IS

Information Security Exam Solutions

This README contains summarized answers to various questions from past Information Security exams. These solutions cover topics like digital forensics, firewalls, intrusion detection, network security, encryption, and more. **Note**: These answers are for study purposes. Always refer to official course materials for detailed explanations.

FA 22 Terminal Examination (18/01/2023)

Q1

- **Role of Antivirus in System Security**: Antivirus software protects systems by detecting, blocking, and removing malware. Regular updates are essential to defend against new threats.
- **Steps for Digital Forensic Investigation**:
  i. Identify and secure the scene
  ii. Collect and preserve digital evidence
  iii. Analyze data for unauthorized access signs
  iv. Document findings for court use

Q2

- **Difference between IDS and IPS**:

    - IDS (Intrusion Detection System): Monitors network activity; does not block threats.
    - IPS (Intrusion Prevention System): Actively monitors and blocks identified threats.
- **Firewall Processing Modes**:
    - Packet Filtering: Filters packets based on IP and port.
    - Stateful Inspection: Tracks active connections.
    - Proxy Service: Acts as intermediary between users and internet.

Q3

- **Network Security Architecture**: Key components include firewalls, IDS/IPS, routers, and switches, with a layered structure.
- **Improving Security with Network Devices**:
    - Routers manage traffic between networks.
    - Switches segment networks, reducing broadcast traffic.

Q4

- **Authorization vs. Authentication**:
    - Authentication verifies identity (e.g., passwords).
    - Authorization grants access based on identity (e.g., roles).
- **Types of Authorization and Authentication**: Includes password-based, biometric, and multi-factor for authentication; role-based for authorization.

Q5

- **System Recovery through Backup**: Backups (full, incremental, differential) enable data restoration post-loss.
- **Physical Vulnerability Components**: Involves access control, surveillance, and secure data storage.

Q6

- **Cyber-attacks Examples**: Includes phishing, DDoS, and malware attacks.
- **Preventing Cyber-attacks**: Use firewalls, antivirus, network monitoring, and employee training.

FA 23 Terminal Examination (08/01/2024)

Q1

- **Digital Forensics in Identifying Illegal Activities**: Digital forensics examines unauthorized access, utilizing tools like disk imaging.

Q2

- **Information Security Components**: Confidentiality, integrity, and availability (CIA triad) with firewalls, IDS, and authentication systems.
- **Firewall Purpose**: Blocks unauthorized access through modes like packet filtering, proxy, and stateful inspection.

Q3

- **Pseudo Code for RSA Algorithm**:
  i. Choose primes (p) and (q).
  ii. Calculate (n = p \times q) and (\phi(n) = (p-1)(q-1)).
  iii. Select public key (e) with gcd(e, (\phi(n))) = 1.
  iv. Calculate private key (d), where (d \times e \equiv 1 \mod \phi(n)).
- **RSA Encryption Example**: Encrypt message (M = 4) using RSA and generated keys.

Q4

- **Types of Cyber-attacks**: Malware, phishing, DDoS.
- **Preventing Cyber-attacks**: Firewalls, audits, and training.

Q5

- **Presentation Topic Explanation**: Choose a relevant topic, outline requirements, and explain importance in security.

Fall 22 Mid Term (16/05/2022)

Q1

- **System Compromise by Worms and Viruses**: Worms spread autonomously, viruses need host files; both impact system performance.
- **Risk Assessment**: Identifying risks, assessing likelihood, and implementing controls.

Q2

- **Purpose of Digital Forensics**: Investigates digital evidence for unauthorized activities.

- **Hash Function in Security**: Verifies data integrity through unique hashes.

Q3

- **Define IDS and IPS with Example**: IDS detects threats (e.g., Snort); IPS blocks them (e.g., Cisco IPS).
- **Honey Pots Purpose**: Attract attackers to study attack patterns.

Q4

- **Limitations of Firewalls**: Cannot guard against internal threats; limited protection for encrypted data.
- **Cipher Text and Key Role**: Cipher text is encrypted data; keys are essential for encryption/decryption.

Q5

- **Data Encryption Standard (DES)**: Uses 16 rounds of permutations and substitutions on 64-bit blocks with a 56-bit key.

> **Disclaimer**: This is a study reference and should be cross-checked with official materials and guidelines.

Paper 1 Q.No 1 (CLO-1, PLO-1) a) Discuss the Critical Characteristics of Information.

Information should have confidentiality, integrity, and availability (CIA Triad). Other characteristics: authenticity, non-repudiation, reliability, and accuracy. b) What is the purpose of balancing security and access? Discuss with example.

To ensure that while information is protected, users can still access necessary resources. Example: In a hospital system, doctors need access to patient records, but patient data must remain confidential. Q.No 2 (CLO-2, PLO-2) a) What are Cyber-attacks? Name the most common ones with brief explanations of how these attacks are launched.

Cyber-attacks: Actions that compromise digital systems. Examples: Phishing (tricking users to reveal info), DDoS (overwhelming systems), Malware (damaging software). b) How these attacks could be prevented using defensive solutions? Suggest solutions.

Using firewalls, intrusion detection systems (IDS), and regular updates to reduce vulnerabilities. Q.No 3 (CLO-3, PLO-7) a) Discuss Network Security Architecture and its component in detail with the help of a diagram.

Components: Firewalls, IDS, IPS, VPNs, etc. A diagram can represent the layered security approach (network, application, endpoint). b) Discuss the purpose of firewall along with its different processing modes.

Firewalls block unauthorized access. Processing modes: Packet filtering, Stateful inspection, Proxy, Next-Gen Firewall. Q.No 4 (CLO-3, PLO-7) a) Write pseudo code for RSA algorithm.

Basic pseudo code:

```
Select p, q (prime numbers)
n = p * q
ϕ(n) = (p-1)*(q-1)
Select e (1 < e < ϕ(n) and gcd(e, ϕ(n)) = 1)
Calculate d (e * d ≡ 1 (mod ϕ(n)))
Public key: (e, n), Private key: (d, n)
Encrypt: C = M^e mod n, Decrypt: M = C^d mod n
```

b) Using RSA public-key encryption algorithm encrypt plaintext M=4. Use prime numbers 3 and 5 to generate the public and private keys.

- $n = 3 \times 5 = 15, \varphi(n) = (3-1)(5-1) = 8.$
- Choose $e = 3$, calculate d: $d = 3$.
- Encryption and decryption with steps shown.

Q.No 5 (CLO-4, PLO-1) Explain in detail the maintenance model of information security based on five modules/areas with Diagram.

Typical modules: Risk Management, Incident Response, Access Control, Data Protection, Compliance. Paper 2 Q.No 1 (CLO-1, PLO-2) a) Elaborate different cybersecurity laws and define the procedure for launching complaints in case of a breach.

Discuss laws like GDPR, CCPA. Procedure includes reporting to data protection authorities, filing a cybercrime report. Q.No 2 (CLO-1, PLO-4) a) Discuss the DES algorithm and its working process with step-by-step details.

Steps: Key generation, initial permutation, 16 rounds of processing, final permutation. Q.No 3 (CLO-2, PLO-7) a) Differentiate between active and passive attacks with examples related to CIA.

Active: Altering data (Integrity). Passive: Eavesdropping (Confidentiality). Q.No 4 (CLO-2, PLO-2) a) Investigate forensic techniques and devise a mechanism for securing evidence.

Techniques: Imaging, Hashing. Mechanism: Chain of custody, secure storage. Q.No 5 (CLO-3, PLO-7) a) Honey Pots working and ensuring security.

Honey Pots deceive attackers, collect intelligence on attack vectors. b) Risk assessment and mitigation strategies.

Risk identification, analysis, prioritization. Mitigation: Avoidance, reduction, transference, acceptance. Paper 3 Q.No 1 (CLO-3, PLO-7) a) How Honey Pot creates a parallel system for attack detection.

Discusses the decoy setup and its use in monitoring attackers' behavior. Q.No 2 (CLO-3, PLO-7) a) Define IDS and IPS systems with examples.

IDS: Detects threats, e.g., Snort. IPS: Prevents attacks, e.g., Cisco’s IPS solutions. Q.No 3 (CLO-1, PLO-1) a) Differentiate between worms and viruses with examples.

Worms spread independently; viruses attach to files. Example: Worm - WannaCry, Virus - ILOVEYOU. No. 4 (CLO-1, PLO-1) a) Define risk assessment and discuss mitigation strategies.

Identify, analyze, and manage potential risks. No. 5 (CLO-3, PLO-7) a) Cybersecurity laws for information protection with reference to national and international standards. Here’s a concise overview of GDPR, HIPAA, and national data protection laws:

1. GDPR (General Data Protection Regulation) Scope: EU law protecting personal data of EU citizens, applying worldwide to companies processing EU data. Key Points: Requires explicit consent, grants rights like data access and erasure, mandates data breach notifications within 72 hours, and enforces strict fines (up to 4% of global revenue). Impact: Inspired similar data privacy laws worldwide, setting a global standard.

2. HIPAA (Health Insurance Portability and Accountability Act) Scope: U.S. law protecting health information handled by healthcare entities and their associates. Key Rules: Privacy Rule: Protects health data privacy. Security Rule: Safeguards electronic health data. Breach Notification: Requires notification of data breaches. Penalties: Fines up to $1.5 million for repeat violations, with criminal penalties possible for severe cases.

3. National Data Protection and Cybercrime Laws United States: CCPA grants California residents data rights; CFAA and COPPA address cybercrime and children’s data. Pakistan: PECA criminalizes cybercrimes; Personal Data Protection Bill (proposed) would provide privacy protections. India: PDPB (proposed) is GDPR-inspired, with IT Act covering cybersecurity. China: PIPL enforces strict data privacy, data localization, and user rights.

Global Impact These laws collectively aim to protect privacy, enhance cybersecurity, and set data handling standards, fostering greater trust and transparency in data usage globally.