Unit-wise Question Bank – Introduction to Cyber Security

UNIT – I: Information Security Fundamentals & Best Practices

Part-A (2 Marks – Short Answer)

1. Define Information Security.
2. What is meant by "Compromised Computer"?
3. List two safe internet usage practices.
4. Write the importance of securing computer networks.
5. Give two examples of secure communication methods.
6. Define Privacy Guidelines.
7. What is the main purpose of network security?
8. State any two information security best practices.

Part-B (12 Marks – Long Answer)

1. Explain different types of cyber threats to personal computers and networks.
2. Discuss "Information Security Best Practices" in detail.
3. Explain privacy guidelines with real-time examples.
4. Describe the process of securing computer networks.
5. Explain "Safe Internet Usage" in detail.
6. Write about secure communication protocols with examples.
7. Explain the importance of protecting your computer and its contents.
8. Discuss basics of networking relevant to cyber security.

UNIT – II: Ethics in Cyber Security & Cyber Law

Part-A (2 Marks – Short Answer)

1. Define Cyber Law.
2. What is meant by "Fair Use" in cyber security?
3. Define Intellectual Property.
4. Give an example of a cybercrime.
5. What is Ethical Hacking?
6. Mention any two types of electronic evidence.
7. Define Freedom of Speech in the context of cyber space.

8. List two types of internet fraud.

Part-B (12 Marks – Long Answer)

1. Discuss privacy and intellectual property in cyber security.
2. Explain professional ethics in cyber security with examples.
3. Write about trademarks and their importance in cyber law.
4. Describe various types of internet fraud with examples.
5. Explain cybercrimes and their classification.
6. Discuss the role of cyber laws in India.
7. Explain the concept of electronic evidence and its legal value.
8. Discuss ethical hacking and its types.

UNIT – III: Penetration Testing

Part-A (2 Marks – Short Answer)

1. Define penetration testing.
2. List any two types of penetration testing.
3. What is meant by web application test scope?
4. Define vulnerability in cyber security.
5. Name two web architectures.
6. What is the main goal of penetration testing?
7. Define client in web context.
8. Define server in web context.

Part-B (12 Marks – Long Answer)

1. Explain the different types of penetration testing.
2. Discuss the process of defining a web application test scope.
3. Describe the various types of vulnerabilities in web applications.
4. Explain different types of web architectures.
5. Discuss the role of servers and clients from a penetration tester’s perspective.
6. Explain steps involved in a penetration testing process.
7. Write about tools used for penetration testing.
8. Discuss security issues identified during penetration testing.

UNIT – IV: Web Application Security & Forensics

Part-A (2 Marks – Short Answer)

1. What is SQL Injection?
2. Expand XSS and explain briefly.
3. What is CSRF?
4. Define Session Hijacking.
5. What is the purpose of CAPTCHA?
6. Mention any two forensic technologies.
7. Define Audit Trails.
8. Give an example of outsider threat.

Part-B (12 Marks – Long Answer)

1. Explain SQL Injection, XSS, and CSRF with examples.
2. Describe password vulnerabilities and prevention techniques.
3. Explain the concept of SSL and its importance.
4. Discuss Local and Remote File Inclusion attacks.
5. Explain the process of collecting digital evidence.
6. Describe evidentiary reporting in forensics.
7. Discuss layered defense strategy in network security.
8. Explain outsider threat protection methods.

UNIT – V: Risk Management & Incident Response

Part-A (2 Marks – Short Answer)

1. Define Asset Evaluation.
2. What is Risk Identification?
3. Expand CIA in cyber security.
4. What is Risk Quantification?
5. Define Business Continuity.
6. Name any two forensic tools.
7. Define Incident Detection.
8. What is meant by Proactive Cyber Service?

Part-B (12 Marks – Long Answer)

1. Explain asset evaluation and business impact analysis.
2. Describe risk identification and risk quantification methods.
3. Explain the phases of incident response: preparation, detection, containment, eradication, recovery.
4. Discuss the CIA triangle and its significance.
5. Write about security policy and compliance.
6. Describe the use of forensic tools FTK and EnCase in investigation.
7. Discuss proactive and post-incident cyber services.
8. Explain cyber incident analysis and response.