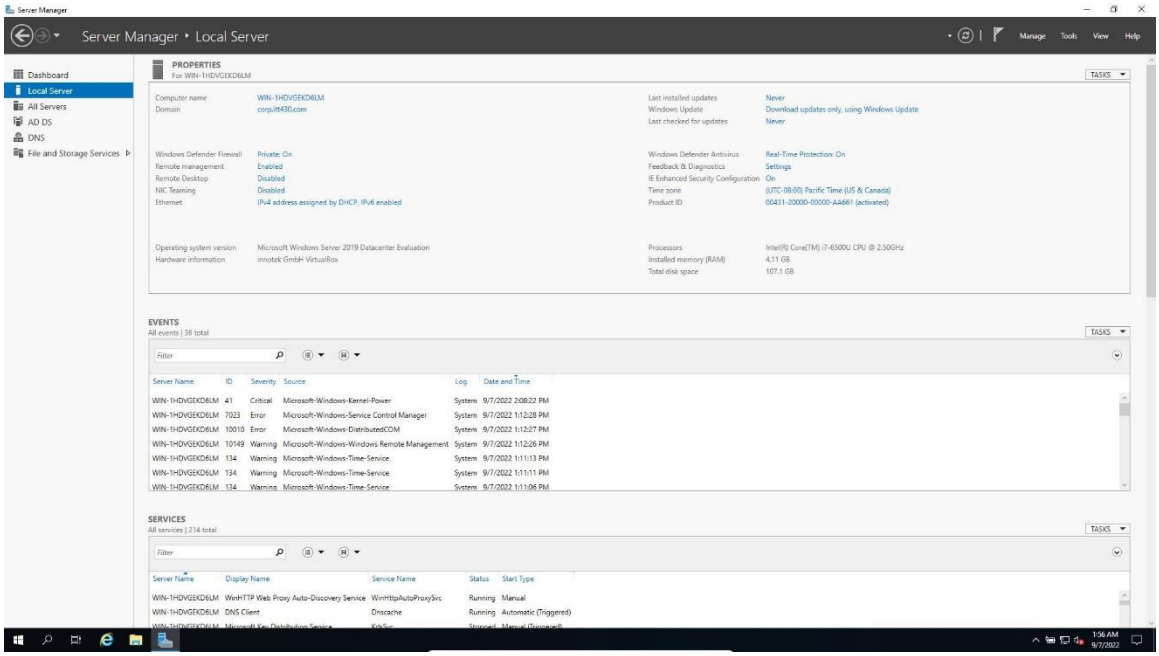


Figure 7.2: Create a Local Domain & Applications

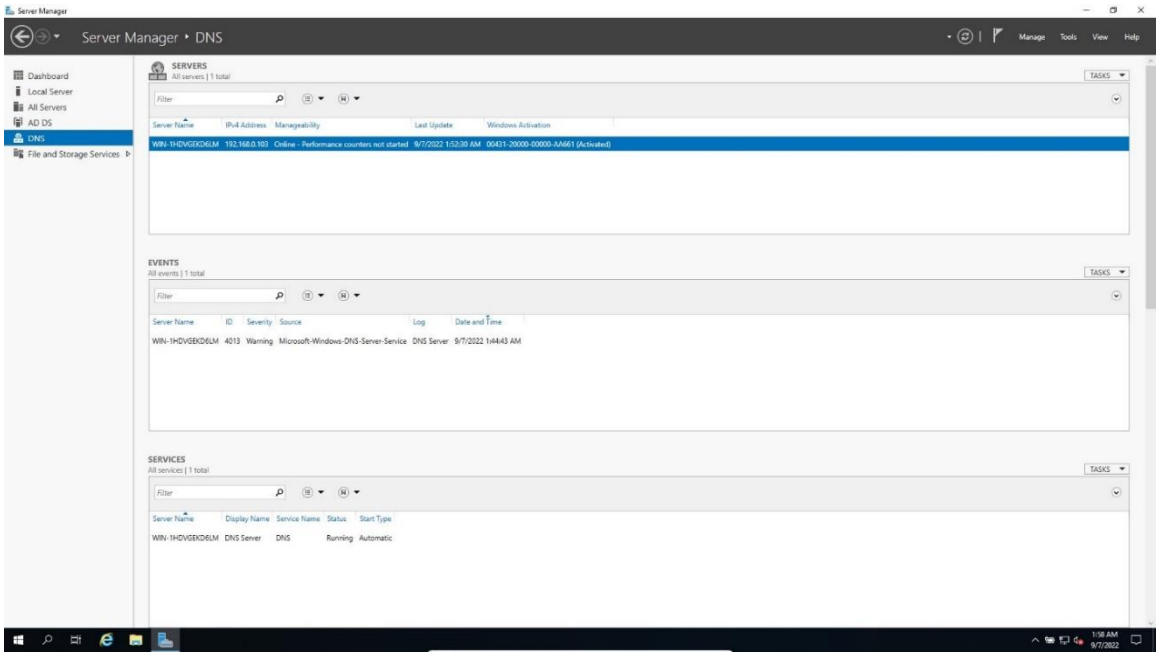


Figure 7.3: Create a Local Domain & Applications

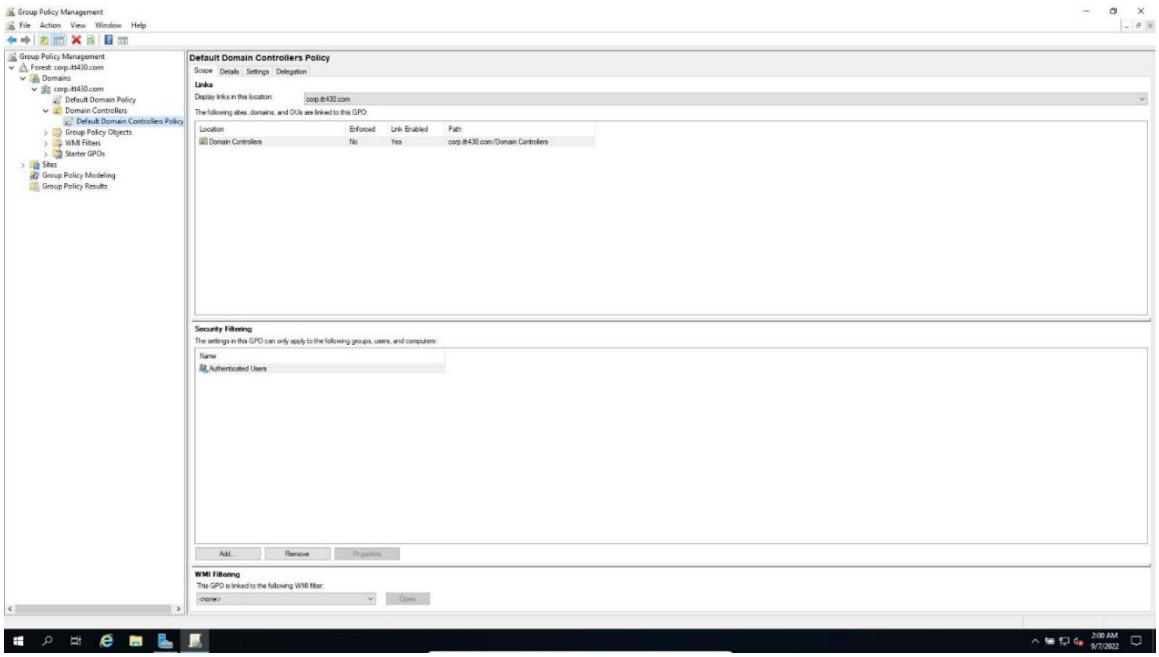


Figure 7.4: Create a Local Domain & Applications

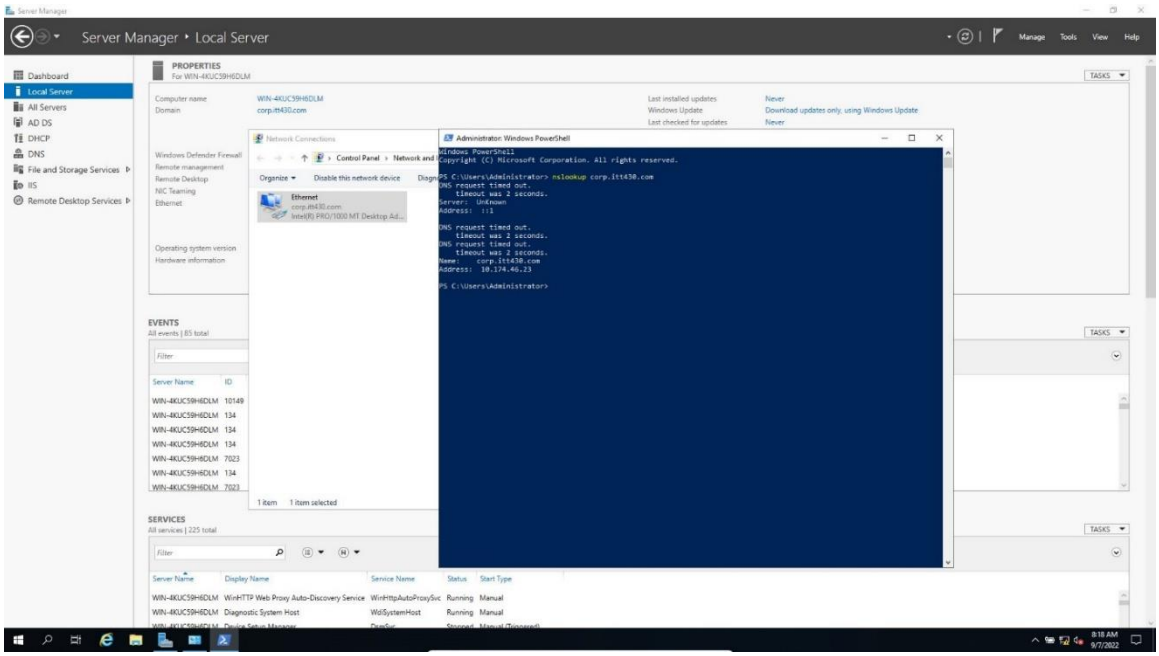


Figure 7.5: Create a Local Domain & Applications

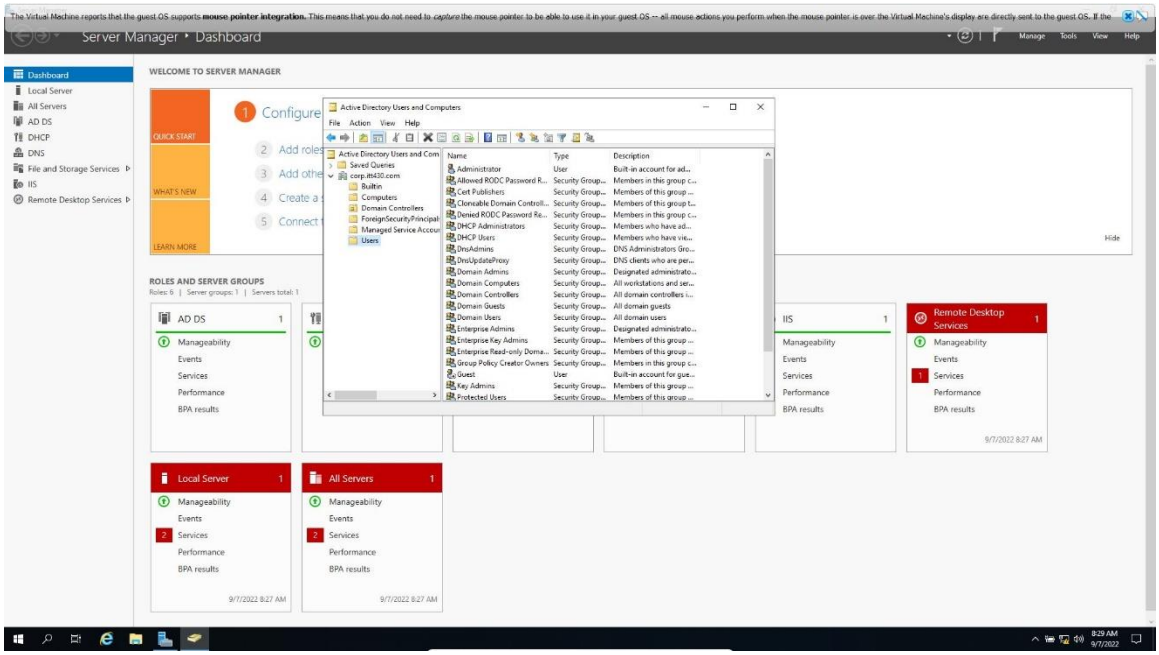


Figure 7.6: Create a Local Domain & Applications

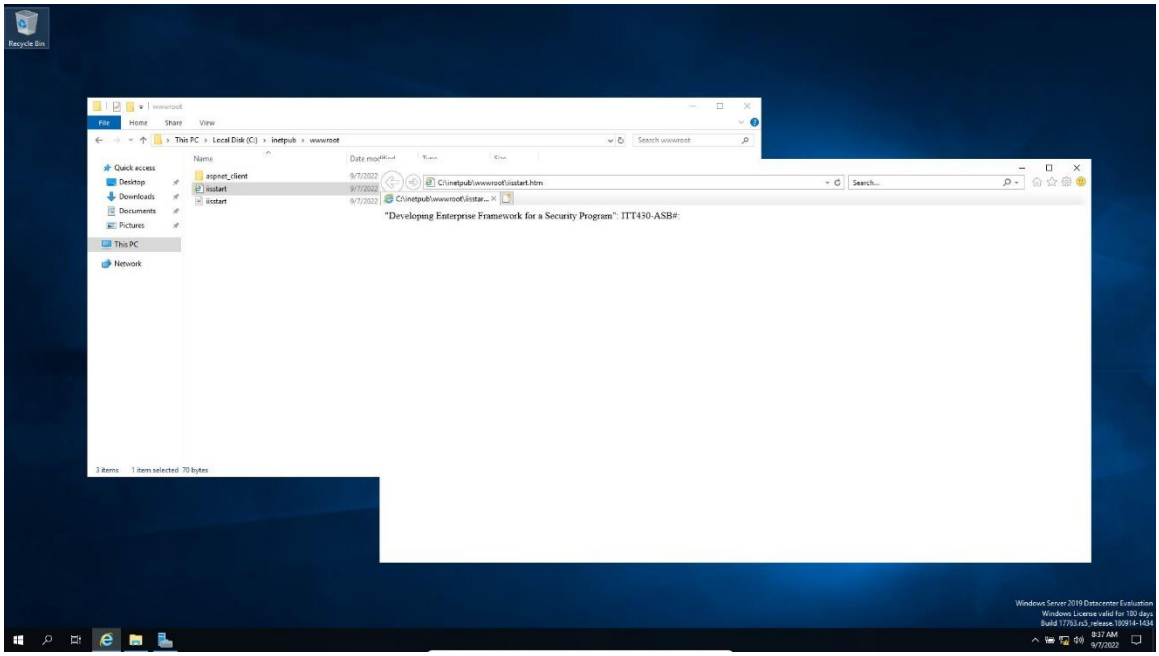


Figure 7.7: Create a Local Domain & Applications

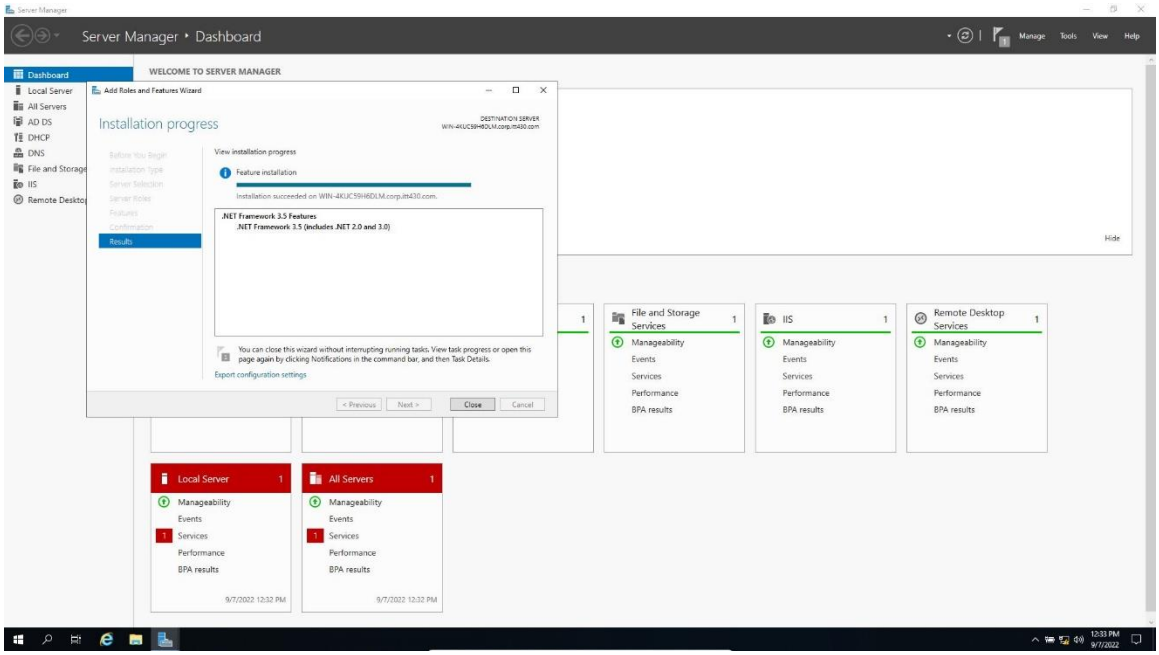


Figure 7.8: Create a Local Domain & Applications

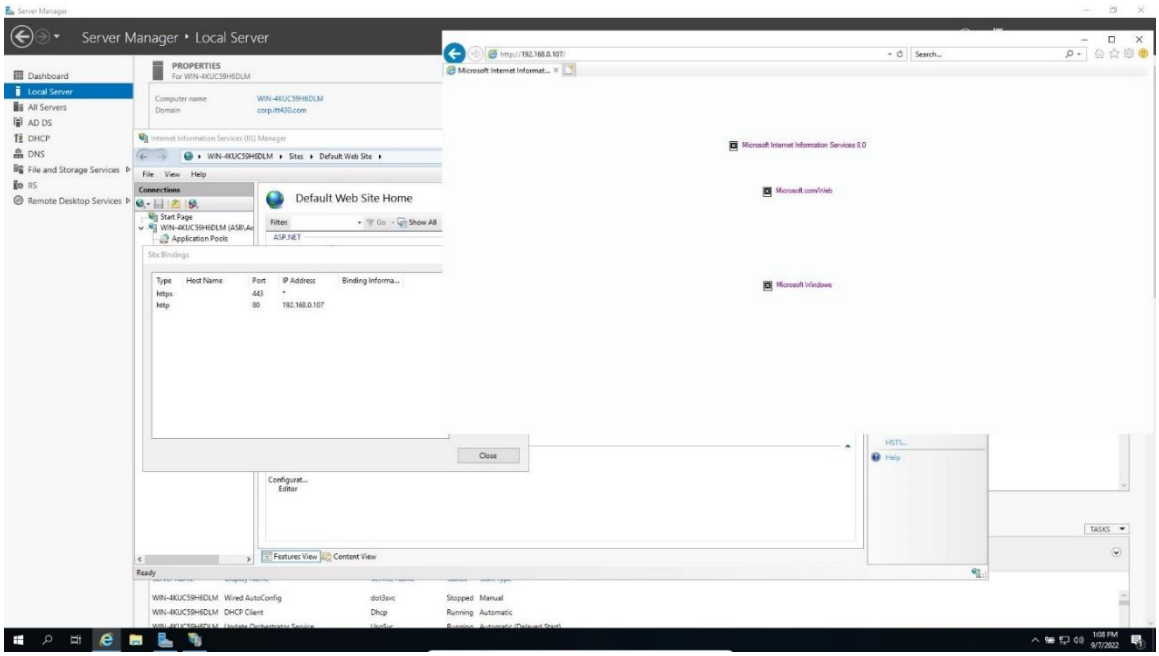


Figure 7.9: Create a Local Domain & Applications

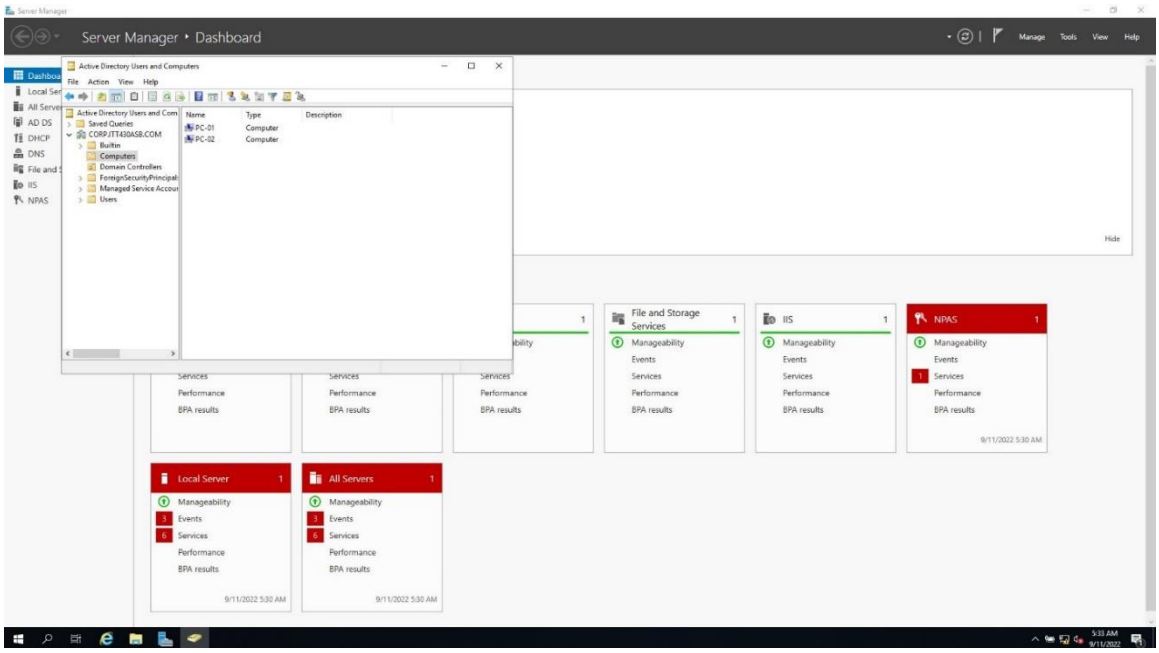


Figure 7.10: Create a Local Domain & Applications

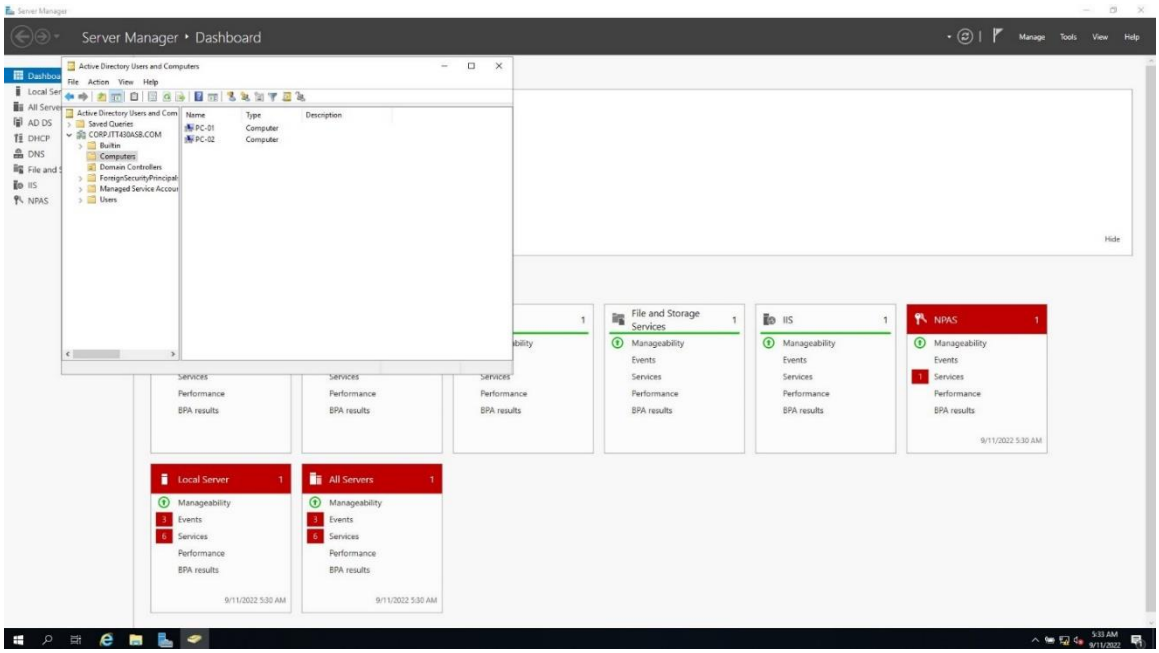


Figure 7.11: Create a Local Domain & Applications

7.2 Risk Management

Part 1: For all businesses, including small and medium-sized operations, risk management is essential (SMPs). This includes both protecting the company's resources, finance, and operations as well as aiding in effective corporate governance, compliance with the law, and due diligence. Risk management that works will protect the company's reputation, integrity, and position.

It is critical to create a hazard identification "culture" inside the organization. This emphasizes how important it is for all employees to include risk assessment into their daily work. A risk assessment culture seeks to create an environment in which partners and employees intuitively seek out hazards and consider their consequences while making sound operational decisions [11].

The following eight steps make up a risk management program:

- Create a risk management framework using the risk policy as a foundation.
- Create the Context.
- Determine Risks.
- Assess and Analyze Risks
- Deal with and control risks.
- Consult and communicate.
- Watch and evaluate.
- Record

Part 2: The possibility that your company may be exposed to or incur losses as a consequence of a hack or data breach is referred to as cybersecurity risk. A better, more complete explanation would include the potential loss or harm to technological infrastructure, technology usage, or an organization's reputation.

- Determining which assets must be safeguarded.
- Identifying the required threats and vulnerabilities.

- Finding weak places that can be abused.
- Determining the amount of risk offered by threat agents.
- Calculating the commercial impact of realized risks.
- Creating a risk assessment for security.
- Recommending a degree or threshold of risk acceptability.
- Advising on the best way to establish controls.

Part 3: Assessments should be conducted by an expertise or group of specialists who are informed about the issue under investigation. Supervisors & employees who are on the processes under assessment should be involved, either as team members or as information providers, since they are the most acquainted with the operation.

In order to do an assessment, you should typically:

- Recognize dangers.
- Determine the likelihood and degree of damage, such as an incident or sickness.
- Consider both routine operating situations and uncommon incidents, such as maintenance, closure, power failures, emergencies, extreme weather, and so on.
- Examine all available health and safety data on the hazard, such as Safety Data (SDS), automaker literature, data from credible sources, lab tests, workplace evaluation reports, & records of industrial accidents (collisions), including info on the nature & frequency of a occurrence, ailments, injuries, near-misses, and so on.
- Recognize the bare minimum of legal requirements in your area.
- Using the risk control hierarchy, determine the measures needed to lower the risk or remove the hazard.
- Conduct a review to evaluate if the risk was successfully managed or the danger was eliminated.
- Maintain a close eye on everything to ensure that the controller is still operational.

- Maintain any documents or paperwork that may be necessary. A explanation of the risk management approach, a breakdown of any assessments, or an explanation of the conclusions reached may be included in the documentation.

Organizations evaluate their risks in a variety of business domains, from security to finance. Risk evaluations for cybersecurity only include digital assets and data.

The two primary approaches for risk assessment are quantitative and qualitative:

Quantitative risk evaluation:

In quantifiable risk assessments, a team uses measurable data points to evaluate and quantify risk, with a heavy focus on statistics.

In order to conduct a quantitative risk assessment, your company will first create two lists: one of possible threats and one of your most important digital assets. The second list might contain important assets like your IT infrastructure, priceless data, and other resources. Once you've created a list of your assets, you'll need to give each thing a monetary value. This may be difficult for items with no set monetary worth, such as customer data or other important information.

Qualitative risk analysis:

A qualitative risk evaluation focuses on what would actually happen on a regular schedule if one of the threats on your list materialized rather than statistics.

While a risk evaluation is straightforward and focuses on data, a qualitative vulnerability assessment technique entails interacting with officials from different divisions or departments and asking them concerns about how a attack or breach would impact their operations. Inquire particularly about how a team's production might be affected if they were not able to access key platforms, applications, or information. These interviews will show an examiner which systems and systems are necessary for a specific team and which aren't. You may also ask teams that engage directly with consumers how a breach would

affect service delivery, or those in control of suppliers how an attack would disrupt supply chains.

Risk Vulnerability:

An evaluation of vulnerability may start with a risk assessment but then go further to determine how effectively the present infrastructure is protected from possible dangers. Steps might consist of the following:

- Identify Assets and Risks: Identify your most important IT assets and their locations, including both on-site and cloud storage. Make a list of all known hazards and dangers that you intend to evaluate. Ideally, you'll have a security baseline to compare the system configuration against.
- Define a baseline for the system: Draw up a thorough picture of the organizational structure, the applications and software currently in use, and the level of expertise held by those utilizing the IT assets. It will be simpler to identify weak points and prioritize solutions if you have a general understanding of how a business uses technology.
- Run a Vulnerability Scan: The following step is to run a vulnerability scan. This may be done using a variety of plug-ins and programs specifically made for vulnerability assessment. A vulnerability scan may identify configuration flaws as well.
- Produce a Vulnerability Report: Finally, put together a document that provides a summary of each vulnerability that has been found, as well as its possible effects and suggested mitigation measures.

Part 4: Determine, in general:

- Your risk assessment parameters (be clear about what you're evaluating, such as the product's lifespan, the physical region where the job activity occurs, or the sorts of dangers).

- The necessary resources (training a team of people to carry out the evaluation, the various kinds of information sources, and so forth).
- What type of risk analysis measures will be put in place? (How precise the scale or characteristics must be to deliver the most meaningful assessment?).
- Who are the parties involved? (Managers, supervisors, employees, labor representatives, suppliers, and so on).
- Local legislation, rules, codes, and standards, as well as corporate policies and procedures, are all relevant.

Part 5: After you've determined the priorities, the firm may choose how to manage each particular risk. The following categories are frequently used to classify hazard mitigation techniques:

- Elimination (including substitution) (including substitution).
- engineering constraints
- administrative measures
- devices for personal protection.

It's crucial to keep track of your assessment and any control measures you adopt. You might be obligated to keep evaluations for a certain period of time. Look up the regulations within your authority.

The extent of keeping records or documentation will be determined by:

- The amount of danger that exists.
- Laws and regulations.
- Requirements for any existing management systems.
- Your records must demonstrate that you:
- Successfully completed a hazard analysis.
- Assessed the dangers' potential risks.
- Implemented risk-appropriate control mechanisms.
- Reviewed and kept an eye on all workplace dangers.

7.3 Framework Alignment Evaluation

There are five primary frameworks [4]:

1. COSO Framework: The COSO Framework provides a framework for establishing internal controls that will be incorporated into business operations. These controls, taken together, give reasonable confidence that the company is functioning ethically, transparently, and in compliance with industry norms. COSO stands for Association of Sponsoring Organizations. The framework was developed in 1992 by a team chaired by Executive Vice President & General Counsel James Treadway, Jr., in collaboration with many private sector entities, including the following:
    - The American Accounting Association (AAA)
    - International Association of Financial Executives
    - The Internal Auditors Institute
    - AICPA stands for the American Association of Certified Public Accountants.
    - The Institute for Management Accountants (previously the National Organization of Cost Accountants) is a professional accounting organization.

2. COBIT: The COBIT business approach entails connecting business objectives with IT infrastructure by offering multiple maturity models & metrics that assess performance while defining related business obligations of IT operations. COBIT 4.1's core emphasis was shown using a process-based model segmented into four distinct domains, including:
    - Organization and planning
    - Providing and Support
    - Purchasing and Implementation
    - Evaluating and Monitoring

This is all further explained by 34 procedures based on the particular line of duties. COBIT is a well-known business framework that has been recognized by several international standards, notably ITIL, CMMI, COSO, PRINCE2, TOGAF, PMBOK, TOGAF, & ISO 27000. COBIT serves as a guideline integrator, bringing all options under one roof.

3. ISO 27001: The ISO framework contains a set of rules and practices that business may utilize. ISO 27001 establishes a framework to assist businesses of any size or industry in protecting their information in a methodical and cost-effective manner by implementing an Information Security (ISMS). ISO 27001's fundamental purpose is to safeguard three types of information:

    - Confidentiality: only authorized individuals have access to information.
    - Only authorized individuals may modify the information.
    - Availability: The data must be available to authorized personnel at all times.
    - A Management System for Information Security (ISMS) is a collection of guidelines that a business must follow in order to:
    - Identify stakeholders & their information security expectations of the firm.
    - Determine the hazards associated with the information.
    - To achieve the defined requirements and manage risks, develop controls (safeguards) as well as other mitigation strategies.
    - Set clear goals for what has to be accomplished in terms of information security.
    - Implement all risk management controls and methodologies.
    - Continuously assess if the installed controls are performing as planned.
    - Continuously enhance the overall performance of the ISMS.

4. ITIL 4 presents four aspects that must be addressed while providing a service or products. This guarantees that the whole company is considered, preventing

wasteful operations. It encourages businesses to chart the four dimensions anytime they develop a product or service so giving a framework for long-term strategic strategy. The four dimensions replace the Four Ps of the previous edition, ITIL 3. (Products, People, Partners, Processes).

ITIL 4's four dimensions are as follows:

- Organizations and Individuals — This dimension is based on the organization's structure and governance, as well as the people participating in every area of the service. Suppliers, customers, workers, and supervisors are all included.
- Organizations should think about how their teams are linked, the quality of training, and the sort of organizational culture they have.
- Information & Technology — This aspect refers to the tools, information, and information required to enable product delivery as well as IT management and governance. Considerations could include support service's skills and capacity, as well as the technology necessary for the service.
- Partners & Suppliers — This component focuses on the external partners and suppliers who assist enterprises in delivering goods and services. A crucial component of this dimension is the comparison of the in vs outsourced skills. Organizations should think about and assess outsourcing costs, as well as dependability, performance, and capacity.
- Value Streams & Processes – This dimension is concerned with the delivery of services and goods. The notion of a Value Chain, the operational model for delivering services or products, is introduced in ITIL 4. The Value Delivery Chain will be discussed in more depth later in the article, but it may be utilized for both incident response and product creation.

5. The NIST 800-53 structure provides a variety of controls and guidelines across numerous access and safety control families defined by a baseline of effect. These baselines are distinguished by:
    - Significant influence
    - Medium influence
    - Impact is minimal.

    The measures are then classified into 20 different control and security families. We've included examples of related controls beside them.
    - AC (Access control): User administration and monitoring, implementing the concept of least privilege, and separating roles.
    - AT (Awareness and training): Supplying staff with awareness and security training, as well as advanced technical instruction for more privileged users.
    - AU (Audit & accountability): Assessing and keeping records, as well as providing accompanying analysis and reporting.
    - CA (Assessment, authorization, and monitoring): Penetrating public networks & monitoring connections to other systems.
    - Configuration management (CM) is the process of implementing attempt to change controls and establishing permitted software rules.
    - CP (Contingency planning): Creating & testing business continuity plans, as well as other processing and storage options.
    - IA (Identification & authentication) is the process of managing credentials and implementing authentication rules and systems for people, devices, and services.
    - Individual involvement (IP) is the process of obtaining permission and approving privacy rules and practices.
    - Setting up incident management training as well as accompanying reporting and monitoring systems (IR).

- MA (Maintenance): The continuing maintenance of a system, staff, and tools.
- MP (Media protection) is the process of securing and safeguarding media access, usage, storage, and movement.
- Setting rules for collecting, utilizing, and exchanging personally identifiable information (PA) (PII)
- PE (Physical and ecological protection): Ensuring emergency power access, safeguarding physical access, and defending against physical danger and harm.
- PM (Professional): Having established risk management, insider threat, and scalable architectural techniques.
- PL (Planning): Having comprehensive security architecture solutions in place (such as defense in depth and third-party vendor security)
- PS (Personnel security): Assessing both internal and external employees, as well as establishing termination & transfer security procedures.
- RA (Risk assessment): Vulnerability scanning, continuing privacy impact assessments, and risk assessments.
- SA (System & services acquisition): Putting security in place throughout the system's lifecycle, as well as new vendor contracts and acquisitions.
- SC (System & communications protection): Application partitioning, cryptographic key management, and password and other sensitive data security.
- System and data integrity (SI) is the implementation of system monitoring, warning systems, and fault correction procedures.

7.4 Creating Information System Contingency Plan

7.4.1 Analysis of Business Impact

1. A business impact assessment (BIA) is a methodical procedure for determining and evaluating the probable consequences of a disruption in vital company activities caused by a catastrophe, accident, or emergency. A business impact analysis (BIA) is an integral component of every organization's business continuity strategy (BCP). It contains an exploratory element to identify risks and vulnerabilities, as well as a planning element to design risk-mitigation measures. The final outcome is indeed a business impact study report that explains the possible hazards unique to the enterprise under consideration.

One of the fundamental assumptions underlying a BIA is that each component of the organization is dependent on the continuing operation of the others. Some, however, are more critical than others and need a bigger deployment of operational and financial resources in the case of a crisis [12].

A costing system for proposed additional or improved controls includes the following:

- calculating the effect of adopting new or improved controls
- calculating the effect of not installing new or improved controls
- Estimating the implementation expenses. Among them include, but aren't restricted to, the following:

❖ Purchases of hardware and software
❖ Compromised operational effectiveness if performance of the system or functionality is reduced in order to improve security.
❖ The cost of introducing new rules and processes Hiring more people to execute recommended rules, procedures, or services
❖ Training expenses
❖ Maintenance expenses

- Assessing the implementation benefits and expenses against data and system criticality to identify the relevance of adopting new controls to the company, given their costs & relative effect.

  The security needs checklist is the result of this approach. The following official regulatory & security guidelines, as well as sources related to the IT systems processing environment, may be utilized to compile such a checklist:

❖ CSA of 1987
❖ Publications on Federal Data Processing Standards
❖ OMB Circular A-130, November 2000
❖ 1974 Privacy Act
❖ The IT system's security strategy was evaluated.
❖ The security policies, procedures, and standards of the organization
❖ Industry customs

It is the responsibility of the information and system owners to ensure that sufficient controls have been established to address the integrity, confidentiality, & availability of the computer systems and data that they hold. Changes to their Computer systems are typically the responsibility of the information and system owners. As a result, they must normally authorize and sign off on modifications to their IT system (e.g., system enhancement, major changes to the software and hardware). As a result, system and data owners must recognize their role inside the process of risk management & fully support it.

2. Organizations may assess the degree of risk reduction created by new or improved control in terms of decreased threat probability or effect, two factors that characterize the level of danger to the corporate mission.

Implementing new or improved controls may reduce risk by

- By removing some of the system's vulnerabilities (flaws and weaknesses), the number of probable threat-source/vulnerability pairings is reduced.

- Including a targeted restriction to minimize a danger source's capabilities and motivation

  For example, a department finds that the expense of installing and keeping add-on security software for the stand-alone PC where sensitive data are stored is not justified, but that administrative and physical measures should be introduced to make physical access to the that PC extremely hard (e.g., store the PC in a locked room, with the key kept by the manager).
- Reducing the scale of the negative effect (for example, restricting the scope of the a vulnerability or changing that nature of the connection between both the IT system as well as the purpose of the company).

  The residual risk is the risk that remains after the deployment of new or improved controls.

No IT system is completely risk-free, and not all applied safeguards can completely remove or decrease the overall risk to zero. According to Budget Circular A-130, an organization's senior management or the Das, who are in charge of preserving the organization's IT assets and purpose, must approve (or accredit) the IT systems to commence or continue operations. This permission or certification must take place at least every three years or whenever important improvements to the IT system are implemented. The goal of this procedure is to identify hazards that have not been adequately handled and assess if further controls are required to minimize the risks found in the IT systems. After the relevant controls for the risks identified have been implemented, the DAA will sign a declaration admitting any residual risk & permitting the operations of the new computer system or the ongoing processing of the current IT system. If the risk rating hasn't been reduced to a satisfactory amount, the risk assessment cycle must be restarted in order to find a means to decrease the remaining risk to acceptable levels.

3.

Magnitude of Impact	Impact Definition
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

4. The outcomes of the risk assessment (threat sources & vulnerabilities identified, risks evaluated, and proposed controls supplied) should be recorded in an official police report or briefing. A risk assessment document is a project from inception that assists upper leadership, the mission owners, in making policy, procedure, budget, & systems operational and management choices. A risk assessment report, unlike an auditor or investigation report, should not be portrayed in an accusing way, but rather as a methodical & analytical approach to analyzing risk so that top management understands the risks and allocates resources to prevent and repair possible losses. As a result, some individuals prefer to treat the threat/vulnerability combinations in the risk evaluation report as observations rather than results. An framework for the risk evaluation report is provided in Appendix B.

5. Controls that identify violations or attempted breaches of security policy include audit trails, penetration detection techniques, and checksums. To recover lost computer resources, recovery controls may be employed. They are required as a supplement to the supportive and preventative technological measures, since none of the other measures are flawless. Controls for detection and recovery include—

- Audit. The auditing of safety events, as well as the tracking and monitoring of system irregularities, are critical components in the identification and recovery from security breaches after the fact.
- Detection and containment of intrusions. It is critical to identify security breaches (e.g., system breaches, suspicious activity) in order to respond in a timely way. It's also pointless to identify a security violation if no meaningful reaction can be launched. These two skills are provided by intrusion detection and confinement control.
- Evidence of completeness. The proof-of-wholeness control (for example, a system integrity tool) examines system integrity and irregularities, identifying exposures and possible dangers. This control doesn't really prevent breaches of security policy, but rather identifies them and assists in determining the sort of remedial action required.
- Return to the Secure State. Following a security compromise, this service allows a system to restore to a known secure state.
- Virus detection and removal. Virus detection and removal software placed on servers & user desktops detects, identifies, & eliminates software viruses to guarantee the integrity of the system and data.

7.4.2 Plan for Incident Response (IRP)

1. A brief summary:

An incident response strategy is a collection of instructions designed to assist IT personnel in detecting, responding to, and recovering from network security issues. These strategies address risks such as theft, data loss, & service disruptions that affect everyday operations. A proper event response plan provides a plan of action for any and all major situations. Some accidents result in large network or data breaches, which may have a long-term effect on your firm. When a substantial interruption occurs, your firm need a complete, detailed incident response strategy to assist IT workers in promptly stopping, containing, and

controlling the problem. Create a plan for disaster recovery for physical disruptors such as natural catastrophes and floods.

2. Responsibilities and roles (from the end user to the CISO):

- Implementing and managing your company's cybersecurity program
- Bringing cybersecurity and business goals together
- Cybersecurity reporting
- Surveillance of Incident Response Activities
- Business continuity and catastrophe recovery management
- Encourage a robust information security culture.
- Relationship management with vendors
- Effective use of cybersecurity funds
- Managing the organization's cybersecurity employees
- Cybersecurity education and training

3. Reporting requirements:

I. Form a cybersecurity response team for incidents.
The size of your CIRT is determined by the size of your firm, the likelihood for data loss, as well as its global reach. However, designate a crew chief who will be responsible for responsibility of reacting to and dealing with an event.
Pay particular attention to CIRT coaching: each CIRT member should be familiar with your organization's core cybersecurity policies and processes, as well as their specialized duties in the event of an attack.

II. Plan out all processes ahead of time.
Among the most popular attack vectors are:

- Media that is external or detachable (for instance, an infected USB device)
- Equipment loss or theft (a lost corporate laptop or authorization token)

- Web (attacks performed from a web application) (attacks executed from a web application)
- Email sabotage (emails with a link to a malicious website)
- Impersonation (spoofing & man-in-the-middle attacks) (spoofing and man-in-the-middle attacks)
- Incorrect use (access misuse)
- Attrition (brute-force assaults) (brute-force attacks)
- Other (all other assaults) (all other attacks)

III. Keep track of user and network activities.

Monitoring everything that occurs on your network is one of the finest strategies to avoid a possible attack. Consider installing the user activity monitoring system to handle the issue of insider threats and security concerns associated with subcontractors. By monitoring individual user behavior as well as network activity, you can:

- Early detection and termination of an assault
- Gather proof and important data for later examination.

You may go even farther by implementing a system that includes behavioral user tracking capability. Such systems may identify abnormalities and variations from baseline user activity inside the monitored infrastructure using AI-powered technologies. Build a threat intelligence incident management strategy to limit your own organizational risks.

When selecting a user activity health monitoring system, seek for one with a flexible incident management mechanism. Setting bespoke real-time notifications and automating at least certain SOPs can help you respond to cybersecurity events in a timely manner.

IV. Start taking care of backups & recovery plans.

As with resolving an event, it is preferable to consider recovery from an incident first before breach occurs, and to provide specific examples on data recovery methods for various circumstances.

Restored service. Following an event, the following two stages are crucial for returning your organization's systems to regular operation:

- Check the network to make sure that almost all systems are up and running.
- Recertify any systems and components that may have been impacted by the event as operable.

V. What to consider while revising your incident response strategy

Whenever your company undergoes a big shift, whether it is entering a new market or modifying its core systems, these adjustments should be reflected in your IRP.

- New attack vectors & security issues affecting your company
- Local & industry cybersecurity standards are being updated and changed.
- Lessons from prior breaches and assaults
- Procedures for addressing incidents and solutions that may be enhanced

4. Diagram of example processes - from event to resolution

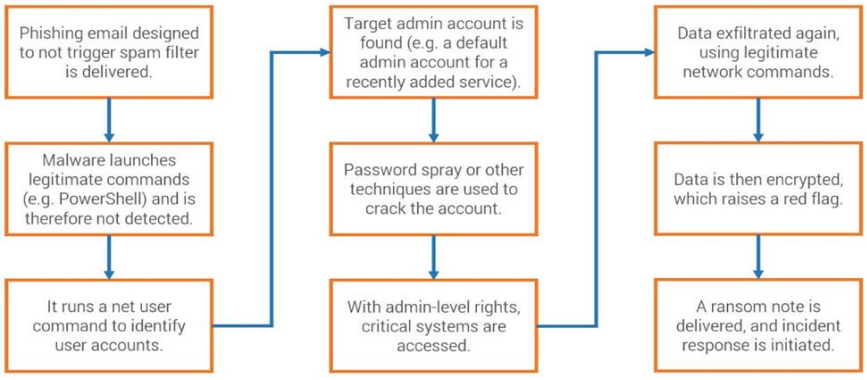


Figure 7.4.1: From occurrence to conclusion

5. Explain the six phases of incident management as they apply to the company:

I. Preparation

An effective response to an incident outlines the measures a company should take far in advance of a disruptive occurrence. The strategy starts by explaining how a company might decrease the likelihood of a data leak. The planning step should link corporate data protection policies with security objectives and technology defenses. You must, at the very least, guarantee that personnel have undertaken information security personnel awareness training. They should ideally also obtain incident response training. Similarly, you should conduct a system audit to verify that your critical data is securely safeguarded.

II. Identification

The second clause of incident management planning refers to the actions taken by a company to determine whether its assets have been hacked. You are better able to stop an infiltration if you can detect it soon. Even if it isn't feasible, you can speed up the reaction and reduce damage, save you money and time.

When determining a security issue, you should consider the following:

- Who found the hole?
- What is the magnitude of the breach?
- Is it having an impact on our operations?
- What is the root of the stalemate?

III. Containment

The third phase discusses the procedures you can take to limit harm once you've been infiltrated. Depending on the circumstances of the situation, this may include removing the criminal hackers from your networks or isolating an already compromised data. During this stage, examine if systems should be taken down or

removed, as well as whether there are any urgent measures you can take to address vulnerabilities.

IV. Eradication

The fourth phase of a cybersecurity incident response strategy focuses on repairing the flaw that allowed the security leak to occur. The details will vary on the sort of occurrence, but at this point, you must determine how the data was leaked and how to eliminate the danger. If your firm was infested with malware, for instance, you would uninstall the bad software & isolate the afflicted areas. Meanwhile, if the assault was carried out because a criminal hackers obtained an employee's login credentials, their account would be frozen.

V. Recovery

Once the danger has been eliminated, you may proceed to the last step of cyber event response, which is restoring your systems to operational status. This may be more complicated in some cases than the others, but it is an important element of the process that ought to be handled with care. Without a suitable recovery procedure in place, you may stay exposed to similar assaults, compounding the harm. Once the problem has been resolved, you should test & monitor the impacted systems as a component of the recovery process. This guarantees that the procedures you implement function as planned and allows you to remedy any errors.

VI. Learning experiences

The last step in the cyber response strategy is to assess the event and identify areas for improvement. Everyone on your incident management team should gather to discuss whether elements of the plan succeeded and what challenges you experienced.

6. This presentation shows a flowchart of the problem and escalation process, which includes the numerous processes involved in this procedure. To raise your presentation level, introduce Escalation Administration System Problem and Instigation Process Flow Chart. With six levels, this design is an excellent choice for educating and enticing your audience. Using this template, disseminate information on discovery, validation & prioritization, analysis, monitoring and reporting, resolution & closure, and escalation. Take use of it right now to get the maximum advantages.

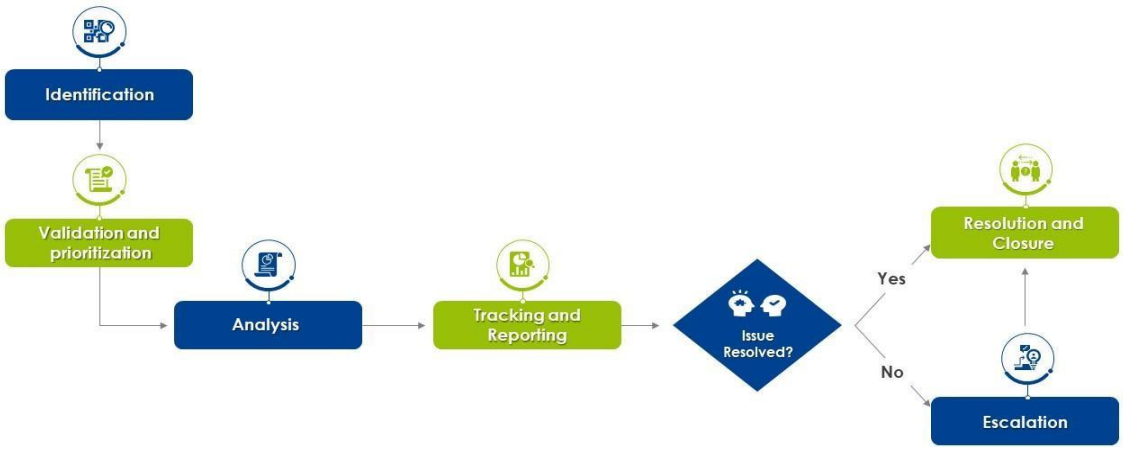


Figure 7.4.2: Diagram of the issue and escalation procedure

7.4.3 Plan for Disaster Recovery (DRP)

1. Purpose:

   A disaster recovery plan's objective is to thoroughly describe the consistent measures that must be performed before, during, and following a natural or man-made catastrophe so that the whole team can implement those actions. A plan for disaster recovery should handle both purposeful and unintentional man-made catastrophes, such as the consequences from terrorists or hacking, as well as accidental disasters, such as equipment failure.

2. Scope:

   Identifying essential IT network systems, prioritising the RTO, and describing the processes required to restart, reconfigure, & recover networks and systems are all part of a DRP checklist. The strategy should at the very least limit any negative impact on company operations. In the case of an unanticipated occurrence, all staff should be familiar with basic emergency procedures.

3. Responsibilities and roles:

   A plan for disaster recovery (DRP) is a written, organized method that specifies how an organization may restart operations swiftly after an unanticipated occurrence. A disaster recovery plan (DRP) is an integral part of a company's continuity strategy (BCP). It refers to parts of an organization that rely on a working information and technology (IT) infrastructure. A DRP tries to assist an organization in resolving data loss and recovering functions of the system so that it may continue to operate inside the aftermath of an event, even if at a low level.

   The plan comprises of procedures to mitigate the consequences of a catastrophe so that the organization can continue to function or restart mission-critical tasks as soon as possible. A DRP typically includes an examination of business operations and continuity requirements. An organization often does a business impact assessment (BIA) & risk analysis (RA) before developing a comprehensive strategy, and it creates recovery targets.

   As cybercrime & security breaches grow more complex, organizations must establish their data recovery & protection policies. The capacity to manage events rapidly may decrease downtime & minimize reputational and financial harm. DRPs also assist firms in meeting regulatory obligations while also giving a clear path to recovery.

4. Resources required:
    - budget
    - insurance protection
    - People & physical facilities are examples of resources.
    - risk management strategy of the management team
    - technology
    - information and data storage
    - suppliers
    - conformity requirements

5. Once corporate decision-makers acknowledge the importance of training, ensuring that the signal is transmitted from the bottom so that workers know that training is serious business and also that attendance or engagement is needed. Here seem to be a few short protocols that all staff should be aware of:
    - If they need to telecommute until the emergency scenario passes, they must access to the VPN or the firm cloud service
    - How to contact other staff if needed (all staff must be given a list of their names and contact information.)
    - How to get access to other methods of communication, like an urgent voicemail recording that delivers scenario updates to staff

6. Schedules for exercise and testing:

    DRPs are validated via testing to uncover flaws and give opportunity to address issues before a crisis happens. Testing may provide evidence that an emergency response strategy is successful and meets RPOs and RTOs. Because IT technologies and systems are continually developing, disaster recovery testing ensures that a disaster recovery strategy is up to date. Budget limits, resource constraints, as well as a lack of management permission have all been cited as

reasons for not testing DRPs. Time, money, and preparation are required for DR testing. It may also be dangerous if the test includes the use of live data.

The difficulty of DR testing varies. A thorough debate of the DRP is conducted during a plan review to check for missing items and discrepancies. Participants in a tabletop test move through plan actions step by step to show if DR team members understand their responsibilities in an emergency. A simulation test employs resources such as restoration sites & backup systems to perform a full-scale test in the absence of a genuine failover.

7. Schedule routine maintenance:

   When developing a disaster response maintenance plan, ensure that top management reviews and approves it. The following are key actions for good disaster recovery plan maintenance:

   Create a continuous maintenance schedule for your operations. Risk assessments, financial impact analyses (including updates to current risk assessments & BIAs), program reviews, planned exercises, address book updates, and plan awareness and training initiatives will all be part of this.

   You may create basic maintenance routines using a worksheet; use the following categories as a starting point:

   - Coordination of disaster recovery maintenance efforts with current IT activities like as change management & hardware/software maintenance, as well as your help desk, is recommended.
   - Document all maintenance operations, including the date and time maintenance was completed, a description of maintenance activities, and any necessary approvals.

- To offer a secure archive for maintenance tasks, use existing corporate resources such as a Share-point Online collaboration area.
- Create frequent maintenance reports for management (for example, quarterly) that highlight the state of maintenance efforts and concerns that must be addressed.

7.4.4 Business Continuity Plan (BRP)

1. Both cold and hot sites offer safe off-site places that are unaffected by the majority of physical calamities that might cause the failure, such as harsh weather or fire. Both of these buildings have basic heating, air, air conditioning, and electricity operations, in addition to communications equipment.

Cold and warm sites are provided as external or internal services in a variety of ways. Organizations may have an inside hot site, which could serve as a data backup center or field office, if the resources exist. Maintaining regional offices or office area without server software or hardware is another privately owned approach for a business to have a disaster plan without a complete replica of a data center. There are other vendors who offer equipment and dedicated or shared hot or cold locations.

The key distinction between a hot and a cold site is readiness to go live. A hot site offers redundancy and is effectively a second computer system that will results in minimum to no downtime if data is recently backed up and all IT systems are operational. Setting up a cold site necessitates preparation for setup resources and time.

The Advantages of a Plan for Business Continuity

Businesses are vulnerable to a variety of calamities ranging in severity from small to catastrophic. Contingency planning planning is often intended to assist a firm in continuing to operate in the case of a significant calamity, such as a fire. BCPs vary from disaster

recovery plans in that they concentrate on the recovery of the a company's IT system following a catastrophe.

2. Many businesses must take numerous steps to create a good BCP. They are as follows:

- Business Impact Assessment: Here, the company will identify time-sensitive tasks and resources. (More on this later.)
- In this section, the company must identify and take procedures to restore vital business operations.
- The formation of a continuity team is required. This group will design a strategy to deal with the interruption.
- Training and testing are required for the continuity crew. Team members should also do activities that review the plan and strategy.

3. The recovery approach should prioritize restoring or regaining what was lost during the catastrophe stage:

- People, processes, facilities, records, and equipment, among other things
- What has the tragedy taken away from the organization?
- What resources must be recovered in order for the company to perform its core business functions?
- How soon must these assets be available?
- How can these resources be obtained in a reasonable amount of time?
- What resources might the organization build or develop in advance of a disaster?
- Because the vital resource is assured, the approach provides the maximum degree of recovery certainty.
- Facilities, such as a hot site, might be developed so that critical services can be restored quickly following a catastrophe.

An company that does not want to possess extra resources may lease them. Some groups may decide to acquire resources solely in the event of a calamity. Consider regaining the

resources required to continue important company activities while establishing a recovery plan. It is helpful if you bear in mind that restoration is within the RTOs for these critical activities.

4. Plans for business continuity include recognizing all potential hazards to the company's operations. The strategy should also evaluate how such risks would effect operations and put protections and procedures in place to reduce them. There must also be testing methods in place to confirm that these precautions and procedures are effective. Finally, a review procedure should be implemented to ensure that the plan remains up to date.

A contingency planning impact study, which evaluates the implications of interruption of company operations and processes, is an essential aspect of building a BCP. It also makes judgments on recovery priorities and tactics based on the information. To assist in doing a business continuity study, FEMA offers an operational and economic impact worksheet. These files describe the financial and operational consequences of the loss of certain corporate services and processes. They also determine when the absence of a process or function might have the specified business consequences.

5. Business continuity plans (BCPs) and disaster recovery plans (DRPs) are similar in essence, with the latter focusing on information and technology technology (IT) infrastructure. BCPs are broader in scope, concentrating on the whole enterprise, such as customer support & supply chain.

BCPs are concerned with lowering total expenses or losses, whereas disaster recovery plans are mainly concerned with technology outages and associated expenses. Only IT people, who establish and monitor the policy, are often involved in disaster recovery plans. BCPs, on the other hand, tend to have additional staff educated on possible procedures.

6. Testing is a critical element in continuing BCP management. How should you test your business continuity plan? And, at what point in the contingency planning lifecycle should we test the continuity plan?

Of course, the true litmus test is an occurrence. However, conducting contingency planning drills will provide you with the certainty that the plan is strong enough to tackle a genuine disaster, and it will allow you to assess this in a less stressful manner than preparing for a true crisis.

- Planning for business continuity (BCP) refers to the basic actions that a company takes to develop a recovery and preventive strategy against possible risks such as natural catastrophes or cyber-attacks.
- Business plan, organization, recovery, and training are all phases that businesses must take while developing a Business Continuity Plan.
- BCPs are intended to safeguard assets and workers so that they can resume normal operations as soon as a crisis hits.
- BCP should consider how these risks may impact operations.
- BCP should put in place protections and processes to reduce risks.
- BCPs should be checked on a regular basis to verify that there are no obvious weaknesses that can be detected and fixed.
- BCP should examine and test the procedure to make sure that it is functional and up to date.

There are three basic forms of business continuity testing: table-top exercises, organized walk-throughs, and comprehensive catastrophe simulation testing. First, to begin, table-top or position exercises enable everyone engaged in the plan to go over it & identify potential missing steps, inconsistencies, or inaccuracies. Second, a stroll is a more thorough examination of your strategy, with everyone engaged reviewing their individual duties to identify any flaws. Third, a comprehensive catastrophe simulation takes a step further, establishing a scenario that mimics a real disaster to assess if your strategy allows you to continue operating. It ought to include your entire department as well as any suppliers or important external partners, such as security or maintenance firms.

7.5 PowerShell Security Automation

7.5.1 PowerShell Installation:

1. Check the PowerShell version using Get-Host or $PSVersion Table [6]:

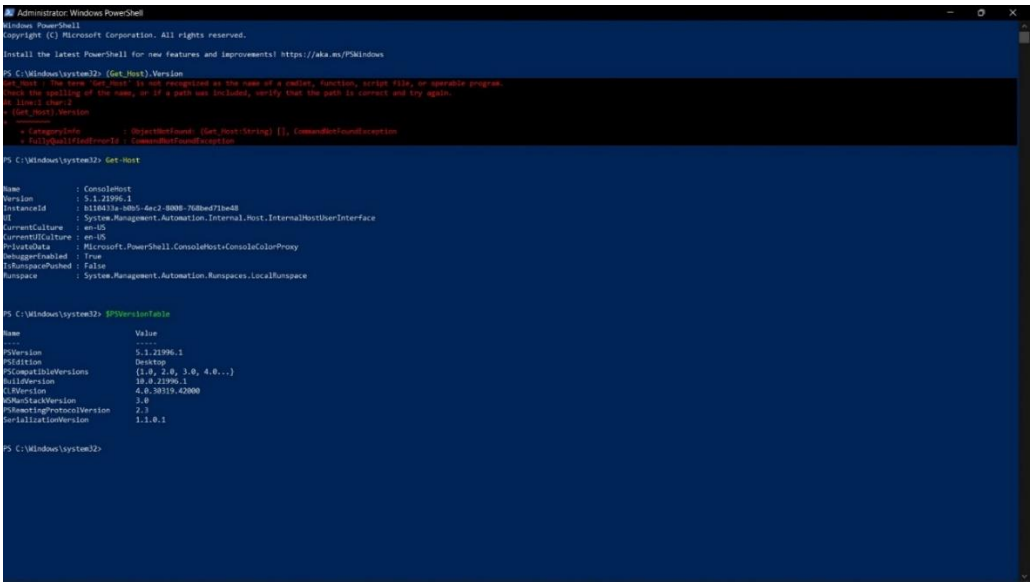


Figure 7.5.1: Get-Host or $PSVersion

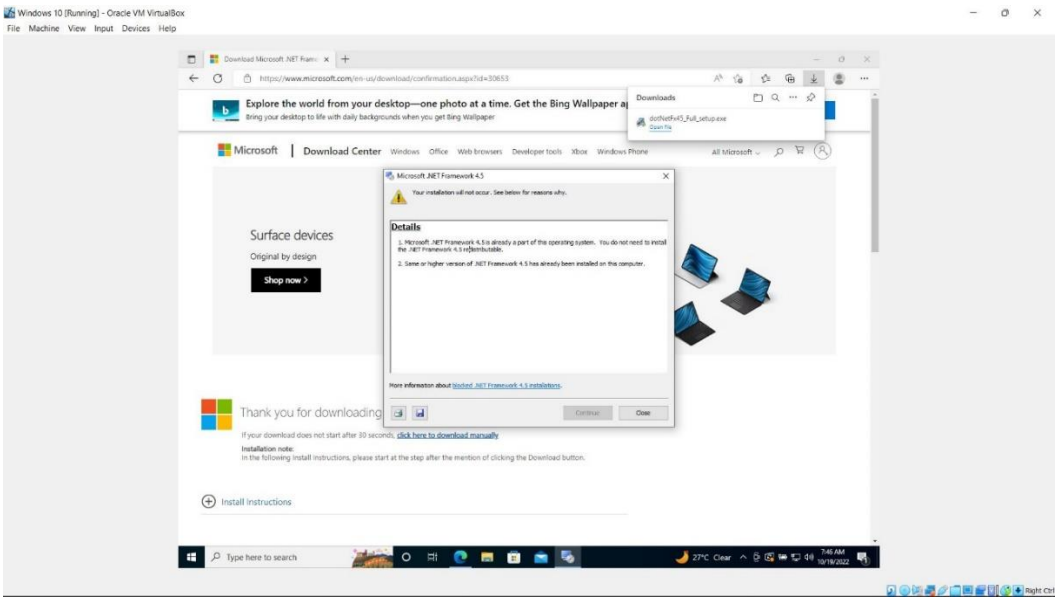


Figure 7.5.2: Get-Host or $PSVersion

2. Using Get-ExecutionPolicy, you may test the ability to execute scripts [6]:

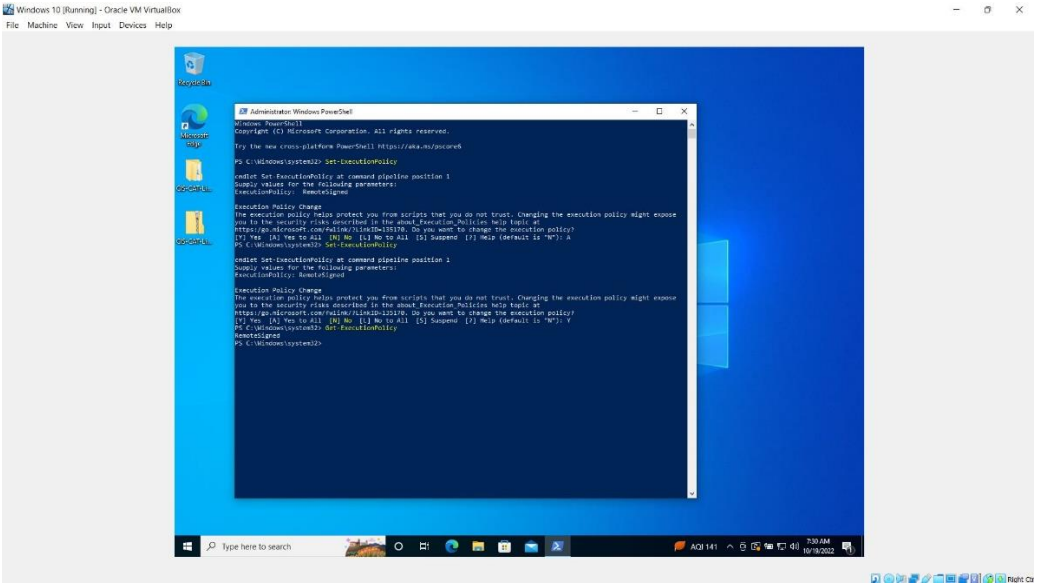


Figure 7.5.3: Get-ExecutionPolicy

7.5.2 File and Do Internet Research to Construct a Script:

1. Source: Member Server Make a folder called C:ITT430-Files:

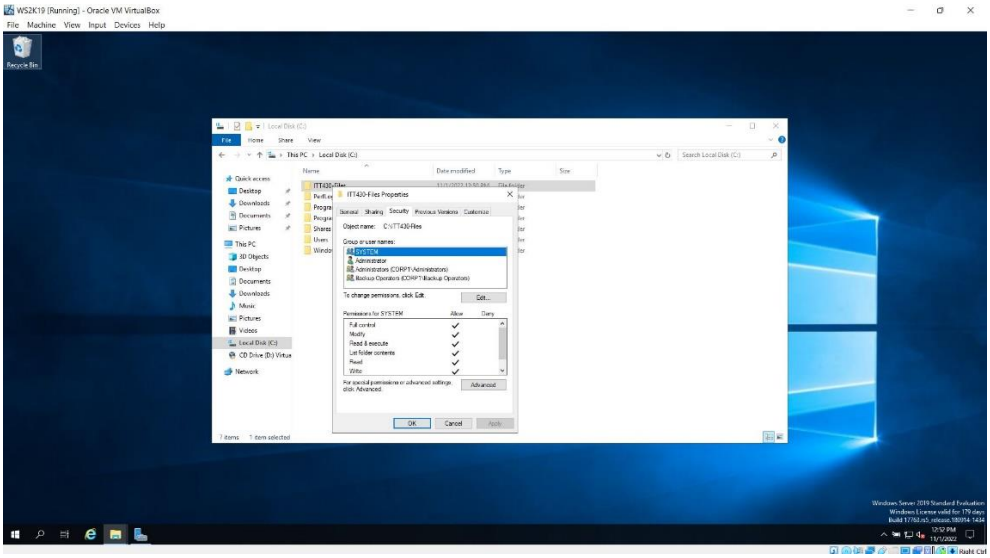


Figure 7.5.4: Internet Research and File

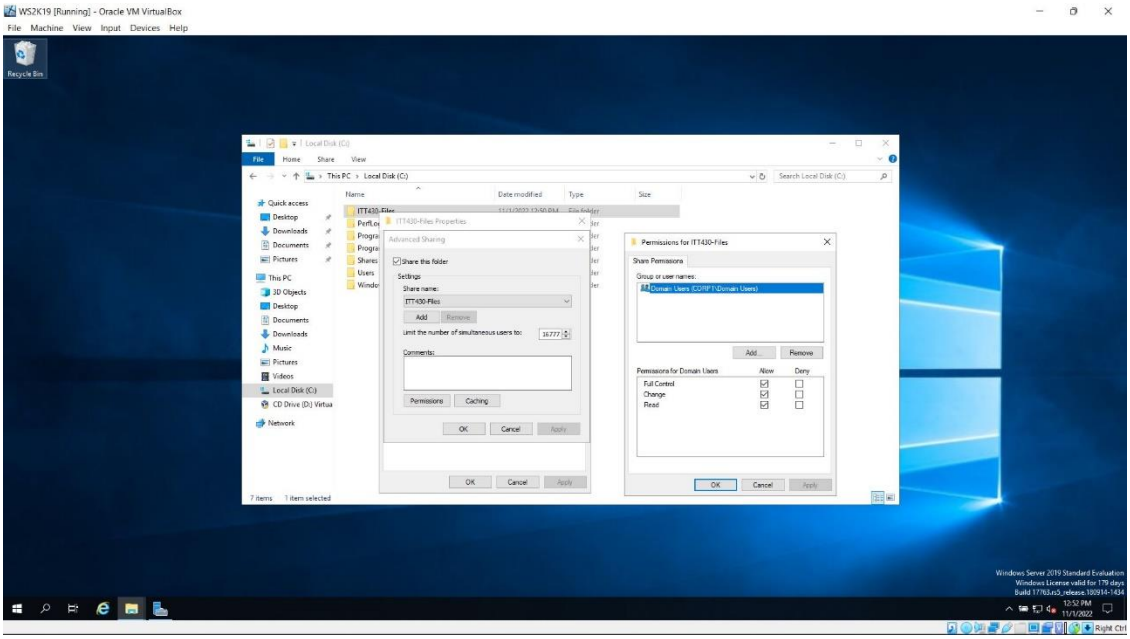


Figure 7.5.5: Internet Research and File

2. Transfer Server (recipient): Make a folder called C:ITT430-Storage. Share this folder with the rest of your domain:

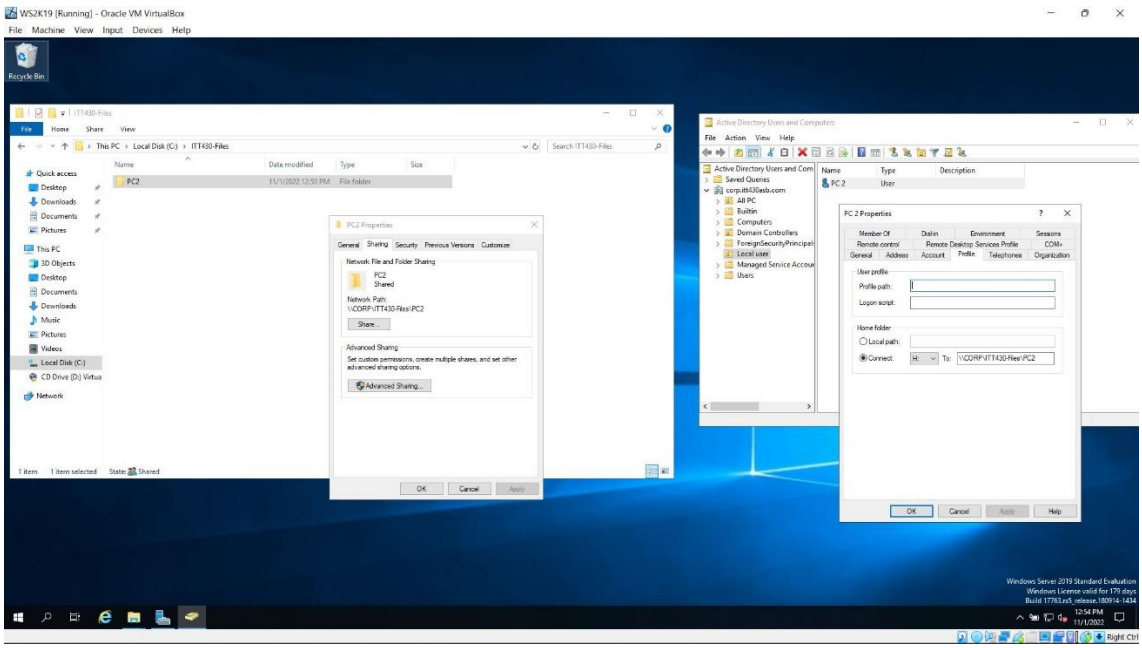


Figure 7.5.6: Subdirectory in the same directory as the rest of the domain.

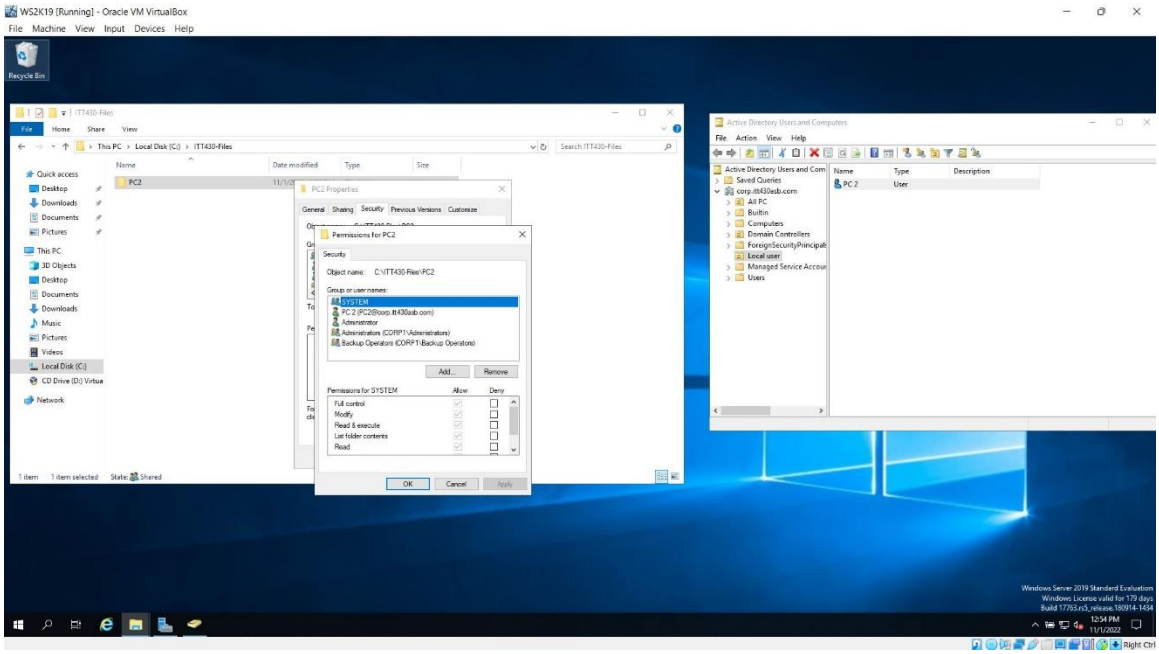


Figure 7.5.7: Subdirectory in the same directory as the rest of the domain.

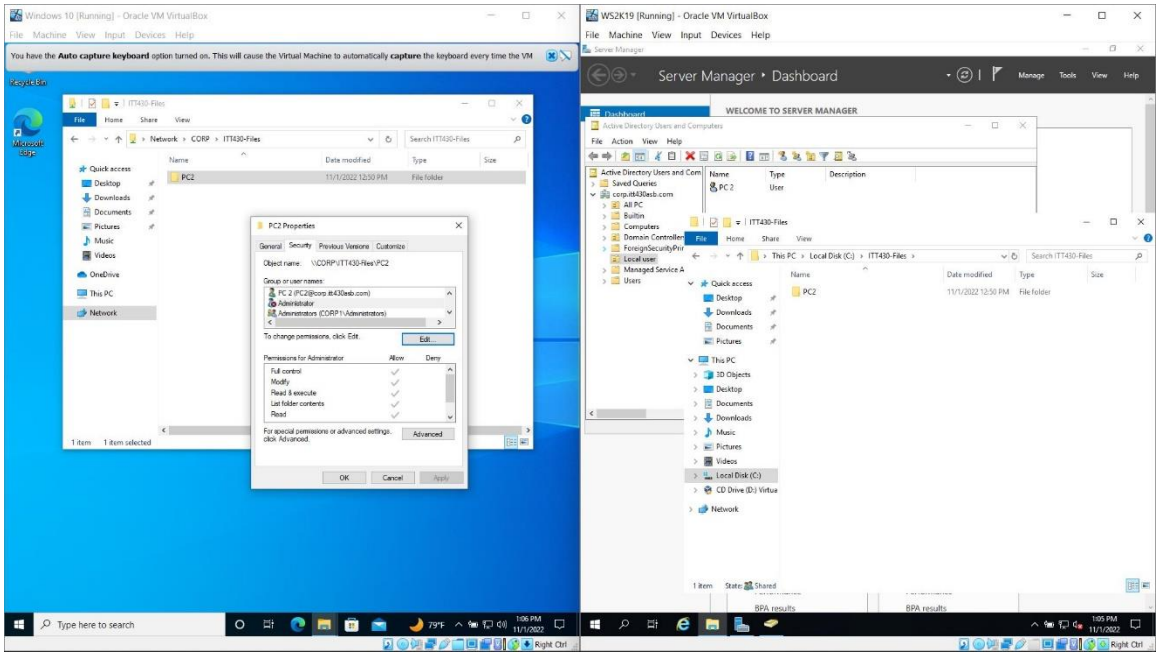


Figure 7.5.8: Subdirectory in the same directory as the rest of the domain.

3. Schedule the following job to run each hour:

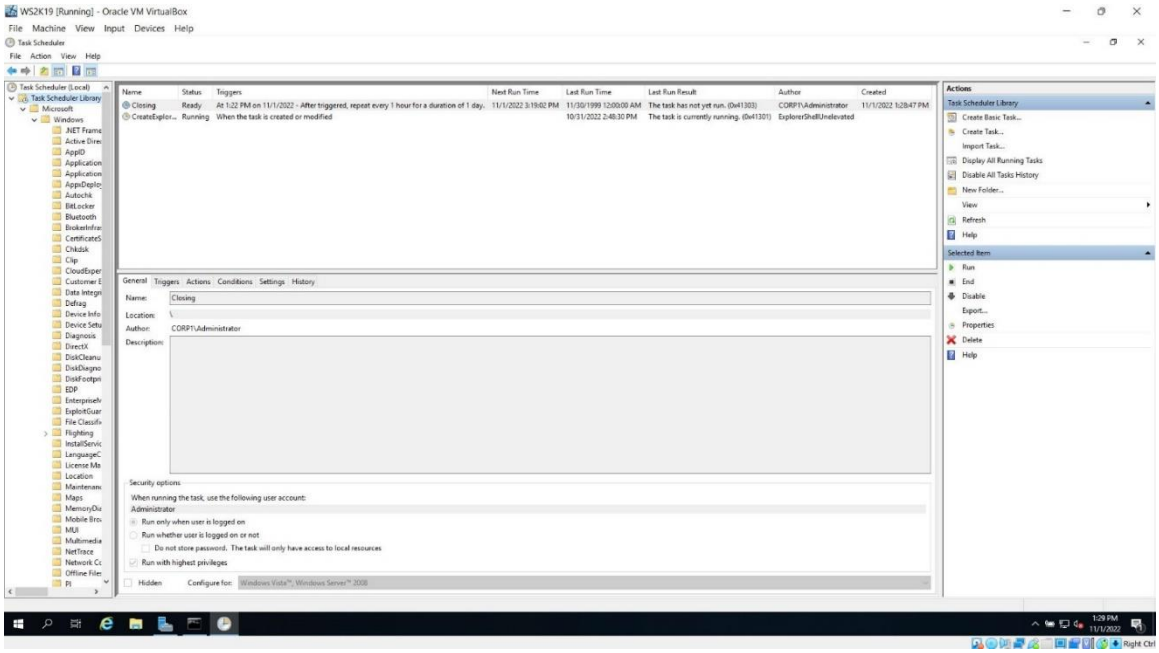


Figure 7.5.9: Job must be completed every hour

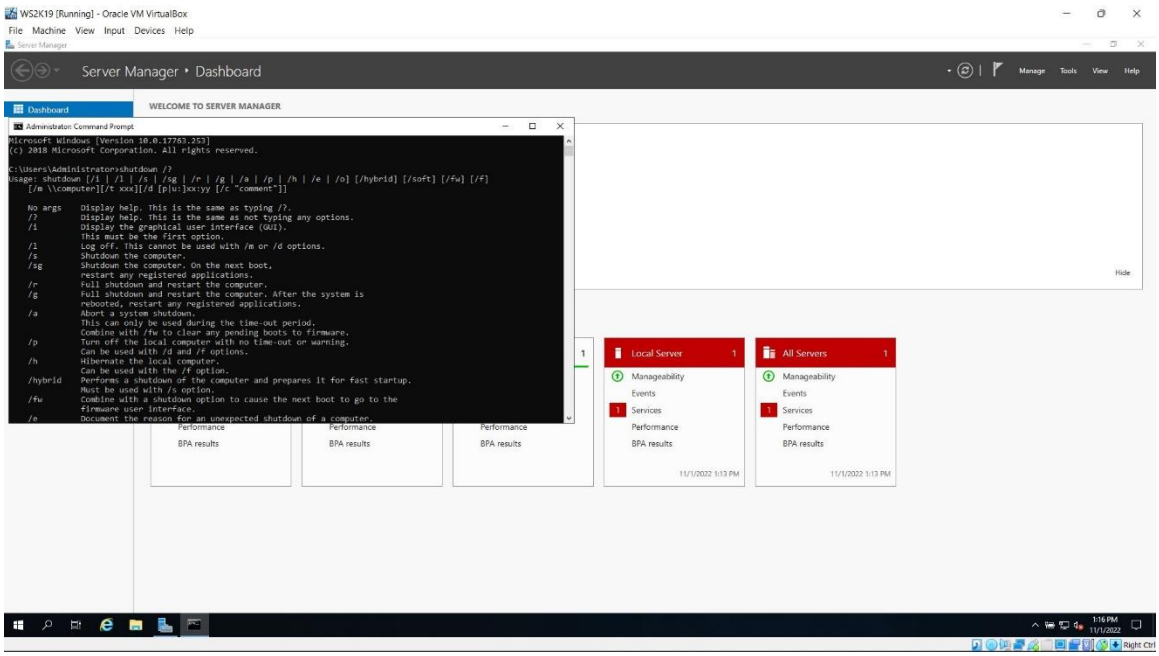


Figure 7.5.10: Job must be completed every hour

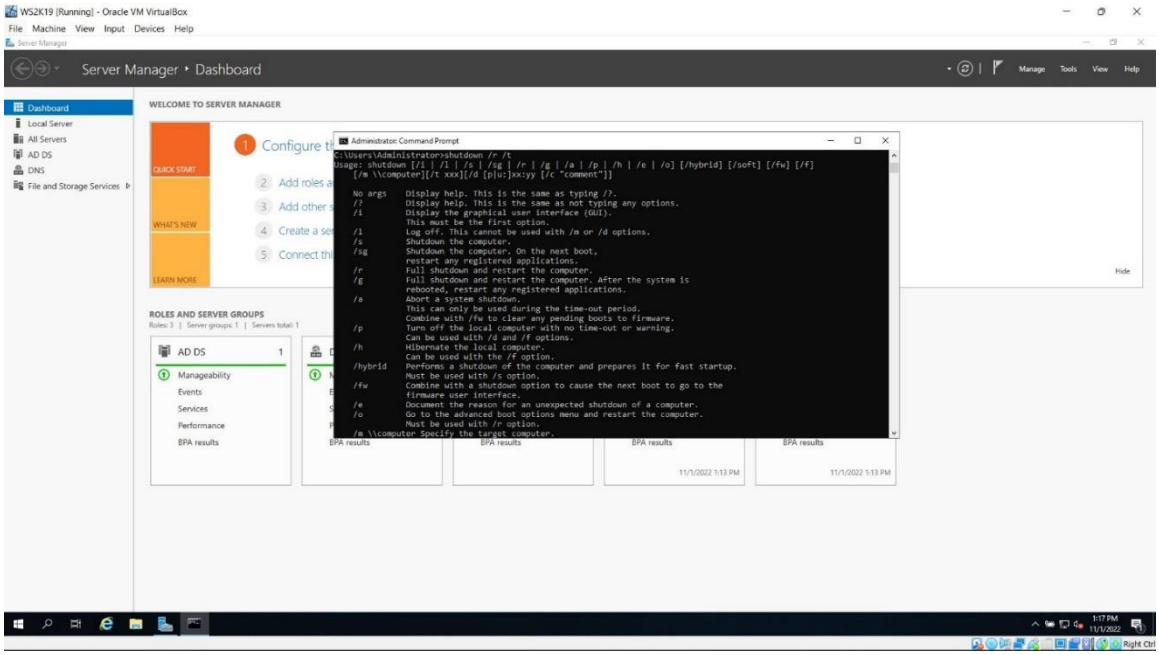


Figure 7.5.11: Job must be completed every hour

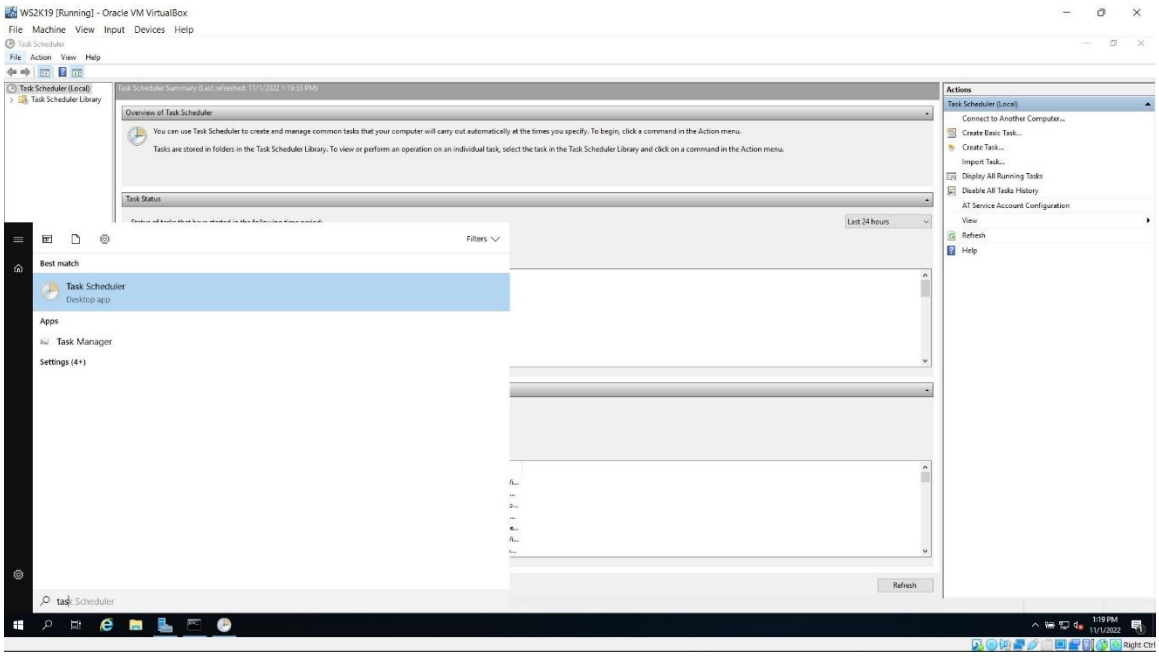


Figure 7.5.12: Job must be completed every hour

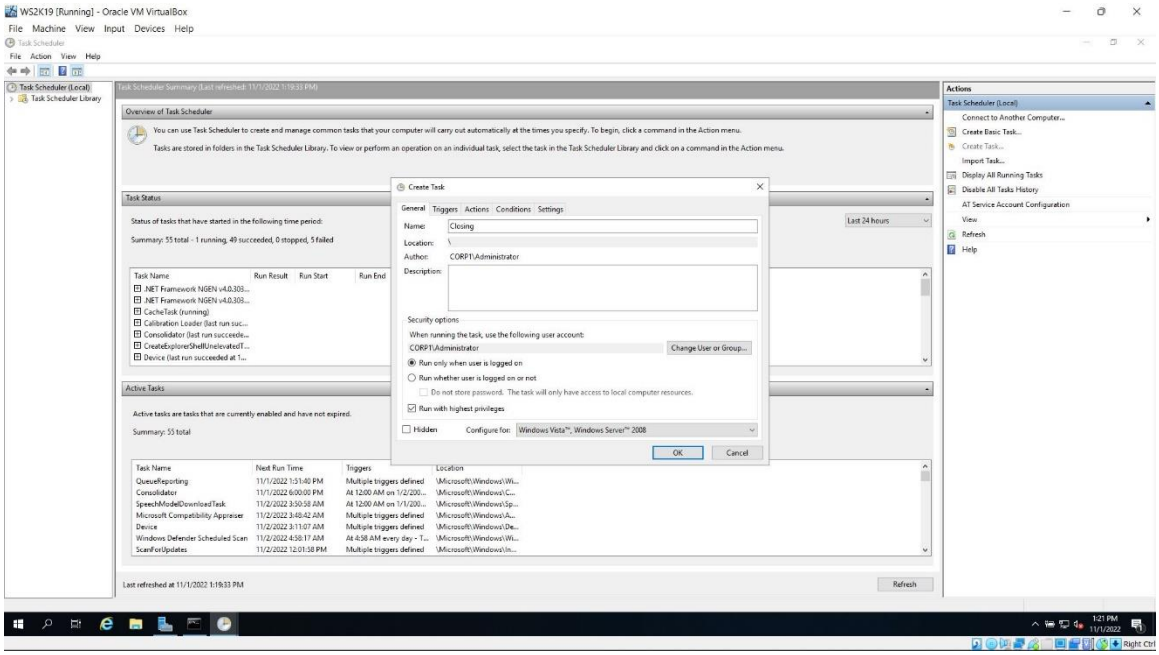


Figure 7.5.13: Job must be completed every hour

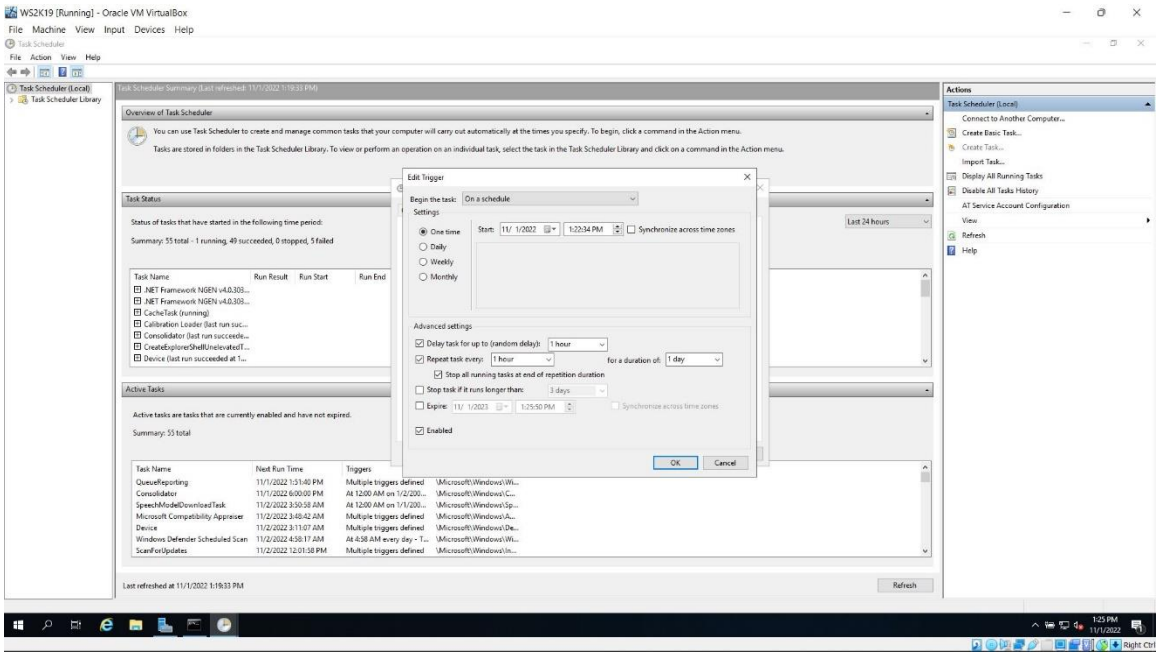


Figure 7.5.14: Job must be completed every hour

7.5.3 Create a script that deactivate Active Directory users who haven't signed in for 45 days:

```
# Gets time stamps for all User in the domain that have NOT logged in since after specified date


import-module activedirectory

$domain = "Your Domain Name"

$DaysInactive = 45

$time = (Get-Date).Adddays(-($DaysInactive))


# Get all AD User with lastLogonTimestamp less than our time and set to enable

Get-ADUser -Filter {LastLogonTimeStamp -lt $time -and enabled -eq $true} -Properties
LastLogonTimeStamp |


# Output Name and lastLogonTimestamp into CSV

select-object Name,@{Name="Stamp";
Expression={[DateTime]::FromFileTime($_.lastLogonTimestamp).ToString('yyyy-MM-
dd_hh:mm:ss')}} | export-csv OLD_User.csv -notypeinformation
```

CHAPTER 8

OVERALL WORK AND TESTING

Cybersecurity refers to the safeguarding of internet-connected equipment and services from harmful assaults by hackers, spammers, & cybercriminals. Companies employ the approach to guard against phishing attempts, ransomware, identity theft, data leaks, and financial losses.

Look about modern environment, and you'll discover that technology is more important in everyday life than it has ever been. The advantages of this trend vary from near-instant Internet connectivity to contemporary comforts afforded by home automation technologies and ideas such as the Internet of Things.

With so much good that technology provides, it might be difficult to comprehend that potential risks lurk behind every gadget and platform. Nonetheless, despite society's optimistic view of contemporary developments, cyber security dangers posed by modern technology are a serious hazard.

A continuous growth in cybercrime exposes weaknesses in the gadgets and services we've grown to rely on. This issue compels us to consider what cyber security was, why it's important, and what we can learn about it.

So, what exactly is cyber security, and how dangerous are cyber security risks nowadays? Continue reading to find out.

8.1 The Usage of a Firewall but Also Its Implementation

A network firewall is a traffic management and monitoring system. It is used to defend the framework from viruses, viruses, worms, and other threats, as well as to prevent unwanted access from a secure network [17].

The following are the procedures for installing and configuring the firewall:

- Change a firewall device's default password.
- Disable the functionality of remote administration.
- Configure port forwarding to allow certain programs, such as an FTP server or a web server, to work properly.
- Installation of a firewall on a network with an existent DHCP server might result in issues unless the firewall's DHCP is deactivated.
- Ascertain that the firewall is set to strict security policies.

8.2 Assessment of Vulnerabilities and Penetration Testing

- Vulnerability assessment & penetration testing are two distinct words that both serve an important purpose in network security.
- Vulnerability assessment is a process that defines, detects, and prioritizes vulnerabilities in computer networks, network infrastructure, applications, and other systems, and provides the company with the knowledge needed to correct the faults.
- Penetration testing, often known as pen testing and ethical hacking, is a kind of security testing. It is the method of testing a network, system, or application to for vulnerabilities that attackers may exploit. It is most often used to supplement a firewall for web-based applications in the context of online application security (WAF).

8.3 A Three-person Handshake Procedure

A three-way handshake process is used in TCP (Transmission Control Protocol) network for transmission of data in a reliable way between the host and the client.

It’s called a three-way handshake because three segments are exchanged between the server and the client.

- SYN: If the client wishes to connect to the server, it sends a section with the SYN (Synchronize Remain In effect) to a server if indeed the server is online and has access points.
- SYN + ACK: If the server has open ports, it answers to the customer requests using SYN-ACK signal bits set.
- ACK: A client acknowledges a server's answer by sending an ACK(Acknowledgement) packet to the server.

8.4 Http Response Codes

HTTP response codes indicate whether or not an HTTP request has indeed been completed.

- 1xx (Informal) - The request was received, and the procedure is ongoing.
- 2xx (Success) - The application was received and accepted successfully.
- 3xx (Redirection) - Additional action is required to finish it.
- 4xx (Client Error) - Response is invalid or contains wrong syntax.
- 5xx (Server Error) - This server is unable to complete the request.

8.5 The Tactics Are Used in The Prevention of A Brute Force Attack

Brute Force Assault is a trial and mistake strategy used by application programs to decipher encrypted information such as encrypting data keys or passwords rather than employing intellectual tactics. It is a technique of identifying the correct credentials by repeatedly trying all conceivable approaches [17].

The following procedures will help you prevent brute force attacks:

- Increasing password complexity: Use various character types to make passwords more secure.
- Limit login attempts: specify a maximum number of login failures.
- Two-factor authentication: Use this security measure to prevent brute force attacks.

8.6 Kept up to Speed on The Most Recent Cybersecurity News

The following methods can assist you in keeping up with the most recent cybersecurity updates:

- Follow security professionals' news websites and blogs.
- Examine social media security concerns.
- Examine the vulnerability alert feeds & advisory websites.
- Attend live cybersecurity events.

8.7 You Comprehend Meant by Cybersecurity Compliance

The following methods can assist you in keeping up with the most recent cybersecurity updates:

- Compliance entails adhering to a set of norms established by an organization/government/independent party.
- It aids in the definition and achievement of IT goals, as well as the mitigation of hazards via procedures like as vulnerability management.

8.8 The Application of Patch Management

- Patch management's goal is to keep multiple systems inside a network updated and protected from malware and hacker threats.
- Many corporate patch management technologies handle the patching processes by installing or installing agents on a targeted device, and they act as a conduit between centralize patch servers and patched machines.

8.9 Security Program Roadmap

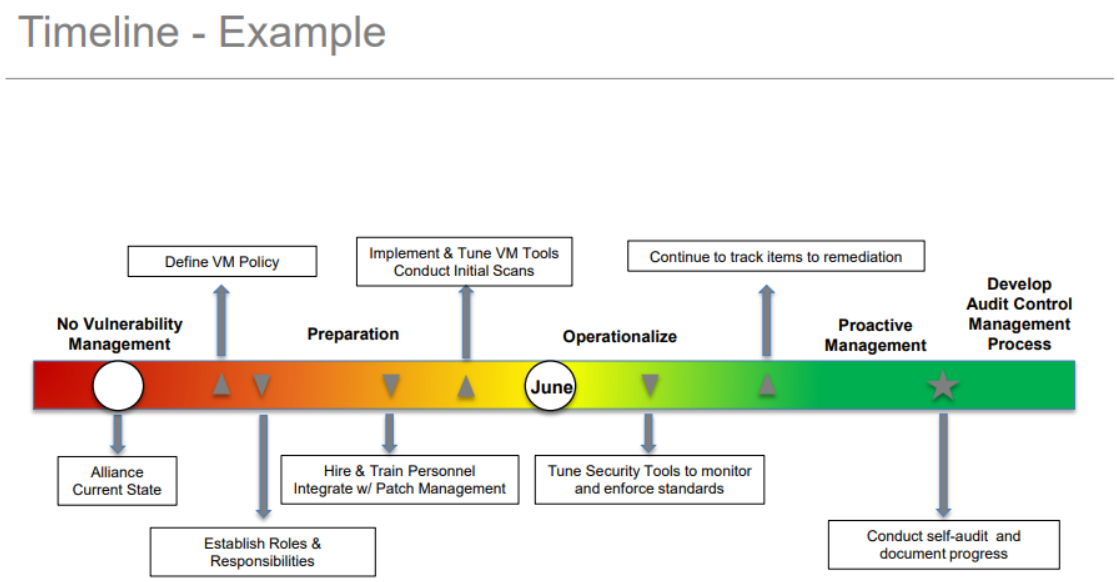


Figure 8.1: Roadmap for the Security Program

CHAPTER 9

CONCLUSION AND PROSPECTS

9.1 Discussion

The main causes of information security problems are the difficulty of information systems, the intrinsic nature of information systems (IT), and human frailty in making a judgement about what activities and data are safe or hazardous from an internet security point of view when such activities and details are highly complex. Since none of these factors are expected to change in the foreseeable future, there are no magic alternatives even combination of solutions—that would "solve the issue" forever.

Threats to cybersecurity change throughout time as well. Hackers adapt by developing new tools and techniques to penetrate security when new defenses are established to thwart more current efforts. As informational technology becomes increasingly prevalent in society, the incentives to compromise the security of established IT systems grow. Innovation results in new information technology applications, but it also generates new chances for thieves, terrorists, and other enemies to function, as well as new security holes that hostile actors may exploit. The number of individuals who have access to the internet is growing, which increases the amount of potential consumers and criminals.

As a consequence, upgrading a system's security posture, by extension, the enterprise in which it is integrated be viewed as a continual endeavor rather than a one-time event. Adversaries constantly change and improve their intrusion methods, particularly at the upper end of the risk spectrum, and the defender must do the same.

For instance, in response to end-user security concerns, the majority of large IT companies have recently made substantial efforts to strengthen the security of their products. The majority of today's products are, on the whole, safer than earlier models. Funding for cybersecurity research has grown dramatically.

Finally, the essential policy issue is not how to fix the security problem, but how to manage it. War, terrorism, crime, starvation, drug abuse, and other social crises are seldom "solved" or erased off the policy platform permanently. These problems' relevance may rise or decrease depending on the context, and no one expects them to be totally fixed such that they will never start coming up again. This also applies to cybersecurity concerns.

9.2 Future work and Further Development

Certain attack techniques will likely persist due to their effectiveness. These are the threats that, in the view of our experts, continue to imperil cyber security. In 2021, remote work will provide the greatest cyber security concern. Because of the ongoing implementation of several COVID-19 guidelines, virtual organizations (and the related cyber risks) will remain prevalent.

Because of pandemic concerns, organizations have encouraged remote work, making it simpler for bad actors to identify vulnerable or poorly constructed equipment that connect to the internet. Ernie Sherman, a Field - effect transistor partner as well as the President of Fueled Networks, a controlled and it security agencies provider that assists companies in planning, managing, & aligning such services with their clients' corporate strategy, believes that the shift forward into working from home is the latest craze in computer security this year. The challenge is that we must embrace a zero-trust mindset and assume that corporate resources & unsecured devices share the same environment and should be suitably protected. We could no longer presume that perimeter security protects business resources.

Cybercriminals have preyed on distracted or busy remote workers and will continue to do so in the past.

Looking forward, a few issues about the future and cyber defense emerge. One of these is the significance of focusing more on preventive and preparedness. It is critical to plan your reaction to a security incident or data breach. Playbooks for crisis planning and response are likely to become more widely available. Employee training at all degrees will reduce the effect of human error. As regulatory concerns become more relevant, ensuring that

cyber security procedures are robust enough to meet that standard during audits and compliance assessments will probably be front of mind.

Businesses may want to concentrate on securing their operations first and foremost. As assaults continue to develop, establishing a solid foundation of best practices and healthy habits is essential.

It may be difficult to glance at the calendar and predict what the future may bring in a topic as complex and fluid as cyber security. However, by devoting the effort required to lay the groundwork now, you may position your organization for results of this case when changes occur and new problems, whatever they might be, arise.

9.3 Conclusion

Overall, we've looked at a few of the interviews you could face if you apply for a pentesting position. If a pentester is presently engaged in this industry, these questions may also be posed to them.

It is vital to remember that although responding to these questions will indicate to the examiner you in-depth understanding of pentesting, being a great pentester requires other qualitative talents as well. For example, you must be able to work effectively with people in a team-oriented environment & work long hours.

Pentesting also need a tremendous amount of patience on our behalf, since these types of activities do not take place in a single day. It might take weeks or months to complete a good pentest.

Finally, you must be able to translate all of the technical language related with the findings you have acquired into a level that our customer can comprehend and apply. In your interview, you will be evaluated on these qualitative elements as well.

REFERENCE

[1] BugsBD Limited, Obtainable at < https://bugsbd.com/ >, Last Visited on 01 August, 2022

[2] OWASP, Obtainable at < https://owasp.org/www-project-top-ten/ >, Last Visited on 01 August, 2022

[3] BugsBD Limited Office, Obtainable at < https://23.226.65.98/bugsbdcrm/admin/authentication >, Last Visited on 01 August, 2022

[4] Microsoft, Obtainable at < https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/set-up-routing-remote-access-intranet >, Last Visited on 01 August, 2022

[5] Microsoft Windows Server 2019, Obtainable at < https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019 >, Last Visited on 01 August, 2022

[6] PowerShell security features, Obtainable at < https://learn.microsoft.com/en-us/powershell/scripting/learn/security-features?view=powershell-7.3 >, Last Visited on 01 August, 2022

[7] VirtualBox, Obtainable at < https://www.virtualbox.org/ >, Last Visited on 01 August, 2022

[8] Kali Linux, Obtainable at < https://www.kali.org/ >, Last Visited on 01 August, 2022

[9] Wire Shark, Obtainable at < https://www.wireshark.org/ >, Last Visited on 01 August, 2022

[10] Virous Total, Obtainable at < https://www.virustotal.com/gui/home/upload >, Last Visited on 01 August, 2022

[11] Risk Management, Obtainable at < https://hyperproof.io/resource/cybersecurity-risk-management-process/#:~:text=and%20manage%20risk.-

,What%20is%20Cybersecurity%20Risk%20Management%3F,has%20a%20role%20to%20play. >, Last Visited on 01 August, 2022

[12] Clients and Server, Obtainable at < https://developer.mozilla.org/en-US/docs/Learn/Getting_started_with_the_web/How_the_Web_works#:~:text=The%20browser%20sends%20an%20HTTP,internet%20connection%20using%20TCP%2FIP. >, Last Visited on 01 August, 2022

[13] Osi Model, Obtainable at < https://www.forcepoint.com/cyber-edu/osi-model#:~:text=The%20OSI%20Model%20(Open%20Systems,between%20different%20products%20and%20software. >, Last Visited on 01 August, 2022

[14] Phases of Hacking, Obtainable at < https://www.greycampus.com/opencampus/ethical-hacking/phases-of-hacking >, Last Visited on 01 August, 2022

[15] Try to Hack Me, Obtainable at < https://tryhackme.com/login >, Last Visited on 01 August, 2022

[16] Hack the Box, Obtainable at < https://www.hackthebox.com/ >, Last Visited on 01 August, 2022

[17] Cyber Security Attack, Obtainable at < https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks#:~:text=What%20are%20the%20four%20types,attack%2C%20and%20SQL%20injection%20attack. >, Last Visited on 01 August, 2022

[18] Cyber Security Framework, Obtainable at < https://www.simplilearn.com/what-is-a-cyber-security-framework-article >, Last Visited on 01 August, 2022

201-15-13776_Partho_Protim_Halder_1.docx

ORIGINALITY REPORT

16%	15%	4%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	dspace.daffodilvarsity.edu.bd:8080 Internet Source	5%
2	pdfcoffee.com Internet Source	2%
3	documents.mx Internet Source	2%
4	resources.infosecinstitute.com Internet Source	1%
5	mindmajix.com Internet Source	1%
6	www.peoplehum.com Internet Source	1%
7	www.parasoft.com Internet Source	1%
8	www.ekransystem.com Internet Source	<1%
9	www.networkangel.net Internet Source	<1%