# ASSIGNMENT FRONT SHEET

| | | | |
|---|---|---|---|
| **Qualification** | **BTEC Level 5 HND Diploma in Computing** | | |
| **Unit number and title** | **Unit 5: Security** | | |
| **Submission date** | 10/12/2020 | **Date Received 1st submission** | |
| **Re-submission Date** | 18/12/2020 | **Date Received 2nd submission** | |
| **Student Name** | PHAM CAO NGUYEN | **Student ID** | GCC18074 |
| **Class** | GCC0801 | **Assessor name** | LE HUYNH QUOC BAO |
| **Student declaration**<br><br>I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice. | | | |
| | | **Student's signature** | CAONGUYEN |

**Grading grid**

| P1 | P2 | P3 | P4 | M1 | M2 | D1 |
|---|---|---|---|---|---|---|
| | | | | | | |

| ❒ Summative Feedback: | ❒ Resubmission Feedback: |
|---|---|
| | |

| Grade: | Assessor Signature: | Date: |
|---|---|---|
| Signature & Date: | | |

# Assessment Brief

| | | | |
|---|---|---|---|
| **Qualification** | **BTEC Level 5 HND Diploma in Computing** | | |
| **Unit number** | Unit 5: Security | | |
| **Assignment title** | Security Presentation | | |
| **Academic Year** | 2020 | | |
| **Unit Tutor** | | | |
| **Issue date** | | **Submission date** | |
| **IV name and date** | Khoa Canh Nguyen, Michael Omar, Nhung 9th/01/2020 | | |

**Submission Format**

The submission is in the form of two documents/files:

1. A ten-minute Microsoft® PowerPoint® style presentation to be presented to your colleagues. The presentation can include links to performance data with additional **speaker notes** and a **bibliography using the Harvard referencing system.** The presentation slides for the findings should be submitted with speaker notes as one copy.
2. A detailed report that provides more thorough, evaluated or critically reviewed technical information on all of the topics.

You are required to make use of the font **Calibri, Font size 12, Line spacing 1.5, Headings,** P**aragraphs**, S**ubsections and illustrations** as appropriate, and all work must be **supported with research and referenced** using the **Harvard referencing system.**

**Unit Learning Outcomes**

| |
|---|
| **LO1** Assess risks to IT security.<br>**LO2** Describe IT security solutions. |
| **Assignment Brief and Guidance** |
| You work as a trainee IT Security Specialist for a leading Security consultancy in Vietnam called FPT Information security FIS.<br><br>FIS works with medium sized companies in Vietnam, advising and implementing technical solutions to potential IT security risks. Most customers have outsourced their security concerns due to lacking the technical expertise in house. As part of your role, your manager Jonson has asked you to create an engaging presentation to help train junior staff members on the tools and techniques associated with identifying and assessing IT security risks together with the organizational policies to protect business critical data and equipment.<br><br>In addition to your presentation you should also provide a detailed report containing a technical review of the topics covered in the presentation.<br><br>Your presentation should:<br><br>1. **Identify** the security threats FIS secure may face if they have a security breach. Give an example of a recently publicized security breach and discuss its consequences<br>2. **Describe** a variety of organizational procedures an organization can set up to reduce the effects to the business of a security breach.<br>3. **Propose** a method that FIS can use to prioritize the management of different types of risk<br>4. **Discuss** three benefits to FIS of implementing network monitoring system giving suitable reasons.<br>5. Investigate network security, **identifying** issues with firewalls and **IDS** incorrect configuration and **show** through examples how different techniques can be implemented to improve network security.<br>6. **Investigate** a 'trusted network' and through an analysis of positive and negative issues determine how it can be part of a security system used by FIS.<br><br>Your detailed report should include a summary of your presentation as well as additional, evaluated or critically reviewed technical notes on all of the expected topics. |

| **Learning Outcomes and Assessment Criteria** | | |
|---|---|---|
| **Pass** | **Merit** | **Distinction** |
| **LO1** Assess risks to IT security | | |
| **P1** Identify types of security threat to organisations.<br>Give an example of a recently publicized security breach and discuss its | **M1** Propose a method to assess and treat IT security risks. | **LO1 & 2**<br>**D1** Investigate how a 'trusted network' may be part of an IT security solution. |

| | | |
|---|---|---|
| consequences.<br><br>**P2** Describe at least 3 organisational security procedures. | | |
| **LO2** Describe IT security solutions | | |
| **P3** Identify the potential impact to IT security of incorrect configuration of firewall policies and IDS.<br><br>**P4** Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security. | **M2** Discuss three benefits to implement network monitoring systems with supporting reasons. | |

# Contents

## P1 Identify types of security threat to organisations. [2]

Currently, some companies in Vietnam are worried about the risk of security of hidden information technology that business customers should be concerned about.

## Give an example of a recently publicized security breach and discuss its consequences. [1]

- **For example**

- On 29 July 2016, a group suspected coming from China launched hacker attacks on the website of Vietnam Airlines with client information leaked and on flight information screens at Vietnam's 2 biggest airports, “Tan Son Nhat” International Airport and “Noi Bai” International Airport, posting derogatory messages against Vietnam and the Philippines in their territorial row against China in the South China Sea.

- According to the Civil Aviation Administration of Vietnam, at 13h46 on 29 July the IT-systems of VietJet, Vietnam Airlines to do the flight check-ins at the “Tan Son Nhat” International Airport were attacked and had to stop working. At 16h07’ A team of self-proclaimed Chinese Hackers attacked flight information screens at “Noi Bai” International Airport, posting notices that state media said criticized the Philippines and Vietnam and their claims in the South China Sea. The hackers also took control of the speaker system at Noi Bai airport for a few minutes, during which the speakers broadcast a male voice distorting Viet Nam's claims over the East Sea in English. The check-ins system of Vietnam Airlines there was also attacked and had to switch to manual procedure completion, which lead to flight delays. Altogether, “Noi Bai” airport has 30 flight, and “Tan Son Nhat” more than 60 flight delayed from 15 til more than an hour, affect about 2.000 passengers.

- The official website of Vietnam Airlines, vietnamairlines.com, was also hacked by the same group at about 4pm the same day. The website page was replaced by the same picture that appeared on the airports’ screens. The website was back to normal at 18.30pm, however, the airlines’ customer database was stolen and made public on the internet, according to a press release from Vietnam Airlines. The airlines advised its members to change their account passwords as soon as the network system is recovered.

- Another 2 webpages were also compromised, are the webpage from Vietnam Football Federation on the same day and from National Economics University (Vietnam) the next day.

- On next day, 50% of the computers can check in again, but the flight information screens are still off at “Noi Bai” airport. The speaker system is also still not working again.

At “Tan Son Nhat” airport the situation is similar to “Noi Bai” with no flight information screens and no speaker system.

❖ **Digital Security Risks:**

**I. MALWARE.**

- 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.

- There are several types of malware which can attack the machine of a user:

○ **Circulation/Infection.**

**1. Viruses.**

- A virus is a malicious type that can copy itself to other computers and propagate. When a user begins one of those contaminated applications, viruses propagate to other machines by linking themselves to different programs and using javascript. Viruses can also distribute bugs in web applications by way of script archives, attachments, and cross-site scripting. Viruses can be used for stolen information, malicious machines and networks, botnets and stealing of capital, notoriety making, etc.
- Programs that silently bind and execute to another document or program upon opening that document or program.
- It could include instructions that trigger issues ranging from showing an irritating warning to removing files from a hard drive to constantly crashing a device.
- Antivirus software defends against viruses.

- Drawback to antivirus software is that it must be modified to detect new viruses.
- Updates (definition files or signature files) can be downloaded automatically from the internet to a user's computer.

**2. Worms.**

✓ The most every kinds of ransomware are machine worms. By using operating system bugs, they propagate across computer networks. Worms normally harm their host networks by bandwidth consumption and web servers overload. Computer worms can also contain payloads to host computers that damage them. Payloads are bits of code written to work beyond merely passing the worm on infected machines. Payloads are usually intended for data copying, removing or botnets generating archives. Computer worms can be categorized as a form of computer virus but computer worms are differentiated from popular viruses by a number of features. An important difference is that machine worms can reproduce themselves and propagate independently whereas viruses rely on human activity (run a program, open a file, etc). It is not appropriate to reproduce them. Worms often communicate through send mass emails to user contacts with infected attachments.

✓ Although similar in nature, worms are different from viruses in two regards:

- A virus, such as an e-mail message, sticks itself to a computer document and is transmitted by going along with the document.
- To initiate the infection, a virus requires the user to perform some kind of operation, such as beginning a program or reading an e-mail address.
- Worms are typically transmitted as separate executable programs via e-mail attachments.
- In many instances, reading the e-mail message starts the worm.
- If the worm does not start automatically, attackers can trick the user to start the program and launch the worm.

**3. Trojan horses.**

- Programs that mask their true intent and then when triggered, reveal themselves.
- Might disguise itself as free programs for calendars or other interesting software.
- A Trojan horse usually referred to as a 'Trojan,' is a form of malware. It masks itself as a standard user who downloads or installs malware. The Trojan may provide remote access to an infected machine from a malicious group. Once an intruder has access to the infected computer, it can steal data (logins, financial data, and even the electronic money), install additional malware, modify files, track the user's operation (screen

views, keylogging, etc), botnets using the device, and anonymize the attacker's Internet activity.

**Common strategies:**

- Giving the name of a file connected with a benevolent program to a malicious program.
- Combining two or more executable programs into a single filename.

**Defend against Trojan horses with the following products:**

- One of the best protections against combination systems is antivirus tools.
- Special software that alerts you to a Trojan horse program in life.
- Anti-Trojan horse software which disinfects a Trojan horse-containing device.

4. **Rootkit.**

- 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.

- **Collect data.**

1. **Spyware.**

- 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.

**2. Adware**

- 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.

**3. Ransomware**

- 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.

- **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.

- **Launch attacks**

**Zombie and botnet**

- One of the most common malware payloads currently held by trojans, worms, and viruses is software that allows the infected device to be placed under an attacker's remote control.
- This infected robot (bot) computer is known as a zombie.
- They build a botnet under the control of the attacker when hundreds, thousands, or even hundreds of thousands of zombie computers are collected into a logical computer network (bot herder).
- Infected zombie computers are waiting for orders from the bot herders through a command and control (C&C or C2) structure about which computers to attack and how.
- A common botnet C&C mechanism used today is the Hypertext Transport Protocol (HTTP).

- By automatically logging into a website that the bot herder runs, a zombie will obtain its instructions.
- A third-party website on which data has been put that the zombie knows how to view as commands is another way to obtain instructions.
- Some botnets also use blogs or send specially coded attack commands through posts or notes posted on Facebook on the Twitter social network service.

  + Six intruder categories: hackers, crackers, script kiddies, spies, staff, and cyber-terrorists

  + Identity attacks attempt to assume the identity of a valid-user

  + Service denial (DoS) attacks flood requests from a server or system, rendering it unable to respond to legitimate requests.

  + Malicious code (malware) consists of computer programs that are developed deliberately to hack into machines or cause computer mayhem.

- **Networking-Based Attacks**

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

- 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.

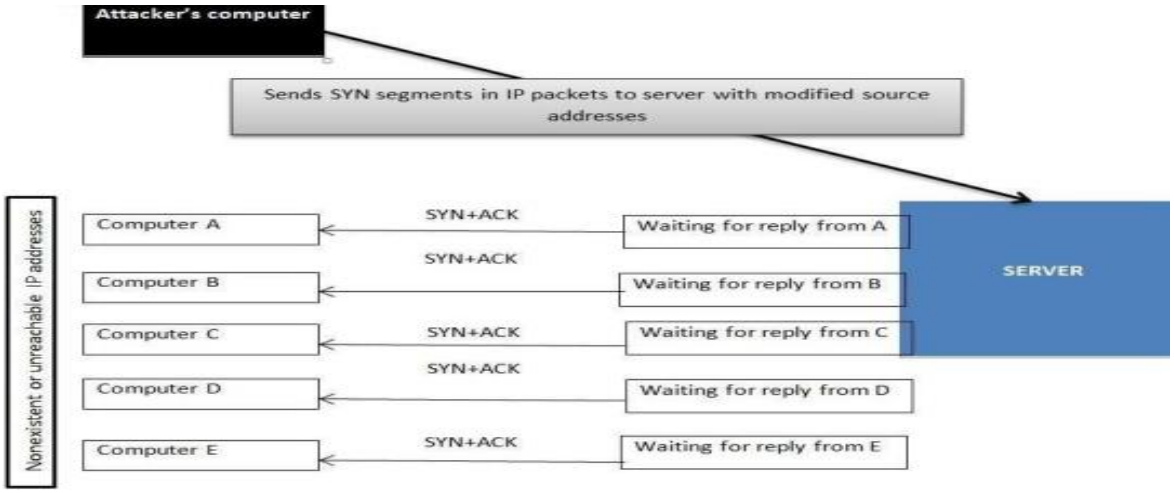
**2. Types of DoS attacks**

- 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.

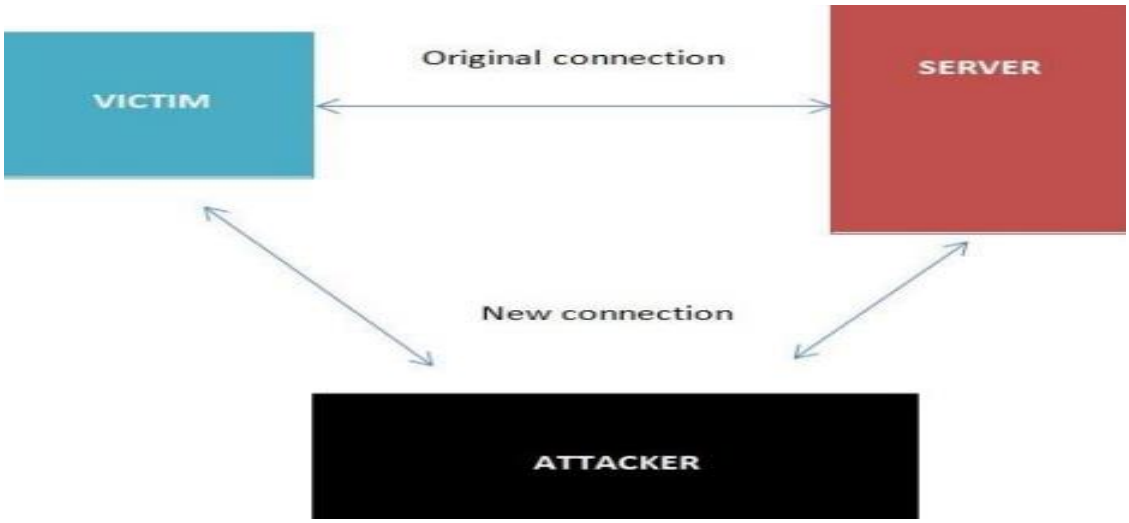
**4. SYN Flood attack**




- 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**

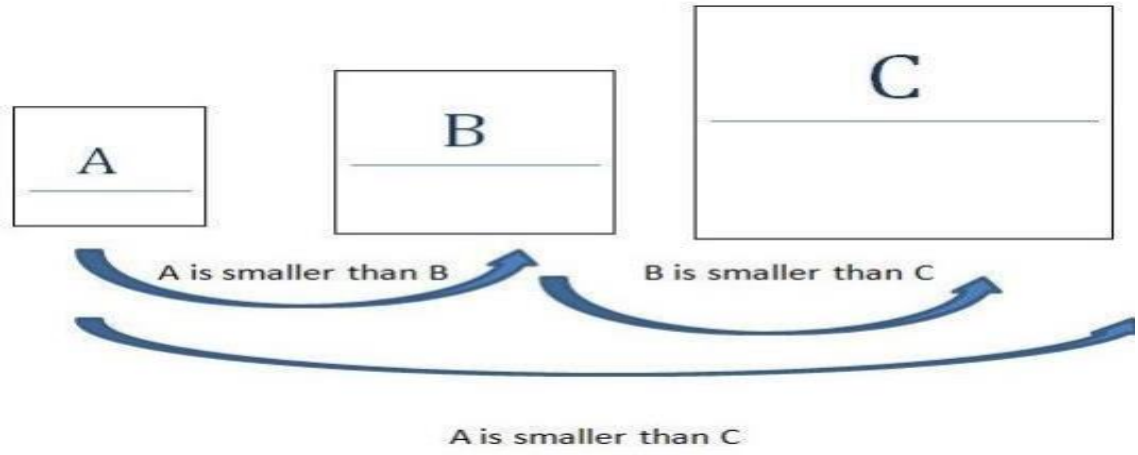
- ARP Poisoning: An attacker can modify the MAC address in the ARP cache so that the corresponding IP address points to a different computer.

| 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<br>192.146.118.4=>00-AA-BB-CC-DD-04 | 192.146.118.3=>00-AA-BB-CC-DD-03<br>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<br>192.146.118.4=>00-AA-BB-CC-DD-04 | 192.146.118.2=>00-AA-BB-CC-DD-02<br>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<br>192.146.118.3=>00-AA-BB-CC-DD-03 | 192.146.118.2=>00-AA-BB-CC-DD-02<br>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.

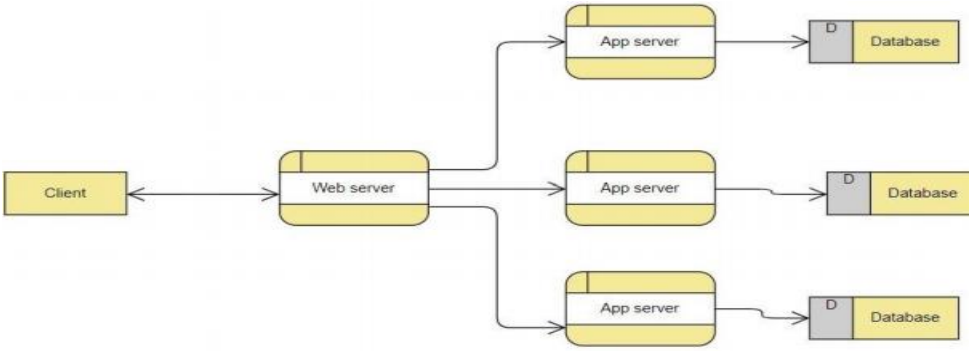
- **Introduction**

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.

- **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:**

- 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.

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**

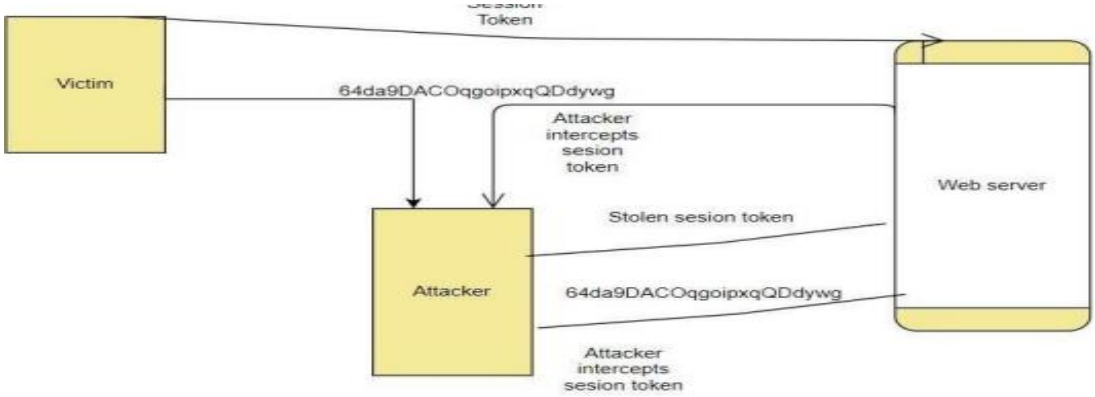
- A cookie can contain a variety of information based on the user's preferences when visiting a website.
- Several different types of cookies exist: First-party cookie, Third-party cookie, Session cookie.
- First-party cookies can be stolen and used to impersonate the user.
- Third-party cookies can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

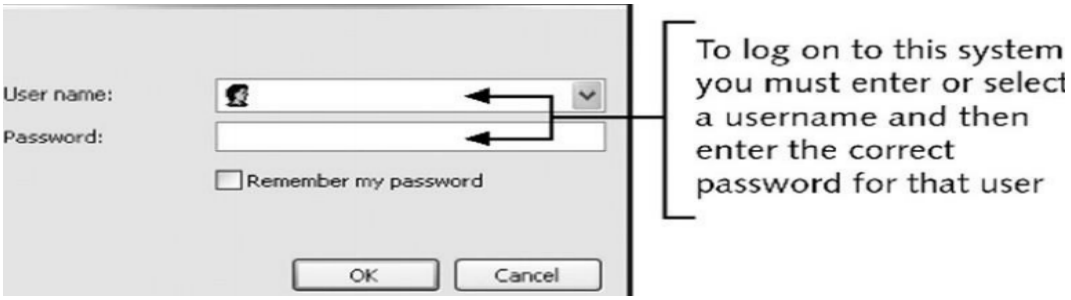
terms, Social Engineering is a complex internet fraud that has a very high success rate. Some well-known types of Social Engineering include Malware Attacks, Application Attacks, Network Attacks, etc.

- 


- 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.




- 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:

### ○ 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.

  - **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.

  - **Replay attack:**

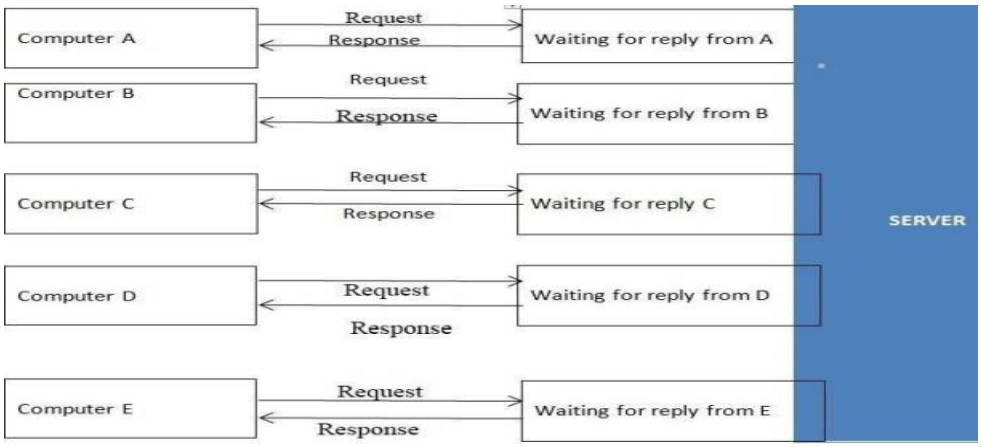
- When cyber criminals send a message onto a secure network, intercept it and then disrupt or divert the user to do what the attacker wants, a repeat attack occurs. It is a phenomenon that is malicious. After the network catches it a hacker does not even need the specialized skills to decipher the message. 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.
    - **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. [3]

- **What is security procedure?**

- A security protocol is a set series of needed tasks undertaken by a particular purpose or feature of defense. Procedures are typically structured as a sequence of steps to be taken to reach an end goal as a clear and repeated method or loop. When introduced, security protocols include a series of policies in order to perform the organization's security affairs that will promote preparation, process auditing, and process development. Procedures offer a starting point for the introduction of the continuity required to minimize security process inconsistency, which improves security control within the enterprise. Decreasing variability is also a positive way for the safety department to reduce duplication, improve efficiency, and maximize performance.

- **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. [4]

- **Firewall**

- 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

- 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.

- **Intrusion detection system (IDS).** [5]

- 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 an attack and alert the network administrator.
- Based on the surveillance scope, IDS is divided into 2 categories:
  - ✓ Network-Based IDS (NIDS): These are network-wide control IDSs. The data packets circulated on the network are the main information source for the NIDS. Usually, NIDS are mounted at the network entry, which can be in front of or behind the firewall.
  - ✓ Host-based IDS (HIDS): These are IDSs that track each specific computer's activities. Therefore, in addition to data traffic to and from the server, the primary source of HIDS information also includes system log data and system audit data (system audit).
- Based on implementation techniques, IDS is also divided into 2 categories:
  - ✓ Signature-based IDS: The signature-based IDS detects intrusions by analyzing network traffic and device logs based on intrusion intrusions. This technique

requires a signature database to be maintained, and any time a new intrusion type or technique is implemented, this database must be updated periodically.

- ✓ Anomaly-based IDS: detection of intrusion by contrasting current activity (statistically) with the system's usual operation to detect abnormalities that may be a sign of intrusion. For instance, under normal conditions, traffic on the network interface of a server is approximately 25 percent of the full bandwidth of communication. If this traffic rises unexpectedly to 50 percent or more at some point, then it can be concluded 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

- **Potential consequences of incorrect IDS configuration.** [7]

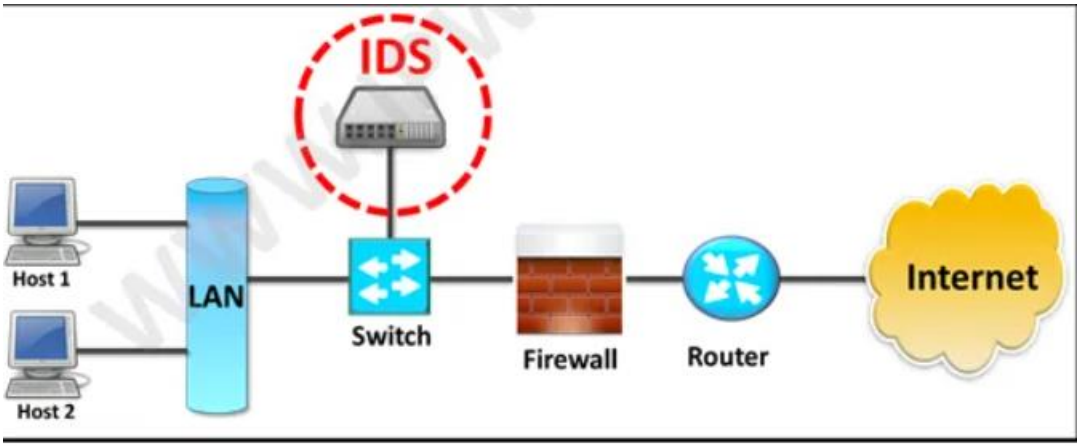
- Consequences of misconfiguring the IDS system: Misconfiguring the IDS system can lead to some serious consequences, such as:
  - ✓ This misconfiguration bug would be purposely used by certain networks to circumvent IDS control to access the device that IDS protects.
  - ✓ IDS will not be able to fully monitor or monitor the traffic accessing the system.
  - ✓ The IDS system may fail and report on normal access.
  - ✓ In the systems it protects, the IDS can misreport activities.
- Consequences of Firewall misconfiguration: Close to IDS, yet misconfiguring the firewall may have several more extreme consequences than IDS:
  - ✓ Improperly configuring a firewall may trigger a range of firewall device vulnerabilities. Hackers can take advantage of this weakness to delete or steal device data that is secured by the firewall.
  - ✓ Improperly configuring a firewall will cause it to become inoperable or function against the configurator's desired rules. Enabling invalid access, for example, and blocking valid access.
  - ✓ Incorrectly configuring a firewall will prevent the firewall from functioning. And then the system that is secured by the firewall will face the possibility of a system crash.

- **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-

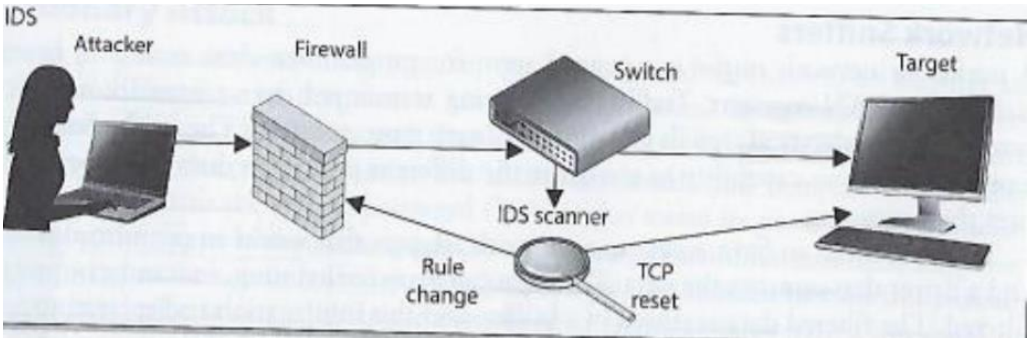
based. A host-based intrusion detection system is installed on the client computer, while a network-based intrusion detection system resides on the network.

- 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.



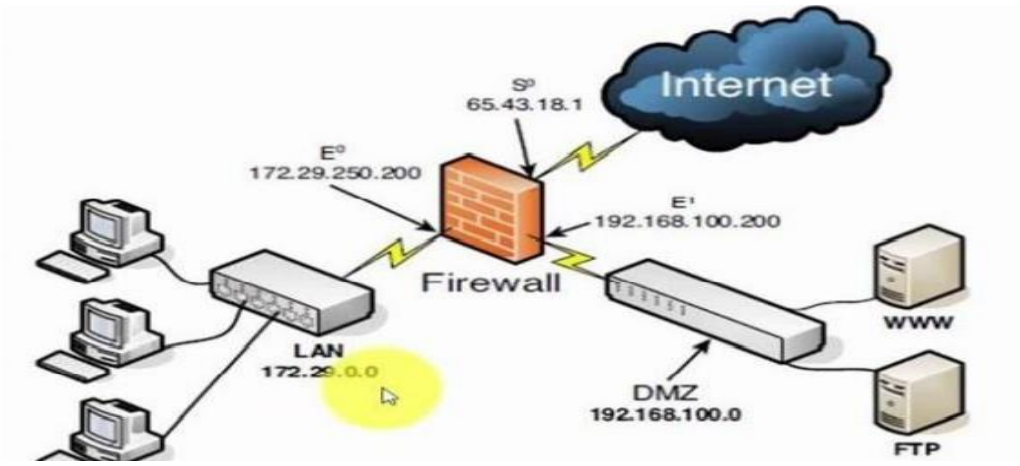
## P4 Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security. [6]

- **Demilitarized zone (DMZ).**

- 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.
- 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

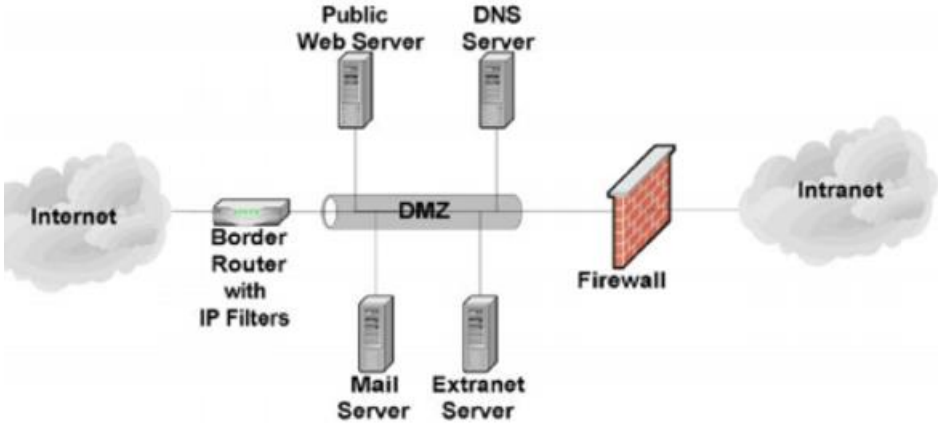
- **Single firewall**

- 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.



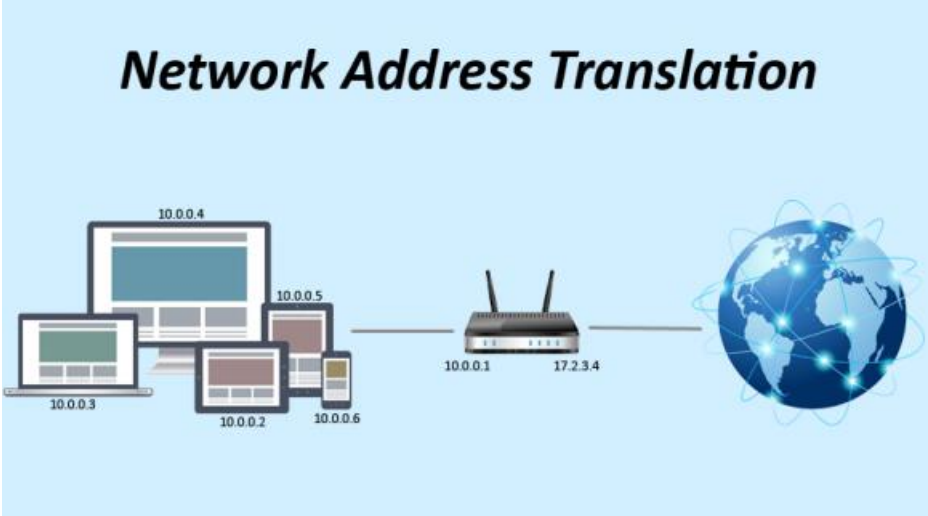

-

- 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.

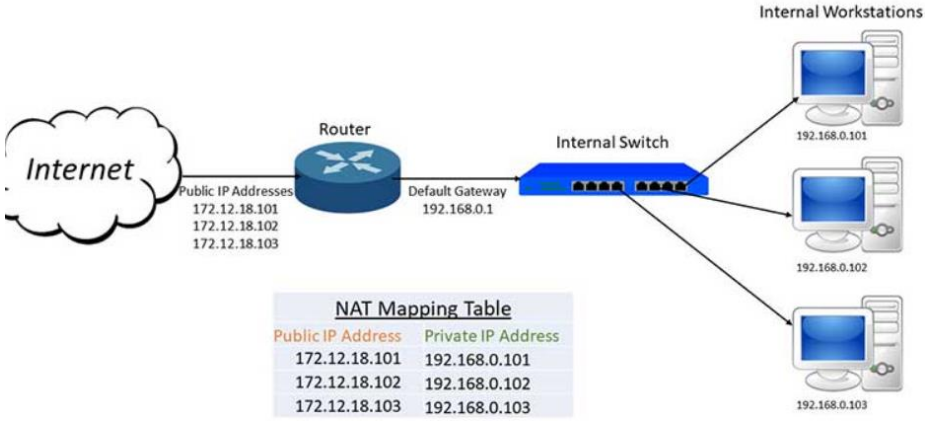
- **NAT (Network Address Translation)**

- 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.



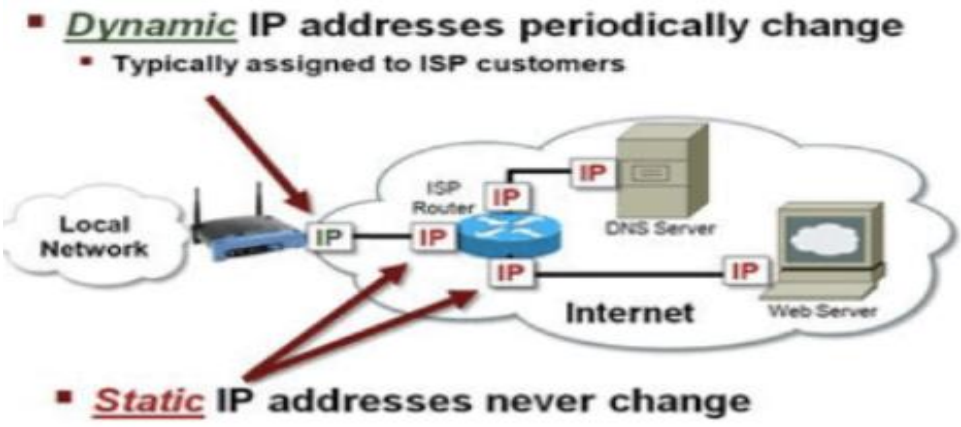

- In a network, for example, two A and B servers are connected. Now both need the same destination at the same time on the same ports, say 1000, on the server-side. If NAT converts an IP address to just 34, so all of their IP addresses will be hidden by the public IP address of the network and sent to 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.
- 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.
- 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.




- **Static IP:**

- 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.

✓ **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.

○ **Conclusion**

- What I have mentioned above and concrete examples to make people understand information technology security better, and this is a crucial job to help the business develop more and quicker. My presentation will assist you with the methods and procedures used in the detection and assessment of IT security threats, along with corporate strategies to secure the business's sensitive data and equipment.
- 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.

## References

[1] https://en.wikipedia.org/wiki/Vietnamese_airports_hackings

[2] Almutairi, M. and Riddle, S., 2017, May. Security threat classification for outsourced IT projects. In *2017 11th International Conference on Research Challenges in Information Science (RCIS)* (pp. 447-448). IEEE.

[3] Chia, P.A., Maynard, S.B. and Ruighaver, A.B., 2002. Understanding organizational security culture. *Proceedings of PACIS2002. Japan*, *158*.

[4] Liu, D., Miller, S., Lucas, M., Singh, A. and Davis, J., 2006. *Firewall policies and VPN configurations*. Elsevier.

[5] 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.

[6] Biskup, J., 2008. *Security in Computing Systems: Challenges, Approaches and Solutions*. Springer Science & Business Media.

[7] Zhou, W., Jia, Y., Peng, A., Zhang, Y. and Liu, P., 2018. The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. *IEEE Internet of Things Journal*, *6*(2), pp.1606-1616.