NOORUL ISLAM COLLEGE OF ENGINEERING, KUMARACOIL

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

CLASS : SEVENTH SEMESTER B.E CSE

SUBJECT : CS1014-INFORMATION SECURITY

Prepared By,

A. Anitha.M.E

Lecturer/CSE

Signature of HOD **Signature of Principal**

CS1014-INFORMATION SECURITY

TWO MARKS

1. **Define Information Security.**
   It is a well-informed sense of assurance that the information risks and controls are in balance.

2. **What is Security?**
   Security is "the quality or state of being secure-to be free from danger".

3. **What are the multiple layers of Security?**
   - **Physical Security**
   - **Personal Security**
   - **Operations Security**
   - **Communication Security**
   - **Network Security**
   - **Information Security**

4. **What are the characteristics of CIA triangle?**
   - **Confidentiality**
   - **Integrity**
   - **Availability**

5. **What are the characteristics of Information Security?**
   - **Availability**
   - **Accuracy**
   - **Authenticity**
   - **Confidentiality**
   - **Integrity**
   - **Utility**
   - **Possession**

6. **What is E-mail Spoofing?**
   It is the process of sending an e-mail with a modified field.

7. **What is UDP Packet Spoofing?**
   User Data Protocol (UDP) Packet Spoofing enables the attacker to get unauthorized access to data stored on computing systems.

8. **What are the measures to protect the confidentiality of information?**

- **Information Classification**
- **Secure document storage**
- **Application of general Security Policies.**
- **Education of information end-users**

9. What is Utility of information?

Utility of information is the quality or state of having value for some purpose or end.

10. What are the components of information system?

- **Software**
- **Hardware**
- **Data**
- **People**
- **Procedures**
- **Networks.**

11. What are the functions of Locks & Keys?

Locks & Keys are the traditional tools of physical security, which restricts access to, and interaction with the hardware components of an information system.

12. What is Network Security?

It is the implementation of alarm and intrusion systems to make system owners aware of ongoing compromises.

13. Differentiate Direct and Indirect attacks.

Direct Attack	Indirect Attack
It is when a hacker uses his personal computer to break into the system	It is when a system is compromised and used to attack other systems, such as in a distributed deniel of service attack.
Originate from the threat itself	Originate from a system or resource that itself has attacked & it is malfunctioning or working under the control of a threat.

14. What is SDLC?

The Systems Development Life Cycle is a methodology for the design and implementation of an information system in an organization.

15. What is a methodology?

Methodology is a formal approach to solve a problem based on a structured sequence of procedures.

16. What are the phases of SDLC Waterfall method?

- **Investigation**
- **Analysis**
- **Logical Design**
- **Physical Design**
- **Implementation**
- **Maintenance & change.**

17. What is enterprise Information Security Policy?

This policy outlines the implementation of a security program within the organization.

18. What is Risk Management?

It is the process of identifying, assessing and evaluating the levels of risk facing the organization.

19. What are the functions of Information Security?

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

20. What is PKI?

Public Key Infrastructure is an integrated system of software, encryption methodologies and legal agreements that can be used to support the entire information infrastructure of an organization.

21. What is the use of Digital Certificates?

Digital Certificates are used to ensure the confidentiality of Internet Communications and transactions.

22. What is Firewall?

Firewall is a device that keeps certain kinds of network traffic out of a private network.

23. What are caching network appliances?

Caching network appliances are devices that store legal copies of Internet contents such as WebPages that are frequently referred to by employees.

24. What are appliances?

Appliances display the cached pages to users rather than accessing pages from the server each time.

25. What is a threat?

Threat is an object, person or other entity that represents a constant danger to an asset.

26. What are Hackers?

Hackers are people who use and create computer software for enjoyment or to gain access to information illegally.

27. What are the levels of hackers?

- **<u>Expert Hacker</u>**
  Develops software codes
- **<u>Unskilled Hacker</u>**
  Uses the codes developed by the experts

28. What are script kiddies?

These are hackers of limited skills who expertly written software to exploit a system but not fully understand or appreciate the systems they hack.

29. What is a Phreaker?

A Phreaker hacks the public telephone network to make free calls.

30. What is Malicious code?

These are programs, which are designed to damage, destroy, or deny service to the target system

31. What are the types of virus?

- **Macro virus**
- **Boot virus**

32. What are trojan horses?

They are software programs that hide their true nature and reveal their designed behavior only when activated.

33. What is a polymorphic threat?

It is one that changes its apparent shape over time.

34. What is intellectual propery?

It is the ownership of ideas and control over the tangible or virtual representation of those ideas.

35. What is an attack?

It is a deliberate act that exploits vulnerability.

36. What vulnerability?

It is an identified weakness of a controlled system with controls that are not present or no longer effective.

37. What are the attack replication vectors?

- **Ip scan and attack**
- **Web browsing**
- **Virus**
- **Shares**
- **Mass mail**
- **SNMP**

`38. What is a brute force attack?

Trying every possible combination of options of password.

39. What are sniffers?

Sniffers are programs or device that can monitor data traveling over an network.

40. What is social engineering?

It is the process of using social skills to convince people to reveal access credentials to the attackers.

41. What are the types of Laws?

- **Civil Law**
- **Criminal Law**
- **Tort Law**

42. Differentiate Private & Public Laws.

<u>Private Laws:</u>

- **This Law regulates the relationship between the individual and the organization.**
- **Eg: Family Law, Commercial Law, Labor Law**

<u>Public Law:</u>

- **This Law regulates the structure and administration of government agencies and their relationship with the citizens, employees and other governments.**
- **Eg: Criminal Law, Administrative Law, Constitutional Law.**

43. What are the fundamental principles of HIPAA.

1. **Consumer control of medical information.**
2. **Boundaries on the use of medical information.**
3. **Accountability for the privacy of private information.**
4. **Security of health information.**

44. What are the general categories of unethical and illegal behaviour?

- **Ignorance**
- **Accident**
- **Intent**

45. What is deterrence?

- **It is the best method for preventing illegal or unethical activity.**
- **Examples are laws, Policies and technical controls.**

46. What is Risk Management?

Risk Identification is conducted within the larger process of identifying and justifying risk control known as risk management.

47. What are the communities of interest?

- **Information Security**
- **Management and users**
- **Information Technology**

48. What are the responsibilities of the communities of interests?

- **Evaluating the risk controls**
- **Determining which control options are cost effective for the organization**
- **Acquiring or installing the needed controls.**
- **Overseeing that the controls remain effective.**

49. Write about MAC.

- **It is also called as electronic serial number or hardware addresses.**
- **All network interface hardware devices have a unique number.**
- **The number is used by the network operating system as a mechanism to identify a specific network device.**

50. What is Public key infrastructure certificate authority?

It is a software application that provides cryptographic key management services.

51. What is Clean desk policy?

This requires each employee to secure all information in its appropriate storage container at the end of each day.

52. What is risk assessment?

It is the process of assessing the relative risk for each of the vulnerabilities.

53. What is Likelihood?

Likelihood is the overall rating of the probability that a specific vulnerability within an organization will be successfully attacked.

54. What is Residual Risk?

It is the risk that remains to the information asset even after the existing control has been applied.

55. What are Policies?

Policies are documents that specify an organization's approach to security.

56.What are the types of security policies?

- **General Security Policy**
- **Program Security Policy**
- **Issue-Specific Policies**

57. What are the types of access controls?

- **Mandatory Access Controls(MACs)**
- **Nondiscretionary controls**
- **Discretionary Controls(DAC)**

58. What are the Risk Control Strategies?

- **<u>Avoidance</u> – It is the risk control strategy that attempts to prevent the exploitation of the vulnerability.**
- **<u>Transference</u> – It is the control approach that attempts to shift the risk to other assets,other processes ,or other organizations.**
- **<u>Mitigation</u> – It is the control approach that attempts to reduce the impact caused by the exploitation of vulnerability through planning and preparation.**
- **<u>Acceptance</u>. – It is the choice to do nothingto protect vulnerability and to accept the outcome of an exploited vulnerability.**

59. What are the common methods for Risk Avoidance?

- **Avoidance through Application of Policy**
- **Avoidance through Application of training and education**
- **Avoidance through Application of technology**

60. What are the types of plans in Mitigation strategy?

- **The Disaster Recovery Plan(DRP)**
- **Incident Response Plan(IRP)**
- **Business Continuity Plan(BCP)**

61. What is a hot site?

- **It is also known as business recovery site.**
- **It is a remote location with systems identical or similar to the home site.**

62. What are the ways to categorize the controls?

- **Control function**
- **Architectural Layer**
- **Strategy Layer**
- **Information Security Principle.**

63. Differentiate Preventive and Detective controls.

Preventive Controls	Detective Controls
1. Stop attempts to exploit vulnerability by implementing a security principle, such as authentication or confidentiality	1. It warn organizations of violations of security principles, organizational policies or attempts to exploit vulnerability.
2. It uses the technical procedure such as encryption or combination of technical means and enforcement methods.	2. It use techniques such as audit trials,intrusion detection and configuration monitoring.

64. What are the commonly accepted information security Principles?

- **confidentiality**
- **Integrity**
- **Availability**
- **Authentication**
- **Authorization**
- **Accountability**
- **Privacy.**

65. What is benefit?

It is the value that the organization recognizes by using controls to prevent loses associated with a specific vulnerability.

66. What is asset valuation?

It is the process of assigning financial value or worth to each information asset.

66. What is a Policy?

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

67. Differentiate mission & Vision.

Mission: Mission of an organization is a written statement of an organization's purpose.

Vision: Vision of an organization is a written statement of an organization's goals.

68. What is Strategic Planning?

It is the process of moving the organization towards its vision by accomplishing its mission.

69. What are the general groups of System-Specific Policy?

- **Access Control Lists**
- **Configuration Rules.**

70. What is a Capability table?

- **It is a list associated with users and groups**
- **Specifies which subjects and objects a user or group can access.**
- **These are frequently complex matrices rather than simpl;e lists or tables.**

71. What is "Agreed Upon Procedures"?

It is a document that outlines the policies and technologies necessary to security systems that carry the sensitive cardholder information to and from from VISA systems.

72. What is redundancy?

Implementing multiple types of technology and thereby preventing failure of one system from compromising the security of the information is referred to as redundancy.

73. What is a Firewall?

It is a device that selectively discriminates against information flowing into or out of the organization.

74. What is Firewall Subnet?

It consists of multiple firewalls creating a buffer between the outside and inside networks.

75. What is DMZs?

- **A buffer against outside attack is referred to as Demilitarized Zone.**
- **It is a no-man's-land between the inside and outside networks where some organizations place Web Servers.**
- **The servers provide access to organizational Web pages without allowing Web requests to enter the interior networks.**

76. What are the 2 versions of IDS?

- **Hot-based IDS**
- **Network-based IDS**

77. What is Contingency Planning?

It is the entire planning conducted by the organization to prepare for, react to, and recover from events that threaten the security of information and information assets in the organization.

78. Who are the members of the contingency team?

- **Champion**
- **Project Manager**
- **Team Members.**

79. What are the stages in the Business Impact Analysis Step>?

- **Threat attack identification**
- **Business unit analysis**
- **Attack success scenarios**
- **Potential damage assessment**
- **Subordinate plan classification**

80. What is an attack profile?

It is a detailed description of activities that occur during an attack.

81. What is an incident?

It is any clearly identified attack on the organization's information assets that would threaten the asset's confidentiality, integrity, or availability.

82. What are the phases of Incident Response?

- **Planning**
- **Detection**
- **Reaction**
- **Recovery.**

83. What are the 5 testing strategies of Incident Planning?

- **Checklist**
- **Structured walk-through**
- **Simulation**
- **Parallel**
- **Full interruption**

84. What is an alert roster?

It is a document containing contact information for individuals to be notified in the event of an incident.

85. What are the 2 ways to activate an alert roster?

- **Sequential roster – It is activated as a contact person calls each person on the roster.**
- **Hierarchical roster – It is activated as the first person calls a few other people on the roster, who in turn call a few people.**

86. What is computer forensics?

It is the process of collecting, analyzing and preserving computer related evidence.

87. What are Honey pots?

These are computer servers configured to reassemble production systems, containing rich information just begging to be hacked.

88. What is enticement?

It is the process of attracting attention to a system by placing tantalizing bits of information in key locations.

89. What is entrapment?

It is the action of luring an individual into committing a crime to get a conviction.

90. What is Mutual agreement?

It is a contract between two or more organization's that specifies how each to assist the other in the event of a disaster.

91. What is intrusion?

An intrusion is a type of attack on information assets in which the instigator attempts to gain entry into a system or disrupt the normal operations of a system with, almost always, the intent to do malicious harm.

92. What is IDS?

IDS stands for Intrusion Detection Systems. It works like a burglar alarm in that it detects a violation of its configuration and activates and alarm. This alarm can be audible and/or visual or it can be silent.

93. What is Signature based IDSs?

Signature based IDSs, also known as knowledge based IDSs, examine data traffic for patterns that match signatures, which are pre-configured, predetermined attack patterns.

94. What are Honey pots?

Honey pots are decoy systems, which means they are designed to lure potential attackers away from critical systems.
In the security industry, these systems are also known as decoys, lures, or fly-traps.

95. What is the use of Scanning and analysis tools?

Scanning and analysis tools are used to pinpoint vulnerabilities in systems, holes in security components, and unsecured aspects of the network. Although these tools are used by attackers, they can also be used by an administrator not only to learn more about his/her own system but also identify and repair system weaknesses before they result in losses.

96. What are the factors of authentication?

- **What a supplicant knows**
- **What a supplicant has**
- **Who a supplicant is**
- **What a supplicant produces**

97. What is Hash function?

Hash functions are mathematical algorithms that generate a message summary or digest that can be used to confirm the identity of a specific message and to confirm that the message has not been altered.

98. What is PKI?

PKI – Public Key Infrastructure

It is an integrated system of software, encryption methodologies, protocols, legal agreements and third party services that enables users to communicate securely. It includes digital certificates and certificate authorities.

99. What is Steganography?

Steganography is the process of hiding information, and while it is not properly a form of cryptography, it is related to cryptography in that both are ways of transmitting information without allowing it to be revealed in transit.

100. What are the protocols used in Secure Internet Communication?

- **S-HTTP(Secure Hypertext Transfer Protocol)**
- **SSL(Secure Socket Layer)**
- **SSL Record Protocol**
- **Standard HTTP**

101. What is Physical security?

Physical security addresses the design, implementation, and maintenance of countermeasures that protect the physical resources of an organization. This means the physical protection of the people, the hardware, and the supporting system elements and resources associated with the control of information in all its states: transmission, storage and processing.

102. What are the controls of protecting the Secure Facility?

- **Walls, Fencing, Gates**
- **Guards**
- **Dogs**
- **ID Cards and Badges**
- **Locks and keys**
- **Mantraps**
- **Electronic Monitoring**
- **Alarms and Alarm Systems**
- **Computer Rooms and Wiring Closets**
- **Interior Walls and Doors**

103. What are the basic types of Fire Detection Systems?

- **Thermal Detection**
- **Smoke Detection**
- **Flame Detection**

104. What is TEMPEST?

TEMPEST is a technology that prevents the loss of data that may result from the emissions of electromagnetic radiation.

105. What is UPS? What are the types of UPS?

UPS- Uninterruptible Power Supply

It is a electrical device that serves as a battery backup to detect the interruption of power to the power equipment.

The basic configurations are,

- **Standby or offline UPS**
- **Ferroresonant Standby UPS**
- **Line-interactive UPS**
- **True online UPS**

106. What are the relevant terms for electrical power influence?

- **Fault: Momentory Interruption in power**
- **Blackout: Prolonged Interruption in power**
- **Sag: Momentary drop in power voltage levels**
- **Brown out: Prolonged drop in power voltage levels**
- **Spike: Momentory increase in power voltage levels**
- **Surge: Prolonged increase in power voltage levels**

107. What is fail-safe lock?

It is usually used on an exit,where it is essential for human safety in the event of a fire.It is used when human safety is not a factor.

108. What are the conditions cotrolled by HVAC Systems?

- **Temperature**
- **Filtration**
- **Humidity**
- **Static Electricity.**

16-MARKS

1.Explain the Critical Characteristics of Information

- **Availability**
- **Accuracy**
- **Authenticity**
- **Confidentiality**
- **Integrity**
- **Utility**
- **Possession**

2. Explain the Components of an Information System

- **Software**
- **Hardware**
- **People**
- **Data**
- **Procedures**
- **Networks**

3. Explain SDLC in detail.

- **Methodology**
- **Phases**
- **Phases**
- **Investigation**
- **Analysis**
- **Logical Design**
- **Physical Design**
- **Implementation**
- **Maintenance and change**

4. Explain SecSDLC in detail

- **Investigation**
- **Analysis**
- **Logical Design**
- **Physical Design**
- **Implementation**
- **Maintenance and change**

5. Explain the functions of an Information security organization

- **Protects the organization's ability to function**
- **Enabling safe operation of applications**
- **Protecting data that organizations collect and use**
- **Safeguarding technology assets in organizations**

6. Explain the categories of Threat in detail.

- **Acts of human error or failure**
- **Deviations in QOS by service providers**
- **Deliberate acts of espionage or trespass**
- **Deliberate acts of information extortion**
- **Deliberate acts of Sabotage or vandalism**
- **Deliberate acts of theft**
- **Deliberate software attacks**
- **Compromises to Intellectual Property**
- **Forces of Nature.**

7. Explain the types of Attacks in detail?

- **Malicious code**
- **Hoaxes**
- **Back Doors**
- **Password Crack**
- **Brute Force**
- **Dictionary**

8. Explain General Computer Crime Laws.

- **Computer Fraud & abuse Act 0f 1986**
- **USA Patriot Act of 2001**
- **Communications Decency Act**
- **Computer Security Act of 1987**

9. Explain Ethical Concepts in Information Security.

- **Cultural Differences in Ethical Concepts**
- **Software License Infringement**
- **Illicit use**
- **Misuse of corporate resources**

10. Explain Risk Management in detail.

- **Know Yourself**
- **Know Your Enemy**
- **All Communities of Interest**

11. Explain Risk Identification in detail

- **Asset Identification & Valuation**
- **Automated Risk Management tools**
- **Information Asset Classification**
- **Information Asset Valuation**
- **Listing Assets in order of importance**
- **Data Classification & Management**
- **Threat Identification**

12. Explain Risk assessment in detail.

- **Introduction**
- **Likelihood**
- **Valuation of Information Assets**
- **Percentage of Risk Mitigated by Controls**
- **Access Controls**

13. Explain Risk Control strategies in detail

- **Avoidance**
- **Mitigation**
- **Acceptance**
- **Transference**

14. Explain Risk Mitigation strategy Selection

- **Evaluation, Assessment and Maintenance of Risk controls**
- **Categories of controls**
- **Architectural Layer**
- **Strategy Layer**
-

15. Explain the types of Policies in detail.

- **General security Policy**
- **Issue-Specific Policy**
- **System-specific Policy**

16. Explain NIST Security Models in detail.

- **NIST Special Publication SP 800-12**
- **NIST Special Publication SP 800-14**
- **NIST Special Publication SP 800-18**

17. Explain VISA International Security Model in detail.

- **Baselining and best Business Practises**

18. Explain the design of Security Architecture in detail.

- **Defense in Depth**
- **Security Perimeter**
- **Key Technology Components**

19. Explain the Major Steps in Contingency Planning.

- **Business Impact Analysis**
- **Incident Response Planning**
- **Disaster Recovery Planning**
- **Business Continuity Planning.**

20.Explain Information Security Policy, Standards and Practices in detail.

- **Definitions**
- **Security Program Policy(SPP)**
- **Issue-Specific Security Policy(ISSP)**
- **Systems-Specific Policy(SysSP)**
- **ACL Policies**
- **Policy Management**

21. Explain protocols for Secure communication in detail.

- **S-HTTP & SSL**
- **Secure/Multipurpose Internet Mail Extension(S/MIME)**
- **Internet Protocol Security(IPSec)**

22. Explain Staffing the security in detail.

- **Qualifications and Requirements**
- **Entry into the Security Profession**
- **Information Security Positions**

23. Explain the fire safety in Physical security.

- **Fire Detection & Response**
- **Fire Detection**
- **Fire Suppression**
- **Gaseous Emission Systems**

24. Explain the Cryptographic algorithms in detail.

- **Data Encryption Standards(DES)**
- **Public Key Infrastructure(PKI)**
- **Digital Signatures**
- **Pretty Good Privacy(PGP)**

25. Explain IDS in detail

- **Host-based Ids**
- **Network-based IDS**
- **Signature-based IDS**
- **Statistical Anomaly-based IDS**

26. Explain the type of encryption/decryption method.

Conventional Methods:

- **Character-Level Encryption: Substitutional & Transpositional**
- **Bit-Level Encryption: Encoding/Decoding, Permutation, Substitution, Product, Exclusive-Or & Rotation**

Public key Methods

27. Explain about RSA algorithm.

- **Public key Encryption technique.**
- **Encryption algorithm**
- **Decryption algorithm**
- **Security in RSA**

28.Explain about secret key encryption algorithm.

- **Data Encryption Standard**
- **Algorithm**
- **Sub key generation**

29. Explain Scanning and Analysis Tools in detail

- **Footprinting**
- **Fingerprinting**
- **Port Scanners**
- **Vulnerability Scanners**
- **Packet Sniffers**
- **Content Filters**

30. Explain Firewalls in detail.

- **Development of Firewalls(5 generations)**
- **Firewall Architecture**
- **Packet Filtering Routers**
- **Screened Host Firewall Systems**
- **Dual-homed Host Firewalls**
- **Screened Subnet Firewalls(with DMZ)**
- **SOCKS Server**
- **Configuring and Managing Firewalls**