Cyber Security — Question Bank: Answer Key (Revised)

Semester: 5 • AY 2025–26 • Course Code: 1010043362

Note: Responses are sized to marks, aligned to CO tags, and mirror the exact numbering from the provided question bank.

Unit 1: Introduction to Cyber Crime

Q1 (3M, CO-1, R): What is Cyber Crime? Write down its type.

- Cyber crime: unlawful acts using computers, networks, or data as tool/target/place.
- **Against individuals:** identity theft, cyberstalking, online harassment.
- **Against property:** data theft, ransomware, IP infringement.
- **Against organizations/state:** DDoS, espionage, critical-infrastructure attacks.

Q2 (4M, CO-1, R): Define Cyber Space and Cyber Security.

- **Cyberspace:** interconnected digital environment of networks, devices, software, and data.
- **Cyber security:** protection of systems/networks/data via policies, processes, and technologies to ensure CIA.
- Covers governance, technical controls (auth, encryption, monitoring), and human factors (awareness).
- Enables business continuity and risk reduction.

Q3 (3M, CO-1, R): Who are Cyber Criminals? Classify cyber crimes.

- **Actors:** script kiddies, black/white/gray hats, insiders, organized crime, hacktivists, state/APT.
- **Classes:** against person, property, organization/state (as in Q1).
- Motives: profit, ideology, espionage, challenge.

Q4 (4M, CO-1, U): Explain: Vulnerability, Threat, Exploit, Attack.

- **Vulnerability:** weakness (e.g., default creds).
- **Threat:** potential cause of harm (e.g., ransomware gang).
- **Exploit:** method/code abusing a vulnerability (SQLi payload).
- **Attack:** execution of a threat breaching CIA (DDoS).

Q5 (3M, CO-1, R): What is Attack? Explain in brief.

- Compromise of CIA by abusing vulnerabilities.
- Examples: brute-force login; DDoS; privilege escalation.

Q6 (8M, CO-1, R): What is Hacking?

- Discovery/exploitation of weaknesses for unauthorized access or manipulation.
- Ethical vs malicious based on authorization/intent.
- Goals: data theft, disruption, testing, prestige.
- Tools: scanners, exploit frameworks, crackers, social engineering.

Q7 (8M, CO-1, U): Explain types of Hacker.

Black-hat; **White-hat**; **Gray-hat**; **Script kiddies**; **Hacktivists**; **Insiders**; **State/APT**; **Cybercriminal groups**.

Q8 (8M, CO-1, U): Phases of Hacking.

Recon → Scanning/Enumeration → Exploitation → PrivEsc/Lateral Movement → Persistence → Cover tracks → Exfiltration/Impact → (Ethical) Reporting.

Q9 (3M, CO-1, R): What is Vulnerability? Give small example.

- Weakness exploitable by an attacker.
- Example: outdated CMS enabling SQLi to dump users.

Q10 (3M, CO-1, R): Define Cybercrime and Information Security.

- Cybercrime: unlawful acts using digital means.
- InfoSec: safeguarding information assets to ensure CIA via controls/governance.

Q11 (6M, CO-1, R/U): What is an active attack? Explain any two.

- Active attacks modify/interrupt operations or data.
- **MitM:** intercept & alter traffic (ARP spoof).
- **SQLi:** modifies queries to read/alter DB; bypass auth.

Q12 (6M, CO-1, R/U): What is a passive attack? Explain any two.

- Passive attacks eavesdrop without changing data.
- **Traffic analysis** and **password sniffing** on unencrypted channels.

Q13 (6M, CO-1, R/U): What is hacking? Discuss phases of hacking.

Definition as above; phases: Recon → Scanning → Exploit → PrivEsc → Persistence → Cover tracks.

Unit 2: Basics of Cyber Attacks

Q1 (3M, CO-2, R): What is malware? Types of malwares.

- Malware: software built to disrupt/spy/extort/control.
- Types: virus, worm, trojan, ransomware, spyware/adware, rootkit, bot, keylogger, wiper.

Q2 (4M, CO-2, R): How keylogger and spyware works?

- Keyloggers hook keystrokes; exfiltrate logs.
- Spyware monitors activity (browser, clipboard, mic/cam).
- Delivery: phishing/drive-by/pirated bundles.
- Mitigation: EDR, patching, awareness, least privilege.

Q3 (3M, CO-2, U): Difference between Virus and Worms.

- Virus needs host; spreads when host runs.
- Worm self-replicates via network vulns; faster spread.
- Impact: worms cause network congestion.

Q4 (4M, CO-2, R): What is Proxy Server?

- Intermediary to forward requests; caches/filters/logs/authenticates.
- Privacy, performance, and control benefits.

Q5 (4M, CO-2, R): What is Trojan and backdoors?

- Trojan masquerades as legit app; drops payload.
- Backdoor bypasses auth; enables remote control/data theft.

Q6 (3M, CO-2, U): Explain term Anonymizers.

- Services that hide identity/IP by relays (e.g., Tor); break linkability.

Q7 (3M, CO-2, U): Explain: Cyber Defamation, Software Piracy, Computer Sabotage.

- Cyber defamation harms reputation with false online statements.
- Software piracy: unauthorized copying/use.
- Computer sabotage: intentional system/data damage.

Q8 (6M, CO-2, R): What is malware? Explain types of malwares.

- As in Q1, with brief functions: infect, auto-spread, disguise, encrypt, spy, hide, botnet, log keys, wipe.

Q9 (4M, CO-2, A): Prevent viruses/worms spread in LAN.

- Patch & scan; disable SMBv1.
- Endpoint protection/EDR; allow-listing; disable macros.
- Segmentation; least privilege; restrict lateral movement.
- Filter email/web; backups; IR runbooks.

Q10 (6M, CO-2, R): What is cyber defamation? Give one example.

- False online statements that harm reputation.
- Example: fabricated allegation campaign on social media.

Q11 (3M, CO-2, R): What is buffer overflow? Give one example.

- Bounds overflow overwrites memory/control flow.
- Example: unsafe gets() enabling return-address overwrite.

Q12 (6M, CO-2, R/U): Role of Proxy Servers & Anonymizers in Phishing.

- Attacker reverse-proxy captures credentials.
- Defender proxy blocks known domains; analysts use sandbox/anonymizer.
- SPF/DKIM/DMARC; MFA; awareness.

Unit 3: Various Cyber Attacks

Q1 (2M, CO-2, U): Brief example of Email Spoofing.

- Forged ‘From’ as admin@company.com asking reset via malicious link.

Q2 (3M, CO-2, U): Explain any three terms.

- Salami attack (skimming cents).
- Data diddling (altering inputs).
- Email bombing (mass flood).

Q3 (3M, CO-2, R): Social Engineering and its types?

- Phishing/spear-phishing, vishing, smishing, baiting, pretexting, tailgating, quid-pro-quo.

Q4 (4M, CO-2, U): Botnet and Architecture.

- Bots + C2; centralized/P2P/fast-flux; C2 distributes commands/updates; used for spam/DDoS.

Q5 (3M, CO-2, R): DoS — how it works?

- Resource exhaustion (SYN/HTTP flood); unavailability for legit users.

Q6 (3M, CO-2, U): DDoS Attacks.

- Distributed flooding, amplification, hard to block; needs upstream/CDN scrubbing.

Q7 (3M, CO-2, U): SQL Injection.

- Unsanitized input alters queries; fix with prepared statements, least-priv DB, WAF.

Q8 (6M, CO-2, U): Email spoofing — working + example.

- SMTP lacks auth; headers forged/typosquat domains.
- Use SPF/DKIM/DMARC.
- Example: ceo@compnay.com demands urgent transfer.

Q9 (3M, CO-2, R): Forgery & documents.

- Definition + examples: IDs, passports, certificates, cheques, invoices, bank statements, e■tickets, digital signatures.

Q10 (4M, CO-2, U): Credit card fraud & misuse.

- Skimming, phishing, POS malware, breaches, lost/stolen cards; used for purchases/cash advances.

Q11 (6M, CO-2, A): Botnet C&C; coordinating spam.

- C2 sends templates/targets; rotates infrastructure; feedback loops tune campaigns.

Q12 (4M, CO-2, U): Phishing — how it works.

- Impersonation + lure → fake site → credential harvest/malware; mitigate with MFA/awareness/filters.

Q13 (4M, CO-2, U): DoS vs DDoS.

- Origin (single vs distributed); scale; mitigation differences.

Q14 (6M, CO-2, A): SQLi on login form.

- Concatenated query; payload ' OR '1'='1; prevention as above.

Q15 (6M, CO-2, A): Unsecured Wi■Fi password sniffing & protections.

- Capture plaintext on open/WEP; MitM via ARP spoof.
- Use HTTPS/VPN/WPA3/client isolation/MFA.

Unit 4: Understanding Digital Forensics and Cyber Law

Q1 (5M, CO-3, R): Cyber Crime & types.

- Definition; types across person/property/org-state with examples.

Q2 (3M, CO-3, U): Need for digital forensic labs.

- Admissible evidence handling; specialized tools; chain of custody.

Q3 (7M, CO-3, R): Cybercrime investigator.

- Collect/preserve/analyze evidence; correlate logs; report/testify; legal procedures; tools; skills; outcome.

Q4 (4M, CO-3, U): Digital Evidence & rules.

- Probative data types; principles: legality, integrity, authenticity, relevance, reliability, chain of custody.

Q5 (5M, CO-3, U): Digital Forensic Life Cycle.

- Preparation → Identification → Preservation → Collection → Examination/Analysis → Documentation → Presentation → Review.

Q6 (0.5M, CO-3, U): Why IT Act 2000?

- E-records/signature recognition; offences; penalties; procedures.

Q7 (4M, CO-3, U): IT Act 2008 Amendments.

- 66C/66D/66F; Sec 79 intermediary due diligence; increased penalties.

Q8 (6M, CO-3, U/A): IT Act 2000 — Section 66A.

- 66A struck down in 2015 (*Shreya Singhal*); earlier penalized 'offensive' messages.

Q9 (3M, CO-3, U): Sections & rules list.

- Sec 43, 65, 66, 66C, 66D, 66E, 66F, 67, 67A, 67B, 69, 70, 72, 79.

Q10 (4M, CO-3, U): Incident Response Lifecycle.

- Preparation → Detection/Analysis → Containment → Eradication → Recovery → Post-incident review.

Unit 5: Introduction to Network Defense

Q1 (4M, CO-4, R): Firewall & need.

- Policy enforcement between zones; reduces attack surface; segmentation; monitoring.

Q2 (4M, CO-4, U): How firewalls protect.

- ACLs/stateful inspection; NAT; protocol/app filtering; IDS/IPS; logging; zone policies.

Q3 (4M, CO-4, U): Stateless vs Stateful.

- Per-packet vs session-aware; speed vs context/security.

Q4 (4M, CO-4, U): Packet Filter vs Firewall.

- Packet filter is a basic firewall subset; ‘firewall’ includes stateful/app/next■gen features.

Q5 (4M, CO-4, U): NAT.

- Maps private→public; static/dynamic/PAT; masks internal hosts; side effect: breaks end■to■end.

— End of Revised Answer Key —