Assignment
PBEL Batch-2

Name-Jayantika Sharma

ABES Engineering College

1st August,25

Supervisor's Name:Mr.Aysuh Kumar

1.What is cybersecurity? Why is it important in today's digital world?

- Cybersecurity is the practice and process for protecting sysyems,networks,programs and data from unathorized access,attack,etc.

  This ensures CIA Triad.

- Importance:-

1. Protects senstive data such as personal information,bank details, etc from being stolen and unauthorized access and breach.

2. Maintains Confidentiality Intergrity Availability Triad.

3. Prevents Data Leak and manipulaion in a system.

2.Define the CIA Triad in cybersecurity.

- CIA Triad is a fundamental and core principle in information security.

Confidentiality: Ensures that information is access by the authorized individual only, safegaurds data from unauthorized individuals.

Integrity: Ensures that data is not manipulated and preserved its integrity and accuracy.

Availability: Ensures system and data are accessible to authorized individuals only.

3.What is the difference between a virus, a worm, and a trojan horse?

Virus,worm and trojan horse are all malwares.

Virus	Worm	Trojan Horse
Attack to files and spreads when shared. Ex:ILOVEYOU Virus,Michelangelo Virus	Replicates and spreads across network without user. Ex:Morris,Mydoom	Disguises as a legitimate and convincing software and tricks the user. Ex:Zloader ,QakBot

4.Explain the term phishing with an example.

Phishing is a cyberattack ,where attackers impersonate trusted entities to deceive individuals into revealing sensitive information like passwords and credit card numbers.

Type:

Spear Phishing	Whaling Phishing	Clone Phishing
Target is a specific individual. Ex: Ubiquiti Networks – $46.7 Million Fraud	Target is a high profile executives within an organization. Ex:Mattel Inc. ($3 million loss and recovery)	Targets cusyomer of a organization and duplicateblegitimate email to trick them. Ex:Google Documents Clone Phishing

5.What is ethical hacking? How is it different from malicious hacking?

Ethical Hacking:	**Malicious Hacking**
It is an authorized practice of testing systems for vulnerabilities and loopholes to improve security. Goal: protect digital assets and prevent cyberattacks.	It is an unauthorized and intended to exploit or harm systems for personal gain or damage. Goal: To steal data, cause disruption, or gain financial or political benefits through exploitation

6.List any five common types of cyber-attacks and describe them briefly

Common types of cyber-attacks include phishing, ransomware, denial-of-service, SQL injection, and man-in-the-middle attacks

Phishing involves fraudulent emails or messages that appear to be from legitimate sources, tricking individuals into providing sensitive information, such as passwords or credit card details.

Ransomware is a type of malware that encrypts the victim's files, rendering them inaccessible until a ransom is paid to the attacker. This can cause significant operational disruptions and financial losses for both individuals and organizations.

Denial-of-Service (DoS) attacks overwhelm a target server or network with excessive traffic, causing legitimate users to be unable to access services.

SQL injection attacks exploit vulnerabilities in a web application's database layer by injecting malicious SQL queries through input fields. This can allow attackers to gain unauthorized access to sensitive data, manipulate databases

Man-in-the-Middle (MitM) attacker secretly intercepts and relays communications between two parties who believe they are directly communicating with each other. This can be executed over unsecure connections like public Wi-Fi, making it easier for attackers to capture sensitive data

7.How does two-factor authentication improve security?

Two-factor authentication enhances security by requiring two distinct forms of verification, making unauthorized access much more difficult.

Two-factor authentication adds an extra layer of security to the standard username and password login process.

Benefits:

1. Increased Security
2. Protection Against Phishing
3. Enhance user's confidentiality.

8.Describe any recent cybercrime incident in India. What were its consequences?

Star Delta Health Breach

Date	Action	Description
Early August,24	Breach and ransom demand	Infiltrate in the system and demands $68,000.
August 13,24	Ransom letters to executive	Blackmail CEO/CFO,through emails.
August 14,24	Notify Authority	Internal Investigation takes place.
August 22,24	Public leakage of consumer information.	Information was leaked through Telegram.
October,24	Legal Actions	Permanently removing data.

- Hacker: xenZen
- Ransom Demanded:$68000
- Scale of Breach: Data of 31.2 million customers.
- Consequences:

Financial:

- $30million penalty under "India's Digital Personal Data Protection Act" for mishandling of Data.
- 11% stock Drop.

Legal consequences:

- The company faces regulatory warnings affecting it’s ability to conduct digital business without scrutiny.

9.Create a cybersecurity awareness guide for college students, listing Do’s and Don’ts.

Do's

- Use strong, unique passwords for each account—combine uppercase, lowercase, numbers, and symbols; avoid personal info and common words.
- Enable multi-factor authentication (MFA) wherever possible for extra security.
- Back up important files frequently to an external drive or secure cloud storage.

- Use VPNs on public Wi-Fi; avoid sensitive transactions like banking via unsecured networks.

Don't

- Don’t reuse the same password across multiple accounts—if one
- gets hacked, others become easy targets.
- Don’t disable your firewall or antivirus for convenience—they are critical layers of defense.
- Don’t plug in or use external devices (like USBs) without scanning for malware.

10.Discuss the major components and uses of a firewall in network security.

A firewall is a fundamental component of network security, serving as a barrier between trusted internal networks and untrusted external networks. Major components:

Hardware	Dedicated devices running firewall software, physically separating internal and external networks.
Software	Rules and policies set to monitor and filter traffic. This includes web application firewalls (WAFs) and host-based firewalls
Packet Filtering	Examines the headers of data packets (source/destination IP, ports, protocol) and allows or blocks them based on predefined rules.
Inspection	Tracks the state of active connections, making more informed decisions by understanding ongoing traffic context.

Uses:

Traffic Monitoring & Filtering: Inspects inbound and outbound network traffic, blocking suspicious or explicitly forbidden connections based on policy.

Prevention of Unauthorized Access: Stops hackers or malicious users from accessing internal resources without permission.

Virus and Malware Defense: Blocks traffic associated with known malware or dangerous patterns, working with antivirus software to strengthen defense layers.

Network Segmentation: Divides large networks into smaller, more secure zones—limiting lateral movement and reducing damage if a breach occurs.