SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)

SRM Nagar, Kattankulathur – 603 203

DEPARTMENT OF CYBER SECURITY

QUESTION BANK

II YEAR - III SEMESTER

CY3362– INTRODUCTION TO CYBER SECURITY

Regulation – 2023

Academic Year: 2025 – 2026 (ODD)

Prepared by,

Ms.S.Nivedha, Assistant Professor / Cyber Security

SRM VALLIAMMAI ENGINEERING COLLEGE

SRM Nagar, Kattankulathur-603203

DEPARTMENT OF CYBER SECURITY

QUESTION BANK

SUBJECT : CY3362 – INTRODUCTION TO CYBER SECURITY
SEM / YEAR : III SEMESTER/ II YEAR

UNIT -I INTRODUCTION

Cyber Security – History of Internet – Impact of Internet – CIA Triad; Reason for CyberCrime – Need for Cyber Security – History of Cyber Crime; Cybercriminals – Classification of Cybercrimes – A Global Perspective on Cyber Crimes; Cyber Laws – The Indian IT Act – Cybercrime and Punishment.

UNIT –I [PART-A] – 2 Marks

Q.No	Question	Competence	Level
1	Define cybersecurity.	Remembering	BTL1
2	Differentiate between confidentiality, integrity, and availability in the context of cybersecurity.	Understanding	BTL2
3	Explain the role of encryption in ensuring data security.	Understanding	BTL2
4	Explain the difference between authentication and authorization in the context of access control.	Understanding	BTL2
5	Define phishing.	Remembering	BTL1
6	When was the concept of the internet first proposed, and by whom?	Remembering	BTL1
7	What was the initial purpose of ARPANET, the precursor to the internet?	Remembering	BTL1
8	Describe the significance of the TCP/IP protocol suite in the development of the internet.	Understanding	BTL2
9	What year marked the establishment of the first successful connection between two nodes on ARPANET?	Remembering	BTL1
10	Briefly explain the role of the National Science Foundation (NSF).	Understanding	BTL2
11	What event led to the popularization of the World Wide Web (WWW) and its eventual integration into the internet?	Remembering	BTL1
12	Who coined the term "surfing the internet," and what does it refer to?	Remembering	BTL1
13	How has the internet transformed communication between individuals globally?	Understanding	BTL2
14	Discuss two ways in which social media platforms have influenced society.	Understanding	BTL2
15	Describe the impact of the internet on privacy and data security concerns.	Understanding	BTL2
16	What was the significance of the creation of the Internet Engineering Task Force (IETF) in the evolution of the internet?	Understanding	BTL2
17	What are three reasons behind cybercrime?	Understanding	BTL2
18	State two reasons highlighting the importance of cyber security measures.	Understanding	BTL2
19	Name two categories of cybercrimes and provide a brief description of each.	Understanding	BTL2
20	Differentiate between computer-related crimes and cyber-enabled crimes, giving examples for each.	Remembering	BTL1
21	Differentiate between cybercrimes against individuals and	Remembering	BTL1

	cybercrimes against organizations, citing examples for clarity.		
22	Highlight two challenges in combating transnational cybercrimes on a global scale.	Understanding	BTL2
23	Identify two key objectives of the Indian IT Act and explain their significance in combating cybercrimes.	Understanding	BTL2
24	List two offenses punishable under the Indian IT Act and describe the penalties associated with each.	Understanding	BTL2

UNIT –I [PART-B] – 16 Marks

Q.No	Question	Marks	Competence	Level
1	Analyse the development of the Internet and discuss its impact on modern society and the corresponding evolution of cyber security measures.	16	Analyzing	BTL4
2	Explain the CIA Triad in detail. How does each component contribute to a comprehensive cyber security strategy?	16	Understanding	BTL2
3	Discuss the impact of the Internet on global communication and commerce, including changes in business practices, and associated benefits and challenges. Provide relevant examples	16	Analyzing	BTL4
4	Analyse the social, educational, and cultural impacts of the Internet, focusing on information access, education, social media, and cultural norms, and discuss both positive and negative consequences.	16	Analyzing	BTL4
5	How do the principles of the CIA Triad help in creating strong cyber security strategies?	16	Understanding	BTL2
6	Describe how organizations ensure Confidentiality, Integrity, and Availability, and discuss the challenges they face. Provide examples.	16	Understanding	BTL2
7	Analyse the different motivations for committing cybercrime. Explain how economic, social, and technological factors play a role in driving individuals or groups to engage in cybercrime	16	Analyzing	BTL4
8	Explain why cyber security is essential in today's digital world. Discuss the risks and threats that individuals and organizations face online, and describe the potential consequences of cyber-attacks.	16	Understanding	BTL2
9	Explain the concept of cyber criminals, including their motivations and methods in conducting illegal activities online.	16	Understanding	BTL2
10	What are the classifications of cybercrimes, and how do they vary in terms of their nature and impact?	16	Understanding	BTL2
11	Describe the different types of cybercrimes and how they affect people and organizations worldwide.	16	Understanding	BTL2
12	Discuss how countries collaborate to tackle cyber threats and cite specific cases to illustrate your points.	16	Analyzing	BTL4
13	Discuss cyber laws and their significance, focusing on the Indian IT Act.	16	Analyzing	BTL4
14	Explain key provisions of the Act, its impact on cybercrime prevention, and examples of its application in addressing digital offenses.	16	Understanding	BTL2
15	Discuss the punishment prescribed under cyber laws, examining their effectiveness in deterring digital offenses and ensuring	16	Analyzing	BTL4

	accountability.			
16	Discuss the key advancements in cybersecurity over the past two decades and their impact on individuals, organizations, and nations. Provide specific examples.	16	Evaluating	BTL5
17	Compare the effectiveness of cybercrime legislation and enforcement in different countries. Discuss the role of international cooperation and provide case studies to illustrate successes and challenges.	16	Evaluating	BTL5

UNIT – II : ATTACKS AND COUNTERMEASURES

OSWAP; Malicious Attack Threats and Vulnerabilities: Scope of Cyber-Attacks – Security Breach – Types of Malicious Attacks – Malicious Software – Common Attack Vectors – Social engineering Attack – Wireless Network Attack – Web Application Attack – Attack Tools – Countermeasures.

UNIT-II [PART-A]- 2 Marks

Q.No	Question	Competence	Level
1	What does OSWAP stand for, and what is its primary objective?	Remembering	BTL1
2	Differentiate between a vulnerability and an exploit, providing examples for each.	Understanding	BTL2
3	Explain the concept of SQL injection and how it can be prevented.	Understanding	BTL2
4	Define Cross-Site Scripting (XSS) and provide two examples of how it can be exploited.	Understanding	BTL2
5	What are the three main categories of security threats? Briefly explain each category.	Understanding	BTL2
6	Explain the term "zero-day exploit" and why it poses a significant threat to cybersecurity.	Remembering	BTL1
7	Describe the role of penetration testing in identifying and mitigating security vulnerabilities.	Understanding	BTL2
8	Define the scope of cyber-attacks and provide three examples of cyber-attack targets.	Understanding	BTL2
9	Discuss the concept of data exfiltration in the context of a security breach.	Understanding	BTL2
10	Describe the role of social engineering in cyber-attacks and provide two examples of social engineering techniques.	Understanding	BTL2
11	Explain the term "supply chain attack" and discuss its significance in cybersecurity.	Understanding	BTL2
12	Explain the term "data breach notification".	Remembering	BTL1
13	Define Denial of Service (DoS) attacks and Distributed Denial of Service (DDoS) attacks, highlighting the difference between them.	Understanding	BTL2
14	Describe the characteristics of a Man-in-the-Middle (MitM) attack and provide two examples of scenarios where MitM attacks can occur.	Understanding	BTL2
15	Discuss the concept of "spear phishing" and explain why it is often more effective than traditional phishing attacks.	Remembering	BTL2
16	Define the term "ransomware" and describe two common methods used by ransomware to infect systems.	Understanding	BTL1
17	Differentiate between "adware" and "spyware," providing examples of each.	Understanding	BTL2
18	Explain the term "trojan horse".	Understanding	BTL2
19	Discuss the role of a "botnet".	Understanding	BTL2

20	Define the term "rootkit".	Understanding	BTL2
21	Describe the characteristics of a "logic bomb".	Understanding	BTL2
22	Explain the term "watering hole attack" and provide an example of how it can be executed.	Understanding	BTL2
23	Describe the characteristics of a "drive-by download" attack and how it can infect a user's system.	Understanding	BTL2
24	Define the term "malvertising".	Understanding	BTL2

UNIT -II [PART-B]- 16 Marks

Q.No	**Question**	**Marks**	**Competence**	**Level**
1	Define OSWAP (Open Web Application Security Project) and explain its significance in modern cybersecurity practices.	16	Understanding	BTL2
2	Discuss the different types of malicious attacks commonly encountered in cybersecurity, providing examples for each.	16	Analyzing	BTL4
3	Explain the concept of threat, vulnerability, and risk in the context of cybersecurity, illustrating with relevant examples.	16	Understanding	BTL2
4	What are the main objectives of a security breach? Discuss the potential consequences of a successful breach on an organization.	16	Understanding	BTL2
5	Compare and contrast different types of malicious software (malware), highlighting their functionalities and potential impact on systems.	16	Analyzing	BTL4
6	Describe common attack vectors used by cybercriminals to exploit vulnerabilities in computer systems and networks.	16	Applying	BTL3
7	Discuss the role of social engineering in cybersecurity attacks, providing examples of common techniques used by attackers.	16	Analyzing	BTL4
8	Analyze the scope of cyber-attacks in today's interconnected world, considering factors such as motives, targets, and impact.	16	Analyzing	BTL4
9	Explain the concept of wireless network attacks and discuss common strategies employed by attackers to compromise wireless networks.	16	Understanding	BTL2
10	Outline the various tools and techniques used for conducting web application attacks, highlighting methods for exploiting vulnerabilities.	16	Understanding	BTL2
11	Discuss the importance of implementing countermeasures to mitigate the risks posed by cyber-attacks, providing examples of effective strategies.	16	Analyzing	BTL4
12	Evaluate the impact of a security breach on an organization's reputation and financial stability, considering both short-term and long-term effects.	16	Evaluating	BTL5
13	Describe the steps involved in conducting a security risk assessment for an organization's IT infrastructure.	16	Applying	BTL3
14	Discuss the challenges associated with securing Internet of Things (IoT) devices against cyber-attacks, considering factors such as scalability and diversity.	16	Analyzing	BTL4
15	Explain the concept of zero-day vulnerabilities and their significance in cybersecurity, discussing strategies for mitigating the risks associated with them.	16	Understanding	BTL2
16	Analyze the role of encryption in protecting sensitive data from unauthorized access, discussing its strengths and limitations.	16	Analyzing	BTL4
17	Discuss the importance of security awareness training for employees in preventing social engineering attacks, providing examples of effective training methods.	16	Analyzing	BTL4

UNIT – III : RECONNAISSANCE

Harvester – Whois – Netcraft – Host – Extracting Information from DNS – Extracting Information from E-mail Servers – Social Engineering Reconnaissance; Scanning – PortScanning – Network Scanning and Vulnerability Scanning – Scanning Methodology – Ping Sweer Techniques – Nmap Command Switches.

UNIT-III [PART-A]- 2 Marks

Q.No	Question	Competence	Level
1	What is the primary function of a harvester in cybersecurity?	Understanding	BTL2
2	What information can typically be obtained from a WHOIS lookup?	Understanding	BTL2
3	How can WHOIS data be used in cybersecurity investigations?	Understanding	BTL2
4	How can Netcraft be used to detect phishing sites?	Understanding	BTL2
5	How can the host command be used to find the IP address of a domain?	Understanding	BTL2
6	What is a DNS zone transfer and why is it significant?	Understanding	BTL2
7	Name two types of DNS records that can provide valuable information about a domain.	Understanding	BTL2
8	What is the purpose of an MX record in DNS?	Understanding	BTL2
9	Describe the role of SPF records in email server configuration.	Understanding	BTL2
10	Explain how email headers can be used to trace the origin of an email.	Analyzing	BTL4
11	What is social engineering reconnaissance?	Understanding	BTL2
12	How can social media platforms be used in social engineering reconnaissance?	Understanding	BTL2
13	What is the purpose of port scanning in network security?	Understanding	BTL2
14	Name two tools commonly used for port scanning.	Understanding	BTL2
15	Explain the difference between TCP SYN scan and TCP Connect scan.	Understanding	BTL2
16	What is network scanning and why is it important in cybersecurity?	Analyzing	BTL4
17	Describe one common technique used in network scanning.	Understanding	BTL2
18	How does a ping sweep work in network scanning?	Analyzing	BTL4
19	Name two popular tools used for vulnerability scanning.	Understanding	BTL2
20	How does vulnerability scanning help in risk management?	Analyzing	BTL4
21	What is a ping sweep and why is it used in network scanning?	Understanding	BTL2
22	Name one tool that can be used to perform a ping sweep.	Understanding	BTL2
23	Describe how a ping sweep can identify active hosts on a network.	Understanding	BTL2
24	What is one limitation of using ICMP echo requests in a ping sweep?	Understanding	BTL2

UNIT -III [PART-B]

Q.No	Question	Marks	Competence	Level
1	Discuss the various techniques used in social engineering reconnaissance to gather information about a target.	16	Understanding	BTL2
2	Analyze the role of social media in social engineering reconnaissance. How can organizations protect themselves against information leakage through social media?	16	Analyzing	BTL4
3	Compare and contrast different types of port scanning techniques.	16	Analyzing	BTL4

4	Explain the ethical considerations and legal implications of port scanning. When is port scanning considered illegal, and how can security professionals conduct port scanning responsibly?	16	Understanding	BTL2
5	Describe the process of network scanning and its importance in network security.	16	Understanding	BTL2
6	Evaluate the effectiveness of different network scanning techniques. How can these techniques be used to map a network and identify potential security weaknesses?	16	Evaluating	BTL5
7	Explain the process of vulnerability scanning in detail. Discuss how vulnerability scanners work, the types of vulnerabilities they can detect, and the role of vulnerability scanning in a comprehensive security strategy.	16	Understanding	BTL2
8	Outline a comprehensive scanning methodology for a network security assessment. Include the steps involved, tools used, and best practices for each phase of the scanning process.	16	Understanding	BTL2
9	Analyze the importance of scanning methodology in the context of penetration testing.	16	Analyzing	BTL4
10	Evaluate the effectiveness of various ping sweep techniques in different network environments.	16	Evaluating	BTL5
11	Discuss how Nmap can be used for different types of scans and the information that can be obtained from these scans.	16	Analyzing	BTL4
12	Discuss how Nmap can be used to identify vulnerabilities in a network. Include an explanation of specific Nmap scripts and how they can be leveraged in vulnerability assessment.	16	Analyzing	BTL4
13	Describe a real-world scenario where social engineering reconnaissance led to a successful cyberattack.	16	Understanding	BTL2
14	Provide a case study of a network security assessment where port scanning played a critical role. Discuss the findings, impact, and remediation measures taken.	16	Analyzing	BTL4
15	Discuss a case where vulnerability scanning identified critical security flaws in an organization's network.	16	Analyzing	BTL4
16	Evaluate the role of Nmap in a comprehensive security strategy. Provide an example of how Nmap was used in a real-world security assessment to identify and mitigate potential threats.	16	Evaluating	BTL5
17	Discuss the importance of regular security assessments and audits in maintaining an organization's cybersecurity posture.	16	Analyzing	BTL4

UNIT – IV : INTRUSION DETECTION

Host -Based Intrusion Detection – Network -Based Intrusion Detection – Distributed orHybrid Intrusion Detection – Intrusion Detection Exchange Format – Honeypots – Example System Snort.

UNIT -IV [PART-A]- 2 Marks

Q.No	Question	Competence	Level
1	Define host-based intrusion detection (HIDS) and provide an example.	Remembering	BTL1
2	How does HIDS differ from network-based intrusion detection (NIDS)?	Understanding	BTL2
3	What are the primary advantages of using HIDS?	Understanding	BTL2
4	Explain the typical components of a HIDS system.	Remembering	BTL1
5	Compare signature-based and anomaly-based detection in HIDS.	Analyzing	BTL4
6	Discuss the challenges of deploying HIDS in cloud environments.	Understanding	BTL2

7	How can HIDS contribute to incident response processes?	Understanding	BTL2
8	Name two popular HIDS tools and their key features.	Remembering	BTL1
9	What are the limitations of HIDS?	Understanding	BTL2
10	Describe a scenario where HIDS would be more effective than NIDS.	Analyzing	BTL4
11	Define network-based intrusion detection (NIDS) and provide an example.	Remembering	BTL1
12	How does NIDS analyze network traffic to detect intrusions?	Understanding	BTL2
13	Discuss the advantages of using NIDS in a network security architecture.	Understanding	BTL2
14	Compare signature-based and anomaly-based detection in NIDS.	Analyzing	BTL4
15	What are the challenges of detecting encrypted traffic with NIDS?	Understanding	BTL2
16	How does NIDS handle false positives and false negatives?	Understanding	BTL2
17	Name two popular NIDS tools and their functionalities.	Remembering	BTL1
18	Explain how NIDS contributes to real-time threat intelligence sharing.	Understanding	BTL2
19	Discuss the role of NIDS in detecting insider threats.	Understanding	BTL2
20	Define distributed intrusion detection systems (DIDS) and their advantages.	Remembering	BTL1
21	How does a hybrid intrusion detection approach combine HIDS and NIDS?	Understanding	BTL2
22	Give an example of a hybrid IDS system and describe its components.	Analyzing	BTL4
23	Compare the performance considerations of DIDS versus standalone IDS.	Analyzing	BTL4
24	Explain how DIDS scales in a large enterprise network.	Understanding	BTL2

UNIT -IV [PART-B]

Q.No	**Question**	**Marks**	**Competence**	**Level**
1	Explain the architecture of a typical host-based intrusion detection system (HIDS) and discuss the role of each component in detecting and responding to intrusions.	16	Understanding	BTL2
2	Compare and contrast signature-based and anomaly-based detection methods in HIDS. What are the advantages and limitations of each approach?	16	Analyzing	BTL4
3	Discuss the challenges associated with deploying and managing HIDS in a dynamic and distributed computing environment, such as cloud infrastructure or containerized environments.	16	Analyzing	BTL4
4	Describe how HIDS integrates with host operating systems and other security tools to enhance overall security posture.	16	Analyzing	BTL4
5	Explain the process of incident response in the context of HIDS.	16	Understanding	BTL2
6	Outline the architecture of a network-based intrusion detection system (NIDS) and explain the function of each component in monitoring network traffic for potential threats.	16	Understanding	BTL2
7	Compare the detection capabilities of signature-based and anomaly-based methods in NIDS.	16	Analyzing	BTL4

8	Discuss the challenges NIDS faces in detecting advanced persistent threats (APTs) and encrypted network traffic.	16	Analyzing	BTL4
9	Describe the integration of NIDS with other network security tools, such as firewalls and SIEM systems.	16	Understanding	BTL2
10	Explain the role of NIDS in supporting regulatory compliance requirements, such as PCI DSS or GDPR.	16	Understanding	BTL2
11	Define distributed intrusion detection systems (DIDS) and hybrid intrusion detection systems.	16	Understanding	BTL2
12	Discuss the operational challenges and potential security risks associated with implementing a DIDS or hybrid IDS solution across geographically dispersed locations or diverse network environments.	16	Analyzing	BTL4
13	Explain the role of central management and coordination in a DIDS architecture. How does centralized management facilitate effective threat detection and response?	16	Understanding	BTL2
14	Compare the performance considerations of DIDS versus standalone HIDS and NIDS.	16	Analyzing	BTL4
15	Define the Intrusion Detection Message Exchange Format (IDMEF) and explain its significance in standardizing communication between different IDS systems.	16	Understanding	BTL2
16	Describe the structure and key components of an IDMEF message.	16	Understanding	BTL2
17	Explain how IDMEF supports incident response and forensic analysis processes.	16	Understanding	BTL2

UNIT – V : INTRUSION PREVENTION

Firewalls and Intrusion Prevention Systems: Need for Firewalls – Firewall Characteristics and Access Policy – Types of Firewalls – Firewall Basing – Firewall Location and Configurations –Intrusion Prevention Systems – Example Unified Threat Management Products.

[PART-A]- 2 Marks

Q.No	Question	Competence	Level
1	What is the primary function of a firewall in network security?	Remembering	BTL1
2	Explain the difference between stateful inspection and packet filtering in firewalls.	Understanding	BTL2
3	Discuss the role of access control lists (ACLs) in firewall rules.	Understanding	BTL2
4	What are the characteristics of a next-generation firewall (NGFW)?	Understanding	BTL2
5	Compare hardware-based and software-based firewalls.	Analyzing	BTL4
6	How does a firewall enforce security policies on incoming and outgoing traffic?	Understanding	BTL2
7	Describe the concept of firewall basing and its implications.	Understanding	BTL2
8	What is the role of proxy servers in firewall architectures?	Understanding	BTL2
9	Explain the importance of default-deny and default-allow policies in firewall configurations.	Understanding	BTL2
10	Discuss the benefits and limitations of application-layer firewalls.	Understanding	BTL2
11	Where should a firewall typically be placed in a network architecture and why?	Understanding	BTL2
12	Explain the concept of firewall DMZ (Demilitarized Zone) and its	Understanding	BTL2

	purpose.		
13	What considerations are important when configuring a firewall for a cloud environment?	Understanding	BTL2
14	Describe the role of network address translation (NAT) in firewall configurations.	Understanding	BTL2
15	How can firewalls be configured to protect against application layer attacks?	Understanding	BTL2
16	Discuss the challenges in managing firewall rules across a large enterprise network.	Understanding	BTL2
17	Compare stateful and stateless firewall inspection methods.	Analyzing	BTL4
18	What are the advantages and disadvantages of deploying a virtual firewall?	Understanding	BTL2
19	Explain the concept of a transparent firewall and its benefits.	Understanding	BTL2
20	How does a web application firewall (WAF) differ from traditional firewalls?	Understanding	BTL2
21	Define intrusion prevention systems (IPS) and distinguish them from intrusion detection systems (IDS).	Remembering	BTL1
22	Discuss the inline and passive modes of deployment for IPS.	Understanding	BTL2
23	How do IPS systems use signatures and heuristics to detect and prevent attacks?	Understanding	BTL2
24	Explain the role of deep packet inspection (DPI) in IPS operations.	Understanding	BTL2

UNIT -V [PART-B] – 16 Marks

Q.No	Question	Marks	Competence	Level
1	Explain the architecture of a typical host-based intrusion detection system (HIDS) and discuss the role of each component in detecting and responding to intrusions.	16	Understanding	BTL2
2	Compare and contrast signature-based and anomaly-based detection methods in HIDS. What are the advantages and limitations of each approach?	16	Analyzing	BTL4
3	Describe the firewall basing configurations (host-based, network-based, and cloud-based).	16	Analyzing	BTL4
4	Discuss the advantages and disadvantages of each configuration with respect to network security management and protection against cyber threats.	16	Evaluating	BTL5
5	Discuss the factors that organizations should consider when determining the placement of firewalls within their network architecture.	16	Evaluating	BTL5
6	Describe the role and functionality of intrusion prevention systems (IPS) in network security.	16	Understanding	BTL2
7	Compare and contrast signature-based and behavior-based IPS technologies.	16	Analyzing	BTL4
8	Explain the concept of unified threat management (UTM).	16	Understanding	BTL2
9	Discuss the challenges and considerations organizations face when deploying and managing intrusion prevention systems.	16	Analyzing	BTL4
10	Examine the integration of intrusion prevention systems with other security technologies such as firewalls, SIEM and endpoint protection platforms.	16	Evaluating	BTL5
11	Explain the role of firewalls in network security. Discuss the key characteristics of firewalls .	16	Understanding	BTL2

12	Compare and contrast different types of firewalls. Provide scenarios where each type would be most effective.	16	Analyzing	BTL4
13	Describe the different types of firewalls (packet-filtering, stateful inspection, proxy, and next-generation firewalls).	16	Analyzing	BTL4
14	Discuss the concept of firewall basing (host-based, network-based, and cloud-based). What are the advantages and disadvantages of each configuration?	16	Analyzing	BTL4
15	Explain the importance of firewall access policies. Discuss the components of an effective access policy and provide examples of rules and criteria that should be included to enhance network security.	16	Evaluating	BTL5
16	How do IPS differ from firewalls and other security measures in terms of threat detection and response?	16	Evaluating	BTL5
17	Describe the role and functionality of intrusion prevention systems (IPS) in network security.	16	Understanding	BTL2