92	**Nuclear Power Plant Company Bangladesh limited** **Post: Engineer (Cyber Security Analyst)** **Exam Taker: DUET Time: 1 hour** **Exam Date: 11.07.2026**

1. What is the CIA Triad? Explain its three components.

The CIA Triad is the foundation of information security. It consists of:

• Confidentiality: Ensures information is accessible only to authorized users through authentication, access control, and encryption.

• Integrity: Ensures data remains accurate, complete, and unaltered except by authorized users. Hashing, digital signatures, and checksums help maintain integrity.

• Availability: Ensures systems and data are available whenever needed. Backups, redundancy, disaster recovery, and fault tolerance improve availability.

Together, these three principles guide the design of secure information systems.

2. What is a Man-in-the-Middle (MITM) Attack?

A MITM attack occurs when an attacker secretly intercepts and possibly modifies communication between two parties without their knowledge. The attacker can steal credentials, financial information, or inject malicious data. HTTPS, VPNs, certificate validation, and multi-factor authentication help prevent MITM attacks.

3. What is ARP Spoofing (ARP Poisoning)? How does it work?

Definition

ARP Spoofing (ARP Poisoning) is a **Layer 2 (Data Link Layer)** cyberattack in which an attacker sends **forged ARP (Address Resolution Protocol) messages** on a Local Area Network (LAN). The attacker associates **their own MAC address** with the IP address of another device (usually the default gateway or a victim), causing network traffic to be redirected through the attacker's device.

As a result, the attacker can **intercept, monitor, modify, or block** communication between devices.

How ARP Works Normally

Before understanding ARP Spoofing, consider how ARP functions:

1. A computer wants to send data to the default gateway (e.g., **192.168.1.1**).
2. It broadcasts an **ARP Request**:
   "Who has IP 192.168.1.1? Tell me your MAC address."
3. The router replies with its **MAC address**.
4. The computer stores this information in its **ARP cache** and sends data to the router.

How ARP Spoofing Works

1. The attacker joins the same **Local Area Network (LAN)**.
2. The attacker sends **fake (forged) ARP Reply** messages to the victim.
3. The forged reply falsely claims:

- "I am the default gateway."

4. The victim updates its ARP cache with the attacker's MAC address.
5. The victim now sends all network traffic to the attacker instead of the real router.
6. The attacker can:
   - ✓ Read sensitive information (passwords, emails, banking data)
   - ✓ Modify transmitted data
   - ✓ Forward packets to the real router (Man-in-the-Middle attack)
   - ✓ Drop packets and cause a Denial-of-Service (DoS)

4. What is Cloud Computing? Mention its advantages.

Cloud computing delivers computing resources (servers, storage, databases, networking, software) over the Internet on demand.

Advantages:

• Lower cost
• Scalability
• High availability
• Anywhere access
• Automatic updates
• Backup and disaster recovery
• Faster deployment

5. Why is Packet Switching better?

Packet switching divides data into packets that travel independently. It offers efficient bandwidth utilization, supports multiple users simultaneously, provides fault tolerance through alternate routes, reduces cost, and is ideal for Internet communication compared with circuit switching.

6. How do you use Intrusion Detection System (IDS) in NPCBL Cybersecurity?

An **Intrusion Detection System (IDS)** is a cybersecurity solution that continuously monitors network traffic, servers, and critical systems to detect unauthorized access, cyberattacks, and suspicious activities. In **NPCBL (Nuclear Power Plant Company Bangladesh Ltd.)**, IDS is essential for protecting critical infrastructure, ensuring operational safety, and maintaining uninterrupted power generation.

Uses of IDS in NPCBL Cybersecurity

1. Protect Industrial Control Systems (ICS) and SCADA

- IDS monitors **SCADA (Supervisory Control and Data Acquisition)** systems, **Industrial Control Systems (ICS)**, and **Distributed Control Systems (DCS)**.
- It detects unauthorized commands, abnormal communication, and attempts to manipulate plant operations.

2. Monitor Critical Network Traffic

- IDS continuously analyzes network packets between control rooms, engineering workstations, servers, and field devices.

- It identifies suspicious traffic, malware, and unauthorized access attempts.

3. Detect Cyber Attacks

IDS helps detect attacks such as:

- Malware and ransomware
- Denial-of-Service (DoS/DDoS)
- SQL Injection
- Brute-force login attempts
- Zero-day exploits
- Insider threats
- Network scanning and reconnaissance

4. Secure Nuclear Plant Infrastructure

- Monitors critical servers, databases, operator consoles, and engineering systems.
- Detects unauthorized configuration changes or access to sensitive operational data.

5. Protect Remote Access

- Monitors VPN and remote maintenance connections.
- Detects unauthorized remote logins and suspicious administrator activities.

6. Generate Real-Time Alerts

- When suspicious activity is detected, IDS immediately alerts the **Security Operations Center (SOC)** or cybersecurity team.
- Early detection enables rapid incident response before attacks affect plant operations.

7. Maintain Security Logs

IDS records important information such as:

- Source and destination IP addresses
- Time of attack
- Type of attack
- Affected systems
- Severity level

These logs support forensic investigations and regulatory compliance.

8. Integrate with SIEM

- IDS is integrated with a **Security Information and Event Management (SIEM)** system.
- SIEM collects logs from firewalls, IDS, antivirus, servers, and network devices, providing centralized monitoring and faster threat analysis.

9. Support Regulatory Compliance

- Helps NPCBL comply with national cybersecurity regulations and international nuclear cybersecurity standards by maintaining audit trails and continuous monitoring.

7. Differentiate between DoS and DDoS attacks.

DoS: Single attacking device, easier to trace, limited traffic.

DDoS: Multiple compromised devices (botnet), much larger traffic, difficult to stop, more damaging.

DoS (Denial of Service)	DDoS (Distributed Denial of Service)
Single system targets victim system	Multiple systems attack victim system

Traffic originates from one location	Traffic originates from multiple locations
Sends limited volume of packets compared to DDoS	Sends massive volume of traffic to overwhelm target
Slower compared to DDoS attacks	Faster and more powerful due to distributed sources
Easier to block since only one source is involved	Difficult to block due to multiple attacking sources
Easier to trace origin of attack	Very difficult to trace origin
Uses single device or tools for attack	Uses multiple compromised devices (botnet)
Causes moderate impact on target system	Causes severe impact and complete service disruption

8. Compare Wi-Fi, Bluetooth, and WiMAX.

Wi-Fi: Local wireless networking, range about 50–100 m, high speed. Bluetooth: Short-range communication (10–100 m), low power, connects peripherals. WiMAX: Metropolitan wireless broadband, several kilometers coverage, used for ISP connectivity.

A detailed comparison of their core technical metrics illustrates these operational differences:

Feature	Bluetooth	Wi-Fi	WiMAX
Primary Use	Device-to-device pairing (e.g., headsets, mice)	High-speed Local Area Network/Internet access	Long-range broadband (e.g., city-wide internet)
IEEE Standard	802.15.1	802.11a/b/g/n/ac/ax	802.16
Range	Very short (up to ~ 10 meters)	Short to medium (up to ~ 100 meters)	Long (up to ~ 50-90 km)
Data Rate	~ 1 Mbps - 3 Mbps	~ 54 Mbps - 9.6 Gbps	Up to ~ 70 Mbps - 1 Gbps
Frequency Band	2.4 GHz	2.4 GHz, 5 GHz, 6 GHz	2 - 11 GHz, 10 - 66 GHz
Network Type	WPAN (Wireless Personal Area Network)	WLAN (Wireless Local Area Network)	WMAN (Wireless Metropolitan Area Network)
Hardware	Bluetooth adapter/chip	Wireless router and adapter	Base stations and receivers

9. Compare IPv4 and IPv6. How is IPv6 more secure?

IPv4	IPv6
Uses a 32-bit IP address.	Uses a 128-bit IP address.
Uses decimal dot-separated notation (e.g., 192.168.0.1).	Uses hexadecimal colon-separated notation (e.g., 2001:db8::1).

Provides a limited address space of about 4.3 billion addresses.	Provides an extremely large address space for future growth.
Supports manual configuration and DHCP.	Supports SLAAC, DHCPv6, and manual configuration.
End-to-end connectivity is often affected due to NAT.	End-to-end connectivity is restored without NAT.
IPsec support is optional.	IPsec support is built into the protocol design.
Fragmentation is performed by both sender and routers.	Fragmentation is performed only by the sender.
Does not support flow-based packet identification.	Uses a Flow Label field for packet flow identification.
Includes a header checksum.	Does not include a header checksum.
Supports broadcast communication.	Uses multicast and anycast instead of broadcast.
Header size is variable (20–60 bytes).	Header size is fixed at 40 bytes.
Uses address classes (A, B, C, D, and E).	Does not use address classes.

IPv4 uses 32-bit addresses; IPv6 uses 128-bit addresses. IPv6 provides a vastly larger address space, simplified headers, better routing efficiency, and supports IPSec natively, Secure Neighbor Discovery, and eliminates NAT in many deployments, making end-to-end security easier.

10. What is Subnetting? 192.169.0.1/24 Valid usable IP?

Subnetting divides a network into smaller logical subnetworks to improve performance, management, and security.
For 192.169.0.1/24:
Network address: 192.169.0.0
Broadcast address: 192.169.0.255
Usable host range: 192.169.0.1 – 192.169.0.254
Therefore, 192.169.0.1 is a valid usable host IP.

11. Compare Encryption, Hashing, and Digital Signature.

Encryption converts plaintext into ciphertext using a key and is reversible.
Hashing converts data into a fixed-length hash and is one-way.
Digital Signature uses private/public key cryptography to verify authenticity, integrity, and non-repudiation.
Core Differences:

Feature	Encryption	Hashing	Digital Signature
Primary Goal	Confidentiality (hide data)	Integrity (check if data changed)	Authenticity & Non-repudiation

Reversibility	**Reversible** (two-way)	**Irreversible** (one-way)	**Reversible** using a public key
Process	Uses an algorithm + a key to scramble/unscramble text	Maps arbitrary data to a fixed-length mathematical fingerprint	Hashes the data, then encrypts that hash with a private key
Main Use Case	Securing messages in transit, VPNs, or database data	Storing passwords safely, verifying file downloads	Signing contracts, securing software updates

12. Translate into Bangla.

English: "Cybersecurity prevents information systems from unauthorized access."
Bangla: "সাইবার নিরাপত্তা তথ্যপ্রযুক্তি ব্যবস্থা বা তথ্য ব্যবস্থা অননুমোদিত প্রবেশ, ব্যবহার ও আক্রমণ থেকে সুরক্ষা প্রদান করে।"

13. Full form: OTP, VPN

OTP = One-Time Password
VPN = Virtual Private Network

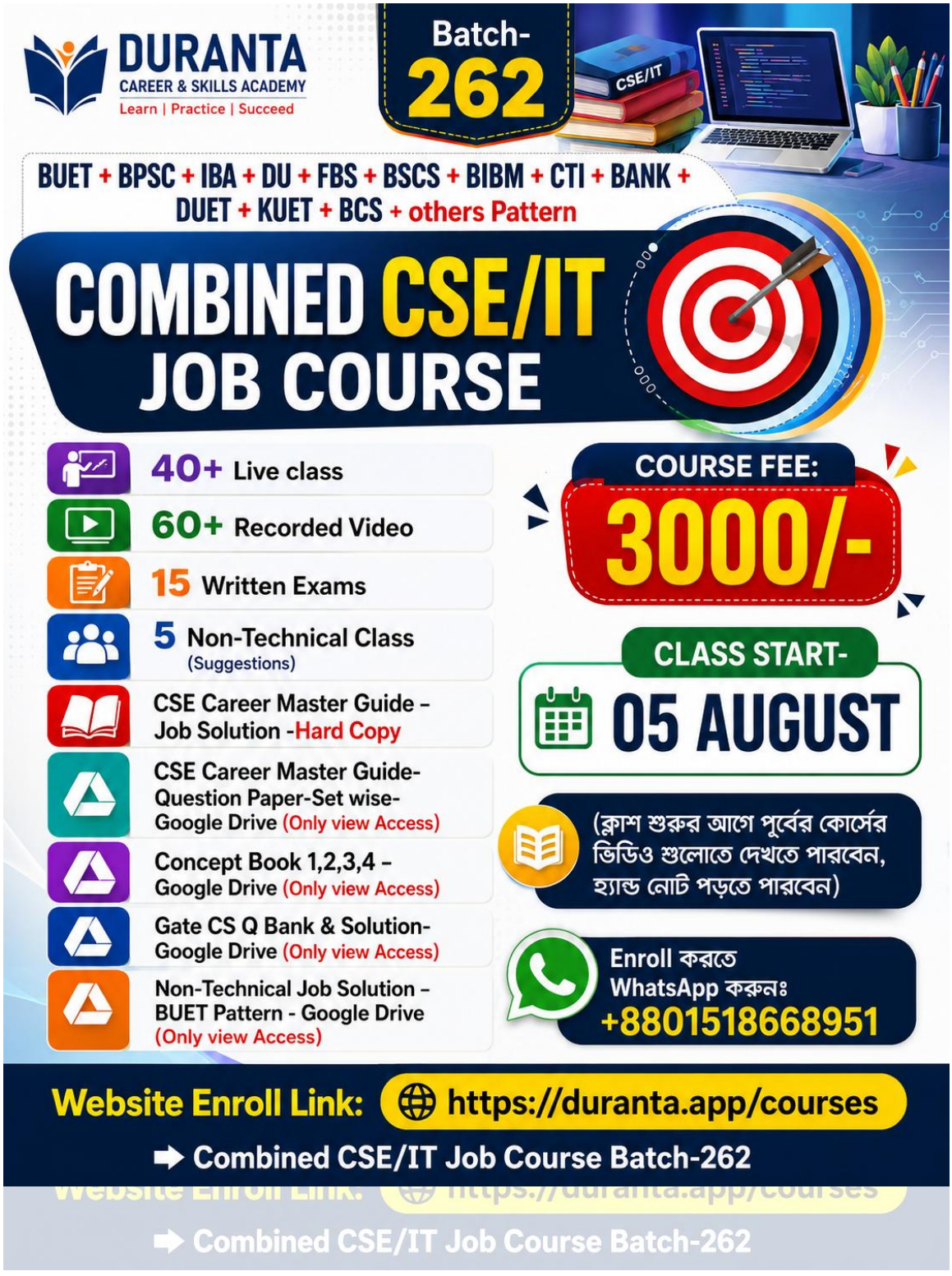
14. What is the Cyber Security Act of Bangladesh? State its main objectives.

The Cyber Security Act, 2023 is Bangladesh's law for preventing cybercrime and protecting digital systems. Its objectives include:

- Prevent cybercrime
- Protect critical information infrastructure
- Safeguard digital transactions
- Protect personal and organizational data
- Establish legal procedures for investigation and prosecution
- Promote national cybersecurity

15. Will Artificial Intelligence (AI) replace jobs? Explain your opinion with reasons.

AI will replace some repetitive and routine jobs but is unlikely to replace all jobs. It automates repetitive work, improves productivity, and creates new roles in AI development, cybersecurity, data science, and digital services. Human creativity, ethics, leadership, communication, and complex decision-making remain essential. Therefore, workers should continuously learn new skills and adapt to AI-assisted workplaces.


DURANTA
CAREER & SKILLS ACADEMY
Learn | Practice | Succeed
Batch-
262
CSE/IT
BUET + BPSC + IBA + DU + FBS + BSCS + BIBM + CTI + BANK +
DUET + KUET + BCS + others Pattern
COMBINED CSE/IT
JOB COURSE
40+ Live class
60+ Recorded Video
15 Written Exams
5 Non-Technical Class
(Suggestions)
CSE Career Master Guide –
Job Solution -Hard Copy
CSE Career Master Guide-
Question Paper-Set wise-
Google Drive (Only view Access)
Concept Book 1,2,3,4 –
Google Drive (Only view Access)
Gate CS Q Bank & Solution-
Google Drive (Only view Access)
Non-Technical Job Solution –
BUET Pattern - Google Drive
(Only view Access)
COURSE FEE:
3000/-
CLASS START-
05 AUGUST
(ক্লাশ শুরুর আগে পূর্বের কোর্সের
ভিডিও গুলোতে দেখতে পারবেন,
হ্যান্ড নোট পড়তে পারবেন)
Enroll করতে
WhatsApp করুনঃ
+8801518668951
Website Enroll Link: https://duranta.app/courses
Combined CSE/IT Job Course Batch-262