UNIT 1 – INTRODUCTION

PART A

1. What are the multiple layers of Security?

• Physical Security

• Personal Security

• Operations Security

• Communication Security

• Network Security

• Information Security

2. What are the characteristics of CIA triangle?

• Confidentiality

• Integrity

• Availability

3. What are the characteristics of Information Security?

• Availability

• Accuracy

• Authenticity

• Confidentiality

• Integrity

• Utility

• Possession

4. Who are the team members of Information Security Project?

- Champion
- Team Leader

- Security policy developers
- Risk assessment specialists
- Security Professionals
- System Administrators
- End users

5. 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

6. What is SDLC?

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

7. **What are the phases of SDLC Waterfall method?**

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

8. What is enterprise Information Security Policy?

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

9. 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.

10. What is Information Security?

Information security – is the protection of information and its critical elements, including the systems and hardware that use ,store, and transmit the information

PART B

1. **Explain Systems Development Life Cycle (SDLC) in Detail.**

   It is the most important phase and it begins with an examination of the event or plan that initiates the process.

   During this phase, the objectives, constraints, and scope of the project are specified.

   • Investigation

   • Analysis

   • Logical Design

   • Physical Design

   • Implementation

   • Maintenance and change

2. **What are the phases in the Security Systems development life cycle? Explain in detail.**

   • Investigation

   • Analysis

   • Logical Design

   • Physical Design

   • Implementation

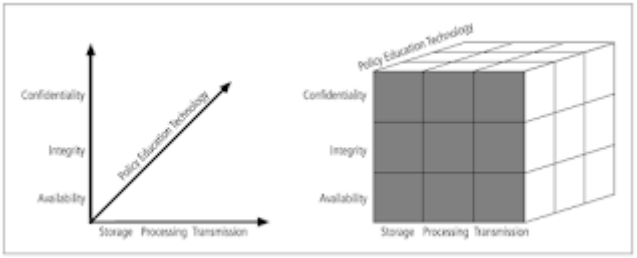
   • Maintenance and change

3. **Discuss in detail the NSTISSC security model.**

   National Security Telecommunications & Information systems security committee' document.

   It is now called **the National Training Standard for Information security professionals.**

   The NSTISSC Security Model provides a more detailed perspective on security.



4. **Explain the Components of an Information System.**
    a. Software
    b. Hardware
    c. People
    d. Data
    e. Procedures
    f. Networks
5. **Explain the functions of an Information security organization**
    a. Protects the organization's ability to function
    b. Enabling safe operation of applications
    c. Protecting data that organizations collect and use
    d. Safeguarding technology assets in organizations

UNIT II SECURITY INVESTIGATION

PART A

1. Differentiate Direct and Indirect attacks.

Direct Attack

1. It is when a hacker uses his personal computer to break into the system
2. Originate from the threat itself

Indirect Attack

1. It is when a system is compromised and used to attack other systems, such as in a distributed denial of service attack.
2. Originate from a system or resource that itself has attacked & it is malfunctioning or working under the control of a threat.

2. What is Information Security?

Information security, often shortened to infosec, is the practice, policies and principles to protect digital data and other kinds of information. infosec responsibilities include establishing a set of business processes that will protect information assets.

3. What is intellectual property?

It is the ownership of ideas and control over the tangible or virtual representation of those ideas. It is a deliberate act that exploits vulnerability.

4. 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.

5. 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.

6. What is a brute force attack?

Trying every possible combination of options of password.

7. What is a malicious code?

- This kind of attack includes the execution of viruses, worms, Trojan horses, and activeweb 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

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

- Ignorance
- Accident
- Intent

9. Differentiate Private & Public Laws.Private Laws:

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

This Law regulates the structure and administration of government agencies and theirrelationship with the citizens, employees and other governments.

- Eg: Criminal Law, Administrative Law, Constitutional Law.

10. What is social engineering?

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

PART B

1. **Explain in detail the different types of attacks.**

   An attack is an act of or action that takes advantage of a vulnerability to compromise a controlled system.

   Attack Replication Vectors

   1. IP scan & attack
   2. Web browsing
   3. Virus

2. **Explain General Computer Crime Laws.**

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

3. **Explain Ethical Concepts in Information Security.**

   a. Cultural Differences in Ethical Concepts
   b. Software License Infringement
   c. Illicit use
   d. Misuse of corporate resources

4. **Explain about Access Control Matrix in detail.**

   An access control matrix is a table that defines access permissions between specific subjects and objects. A matrix is a data structure that acts as a table lookup for the operating system.

5. **Write about different Policies in Detail.**

   - Security policies
   - Confidentiality policies
   - Integrity policies
   - Hybrid policies

UNIT III SECURITY ANALYSIS

PART A

1. What is Risk Management?

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

2. What are the types of access controls?

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

3. 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

4. What are the Risk Control Strategies?

- Avoidance – It is the risk control strategy that attempts to prevent the exploitation of thevulnerability.
- Transference – It is the control approach that attempts to shift the risk to otherassets, other processes, or other organizations.
- Mitigation – It is the control approach that attempts to reduce the impact caused by the exploitation of vulnerability through planning and preparation.
- Acceptance. – It is the choice to do nothing to protect vulnerability and to accept theoutcome of an exploited vulnerability.

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

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

6. 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

7. What are the ways to categorize the controls?

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

8. 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.

9. What is Residual Risk?

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

10. What are Policies?

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

PART B

1. Explain Risk Management in detail.

a. **Risk Identification**: It is the process of examining and documenting the security posture of an organization's information technology and the risk itfaces.
b. **Risk Assessment**: It is the documentation of the results of risk identification.
c. **Risk Control**: It is the process of applying controls to reduce the risks to an organization's data and information systems.

2. Explain Risk assessment in detail.

Assigns a risk rating or score to each Information asset. It is useful in gauging the relative risk to each vulnerable asset.

3. Explain Risk Control strategies in detail.

a. Avoidance
b. Mitigation
c. Acceptance
d. Transference

4. 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

5. Explain about Information Flow and Confinement Problem.

The confinement problem is the problem of preventing a server from leaking information that the user of the service considers confidential.

UNIT IV LOGICAL DESIGN

PART A

1. What are the types of security policies?

a. General Security Policy
b. Program Security Policy
c. Issue-Specific Policies

2. What is the commonly accepted information security Principles?

- Confidentiality
- Integrity
- Availability
- Authentication
- Authorization
- Accountability
- Privacy

3. What are the Types of Policies?

1. Enterprise information Security program Policy(EISP)
2. Issue-specific information Security Policy (ISSP)
3. Systems-specific information Security Policy (SysSP)

4. What is Information Security Blueprint?

It is the basis for the design, selection, and implementation of all security policies, education and training programs, and technological controls.

5. What is Defense in Depth?

One of the basic foundations of security architectures is the implementation of security inlayers. This layered approach is called defense in depth.

6. What do you meant by Security Perimeter?

A Security Perimeter is the first level of security that protects all internal systems from outside threats.

7. What are Honey pots?

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

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

a. Checklist
b. Structured walk-through
c. Simulation
d. Parallel
e. Full interruption

9. What are the stages in the Business Impact Analysis Step?

a. Threat attack identification
b. Business unit analysis
c. Attack success scenarios
d. Potential damage assessment
e. Subordinate plan classification

10. Who are the members of the contingency team?

a. Champion
b. Project Manager
c. Team Members.

PART B

1. Explain NIST Security Models in detail.

a. NIST Special Publication SP 800-12
b. NIST Special Publication SP 800-14
c. NIST Special Publication SP 800-18

2. Explain VISA International Security Model in detail.

- ✓ It promotes strong security measures in its business associates and has established guidelines for the security of its information systems.
- ✓ It has developed two important documents
  1. Security Assessment Process

2. Agreed Upon Procedures.

3. Explain the design of Security Architecture in detail.

a. Defense in Depth

b. Security Perimeter

c. Key Technology Components

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

a. Definitions

b. Security Program Policy(SPP)

c. Issue-Specific Security Policy(ISSP)

d. Systems-Specific Policy(SysSP)

e. ACL Policies

f. Policy Management

5. Explain about ISO 17799/BS 7799.

ISO 17799 / BS 7799 standard details the requirements for setting and implementing an Information Security Management System. BSI's globally acclaimed 'Associate Consultant' programme defines best practices to help organisations to manage their most important asset, information.

UNIT V PHYSICAL DESIGN

PART A

1. 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.

2. 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 flytraps.

3. 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.

4. What are the factors of authentication?

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

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

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

6. 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.

7. How firewalls are categorized by processing mode?

The five processing modes are

1) Packet filtering
2) Application gateways
3) Circuit gateways
4) MAC layer firewalls
5) Hybrids
6) What is PKI?

8. What is 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.

9. 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.

10. 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.

PART B

1. Explain Scanning and Analysis Tools in detail.

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

2. Explain Firewalls in detail.

- Development of Firewalls(5 generations)
- Firewall Architecture
- Packet Filtering Routers

3. Explain about secret key encryption algorithm.

- Data Encryption Standard
- Algorithm
- Sub key generation

4. Explain IDS in detail

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

5. Explain the Cryptographic algorithms in detail.

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