INFORMATION TECHNOLOGY SUPPORT SERVICE

Level II

Learning Guide #29

Unit of Competence: -	**Care for Network and Computer Hardware**
Module Title: -	**Caring for Network and Computer Hardware**
LG Code:	EIS ITS2 M07 1019 LO3-LG29
TTLM Code:	**EIS ITS2 TTLM 1019 V1**

LO3:- Monitor threats to the network

Instruction Sheet	Learning Guide #29

This learning guide is developed to provide you the necessary information regarding the Following content coverage and topics –

- Using third-party software to evaluate and report on system security
- Identifying security threats
- Ensuring carry-out spot checks and other security strategies
- Investigating and implementing inbuilt or additional encryption facilities
- Preparing and presenting an audit report and recommendation
- Obtaining approval for recommended changes

This guide will also assist you to attain the learning outcome stated in the cover page.

Specifically, upon completion of this Learning Guide, you will be able to –

- Use third-party software or utilities to evaluate and report on system security
- Review logs and audit reports to identify security threats
- Carry-out spot checks and other security strategies to ensure that procedures are being followed
- Investigate and implement inbuilt or additional encryption facilities
- Prepare and present an audit report and recommendations to appropriate person
- Obtain approval for recommended changes to be made

Learning Instructions:

1. Read the specific objectives of this Learning Guide.
2. Follow the instructions described below 3 to 4.
3. Read the information written in the information “Sheet 1, Sheet 2, Sheet 3, Sheet 4, Sheet 5 and Sheet 6” **in page 1, 4, 10,14, 20,and 23** respectively.
4. Accomplish the “Self-check 1, Self-check t 2, Self-check 3 , Self-check 4, Self-check 5 and Self-check 6” **in page 3, 9, 13, 19,22,and 25** respectively

Information Sheet – 1	Using third-party software to evaluate and report on system security

1.1. Introduction

Computer network : is a system in which computers are connected to share information and resources. The connection can be done as peer-to-peer or client/server or LAN or WAN.

The term network monitoring describes the use of a system that constantly monitors a computer network for slow or failing components and that notifies the network administrator (via email, pager or other alarms) in case of outages. It is a subset of the functions involved in network management.

Network security consists of the **requirements** and **policies** adopted by the network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network-accessible resources.

1.2. Network threats

Network threats are intentional activities to cause damage, misusing resources, or other aggressive action on network system.

Some of Network threats

- Unauthorized accessing
- Misusing of resources
- Modification of network resources
- Denial of services

There are different ways to monitor threats to the network. Some of them are: -

- By using software Utilities
- By using security mechanism
- By Using encryption facilities

1.3. Identifying security threats

Explain why security is important

Computer and network security help to keep data and equipment functioning and provide access only to appropriate people. Everyone in an organization should give high priority to security because everyone can be affected by a lapse in security.

Theft, loss, network intrusion, and physical damage are some of the ways a network or computer can be harmed. Damage or loss of equipment can mean a loss of productivity. Repairing and replacing equipment can cost the company time and money. Unauthorized use of a network can expose confidential information and reduce network resources.

1.4. Describe security threats

To successfully protect computers and the network, a technician must understand both types of threats to computer security:

- Physical – Events or attacks that steal, damage, or destroy equipment, such as servers, switches, and wiring
- Data – Events or attacks that remove, corrupt, deny access, allow access, or steal information

Threats to security can come from the inside or outside of an organization, and the level of potential damage can vary greatly:

- Internal – Employees have access to data, equipment, and the network
    - Malicious threats are when an employee intends to cause damage.
    - Accidental threats are when the user damages data or equipment unintentionally.
- External – Users outside of an organization that do not have authorized access to the network or resources
    - Unstructured – Attackers use available resources, such as passwords or scripts, to gain access and run programs designed to vandalize
    - Structured – Attackers use code to access operating systems and software

Physical loss or damage to equipment can be expensive, and data loss can be detrimental to your business and reputation. Threats against data are constantly changing as attackers find new ways to gain entry and commit their crimes.

Self Check 1	Choose Test

Name:_____ Date:_____

Instruction: Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

I. choose the best answer from the following question

_____1. _____is a system in which computers are connected to share information and resources

A/Network threat B/Network Security C/Computer Network D/Protocol

_____2.Which one is not Network threats are intentional activities to cause damage, misusing resources, or other aggressive action on network system.

A/Unauthorized accessing B/ Misusing of resources C/Denial of services D/All

Note: **Satisfactory rating – 1 points Unsatisfactory - below 1 points**

You can ask you teacher for the copy of the correct answers.

Answer Sheet

Score = _____

Rating: _____

Information Sheet – 2	Identifying security threats

2.1. Introduction

Computer Security: The prevention and protection of (computer) assets from unauthorized access, use, alteration, degradation, destruction, and other threats.

Network security involves the authorization of access to data in a network which is controlled by the network administrator and the organization policies. Users choose or an ID and password or authenticating information that allows them access to information and program within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done.

Privacy: The right of the individual to be protected against interruption into his personal life or affairs, or those of his family, by direct physical means or by publication of information.

Security/Privacy Threat: Any person, act, or object that poses a danger to computer security/privacy.

2.2. Computer Security and Privacy/Vulnerabilities

- Physical vulnerabilities (Eg. Buildings)
- Natural vulnerabilities (Eg. Earthquake)
- Hardware and Software vulnerabilities (Eg. Failures)
- Media vulnerabilities (Eg. Disks can be stolen)
- Communication vulnerabilities (Eg. Wires can be tapped)
- Human vulnerabilities (Eg. Insiders)

With an increasing amount of people getting connected to networks, the security threats that cause massive harm are increasing also.

Network security is a major part of a network that needs to be maintained because information is being passed between computers etc and is very vulnerable to attack

Over the past five years people that manage network security have seen a massive increase of hackers and criminals creating malicious threats that have been pumped into networks across the world.

2.2.1. Viruses and Worms:

- A Virus is a “program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes.
- Viruses can cause a huge amount of damage to computers.
- An example of a virus would be if you opened an email and a malicious piece of code was downloaded onto your computer causing your computer to freeze.
- In relation to a network, if a virus is downloaded then all the computers in the network would be affected because the virus would make copies of itself and spread itself across networks.
- A worm is similar to a virus but a worm can run itself whereas a virus needs a host program to run.

Solution: Install a security suite, such as Kasper sky Total Protection that protects the computer against threats such as viruses and worms.

2.2.2. Trojan Horses:

- A Trojan horse is “a program in which malicious or harmful code is contained inside it appears that harmless programming or data in such a way that it can get control and do its chosen form of damage, such as corrupted the file allocation table on your hard disk.
- In a network if a Trojan horse is installed on a computer and tampers with the file allocation table it could cause a massive amount of damage to all computers of that network.
- Solution: Security suites, such as Norton Internet Security, will prevent you from downloading Trojan Horses.

2.2.3. SPAM:

- SPAM is “flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it.
- SPAM may not be the biggest risk to a network because even though it may get maddening and plentiful it still doesn’t destroy any physical elements of the network.
- Solution: SPAM filters are an effective way to stop SPAM, these filters come with most of the e-mail providers on line. Also you can buy a variety of SPAM filters that work effectively.

2.2.4. Phishing:

- Phishing is “an e-mail fraud method in which the performer sends out legitimate-looking emails in an attempt to gather personal and financial information from recipients.
- phishing is one of the worst security threats over a network because a lot of people that use computers linked up to a network are unpaid and would be very vulnerable to giving out information that could cause situations such as theft of money or identity theft.
- Solution: Similar to SPAM use Phishing filters to filter out this unwanted mail and to prevent threat.

2.2.5. Packet Sniffers:

- A packet sniffer is a device or program that allows listen on traffic traveling between networked computers. The packet sniffer will capture data that is addressed to other machines, saving it for later analysis.
- In a network a packet sniffer can filter out personal information and this can lead to areas such as identity theft so this is a major security threat to a network.
- Solution: “When strong encryption is used, all packets are unreadable to any but the destination address, making packet sniffers useless. So one solution is to obtain strong encryption.

2.2.6. Maliciously Coded Websites:

- Some websites across the net contain code that is malicious.
- Malicious code is “Programming code that is capable of causing harm to availability, integrity of code or data, or confidentiality in a computer system.
- Solution: Using a security suite, such as AVG, can detect infected sites and try to prevent the user from entering the site.

2.2.7. Password Attacks:

- Password attacks are attacks by hackers that are able to determine passwords or find passwords to different protected electronic areas.
- Many systems on a network are password protected and hence it would be easy for a hacker to hack into the systems and steal data.
- This may be the easiest way to obtain private information because you are able to get software online that obtains the password for you.
- Solution: At present there is no software that prevents password attacks.

2.2.8. Hardware Loss and Residual Data Fragments:

- Hardware loss and residual data fragments are a growing worry for companies, governments etc.
- An example this is if a number of laptops get stolen from a bank that have client details on them, this would enable the thief's to get personal information from clients and maybe steal the clients identities.
- This is a growing concern and as of present the only solution is to keep data and hardware under strict surveillance.

2.2.9. Shared Computers:

- Shared computers are always a threat.
- Shared computers involve sharing a computer with one or more people.
- The following are a series of tips to follow when sharing computers: "Do not check the "Remember my ID on this computer" box
- Never leave a computer unattended while signed-in … Always sign out completely …Clear the browsers cache … Keep an eye out for "shoulder surfers" … Avoid confidential transactions … Be wary of spy ware … Never save passwords … Change your password often.

2.2.10. Zombie Computers and Botnets:

- A zombie computer or "drone" is a computer that has been secretly compromised by hacking tools which allow a third party to control the computer and its resources remotely.
- A hacker could hack into a computer and control the computer and obtain data.
- Solution: Antivirus software can help prevent zombie computers.

Solution: Network Intrusion Prevention (NIP) systems can help prevent botnets

2.3. Explain web security

Web security is important because so many people visit the World Wide Web every day. Some of the features that make the web useful and entertaining can also make it harmful to a computer.
Tools that are used to make web pages more powerful and versatile are: -

- **ActiveX** – Technology created by Microsoft to control interactivity on web pages. If ActiveX is on a page, an applet or small program has to be downloaded to gain access to the full functionality.
- **Java** – Programming language that allows applets to run within a web browser. Examples of applets include a calculator or a counter.

- **JavaScript** – Programming language developed to interact with HTML source code to allow interactive websites. Examples include a rotating banner or a popup window.

Attackers may use any of these tools to install a program on a computer. To prevent against these attacks, most browsers have settings that force the computer user to authorize the downloading or use of ActiveX, Java, or JavaScript.

2.4. Define adware, spyware, and grayware

Adware is a software program that displays advertising on your computer. Adware is usually distributed with downloaded software. Most often, adware is displayed in a popup window. Adware popup windows are sometimes difficult to control and will open new windows faster than users can close them.

Grayware or malware is a file or program other then a virus that is potentially harmful. Many grayware attacks are phishing attacks that try to persuade the reader to unknowingly provide attackers with access to personal information. As you fill out an online form, the data is sent to the attacker. Grayware can be removed using spyware and adware removal tools.

Spyware, a type of grayware, is similar to adware. It is distributed without any user intervention or knowledge. Once installed, the spyware monitors activity on the computer. The spyware then sends this information to the organization responsible for launching the spyware.

2.5. Explain Denial of Service

Denial of service (DoS) is a form of attack that prevents users from accessing normal services, such as e-mail and a web server, because the system is busy responding to abnormally large amounts of requests. DoS works by sending enough requests for a system resource that the requested service is overloaded and ceases to operate.

Common DoS attacks include the following:

- Ping of death – A series of repeated, larger than normal pings that crash the receiving computer
- E-mail bomb – A large quantity of bulk e-mail that overwhelms the e-mail server preventing users from accessing it

Distributed DoS (DDoS) is another form of attack that uses many infected computers, called zombies, to launch an attack. With DDoS, the intent is to obstruct or overwhelm access to the targeted server. Zombie computers located at different geographical locations make it difficult to trace the origin of the attack.

Self Check 2	Choose Test

Name:_____ Date:_____

Instruction: Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

I. choose the best answer from the following question

_____1. _____ the prevention and protection of (computer) assets from unauthorized access,

use, alteration, degradation, destruction, and other threats.

A/Network Security B/Computer Security C/Network threat D/Protocol

_____2._____ is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes.

A/Packet Sniffers B/Phishing C/SPAM D/Viruses

_____3._____ an e-mail fraud method in which the performer sends out legitimate-looking emails in an attempt to gather personal and financial information from recipients.

A/Packet Sniffers B/Phishing C/SPAM D/Viruses

_____4._____ is a device or program that allows listen on traffic traveling between networked computers.

A/Viruses B/Packet Sniffers C/Phishing D/SPAM

_____5._____ is flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it.

A/Viruses B/Packet Sniffers C/SPAM D/Phishing

Note: **Satisfactory rating – 2 points** **Unsatisfactory - below 2 points**

You can ask you teacher for the copy of the correct answers.

Answer Sheet

Score = _____

Rating: _____

Information Sheet – 3	Ensuring carry-out spot checks and other security strategies

3.1. Physical monitoring threats

Use the following Physical threats controlling :-

- Fence
- Guards
- Gate locks
- Lock devices(network device and computers)

- **Authentication (Password):** Password prevention is also very vital. One of the best mechanisms is to ascertain that crasher can't even gain access to the coded password.
- **Organizational policies**

Physical security: Physical Security

Your organization should be aware how physically secure every aspect of its network is because if an intruder gets physical access, they can get your data. Be sure the organization properly secures locations and consider the following:

- **Servers** - Contain your data and information about how to access that data.
- **Workstations** - Man contain some sensitive data and can be used to attack other computers.
- **Routers, switches, bridges, hubs** and any other network equipment may be used as an access point to your network.
- **Network wiring and media** and where they pass through may be used to access your network or place a wireless access point to your network.
- **External media** which may be used between organizational sites or to other sites the organization does business with.
- Locations of staff that may have information that a hostile party can use.
- Some employees may take data home or may take laptops home or use laptops on the internet from home then bring them to work. Any information on these laptops should be considered to be at risk and these laptops should be secure according to proper policy when connected externally on the network.

3.2. Threats to Security

- Internal threats - employees of the organization.
- Deliberate data damage - "just for fun" or with more shady intent, some people might delight in corrupting data or deleting it completely.
- Industrial intelligence - the process of a person retrieving data from a server for a purpose.
- Physical equipment theft - If an important piece of equipment is stolen (for example, the server or a backup tape), the intruder will have access to your data.
- A firewall is a 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.

3.3. Protect your password.

Never share your password with anyone, not even a relative or colleague. If another person has your password, they can, for all computer purposes, be you. This extends far beyond simply reading your email.

It's very important to use different passwords for different systems. This limits the damage a malicious person can do should a password fall into the wrong hands.

Following are some measures that you can take in order to minimize the risks associated with malicious human threats:

- ***Data Storage in Safe Locations:*** Keep your data in safe and secure locations that have limited access to others.
- ***Virus and Spyware Protection:*** You must open an e-mail attachment or install any software from a Web site with caution. The most reliable way is to install antivirus and anti-spyware software from a reputable vendor.
- ***Human Errors:*** Many times, damage to a computer is due to unintentional human error. For example, you may accidentally delete an important file, causing the computer to malfunction.
- ***Hardware Damage:*** Computer components, being delicate, run the risk of getting damaged due to carelessness..
- ***Protecting hardware from accidental and environmental damages:*** You can take various measures to avoid any unintentional damage to your computer. Keep the computer in an area that is dust-free, free from vibration, and out of the way of possible impact, should be well-ventilated to prevent any damage due to heat.
- ***Backing up Data:*** Regularly back up important computer data. Creating multiple copies of data provides protection against loss of data due to accidental erasure or destruction of data.

Identify security procedures

A security plan should be used to determine what will be done in a critical situation. Security plan policies should be constantly updated to reflect the latest threats to a network. A security plan with clear security procedures is the basis for a technician to follow. Security plans should be reviewed on a yearly basis.

There are different security strategies

- ✓ Privacy
- ✓ Authentication
- ✓ Authorization and integrity

Privacy is the ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively. The boundaries and content of what is considered private differ among cultures and individuals, but share basic common themes.

Authentication is the act of confirming the truth of an attribute of a datum or entity.

Authorization is the process of giving someone permission to do or have something. In multi-user computer systems, a system administrator defines for the system which users are allowed access to the system and what privileges of use (such as access to which file directories, hours of access, amount of allocated storage space, and so forth).

Integrity is a concept of consistency of actions, values, methods, measures, principles, expectations, and outcomes. In ethics, integrity is regarded as the honesty and truthfulness or accuracy of one's actions.

Self Check 3	Write Test

Name:_____ Date:_____

Instruction: Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

I. Write the answer briefly

1. Write method Physical threats controlling ?

2. Write some measures that you can take in order to minimize the risks associated with malicious human threats?

Note: **Satisfactory rating – 1 points** **Unsatisfactory - below 1 points**

You can ask you teacher for the copy of the correct answers.

Answer Sheet

Score = _____

Rating: _____

Information Sheet – 4	Investigating and implementing inbuilt or additional encryption facilities

4.1. Data Encryption

Encrypting data uses codes and ciphers. Traffic between resources and computers on the network can be protected from attackers monitoring or recording transactions by implementing encryption. It may not be possible to decipher captured data in time to make any use of it.

Virtual Private Network (VPN) uses encryption to protect data. A VPN connection allows a remote user to safely access resources as if their computer is physically attached to the local network.

4.2. Port Protection

Every communication using TCP/IP is associated with a port number. HTTPS, for instance, uses port 443 by default. A firewall is a way of protecting a computer from intrusion through the ports. The user can control the type of data sent to a computer by selecting which ports will be open and which will be secured. Data being transported on a network is called traffic.

4.3. Data Backups

Data backup procedures should be included in a security plan. Data can be lost or damaged in circumstances such as theft, equipment failure, or a disaster such as a fire or flood. Backing up data is one of the most effective ways of protecting against data loss. Here are some considerations for data backups:

- **Frequency of backups** – Backups can take a long time. Sometimes it is easier to make a full backup monthly or weekly, and then do frequent partial backups of any data that has changed since the last full backup. However, spreading the backups over many recordings increases the amount of time needed to restore the data.
- **Storage of backups** – Backups should be transported to an approved offsite storage location for extra security. The current backup media is transported to the offsite location on a daily, weekly, or monthly rotation as required by the local organization.
- **Security of backups** – Backups can be protected with passwords. These passwords would have to be entered before the data on the backup media could be restored.

4.4. Implementing encryption Facilities

One of the most effective ways to eliminate data loss or theft is to encrypt the data as it travels across the network. However, not all data protection solutions are created equal. While most solutions offer standard AES 256-bit encryption, there are other attributes that must be considered:

Some of encryption facilities are: -

- **Public Key Infrastructure (PKI)** is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.[1] In cryptography, a PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA). The user identity must be unique within each CA domain. The binding is established through the registration and issuance process, which, depending on the level of assurance the binding has, may be carried out by software at a CA, or under human supervision. The PKI role that assures this binding is called the Registration Authority (RA). The RA ensures that the public key is bound to the individual to which it is assigned in a way that ensures non-repudiation.
- **Pretty Good Privacy (PGP)** is a popular program used to encrypt and decrypt e-mail over the Internet. It can also be used to send an encrypted digital signature that lets the receiver verify the sender's identity and know that the message was not changed en route. Available both as freeware and in a low-cost commercial version, PGP is the most widely used privacy-ensuring program by individuals and is also used by many corporations.

4.5. Symmetric and Asymmetric ciphers

- In a **symmetric cipher**, both parties must use the same key for encryption and decryption. This means that the encryption key must be shared between the two parties before any messages can be decrypted. Symmetric systems are also known as shared secret systems or private key systems.Symmetric ciphers are significantly faster than asymmetric ciphers, but the requirements for key exchange make them difficult to use.
- In an **asymmetric cipher**, the encryption key and the decryption keys are separate. In an asymmetric system, each person has two keys. One key, the public key, is shared publicly. The second key, the private key, should never be shared with anyone.

When you send a message using asymmetric cryptography, you encrypt the message using the recipients' public key. The recipient then decrypts the message using his private key. That is why the system is called asymmetric.

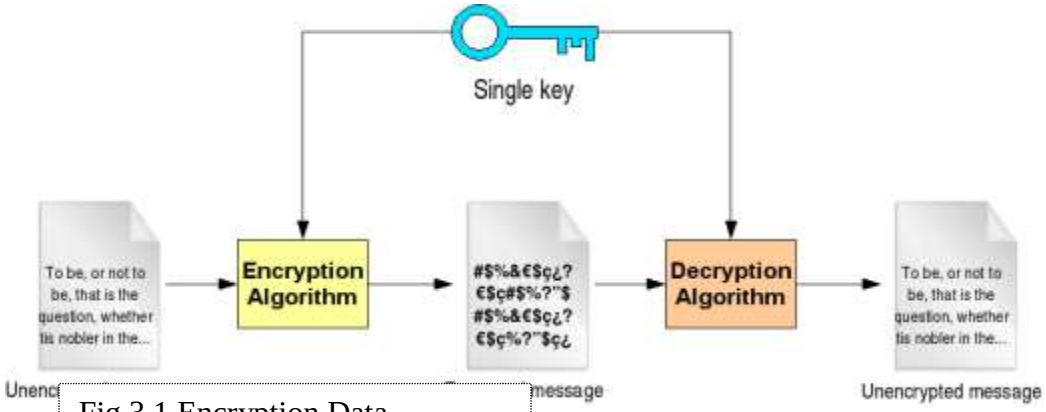

Fig 3.1 Encryption Data

Because asymmetric ciphers tend to be significantly more computationally intensive, they are usually used in combination with symmetric ciphers to implement effect public key cryptography. The asymmetric cipher is used to encrypt a session key and the encrypted session key is then used to encrypt the actual message.

Symmetric ciphers are the oldest and most used cryptographic ciphers. In a symmetric cipher, the key that deciphers the cipher text is the same as (or can be easily derived from) the key enciphers the clear text. This key is often referred to as the secret key. The most widely used symmetric ciphers are DES and AES.

Unlike a symmetric cipher, an asymmetric cipher uses two keys: one key that is kept secret and known to only one person (the private key) and another key that is public and available to everyone (the public key). The two keys are mathematically interrelated, but it's impossible to derive one key from the other. Well-known asymmetric ciphers are the Diffie-Hellman algorithm, RSA, and DSA.

What are the advantages and disadvantages of using an asymmetric cipher instead of a symmetric cipher?

- An important advantage of asymmetric ciphers over symmetric ciphers is that no secret channel is necessary for the exchange of the public key. The receiver needs only to be assured of the authenticity of the public key. Symmetric ciphers

require a secret channel to send the secret key—generated at one side of the communication channel—to the other side.

- Asymmetric ciphers also create lesser key-management problems than symmetric ciphers. Only 2n keys are needed for n entities to communicate securely with one another. In a system based on symmetric ciphers, you would need n(n ? 1)/2 secret keys. In a 5000-employee organization, for example, the companywide deployment of a symmetric crypto-based security solution would require more than 12 million keys. The deployment of an asymmetric solution would require only 10,000 keys.
- A disadvantage of asymmetric ciphers over symmetric ciphers is that they tend to be about "1000 times slower." By that, I mean that it can take about 1000 times more CPU time to process an asymmetric encryption or decryption than a symmetric encryption or decryption.
- Another disadvantage is that symmetric ciphers can be cracked through a "brute-force" attack, in which all possible keys are attempted until the right key is found.

Because of these characteristics, asymmetric ciphers are typically used for data authentication (through digital signatures), for the distribution of a symmetric bulk encryption key (aka a digital envelope), for non-repudiation services, and for key agreement. Symmetric ciphers are used for bulk encryption.

4.6. **Sniffers** monitor network data. A sniffer can be a self-contained software program or a hardware device with the appropriate software or firmware programming. Sniffers usually act as network probes or "snoops." They examine network traffic, making a copy of the data without redirecting or altering it. Some sniffers work only with TCP/IP packets, but the more sophisticated tools can work with many other protocols and at lower levels including Ethernet frames.

4.7. **Secure Shell** (**SSH**) is a network protocol for secure data communication, remote shell services or command execution and other secure network services between two networked computers that it connects via a secure channel over an insecure network: a server and a client (running SSH server and SSH client programs, respectively).[1] The protocol specification distinguishes two major versions that are referred to as SSH-1 and SSH-2.

4.8. **Deslogin** is a remote login program which may be used safely across insecure networks. With deslogin, you may log into a secure remote host from a secure local

host without worry about your login password or session information being made visible across the network. Deslogin is a simple stand-alone client and server, which may be used on machines which don't have more sophisticated security packages such as SPX or Kerberos. No centralized key distribution package is required. Unlike unix Login programs, authentication relies upon arbitrarily long pass phrases rather than eight-character user passwords.

4.9. **PKZIP** is an archiving tool originally written by Phil Katz and marketed by his company PKWARE, Inc. The common "PK" prefix used in both PKZIP and PKWARE stands for "Phil Katz".

Secure Sockets Layer (SSL) a protocol for encrypting information over the Internet

4.10. A **digital signature** or **digital signature scheme** is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

Self Check 4	Write Test

Name:_____ Date:_____

Instruction: Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

I. Write the answer briefly

1. Define Data Encryption?

2. Write types Data Backups?

3. Define Secure Shell (SSH)?

4. What the difference between Symmetric and Asymmetric ciphers?

Note: **Satisfactory rating – 2 points** **Unsatisfactory - below 2 points**

You can ask you teacher for the copy of the correct answers.

Answer Sheet

Score = _____

Rating: _____

Information Sheet – 5	Preparing and presenting an audit report and recommendation

5.1. Introduction to Multiple layer of security

There are multiple layers of security in a network, including physical, wireless, and data. Each layer is subject to security attacks. The technician needs to understand how to implement security procedures to protect equipment and data.

Fig 3.2 Multiple Layer

Explain what is required in a basic local security policy

Though local security policies may vary between organizations, there are questions all organizations should ask:

- What assets require protection?
- What are the possible threats?
- What to do in the event of a security breach?

A security policy should describe how a company addresses security issues:

- Define a process for handling network security incidents
- Define a process to audit existing network security
- Define a general security framework for implementing network security
- Define behaviors that are allowed
- Define behaviors that are prohibited

- Describe what to log and how to store the logs: Event Viewer, system log files, or security log files
- Define network access to resources through account permissions
- Define authentication technologies to access data: usernames, passwords, biometrics, smart cards

Explain the tasks required to protect physical equipment

Physical security is as important as data security. When a computer is taken, the data is also stolen.

There are several methods of physically protecting computer equipment,

- Control access to facilities
- Use cable locks with equipment
- Keep telecommunication rooms locked
- Fit equipment with security screws
- Use security cages around equipment
- Label and install sensors, such as Radio Frequency Identification (RFID) tags, on equipment

For access to facilities, there are several means of protection:

- Card keys that store user data, including level of access
- Berg connecters for connecting to a floppy drive
- Biometric sensors that identify physical characteristics of the user, such as fingerprints or retinas
- Posted security guard
- Sensors, such as RFID tags, to monitor equipment

Self Check 5	Write Test

Name:_____ Date:_____

Instruction: Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

I. Write the answer briefly

1. Define security policy should describe a company addresses security issues?

2. Write methods of physically protecting computer equipment?

Note: **Satisfactory rating – 1 points** **Unsatisfactory - below 1 points**

You can ask you teacher for the copy of the correct answers.

Answer Sheet

Score = _____

Rating: _____

Information Sheet – 6	Obtaining approval for recommended changes

6.1. Describe ways to protect data

The value of physical equipment is often far less than the value of the data it contains. The loss of sensitive data to a company's competitors or to criminals may be costly. Such losses may result in a lack of confidence in the company and the dismissal of computer technicians in charge of computer security. To protect data, there are several methods of security protection that can be implemented.

6.2. Password Protection

Password protection can prevent unauthorized access to content. Attackers are able to gain access to unprotected computer data. All computers should be password protected. Two levels of password protection are recommended:

- BIOS – Prevents BIOS settings from being changed without the appropriate password
- Login – Prevents unauthorized access to the network

Network logins provide a means of logging activity on the network and either preventing or allowing access to resources. This makes it possible to determine what resources are being accessed. Usually, the system administrator defines a naming convention for the usernames when creating network logins. A common example of a username is the first initial of the person's first name and then the entire last name. You should keep the username naming convention simple so that people do not have a hard time remembering it.

When assigning passwords, the level of password control should match the level of protection required. A good security policy should be strictly enforced and include, but not be limited to, the following rules:

- Passwords should expire after a specific period of time.
- Passwords should contain a mixture of letters and numbers so that they cannot easily be broken.
- Password standards should prevent users from writing down passwords and leaving them unprotected from public view.

- Rules about password expiration and lockout should be defined. Lockout rules apply when an unsuccessful attempt has been made to access the system or when a specific change has been detected in the system configuration.

To simplify the process of administrating security, it is common to assign users to groups, and then to assign groups to resources. This allows the access capability of users on a network to be changed easily by assigning or removing the user from various groups. This is useful when setting up temporary accounts for visiting workers or consultants, giving you the ability to limit access to resources.

6.3. Explain social engineering

A ***social engineer*** is a person who is able to gain access to equipment or a network by tricking people into providing the necessary access information. Often, the social engineer gains the confidence of an employee and convinces the employee to divulge username and password information.

Here are some basic precautions to help protect against social engineering:

- Never give out your password
- Always ask for the ID of unknown persons
- Restrict access of unexpected visitors
- Escort all visitors
- Never post your password in your work area
- Lock your computer when you leave your desk
- Do not let anyone follow you through a door that requires an access card

6.4. Explain TCP/IP attacks

TCP/IP is the protocol suite that is used to control all of the communications on the Internet. Unfortunately, TCP/IP can also make a network vulnerable to attackers.

Self Check 6	Write Test

Name:_____ Date:_____

Instruction: Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

I. Write the answer briefly

1. List two levels of password protection are recommended?

2. Write some basic precautions to help protect against social engineering?

Note: **Satisfactory rating – 1 points** **Unsatisfactory - below 1 points**

You can ask you teacher for the copy of the correct answers.

Answer Sheet

Score = _____

Rating: _____

List of Reference Materials

1. **BOOKS**
2. **https://training.gov.au/Training/Details/ICTSAS506**
3. **web1.keira-h.schools.nsw.edu.au/faculties/IT**