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		**Date Received 2nd submission**	
Student Name	PHAM CAO NGUYEN	**Student ID**	GCC18074
Class	GCC0801	**Assessor name**	LE HUYNH QUOC BAO
Student declaration 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. **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. 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. In addition to your presentation you should also provide a detailed report containing a technical review of the topics covered in the presentation. Your presentation should: 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 2. **Describe** a variety of organizational procedures an organization can set up to reduce the effects to the business of a security breach. 3. **Propose** a method that FIS can use to prioritize the management of different types of risk 4. **Discuss** three benefits to FIS of implementing network monitoring system giving suitable reasons. 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. 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. 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		

<table>
<tr><td>P1 Identify types of security threat to organisations.
Give an example of a recently publicized security breach and discuss its consequences.

P2 Describe at least 3 organisational security procedures.</td><td>M1 Propose a method to assess and treat IT security risks.</td><td rowspan="3">LO1 & 2
D1 Investigate how a ‘trusted network’ may be part of an IT security solution.</td></tr>
<tr><td colspan="2">LO2 Describe IT security solutions</td></tr>
<tr><td>P3 Identify the potential impact to IT security of incorrect configuration of firewall policies and IDS.

P4 Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security.</td><td>M2 Discuss three benefits to implement network monitoring systems with supporting reasons.</td></tr>
</table>

UNIVERSITY of GREENWICH
Alliance with FPT Education

BTEC

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.

- 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.

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.

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 protection 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.

○ **Collect data.**

1. Spyware.

Spyware is a common term used to describe malware that remotely spies on users by capturing data without their key logger permission that quietly records and retains any keystroke that a user types on the keyboard of the computer. The intruder then checks for some valuable information, such as passwords, credit card numbers, or personal information, in the intercepted text.

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.

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.

- **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.

- **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

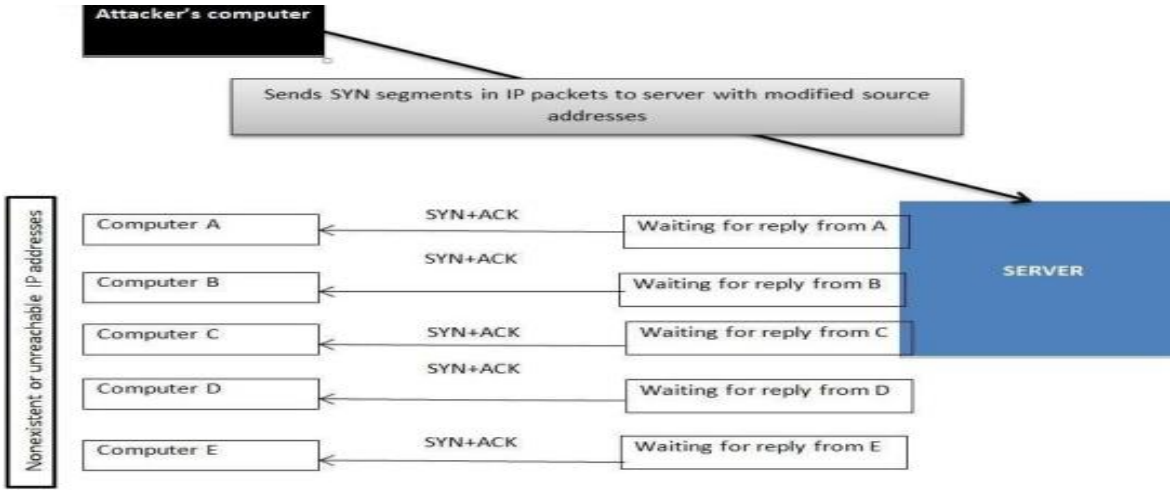
- Ping flood
- A large number of ICMP echo requests are submitted rapidly by several machines, flooding a server (as well as the network) to the point that it will not respond enough quickly and will lose valid connections to other clients and deny all new connections.

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.

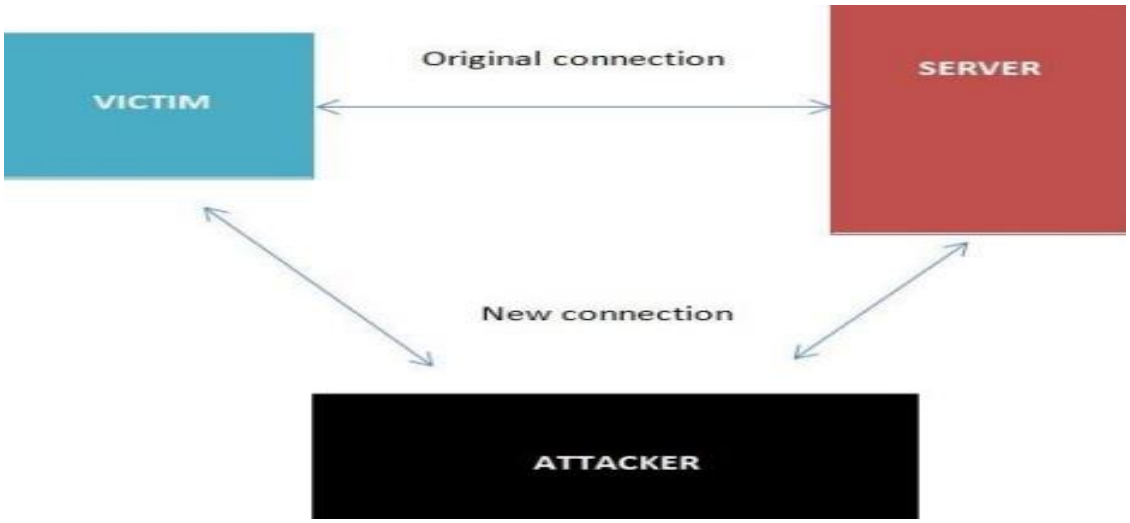
4. SYN Flood attack



- 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

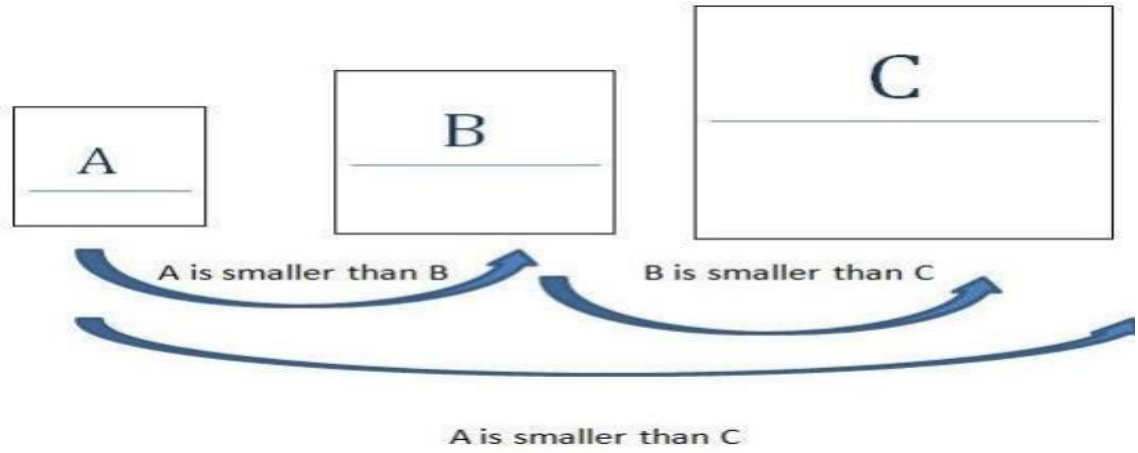
- ARP Poisoning: An attacker can modify the MAC address in the ARP cache so that the corresponding IP address points to a different computer.

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-03 192.146.118.4=>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

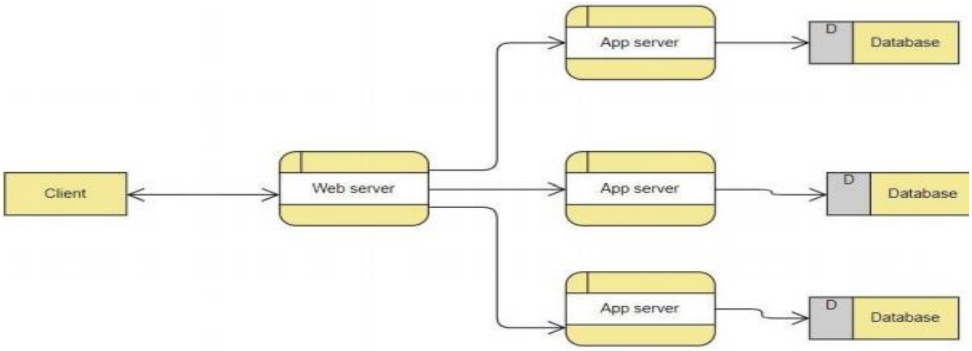
- Privilege Escalation: leveraging a security flaw to obtain access to services that the user would usually be prevented from accessing.
- Transitive Access: System A can access System B, and because System B can access System C, then System A can access System C.



II. Application Attacks.

- **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.

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.

3. **Cross-site scripting:**

Cross-site scripting (XSS) is a form of vulnerability in computer security often used in web applications. XSS helps hackers to execute client-side scripts on web sites visited by other entities. To bypass access controls like the same-origin policy, an attacker can use cross-site scripting vulnerabilities.

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

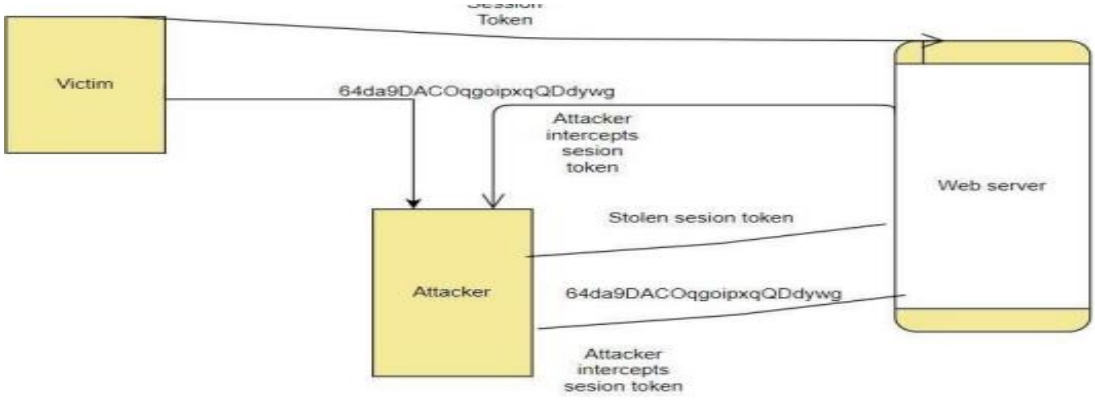
- A cookie can contain a variety of information based on the user's preferences when visiting a website.
- Several different types of cookies exist: First-party cookie, Third-party cookie, Session cookie.
- First-party cookies can be stolen and used to impersonate the user.
- Third-party cookies can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

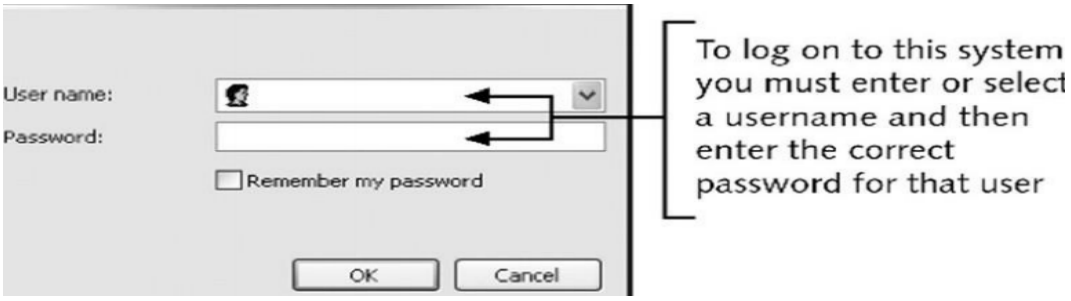
- Today, the most possible focus of threats is the global computing infrastructure.
- Attackers are getting more experienced, going away from hunting for bugs in individual device programs to testing the underlying software and hardware architecture itself.

Social Engineering

- 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.

III. Networking-Based Attacks:

- 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.

2. Interception:

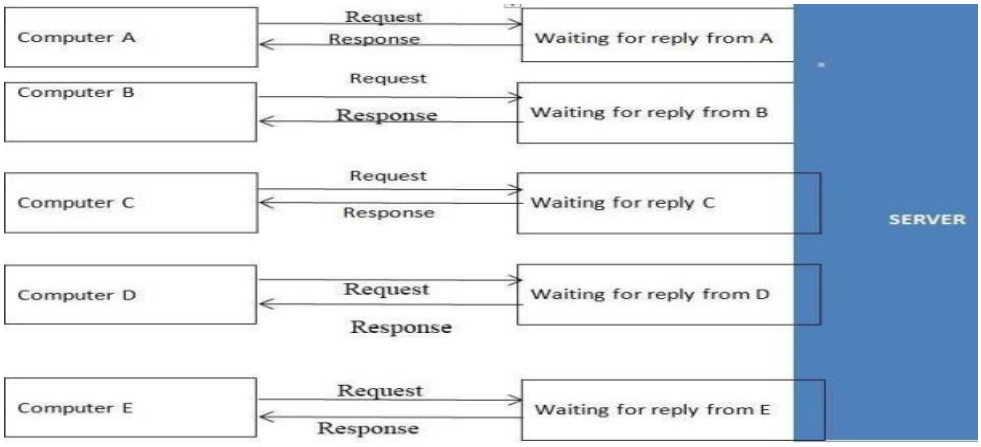
A network link is compromised or not usable for legitimate use in the event of an intruder attack. These are attacks on the network's efficiency.

3. Poisoning

- Address Resolution Protocol poisoning (ARP poisoning) is a type of attack in which the attacker modifies the Media Access Control (MAC) address and attacks the Ethernet LAN by altering the target computer's ARP cache with the modified request and answer packets of the ARP. This modifies the MAC Ethernet address to the hacker's known MAC address to trace it. Because the ARP responses are fake, the target machine transfers the frames to the hacker's device first instead of transmitting them to the original destination.
- As a consequence, both the details of the system and the safety of the consumer are violated. A successful attempt at ARP poisoning is undetectable to the patient.

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.



P2 Describe organizational security procedures. [3]

You need to define the exact data your corporation wants to secure before you can perform data management with your organization. Businesses themselves also do not know, or just know a portion of, precisely which data needs to be secured.

1. **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.

2. **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.

3. **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.

4. **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.

5. **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...

6. **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).

7. **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.

8. **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.

9. **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.

10. **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.

11. **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).

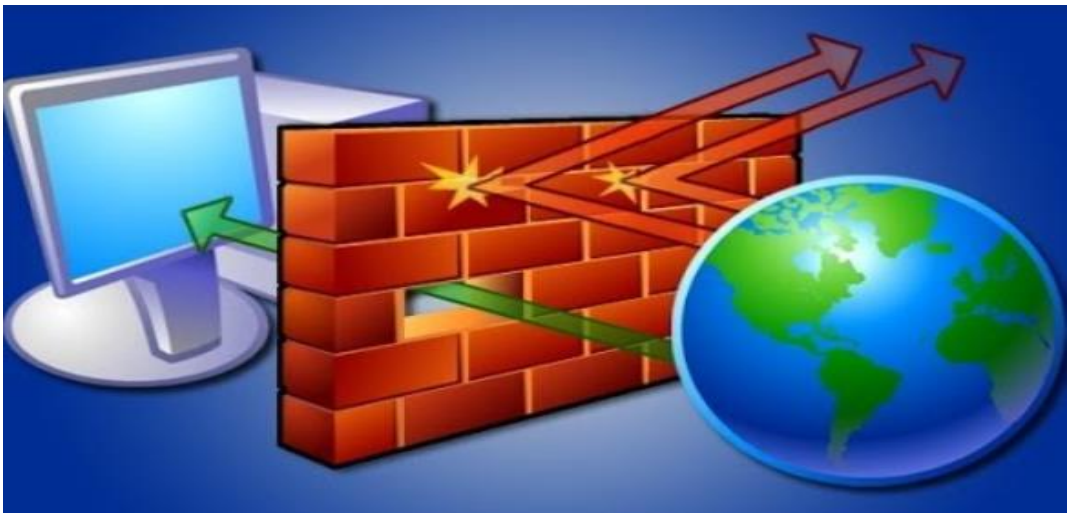
- **Testing procedures: ex: data, network, systems, operational impact of security breaches, WANs, intranets, wireless access systems.**
- Network security: This involves looking for vulnerabilities in the network infrastructure (resources and policies).
- System software security: Asses weaknesses in 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]

Introduction

- Firewall is a network security system that analyzes and records the data's overall security strategy that reaches or goes beyond the network inside your network. This serves as a firewall for the internal network. We would consider a firewall in both hardware and device countries. Firewall software is in general, an application that is built on our PCs to connect securely across the network. It would prohibit attacks flowing into our PCs from other networks. And it's better than firewall physique. A hardware firewall requires a server to be implemented so it is quite expensive and used in large organizations. This device is placed between the router and the internet.



- Firewalls defend devices from attacks, both external and internal. While firewalls were initially common in business environments, a firewall to protect against Internet-borne threats is now being introduced by most home networks with a broadband Internet link. An application, computer system, or group of systems that controls the flow of traffic between two networks is essentially a firewall.
- The most common use of a firewall is to protect a private network from a public network such as the Internet. However, firewalls are also increasingly used to separate a sensitive area of a private network from less-sensitive areas.

- At its most basic, a firewall is a device (a computer system running firewall software or a dedicated hardware device) that has more than one network interface. It manages the flow of network traffic between those interfaces.

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.

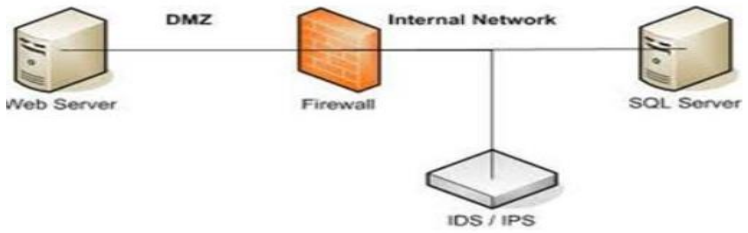
Network Address Translation (NAT): Allows for multiple IP's tohide behind one. More on this later.

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.

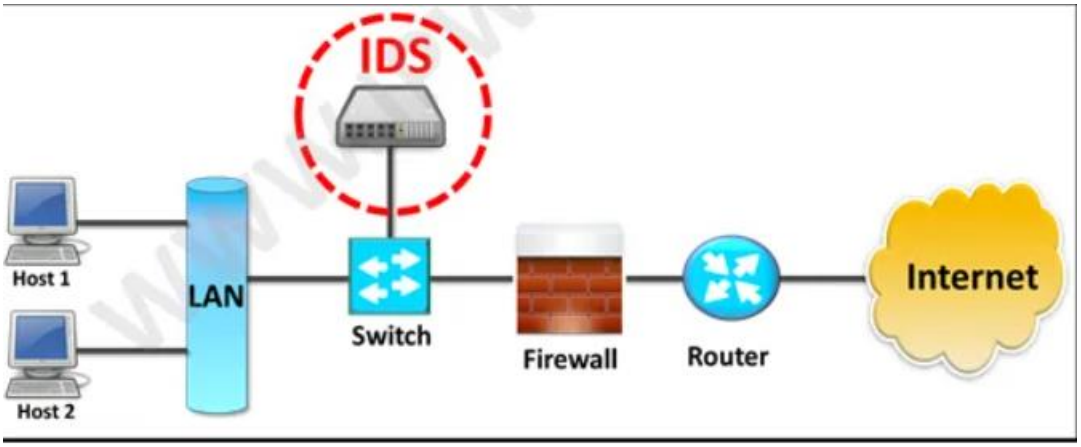
Intrusion detection system (IDS). [5]

- An intrusion detection system (IDS) is a system that monitors network traffic for suspicious activity and alerts when such activity is discovered. While anomaly detection and reporting are the primary functions, some intrusion detection systems are capable of taking actions when the malicious activity or anomalous traffic is detected, including blocking traffic sent from suspicious Internet Protocol (IP) addresses.
- An IDS can be contrasted with an intrusion prevention system (IPS), which monitors network packets for potentially damaging network traffic, like an IDS, but has the primary goal of preventing threats once detected, as opposed to primarily detecting and recording threats.



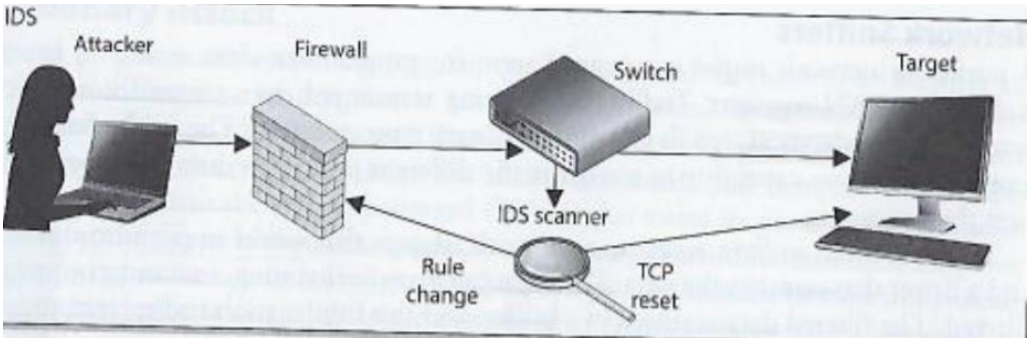
How do intrusion detection systems work?

- 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:

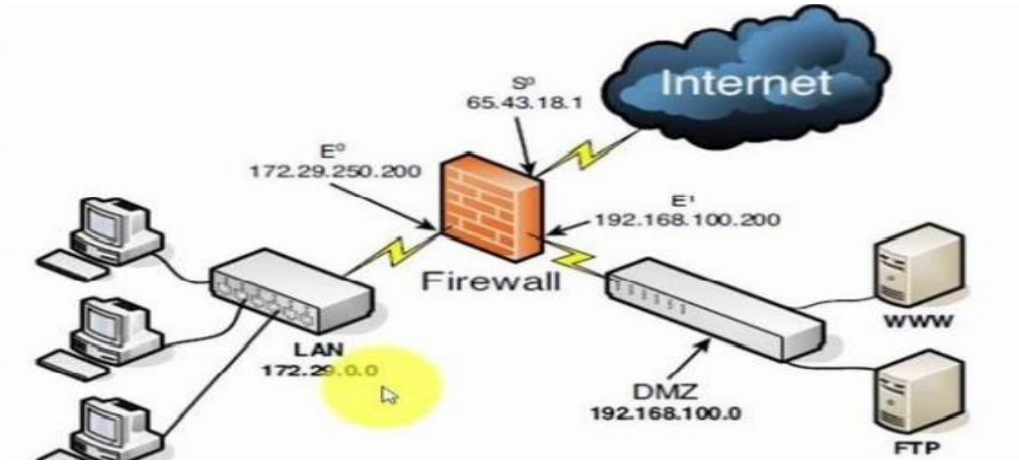
- Disconnect communications and block transmission of traffic
- Block a user from accessing a resource
- Send alerts of an event trigger to other hosts, IDS monitors, and administrators.
- IDS-Detect something bad may be taking place and send an alert.



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

Demilitarized zone (DMZ). [6]

- 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.
- Using DMZs gives your firewall configuration an extra level of flexibility, protection, and complexity.



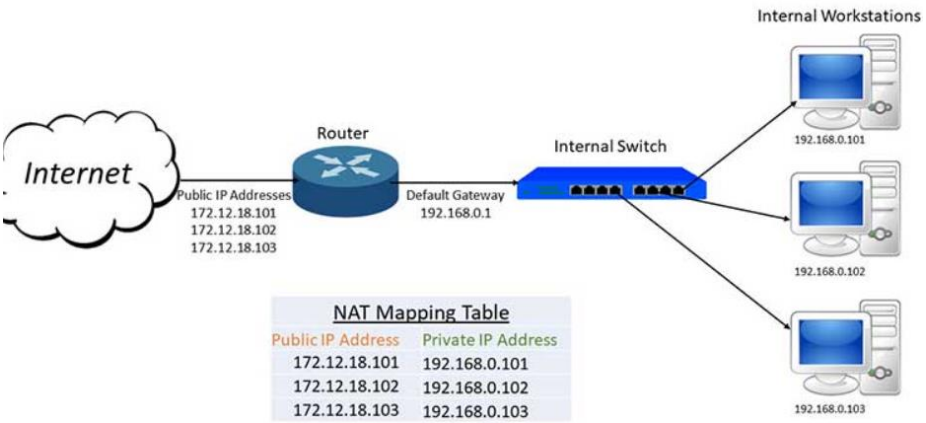
- You can build an extra move by using a DMZ that makes it harder for an attacker to obtain access to the internal network.

- 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.

NAT (Network Address Translation)

- 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.



Static IP:

Static IP is a FIXED IP address that is reserved for one person or the user group that their Internet-connected device is always placed AN IP address. As a user-set IP address, typically for businesses, companies, ...Normally static IP is given to a server with its own purpose (Web server, Mail…). So that many people can access without interrupting those processes.

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.

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.