Cyber Security (PEC-IT702F) – Important Questions & Key Topics

■ Top 10 Most Important Questions (with Hints)

- 1. Explain the phases of Cyber Forensics investigation.
  Hint: Identification, Preservation, Collection, Examination, Analysis, Presentation.

- 2. Discuss the Ethical Hacking life cycle in detail.
  Hint: Reconnaissance, Scanning, Gaining Access, Maintaining Access, Covering Tracks.

- 3. What are different types of hackers and cyber crimes?
  Hint: White/Black/Grey Hat, Cyber terrorism, Cyber stalking, Phishing, Fraud.

- 4. Define and explain the CIA Triad.
  Hint: Confidentiality, Integrity, Availability – core pillars of security.

- 5. Explain Vulnerability Assessment and Penetration Testing (VAPT).
  Hint: Identify weaknesses, exploit them safely, report findings.

- 6. Discuss Social Engineering attacks and prevention measures.
  Hint: Phishing, Pretexting, Baiting, Tailgating; use awareness and training.

- 7. What are malware threats? Explain types of malicious software.
  Hint: Virus, Worms, Trojan horse, Ransomware, Spyware.

- 8. Write short notes on IT Act 2000 and Cyber Ethics.
  Hint: Legal framework for e-governance, cybercrime prevention, and digital signatures.

- 9. Explain Information Security Management and ISO 27001.
  Hint: Framework for managing information risks via ISMS policies and controls.

- 10. Describe the Computer Forensics process and tools.
  Hint: Tools – EnCase, FTK, Autopsy; Process – Acquisition, Analysis, Reporting.

■ Study Priority (Focus Order)

- 1■■ Unit 4 – Cyber Forensics & Auditing (Highest marks weightage)
- 2■■ Unit 3 – Ethical Hacking & Security Engineering
- 3■■ Unit 2 – Hackers and Cyber Crimes
- 4■■ Unit 5 – Cyber Ethics & Laws
- 5■■ Unit 1 – Introduction to Cyber Security

■ Quick 4-Week Revision Plan

- Week 1 – Unit 4: Forensics + Audit + ISO concepts
- Week 2 – Unit 3: Ethical Hacking phases + Security engineering
- Week 3 – Unit 2 + Unit 1: Malware + Hacker types + CIA Triad
- Week 4 – Unit 5 + Full Revision: IT Act + Cyber laws + Recap all