CSDF VIVA QUESTION – ANSWERS

1. What is CSDF?

Ans: CSDF stands for Cyber Security and Digital Forensics. It focuses on protecting systems from cyberattacks and investigating digital crimes using forensic methods.

2. What is Cyber Security?

Ans: Cyber Security is the practice of protecting computers, networks, and data from unauthorized access, damage, or attack.

3. What is Digital Forensics?

Ans: Digital Forensics is the process of collecting, preserving, analyzing, and presenting digital evidence in a legally acceptable manner.

4. What are the main goals of Cyber Security?

Ans:The main goals are defined by the CIA Triad:

- Confidentiality – Protecting information from unauthorized access.
- Integrity – Ensuring data accuracy and trustworthiness.
- Availability – Ensuring data and resources are available when needed.

5. What are the phases of Digital Forensics?

Answer:

- Identification – Recognize potential evidence.
- Preservation – Secure and protect data from alteration.
- Collection – Gather digital evidence legally.
- Examination – Analyze data using forensic tools.
- Analysis – Interpret evidence to reconstruct events.
- Presentation – Present findings in court or reports.

6. What is the difference between Cyber Security and Digital Forensics?

Ans:

Cyber Security is preventive — it focuses on protecting systems before an attack happens.

Digital Forensics is reactive — it deals with investigating incidents after an attack or crime occurs

7. What is the importance of Digital Forensics in investigations?

Answer:

It helps investigators find how, when, and who committed a cybercrime by analyzing digital traces such as emails, logs, deleted files, and network activity. It provides crucial evidence for court cases.

8. What is meant by Chain of Custody in forensics?

Answer:

It is a documented process that tracks the handling of digital evidence from collection to presentation in court. It ensures that evidence is not tampered with and maintains its integrity.

.

Practical 1: Tracking Emails and Investigating Email Crimes

1. What are Email Crimes?

Email crimes include phishing, spamming, spoofing, identity theft, and spreading malware through emails.

2. What is Email Forensics?

Email Forensics is the process of analyzing emails to trace the sender's origin, detect fraud, and gather digital evidence.

3. What are the common techniques used in Email Forensic Investigation?

- Header Analysis
- Metadata Extraction
- IP Tracing
- Keyword Searching
- Log Correlation

4. What is an Email Header?

An email header contains metadata such as sender, receiver, IP address, subject, timestamps, and routing information.

5. What is MX Toolbox?

MX Toolbox is an online tool used to analyze email headers, trace sender IPs, and detect spam or blacklisted domains.

Practical 2: CAPTCHA Generation and Verification

7. What is CAPTCHA?

CAPTCHA stands for Completely Automated Public Turing test to tell Computers and Humans Apart. It's used to differentiate humans from bots.

8. Why is CAPTCHA used?

It prevents automated form submissions, fake registrations, brute-force login attempts, and spamming.

9. What are the types of CAPTCHA?

- Text CAPTCHA
- Image CAPTCHA
- Audio CAPTCHA
- Google reCAPTCHA

10. How do you import and verify CAPTCHA in Python?

Use:

```
from captcha.image import ImageCaptcha
```

to generate images and verify user input with the generated text.

Practical 3: WiFi Intrusion Detection and Prevention

11. What is IEEE 802.11?

It is the set of standards defining communication for wireless local area networks (WiFi).

12. What is WiFi Intrusion Detection?

It involves monitoring wireless traffic to detect unauthorized access or hacking attempts.

13. What tools can be used for WiFi intrusion detection?

Wireshark, Snort, Aircrack-ng, Kismet, NetStumbler.

14. What is the difference between IDS and IPS?

IDS (Intrusion Detection System): Detects and alerts.

IPS (Intrusion Prevention System): Detects and blocks malicious activity in real-time.

Practical 4: Recovering Permanently Deleted Files and Partitions

15. What happens when a file is deleted?

The file's pointer is removed from the directory table, but data remains on disk until overwritten.

16. How can permanently deleted files be recovered?

By scanning unallocated disk space using tools like Recuva, Autopsy, or TestDisk.

17. What is the difference between Quick Format and Full Format?

- Quick Format: Deletes only file references.
- Full Format: Deletes data and checks disk sectors.

18. What is the full form of SSD?

Solid State Drive.

Practical 5: Log Capturing and Event Correlation

19. What is Log Capturing?

It is the process of collecting and storing system or network logs for monitoring and forensic analysis.

20. Why is Log Capturing important?

It helps detect intrusions, analyze system behavior, and provide evidence during investigations.

21. What is Event Correlation?

It combines data from multiple log sources to detect related security events or attack patterns.

22. What are the uses of the who and last commands?

- who → Displays currently logged-in users.
- last → Shows user login history.

Practical 6: Vulnerability Assessment using Wireshark or SNORT

23. What is Wireshark?

Wireshark is a network protocol analyzer used to capture and inspect packets to identify suspicious network activities.

24. What is SNORT?

SNORT is an open-source Intrusion Detection and Prevention System (IDS/IPS) used to detect network-based attacks using rule signatures.

25. What is Vulnerability Assessment?

It's the process of identifying, quantifying, and prioritizing security weaknesses in a system or network.

26. What are common attacks detected by SNORT?

Port scans, SQL injection, denial-of-service attacks, buffer overflows, and ARP spoofing.

Practical 7: Study of Honeypot

27. What is a Honeypot?

A Honeypot is a decoy system designed to lure attackers and record their actions for study.

28. What are the types of Honeypots?

Low-interaction: Simulates limited services.

High-interaction: Runs full systems for detailed monitoring.

29. What are key components of a Honeypot?

Data capturing module, alert system, control system, and reporting mechanism.

30. What is a Honeyfarm?

A centralized environment that contains multiple Honeypots to collect and analyze attack data at scale.