UNIT-I

1) What are the four important functions, the information security performs in an organization?
Information security performs four important functions for an organization:

- Protects the organization's ability to function
- Enables the safe operation of applications implemented on the organization's IT systems
- Protects the data the organization collects and uses
- Safeguards the technology assets in use at the organization

2) What are threats?

- A threat is an object, person, or other entity that represents a constant danger to an asset
- Management must be informed of the various kinds of threats facing the organization
- By examining each threat category in turn, management effectively protects its information through policy, education and training, and technology controls

(3) What are the different categories of threat? Give Examples.

(4) What are different acts of Human error or failure?
Includes acts done without malicious intent. It is Caused by:

- Inexperience
- Improper training
- Incorrect assumptions
- Other circumstances

(5) How human error can be prevented?

Much human error or failure can be prevented with training and ongoing awareness activities, but also with controls, ranging from simple procedures like asking users to type a critical command twice, to more complex procedures ,such as the verification of the commands by a second party (Eg key recovery actions in PKI systems)

(6) What is Intellectual property?

Intellectual property is "the ownership of ideas and control over the tangible or virtual representation of those ideas" . Many organizations are in business to create intellectual property

- trade secrets
- copyrights
- trademarks
- patents

7) How Intellectual property can be protected?
Enforcement of copyright has been attempted with technical security mechanisms, such as using digital watermarks and embedded code. The most common reminder of the individual's obligation to fair and responsible use is the license agreement window that usually pops up during the installation of a new software.

8) What is a deliberate act of espionage or trespass?

- Broad category of activities that breach confidentiality

        - Unauthorized accessing of information
        - Competitive intelligence vs. espionage
        - Shoulder surfing can occur any place a person is accessing confidential information
    - Controls implemented to mark the boundaries of an organization's virtual territory giving notice to trespassers that they are encroaching on the organization's cyberspace
    - Hackers uses skill, guile, or fraud to steal the property of someone else

9) Who are Hackers? What are the two hacker levels?

The classic perpetrator of deliberate acts of espionage or trespass is the hacker. Hackers are "people who use and create computer software [to] gain access to information illegally". Generally two skill levels among hackers:

- Expert hacker
- unskilled hacker(Script kiddies)

10) What is information extortion?

Information extortion is an attacker or formerly trusted insider stealing information from a computer system and demanding compensation for its return or non-use
Extortion found in credit card number theft(A Russian hacker named Maxus,who hacked the online vendor and stole everal hundred thousand credit card numbers.

11) What is deliberate acts of sabotage and vandalism?

- Individual or group who want to deliberately sabotage the operations of a computer system or business, or perform acts of vandalism to either destroy an asset or damage the image of the organization
- These threats can range from petty vandalism to organized sabotage
- Organizations rely on image so Web defacing can lead to dropping consumer confidence and sales
- Rising threat of hacktivist or cyber-activist operations – the most extreme version is cyber-terrorism

12) What is Cyber terrorism?

Cyberterrorism is amost sinister form of hacking involving cyberterrorists hacking systems to conduct terrorist activities through network or internet pathways.
An example was defacement of NATO web pages during the war in Kosovo.

13)What are the deliberate acts of theft?

- Illegal taking of another's property - physical, electronic, or intellectual
- The value of information suffers when it is copied and taken away without the owner's knowledge
- Physical theft can be controlled - a wide variety of measures used from locked doors to guards or alarm systems
- Electronic theft is a more complex problem to manage and control - organizations may not even know it has occurred

14) What are deliberate software attacks?
¬ When an individual or group designs software to attack systems, they create malicious code/software called malware
o Designed to damage, destroy, or deny service to the target systems
¬ Includes:

- macro virus
- boot virus
- worms
- Trojan horses
- logic bombs
- back door or trap door
- denial-of-service attacks
- polymorphic
- hoaxes

15) What are the forces of Nature affecting information security?

- Forces of nature, force majeure, or acts of God are dangerous because they are unexpected and can occur with very little warning
- Can disrupt not only the lives of individuals, but also the storage, transmission, and use of information
- Include fire, flood, earthquake, and lightning as well as volcanic eruption and insect infestation
- Since it is not possible to avoid many of these threats, management must implement controls to limit damage and also prepare contingency plans for continued operations

16)What are technical hardware failures or errors?

- Technical hardware failures or errors occur when a manufacturer distributes to users equipment containing flaws
- These defects can cause the system to perform outside of expected parameters, resulting in unreliable service or lack of availability
- Some errors are terminal, in that they result in the unrecoverable loss of the equipment
- Some errors are intermittent, in that they only periodically manifest themselves, resulting in faults that are not easily repeated

17) What are technical software failures or errors?

- This category of threats comes from purchasing software with unrevealed faults
- Large quantities of computer code are written, debugged, published, and sold only to determine that not all bugs were resolved
- Sometimes, unique combinations of certain software and hardware reveal new bugs

- Sometimes, these items aren't errors, but are purposeful shortcuts left by programmers for honest or dishonest reasons

18) What is technological obsolescence?

- When the infrastructure becomes antiquated or outdated, it leads to unreliable and untrustworthy systems
- Management must recognize that when technology becomes outdated, there is a risk of loss of data integrity to threats and attacks
- Ideally, proper planning by management should prevent the risks from technology obsolesce, but when obsolescence is identified, management must take action

19) What is an attack?

- An attack is the deliberate act that exploits vulnerability
- It is accomplished by a threat-agent to damage or steal an organization's information or physical asset
    - An exploit is a technique to compromise a system
    - A vulnerability is an identified weakness of a controlled system whose controls are not present or are no longer effective
    - An attack is then the use of an exploit to achieve the compromise of a controlled system

20) What is a malicious code?

This kind of attack includes the execution of viruses, worms, Trojan horses, and active web scripts with the intent to destroy or steal information. The state of the art in attacking systems in 2002 is the multi-vector worm using up to six attack vectors to exploit a variety of vulnerabilities in commonly found information system devices

21) Define Virus

Virus - Each infected machine infects certain common executable or script files on all computers to which it can write with virus code that can cause infection

22) Define Hoaxes

Hoaxes - A more devious approach to attacking computer systems is the transmission of a virus hoax, with a real virus attached

23) What is Distributed Denial-of-service (DDoS)?

DDoS is an attack in which a coordinated stream of requests is launched against a target from many locations at the same time

24) What is Back Door?

Back Doors - Using a known or previously unknown and newly discovered access mechanism, an attacker can gain access to a system or network resource

25) Define Dictionary attack

The dictionary password attack narrows the field by selecting specific accounts to attack and uses a list of commonly used passwords (the dictionary) to guide guesses

26.)What are the attack replication vectors?

27) What are the various forms of attacks.

- IP Scan and Atack
- Web Browsing
- Virus
- Unprotected Shares
- Mass Mail
- SNMP
- Hoaxes
- Back Doors
- Password Crack
- Brute Force
- Dictionary
- Denial of Service
- Distributed DoS

28) What is Denial-of-service (DoS) ?

- attacker sends a large number of connection or information requests to a target
- so many requests are made that the target system cannot handle them successfully along with other, legitimate requests for service
- may result in a system crash, or merely an inability to perform ordinary functions

29) Define Spoofing

It is a technique used to gain unauthorized access whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host

30)Define Man-in-the-Middle

Man-in-the-middle is an attacker sniffs packets from the network, modifies them, and inserts them back into the network

16 Marks

1) Explain the four important functions, the information security performs in an organization
2) What are dual homed host firewalls? Explain
3) What are deliberate acts of Espionage or tresspass. Give examples.
4) What deliberate software attacks?
5) Explain in detail the different types of cryptanalytic attacks
6) Enumerate different types of attacks on computer based systems.
7) What are different US laws and International laws on computer based crimes?
8) Explain in detail the Legal, Ethical and Professional issues during the security investigation
9) What are threats? Explain the different categories of threat
10) What is the code of ethics to be adhered to by the information security personnel stipulated by different professional organizations?
11) What is Intellectual property? How it can be protected?
12) Who are Hackers? Explain its levels
13) Explain the attack replication vectors
14) Discuss in detail the forces of Nature affecting information security
15) Explain deliberate software attacks

UNIT-II

1. What is a policy?

A policy is a plan or course of action, as of a government, political party, or business, intended to influence and determine decisions, actions, and other matters

2. What are the three types of security policies?

Management defines three types of security policy:

- General or security program policy
- Issue-specific security policies
- Systems-specific security policies

3. What is Security Program Policy?

A security program policy (SPP) is also known as

- A general security policy
- IT security policy
- Information security policy

4. Define Issue-Specific Security Policy (ISSP)

The ISSP:

- addresses specific areas of technology
- requires frequent updates
- contains an issue statement on the organization's position on an issue
- 5. What are ACL Policies?

ACLs allow configuration to restrict access from anyone and anywhere

ACLs regulate:

- Who can use the system
- What authorized users can access
- When authorized users can access the system
- Where authorized users can access the system from
- How authorized users can access the system

6. What is Information Security Blueprint?

The Security Blue Print is the basis for Design,Selection and Implementation of Security Policies,education and training programs,and technology controls.

7. Define ISO 17799/BS 7799 Standards and their drawbacks

- One of the most widely referenced and often discussed security models is the Information Technology – Code of Practice for Information Security Management, which was originally published as British Standard BS 7799
- This Code of Practice was adopted as an international standard by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) as ISO/IEC 17799 in 2000 as a framework for information security

8. Mention the Drawbacks of ISO 17799/BS 7799

Several countries have not adopted 17799 claiming there are fundamental problems:

- The global information security community has not defined any justification for a code of practice as identified in the ISO/IEC 17799
- 17799 lacks "the necessary measurement precision of a technical standard"
- There is no reason to believe that 17799 is more useful than any other approach currently available

- 17799 is not as complete as other frameworks available
- 17799 is perceived to have been hurriedly prepared given the tremendous impact its adoption could have on industry information security controls

9. What are the objectives of ISO 17799?

Organizational Security Policy is needed to provide management direction and support

Objectives:

- Operational Security Policy
- Organizational Security Infrastructure
- Asset Classification and Control
- Personnel Security
- Physical and Environmental Security
- Communications and Operations Management
- System Access Control
- System Development and Maintenance
- Business Continuity Planning
- Compliance

10. What is the alternate Security Models available other than ISO 17799/BS 7799?

- Another approach available is described in the many documents available from the Computer Security Resource Center of the National Institute for Standards and Technology (csrc.nist.gov) – Including:
- NIST SP 800-12 - The Computer Security Handbook
- NIST SP 800-14 - Generally Accepted Principles and Practices for Securing IT Systems
- NIST SP 800-18 - The Guide for Developing Security Plans for IT Systems

11. Lis the management controls of NIST SP 800-26

- Risk Management
- Review of Security Controls
- Life Cycle Maintenance
- Authorization of Processing (Certification and Accreditation)
- System Security Plan

12. Mention the Operational Controls of NIST SP 800-26

- Personnel Security
- Physical Security
- Production, Input/Output Controls
- Contingency Planning
- Hardware and Systems Software
- Data Integrity
- Documentation
- Security Awareness, Training, and Education
- Incident Response Capability

- 13. What are the Technical Controls of NIST 800-26?

- Identification and Authentication
- Logical Access Controls
- Audit Trails

14. What is Sphere of protection?
    - The "sphere of protection" overlays each of the levels of the "sphere of use" with a layer of security, protecting that layer from direct or indirect use through the next layer
    - The people must become a layer of security, a human firewall that protects the information from unauthorized access and use
    - Information security is therefore designed and implemented in three layers
        - policies
        - people (education, training, and awareness programs)
        - technology

15. What is Defense in Depth?
    - One of the foundations of security architectures is the requirement to implement security in layers
    - Defense in depth requires that the organization establish sufficient security controls and safeguards, so that an intruder faces multiple layers of controls

16. What is Security perimeter?
    - The point at which an organization's security protection ends, and the outside world begins is referred to as the security perimeter

17. What are the key technological components used for security implementation?
    - A firewall is a device that selectively discriminates against information flowing into or out of the organization
    - The DMZ (demilitarized zone) is a no-man's land, between the inside and outside networks, where some organizations place Web servers
    - In an effort to detect unauthorized activity within the inner network, or on individual machines, an organization may wish to implement Intrusion Detection Systems or IDS

18. What is Systems-Specific Policy (SysSP)?
    - SysSPs are frequently codified as standards and procedures used when configuring or maintaining systems
    - Systems-specific policies fall into two groups:
    - Access control lists (ACLs) consist of the access control lists, matrices, and capability tables governing the rights and privileges of a particular user to a particular system

19. What is the importance of blueprint?
    - The blueprint should specify the tasks to be accomplished and the order in which they are to be realized. It should serve as a scaleable,upgradable,and comprehensive paln for the information security needs for coming years.

20. What are the approaches of ISSP?

Three approaches:

- Create a number of independent ISSP documents
- Create a single comprehensive ISSP document
- Create a modular ISSP document

16 Marks

1. What are ISO 7799 and BS7799? Explain their different sections and salient features.
2. Explain salient features of NIST security models.
3. Explain with diagrams the design of security architecture.
4. Explain how information security policy is implemented as procedure
5. What are the three types of security policies? Explain
6. Compare and contrast the ISO 17700 wit BS 7799 NIST security model
7. Explain the NIST security model
8. List the styles of security architecture models. Discuss them in detail
9. Explain NIST SP 800-14
10. Explain Sphere of protection with a neat sketch
11. Explain the key technological components used for security implementation
12. Write short notes on

i. Defense in depth

ii. Security perimeter

13. Write short notes on

iii. Incident Response plan(IRP)

iv. Disaster Recovery Plan

v. Business Continuity Plan

14. What is Business Impact Analysis? Explain different stages of BIA in detail.
15. Explain Key technology component

UNIT-III

1. What is risk management?

Risk management is the process of identifying vulnerabilities in an organization's information systems and taking carefully reasoned steps to assure

- Confidentiality
- Integrity
- Availability

of all the components in the organization's information systems

2. What the roles to be played by the communities of interest to manage the risks an organization encounters?

It is the responsibility of each community of interest to manage risks; each community has a role to play:

- Information Security
- Management and Users
- Information Technology

3. What is the process of Risk Identification?

- A risk management strategy calls on us to "know ourselves" by identifying, classifying, and prioritizing the organization's information assets
- These assets are the targets of various threats and threat agents and our goal is to protect them from these threats

4. What are asset identification and valuation.

This iterative process begins with the identification of assets, including all of the elements of an organization's system: people, procedures, data and information, software, hardware, and networking elements

5. What is Asset Information for People?

- Position name/number/ID
- Supervisor
- Security clearance level
- Special skills

6. What are Hardware, Software, and Network Asset Identification?

When deciding which information assets to track, consider including these asset attributes:

- Name
- IP address
- MAC address
- Element type
- Serial number
- Manufacturer name
- Manufacturer's model number or part number
- Software version, update revision, or FCO number

- Physical location
- Logical location
- Controlling entity

7. What are Asset Information for Procedures?

• Description
• Intended purpose
• What elements is it tied to
• Where is it stored for reference
• Where is it stored for update purposes

8. What are the Asset Information for Data?

• Classification
• Owner/creator/manager
• Size of data structure
• Data structure used – sequential, relational
• Online or offline
• Where located
• Backup procedures employed

9. How information assets are classified?

• Examples of these kinds of classifications are:
• confidential data
• internal data
• public data
• Informal organizations may have to organize themselves to create a useable data classification model
• The other side of the data classification scheme is the personnel security clearance structure

10. Define the process of Information asset valuation.

• Create a weighting for each category based on the answers to the previous questions
• Which factor is the most important to the organization?
• Once each question has been weighted, calculating the importance of each asset is straightforward
• List the assets in order of importance using a weighted factor analysis worksheet

11. What are the Questions to assist in developing the criteria to be used for asset valuation?

• Which information asset is the most critical to the success of the organization?
• Which information asset generates the most revenue?
• Which information asset generates the most profitability?
• Which information asset would be the most expensive to replace?
• Which information asset would be the most expensive to protect?
• Which information asset would be the most embarrassing or cause the greatest liability if revealed?

12. Define data classification and management.

• A variety of classification schemes are used by corporate and military organizations
• Information owners are responsible for classifying the information assets for which they are responsible
• Information owners must review information classifications periodically
• The military uses a five-level classification scheme but most organizations do not need the detailed level of classification used by the military or federal agencies

13. What are security clearances?
• The other side of the data classification scheme is the personnel security clearance structure
• Each user of data in the organization is assigned a single level of authorization indicating the level of classification
• Before an individual is allowed access to a specific set of data, he or she must meet the need-to-know requirement
• This extra level of protection ensures that the confidentiality of information is properly maintained

14. Explain the process of threat identification?
Threat Identification
• Each of the threats identified so far has the potential to attack any of the assets protected
• This will quickly become more complex and overwhelm the ability to plan
• To make this part of the process manageable, each step in the threat identification and vulnerability identification process is managed separately, and then coordinated at the end of the process

15. How to identify and Prioritize Threats?
• Each threat must be further examined to assess its potential to impact organization - this is referred to as a threat assessment
• To frame the discussion of threat assessment, address each threat with a few questions:
• Which threats present a danger to this organization's assets in the given environment?
• Which threats represent the most danger to the organization's information?
• How much would it cost to recover from a successful attack?
• Which of these threats would require the greatest expenditure to prevent?

16. What are the different threats faced by an information system in an Organization?

17. What is Vulnerability Identification?
• We now face the challenge of reviewing each information asset for each threat it faces and creating a list of the vulnerabilities that remain viable risks to the organization
• Vulnerabilities are specific avenues that threat agents can exploit to attack an information asset
• Examine how each of the threats that are possible or likely could be perpetrated and list the organization's assets and their vulnerabilities
• The process works best when groups of people with diverse backgrounds within the organization work iteratively in a series of brainstorming sessions

18. What is Risk assessment?

• We can determine the relative risk for each of the vulnerabilities through a process called risk assessment

• Risk assessment assigns a risk rating or score to each specific information asset, useful in gauging the relative risk introduced by each vulnerable information asset and making comparative ratings later in the risk control process

19. Mention the Risk Identification Estimate Factors

- Likelihood
- Value of Information Assets
- Percent of Risk Mitigated
- Uncertainty

20. Give an example of Risk determination.

For the purpose of relative risk assessment:
risk = likelihood of vulnerability occurrence times value (or impact) -
percentage risk already controlled + an element of uncertainty

Information Asset A has an value score of 50 and has one vulnerability:

• Vulnerability 1 has a likelihood of 1.0 with no current controls and you estimate that assumptions and data are 90 % accurate

Asset A: vulnerability rated as 55 = (50 * 1.0) – 0% + 10%

21. What is residual risk?

• For each threat and its associated vulnerabilities that have any residual risk, create a preliminary list of control ideas

• Residual risk is the risk that remains to the information asset even after the existing control has been applied

22. What is access control?

One particular application of controls is in the area of access controls

• Access controls are those controls that specifically address admission of a user into a trusted area of the organization

• There are a number of approaches to controlling access

• Access controls can be - discretionary , mandatory , nondiscretionary

23. What are the different types of Access Controls?

• Discretionary Access Controls (DAC)
• Mandatory Access Controls (MACs)
• Nondiscretionary Controls
• Role-Based Controls
• Task-Based Controls
• Lattice-based Control

24. What is the goal of documenting results of the risk assessment?

• The goal of this process has been to identify the information assets of the organization that have specific vulnerabilities and create a list of them, ranked for focus on those most needing protection first
• In preparing this list we have collected and preserved factual information about the assets, the threats they face, and the vulnerabilities they experience

25. Mention the strategies to control the vulnerable risks.
Four basic strategies are used to control the risks that result from vulnerabilities:

- Apply safeguards (avoidance)
- Transfer the risk (transference)
- Reduce the impact (mitigation)
- Inform themselves of all of the consequences and accept the risk without control or mitigation (acceptance)

26. What are the different risk control strategies?

- Avoidance
- Transference
- Mitigation
- Acceptance

27. Write short notes on Incidence Response Plan
The actions an organization can perhaps should take while the incident is in progress are documented in what is known as Incident Response Plan(IRP).
Answers to the following type of questions will be provided in IRP:
a. What should the administrator should do first?
b. Whom should they contact?
c. What should they document?

28. Define Disaster Recovery Plan

The most common mitigation procedure is Disaster Recovery Plan(DRP). The DRP includes the entire spectrum of activities used to recover from the incident and strategies to limit losses before and after the disaster. DRP usually include all preparations for the recovery process, strategies to limit losses during the disaster.

29. Define Business Continuity Plan

The BCP is the most strategic and long term of the three plans. It encompasses the continuation of business activities if a catastrophic event occurs,such as the loss of an entire database,building or entire operations center. The BCP includes the planning the steps necessary to to ensure the continuation of the organization when the scope or scale of a disaster exceeds the ability of the DRP to restore operations.

30. What are different categories of controls?

- Control Function
- Architectural Layer
- Strategy Layer
- Information Security Principles

16 Marks

1. What is risk management? State the methods of identifying and assessing risk management
2. Discuss in detail the process of assessing and controlling risk management issues
3. What is risk management? Why is the identification of risks by listing assets and vulnerabilities is so important in the risk management process?
4. Explain in detail different risk control strategies
5. Explain asset identification and valuation
6. Explain in detail the three types of Security policies (EISP,ISSP and sysSP).
7. What is Information Security Blue print? Explain its salient features.
8. Explain the roles to be played by the communities of interest to manage the risks an organization encounters
9. Explain the process of Risk assessment
10. Explain briefly the plans adopted for mitigation of risks
11. Explain how the risk controls are effectively maintained in an organization
13) Write short notes on

a) Incidence Response Plan b)Disaster Recovery Plan c)Business continuity plan

12. Explain in detail the process of asset identification for different categories
13. Explain the process of Information asset valuation
14. Discuss briefly data classification and management
15. Explain the process of threat identification?
16. Explain the process of vulnerability identification and assessment for different threats faced by an information security system

UNIT-IV

1. What are firewalls?

A firewall is any device that prevents a specific type of information from moving between the untrusted network outside and the trusted network inside
The firewall may be:

- a separate computer system
- a service running on an existing router or server
- a separate network containing a number of supporting devices

2. Explain different generations of firewalls.

- First Generation - packet filtering firewalls
- Second Generation-application-level firewall or proxy server
- Third Generation- Stateful inspection firewalls
- Fourth Generation-dynamic packet filtering firewall
- Fifth Generation- kernel proxy

3. Mention the functions of first generation firewall

Examines every incoming packet header and selectively filters packets based on address, packet type, port request, and others factors

4. What are the restrictions of first generation firewall?
The restrictions most commonly implemented are based on:

- IP source and destination address
- Direction (inbound or outbound)
- TCP or UDP source and destination port-requests

5. What is the advantage of Second Generation firewalls?

The primary disadvantage of application-level firewalls is that they are designed for a specific protocol and cannot easily be reconfigured to protect against attacks on protocols for which they are not designed

6. Define stateful inspection firewall

It keeps track of each network connection established between internal and external systems using a state table which tracks the state and context of each packet in the conversation by recording which station sent what packet and when

7. What is the disadvantage of third generation firewalls?

The primary disadvantage is the additional processing requirements of managing and verifying packets against the state table, which can possibly expose the system to a DoS attack. These firewalls can track connectionless packet traffic such as UDP and remote procedure calls (RPC) traffic

8. What is the function of Fifth Generation firewall?

The final form of firewall is the kernel proxy, a specialized form that works under the Windows NT Executive, which is the kernel of Windows NT. It evaluates packets at multiple

layers of the protocol stack, by checking security in the kernel as data is passed up and down the stack

9. How firewalls are categorized by processing mode?
The five processing modes are

- Packet filtering
- Application gateways
- Circuit gateways
- MAC layer firewalls
- Hybrids

10) What is the drawback of packet-filtering router?

The drawback of packet-filtering router includes a lack of auditing and strong authentication

11) What are Screened-Host Firewall Systems

Screened-Host firewall system allows the router to pre-screen packets to minimize the network traffic and load on the internal proxy

12) What is the use of an Application proxy?

An Application proxy examines an application layer protocol, such as HTTP, and performs the proxy services

13) What are dual homed host firewalls?

The bastion-host contains two NICs (network interface cards)
One NIC is connected to the external network, and one is connected to the internal network
With two NICs all traffic must physically go through the firewall to move between the internal and external networks

14) What is the use of NAT?

A technology known as network-address translation (NAT) is commonly implemented to map from real, valid, external IP addresses to ranges of internal IP addresses that are non-routable

15) What are Screened-Subnet Firewalls?
• Consists of two or more internal bastion-hosts, behind a packet-filtering router, with each host protecting the trusted network
• The first general model consists of two filtering routers, with one or more dual-homed bastion-host between them
• The second general model involves the connection from the outside or untrusted network

16) What are the factors to be considered while selecting a right firewall?
o What type of firewall technology offers the right balance of protection features and cost for the needs of the organization?
o What features are included in the base price? What features are available at extra cost? Are all cost factors known?

o How easy is it to set up and configure the firewall? How accessible are staff technicians with the mastery to do it well?
o Can the candidate firewall adapt to the growing network in the target organization?

17) What are Sock Servers?
The SOCKS system is a proprietary circuit-level proxy server that places special SOCKS client-side agents on each workstation
18) What are the recommended practices in designing firewalls?
• All traffic from the trusted network is allowed out
• The firewall device is always inaccessible directly from the public network
• Allow Simple Mail Transport Protocol (SMTP) data to pass through your firewall, but insure it is all routed to a well-configured SMTP gateway to filter and route messaging traffic securely
• All Internet Control Message Protocol (ICMP) data should be denied
• Block telnet (terminal emulation) access to all internal servers from the public networks
• When Web services are offered outside the firewall, deny HTTP traffic from reaching your internal networks by using some form of proxy access or DMZ architecture

19) What are intrusion detection systems(IDS)?
• IDSs work like burglar alarms
• IDSs require complex configurations to provide the level of detection and response desired
• An IDS operates as either network-based, when the technology is focused on protecting network information assets, or host-based, when the technology is focused on protecting server or host information assets
• IDSs use one of two detection methods, signature-based or statistical anomaly-based

20) What are different types of IDSs?
- Network-based IDS
- Host-based IDS
- Application-based IDS
- Signature-based IDS
- Statistical Anomaly-Based IDS

21) Define NIDS
A network-based IDS (NIDS) resides on a computer or an appliance connected to a segment of an organization's network and monitors traffic on that network segment, looking for indications of ongoing or successful attacks.

22) What is HIDS?
A Host-based IDS (HIDS) works differently from a network-based version of IDS. A host-based IDS resides on a particular computer or server, known as the host and monitors activity only on that system. HIDs are also known as System Integrity Verifiers as they benchmark and monitor the status of key system files and detect when an intruder creates , modifies or deletes monitored files.

23. What is the use of HIDS?

A HIDs is also capable of monitoring system configuration databases,such as windows registries,in addition to stored configuration files like .ini,.cfg,and .dat files.

24.What is Application-based IDS?
A refinement of Host-based IDs is the application-based IDS(AppIDS). The application based IDs examines an application for abnormal incidents. It looks for anomalous occurrences such as users exceeding their authorization,invalid file executions etc.

25.What is Signature-based IDS?
A signature-based IDS(also called Knowledge-based IDs) examines data traffic in search of patterns that match known signatures – that is,preconfigured ,predetermined attack patterns.

26.What is LFM?
Log File Monitor(LFM) is an approach to IDS that is similar to NIDS. Using LFm the system reviews the log files generated by servers,network devices,and wven other IDSs. These systems look for patterns and signatures in the log files that may indicate an attack or intrusion is in process or has already succeeded.

27.What are Honey Pots?
Honey pots are decoy systems designed to lure potential attackers away from critical systems and encourage attacks against the themselves. These systems are created for the sole purpose of deceiving potential attackers. In Industry they are known as decoys,lures,and fly-traps.

29. What are Honey Nets?
When a collection of honey pots connects several honey pot systems on a subnet,it may be called a honey net.

30.What are Padded Cell Systems?
A Padded Cell is a honey pot that has been protected so that it cannot be easily compromised. In otherwords,a padded cell is a hardened honey spot..

31.What are the advantages and disadvantages of using honey pot or padded cell approach?
Advantages:

- Attackers can be diverted to targets that they cannot damage.
- Administrators have time to decide how to respond to an attacker.
- Attackers action can be easily and extensively monitored
- Honey pots may be effective at catching insiders who are snooping around a network.

Disadvantages:

- The legal implication of using such devices are not well defined.
- Honey pots and Padded cells have not yet been shown to be generally useful security technologies.
- An exper attacker,once diverted into a decoy system,may become angry and launch a hostile attack againt an organization’s systems
- Admins and security managers will need a high level of expertise to use these systems.

32.What are foot printing and finger printing?

One of the preparatory part of the attack protocol is the collection of publicly available information about a potential target,a process known as footprinting. Footprinting is the organized research of the Internet addresses owned or controlled by the target organization. The next phase of the attack protocol is a second intelligence or data-gathering process called fingerprinting. This is systematic survey of all of the target organization's Internet addresses(which are collected during the footprinting phase); the survey is conducted to ascertain the network services offered by the hostsin that range. Fingerprinting reveals useful information about the internal structure and operational nature of the target system or network for the anticipated attack.

33. What are Vulnerability Scanners?

- Vulnerability scanners are capable of scanning networks for very detailed information
- As a class, they identify exposed usernames and groups, show open network shares, expose configuration problems, and other vulnerabilities in servers

34. Define Packet Sniffers

A network tool that collects copies of packets from the network and analyzes them
Can be used to eavesdrop on the network traffic
To use a packet sniffer legally, you must be:

- on a network that the organization owns
- under direct authorization of the owners of the network
- have knowledge and consent of the content creators (users)

35.What is Cryptography?.

Cryptography, which comes from the Greek work kryptos,meaning "hidden",and graphein,meaning "to write",is aprocess of making and using codes to secure the transmission of information.

36.What is Cryptoanalysis?

Cryptoanalysis is the process of obtaining the original message(called plaintext) from an encrypted message(called the ciphertext) without knowing the algorithms and keys used to perform the encryption.

37. Define Encryption

Encryption is the process of converting an original message into a form that is unreadable to unauthorized individuals-that is,to anyone without the tools to convert the encrypted message back to its original format.

38.Define Decryption

Decryption is the process of converting the cipher text into a message that conveys readily understood meaning.

39.What is Public Key Infrastructure (PKI)?

PKI or Public Key Infrastructure

- Public Key Infrastructure is the entire set of hardware, software, and cryptosystems necessary to implement public key encryption
- PKI systems are based on public-key cryptosystems and include digital certificates and certificate authorities (CAs) and can:
    - Issue digital certificates
    - Issue crypto keys
    - Provide tools to use crypto to secure information
    - Provide verification and return of certificates

40. What are the PKI Benefits

    PKI protects information assets in several ways:
        - Authentication
        - Integrity
        - Privacy
        - Authorization
        - Nonrepudiation

41. How E-mail systems are secured?

- Encryption cryptosystems have been adapted to inject some degree of security into e-mail:
    - S/MIME builds on the Multipurpose Internet Mail Extensions (MIME) encoding format by adding encryption and authentication
    - Privacy Enhanced Mail (PEM) was proposed by the Internet Engineering Task Force (IETF) as a standard to function with the public key cryptosystems
    - PEM uses 3DES symmetric key encryption and RSA for key exchanges and digital signatures
    - Pretty Good Privacy (PGP) was developed by Phil Zimmerman and uses the IDEA Cipher along with RSA for key exchange

42. What are the seven major sources of physical loss?
    - Temperature extremes
    - Gases
    - Liquids
    - Living organisms
    - Projectiles
    - Movement
    - Energy anomalies

43. What is a Secure Facility?
    - A secure facility is a physical location that has been engineered with controls designed to minimize the risk of attacks from physical threats
    - A secure facility can use the natural terrain; traffic flow, urban development, and can complement these features with protection mechanisms such as fences, gates, walls, guards, and alarms

44. What are the controls used in a Secure Facility?
        - Walls, Fencing, and Gates
        - Guards

- Dogs, ID Cards, and Badges
- Locks and Keys
- Mantraps
- Electronic Monitoring
- Alarms and Alarm Systems
- Computer Rooms
- Walls and Doors

45. What are the functions of Chief Information Security officer?
The CISO performs the following functions:

- Manages the overall InfoSec program
- Drafts or approves information security policies
- Works with the CIO on strategic plans, develops tactical plans, and works with security managers on operational plans
- Develops InfoSec budgets based on funding
- Sets priorities for InfoSec projects & technology
- Makes decisions in recruiting, hiring, and firing of security staff
- Acts as the spokesperson for the security team

16 Marks

1. Explain in detail
i. Firewalls categorized by processing mode
ii. Different generations of firewall
2. Explain in detail different firewall architectures (OR) Write short notes on
iii. Packet filtering Routers
iv. Screened Host fire wall
v. Screened subnet firewalls (with DMZ)
3. What are the factors to be considered in selecting a right firewall?
4. Explain How firewalls are configured and managed?
5. Outline some of the best practices for firewall use.
6. What are fire wall rules? Explain different fire wall rule sets.
7. What is Iintrusion Detection System(IDS)? Explain different reasons for using IDS and different terminologies associated with IDS.
8. What are different types of Intrusion Detection Systems available? Explain with diagrams
9. Write short notes on
vi. Network-based IDS
vii. Host-based IDS
viii. Application-based IDS
ix. Signature-based IDS

10. What are Honey pots,Honey Nets and Padded cell systems? Explain each.
11. What is Attacking Protocol? Explain a) Foot printing and b) Finger printing.
12. What are the purposes of Scanning and Analysis tools? Who will be using these tools? Explain the functioning of few of these tools.
13. What is cryptography? Define various encryption terms used.

14. What is RSA algorithm? Explain different steps>
15. What are different possible attacks on crypto systems?
16. List and describe four categories of locks?
17. Explain with a diagram different positions in Information security.