



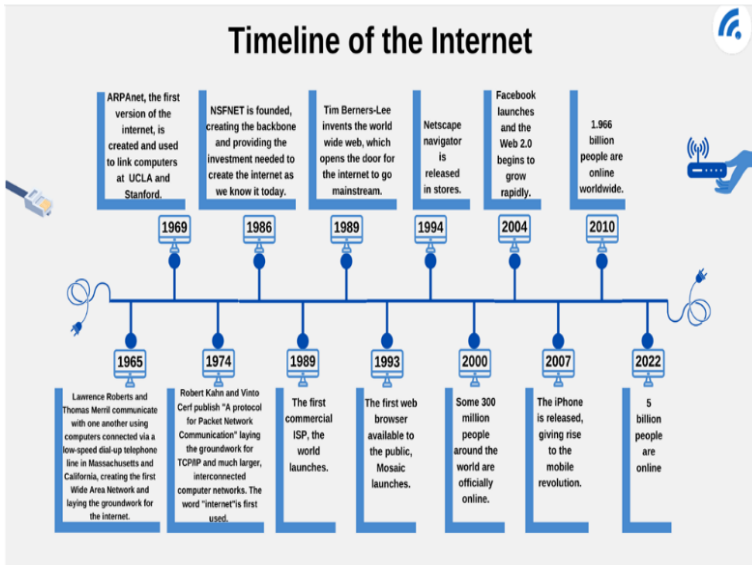
RV College of Engineering®
Department of Computer Science and Engineering
CIE - I: Test Paper

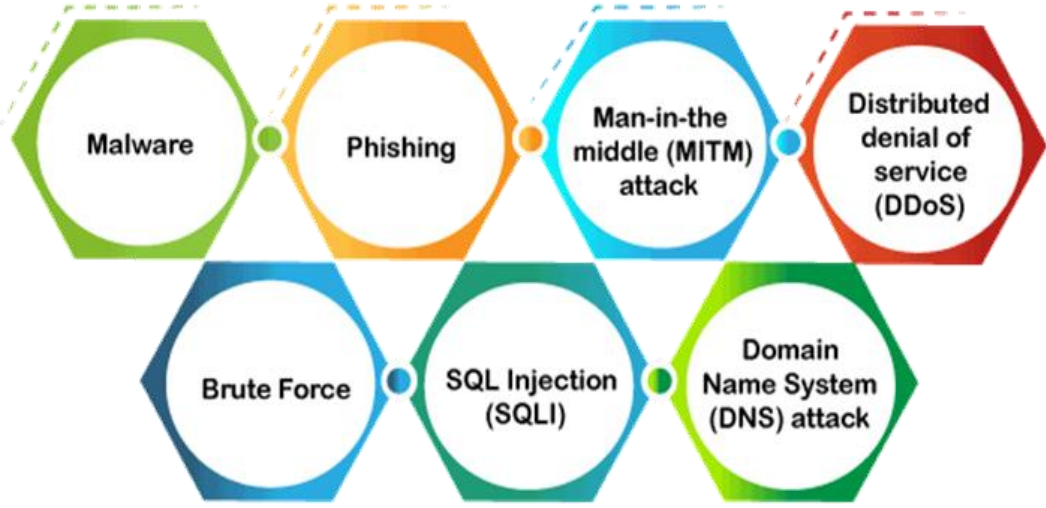
Course & Code

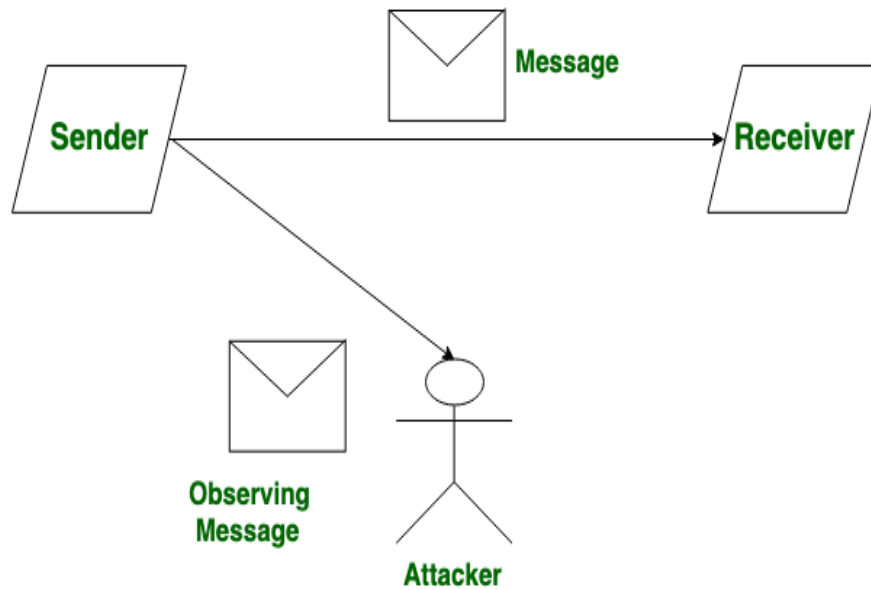
INTRODUCTION TO CYBER SECURITY
(CS124BTF)

Semester: II

Scheme & Solutions

Sl.no.	Questions	Marks																											
1.a	<p>Evolution phase of the Internet</p>  <p>Timeline of the Internet</p> <ul style="list-style-type: none"> 1965: Lawrence Roberts and Thomas Merrill communicate with one another using computers connected via a low-speed dial-up telephone line in Massachusetts and California, creating the first Wide Area Network and laying the groundwork for the Internet. 1969: ARPANet, the first version of the Internet, is created and used to link computers at UCLA and Stanford. 1974: Robert Kahn and Vinton Cerf publish "A protocol for Packet Network Communication" laying the groundwork for TCP/IP and much larger, interconnected computer networks. The word "Internet" is first used. 1986: NSFNET is founded, creating the backbone and providing the investment needed to create the Internet as we know it today. 1989: The first commercial ISP, the world launches. 1989: Tim Berners-Lee invents the world wide web, which opens the door for the Internet to go mainstream. 1993: The first web browser available to the public, Mosaic launches. 1994: Netscape navigator is released in stores. 2000: Some 300 million people around the world are officially online. 2004: Facebook launches and the Web 2.0 begins to grow rapidly. 2007: The iPhone is released, giving rise to the mobile revolution. 2010: 1.966 billion people are online worldwide. 2022: 5 billion people are online. 	06																											
1.b	<table border="1"> <thead> <tr> <th>Parameters</th><th>CYBER SECURITY</th><th>INFORMATION SECURITY</th></tr> </thead> <tbody> <tr> <td>Basic Definition</td><td>It is the practice of protecting the data from outside the resource on the internet.</td><td>It is all about protecting information from unauthorized users, access, and data modification or removal in order to provide confidentiality, integrity, and availability.</td></tr> <tr> <td>Protect</td><td>It is about the ability to protect the use of cyberspace from cyber attacks.</td><td>It deals with the protection of data from any form of threat.</td></tr> <tr> <td>Scope</td><td>Cybersecurity to protect anything in the cyber realm.</td><td>Information security is for information irrespective of the realm.</td></tr> <tr> <td>Threat</td><td>Cybersecurity deals with the danger in cyberspace.</td><td>Information security deals with the protection of data from any form of threat.</td></tr> <tr> <td>Attacks</td><td>Cybersecurity strikes against Cyber crimes, cyber frauds, and law enforcement.</td><td>Information security strikes against unauthorized access, disclosure modification, and disruption.</td></tr> <tr> <td>Professionals</td><td>Cyber security professionals deal with the prevention of active threats or Advanced Persistent threats (APT).</td><td>Information security professionals are the foundation of data security and security professionals associated with it are responsible for policies, processes, and organizational roles and responsibilities that assure confidentiality, integrity, and availability.</td></tr> <tr> <td>Deals with</td><td>It deals with threats that may or may not exist in the cyber realm such as protecting your social media account, personal information, etc.</td><td>It deals with information Assets and integrity, confidentiality, and availability.</td></tr> <tr> <td>Defense</td><td>Acts as first line of defense.</td><td>Comes into play when security is breached.</td></tr> </tbody> </table>	Parameters	CYBER SECURITY	INFORMATION SECURITY	Basic Definition	It is the practice of protecting the data from outside the resource on the internet.	It is all about protecting information from unauthorized users, access, and data modification or removal in order to provide confidentiality, integrity, and availability.	Protect	It is about the ability to protect the use of cyberspace from cyber attacks.	It deals with the protection of data from any form of threat.	Scope	Cybersecurity to protect anything in the cyber realm.	Information security is for information irrespective of the realm.	Threat	Cybersecurity deals with the danger in cyberspace.	Information security deals with the protection of data from any form of threat.	Attacks	Cybersecurity strikes against Cyber crimes, cyber frauds, and law enforcement.	Information security strikes against unauthorized access, disclosure modification, and disruption.	Professionals	Cyber security professionals deal with the prevention of active threats or Advanced Persistent threats (APT).	Information security professionals are the foundation of data security and security professionals associated with it are responsible for policies, processes, and organizational roles and responsibilities that assure confidentiality, integrity, and availability.	Deals with	It deals with threats that may or may not exist in the cyber realm such as protecting your social media account, personal information, etc.	It deals with information Assets and integrity, confidentiality, and availability.	Defense	Acts as first line of defense.	Comes into play when security is breached.	04
Parameters	CYBER SECURITY	INFORMATION SECURITY																											
Basic Definition	It is the practice of protecting the data from outside the resource on the internet.	It is all about protecting information from unauthorized users, access, and data modification or removal in order to provide confidentiality, integrity, and availability.																											
Protect	It is about the ability to protect the use of cyberspace from cyber attacks.	It deals with the protection of data from any form of threat.																											
Scope	Cybersecurity to protect anything in the cyber realm.	Information security is for information irrespective of the realm.																											
Threat	Cybersecurity deals with the danger in cyberspace.	Information security deals with the protection of data from any form of threat.																											
Attacks	Cybersecurity strikes against Cyber crimes, cyber frauds, and law enforcement.	Information security strikes against unauthorized access, disclosure modification, and disruption.																											
Professionals	Cyber security professionals deal with the prevention of active threats or Advanced Persistent threats (APT).	Information security professionals are the foundation of data security and security professionals associated with it are responsible for policies, processes, and organizational roles and responsibilities that assure confidentiality, integrity, and availability.																											
Deals with	It deals with threats that may or may not exist in the cyber realm such as protecting your social media account, personal information, etc.	It deals with information Assets and integrity, confidentiality, and availability.																											
Defense	Acts as first line of defense.	Comes into play when security is breached.																											

2.a	<p>A threat in cybersecurity is a malicious activity by an individual or organization to corrupt or steal data, gain access to a network, or disrupt digital life in general. <i>List of all threats- 02 marks, explanation – 06 marks</i></p> <p style="text-align: center;">Types of Cyber Threats</p> 	06
2.b	<p>Security System Development Life Cycle (SecSDLC) is defined as the set of procedures that are executed in a sequence in the software development cycle (SDLC). It is designed such that it can help developers to create software and applications in a way that reduces the security risks at later stages significantly from the start. SecSDLC eliminates security vulnerabilities. Its process involves identification of certain threats and the risks they impose on a system as well as the needed implementation of security controls to counter, remove and manage the risks involved. ---2 M</p> <p>Phases involved are as follows:</p> <ol style="list-style-type: none"> 1.System Investigation 2.System Analysis 3.Logical Design 4.Physical Design 5.Implementation 6.Maintenance ---2 M 	04
3.a	<p>Passive attacks</p> <ul style="list-style-type: none"> • Gathering information about a target without his/her knowledge • Internet searches or by googling. <p>Passive Attacks: Passive Attacks are the type of attacks in which, The attacker observes the content of messages or copy the content of messages. Passive Attack is a danger for Confidentiality. Due to passive attack, there is no any harm to the system. The most important thing is that In passive attack, Victim does not get informed about the attack.</p>	06



Passive Attack

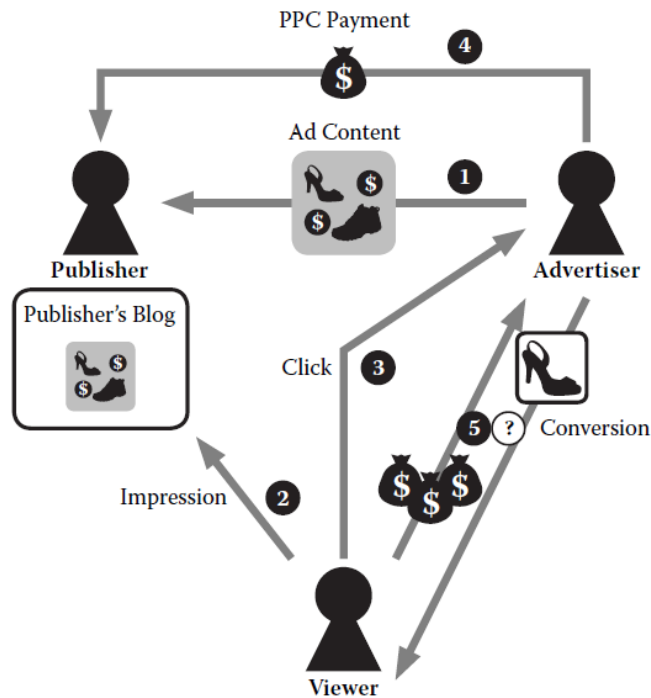
In passive attacks, the attacker observes the messages, then copy and save them and can use it for malicious purposes. The attacker does not try to change the information or content he/she gathered. Although passive attacks do not harm the system, they can be a danger for the confidentiality of the message.

- In passive attacks, the attacker observes the messages, then copy and save them and can use it for malicious purposes.
- In passive attacks, information remains unchanged.
- Unlike active attacks, in passive attacks, victims do not get informed about the attack.
- The passive attacks do not harm the system.
- In passive attacks, the system resources remain unchanged.
- They can be dangerous for confidentiality of the message.
- In active attacks, attention is on prevention.
- It involves traffic analysis, the release of a message.
- Unlike active attacks, passive attacks are easy to prohibit.

Passive attack and explanation – 3 marks

3 tools with explanation – 3 marks

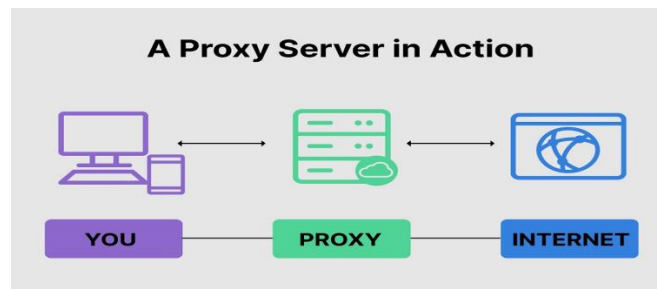
3.b



- Pay-per-click is a model of digital advertising where the advertiser pays a fee each time one of their ads is clicked.
- Stake holders involved in this model and their role are
- Advertiser, Publisher, and the Viewer
- The advertiser is a company that produces content it would like to display to potential customers.
- The publisher is a creative outlet that produces content that will draw visitors to its medium
- Visitors view the ad and, ideally, purchase the advertised product or service.

Diagram – 2 marks Explanation – 2 marks

4.a



In computer networking, a proxy server is a server application that acts as an intermediary between a client requesting a resource and the server

Attackers use proxies to:

1. IP address masking
2. Anonymity
3. Geographical obfuscation
4. Access control bypass
5. Traffic encryption

06

4.b	<p>While filling the application:</p> <ul style="list-style-type: none"> • Stay with computer: should not leave system un-attended. • Be alert: careful about the shoulder snooping for username and password. • Use Virtual Keyboard: Better to use s/w keyboard to avoid the hacking for pin. • while doing online fee payment. • Security warnings: warning messages posted by financial organizations while accessing the financial accounts in cyber cafe 2 marks <p>After filling the application:</p> <ul style="list-style-type: none"> • Always logout: Logout of the services that were used with username and password credentials • Change password: Change the password / pin of the financial account on your personal lap-top or Desktop 2 marks 	
5.a	Analyze the steps involved in “How the criminals plan their attack” Justify your answer.	06
5.b	Explanation for Shoulder surfing -2 marks Dumpster Driving -2 marks	04