UNIVERSITY of GREENWICH
Alliance with FPT Education

BTEC

ASSIGNMENT FRONT SHEET

Qualification	**BTEC Level 5 HND Diploma in Computing**		
Unit number and title	**Unit 5: Security**		
Submission date		**Date Received 1st submission**	
Re-submission Date		**Date Received 2nd submission**	
Student Name	VO NHUT HUY	**Student ID**	GCC18169
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	VO NHUT HUY

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 organisational 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 organisational procedures an organisation 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.

<table>
<tr><th colspan="3">Learning Outcomes and Assessment Criteria</th></tr>
<tr><th>Pass</th><th>Merit</th><th>Distinction</th></tr>
<tr><td colspan="2">LO1 Assess risks to IT security</td><td rowspan="5">LO1 & 2
D1 Investigate how a 'trusted network' may be part of an IT security solution.</td></tr>
<tr><td>P1 Identify types of security risks to organisations.

P2 Describe organisational security procedures.</td><td>M1 Propose a method to assess and treat IT security risks.</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 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.</td><td>M2 Discuss three benefits to implement network monitoring systems with supporting reasons.</td></tr>
</table>

P1 Identify types of security risks to organizations.

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

- Digital Security Risks:

I. MALWARE

● Malware is software that enters a computer system without the user's knowledge or consent and then performs an unwanted and usually harmful action.

● Strictly speaking, malware uses a threat vector to deliver a malicious "payload" that performs a harmful function once it is invoked.

- More specifically, there are the following malware:

● Oligomorphic malware: this malware changes its internal code to one of a set number of predefined mutations whenever it is executed. However, because oligomorphic malware has only a limited number of mutations, it will eventually change back into a previous version that may then be detected by a scanner.

● Polymorphic malware: Malware code that completely changes from its original form whenever it is executed is known as polymorphic malware. This is usually accomplished by the malware containing "scrambled" code that, when the malware is activated, is "unscrambled" before it is executed.

● Metamorphic malware can actually rewrite its own code and thus appears different each time it is executed. It does this by creating a logical equivalent of its code whenever it is run.

There are many types of malware that can invade a user's computer:

- Most common types:

- **Circulation/Infection**

1.Viruses

+ Programs that secretly attach to another document or program and execute when that document or program is opened

+ Might contain instructions that cause problems ranging from displaying an annoying message to erasing files from a hard drive or causing a computer to crash repeatedly.

+ Antivirus software defends against viruses is

+ Drawback of antivirus software is that it must be updated to recognize 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 attaches itself to a computer document, such as an e-mail message, and is spread by traveling along with the document

+A virus needs the user to perform some type of action, such as starting a program or reading an e-mail message, to start the infection

+ Worms are usually distributed via e-mail attachments as separate executable programs

+ 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 hide their true intent and then reveals themselves when activated

+ Might disguise themselves as free calendar programs or other interesting software

Common strategies:

+ Giving a malicious program the name of a file associated with a benign program

+ Combining two or more executable programs into a single filename

Defend against Trojan horses with the following products:

+ Antivirus tools, which are one of the best defenses against combination programs

+ Special software that alerts you to the existence of a Trojan horse program

+ Anti-Trojan horse software that disinfects a computer containing a Trojan horse

4. Rootkit

+ A rootkit is a set of software tools used to hide the actions or presence of other types of software.

+ Rootkits do this by changing the operating system to force it to ignore their malicious files or activity.

+ 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 general term used to describe software that secretly spies on users by collecting information without their consent

Key logger that silently captures and stores each keystroke that a user types on the computer's keyboard. The attacker then searches the captured text for any useful information such as passwords, credit card numbers, or personal information.

2. Adware

Adware delivers advertising content in a manner that is unexpected and unwanted by the user. Once the adware malware becomes installed, it typically displays advertising banners, popup ads, or opens new web browser windows at random intervals

3. Ransomware

+ Ransomware prevents a user's device from properly operating until a fee is paid.

+ One type of ransomware locks up a user's computer and then displays a message that purports to come from a law enforcement agency.

– **Delete data**

1. Logic Bombs

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**

1. Back doors

+ The payload of some types of malware attempts to modify the system's security settings so that more insidious attacks can be made.

+ One type of malware in this category is called a backdoor. A backdoor gives access to a computer, program, or service that circumvents any normal security protections.

+ Backdoors that are installed on a computer allow the attacker to return at a later time and bypass security settings.

– **Launch attacks**

1. Zombie and botnet

+ One of the most popular payloads of malware today carried by Trojans, worms, and viruses is software that will allow the infected computer to be placed under the remote control of an attacker.

+ This infected robot (bot) computer is known as a zombie.

+ When hundreds, thousands, or even hundreds of thousands of zombie computers are gathered into a logical computer network, they create a botnet under the control of the attacker (bot herder).

+ Infected zombie computers wait for instructions through a command and control (C&C or C2) structure from the bot herders regarding which computers to attack and how.

+ A common botnet C&C mechanism used today is the Hypertext Transport Protocol (HTTP).

+ A zombie can receive its instructions by automatically signing in to a website that the bot herder operates

+ Another way to receive instructions is to a third-party website on which information has been placed that the zombie knows how to interpret as commands.

+ Some botnets even use blogs or send specially coded attack commands through posts on the Twitter social networking service or notes posted in Facebook.

- Six categories of attackers: hackers, crackers, script kiddies, spies, employees, and cyberterrorists
- Identity attacks attempt to assume the identity of a valid user
- Denial of service (DoS) attacks flood a server or device with requests, making it unable to respond to valid requests
- Malicious code (malware) consists of computer programs intentionally created to break into computers or to create havoc on computers

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.

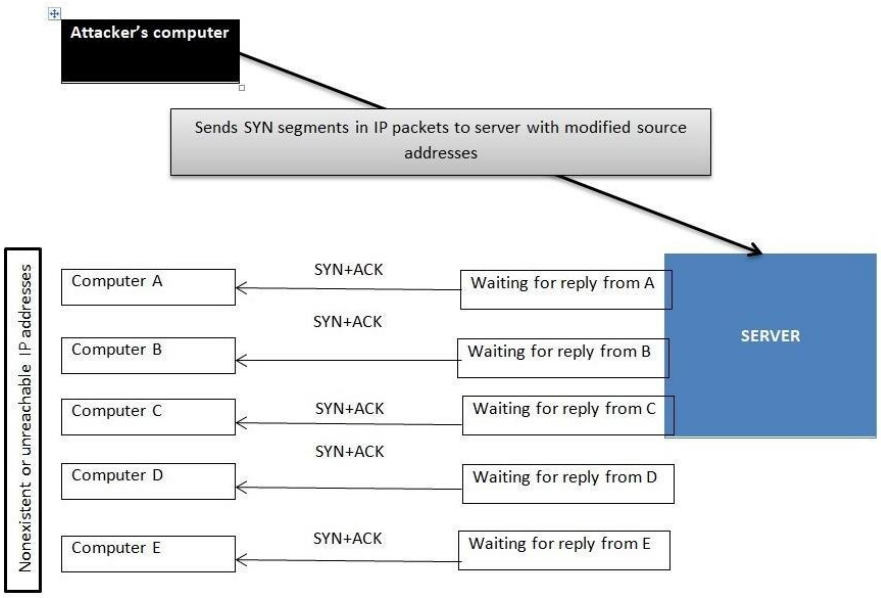
2. Types of DoS attacks

- Ping flood
- Multiple computers rapidly send a large number of ICMP echo requests, overwhelming a server (as well as the network) to the extent that it cannot respond quickly enough and will drop legitimate connections to other clients and refuse any new connections.

3. Smurf attack

- An attacker broadcasts a ping request to all computers on the network but changes the address from which the request came to the victim's computer.
- Each of the computers then sends a response to the victim's computer so that it is quickly overwhelmed and then crashes or becomes unavailable to legitimate users.

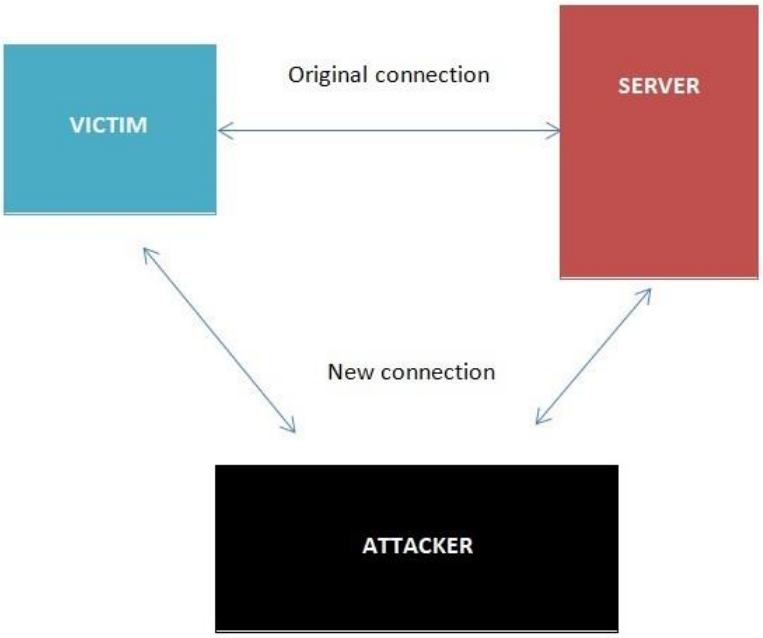
4. SYN Flood attack



- Interception

  + Man-in-the-Middle attack

  + Replay attack



- A replay attack is similar to a passive man-in-the-middle attack.
- Attackers make a copy of the transmission before sending it to the recipient. Later, the attacker can send the original message to the server, and the server may respond. Now a trusted relationship has been established between the attacker and the server.
- The attacker can begin to change the content of the captured message and code. If he eventually makes the correct modification, the server will respond, letting the attacker know he has been successful.

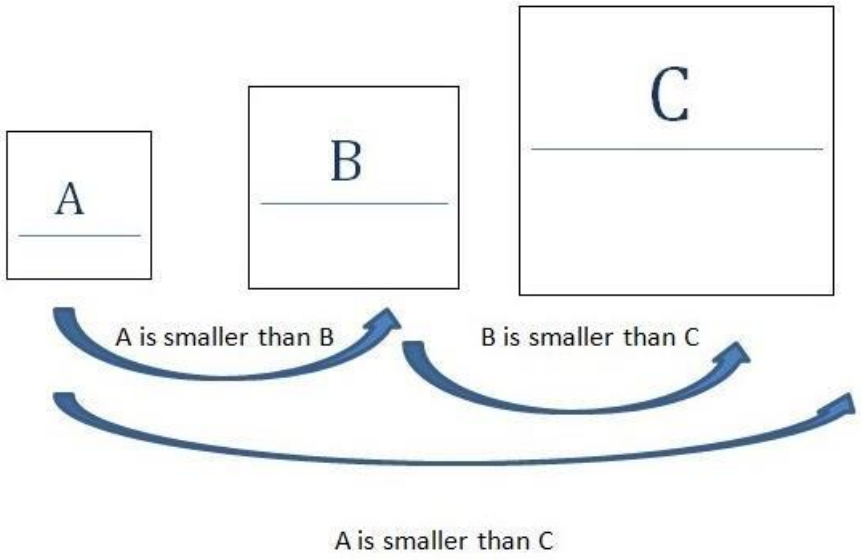
Poisoning

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

- 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: is exploiting a vulnerability in software to gain access to resources that the user normally would be restricted 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.



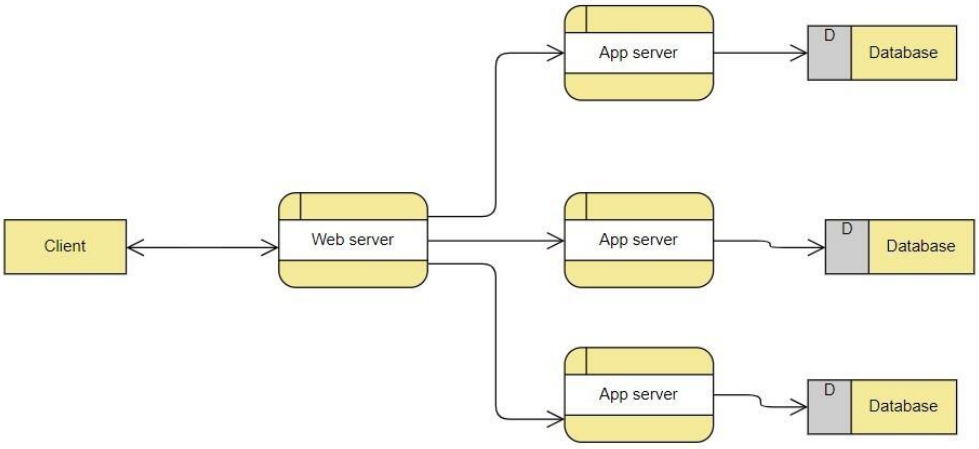
II. Application Attacks

- **Server-Side Web Application Attacks**

+ On the Internet, a web server provides services that are implemented as web applications.

+ An important characteristic of server-side web applications is that they create dynamic content based on inputs from the user.

+ Many server-side web application attacks target the input that the applications accept from users



1. **SQL injection:**

Tons of SQL injection jobs are executed by inserting SQL queries into the interaction data between the client and the Scholars application. The process of exploiting SQL injection error in public can help hackers to retrieve sensitive data in the database, to silence the database (insert/update/delete), execute actions with the rights of the Administrator VI) and higher can control the server operating system

2. **XML Injection:**

Is an assault strategy used to modify or break the XML framework or process logic of the application? The deliberate meaning of the specification can be changed by inserting unwanted XML material and/or constructs into an XML document.

3. **Cross-site scripting:**

Cross-site scripting (XSS) is a form of computer security weakness commonly found in web applications. XSS allows offenders to apply client-side scripts on web pages accessed by other people. An intruder may use cross-site scripting vulnerabilities to circumvent access controls such as the same-origin policy

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**

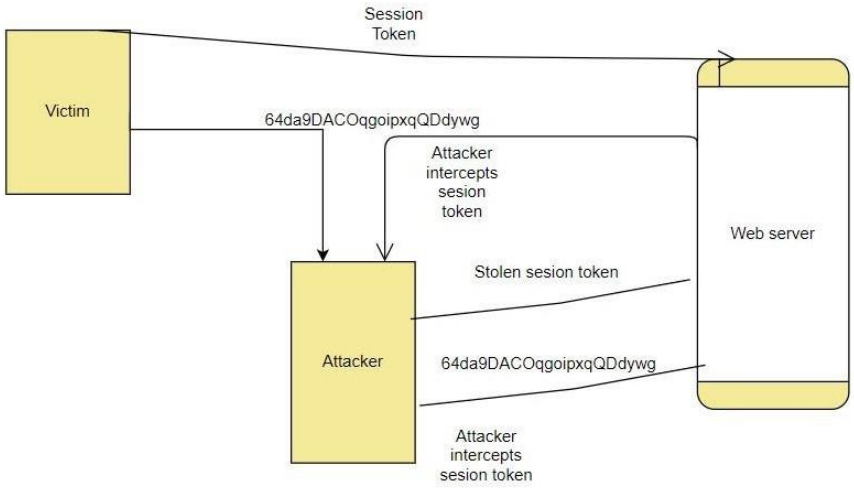
+ A cookie can contain a variety of information based on the user's preferences when visiting a website.
+ Several different types of cookies exist: First-party cookie, Third-party cookie, Session cookie.
+ First-party cookies can be stolen and used to impersonate the user.
+ Third-party cookies can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

- **Attachments**

+ Attachments are files that are coupled to email messages.
+ Malicious attachments are commonly used to spread viruses, Trojans, and other malware when they are opened

- **Session Hijacking**

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



Malicious Add-ons

+ 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.

+ Attackers can take advantage of vulnerabilities in ActiveX to perform malicious attacks on a computer.

Impartial Overflow Attacks

+ Buffer Overflow Attack: A buffer overflow attack occurs when a process attempts to store data in RAM beyond the boundaries of a fixed-length storage buffer.

+ Integer Overflow Attack: the condition that occurs when the result of an arithmetic operation—like addition or multiplication—exceeds the maximum size of the integer type used to store it.

+ Arbitrary/Remote Code Execution: allows an attacker to run programs and execute commands on a different computer.

Social Engineering Attacks

- Today, the global computing infrastructure is most likely target of attacks
- Attackers are becoming more sophisticated, moving away from searching for bugs in specific software applications toward probing the underlying software and hardware infrastructure itself.

Social Engineering

- Easiest way to attack a computer system requires almost no technical ability and is usually highly successful

- Social engineering relies on tricking and deceiving someone to access a system

- Social engineering is not limited to telephone calls or dated credentials

- 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

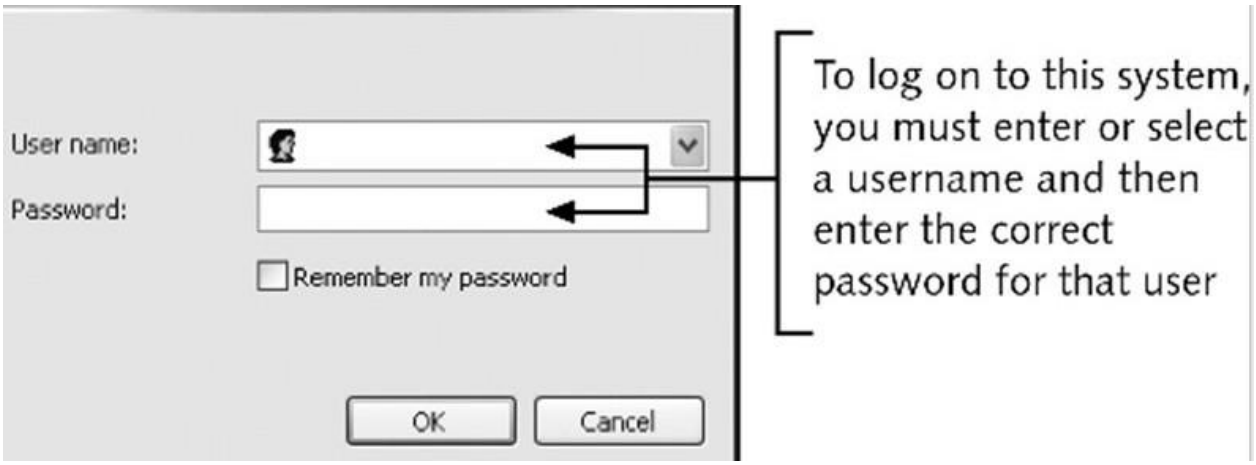
- Educate all employees about the policies and ensure that these policies are followed

Password Guessing

- Password: secret combination of letters and numbers that validates or authenticates a user

- Passwords are used with usernames to log on to a system using a dialog box

- Attackers attempt to exploit weak passwords by password guessing



- 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

- Whereas an active man-in-the-middle attack changes the contents of a message before sending it on, a replay attack only captures the message and then sends it again later

- Takes advantage of communications between a network device and 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

- Certain types of local area networks (LANs), such as Ethernet, must also have another address, called the media access control (MAC) address, to move information around the network

- Computers on a network keep a table that links an IP address with 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 risks that are initiated and managed by computers or systems other than those under attack.

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 straightforward denial of service assault where the intruder overwhelms the target with an ICMP "echo message" (ping) packet. This is most successful by using the flood ping alternative that sends ICMP packets as quickly as possible without waiting for answers.

+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 type of denial of service attack in which the intruder sends a series of SYN requests to the target system in an effort to drain sufficiently server resources to make the device unresponsive to legitimate traffic.

2. Interception:

-In the case of an intrusion attack, a network connection is made compromised or not accessible for legal usage. These are assaults on the performance of the network.

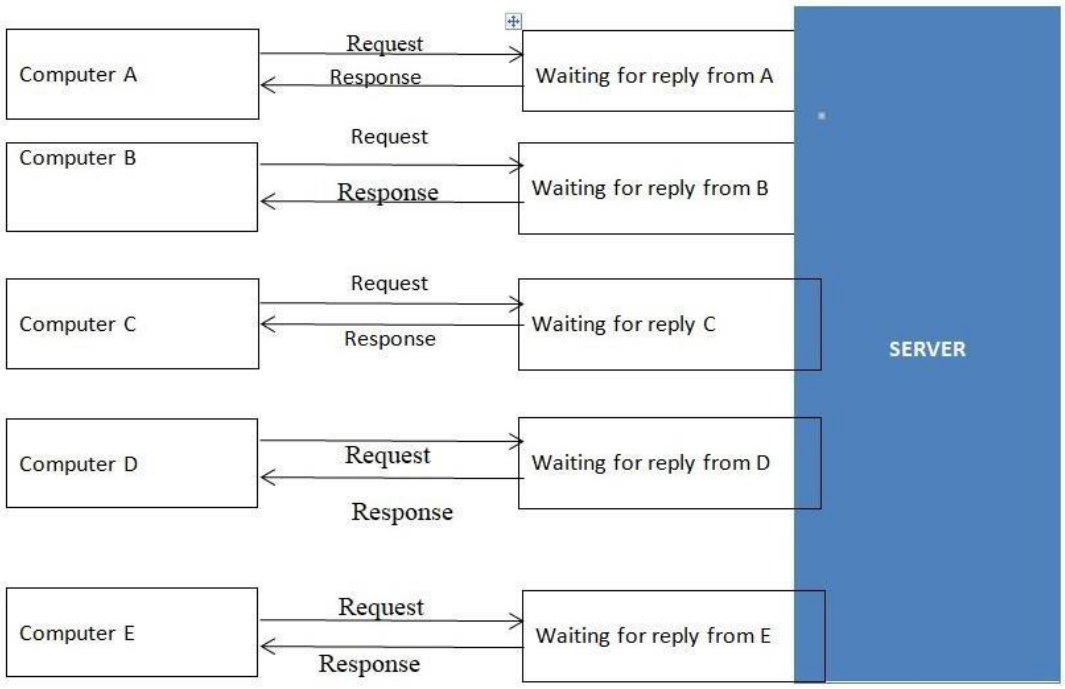
3. Poisoning

- Address Resolution Protocol poisoning (ARP poisoning) is a form of attack in which the attacker alters the address of the Media Access Control (MAC) and targets the Ethernet LAN by modifying the ARP cache of the target computer with the modified ARP request and reaction packets. This modifies the-Ethernet MAC address to the identified MAC address of the hacker to track 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: utilizes a loophole in applications to control information that the consumer will usually be prevented from accessing.



P2 Describe organizational security procedures.

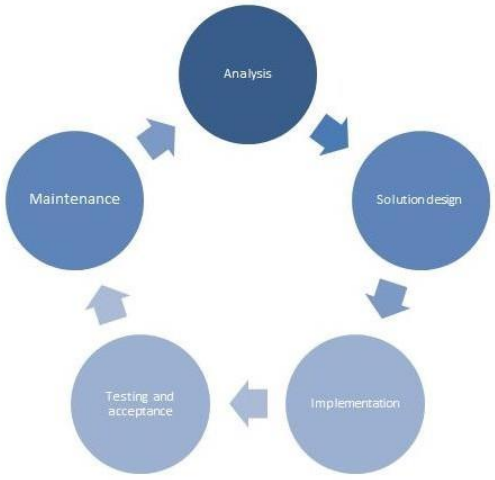
● Business continuance(Maintain essential functions during/after an attack)

- While a security audit will identify weaknesses that ought to be addressed, and an organisation should make every effort to remedy any shortfall, there will always be a risk of a security breach.

- For this reason, an analysis of risks should be carried out and a contingency plan drawn up.

- This contingency plan should cover backup, offsite storage, data recovery procedures, access to immediate hardware replacement, plus insurance that covers replacement, loss of business and all the recovery work.

Business Continuity planning lifecycle



● Backup/restoration of data

- Employees who are responsible for data recovery should also know the procedures to follow.

- The aim should be to plan ahead so that the whole system can be up and running again within a specified time-scale, e.g. 24 hours.

- Then, if the worst case scenario happens, disaster recovery should be as smooth as possible. The contingency plan has to be developed from a full risk analysis, so that every eventuality is taken into consideration

● **Audits**

- An organisation that is unaware of how and where security breaches might occur could soon be faced with a situation that will be costly, and could be very embarrassing.

- Instead, a security audit should be conducted to check what might go wrong, and to plan improvements before a hacker – or some other individual – takes advantage of the situation.

●**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.

+ **Testing procedures - operational impact**

Costs

- If data is lost, costs are incurred in recovering the data.
- If software is corrupted, a copy should be available, but the replacement will take time and incur staff costs.
- Depending on how serious a breach was experienced, there may be a need to consult specialists, and this too will incur extra costs

Loss of business

- A security breach can result in the collapse of an ICT system.
- The time during which normal service is not available is called **downtime**.
- Organizations that rely on an ICT system to take orders will suffer a loss of business during the downtime. Some customers will come back later, but some will not; they will already have taken their business elsewhere.

If a security breach causes data loss, and it proves difficult to recover that data, then the result can be disastrous for an organization.

In the NorthStar Secure Company, we use the following privacy policies:

- **Assess network security risks:**

-Once you've mastered all the data your business has, you'll need to take a review of the risks that your business data may encounter.

-Cases of network security incidents.

-The assessment of cyber-security risks to data can be carried out by NorthStar Secure dedicated cyber security personnel department or thanks to the consultation of cyber security experts. They have enough knowledge and experience to point you out potential risks to business data you may not know.

-Once you have identified the risk of risk for the data you need to protect, you need to take security measures to assess the network of your business.

-This will allow you to know exactly which security risks are and will likely have occurred to the general enterprise network system, and ***the enterprise data*** privacy in particular. Thereby implementing measures to protect the system or implement security solutions in accordance with the model, financial and business requirements.

- **Data Security governance:**

- The risk of security for enterprise data is always regular. Therefore, it is not possible to implement security measures in a short period of time, which requires regular and continuous execution. If possible, every business should have a dedicated leader or individual, with the knowledge of security and *data security of the business* responsible for monitoring the implementation of security measures, processes to ensure data safety.

- This will help minimize cyber security risks for your business, your business data.

- **Configure the system securely:**

- All components within the system (including software and hardware) are configured to meet the privacy policy requirements as well as effective measures to help ensure the safety of data. These standards may be password, account, service or system configuration policies, etc.

- Enforce strong passwords: Weak passwords can be the best friend of the intruder and the secret to breaking the code. Ensuring that all the employees have strong and secure passwords will help protect the company.

- A strong password should be one that is hard to guess, either through human guessing or specialized software. A strong password should be used:

+ At least 9 characters

+ Contains both uppercase and lowercase letters

+ With numeric characters

-Encrypt everything: All confidential information should be encrypted in order to keep the information inaccessible without access to the

- **Control access:**

- The policy on the authorization, access control is indispensable to the network system of a business. These policies help to control access in and out of the system efficiently.

- To do this, you need to ask the user to only be provided the necessary access rights to do their work. The preferred account must be strictly limited to the main systems, the role of the database administrator or locking system. User activity, particularly in relation to sensitive information, that data and the user's account must be kept and managed strictly.

- **Enhances protection, prevention of malicious software.**

- The company should also implement solutions for prevention and protection of data before the risk of malicious code. There are now many solutions to prevent malicious code infection at different levels: individual malicious code prevention solution for users, centralized anti-malware solutions, or anti-malware solutions in gateway etc.

- **Update regular Patches:**

- More and more new methods of attack, so no system can say it's always safe. So, updating the operating system patches and software is an indispensable job.

- Of course, in order to ensure the security of the system at the highest level, the company needs to implement a wide range of security solutions simultaneously combining different security policies.

LO2 Describe IT security solutions

IT security solution evaluation:

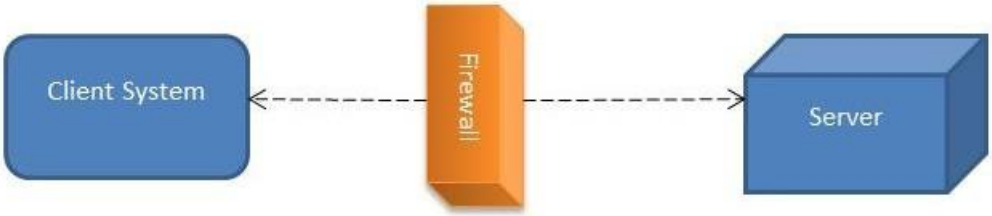
- Network Security infrastructure: evaluation of NAT, DMZ, FWs.
- Network performance: RAID, Main/Standby, Dual LAN, server balancing. Data security: explain asset management, image differential/incremental backups, SAN servers.
- Data centre: replica data centres, virtualisation, secure transport protocol, secure MPLS routing and remote access methods/procedures for third-party access.

Security vulnerability: logs, traces, honeypots, data mining algorithms, vulnerability testing.

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

Introduction

Firewall is a network security system that analyzes and monitors the overall security policy of your data that comes within your network or goes outside the network. This acts to the internal network as a shield. In both hardware and software state we will consider firewall. In general, firewall software is a program installed on our PCs to communicate safely over the network. It will stop threats from other networks coming into our PCs. And it's better than firewall physique. Hardware firewall requires a server to be implemented so it is quite expensive and used in large organization. This device is placed between the router and the internet.



Firewalls

Firewalls protect systems from both external and internal threats. Although firewalls initially became popular in corporate environments, most home networks with a broadband Internet connection now also implement a firewall to protect against Internet-borne threats.
Essentially a firewall is an application, device, system, or group of systems that controls the flow of traffic between two networks.
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:** Most firewalls can be configured to provide some level of content filtering. This can be done for both inbound and outbound content. This is often done when organizations want to control employee access to Internet sites.
- **Signature identification:** A signature is a unique identifier for a particular application. In the antivirus world, a signature is an algorithm that uniquely identifies a specific virus. Firewalls can be configured to detect certain signatures associated with malware or other undesirable applications and block them before they enter the network.
- **Virus scanning services:** As web pages are downloaded, content within the pages can be checked for viruses. This feature is attractive to companies concerned about potential threats from Internet-based sources.
- **Network Address Translation (NAT):** Allows for multiple IP's tohide behind one. More on this later.
- **URL filtering:** By using a variety of methods, the firewall can choose to block certain websites from being accessed by clients within the organization. This blocking allows companies to control what pages can be viewed and by whom.
- **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 approach to bandwidth management is to divide the available bandwidth into sections and then make just a certain section available to a user or system.
- VPN stands for Virtual Private Network which helps in preventing the data breach. It is a type of network which once enabled, keeps the data that is shared over the network encrypted. This network establishes a secure connection between the devices, on which the data is shared.
- A firewall can be defined as a device that is installed to keep the track of the traffic visiting or accessing the data, checking if the user is authorized to access the network or not. As per the rules set or designed, the firewall can allow or block unauthorized users from accessing the network.
- If the configuration of these things is done incorrectly then it can be a major threat to the data breach. Human mistakes can lead to the incorrect configuration, which in turn can result in loss of personal data.

1. Wrong firewall configuration

- VPNs can keep North Star data safe when transmitted over networks, but this is not the only aspect that can protect the data when transmitted, it protects the computers of the employees from data packets. Bad is getting into the system. The way it works, though, is allowing certain products to be accessed and blocking unauthorized files, whether it's because they're dangerous or it's against administrator laws.
- If the corporate firewall is configured poorly, this could lead to the loss of many extremely dangerous but really significant packets while sending, which can cause the user to lose a great deal of private data. For certain projects it is important to lose data in the system which can trigger several different problems. In addition, a properly configured firewall will retain malicious packets while a firewall is not properly configured to allow malicious packages after they think they're good. Furthermore, the wrong configuration of the firewall makes the firewall inactive or very weak so the virus is easy to penetrate and the company's data source is not protected by hackers and hackers.

2. Third-party VPN's and internal leaks

- A VPN is used to enable secure online data transmission, with packets typically having to go through public

domains to be successfully transferred when sending data. Nevertheless, a VPN is a secure connection that consists of two private IP addresses that connect privately to each other, which means that when two entities want to transfer files or data to each other, they can go through a private network rather than risk putting it in the public domain in which it can be accessed and tracked.

- Although this implementation is extremely useful for North Star, there can be huge limitations when using third-party VPNs, because it is a private network, requires providers, and many different companies provide VPNs. However, it can be quite risky to have a VPN this way. This is because while it's a private network, there are many ways in which data can be leaked into this network. Either accidentally or intentionally, data leaks may occur that can expose the entire point of the private network, and may impact North Star, depending on the type of data being leaked, if the data is extremely important. If anything, business could get fatal.

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)

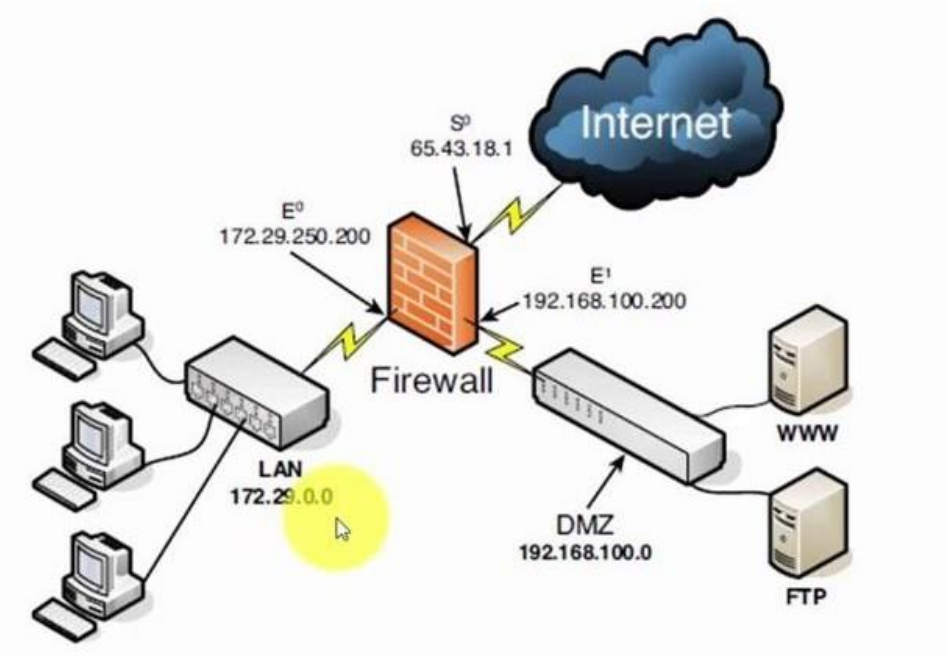
- An important firewall-related concept is the demilitarized zone (DMZ), sometimes called a perimeter network.

- A DMZ is part of a network where you place servers that must be accessible by sources both outside and inside your network.

- Not connected directly to either network and it must always be accessed through the 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.



- By using a DMZ, you can create an additional step that makes it more difficult for an intruder to gain access to the internal network.

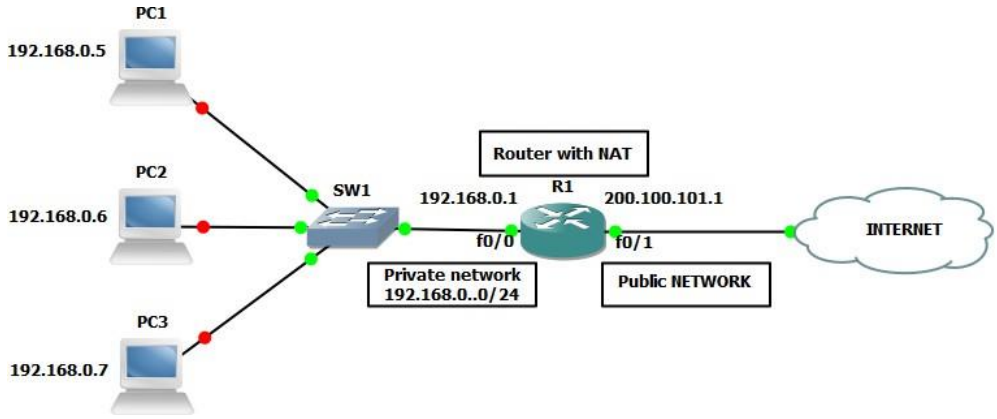
- Using the example opposite an intruder who tried to come in through Interface 1 would have to spoof a request from either the web server or proxy server into Interface 2 before it could be forwarded to the internal network.
- Although it is not impossible for an intruder to gain access to the internal network through a DMZ, it is difficult.
- Usage of Client Puzzle Protocol is ne of approaches to resolve provider / attack aim DDOS attacks. This Client Puzzle Protocol is designed to withstand attacks that reduce the server's ability to initiate service requests by connecting using the Demilitarized Zone approach that is controlled in micro devices. DMZ is the abbreviation of the Demilitarized Zone, also known as the defense zone, as well as the perimeter network used to secure the internal system where all ports are open so that they may be accessed by outsiders. Therefore, if an attack occurs or someone deliberately attacks the server using DMZ, the attacker can only access the host in DMZ, 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)

- 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.

REFERANCES

♦ Sean Convery, Cisco Press, Network Security Architectures, April 19, 2004

♦ Books GCC0701

♦ Jazib Frahim, *Cisco ASA: All-in-One firewall, IPS, and VPN Adaptive Security Appliance*, CCIE No. 5459, Omar Santos, Cisco Press, October 21, 2005