DHANALAKSHMI SRINIVASAN ENGINEERING COLLEGE
(AUTONOMOUS)
(Approved by AICTE & Affiliated to Anna University, Chennai)
Re-Accredited by NAAC with 'A' Grade
Accredited by NBA for AERO, BME, CSE, ECE, EEE, IT & MECH.
PERAMBALUR-621212, TAMILNADU, INDIA.
Website: www.dsengg.ac.in

DEPARTMENT OF CYBER SECURITY

U23CBT45 INTRODUCTION TO CYBER SECURITY
QUESTION BANK

(16 Marks Questions)

UNIT I - INTRODUCTION

1. Discuss the history of the internet and its impact on modern society. How has the evolution of the internet influenced cybersecurity challenges?

2. Explain the CIA Triad in cybersecurity. How do confidentiality, integrity, and availability help in securing digital assets?

3. What are the key reasons for cybercrime? Discuss the various motivations behind cybercriminal activities and their impact on individuals and organizations.

4. Why is cybersecurity essential in the digital age? Explain the growing need for cybersecurity measures to combat cyber threats and protect critical infrastructure.

5. Trace the history of cybercrime. How have cybercriminal activities evolved over time, and what major incidents have shaped cybersecurity laws and practices?

6. Who are cybercriminals? Discuss the different types of cybercriminals, including hackers, insiders, hacktivists, cyber terrorists, and state-sponsored attackers.

7. Classify cybercrimes into different categories. How do cybercrimes such as identity theft, financial fraud, cyberstalking, and cyber terrorism affect individuals and nations?

8. Provide a global perspective on cybercrime. How do different countries handle cyber threats, and what international efforts exist to combat cybercriminal activities?

9. What are cyber laws, and why are they important? Discuss the role of legal frameworks in preventing cybercrimes and protecting digital rights.

10. Explain the Indian IT Act and its significance in cybersecurity. How does it address cybercrimes, and what are the legal consequences for cybercriminal activities in India?

UNIT II - ATTACKS AND COUNTERMEASURES

1. What is OWASP, and how does it contribute to cybersecurity? Discuss its role in identifying and mitigating web application vulnerabilities.

2. Explain the scope of cyber-attacks. How do cybercriminals target individuals, organizations, and governments, and what are the potential consequences?

3. What is a security breach? Discuss different types of security breaches and their impact on organizations and individuals.

4. Describe the various types of malicious attacks, including Denial-of-Service (DoS), Man-in-the-Middle (MitM), SQL Injection, Cross-Site Scripting (XSS), and Ransomware.

5. What is malicious software (malware)? Explain different types of malware, such as viruses, worms, trojans, ransomware, spyware, and rootkits.

6. Discuss common attack vectors used by cybercriminals. How do attackers exploit weaknesses in software, networks, and human behavior to compromise systems?

7. What is social engineering in cybersecurity? Explain different social engineering attacks such as phishing, baiting, pretexting, and tailgating.

8. Describe wireless network attacks. How do cybercriminals exploit vulnerabilities in Wi-Fi networks, and what security measures can be taken to prevent such attacks?

9. What are web application attacks? Explain common web-based threats like SQL Injection, Cross-Site Request Forgery (CSRF), and Broken Authentication.

10. What are some common attack tools used by hackers? Discuss the role of tools like Metasploit, Wireshark, Aircrack-ng, and John the Ripper in cybersecurity, along with countermeasures to defend against them.

UNIT III - RECONNAISSANCE

1. What is Harvester, and how is it used in information gathering? Explain its role in cybersecurity reconnaissance.

2. Explain the function of Whois in gathering domain and IP-related information. How can attackers and security professionals use Whois data?

3. What is Netcraft, and how does it help in gathering website intelligence? Discuss its role in identifying server details, technologies, and security risks.

4. How can information be extracted from DNS records? Explain the importance of DNS reconnaissance techniques such as zone transfers and subdomain enumeration.

5. Describe the methods used to extract information from email servers. How can attackers exploit email servers, and what security measures can be implemented?

6. What is Social Engineering Reconnaissance? Discuss different techniques used by attackers to gather sensitive information through social engineering.

7. Explain the concept of network scanning and vulnerability scanning. How are these techniques used in penetration testing and cybersecurity assessments?

8. What is port scanning? Discuss different types of port scanning techniques and their role in identifying open and vulnerable network ports.

9. Explain the methodology behind scanning techniques. What are the key steps involved in performing a comprehensive network scan?

10. What are Ping Sweep techniques? How do they help in mapping live hosts within a network? Explain different ping sweep methods.

11. Describe the different Nmap command switches and their usage in network scanning. How can Nmap be used for reconnaissance, vulnerability detection, and penetration testing?

UNIT IV - INTRUSION DETECTION

1. What is Host-Based Intrusion Detection (HIDS)? Explain its working mechanism, advantages, and challenges in monitoring system security.

2. Describe Network-Based Intrusion Detection Systems (NIDS). How do they analyze network traffic, and what are their strengths and limitations?

3. What is a Distributed or Hybrid Intrusion Detection System (DIDS)? How does it combine the features of both HIDS and NIDS for improved threat detection?

4. Explain the Intrusion Detection Exchange Format (IDXP) and Intrusion Detection Message Exchange Format (IDMEF). How do these standards help in sharing security threat information?

5. What are Honeypots in cybersecurity? Discuss their types, functions, and role in detecting and mitigating cyber threats.

6. Compare and contrast low-interaction and high-interaction honeypots. How do they help security professionals in understanding attacker behavior?

7. Explain Snort as an Intrusion Detection and Prevention System (IDS/IPS). Discuss its working principles, different modes of operation, and how it detects security threats.

8. How do organizations implement and configure Intrusion Detection Systems (HIDS, NIDS, and DIDS) to enhance network security? Discuss best practices and challenges.

UNIT V - INTRUSION PREVENTION

1. Why are firewalls essential in network security? Explain their role in protecting an organization's IT infrastructure.

2. Discuss the key characteristics of firewalls. How do access policies help in enforcing security rules in a firewall configuration?

3. Explain the different types of firewalls, including packet filtering firewalls, stateful inspection firewalls, proxy firewalls, and next-generation firewalls (NGFWs). How do they differ in functionality?

4. What is firewall basing? Compare and contrast host-based firewalls and network-based firewalls, highlighting their advantages and use cases.

5. Describe the different firewall placement strategies in a network. How do configurations like perimeter firewalls, DMZ firewalls, and internal segmentation firewalls enhance security?

6. What is an Intrusion Prevention System (IPS)? Explain its working mechanism, types (Network-based IPS, Host-based IPS, Wireless IPS, and Content-based IPS), and how it differs from an Intrusion Detection System (IDS).

7. How do firewalls and Intrusion Prevention Systems (IPS) work together to provide a layered security approach? What are the advantages of combining both technologies?

8. Explain the challenges and limitations of traditional firewalls. How do modern firewalls, such as Next-Generation Firewalls (NGFWs), address these challenges?

9. What is Unified Threat Management (UTM)? Discuss its components, advantages, and how it integrates multiple security features into a single solution. Provide examples of well-known UTM products.

10. How do organizations choose the right firewall or intrusion prevention system? Discuss factors like network size, security requirements, performance considerations, and cost-effectiveness.