FREE EDITION · NOTES + 3 SAMPLE MCQS

CUET · COMPUTER SCIENCE · CLASS XII · CODE 308

Security Aspects

CUET unit: Security Aspects (Network Security, Malware, Cyber Threats and Prevention)

By **UniDrill** · NCERT-grounded study material

WWW.UNIDRILL.IN

UniDrill

📌 Snapshot

- The foundational concepts of network security: connected systems are inherently vulnerable, and they face a range of threats.
- Major categories of malware (Virus, Worm, Ransomware, Trojan, Spyware, Adware, Keylogger) have precise technical distinctions that NTA tests heavily.
- Protective technologies — antivirus detection methods, firewalls, HTTPS, and cookies — go deep enough for application-level MCQs.
- Hackers are classified into White Hat, Black Hat, and Grey Hat types, a favourite NTA distinction question.
- Network security threats (DoS, DDoS, Intrusion, Snooping, Eavesdropping) are covered in Section 12.9, rounding out all angles of threat and defence that CUET tests.

📖 Detailed Notes

2.1 Core concepts

- **Network security** is concerned with protection of devices and data from illegitimate access or misuse; threats include all ways to exploit vulnerabilities in a network or communication system. (NCERT §12.1, p. 223)
- A computer with no external link is free from network security threats, but staying disconnected is not a practical solution in a fully connected world. (NCERT §12.1, p. 223)
- **Malware** (MALicious softWARE) is any software developed with an intention to damage hardware, steal data, or cause trouble to the user; types include Viruses, Worms, Ransomware, Trojans, Spyware, Adware, and Keyloggers. (NCERT §12.2, p. 224)
- A **Virus** is a piece of software code that performs malicious activities and hampers CPU time, memory, personal files, or sensitive information; it spreads by copying/inserting its code into executable files and remains dormant until a user opens the infected file. (NCERT §12.2.1, p. 224)
- The term "computer virus" was coined by **Fred Cohen in 1985**; well-known examples include CryptoLocker, ILOVEYOU, MyDoom, Sasser, Netsky, Slammer, and Stuxnet. (NCERT §12.2.1, p. 224)

- A **Worm** is standalone malware that does not need a host program; unlike a virus it self-replicates without human triggering and spreads through the network. Examples: Storm Worm, Sobig, MSBlast, Code Red, Nimda, Morris Worm. (NCERT §12.2.2, p. 224–225)
- **Ransomware** targets user data — it either blocks access or threatens to publish data online and demands ransom payment; WannaCry (May 2017) infected ~200,000 computers across 150 countries and demanded Bitcoin payment. (NCERT §12.2.3, p. 225)
- A **Trojan** looks like legitimate software but once installed acts like a virus or worm; it does NOT self-replicate, spreads only through user interaction (email attachment, file download), and may create backdoors. (NCERT §12.2.4, p. 225–226)
- **Spyware** gathers information about a person/organisation without their knowledge, records it, and sends it to an external entity; it can track internet usage, credit card details, login credentials, and personal identity. (NCERT §12.2.5, p. 226)
- **Adware** generates revenue for its developer by displaying advertisements via pop-ups, web pages, or installation screens; it is usually annoying but harmless, yet often paves way for other malware. (NCERT §12.2.6, p. 226–227)
- A **Keylogger** records every key pressed on a keyboard and may send that log to an external entity; it can be software-based malware or hardware-based (thin transparent keyboard placed atop the actual keyboard). Using an online virtual keyboard randomises the key layout each session, making keylogging very difficult. (NCERT §12.2.7, p. 227–228)
- **On-screen keyboard** uses a fixed QWERTY layout (exploitable by keylogger software); **online virtual keyboard** randomises the key layout every time it is used, making it safer against keyloggers. (NCERT §12.2.7, p. 227–228)
- **Malware distribution channels:** Downloaded from the Internet, Spam Email (unsolicited email with embedded hyperlinks/attachments), Removable Storage Devices (pen drives, SSD cards, mobile phones), and Network Propagation (worms). (NCERT §12.2.8, p. 228)
- Common signs of malware infection include: frequent pop-ups, changed browser homepage, mass emails sent from your account, unusually slow computer, unknown programs starting up, programs opening/closing automatically, sudden lack of storage space, programs/files appearing or disappearing. (NCERT §12.2.9, p. 229)
- **Antivirus** (anti-malware) software was initially developed to detect and remove viruses; it now covers prevention, detection, and removal of a wide range of malware. (NCERT §12.3, p. 230)
- **Five antivirus detection methods:** (A) Signature-based — uses Virus Definition File (VDF); (B) Sandbox detection — executes suspected file in a virtual environment; (C) Data mining techniques — uses ML to classify files as benign/malicious; (D) Heuristics — compares source code against known virus patterns in heuristic

database; (E) Real-time protection — anti-malware runs in background and monitors active memory. (NCERT §12.3.1, p. 230–231)

- **Spam** is unsolicited bulk digital communication (most commonly email); email services like Gmail and Hotmail use automatic spam detection algorithms. (NCERT §12.4, p. 231)
- **HTTP** (Hyper Text Transfer Protocol) sends data as-is over the network, leaving it vulnerable to hackers; suitable for public information websites. **HTTPS** (Hyper Text Transfer Protocol Secure) encrypts data before transmission and decrypts at the receiver end; HTTPS websites require an **SSL Digital Certificate**. (NCERT §12.5, p. 231–232)
- A **Firewall** is a network security system that protects a trusted private network from unauthorised access or traffic from an untrusted outside network; it can be implemented in software, hardware, or both and acts as the first barrier against malware. (NCERT §12.6, p. 232)
- **Types of Firewall:** (1) Network Firewall — placed between two or more networks, monitors inter-network traffic; (2) Host-based Firewall — placed on a single computer, monitors traffic to and from that machine. (NCERT §12.6.1, p. 233)
- A **Cookie** (derived from "magic cookie" in Unix) is a small file or data packet stored by a website on the client's computer; edited only by the website that created it. Used to store browsing info: shopping cart items, login credentials, language preference, search queries, etc. (NCERT §12.7, p. 233)
- **Types of cookies:** Session cookies (track current session, auto-terminate on time-out), Authentication cookies (check if user is already logged in). "Zombie cookies" get recreated after being deleted; "supercookies" can disguise as malware. Third-party cookies track users across websites for advertising. (NCERT §12.7.1, p. 233–234)
- **Hackers and Crackers** have thorough knowledge of computer systems, OS, networks, and programming to find loopholes and gain unauthorised access. (NCERT §12.8, p. 234)
- **White Hat hackers** (Ethical Hackers) use their knowledge to find and fix security flaws; organisations hire them. (NCERT §12.8.1, p. 234)
- **Black Hat hackers** (Crackers) use knowledge unethically to break the law and exploit system flaws. (NCERT §12.8.2, p. 234)
- **Grey Hat hackers** hack systems for the fun of it — not for monetary or political gain; they are neutral. A **hacktivist** is a hacker aiming to bring about political and social change. (NCERT §12.8.3, p. 234–235)
- **Denial of Service (DoS)** attack floods a victim's resource with illegitimate requests, making it appear busy and unavailable to legitimate users; can target web servers, email servers, network storage, or connections. (NCERT §12.9.1, p. 235)
- **DDoS (Distributed DoS)** uses compromised computers (Zombies) distributed across the globe, controlled via malicious "Bot" software forming a "Bot-Net"; much

harder to counter than a simple DoS because attacks come from multiple distributed sources. (NCERT §12.9.1, p. 235)

- **Intrusion Problems** (§12.9.2): Unauthorised activity on a network; methods include Asymmetric Routing (sending packets through multiple paths to bypass sensors), Buffer Overflow Attacks (overwriting memory with malicious code), and Traffic Flooding (flooding the intrusion detection system with packets). (NCERT §12.9.2, p. 236)
- **Snooping** (also called Sniffing) is the secret capture and analysis of network traffic; the snooping device reproduces exact traffic packets back into the channel so nothing appears to have happened. Network hubs/switches have a SPAN (Sniffer Port Analyser) function. (NCERT §12.9.3, p. 236–237)
- **Eavesdropping** is an unauthorised real-time interception of private communication between two entities over a network; targets include VoIP calls, instant messages, video conferences, and fax transmissions. Unlike snooping (store for later analysis), eavesdropping happens in real time. (NCERT §12.9.4, p. 237–238)

2.2 Definitions to memorise

Term	Definition	Page
Malware	Any software developed with intention to damage hardware, steal data, or cause trouble; short for MALicious softWARE	224
Virus	Piece of software code that performs malicious activities; spreads by copying code into executable files; needs human triggering	224
Worm	Standalone malware that self-replicates and spreads through networks without human triggering or a host program	224–225
Ransomware	Malware that blocks user access to their data or threatens to publish it and demands ransom payment	225
Trojan	Malware disguised as legitimate software; does not self-replicate; spreads via user interaction; may create backdoors	225–226
Spyware	Malware that gathers and sends user information to an external entity without the user's knowledge or consent	226
Adware	Malware that displays online advertisements via pop-ups/web pages to generate revenue for its developer	226–227
Keylogger	Malware (or hardware device) that records keystrokes and sends them to an external entity	227
Virus Definition File (VDF)	Signature database used by antivirus software containing known virus signatures; must be updated continuously	230
Spam	Any unsolicited bulk digital communication (email, messages, ads); most widely recognised form is email spam	231

Term	Definition	Page
HTTP	Hyper Text Transfer Protocol; transmits data as-is over the network without encryption	231
HTTPS	Hyper Text Transfer Protocol Secure; encrypts data before transmission; requires SSL Digital Certificate	231–232
Firewall	Network security system protecting a trusted private network from unauthorised access from an untrusted network	232
Cookie	Small file or data packet stored by a website on the client's computer to retain browsing information	233
DoS	Denial of Service; attack that floods a resource with illegitimate requests to make it unavailable to legitimate users	235
DDoS	Distributed Denial of Service; DoS attack using a network of compromised Zombie computers (Bot-Net)	235
Snooping / Sniffing	Secret capture and analysis of network traffic by malicious users or for network troubleshooting	236–237
Eavesdropping	Unauthorised real-time interception of private communication between two entities over a network	237–238
White Hat Hacker	Ethical hacker who uses knowledge to find and fix security flaws; hired by organisations	234
Black Hat Hacker	Cracker who exploits system flaws unethically and illegally	234
Hacktivist	Hacker who aims to bring about political and social change	234
Bot-Net	A network of compromised "Zombie" machines used to launch DDoS attacks	235
Zombie	A compromised computer remotely controlled by an attacker	235
Sandbox	Isolated virtual environment used to safely execute and analyse suspicious files	230
Heuristic Database	Repository of known virus code patterns used in heuristic detection	231
SSL Digital Certificate	Cryptographic certificate required for HTTPS-enabled websites	232
Buffer Overflow	Intrusion attack that overwrites memory with malicious code	236
SPAN port	Sniffer Port Analyser function on a network device used for traffic capture	237
Backdoor	Hidden access mechanism left by a Trojan for later exploitation	226
WannaCry	2017 ransomware that infected ~200,000 machines and demanded Bitcoin	225
Fred Cohen	Researcher who coined the term "computer virus" in 1985	224
	Anti-malware mode that monitors active memory continuously	231

Term	Definition	Page
Real-time protection		
Authentication cookie	Cookie used to remember a logged-in user across requests	233
Third-party cookie	Cookie set by a domain other than the one in the address bar; used for tracking	234

2.3 Diagrams / processes to remember

- **Figure 12.1: A ransomware** (p. 225) — Illustrates the "pay for unlock" concept; reinforces how ransomware holds data hostage and demands payment.
- **Figure 12.2: A Trojan horse** (p. 226) — Visual analogy of the wooden horse of Troy; helps remember that a Trojan appears legitimate on the outside but hides malicious code inside.
- **Figure 12.3: QWERTY keyboard layout (On-Screen Keyboard)** (p. 227) — Shows the fixed layout that keylogger software can exploit.
- **Figure 12.4: Online virtual keyboard** (p. 228) — Shows the SBI Online banking page with "Enable Virtual Keyboard" option; illustrates randomised layout as a defence against keyloggers.
- **Figure 12.5: A firewall between two networks** (p. 232) — Shows LAN on one side, WAN on the other, with the firewall brick wall in between; key for understanding Network Firewall placement.
- **Figure 12.6: Eavesdropping** (p. 237) — Shows an attacker intercepting communication between two computers in real time; contrasts with snooping (store-and-replay).

2.4 Common confusions / NTA trap points

- **Virus vs. Worm:** A virus needs a host program and human triggering (user must open the infected file); a worm is standalone and self-replicates through the network without any human action. NTA regularly tests this distinction.
- **Trojan vs. Virus:** A Trojan does NOT self-replicate or infect other files; it relies entirely on user interaction (e.g., opening an email attachment). Students confuse Trojans with viruses because both cause harm once active.
- **Snooping vs. Eavesdropping:** Snooping captures and stores network traffic for later analysis (not real-time); eavesdropping is real-time interception. NTA likes "Which of the following is correct about snooping/eavesdropping?" questions.
- **DoS vs. DDoS:** In DoS a single attacker floods the target; in DDoS the requests come from many compromised Zombie machines forming a Bot-Net. A simple DoS can be countered by blocking one IP source; DDoS cannot because it comes from multiple distributed locations.

- **On-screen keyboard vs. Online virtual keyboard (NCERT § 12.2.7, p. 227-228).** On-screen keyboard has a fixed QWERTY layout (exploitable); online virtual keyboard randomises layout each time (safe against keyloggers).
- **Cookies are NOT malware (NCERT § 12.7, p. 233).** They are storage files; third-party cookies can be invasive but cookies themselves are not viruses.
- **HTTPS requires SSL Certificate (NCERT § 12.5, p. 232).** Browser shows a padlock icon when an SSL Cert is present.
- **Firewall ≠ antivirus (NCERT § 12.6, p. 232).** A firewall filters traffic; antivirus detects/removes malware in files.
- **Adware vs Spyware (NCERT § 12.2.5-6, p. 226-227).** Adware shows ads; spyware steals info silently. NTA distractor: claims adware steals data.
- **DDoS uses many sources (NCERT § 12.9.1, p. 235).** Blocking one IP cannot stop it.
- **VDF must be updated (NCERT § 12.3.1, p. 230).** Outdated antivirus misses new variants.

🎯 Practice MCQs

Q1. Which of the following correctly distinguishes a computer worm from a computer virus?

A. A worm requires a host program to insert its code, whereas a virus is standalone

B. A worm is standalone and self-replicates through the network without human triggering, whereas a virus needs a host program and user action to activate

C. A worm targets only hardware, whereas a virus targets only software

D. A worm demands ransom payment, whereas a virus only corrupts files

Q2. Consider the following statements about antivirus detection methods: **Statement I:** In signature-based detection, the antivirus uses a Virus Definition File (VDF) containing known virus signatures, which must be updated on a real-time basis. **Statement II:** In sandbox detection, a new application is executed in the actual system environment so its behaviour can be observed under real conditions. Which of the above statements is/are correct?

A. Statement I only

B. Statement II only

C. Both Statement I and Statement II

D. Neither Statement I nor Statement II

Q3. WannaCry, the 2017 ransomware that infected approximately 200,000 computers across 150 countries, extracted money from its victims by:

A. Stealing banking passwords and draining accounts directly

B. Encrypting user data and demanding ransom in Bitcoin cryptocurrency

C. Spying on users through their webcams and selling the footage

D. Displaying pop-up advertisements that charged users per click

🔒 **12 more MCQs + answer key**
Get UniDrill Pro · ₹199/year · unidrill.in/pricing

📊 PYQ Alignment

Chapter 12 (Security Aspects) has consistent representation in CUET Computer Science papers, typically contributing 2–4 questions per year, with the most frequent question types focusing on malware identification and distinction (especially Virus vs. Worm vs. Trojan), hacker classification (White/Black/Grey Hat), and HTTP vs. HTTPS; in recent years, network threats like DoS/DDoS and snooping vs. eavesdropping have also appeared as NTA shifts toward applied and conceptual questions rather than pure recall. See PYQ archive for Computer Science.