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	Nguyen Quoc Viet	**Student ID**	GCC18157
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 Quoc Viet

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.

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.	

LO1 Assess risks to IT security

IT security risks:

Risks: unauthorised use of a system; unauthorised removal or copying of data or code from a system; damage to or destruction of physical system assets and environment; damage to or destruction of data or code inside or outside the system; naturally occurring risks. Organisational security: business continuance; backup/restoration of data; audits; testing procedures e.g. data, network, systems, operational impact of security breaches, WANs, intranets, wireless access systems.

P1 Identify types of security risks to organisations.

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:

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

- Concealment

1. 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.

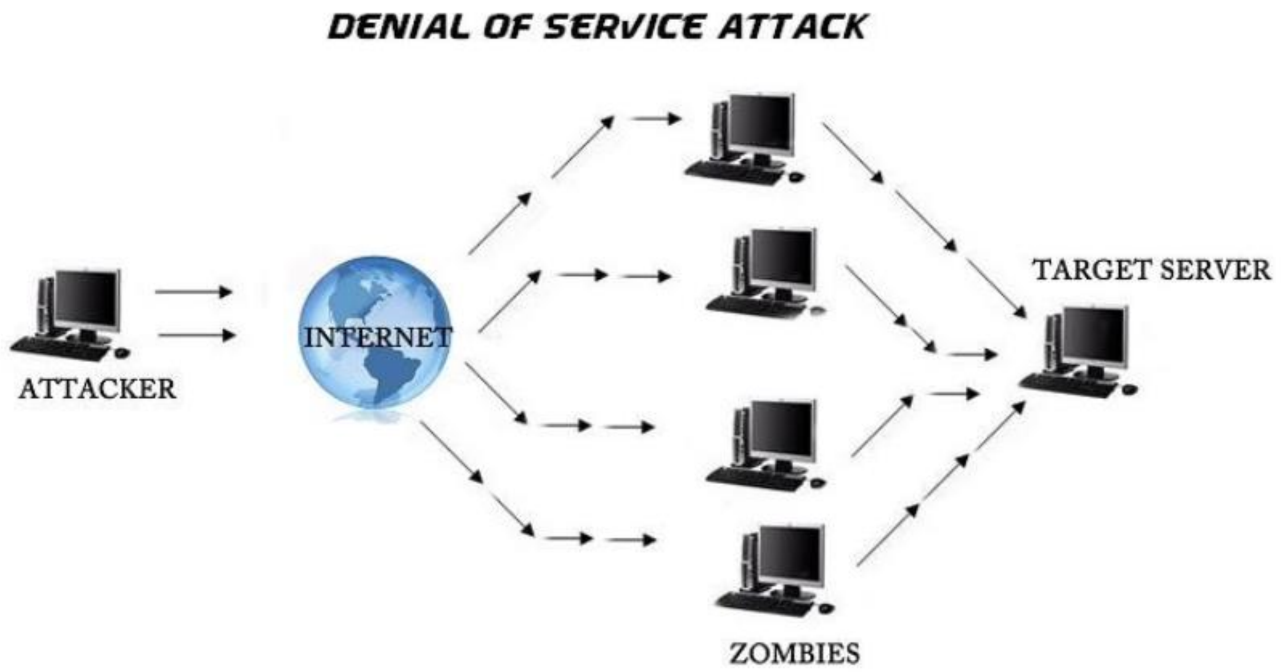
Types of DoS attacks

- 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.

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.

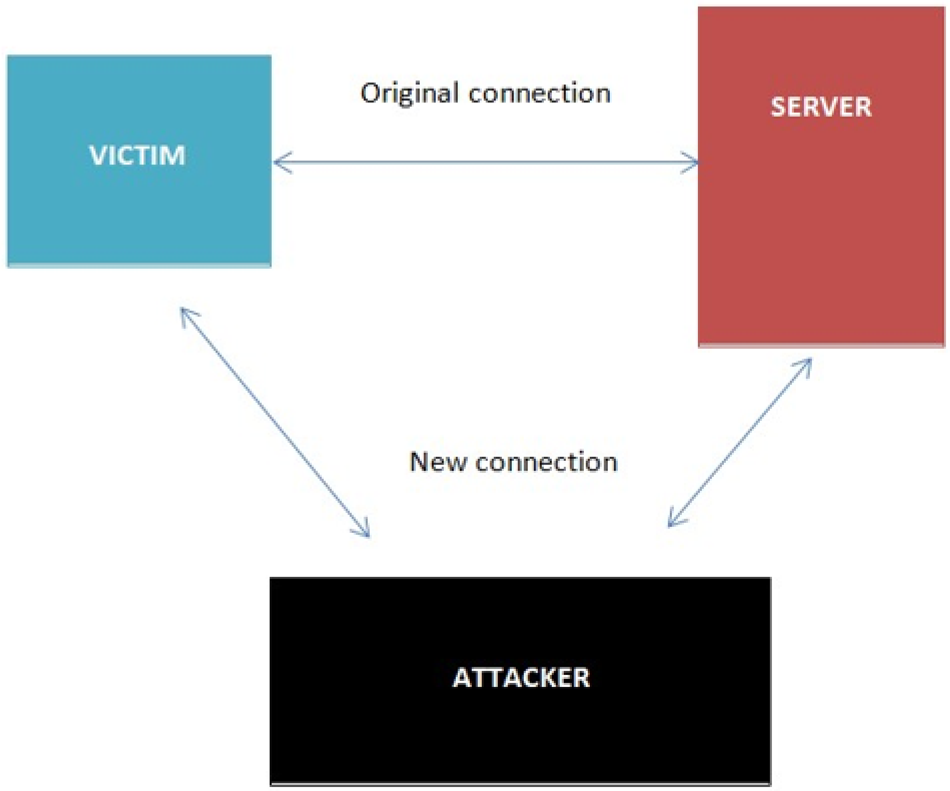
SYN Flood attack



- Interception

  + Man-in-the-Middle attack

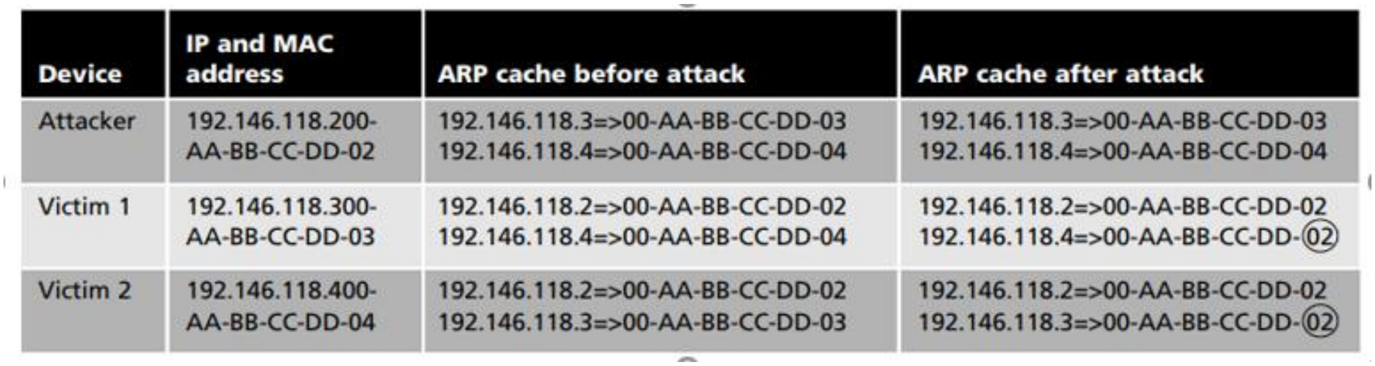
  + Replay attack



- 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



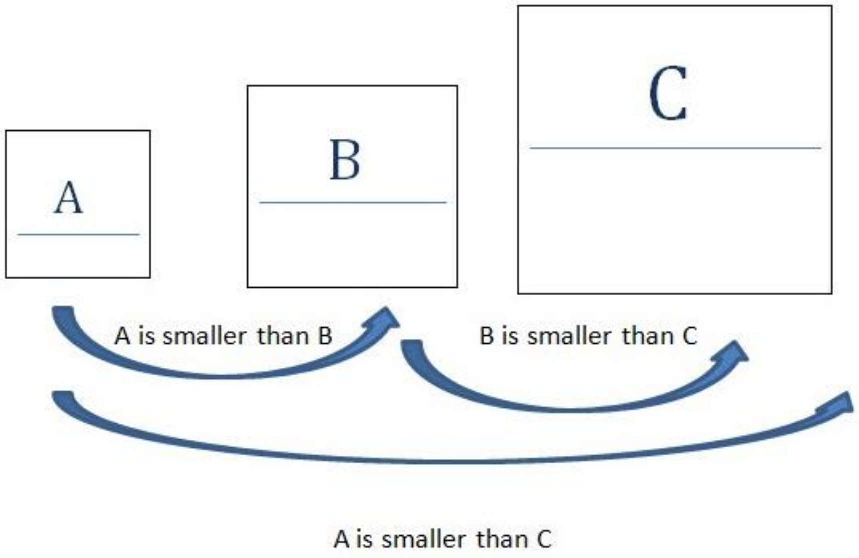
Device	IP and MAC address	ARP cache before attack	ARP cache after attack
Attacker	192.146.118.200- AA-BB-CC-DD-02	192.146.118.3=>00-AA-BB-CC-DD-03 192.146.118.4=>00-AA-BB-CC-DD-04	192.146.118.3=>00-AA-BB-CC-DD-03 192.146.118.4=>00-AA-BB-CC-DD-04
Victim 1	192.146.118.300- AA-BB-CC-DD-03	192.146.118.2=>00-AA-BB-CC-DD-02 192.146.118.4=>00-AA-BB-CC-DD-04	192.146.118.2=>00-AA-BB-CC-DD-02 192.146.118.4=>00-AA-BB-CC-DD-02
Victim 2	192.146.118.400- AA-BB-CC-DD-04	192.146.118.2=>00-AA-BB-CC-DD-02 192.146.118.3=>00-AA-BB-CC-DD-03	192.146.118.2=>00-AA-BB-CC-DD-02 192.146.118.3=>00-AA-BB-CC-DD-02

- DNS Poisoning is a process of substituting a DNS address so that the computer is automatically redirected to another device

Hình netword sline 11

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.



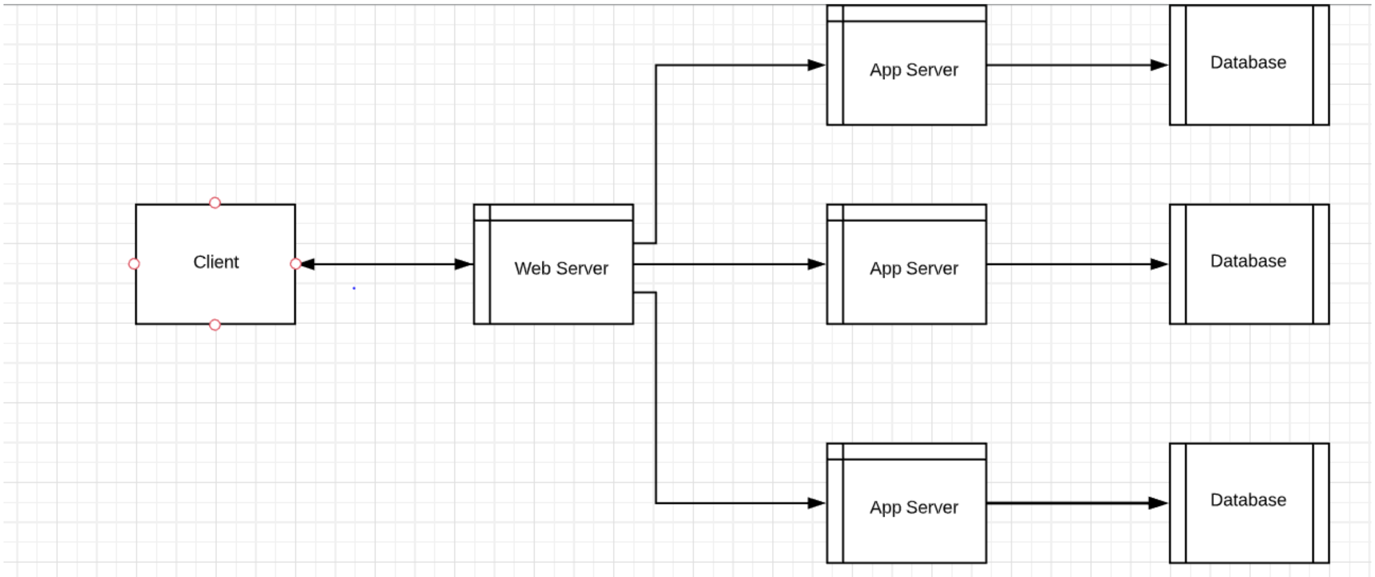
Application Attacks

- 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

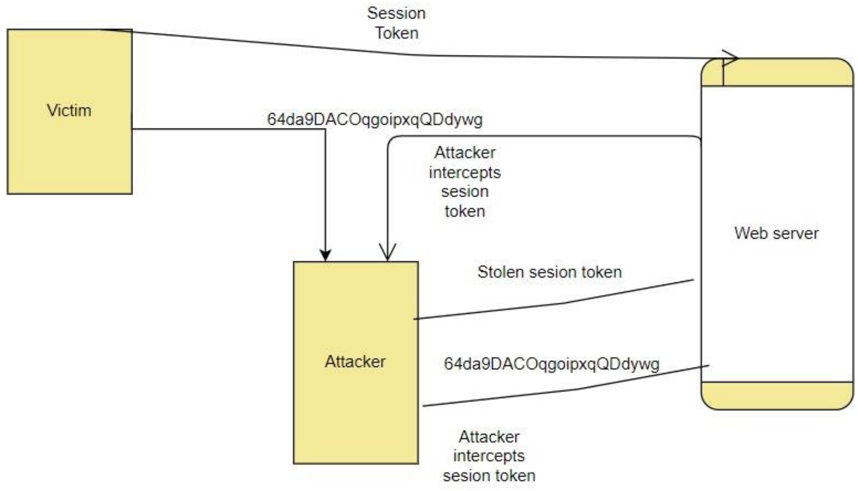
+ Client-side attacks target vulnerabilities in client applications that interact with a compromised server or process malicious data.

+ 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:

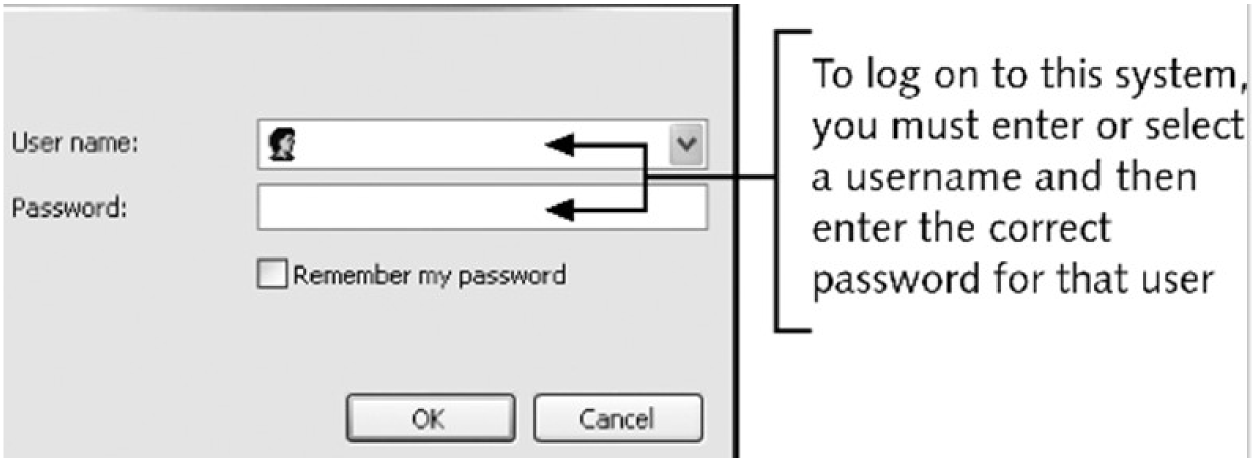
- When passwords are given out
- Who can enter the premises
- What to do when asked questions by another employee that may reveal protected information

- 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



To log on to this system, you must enter or select a username and then enter the correct password for that user

- 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

- Brute force: attacker attempts to create every possible password combination by changing one character at a time, using each newly generated password to access the system
- Dictionary attack: takes each word from a dictionary and encodes it (hashing) in the same way the computer encodes a user's password

- Software exploitation: takes advantage of any weakness in software to bypass security requiring a password

- Buffer overflow: occurs when a computer program attempts to stuff more data into a temporary storage area than it can hold
- 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
  Weak Key
  ● ***Cryptography:***
- Science of transforming information so it is secure while being transmitted or stored
- Does not attempt to hide existence of data; "scrambles" data so it cannot be viewed by unauthorized users

- Encryption: changing the original text to a secret message using cryptography
- Success of cryptography depends on the process used to encrypt and decrypt messages
- Process is based on algorithms
- Algorithm is given a key that it uses to encrypt the message
- Any mathematical key that creates a detectable pattern or structure (weak keys) provides an attacker with valuable information to break the encryption

● ***Mathematical Attacks***

- Cryptanalysis: process of attempting to break an encrypted message

- Mathematical attack: analyzes characters in an encrypted text to discover the keys and decrypt the data

● ***Birthday Attacks***

- Birthday paradox:

+ When you meet someone for the first time, you have a 1 in 365 chance (0.027%) that he has the same birthday as you

+ If you meet 60 people, the probability leaps to over 99% that you will share the same birthday with one of these people

- Birthday attack: attack on a cryptographical system that exploits the mathematics underlying the birthday paradox

● ***Examining Identity Attacks***

+ Category of attacks in which the attacker attempts to assume the identity of a valid user

Man-in-the-Middle Attacks

- Make it seem that two computers are communicating with each other, when actually they are sending and receiving data with a computer between them

- Can be active or passive:

+ Passive attack: attacker captures sensitive data being transmitted and sends it to the original recipient without his presence being detected

+ Active attack: contents of the message are intercepted and altered before being sent on

Replay

- 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

Identifying Denial of Service Attacks

- Denial of service (DoS) attack attempts to make a server or other network device unavailable by flooding it with requests

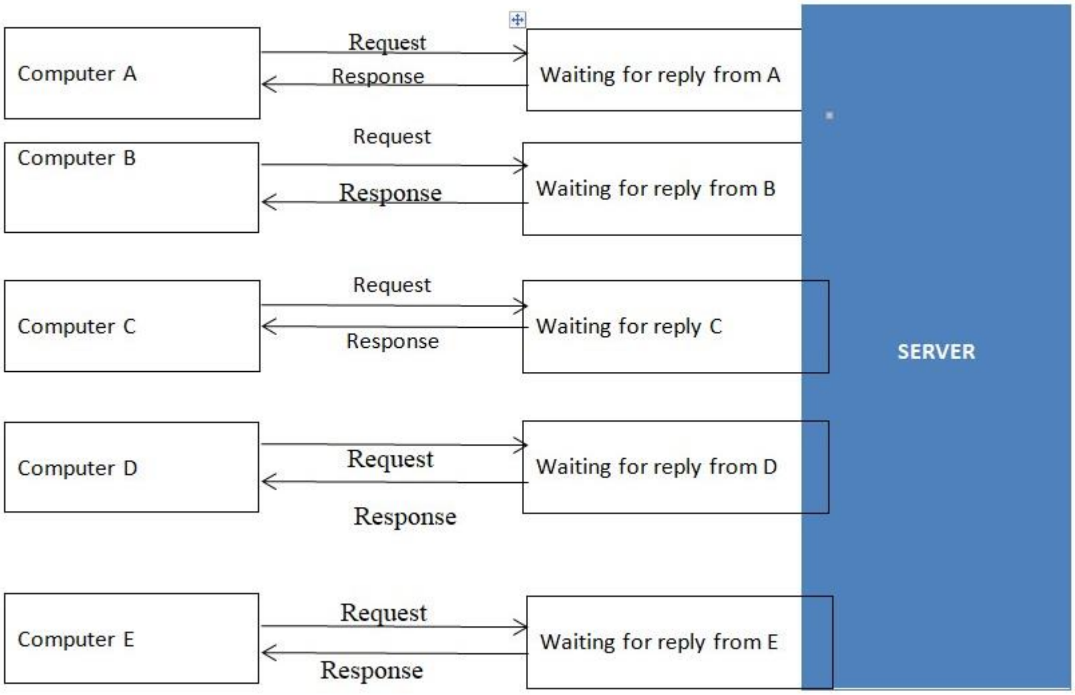
- After a short time, the server runs out of resources and can no longer function

- Known as a SYN attack because it exploits the SYN/ACK “handshake”

- Another DoS attack tricks computers into responding to a false request

- An attacker can send a request to all computers on the network making it appear a server is asking for a response

- Each computer then responds to the server, overwhelming it, and causing the server to crash or be unavailable to legitimate users



- Distributed denial-of-service (DDoS) attack:

+ Instead of using one computer, a DDoS may use hundreds or thousands of computers

+ DDoS works in stages

Assessing risks to IT security IT security risks

● “The wonderful thing about the Internet is that you’re connected to everyone else… The terrible thing about the Internet is that your connected to everyone else…”

Dr. Vinton Cerf - co-designer of the TCP/IP protocols and the architecture of the Internet.

● Access to the information and services the Internet provides, comes risk.

● Risk of information loss, or corruption, of data theft and worse. These risks have to be mitigated with security solutions.

IT Threats

- A threat is an event that could exploit a vulnerability (an attack waiting to happen) and cause a negative impact on the network.

- Threats in the digital world typically mimic threats in the physical world.

- Theft, vandalism, eavesdropping are all threats that have moved from the real world into cyberspace, typically via the Internet.

- There are some significant differences however, in terms of the distance these attacks can be carried out, the automation involved, and the propagation(Spreading) of attack techniques

IT security risks

- unauthorised use of a system

- unauthorised removal or copying of data or code from a system

- damage to or destruction of physical system assets and environment

- damage to or destruction of data or code inside or outside the system naturally occurring risks

Unauthorised use of a system

- Software should be used only by those authorised to do so.

- Someone – a hacker – may access confidential data.

- The hacker may read the data or copy it, but do no damage to it.

- However, simply reading data can also cause damage to an organisation, even if that data is not deleted or altered.

- Obtaining personal details of an individual can lead to identity theft.

- If you become the victim of identity theft, you might have difficulty obtaining credit for a credit card, loan or mortgage until the confusion is resolved.

Unauthorised removal or copying of data or code from a system

- Someone may pass data on to another person who is not authorised to read it; this is called data theft.

- Data related to new products or business plans of an organisation is sensitive.

- If this data fell into the wrong hands, e.g. a competitor, the organisation would lose any competitive edge that secrecy would have given them.

- The worst-case scenario is for the data to be removed altogether. Imagine the chaos if all the personnel records of an organisation – the contact details of all employees, their pay records and details of promotions, pensions, etc. – were removed

Damage to or destruction of physical system assets and environment

- Someone may damage the hardware in the ICT system. A hard disk holds a lot of data.

- If the disk was sabotaged, the data would become inaccessible. The hardware in an ICT system can be worth many hundreds of thousands of pounds.

- If any of it is damaged or stolen then it will take time to replace it.

- The cost of replacement is usually covered by insurance, so the main problem is the time delay in installing replacement equipment.

- This delay can result in lost business and, as a consequence, the organisation may lose money. Consequential loss may not be covered by insurance, so this is a 'real' loss. Damage to data or code Data or software should only be altered or deleted by someone who is authorised to do so. A hacker may damage – i.e. amend or delete – the data or software.

Damage to or destruction of data or code inside or outside the system

- Data or software should only be altered or deleted by someone who is authorised to do so.

- A hacker may damage – i.e. amend or delete – the data or software.

- Data and software may also be damaged by virus attack.

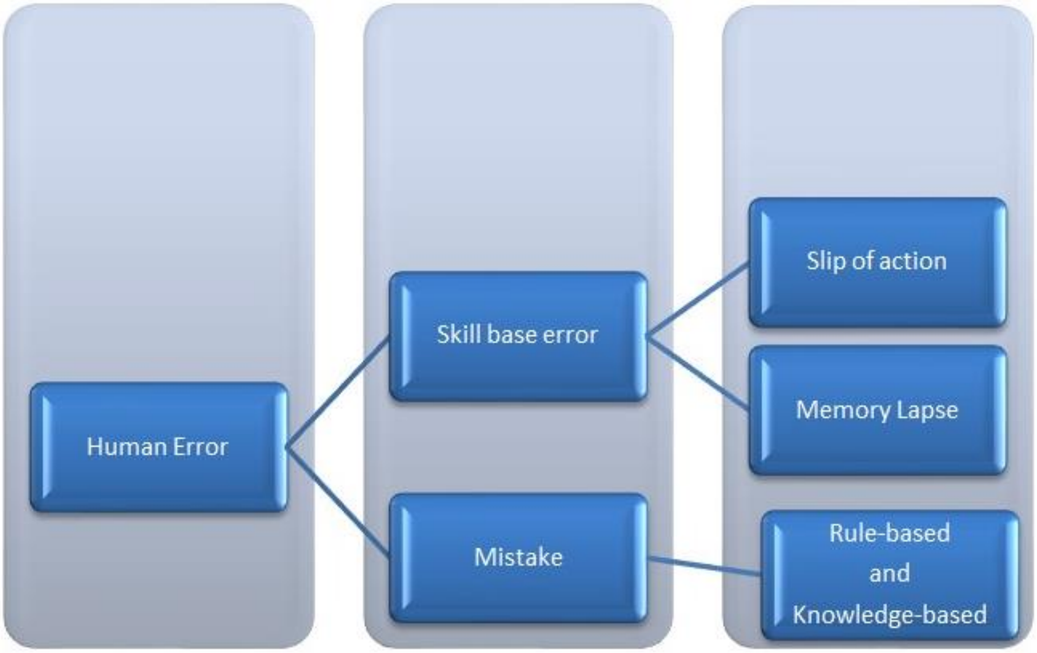
Naturally occurring risks.

- Human actions

E.g. Human error, employee that disregards policy

- Systems issues

E.g. Out of date or incorrectly configured/installed anti virus and firewall, confusion over backup policy could result in accidental overwrite, poor group policy configuration, incorrect user access levels.



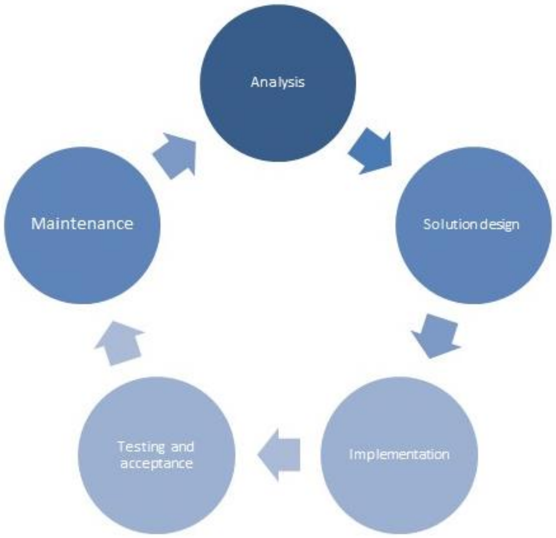
P2 Describe organizational security procedures.

● ***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 e.g. 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.

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.

Firewalls

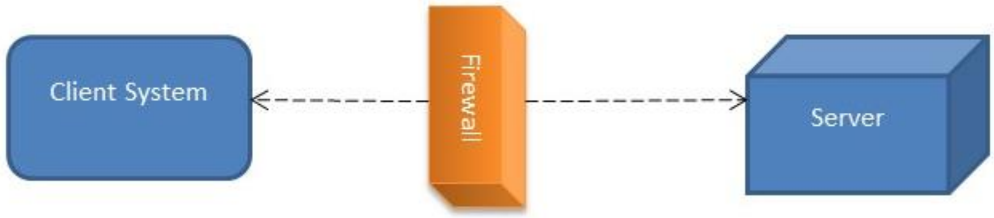
● Firewalls protect systems from both external and internal threats. Although firewalls initially became popular in corporate environments, most home networks with a broadband Internet connection now also implement a firewall to protect against Internet-borne threats.

● 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.

● How it manages the flow and what it does with certain types of traffic depends on its configuration.



● 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 to hide 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.

The potential impact on security when configuring the wrong third-party VPN policy.

VPNS are also known as virtual private networks, allowing users to set up virtual private networks with a different network on the Internet. VPNS can be used to access sites that restrict geo-location access, protecting your browsing activity from "curiosity" on public Wi-Fi networks by setting up virtual private networks for you.

- Several organizations or people at home can use a variety of methods to safeguard their devices, many of which are common practices, e.g. data encryption, firewall, etc. One of the approaches citizens can use is to set up a VPN (Virtual Private Network).
- VPNs are used to facilitate secure data sharing, normally when sending data, packets would have to pass across public domains in order to be successfully transmitted. Nevertheless, a VPN is a secure link that requires two IP addresses communicating to each other anonymously, which ensures that if the two networks want to transfer files or data to each other, they can go through a private network rather than risk putting it on a public domain in which it can be accessed and monitored.

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

Demilitarized zone

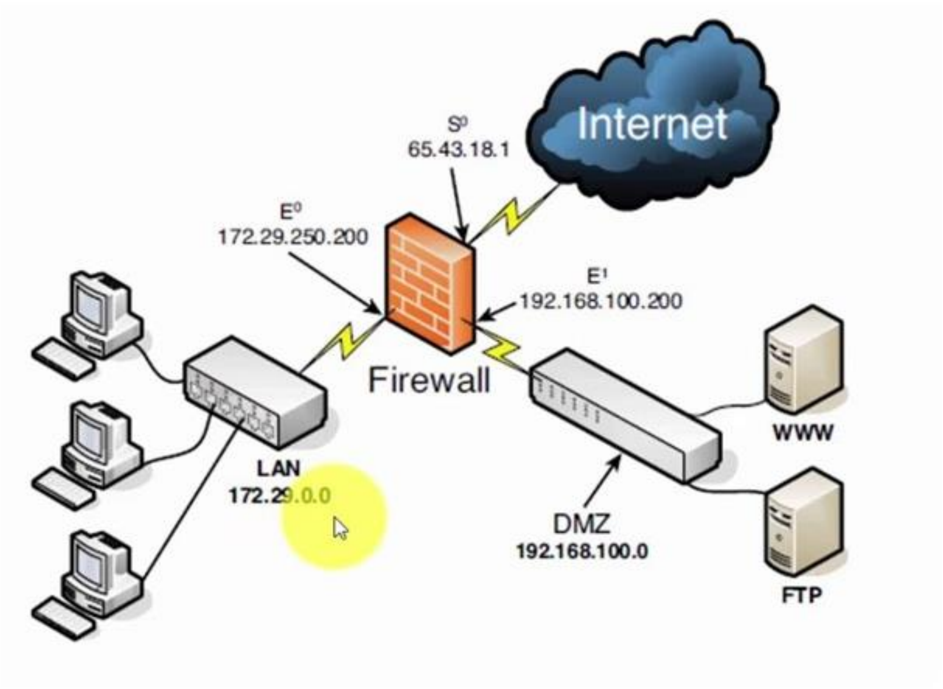
- An important firewall-related concept is the demilitarized zone (DMZ), sometimes called a perimeter network.

- 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.

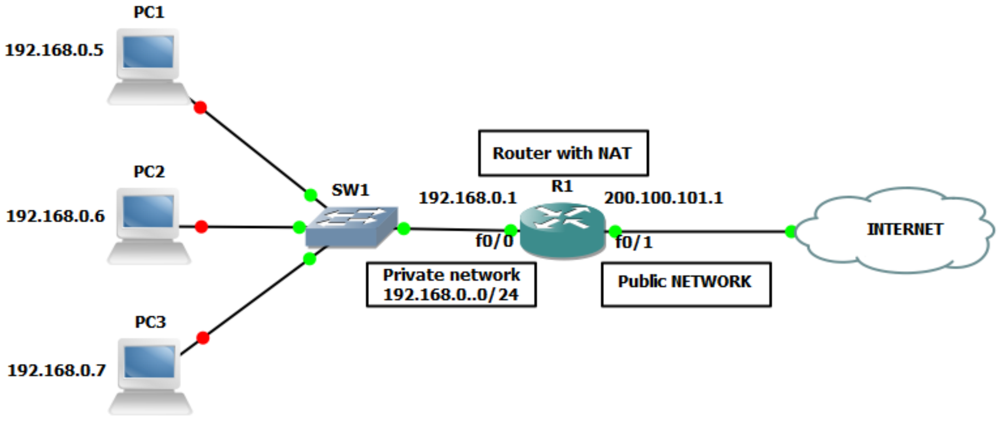
- Although it is not impossible for an intruder to gain access to the internal network through a DMZ, it is difficult

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.



Network performance:

RAID Level	Description	Advantage	Disadvantage	Required Disks
RAID 0	Disk striping	Increased read and write performance. RAID 0 can be implemented with two or more disks.	Does not offer any tolerance.	Two or more
RAID 1	Disk mirroring	Provides fault Can also be used with separate disk controllers, reducing the single point of failure. This is called disk duplexing.	RAID 1 has 50% overhead and suffers from poor write performance.	Tow
RAID 5	Disk striping with distributed parity	Can recover a single disk failure. Increased read performance over a poor write single disk. Disks can be added to the array	May slow down the network during regeneration time, and performance may suffer.	Min of three

		to increase storage capacity		
RAID 10	Striping with mirrored volumes	Increased performance with striping. Offers mirrored fault tolerance	High overhead, as with mirroring	Four

Main/Standby

- Stndby servers are a fault-tolerance measure in which a second server is identically configured to the first one.

- The second server can be stored remotely or locally and set up in a failover configuration.

- In a failover configuration, the secondary server connects to the primary and is ready to take over the server functions at a moment's notice. If the secondary server detects that the primary has failed, it automatically cuts in.

- Network users will not notice the transition, because little or no disruption in data availability occurs.

- The primary(Main) server communicates with the secondary server by issuing special notification notices called heartbeats.

- If the secondary server stops receiving the heartbeat messages, it assumes that the primary(main) has died and therefore assumes the primary server configuration

Dual LAN (AKA NIC Teaming or link aggregation or trunking):

- Combining two or more physical Ethernet links into a single logical link.

- If two 1Gb/s ports were aggregated, you would get a total aggregated(group) bandwidth of 2Gb/s.

-If one physical part of the logical link fails, traffic will failover to the remaining active links.

- Consider that if you're transferring a file from one PC to another over a 2Gb aggregated link, you'll find that the total maximum transfer rate will top out at 1Gb/s.

- Start two file transfers, however, and you'll see the benefits of aggregated bandwidth.

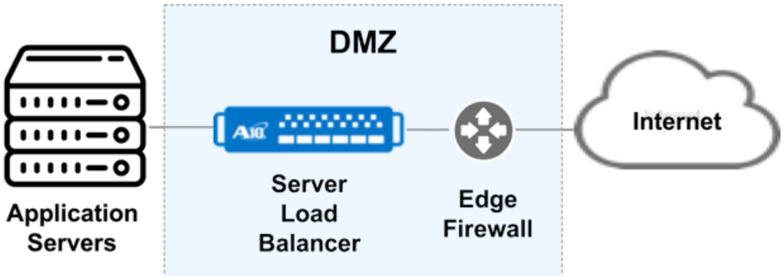
- In simple terms, link aggregation increases the number of lanes on a highway but it doesn't increase the speed limit.

Server balancing(Load balancing):

- Network servers are the workhorses of the network. They are relied on to hold and distribute data, maintain backups, secure network communications, and more.

- The load of servers is often a lot for a single server to maintain. This is where load balancing comes into play.

- Load balancing is a technique in which the workload is distributed between several servers. This feature can take networks to the next level; it increases network performance, reliability, and availability.



- Increases redundancy and therefore data availability.
- Increases performance by distributing the workload.
- Implemented through Server Clustering

Data security: Asset management:

- As part of your network risk management the assets used should be considered and assessed by performance, configuration, and behaviour.

- Plan and organise devices:

  - What functions do they perform? How and where are they used? Who is responsible for them? Expected lifespan of each device including the refresh cycles, lease date or end of life warranty.

-Monitor your devices:

  - Consider performance, health, and risk exposure, and make informed decisions about changes to your environment.
  - Consider then how you identify the scope of unexpected changes in your environment and how can you address them at-scale when they occur? What’s your action plan if a device is lost or stolen? How will you discover that it’s gone?

- ***Device Retirement:***
  - Ensure that the devices important to you are monitored and protected.
  - Establish a process for your devices’ end of life.
  - Device’s should be collected, secured, sanitized, and removed from your environment when the time comes.
  - How will you manage device returns when employees leave or change roles?
  - How do you manage timely and secure device end-of-life?

– How can you confirm that are they safely decommissioned from your organisation?

Data security: (Storage area network) SAN servers

- A centralised subnetwork of storage devices, usually found on high-speed networks and shared by all servers on a network.

- An SAN makes a network of storage devices accessible to potentially multiple servers/devices.

- Often combined with “Fibre Channel” technology that defines over 5 gigabit-per-second data transfer over fiber-optic cable.

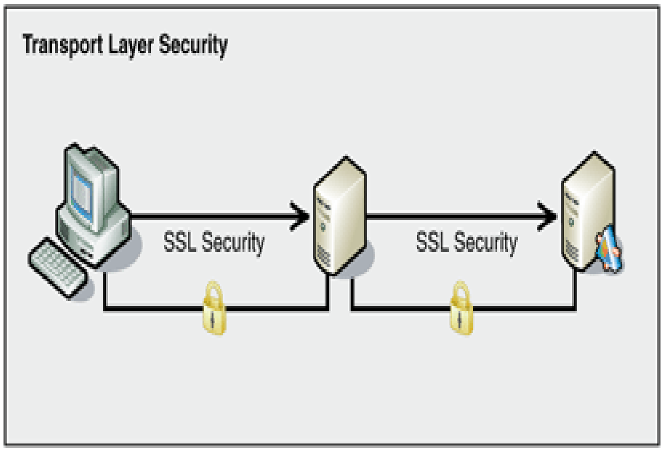
- Advantages include Storage Virtualization, High-Speed Disk Technologies(Fibre Channel), Centralized Backup, Dynamic Failover Protection(Provides continuous network operation, even if a server fails or goes offline for maintenance, which enables built-in redundancy and automatic traffic rerouting.)

https://www.techrepublic.com/blog/data-center/diy-san-windows-server-2012-storage-spaces-and-iscsi-target

Data centres

- ■ For larger businesses and networks data centres can be created. A data centre centralizes an organisation's IT operations and equipment, as well as where it stores, manages, and disseminates its data.
- ■ Replica data centres can be created to synchronise and maintain mirror like functionality so if one goes down the network keeps running.
- ■ Data centres can use virtualisation so lots of physical servers can be converted into 1 virtual server

Secure Transport Protocol:



- ■ Cryptographic protocols designed to provide communications security over a network and in data centres.
- ■ TLS(Transport Layer Security) replaces SSL(Secure Sockets Layer) as the current most secure option.
- ■ Websites can use TLS to secure all communications between their servers and web browsers.
- ■ TLS used in the context of web servers is known as HTTPS(Hyper Text Transfer Protocol Secure) (that is HTTP over TLS).

Secure MPLS (Multiprotocol Label Switching) routing:

- ■ MPLS is a switching technology used frequently with data centres to make packet forwarding happen.

- A technology designed to speed up network traffic flow by moving away from the use of traditional routing tables.
- Instead of routing tables, MPLS uses short labels to direct packets and forward them through the network.
- Because labels refer to paths and not endpoints, packets destined for the same endpoint can use a variety of LSPs(label-switched path) to get there:
    - The packet follows the channel to its destination, thereby eliminating the need to check the packet for forwarding information at each hop and reducing the need to check routing tables.
- The multiprotocol part of the name refers to the fact that MPLS works with a variety of protocols, including Frame Relay, ATM, and IP.

Remote access methods/procedures for third-party access:

- Remote management allows centrally located personnel and applications to monitor, manage, and respond to globally distributed networks and systems from a single location.
- With these tools, IT managers can respond to problems quickly and perform corrective actions from anywhere in the world at anytime.
- This addresses staffing issues and ensures effective systems management.
- Remote access methods should be able to:
    - Remotely configure, monitor, and manage equipment
    - Access equipment over the network (in-band), through a single modem connection (out-of-band), or via the Internet (IP-based management)
    - Connect equipment that lacks a network interface
    - Secure access to mission-critical equipment

Security vulnerability: Logs

- A system's security log contains events related to security incidents such as successful and unsuccessful logon attempts and failed resource access.
- Security logs can be customized, meaning that administrators can fine-tune exactly what they want to monitor.
- Some administrators choose to track nearly every security event on the system. Although this might be prudent, it can often create huge log files that take up too much space
- Each event in a security log contains additional information to make it easy to get the details on the event:

    Date: The exact date the security event occurred.

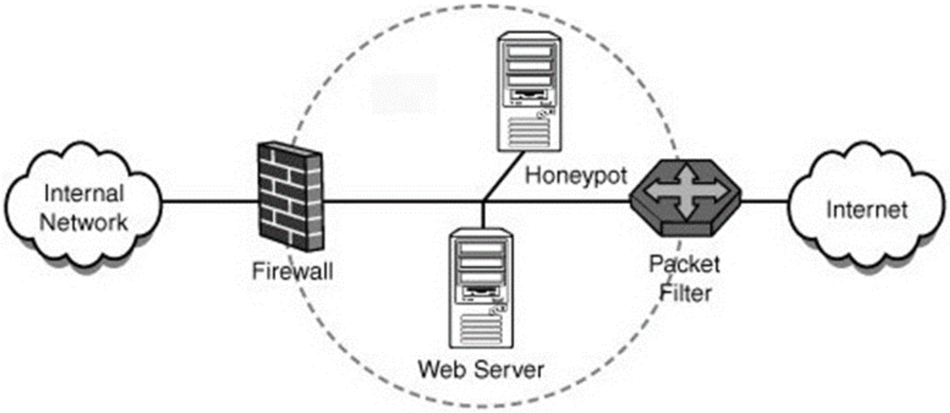
Time: The time the event occurred. . User: The name of the user account that was tracked during the event. .

Computer: The name of the computer used when the event occurred. .

Event ID: The Event ID tells you what event has occurred. You can use this ID to obtain additional information about the particular event.

Honeypots

- Honeypots are a rather clever approach to network security but perhaps a bit expensive.
- It’s a a system set up as a decoy to attract and deflect attacks from hackers.
- The server decoy appears to have everything a regular server does—OS, applications, and network services.
- The attacker thinks he is accessing a real network server, but he is in a network trap.

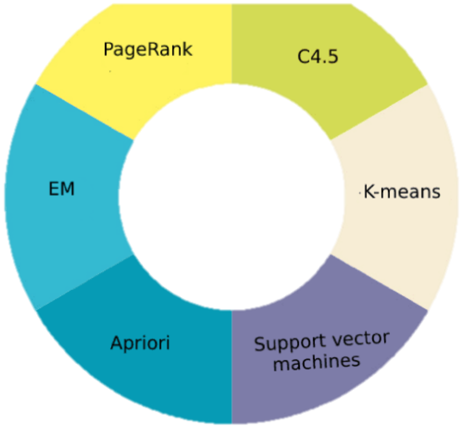


- The honeypot has two key purposes. It can give administrators valuable information on the types of attacks being carried out.
- In turn, the honeypot can secure the real production servers according to what it learns. Also, the honeypot deflects attention from working servers, allowing them to function without being attacked.
- A honeypot can .
  - Deflect the attention of attackers from production servers.
  - Deter attackers if they suspect their actions may be monitored with a honeypot.
  - Allow administrators to learn from the attacks to protect the real servers.
  - Identify the source of attacks, whether from inside the network or outside.

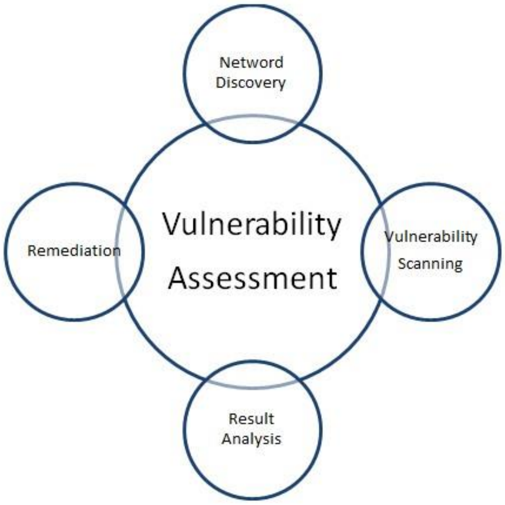
Data mining algorithms

- Data mining techniques can then be used to analyse the data collected by the honeypot and to detect important patterns and attacks.
- Using data mining algorithms we can learn statistical patterns of logs adaptively and to detect intrusions as statistical anomalies relative to the learned patterns.
- We can then use this information to detect weaknesses in our networks and IT security.

Mining Algorithms Examples



Vulnerability testing



- A software program that contains a database of known vulnerabilities against your system to identify weaknesses.
- It is highly recommended that you obtain such a vulnerability scanner and run it on your network to check for any known security holes.
- It is always preferable for you to find them on your own network before someone outside the organisation does by running such a tool against you.
- The vulnerability scanner may be a port scanner (such as NMAP: http://nmap.org/), a network enumerator, a web application, or even a worm.
- In all cases it runs tests on its target against a gamut of known vulnerabilities