Definition

*Security is a state of being secure and free from danger or harm

*Intellectual property is the ownership of ideas and control over the tangible or virtual representation of those ideas

*Threat : a potential risk to an asset's loss of value

*Attack: an intentional or unintentional act that can damage or otherwise compromise information and the systems that support it.

*Exploit: A technique used to compromise a system

*Vulnerability: A potential weakness in an asset or its defensive control system(s)

*Threat agent –The specific instance or a component of a threat.

*confidentiality: An attribute of information that describes how data is protected from disclosure or exposure to unauthorized individuals or systems.

*Authentication : The access control mechanism that requires the validation and verification of an unauthenticated entity's purported identity.

2) Risk management concepts :

*Risk assessment- A determination of the extent to which an organization's information assets are exposed to risk

* Risk control- The application of controls that reduce the risks to an organization's information assets to an acceptable level.

* Risk identification- The recognition, enumeration, and documentation of risks to an organization's information assets.

3) List of malware:

*spyware – any technology that aids in gathering information about people or organizations whiteout their knowledge.

*Trojan horse – a malware that hides its true nature and reveals its designed behaviour only activated .

* worm -a type of malware that capable of activation and replication without being attached to an existing program

*virus -a type of malware that is attached to other executable programs whereby when activated ,it can replicate and propagates itself to multiple systems also spreads by multiple communications vectors.

*Back-door- a malware payload that provides access to a system by bypassing normal access control .

4)Business continuity plan(BCP) processes:

Business continuity planning prepares an organization to restablish or relocate critical business operations during a disaster that affects operations at the primary site.

i) Developing Continuity Programs- Once the incident response and disaster recovery plans are in place, the organization needs to consider finding temporary facilities to support its continued viability in a disaster. When a disaster strikes, these functions are the first to be reestablished at the alternate site.

ii) Site and Data Contingency Strategies

iii) crisis management- An organization's set of planning and preparation efforts for dealing with potential human injury, emotional trauma, or loss of life as a result of a disaster.

iv) The Consolidated Contingency Plan-an organization can build a single document that combines all aspects of the contingency policy and plan.

v) Law Enforcement Involvement

5) mapping port number with their protocol

20= File Transfer [Default Data] (FTP)

21 =File Transfer [Control] (FTP)

23= Telnet 25 Simple Mail Transfer Protocol (SMTP)

53= Domain Name System (DNS) 80 Hypertext Transfer Protocol (HTTP)

110= Post Office Protocol version 3 (POP3)

161 =Simple Network Management Protocol (SNMP)

6)

i)firewall-inspect all incoming and outgoing traffic. They monitor and log traffic to provide a record of successful and unsuccessful attacks and also have alarms that alert you to suspected breaches.

ii)VPN-A private, secure network operated over a public and insecure network. A VPN keeps the contents of the network messages hidden from observers who may have access to public traffic by Encapsulation ,Encryption , Authentication of incoming and outgoing data

iii)Kerberos- An authentication system that uses symmetric key encryption to validate an individual user's access to various network resources by keeping a database containing the private keys of clients and servers that are in the authentication domain it supervises entails Authentication server (AS), Key Distribution Center (KDC) and Kerberos ticket granting service (TGS),

iv) RADIUS- A computer connection system that centralizes the management of user authentication by placing the responsibility for authenticating each user on a central authentication server also

entails verification of the authenticated individual or system is allowed to make a given type of connection.

7) Distinguish between IDS and IPS:

IDS:

- Detection and monitoring tools
- These tools do not take actions on their own
- Requires a human or another system to look at the results.

IPS:

-Is a control system

-The control system accepts and reject a packet based on the ruleset

-Requires that the database gets regularly updated with new threat data