Cyber Security Lab Viva – Questions and Answers

1. IT Act – Indian Perspective

Q: What is the IT Act, and why was it introduced?

A: It is a law to protect electronic transactions and prevent cybercrime in India.

Q: Name and explain any two important sections of the IT Act.

A: Section 66: Hacking, Section 67: Publishing obscene content online.

Q: What does Section 66 deal with?

A: It deals with hacking and illegal access to computer systems.

Q: Is there any punishment under Section 67?

A: Yes, it includes imprisonment and fine for publishing obscene material online.

2. Recent Cyber Incidents

Q: Can you explain what ransomware is? Give an example.

A: Ransomware locks data and demands payment. Example: WannaCry.

Q: What is phishing and how can one avoid it?

A: Phishing is a fake email trick to steal data. Avoid by checking links and senders.

Q: Mention a recent data leak incident in India.

A: Example: Aadhaar data leak or Facebook user data exposure.

3. Information Gathering Tools

Q: What does Nmap do?

A: It scans networks and finds open ports.

Q: Which tool would you use to gather emails and domain names?

A: theHarvester.

Q: What is Recon-ng mainly used for?

A: Web-based information collection like domains and emails.

4. Vulnerability Analysis Tools

Q: What is the purpose of OpenVAS?

A: To scan for security weaknesses in systems.

Q: How is Nikto different from Nessus?

A: Nikto scans web servers; Nessus scans full systems.

Q: What kind of vulnerabilities does Nessus detect?

A: Password issues, open ports, and missing patches.

5. Web Application Analysis Tools

Q: What is OWASP ZAP used for?

A: It scans web apps for security flaws automatically.

Q: How does Burp Suite help in web security testing?

A: It tests logins, forms, and finds web vulnerabilities.

Q: Which tool can detect XSS or SQL injection?

A: OWASP ZAP or Burp Suite.

6. Database Assessment Tools

Q: What is Sqlmap used for?

A: It finds and exploits SQL injection flaws.

Q: Can Nmap scan database ports? How?

A: Yes, using specific Nmap scripts for DB services.

Q: How can you detect SQL injection in a website?

A: By using Sqlmap or testing input fields manually.

7. Sniffing and Spoofing Tools

Q: What does Wireshark do?

A: It captures and analyzes network packets.

Q: What is a Man-In-The-Middle (MITM) attack?

A: An attacker intercepts communication between two systems.

Q: How can Ettercap be used in spoofing?

A: It performs ARP spoofing to intercept data.

8. Forensics Tools

Q: What is digital forensics?

A: It is the recovery and investigation of digital evidence.

Q: What can Autopsy be used for?

A: To recover deleted files and analyze drives.

Q: How does Volatility help in forensics?

A: It analyzes memory dumps to find traces of activity.

9. Reporting Tools

Q: Why is reporting important after a cyber security assessment?

A: It documents findings and helps in fixing issues.

Q: Name two tools used for generating security reports.

A: Dradis and Faraday.

Q: What makes Dradis useful in team environments?

A: It allows team members to collaborate on reports.