ASSIGNMENT 1 FRONT SHEET

Qualification	**TEC Level 5 HND Diploma in Computing**		
Unit number and title	**Unit 5: Security**		
Submission date	January 3,2020	**Date Received 1st submission**	
Re-submission Date		**Date Received 2nd submission**	
Student Name	NGUYEN CHI HAI	**Student ID**	GCC18033
Class	GCC0701	**Assessor name**	THAI MINH TUAN
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	NGUYEN CHI HAI

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	2019 – 2020		
Unit Tutor			
Issue date	18 Dec 2019	**Submission date**	**1st: 03 Jan 2020** **2nd: 10 Jan 2020**
IV name and date			

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 Swindon called *NorthStar Secure*

NorthStar Secure works with medium sized companies in the 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 Khuong, 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:

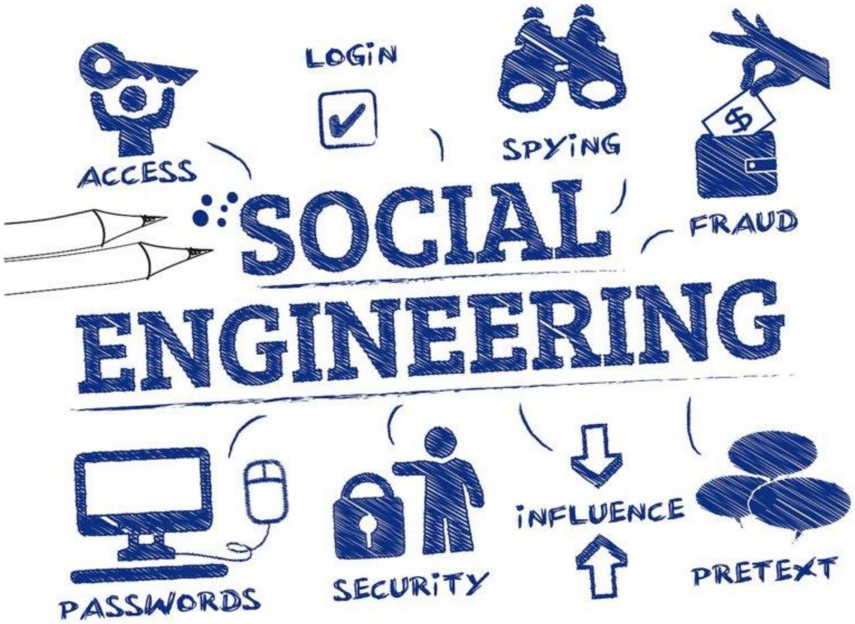
1. **Identify** the risks NorthStar Secure may face if they have a security breach. Give an example of a recently publicized security breach and discuss its consequences
2. **Describe** a variety of organizational procedures an organization can set up to reduce the effects to the business of a security breach.
3. **Propose** a method that NorthStar Secure can use to prioritize the management of different types of risk
4. **Discuss** three benefits to NorthStar of implementing network monitoring system giving suitable reasons.
5. Investigate network security, **identifying** issues with firewalls and VPN's 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 NorthStar Secure

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		**LO1 & 2** **D1** Investigate how a 'trusted network' may be part of an IT security solution.
P1 Identify types of security risks to organisations. **P2** Describe organisational security procedures.	**M1** Propose a method to assess and treat IT security risks.	
LO2 Describe IT security solutions		
P3 Identify the potential impact to IT security of incorrect configuration of firewall policies and third-party VPNs. **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.	

P1: Identify types of security risks to organizations.

- Threats.
  - 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. (Securitybox., n.d.)



Social Engineering

- Malware Attacks.

  Introduction

  A malware assault arises when a software attacker develops malware and installs it on a system without someone understanding it to obtain access to or harm sensitive information. Virus, spyware, ransomware and trojan horses are various forms of malware.
  Malware attacks can occur on all types of devices, including Microsoft Windows, macOS, Android, and iOS systems.

  (Symantec, n.d.)

  1. Virus.
     - 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. (DuPaul, n.d.)

2. Worm.
   - 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. (DuPaul, n.d.)

3. Trojan Horses.
   - A Trojan horse, commonly called a' Trojan,' is a form of malware that masks itself as a normal user downloading or installing malware. A Trojan may provide an infected computer with a malicious party remote access. 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. (DuPaul, n.d.)

4. Ransomeware.
   - Ransomware is a kind of ransomware that keeps a computer system hostage for a ransom. The malware prevents the user from accessing the device by either encrypting hard disk files or locking the machine and displaying messages which require the user to pay the malware maker for removing the restrictions and restoring access to the computer. Typically, Ransomware spreads through a downloaded file and some

other vulnerability in a network service like a normal computer worm ends up on a computer. (DuPaul, n.d.)

5. Adware.
   - Adware is a form of malware that automatedly delivers notoriety (Short for advertising-supported software). Common examples of adware include pop-up ads on software-displayed websites and advertising. Software and applications often offer "free" versions bundled with adware. The bulk of adware is ads funded, written or used as a method for generating income. While some adware is intended only to provide advertising, it is not rare for spyware to detect user activity and steal information from adware. Due to the addition of spyware capabilities, adware and spyware bundles are much more dangerous than adware alone. (DuPaul, n.d.)

6. Spyware.
   - Spyware is a malware category that operates without its awareness by spying on user activity. The tools for espionage could include tracking activity, keystrokes analysis, data collection (account information, logins, financial information) and more. Spyware often also includes extra features, from changing program or application security settings to interacting with network links. Spyware spreads through the use of software vulnerabilities, the combination of legitimate programs or Trojan software. (DuPaul, n.d.)

7. Rootkid.
   - A rootkit is a form of malicious software intended to enter or monitor a computer remotely without users or security programs finding it. Once a rootkit is mounted, the malicious party behind the rootkit is able to execute files remotely, access / steal details, change device settings, modify software (especially protection software that might detect a rootkit). Thanks to its persistent service, rootkit avoidance, identification and elimination may be hard. Since rootkits conceal their existence on a continuous basis, traditional security products can not identify and uninstall rootkits. The identification of rootkits also requires manual approaches, such as device inspection, signature testing and review of data dump. Organizations and customers should periodically fix bugs of apps, programs and operating systems to upgrade virus descriptions to prevent unauthorized updates and check static data to insure they defend themselves from rootkits. (DuPaul, n.d.)

8. Back Doors.
    - A loophole applies to any mechanism in the field of cybersecurity that allows allowed and unauthorized users to bypass standard security measures and achieve high-level access (aka rotary access) from a computer system, network or software application. After delivery, cyber criminals will capture personal and financial details from a backdoor and install additional malware, and hijack appliances. (Malwarebytes, n.d.)

- 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.

1. Cross-Site Scripting (XSS)
    - 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. (Veracode, n.d.)

2. SQL Injection
    - The SQL Injection is a code protection flaw that enables an intruder to manipulate the database of an application–enabling them to view or to extract data, to alter the data-driven behaviour of an application and other unintended stuff–by tricking an application to issue unnecessary SQL commands. The most popular vulnerabilities to computer integrity are SQL injections. An intruder can include their very own SQL

commands that the database performs if the program refuses to properly sanitize this untrusted data before applying it to an SQL query. These SQLi vulnerabilities are a major web applications concern and many companies are susceptible to potential data breaches resulting out of SQL injection. SQLi vulnerabilities are easy to prevent. (Veracode, n.d.)

3. XML Injection
   - 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. (Dahiya, n.d.)

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 root directory and the Access Control Lists (ACL) are the two authentication methods web servers use to limit user access. The key directory on a computer file system is the root directory. User access is limited to the root directory, which means that users can not access directories or files outside the root. To determine user access rights and privileges, administrators use Acces Control Lists to view, download, and execute data.

- Network 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. (Akamai, n.d.)

1. Denial of Service (DoS)
   - DoS attacks are a tool that prevents authorized users from accessing a network or a web site and prevents connectivity assaults. In fact, the

attack objective (normally the site server) is overwhelmed because of heavy traffic or because malicious requests are made that render the aim attack. The computer became faulty or crashed completely. Some well-known types of Denial of Service Attacks include: Buffer overflow, Smurf attack, SYN flood, etc. (Binance, n.d.)

- Buffer overflow:
    - A buffer overflow is a common software coding error that an attacker could use to get a system access. It is important to understand the buffer overflows, the dangers that they pose to your applications and what techniques attackers use to successfully exploit these vulnerabilities to mitigate buffer overflow vulnerabilities. (Veracode, n.d.)
- Smurf attack:
    - Smurf is a network layer denial of service (DDoS), which is called after the malware DDoS.Smurf and allows it to be performed. Smurf attacks are identical to ping flooding, because both are done by submitting ICMP Echo request packets. Smurf attacks are close. However Smurf is a vector of amplification attack, which increases its damage potential by utilizing the features of broadcast networks, unlike regular ping floods. (Imperva, n.d.)
- 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 high-capacity devices that maintain millions of connections can take this type of attack down. (Netscout, n.d.)

2. Interception
    - Every wireless network that requires the username and password to access the local network will detect and track traffic assaults. A variety of sniffing device typically includes a username and password to accomplish this function by collecting the initial part of the relation. The attacker will disguise it as a legitimate user and enter the network with

these credentials. Some well-known types of Interception Attacks include: Man-in-the-Middle attack, Replay attack, etc.

- 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. (Veracode, n.d.)
- Replay attack:
    - A repeat attack occurs as cyber criminals send a message onto a secure network, intercept it and then interrupt or divert the user to do what the intruder wishes. It is a malicious phenomenon. A hacker does not even need the advanced skills to decode the message after the network catches it. Through merely restoring the whole lot, the assault will succeed. (Kaspersky, n.d.)

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 Resolutions Protocol (ARP) poisoning is when a falsified ARP message is sent by an attacker via a local area network (LAN) to connect the MAC address of an attacker with the IP address of a legible network device or server. Once the MAC address of the intruder is attached to an initial Address, any message sent to the correct MAC address can be sent. As a consequence, an intruder can reveal to the valid MAC address intercept, change or obstruct. The word address resolution refers to the process of locating a MAC that is part of the IP

address for a network device. The address resolution protocol (ARP) is a mechanism for mapping IP network addresses to device addresses of a data related protocol, which is used for Internet Protocol (IP), especially IPv4. The protocol functions under the network layer as part of the OSI network and OSI access layer interface. It is used for Ethernet as IPv4 is introduced. (Doubleoctopus, n.d.)

4. Attacks on Access Rights.
    - 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. (Rouse, n.d.)

- ❖ Natural Impact:
    - ➢ The impact of nature on the hardware of the company system includes: Fire, Tsunami, Earthquake, etc. It has a significant impact on an organization's system that can be corrupted and, worse, lose all of an organization's data.
- ❖ Human impact:
    - ➢ Besides natural disasters, it is partly due to humans. Human impact on an organization's system is not as small as: Employees are bribed by a rival organization, Employees who are prejudiced against the organization or its leaders will sabotage, Human accidentally or intentionally damaging the system does not accept responsibility, etc.

P2: Describe organizational security procedures.

Introduction

Safety issues the defense of corporate properties, including staff, documents, facilities and networks from threats, the use, in the context of vulnerability testing / security policies and techniques of identification, disclosure of safety violations and efficient response.

- Impacts organizational.
    1. Security vulnerabilities.
        - ➢ Security vulnerabilities are weaknesses in the design and configuration of the system. They allow an attacker to steal the database, gain administrative rights, overwrite content, and perform many other misconducts. Usually in a business will be affected by 2 types of vulnerabilities:
            - Vulnerabilities exist in software and equipment used by enterprises (objectively): For example, vulnerabilities exist in Windows, WordPress, Skype, CRM software, Wi-Fi router / modem devices, etc.

        - Gaps arising when enterprises design software or applications (subjective): The most common are web and mobile application vulnerabilities such as Cross-site Scripting, SQL injection, authorization errors, misconfiguration errors, etc.
    - Solution:
        - All these technology problems are risky only if hackers locate them and use them. So, organization prevent attacks if they "patched" holes in time (although this is not easy). Here are some successful risk management solutions:
            - Upgrade devices, operating systems, and programs to LATEST so that the user gets updates as soon as possible.
            - Do not use tools for crack. The crack app is sometimes the "back door" for hackers to target businesses.
            - Use the entire system with automated scanning of vulnerability and vulnerability assessment tools. The bulk of simple bugs are therefore observed.
            - Perform regular pen-tests to detect vulnerabilities in applications and products like Web sites, mobile apps, IoTs and software. For organization that rely on a website / mobile app, this is even more essential for increasing the number of users.

2. IOT Device is not safe.
    - The common safety weaknesses of the IoT systems used include: loose authentication, unencrypted information transmission and SQL vulnerabilities (using default log-in information credentials). Failure to check and encrypt security changes for injection and salesmen. By using these weaknesses, hackers can easily hijack personal data, login and malicious code into the system of the device.
    - Solution:
        - One of the most important factors in ensuring the security of the internal IoT system is the process of evaluating and selecting equipment suppliers for the organization. The owners of the organization should ensure that their partners comply with safety requirements and have support forms to resolve device safety problems immediately during the functioning process.
        - In addition, the unit needs to perform self-examination and assessment of device security with the following basic steps:
            - Do not use devices that do not support software upgrades, firmware or change passwords.
            - Change the default login name and password before connecting the device to the Internet.

- The password used on each IoT device must be unique, especially for devices with direct Internet connection.
- Always install the latest patches for these devices through software and firmware updates to minimize the risk of device attacks.
- Check the security and data usage policy of the application (application) used to control the device.
- Installing IoT device system on a private network, setting up firewalls and constantly monitoring to detect abnormal signs.

3. BYOD (Bring your own device).
   - Data exchange is a difficult issue for BYOD-applied systems, provided that these machines do not follow data security requirements, which could contribute to data leakage. In the transmission, handling and retrieval of data on personnel computers it is difficult to ensure security and exposure to internal data. Personal devices are also at increased risk for malware infection because they can't control the networks with which they connect: home networks, public wireless networks, etc. For public WLAN, internals are at risk of exposure to an assault or observation by an individual in the center.
   - Solution:
     - Organizations implementing BYOD initiatives will guarantee mandatory safety procedures for computers connected to network infrastructure and accessing client sensitive information. The terms and conditions of the BYOD system should be followed:
       - Used computers are constantly updated to deter malware attempts by recently discovered bugs through security patches.
       - Apply forms of information security such as mobile device administration (MDM), app virtualization and containerization.
       - Limit IP access: only allow for IP address access to the company's admin page. As such, staff cannot access the remote management page.
       - Simply and for the right purpose open access to data. Various locations need access to various data types. If not required, prevent access to sensitive data.
       - Check third parties ' security controls and ensure they meet your requirements with respect to their data protection practices and have the right to audit them.
       - Instruct your workers to ensure they learn and understand the importance of your data protection policies.
4. Data theft.

- Theft of data is the theft of information from a suspected person located on machines, websites or other tools, in order to jeopardize the security of privacy or to gain private details. To individual computer users as well as large companies and organizations, data theft is an ever growing problem. Data theft occurs both externally and internally and reduces the risk of corporate insider data theft is nothing short of easy. This is particularly the case as system administrators and staff have access to technology such as computers for applications, desktops and electronic devices such as USB hubs, smart phones or other portable or mobile devices.
- Solution:
  - With the likelihood of data theft rising into an issue, organization and organizations will take steps to protect their sensitive data. Every organizations can take certain steps to protect its information:
    - Protect clients, staff and records by preserving sensitive data storage devices in a secured, secure area and reducing sensitive information exposure.
    - Delete any sensitive data correctly before disposing of them and delete them from servers and appliances.
    - Using password protection for all business computers and devices and require employees to be able to change frequently with specific usernames and secure passwords.
    - Sensitive data is encrypted, all computers, including e-mails containing sensitive data are authenticated, and validated.
    - By using antivirus and anti-spyware applications in all enterprise machines, you are defending against viruses and malware.
    - Keep the operating systems and software up to date by installing security patches, web browsers, operating systems and antivirus software as early as possible.
    - Properly configured firewall access to your network, secure and encrypted remote access via virtual private networks and Wi-Fi networks.
    -

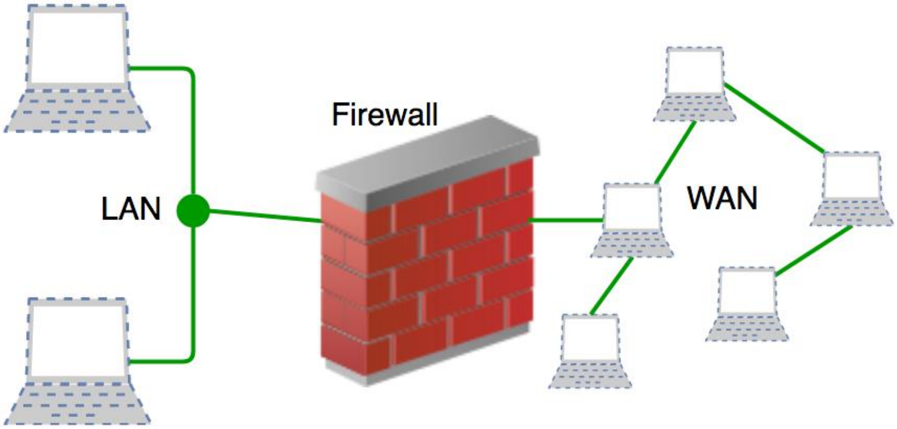
5. Human Impact.
   - It is partially individual in relation to natural disasters. Workers are bribed by competing companies, workers affected or sabotaged by the company, individuals who accidentally or intentionally damage the institution acknowledge no duties, etc.
   - Solution:
     - To overcome the situation mentioned above, an organization needs to have a strict monitoring system for all employees of that organization.

Security camera system in an optimal way to minimize and prevent the aforementioned errors. Administrators of an organization need to strictly examine the abnormal actions of its members to provide timely solutions to prevent the undesirable behaviors of the organization.

6. Natural Disaster.
   - Included are: explosion, flood, earthquake and other consequences of nature on hardware of our business system. It has an important impact on a corruptible network in entities and, worst, the destruction of all records for an organization.
   - Solution:
     - In order to limit and overcome the above disadvantages, we need to regularly back up data, update information on natural disasters in time to find ways to limit and prevent unfortunate incidents, Fire protection systems should be maintained and inspected rigorously on a regular basis.

P3: Identify the potential impact to IT security of incorrect configuration of firewall policies and third-party VPNs.

1. FWs (Firewalls)
   - In programming, an input and outgoing network traffic management and control system built on default security rules is a firewall. Typical boundaries between an internal trust and a untrustworthy external network like the Web are established with a firewall. (Wikipedia, n.d.)
   - Firewalls are often divided into network firewalls or host firewalls. Network firewalls block and operate on network hardware traffic from two or more networks. The host-based firewalls run on and off these machines on host computers. (Wikipedia, n.d.)

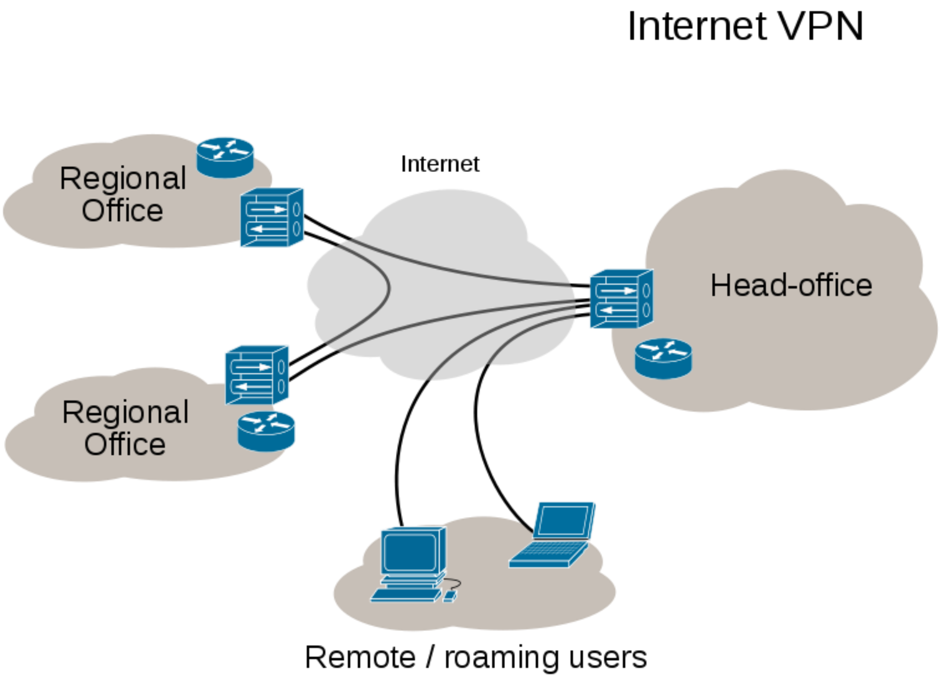


Firewalls

- Problem with incorrect firewall configuration:
    - The data will be stolen by hackers because the firewall cannot prevent unauthorized access.

2. VPN (Virtual Private Network)

- VPN (Virtual Private Network) is a network dedicated to connecting computers together through the public Internet. Computers participating in virtual private networks will "see each other" like in a local area network - LAN (Local Area Network).



- Problem with incorrect VPN configuration:
    - Error Connecting to Firmware on Client VPN
        - ✓ The Cisco VPN Client often has issues with older routers, mostly owing to the configuration of the system. If you experience this issue, please upgrade your router to the latest version of the firmware. Many routers often have problems with Cisco VPN Clients. (ThuThuat, n.d.)

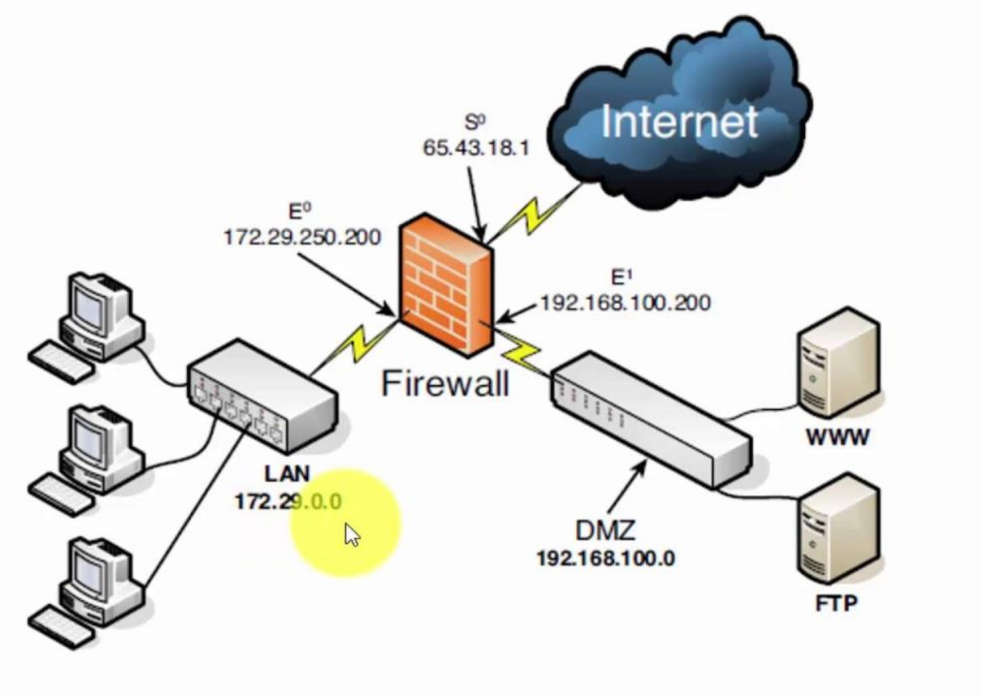
    - Having trouble establishing a VPN connection with NAT device:
        - ✓ This issue can be found on Cisco VPN hardware devices because it is implicit in the way IPSec operated before it came up with specifications that require network packet names to be changed during data transmission. To fix this problem, turn NAT-Traversal (NAT-T)

on your device and open the UDP port 4500 on the firewall. (ThuThuat, n.d.)

<u>**P4**: Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security.</u>

1. Demilitarized zone (DMZ)

- A DMZ is a physical or logical network for connecting hosts which provide an interface with an unconfident external network-usually the Internet-while maintaining a separate and separated internet network – usually a corporate network – in an external Network. (Doubleoctopus, n.d.)

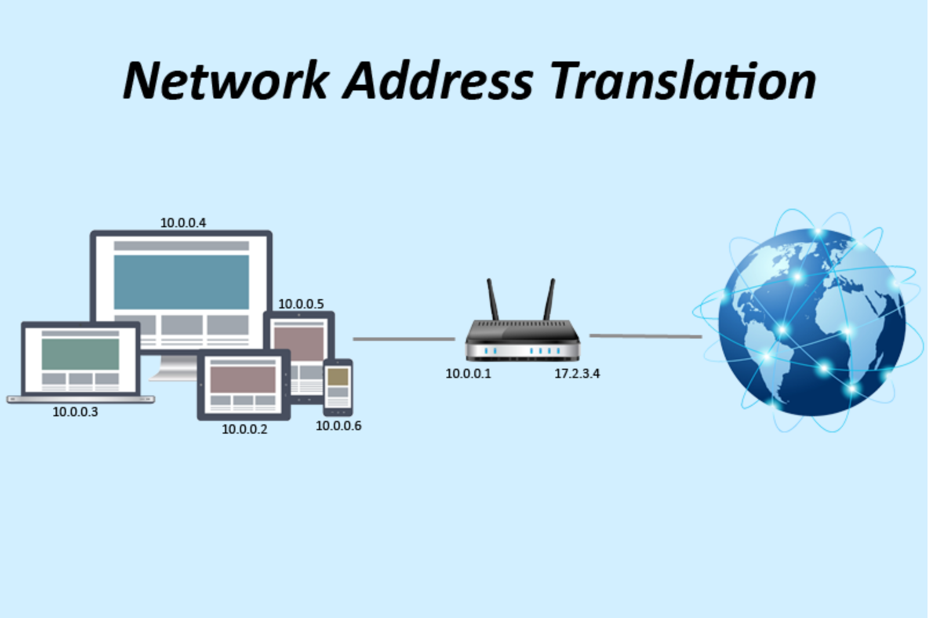


Demilitarized zone (DMZ)

- As networks that are most vulnerable to attacks, they are' quarantined' within the DMZ, from where they have restricted access to the private network and which offer resources for the customer from outside the local network, such as fax, site and Domain name domains (DNS) server. DMZ host communicates with both the internal and external networks, but intercompatibility is strictly restricted with internal network host.
- The DMZ segregated via a secure gateway to funnel the data from DMZ to the personal network. The DMZ is a firewall. In fact, the DMZ itself has a protection gateway to handle inbound data from the external network. (Doubleoctopus, n.d.)

- A DMZ's ultimate aim is to provide untrusted networks with access to resources while retaining a safe private network. In particular, web servers, email servers, FTP servers, and VoIP servers are important services in the DMZ framework. (Doubleoctopus, n.d.)

2. Network Address Translation (NAT)
   - Network Address Translation (NAT) is the mechanism in which a network system, normally a firewall, assigns a public address within a private network to a machine (or computer group). The key use of NAT is to limit the number of public IP addresses to be used for economic and security reasons by the agency or corporation. (whatismyipaddress, n.d.)

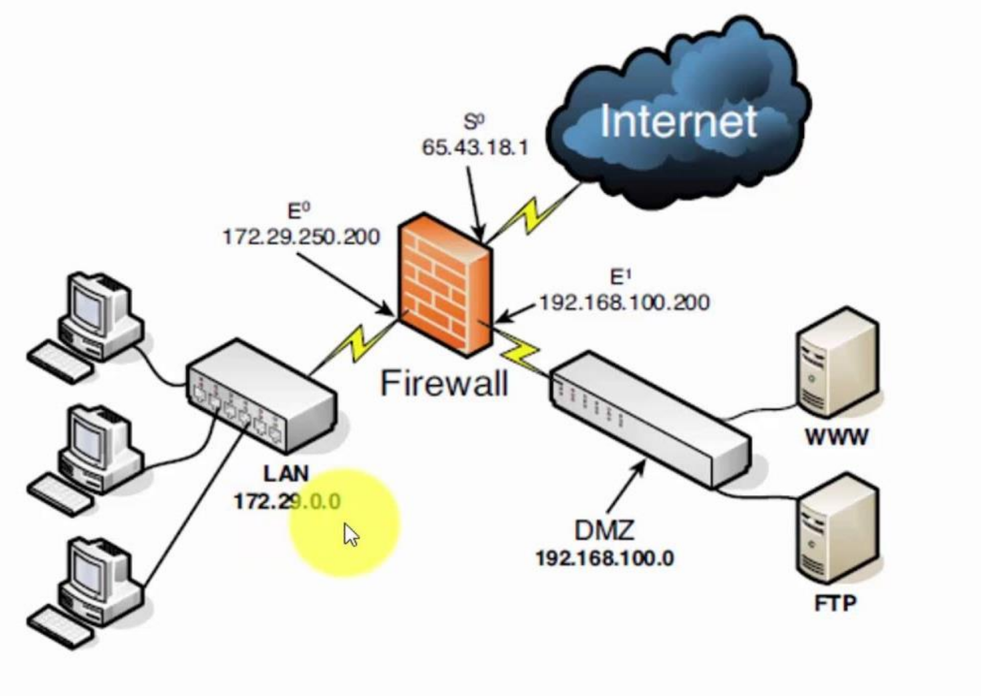


Network Address Translation (NAT)

   - A large private network uses private addresses to form the most common form for Network Translations (10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255 or 192.168.0 to 192.168.255.255). With machines, such as workstations that have connections to file-servers and printers, the private addressing scheme works very well. Private network routers can easily connect traffic to private addresses. Nevertheless, these machines must have a public address to reach services outside the network, such as the Internet, and respond to their queries. That's where NAT is at risk. (whatismyipaddress, n.d.)

3. Static IP
   - A static IP address is an IP address that has been manually configured for a computer, opposed to one that has been allocated to a DHCP server. It's considered stagnant because it's not going to change. It's the exact opposite of the dynamic IP address that varies. (Lifewire, n.d.)

- Conclusion:
  - The DMZ is isolated using a security gateway (i.e. firewall) to filter traffic between the DMZ and the private network. The DMZ itself also has a security gateway in front of it to filter incoming traffic from the external network. The DMZ is segregated by using a protection gateway (i.e. firewall) to redirect data between the DMZ and the private network. The DMZ itself also has a security gateway in front of it to filter incoming traffic out of the external network.



  - Firewalls closely examine incoming traffic on the basis of pre-established rules and filter traffic originating from unsecured or unknown sites to prevent attacks. Firewalls protect traffic at the entry point of a machine named ports, where knowledge is shared with external devices. Only trustworthy individuals (source addresses) are allowed to enter the house (destination address) at all— then it is filtered further so that people inside the house are only allowed to access other rooms (destination ports) based on whether they are the host, the child or the visitor. The occupant is allowed to enter any space (any port) while children and visitors are allowed to enter a certain number of rooms (specific ports).
  - 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

Akamai, n.d. *Akamai.* [Online]
Available at: https://www.akamai.com/us/en/resources/network-attacks.jsp
[Accessed 25 12 2019].

Binance, n.d. *binance.* [Online]
Available at: https://www.binance.vision/vi/security/what-is-a-dos-attack
[Accessed 25 12 2019].

Dahiya, A., n.d. *Medium.* [Online]
Available at: https://medium.com/@dahiya.aj12/what-is-xml-injection-attack-279691bd00b6
[Accessed 25 12 2019].

Doubleoctopus, n.d. *Doubleoctopus.* [Online]
Available at: https://doubleoctopus.com/security-wiki/threats-and-tools/address-resolution-protocol-poisoning/
[Accessed 25 12 2019].

Doubleoctopus, n.d. *Doubleoctopus.* [Online]
Available at: https://doubleoctopus.com/security-wiki/network-architecture/demilitarized-zone/
[Accessed 31 12 2019].

DuPaul, N., n.d. *Veracode.* [Online]
Available at: https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101
[Accessed 25 12 2019].

Imperva, n.d. *imperva.* [Online]
Available at: https://www.imperva.com/learn/application-security/smurf-attack-ddos/
[Accessed 26 12 2019].

Kaspersky, n.d. *Kasperky.* [Online]
Available at: https://www.kaspersky.com/resource-center/definitions/replay-attack
[Accessed 26 12 2019].

Lifewire, n.d. *Lifewire.* [Online]
Available at: https://www.lifewire.com/what-is-a-static-ip-address-2626012
[Accessed 31 12 2019].

Malwarebytes, n.d. *Malwarebytes.* [Online]
Available at: https://www.malwarebytes.com/backdoor/
[Accessed 25 12 2019].

Netscout, n.d. *netscout.* [Online]
Available at: https://www.netscout.com/what-is-ddos/syn-flood-attacks
[Accessed 26 12 2019].

Rouse, M., n.d. *searchsecurity.* [Online]
Available at: https://searchsecurity.techtarget.com/definition/privilege-escalation-attack
[Accessed 26 12 2019].

Securitybox., n.d. *Securitybox..* [Online]
Available at: https://securitybox.vn/3363/tong-quan-ve-social-engineering/
[Accessed 25 12 2019].

Symantec, n.d. *Norton.* [Online]
Available at: https://us.norton.com/internetsecurity-malware-malware-101-how-do-i-get-malware-complex-attacks.html
[Accessed 25 12 2019].

ThuThuat, n.d. *ThuThuat.* [Online]
Available at: https://thuthuat.taimienphi.vn/10-loi-thuong-gap-cua-vpn-va-cach-khac-phuc-15656n.aspx
[Accessed 31 12 2019].

Veracode, n.d. *Veracode.* [Online]
Available at: https://www.veracode.com/security/xss
[Accessed 25 12 2019].

Veracode, n.d. *Veracode.* [Online]
Available at: https://www.veracode.com/security/sql-injection
[Accessed 25 12 2019].

Veracode, n.d. *Veracode.* [Online]
Available at: https://www.veracode.com/security/directory-traversal
[Accessed 25 12 2019].

Veracode, n.d. *Veracode.* [Online]
Available at: https://www.veracode.com/security/buffer-overflow
[Accessed 26 12 2019].

Veracode, n.d. *Veracode.* [Online]
Available at: https://www.veracode.com/security/man-middle-attack
[Accessed 25 12 2019].

whatismyipaddress, n.d. *whatismyipaddress.* [Online]
Available at: https://whatismyipaddress.com/nat
[Accessed 31 12 2019].

Wikipedia, n.d. *Wikipedia.* [Online]
Available at: https://en.wikipedia.org/wiki/Firewall_(computing)
[Accessed 31 12 2019].

Index of comments

2.1 Strengths:
- Understand fundamental concepts of security such as important security risk, security procedures, firewall, VPN, DMZ, NAT.
- The report covers required topics clearly.

Weaknesses:
- The report should be written in a formal style

Improvement: address the weaknesses stated above, resubmit powerpoint slides

Grade: pass

2.2 04/02/2020

2.3 Thai Minh Tuan

2.4 Pass