


ASSIGNMENT FRONT SHEET

Qualification	BTEC Level 5 HND Diploma in Computing		
Unit number and title	Unit 5: Security		
Submission date	11/12/2020	Date Received 1st submission	
Re-submission Date		Date Received 2nd submission	
Student Name	Do Duc Tai	Student ID	GCH190834
Class	GCH0803	Assessor name	Michael Omar
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	

Grading grid

P1	P2	P3	P4	M1	M2	D1

☐ **Summative Feedback:**☐ **Resubmission Feedback:****Grade:****Assessor Signature:****Date:****Internal Verifier's Comments:****Signature & Date:**

Table of Contents

Introduction.....	5
Contents	6
I. P1 Identify types of security threat to organisations.....	6
1. Define threat	6
2. Identify threats agents to organizations.....	6
3. Types of threat that organization will face	7
4. An example of a recently publicized security breach and discuss its consequences	15
II. P2 Describe some organizational security procedures	16
III. P3 Identify the potential impact to IT security of incorrect configuration of firewall policies and IDS	17
1. Firewall	17
2. IDS	19
3. The potential impact(Threat-Risk) of FIREWALL and IDS incorrect configuration to the network	20
IV. P4 Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security.....	21
1. DMZ	21
2. Static IP.....	21
3. NAT	22
Conclusion	23
Evaluate	24
PowerPoints	24
References.....	29

Table of figures

Figure 1-Type of malware.....	7
Figure 2-Social engineering	9
Figure 3-Baiting attack.....	9
Figure 4-Phishing attack	10
Figure 5-Pop-up window	10
Figure 6-Man-in-the-Middle Attack	14
Figure 7-Replay Attack	14
Figure 8-Firewall.....	19
Figure 9-IDS	20
Figure 10-DMZ.....	21
Figure 11-Static IP.....	22
Figure 12-NAT.....	23

Introduction

In this semester, the author has learned about security systems and how to secure a system. Therefore, author's assessor gave him this assignment. Here is the scenario: Working as a trainee IT Security Specialist for a leading Security consultancy in Vietnam called FPT Information security FIS, the author has 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 this report, author will discuss some issue, such as: identifying the security threats FIS secure may face if they have a security breach and giving an example of a recently publicized security breach and discuss its consequences then describe a variety of organizational procedures an organization can set up to reduce the effects to the business of a security breach. Next, he proposes a method that FIS can use to prioritize the management of different types of risk. Then, he will discuss three benefits to FIS of implementing network monitoring system giving suitable reasons. Finally, he will 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 and 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.

Contents

I. P1 Identify types of security threat to organisations

1. Define threat

A threat can be defined as a potential for security intrusion, which exists when there is an entity, capability, circumstance, action or event that could cause harm through vulnerabilities of security. It gives instructor an ability to obtain illegal admission to organization, to take data without detection, or execute other malicious pursuits. Organization's security is at risk or vulnerable if or when there is a weakness or vulnerability within organization's computer (Scott, 2020).

2. Identify threats agents to organizations

An individual or group that acts, or has the power to, exploit a vulnerability or conduct other damaging activities. For example, threat agents are malicious hackers, organized crime, insiders (including system administrators and developers), terrorists, and nation states.

- Nation state: Nation-State actors aggressively target and gain persistent access to public and private sector networks to compromise, steal, change, or destroy information. They may be part of a state apparatus or receive direction, funding, or technical assistance from a nation-state. Nation-state has been used interchangeably with Advanced Persistent Threat (APT), however APT refers to a type of activity conducted by a range of actor types.

Motivation: Espionage, political, economic, or military

Affiliation: Nation-states or organizations with nation-state ties

Common TTPs: Spear-phishing password attacks, social engineering, direct compromise, data exfiltration, remote access trojans, and destructive malware.

- Natural disaster: Whilst not a cyber-attack, these events can have the same net effect to your ability to do business. If you cannot access your offices, data centres, or files stored on the cloud, then you are still experiencing a data disaster, and this must be taken into account.
- Organized crime: Their limited offensive cyber activity is typically disruptive or harassing in nature. Terrorist organization's primarily use the internet for communications and recruitment. Criminals are targeting personal data for a number of different reasons; credit card fraud, identity theft, bank account fraud and so on. These crimes are now being perpetrated on an

industrial scale. Methodologies vary from phishing attacks to ‘Watering Hole’ websites, but the end result is the same; you and your data are being extracted and used for nefarious means.

Motivation: Political or ideological; possibly for financial gain, espionage, or as propaganda

Affiliation: Individuals, organizations, or nation-states

Common TTPs: Defacements and claimed leaks

- **Employee:** They are current or former employees who have access to an organization's networks, systems, or data. Malicious insiders intentionally exceed or misuse their access in a manner that negatively affects the confidentiality, integrity, or availability of the organization's information or information systems. This differs from unwitting insiders who unintentionally cause damage to their organization's information systems through their actions, such as clicking on malicious links in a phishing email.

Motivation: Financial gain or to seek revenge

Affiliation: Current or former employee, contractor, or other partner who has authorized access.

Common TTPs: data exfiltration or privilege misuse

3. Types of threat that organization will face

There are four common types of threat that organization will face

a. Malware Attack

Malicious software, more commonly known as malware, is a threat to your devices and your cybersecurity. A malware attack is when cybercriminals create malicious software that's installed on computer without user's knowledge to gain access to personal information or to perform an unwanted and harmful action to the device, usually for financial gain. Malware attacks can reach all sorts of devices and operating systems, including

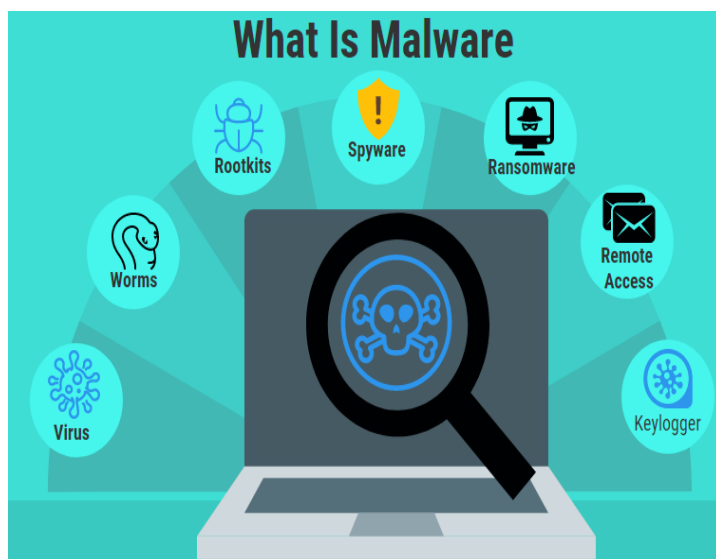


Figure 1-Type of malware

Microsoft Windows, macOS, Android, and iOS, etc. Different types of malware include viruses, spyware, ransomware, and Trojan horses (Johansen, 2019).

Types of mutating malware:

- Oligomorphic malware: This malware converts its internal code into one of several predefined mutations whenever it is executed. However, since polymorphic malware only has a limited number of mutations, it will eventually change back into a previous version that the scanner can then detect.
- Polymorphic malware: Malware code that completely changes from its original form whenever it is executed is known as polymorphic malware. This is code that uses a polymorphic engine to mutate while keeping the original algorithm intact. That is, the code changes itself each time it runs, but the function of the code will not change at all. For example, $1+3$ and $6-2$ both achieve the same result while using different code.
- Metamorphic malware: The malware can actually rewrite code on its own and therefore appear different each time it is executed. It does this by generating a logical equivalent code whenever it is run.

b. Social Engineering Attack

Social engineering attack is the term used for a wide range of malicious activities performed through human interactions. It uses psychological manipulation to trick users into making a security mistake or provide sensitive information. It is also known as non-technical attack (Bennatan, 2020).



Figure 2-Social engineering

Types of social engineering attack:

- **Baiting:** Baiting attacks use a vain promise to arouse the victim's greed or curiosity. They lure users into traps to steal their personal information or infect their systems with malware. Most baiting use physical device to spread malware. For example, attackers leave bait - often malware-infected flash drives - in conspicuous areas where potential victims are likely to see them (e.g. bathrooms, lifts, yards parking of a targeted company). Scammers can take advantage of the offering of free music or movie downloads to trick users into giving out their information.



Figure 3-Baiting attack

- **Phishing:** Phishing scams are email and text message campaigns that create a sense of urgency, curiosity, or fear in a victim. It then prompts them to provide sensitive information, click on links to malicious websites, or open attachments that contain malware (Bennatan, 2020).



Figure 4-Phishing attack

- **Pop-up window:** Pop-up tricks users into clicking on a hyperlink that redirects them to an attacker's website, asking them for personal information, or asking them to download software that may contain a virus. attached in the backend program (Beal, 2015).

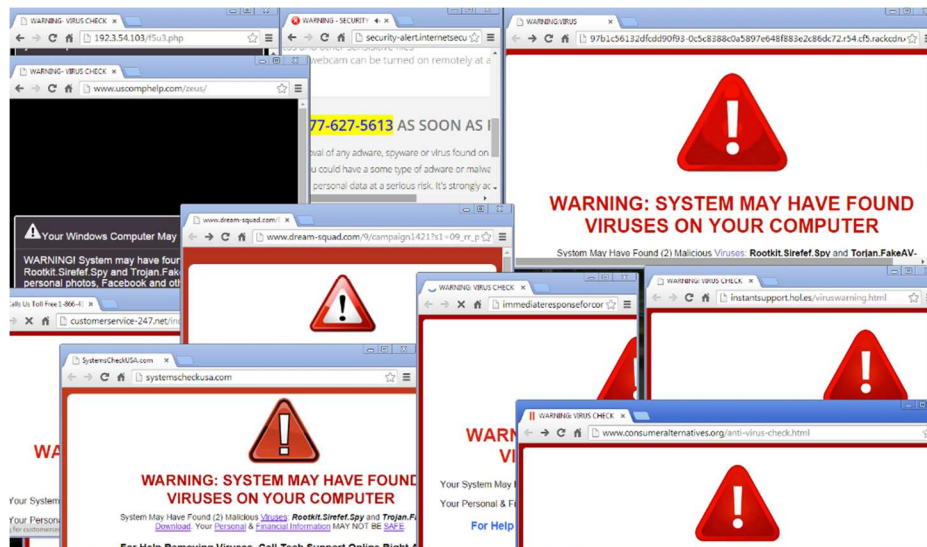


Figure 5-Pop-up window

- **Dumpster diving:** The dumpster diving is a technique used to obtain information that can be used to launch an attack on a computer network. Trash diving isn't limited to rummaging through the trash to look for obvious treasures like access codes or passwords written on sticky notes. Visibly

innocent information such as a phone list, calendar, or organization chart can be used to assist an attacker using social techniques to gain access to the network (Rouse, 2005).

c. Application Attack

- **Sever-Side Web Application Attack:** On the Internet, the web server providing the service is deployed like web applications. One important feature of server-side web applications is that they generate dynamic content based on user's input. Many server-side web application attacks target the input the application accepts from the user.

There are some types of Sever-Side attack:

- **Cross-Site Scripting (XSS):** Cross-Site Scripting (XSS) attacks are a type of attack in which malicious code is delivered to benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, usually in the form of a browser-side script, to another end user. Flaws allow these attacks to be fairly commonplace and occur anywhere a web application uses input from the user in the output it generates without authenticating or encrypting it. An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way of knowing that the script has not been trusted and will execute the script. Since it assumes that the script comes from a trustworthy source, the malicious script can access any cookies, session tokens, or other sensitive information kept by the browser and used with that website. These scripts can even rewrite the content of the HTML page (KirstenS, 2009).
- **SQL Injection:** SQL injection is a web security vulnerability that allows an attacker to intervene with the queries an application makes against its database. It usually allows an attacker to see data that they normally couldn't get. This may include data that belongs to other users or any other data that the application itself can access. In many cases, an attacker can modify or delete this data, causing persistent changes to the app's content or behaviour (Kettle, 2020).
- **XML Injection:** XML Injection is an attack technique used to manipulate or compromise the logic of an XML application or service. Incorporating unwanted XML structures and content into an XML message can change the intended logic of the application. Furthermore, XML insertion can cause malicious content to be inserted into the resulting message or document (Auger, 2010).

- **Directory Traversal/Command Injection:** Command-injection is a type of attack where the primary goal is for the vulnerable application's host operating system to execute system commands. These types of attacks can occur when unsafe user input is transferred from the application to the system. The commands provided are executed at the privileged level of the application, for example the web server can be run with either the www-data user or the Apache user, not the root user. Directory-traversal is when the server allows an attacker to read files or directories outside of the normal web server directory.
- **Client-side Application Attacks:** Client-side attacks happen when a user downloads malicious content. The flow of data is reversed compared to server-side attacks: client-side attacks start with victims downloading content from attackers. Client-side attacks are difficult to mitigate for organizations with the Internet. Client applications include word processing software, spreadsheets, media players, Web browsers, and more. Most inbound firewalls are much more limited than outbound; they are designed to "stop the bad guys" and mitigate server-side attacks from untrusted networks. They often fail to prevent client-side attacks (Conrad, 2017).

There are six types of Client-Side Application Attack:

- **Header Manipulation:** The Header Manipulation is a means to an end, not an end. At its root, the vulnerability is simple: the attacker passes the malicious data to a vulnerable application, and the application includes the data in the HTTP response header.
- **Cookies:** Cookies can contain many different information based on preferences when accessing a website. Several different types of cookies exist: First Party Cookies, Third Party Cookies, Session Cookies. First party cookies can be stolen and used to impersonate a user. Third party cookies can be used to track a user's browsing or purchasing habits.
- **Attachments:** Attachments are files that are paired with email messages. Malicious attachments are often used to spread viruses, Trojans, and other malware when they are opened.
- **Session hijacking:** This is an attack in which an attacker tries to impersonate a user using their session token.

- **Malicious Add-ons:** Attackers can create malicious add-ons that launch attacks on users' computers. One way to write these malicious add-ons is to use Microsoft's ActiveX. Attackers can take advantage of vulnerabilities in ActiveX to carry out malicious attacks on computers.
- **Impartial Overflow Attacks:**
 - o Buffer Overflow Attack: A buffer overflow attack occurs when a process tries to store data in RAM beyond the boundaries of a fixed-length storage buffer.
 - o Integer overflow attack: conditions that occur due to an arithmetic operation - such as addition or multiplication - exceed the maximum size of the integer type used to store it.
 - o Arbitrary / Remote code execution: allows an attacker to run a program and execute commands on another computer.

d. Networking-Based Attacks

Networking-Based Attack includes:

- A Denial of Service (DoS) attack is an attack that aims to shut down a computer or network, leaving the intended user inaccessible. DoS attacks do this by flooding the target with traffic or sending it information that is causing the crash. In both cases, a DoS attack deprives a legitimate user (i.e. an employee, member, or account holder) of the service or resource they expect. There are three types of DoS: Ping flood, Smurf attack, SYN flood attack.
- **Interception:** In an interception attack, an unauthorized individual gains access to confidential or private information. Interception attacks are attacks against network confidentiality. Examples of Interception attacks: Eavesdropping on communication, wiretapping telecommunications networks.
 - o Man-in-the-middle attack: A man-in-the-middle (MitM) attack is when an attacker intercepts communications between two parties to secretly eavesdrop or modify traffic between the two parties. Attackers can use MitM attacks to steal credentials or personal information, track the victim or sabotage communications or corrupt data (Swinhoe, 2019).

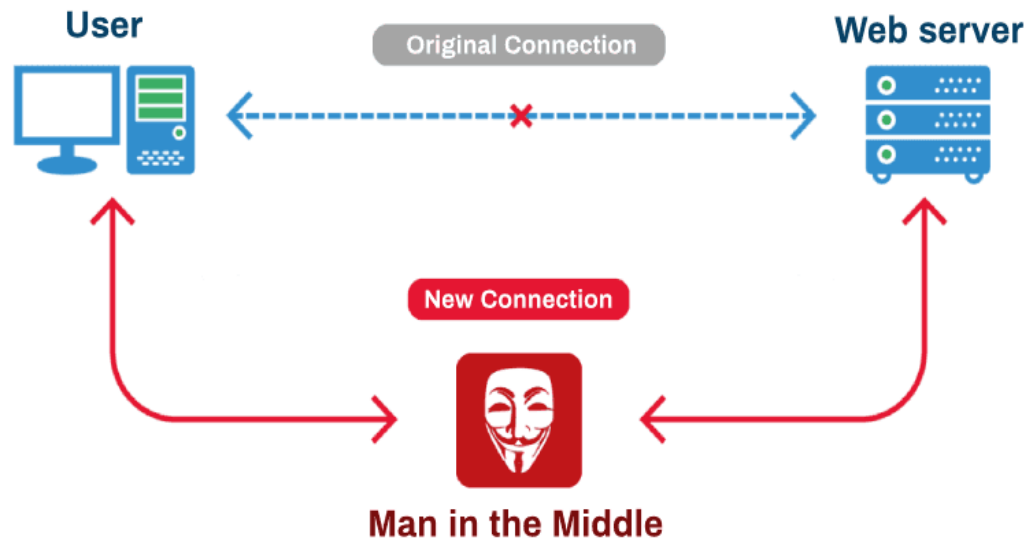


Figure 6-Man-in-the-Middle Attack

- **Replay attack:** A replay attack occurs when cybercriminals eavesdrop on a secure network communication, intercept it and then fraudulently delay or resend to manipulate the recipient to do what the hacker wants. Even more peril of replay attacks is that a hacker does not even need advanced skills to decrypt a message after retrieving it from the network. The attack can be successful just by resending the whole thing (Swinhoe, 2019).

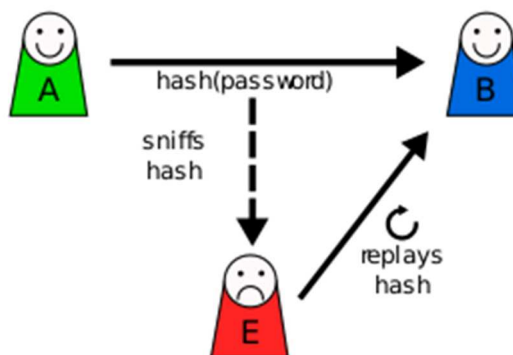


Figure 7-Replay Attack

- **Poisoning:** This attack seeks to damage the AI model itself, so it is inherently faulty so that the attacker can clearly control the output. In a poison attack, the attacker compromises the learning

process in such a way that the system fails on inputs selected by the attacker and continues to build a backdoor through which he can check control. output even in the future (Goled, 2020). There are two types of poisoning attack:

- ARP Poisoning: An attacker can modify the MAC address in the ARP buffer so that the corresponding IP address points to another computer.
- DNS Poisoning: This is the process of replacing a DNS address so that one computer is automatically redirected to another.
- **Attack on Access Right:**
 - Privilege upgrade: This is the exploitation of vulnerabilities in software to gain access to resources that are often restricted to users.
 - Bridging access: System A can access System B and since System B can access System C, System A can access System C.

4. An example of a recently publicized security breach and discuss its consequences

Example:

In one of the largest security breaches in history, Florida-based data aggregation and marketing firm Exactis revealed a database of nearly 340 million personal records.

The breach was uncovered in June when a security researcher found exposed data on an unprotected server allowing public access. The data includes 230 million consumer records and 110 million business contacts. Number represents every adult in the United States.

The data does not contain social security numbers or credit card information. However, it does include other types of Personally Identifiable Information (PII) such as phone numbers, home addresses and email addresses. All criminal information required to commit identity theft.

Each consumer profile also contains over 400 variables that can be used to build detailed personal profiles. This includes information such as preferences, buying habits, marital status, political and religious parties, evils, and pet ownership.

Consequences: The data which were exposed contains of Personally Identifiable Information (PII) of over 200 million customers and it can be used to build detail personal profiles.

Some solutions:

- Make sure you know who has access to folders before you put sensitive data in it!
- Make sure you do not include sensitive information in publicly accessible locations from the Internet. Tested twice. If you can go online without a password, so can everyone else.
- Always safely transmit sensitive data. This includes remote access and client / server transmission.
- Do not use an open / unencrypted wireless network when working with or sending this data.
- Don't email or IM (instant messages) unencrypted sensitive data.
- Don't forget sensitive data in attachments, screenshots, test data, etc. These data should also be sent securely.
- Do not send paper mail showing a person's Social Security number, financial account information or Driver's License / State ID Number.

II. P2 Describe some organizational security procedures

1. Acceptable Use Policy (AUP)

The AUP sets out obligations and practices by which employees using an organization's IT assets must agree to access the corporate network or the internet. That is the standard referral policy for new employees. They are given an AUP to read and sign before being issued a network ID. The IT, security, legal and human resources departments should discuss what is covered by this policy.

2. Access control policy (ACP)

ACP outlines employee access rights related to the organization's data and information systems. Some of the topics commonly covered in this policy are access control standards, such as NIST's Access Control and Implementation Guidelines. Other items covered in this policy are standards for user access, network access control, operating system software control, and complexity of company passwords. Additional frequently cited additional items include methods of monitoring how corporate systems are accessed and used; how to secure unattended workstations; and access is deleted when an employee leaves the organization.

3. Change Management Policy

A change management policy against a formal process for making changes to IT services / operations, software development, and security. The goal of a change management program is to increase awareness and understanding of proposed changes across the organization and to ensure that all changes are methodically carried out to minimize any impact. adversely affecting services and customers.

4. Information security policy

An organization's information security policies are often high-level policies that can include a large number of security controls. A company-issued key information security policy to ensure that all employees use information technology assets on a wide range of the organization or its network, and comply with established rules and guidelines. tell. I have seen asking employees to sign this document to confirm that they have read it (usually done when signing AUP policy). This policy is designed so that employees recognize that there are rules for which they will be held accountable regarding the sensitivity of company information and IT assets.

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

1. Firewall

A firewall is a device (a combination of hardware and software) or an application (software) designed to control the flow of Internet Protocol (IP) traffic to a network or electrical device. Firewalls are used to monitor network traffic and enforce policies based on the instructions contained in the Firewall Code. Firewalls represent one component of the strategy to combat malicious activities and attacks on computer resources and information accessible to the network. Other components include, but are not limited to, anti-virus software, intrusion detection software, patch manager, strong passwords / passwords, and spyware detection utilities. A firewall policy defines how an organization's firewall will handle incoming and outgoing network traffic for specific IP addresses and ranges, protocols, applications, and content types based on the organization's information security policies.

Firewall's usage and advantages in a network:

1. Monitors Network Traffic

All the benefits of firewall security start with the ability to monitor network traffic. The data coming and going out of your system gives threats to your activities. By monitoring and analysing network traffic, firewalls take advantage of pre-set rules and filters to keep your system protected. With a well-trained IT team, you can manage your protection levels based on what you see in and out through your firewall.

2. Stops Virus Attacks

Nothing can close your digital activities faster and harder than a virus attack. With hundreds of thousands of new threats developing every day, it is important that you put in place defensive measures to keep your system healthy. One of the most visible benefits of a firewall is its ability to control the points of your system and prevent virus attacks. The cost of the damage caused by a virus to attack your system can be very high, depending on the virus.

3. Prevents Hacking

Unfortunately, a growing trend of businesses moving toward digital activities invites thieves and bad guys to do the same. With the proliferation of data theft and criminals holding systems hostage, firewalls become even more important, as they prevent hackers from accessing your data, emails, systems without unauthorized access. and more. Firewalls can stop hackers completely or prevent them from choosing their target more easily.

4. Stops Spyware

In a data-driven world, a much-needed benefit is to prevent spyware from accessing and entering your system. As the systems become more complex and powerful, the entry points that criminals can use to gain access to your system also increase. One of the most common ways unwanted people gain access is by using spyware and malware - programs designed to break into your system, take control of your computer. account and steal your data. Firewalls act as an important blockade against these malicious programs.

5. Promotes Privacy

An overarching benefit is the promotion of privacy. By proactively working to keep your data and that of your customers safe, you build a secure environment that your customers can trust. No one likes their data to be stolen, especially when it may be obvious that steps may have been taken to prevent the intrusion.

In addition, an upgraded data protection system can be a competitive advantage and a point of sale for customers and customers. Benefits increase the more sensitive the data your company processes.

How firewall works:

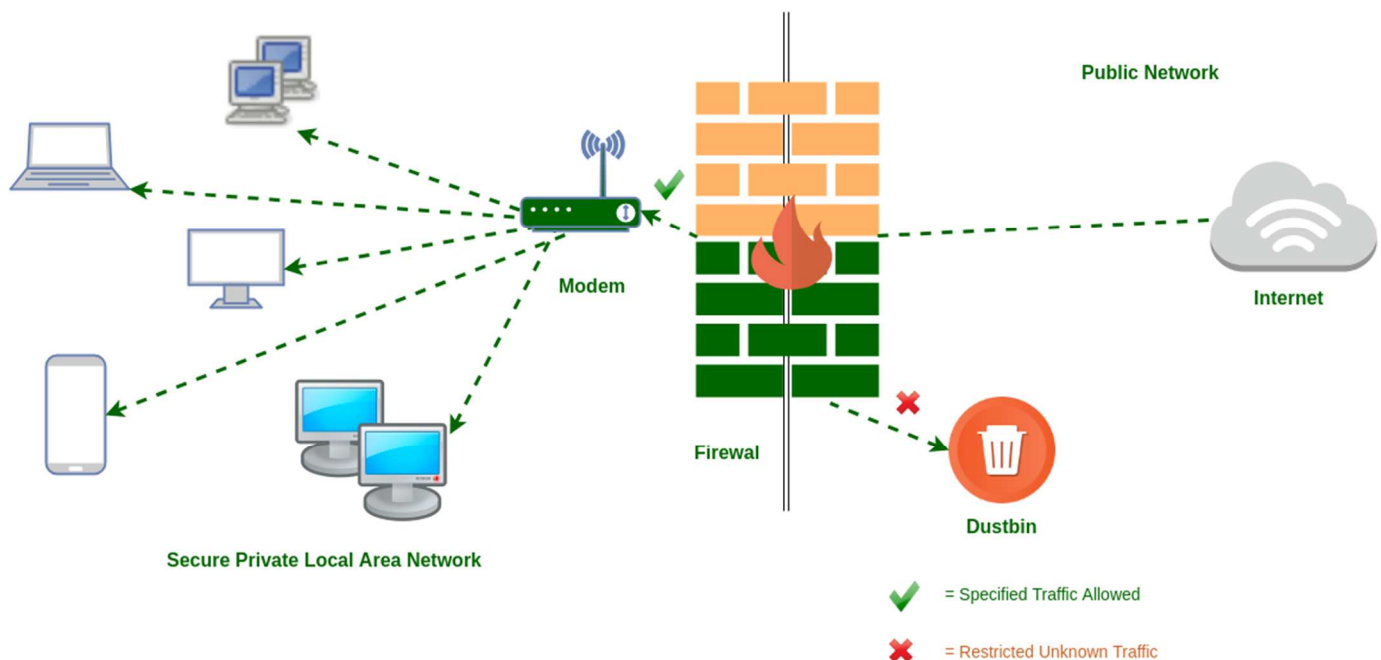


Figure 8-Firewall

2. IDS

Intrusion detection system (IDS) is a software application that monitors a device or network to look for malicious activity or policy violations. Any malicious or disruptive activity is typically reported or collected centrally using security information and event management systems.

An IDS can be used to help analyse the quantity and types of attacks; organizations can use this information to change their security systems or implement more effective controls. An intrusion detection system can also help companies identify bugs or problems with their network device configurations.

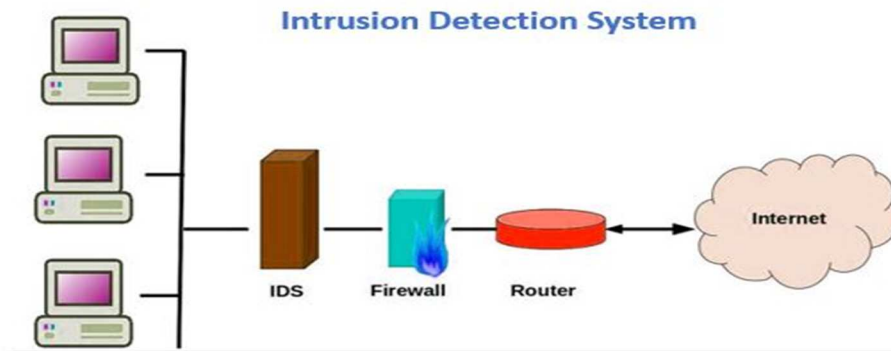


Figure 9-IDS

3. The potential impact(Threat-Risk) of FIREWALL and IDS incorrect configuration to the network

Firewalls and IDS are an essential part of your network's security, and a misconfigured firewall or IDS can damage your organization and make it easy for an attacker to access. Misconfiguration, however, is alarmingly common leading to these impact:

- Firewalls are typically set up with an open policy that allows traffic from any source to any destination. This is because IT teams don't know exactly what they need in the first place and thus start with broad rules and work in reverse. However, due to time pressures or simply not taking it as a priority, they have never finished defining firewall policies. This leaves the network in a permanent state of communication and increases the risk of compromise
- The desired traffic did not reach its intended destination.
- User easily access to dangerous malware or website.
- Creating security vulnerabilities

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

1. DMZ

- a. Definition: In IT security, a demilitarized zone (or DMZ) refers to a subnet that hosts services exposed and accessible from outside a business. It acts as a buffer zone with unsecured networks such as the Internet.

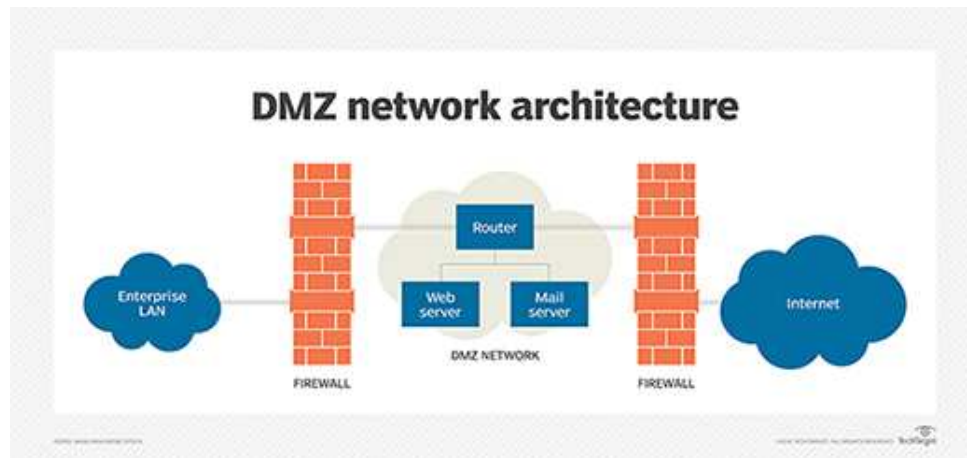


Figure 10-DMZ

- b. Security Function:

The purpose of DMZs is to strengthen the level of security of the company's local network. In this system, an outward-facing protected and monitored network node has access to the items exposed within the cloud zone while the rest of the network is protected by a firewall. When properly implemented, DMZs help organizations find and correct security vulnerabilities before they reach the internal network, where the most valuable resources are stored.

2. Static IP

- a. Definition: An Internet Protocol (IP) address is a unique number assigned to each computer on a network. A computer on the Internet can have a static IP address, which means it stays the same over time, or a dynamic IP address, which means the address can change over time.

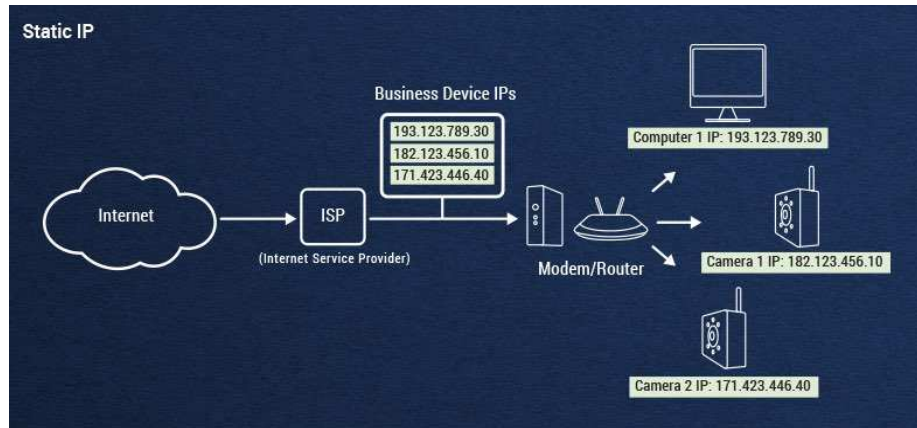


Figure 11-Static IP

b. Security function

A static IP address is assigned permanently to your network, and you or the administrator will need to assign the address manually. A static IP address is suitable for those who are concerned about their online security as it can provide them an added layer of protection. Since you're the only individual who knows the IP address, it's nearly impossible for anyone else to figure it out. Additionally, a Static IP address is reserved for you only, meaning no one else can gain access to it unless you permit it. You can also customize it according to your security needs. For example, a static IP address can help you get a more secure way of using your security camera. You can easily set it up on your security camera and access it from any corner of the globe. You can rest assured about your online security as the Static IP is reserved for you, hence inaccessible by others.

3. NAT

- a. Definition: Network address translation (NAT) is designed to preserve IP addresses. It allows private IP networks to use unregistered IP addresses to connect to the Internet. NAT works on a router, typically connecting two networks together and turning private (not globally unique) addresses in the local network into legitimate ones, before packets are moved to another network.

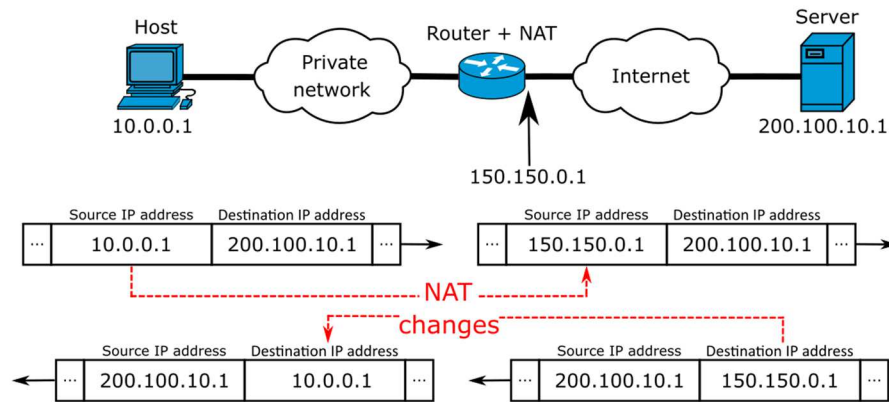


Figure 12-NAT

b. Security function

Basically, NAT allows a single device, such as a router, to act as an agent between the Internet (or public network) and a local network (or private network), which means that only a single unique IP address is required to represent an entire group of computers to anything outside their network. NAT helps improve security and decrease the number of IP addresses an organization needs. NAT gateways sit between two networks, the inside network and the outside network. The gateway makes outbound traffic from an inside system appear to be coming from one of the valid external addresses. In large networks, some servers may act as Web servers and require access from the Internet. These servers are assigned public IP addresses on the firewall, allowing the public to access the servers only through that IP address. However, as an additional layer of security, the firewall acts as the intermediary between the outside world and the protected internal network.

Conclusion

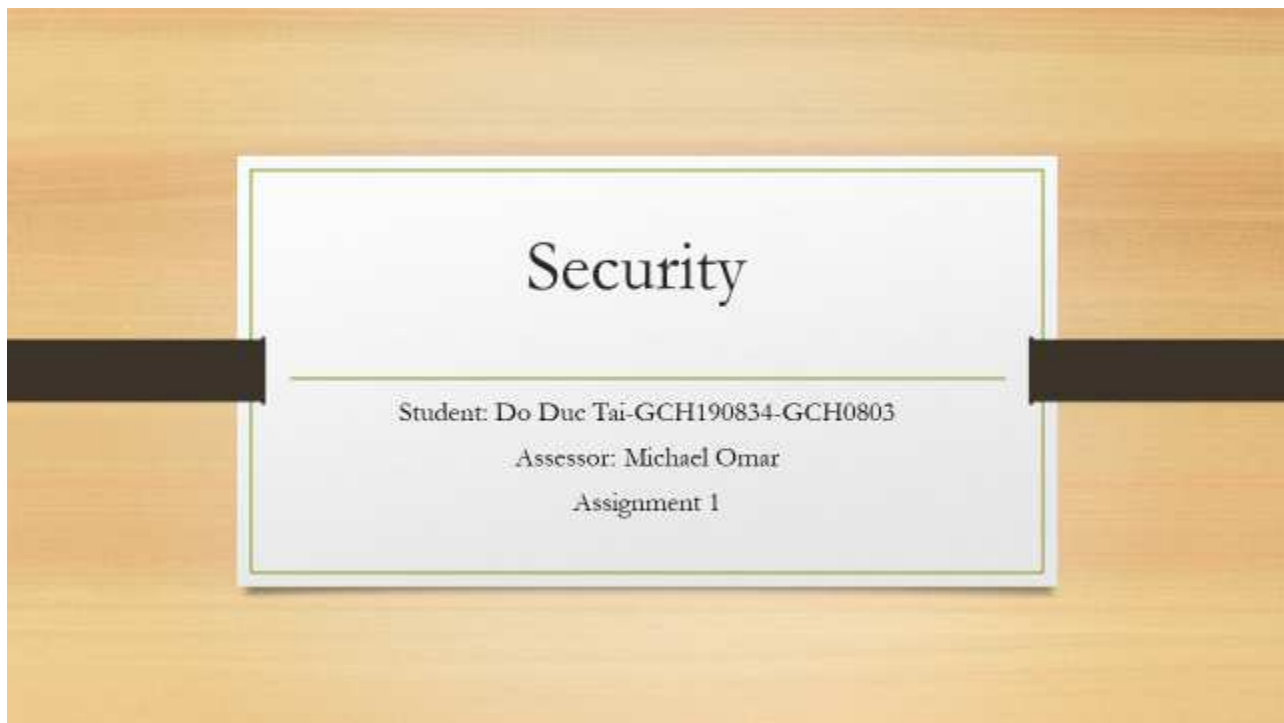
The challenge of keeping computers safe has become increasingly difficult and attacks can be performed without human intervention and infect millions of computers in a few hours. Information security protects the integrity, confidentiality and availability of information on devices that store, manipulate and transmit information through products, people and processes. In the report, you can see information security has its own set of terminology and a threat is an event or an action that can defeat security measures and result in a loss. Organizations and users must keep their confidential information

up to date as security intrusions and sabotages become increasingly sophisticated and difficult to deal with in a short period of time.

Evaluate

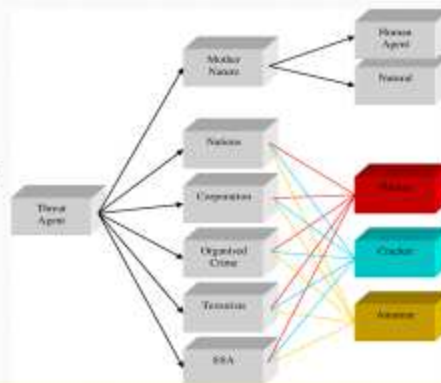
In this assignment, author had contributed his knowledge that he learned. This report may not be so detail but overall it reached all Pass conditions and it lack of conditions to get Merit and Distinction so it need to be improve and more professional in the future. During doing the assignment, it helps author understand better in some sessions but some sessions are still quite difficult to fully clear.

PowerPoints



Identify types of security threat to organisations

- **Threat:** It can be defined as a potential for security intrusion, which exists when there is an entity, capability, circumstance, action or event that could cause harm through vulnerabilities of security.
- **Threat agent:** An individual or group that acts, or has the power to, exploit a vulnerability or conduct other damaging activities. For example, threat agents are malicious hackers, organized crime, insiders (including system administrators and developers), terrorists, and nation states.



Identify types of security threat to organisations

- **Types of threat that organization will face:**

Malware Attack

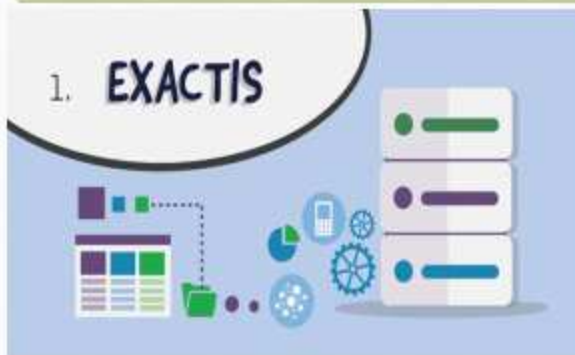
Social Engineering Attack

Application Attack

Networking-Based Attacks



Example of a recently publicized security breach and discuss its consequences



Consequences: The data which were exposed contains of Personally Identifiable Information (PII) of over 200 million customers and it can be used to build detail personal profiles.

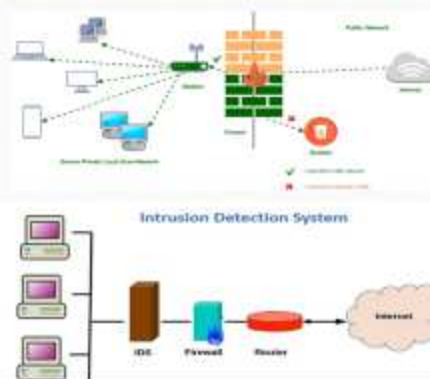
Describe some organizational security procedures

- Acceptable Use Policy (AUP)
- Access control policy (ACP)
- Change Management Policy
- Information security policy



The potential impact to IT security of incorrect configuration of firewall policies and IDS

- **Firewall:** This is a system designed to prevent unauthorized access to or from a private network. You can implement a firewall in either hardware or software form, or a combination of both. Firewalls prevent unauthorized internet users from accessing private networks connected to the internet, especially intranets.
- **Intrusion detection system (IDS)** is a software application that monitors a device or network to look for malicious activity or policy violations. Any malicious or disruptive activity is typically reported or collected centrally using security information and event management systems.



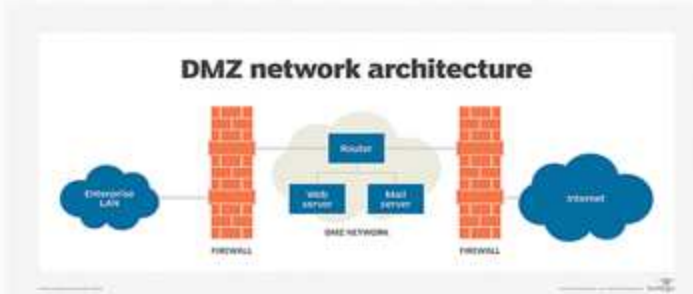
The potential impact of FIREWALL and IDS incorrect configuration to the network

- The network is in a permanent state of communication and increases the risk of compromise
- The desired traffic did not reach its intended destination.
- User easily access to dangerous malware or website.
- Creating security vulnerabilities



DMZ, Static IP and NAT

- DMZ: In IT security, a demilitarized zone (or DMZ) refers to a subnet that hosts services exposed and accessible from outside a business. It acts as a buffer zone with unsecured networks such as the Internet.



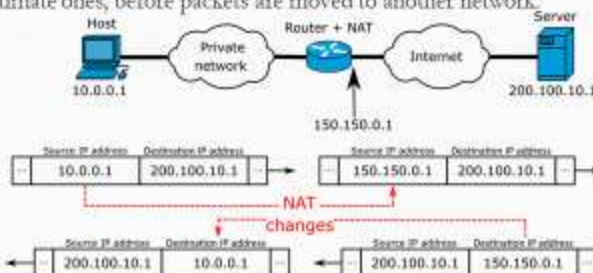
DMZ, Static IP and NAT

- A static IP address is assigned permanently to your network, and you or the administrator will need to assign the address manually. A static IP address is suitable for those who are concerned about their online security as it can provide them an added layer of protection.



DMZ, Static IP and NAT

- Network address translation (NAT) is designed to preserve IP addresses. It allows private IP networks to use unregistered IP addresses to connect to the Internet. NAT works on a router, typically connecting two networks together and turning private (not globally unique) addresses in the local network into legitimate ones, before packets are moved to another network.



References

Auger, R., 2010. *XML Injection*. [Online]

Available at:

<http://projects.webappsec.org/w/page/13247004/XML%20Injection#:~:text=XML%20Injection%20is%20an%20attack,intend%20logic%20of%20the%20application.>

[Accessed 11 12 2020].

Beal, V., 2015. *pop-up window*. [Online]

Available at:

https://www.webopedia.com/TERM/P/pop_up_window.html#:~:text=A%20window%20that%20suddenl y%20appears,it%20then%20disappears.&text=Also%20see%20pop%20Dup%20ad.

[Accessed 9 12 2020].

Bennatan, R., 2020. *Social Engineering*. [Online]

Available at: <https://www.imperva.com/learn/application-security/social-engineering-attack/>

[Accessed 9 12 2020].

Conrad, E., 2017. *Client-Side Attack*. [Online]

Available at: sciencedirect.com/topics/computer-science/client-side-attack

[Accessed 11 12 2020].

Goled, S., 2020. *What Is Poisoning Attack & Why It Deserves Immediate Attention*. [Online]

Available at: <https://analyticsindiamag.com/what-is-poisoning-attack-why-it-deserves-immediate-attention/>

[Accessed 11 12 2020].

Johansen, A. G., 2019. *Malware attacks: What you need to know*. [Online]

Available at: <https://us.norton.com/internetsecurity-malware-malware-101-how-do-i-get-malware-complex-attacks.html>

[Accessed 9 12 2020].

Kettle, J., 2020. *SQL injection*. [Online]

Available at: <https://portswigger.net/web-security/sql-injection>

[Accessed 11 12 2020].

KirstenS, 2009. *Cross Site Scripting (XSS)*. [Online]

Available at: <https://owasp.org/www-community/attacks/xss/>

[Accessed 11 12 2020].

Rouse, M., 2005. *dumpster diving*. [Online]

Available at: <https://searchsecurity.techtarget.com/definition/dumpster-diving>

[Accessed 10 12 2020].

Scott, G., 2020. *HOW TO IDENTIFY NETWORK SECURITY THREATS AND VULNERABILITIES?*. [Online]

Available at: <https://blog.eccouncil.org/how-to-identify-network-security-threats-and-vulnerabilities/#:~:text=A%20network%20security%20threat%20is,vulnerability%20within%20your%20computer%20network.>

[Accessed 9 12 2020].

Swinhoe, D., 2019. *What is a man-in-the-middle attack? How MitM attacks work and how to prevent them*. [Online]

Available at: [https://www.csoonline.com/article/3340117/what-is-a-man-in-the-middle-attack-how-mitm-attacks-work-and-how-to-prevent-](https://www.csoonline.com/article/3340117/what-is-a-man-in-the-middle-attack-how-mitm-attacks-work-and-how-to-prevent-them.html#:~:text=A%20man%2Din%2Dthe%2Dmiddle%20(MitM)%20attack,traffic%20traveling%20between%20the%20two.)

[them.html#:~:text=A%20man%2Din%2Dthe%2Dmiddle%20\(MitM\)%20attack,traffic%20traveling%20between%20the%20two.](https://www.csoonline.com/article/3340117/what-is-a-man-in-the-middle-attack-how-mitm-attacks-work-and-how-to-prevent-them.html#:~:text=A%20man%2Din%2Dthe%2Dmiddle%20(MitM)%20attack,traffic%20traveling%20between%20the%20two.)

[Accessed 11 12 2020].