Cyber Security — PEC-IT702F

Course: Cyber Security (PEC-IT702F) — B.Tech IT — Semester VII

Goal: Simple, clear, and complete notes covering Units 1 to 5. Each topic is explained in plain language, with examples, diagrams described in words (so you can sketch them), common attacks, defenses, and short/long questions for revision.

Quick study tips before we start

- Read one unit at a time and *summarize* each section in 2–3 lines in your own words.
- Make flashcards for key terms (CIA triad, malware types, reconnaissance, phishing, etc.).
- Practice explaining concepts aloud — teaching helps retention.
- For commands/tools, practice on a safe lab (VM) if you can.

Unit 1 — Introduction to Cyber Security (6 hours)

1.1 What is Cyber Security?

Cyber Security means protecting computers, networks, programs, and data from theft, damage, or unauthorized access. It covers both technical measures (firewalls, encryption) and human/organizational measures (policies, training).

Example: If your bank uses encryption and login controls to protect accounts, that is cyber security.

1.2 Why Cyber Security matters

- **Personal:** Protects your photos, passwords, money.
- **Business:** Prevents financial loss and loss of customer trust.
- **Nation:** Keeps critical services (power, hospitals, banking) safe.

1.3 Cyberspace

A term for the electronic environment where digital communication occurs — internet, cloud, email, local networks. Think of it as a virtual country with roads (networks) and buildings (servers).

1.4 Cyber threats and actors

- **Threats:** Actions that can harm systems (malware, phishing, DDoS).
- **Actors:** People or groups behind threats — script kiddies, cybercriminals, hacktivists, nation-state attackers.

1.5 Cyberwarfare and cyber terrorism

- **Cyberwarfare:** State-sponsored operations that target another state's systems for strategic objectives (espionage, disruption).
- **Cyber terrorism:** Use of cyber-attacks to spread fear or cause physical harm (e.g., targeting hospital systems).

1.6 CIA Triad — the foundation

- **Confidentiality:** Only authorized users can access the data.
- Methods: passwords, encryption, access control lists (ACLs).
- **Integrity:** Data is accurate and unaltered.
- Methods: checksums, digital signatures, version control.
- **Availability:** Data/systems are accessible when needed.
- Methods: redundancy, backups, disaster recovery.

Sketch idea: Draw a triangle with C, I, A at the corners — write controls that support each corner.

1.7 Cybersecurity of critical infrastructure

Critical infrastructure includes power grids, water, hospitals, transport, finance. Attacks here can cause real-world damage.

Defenses include: network segmentation, strict access controls, real-time monitoring, and incident response plans.

1.8 Organizational implications

Organizations must create policies, incident response teams, perform risk assessments, and educate staff. Security is not only technical — it's also people and processes.

Unit 2 — Hackers and Cyber Crimes (7 hours)

2.1 Who is a hacker? Types explained simply

- **White Hat:** Ethical hackers who test systems to find fixes.
- **Black Hat:** Criminal hackers who exploit systems for gain.
- **Grey Hat:** Between white and black — may hack without permission but not for profit.
- **Script Kiddie:** Beginner using others' tools.
- **Hacktivist:** Hacker with political/social motives.

2.2 Hackers vs Crackers

- **Hacker (general):** Someone skilled with systems; connotation varies.
- **Cracker:** Specifically someone who breaks security to cause harm.

2.3 Anatomy of a cyber-attack (simplified)

1. **Reconnaissance:** Gather information about target.
2. **Scanning:** Check for open ports and services.
3. **Gaining access:** Exploit vulnerabilities.
4. **Maintaining access:** Install backdoors or accounts.
5. **Covering tracks:** Delete logs or use proxies.

This is the typical flow followed by both pentesters and attackers.

2.4 Malware: types and behavior

- **Virus:** Needs a host file; infects files and spreads when files are shared.
- **Worm:** Self-replicates across networks without user action.
- **Trojan Horse:** Disguises as legitimate software but performs malicious tasks.
- **Backdoor:** Hidden entry that bypasses normal authentication.
- **Ransomware:** Encrypts user data and demands payment.
- **Spyware/Keylogger:** Records user activity to steal credentials.

Example scenario: A user opens a downloaded file (Trojan). The Trojan installs ransomware that encrypts files and demands Bitcoin.

2.5 Sniffing and Man-in-the-Middle (MitM)

- **Sniffing:** Passive capture of network traffic using tools like Wireshark.
- **MitM:** Attacker intercepts and possibly alters communication (e.g., a fake Wi-Fi hotspot).

Protection: Use strong encryption (HTTPS, TLS), VPNs, and avoid untrusted networks.

2.6 Gaining access and privilege escalation

- **Initial access:** Could be through stolen credentials, unpatched services, or phishing.
- **Privilege escalation:** After initial access, attackers find ways to gain higher privileges (e.g., from user to admin) to control more of the system.

Mitigation: Least privilege principle, regular patching, and monitoring for unusual behavior.

2.7 Hiding files and covering tracks

Attackers may hide files (rootkits) or delete logs. Digital forensics later tries to recover evidence.

2.8 Worms, Trojans, viruses, backdoors in detail

- **Worm Details:** Propagate quickly across a vulnerable service (e.g., SMB vulnerability exploited by WannaCry).
- **Trojan Details:** Often rely on social engineering to get installed.

Case study: Brief mention of WannaCry (ransomware worm in 2017) — it leveraged a Windows SMB vulnerability and caused wide disruption.

Unit 3 — Ethical Hacking and Social Engineering (8 hours)

3.1 Ethical Hacking: definition and scope

Ethical hacking (also called penetration testing) is legally testing systems to find weaknesses. Scope must be agreed in writing before testing.

Why it's useful: Fix weaknesses before criminals use them.

3.2 Ethical hacking process (phases)

1. **Planning and Reconnaissance** — Identify targets and permitted actions.
2. **Scanning** — Use tools to map services and find vulnerabilities.
3. **Gaining Access** — Exploit vulnerabilities (only within agreed scope).
4. **Maintaining Access** — Check if persistent access is possible (to test long-term risk).
5. **Analysis and Reporting** — Provide clear, prioritized fixes for the owner.

Tools used: Nmap (scanning), Metasploit (exploits), Burp Suite (web testing), Nikto (web server scanning).

3.3 Threat modelling

Threat modelling is a structured way to identify assets, threats, and controls. - **Steps:** Identify assets → draw attack surface → identify threats → prioritize and plan controls.

Use simple templates: STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege).

3.4 Vulnerability assessment vs Penetration testing

- **Vulnerability Assessment (VA):** Automated scanning that lists potential issues.
- **Penetration Test (pentest):** Exploitation attempts to show real-world impact.

Both are important: VA finds many issues, pentest proves which are dangerous.

3.5 Types of penetration testing

- **Black box:** Tester knows nothing beforehand.
- **White box:** Tester has full system details.
- **Grey box:** Tester has limited knowledge (like a real insider).

3.6 Social engineering: how attackers exploit people

Social engineering tricks people rather than systems. Common methods: - **Phishing:** Scam emails asking for credentials. - **Spear phishing:** Targeted phishing at specific people. - **Pretexting:** Fake identity to build

trust. - **Baiting:** Promise of free content to lure victims. - **Tailgating:** Physically following someone into secure places.

Real life tip: Always verify identity by calling an official number and think twice before clicking links.

3.7 Insider threats

An insider is someone within the organization who misuses access. They can be malicious or careless.

Prevention: Background checks, monitoring, separation of duties, and behavior analytics.

3.8 Preventing social engineering and insider attacks

- **User training and awareness** (most effective).
- **Two-factor authentication (2FA).**
- **Data classification and least privilege.**
- **Monitoring and logging.**

Unit 4 — Cyber Forensics and Auditing (10 hours)

4.1 What is Cyber Forensics?

Cyber forensics is the process of collecting, preserving, analyzing, and presenting digital evidence in a way that is acceptable in legal proceedings.

Difference from incident response: Incident response focuses on restoring systems and stopping ongoing attacks; forensics focuses on evidence collection for prosecution and learning.

4.2 Computer equipment and storage media

Understand common storage and how data persists: - **Hard drives (HDD/SSD)** — files, deleted file recovery. - **Removable media** — USB drives. - **Mobile devices** — call logs, SMS, app data. - **Cloud storage** — logs and copies stored by providers.

4.3 Role of the forensic investigator

A forensic investigator must: - Work methodically to avoid altering evidence. - Follow legal chain-of-custody procedures. - Use tools to image (duplicate) data and analyze it.

4.4 Forensic investigation process (step-by-step)

1. **Preparation:** Understand laws and get legal permissions.
2. **Identification:** Identify potential evidence sources.
3. **Collection:** Create bit-for-bit images of drives and capture volatile data (RAM) if needed.
4. **Preservation:** Store images securely and log the chain of custody.

5. **Examination:** Use tools to recover deleted files, read logs, and extract artifacts.
6. **Analysis:** Correlate evidence to build timeline and find the cause.
7. **Presentation:** Write clear reports and prepare for testimony if needed.

Tools: Autopsy, Sleuth Kit, EnCase (commercial), FTK, Volatility (for memory analysis).

4.5 Collecting network-based evidence

Network evidence includes packet captures (pcap files), firewall logs, web server logs, and authentication logs.

How to capture: Use tcpdump or Wireshark in a safe place; preserve timestamps and metadata.

4.6 Writing computer forensics reports

Reports should be clear, factual, and explain technical findings in plain English. Include: - Scope and objectives. - Methodology (how data was collected). - Findings with timestamps and evidence IDs. - Conclusions and recommended actions.

4.7 Auditing and information security management

Auditing: Regular checks (manual and automated) to ensure policies and controls are in place and working.

Information Security Management System (ISMS): A framework (policies, procedures, and controls) to manage security systematically.

4.8 ISO 27001:2013 (intro)

ISO 27001 is an international standard for ISMS. Key ideas: - Risk assessment and treatment. - Management support and continual improvement. - Controls for access, physical security, operations, and business continuity.

Note: Remember the plan-do-check-act (PDCA) model: Plan (policy), Do (implement), Check (audit), Act (improve).

Unit 5 — Cyber Ethics and Laws (7 hours)

5.1 Cyber ethics

Cyber ethics are moral guidelines for using computers and the internet responsibly: respect privacy, avoid piracy, don’t spread malware, and follow laws.

5.2 E-Commerce and E-Governance

- **E-Commerce:** Buying/selling online — needs secure payment systems and trust.

- **E-Governance:** Government services online — requires data protection and reliable systems.

5.3 Certifying Authority and Controller

- **Certifying Authority (CA):** Issues digital certificates to verify identities (used in HTTPS and digital signatures).
- **Controller:** In some legal frameworks, a supervisory entity for certification and regulation.

5.4 Offences under the Information Technology Act (IT Act) — India (high-level)

Key offences often covered (simplified): - **Hacking and unauthorized access.** - **Identity theft and impersonation.** - **Publishing obscene material online.** - **Cyber terrorism and threats.** - **Cheating by personation through a computer resource.**

Penalties: Fines and imprisonment depending on severity. (Always refer to the Act for exact sections and penalties.)

5.5 Computer offences and penalties (examples)

- Unauthorized access to a computer system — may attract imprisonment and fines.
- Tampering with source code — serious offence.
- Breach of privacy and data theft — civil and criminal consequences.

5.6 Intellectual Property Rights (IPR) in cyberspace

Protects creations like software, databases, and websites. Includes: - **Copyright** (code, web content), - **Patents** (inventions), - **Trademarks** (brand names), - **Trade secrets** (confidential business info).

5.7 Network Layer: IPSec (brief introduction)

IPSec provides security at the IP layer — it offers encryption, authentication and integrity for IP packets. - Two main modes: **Transport** (protects payload) and **Tunnel** (protects whole IP packet). - Components: **AH (Authentication Header)** and **ESP (Encapsulating Security Payload)**.

Use: Secure VPN connections.

Revision Section — Key Points to Memorize

- CIA Triad: Confidentiality, Integrity, Availability.
- Malware types: Virus, Worm, Trojan, Ransomware, Spyware.
- Phases of an attack and phases of ethical hacking.
- Social engineering techniques: Phishing, Pretexting, Baiting, Tailgating.
- Forensics steps: Identification → Collection → Preservation → Analysis → Reporting.
- ISO 27001 basic idea and PDCA model.
- Basic Indian IT Act offences (know examples rather than memorizing sections unless required).

Practice Questions (Important) — mix of short and long (good for last-minute revision)

1. Define Cyber Security and explain the CIA Triad. (Long)
2. Explain the difference between a virus, worm, and Trojan with one example each. (Short)
3. What is social engineering? Describe two common social engineering attacks and how to defend against them. (Long)
4. What is a penetration test? Explain its phases.
5. Describe the cyber forensics process and list three tools used in forensics. (Short)
6. Explain what ISO 27001 is and why organizations use it. (Short)
7. Define ransomware and explain how an organization should respond to a ransomware attack. (Long)
8. What is privilege escalation and what controls can prevent it? (Short)
9. Explain what a Certifying Authority (CA) does. (Short)
10. Describe how sniffing works and how TLS/HTTPS protect against it. (Long)

Sample Answers — Brief and Clear (for quick last-minute study)

Q1 (short): *Define Cyber Security and explain the CIA Triad.* - Cyber Security protects digital assets from threats. CIA: Confidentiality (privacy), Integrity (correctness), Availability (accessibility).

Q2 (short): *Difference between virus, worm, Trojan.* - Virus: attaches to files — spreads when files shared. Worm: self-replicates over networks. Trojan: hides as legitimate program to trick users.

Q3 (long): *Social engineering — attacks and defense.* - Attacks: Phishing (fake emails) and Pretexting (fake identity). Defense: employee training, verification steps, 2FA, don't click unknown links.

Q4 (short): *What is a penetration test?* — Legal tests to find exploitable vulnerabilities, usually in phases: recon, scan, exploit, maintain, report.

Short glossary (one-line definitions)

- **Exploit:** Code or technique that takes advantage of a vulnerability.
- **Zero-day:** Vulnerability unknown to defenders and unpatched.
- **Patch:** Software update that fixes bugs or vulnerabilities.
- **Firewall:** Device or software that controls incoming/outgoing network traffic.
- **IDS/IPS:** Intrusion Detection/Prevention Systems — detect and block attacks.

How to use these notes in the next 24 hours

1. Read a unit and summarize it in your own words (15–20 minutes per unit).
2. Solve the practice questions above (30–40 minutes).
3. Memorize the glossary and CIA triad (15 minutes).
4. Rest well — sleep helps memory consolidation.

If you want, I can now: - Convert this document into a printable PDF or share it as a study sheet. - Create 30 mock MCQs and short-answer questions for quick practice. - Quiz you interactively on any unit.

Tell me which one you prefer next.

UNIT 5: CYBER ETHICS AND LAWS

5.1 Introduction to Cyber Laws

Cyber laws are the rules and regulations that control how people use computers, the internet, and digital data. They help protect users from misuse, fraud, identity theft, and online crimes. Without cyber laws, it would be difficult to punish criminals who commit crimes using computers.

5.2 E-Commerce and E-Governance

E-Commerce refers to buying and selling products or services online. It includes online shopping, digital payments, and online banking. Cyber laws make sure online transactions are safe and protect consumers from fraud.

E-Governance means delivering government services through digital platforms. Examples include online tax filing, Aadhaar services, and digital certificates. Cyber laws ensure protection of citizens' data and prevent misuse of government systems.

5.3 Certifying Authority (CA) and Controller

A **Certifying Authority (CA)** issues **Digital Certificates** used for verifying identity during online transactions. Examples include eMudhra and NIC.

The **Controller of Certifying Authorities (CCA)** regulates all CAs in India and ensures they follow proper security guidelines.

5.4 Offences under IT Act 2000

The **Information Technology Act 2000** is India's main cyber law. It covers offences such as: - Unauthorized access or hacking - Identity theft - Data theft - Damage to computer systems - Publishing obscene or harmful content online - Cyber harassment and stalking

5.5 Penalties under IT Act 2000

Different penalties include: - Fines (₹1 lakh to several crores depending on the offence) - Imprisonment (up to 3 years or more) - Compensation to victims

The Act was amended in 2008 to include new crimes like cyber terrorism and identity theft.

5.6 Intellectual Property Rights (IPR) in Cyberspace

IPR protects creations of the mind, such as: - Software programs - Digital content - Music, videos, books - Website designs

IPR laws ensure that creators receive credit and financial benefit from their work. Online piracy, illegal downloads, and unauthorized copying violate IPR.

5.7 IPSec at Network Layer

IPSec (Internet Protocol Security) is a security protocol used to protect data travelling across networks, especially in VPNs.

IPSec provides: - **Confidentiality** – Data is encrypted. - **Integrity** – Data is not altered during transfer. - **Authentication** – Confirms sender identity.

IPSec uses two main modes: - **Transport Mode** – Protects only the message data. - **Tunnel Mode** – Protects the entire IP packet. Useful for secure VPN connections.

Summary of Unit 5

- Cyber laws prevent online crimes and protect digital transactions.
- Digital certificates verify user identity.
- IT Act 2000 defines cyber offences and penalties.
- IPR protects digital creations.
- IPSec ensures secure communication at the network layer.