Contents

P1 Identify types of security threat to organisations.

- **Introduction [18]**
  - Hackers, ransomware, worms, malicious software, cyber intrusions, data theft, and other dangers abound on the internet nowadays. The threat denotes the type of action that is likely to cause damage, while vulnerability (also known as vulnerabilities or breaches) denotes the extent of vulnerability to threats in a given situation. Finally, the countermeasure is all of the actions implemented to prevent the threat.
  - With daily growing threats to sensitive data in both number and sophistication, organizations are unable to afford a scattershot approach to security. Instead, in their unique security posture, they need to focus their limited IT budgets and resources on specific vulnerabilities.
  - To do so, the threats to the security, credibility, or usefulness of their databases or information systems must be identified, assessed, and prioritized based on the likelihood of an incident and the impact it will have on the business. As a result, the procedure is known as an IT risk assessment.
  - A risk assessment of IT is required by most regulatory regulations. Of starters, if your company is required to comply with HIPAA or is likely to face GDPR audits, doing an information security risk appraisal is a must to avoid non-compliance and hefty fines.
- **Digital Security Risks:**
  - **MALWARE. [1]**
    - Malware is malware that without the permission or consent of the user, enters a computer device, and then takes an unauthorized and generally harmful operation.
    - Strictly speaking, a threat vector is used by malware to deliver a destructive payload that executes a damaging operation once invoked.
    - More specifically, there is the following malware:
    - Oligomorphic malware: Once it is run, this malware switches the internal code to one of a given number of predefined mutations. However, as there are only a finite number of mutations in oligomorphic malware, it can inevitably transform back into a previous form that can then be found by a scanner.
    - Polymorphic malicious: Malware code is classified as polymorphic malware that differs entirely from its original nature once it is performed. This is typically achieved by “scrambled” code malware that is “unscrambled” as the malware is triggered before it is executed.
    - In particular, metamorphic malware will rewrite its own code and thus appear distinct each time it is executed. It does this by, once it is run, generating a logical counterpart of its code. (Rieck, Holz, Willems, Düssel, Laskov,2008)
  - **Circulation/Infection.**

1. **Viruses. [2]**
   - ✓ **Definition:**

- A computer virus, much like a flu virus, is designed to spread from host to host and has the ability to replicate itself. Similarly, in the same way that flu viruses cannot reproduce without a host cell, computer viruses cannot reproduce and spread without programming such as a file or document.
- In more technical terms, a computer virus is a type of malicious code or program written to alter the way a computer operates and is designed to spread from one computer to another. A virus operates by inserting or attaching itself to a legitimate program or document that supports macros in order to execute its code. In the process, a virus has the potential to cause unexpected or damaging effects, such as harming the system software by corrupting or destroying data. (Harley, Slade, Gattiker, 2001)

✓ **How does a computer virus attack?**

- Once a virus has successfully attached to a program, file, or document, the virus will lie dormant until circumstances cause the computer or device to execute its code. In order for a virus to infect your computer, you have to run the infected program, which in turn causes the virus code to be executed.
- This means that a virus can remain dormant on your computer, without showing major signs or symptoms. However, once the virus infects your computer, the virus can infect other computers on the same network. Stealing passwords or data, logging keystrokes, corrupting files, spamming your email contacts, and even taking over your machine are just some of the devastating and irritating things a virus can do.
- While some viruses can be playful in intent and effect, others can have profound and damaging effects. This includes erasing data or causing permanent damage to your hard disk. Worse yet, some viruses are designed with financial gains in mind.
- Viruses: A virus is a small piece of software that piggybacks on real programs. For example, a virus might attach itself to a program such as a spreadsheet program. Each time the spreadsheet program runs, the virus runs, too, and it has the chance to reproduce (by attaching to other programs) or wreak havoc.

✓ **Solution**

- When you arm yourself with information and resources, you’re wiser about computer security threats and less vulnerable to threat tactics. Take these steps to safeguard your PC with the best computer virus protection:
  - Use antivirus protection and a firewall
  - Get antispyware software
  - Always keep your antivirus protection and antispyware software up-to-date
  - Update your operating system regularly

- Increase your browser security settings
- Avoid questionable Websites
- Only download software from sites you trust.
- Carefully evaluate free software and file-sharing applications before downloading them.
- Don’t open messages from unknown senders
- Immediately delete messages you suspect to be spam

- An unprotected computer is like an open door for computer viruses. Firewalls monitor Internet traffic in and out of your computer and hide your PC from online scammers looking for easy targets. Products like Webroot Internet Security Complete and Webroot Antivirus provide complete protection from the two most dangerous threats on the Internet – spyware and computer viruses. They prevent viruses from entering your computer, stand guard at every possible entrance of your computer and fend off any computer virus that tries to open, even the most damaging and devious strains.
- While free antivirus downloads are available, they just can’t offer the computer virus help you need to keep up with the continuous onslaught of new strains. Previously undetected forms of polymorphic malware can often do the most damage, so it’s critical to have up-to-the-minute, guaranteed antivirus protection. (Harley, Slade, Gattiker, 2001)

2. **Worms. [3]**

✓ **Definition:**

- The term “computer worm” was first used in 1975 in the novel “The Shockwave Rider” by John Brunner. In this novel, the protagonist of the story creates a worm that collects data. In the early days of computer science, worms were designed to exploit a system’s vulnerabilities. Instead of seriously damaging the infected computers, they just kept multiplying in the background. Today, however, the purpose of computer worms has changed. Today, attackers often use them to gain full access to their victims’ computers.
- Computers connected to a network are susceptible to various forms of malware, including computer worms. A computer worm is malware that reproduces itself and spreads over network connections. The computer worm does not usually infect computer files, but rather infects another computer on the network. This is done by the worm replicating itself. The worm passes this ability on to its replica, which allows it to infect other systems in the same way. The difference between computer worms and viruses can also be found here. Computer worms are stand-alone programs that replicate themselves and run in the background, while viruses require a host file to infect. (Erbschloe, 2004)

✓ **How does a Computer Worm work?**

- In order to spread, computer worms use vulnerabilities in networks. The worm is looking for a back door to penetrate the network unnoticed. To get computer worms into circulation for the first time, hackers often send phishing e-mailsor instant messages with malicious attachments. Cyber criminals try to camouflage the worm so that the recipient is willing to run the program. For this purpose, for example, double file extensions are used and / or a data name that looks harmless or urgent, such as “invoice”. When the user opens the attachment or link, they will immediately download the malware (computer worm) into the system or be directed to a dangerous website. In this way, the worm finds its way into the user’s system without them noticing. Once executed, the worm seeks a way to replicate and penetrate other systems. One way of doing this, for example, is for the worm to send an email to all contacts on the infected computer, which contains replicas of the worm.
- Many worms now have what is known as a payload. Payload is translated as the “payload” and in this case an attachment that the worm brings with it. The worm can, for example, carry ransomware, viruses or other malware, which then cause damage to the infected systems. These can then, for example, delete files on the PC or encrypt files in the event of a blackmail attack. A computer worm can also install a back door that can later be exploited by other malware programs. This vulnerability gives the worm’s author control over the infected computer. (Erbschloe, 2004)

✓ **Solution**

- In the meantime, mixed forms of different malware are often used in malware campaigns. For example with the WannaCry ransomware or Petya / Not-Petya ransomware. These have a worm component so that the malware can replicate and spread through back doors in other systems in the network.
- Since the worm or its programmer can use the computing power of the infected system, they are often integrated into a botnet. These are then used by cyber criminals, for example for DDoS attacks or cyptominig.
- There are several steps that administrators can take in order to prevent computer worms from infecting network devices. Having robust security from an IT perspective can prevent computer worms before they even access the network, or neutralize them as soon as they enter.
- It’s crucial for admins to update their devices regularly. Vendors will frequently release vulnerability patches in updates that prevent malware from gaining entry. Devices running an out-of-date operating system put other devices in the network at risk; this is because they can act as a Patient 0 for a worm attack. (Erbschloe, 2004)

3. Trojan horses. [21]

✓ **Definition:**

- A Trojan horse, or Trojan, is a type of malicious code or software that looks legitimate but can take control of your computer. A Trojan is designed to damage, disrupt, steal, or in general inflict some other harmful action on your data or network.
- A Trojan acts like a bona fide application or file to trick you. It seeks to deceive you into loading and executing the malware on your device. Once installed, a Trojan can perform the action it was designed for.
- A Trojan is sometimes called a Trojan virus or a Trojan horse virus, but that's a misnomer. Viruses can execute and replicate themselves. A Trojan cannot. A user has to execute Trojans. Even so, Trojan malware and Trojan virus are often used interchangeably. (Huang, Rau, Salvendy,2010)

✓ **How do Trojans work?**

- A Trojan horse is a type of malware that downloads onto a computer disguised as a legitimate program. A Trojan horse is so-called due to its delivery method, which typically sees an attacker use social engineering to hide malicious code within legitimate software. However, unlike computer viruses or worms, a Trojan does not self-replicate, so it needs to be installed by a valid user.
- A simple way to answer the question "what is Trojan" is it is a type of malware that typically gets hidden as an attachment in an email or a free-to-download file, then transfers onto the user's device. Once downloaded, the malicious code will execute the task the attacker designed it for, such as gain backdoor access to corporate systems, spy on users' online activity, or steal sensitive data.
- Indications of a Trojan being active on a device include unusual activity such as computer settings being changed unexpectedly.
- How Do Trojans Work?
- Unlike computer viruses, a Trojan horse cannot manifest by itself, so it needs a user to download the server side of the application for it to work. This means the executable (.exe) file should be implemented and the program installed for the Trojan to attack a device's system.
- A Trojan virus spreads through legitimate-looking emails and files attached to emails, which are spammed to reach the inboxes of as many people as possible. When the email is opened and the malicious attachment is downloaded, the Trojan server will install and automatically run every time the infected device is turned on.
- Devices can also be infected by a Trojan through social engineering tactics, which cyber criminals use to coerce users into downloading a malicious application. The malicious file could be hidden in banner advertisements, pop-up advertisements, or links on websites.
- A computer infected by Trojan malware can also spread it to other computers. A cyber criminal turns the device into a zombie computer, which means they have

remote control of it without the user knowing. Hackers can then use the zombie computer to continue sharing malware across a network of devices, known as a botnet.

- For example, a user might receive an email from someone they know, which includes an attachment that also looks legitimate. However, the attachment contains malicious code that executes and installs the Trojan on their device. The user often will not know anything untoward has occurred, as their computer may continue to work normally with no signs of it having been infected.
- The malware will reside undetected until the user takes a certain action, such as visiting a certain website or banking app. This will activate the malicious code, and the Trojan will carry out the hacker's desired action. Depending on the type of Trojan and how it was created, the malware may delete itself, return to being dormant, or remain active on the device.
- Trojans can also attack and infect smartphones and tablets using a strand of mobile malware. This could occur through the attacker redirecting traffic to a device connected to a Wi-Fi network and then using it to launch cyberattacks. (Huang, Rau, Salvendy,2010)

✓ **Solution**

- As with protecting against most common cybersecurity threats, effective cybersecurity software should be your front line of protection. An effective internet security solution should run fast, frequent scans and alert you as soon as a Trojan virus is detected.
- If you're reading this because it's already too late, see our page on removing malware infecting your computer. If you're reading this to stay safe from these types of attacks in the future, there are a few best practices in addition to installing cybersecurity software to help keep yourself safe:
- Never download or install software from a source you don't trust completely
- Never open an attachment or run a program sent to you in an email from someone you don't know.
- Keep all software on your computer up to date with the latest patches
- Make sure a Trojan antivirus is installed and running on your computer

4. **Rootkit. [17]**

- Rootkit is a malicious program that installs and executes malicious code on a system without user consent in order gain administrator-level access to a computer or network system. There are different types of Rootkit virus such as Bootkits, Firmware Rootkits, Kernel-Level Rootkits and application Rootkits
- A rootkit is a set of software tools used to hide the actions or presence of other types of software.
- By modifying the operating code, rootkits do this to cause it to ignore their malicious files or behavior.

- Rootkits also hide or remove all traces of evidence that may reveal the malware, such as log entries.
- A rootkit is a type of malicious software that is intended to remotely access or monitor a device without it being detected by users or security programs. The malicious party behind the rootkit will remotely execute files, access/steal data, alter system settings, adjust software once a rootkit is installed (especially protection software that might detect a rootkit). Rootkit avoidance, detection and removal can be difficult, due to its continuous operation. Since rootkits hide their presence on a continuous basis, rootkits may not be detected and uninstalled by conventional protection items. Manual methods, such as system verification, signature checking and data dump analysis, often include the detection of rootkits. To avoid unwanted changes and review static data and ensure that they protect themselves against rootkits, companies and consumers can regularly patch vulnerabilities in applications, programs and operating systems and upgrade virus definitions. (Blunden, 2012)

○ **Collect data.**

1. **Spyware. [4]**
   - Spyware is a form of malware that works by spying on user behavior without its knowledge. The spying techniques could include monitoring behavior, review of keystrokes, a compilation of data (account records, logins, financial information), and more. Additional functions, from modifying software or device security parameters to communicating with network connections, are often frequently used in Spyware. Spyware spreads through the use of software vulnerabilities, the combination of legitimate programs or Trojan software. (Erbschloe,2004)
2. **Adware. [5]**
   - In a way that is unexpected and unwanted by the user, Adware delivers advertising content. When the adware malware becomes installed, it usually shows advertisement banners, popup advertisements, or opens new web browser windows at irregular intervals.
   - Adware is a type of malware that delivers notoriety automatically (Short for advertising-supported software). Pop-up advertisements on software-displayed websites and advertisements are typical examples of adware. “free” versions packaged with adware are often sold by apps and applications. The bulk of adware is advertisement funded, written, or used as a revenue generation tool. While some adware is only meant to provide ads, it is not unusual for spyware to monitor user behavior and steal adware data. Adware and spyware packages are much more risky than adware alone, owing to the inclusion of spyware features. (Erturk,2012)
3. **Ransomware [6]**

- Ransomware prevents a user's device from properly operating until a fee is paid.
- One type of ransomware locks up the machine of a victim and then shows a message from a law enforcement agency that purports to arrive.
- Ransomware is a ransomware category that retains a computer system Hostage because of a ransom. By either encrypting hard disk files or locking the system and showing notifications that force the user to pay the malware creator to delete the restrictions and recover access to the computer, the malware prohibits the user from accessing the unit. Ransomware typically travels via a downloaded file and like a typical computer worm, any other flaw in a network service ends up on a computer.

4. **Careless employees**
   - Employees are a company's greatest security concern and they know everything about it, including where sensitive data is stored and how to access it. Malware breaches, as well as careless employees, are examples of cybersecurity risks to companies. They recall passwords with a basic password and even swap passwords. Another common problem is that employees opening suspicious email attachments, clicking on the link, or visit malicious websites, which can introduce malware into the system.
5. **Natural disaster.**
   - sometimes natural disasters occur suddenly and have a chance of destroying the hardware of the organization, usually, this can be prevented by making backups and have them securely protected.

- **Delete data**

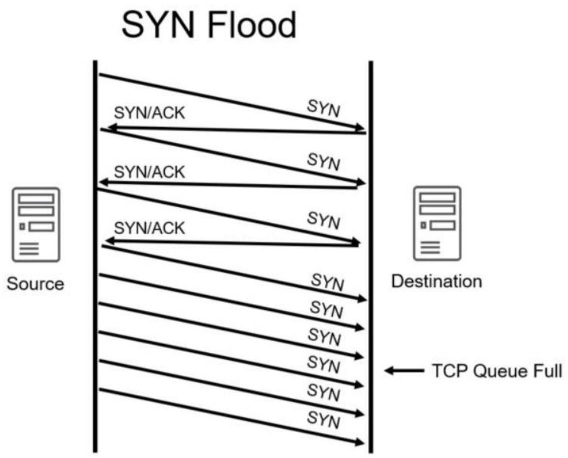
  A computer program that lies dormant until triggered by a specific event, for example:
  - A certain date being reached on the system calendar.
  - A person's rank in an organization dropping below a specified level.
- **Modify system Security**

  Back doors
  - The payload of certain forms of malware tries to change the security settings of the device in order to make more insidious attacks possible.
  - In this category, one kind of malware is called a backdoor. A backdoor provides access to a computer, program, or service that bypasses all ordinary security precautions.
  - Backdoors that are installed on a computer allow the attacker to return at a later time and bypass security settings.
  - In the area of cryptography, a workaround refers to every process that.
  - It enables authorised and unauthorized users to circumvent standard security measures and obtain high-level access from an operating system, network or device application (aka rotary access). Cyber attackers can grab confidential and

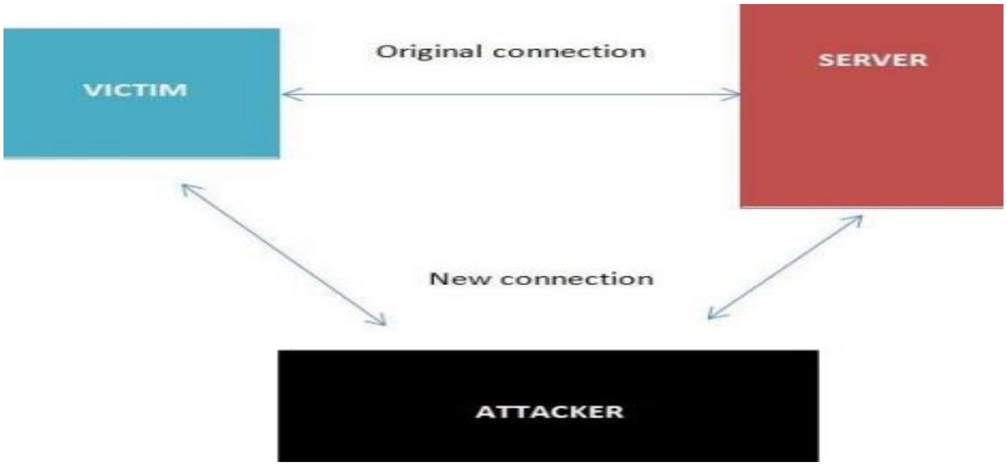
financial information from a backdoor after delivery and add extra malware and hijack appliances after delivery.

- **Networking-Based Attacks**

1. **Denial of Service (DoS) [19]**
   - A DoS attack is a deliberate attempt to prevent authorized users from accessing a system by overwhelming that system with requests.
   - Most DoS attacks today are actually distributed denial of service (DDoS) attacks: instead of using one computer, a DDoS may use hundreds or thousands of zombie computers in a botnet to flood a device with requests. (Liu, Yang, Xia,2010)
2. **Types of DoS attacks**
   - Ping flood
   - A large number of ICMP echo requests are submitted rapidly by several machines, flooding a server (as well as the network) to the point that it will not respond enough quickly and will lose valid connections to other clients and deny all new connections.
3. **Smurf attack**
   - An intruder broadcasts a ping message to all network machines but switches the address from which the request came to the computer of the victim.
   - Each computer then sends a reaction to the computer of the victim such that it is overloaded quickly and then fails or becomes useless to legal users.
4. **SYN Flood attack**



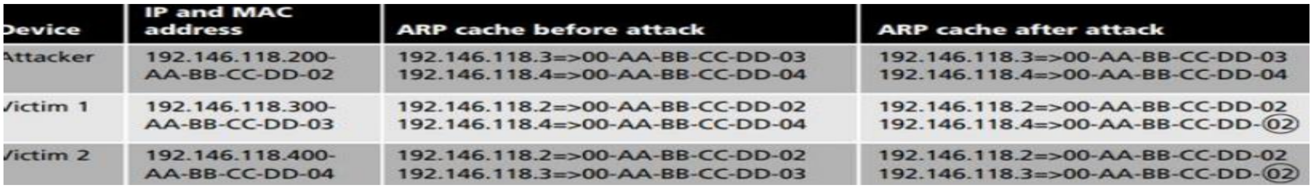
   - Interception
     + Man-in-the-Middle attack
     + Replay attack



- A replay attack is similar to a passive man-in-the-middle attack.
- Before transmitting it to the receiver, attackers produce a copy of the transmission. Later, the intruder is able to give the server the original message and the server is able to reply. Now between the intruder and the server, a trusting relationship has been established.
- The intruder will begin to modify the substance of the message and code captured. The server will reply if he actually makes the right change, letting the intruder know he has been successful.

Poisoning

- ARP Poisoning: An attacker can modify the MAC address in the ARP cache so that the corresponding IP address points to a different computer.



Device	IP and MAC address	ARP cache before attack	ARP cache after attack
Attacker	192.146.118.200- AA-BB-CC-DD-02	192.146.118.3=>00-AA-BB-CC-DD-03 192.146.118.4=>00-AA-BB-CC-DD-04	192.146.118.3=>00-AA-BB-CC-DD-03 192.146.118.4=>00-AA-BB-CC-DD-04
Victim 1	192.146.118.300- AA-BB-CC-DD-03	192.146.118.2=>00-AA-BB-CC-DD-02 192.146.118.4=>00-AA-BB-CC-DD-04	192.146.118.2=>00-AA-BB-CC-DD-02 192.146.118.4=>00-AA-BB-CC-DD-02
Victim 2	192.146.118.400- AA-BB-CC-DD-04	192.146.118.2=>00-AA-BB-CC-DD-02 192.146.118.3=>00-AA-BB-CC-DD-03	192.146.118.2=>00-AA-BB-CC-DD-02 192.146.118.3=>00-AA-BB-CC-DD-02

- DNS Poisoning is a process of substituting a DNS address so that the computer is automatically redirected to another device

Attacks on Access Rights

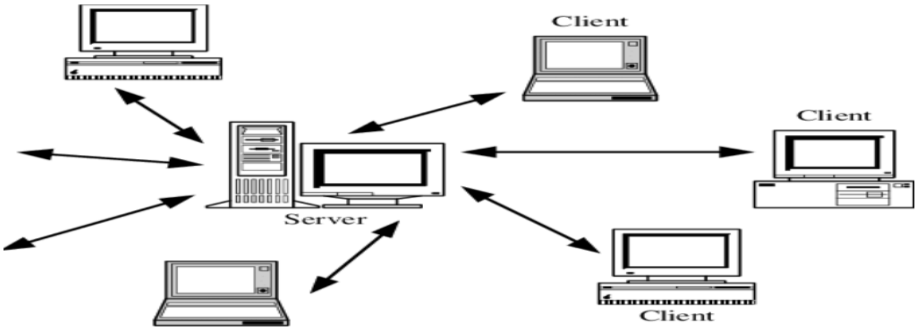
- Privilege Escalation: leveraging a security flaw to obtain access to services that the user would usually be prevented from accessing.
- Transitive Access: System A can access System B, and because System B can access System C, then System A can access System C.

II. Application Attacks. [7]

- **Introduction**

It is important to take precautions to stay secure while people use the internet. Due to the fact that now, not only viruses are being used to target the consumer but also other programs. The applications you use daily may contain infections that can seriously damage the system. Here are attacks of some application type commonly used. (Vétillard, Ferrari, 2010)

- **Server-Side Web Application Attacks**
  - On the Internet, utilities that are introduced as online apps are delivered by a web server.
  - An significant aspect of web apps on the server side is that they generate interactive content based on user inputs.
  - Many web application server-side attacks target the feedback that users embrace from the applications.



1. **SQL injection: [20]**
   - Through injecting SQL queries into the interaction data between the database and the Scholars program, lots of SQL injection jobs are run. The method of publicly leveraging SQL injection error will help hackers recover confidential data in the database, quiet the database (insert/update/delete), perform Administrator VI privileges actions, and more can monitor the operating system of the server.
   - The SQL Injection is a defect in the security of code that allows an attacker to Manipulate an application's database, allowing them to access or retrieve information, change an application's data-driven actions and other unintended items, by tricking an application to issue unwanted SQL commands. SQL injections are the most common vulnerabilities to machine integrity. If the software refuses to correctly sanitize this untrusted data until submitting it to a SQL query, an attacker may include its very own SQL commands that the database executes. These SQLi vulnerabilities are a major concern for web applications and many businesses are vulnerable to possible data breaches arising from the injection of SQL. Vulnerabilities in SQLi are simple to avoid. (Clarke-Salt, 2009)
2. **XML Injection:**
   - Is an attack technique used for altering or destroying the application's XML framework or process logic? It is possible to alter the intentional purpose of the standard by adding unnecessary XML content and/or constructs into an XML document.
   - XML is the eXtensible markup language for storing and transmitting information. XML utilizes a tree-like attribute and data layout, as with HTML.

XML does not use predefined tags. It is used in all areas, from the Internet (XML-RPC, SOAP, SOAP, REST and WSDL) papers (XML, HTML, DOCX) to the SVG and RSS image files. An XML parser (also known as the XML processor) is essential to read XML data.

3. **Cross-site scripting:**

A flaw of XSS arises as web applications accept data from users and include it dynamically in web pages without validating it correctly first. XSS vulnerabilities allow an intruder to execute arbitrary commands in a browser of the user and view arbitrary content. An XSS intrusion effectively allows an attacker to access the computer of the user or the web application's compromised account. While XSS is allowed by insecure web-based websites, XSS attackers are consumers of the framework, not the site itself. The strength of an XSS security vulnerability is because the malicious code is being run during the victim's session so that the intruder will overcome regular safety constraints.

Client-side Application Attacks.

- Client-side attacks target vulnerabilities in client applications that interact with a compromised server or process malicious data.
- One example of a client-side attack results in a user’s computer becoming compromised just by viewing a webpage and not even clicking on any content.
- One commonly attack is drive-by-download.

Header Manipulation.

- The HTTP header consists of fields that contain information about the characteristics of the data being transmitted.
- An attacker can modify the HTTP headers to create an attack using HTTP header manipulation.
- HTTP header manipulation is not an actual attack, but rather the vehicle through which other attacks, such as XSS, can be launched.

Cookies

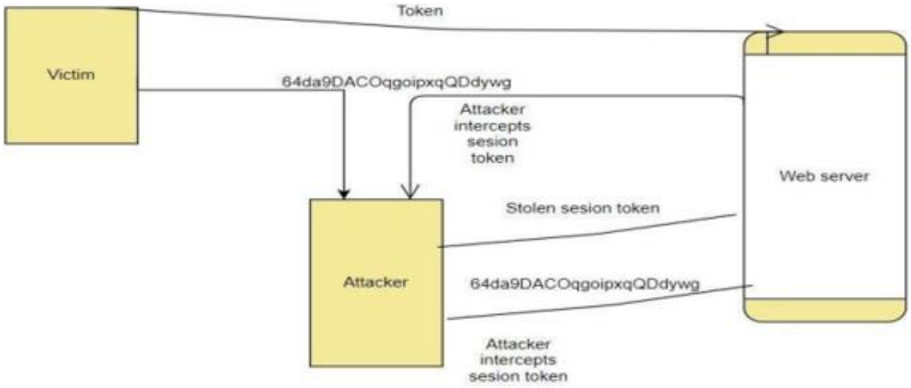
- A cookie can contain a variety of information based on the user’s preferences when visiting a website.
- Several different types of cookies exist: First-party cookie, Third-party cookie, Session cookie.
- First-party cookies can be stolen and used to impersonate the user.
- Third-party cookies can be used to track the browsing or buying habits of a user.

Attachments

- Attachments are files that are coupled to email messages.
- When opened, malicious attachments are widely used to distribute viruses, trojans, and other malware.

Session Hijacking

- Session hijacking is an attack in which an attacker attempts to impersonate the user by using her session token.



Malicious Add-ons

- To execute malicious attacks on a computer, attackers can take advantage of vulnerabilities in ActiveX.
- Attackers can create malicious add-ons to launch attacks against the user's computer.
- One way in which these malicious add-ons can be written is by using Microsoft's ActiveX.

Impartial Overflow Attacks.

- Buffer Overflow Attack: When a process tries to store data in RAM outside the constraints of a fixed-length storage buffer, a buffer overflow attack occurs.
- Integer Overflow Attack: The condition that happens when the outcome of an arithmetic operation reaches the full size of the integer form used to store it such as addition or multiplication.
- Arbitrary/Remote Code Execution: allows an attacker to run programs on a separate machine and execute instructions.

Social Engineering Attacks

- Today, the most possible focus of threats is the global computing infrastructure.
- Attackers are getting more experienced, going away from hunting for bugs in individual device programs to testing the underlying software and hardware architecture itself.

Social Engineering

- Social engineering is an attack technique that bursts into an entity, corporation, or business structure. The assault on Social Engineering is a method of manipulating network users, breaching the security system, stealing data, or theft of funds. In other terms, Social Engineering is a complex internet fraud that has a very high success rate. Some well-known types of Social Engineering include Malware Attacks, Application Attacks, Network Attacks, etc.
- The easiest way to target a computer device takes virtually no technological skill and is generally incredibly accurate.

- Social engineering depends on tricking others to enter a device and tricking them
- Social engineering is not limited to dated certificates or telephone calls
- Dumpster diving: digging through trash receptacles to find computer manuals, printouts, or password lists that have been thrown away
- Phishing: sending people electronic requests for information that appear to come from a valid source
- Develop strong instructions or company policies regarding:

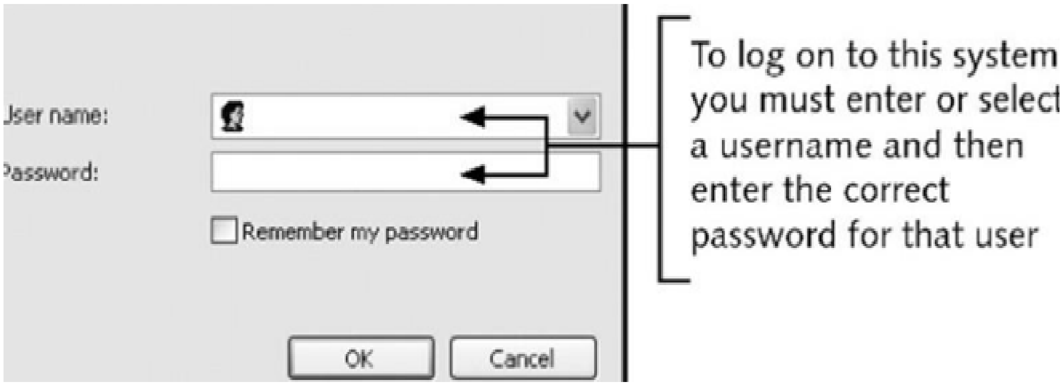
  + When passwords are given out

  + Who can enter the premises

  + What to do when asked questions by another employee that may reveal protected information
- Educate all employees about the policies and ensure that these policies are followed

Password Guessing

- Password: a secret blend of letters and numbers validating or authenticating a person.
- Passwords with usernames are used to log in to a device from a dialog box.
- Through password guessing, attackers try to exploit weak passwords.



To log on to this system you must enter or select a username and then enter the correct password for that user

- Characteristics of weak passwords:

  + Using a short password (XYZ).

  + Using a common word (blue).

  + Using personal information (name of a pet).

  + Using same password for all accounts.

  + Writing the password down and leaving it under the mouse pad or keyboard.

  + Not changing passwords unless forced to do so.
- Policies to minimize password-guessing attacks:

  + Passwords must have at least eight characters.

  + Passwords must contain a combination of letters, numbers, and special characters.

  + Passwords should expire at least every 30 days.

  + Passwords cannot be reused for 12 months.

+ The same password should not be duplicated and used on two or more systems.

- Similar to an active man-in-the-middle attack
- While an active man-in-the-middle attack affects the content of a message until it is received, the message is only captured by a replay attack and only sent again later.
- Takes advantage of network interface interactions with a file server

TCP/IP Hijacking

- With wired networks, TCP/IP hijacking uses spoofing, which is the act of pretending to be the legitimate owner
- One particular type of spoofing is Address Resolution Protocol (ARP) spoofing
- In ARP spoofing, each computer using TCP/IP must have a unique IP address
- In order to transfer information across the network, some types of local area networks (LANs), such as Ethernet, must also have another address, called the media access control (MAC) address,
- Network computers retain a table that connects an IP address to the corresponding address.
- In ARP spoofing, a hacker changes the table so packets are redirected to his computer.

4. **Directory Traversal/Command Injection**

- Directory traversal is a sort of HTTP hack that attackers use to enter a small file and file without authorization. CWE-SANS Top 25 Most Dangerous Code Errors.1 Traversal directory assaults using web server code to bypass improper security mechanisms to reach archives and data stored outside the site root domain. directory traversal, which is also known as the route crossing. An intruder that triggers a flaw in the directory is able to compromise the whole web server.
- The two authentication methods web servers use to restrict user access are the root directory and the Access Control Lists (ACL). A root directory is the main directory on a computer file system. User access is limited to the root directory, which ensures that folders or files outside the root directory cannot be accessed by users. Administrators use Access Control Lists to view, download, and execute data in order to evaluate user access rights and privileges.

III. Networking-Based Attacks: [8]

- **Introduction**
  - Network security attacks constitute illegal activity for the loss, alteration, or stoling of sensitive data against individual, business, or government IT infrastructure. As more businesses allow workers to view mobile devices info, networks become prone to computer extortion or full data or network loss.
  - Network-based attacks are dangers that machines or devices other than the ones under attack initiate and handle.

1. **Denial of Service (DoS).**

- DoS is a technical attack in the public in order not to allow valid access to the Server. This attack technique usually occurs in layering and the application class.
- Types of DoS attacks: Ping flood, Smurf attack, SYN flood:

+ Ping flood: Ping flood is a basic denial of service attack where with an ICMP “echo message” (ping) packet, the attacker overwhelms the target. By using the flood ping alternative that sends ICMP packets as quickly as possible without waiting for replies, this is the most convenient.

+Smurf attack: The Smurf assault is a distributed denial-of-service attack in which a vast number of internet Control Message Protocol (ICMP) packets representing the intended victim's spoofed source IP are sent to a computer network using an IP address.

+A SYN flood is a form of denial of service attack in which the attacker sends a sequence of SYN requests to the target machine to make the computer unresponsive to legitimate traffic in an attempt to drain adequate server resources.

- DoS attacks are a weapon that prevents a network or a website from being accessed by approved users and prevents connectivity attacks. In fact, the target of the attack (usually the site server) is overloaded because of heavy traffic or because malicious requests are made to attack the target. The machine became unstable or crashed entirely. Buffer overflow, Smurf attack, SYN flood, etc. are some well-known examples of Denial of Service Attacks.

○ **Buffer overflow:**

- A buffer overflow is a common error in software coding that could be used by an attacker to get access to a device. The buffer overflows, the hazards they pose to your applications and what methods attackers use to successfully exploit these vulnerabilities to mitigate buffer overflow vulnerabilities are essential to understand.

○ **Smurf attack:**

- Smurf is a denial of service (DDoS) network layer that is named after the DDoS.Smurf malware and makes it possible to execute it. Smurf attacks are similar to ping flooding, as both are conducted by sending request packets from ICMP Echo. Smurf assaults are near by. However, Smurf is a vector of amplification attack, which unlike normal ping floods, increases its damage capacity by using the features of broadcast networks.

○ **SMY flood:**

- A SYN Flood is a popular type of Denial-of-Service (DDoS) assault that can threaten any Internet-linked network providing services such as Web Server, Email Server, File Transfer, and Transmission Control Protocol (TCP) services. A SYN flood is a TCP State Exhaustion Attack which tries to use link state tables in many components of the network, such as load balancers, firewalls, IPS (IPs) and application servers. Even highcapacity devices that maintain millions of connections can take this type of attack down.

2. **Interception:**

   - Any wireless network that requires a username and password Accessing the local network can detect traffic attacks and monitor them. Usually, a username and password are used in a range of sniffing devices to achieve this purpose by obtaining the initial part of the relationship. It will be disguised as a legitimate user by the attacker and access the network with these credentials. Man-in-the-Middle attack, replay attack, etc. are some well-known forms of interception attacks.

   o **Man-in-the-Middle attack:**

   - A Man-in-the-Middle attack is a kind of cyber attack, when a malicious actor enters into a conversation between two parties, embodies both sides and gets to know information that the two sides tried to send to each other. A middle-in - one intrusion enables a malicious artist to capture, send and receive data intended for another user, or not intended, without any outside party being notified until it is too late. Man-in - the-middle threats, including MITM, MitM, MiM or MIM, can be abbreviated in many respects.

   o **Replay attack:**

   - When cyber criminals send a message onto a secure network, intercept it and then disrupt or divert the user to do what the attacker wants, a repeat attack occurs. It is a phenomenon that is malicious. After the network catches it a hacker does not even need the specialized skills to decipher the message. The attack would succeed by merely restoring the whole lot.

3. **Poisoning**

   - Computer analysis algorithms are often retrained to handle adjustments in the underlying distributor's data during operations. For example, a sample collected (Tr) may be retrained by an intrusion detection system (IDS). An intruder will insert carefully designed experiments into the training data to continuously disrupt the whole learning process. In this case, a Therefore, poisoning can be called an adverse contamination of the training data.

   o **ARP Poisoning:**

   - Address Resolution Protocol (ARP) poisoning occurs when an attacker sends a falsified ARP message through a local area network (LAN) to link an attacker's MAC address to the IP address of a readable network computer or server. Once the intruder's MAC address is added to the initial address, it is possible to send any message sent to the correct MAC address. As a result, an attacker will intercept, modify or block the valid MAC address to expose the valid MAC address. The word address resolution refers to the method of finding a MAC for a network computer that is part of the IP address. A mechanism for mapping IP network addresses to device addresses of a data-related protocol used for Internet Protocol (IP), especially IPv4, is the Address Resolution Protocol (ARP). As part of the OSI network and OSI access layer interface, the protocol operates under the network layer. When IPv4 is implemented, it is used for Ethernet.

4. **Attacks on Access Rights**
    - Privilege Escalation: uses a backdoor of software to manipulate data that would normally be stopped from being viewed by the user.
    - A network manipulation intrusion that utilizes configuration bugs or implementation vulnerabilities to make the intruder elevated network access to related data and programs. The attacker is the victim of privilege escalation. Not every device intrusion provides full access to the compromised network for an unauthorized user. In such cases, elevation is necessary. In such circumstances. There are two forms of escalation of privileges: vertical and horizontal.

❖ **Natural Impact:**

✓ The effect of nature on the company system's hardware includes: explosions, tsunamis, earthquakes, etc. It has an important influence on the structure of an organization that can be compromised and worse, losing all the data of an organization.

❖ **Human impact:**

✓ It is largely due to humans, in addition to natural disasters. The human influence on the structure of an organization is not as minimal as: workers are bribed by a rival organization, employees who are prejudiced against the organization or its leaders are sabotaged, human beings do not take responsibility for unintentionally or deliberately destroying the system, etc.

P2 Describe organizational security procedures. [9]

○ **What is security procedure?**

- A protection protocol is a collection of required tasks carried out by a specific function or safety element. Procedures are normally organized as a straightforward and repeatable process or loop of steps to be taken to achieve an end target. Since first adopted, security protocols consist of a set of rules that facilitate planning, process auditing, and process improvement in order to carry out the organization’s security relations. Procedures provide a starting point for introducing the consistency needed to reduce security process inconsistency, which enhances corporate security control. Reduced uncertainty is also a good way for the safety department to cut down on waste, increase production, and enhance results.

○ **Acceptable Use Policy (AUP).**

- In order to access the corporate network or the Internet, an AUP stipulates the restrictions and procedures that an individual using organizational IT properties must agree to. For new hires, it is a traditional onboarding policy. Until being issued a network ID, they are given an AUP to read and sign. It is advised that the IT, defense, legal, and HR departments of organizations address what is contained in this policy. At SANS, you will find an example that is available for reasonable use.

- **Access Control Policy (ACP).**
  - With respect to the records and information infrastructure of an organization, the ACP outlines the access provided to personnel. Access management guidelines, such as NIST's Access Control and Implementation Manuals, are some of the subjects usually contained in the regulation. Standards for device access, network access restrictions, operating system machine controls, and the sophistication of company passwords are other things protected in this regulation. Additional supplementary elements often outlined include strategies for tracking how to navigate and use organizational systems; how to protect unattended workstations; and how to revoke access after an individual exits the company. At IAPP, an outstanding example of this policy is available.
- **Change Management Policy.**
  - A strategy of change management refers to a structured mechanism for implementing improvements to IT, product creation, and operations/security services. The purpose of a change management initiative is to improve an organization's visibility and appreciation of the expected changes and to ensure that all changes are methodically carried out to reduce the detrimental effect on programs and customers. At SANS, a good example of an IT change management policy open for fair use is.
- **Information Security Policy.**
  - The information management policy of a company is usually high-level policies that can encompass a great range of security measures. The primary information management policy is provided by the corporation to ensure consistency with its specified rules and standards for all workers who use information infrastructure assets within the breadth of the enterprise or its networks. I have had businesses encourage workers to sign this form to confirm that they have read it (which is generally done with the signing of the AUP policy). This proposal is meant for workers to understand that with respect to the sensitivity of company information and IT properties, there are laws they will be kept responsible for. An outstanding example of a cybersecurity strategy that is available for free is offered by the State of Illinois.
- **Incident Response (IR) Policy.**
  - A coordinated approach to how the organization can handle an incident and address the effect on activities is the incident management strategy. It is the one policy that CISOs intend to never have. The purpose of this regulation, however, is to explain the process of handling an incident in order to minimize the harm to company processes, clients, and decrease recovery time and costs. Carnegie

Mellon University provides an example of a high-level IR plan and SANS offers a plan specific to data breaches.

- **Remote Access Policy.**
  - The Remote Access Policy is a guideline that specifies and describes appropriate methods for linking to the internal networks of an entity remotely. I have also seen this strategy include addendums for the use of BYOD properties with regulations. For organizations that have distributed networks with the potential to reach into vulnerable network areas, such as the neighborhood coffee house or unmanaged home networks, this policy is a prerequisite. An example of a remote access policy is available at SANS.
- **Email/Communication Policy.**
  - The email policy of an organization is a manual that is used to formally describe how workers should use the electronic contact medium selected by the corporation. I have seen this policy cover email, blogs, social media, and chat technologies. The primary aim of this proposal is to provide workers with instructions about what is deemed to be the appropriate and inappropriate use of any technology for organizational communication. At SANS, an example of an email policy is available.
- **Disaster Recovery Policy**
  - The disaster response plan of an enterprise will usually require the involvement of both technology and IT departments and will be generated as part of the broader business continuity plan. In the incident management strategy, the CISO and teams can handle an incident. The Corporate Continuity Strategy would be triggered if the incident has a major business effect. At SANS, an instance of a disaster recovery policy is available.
- **Assessing network security risks**

  An evaluation of the risks that your company data can pose needs to be carried out:
  - In case of network security incidents.
  - In the event of natural catastrophes, such as explosions, earthquakes, etc.

  A trained cyber protection officer may conduct computer security risk assessments for details. They have the insight and expertise to point out possible threats to company data that you might not be aware of.
- **Boost employee knowledge of data protection**
  - People are one of the most possible threats to the integrity of business records. Therefore, one of the highest and most important steps to ensure data protection in the sector is the introduction of measures to train and increase awareness among workers in the data security agency.
- **Data security administration**
  - The security threats to business information are still there. Therefore, security interventions cannot be enforced in a limited amount of time, but need to be

carried out on a daily and consistent basis. Each organization should have a particular leader or person with protection and data secrecy expertise of the enterprise responsible for managing the execution of security measures and security data assurance processes.

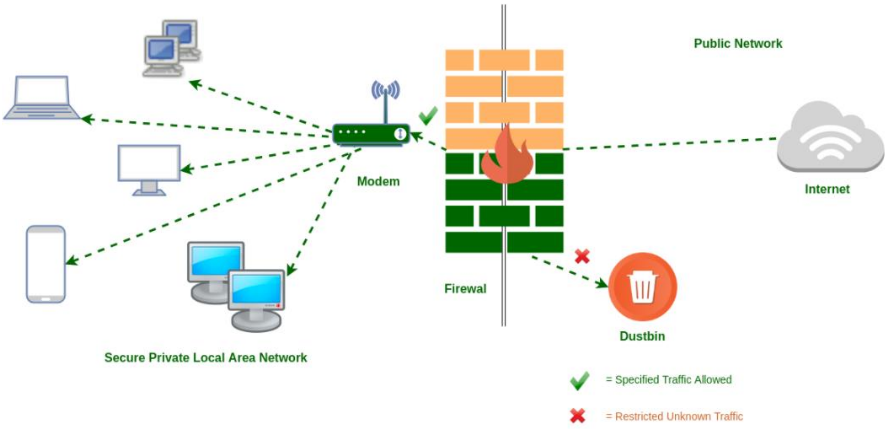
- **Fix and manage incidents**
  - Documents on the method of responding to corporate network security events and data are very important, mitigating the harm to organizations incurred by network security incidents. You may also start recruiting specialist units for review and troubleshooting, in addition.
- **Safely customize the scheme**
  - Both system modules (including software and hardware) designed to fulfill the specifications of the protection policy are also effective steps to help guarantee the security of the business records...
- **Ensuring that the network is broken into different areas**
  - The isolation of different network areas would help distinguish and mitigate the harm caused by network security risks, such as enterprise data leakage, malware infection, in the event of network security events. Poisonous, etc. Using extra firewalls between intranet areas and unreliable remote network areas (Internet zones).
- **Stable corporate data by network security management**
  - To better manage and track network data anomalies early, optimizing identification and avoiding attacks, it is important to use network traffic management systems both internally and externally.
- **Access control**
  - For a company's network, access control is important. Priority accounts must be specifically restricted to major networks, and physical security procedures relating to the regulation of entry to corporate buildings and personal offices (commuters, sirens, magnetic card services, security guards, etc.) are also very important for the management of organizational data access.
- **Increased security from malware**
  - Enterprises can also incorporate solutions for data prevention and malicious code protection. At various stages, there are currently several strategies to prevent the possibility of malware infection: individual user anti-malware solutions, unified anti-malware solutions... You should pick a suitable option for the company, based on the financial circumstances and the size of the company.
- **Updating the patches on a daily basis**
  - More and more new methods of attack are available, so no device at all can be considered to be stable. Updating the fixes and applications of the operating system is also an invaluable task.
- **Perform encryption**

- Finally, prior to sending, execute data encryption. In order to help secure your records, this is an important task. Data encryption allows you to prevent sensitive information from slipping into an attacker's possession in the event of data leakage (due to network security threats or eavesdropping on the transmission line).

- **Testing procedures: ex: data, network, systems, operational impact of security breaches, WANs, intranets, wireless access systems.**
  - Network security: This involves looking for vulnerabilities in the network infrastructure (resources and policies).
  - System software security: Asses weaknesses in software (operating system, database system, and other software) that are depended on
  - Client-side application security: Ensure that the client (browser or any such app/tool) cannot be manipulated.
  - Server-side application security: Server code and its technologies are robust enough to fend off any intrusion.

P3 Identify the potential impact to IT security of incorrect configuration of firewall policies and IDS.

- **Firewall. [10]**
  - Firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predefined security rules. A firewall typically establishes a barrier between a trusted internal network and an untrusted external network, such as the interne. (Shaer, Hamed,2004)


Public Network
Modem
Internet
Firewal
Dustbin
Secure Private Local Area Network
✓ = Specified Traffic Allowed
✖ = Restricted Unknown Traffic

  - Breach avenues: A firewall misconfiguration that results in unintended access can open the door to breaches, data loss, and stolen or ransomed IP. Unplanned outages: A misconfiguration could prevent a customer from engaging with a business, and that downtime leads to lost revenues.
  - Problem with incorrect firewall configuration: The data will be stolen by hackers because the firewall cannot prevent unauthorized access.
  - System security improvements:

+ Prevent invalid access to the system.

+ Monitor access to the URL, ban, or authorize access to the site.

+ User control over user access.

+ Control content of information and packets circulating on the network.

+ Filter packets based on source address, destination address, port number, protocol.

+ Can be used to log all network access attempts and report to the administrator

- We need to have a Firewall Protocol before continuing with the setup. To prevent picking and configuring the firewall inappropriately and reliably.
- A wall is designed and implemented correctly, must be based on a particular policy. That is part of the overall security policy of the organization that uses the firewall.
- Usually, the firewall policy does the following two ways:

  + Deny all, allow only valid traffic.

  + Allow all, prohibit invalid traffic.
- This work is part of network management and security, such as developing a list of ports that are not permitted to be used by Trojans, etc., and then creating rules to ban them. If not, legal traffic would be approved.
- There are many different components of the security policy that are common:

+ Acceptable Usage Statement: Some points to note in this component are:

- ✓ Applications are not allowed to be installed (From sources such as the internet, CD, USB, floppy disk).
- ✓ The program backup mounted on the computer of an organization (allows/does not allow the organization to decide)
- ✓ Use computer accounts, the system must be locked and password secured while no user is present.
- ✓ Only the operations of the company are connected to the machine and the software built on it. It should not be used to bully or harass any human.
- ✓ Email services are allowed.

+ Network Connection Statement: This section is most enforced on the firewall, determining the actual traffic of the network. Some ingredients to note:

- ✓ Only the administrator can perform network scans.
- ✓ Users may use the FTP site to upload and retrieve the appropriate files, but the FTP server might not be available on the local computer.
- ✓ Users can access WWW on port 80 and Email on port 25. But NNTP cannot be accessed on all ports
- ✓ User subnet 10.0.10.0 is allowed to use SSH for remote administration and vice versa.
- ✓ User may not be able to run any Internet chat software.
- ✓ Do not download files larger than 5Mb

- ✓ It is important to install anti-virus software, work well, upgrade the workstation on a weekly basis, and update the server regularly.
- ✓ New hardware can only be mounted on a device by administrators (including NICs and modems)
- ✓ Do not allow unauthorized connections to the internet in any way.

+ Contracted Worker Statement: Some issues that need attention:

- ✓ Temporary or contractually unauthorized users who obtain unauthorized access to services, or carry out network scans, should not copy data to any other system from the server.
- ✓ Do not use FTP, telnet, or SSH without your text-based permission.

+ Firewall Administrator Statement:

- ✓ Firewall administrator must be certified by the firewall provider.
- ✓ Must have SCNA certificate
- ✓ The programs built on the machines on the network must be familiar.
- ✓ You must report directly to the director of the department of defense.
- ✓ 24/24/24 Still be ready
    - It would address several different topics after developing an overarching security strategy, so the volume of data will be very high.

Content filtering: In order to include any form of content filtering, most firewalls can be modified. For both inbound and outbound content, this can be achieved. When companies wish to monitor the access of workers to Internet sites, this is always achieved.

Signature identification: For a single program, a signature is a special identification. A signature is an algorithm in the antivirus universe that distinguishes a single virus uniquely. Firewalls may be designed to detect and block such malware-related signatures or other unwanted programs before they join the network.

Virus scanning services: Content inside the sites will be tested for viruses when web pages are downloaded. For businesses worried about possible risks from Internet-based outlets, this functionality is appealing.

Network Address Translation (NAT): Allows for multiple IP’s tohide behind one. More on this later.

URL filtering: The firewall may opt to block such websites from being viewed by clients inside the company by using a number of techniques. This blocking helps businesses to monitor when and by whom pages can be accessed.

Bandwidth management: Although it’s required in only certain situations, bandwidth management can prevent a certain user or system from hogging the network connection. The most common bandwidth management method is to split the bandwidth available into parts and then build just a certain portion. Accessible to a device or customer.

- o **Consequences of a firewall misconfiguration allows:**

  A firewall misconfiguration that results in unintended access can open the door to breaches, data or information loss and stolen or ransomed IP. A misconfiguration could prevent a customer from engaging with a business, and that downtime leads to lost revenues. Firewall misconfigurations can also have a significant impact on your business.

- **Intrusion Detection System (IDS). [11]**

  IDS is a system that detects signs of intrusion attacks and can initiate actions on other devices to prevent attacks. Unlike firewalls, IDS does not prevent access but only monitors activities on the network to find out the signs of attack and alert the network administrator. (Ashoor, Gore, 2011)

  Based on the surveillance scope, IDS is divided into 2 categories:

  - Network-based IDS (NIDS): These are IDSs that monitor the entire network. The primary source of information for the NIDS is the data packets circulating on the network. NIDS are usually installed at the entrance of the network, which may be in front of or behind the firewall
  - Host-based IDS (HIDS): These are IDSs that monitor the activities of each individual computer. Therefore, the main source of information of HIDS, in addition to data traffic to and from the server, also has system log data and system audit (system audit).

  Based on implementation techniques, IDS is also divided into 2 categories:

  - Signature-based IDS: Signature-based IDS detects intrusions based on intrusions of intrusion, through analyzing network traffic and system logs. This technique requires maintaining a signature database, and this database must be updated regularly every time a new intrusion form or technique is introduced.
  - Anomaly-based IDS: intrusion detection by comparing (statistically) current behavior with the normal operation of the system to detect anomaly that could be a sign of intrusion. For example, under normal conditions, the traffic on a server's network interface is approximately 25% of the maximum communication bandwidth. If at any point this traffic suddenly increases to 50% or more, then it can be assumed that the server is under a DoS attack. In order to function correctly, IDSs of this type must perform a "learning" process, ie monitoring the system's performance under normal conditions to record operational parameters, which is the basis for detection. later abnormalities

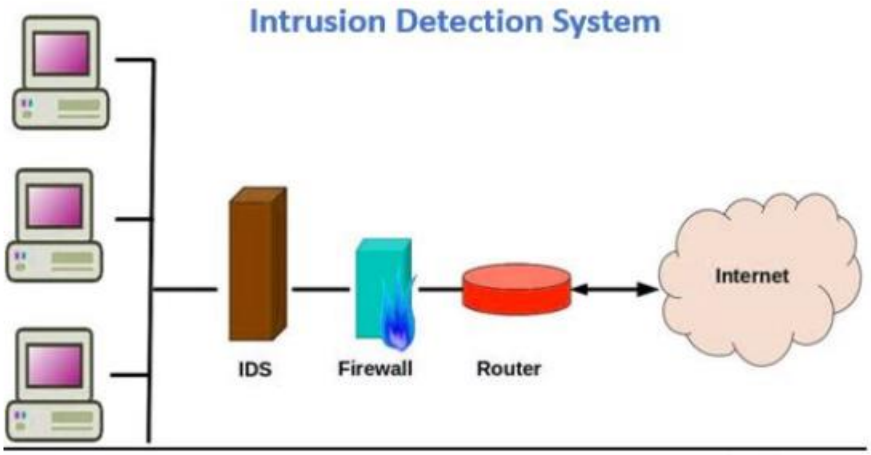
- **Consequences of a IDS misconfiguration allows:**

  - Intrusion detection systems are used with the intent of catching hackers before they do any real damage to the network. They can be networkbased or host-based. An intrusion detection system is based on a host installed on the client, while an intrusion detection system is based on a network located on the network. An intrusion detection system acts as an adaptable safeguard technology for system security after traditional technologies fail. Cyber-attacks will only become more sophisticated, so it is important that protection technologies adapt along with their threats. Intrusion detection systems are used with the intent of catching hackers before they do any real damage to the network. They can be network-based or host-based. An intrusion detection system is based on a host installed on the client, while an intrusion detection system is based on a network located on the network. Misconfiguring the IDS system can lead to some serious consequences, such as:

- Some networks will intentionally take advantage of this misconfiguration error to bypass IDS supervision to access the system that IDS protects.
- IDS will not be able to fully monitor or monitor the traffic accessing the system.
- The IDS system may fail and report on normal access.
- The IDS may misreport activities on the systems it protects.
- Consequences of Misconfiguration of Firewall: Similar to IDS, however misconfiguring the firewall can lead to some more serious consequences than IDS:
- Configuring a firewall incorrectly can cause a number of vulnerabilities in the firewall system. Hackers will take advantage of this vulnerability to destroy or steal data of the system that the
- firewall protects.
- Configuring a firewall incorrectly can cause it to become inoperable or work against the rules desired by the configurator. For example, allow invalid accesses and block valid accesses.

- Configuring a firewall incorrectly can prevent the firewall from working. And then the system that the firewall protects will face the risk of system crash. (Ashoor, Gore, 2011)

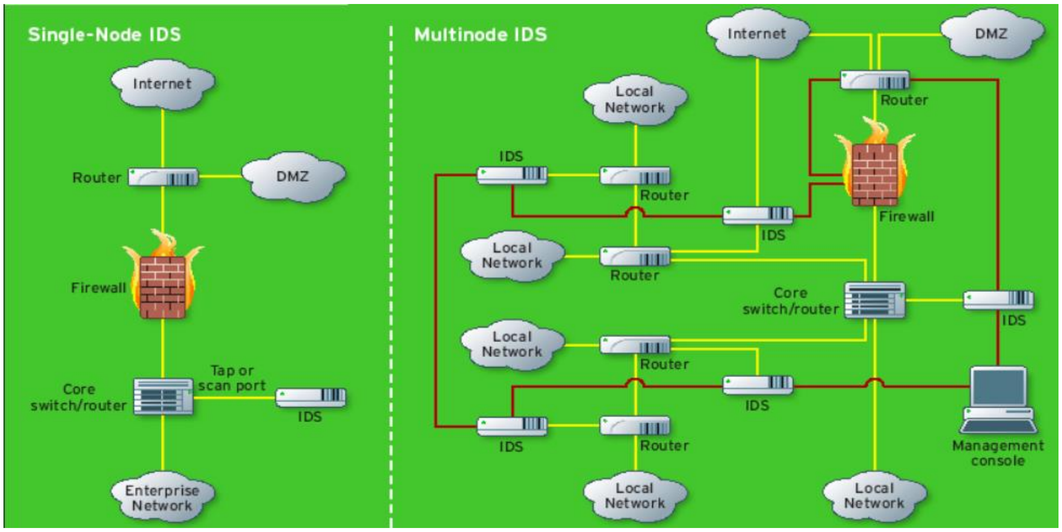
- **How do intrusion detection systems work?**
  - Intrusion detection systems are used to detect anomalies with the aim of catching hackers before they do real damage to a network. They can be either network- or host-based. A host-based intrusion detection system is installed on the client computer, while a network-based intrusion detection system resides on the network.
  - Intrusion detection systems work by either looking for signatures of known attacks or deviations from normal activity. These deviations or anomalies are pushed up the stack and examined at the protocol and application layer. They can effectively detect events such as Christmas tree scans and domain name system (DNS) poisonings.
  - An IDS may be implemented as a software application running on customer hardware or as a network security appliance. Cloud-based intrusion detection systems are also available to protect data and systems in cloud deployments.



- **Possible responses to a triggered event:**
  - Disconnect communications and block transmission of traffic
  - Block a user from accessing a resource
  - Send alerts of an event trigger to other hosts, IDS monitors, and administrators.
  - IDS-Detect something bad may be taking place and send an alert.
- **Potential consequences of incorrect IDS configuration**

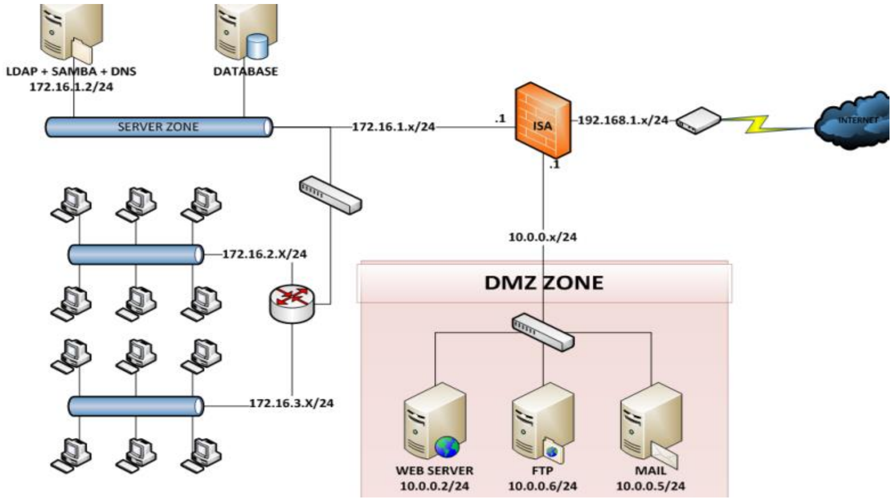
  Misconfiguring the IDS system can lead to some serious consequences, such as:
  - Some networks will intentionally take advantage of this misconfiguration error to bypass IDS supervision to access the system that IDS protects
  - IDS will not be able to fully monitor or monitor the traffic accessing the system.
  - The IDS system may fail and report on normal access.
  - The IDS may misreport activities on the systems it protects.

  Consequences of Misconfiguration of Firewall similar to IDS, however misconfiguring the firewall can lead to some more serious consequences than IDS:
  - Configuring a firewall incorrectly can cause a number of vulnerabilities in the firewall system. Hackers will take advantage of this vulnerability to destroy or steal data of the system that the firewall protects.
  - Configuring a firewall incorrectly can cause it to become inoperable or work against the rules desired by the configurator. For example, allow invalid accesses and block valid accesses.
  - Configuring a firewall incorrectly can prevent the firewall from working. And then the system that the firewall protects will face the risk of a system crash.

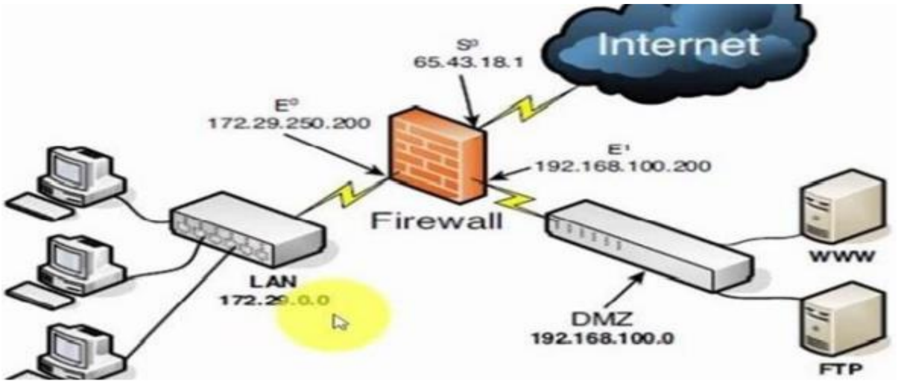


P4 Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security.

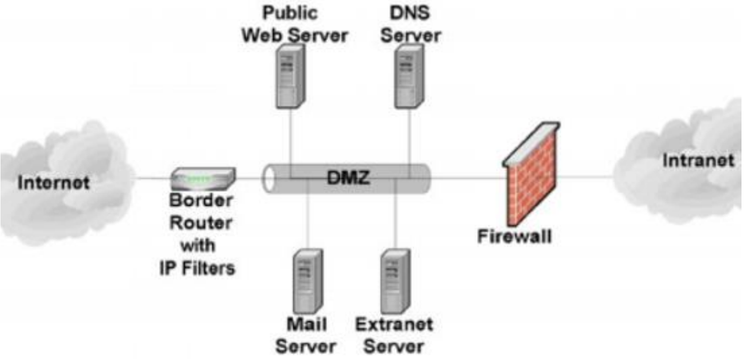
- **Demilitarized zone (DMZ). [12]**
  - Demilitarized zone, also referred to as the ring network, (DMZ). The DMZ is a part of the network where you position servers that must be available from the network's external and internal sources. Do not link to any network directly and it must still be reached through a firewall. The military term DMZ is used when a region of little to no compliance or control is described. (Hunter, 2015)
  - For instance, when an attacker tries to reach Interface 1, a request from a web server or proxy server must be forged into Interface 2 when a single firewall is used to build a DMZ. By adding a corresponding NIC number to the single firewall, two or more separate DMZ zones with different network IDs can be established.
  - An important firewall-related concept is the demilitarized zone (DMZ), sometimes called a perimeter network.
  - A DMZ is part of a network through which you position servers that need to be available both outside and within your network by sources.
  - It is not directly connected to any network and must instead be reached through a firewall.
  - The military term DMZ is used because it describes an area that has little or no enforcement or policing.
  - Deploy DMZ in NorthStar: There are two DMZ models that can be deployed in NorthStar are single firewall (or three legged firewall) and dual firewall.
  - The DMZ is a neutral network area between the local network and the internet



- **Single firewall**
    - A three-NIC (network interface card) system is required. Specifically, one NIC is connected to the external network, the other to the DMZ network, and the other to the internal network.



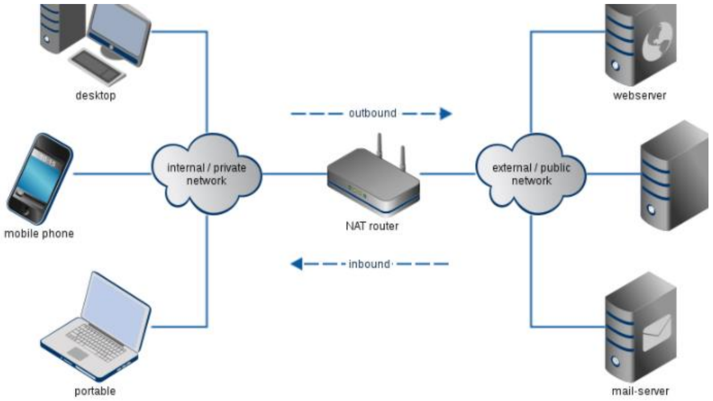
- **Dual firewall**
    - The first firewall (called the front-end firewall) has one NIC attached to the external network (external interface) and the other NIC connected to the DMZ. It involves two firewall modules, each with two NICs, and is organized as follows: (internal interface). The management of traffic from the Internet to the DMZ and the internal network is the responsibility of this front-end firewall.
    - The second firewall has one NIC linked to the DMZ (external interface) and the other NIC connected to the internal network (called the back-end firewall) (internal interface). This back-end firewall is responsible for monitoring access to the internal network from the DMZ and the Internet.
    - Using DMZs gives your firewall configuration an extra level of flexibility, protection, and complexity.



- You can build an extra move by using a DMZ that makes it harder for an attacker to obtain access to the internal network.
- An attacker that attempted to come in via Interface 1 would have to spoof a request from either the web server or proxy server into Interface 2 before it could be forwarded to the internal network using the opposite scenario.
- Although it is not impossible for an intruder to gain access to the internal network through a DMZ, it is difficult.
- One of the ways to address provider/attack target DDOS attacks is the use of the Client Puzzle Protocol. This Client Puzzle Protocol is designed to endure attacks that decrease the capacity of the server to initiate service requests by connecting through the microdevice-controlled Demilitarized Zone approach. DMZ is the Demilitarized Zone abbreviation, also known as the protective zone, as well as the perimeter network used to defend the internal system where all ports are open so that outsiders can reach them. Therefore, if an intrusion happens or anyone purposely targets the server using DMZ, only the DMZ host can be reached by the attacker, not the internal network.
- DMZ’s key function is to monitor network traffic. This is because the basic working concept of DMS is to transfer all network services from one network to another separate network in order to prevent a single point of failure that could lead to a breakdown of the control system.
- Highly helpful for NorthStar so all sources can safely access the servers without jeopardizing the main LAN due to disruption, which can be very significant for NorthStar since it ensures that their individual node is only disconnected from the connection client. This brings to NorthStar an extra layer of protection which allows for more stable server administration, as well as an attack case that can be much smoother because only the DMZ, not the LAN, can be affected.

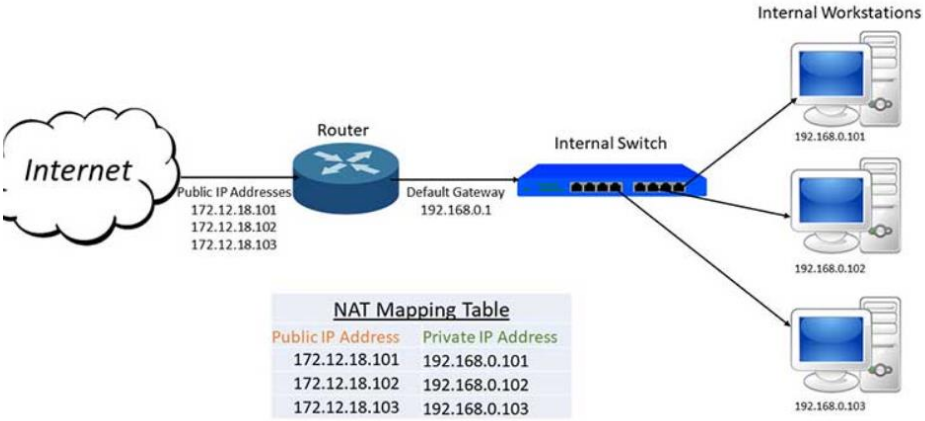
o **NAT (Network Address Translation) [13]**

- Network Address Translation (NAT) is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts. Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table. NAT generally operates on router or firewall. (



- In a network, for example, two A and B servers are connected. Now both need the same destination at the same time on the same ports, say 1000, on the server-side. If NAT converts an IP address to just 34, so all of their IP addresses will be hidden by the public IP address of the network and sent to the destination when their packets arrive at NAT. The destination sends a reply to the public IP address of the router. Therefore, it is not clear to the NAT which server the answer belongs to when a reply is sent (because the source port numbers for both A and B are the same). Therefore, NAT often conceals the source port number and generates an entry in the NAT table to prevent such a problem.
- In the network, we state that the NAT Server machine has an IP of 192.168.1.2 and a machine that installs the Web Server service with an IP of 192.168.1.5, and that the machine on the Internet that accesses our network through the Web protocol is NAT. The server that connects to the machine has an IP of 192.168.1.5 o. We have to create a NAT Server with 2 separate LAN Cards. One Card connects to other computers in the network via Switch, the other Card connects directly to ADSL Router. At that time, the Client want to access the Internet must be through NAT Server and from there NAT Server will through ADSL Router to connect to the Internet. (Audet, Jennings,2007)
- NAT (Network Address Translation) is a technique that allows one or more internal IP addresses to be converted to one or more external IP addresses. Network Address Translation helps the local network address (Private) gain access to the public network (Internet).
- The basic principle of NAT is that many computers can-hide behind a single IP address.
- The main reason you need to do this is because there simply aren’t enough IPv4 addresses to go around.

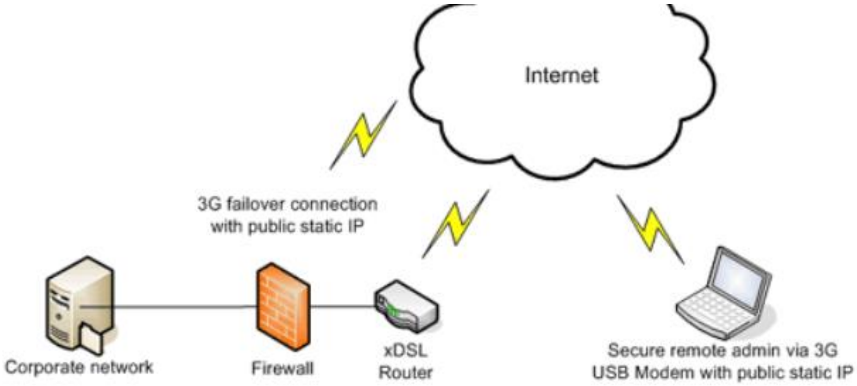
- Using NAT means that only one registered IP address is needed on the system's external interface, acting as the gateway between the internal and external networks.
- Because NAT Server has CPU & RAM much stronger than CPU & RAM of ADSL Router, it has faster processing speed.
- Advantages of implementing NAT:
    - ✓ Saving IPv4 addresses: The number of users accessing the internet is increasing. This leads to the risk of IPv4 address shortages. The NAT technique helps to reduce the number of IP addresses to use
- Helps to conceal IP inside LAN:
    - ✓ NAT can share internet connections for many different computers, mobile devices in LAN with only one public IP address.
- Some reasons that NorthStar should use NAT.
    - ✓ Resolving exam subject matter address of ipv4 company
    - ✓ Hide IP address in LAN
    - ✓ NAT helps network administrators filter incoming and outgoing packets from an IP address and allow or deny access to a specific port.
- Improved security when deploying NAT:
    - ✓ Help administrators to remove packets containing malicious code or malware
    - ✓ Help users conceal IP to avoid IP detection and avoid being tracked.
    - ✓ Help users verify and prevent access with malicious intent



NAT Mapping Table

Public IP Address	Private IP Address
172.12.18.101	192.168.0.101
172.12.18.102	192.168.0.102
172.12.18.103	192.168.0.103

- **Static IP: [14]**
    - A static IP address is an IP address that is manually configured for the device, as opposed to an IP address assigned through a DHCP server. It is called a "static" address because it doesn't change. This is the complete opposite of dynamic IP addresses, which can be changed



- The IP address is used to give the network an address close to how the number of the house and the street name operate. The IP address can be used to identify other networks, since these can be used. If some bad intent is given, use it to find it. Since it is the network address, communication with each other is essential for networks. The distinction between a static IP is that for a single system, a manually programmed IP is installed and will still stay the same as an IP device that will differ by network.
- That implies that security precautions can be applied to that specific IP address by providing a static IP address, allowing more setup and security when a firewall is behind an ever-changing IP update. But not so deep, the protection that this layer will add is a very simple and effective way to secure a specific computer on the network. This approach is a consistent way to provide another layer of protection. (Lu, Sahni,2010)

✓ **Function:**

- Static IP address will help you connect to the Internet quickly without having to re-issue a new IP address.
- A static IP address is required for some services and games. That means that even after rebooting the model, the set IP address does not change.
- Static IP addresses also help speed up web access and download torrent files
- The static IP address is essentially intended for secure communication with local network computers. Companies use network printers with static IP addresses, for instance.
- If there is static IP, the business will use the fax machine to look at the camera from outside.

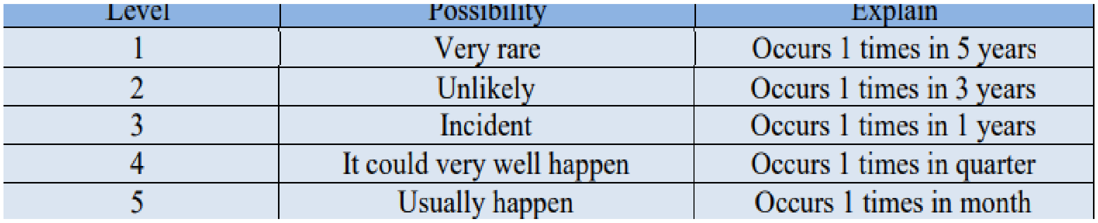
✓ **Advantages of implementing static IP:**

- Better DNS support.
- The static IP address will help you connect to the Internet quickly without having to re-issue a new IP address.
- Static IP addresses also help to speed up access and download files.
- More convenient in remote access.
- More reliable geolocation services and communications.

M1 Propose a method to assess and treat IT security risks. [15]

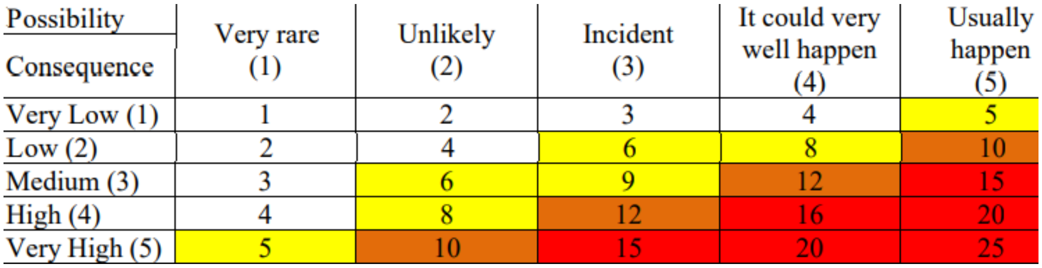
1. **Method to assess and treat risk**

- **Step 1:**
  - List all of the organization's function or activities: The more detailed the listing, the more accurate the assessment may be; the listing will look something like this:
    + According to the administration function.
    + According to geographic factories and offices.
    + According to the organizational structure, functional departments.
    + According to the execution order of processes, processes.
- **Step 2:**
  - Determine the threats and dangers that could exist: We must define the hazards that pose a danger for each job move identified. It is then pursued to classify the potential hazards depending on the above risks. The threat may be person, device, procedure, external, or a mixture of the above.
- **Step 3:**
  - The magnitude of the injury or the potential to inflict it: To assess the seriousness, we must compare the organization's activities in the past to see how anything has occurred. It is simple to calculate the magnitude of the damage if it occurred; if it did not occur, it can be estimated; if it occurred, we would separate the various types of damage to make it simpler. For ease of assessment, it is usually divided into 5 levels of damage from 1 ~ 5, depending on the size of the organization that defines the level of damage differently.
- **Step 4:**
  - Determine the probability: To determine the likelihood, we would look at the organization's operating past and see how often the issue happens, and then break it into levels to make it easy to price (reference example below). If the newly established organization has no data, we can refer to organizations in the same field, the same industry, or the same operating environment.



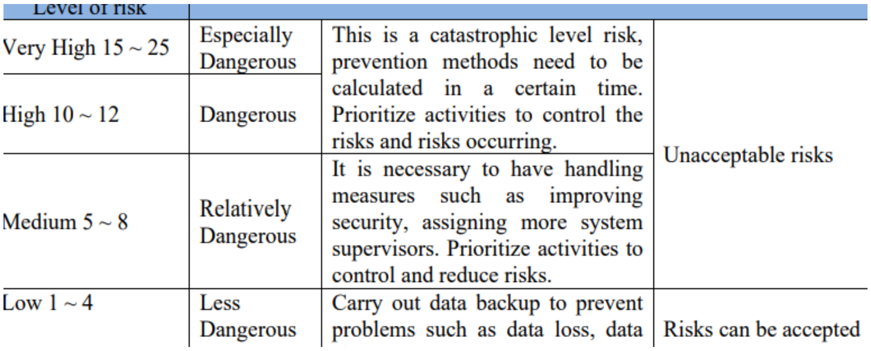
Level	Possibility	Explain
1	Very rare	Occurs 1 times in 5 years
2	Unlikely	Occurs 1 times in 3 years
3	Incident	Occurs 1 times in 1 years
4	It could very well happen	Occurs 1 times in quarter
5	Usually happen	Occurs 1 times in month

- **Step 5:**
  - Determine the risk level: It is split into four categories: low (1–4), medium (5–8), moderate (10–12), and extremely high (15–25).



Possibility Consequence	Very rare (1)	Unlikely (2)	Incident (3)	It could very well happen (4)	Usually happen (5)
Very Low (1)	1	2	3	4	5
Low (2)	2	4	6	8	10
Medium (3)	3	6	9	12	15
High (4)	4	8	12	16	20
Very High (5)	5	10	15	20	25

- **Step 6:**
  - Justification must be established: After the levels of risk have been determined, we must prioritize control measures depending on the various levels of risk. A control measure may be the establishment of a risk management mechanism. Risks, rules, forms, and legislation, to name a handful. Risk management is typically prioritized for operations with a high to an extremely high level of risk, whereas for activities with a low level of risk, it is considered dependent on the needs of the organization.



Level of risk			
Very High 15 ~ 25	Especially Dangerous	This is a catastrophic level risk, prevention methods need to be calculated in a certain time. Prioritize activities to control the risks and risks occurring.	Unacceptable risks
High 10 ~ 12	Dangerous		
Medium 5 ~ 8	Relatively Dangerous	It is necessary to have handling measures such as improving security, assigning more system supervisors. Prioritize activities to control and reduce risks.	
Low 1 ~ 4	Less Dangerous	Carry out data backup to prevent problems such as data loss, data	Risks can be accepted

- **Step 7:**
  - Assign a conductor and ensure that the assessment is followed up on: Following the conclusion of the above evaluation phases, top management will review and authorize the report, and people will be delegated to execute the control mechanisms as well as track and analyze the work's effectiveness. The company can monitor the risks of all operations using this approach, which also helps to reduce the documentation framework and increase performance.

2. **Things that need security**

- **Software:** Software is a set of files that are connected together and are used to manipulate hardware. The software must also be safeguarded. If the program crashes, the hardware will run wrongly or data will be lost. Since the software is a key component of data storage and recovery, it must be shielded from external influences such as hackers.
- **About Software:**
- Check apps, software for security vulnerabilities on a daily basis.
- Upgrade or refresh the program on a regular basis.
- Using security software such as anti-virus, anti-malware, ...

- **Data:** This takes precedence over all else that has to be safeguarded in the system. Individuals and organizations must back up their data and archive it in a secure location.
- **About Data:**
- Data backup: All of the data on the monitor, server, server, and so on can be copied and saved in one or more other storage devices as a backup.
- Data encryption: Converting data from one format to another or into a code that can only be read by someone who has the decryption key or password

M2 Discuss three benefits to implement network monitoring systems with supporting reasons. [16]

A network management system keeps track of the failures, results, and status of devices and computers in a network. The machine comes with logging tools that assists system managers in recording and monitoring data that goes through it.

- The fundamentals of network monitoring:
  - Mastering tracking instruments, facilities, and applications, both internal and open source.
  - For tracking, mastering parts, units, devices, facilities, and appliances.
  - To facilitate the processing and review of monitoring data with methodical methods and solutions. Snort, Wireshark, Nessus, Nmap, and other software are examples.
- Ascertain that the team is well-versed in the industry. Since a network infrastructure is so large, network safety control is critical, and it necessitates knowledge of the system's components, such as:
- The server

- Hub

- Router

- Switch

- Workstation

- Software and applications in workstations and servers.
- SIEM, also known as security information and event management, was developed with the aim of gathering data and information about security incidents in mind. From terminals to consolidated storage, it is measured. We can detect the threats of intruder attacks due to the research findings of network security framework software.
- The main benefits:
- SIEM can track network intrusion and attack issues that traditional sensors are unable to detect.
- Makes troubleshooting simpler but more efficient
- SIEM is an excellent commodity for major businesses, companies, insurers, organisations, and government departments.
- Network monitoring software: Splunk is a network management app that a lot of users use. Splunk is a feature-rich log analysis and architecture framework built on the Lucence and MongoDB platforms. This platform is designed to identify, track, and interpret vast quantities of data from applications, networks, apps, and network infrastructure equipment.
- Advantages:
- Constantly updating data in real-time
- Keywords, search functions, and structure are all included in the smart search engine, from which you can access anything you want.
- Disadvantages:
- It takes a long time to read, use, and run.
- There must be a different structure that is wide enough. Splunk isn't ideal for medium or small-scale applications, of course.
- Solutions for securing the network system: There are three major solutions for securing the monitoring system:
- To address intrinsic shortcomings, a solution to manage and interpret security incidents is a synthesis of the two solutions above. As a result, the documentation will be focused on implementing this approach.
- Focus on capturing and archiving logs for security information processing solutions.
- The aim of a security incident management solution is to review and process logs in order to send alerts to users.
- Problems with the network infrastructure include:
- Printing errors.
- Poor quality cable.
- The transmission is slow.
- DNS error.
- The touch machine cannot connect to wifi.

- Low bandwidth.
- Device not working.
- Cannot grant or obtain an IP address.
- Can’t connect to server.
- To track down issues, a network management system is used:
- The operational status of network devices.
- Connection between devices.
- Unusual practices, such as hacking or tracking invalid entry, should be kept an eye on.
- Device assessment is aided by a network management system:
- The communication status between terminals will be monitored and reported on by the network monitoring system.
- Network monitoring system: A network monitoring system can gather bandwidth data on a routine basis and warn you if the bandwidth is unusually low or high.
- In terms of permissions, the network management system can keep track of all system access thresholds as well as the distinction between legitimate and invalid access.
- Reasons to use a network management system include:
- The administrator will receive instant notification by text message or email when the network monitoring system watches in real time and senses any suspicious activities.
- A network management device capable of determining the source of a problem, assessing it, and diagnosing it.
- It is important to keep track of the state of a security device, assess its efficacy, and further hack it.
- Track all active devices in the network, including computers, workstations, network devices, and software, to increase system capacity.

- **Conclusion**
  - LAN is the local network of an organization that is prevented from unauthorized attacks and intrusion by hackers from outside to protect the system data of a safe organization.
  - What I’ve said so far, as well as specific examples, was intended to help people better understand information technology security, which is a critical task that will help the company grow more quickly. My lecture will include the processes and procedures for detecting and assessing IT security risks, as well as management measures for safeguarding confidential data and facilities in the workplace.

References

[1] Rieck, K., Holz, T., Willems, C., Düssel, P. and Laskov, P., 2008, July. Learning and classification of malware behavior. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment* (pp. 108-125). Springer, Berlin, Heidelberg.
[2] Harley, D., Slade, R. and Gattiker, U.E., 2001. *Viruses revealed*. Berkeley: Osborne/McGraw-Hill.
[3] Erbschloe, M., 2004. *Trojans, worms, and spyware: a computer security professional's guide to malicious code*. Elsevier.
[4] Erbschloe, M., 2004. *Trojans, worms, and spyware: a computer security professional's guide to malicious code*. Elsevier.
[5] Erturk, E., 2012, June. A case study in open source software security and privacy: Android adware. In *World Congress on Internet Security (WorldCIS-2012)* (pp. 189-191). IEEE.
[6] Yaqoob, I., Ahmed, E., ur Rehman, M.H., Ahmed, A.I.A., Al-garadi, M.A., Imran, M. and Guizani, M., 2017. The rise of ransomware and emerging security challenges in the Internet of Things. *Computer Networks*, *129*, pp.444-458.
[7] Vétillard, E. and Ferrari, A., 2010, April. Combined attacks and countermeasures. In *International Conference on Smart Card Research and Advanced Applications* (pp. 133-147). Springer, Berlin, Heidelberg.
[8] Xu, H., Su, J., Zong, X. and Yan, L., 2017, September. Attack identification for software-defined networking based on attack trees and extension innovation methods. In *2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)* (Vol. 1, pp. 485-489). IEEE.
[9] Peltier, T.R., 2016. *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*. CRC Press.
[10] Al-Shaer, E.S. and Hamed, H.H., 2004. Modeling and management of firewall policies. *IEEE Transactions on network and service management*, *1*(1), pp.2-10.
[11] Ashoor, A.S. and Gore, S., 2011. Importance of intrusion detection system (IDS). *International Journal of Scientific and Engineering Research*, *2*(1), pp.1-4.
[12] Hunter, W.C., 2015. The visual representation of border tourism: Demilitarized zone (DMZ) and Dokdo in South Korea. *International Journal of Tourism Research*, *17*(2), pp.151-160.
[13] Audet, F. and Jennings, C., 2007. *Network address translation (NAT) behavioral requirements for unicast UDP*. BCP 127, RFC 4787, January.
[14] Lu, W. and Sahni, S., 2010. Recursively Partitioned Static IP Router Tables. *IEEE Transactions on Computers*, *59*(12), pp.1683-1690.
[15] Mayer, N. and Feltus, C., 2017, October. Evaluation of the risk and security overlay of archimate to model information system security risks. In *2017 IEEE 21st International Enterprise Distributed Object Computing Workshop (EDOCW)* (pp. 106-116). IEEE.
[16] Ramachandran, K.N., Belding-Royer, E.M. and AImeroth, K.C., 2004, October. DAMON: A distributed architecture for monitoring multi-hop mobile networks. In *2004 First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004.* (pp. 601-609). IEEE.
[17] Blunden, B., 2012. *The Rootkit arsenal: Escape and evasion in the dark corners of the system*. Jones & Bartlett Publishers.
[18] Fischer, R., Edward Halibozek, M.B.A. and Walters, D., 2012. *Introduction to security*. Butterworth-Heinemann.
[19] Liu, X., Yang, X. and Xia, Y., 2010. Netfence: preventing internet denial of service from inside out. *ACM SIGCOMM Computer Communication Review*, *40*(4), pp.255-266.
[20] Clarke-Salt, J., 2009. *SQL injection attacks and defense*. Elsevier.

[21] Huang, D.L., Rau, P.L.P. and Salvendy, G., 2010. Perception of information security. *Behaviour & Information Technology*, *29*(3), pp.221-232.