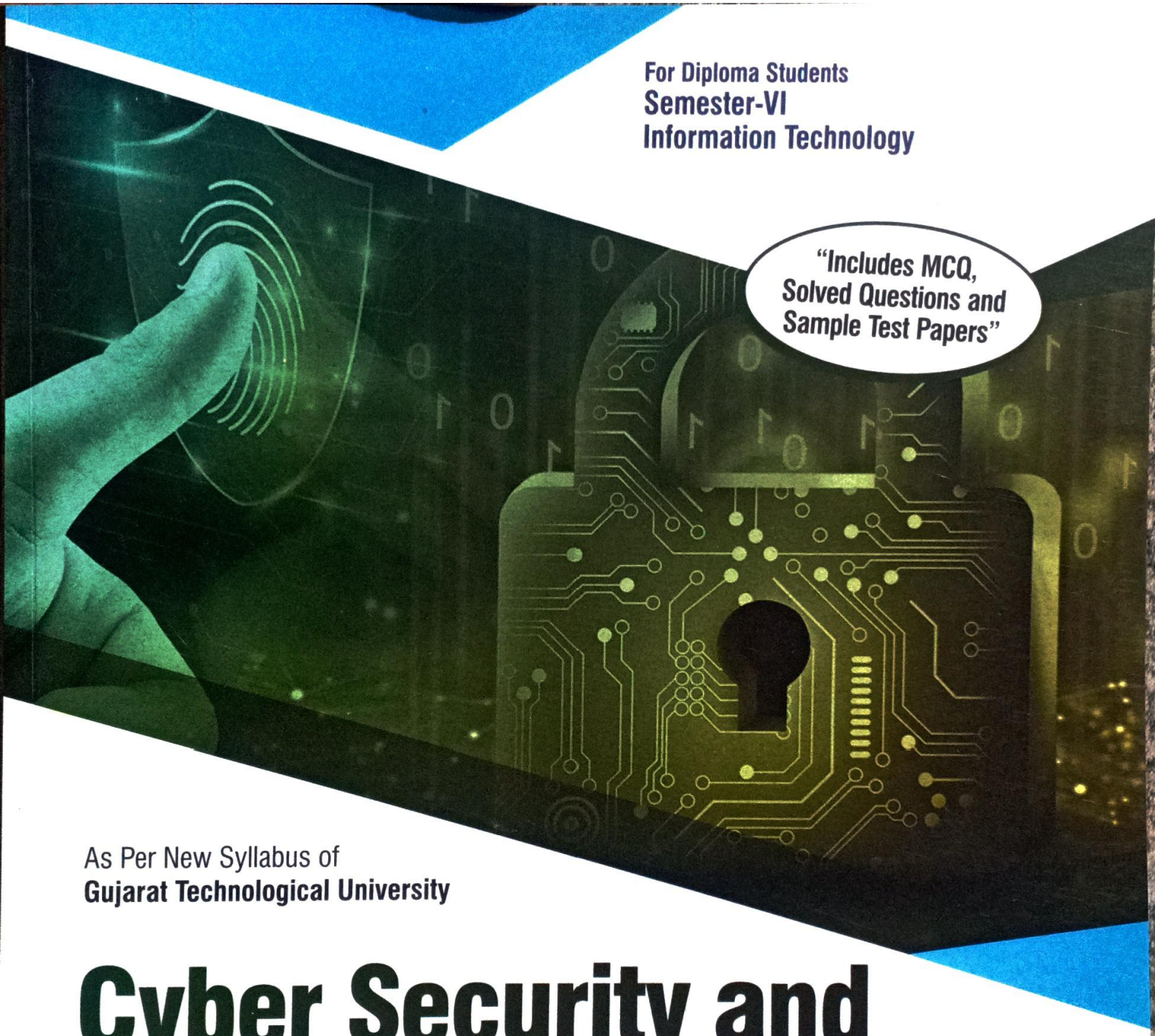
For Diploma Students
Semester-VI
Information Technology



"Includes MCQ, Solved Questions and Sample Test Papers"

As Per New Syllabus of
Gujarat Technological University

Cyber Security and Digital Forensics

J. B. Patel | H. K. Patel | D. K. Thakar

ATUL PRAKASHAN™
GANDHI ROAD, AHMEDABAD.

As per the New Syllabus of Gujarat Technological University (GTU)

This book is specially written for students of

Diploma Information Technology

Semester-6

Subject Code : 4361601

CYBER SECURITY AND DIGITAL FORENSICS

Authors

J. B. Patel
M.E., C.E.
Lecturer, Government Polytechnic, **Dahod.**

H. K. Patel
B.E., I.T.
Sr. Lecturer, SAL Institute of Diploma Studies
Ahmedabad.

D. K. Thakar
B.E., C.E.
Lecturer, SAL Institute of Diploma Studies
Ahmedabad.

First Edition : 2024 - 2025

Price : ₹ 150-00

ATUL PRAKASHAN
GANDHI ROAD, AHMEDABAD.

GUJARAT TECHNOLOGICAL UNIVERSITY (GTU)

Competency-focused Outcome-based Green Curriculum-2021 (COGC-2021)

Diplopa for Information Technology

Subject Code : 4361601

Semester-6

Subject Name : Cyber Security and Digital Forensics

Teaching and Examination Scheme :

Teaching Scheme (In hours)			Total Credits (L+T/2+P/2)	Examination Scheme				Total Marks
				Theory Marks		Practical Marks		
L	T	P	C	CA*	ESE	CA	ESE	
4	–	4	6	30	70	25	25	150

(*) : Out of 30 marks under the theory CA, 10 marks are for assessment of the micro-project to facilitate integration of COs and the remaining 20 marks is the average of 2 tests to be taken during the semester for the assessing the attainment of the cognitive domain UOs required for the attainment of the COs.

Legends : L – Lecture; **T** – Tutorial/Teacher Guided Theory Practice; **P** – Practical; **C** – Credit, **CA** – Continuous Assessment; **ESE** – End Semester Examination.

Underpinning Theory

Unit	Unit Outcomes (UOs)	Topics and Sub-topics
Unit – I Introduction of Information Security and Cryptography	1a. Learn about how to maintain the Confidentiality, Integrity and Availability of a data. 1b. Analyze and design hash and MD5 algorithms.	1.1. Basic Concept of Information Security 1.2. CIA Triad 1.3. OSI Security Architecture (Security Servic Mecha-nisms and Attacks) 1.4. Private & Public Key Cryptography 1.5. Message Digest 5 Hashing & SHA
Unit– II Network and System security	2a. To understand various protocols for network security to protect against the threats in the networks. 2b. Understand the threats and risks to modern data and information systems. 2c. Understand the working and configuration of firewall.	2.1. Types of attacks 2.2. Digital signatures : Definition and Properties 2.3. Pretty Good Privacy (PGP)(brief) 2.4. Secure Socket Layer and Transport Layer Security 2.5. IPsec 2.6. HTTPS (Connection initiation & Connection closure) 2.7. Malicious software: Virus and Related Threats (Trojans, Rootkit, Backdoors, keylogger) 2.8. Firewall : Need and Types 2.9. Proxy Server : Need and Types
Unit – III Cyber Crime	3a. Understand the cybercrimes from the nature of the crime. 3b. Analyze various aspects of Cyber-crimes. 3c. Understand the security and privacy methods in development of modern applications and in organizations to protect people and to prevent cyber-crimes.	3.1 Overview of Cybercrime • Definition • Cybercriminals • Cybercrime 3.2 Classification of cyber-crimes 3.2.1. Organization a. Email Bombing b. Salami Attack c. Logic Bomb d. Trojan Horse e. Web Jacking f. Data diddling

Unit	Unit Outcomes (UOs)	Topics and Sub-topics
	3d. Analyze how particular social engineering attacks are important consideration for cyber security. 3e. Understand the Objectives and features of IT ACT, 2008.	g. Denial of Service/Distributed h. Ransomware 3.2.2. Individual a. Cyber bullying b. Cyber stalking c. Cyber defamation d. Phishing e. Cyber fraud and Cyber theft f. Spyware g. Email spoofing h. Man in the middle attack 3.2.3. Society a. Cyber pornography b. Cyber terrorism c. cyber spying d. Social Engineering Attack e. Online gambling 3.2.4. Property a. Credit Card Fraud b. Software Piracy c. Copyright infringement d. Trademarks violations 3.3 Challenges & Prevention of Cyber Crime 3.4 Cyber Law The Information Technology ACT, 2008 OFFENCES • Section 65 • Section 66 • Section 67
Unit– IV Ethical Hacking	4a. Understand the ethical behaviour with unethical behaviour. 4b. Understand basic terminologyas it relates to the Kali Linux distri-bution. 4c. To learn about various types of attacks, attackers and security threats and vulnerabilities. 4d. To learn about scanning of systems/applications and System Protection.	4.1. Concept of Hacking Types of Hackers 4.2. Basics of Ethical Hacking 4.3. The terminology of Hacking (Vulnerability, Exploit, 0-Day) 4.4. Five Steps of Hacking (Information Gathering, Scanning, Gaining Access, Maintaining Access, Covering Tracks) 4.5. Information Gathering (Active, Passive) 4.6. Introduction to Kali Linux OS • Configuration of Kali Linux • Basic Commands Kali Linux • Vulnerability Scanning/ Vulnerability Based Hacking a. Foot printing b. Scanning c. Password Cracking d. Brute Force Attacks e. Injection Attacks f. Phishing Attacks g. Block chain Attacks 4.7. Port Scanning 4.8. Remote Administration Tool (RAT) 4.9. Protect System from RAT 4.10. What is Sniffing and Mechanism of Sniffing Session Hijacking

Unit	Unit Outcomes (UOs)	Topics and Sub-topics
Unit– V DIGITAL FORENSICS	5a. Describe the basic concepts of Forensic and Branches of Digital Forensic. 5b. Interpret the cyber pieces of evidence, Digital forensic process model and their legal perspective. 5c. To understand the basic digital forensics and techniques for conducting the forensic examination on different digital devices. 5d. To understand how to examine digital evidences such as the data acquisition, identification analysis.	5.1. Introduction to Digital Forensics 5.2. Locard's Principle of Exchange in Digital Forensics 5.3. Branches of Digital Forensics • Disk / Memory Forensics • Network Forensics • Database Forensics • Software forensics • Email Forensics • Malware Forensics • Mobile Forensics 5.4. Phases of digital/computer forensics investigation • Identification • Preservation • Analysis • Documentation • Presentation 5.5. Methods to Preserve a Digital Evidence • Drive Imaging • Hash Values • Chain of Custody 5.6. Critical Steps in Preserving Digital Evidence 5.7. Evidence Role of devices as in Digital Forensics Investigations • Computing Devices • Network Devices and Servers • CCTV • Vehicles

SUGGESTED SPECIFICATION TABLE FOR QUESTION PAPER DESIGN

Unit No.	Unit Title	Teaching Hours	Distribution of Theory Marks			
			R Level	U Level	A Level	Total Marks
1	Overview of Information Security and Cryptography	08	4	4	4	12
2	Network and System Security	10	2	4	6	12
3	Cyber Crime	12	2	6	6	14
4	Ethical Hacking	14	4	6	6	16
5	Digital Forensics	12	2	8	6	16
	Total	**56**	**12**	**30**	**28**	**70**

Legends : R = Remember, U = Understand, A = Apply and above (Revised Bloom's taxonomy)

***Note** : This specification table provides general guidelines to assist students for their learning and to teachers to teach and question paper designers/setters to formulate test items/questions assess the attainment of the UOs. The actual distribution of marks at different taxonomy levels (of R, U and A) in the question paper may vary slightly from the above table.*

Contents

1. Introduction of Information Security and Cryptography ---------- 1 - 26

1.1. Introduction : Basic Concept of Information Security ---------- 02

1.2. CIA Triad ---------- 03

1.3. OSI Security Architecture (Security Servic Mecha-nisms and Attacks) ---------- 06

1.4. Private & Public Key Cryptography ---------- 08

1.5. Message Digesting, Hashing and SHA ---------- 18

Self - Assessment ---------- 26

2. Network and System Security ---------- 27 - 56

2.1. Types of attacks ---------- 28

2.2. Digital signatures ---------- 32

2.3. Pretty Good Privacy (PGP) ---------- 34

2.4. Secure Socket Layer and Transport Layer Security ---------- 35

2.5. IPsec ---------- 40

2.6. HTTPS (Connection initiation & Connection closure) ---------- 42

2.7. Malicious software ---------- 44

2.8. Firewall ---------- 48

2.9. Proxy Server ---------- 52

Self - Assessment ---------- 54

3. Cyber Crime ---------- 57 - 83

3.1 Overview of Cybercrime ---------- 57

3.2 Classification of cyber crimes ---------- 59

3.3 Challenges & Prevention of Cyber Crime ---------- 75

3.4 Cyber Law ---------- 77

Self - Assessment ---------- 83

4. Ethical Hacking ---------- 84- 120

4.1 Concept of Hacking Types of Hackers ---------- 85

4.2 Basics of Ethical Hacking ---------- 88

4.3 Hacking Terminologies ---- 88
4.4 Steps of Hacking Process ---- 91
4.5 Information Gathering ---- 92
4.6 Introduction to Kali Linux Operating System ---- 93
4.7 Port Scanning ---- 112
4.8 Remote Administration Tool (RAT) ---- 114
4.9 Protect System from RAT ---- 115
4.10 Sniffing and Mechanism of Sniffing ---- 115
Self - Assessment ---- 119

5. Digital Forensics ---- 121 - 142

5.1 Introduction to Digital Forensics ---- 122
5.2 Locard's Principle of Exchange in Digital Forensics ---- 124
5.3 Branches of Digital Forensics ---- 126
5.4 Phases of Digital Forensic Investigation ---- 133
5.5 Methods to Preserving Digital Forensic Evidence ---- 135
5.6 Critical Steps in Preserving Digital Evidence ---- 137
5.7 Role of Devices as Evidence in Digital Forensics ---- 138
Self - Assessment ---- 142

➢ **Multiple Choice Questions (MCQs) (Chapterwise) ---- 143 - 150**

- Model Question Paper-1 ---- 151
- Model Question Paper-2 ---- 152

TO THE READER

Authors and publisher would welcome suggestions towards future edition of this book or the pointing out of any misprint or obscurity. Please write to The Technical Editor, ATUL PRAKASHAN, Under Farnandis Bridge, Gandhi Road, Ahmedabad-1.

Chapter 1

INTRODUCTION OF INFORMATION SECURITY AND CRYPTOGRAPHY

1.1 INTRODUCTION : BASIC CONCEPTS OF INFORMATION SECURITY

- WHY INFORMATION SECURITY ?
- WHAT IS INFORMATION SECURITY

1.2 CIA TRIAD : FUNDAMENTAL GOALS OF INFORMATION SECURITY

- CONFIDENTIALITY
- INTEGRITY
- AVAILABILITY
- NON-REPUDIATION, AUTHENTICATION AND ACCOUNTABILITY

1.3 OSI SECURITY ARCHITECTURE

- SECURITY ATTACKS
- SECURITY MECHANISM
- SECURITY SERVICES

1.4 PRIVATE AND PUBLIC KEY CRYPTOGRAPHY

- BASIC CRYPTOGRAPHIC TERMS
- CRYPTOGRAPHIC TECHNIQUES
  - SUBSTITUTION TECHNIQUE
  - TRANSPOSITION TECHNIQUE
- PRIVATE AND PUBLIC KEY CRYPTOGRAPHY

1.5 MESSAGE DIGESTING, 5 HASHING AND SHA

- HASHING
- MESSAGE DIGEST 5 (MD 5)
- SECURE HASHING ALGORITHM(SHA)
- RSA ALGORITHM

- **Self - Assessment**

1.1 INTRODUCTION : BASIC CONCEPTS OF INFORMATION SECURITY

As we know, due to increase in hardware technology speed and internet speed, it became growing very rapidly in different domains like Autonomous Systems, E-commerce, Gaming, Natural Resource Management, Education, Space Exploration, Agriculture, Energy Management, Healthcare, Finance, Retail, Manufacturing, Automotive, Entertainment and Media, Government and Defence, Environmental Conservation, Human Resources, Hospitality and Tourism etc.

In the increasingly globalized digital economy, information assets are critical to the existence of some organizations as well as to any business. It is unacceptable for information to leak. Confidential information about a company's customers, their personal information, finances, or new product line that is obtained by a rival may result in lost revenue, legal action, or even the company's demise.

1.1.1 Why information security ?

Let us understand why information security is important for organisation as well as individuals with some real examples.

- **Protection of Sensitive Personal Information :**

  Online Banking Information security ensures that personal financial data, such as account numbers and passwords, etc are protected from hackers. In the absence of strong security protocols, internet banking systems may be breached, resulting in unapproved access to bank accounts and possible monetary losses for users.

- **Business Confidentiality :**

  Theft of Intellectual Property- Businesses greatly rely on information security to protect their product designs, trade secrets, and intellectual algorithms. If this data is not protected, rivals may obtain sensitive information and suffer large financial losses as well as a loss of competitive advantage.

- **Prevention of Data Breaches :**

  Credit card details are stored in a retail company's customer database. A cyberattack could cause a data breach if this data is improperly safeguarded, exposing the private financial information of thousands of consumers. The company's reputation suffers, regulatory fines are imposed, and the impacted customers suffer losses as well.

- **Maintaining Operational Continuity :**

  Information security guards against ransomware attacks, which have the ability to encrypt important company data and make it unreadable. In the absence of sufficient security measures, a ransomware attack has the potential to cause financial losses and service disruptions by impeding operations until a ransom is paid.

- **Compliance with Regulations :**

  General Data Protection Regulation, or GDPR, for data protection rules to be followed, information security is essential. Organizations managing personal data may face severe fines and legal repercussions if they fail to secure the data in compliance with laws like the GDPR.

- **Protection Against Cyber Threats :**

  Firewalls and antivirus software are examples of information security techniques that guard against malware infections. Without these defences, systems may be susceptible to trojans, worms, or viruses that tamper with data integrity and interfere with regular operations.

In essence, information security is crucial across various domains, including personal privacy, business operations, regulatory compliance, and safeguarding against cyber threats. It's essential to implement robust security measures to mitigate risks.

1.1.2 What is Information Security ?

Information security encompasses more than just protecting data from unwanted access. Preventing unauthorized access, use, disclosure, interruption, alteration, inspection, recording, or destruction of information is the essence of information security. Either physical or electronic information is possible. Information can refer to anything, such as your biometrics, phone number, social network profile, or other details. Therefore, a wide range of academic fields are covered by information security, including cryptography, mobile computing, cyber forensics, online social media, etc.

Effective information security requires a comprehensive approach that considers all aspects of the information environment, including technology, policies and procedures, and people.

Thus, Information security can be defined as

"The practice of protecting sensitive data, systems, networks, and information assets from unauthorized access, disclosure, alteration, destruction, or any form of cyber threat."

It encompasses a set of strategies, technologies, policies, and practices designed to ensure the confidentiality, integrity, and availability of information.

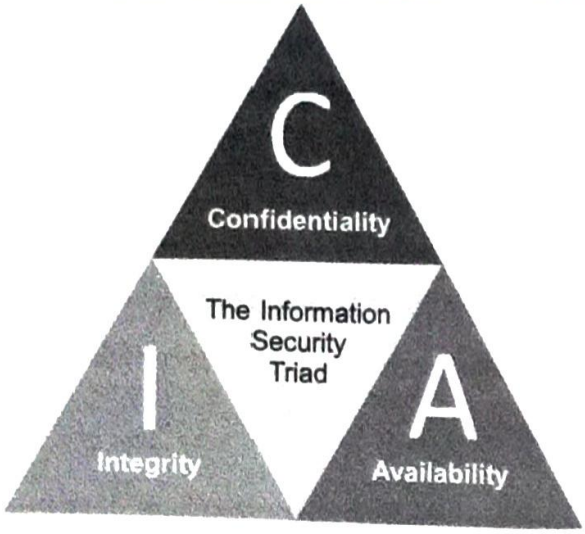
1.2 CIA TRIAD : FUNDAMENTAL OBJECTIVES

When talking about Information Security, the three fundamental objectives are Confidentiality, Integrity and Availability, commonly known as **CIA** triad which is one of the most important models designed to guide policies for information security.

CIA stands for :

1. Confidentiality
2. Integrity
3. Availability

These three CIA triad concepts are considered as fundamental objectives for achieving information security. In the below discussion we will try to understand how these three concepts are important for information security.



[Fig. 1.1 : CIA Triad-Fundamental Objectives]

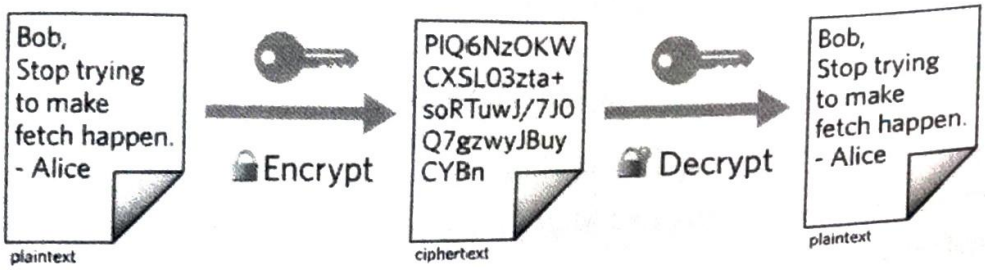
Confidentiality

"Confidentiality refers to that the information is not disclosed or revealed to unauthorised party, except the parties involved in communication."

As an illustration, let's imagine I had a password for my Gmail account, someone saw while I was doing a login into Gmail account. In that instance, confidentiality has been violated and my password has been compromised.

Unauthorized users shouldn't be able to access your personal information. The attacker might attempt to obtain your information by capturing the data with various online tools.

The use of different encryption techniques to protect our data is one of the main ways to prevent confidentiality, Because Encryption techniques prevent the attacker from being able to decrypt it, even if they manage to obtain access to it.



[Fig. 1.2 : Confidentiality using Encryption]

AES (Advanced Encryption Standard) and DES (Data Encryption Standard) are two examples of encryption standards.

Integrity

The next CIA component for discussion is integrity. *The **Integrity** refers to make sure that data has not been modified by unauthorised party.*

To check whether our data has been modified or not, we can use hash functions. Two common types of hash functions are : SHA (Secure Hash Algorithm) and MD5 (Message Direct 5).

des a general description of Security Services, Security
rity attacks.

es from an intelligent threat; that is, an intelligent
method or technique) to evade security services

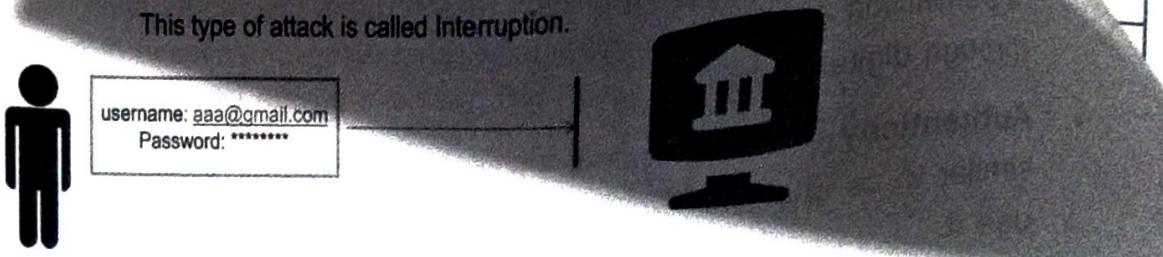
ith the goal to obtain unauthorized access
security policies that are in place in

ed by an organization.

Let's a
sive attack.
function wil
When receiver 'B' receiv
value. Now, if sender hash value =
maintained and the contents were not modified.

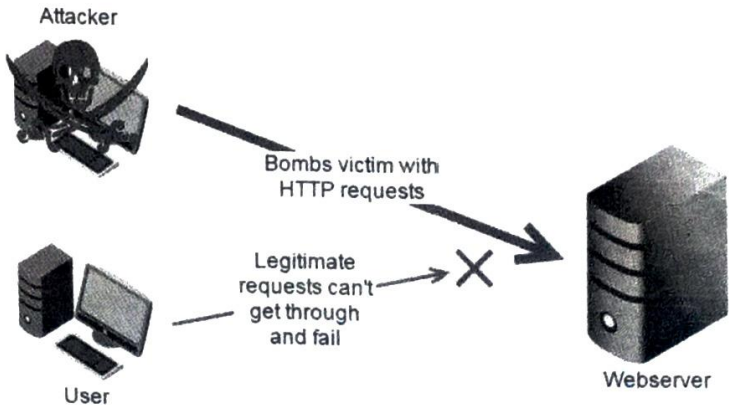
Availability

Availability *refers to ensure that, the system or network is*
authorised users. This applies to systems as well as data. Attacks such as
DDoS(Distributed Denial of Services) may render a network unavailable as the reso
get exhausted.
ge is

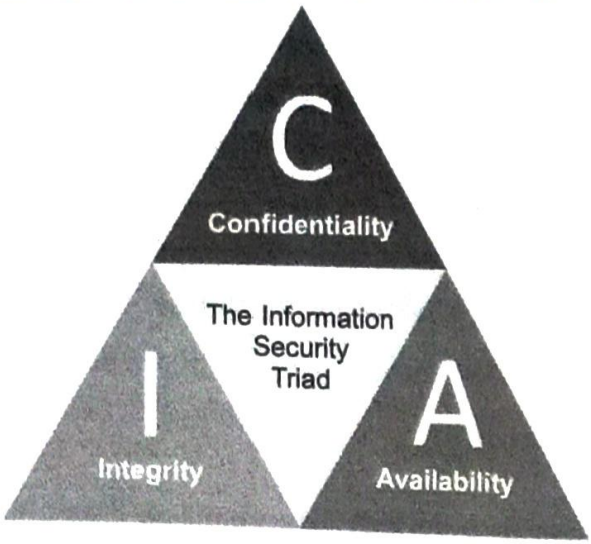


[Fig. 1.4 : Availability : Type of Interruption Attack]

To make the resources like systems, networks, or web servers unavailable to its *legitimate* users, attackers apply attacks like Denial of Services (DOS) and Distributed Denial of Services *(DDOS)*.



[Fig. 1.5 : DOS Attack to Make Resource Unavailable]



[Fig. 1.1 : CIA Triad-Fundamental Objectives]

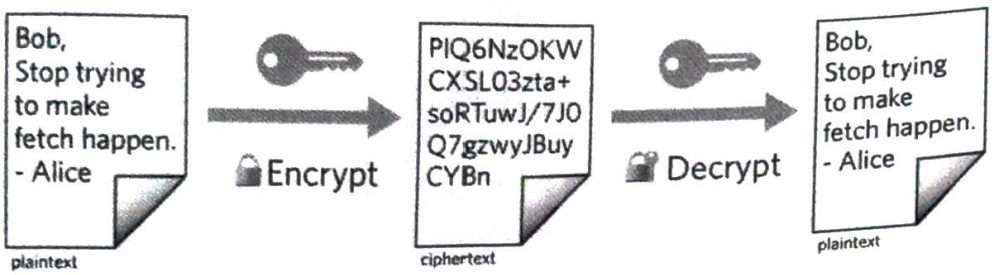
Confidentiality

"Confidentiality refers to that the information is not disclosed or revealed to unauthorised party, except the parties involved in communication."

As an illustration, let's imagine I had a password for my Gmail account, someone saw while I was doing a login into Gmail account. In that instance, confidentiality has been violated and my password has been compromised.

Unauthorized users shouldn't be able to access your personal information. The attacker might attempt to obtain your information by capturing the data with various online tools.

The use of different encryption techniques to protect our data is one of the main ways to prevent confidentiality, Because Encryption techniques prevent the attacker from being able to decrypt it, even if they manage to obtain access to it.



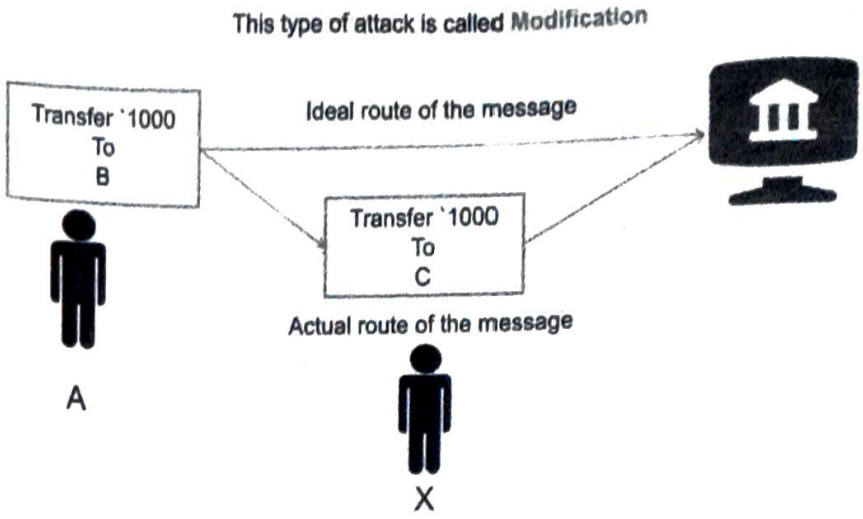
[Fig. 1.2 : Confidentiality using Encryption]

AES (Advanced Encryption Standard) and DES (Data Encryption Standard) are two examples of encryption standards.

Integrity

The next CIA component for discussion is integrity. *The **Integrity** refers to make sure that data has not been modified by unauthorised party.*

To check whether our data has been modified or not, we can use hash functions. Two common types of hash functions are : SHA (Secure Hash Algorithm) and MD5 (Message Direct 5).

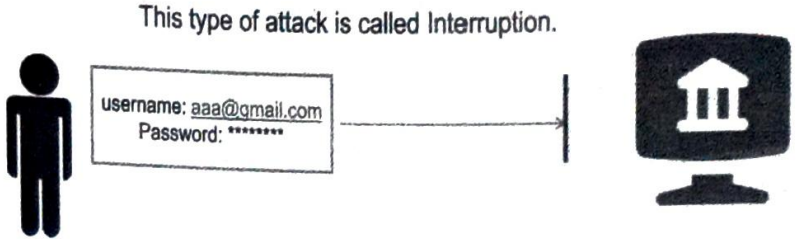


[Fig. 1.3 : Integrity : Types of Modification Attack]

Let's assume Sender 'A' wants to send data to Receiver 'B' with maintaining data integrity. A hash function will run over the data and produce an arbitrary hash value which is then attached to the data. When receiver 'B' receives the packet, it runs the same hash function over the data which gives a hash value. Now, if sender hash value = Receiver hash value, then it means that the data's integrity has been maintained and the contents were not modified.

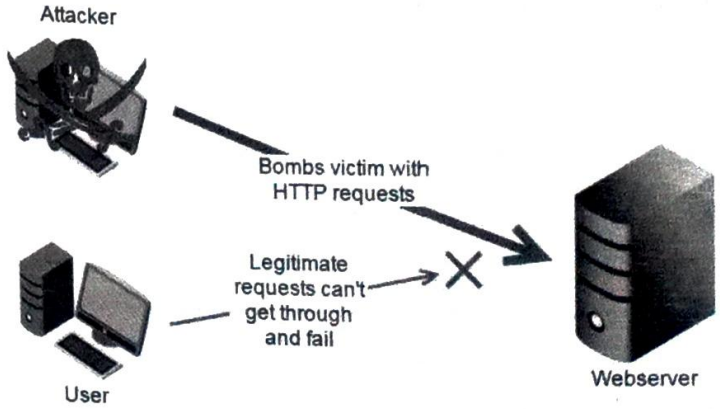
Availability

Availability *refers to ensure that, the system or network is timely and reliably available to its authorised users.* This applies to systems as well as data. Attacks such as DoS (Denial of Services or DDoS(Distributed Denial of Services) may render a network unavailable as the resources of the network get exhausted.

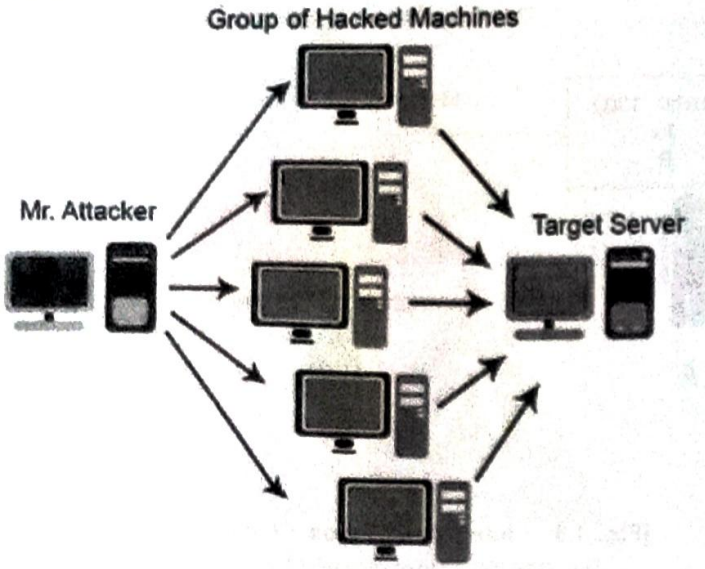


[Fig. 1.4 : Availability : Type of Interruption Attack]

To make the resources like systems, networks, or web servers unavailable to its legitimate users, attackers apply attacks like Denial of Services (DOS) and Distributed Denial of Services (DDOS).



[Fig. 1.5 : DOS Attack to Make Resource Unavailable]



[Fig. 1.6 : DDOS Attack to Make Resource Unavailable]

To ensure availability, the network administrator should maintain hardware, make regular upgrades, have a plan for fail-over, and prevent bottlenecks in a network. The impact may be significant to the companies and users who rely on the network as a business tool. Thus, proper measures should be taken to prevent such attacks.

Apart from these three TRIAD objectives, there are some other principles which governs information security.

These principles are as under :

- **Non repudiation** – non repudiation refers to that the sender can't deny about sent message or a transaction and receiver can't deny about received message or a transaction.This is achieved through digital signature signed with sender's private key
- **Authenticity** – The process of identifying someone's identification by confirming that they are similar to as what it is claiming for is known as authentication. Both the client and the server can use it.

  When someone needs to access the data, the server utilizes authentication since it needs to know who is gaining access. When the client needs to verify that the server is who it says it is, it uses it. The username and password are usually used by the server to complete the authentication process. Cards, fingerprints, voice recognition, and retinal scans are some more ways that the server can authenticate users.
- **Accountability** – means that it should be possible to trace actions of an entity uniquely to that entity. By another way, making sure every action can be tracked back to a single person, not just a group.

1.3 OSI SECURITY ARCHITECTURE

The International Telecommunication Union (ITU) recommends the Open System Interconnection (OSI) security architecture, which outlines a methodical way to specify security needs and methods to satisfy those criteria.

The OSI security architecture provides a general description of Security Services, Security mechanisms, as well as a description of security attacks.

1.3.1 Security Attacks :

Attack : An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

A security attack is an activity or act made upon a system with the goal to obtain unauthorized access to information or resources. It is usually carried out by evading security policies that are in place in organizations or individual devices.

Thus, any action that compromises the security of information owned by an organization.

Security attacks can be classified in two types : Active attack and Passive attack.

Difference between threats and attacks :

THREAT	ATTACK
Threat can be intentional or unintentional	Attack is intentional
May or may not be malicious	Attack is malicious
Circumstance that has the ability to cause damage	Objective is to cause damage
Information may or may not be altered or damaged	Chance for information alteration and damage is very high
Comparatively hard to detect	Comparatively easy to detect
Can be blocked by control of vulnerabilities	Cannot be blocked by just controlling the vulnerabilities
Can be classified into Physical threat, internal threat, external threat, human threat, and non-physical threat.	Can be classified into Virus, Spyware, Phishing, Worms, Spam, Botnets, DoS attacks, Ransom-ware, Breaches.

Threats : A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.

That is, a threat is a possible danger that might exploit a vulnerability.

1.3.2 Security Mechanism :

According to the Internet Security Glossary Version 2 (RFC 4949), a security mechanism is *"A method or process (or a device incorporating it) that can be used in a system to implement a security service that is provided by or within the system".*

Some of the examples of security mechanism are authentication exchange, checksum, digital signature, encryption, and traffic padding. Security mechanisms described in the OSI security architecture are as under :

- Specific Security Mechanisms
  - Encipherment
  - Digital Signature mechanisms
  - Access Control
  - Data Integrity
  - Authentication Exchange
  - Traffic Padding
  - Routing Control
  - Notarization
- Pervasive Security Mechanisms
  - Trusted Functionality
  - Security Label
  - Event Detection
  - Security Audit Trail
  - Security Recovery

1.3.3 Security Services :

According to the Internet Security Glossary Version 2 (RFC 4949), a security service is

"A processing or communication service that is provided by a system to give a specific kind of protection to system resources".

The OSI security architecture classifies security services as follows:

- Authentication
- Access Control Service
- Data Confidentiality
- Data integrity
- Non-repudiation

1.4 CRYPTOGRAPHY AND CRYPTOGRAPHIC TECHNIQUES

1.4.1 Basic Cryptographic Terms :

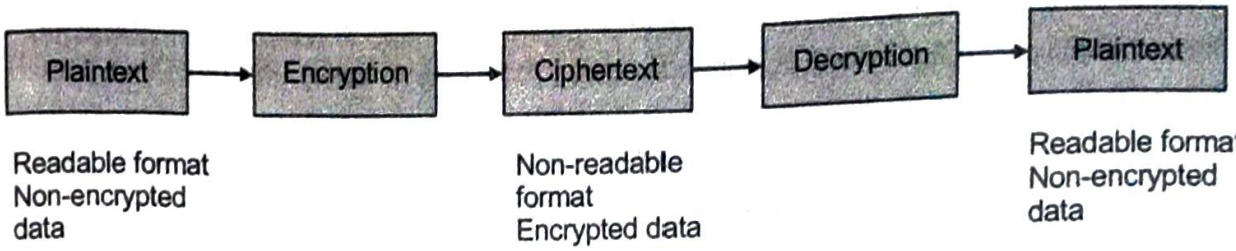
Cryptography - *"Cryptography is the art of achieving security by encoding messages to make them non-readable."*

Cryptanalysis - *"Cryptanalysis is the technique of decoding messages from a non-readable format back to a readable format without knowing how they were initially converted from readable format to nonreadable format."*

In other words, it is like breaking a code. These concepts are shown in Fig. 1.7.

Cryptology - *"Cryptology is a combination of cryptography and cryptanalysis."*

Cryptography + Cryptanalysis = Cryptology



[Fig. 1.7 : Elements of Cryptography Process]

Plaintext or Clear text - "Any original message that can be readable and understandable by the sender, the recipient, and also by anyone else who gets access to that message."

Cipher text - When any original plain-text message is codified using any suitable scheme into the form which is not understandable by other than the sender and the recipient, then such resulting message is called cipher text.

Encryption - The process of encoding plaintext messages into cipher text messages is called encryption.

Decryption -The reverse process of transforming cipher-text messages back to plain text messages is called decryption.

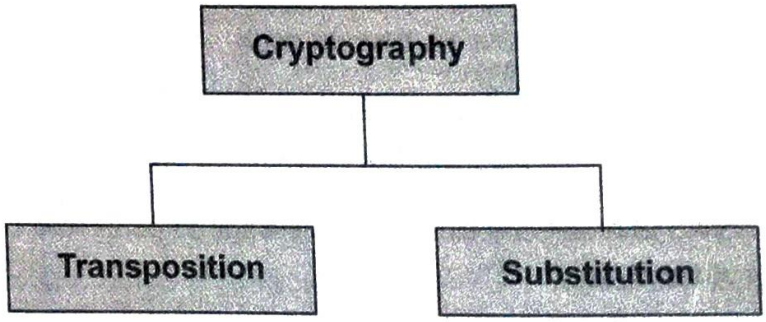
Every encryption and decryption process has two aspects : the algorithm and the key used for encryption and decryption.

1.4.2 Cryptographic techniques :

As shown in Fig. 1.8, there are two primary ways in which a plain-text message can be codified to obtain the corresponding cipher text :

A. Substitution Techniques

B. Transposition Techniques



[Fig. 1.8 : Types of Classical Cryptographic Techniques]

[A] Substitution techniques :

In the substitution-cipher technique, the characters of a plain-text message are replaced(substituted) by other characters, numbers or symbols. Some of the substitution techniques are discussed below.

- **Caesar Cipher**

Caesar cipher was the first and simplest example of substitution cipher technique. It was first proposed by Julius Caesar, and so is termed as Caesar cipher. The Caesar cipher is a special case of substitution technique wherein each alphabet in a message is replaced by an alphabet three places down the line. For instance, using the Caesar cipher, the plain-text alphabet A will become D, alphabet B will become E and so on.

Example :

Plaintext	H	E	L	L	O
Ciphertext	K	H	O	O	R

[Converting plain text into ciphertext]

The Caesar cipher is considered as a very weak scheme of cryptography. To get the original plain text message, we required to just reverse of the Caesar cipher process - i.e. replace each alphabet in a cipher-text message produced by Caesar cipher with the alphabet that is three places up the line.

Ciphertext	K	H	O	O	R
Plaintext	H	E	L	L	O

[Converting Cipher text into Plain text]

- **Modified Version of Caesar Cipher**

As we discussed, the Caesar cipher is very simple to implement but it is the weakest technique to break down. How can we complicate a Caesar cipher a bit more? Now instead of replacing each character of plaintext message by an alphabet three places down the line, we replace it with any of the remaining 25 alphabets. Once the replacement technique has been determined then it will be applied to all other alphabets in that message.

We can see that to convert the cipher text into plaintext we need to apply 25 different attempts in the worst possible case. So, we can say that the modified version of Caesar cipher more complicated to break down because we have to apply all possible permutation and combinations.

"An attack on a cipher-text message, wherein the attacker attempts to use all possible permutations and combinations, is called a ***brute-force attack.***"

"The process of trying to break any cipher-text message to obtain the original plain-text message itself is called ***cryptanalysis.***"

"The person attempting a cryptanalysis is called a ***cryptanalyst.***"

- **Mono-alphabetic Cipher**

The primary limitation of the Caesar cipher is its predictability. Once we determined to replace an alphabet in the original plain text with an alphabet which is k positions up or down order, we use the same scheme (same k position) for all the alphabets. Due to this cryptanalyst has to try only 25 possibilities to crack the ciphertext.

In mono alphabetic cipher instead of using uniform pattern, we replace alphabet each time differently that is each A can be replaced by any other alphabet (B through Z), each B can also be replaced by any other random alphabet (A or C through Z), and so on.

With mono alphabetic Cipher, we can now have (26 * 25 * 24 * 23 * ... 2) or $4 * 10^{26}$ possibilities! So, it becomes very hard for cryptanalyst to crack. It might actually take years to try out these many combinations even with the most modern computers.

- **Homophonic Substitution Cipher**

This technique is very similar to mono-alphabetic cipher. But, the difference between the two techniques is that replacement alphabet set in case of the simple substitution techniques is fixed (e.g. replace A with D, B with E, etc.), in the case of homophonic substitution cipher, one plain-text alphabet can be replaced with alphabet from chosen set. For example, A can be replaced by E, G, I, K; B can be replaced by F, H, J, L, etc.

- **Polygram Substitution Cipher**

In the PolyGram substitution cipher technique, instead of replacing alphabets one by one at a time, a block of alphabets is replaced with another block. For example, HELLO could be replaced by DKNNW, but HELL could be replaced by a totally different cipher text block TLEF.

HELLO ----------> DKNNW

HELL ----------> TLEF

(Plaintext) (ciphertext)

This shows that in the Polygram substitution cipher, the replacement of plain text happens block by block, rather than character by character.

- **Playfair Cipher**

The Playfair cipher, also known as **Playfair square**, is a cryptographic method for manually encrypting data. Charles Wheatstone created this scheme in 1854, but it eventually gained popularity under the name of Playfair, Wheatstone's friend, who became the scheme's public face. It is a multiple letter encryption technique.

Encryption process using Playfair Cipher

1. Construct 5 * 5 matrix and fill it up with characters without repeating from the given keyword.

Example

Keyword MONARCHY

M	O	N	A	R
C	H	Y		

- Fill all remaining places in the Playfair square using letters from alphabet without repeating.

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Note : In English alphabets there are 26 letters, but we have only 5 * 5 (Total 25) places. So, I and J are placed in the same box.

3. Create Digrams by combining two-two alphabets from the given plain text message.

Example :

Plaintext : ATTACK

Diagram : AT TA CK

(A) If there is a singlecharacter in the last Diagram, then use filler character X.

Example :

Plaintext : NESO ACADEMY

Diagram : NE SO AC AD EM Y

New Diagram : NE SO AC AD EM YX

(B) If there is repeating character in the Diagram, use filler character as under.

Example :

Plaintext : BALLOON

Diagram : BA LL OO N

New Diagram : BA LX LO ON

4. Check each character of the Diagram in the matrix, and replace as per below rules.

   (A) if both characters are in the same column, replace them with one downward character.

   (B) if both characters are in the same row, replace them with one right side character.

   (C) if characters are in different row and different column, replace with last character in the same row.

   Example - 1

Plaintext	ATTACK		
Diagram	AT	TA	CK
Ciphertext	RS	SR	DE
Process step	4C	4C	4C

   Example – 2

Plaintext	MOSQUE		
Diagram	MO	SQ	UE
Ciphertext	ON	TS	ML
Process step	4B	4B	4A

[B] Transposition techniques :

In contrast to the substitution techniques, Transposition techniques perform some permutation over the plain text, instead of replacing one alphabet with another alphabet. For example, if given plaintext is HELLO, then Ciphertext may be LHELO. Here we can observe that In ciphertext, letters are same as plain text but placed at different position.

Some of the common transposition techniques are discussed as under.

- **Rail-Fence Technique**

  Rail-fence technique is the simplest transposition technique which work with algorithm as written below.

  Step 1. Write alternate letters of the given plaintext into first line.

  Step 2. Write remaining letters of the given plaintext into second line.

  Step3. Read the first line and then read the second line. Output of the step 3 is Ciphertext of the given plaintext.

Example

Plaintext : YOU ARE BEST FRIEND

Plaintext	YOU ARE BEST FRIEND
Step 1	YURBSFIN
Step 2	OAEETRED
Step 3	YURBSFINOAEETRED

Plaintext : YOU ARE BEST FRIEND

Ciphertext : YURBSFINOAEETRED

- **Simple Columnar Transposition Technique**

Columnar transposition technique is similar like simple rail fence technique with minor change in processing method. There are two types of columnar transposition techniques.

(1) Basic Simple Columnar Transposition Technique

Basic Simple Columnar Transposition Technique works with algorithm as written below.

Step 1. Write the letters of given plain text row by row into table with predefined size.

Step2. Read the letter from the table column wise. No need to read columns in sequence. (columns 1, 2, 3...). You are allowed to read columns randomly like column 3, 1, 2 etc...

Step 3. The output of the step 2 is Ciphertext.

Example

Plaintext : YOU ARE MY BEST FRIEND

Step 1. Consider table of five columns and write letters of plaintext row wise as below.

Column 1	Column 2	Column 3	Column 4	Column 5
Y	O	U	A	R
E	M	Y	B	E
S	T	F	R	I
E	N	D		

Step 2. Now decide the sequence of column as column 2, 4, 1, 3, 5. Read the letters from the table as the sequence decided.

Step 3. The output ciphertext would be : OMTNABRYESEUYFDREI

(2) Transposition Technique with Multiple round

To increase the complexity, the Basic Columnar Transposition Technique is carried out with multiple rounds. The basic process is as the case of Basic Columnar Transposition technique.

The basic algorithm for transposition technique with multiple rounds is as under.

Step 1. Write the letters of given plain text row by row into table with predefined size.

Step 2. Read the letter from the table column wise. No need to read columns in sequence. (columns 1, 2, 3...). You are allowed to read columns randomly like column 3, 1, 2 etc...

Step 3. The output of the step 3 is Ciphertext with round 1.

Step 4. Repeat steps 1 to 3 as many times as you decided.

Example

Plaintext : YOU ARE MY BEST FRIEND

Step 1. Consider table of five columns and write letters of plaintext row wise as below.

Column 1	Column 2	Column 3	Column 4	Column 5
Y	O	U	A	R
E	M	Y	B	E
S	T	F	R	I
E	N	D		

Step 2. Now decide the sequence of column as column 2, 4, 1, 3, 5. Read the letters from the table as the sequence decided.

Step 3. The output ciphertext would be : OMTNABRYESEUYFDREI

Step 4. Repeat step 1 to 3 for the ciphertext : OMTNABRYESEUYFDREI so the new table representation will be as below.

Column 1	Column 2	Column 3	Column 4	Column 5
O	M	T	N	A
B	R	Y	E	S
E	U	Y	F	D
R	E	I		

Step 5. Now decide the sequence of column as column 2, 4, 1, 3, 5. Read the letters from the table as the sequence decided.

Step 6. The output ciphertext would be : MRUENEFOBERTYYIASD

- **Vernam Cipher (One-Time Pad)**

The Vernam cipher, uses a random set of non-repeating characters as the input cipher text. This technique uses such input ciphertext to convert plain text into ciphertext. Here it is never repeated so-called one-time pad. The length of the input cipher text is equal to the length of the original plain text. The algorithm used in the Vernam cipher is as under.

Step 1. Assign each letter in the plaintext with number i.e. A = 0, B = 2, ... Z = 25.

Step 2. Assign each letter in the input ciphertext with the number same as step 1.

Step 3. Add corresponding plaintext alphabet number with the input ciphertext number.

Step 4. If the sum is greater than 25, subtract 26 from the sum.

Step 5. Translate each number of sums back to the corresponding letter.

Example

Plaintext : HOW ARE YOU

Plaintext	H	O	W	A	R	E	Y	O	U
Corresponding Number	7	14	22	0	17	4	24	14	20
Input Ciphertext	N	W	Z	Q	R	P	V	B	D
Corresponding Number	13	22	25	16	17	15	21	1	3
Sum of corresponding No.	20	36	47	16	34	19	45	15	23
Subtract 26, if sum > 25	20	10	21	16	8	19	19	15	23
convert into corresponding letter, called ciphertext	U	K	V	Q	I	T	T	P	X

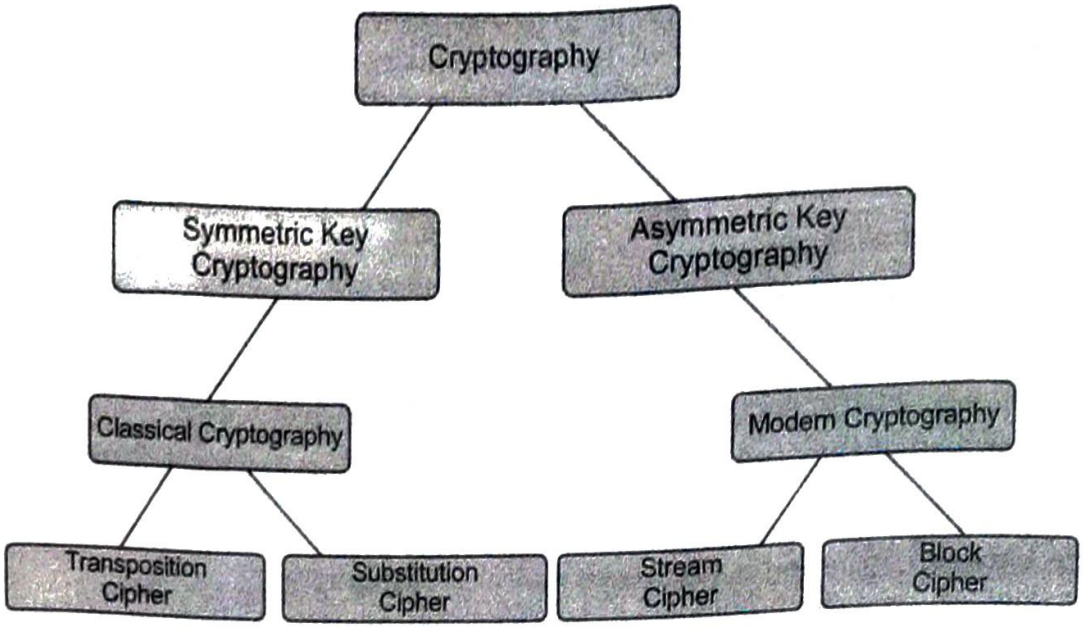
In this technique, one-time pad is discarded after a single use, so this technique is highly secure and suitable for small plain-text message, but this technique is impractical for large messages.

- **Book Cipher/Running-Key Cipher**

A portion of text from a book is used to produce cipher text; this text acts as a one-time pad, and characters from the book are added to the input plain-text message in a manner similar to the Vernam cipher. This basic idea behind the book cipher, also incorrectly called running-key cipher, is quite simple.

1.4.3 Private and Public key cryptography :

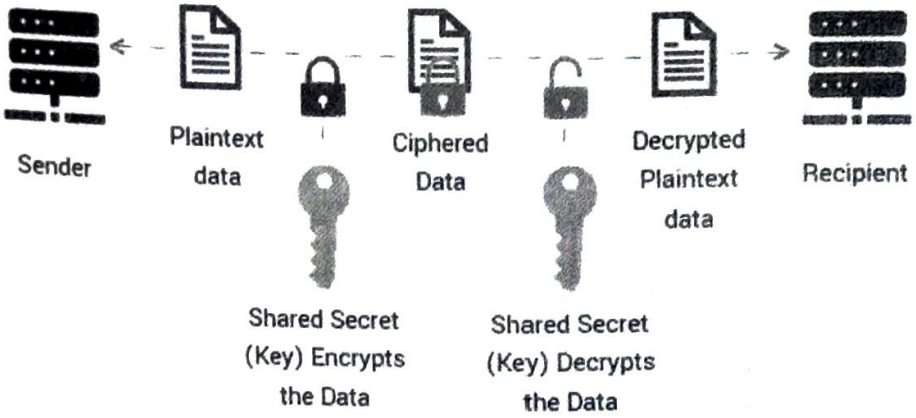
Encryption is the process of converting the original message called plaintext into unintelligible message called ciphertext by the sender. For such conversion sender uses two important components namely **an algorithm** and **the key.** Cryptography can be classified in to two categories as depicted in fig. 1.9.



[Fig. 1.9 : Classification of Cryptographic Techniques]

(1) Symmetric Key Cryptography

In Symmetric-key encryption the message is encrypted by using a key at the sender side and the same key is used to decrypt the message at the receiver side. Such kind of cryptography uses a same key for encryption as well as decryption. In this method of cryptography, key should be kept secret for sender and receiver. Such key is called secret or private key and the method is called symmetric key cryptography or private key cryptography. This method is easy to use but less secure because it requires a safe method to transfer the key from sender to receiver.



[Fig. 1.10 : Symmetric (Shared) Key Cryptography]

In the above figure 1.10, we can see that same key is used for encryption (sender side) as well as for decryption (receiver side). Symmetric key cryptography emerges the key exchange problem. Symmetric key cryptography is also known as Common Key Cryptography because both the sender and receiver use the same key.

(2) Asymmetric Key Cryptography

One of the major problems with the symmetric key cryptography is how safely transfer the key from sender side to receiver side. This problem is called **key exchange problem**. Asymmetric Key cryptography uses two different keys : one is public key for encryption at sender side and another is private key for

decryption at receiver side. By using two different key such method solves the key exchange problem of symmetric cryptography. It is more secure than the symmetric key encryption technique but is much slower.

[Fig. 1.11 : Asymmetric (Public) Key Cryptography]

Difference between Symmetric and Asymmetric cryptography

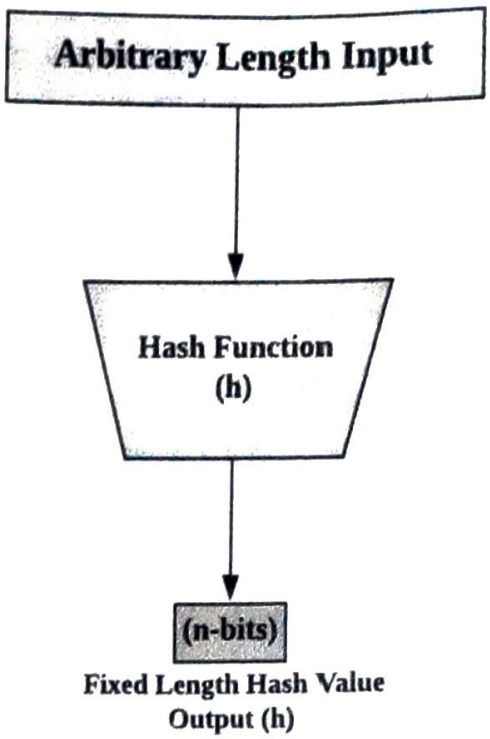
Symmetric Key Encryption (Private Key Cryptography)	Asymmetric Key Encryption (Public Key Cryptography)
Single key for both Encryption and Decryption.	A public key is used for Encryption and a private key used for Decryption.
The size of cipher text is the same or smaller than the original plain text.	The size of cipher text is the same or larger than the original plain text.
The encryption process is very fast.	The encryption process is slow.
Used to transfer large amount of data.	Used to transfer small amounts of data.
Only provides confidentiality.	Provides confidentiality, authenticity, and non-repudiation.
The length of key used is 128 or 256 bits	The length of key used is 2048 or higher
Resource utilization is low as compared to asymmetric key encryption.	Resource utilization is high.
More efficient	Less efficient.
Less secure because uses same key.	More secure as two keys are used here- one for encryption and the other for decryption.
Examples : 3DES, AES, DES and RC4	Examples : Diffie-Hellman, ECC, El Gamal, DSA and RSA

1.5 MESSAGE DIGESTING, HASHING AND SHA

1.5.1 Hashing

Hashing is the process of generating a fixed-size output value from variable length block of data as an input. The fixed size output value is called hash value and the algorithm used for such conversion is

called hash function. Hash function is nothing but a mathematical formula. The working flow of hashing is as depicted in the below figure 1.12.



[Fig. 1.12 : Working Flow of Hashing Function]

E.g. if our input value is "hello" then "5d41510abc4b2a76b9719d911017c592" is the output value after applying hashing. Similarly, the output value for the input value "God is Great" is "5ee878141e0cb782e0729066a7d88852". From these two examples we can observe that even though both the inputs with different length, both the output of the hashing function with the same length.

The main objective of the hash function is to achieve data integrity. The change in any bit or bits of the message will generate different hash value. The hash functions used for security applications is referred to as Cryptographic Hash Function.

Applications of hash functions.

- *Database indexing* : In databases and other data storage systems, hashing is used to efficiently index and retrieve data.
- *Storage of passwords* : By running a hash function over the password and saving the hashed result instead of the password in plain text, hashing is a secure way to save passwords.
- *Data compression* : To efficiently encode data, hashing is employed in data compression methods like the Huffman coding scheme.
- *Cryptography* : Digital signatures, Message Authentication Codes (MACs), and key derivation functions are all produced via hashing.
- *Load balancing* : Hashing is used to distribute requests among servers in a network via load-balancing techniques like consistent hashing.
- *Blockchain* : The proof-of-work algorithm, which is a component of blockchain technology, uses hashing to protect the consensus and integrity of the blockchain.

- *Image processing* : Perceptual hashing is one application of hashing used in image processing to identify and stop image duplication and alteration.
- *File comparison* : To compare and confirm the integrity of files, hashing is employed in file comparison methods like the MD5 and SHA-1 hash functions.
- *Fraud detection* : To identify and stop unwanted activity, hashing is utilized in cybersecurity applications like intrusion detection and antivirus software.

1.5.2 Cryptographic Hashing Algorithms

Hashing functions are generally used for data integrity and authentication of sender. Data integrity assures that the message received at receiver side is exactly same as sent by sender. Authentication is achieved through Digital Signature. Some of the important hashing algorithms are :

- Message Digest (MD 5)
- Secured Hashing Algorithm (SHA)
- Cyclic Redundancy Check (CRC)

[A] Message Digest (MD 5)

A message of any length can be entered into the MD5 cryptographic hash function method, which converts it into a fixed-length message of 16 bytes (128 Bits). The message-digest algorithm is known as the MD5 algorithm. MD5 was created with enhanced security features to replace MD4. MD5 always produces a digest size output of 128 bits. Ronald Rivest created MD5 in 1991.

Working of MD5

The MD5 algorithm proceeds as follows :

1. Append Padding Bits :

In the first step, we modify the original message by adding padding bits so that the message's overall length is 64 bits shorter than multiple of 512.

E.g. Assume a 1000-bit message is sent to us. We now need to append padding bits to the original message. Here, the original message will be appended with 472 padding bits. The output of the first step will have a size of 1472 once the padding bits are added, which is 64 bits less than an exact multiple of 512 (512*3 = 1536).

Thus Length (original message + padding bits) = 512 * i – 64 where i = 1,2,3 . . .

2. Padding Length

To make your final string a multiple of 512, you must add a few more characters. To accomplish this, take the first input's length and express it as 64 bits. Thus prepare final data to be hashed in multiple of 512 bits.

3. Initialize MD buffer :

we use the 4 buffers i.e. J, K, L, and M. The size of each buffer is 32 bits.

J = 01 23 45 67

K = 89 ab cd ef

L = fe dc ba 98

M= 76 54 32 10

4. Process Each 512-bit Block :

This step is the core of the MD5 algorithm. Here, 4 rounds carried out and in each round 16 operations are performed. Thus, during this a total of 64 operations are performed in 4 rounds. We apply a different function on each round i.e. for the 1st round we apply the F function, for the 2ndround G function, 3rdround H function, and 4th round I function.

We perform OR, AND, XOR, and NOT operations for calculating functions. We use 3 buffers for each function i.e. K, L, M.

- F(K,L,M) = (K AND L) OR (NOT K AND M)
- G(K,L,M) = (K AND L) OR (L AND NOT M)
- H(K,L,M) = K XOR L XOR M
- I(K,L,M) = L XOR (K OR NOT M)

After all, rounds have been performed, the buffer J, K, L, and M contains the MD5 output starting with the lower bit J and ending with Higher bits M.

Advantages of using MD5

- The MD5 algorithm has the advantages of being quicker and easier to comprehend.
- The MD5 method produces a 16-byte strong password. The MD5 algorithm is used by all developers, including web developers, to safeguard user passwords.
- The MD5 method requires comparatively little memory to incorporate.

Disadvantages of using MD5

- MD5 generates the same hash function for different inputs.
- MD5 provides poor security over other advanced algorithms.
- MD5 is neither a symmetric nor asymmetric algorithm.

[B] Secure Hashing Algorithm (SHA)

Secure Hashing Algorithm (SHA) is designed on the base of MD4. It produces a 512-bit message digest.

The input message is divided into number of blocks where each contains 1024 bits. The SHA algorithm is carried out with below steps.

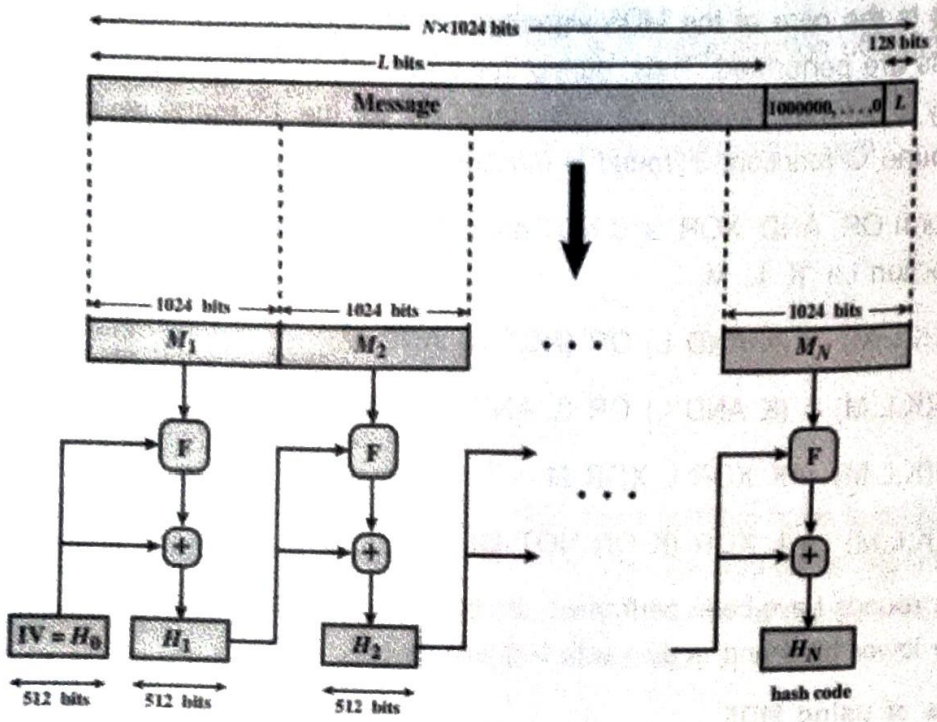
Step 1. Append padding bits.

The message is appended with padding bits so the message is congruent to 896 modulo 1024. The padding bits consists of all o with leading 1.

Step 2. Append Length.

A block of 128 bits is appended to the message. This block contains the length of the original message (before the padding). The message is now integer multiple of 1024 bits in length.

In the below figure 1.13, message is represented as the sequence of 1024 bit blocks M1, M2...Mn the total length of the expanded message is n × 1024 bits.



[Fig. 1.13 : Secure Hashing Message Digesting Process]

Step. 3 Initialise Hash buffer.

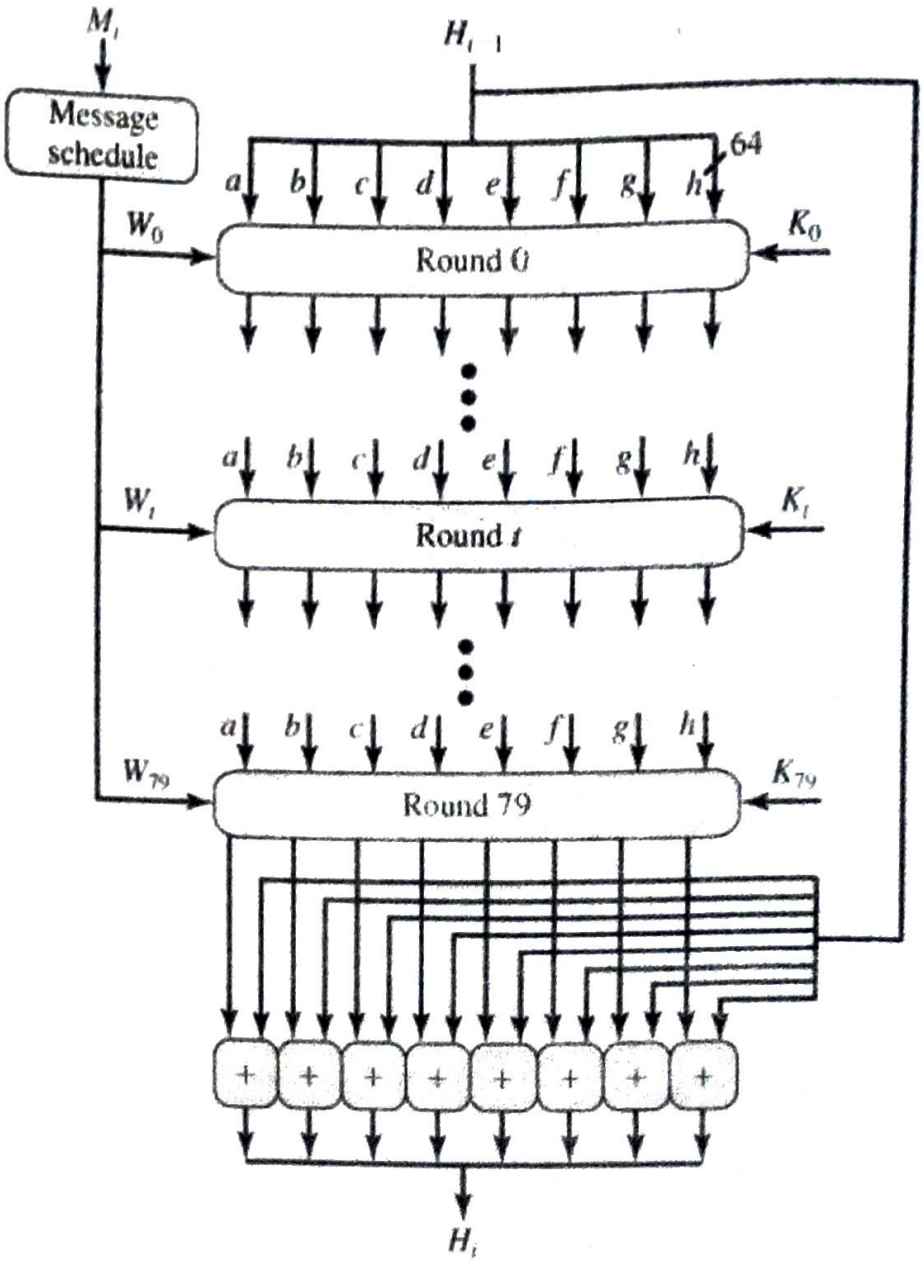
A buffer with capacity of 512 bits can be used to store intermediate as well as final result of the hash function.This Buffer is represented as the collection of eight 64 bits registers namely a, b, c, d, e, f, g, h. these registers are initialised to the 64-bit registers(Hexadecimal values) obtained by taking the first sixty-four bits of the fractional parts of the square roots of the first eight prime numbers.

Step. 4 Process message in 1024 – bit (128 word) blocks

The core part of this algorithm is the module F which is also known as round function. This function consists of 80 rounds. Each round takes input :

- 512-bit buffer value (H_{i-1})
- 64-bit words W_t obtained from the current data block by message schedule.
- Additive constant K_t which represents the first sixty-four bits of the fractional parts of the cube roots of the first eighty prime numbers.

The buffer content is updated after each round completion.



[Fig. 1.14 : Secure Hashing Algorithm (SHA)]

Step. 5 Output

The core part of this algorithm is the module F which is also known as round function. This function consists

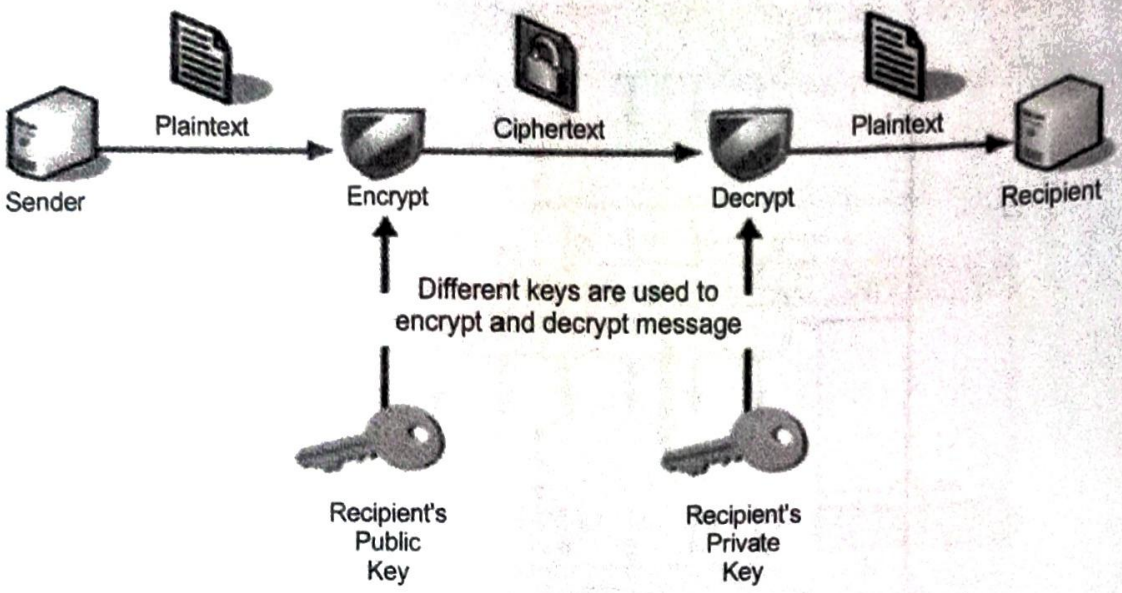
After all the N blocks (1024 bits) have been processed, the output from the Nth stage is the 512-bit message digest.

[C] RSA Algorithm

RSA algorithm was invented by Rivest, Shamir and Adleman in year 1978 and hence name **RSA** algorithm. It is an asymmetric cryptography algorithm. Asymmetric cryptography algorithm uses a linked pair of two different keys (public key, private key). The two keys are linked, but the

private key can not be derived from the public key. The Public Key is given to everyone and the Private key is kept private. This algorithm is also known as public key encryption algorithm. The below figure illustrates the working of RSA algorithm.

Sender uses a recipient's **public key** for converting plaintext into ciphertext. Sender sends ciphertext to receiver. On arrival of ciphertext receiver uses recipient's **private key** for converting the ciphertext into plaintext.



[Fig. 1.15 : Illustration of RSA Algorithm]

RSA Algorithm to construct pair of public key and private key

Step 1. Select any two large prime numbers, p and q

Step 2. Find the number n by multiplying p and q.

$n = P \times Q$, where n is the modulus for encryption and decryption.

Step 3. Calculate totient of n using $\varphi(n) = (P-1) \times (Q-1)$

Step 4. Choose a number **e** less than **n**, such that n is relatively prime to $\varphi(n)$.

It means that **e** and $\varphi(n)$ have no common factor except 1.

Step 5. Compute d such that $d \times e = 1 \bmod \varphi(n)$

$\Rightarrow d = e^{-1} \bmod \varphi(n)$

$\Rightarrow$ or $d = (1 + k \cdot \varphi(n)) / e$ where k = 0, 1, 2...

Step 6. Construct pair of public key and private key as under

Public key PU = {e, n}

Private ke PR = {d, n}

Step 7. Compute ciphertext C from plaintext M using public key PU as below. (Encryption)

$C = M^e \bmod n$

Step 8. Compute plaintext M from ciphertext C using Private key PR as below. (Decryption)

$M = C^d \bmod n$

Example :

Encrypt plaintext 9 using the RSA public-key encryption algorithm. This example uses prime numbers 7 and 11 to generate the public and private keys.

Solution :

Step 1 : Select two large prime numbers, p, and q.

$p = 7$ and $q = 11$

Step 2 : Multiply these numbers p and q to find n.

$n = p \times q$

$n = 7 \times 11$

$n = 77$

Step 3 : Calculate totient of n using $\varphi(n) = (P - 1) \times (Q - 1)$

$\varphi(n) = (p - 1) \times (q - 1)$

$\varphi(n) = (7 - 1) \times (11 - 1)$

$\varphi(n) = 6 \times 10$

$\varphi(n) = 60$

Step 4 : Choose a number **e** less than **n**, such that e is relatively prime to $\varphi(n)$.

Let $e = 7$ [Because 7 and 60 have no common factor except 1]

Step 5 : Compute d such that

$d = (1 + k \times \varphi(n)) / e$ where $k = 0, 1, 2...$

$\Rightarrow d = (1 + 0 \times 60) / 7$ for $k = 0$

$= 1/7$

$\Rightarrow d = (1 + 1 \times 60) / 7$ for $k = 1$

$= 1/7$

$\Rightarrow$ continue until we get integer result.

$\Rightarrow d = (1 + 5 \times 60) / 7$ for $k = 5$

$= 301/7$

$d = 43$

Step 6 : Construct pair of public key and private key as under

Public key PU $= \{e, n\} = \{7,77\}$

Private key PR $= \{d, n\} = \{43, 77\}$

Step 7 : Compute ciphertext C from plaintext M using public key PU. (Encryption)

$C = M^e \bmod n$

$= 9^7 \bmod 77$

$= 37$

Step 8 : Compute plaintext M from ciphertext C using Private key PR. (Decryption)

$M = C^d \bmod n$

$= 37^{43} \bmod 77$

$= 9$

In the above example plaintext M = 9 and cipher text C = 37.

Self - Assessment

Q. 1 Answer the below short questions :

(1) Why we need to secure Information ?

(2) What is Information security ?

(3) List out various goals of Information security.

(4) List out basic components of the OSI Security Architecture.

(5) Define the terms : Confidentiality, Integrity, Availability, Nonrepudiation, accountability, Authenticity

(6) Define the terms : Plaintext, Ciphertext, Cryptography, Cryptanalysis, Encryption, Decryption, Algorithm, Cryptology

(7) Differentiate : Attack and threat.

(8) List out different Substitution encryption techniques.

(9) List out different Transposition encryption techniques.

(10) What do you mean by brute-force attack? Explain with simple example.

Q. 2 Explain the below questions :

(1) Explain fundamental goals of Information Security.

(2) Explain OSI Security Architecture in brief.

(3) Short note on : Cryptography

(4) What do you mean by Substitution technique ? Explain with one simple technique.

(5) Explain Play fair cipher technique with suitable example.

(6) What do you mean by Transposition technique ? Explain with simple example.

(7) Explain Basic simple columnar transposition technique.

(8) Explain Vernam Cipher technique with suitable example.

(9) Differentiate : Symmetric Cryptography V/s Asymmetric Cryptography.

(10) Explain hashing with suitable example and working diagram.

(11) Explain hashing with its applications.

(12) Explain Message Digest 5 with its working, advantages and disadvantages.

(13) Explain Secure Hashing Algorithm in brief.

(14) Explain RSA Algorithm with suitable example.

★★★

Chapter 2

NETWORK AND SYSTEM SECURITY

2.1 TYPES OF ATTACKS

- GENERAL POINT OF VIEW
- TECHNICAL POINT OF VIEW
- IMPLEMENTATION POINT OF VIEW

2.2 DIGITAL SIGNATURES

- WHAT IS DIGITAL SIGNATURE?
- PROPERTIES OF DIGITAL SIGNATURE
- WORKING OF DIGITAL SIGNATURE

2.3 PRETTY GOOD PRIVACY (PGP)

- INTRODUCTION - PGP
- E MAIL AUTHENTICATION USING PGP

2.4 SECURE SOCKET LAYER AND TRANSPORT LAYER SECURITY

- SECURE SOCKET LAYER
- TRANSPORT LAYER SECURITY

2.5 IPSEC

- INTRODUCTION – IPSEC
- IP SECURITY ARCHITECTURE

2.6 HTTPS (CONNECTION INITIATION & CONNECTION CLOSURE)

- INTROCUTION – HTTPS
- WORKING OF HTTPS
- DIFFERENCE BETWEEN HTTP AND HTTPS
- ADVANTAGES USING HTTPS

2.7 MALICIOUS SOFTWARE

- WHAT IS MALWARE?
- COMMON TYPES OF MALWARES
  THREATS (TROJAN, ROOTKIT, BACKDOORS, KEYLOGGER ETC...)

2.8 FIREWALL

- NEED OF FIREWALLS
- WHAT IS FIREWALL?
- TYPES OF FIREWALLS
- ADVANTAGES AND DISADVANATAGES

2.9 PROXY SERVER

- PROXY SERVERS AND ITS WORKING
- TYPES OF PROXY SERVERS
- NEED FOR USING PROXY SERVERS

○ **Self - Assessment**

2.1 TYPES OF ATTACKS

Attack : An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

A security attack is an activity or act made upon a system with the goal to obtain unauthorized access to information or resources. It is usually carried out by evading security policies that are in place in organizations or individual devices.

Thus, attack is any action that compromises the security of information owned by an organization.

Security attacks can be classified in three ways:

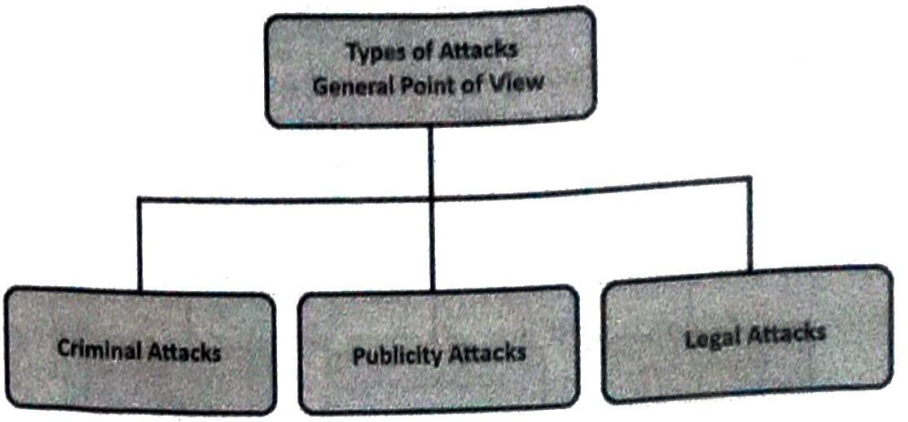
- General point of view
- Technical point of view
- Implementation point of view

2.1.1 General point of view

As a common non-technical person point of view security attacks can be classified into three types as depicted in the figure 2.1.

1. Criminal Attack

The main aim of attacker in criminal attack is to maximize financial gain or harm to other or their systems. Some of the examples of criminal attacks are: fraud, scams, identity theft, intelligent property theft, brand theft etc...



[Fig. 2.1 : Types of Attacks: General point of View]

2. Publicity Attack

The sole aim of an attacker in publicity attack is to get publicity instead of financial gain. Generally, this type of attackers are not usually hardcore criminals. They are people like students or employees who tries to get publicity through applying new approach of attack. Example of such attack is damage or hijacking web page of popular web site.

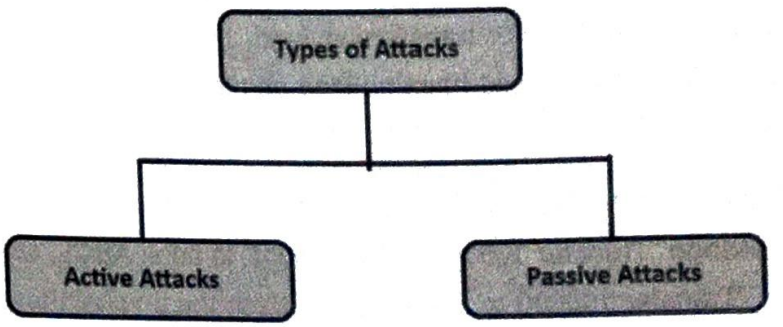
3. Legal Attack

The aim of the attacker is to exploit the weakness of the judge and the jury in technological matters. This form of attack is quite new and unique in which the attacker tries to convince the judge and the jury that there is inherent weakness in the computer system and he is not responsible for any wrongful activity.

Ex. Attacker excuse that he has just clicked as the system asked. He done nothing.

2.1.2 Technical point of view

As a technical point of view, attacks can be grouped into two types: passive attacks and active attacks, as shown infigure 2.2.



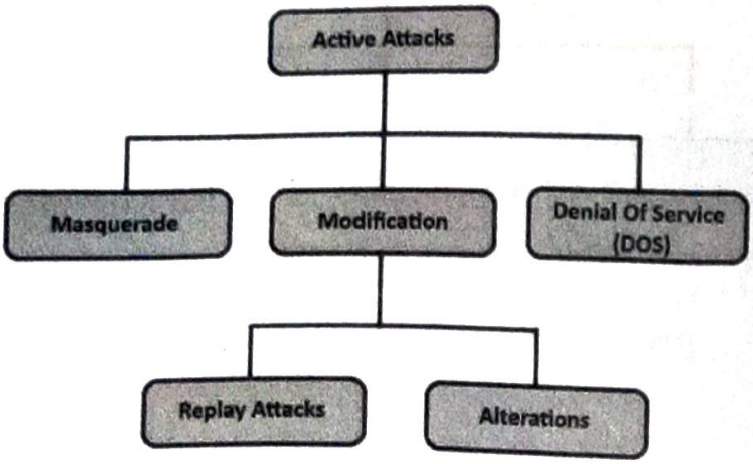
[Fig. 2.2 : Types of Attacks: Technical Point of View]

1. Active Attacks

Active attacks are the attacks in which attacker not only observes traffic but also tries to modify the original message or creates false message. These kinds of attacks cannot be easily prevented. Such kind

of attacks can be detected with some effort, and attempts can be made to recover from it.

These attacks can be further classified as depicted in the figure 2.3.



[Fig. 2.3 : Types of Active Attacks]

- **Masquerade** – Pose as another entity.

  When an attacker tries to pretends to be another entity, then attack is called masquerade attack. User C might pose himself as user A and send a message to user B. User B might be led to believe that the message indeed came from user A and he work as on message. Generally, masquerade attacks embedded with some other kind of active attacks

- **Modification** – Change of original message.

  Modification attacks are that kind of attacks in which attacker tries to modify the original message. These attacks are further classified as : **Replay attack** and **alteration attack**.

  In a **replay attack**, a user captures a message, and re-sends them. For example, suppose user A wants to transfer some amount to user C's bank account. User A might send an electronic message to bank B, requesting for transferring fund. User C could capture this message, and send again to bank B. Bank B would have no idea about this second unauthorised message, and would treat it as second message, and transfers fund two times.

  Alteration of messages involves some change in the original message. For example, suppose user A sends message "Transfer 10000 to B's account" to bank ABCL. User C might capture this, and change it to "Transfer 100000 to B's account". Here the original message is altered in terms of amount.

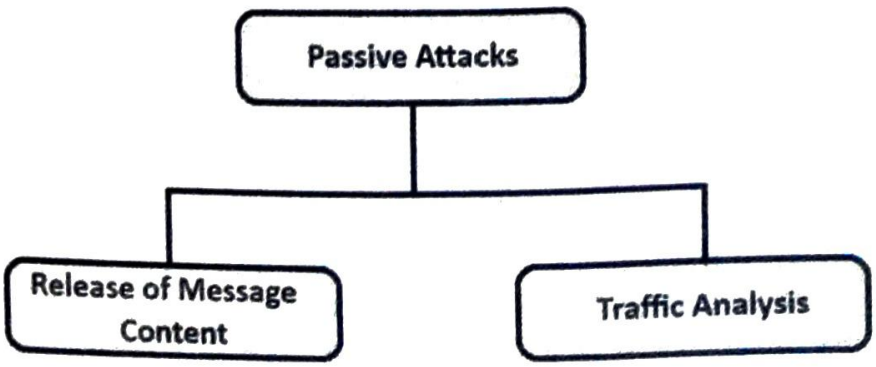
- **Denial Of Service (DOS) attacks.**

  Denial Of Service (DOS) attack attempts to make resources unavailable to its legitimate users. For example, an attacker sends thousands of requests to the server and make it busy. So, server can's response to legitimate user.

2. Passive Attacks

Passive attacks are those attacks in which the attacker just observes or monitors message during transmission. The aim of an attacker is to obtain information only. The term passive indicates, no attempt for any modification in original message. Due to this passive attack are harder to detect. To deal with passive attacks preventive actions are carried out, rather than detection or corrective actions.

Below Figure 2.4 shows further classification of passive attacks into two sub-categories. These categories are, namely **release of message contents** and **traffic analysis.**



[Fig. 2.4 : Types of Passive Attacks]

- **Release of message Content**

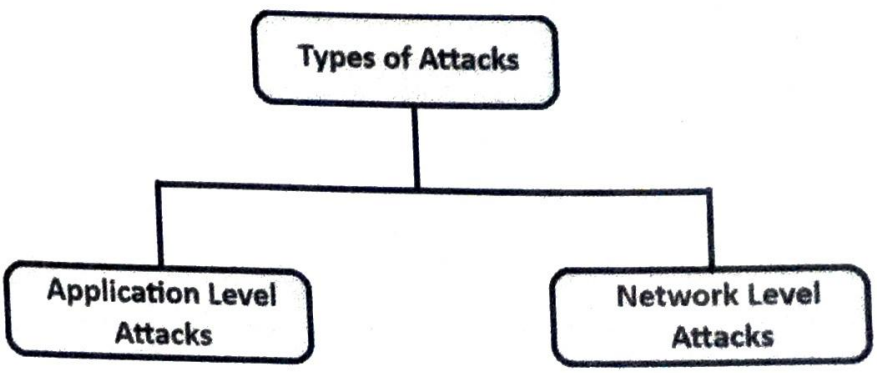
  Release of message contents attack is very simple to understand. Suppose sender wants to send confidential message to recipient without being released to any else. But an attacker accesses this message by somehow. We can prevent release of message attack with encryption like security mechanism.

- **Traffic Analysis**

  Sometime passive attacker collects large number of messages passing through network and figure out similarities between and sort out some pattern. Such attempt of analysing encrypted messages to find out original messages is called traffic analysis.

2.1.3 Implementation point of view

All the discussed attacks above can be further can be classified with implementation point of view as **Application-level attacks** and **Network level attacks** as shown in the figure 2.5.



[Fig. 2.5 : Types of Attacks: Implementation point of view]

1. **Application-level Attacks.**

These are the attacks in which an attacker attempts to access, modify, or prevent access to information of a particular application, or the application itself.

Examples: Access someone's credit-card information, or change the amount in a transaction.

2. **Network-level Attacks.**

Network level attacks are usually applied to the networks with the aim to reduce the capabilities of a network by different ways. These attacks may slow down, or completely halt the computer system network. Once an attacker get control over network, he may apply application-level attacks also.

2.2 DIGITAL SIGNATURE

As we know online electronic data transmission is carried out on the basic important elements like Confidentiality, integrity, availability, non-repudiation, and authentication. Confidentiality is achieved by using cryptographic techniques. Integrity can be achieved by using hashing functions and algorithms like SHA Algorithm and MD5 Message Digest. With the use of various activities by network administrator availability can be maintain. But how can authenticate that a particular message, data, software or document is from specific sender. That is the case where digital signature plays an important role.

2.2.1 What is Digital Signature ?

A ***digital signature*** is a mathematical technique used to validate the authenticity and integrity of a digital document, message or software.

It is the digital equivalent of a handwritten signature or stamped seal, but it offers far more inherent security. A digital signature is intended to solve the problem of tampering and impersonation in digital communications.

Digital signatures can provide evidence of origin, identity and status of electronic documents, transactions or digital messages. Signers can also use them to acknowledge informed consent. In many countries, digital signatures are considered legally in the same way as traditional handwritten document signatures.

2.2.2 Properties of Digital Signature ?

Message Authentication is the mechanism used to protect sender and receiver of digital data transmission from the third party. But it does not protect two communicating parties from each other. Several disputes between them arise like below.

- Receiver may forge an original message and claim that it was sent by sender.

  E. g. Electronic fund transfer takes place, receiver may increase the amount and claims that larger amount had arrived from the sender.

- Sender may deny about sent message.

  E.g. A stockholder sends an instruction to his stockbroker, and then pretends that he never sent such instruction.

In such situations where there is not complete trust between sender and receiver, something more than authentication is needed. The most attractive solution to this problem is the digital signature.

The digital signature must have the following **properties :**

- It must verify the author and the date and time of the signature.
- It must authenticate the contents at the time of the signature.
- It must be verifiable by third parties, to resolve disputes.

Thus, the digital signature function includes the authentication as well as integrity functions.

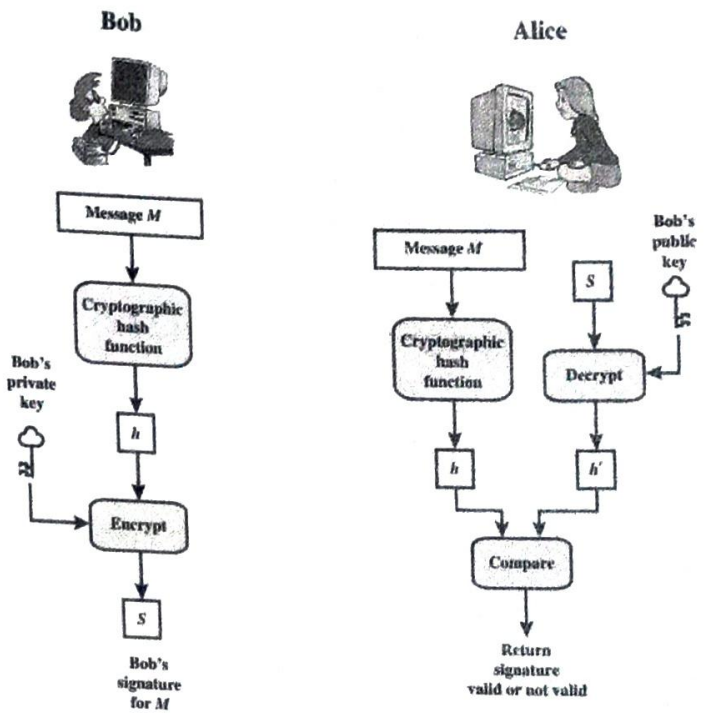
2.2.3 Working of Digital Signature ?

Digital signature uses a three kind of algorithms as described below.

Key Generation Algorithms : Digital signatures are electronic signatures that guarantee a certain sender sent the message. The algorithms which are used to generate keys are called key generation algorithms.

Signing Algorithms : To create a digital signature, hashing algorithms are used create a one-way hash of the electronic data which is to be transmitted. The signing algorithm then encrypts the hash value using the sender's private key (signature key). This encrypted hash value along with original data is known as the digital signature.

Signature Verification Algorithms : Digital signature Verifier receives Digital Signature along with the original data. Verifier then uses Verification algorithm to verify the received digital signature.



[Fig. 2.6 : Digital Signature process Step by Step]

The steps followed in creating digital signature and verifying signature are :

1. Hash value is computed by applying hash function on the message and then hash value is encrypted using private key of sender (Bob) to form the digital signature.

   digital signature = encryption (private key of sender, Hash Value) and

   Hash Value = Hashing algorithm(message).

2. Digital signature is then transmitted with the original message.

   (original message + digital signature is transmitted)

3. Receiver decrypts the digital signature using the public key of sender. (This assures authenticity, as only sender has his private key so only sender can encrypt using his private key which can thus be decrypted by sender's public key).

4. The receiver now has the Hash value from the sender side.

5. The receiver can also compute the hash value from the original message. (actual message is sent with the digital signature).

6. The hash value computed by receiver and the hash value received from the sender (got by decryption on digital signature) need to be same for ensuring integrity.

Digital signatures are used in various financial or business transactions like legal documents and contracts, sales and purchase contracts, financial documents, health data, shipping documents etc...

2.3 PRETTY GOOD PRIVACY(PGP)

2.3.1 Introduction - PGP

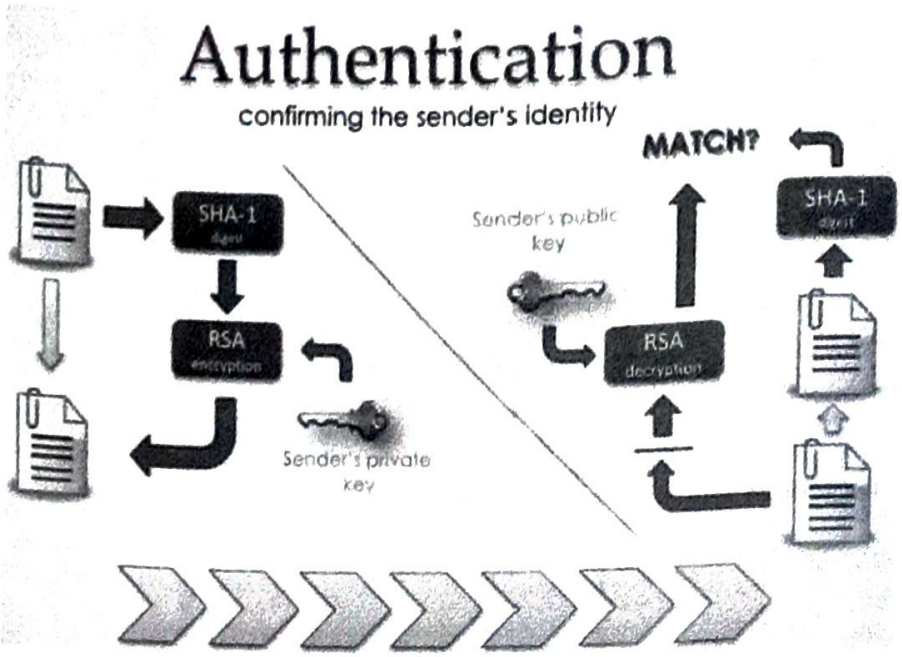
Pretty Good Privacy - PGP, is a popular program that is commonly used to provide two fundamental services confidentiality and authentication for electronic mail and file storage. It was designed by **Phil Zimmermann** in 1991. It uses best cryptographic algorithms such as RSA, Diffie-**Hellman** key exchange, DSS for the public-key encryption (or) asymmetric encryption; CAST-128, 3DES, IDEA is used for symmetric encryption and SHA-1 is used for hashing purposes. PGP software is an open-source software and independent of OS (Operating System) as well as the processor.

The various services are provided by PGP are as under:

- Authentication
- Confidentiality
- Compression
- Email Compatibility
- Segmentation

2.3.2 E mail Authentication using PGP

Authentication of an email is nothing but to check whether it actually came from the person it says or not. The Authentication service in PGP is provided as follows:



[Fig. 2.7 : E mail Authentication service with PGP]

As shown in the above figure 2.7, the hashing algorithm SHA-1 is used and it produces a 160-bit output hash value. Then, with use of sender's private key (KP_a), hash value is encrypted and it's called as Digital Signature. The Message is then appended to the signature. Then the message is compressed to reduce the transmission cost and is sent to the receiver.

At the receiver's end, the data is decompressed and the message, signature are obtained. The signature is then decrypted using the sender's public key (PU_a) and the hash value is obtained. From the message again the hash value is calculated and obtained.

Both the hash values, one is received from the sender and another is calculated at receiver side are compared. If both are same, then the email is authenticated email else it is not.

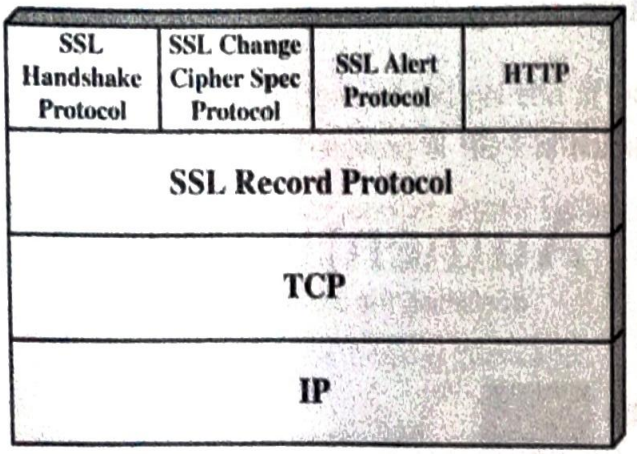
2.4 SECURE SOCKET LAYER AND TRANSPORT LAYER SECURITY

2.4.1 Secure Socket Layer (SSL)

The Secure Socket Layer (SSL) protocol is an Internet protocol for the secure exchange of information between a Web browser and a Web server. It provides two basic security services: authentication and confidentiality. Logically, it provides a secure pipeline between the Web browser and the Web server during communication. Netscape Corporation developed SSL in 1994.

SSL Architecture:

The Secure socket layer (SSL) is not a single protocol, but it is two layers of protocols as illustrated in below figure 2.8.



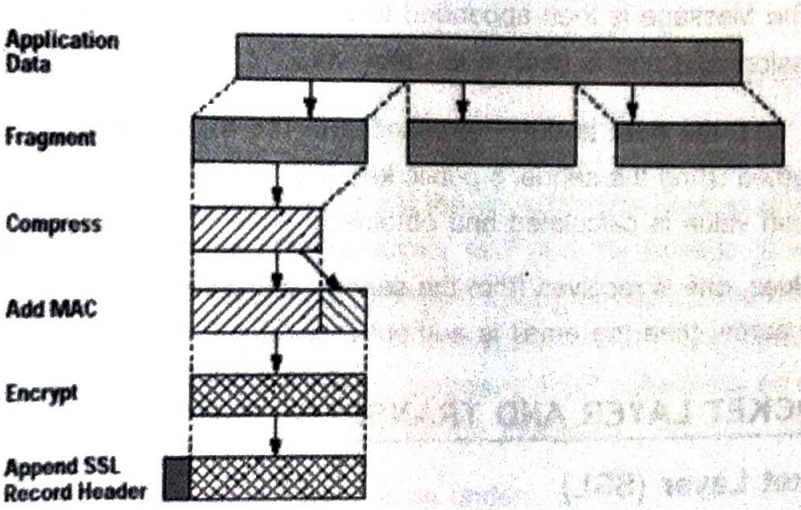
[Fig. 2.8 : SSL Architecture]

The Secure Socket Layer (SSL) is a collection of below protocols.

- SSL record protocol
- Handshake protocol
- Change-cipher spec protocol
- Alert protocol

SSL Record Protocol

The SSL record protocol provides two fundamental security services: Confidentiality and Message Integrity.

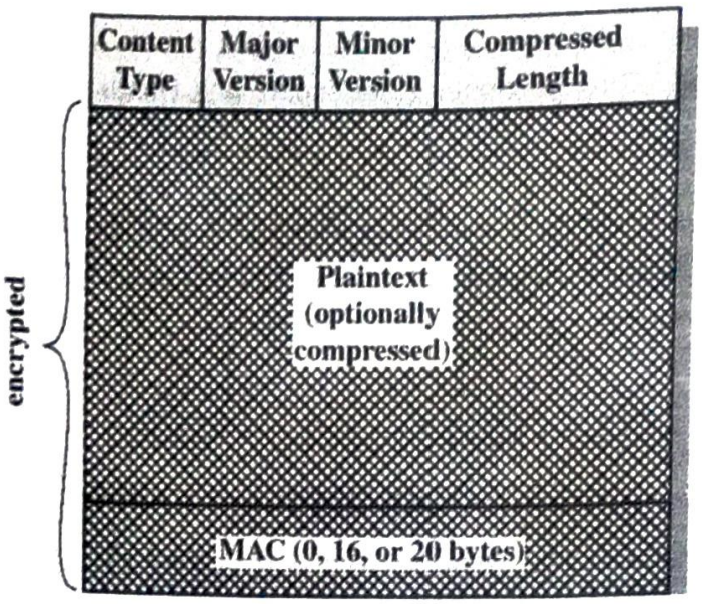


[Fig. 2.9 : SSL Record Protocol Operation]

The SSL Record Protocol operation is as under:

- *Fragmentation* : the original data is fragmented into blocks of 214 Bytes or less.
- *Compression* : each fragment is compressed. This is optional. Compression must be lossless.
- *Appending MAC Code* : Message Authentication Code is appended to fragment.

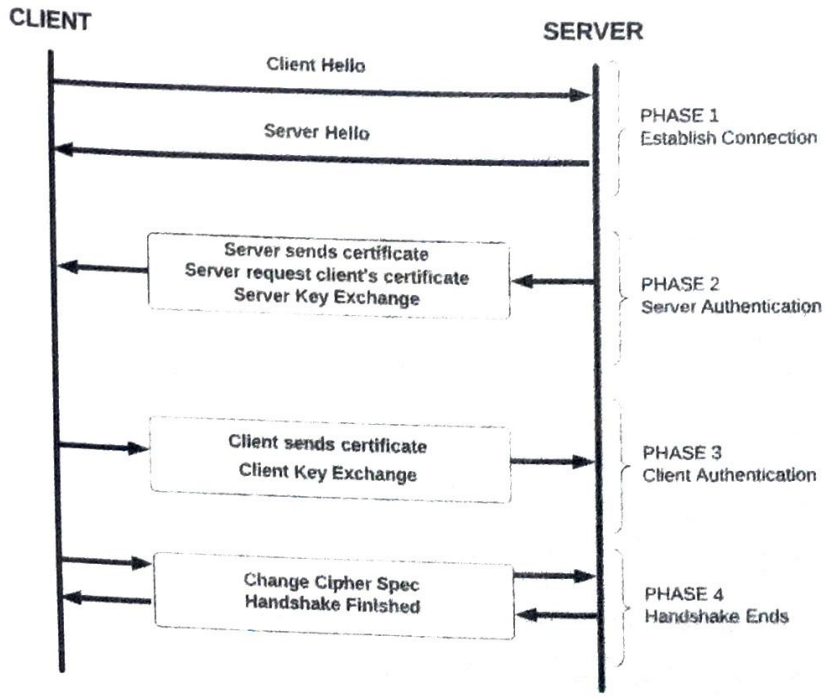
- *Encryption* : The compressed message with appended MAC Code is encrypted using symmetric encryption algorithms like AES, DES, 3DES etc...
- *Add SSL header* : Finally, SSL header is appended to the encrypted fragment. The header consists of the fields like Content Type (8 bits), Major Version (8 bits), Minor Version (8 bits), Compressed Length (16 bits).



[Fig. 2.10 : SSL Record Format]

SSL Handshake Protocol

Handshake Protocol is used to establish sessions. This protocol allows the client and server to authenticate each other by sending a series of messages to each other. Handshake protocol uses four phases to complete its cycle.

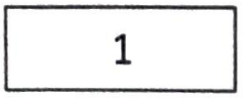


[Fig. 2.11 : SSL Handshake Protocol]

- **Phase-1 :** In Phase-1 both Client and Server send hello-packets to each other. In this IP session, cipher suite and protocol version are exchanged for security purposes.
- **Phase-2 :** Server sends his certificate and Server-key-exchange. The server end phase-2 by sending the Server-hello-end packet.
- **Phase-3 :** In this phase, Client replies to the server by sending his certificate and Client-exchange-key.
- **Phase-4 :** In Phase-4 Change-cipher suite occurs and Handshake Protocol ends.

Change Cipher Protocol

This protocol consists of a single message of single byte with the value 1. It uses the SSL record protocol. Unless Handshake Protocol is completed, the SSL record Output will be in a pending state.



1 Byte

[Fig. 2.12 : Change Cipher Spec Protocol]

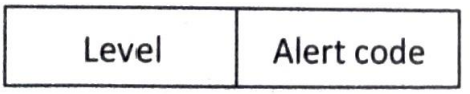
After the handshake protocol, the Pending state is converted into the current state.

This protocol's purpose is to cause the pending state to be copied into the current state.

Alert Protocol

The Alert protocol is used to convey SSL-related alerts to the peer entity. Each message in this protocol consists of 2 bytes.

- The first byte indicates the severity of the message by value warning (1) and fatal (2).
- The second byte contains s code that indicate the specific alert.



2 Byte

[Fig. 2.13 : Alert Protocol]

Warning Error (Level = 1) :

This Alert has no impact on the connection between sender and receiver. Some of them are:

- **Bad certificate:** When the received certificate is corrupt.
- **No certificate:** When an appropriate certificate is not available.

Fatal Error (level = 2):

This Alert breaks the connection between sender and receiver. Some of them are :

- **Handshake failure :** When the sender is unable to negotiate an acceptable set of security parameters given the options available.

- **Decompression failure:** When the decompression function receives improper input.

2.4.2 Transport Layer Security (TLS)

The Secure Sockets Layer (SSL) and the Transport Layer Security (TLS) protocols are currently the two most used ones for delivering security at the transport layer.

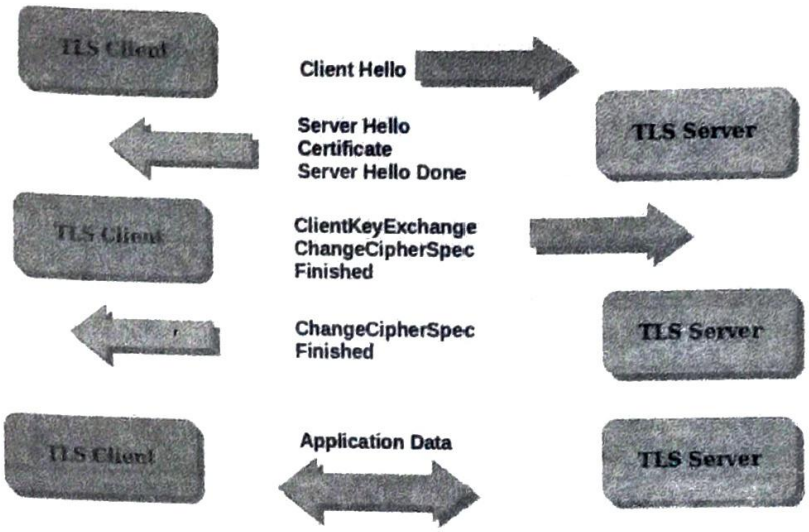
TLS evolved from a previous encryption protocol called Secure Sockets Layer (SSL), which was developed by Netscape. TLS version 1.0 actually began development as SSL version 3.1, but the name of the protocol was changed before publication in order to indicate that it was no longer associated with Netscape. Because of this history, the terms TLS and SSL are sometimes used interchangeably.

Working of TLS

A TLS connection is initiated using a sequence known as the TLS handshake. When a user navigates to a website that uses TLS, the TLS handshake begins between the user's device (also known as the client device) and the web server.

During the TLS handshake, the user's device and the web server:

- Specify which version of TLS (TLS 1.0, 1.2, 1.3, etc.) they will use.
- Decide on which cipher suites (see below) they will use.
- Authenticate the identity of the server using the server's TLS certificate.
- Generate session keys for encrypting messages between them after the handshake is complete.



[Fig. 2.14 : Working of TLS]

The TLS handshake establishes a cipher suite for each communication session. The cipher suite is a set of algorithms that specifies details such as which shared encryption keys, or session keys, will be used for that particular session.

The handshake also handles authentication.

Once data is encrypted and authenticated, it is then signed with a message authentication code (MAC). The recipient can then verify the MAC to ensure the integrity of the data.

2.5 IPSEC

2.5.1 Introduction - IPsec

IPsec (Internet Protocol Security) is a large set of protocols and algorithms. The Internet Engineering Task Force (IETF), developed the IPsec protocols for the purpose of providing security at the IP layer through authentication and encryption of IP network packets.

Originally, it was defined with two protocols for securing the IP packets which were Authentication Header (AH) and Encapsulating Security Payload (ESP). The former protocol i.e. AH provides data integrity and non-replay services, and the latter protocol i.e. ESP encrypts and authenticates data.

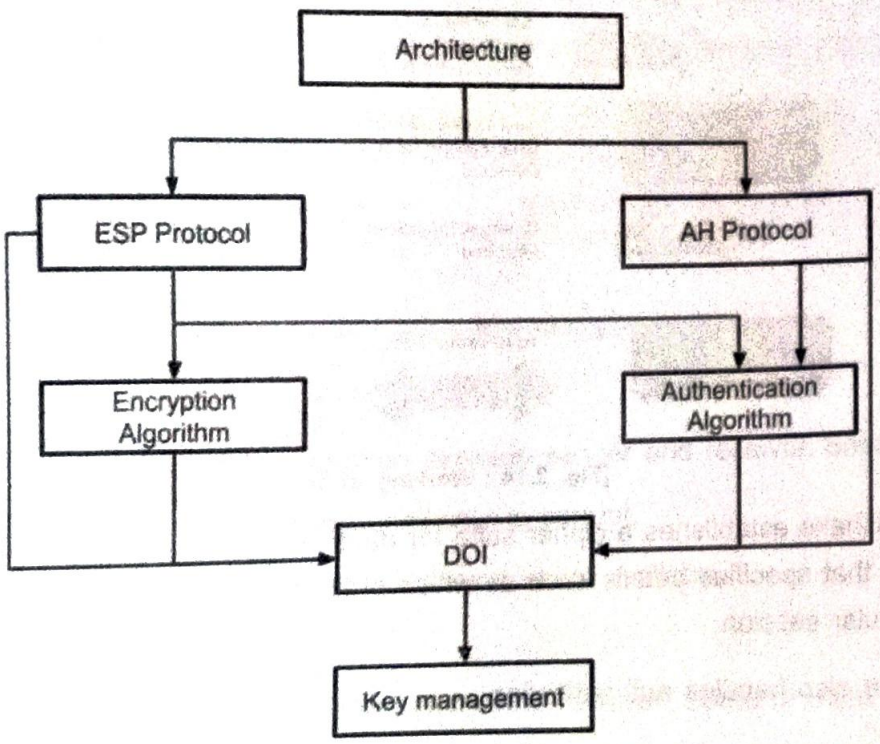
Thus, IPsec provides the basic services as listed below:

- Confidentiality
- Authentication
- Integrity
- Non-Replay

2.5.2 IP Security Architecture

1. Architecture:

Architecture or IP Security Architecture covers the general concepts, definitions, protocols, algorithms, and security requirements of IP Security technology.

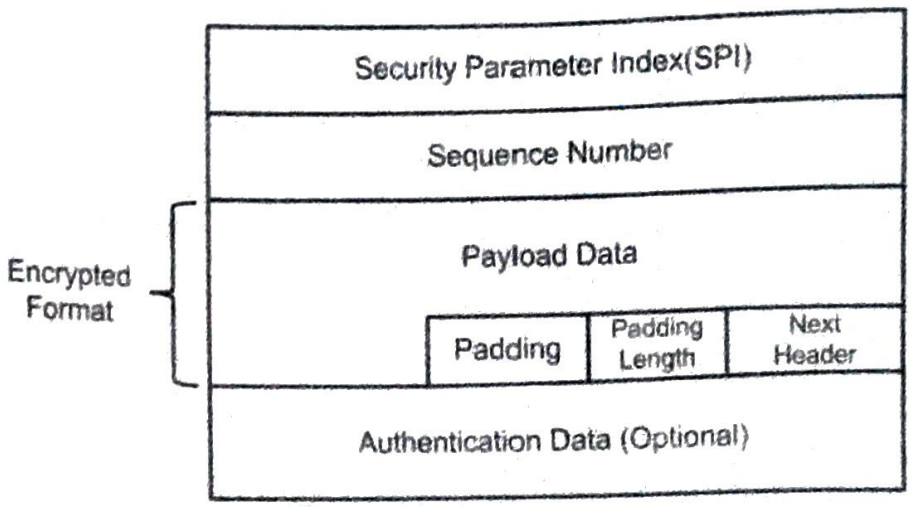


[Fig. 2.15 : IP Security Architecture]

2. ESP Protocol :

ESP (Encapsulation Security Payload) provides a confidentiality service. Encapsulation Security Payload is implemented in either two ways:

- ESP with optional Authentication.
- ESP with Authentication.



[Fig. 2.16 : ESP Packet Format]

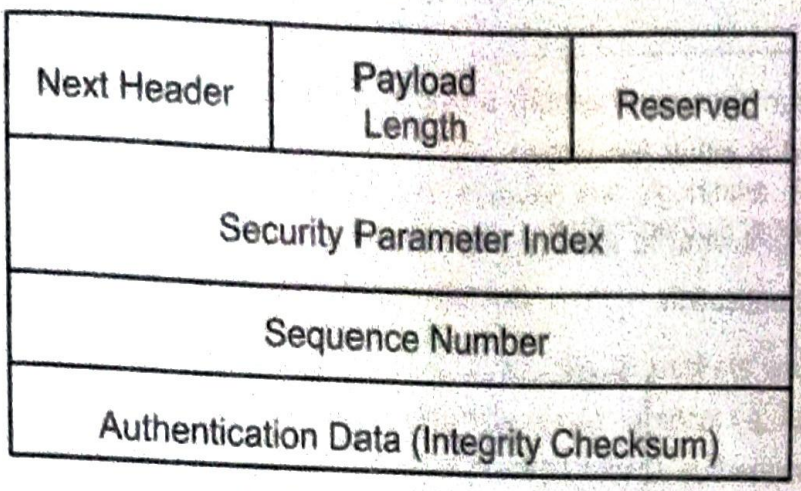
- **Security Parameter Index (SPI) :** This parameter is used by Security Association. It is used to give a unique number to the connection built between the Client and Server.
- **Sequence Number :** Unique Sequence numbers are allotted to every packet so that on the receiver side packets can be arranged properly.
- **Payload Data :** Payload data means the actual data or the actual message. The Payload data is in an encrypted format to achieve confidentiality.
- **Padding :** Extra bits of space are added to the original message in order to ensure confidentiality. Padding length is the size of the added bits of space in the original message.
- **Next Header :** Next header means the next payload or next actual data.
- **Authentication Data:** This field is optional in ESP protocol packet format.

3. Encryption algorithm :

The encryption algorithm is the document that describes various encryption algorithms used for Encapsulation Security Payload.

4. AH Protocol :

AH (Authentication Header) Protocol provides both Authentication and Integrity service. Authentication Header is implemented in one way only: Authentication along with Integrity.



[Fig. 2.17 : AH Packet Format]

Authentication Header covers the packet format and general issues related to the use of AH for packet authentication and integrity.

5. Authentication Algorithm :

The authentication Algorithm contains the set of documents that describe the authentication algorithm used for AH and for the authentication option of ESP.

6. DOI (Domain of Interpretation) :

DOI is the identifier that supports both AH and ESP protocols. It contains values needed for documentation related to each other.

7. Key Management :

Key Management contains the document that describes how the keys are exchanged between sender and receiver.

2.6 HTTPS (CONNECTION INITIATION & CLOSURE)

2.6.1 Introduction - HTTPS

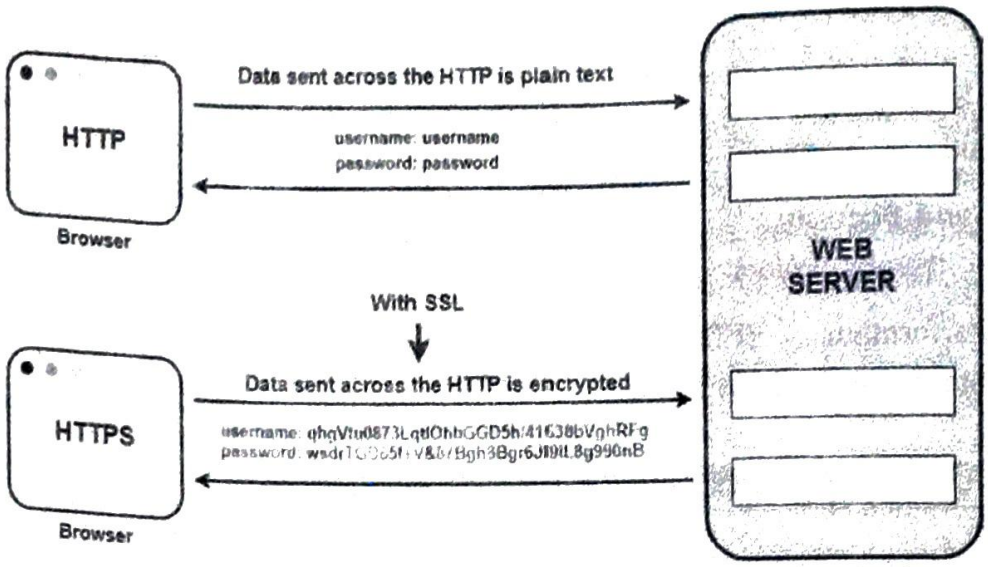
Hypertext transfer protocol secure (HTTPS) is the secure version of HTTP, which is the primary protocol used to send data between a web browser and a website. HTTPS is particularly important when users transmit sensitive data, such as by logging credentials for a bank account, email service, or health insurance provider.

In modern web browsers such as Chrome, websites that do not use HTTPS are marked differently than those that are.

2.6.2 Working of HTTPS

HTTPS uses an encryption protocol to encrypt the communication data. The protocol used for this encryption is called Transport Layer Protocol (TLS), formerly it was known as Secure Socket Layer (SSL). This protocol uses an asymmetric public key infrastructure. It uses two different keys: the private key and the public key.

When information is sent over regular HTTP, the information is broken into packets of data that can be easily "sniffed" using free software. This makes communication over the an unsecure medium, such as public Wi-Fi, highly vulnerable to interception.



[Fig. 2.18 : Working with HTTPS]

With HTTPS, traffic is encrypted such that even if the packets are sniffed or otherwise intercepted, they will come across as nonsensical characters.

2.6.3 Difference between HTTP and HTTPS

HTTP	HTTPS
The full form of HTTP is Hypertext Transfer Protocol	The full form of HTTPS is Hypertext Transfer Protocol Secure.
It operates on application layer.	It operates at the transport layer.
The data is transferred in plain text form.	The data is transferred in encrypted form, i.e., ciphertext.
By default, this protocol operates on port number 80.	By default, this protocol operates on port number 443.
The URL start with http://	The URL start with https://
This protocol does not need any certificate.	But this protocol requires an SSL (Secure Socket Layer) certificate.
Communication carried out without encryption.	Communication carried out with encryption.
Faster than HTTPS.	Slower than HTTP.
It is un-secure.	It is highly secure.
Examples of HTTP websites are Educational Sites, Internet Forums, etc.	Examples of HTTPS websites are shopping websites, banking websites, etc.

2.6.4 Advantages of using HTTPS

- **Secure Communication** : HTTPS establishes a secure communication link between the communicating system by providing encryption during transmission.
- **Data Integrity** : By encrypting the data, HTTPS ensures data integrity. This implies that even if the data is compromised at any point, the hackers won't be able to read or modify the data being exchanged.
- **Privacy and Security** : HTTPS prevents attackers from accessing the data being exchanged passively, thereby protecting the privacy and security of the users.
- **Faster Performance** : HTTPS encrypts the data and reduces its size. Smaller size accounts for faster data transmission in the case of HTTPS.

2.7 MALICIOUS SOFTWARE

The number of internet users are increased due to improvement in internet technology, reduced cost of hardware, and advancement of mobile technology. So, people are dependent because of their professional, social and personal activities. With the use of internet, they can perform so many tasks online with clicks in seconds. But there is also another side of coin.

There are so many people who attempts to damage our Internet-connected computers, violate our privacy and make unavailability of the Internet services. Such people are called attackers and they use malwares for such activities.

2.7.1 What is Malware ?

Malware – "A short name of malicious software, is an umbrella term that describes any malicious program or code that is harmful to systems. It is specifically designed to disrupt, damage, or gain unauthorized access to a computer system."

How can malware affect your system ?

- Your computer slows down.
- Your screen is inundated with annoying ads.
- Your system crashes.
- You notice a mysterious loss of disk space.
- There's a weird increase in your system's Internet activity.
- Your browser settings change.

  homepage changed or you have new toolbars, extensions, or plugins installed etc.
- Your antivirus product stops working and you cannot turn it back on, leaving you unprotected against the malware that disabled it.
- You lose access to your files or your entire computer.

Adware, Spyware, Virus, Worms, Trojans, Ransomware, Rootkit, keylogger etc are the various forms of malware. Each of these have different working method and affects our system or network very differently.

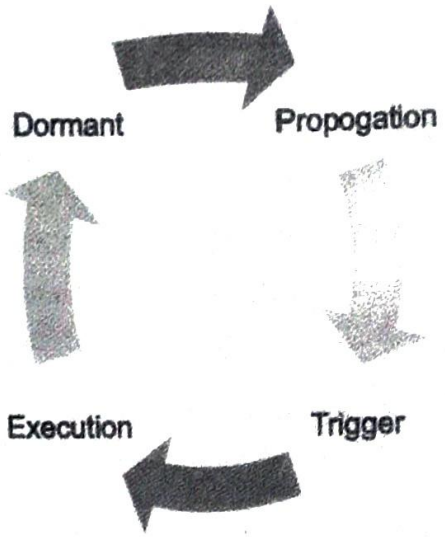
2.7.2 Common types of Malwares :

1. Virus

A virus is a piece of program code (malicious software) that attaches itself to legitimate program code, and runs when the legitimate program runs. It can then infect other programs in that computer, or programs that are in other computers but on the same network. Virus is capable to delete all the files from the current user's computer, and virus can self-propagate by sending its code to all other users whose email addresses are stored in the currently infected computer system.

- **Virus Lifecycle**

During its lifetime, a virus goes through four phases as depicted in the below figure.



[Fig. 2.19 : Virus Life Cycle]

(a) Dormant Phase : During this phase the virus is in idle mode.

(b) Propagation Phase : In this phase, a virus propagate itself by copying self-code, and each copy starts creating more and more copies of itself.

(c) Triggering Phase : A dormant virus is triggered based on a certain action or event (e.g. certain key press, a certain date or time is reached, etc).

(d) Execution Phase : The actual work of the virus starts in this phase, which could be harmless (just display some message on screen) or destructive (delete a file or corrupt a file).

- **Types of Viruses**

Viruses can be classified into different categories on the base of their working and implementation method:

(a) Parasitic Virus : Such a virus attaches itself to executable files and keeps replicating. When an infected file is executed, the virus attaches to other executable files. This is the most common type of virus.

(b) Memory-resident Virus : This virus resides in main memory and then infects every executable program that is executed.

(c) Boot sector Virus : That infects the master boot record of the disk and spreads on the disk during booting process of the computer.

(d) Stealth Virus : This virus has an in-built intelligence, due to which it can prevent anti-virus software programs from detecting it.

(e) Polymorphic Virus : Such virus continuously changes its signature (identity) on every execution, so it makes difficult to detect it.

(f) Metamorphic Virus : It changes its signature like a polymorphic virus, and also rewrites itself. So, it becomes even more harder to detect it than polymorphic virus.

2. Worms

Worms are Similar in concept to a virus, but different in implementation point of view. The big difference between virus and worm is (1) A virus can modify a program to which it is attached but a worm, does not modify a program. (2) Worms can spread across systems on their own, whereas viruses need some triggering action from a user in order to initiate the infection.

Thus, the basic aim of virus is to destroy files in the system whereas aim of worm is to replicate itself repeatedly and consuming system resources, by this way slow down system or network performance.

3. Keyloggers

Keyloggers, also known as keystroke loggers or keyboard capturing software, are tools or programs designed to record and monitor keystrokes on a computer or mobile device.

Applications of keyloggers

Keyloggers can be used for legitimate purpose as well as malicious.

1. Legitimate purpose :

- System Monitoring: Keyloggers are sometimes used by system administrators or employers to monitor and track computer usage within an organization for security or productivity purposes.
- Parental Control: Keyloggers can be employed by parents to monitor their children's online activities and ensure their safety.
- Law Enforcement: Keyloggers may be used by law enforcement agencies during investigations to gather evidence or track suspect activities with proper legal authorization.

2. **Malicious purpose :**

- Information Theft: Malicious keyloggers are designed to capture sensitive information, such as usernames, passwords, credit card details, or personal data, entered by users on a compromised system. Attackers can use this information for identity theft, financial fraud, or unauthorized access to accounts.
- Credential Harvesting: Keyloggers can be used to capture login credentials for various online services, including email accounts, social media platforms, or banking websites. These stolen credentials can be sold on the dark web or used for further unauthorized activities.
- Remote Access: Some keyloggers allow attackers to remotely access the compromised system and monitor keystrokes in real-time, providing unauthorized access to sensitive data or control over the system.

3. Types of keyloggers

There are several types of keyloggers, each with its own characteristics and methods of operation. Here are some common types of keyloggers :

1. Hardware Keyloggers: Hardware keyloggers are physical devices that are physically attached between the keyboard and the computer or inserted into the USB port. They record keystrokes directly from the keyboard.
2. Software Keyloggers: Software keyloggers are programs or malicious software installed on a computer or mobile device. They run in the background and record keystrokes, capturing the information entered by the user.
3. Memory-Injection Keyloggers: Memory-injection keyloggers inject malicious code into running processes or the memory of a target system. They intercept and record keystrokes by hooking into the operating system's keyboard events.
4. Form Grabbing Keyloggers: Form grabbing keyloggers target web browsers and capture information submitted through online forms.

4. Trojan horse

A Trojan, or Trojan horse, is one of the most dangerous malware types. It usually represents itself as something useful in order to trick you. Once it's on your system, the attackers behind the Trojan gain unauthorized access to the affected computer. From there, Trojans can be used to steal financial information or install other forms of malware, often ransomware.

5. Rootkit

Rootkit is a form of malware that provides the attacker with administrator privileges on the infected system, also known as "root" access. Typically, it is also designed to stay hidden from the user, other software on the system, and the operating system itself.

6. Adware

Adware is unwanted software designed to throw advertisements up on your screen, most often within a web browser. Typically, it uses an underhanded method to either disguise itself as legitimate, or piggyback on another program to trick you into installing it on your PC, tablet, or mobile device.

7. Spyware

Spyware is malware that secretly observes the computer user's activities without permission and reports it to the software's author.

8. Backdoors

Backdoor allows someone to enter your house, not from the legal way that is the front door. In technical terms, the backdoor is any sort of method which allows hacker, or even government to access your system without your permission. A Backdoor can be installed on your system by hackers in the form of some malware application or using your device's software vulnerabilities.

All the malware like rootkits, trojans, spyware, keyloggers, worms and even ransomware are considered to be backdoors if installed in user's devices without their permission or knowledge.

2.8 FIREWALL

2.8.1 Need of Firewall

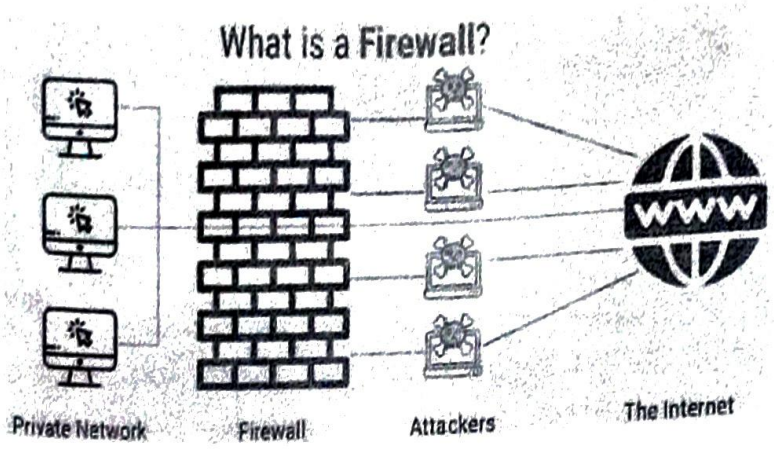
The unparalleled improvement in the internet technology has opened the possibilities to connect any computer with any other computer in the world. It's a great advantage for the individual as well as business houses or organisations. But the problems with the large organisations are: (1) They have large amount of confidential data that must be keep secret from their business rivals. (2) They must have mechanism that can protect these valuable and confidential information from outsider. Firewall is a such mechanism which protects individual or corporate network from outside attacker.

2.8.2 What is Firewall ?

A firewall is a network security device or software that acts as a barrier between an internal network and external networks or the internet. Its primary purpose is to monitor and control incoming and outgoing network traffic based on predetermined security rules.

Conceptually, a firewall can be compared with a security person standing outside a house of nation's president. He physically checks every person who enters into or exit from the house. If security person finds a suspicious person, he stops that person. Firewall also works like security person and checks every data packet enters or exits from the private network.

Firewalls are designed to prevent unauthorized access to a network by filtering and blocking potentially harmful or malicious traffic while allowing legitimate communication to pass through. They examine network packets, which are small units of data, and apply rules to determine whether the packets should be allowed or blocked.



[Fig. 2.20 : Firewall working Architecture]

Firewalls play a crucial role in network security by protecting against various threats, such as unauthorized access attempts, malware infections, distributed denial-of-service (DDoS) attacks, and data breaches. They are an essential component of a comprehensive security strategy and are commonly used in both home networks and large-scale enterprise environments.

2.8.3 Types of Firewalls

Firewalls can be implemented in various forms. On the base of implementation firewalls can be classified in two categories.

- Network Based Firewall
- Host Based Firewall

1. Network Based Firewall

Network Firewalls are the devices that are used to prevent private networks from unauthorized access. The major purpose of the network firewall is to protect an inner network by separating it from the outer network. Inner Network can be simply called a network created inside an organization and a network that is not in the range of inner network can be considered as Outer Network.

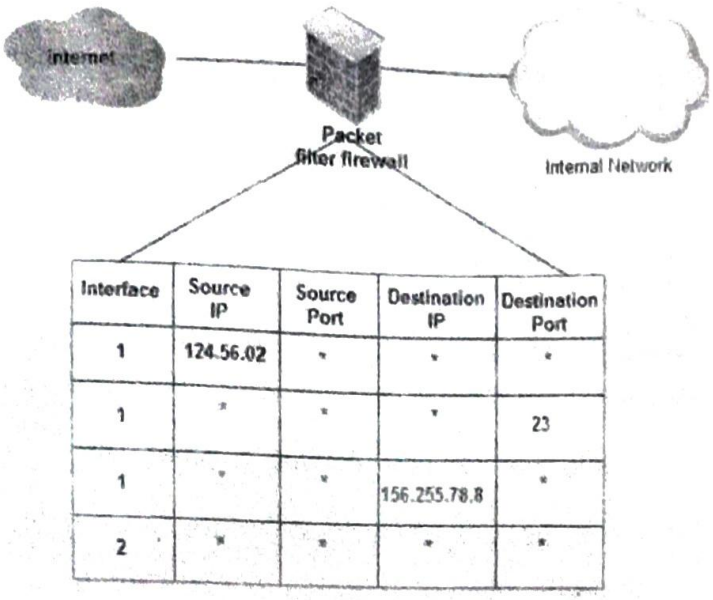
Types of Network based firewalls

- **Packet filtering firewall (First Generation firewall)**

  As the name suggest Packet filtering firewall is used to monitor incoming and outgoing packets, and decide whether to allow them or stop based on protocols, ports, source and destination IP addresses, and other factors. Every packet is handled separately by packet firewalls. Packet filtering firewalls are also known as static firewall.

  Working of packet filter firewall

  (a) Receive each incoming packet to the packet filter node which is also called **filtering router** or **screening router.**



Interface	Source IP	Source Port	Destination IP	Destination Port
1	124.56.02	*	*	*
1	*	*	*	23
1	*	*	156.255.78.8	*
2	*	*	*	*

[Fig. 2.21 : Filtering Rule Table]

(b) Apply set of predefined rules on each packet, If there is a match with one of the set rules, decide whether to accept or discard the packet based on that rule. For example, a rule could specify: disallow all incoming traffic from an IP address 157.28.19.14

(c) If there is no match with any rule, take the default action. The default can be discarding all packets or accept all packets.

- **Stateful Inspection Firewall (Second generation Firewall)**

Stateful inspection firewalls include both packet filtering and TCP handshake verification, making stateful inspection firewalls superior to packet-filtering firewalls.

When a user establishes a connection and requests data, the firewall creates a database (state table). The database is used to store session information such as source IP address, port number, destination IP address, destination port number, etc. Connection information is stored for each session in the state table. Using stateful inspection technology, these firewalls create security rules to allow anticipated traffic.

In most cases, stateful inspection firewalls are implemented as additional security levels. Advantage of this firewall is more secure than stateless firewall. The disadvantage is it increases the load and puts more pressure on computing resources. So, it leads to slower transfer rate for data packets than other solutions.

- **Next Generation Firewalls**

Many of the latest released firewalls are usually defined as 'next-generation firewalls'. However, there is no specific definition for next-generation firewalls. This type of firewall is usually defined as a security device combining the features and functionalities of other firewalls. These firewalls include deep-packet inspection (DPI), surface-level packet inspection, and TCP handshake testing, etc.

NGFW includes higher levels of security than packet-filtering and stateful inspection firewalls. Unlike traditional firewalls, NGFW monitors the entire transaction of data, including packet headers, packet contents, and sources. NGFWs are designed in such a way that they can prevent more sophisticated and evolving security threats such as malware attacks, external threats, and advance intrusion.

2. Host Based Firewall

These are software applications installed on individual computers or devices to control traffic to and from that specific device. They provide an added layer of security, especially when devices are connected to untrusted networks.

2.8.4 Advantages and Disadvantages of Firewalls

Advantages of using Firewall

1. **Preventing unwanted access :** By restricting incoming traffic from specific IP addresses or networks, firewalls can stop hackers and other bad actors from getting easy access to a system or network. safeguarding against unauthorized access.
2. **Avoiding malware and additional dangers :** Prevention of malware and other threats: Firewalls can be configured to stop traffic that is connected to known malware or other security issues, helping to thwart these types of attacks.
3. **Control of network access :** Firewalls can be used to restrict access to specific servers or applications, as well as to specific network resources or services, by limiting access to designated persons or groups.
4. **Network activity monitoring :** Firewalls can be configured to log and monitor every activity on the network.
5. **Regulation compliance :** Many industries are bound by rules that demand the usage of firewalls or other security measures. Organizations can comply with these rules and prevent any fines or penalties by using a firewall.
6. **Network segmentation :** By using firewalls to split up a bigger network into smaller subnets, the attack surface is reduced and the security level is raised.

Disadvantages of using Firewall

1. **Complexity :** Set up of firewall can be time-consuming and difficult, especially for bigger networks or companies with a wide variety of devices.
2. **Limited Visibility :** Firewalls can only observe and manage traffic at the network level.
3. **False sense of security :** Some businesses may place an excessive amount of reliance on their firewall and disregard other crucial security measures like endpoint security or intrusion detection systems.

4. **Limited adaptability :** Because firewalls are frequently rule-based, they might not be able to respond to fresh security threats.
5. **Performance impact :** Network performance can be significantly impacted by firewalls, particularly in the case of lot of traffic.
6. **Limited scalability :** Because firewalls are only able to secure one network, businesses that have several networks must deploy many firewalls, which can be expensive.
7. **Limited VPN support :** Some firewalls might not allow complex VPN features like split tunnelling, which could restrict the experience of a remote worker.
8. **Cost :** Purchasing many devices or add-on features for a firewall system can be expensive, especially for businesses.

2.9 PROXY SERVER

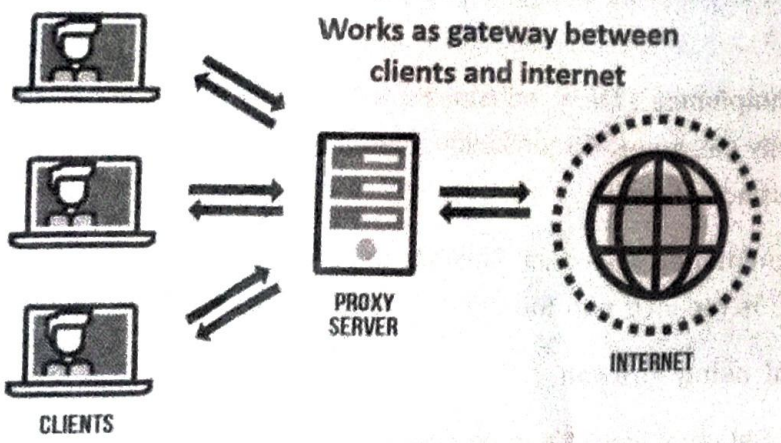
2.9.1 Proxy servers and its working

The proxy server is a computer on the internet that accepts the incoming requests from the client and forwards those requests to the destination server. It works as a gateway between the end-user and the internet. It plays an intermediary role between users and targeted websites or servers.

There are two main purposes of proxy server:

- To keep the system behind it anonymous.
- To speed up resource access using concept of caching.

Working mechanism of proxy server :



[Fig. 2.22 : Working of proxy server]

The proxy server accepts the request from the client and produces a response based on the following conditions :

1. If the requested data or page already exists in the local cache, the proxy server itself provides the required data or page to the client.

2. If the requested data or page does not exist in the local cache, the proxy server forwards that request to the destination server.

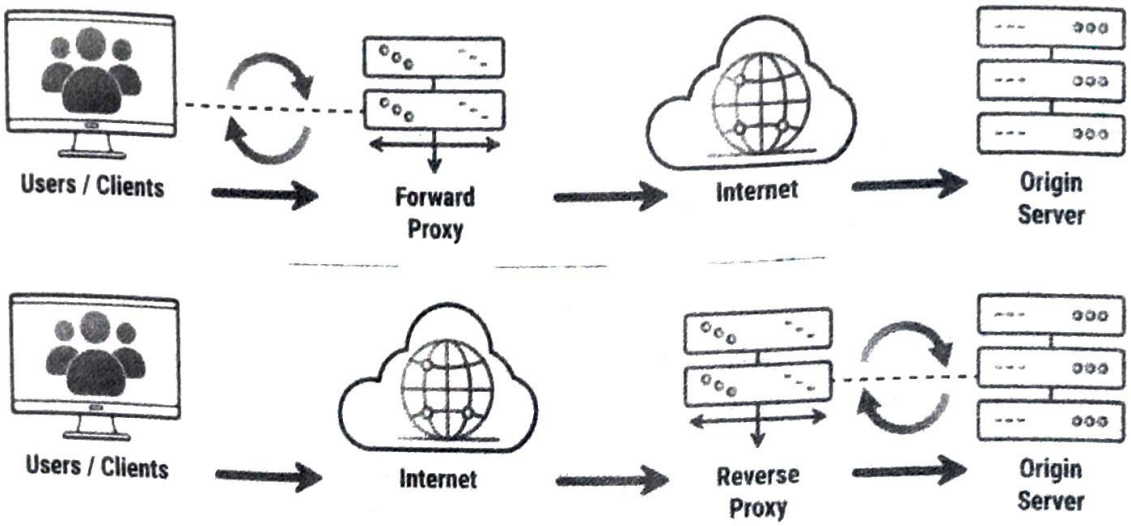
3. The proxy servers transfer the replies to the client and also being cached to them.

Therefore, it can be said that the proxy server acts as a client as well as the server.

2.9.2 Types of proxy servers

Open or Forward Proxy Server :

Forward proxy server refers to those sorts of intermediaries that get demands from web clients and afterward peruse destinations to gather the mentioned information. After collecting the data from the sites, it forwards the data to the internet users directly. It bypasses the firewall made by authorities. The following image shows forward proxy configuration.



[Fig. 2.23 : Forward Proxy V/s Reverse proxy]

Reverse Proxy Server :

It is a proxy server that is installed in the neighbourhood of multiple other internal resources. It validated and processes a transaction in such a way that the clients do not communicate directly. The most popular reverse proxies are **Varnish** and **Squid**. The above image shows the reverse proxy configuration.

Transparent Proxy :

It is a proxy server that does not modify the request or response beyond what is required for proxy authentication and identification. It works on port 80.

Non-Transparent Proxy :

It is an intermediary that alters the solicitation reaction to offer some extra types of assistance to the client. Web demands are straightforwardly shipped off the intermediary paying little mind to the worker from where they started.

Web Proxy Server : The proxy server targeted to the WWW is called a web proxy server.

Public Proxy :

A public proxy is available free of cost. It is perfect for the user for whom cost is a major concern while security and speed are not. Its speed is usually slow. Using a public proxy puts the user at high risk because information can be accessed by others on the internet.

Residential Proxy :

It assigns an IP address to a specific device. All requests made by the client channelled through that device. It is ideal for the users who want to verify ads that display on their websites. Using the residential proxy server, we can block unwanted and suspicious ads from competitors. In comparison to other proxy servers, the residential proxy server is more reliable.

HTTP Proxy :

HTTP proxies are those proxy servers that are used to save cache files of the browsed websites. It saves time and enhances the speed because cached files reside in the local memory. If the user again wants to access the same file proxy itself provides the same file without actually browsing the pages.

2.9.3 Need for using proxy servers

- It reduces the chances of data breaches.
- It adds a subsidiary layer of security between server and outside traffic.
- It also protects from hackers.
- It filters the requests.
- It improves the security and enhances the privacy of the user.
- It hides the identity (IP address) of the user.
- It controls the traffic and prevents crashes.

Self - Assessment

Q. 1 Answer the below short questions :

(1) What do you mean by attack? List out various types of attacks.

(2) Differentiate: Active attacks V/s Passive attacks.

(3) Explain types of attacks in general point of view.

(4) Explain types of attacks in technical point of view.

(5) Explain types of attacks with implementation point of view.

(6) What is Digital Signature?

(7) List out properties of Digital Signature.

(8) Write down steps to create Digital Signature and its verification.

(9) What is PGP ? List out various services provided by PGP.

(10) Explain e-mail authentication process using PGP.

(11) What is SSL? List of various protocols of SSL.

(12) Draw the architecture of SSL.

(13) Draw the SSL Record format.

(14) Explain Change Cipher protocol and alert protocol.

(15) what is TLS? How it is different than SSL?

(16) What is IPsec? List out various services provided by IPsec.

(17) Draw the architecture of IPsec.

(18) Draw the format of ESP Packet.

(19) Draw the format of AH Packet.

(20) Differentiate: HTTP V/s HTTPS

(21) List out advantages of using HTTPS.

(22) What is Malware? List out common types of Malwares.

(23) What is virus? Explain Virus Life Cycle.

(24) List out various types of viruses with their properties.

(25) Define : Worm, Trojan Horse, Ransomware, Rootkit, Keyloggers, Adware, Spyware, Backdoors

(26) What is Firewall? Explain with simple real-life example.

(27) List out various types of firewalls.

(28) Explain advantages of using firewalls.

(29) What is proxy server? List out various types of proxy server.

Q. 2 Explain the below questions :

(1) What is Attack? Explain various types of attacks in detail.

(2) Explain working of Digital Signature with its creation and verification.

(3) Short note on : PGP

(4) Explain SSL Record protocol.

(5) Explain SSL Handshake protocol.

(6) Explain working of Transport Layer Security (TLS) Protocol.

(7) Explain an Architecture of IP Security.

(8) What is HTTPS? Explain working of HTTPs

(9) What is Virus? Explain with its lifecycle and types.

(10) What are keyloggers? Explain its applications.

(11) Explain all about different types of keyloggers.

(12) What is firewall? Explain Packet filtering firewall in detail.

(13) Explain advantages and disadvantages of using firewalls.

(14) What is Proxy server? Explain working of proxy server.

(15) Explain various types of proxy servers in detail.

***

Chapter 3

CYBER CRIME

3.1 OVERVIEW OF CYBERCRIME

- INTRODUCTION TO CYBER CRIME
- INTRODUCTION TO CYBER CRIMINAL

3.2 CLASSIFICATION OF CYBER CRIMES

- ORGANISATIONAL CLASSIFICATION
- INDIVISUAL BASED CLASSIFICATION
- SOCIAL BASED CLASSIFICATION
- PROPERTY BASED CLASSIFICATION

3.3 CHALLENGES AND PREVENTIONS OF CYBER CRIME

- CHALLENGES OF CYBER CRIME
- PREVENTION OF CYBER CRIME

3.4 CYBER LAW

- THE INFORMATION TECHNOLOGY ACT, 2000
- THE INFORMATION TECHNOLOGY ACT, 2008
- SECTION 65 : TAMPERING WITH COMPUTER SOURCE DOCUMENTS
- SECTION 66 : COMPUTER RELATED OFFENCES
- SECTION 67 : PUNISHMENT FOR PUBLISHING OR TRANSMITTING OBSCENE MATERIAL IN ELECTRONIC FORM

○ **Self - Assessment**

3.1 OVERVIEW OF CYBERCRIME

The topic of most discussion in the twenty-first century is cybercrime. The number of people using smartphones and the internet is increasing, which is worrisome for the privacy and security of consumers in the technology industry globally. Because of this, it is imperative that all users understand cybercrime and security. According to this perspective, students should have knowledge about cybercrime and be ready to deal with impacts of it.

3.1.1 Introduction to cyber crime

Cybercrime is a risky attack that can happen to a business or a person. In numerous instances, a cyberattack has resulted in significant losses for both the organization and the person as a result of a data breach. Our day is driven by technology, and computers are now the source of all knowledge. Attacks on computers and other electronic devices are a part of cybercrime. These cyberattacks could be dangerous not just for personal or organizational but also for the country. Currently, there are several instances of cyberattacks in India and around the world, which calls for increased security. If not stopped at the outset, these attacks are also having an impact on the nation's economy.

Everybody thinks that only stealing someone's private data is Cyber Crime. But in defining terms we can say that

"Cyber Crime refers to the use of an electronic device (computer, laptop, etc.) for stealing someone's data or trying to harm them using a computer."

It comprises a wide range of crimes such as cyber fraud, financial scams, cybersex trafficking, ad scams, etc. Cybercrime encloses a wide range of activities, but these can generally be divided into two categories :

1. Crimes that aim at computer networks or devices. These types of crimes involve different threats (like virus, bugs etc.) and denial-of-service (DoS) attacks.
2. Crimes that use computer networks to commit other criminal activities. These types of crimes include cyber stalking, financial fraud or identity theft.

Some Notable Cases :

- One of the most high-profile banking computer crimes happened in 1970. The top teller at New York's Union Dime Savings Bank's Park Avenue branch stole over $1.5 million from hundreds of accounts.
- A hacker organization known as **MOD (Masters of Deception)** is accused of stealing passwords and technical data from Pacific Bell, Nynex, and other telephone providers, as well as six major credit bureaus and two major colleges.
- In January 2012, Zappos.com suffered a security breach that exposed up to 24 million customers' credit card details, personal information, and billing and delivery addresses.
- Unlawful access to camera sensors, microphone sensors, phonebook contacts, all internet-enabled apps, and metadata on mobile phones running Android and iOS appears to have been allowed by Israeli spyware, which was determined to be in use in at least 46 countries across the world.

3.1.2 Introduction to Cybercriminal

"Cybercriminals are individuals or teams of people who use technology to commit malicious activities on digital systems or networks with the intention of stealing sensitive company information or personal data, and generating profit."

Cybercriminals are known to access the cybercriminal underground markets found in the deep web to trade malicious goods and services, such as hacking tools and stolen data. Cybercriminal underground markets are known to specialize in certain products or services.

How cybercriminals are different than Hackers and threat actors :

Hacking does not necessarily count as a cybercrime; as such, not all hackers are cybercriminals. Cybercriminals hack and infiltrate computer systems with malicious intent, while hackers only seek to find new and innovative ways to use a system, be it for good or bad.

Cybercriminals also differ greatly from threat actors in various ways, the first of which is intent. Threat actors are individuals who conduct targeted attacks, which actively pursue and compromise a target entity's infrastructure. Cybercriminals are unlikely to focus on a single entity, but conduct operations on broad masses of victims defined only by similar platform types, online behaviour, or programs used.

Secondly, they differ in the way that they conduct their operations. Threat actors follow a six-step process, which includes researching targets and moving laterally inside a network. Cybercriminals, on the other hand, are unlikely to follow defined steps to get what they want from their victims.

Comparison between Hackers and Cybercriminals

Hackers	Cybercriminal
Hackers are computer programmers who use their skills to breach digital systems	Cybercriminals, on the other hand, are people who use computers to commit crimes
The intension of hackers not always bad. E.g. Ethical hackers, use their knowledge to improve security practices.	The intension of Cyber criminals is always to commit crime.
The most common types of hackers are White hat, Black hat, and Grey hat Hackers.	The common types of Cybercriminals are Hacktivists,Script Kiddies, Insider Threats, Cybercrime Groups
The primary goal of hackers is not a financial aid.	The primary goal of the cybercriminal is financial aids.

3.2 CLASSIFICATION OF CYBERCRIMES

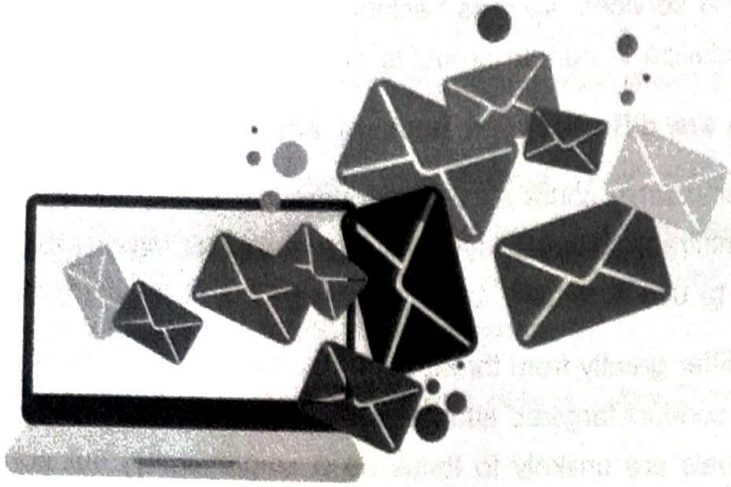
Hacking does not necessarily count as a cybercrime; as such, not all hackers are cybercriminals. Cybercriminals hack and infiltrate computer systems with malicious intent, while hackers only seek

3.2.1 Organizational Classification

A. E mail Bombing

An email bomb is a form of Internet abuse which is perpetrated through the sending of massive volumes of email to a specific email address with the goal of overflowing the mailbox and overwhelming the mail server hosting the address, making it into some form of denial-of-service attack.

An email bomb is also known as a **letter bomb.**



[Fig. 3.1 : E Mail Bombing]

There are three ways to create an email bomb:

- Mass mailing: involves sending numerous duplicates of the same email to one email address. Because of the simplicity of this attack, it can be easily detected by spam filters. To be done on a massive scale, an attacker can use a bot net or zombie net, computers across the globe which are under the attacker's control due to some form of malware such as Trojans, and then instructing the bot net to send millions of emails to a single or a few addresses at once in order to perform a denial-of-service attack. This is harder for spam filters to detect since each email would be coming from a unique source.
- List linking: The technique involves subscribing the email address of victim for attack to different email list subscriptions so it would always receive spam mail from these lists. The user then has to manually unsubscribe from each list.
- ZIP bombing: the latest twist on email bombing using ZIP archived attachments. Mail servers always check email attachments for viruses, especially zip archives and .exe files. The idea here is to place a text file with millions or billions of arbitrary characters or even a single letter repeated millions of times so that the scanner would require a greater amount of processing power to read each one. Combining this with mass mailing techniques ups the potential for a denial-of-service attack to succeed.

Some of the **prevention methods** from e mail bombing are as :

- Strong Email Filters: Implementing robust email filtering solutions can help in identifying and blocking mass email sign-ups and suspicious influxes of emails.
- Monitoring and Alerts: Setting up monitoring systems to alert when there is an unusual spike in email traffic can help in quickly identifying an email bomb attack.
- Regular Security Audits: Conducting regular audits of email systems can help in identifying potential vulnerabilities that could be exploited for email bombing.

- Educating Employees: In organizations, educating employees about email bombs and related Email Security Threats is crucial. Awareness can lead to quicker identification and response to such attacks.
- Backup Communication Channels: Establishing alternative communication channels can ensure continuity of operations in case the primary email system is compromised.
- Collaboration with Email Providers: Working closely with your email service provider can be beneficial. Some providers offer specialized services to mitigate the effects of email bombing.

B. Salami Attack

A Salami Attack, also known as a Salami Slicing Attack, is a fraudulent method where a cybercriminal commits a series of minor, inconspicuous actions or thefts that, when combined, can lead to significant harm or a considerable compromise of data, resources, or assets.

The name "Salami Attack" originates from the idea of a cybercriminal metaphorically slicing off small, seemingly insignificant pieces of data or assets, much like slicing salami thinly.

These attacks are insidious because they are typically carried out in a way that each individual action remains inconspicuous, making it challenging for security systems to detect a breach until significant damage has already occurred.

Types of Salami Attacks

- Financial Salami Attack: This is the most common type, where attackers steal small amounts of money over time, often from multiple accounts or transactions. Attackers may round down transactions or subtly manipulate bank account balances to avoid immediate detection.

  A bank employee programs a system to round down interest calculations and deposits the fractions of a cent into a personal account.

- Data Salami Attack: Attackers gradually steal or manipulate small pieces of data from the database that are not immediately noticeable but lead to large-scale breaches or long-term integrity issues.

  A cybercriminal hacks into a company's database and extracts small portions of customer data (e.g., email addresses or phone numbers) to build a spam list or launch targeted phishing attacks.

- Resource Salami Attack: Attackers consume small amounts of computing resources or network bandwidth from multiple users or organizations to create a larger network for malicious purposes.

  A botnet operator uses thousands of infected devices to launch Distributed Denial of Service (DDoS) attacks on a website, consuming a small portion of each device's bandwidth, but the cumulative effect is a devastating attack.

Some of the **prevention methods** from Salami Attacks are as :

- Regular Audits: Implement comprehensive and frequent audits. These should be unpredictably timed and thoroughly check transaction logs and data records.

- Enhanced Transaction Monitoring: Use advanced monitoring software to detect anomalies in transaction patterns, no matter how small.
- Employee Training: Educate employees about salami attacks, including how to recognize and report suspicious activities.
- Data Validation and Integrity Checks: Regularly validate data and check for integrity to spot any discrepancies that might indicate a salami slicing technique in play.

Salami Attacks may appear inconspicuous and minor in isolation, but when executed systematically, they can lead to significant damage and losses.

C. Logic Bomb

A logic bomb is a malicious piece of code that's secretly inserted into a computer network, operating system, or software application. It lies dormant until a specific condition occurs. When this condition is met, the logic bomb is triggered — devastating a system by corrupting data, deleting files, or clearing hard drives.

Logic bombs are small bits of code contained in other programs. Although they might be malicious, they are not technically malware. Common types of malwares include viruses and worms, which can contain logic bombs as part of their attack strategy. A logic bomb virus would then be a virus that has a logic bomb in its code.

The defining characteristics of a logic bomb are:

- It lies dormant for a specific amount of time.
- Its payload is unknown until it triggers. A payload is the component that carries out the malicious activity.
- It's triggered by a certain condition. The detonator of the logic bomb is the condition that must be met. It's this feature that lets logic code bombs go undetected for long periods of time. Logic bombs with triggers related to dates or specific times are also known as **time bombs**.

D. Trojan Horse

A Trojan, or Trojan horse, is one of the most dangerous malware types. It usually represents itself as something useful in order to trick you. Once it's on your system, the attackers behind the Trojan gain unauthorized access to the affected computer. From there, Trojans can be used to steal financial information or install other forms of malware, often ransomware.

A Trojan is sometimes called a Trojan virus or Trojan horse virus, but those terms are technically incorrect. Unlike a virus or worm, Trojan malware cannot replicate itself or self-execute. It requires specific and deliberate action from the user.

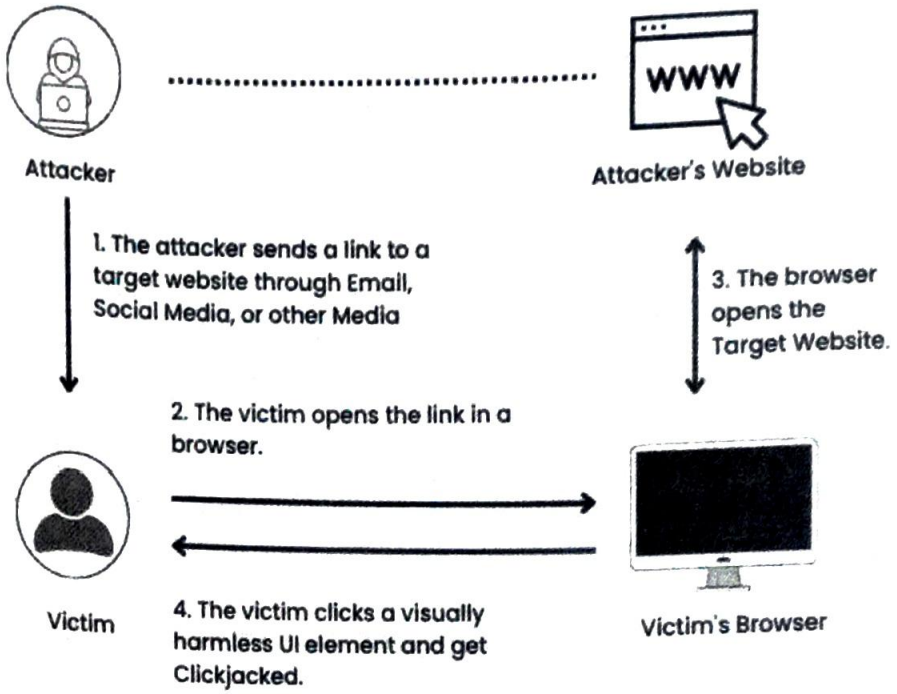
Trojans are malware, and like most forms of malware, Trojans are designed to damage files, redirect internet traffic, monitor the user's activity, steal sensitive data or set up backdoor access points to the system. Trojans may delete, block, modify, leak or copy data, which can then be sold back to the user.

E. Web Jacking

Among the several Cyberattacks; Web Jacking in Cyber Security is one of the most prominent.

Web Jacking is a type of phishing attack which frequently used to obtain user information, such as credit card numbers and login information, in Cyber Security.

In simplest terms, when attackers illegally gain control of an organisation's or individual's website is known as Web Jacking. The hackers implant a fake website, which, when you open it, takes you to another fraudulent website, where the attackers try to extract sensitive information. This crucial data can range from simple account passwords to credit card details.



[Fig. 3.2 : Web Jacking Working Model]

Following are the steps generally followed by attackers in Web Jacking.

- *Fake Website Creation* : Firstly, the hacker creates a fake web page using the same domain name as the targeted web application.
- *Hosting* : The second step is to host it on your computer or shared hosting.
- *Sending link* : This step involves the hacker sending the fake website's link to the victim. The success of the hacker's mission depends fully on whether the victim falls for it.
- *Entering details* : If the victim clicks on the link, it directs them to the malicious website. As the victim enters sensitive information like their login credentials or credit card details, the hacker gets all of it. The attacker can use these freshly retrieved details for nefarious reasons.

How one can be safe from Web Jacking

It is essential that you remain vigilant whenever something unfamiliar enters your system. You never know when you could become a victim of web jacking. This suggests that it is vital to remember a few pointers that can maintain cyber security.

- Avoid clicking suspicious links: The first tip to keep in mind is to avoid clicking on suspicious links that make their way to you via emails or messages.
- Check the legitimacy of the link: Always check the legitimacy of the link by pasting the URL on the address bar. Your first hint at a fraudulent link could be the difference between the URL and the intended website.
- Use of anti-Phishing detection browsers: Make use of browsers with anti-phishing detection.
- Confirm Spellings: If your links include company or institution names, confirm the original spelling.
- Provide fake Data: Another tip to keep in mind is that if or when you come across a shady website that is asking for your details, do not give your original credentials. Instead, put in a fake username and password. This way, you protect your information and can confirm the website's legitimacy.

F. Data Diddling

Data Diddling can be defined as illegal or unauthorized fraudulent alteration of data. It is the process of modifying data before or after it is entered into the system, generating a faulty output. While processing large amounts of data, criminals either alter the input or internally make the program that processes the data to malfunction. Considering the quantum of data being processed, these crimes are difficult to track.

Data Diddling attacks are generally targeted on larger corporations like power supply, telecommunications etc. Organisations incur heavy financial loss due to such attacks.

How can data diddling attacks be avoided ?

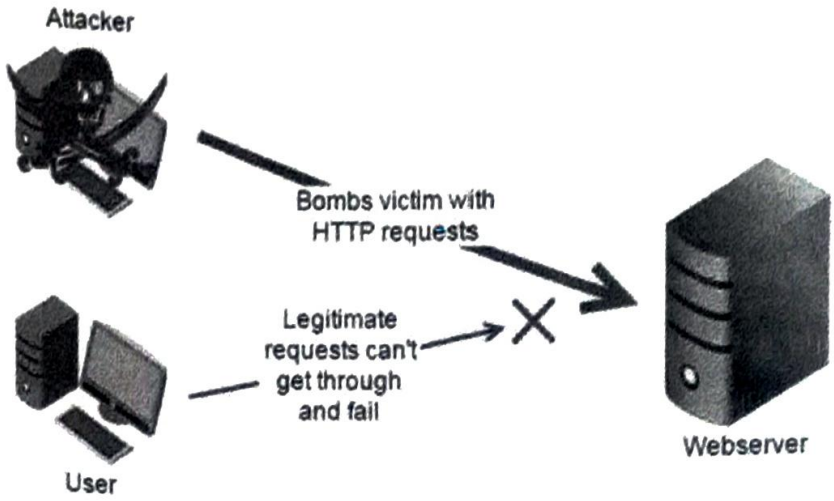
Financial organizations and their clients can prevent misleading data assaults by utilizing a number of countermeasure options:

- Consumers ought to routinely review their monthly statement and transaction history to look for any unusual activity. They can look over these transactions to find any strange credit card charges. If they see anything strange, they should notify their financial institution right away.
- The OWASP (Open Web Applications Security Project) principles must be adhered to in order to guarantee that no application contains undesired or harmful code.
- You should flag an email as phishing and delete it if it contains an attachment or asks for your bank account details or for you to click on a link to reset your password. Global organizations are still being impacted by phishing assaults, which include spear, email, barrel, and whale phishing. Security teams persist in allocating both organizational financial resources and human capital towards impeding data diddling and other related kinds of data theft.

G. Denial of Service / Distributed Denial of Service

A denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. Services affected may include email, websites, online accounts (e.g., banking), or other services that rely on the affected computer or network.

A denial-of-service condition is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users. DoS attacks can cost an organization both time and money while their resources and services are inaccessible.

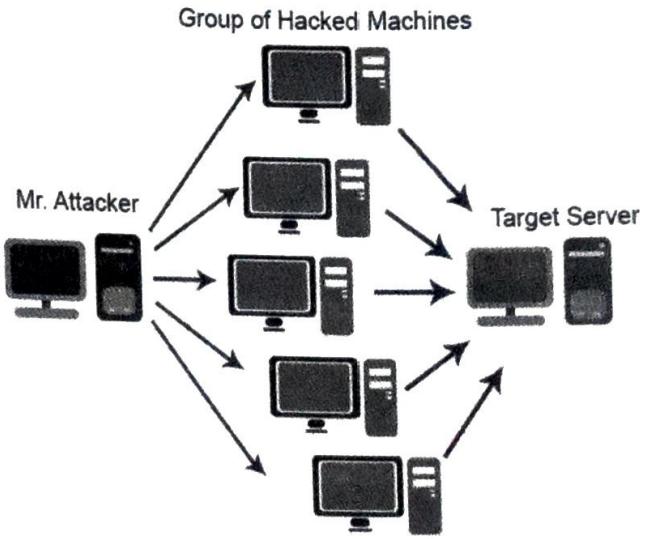


[Fig. 3.3 : Denial of Service Attack]

There are many different methods for carrying out a DoS attack.

- **A Smurf Attack** involves the attacker impersonating the target machine and using its faked source IP address to send Internet Control Message Protocol broadcast packets to several hosts. The targeted host will subsequently get a barrage of responses from the recipients of these spoof packets.
- **A SYN flood** happens when an attacker tries to connect to the target server by sending a request, but fails to finish the connection through the three-way handshake—a Transmission Control Protocol (TCP)/IP network technique that establishes a connection between a local host/client and server. The connected port is left in an occupied state and is not available for new requests due to the unfinished handshake. All open ports will be flooded with requests from an attacker, making it impossible for authorized users to connect.

Distributed Denial of Services Attack



[Fig. 3.4 : Distributed Denial of Service Attack]

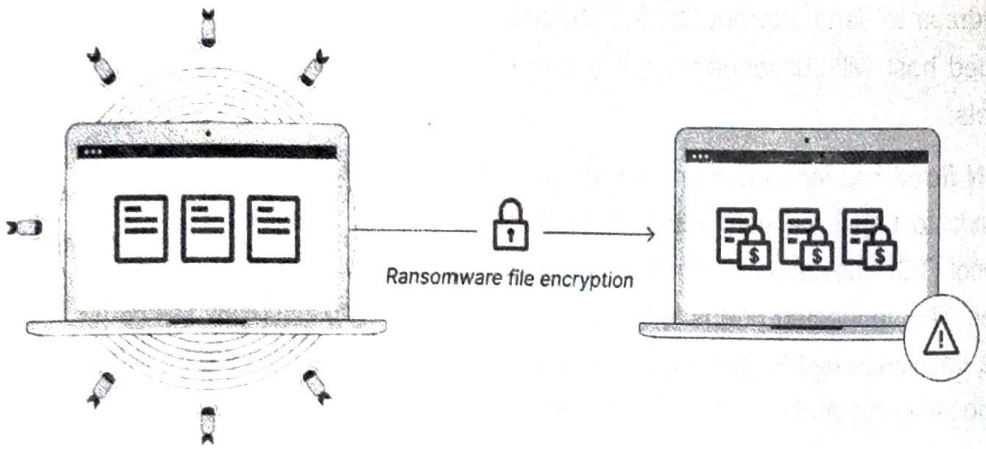
A distributed denial-of-service (DDoS) assault happens when several computers collaborate to attack a single target. A botnet is a collection of compromised internet-connected devices that is frequently used by DDoS attackers to launch massive attacks. Attackers use command and control software to take over many devices by taking advantage of security flaws or device shortcomings. Once in command, a hacker can direct their botnet to attack a target via denial-of-service attacks. In this instance, the attack also affects the infected devices.

Botnets—made up of compromised devices—may also be rented out to other potential attackers. Often the botnet is made available to "attack-for-hire" services, which allow unskilled users to launch DDoS attacks.

DDoS allows for exponentially more requests to be sent to the target, therefore increasing the attack power. It also increases the difficulty of attribution, as the true source of the attack is harder to identify.

G. Ransomware

Malicious software known as ransomware encrypts files and demands payment for their release. Ransomware has the ability to spread swiftly throughout an entire network, and in certain instances, an infection has extended to networks owned by other businesses. Only when the victim pays the ransom can the individual or organization in possession of the malware unlock the files.



[Fig. 3.5 : Ransomware Attack]

Assume Ronak takes Rahi's laptop, puts it in his safe, and demands 20000 Rs. from her before allowing her to get it back. This is basically how ransomware groups work; the only difference is that they do it digitally rather than physically snatching machines away and locking them up.

How Ransomware works ?

Encryption is a vital component of online security and privacy and is frequently utilized for legal purposes. However, ransomware organizations employ malicious encryption to keep everyone, even the rightful owners of the information, from opening and using the encrypted versions of their files.

Now, instead of taking Rahi's laptop, transforms all of her files into a language she is illiterate in. Rahi still has access to the data, but she is unable to view or utilize them, which is comparable to encryption in the context of ransomware. Until she can figure out how to translate them, the files are effectively lost.

However, without the encryption key, decrypting data is nearly impossible, in contrast to interpreting a language.The attacking party keeps the key to themselves, which is why they have the leverage they need to demand payment.

3.2.2 Individual Based Classification

A. Cyber bullying

Cyberbullying is the use of digital communication tools (like the internet and cell phones) to make another person feel angry, sad, or scared. Online bullying is like in-person bullying in two key ways. It's done on purpose. And it tends to happen more than once. The examples include:

- Spreading lies about or posting embarrassing photos or videos of someone on social media.
- Sending hurtful, abusive or threatening messages, images or videos via messaging platforms.
- Impersonating someone and sending mean messages to others on their behalf or through fake accounts.

Cyberbullying leaves a digital footprint – a record that can prove useful and provide evidence to help stop the abuse.

B. Cyber Stalking

Cyberstalking uses the internet and other technologies to harass or stalk another person online, and is potentially a crime. Cyberstalking is an extension of cyberbullying and in-person stalking, can take the form of e-mails, text messages, social media posts, and more.

Even when the recipient says they're not happy or requests them to stop, the conversations usually go on. The content directed at the target is often inappropriate and sometimes even disturbing, which can leave the person feeling fearful, distressed, anxious, and worried.

Here are some examples of things people who cyberstalk might do:

- Post rude, offensive, or suggestive comments online.
- Follow the target online by joining the same groups and forums.
- Send threatening, controlling, or lewd messages or emails to the target.
- Use technology to threaten or blackmail the target.
- Tag the target in posts excessively, even if they have nothing to do with them.
- Comment on or like everything the target posts online.
- Create fake accounts to follow the target on social media.
- Message the target repeatedly.

C. Cyber Defamation

Defamation means giving an "injury to the reputation of a person" resulting from a statement which is false.

Cyber defamation is a new concept but it virtually defames a person through new medium. The medium of defaming the individual's identity is through the help of computers, internet or other digital technologies. If any individual posts or publishes some false statement about the other individual through internet or emails the individual having the defamatory statement with the intention to defame the other about whom the statement has been made would amount to cyber defamation.

D. Phishing

Phishing is a type of cybercrime in which criminals pose as a trustworthy source online to lure victims into providing personal information such as usernames, passwords, or credit card numbers. The goal of any phishing scam is always **stealing personal information**, there are many different types of phishing attacks as described below.

The various types of phishing attacks are: Email Phishing, Spear Phishing, Whaling, Smishing, Vishing, Business Email Compromise (CEO Fraud), Clone Phishing etc....

E. Cyber Fraud and Cyber Theft

Cyber fraud

Cyber fraud involves using online services and software with access to the internet to defraud or take advantage of victims. The term "Cyber fraud" generally covers cybercrime activity that takes place over the internet or on email, including crimes like identity theft, phishing, and other hacking activities designed to scam people out of money.

Cyber theft

Cybercrime is one of the most crucial problems faced by the countries across the globe these days. It includes unauthorized access of information and break security like privacy, password, etc. of any person with the use of internet. Cyber theft is a part of cybercrime which means theft carried out by means of computers or the Internet. The most common types of cyber theft include identity theft, password theft, theft of information, internet time thefts etc.

- Identity theft: Identity theft pertains to illegally obtaining of someone's personal information which defines one's identity for economic benefit. It is the commonest form of cyber theft.
- Internet time theft: It refers to the theft in a manner where the unauthorized person uses internet hours paid by another person. The authorized person gets access to another person's ISP user ID and password, either by hacking or by illegal means without that person's knowledge.
- Intellectual property (IP) theft: Intellectual property (IP) theft is defined as theft of material that is copyrighted, the theft of trade secrets, and trademark violations etc. One of the most commonly and dangerously known consequence of IP theft is counterfeit goods and piracy.

F. Spyware

Spyware is malicious software that enters a user's computer, gathers data from the device and user, and sends it to third parties without their consent. Spyware collects information like user's internet usage,

credit card, and bank account details, or steal credentials. It sends such collected information to advertisers, data collection firms, or malicious actors for a profit.

The common types of spywares are :

- *Adware* : It enters in a device and monitors users' activity then sells their data to advertisers and malicious actors.
- *Infostealer* : It scans device for specific data and instant messaging conversations.
- *Keyloggers* : Keyloggers (Key Stroke logger) are a type of infostealer spyware. They record the keystrokes that a user makes on their infected device, then save the data into an encrypted log file. This spyware method collects all of the information that the user types into their devices, such as email data, passwords, text messages, and usernames.
- *Rootkits* : These enable attackers to deeply infiltrate devices by exploiting security vulnerabilities or logging into machines as an administrator. Rootkits are often difficult and even impossible to detect.
- *Red Shell* : It installs itself onto a device while a user is installing specific PC games, then tracks their online activity. It is generally used by developers to enhance their games and improve their marketing campaigns.
- *System monitors* : These also track user activity on their computer, capturing information like emails sent, social media and other sites visited, and keystrokes.
- *Tracking cookies* : Tracking cookies are dropped onto a device by a website and then used to follow the user's online activity.
- *Trojan Horse Virus* : This brand of spyware enters a device through Trojan malware, which is responsible for delivering the spyware program.

G. E-mail Spoofing

Email spoofing is a technique that is used in spamming and phishing attacks which involves sending email messages with a fake sender address. Email protocols cannot, on their own, authenticate the source of an email. Therefore, it is relatively easy for a spammer or other malicious actors to change the metadata of an email. This way, the protocols think it came the real sender.

E.g. The SMTP (Simple Mail Transport Protocol) doesn't make any provision to authenticate email addresses. So, hackers take advantage of this weakness to fool unsuspecting victims into thinking the mail is coming from someone else.

Difference between E mail Spoofing and Phishing

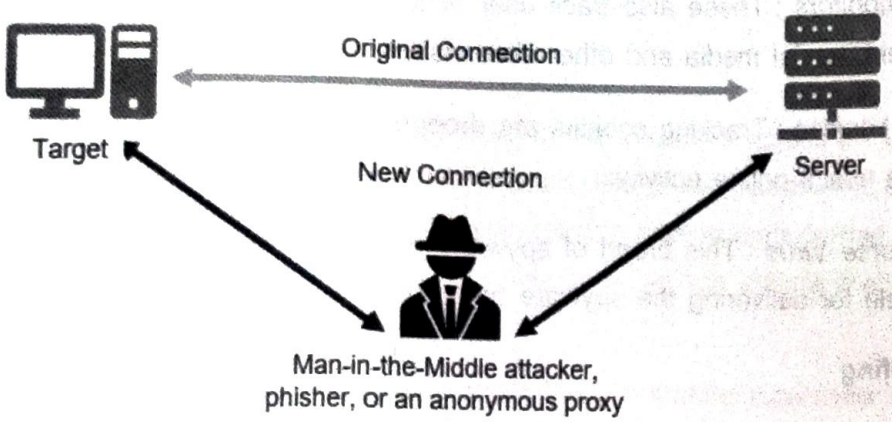
Spoofing	Phishing
Spoofing refers to a form of identity theft where someone uses the identity of a real user.	Phishing involves someone stealing sensitive information such as bank or credit card details.
Spoofing can involve phishing.	Phishing is not an element of spoofing.
With spoofing, the target has to download malware.	Phishing uses social engineering.
Spoofing is used to acquire identity information.	Phishing is aimed at extracting confidential information.

(H) Man in the middle attack

Man-in-the-middle attacks (MITM) are a common type of security attack which allows attackers to manipulate both communicating parties and achieves access to the data that the two parties were trying to deliver to each other.

The attack takes place in between two legitimately communicating parties, allowing the attacker to "listen" to a conversation they should normally not be able to listen to, hence the name "Man-In-The-Middle."

Working of Man In The Middle (MITM) Attack :



[Fig. 3.6 : Man In The Middle Attack]

Regardless of the specific techniques and technologies, the MITM attacks can be carried out with the below work flow order.

1. Sender A sends message to the recipient B.
2. The MITM attacker intercepts the message without sender(A) or receiver(B) knowledge.
3. The MITM attacker changes the message content or removes the message altogether, again, without the knowledge of sender and receiver.

In computing terms, a MITM attack works by exploiting vulnerabilities in network, web, or browser-based security protocols to divert legitimate traffic and steal information from victims.

Some of the Man InThe Middle (MITM) attack types are : *Email Hijacking, Wi-Fi Eavesdropping, DNS Spoofing, Session Hijacking, Secure Sockets Layer (SSL) Hijacking, ARP Cache Poisoning, IP Spoofing, Stealing Browser Cookies*

3.2.3 Social Based Classification

Some of the social based classification are as under :

A. Cyber Pornography

Pornography is a criminal offence which has been considered as one of the corrupt demonstrations causing harm to people. Cyber pornography means an act by using cyberspace to create, display, distribute, import, or publish obscene materials, especially materials related to children who are engaged in sexual acts with adults.

Sexually explicit content has seemingly become a bigger problem than one could have imagined it to be because of technological advancements and easy access of cyberspace.

B. Cyber Terrorism

Cyber Terrorism attack is defined as a "cybercrime that may be used intentionally to cause harm to people on large scale using computer programs and spyware."

Hackers with extensive experience and talent can seriously harm government systems and force a nation to flee out of fear of further attacks. Since this is a sort of terrorism, the goals of such terrorists may be political or ideological.

C. Cyber Spying

Cyber spying, also known as cyber espionage, is a form of Cyber Attack where an attacker obtains information without authorized permission or knowledge by the information holder in a digital setting.

Various methods can be employed to spy digitally: account hacking, tracking behaviour with cookies or keylogging, or implementing malware onto devices such as Trojan horses and spyware are frequently used spying tactics on users. Though pervasive spying in any sense is considered illegal, this does not stop the practice from being carried out on a massive scale through loopholes, especially by those in high power.

D. Social Engineering Attack

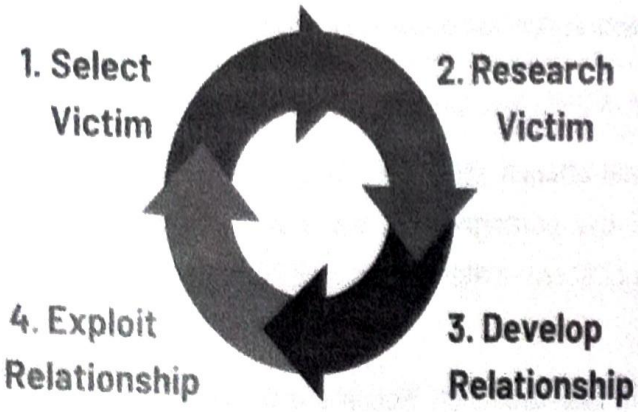
Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Steps of a Social Engineering Attack

Social engineering attacks typically follow these simple steps :

1. **Research :** The attacker identifies victims and chooses a method of attack.

2. **Engage**: The attacker makes contact and begins the process of establishing trust, appealing to greed, helpfulness, or curiosity, and creating a sense of urgency.
3. **Attack**: The attack commences and the attacker collects the payload.
4. **The Gateway**: The attacker covers their tracks and concludes the attack.



[Fig. 3.7: Social Engineering Life Cycle]

Social engineering attacks happen in one or more steps. A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack. Then, the attacker moves to gain the victim's trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources.

E. Online gambling

Government authorities prohibits individuals from betting on sports or gambling contests using a "wire communication facility," which includes the Internet. Yet the Internet allows immediate and anonymous communication that makes it difficult to trace gambling activity. Internet sites can be altered or removed in a matter of minutes. For these reasons organized crime operates internet gambling sites.

Operators alter gambling software to be in their favour so the customer always loses. Unlike real casinos that are highly regulated, Internet gambling is unregulated and dangerous. Individuals gambling on the Internet risk providing credit card numbers and money to criminal gambling operators. Further, minors can gamble on the sites since the Internet is unaware of the age of its users.

3.2.4 Property Based Classification

A. Credit Card Fraud

Credit card fraud is a type of financial crime that involves the unauthorized use of someone else's credit card information to make purchases or access funds. This illicit activity can take various forms, and criminals use different techniques to obtain or use credit card details fraudulently. Here are some common types and aspects of credit card fraud:

- *Stolen Cards* : Criminals may physically steal credit cards from individuals or intercept new cards sent through the mail.

- *Lost or Misplaced Cards* : If someone loses their credit card, it can be found by an unauthorized person who then uses it for fraudulent transactions.
- *Skimming* : Skimming involves using a small device (skimmer) to capture credit card information during a legitimate transaction. This often happens at ATMs, gas pumps, or point-of-sale terminals.
- *Phishing* : Cybercriminals use phishing techniques to trick individuals into providing their credit card information by posing as a trustworthy entity in emails, messages, or websites.
- *Carding* : Carding is a practice where criminals use stolen credit card information to make small online purchases to validate if the card is still active before making larger transactions.
- *Account Takeover* : Hackers may gain unauthorized access to online accounts where credit card information is stored, allowing them to make purchases using the victim's card.
- *Identity Theft* : In cases of identity theft, criminals may use stolen personal information, including credit card details, to open new credit card accounts in the victim's name.
- *Malware and Data Breaches* : Criminals use malware to infect computer systems or exploit vulnerabilities to gain access to large databases containing credit card information. Data breaches at businesses or financial institutions can result in the exposure of thousands or even millions of credit card records.
- *Social Engineering* : Fraudsters may use social engineering techniques to manipulate individuals into revealing their credit card information over the phone or online.

To prevent credit card fraud, individuals and businesses can take various measures, such as monitoring their accounts regularly, using secure and unique passwords, enabling two-factor authentication, and being cautious about sharing personal information.

B. Software Piracy

Software privacy refers to the illegal act of copying, distributing, using, or selling application without the permission or proper licensing from the rightful owners or publishers.

This practice violates intellectual property laws, specifically copyright laws, which are designed to protect the rights of creators and publishers.

Here are some common forms of software piracy :

- *Unauthorised Copying* : This involves installing and using application on multiple computers beyond the terms allowed by the purchased license. For example, using one license to install application on multiple office computers or sharing it with friends.
- *Counterfeiting* : This type of piracy involves creating and selling fake copies of application. These copies often appear legitimate but are illegal reproductions.
- *Internet Piracy* : This involves downloading application from the internet without paying for it or obtaining it through proper channels. It includes using torrent sites, file-sharing networks, or unauthorised download links.

- *Cracking Software* : This is the process of modifying application to remove or disable features that are considered undesirable by the person cracking it, often including copy protection features.
- *Corporate Piracy* : This occurs when businesses use unlicensed application or more copies than permitted by the license. It's a form of piracy that can involve significant financial losses for application companies.
- *OEM (Original Equipment Manufacturer) Unbundling* : This happens when OEM application, which is meant to be sold with specific hardware, is copied and sold separately without the hardware.
- *Softlifting* : This refers to purchasing a single licensed copy of application and then loading it onto several computers, contrary to the license terms.

C. Copyright Infringement

Copyright infringement is the use or production of copyright-protected material without the permission of the copyright holder. Copyright infringement means that the rights afforded to the copyright holder, such as the exclusive use of a work for a set period of time, are being breached by a third party. Music and movies are two of the most well-known forms of entertainment that suffer from significant amounts of copyright infringement.

Living in the digital era, it is becoming less common for authors to express their creative sparkle as physical embodiments. The digital form of expression carries many advantages but also opens some potential threats. One of them is vulnerability to cyberattacks and cybercrime. Some forms of copyrighted work are, by nature, conditioned to be in a digital (electronic) form, such as databases and computer software.

As a consequence, copyright infringement and cybersecurity-related issues are at the point of focus.

D. Trademarks violations

Trademark violations in cybersecurity occur when a company or individual uses a trademarked name, logo, or other intellectual property without proper authorization in the context of cybersecurity products, services, or marketing materials.

Trademark violation may happen in various ways:

1. Product Names : Companies may use trademarked names or terms to market their cybersecurity products or services without authorization from the trademark owner.
2. Domain Names : Registering domain names that include trademarked terms or brands to mislead users or divert traffic is another common form of trademark violation in cybersecurity.
3. Advertising and Marketing : Unauthorized use of trademarked logos, slogans, or other branding elements in advertising materials, online campaigns, or social media posts can constitute trademark infringement.
4. Cybersquatting : This involves registering domain names with the intent to profit from the goodwill associated with someone else's trademark.

5. False Endorsement : Using a trademarked name or logo in a way that suggests endorsement or affiliation with the trademark owner when no such relationship exists can lead to trademark violations.

Trademark violations in cybersecurity can result in legal action, including cease and desist letters, lawsuits for damages, and demands to transfer domain names. It's essential for businesses operating in the cybersecurity space to conduct thorough research and obtain proper authorization when using third-party trademarks to avoid potential legal consequences.

3.3 CHALLENGES AND PREVENTIONS OF CYBERCRIME

The incredible evolution of information society and its dependence on Internet usage in world and particularly in India is laterally accompanied by vulnerability of societies to cybercrime. Cybercriminals are not constrained by geographical limitations as cyberspace is a free-flowing, borderless and a global problem. These crimes can't be deterred by local laws. India to counter Cybercrime has engaged itself in various bilateral agreements like cyber agreement with Russia and a framework agreement with the US, Indo-Israel cyber framework is yet another effort of India to streamline its cyberspace. Even if this effort there are so many challenges of Cybercrime. These bilateral agreements have limited scope and are inadequate and ineffective to deal with cybercrime. Some of the challenges are as under:

3.3.1 Challenges of Cyber Crime

- **Poor awareness about their cyber rights :**

  Cybercrime usually happen with illiterate people around the world who are unaware about their cyber rights implemented by the government of that particular country.

- **Anonymity :**

  Those who Commit cybercrime are anonymous for us so we cannot do anything with these people.

- **Less number of registered cases :**

  Every country in the world faces the challenge of cybercrime and the rate of cybercrime is increasing day by day because the people who even don't register a case of cybercrime and this is major challenge for us as well as for authorities as well.

- **Mostly Educated People are Involved :**

  Committing a cybercrime is not a cup of tea for every individual. The person who commits cybercrime is a very technical person so he knows how to commit the crime and not get caught by the authorities.

- **No Harsh Punishment :**

  In Cybercrime there is no harsh punishment in every cases. But there is harsh punishment in some cases like when somebody commits cyber terrorism in that case there is harsh punishment

for that individual. But in other cases, there is no harsh punishment so this factor also gives encouragement to that person who commits cybercrime.

- **Fragmented and complex regulations :**

  Different countries, and jurisdiction may have different rules regulations and provisions in regard cybercrime.

- **No procedural rules :**

  There are no separate rules of procedure for investigating cybercrime or computer crime. Electronic evidence is very different from traditional criminal evidence, so it is essential to establish standardized and consistent procedures for handling electronic evidence.

- **Shortage of technical staff :**

  There are minimal efforts by states to recruit technical personnel to investigate cybercrime. A regular police officer with a background in humanities and business administration may not understand the nuances of how computers and the Internet work.

  Additionally, the Information Technology (IT) Act of 2000 maintains that offences registered under the Act should be investigated by police officers, not below the rank of inspector. In practice, the number of police inspectors in the district is limited and most field investigations are conducted by deputy inspectors.

- **Lack of Infrastructure – Cyber labs :**

  State cyber forensics labs need to be upgraded as new technologies emerge. Cryptocurrency-related crime continues to be underreported due to the limited ability to solve such crimes. Most government cyber labs are well equipped to analyse hard drives and mobile phones, but many still employ "electronic evidence examiners" so they can provide an expert opinion on electronic records.

3.3.2 Prevention of Cyber Crime :

While it isn't possible to completely eradicate cybercrime and ensure complete internet security, businesses can reduce their exposure to it by maintaining an effective cybersecurity strategy using a defence in depth to securing systems, networks and data. Thus, to deal with cybercrime is very difficult but fortunately, there are many effective ways of preventing cybercrime, including:

- **Use Strong Passwords**

  For each account, keep a unique username and password combination; avoid writing them down. Complex passwords—those with a mix of letters, numbers, and special characters—are more difficult to crack than weak ones because weak passwords can be easily cracked using techniques like Brute force attacks and Rainbow Table attacks.

- **Use reliable antivirus software**

  For both personal computers and mobile devices, make sure to always utilize cutting-edge, reliable antivirus software. As a result, several virus attacks on devices are avoided.

- **Maintain privacy on social media**

  Make sure that only your friends have access to the data on your social media accounts. Additionally, be sure to limit your friend-making to people you know.

- **Always use updated software**

  Use the software on your device whenever you receive updates. This is because outdated versions of the program might occasionally be readily exploited.

- **Avoid Public Network / Use a secure network**

  Public Wi-Fi is not secure. Refrain from executing business or financial transactions over these networks.

- **Avoid opening attachments from scam emails**

  These can lead to malware infections and other types of online fraud on your machine. Never open an attachment that someone you do not know sent you.

- **Use updated operating systems**

  When it comes to internet security, software and operating systems should be updated frequently. This might become dangerous if hackers take advantage of holes in the system.

- **Use of Firewalls**

  Firewalls can control incoming and outgoing traffic on a computer network, blocking external threats from entering.

- **Use of Antivirus software**

  Antivirus software can detect, quarantine, and remove malicious and suspicious applications.

- **Intrusion detection and intrusion prevention systems (IDS/IPS)** monitor network traffic and system logs to identify and respond to potential threats.

Finally, organizations can hire dedicated cyber security professionals such as Computer hacking and forensics investigators, Ethical Hackers, Penetration testing professionals, Network security professionals, Incident responders and Cyber security technicians

3.4 CYBER LAW

3.4.1 The Information Technology ACT, 2000

The Indian IT Act 2000, also known as the Information Technology Act, 2000, is a legislation passed by the Indian government to provide legal recognition and guidelines for electronic transactions, digital signatures, cybersecurity, and the regulation of cyberspace in India. The Act was enacted to address emerging challenges and issues in the digital realm and to establish legal frameworks for electronic commerce, digital communication, and data protection.

Key provisions of the Indian IT Act 2000 include :

1. **Legal Recognition of Electronic Records :** The Act recognizes electronic records and digital signatures as legally valid and equivalent to their paper-based counterparts. This enables the use of electronic documents in legal proceedings.

2. **Offenses and Penalties :** The Act identifies various cyber offenses and prescribes penalties for activities such as unauthorized access to computers, data theft, hacking, identity theft, and spreading of computer viruses. It also covers offenses related to obscenity, pornography, and the protection of children online.

3. **Cybercrime Investigation and Law Enforcement :** The Act grants powers to law enforcement agencies to investigate and prevent cybercrimes. It outlines procedures for the collection and preservation of digital evidence and enables authorities to request assistance from service providers and intermediaries.

4. **Digital Signatures :** The Act recognizes and regulates the use of digital signatures, which serve as a secure method for verifying the authenticity and integrity of electronic records and transactions.

5. **Data Protection and Privacy :** The Act includes provisions related to the protection and privacy of personal data. It outlines guidelines for the collection, storage, and use of personal information by individuals and entities.

6. **Cyber Appellate Tribunal :** The Act established the Cyber Appellate Tribunal (CAT), which serves as an appellate authority for adjudicating appeals against orders issued by the Controller of Certifying Authorities and Adjudicating Officers under the Act.

7. **Network Service Providers' Liability :** The Act includes provisions related to the liability of network service providers, intermediaries, and internet companies for content hosted on their platforms. It provides certain exemptions to intermediaries for content posted by users but also requires them to comply with due diligence and take down objectionable content upon notification.

3.4.2 The Information Technology ACT, 2008

(Ref: https://www.indiacode.nic.in/bitstream/123456789/15983/1/the_information_technology_act%2c_2008.pdf)

The Indian IT Act 2000 has undergone amendments over the years to address emerging challenges in cyberspace, including the introduction of the Information Technology (Amendment) Act, 2008, which expanded the scope of cyber offenses and introduced additional provisions related to data protection and privacy.

Some of them amendments which expanded the scope of cyber offences are as under :

Section 65 : Tampering with Computer Source Documents

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme,

computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation - For the purposes of this section, "Computer Source Code" means the listing of programmes, Computer Commands, Design and layout and programme analysis of computer resource in any form.

Section 66 : Computer Related Offences (Substituted vide ITAA 2008)

If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to two **three** years or with fine which may extend to five lakh rupees or with both.

Explanation : For the purpose of this section, -

(a) the word "dishonestly" shall have the meaning assigned to it in section 24 of the Indian Penal Code;

(b) the word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code.

66 A. Punishment for sending offensive messages through communication service, etc.

(Introduced vide ITAA 2008)

Any person who sends, by means of a computer resource or a communication device,

(a) any **information** that is grossly offensive or has menacing character; or

(b) any **information** which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes **by making** use of such computer resource or a communication device,

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages (Inserted vide ITAA 2008)

shall be punishable with imprisonment for a term which may extend to two **three** years and with fine.

Explanation : For the purposes of this section, terms "Electronic mail" and "Electronic Mail Message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

66 B. Punishment for dishonestly receiving stolen computer resource or communication device (Inserted Vide ITA 2008)

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

66 C. Punishment for identity theft. (Inserted Vide ITA 2008)

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

66 D. Punishment for cheating by personation by using computer resource (Inserted Vide ITA 2008)

Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

66 E. Punishment for violation of privacy. (Inserted Vide ITA 2008)

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both

Explanation. - For the purposes of this section –

(a) "transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons;

(b) "capture", with respect to an image, means to videotape, photograph, film or record by any means;

(c) "Private area" means the naked or undergarment clad genitals, pubic area, buttocks or female breast;

(d) "publishes" means reproduction in the printed or electronic form and making it available for public;

(e) "Under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that —

(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

(ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

66 F. Punishment for cyber terrorism

(1) Whoever, -

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

(i) denying or cause the denial of access to any person authorized to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or

(iii) introducing or causing to introduce any Computer Contaminant. and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life'.

Section 67. Punishment for publishing or transmitting obscene material in electronic form (Amended vide ITAA 2008)

Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to **two three** years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to **five** years and also with fine which may extend to ten lakh rupees.

67A. Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form (Inserted vide ITAA 2008)

Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to **five** years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to **seven years** and also with fine which may extend to ten lakh rupees.

Exception : This section and section 67 does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-

(i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, representation or figure is in the interest of science, literature, art, or learning or other objects of general concern; or

(ii) which is kept or used bona fide for religious purposes.

67B. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form.

Whoever, -

(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or

(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or

(d) facilitates abusing children online or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees :

Provided that the provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form -

(i) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or

(ii) which is kept or used for bonafide heritage or religious purposes

Explanation : For the purposes of this section, "children" means a person who has not completed the age of 18 years.

67C. Preservation and Retention of information by intermediaries

(1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.

(2) Any intermediary who intentionally or knowingly contravenes the provisions of sub section (1) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

Self - Assessment

Q. 1 Answer the below short questions :

(1) What is Cyber Crime? List out two notable cases.

(2) Define the terms: Cybercrime, Cybercriminal.

(3) Differentiate: Hackers V/s Cybercriminals

(4) List out types of cybercrime in terms of Organizational classification.

(5) List out types of cybercrime in terms of Individual based classification.

(6) List out types of cybercrime in terms of Property classification.

(7) What is Salami Attack? List out various Salami Attacks.

(8) What is logic bomb? Why it is called time bomb?

(9) Define the terms : Web Jacking, Data Diddling, DOS Attack, DDOS Attack.

(10) Define the terms : Cyber bullying, Phishing, Spyware, E mail Spoofing.

(11) What is Cyber terrorism?

(12) List out any four challenges in cybercrime.

Q. 2 Explain the below questions:

(1) What is Cybercrime? Explain in detail with defining cybercrime and cybercriminals.

(2) Explain various types cybercrime under Organizational classification.

(3) Explain various types cybercrime under Individual classification.

(4) Explain various types cybercrime under Property classification.

(5) Explain e mail bombing in detail.

(6) Explain Web jacking in detail.

(7) Explain Salami attack in detail.

(8) Explain DOS Attack and DDOS attack. Also differentiate them.

(9) Explain Social based Classified Cybercrime in detail.

(10) Explain Section 65 in brief.

(11) Explain various challenges of Cyber Crime.

***

Chapter 4

ETHICAL HACKING

4.1 CONCEPT OF HACKING AND TYPES OF HACKERS

- INTRODUCTION - HACKING
- TYPES OF HACKING
- TYPES OF HACKERS

4.2 BASICS OF ETHICAL HACKING

- WHAT IS ETHICAL HACKING?
- WHY ETHICAL HACKING?

4.3 HACKING TERMINOLOGIES

- BASIC HACKING TERMINOLOGIES
- VULNERABILITY, EXPLOIT, 0-DAY

4.4 STEPS OF HACKING PROCESS

- SECURE SOCKET LAYER
- TRANSPORT LAYER SECURITY

4.5 INFORMATION GATHERING

- INTRODUCTION - RECONNAISSANCE
- ACTIVE RECONNAISSANCE
- PASSIVE RECONNAISSANCE

4.6 INTRODUCTION TO KALI LINUX OPERATING SYSTEM

- INTRODUCTION – KALI LINUX OS
- INSTALLATION AND CONFIGURATION OF KALI LINUX OS
- BASIC COMMANDS IN KALI LINUX
- VULNERABILITY SCANNING
- VULNERABILITY BASED HACKING

4.7 PORT SCANNING

- WHAT IS PORT SCANNING?
- PORT SCANNING TECHNIQUES

4.8 REMOTE ADMINISTRATION TOOL (RAT)

- INTRODUCTION – REMOTE ADMINISTRATION TOOLS (RAT)
- HOW TO USE RAT TOOLS?

4.9 PROTECT SYSTEM FROM RAT

4.10 SNIFFING AND MECHANISM OF SNIFFING

- INTRODUCTION - SNIFFING
- TYPES OF SNIFFING
- SESSION HIJACKING

o **Self - Assessment**

4.1 CONCEPT OF HACKING AND TYPES OF HACKERS

4.1.1 Introduction

There are various definitions of the hackers in the literature of computer world. The first known event of hacking had taken place in 1960 at MIT and at the same time, the term "Hacker" was originated. Originally the term was used to describe someone who could be a great programmer and had the ability to solve complex problems.

But now a days the term hacker refers as someone who finds loopholes and tries to gain access into the system to steal information that could be important for the victims. This is the negative aspect, but there is also a positive aspect. The positive aspect is that hackers are the people who exposes the vulnerabilities in the system and by this way protects organizations and multiple users.

Thus, ***"Hacking is an activity done to gain unauthorized access to a computer system or a computer network, either to harm the systems or to steal sensitive information available on the computer."***

The computer experts who do the activity of hacking are known as **hackers.**

4.1.2 Types of Hacking

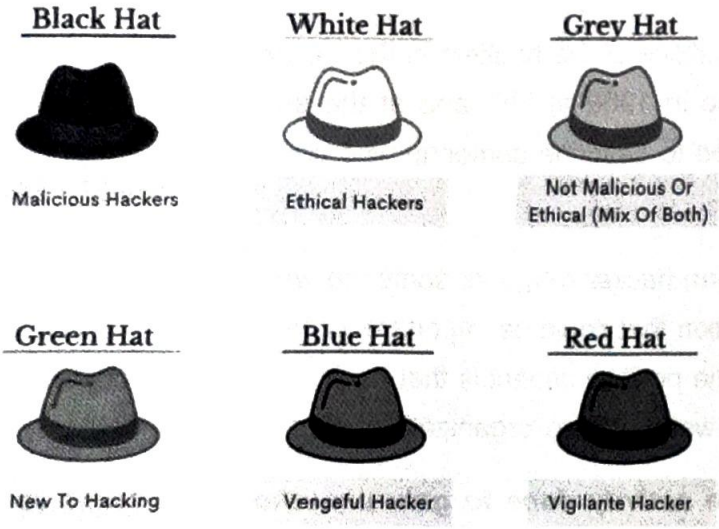
We can classify hacking into different categories, based on what is being hacked. These categories are as under:

- **Password Hacking** – This is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.
- **Computer Hacking** – This is the process of stealing login credentials of computer system like login ID and password by applying different hacking methods and getting unauthorized access to a computer system.

- **Network Hacking** – The word Network hacking refers to the gathering of information about a computer network by using network management and administration tools like Telnet, NS lookup, Ping, Tracert, Netstat, etc. using this information take the control over network with the intent to harm the network system and hamper its operation.
- **Website Hacking** – Hacking a website means taking unauthorized control over a web server and its associated software such as databases and other interfaces.
- **Email Hacking** – It includes getting unauthorized access on an Email account and using it without taking the consent of its owner. It may be also used to get other financial aids.
- **Ethical Hacking** – Ethical hacking involves finding weaknesses in a computer or network system for testing purpose and finally getting them fixed.

4.1.3 Types of Hackers

Based on their intent of hacking a system, Hackers can be classified into different categories such as white hat, black hat, and grey hat hackers.



[Fig. 4.1 : Types of Hackers – Based on Intent]

- **Whites hat Hackers**

White hat hackers (sometimes also called ethical hackers). They employ their technical expertise to defend the planet against malicious hackers. They never intent to harm a system, rather they try to find out weaknesses in a computer or a network system as a part of penetration testing and vulnerability assessments.

Ethical hacking is not illegal and it is one of the demanding jobs available in the IT industry. There are numerous companies that hire ethical hackers for penetration testing and vulnerability assessments.

White hats are employed by businesses and government agencies as data security analysts, researchers, security specialists, etc. White hat hackers, with the permission of the system owner and with good motives, use the same hacking tactics that the black hackers use.

Black hat Hackers

They are also known as crackers and always have a malicious motive and gain illegal access to computer system, networks and websites. The main goal of black hat hackers is getting financial gain like money loundering by stealing secret organizational data, stealing funds from online bank accounts, violating privacy rights, damaging the system, blocking network communication etc. In today's world, the majority of hackers fall into this category.

Grey hat Hackers

Grey hat hackers are combined concept of both black hat and white hat hackers. They act without malicious intent but for their fun, they exploit a security weakness in a computer system or network without the owner's permission or knowledge.

Their intent is to bring the weakness to the attention of the owners and getting appreciation or a little bounty from the owners.

Apart from the above well-known categories of hackers, we have the following categories of hackers based on what they hack and how they hack.

1. **Red Hat Hackers**

   Red hat hackers are again a blend of both black hat and white hat hackers. They are usually on the level of hacking government agencies, top-secret information hubs, and generally anything that falls under the category of sensitive information.

2. **Blue Hat Hackers**

   A blue hat hacker is someone outside computer security consulting firms who is used to bug-test a system prior to its launch. They look for loopholes that can be exploited and try to close these gaps. Microsoft also uses the term Blue Hat to represent a series of security briefing events.

3. **Elite Hackers**

   This is a social status among hackers, which is used to describe the most skilled. Newly discovered exploits will circulate among these hackers.

4. **Script Kiddie**

   A script kiddie is a non-expert who breaks into computer systems by using pre-packaged automated tools written by others, usually with little understanding of the underlying concept, hence the term **Kiddie**.

5. **Neophyte**

   A neophyte, "n00b", or "newbie" or "Green Hat Hacker" is someone who is new to hacking or phreaking and has almost no knowledge or experience of the workings of technology and hacking.

6. **Hacktivist**

A hacktivist is a hacker who utilizes technology to announce a social, ideological, religious, or political message. In general, most hacktivism involves website defacement or denial of-service attacks.

4.2 BASICS OF ETHICAL HACKING

4.2.1 What is Ethical Hacking?

Ethical Hacking is about identifying weakness in computer systems and/or computer networks and coming with countermeasures that protect the weaknesses. Ethical hackers must abide by the following rules.

- Get written permission from the owner of the computer system and/or computer network before hacking.
- Protect the privacy of the organization been hacked.
- Transparently report all the identified weaknesses in the computer system to the organization.
- Inform hardware and software vendors of the identified weaknesses.

4.2.2 Why Ethical Hacking ?

- Information is one of the most valuable assets of an organization. Keeping information secure can protect an organization's image and save an organization a lot of money.
- Fake hacking can lead to loss of business for organizations that deal in finance such as PayPal. Ethical hacking puts them a step ahead of the cyber criminals who would otherwise lead to loss of business.
- Hacking is identifying and exploiting weaknesses in computer systems and/or computer networks.
- Cybercrime is committing a crime with the aid of computers and information technology infrastructure.
- Ethical Hacking is about improving the security of computer systems and/or computer networks.
- Ethical Hacking is legal.

4.3 TERMINOLOGIES USED IN ETHICAL HACKING

4.3.1 Basic Hacking Terminologies

- **Adware** – Adware is software designed to force pre-chosen ads to display on your system.
- **Attack** – An attack is an action that is done on a system to get its access and extract sensitive data.

- **Back door** – A back door, or trap door, is a hidden entry to a computing device or software that bypasses security measures, such as logins and password protections.
- **Bot** – A bot is a program that automates an action so that it can be done repeatedly at a much higher rate for a more sustained period than a human operator could do it. For example, sending HTTP, FTP or Telnet at a higher rate or calling script to create objects at a higher rate.
- **Botnet** – A botnet, also known as zombie army, is a group of computers controlled without their owners' knowledge. Botnets are used to send spam or make denial of service attacks.
- **Brute force attack** – A brute force attack is an automated and the simplest kind of method to gain access to a system or website. It tries different combination of usernames and passwords, over and over again, until it gets in.
- **Buffer Overflow** – Buffer Overflow is a flaw that occurs when more data is written to a block of memory, or buffer, than the buffer is allocated to hold.
- **Clone phishing** – Clone phishing is the modification of an existing, legitimate email with a false link to trick the recipient into providing personal information.
- **Cracker** – A cracker is one who modifies the software to access the features which are considered undesirable by the person cracking the software, especially copy protection features.
- **Denial of service attack (DoS)** – A denial of service (DoS) attack is a malicious attempt to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet.
- **DDoS** – Distributed denial of service attack. In these types of attack instead of using single computer system for attack, an attacker uses multiple computer systems for attack. So, this kind of attack is more difficult to detect than simple DOS attack.
- **Firewall** – A firewall is a filter designed to keep unwanted intruders outside a computer system or network while allowing safe communication between systems and users on the inside of the firewall.
- **Keystroke logging** – Keystroke logging is the process of tracking the keys which are pressed on a computer (and which touchscreen points are used). It is simply the map of a computer/ human interface. It is used by gray and black hat hackers to record login IDs and passwords. Keyloggers are usually secreted onto a device using a Trojan delivered by a phishing email.
- **Logic bomb** – A virus secreted into a system that triggers a malicious action when certain conditions are met. The most common version is the time bomb.
- **Master Program** – A master program is the program a black hat hacker uses to remotely transmit commands to infected zombie drones, normally to carry out Denial of Service attacks or spam attacks.

- **Phreaker** – Phreakers are considered the original computer hackers and they are those who break into the telephone network illegally, typically to make free long-distance phone calls or to tap phone lines.
- **Rootkit** – Rootkit is a stealthy type of software, typically malicious, designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer.
- **Shrink Wrap code** – A Shrink Wrap code attack is an act of exploiting holes in unpatched or poorly configured software.
- **Social engineering** – Social engineering implies deceiving someone with the purpose of acquiring sensitive and personal information, like credit card details or user names and passwords.
- **Spam** – A Spam is simply an unsolicited email, also known as junk email, sent to a large number of recipients without their consent.
- **Threat** – A threat is a possible danger that can exploit an existing bug or vulnerability to compromise the security of a computer or network system.
- **Spoofing** – Spoofing is a technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host.
- **Spyware** – Spyware is software that aims to gather information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge.
- **Cross-site Scripting** – Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side script into web pages viewed by other users.
- **Zombie Drone** – A Zombie Drone is defined as a hi-jacked computer that is being used anonymously as a soldier or 'drone' for malicious activity, for example, distributing unwanted spam e-mails.

4.3.2 Vulnerability, Exploit, 0 – Day

- **Vulnerability** – A vulnerability is a weakness which allows a hacker to compromise the security of a computer or network system.

These hackers can gain illegal access to the systems and cause severe damage to data privacy. Therefore, cybersecurity vulnerabilities are extremely important to monitor for the overall security posture as gaps in a network can result in a full-scale breach of systems in an organization.

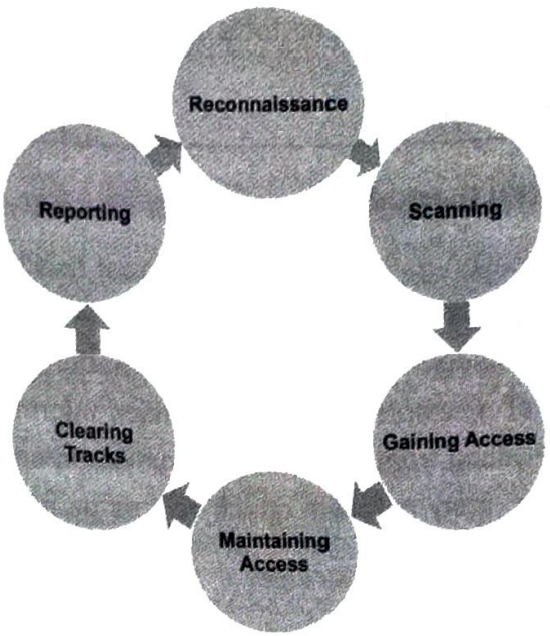
The common source point for vulnerabilities are Misconfigurations, Unsecured APIs, Outdated or Unpatched Software, Zero-day Vulnerabilities, Weak or Stolen User Credentials, Access Control or Unauthorized Access, etc....

- **Exploit** – Exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to compromise the security of a computer or network system.
- **Exploit Kit** – An exploit kit is software system designed to run on web servers, with the purpose of identifying software vulnerabilities in client machines communicating with it and exploiting discovered vulnerabilities to upload and execute malicious code on the client.
- **Zero-day Vulnerabilities** – A zero-day vulnerability refers to a security flaw that has been discovered by a threat actor but is unknown to the enterprise and software vendor. The term "zero-day" is used because the software vendor was unaware of their software vulnerability, and they've had "0" days to work on a security patch or an update to fix the issue; meanwhile it is a known vulnerability to the attacker.

  Zero-day attacks are extremely dangerous for companies because they can be very difficult to detect.

4.4 STEPS OF HACKING PROCESS

Ethical hacking process is carried out with the number of phases. It helps hackers to make a structured hacking attack. Ethical hacking process can be described in different way, but here the ethical hacking process is explained with six phases as depicted in the below figure 4.2.



[Fig. 4.2 : Six phases of Hacking Process]

- **Reconnaissance (Information Gathering)**

  This is the first phase of Hacking process. During this phase the attacker gathers information about a target using active or passive means. The tools that are widely used in this process are NMAP, Hping, Maltego, and Google Dorks.

- **Scanning**

  During the scanning phase, the attacker begins to actively probe a target machine or network for vulnerabilities that can be exploited. The tools used in this process are Nessus, Nexpose, and NMAP.

- **Gaining Access**

  This procedure finds the vulnerability, which you then try to leverage to get access to the system. Metasploit is the main tool utilized in this process.

- **Access Maintaining**

  It is the procedure by which a hacker has previously entered a system. Once inside, the hacker installs backdoors so that, should the necessity arise in the future, he may re-enter the system. The recommended tool for this process is Metasploit.

- **Clearing Tracks**

  In actuality, this procedure is unethical. The removal of all activity logs from the hacking process is the reason for it.

- **Reporting**

  The final step in the ethical hacking is reporting. Here, the ethical hacker gathers information about the work completed, including the tools used, success rate, vulnerabilities discovered, and exploit procedures, and reports it with his results.

  The above-described process is not a standard. Different people can use different approach. One can use a set of different processes and tools as he is comfortable with it.

4.5 INFORMATION GATHERING

4.5.1 Introduction - Reconnaissance

Reconnaissance is the information-gathering stage of ethical hacking, where you collect data about the target system. Reconnaissance is a set of processes and techniques (Footprinting, Scanning & Enumeration) used to covertly discover and collect information about a target system. During reconnaissance, an ethical hacker attempts to gather as much information about a target system as possible. This data can include anything from network infrastructure to employee contact details. The goal of reconnaissance is to identify as many potential attack vectors as possible.

Data collected from reconnaissance may include:

- **Security policies**. Knowing an organization's security policies can help you find weaknesses in their system.
- **Network infrastructure**. A hacker needs to know what type of network the target is using (e.g., LAN, WAN, MAN), as well as the IP address range and subnet mask.
- **Employee contact details**. Email addresses, phone numbers, and social media accounts can be used to launch social engineering attacks.
- **Host information**. Information about specific hosts, such as operating system type and version, can be used to find vulnerabilities.

The reconnaissance process is generally caried out with below steps:

- Gather initial information
- Determine the network range
- Identify active machines
- Discover open ports and access points
- Fingerprint the operating system
- Uncover services on ports
- Map the network

Reconnaissance takes place in two ways: Active Reconnaissance and Passive Reconnaissance

4.5.2 Active Reconnaissance

During this procedure, you will be interacting directly with the targeted computer system in order to obtain information. The data collected with this approach may be accurate and pertinent. However, if you are planning active reconnaissance without authorization, you run the danger of being discovered. The system administrator may take harsh measures against you and monitor your future actions if they find you.

4.5.3 Passive Reconnaissance

During this procedure, you won't be interacting directly (physically linked) to the target computer system in order to collect information from it. By using this method, vital data is gathered without ever having to communicate with the target systems.

4.6 INTRODUCTION TO KALI LINUX OPERATING SYSTEM

4.6.1 Introduction – Kali Linux OS

For the flawless working of a computer, the main responsible system software is an Operating System. Any operating system could be used for any task as we wish, but all they have some special tools or services available for its users which makes them a good OS for the specific purpose. E.g. Windows operating system for office work and gaming, mac OS for designing related purposes as most of the designing software are available with mac OS. In the same way, the Kali Linux is an OS for Network Security, Digital Forensics, Penetration testing, or Ethical Hacking.

Kali Linux is a Debian-derived Linux distribution that is maintained by Offensive Security. Kali Linux is a specially designed OS for network analysts, Penetration testers, or in simple words, it is for cybersecurity and network analysis. The official website of Kali Linux is Kali.org. It was not designed to use it as general-purpose operating system, but it is for the professionals or the people who know how to operate Linux/Kali.

Advantages :

- It has 600+ Penetration testing and network security tools pre-installed.
- It is completely free and open source. So, you can use it for free and even contribute for its development.
- It supports many languages.
- Great for those who are familiar with Linux and Linux commands.
- Could be easily used with Raspberry Pi.

Disadvantages :

- It is not recommended for those who are new to Linux and want to learn Linux.
- It is a bit slower.
- Some software may malfunction.

Many people think that Kali is a tool for hacking or cracking. This is one of the biggest myths about Kali Linux. Kali Linux is just another Debian distribution with a bunch of networking and security tools which is used as a weapon to train or defend yourself not to attack anyone. It is a powerful tool and in case, not used properly, it may lead to losses even.

Kali Linux is an operating system for the professional penetration testers, cybersecurity experts, ethical hackers, or those who know how to operate it. In simple words, if you know how to use Linux and its terminal commands, architecture, system, and file management then Kali Linux is also for you.

4.6.2 Installation and Configuration of Kali Linux OS

Installing Kali Linux (single boot) on your computer is an easy process. In our example, we will be installing Kali Linux in a fresh guest VM, without any existing operating systems pre-installed.

System Requirements

The system requirements for installing Kali Linux may vary depending on what you would like to install and your setup.

- Kali Linux as a basic Secure Shell (SSH) server with no desktop,

  128 MB of RAM (512 MB recommended) and 2 GB of disk space.
- Install the default Xfce4 desktop and the kali-Linux-default **metapackage**,

  at least 2 GB of RAM and **20 GB of disk space**.
- When using resource-intensive applications, such as Burp Suite,

  At least **8 GB of RAM** (and even more for a large web application!).

Installation Prerequisites

This guide will make also the following assumptions when installing Kali Linux:

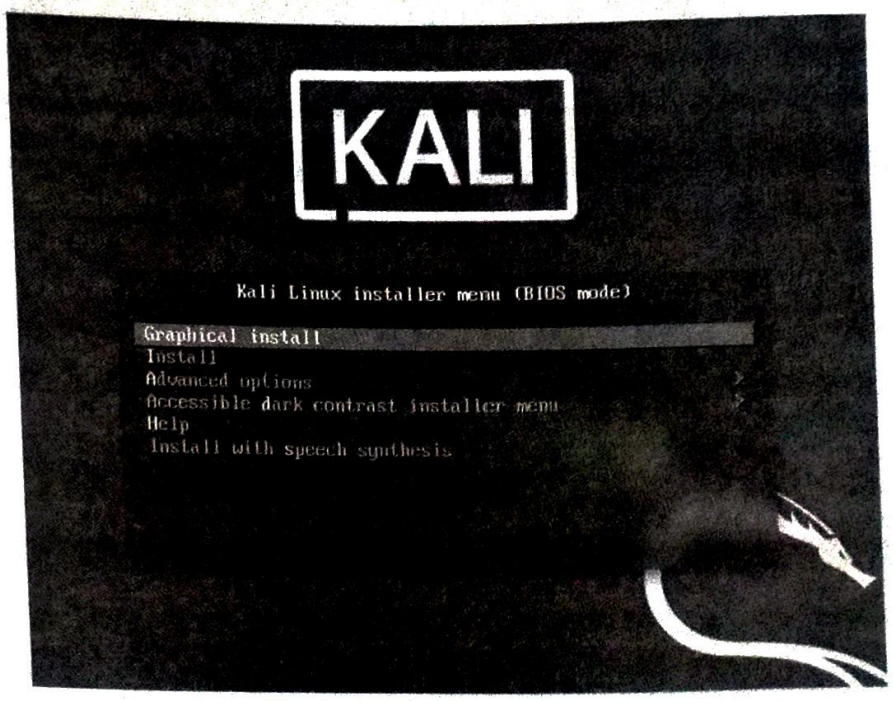
- Using the amd64 installer image.
- CD/DVD drive / USB boot support.
- Single disk to install to.
- Connected to a network (with DHCP & DNS enabled) which has outbound Internet access.

Preparing for the Installation

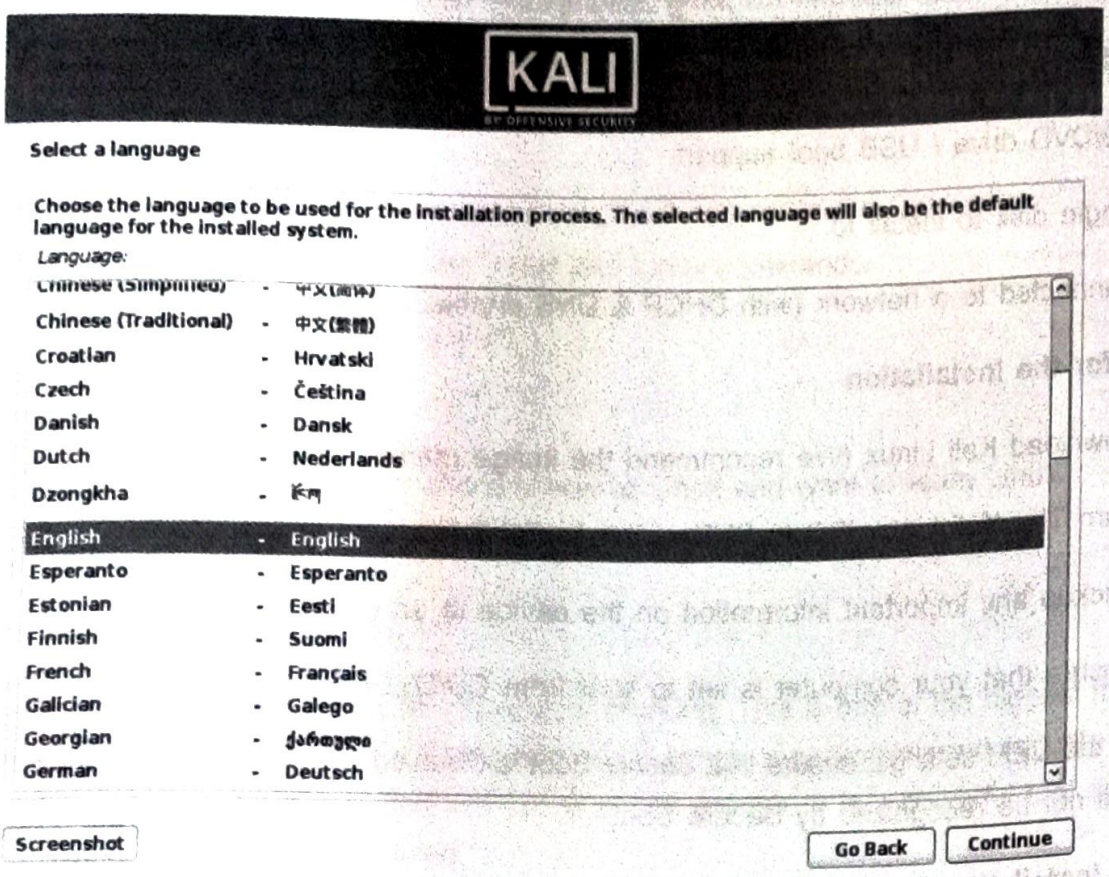
- Download Kali Linux (We recommend the image marked Installer).
- Burn The Kali Linux ISO to DVD or image Kali Linux Live to USB drive.
- Backup any important information on the device to an external media.
- Ensure that your computer is set to boot from CD/DVD/USB in your BIOS/UEFI.
- In the UEFI settings, ensure that Secure Boot is disabled. The Kali Linux kernel is not signed and will not be recognized by Secure Boot.

Kali Linux Installation Procedure

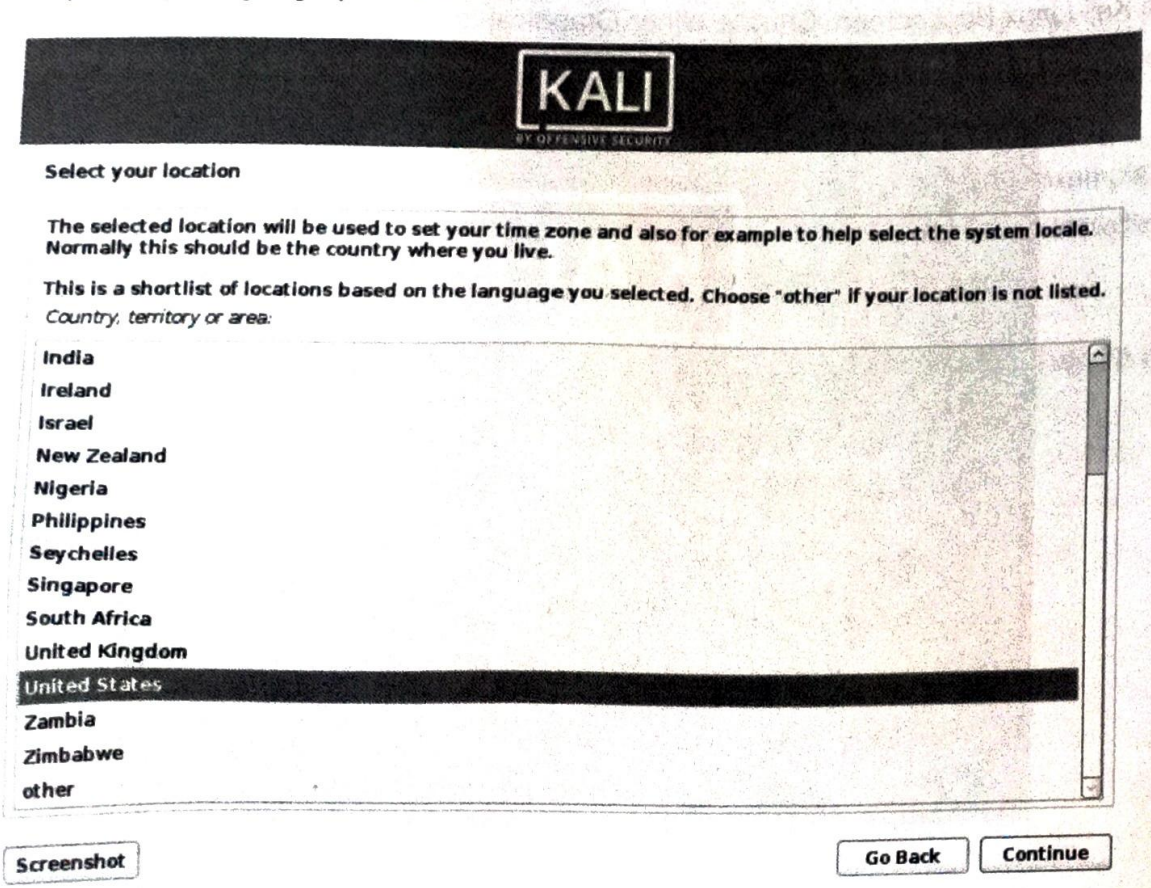
Step 1. To start your installation, boot with your chosen installation medium. You should be greeted with the Kali Linux Boot screen. Choose either Graphical install or Install (Text-Mode). In this example, we chose the Graphical install.



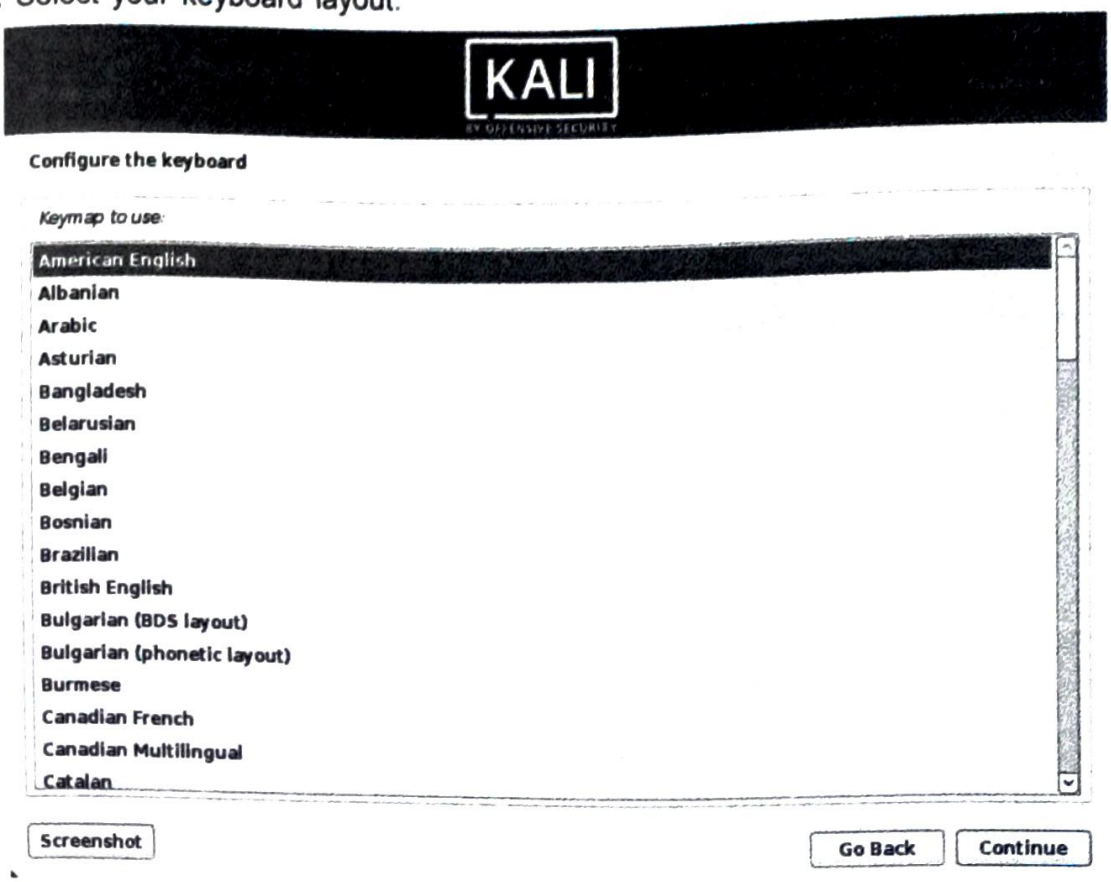
Step 2. Select your preferred language. This will be used for both the setup process and once you are using Kali Linux.



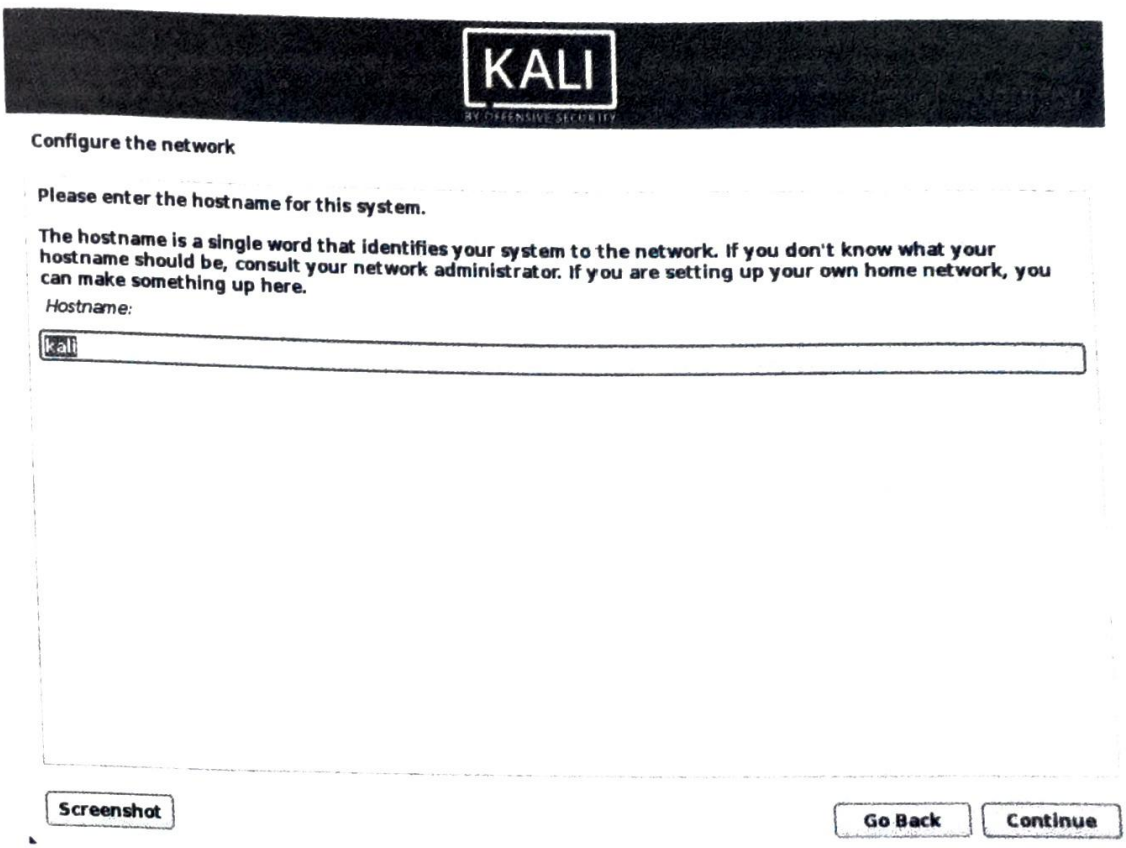
Step 3. Specify your geographic location.



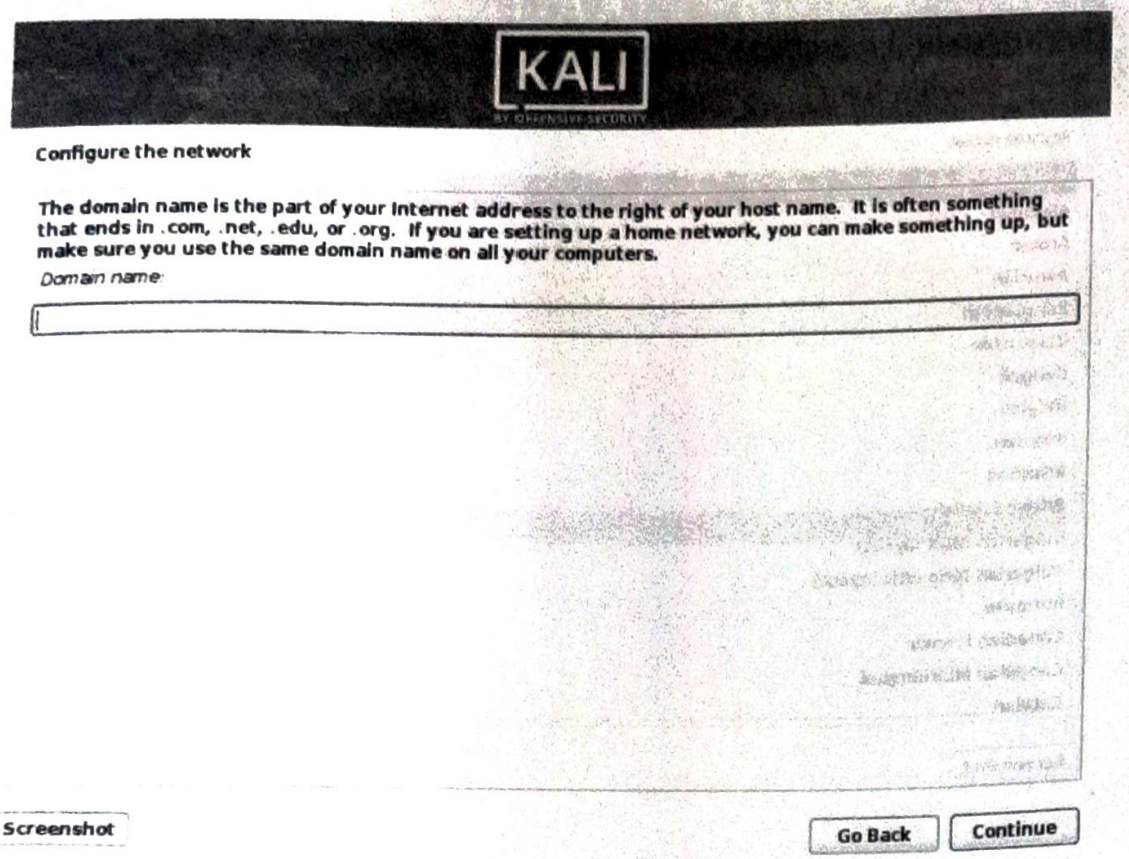
Step 4. Select your keyboard layout.



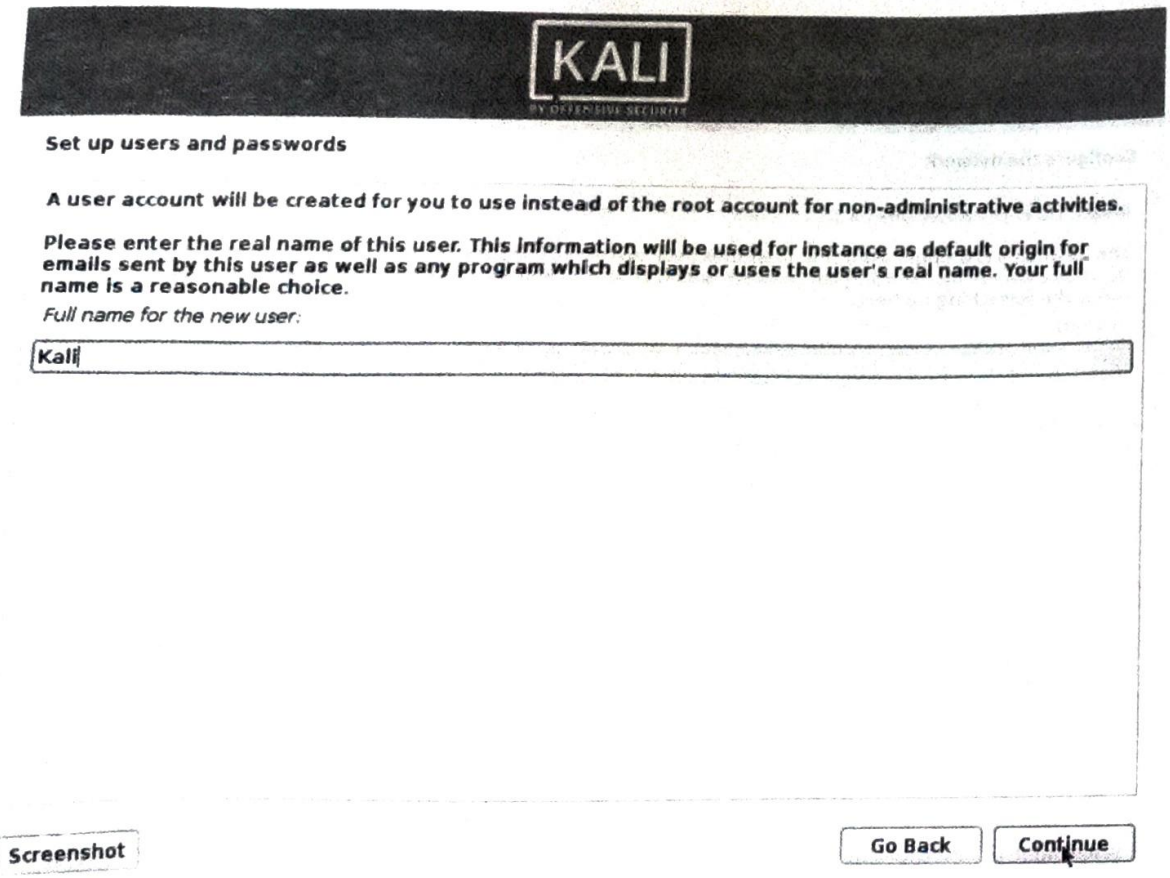
Step 5. The setup will now probe your network interfaces, looks for a DHCP service, and then prompt you to enter a hostname for your system. In the example below, we've entered **kali** as our hostname.

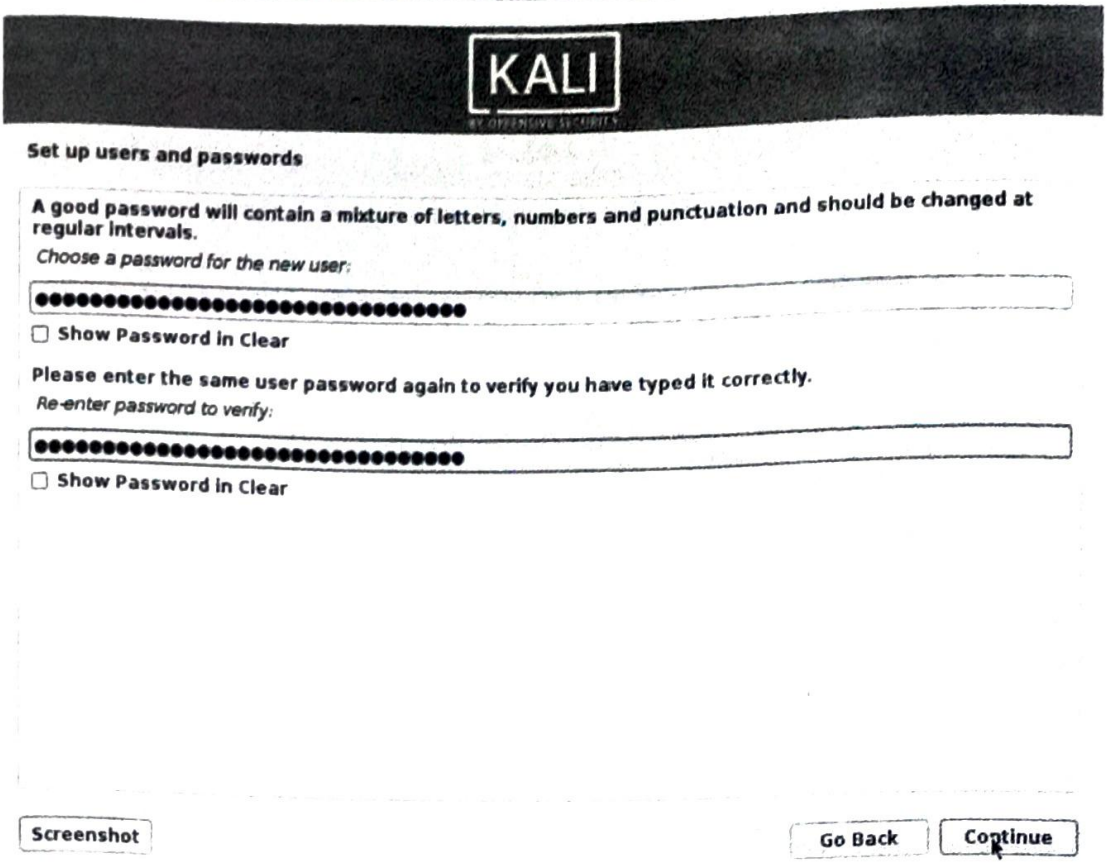


Step 6. You may optionally provide a default domain name for this system. (values may be pulled from DHCP or if there is pre-existing operating systems). select your keyboard layout.

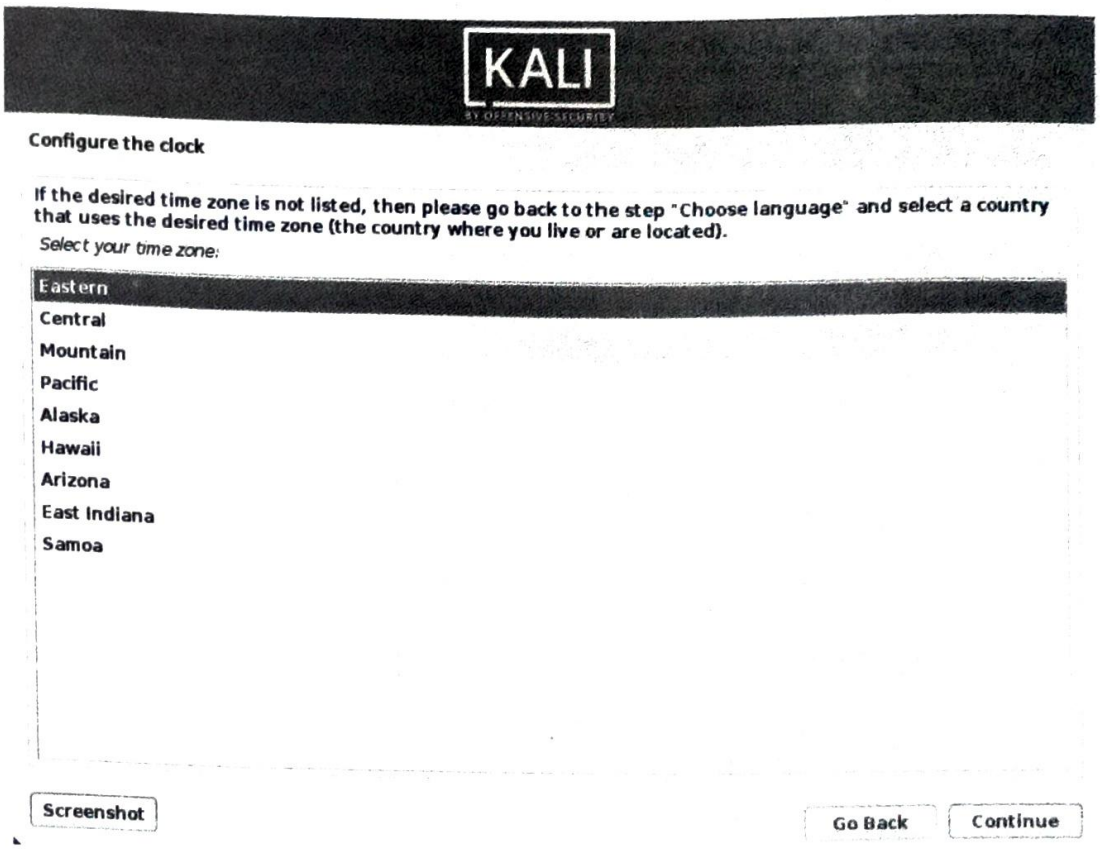


Step 7. Next, create the user account for the system (Full name, username and a password).

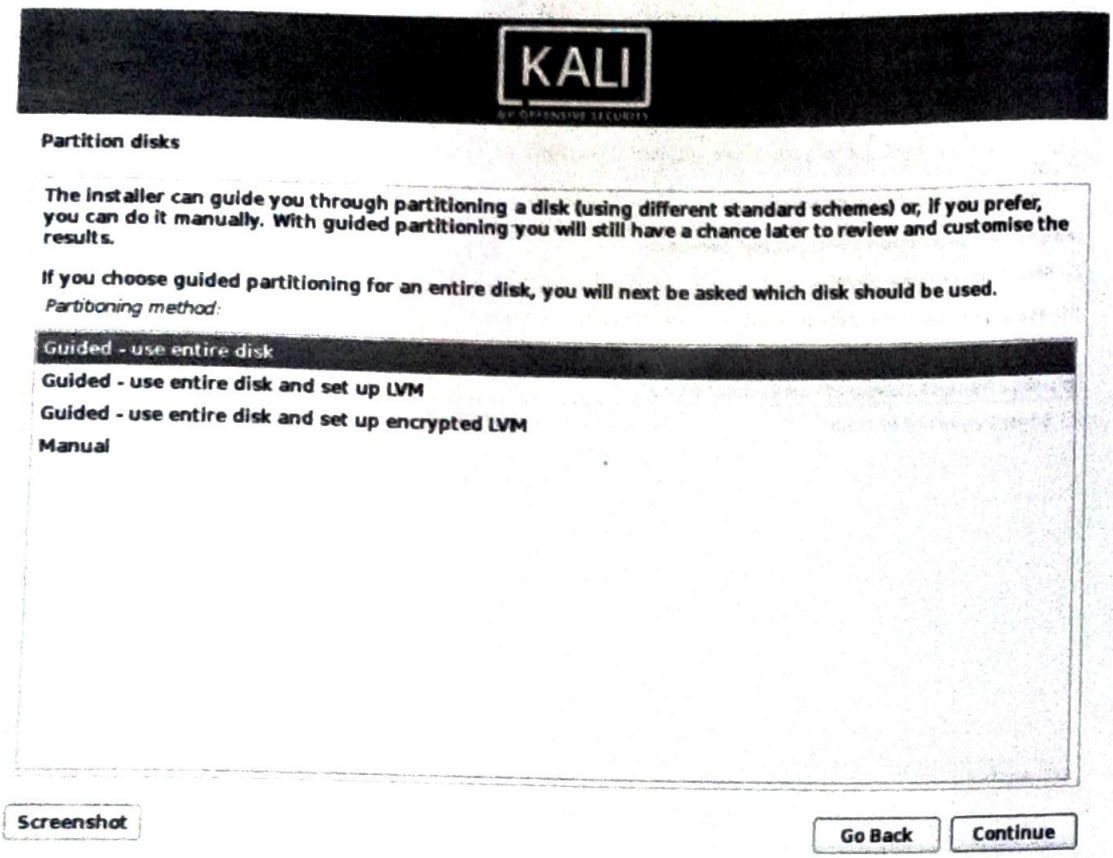




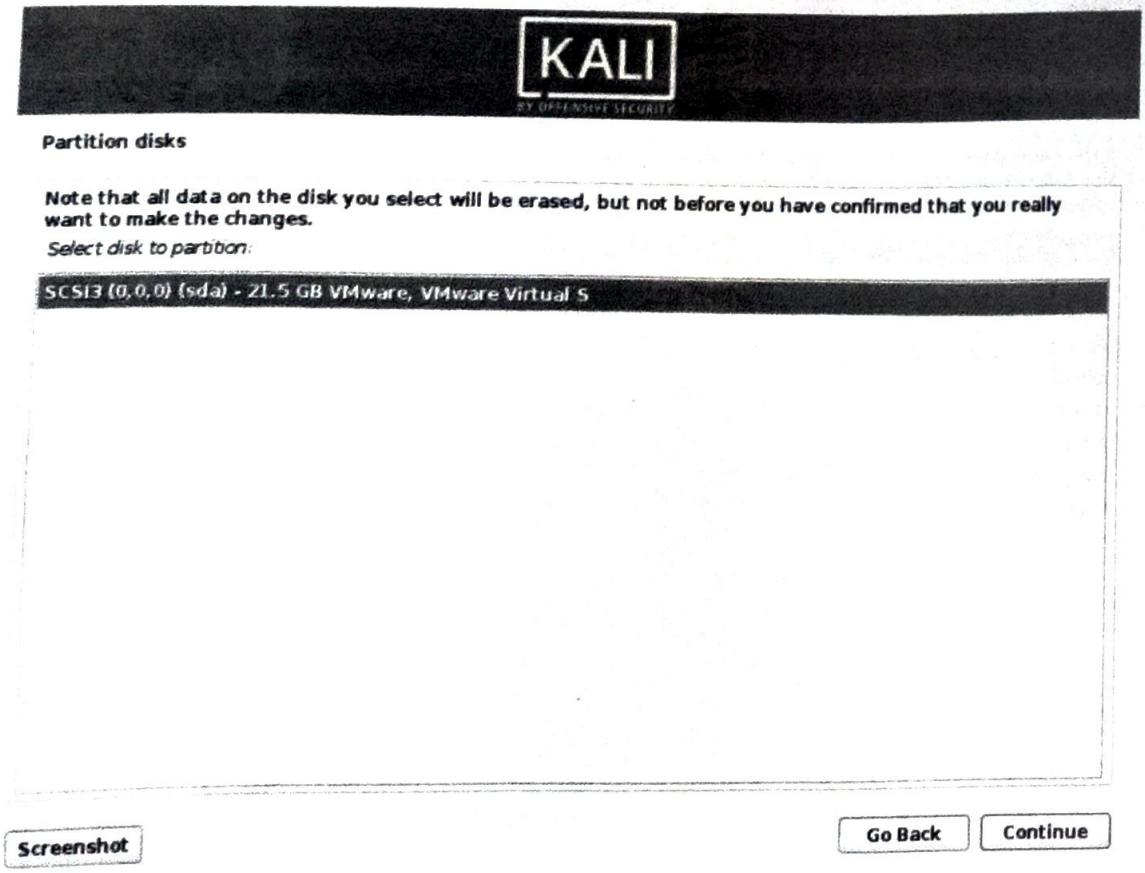
Step 8. Next, set your time zone.



Step 9. The installer will now probe your disks & offer you choices, depending on the setup.

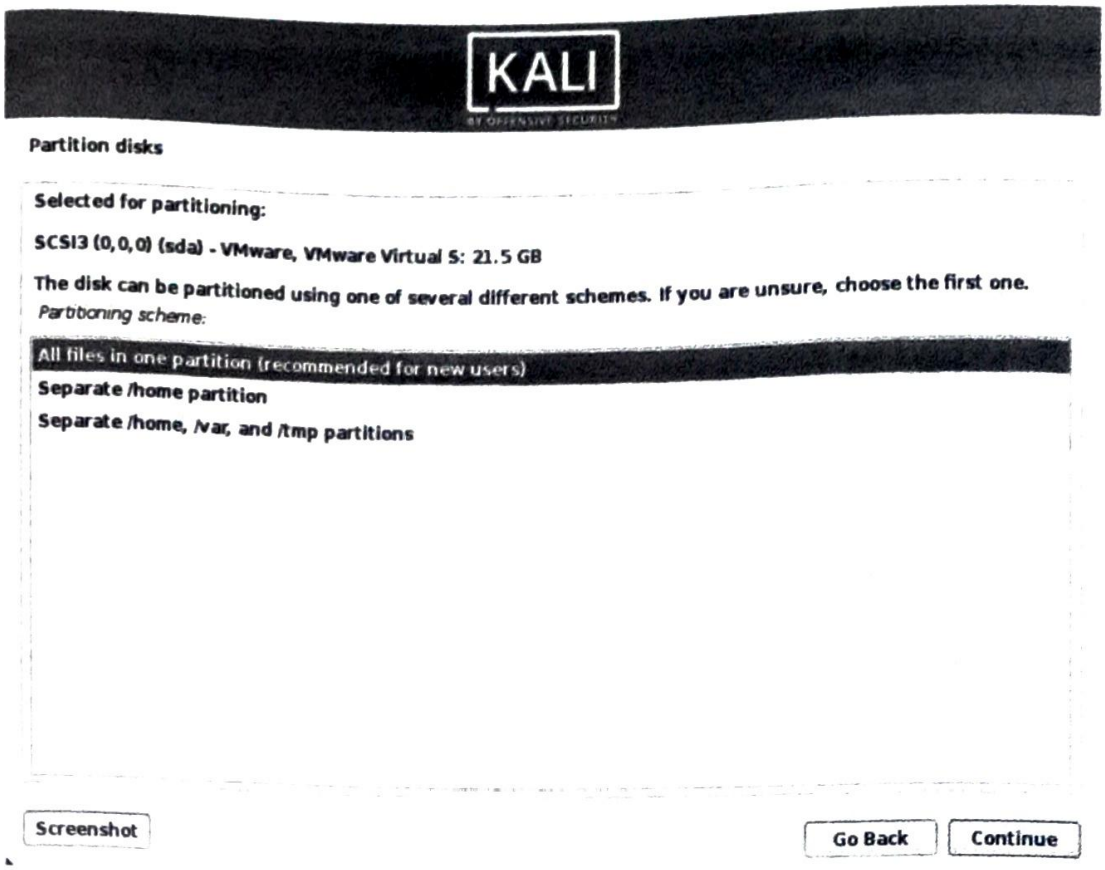


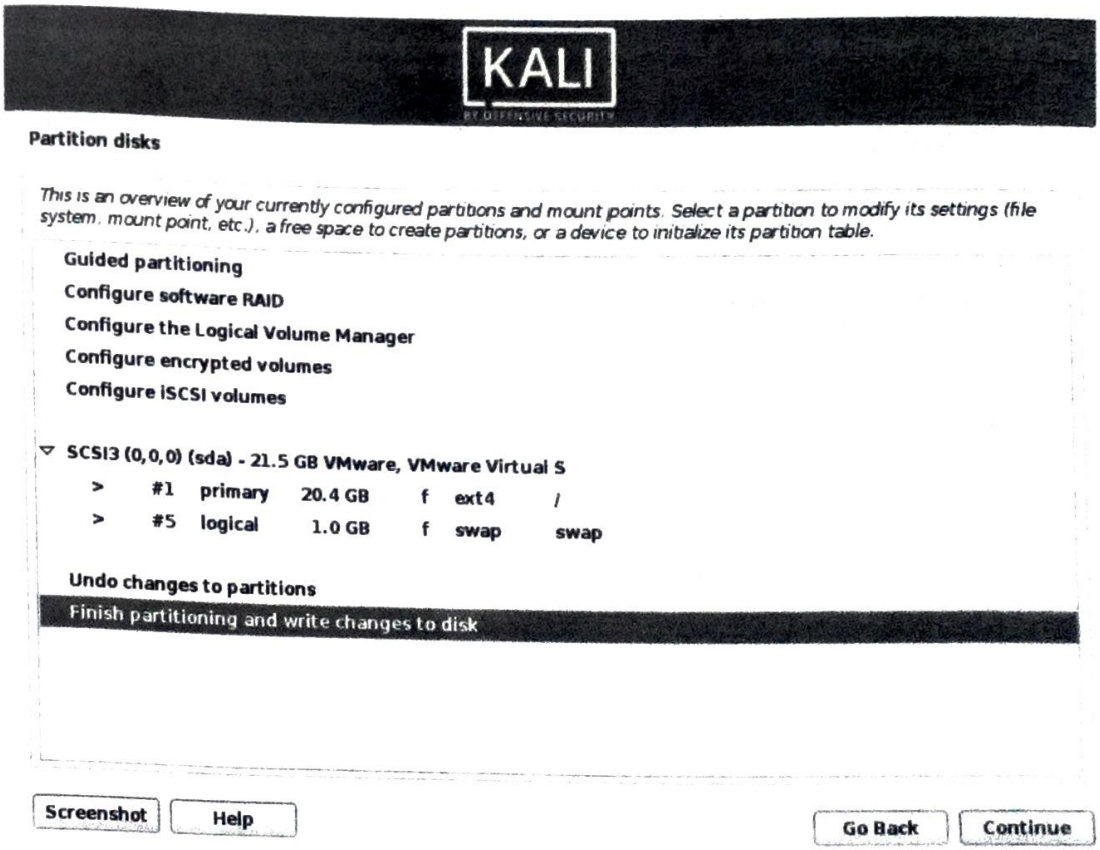
Step 10. Select the disk to be partitioned.



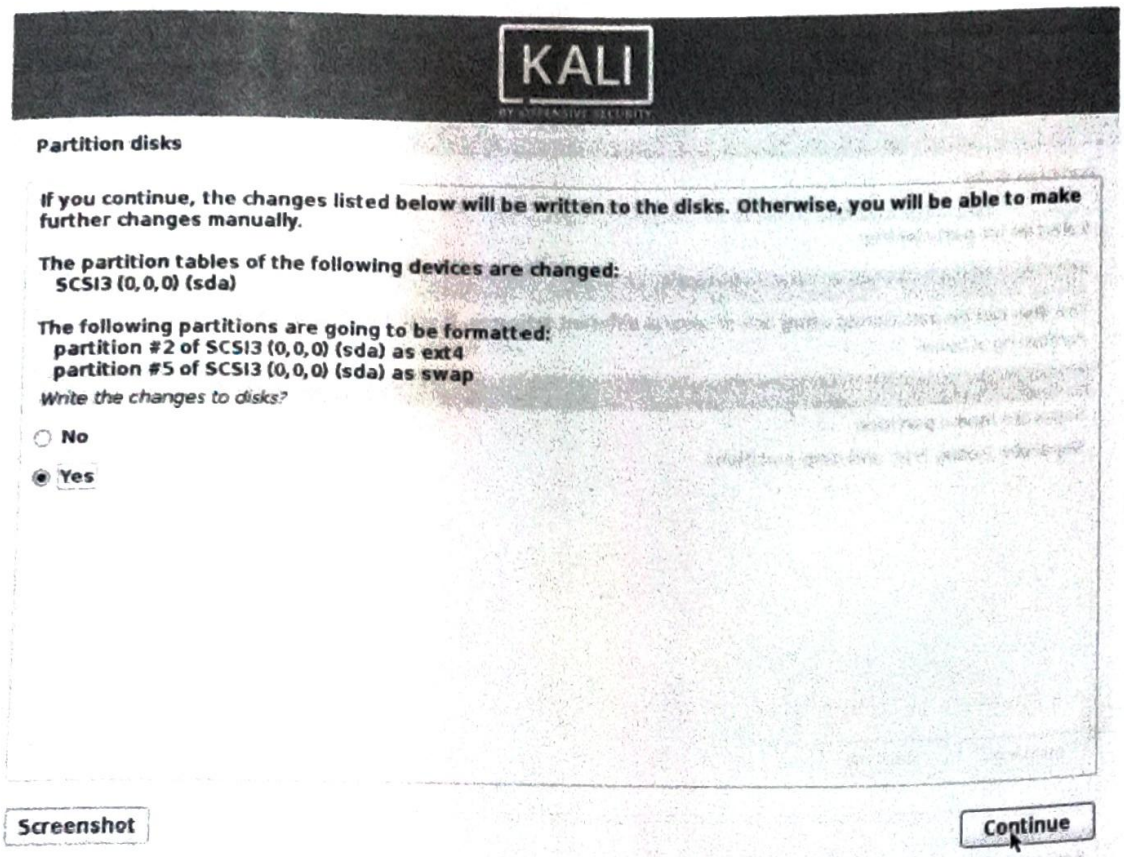
Step 11. Depending on your needs, you can choose to keep all your files in a single partition - the default - or to have separate partitions for one or more of the top-level directories.

If you're not sure which you want, you want "**All files in one partition**".

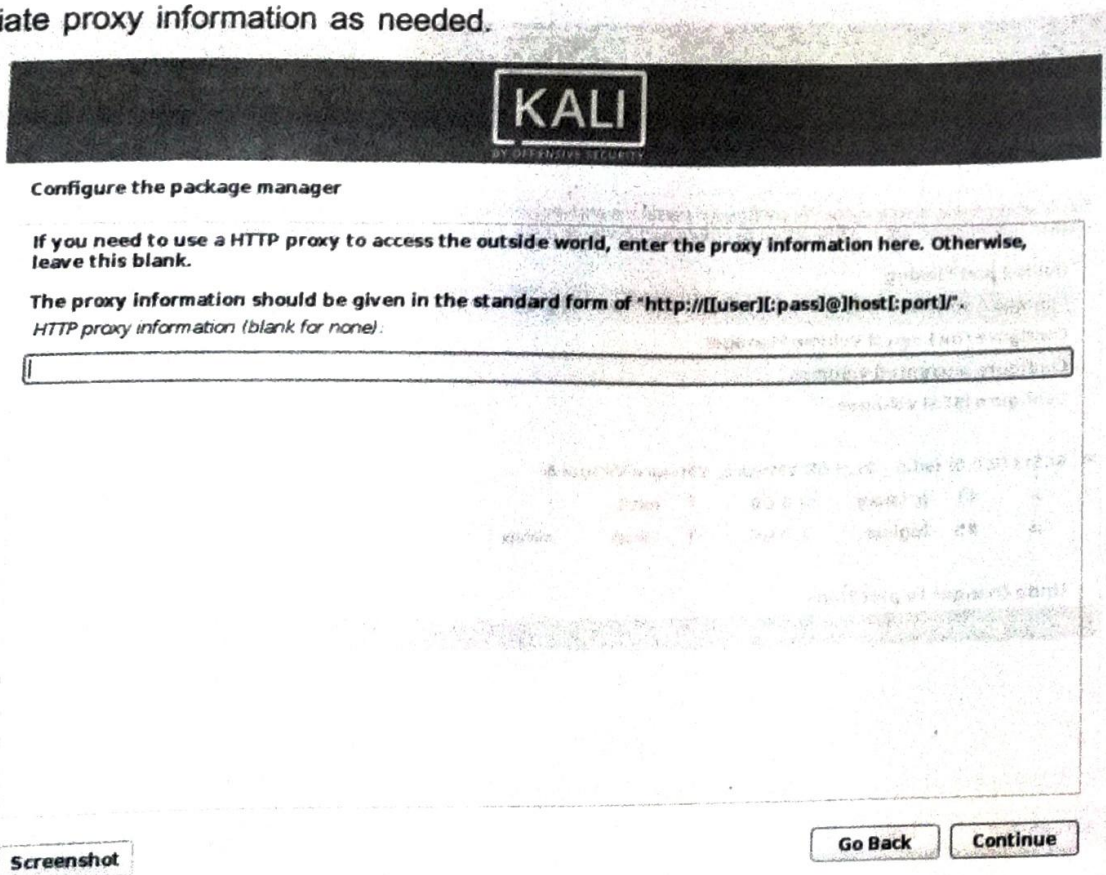




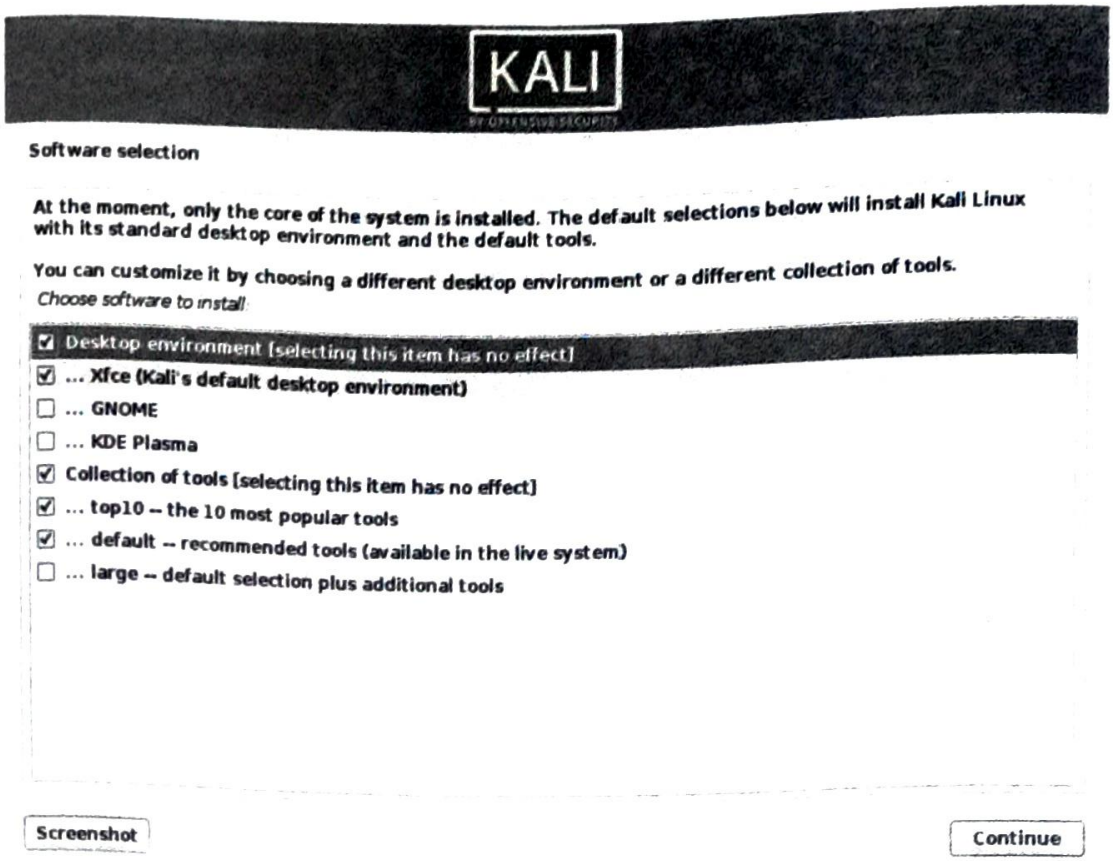
Step 12. Next, you'll have one last chance to review your disk configuration before the installer makes irreversible changes. After you click Continue, the installer will go to work and you'll have an almost finished installation.



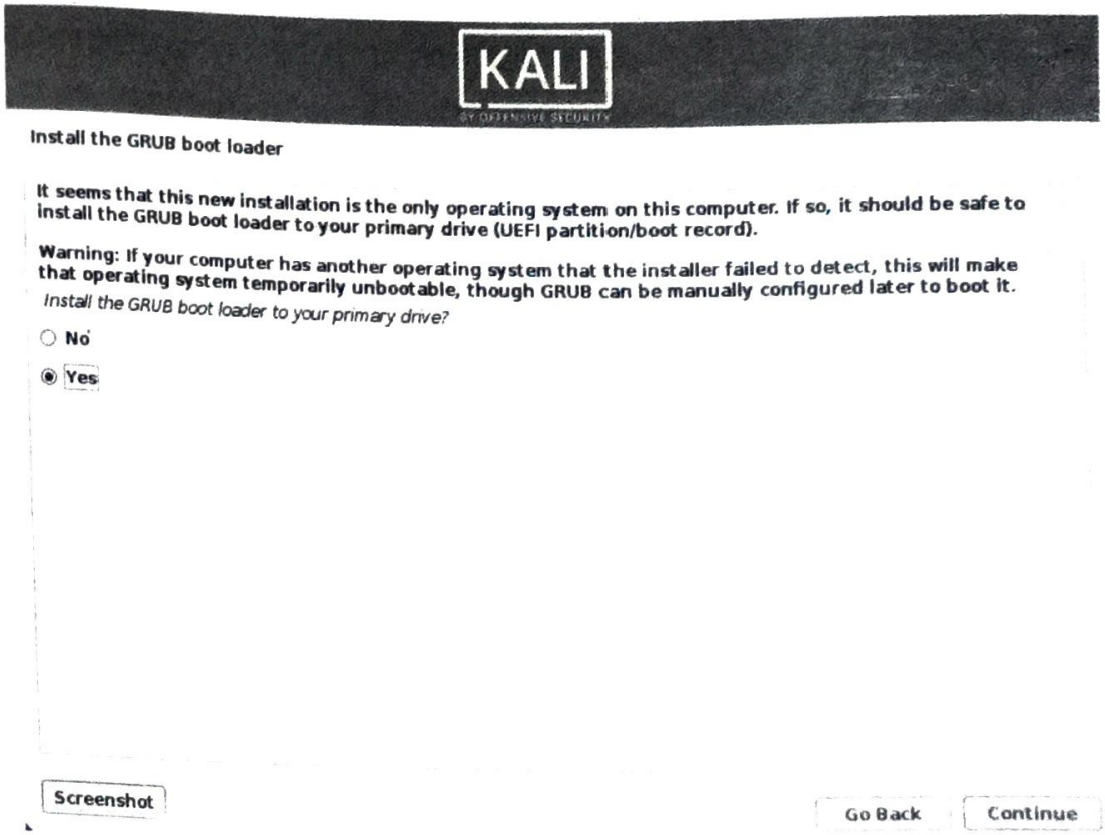
Step 13. Kali Linux uses a central repository to distribute applications. You'll need to enter any appropriate proxy information as needed.



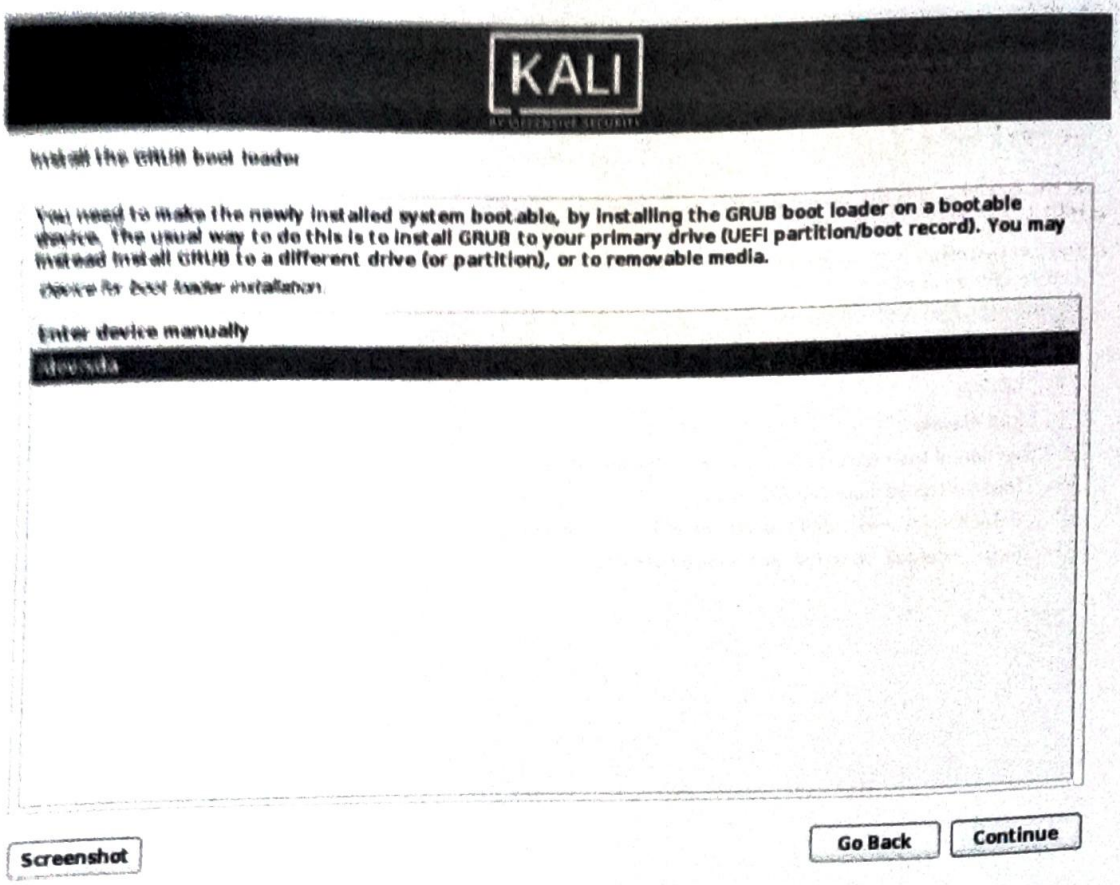
Step 14. Next you can select which metapackages you would like to install. The default selections will install a standard Kali Linux system.



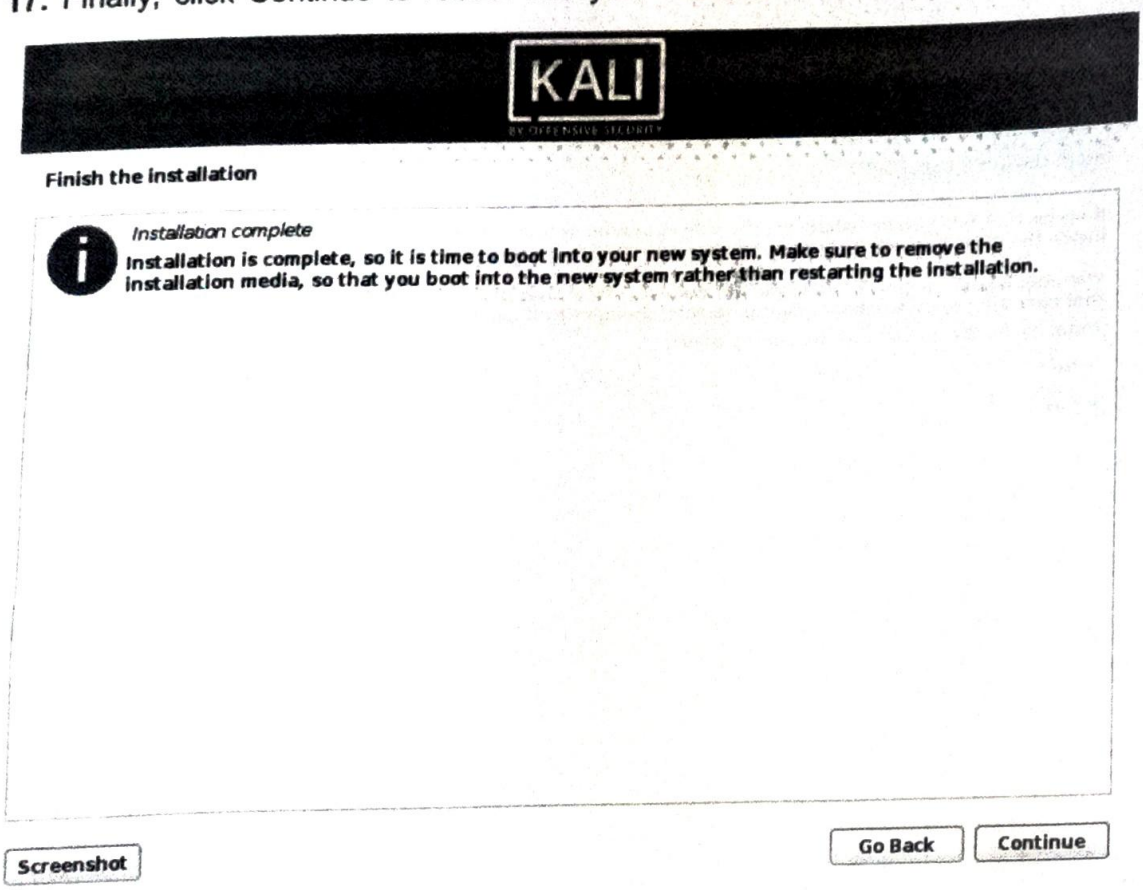
Step 15. Next confirm to install the GRUB boot loader.



Step 16. Select hard drive to install the GRUB bootloader in (By default, it does not select any drive).



Step 17. Finally, click Continue to reboot into your new Kali Linux installation.



4.6.3 Basic commands in Kali Linux

Kali Linux is an open-source operating system. All system hardware and resources, such as CPU, memory, and storage, are directly managed by the operating system. Kali Linux is similar to Unix, but Kali Linux can work on a large number of devices, from mobiles to supercomputers. Linux includes:

- **Kernel :** It is the base component of any operating system. It manages system resources and makes users communicate with hardware by using Kali Linux commands.
- **System userspace :** It contains all the codes of the applications that the user interacts with.
- **Applications :** It consists of all the utilities and software that are used while working. They can be accessed by using Kali Linux commands.

Kali Linux is primarily used by ethical hackers. It contains hundreds of cyber security tools and applications for various information security tasks such as penetration testing, forensics, and reverse engineering.

Some of the more reasons for using Kali Linux are as under:

- Free open-source operating system
- Multi-language support
- Wireless device support
- Completely customizable

Kali Linux – Command Line Essentials

Command-line plays an important role when we are working with Kali Linux. While executing a command in Kali Linux we enter a command on the terminal emulator and it gives us the appropriate output after the execution of the command.

There are some commands in Kali Linux which we use too frequently. So, we should be aware of those commands as it could increase our productivity.

Command Name	Description	Syntax	Example
man	It will display the documentation of ls command	$man [option] ... [command name] ...	$man ls
cd	It will change the directory	$cd [options] directory]	$cd Desktop
ls	It will display all the files and folders in a given directory.	ls [options]... [files]...	$ls DesktopShows all the folders and files in the Desktop directory

Command Name	Description	Syntax	Example
cat	Reads the contents of all files that are in a terminal.	$cat [options].... [filename(s)] ...	$cat text.txt
touch	Creates new files without writing any content in it.	$touch [Option]... [Filename]...	$ touch test1.txtIt creates a file with a text name.
mkdir	Create a new directory in the present directory	$mkdir [Option]..<Directory Name>..	$mkdir testcreates a test folder.
pwd (print working directory)	It shows you the working directory	$pwd [Option]	$pwd
echo	Displays any text as arguments	$echo [Option] [String]	$ echo -e "Welcome"
rm	Used to remove or delete any directory.	$rm [Option] [File]	$rm test123.txt
rmdir	Deletes or removes empty directories.	$rmdir [Option] [Directory_Name]	$ rmdir test
mv	It can move files from one folder to another.	$mv [Source] [Destination]	$mv t1.txt t2.txt
cp	Copies files from one location to another.	$cp [Options] [Source].. [Destination]	$cp t1.txt t2.txt
tree	Lists of contents of a director in the tree fashion.	$tree [Options]	$tree
grep	Searches for word in files and prints lines with that word.	$grep [Options] [Pattern] [Filename]	$grep -ihkp t1.txt
vi	Allows the users to edit the text in the Vim editor.	$vi [Options] [Filename]	$vi t1.txt

Command Name	Description	Syntax	Example
head	Prints the first given number of lines from a file.	$head [Option] [Filename]	$head -n 2 t1.txtIt will print first 2 lines of t1.txt
tail	Prints the last given number of lines from a file.	$ tail -n <number><Filename>	$tail -n 2 t1.txt It will print last 2 lines of t1.txt
wc (word count)	It shows the number of lines, words, bytes and characters.	$wc [Option]... [File]...	$wc t1.txt
history	shows history of commands that you have typed and executed.	$history	$history

4.6.4 Vulnerability Scanning

The practice of finding security holes and weaknesses in the software and systems that run on them is known as vulnerability scanning. It is a component of an organization-protecting vulnerability management program that guards against data breaches.

Vulnerability scanning technologies are used by IT departments or outside security service providers to check for vulnerabilities. By doing this, the effectiveness of countermeasures against a danger or assault can be predicted.

NIS defines vulnerability scanning as:

"A technique to identify hosts/host attributes and associated vulnerabilities."

Software for vulnerability scanning can identify a company's weaknesses, provide assistance in fixing them, and assist in setting priorities for repair activities.

How vulnerability scanning operates:

Regular vulnerability scanning keeps businesses ahead of new vulnerabilities and emerging threats. Vulnerability scanning is a continuous process. Here's a detailed breakdown of how it operates:

- **Generates an asset inventory :** Every system linked to a network is found and listed by the vulnerability scanner. It lists the software, open ports, operating system, and user accounts for every device.
- **Examines the attack surface :** In order to find potential risk exposures and attack routes, the scanner then examines the networks, hardware, software, and systems.

[Fig. 4.3 : Six Step Process of Vulnerability Scanning]

- **In contrast to vulnerability databases :** The vulnerability scanner searches the target attack surface for known vulnerabilities, such as CVEs, and possible routes to sensitive data.
- **Identifies and categorizes :** The scanner finds and categorizes vulnerabilities in systems that an attacker could use against you.
- **Reports:** To assist businesses in setting priorities, the scanner generates reports that detail vulnerabilities and associated fixes.
- **Takes corrective action :** Organizations can take action to address the vulnerabilities found based on the information from the vulnerability scans. Patching, updating software, resetting systems, and putting other security measures in place can all be part of this.

4.6.5 Vulnerability Based Hacking

Hacking can be classified into different categories as described below.

- **Foot printing**

Foot printing is basically the first step where hacker gathers as much information as possible to find ways to intrude into a target system or at least decide what type of attacks will be more suitable for the target.

During this phase, a hacker can collect the following information like Domain name, IP Addresses, Namespaces, Employee information, Phone numbers, E-mails, Job Information etc...

For example, we can use **http://www.whois.com/whois** website to get detailed information like domain name information with its owner, its registrar, date of registration, expiry, name server, owner's contact information, etc.

Another example is to use of **ping command to find out an IP Address.** $ping ambajitemple.com

- **Scanning**

Vulnerability scanning is a specific type that focuses on identifying security flaws and vulnerabilities in systems and software. Scanning software can show a company where its vulnerabilities are, offer support to fix them and help you prioritize remediation efforts.

- **Password Cracking**

Password cracking refers to the act of attempting to uncover or crack passwords that are encrypted or hashed.

The main objectives of password cracking are as :

1. *Recover forgotten passwords* : Password cracking can be used for legitimate purposes, such as helping individuals recover forgotten passwords
2. *Penetration Testing* : Password cracking is sometimes used by security professionals and ethical hackers during authorized penetration testing engagements. By attempting to crack passwords, they can assess the strength of security measures and identify vulnerabilities within an organization's systems and networks. This helps organizations improve their overall security posture by addressing weaknesses.
3. *To gain access* : Another objective of the password cracking is to gain unauthorised access to the system or computer network or server.

Password crackers are tools or programs used by individuals or attackers to recover or crack passwords that have been encrypted or hashed. These tools utilize various methods and techniques to guess or obtain passwords through brute force attacks or exploiting vulnerabilities.

- **Brute Force Attacks**

Brute force attacks involve systematically trying every possible combination of characters until the correct password is found. Password crackers automate this process by attempting different combinations of characters, including letters, numbers, and symbols, until the password is successfully cracked. Brute force attacks can be time-consuming, especially for complex and longer passwords.

- **Injection Attacks**

SQL injection is one of the most common web hacking techniques. SQL injection is the placement of malicious code in SQL statements, via web page input. SQL injection is a code injection technique that might destroy your database.

It occurs when the web application does not properly validate or sanitize user-supplied input, allowing an attacker to inject malicious SQL statements into the application's database queries.

For example, we have an application which selects the user from usermaster table in the database based on userid.

The frontend design for this application is as below.

ENTER USER ID [ ]

The backend logic (SQL statement) for this application is as below.

```
txtuserid = getRequestString("userid");
txtSQL = "SELECT * FROM usermaster WHERE userid = " + txtuserid;
```

In this application, user is required to enter his userid in the above textbox. Then SQL statement written above will be executed and gives the detail for that user as the userid supplied in the textbox.

ENTER USER ID [101 OR 1=1]

SQL Injection statement based on 1=1 always true.

When attacker enters input as written in textbox. The backend SQL statement will be executed as

```
SELECT * FROM usermaster WHERE userid = 105 OR 1=1;
```

The SQL statement above is valid and will return ALL rows from the "usermaster" table, since **OR 1=1** is always TRUE. What if the "usermaster" table contains names and passwords? A hacker might get access to all the user names and passwords in a database.

With the use of various techniques like Parameterized queries, Input Validation and Sanitization, Least Privilege Principle, Secure Coding Practices, Web Application Firewalls, and Regular Security Testing we can prevent from the SQL Injection Attack.

- **Phishing Attacks**

Phishing is a type of cybercrime in which criminals pose as a trustworthy source online to lure victims into providing personal information such as usernames, passwords, or credit card numbers. The goal of any phishing scam is always **stealing personal information**, there are different types of phishing attacks as described.

1. Email Phishing : It is the most common type of phishing which often involves a "spray and pray" technique in which hackers impersonate a legitimate identity or organization and send **mass emails** to as many addresses as they can obtain.

These emails are often written with a sense of urgency, informing the recipient that a personal account has been compromised and they must respond immediately. Their objective is to elicit a certain action from the victim such as clicking a malicious link that leads to a fake login page. After entering their credentials, victims unfortunately deliver their personal information straight into the scammer's hands.

2. Spear Phishing : Rather than using the "spray and pray" method as described above, spear phishing involves sending malicious emails to specific individuals within an organization. Rather than sending out mass emails to thousands of recipients, this method targets certain employees at specifically chosen companies. These types of emails are often more personalized in order to make the victim believe they have a relationship with the sender.

3. Whaling : Whaling closely resembles spear phishing, but instead of going after any employee within a company, scammers specifically target senior executives (or "the big fish," hence the term whaling). This includes the CEO, CFO or any high-level executive with access to more sensitive data than lower-level employees. Often, these emails use a high-pressure situation to hook their victims, such as relaying a statement of the company being sued. This entices recipients to click the malicious link or attachment to learn more information.

4. Smishing : SMS phishing, or smishing, leverages text messages rather than email to carry out a phishing attack. They operate much in the same way as email-based phishing attacks: Attackers send texts from what seem to be legitimate sources (like trusted businesses) that contain malicious links. Links might be disguised as a coupon code (20% off your next order!) or an offer for a chance to win something like concert tickets.

5. Vishing : Vishing—otherwise known as voice phishing—is similar to smishing in that a phone is used as the vehicle for an attack, but instead of exploiting victims via text message, it's done with a phone call. A vishing call often relays an automated voice message from what is meant to seem like a legitimate institution, such as a bank or a government entity.

6. Business Email Compromise (CEO Fraud) : CEO fraud is a form of phishing in which the attacker obtains access to the business email account of a high-ranking executive (like the CEO). With the compromised account at their disposal, they send emails to employees within the organization impersonating as the CEO with the goal of initiating a fraudulent wire transfer or obtaining money through fake invoices.

7. Clone Phishing : This method of phishing works by creating a malicious replica of a recent message you've received and re-sending it from a seemingly credible source. Any links or attachments from the original email are replaced with malicious ones. Attackers typically use the excuse of re-sending the message due to issues with the links or attachments in the previous email.

- **Block chain Attacks**

Blockchain attacks refer to malicious activities aimed at disrupting or compromising the integrity, availability, or confidentiality of blockchain networks and associated assets. Blockchain technology, which underpins cryptocurrencies like Bitcoin and Ethereum, is designed to be secure through its decentralized and distributed nature. However, various attack vectors can still pose risks to blockchain systems. Here are several types of blockchain attacks:

1. 51% Attack : In a 51% attack, a single entity or group controls more than 50% of the computational power (hash rate) of a blockchain network. This enables the attacker to manipulate transaction confirmations, reverse transactions, or double-spend coins.

2. Sybil Attack : A Sybil attack occurs when an attacker creates multiple fake identities or nodes to gain control or influence over a blockchain network. This can lead to network manipulation, denial of service (DoS) attacks, or undermining the consensus mechanism.

3. Denial of Service (DoS) Attack : A DoS attack aims to disrupt the availability of a blockchain network by overwhelming it with a high volume of malicious traffic or transactions. This can prevent legitimate users from accessing the network or executing transactions.

4. Eclipse Attack : In an eclipse attack, an attacker isolates a targeted node by controlling its network connections and surrounding it with malicious nodes. This allows the attacker to manipulate the node's view of the blockchain network, potentially leading to double-spending or other fraudulent activities.

5. Double-Spending : Double-spending occurs when a user spends the same cryptocurrency units more than once. While blockchain technology is designed to prevent double-spending through its consensus mechanism, certain vulnerabilities or attacks, such as 51% attacks, can enable double-spending.

4.7 PORT SCANNING

4.7.1 What is Port Scanning ?

A port scanning is a common technique hackers use to discover open doors or weak points in a network. A port scan attack helps cyber criminals to find open ports and figure out whether they are receiving or sending data. It can also reveal whether active security devices like firewalls are being used by an organization.

When hackers send a message to a port, the response they receive determines whether the port is being usedand if there are any potential weaknesses that could be exploited.

Businesses can also use the port scanning technique to send packets to specific ports and analyse responses for any potential vulnerability. They can then use tools like IP scanning, Network mapper (Nmap), and Netcat to ensure their network and systems are secure.

Port scanning can provide information such as:

- Services that are running
- Users who own services
- Whether anonymous logins are allowed
- Which network services require authentication

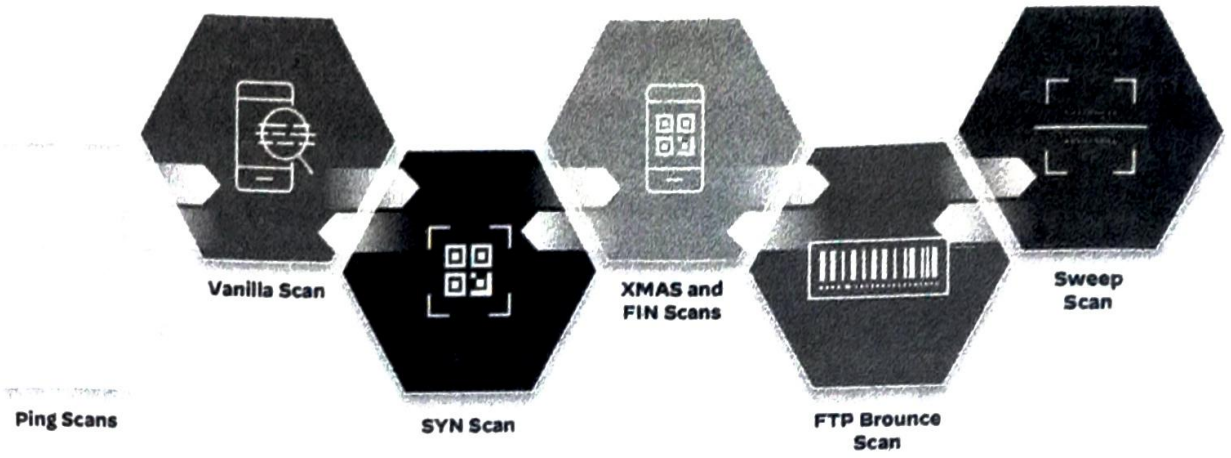
4.7.2 Port Scanning Techniques

A port is a point on a computer where information exchange between multiple programs and the internet to devices or other computers takes place. To ensure consistency and simplify programming processes, ports are assigned port numbers. This, in conjunction with an IP address, forms vital information that each internet service provider (ISP) uses to fulfil requests.

Some of the most popular and most frequently used ports include :

- Port 20 (UDP): File Transfer Protocol (FTP) used for transferring data
- Port 80 (TCP): The World Wide Web Hypertext Transfer Protocol (HTTP)

The various port scanning methods are described under :



[Fig. 4.4 : Port Scanning Methods]

1. **Ping scans :** A ping scan is considered the simplest port scanning technique. They are also known as internet control message protocol (ICMP) requests. Ping scans send a group of several ICMP requests to various servers in an attempt to get a response. A ping scan can be used by an administrator to troubleshoot issues, and pings can be blocked and disabled by a firewall.

2. **Vanilla scan :** Another basic port scanning technique, a vanilla scan attempts to connect to all of the 65,536 ports at the same time. It sends a synchronize (SYN) flag, or a connect request. When it receives a SYN-ACK response, or an acknowledgment of connection, it responds with an ACK flag. This scan is accurate but easily detectable because a full connection is always logged by firewalls.

3. **SYN scan :** Also called a half-open scan, this sends a SYN flag to the target and waits for a SYN-ACK response. In the event of a response, the scanner does not respond back, which means the TCP connection was not completed. Therefore, the interaction is not logged, but the sender learns if the port is open. This is a quick technique that hackers use to find weaknesses.

4. **XMAS and FIN scans :** Christmas tree scans (XMAS scans) and FIN scans are more discrete attack methods. XMAS scans take their name from the set of flags that are turned on within a packet which, when viewed in a protocol analyser like Wireshark, appear to be blinking like a Christmas tree. This type of scan sends a set of flags, which, when responded to, can disclose insights about the firewall and the state of the ports. A FIN scan sees an attacker send a FIN flag, often used to end an established session, to a specific port. The system's response to it can help the attacker understand the level of activity and provide insight into the organization's firewall usage.

5. **FTP bounce scan :** This technique enables the sender to disguise their location by using an FTP server to bounce a packet.

6. **Sweep scan :** This preliminary port scanning technique sends traffic to a port across several computers on a network to identify those that are active. It does not share any information about port activity but informs the sender whether any systems are in use.

4.8 REMOTE ADMINISTRATION TOOL (RAT)

4.8.1 Introduction – Remote Administration Tools (RAT)

Remote administration is the process of remotely accessing or operating any equipment or device like computer from a different place. Remote Administration Tools are software that enable remote administration. Thus, RAT allows someone to access your device remotely from any location. These tools provide someone else access to your files, camera, and even the ability to shut off your device.

Remote Administration tools are generally used for two purposes as described below.

- **Legitimate users :** Technical specialist many times uses the internet and Remote Administration tools to remotely access our computer and fix issues with our system.
- **Hackers :** However, a lot of these remote administration solutions are utilized by hackers to get access to your computer, damage your data, and take crucial data. Hackers typically include a malicious code inside a game or movie that you download, which allows them to quickly get access to your computer.

4.8.2 How one can use – Remote Administration Tools (RAT)

The internet connection on both devices is a basic need if you need to access a system remotely.

With RAT software, the user can establish a remote connection to the host machine located over any other location. When you are online, hackers establish a connection with you and carry out destructive actions such as deleting files, adding data, stealing data, and so on.

Remote Administration tools can be installed in two different ways as described below.

- **Manually :** If you know how to install it, you can manually add a valid RAT to your machine. On the other hand, hackers might install RAT on your system using unique methods. Generally, this approach is used by legitimate users like technicians.
- **Stealthy :** Cybercriminals affix these viruses with an online file, such as a game or movie. The malicious software is also downloaded and installed on your system, giving you access to it.

With the use of these RAT software the below activities can be performed.

- Hackers can create, delete, rename, copy, or edit any file.
- The attacker can also use RAT for executing various commands, changing system settings, running, and controlling applications on the victim's PC.
- Hackers can install optional software or worms.
- Hackers can control hardware, shutdown, or restart a computer without asking the user's permission.
- Hackers can steal passwords, login names, personal documents, and other credentials.

- Hackers can capture screenshots and track a user's activity.
- Hackers can get access to the Camera of the victim's system.

4.9 PROTECT SYSTEM FROM RAT

For protecting your system from RAT software, the system administrator should keep below points in mind.

- Be careful when you are using the internet and downloading files online.
- Be careful when taking a P2P file from other users.
- Always Enable your Anti-Viruses.
- Don't allow any malicious file to your system.
- Update your anti-virus from time to time.
- Regularly update your software
- Restrict the access through the use of Firewall
- Limit users who can log in using Remote Desktop

Top Remote Administration Tools

- DarkComet: Dark Comet is the best RAT and a free RAT as well as the old one as well. This tool has astounding graphical UI that causes the client to control the system. It is best used on windows and can control any windows device very smoothly.
- BlackShades: This is the super RAT shockingly better than DarkComet and it is steady, reliable, and easy to use It's likewise the speediest RAT at any point made on .net and helps Windows.
- JSpy: Jspy Rat is the same as Pussy RAT as created by the same person, with some improvements and in 2013 this was free. It is a decent RAT and one of the safest RAT.
- NJRat: It is an amazing RAT to hack into different systems. It gives us a large number of choices that make it different from others. It is very simple to use. It has the malware to use the camera, microphones getting and deleting files, and many more.
- Plasma Remote Administration Tools: Plasma RAT is a capable remote administration tool (RAT) which is a customer service application. It's not just a conventional standard remote administrator tool, it is intended to control a mass measure of PCs without a moment's delay.

4.10 SNIFFING AND MECHANISM OF SNIFFING

4.10.1 Introduction - Sniffing

"Sniffing is the technique of utilizing sniffing tools to monitor and record every packet that passes over a certain network." It is a method of "tapping phone wires" to listen in on the discussion. Another name for it is computer network "wiretapping."

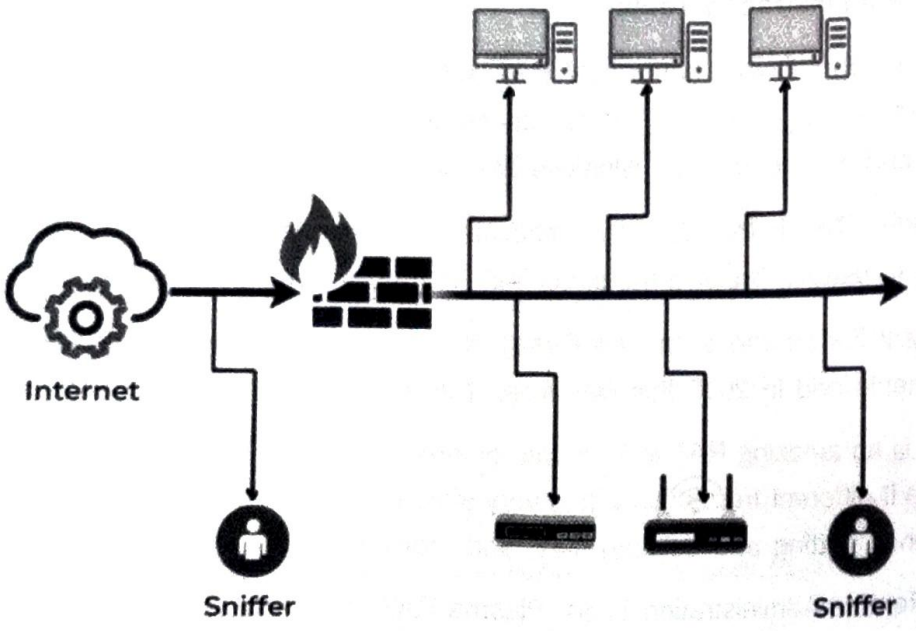
Attackers use sniffers to capture data packets containing sensitive information such as password, account information etc. Sniffers can be hardware or software installed in the system. By placing a packet sniffer on a network in promiscuous mode, a malicious intruder can capture and analyse all of the network traffic.

Sniffing techniques can be used to collect information like email traffic, FTP passwords, Web traffic, Telnet passwords, Router configuration, Chat sessions, DNS traffic etc... All these collected information can be used for other kind of attacks.

How Sniffing Works

Normally, a sniffer sets the system's network interface card (NIC) to promiscuous mode, which allows it to listen to all data transmitted on its segment.

The term promiscuous mode describes the special feature of Ethernet hardware, namely network interface cards (NICs), which enables a NIC to receive any network traffic, even if it is not addressed to it. By comparing the hardware address, also known as the MAC, of the device with the destination address of the Ethernet packet, a NIC may determine by default what traffic is not directed to it. Non-promiscuous mode makes it challenging to employ network monitoring and analysis tools for traffic accounting or diagnosing connectivity problems, even though it makes perfect sense for networking.



[Fig. 4.5 : Working of sniffing]

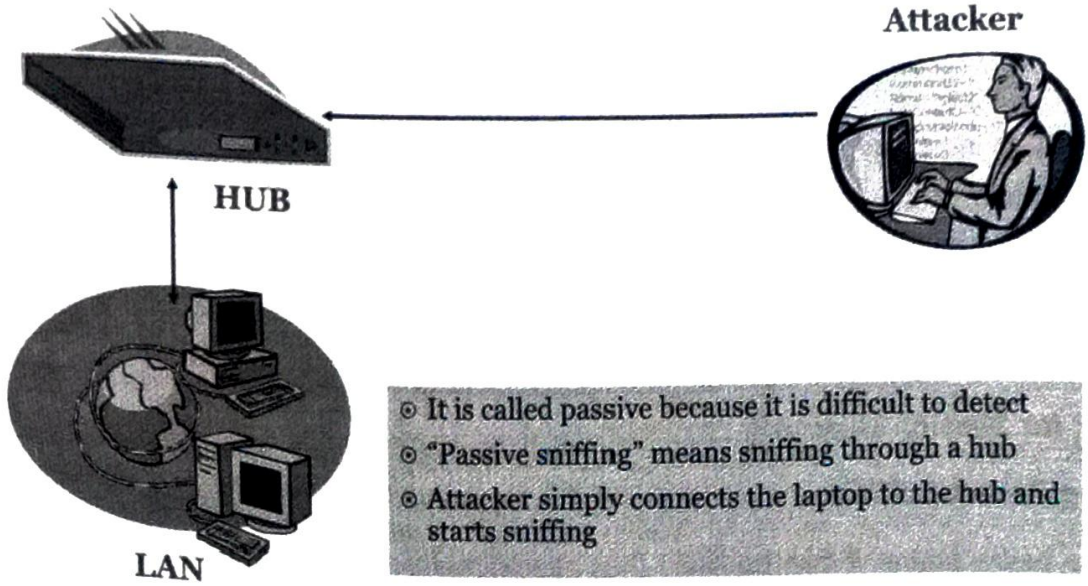
A sniffer can continuously monitor all the traffic to a computer through the NIC by decoding the information encapsulated in the data packets.

4.10.2 Types of sniffing

Sniffing attacks can be classified in either Passive sniffing or Active sniffing based on sniffing method used.

Passive Sniffing:

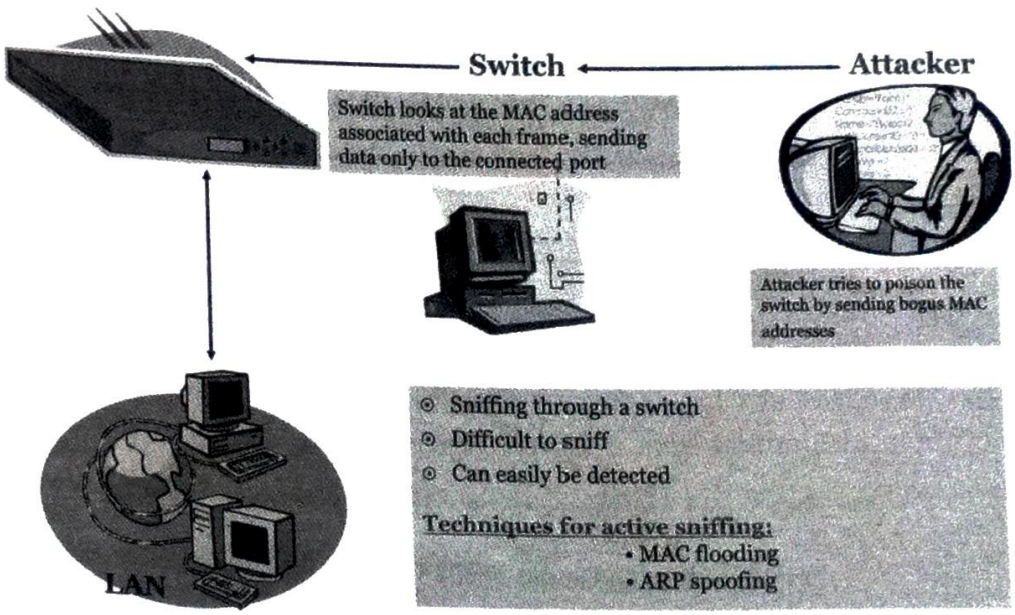
In passive sniffing, an attacker only monitors traffic without any alteration. Passive sniffing works on networks with Hub devices as central device. Hub is a device which works on broadcasting communication technique that is hub accepts packet from one computer and send it to all other computers in the network. But the computer which is intended, will only accept the packet and other computers just ignores packet received from hub. In this kind of communication traffic is visible to all the ports. So, it becomes very easy for an attacker to sniff the traffic and such kind of attack is difficult to discover.



[Fig. 4.6 : Passive Sniffing]

Active Sniffing :

In active sniffing, the traffic is not only monitored, but it may also be altered in some way as the case of attack. Active sniffing is used to sniff a switch-based network. The different kind of techniques used for Active Sniffing are MAC Flooding, DHCP Attacks, DNS Poisoning, Spoofing Attacks, ARP Poisoning etc...



[Fig. 4.7 : Active Sniffing]

The active sniffing techniques are difficult to sniff and easy to detect.

4.10.3 Session Hijacking

A session hijacking attack happens when an attacker takes over your internet session. For instance, while you're checking your credit card balance, paying your bills, or shopping at an online store. Session hijackers usually target browser or web application sessions.

A session hijacking attacker can then do anything you could do on the site. In effect, a hijacker fools the website into thinking they are you. Just as a hijacker can commandeer an airplane and put the passengers in danger, a session hijacker can take over an internet session and cause big trouble for the user.

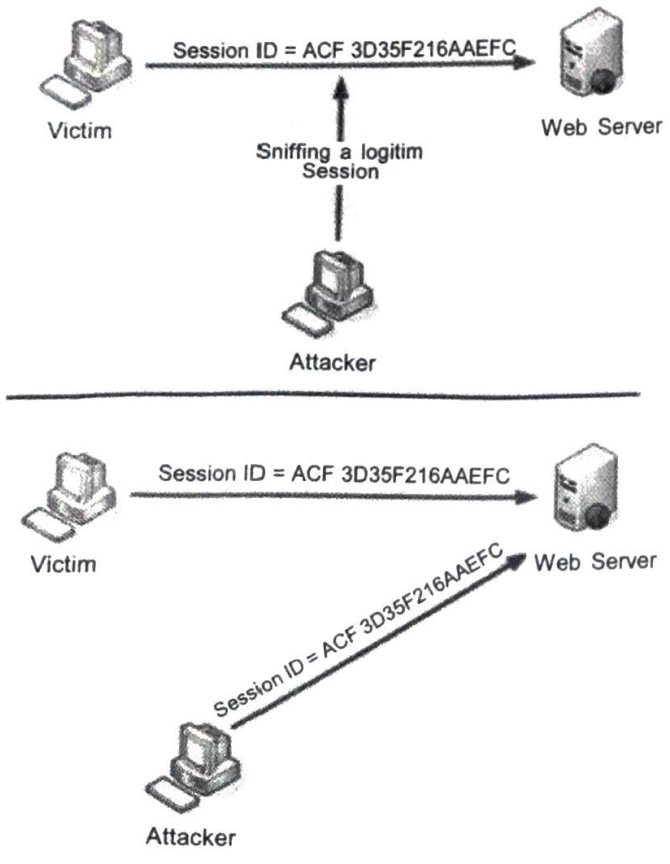
The most common method of session hijacking is called IP spoofing, when an attacker uses source-routed IP packets to insert commands into an active communication between two nodes on a network and disguise itself as one of the authenticated users. This type of attack is possible because authentication typically is only done at the start of a TCP session.

Another type of session hijacking is known as a man-in-the-middle attack, where the attacker, using a sniffer, can observe the communication between devices and collect the data that is transmitted.

Methods for Session Hijacking :

- **Using Packet Sniffers**

  In the below figure, it can be seen that attack captures the victim's session ID to gain access to the server by using some packet sniffers.



[Fig. 4.8 : Session Hijacking with Packet Sniffing]

- **Cross Site Scripting (Malware Scripting)**

  Attacker can also capture victim's Session ID using XSS attack by using javascript. If an attacker sends a crafted link to the victim with the malicious JavaScript, when the victim clicks on the link, the JavaScript will run and complete the instructions made by the attacker.

- **IP Spoofing**

  Spoofing is pretending to be someone else. This is a technique used to gain unauthorized access to the computer with an IP address of a trusted host. In implementing this technique, attacker has to obtain the IP address of the client and inject his own packets spoofed with the IP address of client into the TCP session, so as to fool the server that it is communicating with the victim i.e. the original host.

- **Brute forced Attack (Blind Attack)**

  If attacker is not able to sniff packets and guess the correct sequence number expected by server, brute force combinations of sequence number can be tried.

Self - Assessment

Q. 1 Answer the below short questions :

(1) What is hacking? List out various types of Hacking.

(2) Define the term: Hacking. List out the types of Hackers.

(3) Differentiate: White hat V/s Black hat V/s Grey hat hackers.

(4) What is Ethical hacking? Why ethical hacking is important?

(5) Define the Terms : Attack, Threat, Keystroke logger.

Botnet, Spam, Phishing, Vulnerability

(6) What is 0- Day vulnerability?

(7) List out steps in hacking process.

(8) What is Reconnaissance? Write down steps in Reconnaissance process.

(9) Which kind of information is gathered in Reconnaissance process.

(10) Explain reconnaissance types briefly.

(11) What is KALI Linux Operating System? Why it is important in Ethical hacking?

(12) List out advantages and disadvantages of using Kali Linux OS.

(13) List out any six basic commands of Kali Linux with its uses.

(14) What is Vulnerability Scanning? List out steps in Vulnerability scanning process.

(15) Define the terms : Foot printing, Scanning, Brute force attack

(16) What is password cracking? List out main objectives of password cracking.

(17) What is Phishing? List out various types of Phishing attacks.

(18) What is Port Scanning? List out various Port scanning methods.

(19) What is Remote Administration Tool (RAT)? Which kind of activities can be performed by hackers using RAT Tools.

(20) Write down the points by which we can protect our system from RAT.

(21) What is Sniffing? Differentiate: Active V/s Passive Sniffing

(22) What is Session Hijacking? List out various Session Hijacking methods.

Q. 2 Explain the below questions:

(1) What is hacking? Explain various types of hacking.

(2) Define the term: Hacking. Explain various types of hackers in detail.

(3) Short note on: Ethical Hacking and its importance

(4) Explain hacking process in detail with all is steps.

(5) Explain information gathering in detail with its types.

(6) Explain installation and configuration of Kali Linux with all necessary steps.

(7) Explain any 12 commands of Kali Linux with suitable example.

(8) What is Vulnerability Scanning? Explain vulnerability scanning process in detail.

(9) What is SQL Injection Attack? Explain with one simple example.

(10) What is phishing? Explain different types of phishing attacks.

(11) What is port scanning? Explain various port scanning methods in detail.

(12) Short note on: Remote Administration Tools (RAT).

(13) What is sniffing? Explain its working process.

(14) Differentiate: Active sniffing V/s Passive Sniffing

(15) What is session hijacking? Explain various methods of session hijacking in detail.

***

Chapter 5

DIGITAL FORENSICS

5.1 INTRODUCTION TO DIGITAL FORENSICS

- INTRODUCTION
- WHAT IS DIGITAL FORENSIC?
- ADVANTAGES AND DISADVANTAGES OF DIGITAL FORENSICS

5.2 LOCARD'S PRINCIPAL OF EXCHANGE IN DIGITAL FORENSICS

- LOCARD'S PRINCIPLE IN FORENSIC SCIENCE
- LOCARD'S PRINCIPLE OF EXCHANGE IN DIGITAL FORENSICS
- LIMITATIONS OF LOCARD'S PRINCIPLE OF EXCHANGE

5.3 BRANCHES OF DIGITAL FORENSICS

- TYPES OF DIGITAL FORENSICS
  - ➲ COMPUTER FORENSICS
  - ➲ MEMORY FORENSICS
  - ➲ NETWORK FORENSICS
  - ➲ DATABASE FORENSICS
  - ➲ SOFTWARE FORENSICS
  - ➲ EMAIL FORENSICS
  - ➲ MALWARE FORENSICS
  - ➲ MOBILE FORENSICS

5.4 PHASES OF DIGITAL FORENSIC INVESTIGATION

- OBJECTIVES OF DIGITAL FORENSIC INVESTIGATION
- DIGITAL FORENSIC INVESTIGATION PROCESS MODEL

5.5 METHODS OF PRESERVING DIGITAL FORENSIC EVIDENCE

- WHY SHOULD WE PRESERVE DIGITAL EVIDENCE
- DIGITAL EVIDENCE PREVERSATION METHODS

5.6 CRITICAL STEPS IN PRESERVING DIGITAL EVIDENCE

- CRITICAL STEPS IN PRESERVING DIGITAL EVIDENCE
- KEY POINTS TO REMEMBER TO SPEED UP PRESERVING EVIDENCE

5.7 ROLE OF DEVICES AS EVIDENCE IN DIGITAL FORENSICS

- TYPES OF DEVICES
  - ➲ COMPUTING DEVICES
  - ➲ NETWORKING DEVOCES AND SERVERS
  - ➲ CCTV
  - ➲ VEHICLES

○ **Self - Assessment**

5.1 INTRODUCTION TO DIGITAL FORENSICS

5.1.1 Introduction

We know that once a cyberattack has been occurred on our organization, it may create extreme confusion about cyberattack. You may need to answer some of the questions like how the attack happened, how it affects your data, and how to move forward from here. This information is vital to help both the criminal investigation and to increase your network security and prevent new attacks.

A digital forensics investigation is the first step toward the direction of answering these questions and also helped hundreds of organizations navigate the rough waters of a cyberattack.

5.1.2 What is Digital Forensics ?

"Digital forensics, also known as **computer forensics** or **cyber forensics**, is a branch of forensic science that deals with the investigation, collection, preservation, analysis, and presentation of digital evidence."

It involves the application of scientific methods and techniques to extract and interpret information from digital devices, networks, and online platforms for legal purposes. It provides the forensic team with the best techniques and tools to solve complicated digital-related cases. A digital forensic investigation can help you answer any questions you might have about the attack, including

- What networks, systems, files, or applications were affected?
- How did the incident occur? (Tools, attack methods, vulnerabilities, etc.)
- What data and information were accessed or stolen?
- Are hackers still on my network? Is the incident finished, or is it ongoing?
- Where did the attack come from?

Example Uses of Digital Forensics

- Intellectual Property theft
- Industrial espionage
- Employment disputes
- Fraud investigations
- Inappropriate use of the Internet and email in the workplace
- Forgeries related matters
- Bankruptcy investigations
- Issues concern with the regulatory compliance

The goal is to establish a chain of custody for the digital evidence, ensuring its integrity and admissibility in legal proceedings.

5.1.3 Advantages and Disadvantages of Digital Forensics

Advantages of Digital Forensics

- To ensure the integrity of the computer system.
- To produce evidence in the court, which can lead to the punishment of the culprit.
- It helps the companies to capture important information if their computer systems or networks are compromised.
- Efficiently tracks down cybercriminals from anywhere in the world.
- Helps to protect the organization's money and valuable time.
- Allows to extract, process, and interpret the factual evidence, so it proves the cybercriminal actions in the court.

Disadvantages of Digital Forensics

- Digital evidence accepted into court. However, it is must be proved that there is no tampering
- Producing electronic records and storing them is an extremely costly affair
- Legal practitioners must have extensive computer knowledge
- Need to produce authentic and convincing evidence
- If the tool used for digital forensic is not according to specified standards, then in the court of law, the evidence can be disapproved by justice.
- Lack of technical knowledge by the investigating officer might not offer the desired result.

5.2 LOCARD'S PRINCIPLE OF EXCHANGE IN DIGITAL FORENSICS

5.2.1 Locard's Principle of exchange in Forensic Science

Forensic science has changed the way crime investigations are handled. By examining and analysing the physical evidence and reconstructing the circumstances of the crime, forensic investigators are able to come up with scientific information that they can present in court. A person who is responsible for one of the most important principles in forensic science is Edmond Locard. He came up with the Locard's exchange principle or Locard's theory which states that

"Any action of an individual, and obviously, the violent action constituting the crime, cannot occur without leaving a trace."

A devout viewer of crime investigative series on television will be able to understand the importance of this principle. Haven't we all observed how the investigator goes to the site of a grisly murder and examines the crime scene, to check for blood stains, footprints or fingerprints, murder weapons and even the slightest of traces of blood in the nails? This is known as trace evidence, and according to Locard's principle whenever a crime is committed, trace evidence no matter how small or less, will always be present.

Locard's exchange principle is an important part of forensic science investigation.

"It states that any criminal leaves behind a trace when committing a violent crime. It is the investigator's duty to find this trace evidence and reconstruct the events of the crime."

The trace evidence can be divided into:

- Physical (clothing, glass fragments, paint chips etc)
- Biological (DNA, fingerprints, hair)
- Natural evidence (soil, pollen, seeds and plants)
- Digital evidence (Images, audio, video, files, hard disks etc...)

5.2.2 Locard's Principle of exchange in Digital Forensics

In digital forensics, Locard's Principle of Exchange is still applicable, and it emphasizes the idea that whenever two digital entities come into contact, there will be an exchange of materials or information. This principle serves as a foundational concept in digital investigations and highlights the importance of analysing the traces and artifacts left behind during digital interactions.

Here's how Locard's Principle of Exchange can be applied specifically to digital forensics:

1. **Digital Contact**
   - Whenever there is interaction between digital devices, systems, or users, there is a potential for an exchange of digital information.
   - Examples include file transfers, communication over networks, logins, data access, and other digital transactions.

2. **Exchange of Digital Evidence**

- During digital interactions, data is created, modified, or deleted, leaving behind a trail of digital evidence.
- This digital evidence can include files, logs, metadata, timestamps, network activity records, images, audio, video and other artifacts that reflect the nature of the interaction.

3. **Analysis of Digital Artifacts**

- Digital forensics experts analyse these digital artifacts to reconstruct events, understand the series of actions, and identify relevant information for an investigation.
- It involves examining file structures, computer system logs, network traffic, and other digital traces to piece together the timeline and details of a digital incident.

4. **Chain of Custody and Integrity**

- Locard's Principle reinforces the importance of maintaining a secure chain of custody for digital evidence. This involves documenting the handling, storage, and transfer of digital evidence to ensure its integrity and admissibility in legal proceedings.

5. **Specialized Tools and Techniques:**

- Digital forensics professionals use specialized tools and techniques to acquire, preserve, and analyse digital evidence.
- These tools help investigators extract information from digital devices without altering the original data, maintaining the integrity of the evidence.

Overall, Locard's Principle of Exchange remains a guiding principle in digital forensics, emphasizing the inevitability of data exchange during digital interactions and highlighting the importance of skilful analysis of digital evidence in investigations.

5.2.2 Limitations of Locard's Principle of Exchange

One of the greatest drawbacks of Locard's exchange theory lies in evidence dynamics. This refers to the alteration of physical evidence before it has been examined by investigators.

There are many factors that can lead to the tampering and destruction of evidence.

- Staging (manipulation of objects in crime scene) by the offender
- Secondary transfer of evidence
- Actions of the victim before the crime
- Witness actions
- Natural factors like animal or insect activity, weather, decomposition.
- Fire suppression efforts
- Actions of police, scene technicians and medical personnel.

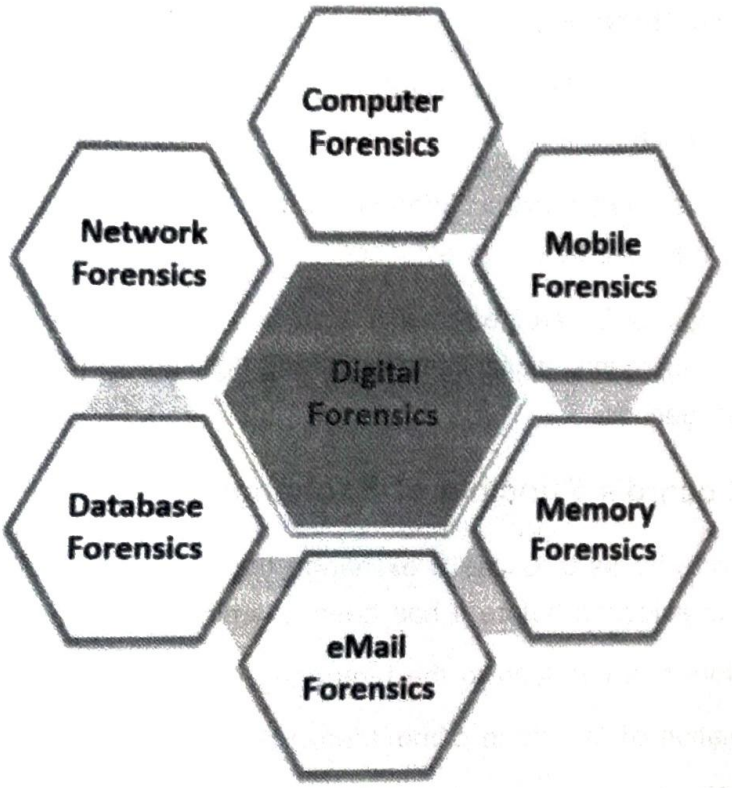
These factors can lead to the removal or obliteration of the evidence. They can often mislead the investigators and cause problems with crime reconstruction. Misinterpretations or misleading evidence can lead to inaccurate crime reconstruction. To avoid this, the investigator needs to make sure that the crime scene investigation and reconstruction is carried out with care.

5.3 BRANCHES OF DIGITAL FORENSICS

Digital forensics, also known as **computer forensics** or **cyber forensics**, is a branch of forensic science that deals with the investigation, collection, preservation, analysis, and presentation of digital evidence. Digital forensics plays a crucial role in modern criminal investigations and is often relied upon in legal proceedings. It helps in identifying perpetrators, proving guilt or innocence,recovering lost or deleted data, protecting digital evidence from tampering, and enhancing the overall integrity of the justice system in the digital age.

5.3.1 Types of Digital Forensics

Digital forensics encompasses various types or sub-disciplines based on the specific areas of focus and the nature of the investigation. Here are some common types of digital forensics:



[Fig. 5.1 : Branches of Digital Forensics]

Computer Forensics

This is the most well-known and widely practiced type of digital forensics. It involves the analysis and investigation of computer systems, including desktops, laptops, servers, and storage devices. Computer forensics aims to recover and examine digital evidence such as files, documents, emails, internet browsing history, and system logs to establish a timeline of events or support legal cases.

When conducting an investigation and analysis of evidence, computer forensics specialists use various techniques; here are some examples:

- **Deleted file recovery**

  This technique involves recovering and restoring files or fragments deleted by a person—either accidentally or deliberately—or by a virus or malware.

- **Reverse steganography**

  The process of attempting to hide data inside a digital message or file is called steganography. Reverse steganography happens when computer forensic specialists look at the hashing of a message or the file contents. A hashing is a string of data, which changes when the message or file is interfered with.

- **Cross-drive analysis**

  This technique involves analysing data across multiple computer drives. Strategies like correlation and cross-referencing are used to compare events from computer to computer and detect anomalies.

- **Live analysis**

  This technique involves analysing a running computer's volatile data, which is data stored in RAM (random access memory) or cache memory. This helps pinpoint the cause of abnormal computer traffic.

Memory Forensics

Memory forensics focuses on the analysis of a computer's volatile memory (RAM) to extract valuable information. Memory forensics is crucial in uncovering malicious activities or detecting sophisticated malware that may not be present on disk.

This is usually achieved by running special software that captures the current state of the system's memory as a snapshot file, also known as a **memory dump**. This file can then be taken offsite and searched by the investigator. It involves examining the contents of the memory at a given time to identify running processes, network connections, open files, passwords, encryption keys, and other volatile data.

This is useful because of the way in which processes, files and programs are run in memory, and once a snapshot has been captured, many important facts can be ascertained by the investigator, such as :

- Processes running
- Executable files that are running
- Open ports, IP addresses and other networking information
- Users that are logged into the system, and from where
- Files that are open and by whom

Memory forensics can be thought of as a current snapshot of a system that gives investigators a near real time image of the system while in use. Hard drive forensics is normally focused on data recovery and decryption, usually made from an image of the drive in question.

Network Forensics

Most of the attacks move through the network before hitting the target and they leave some trace. According to Locard's exchange principle, "every contact leaves a trace," even in cyberspace.

Network forensics deals with the examination of network traffic and data packets to investigate network-based security incidents or cybercrimes. It involves capturing, analysing, and interpreting network traffic to identify potential threats, unauthorized activities, or evidence of malicious actions. Network forensics can provide insights into network intrusions, data breaches, or other network-related offenses.

There are **two methods** of network forensics :

- **"Catch it as you can" method :** All network traffic is captured. It guarantees that there is no omission of important network events. This process is time-consuming and reduces storage efficiency as storage volume grows.
- **"Stop, look and listen" method :** Administrators watch each data packet that flows across the network but they capture only what is considered suspicious and deserving of an in-depth analysis. While this method does not consume much space, it may require significant processing power.

Investigators focus on **two primary sources**:

- **Full-packet data capture :** This is the direct result of the "Catch it as you can" method. Large enterprises usually have large networks and it can be counterproductive for them to keep full-packet capture for prolonged periods of time anyway
- **Log files :** These are the files which reside on web servers, proxy servers, Active Directory servers, firewalls, Intrusion Detection Systems (IDS), DNS and Dynamic Host Control Protocols (DHCP). Unlike full-packet capture, logs do not take up so much space.

Database Forensics

Database forensics is a branch of digital forensics that focuses specifically on the investigation and analysis of databases to uncover evidence related to cybercrimes, security breaches, or other malicious activities. It involves the systematic examination of database systems, structures, contents, and logs to identify, preserve, analyse, and present digital evidence that may be relevant to an investigation.

The different kind of activities performed during database forensics are as under:

- **Data Collection :** The process begins with the collection of data from the database systems under investigation. This may include capturing disk images, memory dumps, transaction logs, and database backups.
- **Data Preservation :** It's crucial to preserve the integrity of the data during the forensic investigation. This involves creating forensic copies of the original data to prevent any alterations or modifications that could compromise its evidentiary value.

- **Data Analysis and Reconstruction** : Forensic analysts examine the database contents and structures to reconstruct events, transactions, and user activities that may be relevant to the investigation. This may involve examining tables, records, metadata, and transaction logs to identify anomalies, unauthorized access, or suspicious activities.

- **Timeline Analysis** : Establishing a timeline of events is essential in database forensics. Analysts correlate timestamps from database logs, transaction records, and system logs to reconstruct the sequence of activities leading up to a security incident or data breach.

- **User and Access Analysis** : Investigators analyse user accounts, permissions, and access logs to determine who had access to the database, what actions they performed, and whether any unauthorized or suspicious activities occurred.

- **Data Recovery and Reconstruction** : In cases where data has been deleted, altered, or corrupted, forensic analysts may employ specialized techniques and tools to recover and reconstruct the original data or transactional history.

- **Documentation and Reporting** : Forensic findings are documented in detail, including the methods used, analysis results, conclusions, and recommendations. A forensic report is prepared to present the findings in a clear and understandable manner, which may be used as evidence in legal proceedings.

- **Legal Considerations** : Database forensics must adhere to legal and regulatory requirements governing the handling, preservation, and admissibility of digital evidence. This may involve obtaining proper authorization, maintaining chain of custody, and ensuring compliance with relevant privacy laws and regulations.

Overall, database forensics plays a crucial role in uncovering digital evidence, identifying perpetrators, and mitigating the impact of cyber incidents on organizations. It requires a combination of technical expertise, analytical skills, and adherence to legal standards to conduct thorough and effective investigations.

Mobile Device Forensics :

The term "mobile devices" encompasses a wide array of gadgets ranging from mobile phones, smartphones, tablets, and GPS units to wearables and PDAs. What they all have in common is the fact that they can contain a lot of user information.

Mobile devices are right in the middle of three booming technological trends: Internet of Things, Cloud Computing, and Big Data.

Nowadays, mobile device use is as pervasive as it is helpful, especially in the context of digital forensics, because these small-sized machines amass huge quantities of data on a daily basis, which can be extracted to facilitate the investigation. These machines allow digitalinvestigators to glean a lot of information.

Information that resides on mobile devices :

- Incoming, outgoing, missed call history
- Phonebook or contact lists
- SMS text, application based, and multimedia messaging content
- Pictures, videos, and audio files and sometimes voicemail messages
- Internet browsing history, content, cookies, search history, analytics information
- To-do lists, notes, calendar entries, ringtones
- Documents, spreadsheets, presentation files and other user-created data
- Passwords, passcodes, swipe codes, user account credentials
- Historical geolocation data, cell phone tower related data, Wi-Fi information
- User dictionary content
- System files, usage logs, error messages
- Deleted data from all of the above

Mobile device forensics focuses on the extraction and analysis of digital evidence from smartphones, tablets, and other mobile devices. It involves the recovery of data such as call logs, text messages, multimedia files, location information, social media activity, and app usage. Mobile device forensics is particularly relevant in cases involving mobile-related crimes or when mobile devices are potential sources of evidence.

E mail Forensics

Due to the rapid spread of internet use all over the world, email has become a primary communication medium for many official activities. Not only companies, but also members of the public tend to use emails in their critical business activities such as banking, sharing official messages, and sharing confidential files. However, this communication medium has also become vulnerable to attacks.

The primary evidence in email investigations is the email header. The email header contains a considerable amount of information about the email like From, To Cc, Bcc, Subject, Date Reply-to, Message-id, References, and Received. This information becomes very vital for the email investigation activity.

Email forensics refers to analysing the source and content of emails as evidence. Investigation of email related crimes and incidents involves various approaches as discussed below.

- **Header Analysis :** Email header analysis is the primary analytical technique. This involves analysing metadata- data like sender, receiver, sending time etc. in the email header. It is evident that analysing headers helps to identify the majority of email-related crimes. Email spoofing, phishing, spam, scams and even internal data leakages can be identified by analysing the header.

- **Server Investigation :** This involves investigating copies of delivered emails and server logs. In some organizations they do provide separate email boxes for their employees by having internal mail servers. In this case, investigation involves the extraction of the entire email box related to the case and the server logs.

- **Network Device Investigation :** In some investigations, the investigator requires the logs maintained by the network devices such as routers, firewalls and switches to investigate the source of an email message. This is often a complex situation where the primary evidence is not perfect.

- **Software Embedded Analysis :** Some information about the sender of the email, attached files or documents may be included with the message by the email software used by the sender for composing the email. This information may be included in the form of custom headers or in the form of MIME content as a Transport Neutral Encapsulation Format (TNEF).

- **Sender Mail Fingerprints :** The "Received" field includes tracking information generated by mail servers that have previously handled a message, in reverse order. The "X-Mailer" or "User-Agent" field helps to identify email software. Analysing these fields helps to understand the software, and the version used by the sender.

- **Use of Email Trackers :** In some situations, attackers use different techniques and locations to generate emails. In such situations it is important to find out the geographical location of the attacker. To get the exact location of the attacker, investigators often use email tracking software embedded into the body of an Email.

When a recipient opens a message that has an email tracker attached, the investigator will be notified with the IP address and geographical location of the recipient. This technique is often used to identify suspects in murder or kidnapping cases, where the criminal communicates via email.

Malware forensics and Malware Analysis

Malware forensics is the process of examining the traces and artifacts left by malware on a compromised system or network. The goal of malware forensics is to identify the source, nature, and impact of the malware infection, and to collect evidence for legal or investigative purposes. Malware forensics typically involves acquiring and analysing disk images, memory dumps, network traffic, registry entries, logs, and other data that can reveal the malware's behaviour, origin, and targets. Malware forensics requires a thorough knowledge of operating systems, file systems, network protocols, and digital forensics tools and techniques.

Difference between Malware Forensics and Malware Analysis

Malware forensics and malware analysis are two related but distinct skills that can help you understand and counter malicious software. The differences between them are based on their goals, methods,tools and techniques used. These differences are discussed as under.

1. **Working and Objectives :** Malware analysis is the process of dissecting and understanding the inner workings of a malware sample or code. The goal of malware analysis is to determine the

functionality, capabilities, and purpose of the malware, and to find ways to detect, remove, or mitigate it. Malware analysis typically involves reverse engineering, debugging, decompiling, or disassembling the malware code, and observing its execution in a controlled environment. Malware analysis requires a solid background in programming, assembly, binary formats, and malware analysis tools and frameworks.

2. **Type of analysis method used :** One of the main differences between malware forensics and malware analysis is the type of analysis they perform: static or dynamic. Static analysis refers to examining the malware without running it, while dynamic analysis refers to observing the malware while it is running.

   Malware forensics often relies on static analysis, as it can provide valuable information about the malware's characteristics, indicators, and persistence mechanisms without risking further infection or damage. Malware analysis often uses dynamic analysis, as it can reveal the malware's behaviour, logic, and communication patterns under different conditions and inputs.

3. **Tools and Techniques used :** Another difference between malware forensics and malware analysis is the tools and techniques they use. Malware forensics uses tools such as FTK Imager, EnCase, Autopsy, Volatility, Wireshark, and RegRipper to acquire and analyze various types of data from infected systems or networks. Malware analysis uses tools such as IDA Pro, Ghidra, OllyDbg, x64dbg, Radare2, Cuckoo Sandbox, and VirusTotal to examine and manipulate malware code or samples.

4. **When they are used ?** Malware forensics is often used in response to a malware incident, such as a ransomware attack, a data breach, or a cybercrime investigation. Malware analysis is often used in research or development of malware detection or mitigation solutions, such as antivirus software, firewall rules, or threat intelligence.

5. **Outcome of the technique :** The outcome of malware forensics is to provide a comprehensive report of the incident, including the timeline, scope, impact, attribution, and recommendations for recovery and prevention. The outcome of malware analysis is to provide a detailed description of the malware's features, functions, and weaknesses, and to develop signatures, patches, or countermeasures.

Both malware forensics and malware analysis also use techniques such as hashing, signature scanning, code obfuscation, encryption, unpacking, and sandboxing to deal with different challenges and scenarios.

Software Forensics

Software forensics is a branch of science that investigates computer software text codes and binary codes in cases involving patent infringement or theft. Software forensics can be used to support evidence for legal disputes over intellectual property, patents, and trademarks.

Software forensics is especially important in patent and trade cases. In these cases, someone might have copied another person's code, but rewritten that code in a way to hide the theft.

Cloud Forensics

Cloud forensics focuses on the investigation of digital evidence stored in cloud computing environments. It involves extracting and analysing data from cloud storage, virtual machines, and other cloud-based services. Cloud forensics addresses the unique challenges of investigating data stored remotely in shared environments and requires specific expertise in handling cloud-based evidence.

Multimedia Forensics

Multimedia forensics deals with the analysis and authentication of digital images, audio recordings, video recordings, and other forms of multimedia. It involves techniques such as image analysis, video forensics, audio forensics, and steganography analysis to determine the authenticity, integrity, or origin of multimedia files.

These are just a few examples of the different types of digital forensics. Depending on the nature of the investigation and the specific digital artifacts involved, other specialized areas of digital forensics may include email forensics, social media forensics, IoT forensics, and more. Each type requires specialized tools, techniques, and expertise to effectively analyse and interpret digital evidence within its respective domain.

5.4 PHASES OF DIGITAL FORENSIC INVESTIGATION

Digital forensics, also known as **computer forensics** or **cyber forensics**, is a branch of forensic science that deals with the investigation, collection, preservation, analysis, and presentation of digital evidence.

It involves the application of scientific methods and techniques to extract and interpret information from digital devices, networks, and online platforms for legal purposes.

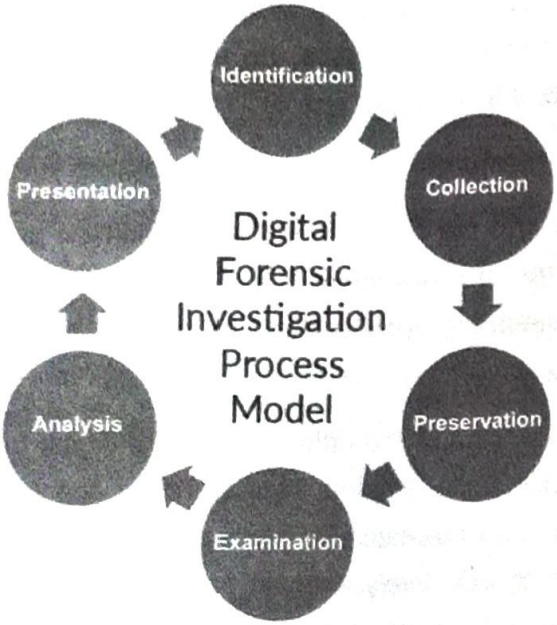
5.4.1 Objectives of Digital Forensic Investigation

The **objectives** of the Digital Forensics Investigation are as under:

- The primary goal of digital forensics is to identify, preserve, and analyse digital evidence to support investigations and legal proceedings.
- It helps to postulate the motive behind the crime and identity of the main culprit.
- Designing procedures at a suspected crime scene which helps you to ensure that the digital evidence obtained is not corrupted.
- Data acquisition and duplication: Recovering deleted files and deleted partitions from digital media to extract the evidence and validate them.
- Helps you to identify the evidence quickly, and also allows you to estimate the potential impact of the malicious activity on the victim
- Producing a computer forensic report which offers a complete report on the investigation process.
- Preserving the evidence by following the chain of custody.

5.4.2 Digital Forensic Investigation Process Model

The Digital Forensic investigation process is carried out as the model shown in the figure 5.2.



[Fig. 5.2 : Digital Forensic Investigation Process Model]

- **Identification and Collection :** The first step is to identify the purpose of investigation, identify the required resources, and to identify potential sources of digital evidence and collect relevant data from the identified sources.

  This includes to find out what evidence is present, where it is stored and lastly how it is stored. It also includes seizing and imaging digital devices, making backups, and capturing network traffic.

- **Preservation :** Digital evidence is fragile and can be easily modified or destroyed. Preservation involves taking measures to protect the integrity and original state of the evidence. So, data is isolated, secured, and preserved.

  This includes creating forensic images, hashing, and storing the evidence in a secure and controlled environment and preventing people from using the digital device so that digital evidence is not tampered with.

- **Analysis :** In this phase, the collected digital evidence is analysed using specialized tools and techniques. This can involve recovering deleted files, examining system logs, analysing network traffic, decrypting encrypted data, and reconstructing digital activities to establish a timeline of events.

- **Examination (Interpretation) :** The analysis results are interpreted to draw conclusions and establish the significance of the evidence. This includes identifying relevant information, establishing links between different pieces of evidence, and identifying potential suspects or leads.

- **Presentation (Documentation and Reporting) :** A comprehensive report is prepared detailing the findings of the investigation. This report is often presented in a clear and concise manner to assist legal professionals, law enforcement agencies, or other stakeholders in understanding the technical aspects of the case.

Digital forensics plays a crucial role in modern criminal investigations and is often relied upon in legal proceedings. It helps in identifying perpetrators, proving guilt or innocence, recovering lost or deleted data, protecting digital evidence from tampering, and enhancing the overall integrity of the justice system in the digital age.

It requires specialized knowledge, skills, and tools to ensure accurate and reliable results. Forensic investigators need to stay updated with the latest technologies, encryption methods, and forensic techniques to address the ever-evolving landscape of digital crimes.

5.5 METHOS TO PRESERVE DIGITAL EVIDENCE

5.5.1 Why Should We Preserve Digital Evidence ?

One of the greatest drawbacks of Locard's exchange theory lies in evidence dynamics. But there are many factors that can lead to the tampering and destruction of evidence.

- Staging (manipulation of objects in crime scene) by the offender
- Secondary transfer of evidence
- Actions of the victim before the crime
- Witness actions
- Natural factors like animal or insect activity, weather, decomposition.
- Fire suppression efforts
- Actions of police, scene technicians and medical personnel.

These factors can lead to the removal or obliteration of the evidence. They can often mislead the investigators and cause problems with crime reconstruction. Misinterpretations or misleading evidence can lead to inaccurate crime reconstruction. To avoid this there is a need to preserve the digital evidence. Due to this fundamental importance of digital evidence preservation, it is necessary to preserve digital evidences in well-structured manner.

5.5.2 Digital Evidence Preservation Methods

In this section, we'll go over three techniques that forensics specialists might employ to protect any evidence before the analysis process begins.

Drive Imaging

Forensic investigators must first produce an image of the evidence before they can start examining it from a source. A forensic procedure called "drive imaging" involves an analyst making a bit-by-bit copy of the original disk.

The following considerations should be made by forensic professionals when examining an image:

- It is possible for crucial and recoverable data to remain on even erased drives.

- Using forensic procedures, experts in the field of forensics can recover all erased files.
- Never examine the original media through forensic examination. Utilize the duplicate image for all operations.

Forensic investigators should construct the image for analysis using a "write blocker," which is a piece of hardware or software that aids in the forensic image's legal defensibility.

Hash Values

Cryptographic hash values such as MD5, SHA1, and others are produced when a forensic investigator prepares a picture of the evidence for analysis. Hash values are important because:

- They are used to confirm that the image is an exact reproduction of the source media and that it is authentic and intact.
- Hashing values are essential when introducing evidence in court since even the smallest change to the data will result in an entirely new hash value.
- A new hash value is generated for any modifications you make to a file on your computer, such as adding new content or changing an already-existing one.
- Analysts can use specialized software to obtain information that is not available in a standard file explorer window, such as the hash value and other file metadata.

In court, it could be questioned whether the evidence was tampered with if the hash values of the image and the original evidence do not match.

Chain of Custody

When forensic investigators gather and transfer media from the client, they should record all actions taken throughout the transfer of media and evidence on Chain of Custody (CoC) forms. They should also get signatures, the time and date of the media handoff. For the following reasons, completing CoC paperwork is imperative:

- The Certificate of Consistency (CoC) serves as proof that the image has been in known possession since its creation.
- A breach in the CoC renders the image's legal value and the analysis it contains void.
- It is troublesome if there are any gaps in the procession record, such as instances where the evidence was left unsupervised in an unguarded area or in plain sight.

5.5.3 Issues with Maintaining Digital Evidence

Some of the issues that arise with preserving evidence are as under.

- **Legal Admissibility**

  This poses the greatest risk. Digital media evidence should be placed under the CoC right away and quarantined if it is a piece of criminal evidence; an investigator can subsequently make an image.

- **Evidence Destruction**

  Future forensic analysis will depend on the program remaining accessible and not being removed from the system in the event that threat actors have installed an application on a server.

- **Media is still in Service?**

  If so, the longer it has been since the occurrence, the greater the chance is that important evidence will be destroyed.

5.6 CRITICAL STEPS IN PRESERVING DIDITAL EVIDENCE

Misinterpretations or misleading evidence can lead to inaccurate crime reconstruction. So, we need to follow a series of steps in order to preserve digital evidence, as even a small inattentive move could lead to a loss of evidence and the break of a case.

5.6.1 Critical Steps in Preserving Digital Evidence

This section will cover the essential actions that must be taken in order to prevent digital evidence loss before delivering the it to the forensic specialists. When it comes to digital evidence preservation, time is crucial.

1. **Do not change the current state of the device :** If the device is OFF, it must be kept OFF and if the device is ON, it must be kept ON. Call a forensics expert before doing anything.
2. **Power down the device :** In the case of mobile phones, If it is not charged, do not charge it. In case, the mobile phone is ON power it down to prevent any data wiping or data overwriting due to automatic booting.
3. **Do not leave the device in an open area or unsecured place :** Ensure that the device is not left unattended in an open area or unsecured area. You need to document things like- where the device is, who has access to the device, and when it is moved.
4. **Do not plug any external storage media in the device :** Memory cards, USB thumb drives, or any other storage media that you might have, should not be plugged into the device.
5. **Do not copy anything to or from the device :** Copying anything to or from the device will cause changes in the slack space of the memory.
6. **Take a picture of the piece of the evidence :** Ensure to take the picture of the evidence from all the sides. If it is a mobile phone, capture pictures from all the sides, to ensure the device has not tampered till the time forensic experts arrive.
7. **Make sure you know the PIN/ Password Pattern of the device :** It is very important for you to know the login credentials of the device and share it with the forensic experts, for them to carry their job seamlessly.
8. **Do not open anything like pictures, applications, or files on the device :** Opening any application, file, or picture on the device may cause losing the data or memory being overwritten

9. **Do not trust anyone without forensics training :** Only a certified Forensics expert should be allowed to investigate or view the files on the original device. Untrained Persons may cause the deletion of data or the corruption of important information.

10. **Make sure you do not Shut down the computer, If required Hibernate it :** Since the digital evidence can be extracted from both the disk drives and the volatile memory. Hibernation mode will preserve the contents of the volatile memory until the next system boot.

5.6.2 Key Points to Remember to Speed Up Preserving Evidence

For the evidence to be professionally acquired by forensics investigators, the device is either seized or a forensic copy is created at the site of the "crime" scene.

The important key points to remember to speed up the process of preserving digital evidence and ease out the process for the authorities:

- Prepare yourself to share your authentication codes like screen patterns and passwords.
- You may also need to share the device manuals, chargers, cables.
- Device interactions will the Internet can also be analysed to build a complete and most appropriate picture of overall activity.
- Have ownership of the device that you plan to submit to the police. In case you do not have the authority or you're not voluntarily submitting the device, then, in that case, Police may need to seize the device under their lawful powers.
- It is easier to share external memory storage than your devices with the police instead of giving your phone away every time, so it is recommended that you have an external memory configured for your phone.
- Regularly back-up your phone data and retain copies of these back-ups for future use. These will help you restore another handset or your phone if needs be at a later today, and also can help to log a trail of incidence.

5.7 ROLE OF DEVICES AS EVIDENCE IN DIGITAL FORENSICS

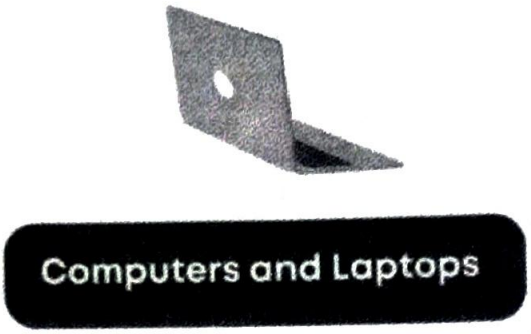
Digital forensic investigators must be adept at extracting evidence from an array of devices, each with unique structures, operating systems, storage capabilities, and security features. A case involving a desktop computer, for example, may require an understanding of operating systems, file systems, and data recovery techniques. Conversely, a case involving a smartphone may call for expertise in mobile operating systems, encryption, GPS technologies, and app data extraction. In network or cloud-based investigations, understanding data transmission, network protocols, cloud architectures, and multi-tenancy environments becomes critical. Thus, the device or system at the centre of the investigation often shapes the strategy and methodologies employed by the investigators.

5.7.1 Types of Devices

Digital forensics is not a single-size-fits-all discipline; it branches out into several areas, each addressing a specific kind of device or system. Some of them are as discussed under.

Computing Devices (Computers and laptops) :

Data preservation is the first step in computer forensics, and it is accomplished by making a forensic image of the system's storage devices. To guarantee data integrity, this procedure is usually carried out with the use of a write-blocking device. Next, the forensic picture is examined for files (both deleted and present), surfing history, email conversations, system logs, information (such as timestamps and file ownership), and metadata. These components may offer vital proof of the ownership, usage, and intent of the gadget.



[Fig. 5.3 : Computing Devices Forensics]

The main sources of difficulty in computer forensics are anti-forensic methods and encryption. Full-disk encryption is a common feature of modern computers that might keep investigators from accessing the data if they don't have the right encryption key.

Anti-forensic techniques, such as data wiping, data hiding, and obfuscation, can also be employed to complicate the investigation. Tools and strategies such as file carving, keyword searching, and hash comparison can help overcome these challenges.

Network Devices and Servers

Network forensics focuses on monitoring and analysing network traffic. Investigators can capture network packets in real-time or from saved logs, using tools like Wireshark or tcpdump. Analysing these packets can reveal suspicious activities, data exfiltration, or malicious network anomalies. Network devices also store log files, providing a record of network events, while servers may contain user data, website logs, and databases.

Network Devices and Servers

- Log files
- Network traffic
- Configuration files
- User account information
- System artifacts

[Fig. 5.4 : Networking Devices Forensics]

Tracking and attributing network activities to specific individuals can be challenging due to network address translation (NAT), proxies, VPNs, or anonymizing networks like Tor. Another challenge is dealing with the high volume of data and isolating relevant information. Furthermore, evidence might be distributed across multiple devices in the network, requiring synchronized investigation.

CCTVs

Video recordings, access logs, and configuration information are all available from closed-circuit television systems. Forensic specialists usually obtain information by taking off the hard drive from the CCTV system's Digital Video Recorder (DVR) and creating an Image.

Closed-Circuit Television Systems (CCTVs)

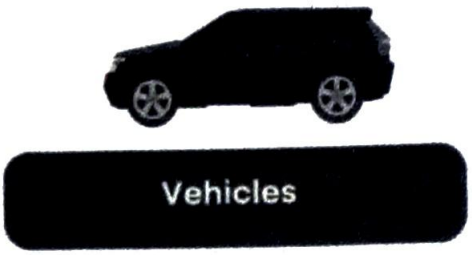
- Video footage
- System configuration
- Log files
- Timestamps and metadata
- Motion detection and alerts

[Fig. 5.5 : CCTV Forensics]

CCTV systems come with their own set of difficulties. For example, video footage is frequently recorded again and over again, making it more difficult to access older data. It may require sophisticated methods to retrieve overwritten or erased video. Moreover, video footage processing and analysis can take a long time, particularly in high-resolution systems where large amounts of data may be involved.

Automobiles:

Several onboard computers, referred to as Electronic Control Units (ECUs), are installed in modern cars and are in charge of multiple operations, including engine control, navigation, communications, and more. A portion of them, known as Event Data Recorders (EDRs), are able to offer vital event data before to, during, and following a collision, such as vehicle speed, brake application, airbag deployment, and seatbelt usage.



[Fig. 5.6 : Vehicle Forensics]

In order to interface with these ECUs via the onboard diagnostics (OBD) port and other interfaces and understand the data that is collected, vehicle forensics requires specialist tools. The process is made much more difficult by the fact that these car systems are proprietary and there are many different manufacturers and models. For security reasons, a lot of car systems encrypt communications as well, which makes forensic extraction difficult.

Other than above discussed devices some other devices are also there like Smartphones and Tablets, Internet of Things (IoT) Devices, Wearables, Drones, Medical Devices, Device Memory, Gaming Consoles, Cloud Storage.

With the varied types of devices and systems involved in digital forensic investigations, a singular approach often proves insufficient. A more encompassing, holistic approach is necessary to conduct an effective and thorough investigation. This involves considering all the digital devices and systems relevant to the case and understanding how data from each device contributes to the overall picture.

Self - Assessment

Q. 1 Answer the below short questions :

(1) What is Digital Forensic? List out information we collect by digital forensics.

(2) List out the examples of Digital Forensics uses.

(3) Write down Locard's principle of exchange in Digital Forensics.

(4) Write down limitations of Locard's principle of exchange.

(5) List out classification of trace evidence.

(6) Write down various branches of Digital Forensics.

(7) Write down objectives of Digital Forensic investigation.

(8) List out various phases of Digital Forensic Investigation process model.

(9) Why should we preserve Digital Evidence? List out three methods for preserving Digital Evidence.

(10) Write down issues which arise for maintaining Digital Evidence.

(11) List out essential actions which require to preserve Digital Evidence.

(12) List out points which be remembered to speed up the evidence preserving process.

(13) Write down the devices which play important role in Digital Forensic investigation.

Q 2. Answer the below long questions:

(1) What is Digital Forensic? Explain in detail with advantages and disadvantages.

(2) Explain Locard's principle of Digital Forensic with suitable example.

(3) Write down Locard's principle of Exchange in Forensic Science. Explain how it can be applied to Digital Forensics.

(4) Explain the Limitations of Locard's Principle of exchange.

(5) List out various branches of Digital Forensics. Explain Computer Forensics and memory Forensics in detail.

(6) Explain Network Forensics and Database Forensics in detail.

(7) Explain Mobile Device Forensics and E mail Forensics in detail.

(8) Explain Digital Forensics Investigation process model in detail.

(9) Why should we preserve Digital forensic evidence? Explain methods for evidence preservation.

(10) Explain essential actions which require to preserve Digital Evidence.

(11) Explain points which be remembered to speed up the evidence preserving process.

(12) Explain devices which play important role in Digital Forensic investigation.

★★★

Multiple Choice Questions (MCQs)

CHAPTER 1

INTRODUCTION OF INFORMATION SECURITY AND CRYPTOGRAPHY

1. What is the primary goal of information security ?

(A) Confidentiality (B) Integrity (C) Availability (D) All of the above

Ans. (D) All of the above

2. Which of the following is an example of a symmetric encryption algorithm ?

(A) RSA (B) AES (C) Diffie-Hellman (D) ECC

Ans. (B) AES

3. Which cryptographic hash function is commonly used for the purpose of password hashing ?

(A) MD5 (B) SHA-1 (C) SHA-256 (D) DES

Ans. (C) SHA-256

4. Which of the following is not a fundamental principle of information security ?

(A) Availability (B) Accessibility (C) Confidentiality (D) Integrity

Ans. (B) Accessibility

5. What does CIA stand for in the context of information security ?

(A) Central Intelligence Agency (B) Computer Incident Assessment

(C) Confidentiality, Integrity, Availability (D) Cybernetic Intrusion Assessment

Ans. (C) Confidentiality, Integrity, Availability

6. Which encryption algorithm is commonly used for secure communication over the internet ?

(A) DES (B) RSA (C) MD5 (D) Caesar cipher

Ans. (B) RSA

7. What is the primary purpose of a message digest in cryptography ?

(A) To encrypt messages (B) To compress messages

(C) To provide message integrity (D) To authenticate messages

Ans. (C) To provide message integrity

8. Which of the following is a characteristic of a cryptographic hash function?

(A) It is reversible (B) It produces a fixed-size output

(C) It requires a secret key for operation (D) It can be decrypted using a public key

Ans. (B) It produces a fixed-size output

9. Which cryptographic property ensures that a small change in the input to a hash function produces a significantly different output ?

(A) Collision resistance (B) Pre-image resistance

(C) Avalanche effect (D) Birthday paradox

Ans. (C) Avalanche effect

10. Which of the following is NOT a potential use case for cryptographic hash functions ?

(A) Password hashing (B) Digital signatures

(C) Data compression (D) Blockchain technology

Ans. (C) Data compression

CHAPTER 2

NETWORK AND SYSTEM SECURITY

1. What is the primary purpose of PGP ?

(A) Secure file transfer (B) Data compression

(C) Email encryption and digital signatures (D) Firewall protection

Ans. (C) Email encryption and digital signatures

2. Which attack involves tricking individuals into revealing sensitive information or performing actions through psychological manipulation ?

(A) Brute force attack (B) Social engineering attack

(C) SQL injection attack (D) Cross-Site Scripting (XSS) attack

Ans. (B) Social engineering attack

3. What is the primary purpose of SSL ?

(A) Encrypting email messages (B) Securing web communication

(C) Managing network traffic (D) Protecting databases

Ans. (B) Securing web communication

4. What is the primary purpose of a digital signature ?

(A) To encrypt the contents of a message

(B) To provide confidentiality to a digital document

(C) To ensure the identity of the sender

(D) To ensure authenticity and integrity of a digital document or message

Ans. (D) To ensure authenticity and integrity of a digital document or message

5. Which cryptographic key is used to create a digital signature ?

(A) Public key (B) Private key (C) Session key (D) Master key

Ans. (B) Private key

6. What does PGP stand for in the context of computer security?

(A) Public Gateway Protocol (B) Pretty Good Privacy

(C) Private Graphical Protocol (D) Protected Group Policy

Ans. (B) Pretty Good Privacy

7. What type of attack floods a network or system with excessive traffic, rendering it unavailable to legitimate users?

(A) Malware attack
(B) Phishing attack
(C) Denial-of-Service (DoS) attack
(D) Man-in-the-Middle (MitM) attack

Ans. (C) Denial-of-Service (DoS) attack

8. What type of attack injects malicious scripts into web pages viewed by other users, potentially stealing sensitive information?

(A) Brute force attack
(B) Social engineering attack
(C) SQL injection attack
(D) Cross-Site Scripting (XSS) attack

Ans. (D) Cross-Site Scripting (XSS) attack

9. Which firewall type inspects each packet passing through the firewall and accepts or rejects it based on predefined rules ?

(A) Stateful inspection firewall
(B) Proxy firewall
(C) Packet-filtering firewall
(D) Next-generation firewall

Ans. (C) Packet-filtering firewall

10. Which firewall type acts as an intermediary between internal and external networks, handling requests on behalf of clients ?

(A) Packet-filtering firewall
(B) Stateful inspection firewall
(C) Proxy firewall
(D) Next-generation firewall

Ans. (C) Proxy firewall

CHAPTER 3

CYBER CRIME

1. What is email bombing in the context of cybersecurity ?

(A) A technique to send a large volume of emails to a target system
(B) A method to encrypt email messages for secure transmission
(C) An approach to authenticate email servers
(D) A strategy to filter spam emails

Ans. (A) A technique to send a large volume of emails to a target system

2. What is the primary objective of a DDoS attack ?

(A) To steal sensitive information
(B) To gain unauthorized access to a system
(C) To overwhelm server resources and disrupt services
(D) To encrypt network traffic

Ans. (C) To overwhelm server resources and disrupt services

3. What is phishing in the context of cybersecurity ?
   (A) A technique to encrypt sensitive data during transmission
   (B) A method to secure network communication
   (C) An attack for tricking individuals into revealing sensitive information
   (D) A process to authenticate email servers

Ans. (C) An attack for tricking individuals into revealing sensitive information

4. Which encryption protocol can help prevent unauthorized access to website content during transmission?
   (A) HTTP (Hypertext Transfer Protocol)
   (B) FTP (File Transfer Protocol)
   (C) SSL/TLS (Secure Sockets Layer/Transport Layer Security)
   (D) SMTP (Simple Mail Transfer Protocol)

Ans. (C) SSL/TLS (Secure Sockets Layer/Transport Layer Security)

5. What is web jacking in the context of cybersecurity ?
   (A) A technique to hijack web servers and host malicious content
   (B) An attack that redirects users to fraudulent websites
   (C) A method to steal sensitive information from web applications
   (D) An attack that takes control of a website's domain or content

Ans. (D) An attack that takes control of a website's domain or content

6. What is the purpose of anti-phishing software ?
   (A) To encrypt email messages for secure transmission
   (B) To prevent unsolicited commercial emails
   (C) To detect and block phishing emails and websites
   (D) To improve network performance

Ans. (C) To detect and block phishing emails and websites

7. What is credit card fraud ?
   (A) A legitimate transaction conducted with a credit card
   (B) Fraudulent use of a credit card or its information for financial gain
   (C) The process of securely storing credit card information
   (D) A type of insurance provided by credit card companies

Ans. (B) Fraudulent use of a credit card or its information for financial gain

8. What is card skimming in the context of credit card fraud ?
   (A) A method of duplicating physical credit cards
   (B) Sending unsolicited emails to obtain credit card information
   (C) Intercepting communication between a user and a payment gateway
   (D) Creating fake websites to trick users into entering credit card details

Ans. (A) A method of duplicating physical credit cards

9. What does Section 65 of the IT Act, 2008, primarily address?

(A) Cyberbullying offenses

(B) Unauthorized access to computer systems

(C) Offenses related to tampering with computer source documents

(D) Data privacy violations

Ans. (C) Offenses related to tampering with computer source documents

10. What is the punishment prescribed under Section 65 of the IT Act, 2008, for offenses related to tampering with computer source documents?

(A) Imprisonment for up to 3 years or a fine of up to Rs. 2,00,000, or both

(B) Imprisonment for up to 5 years or a fine of up to Rs. 5,00,000, or both

(C) Imprisonment for up to 7 years or a fine of up to Rs. 10,00,000, or both

(D) Imprisonment for up to 2 years or a fine of up to Rs. 1,00,000, or both

Ans. (A) Imprisonment for up to 3 years or a fine of up to Rs. 2,00,000, or both

11. What is the primary focus of Section 66 of the IT Act, 2008 ?

(A) Unauthorized access to computer systems

(B) Protection of digital signatures

(C) Offenses related to hacking and computer data theft

(D) Regulation of electronic commerce

Ans. (C) Offenses related to hacking and computer data theft

CHAPTER 4

ETHICAL HACKING

1. What is the primary goal of an ethical hacker ?

(A) To cause harm to computer systems

(B) To gain unauthorized access to sensitive information

(C) To identify and remediate security vulnerabilities

(D) To create chaos in the digital environment

Ans. (C) To identify and remediate security vulnerabilities

2. Which type of hacker is also known as a "white hat" hacker ?

(A) Black hat hacker

(B) Gray hat hacker

(C) Script kiddie

(D) Ethical hacker

Ans. (D) Ethical hacker

3. Which of the following is a penetration testing tool included in Kali Linux ?

(A) Adobe Photoshop (B) Microsoft Word

(C) Wireshark (D) Mozilla Firefox

Ans. (C) Wireshark

4. What is the default username and password for Kali Linux ?

(A) Username: kali, Password: toor (B) Username: root, Password: kali

(C) Username: admin, Password: admin (D) Username: user, Password: password

Ans. (A) Username: kali, Password: toor

5. Which of the following is an example of a password hashing algorithm used for password storage ?

(A) MD5 (Message Digest Algorithm 5) (B) DES (Data Encryption Standard)

(C) ROT13 (Rotate by 13 places) (D) Base64 encoding

Ans. (A) MD5 (Message Digest Algorithm 5)

6. What is password cracking ?

(A) Generating complex passwords for security purposes

(B) Recovering lost passwords from encrypted files

(C) Creating new passwords using machine learning algorithms

(D) Illegally accessing password databases

Ans. (B) Recovering lost passwords from encrypted files

7. What is an injection attack in the context of cybersecurity?

(A) Injecting physical devices into computer systems

(B) Injecting malware into network traffic

(C) Injecting malicious code or commands into input fields or data streams

(D) Injecting cryptographic keys into encryption algorithms

Ans. (C) Injecting malicious code or commands into input fields or data streams

8. Which of the following is a defence mechanism against SQL injection attacks ?

(A) Input validation and sanitization

(B) Enforcing weak password policies

(C) Disabling firewalls

(D) Ignoring security warnings from web browsers

Ans. (A) Input validation and sanitization

9. Which of the following is NOT a feature of RAT tools?

(A) Keylogging (B) Screen capturing

(C) File encryption (D) Webcam hijacking

Ans. (C) File encryption

10. Which of the following is an example of a well-known RAT tool ?

(A) BitTorrent (B) TeamViewer

(C) Adobe Photoshop (D) VLC Media Player

Ans. (B) TeamViewer

11. What is a Remote Access Trojan (RAT) tool primarily used for ?

(A) Automated testing of network vulnerabilities

(B) Monitoring network traffic for security threats

(C) Remotely controlling and accessing compromised systems

(D) Encrypting sensitive data during transmission

Ans. (C) Remotely controlling and accessing compromised systems

CHAPTER 5

DIGITAL FORENSICS

1. What is digital forensics primarily concerned with ?

(A) Recovering lost data from physical storage devices

(B) Investigating crimes involving digital devices and data

(C) Creating backups of important files and documents

(D) Preventing cyber-attacks on network infrastructure

Ans. (B) Investigating crimes involving digital devices and data

2. What is the first step in the digital forensic process ?

(A) Analysis (B) Collection (C) Examination (D) Reporting

Ans. (B) Collection

3. What is steganography in the context of digital forensics ?

(A) The study of cryptographic algorithms

(B) The practice of hiding data within other data

(C) The process of recovering deleted files

(D) The examination of digital artifacts

Ans. (B) The practice of hiding data within other data

4. Which of the following types of information can be obtained through memory forensics ?

(A) Recently deleted files

(B) Internet browsing history

(C) Running processes and open network connections

(D) Encrypted email messages

Ans. (C) Running processes and open network connections

5. Which of the following best describes Locard's Exchange Principle ?

(A) "Every contact leaves a trace."

(B) "Evidence is the key to solving crimes."

(C) "Criminals always return to the scene of the crime."

(D) "The guilty party will always confess under interrogation."

Ans. (A) "Every contact leaves a trace."

6. What is the difference between static and live digital forensics analysis ?

(A) Static analysis involves examining data in real-time, while live analysis involves analysing archived data.

(B) Static analysis involves analysing data stored on physical devices, while live analysis involves examining data in volatile memory.

(C) Static analysis is conducted by law enforcement agencies, while live analysis is performed by private investigators.

(D) Static analysis is more time-consuming than live analysis.

Ans. (B) Static analysis involves analysing data stored on physical devices, while live analysis involves examining data in volatile memory.

7. What is the purpose of creating a forensic image of digital evidence ?

(A) To delete unnecessary files

(B) To encrypt the evidence for security

(C) To preserve the original state of the evidence

(D) To share evidence across multiple platforms

Ans. (C) To preserve the original state of the evidence

8. Which of the following devices is commonly used in digital forensics for data acquisition?

(A) USB mouse (B) External hard drive

(C) Laser printer (D) Webcam

Ans. (B) External hard drive

9. Which of the following devices is often used for creating forensic images of storage media ?

(A) USB flash drive (B) CD-ROM drive

(C) Write-blocking device (D) Forensic imaging tool

Ans. (D) Forensic imaging tool

10. Which of the following is an example of volatile digital evidence ?

(A) Hard disk drive (B) Random access memory (RAM)

(C) Solid-state drive (SSD) (D) Optical disc

Ans. (B) Random access memory (RAM)

★★★

Seat No. : _____ Enrolment No. _____

Subject Code : 4361601 **Date :**

Subject Name : CYBER SECURITY AND DIGITAL FORENSICS

Time : **Total Marks : 30**

Instructions :

1. **Attempt all questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**

MODEL QUESTION PAPERS-1

		Marks	CO (Course Outcome)
Q. 1	**(a)** Explain fundamental goals of Information Security.	**03**	**COa**
	(b) Explain Hashing with its working diagram and list out applications of Hashing.	**07**	**COa**
Q. 2	**(a)** Differentiate: Active Attack V/s Passive Attack	**03**	**COb**
	(b) Write a short note on Digital Signature.	**07**	**COb**
	OR		
	(b) What is firewall? Explain Packet filtering firewall with its working in detail.	**07**	**COb**
Q. 3	**(a)** Differentiate: Symmetric Cryptography V/s Asymmetric Cryptography.	**03**	**COa**
	(b) Explain e mail bombing in detail	**07**	**COc**
	OR		
Q. 3	**(a)** What is Virus? Explain with its lifecycle and types.	**03**	**COb**
	(b) Explain DOS Attack and DDOS attack with differentiation.	**07**	**COc**

***

Seat No. : _____ Enrolment No. _____

Subject Code : 4361601 **Date :**

Subject Name : CYBER SECURITY AND DIGITAL FORENSICS

Time : **Total Marks : 30**

Instructions :

1. **Attempt all questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**

MODEL QUESTION PAPERS-2

		Marks	CO (Course Outcome)
Q.1	**(a)** Explain Section 65 in brief.	**03**	**COc**
	(b) Explain challenges and preventions of Cybercrime.	**07**	**COc**
Q.2	**(a)** What is hacking? Explain various types of hacking.	**03**	**COd**
	(b) What is SQL Injection Attack? Explain with one simple example.	**07**	**COd**
	OR		
	(b) What is phishing? Explain different types of phishing attacks.	**07**	**COd**
Q.3	**(a)** What is Digital Forensics? List out its advantages and Disadvantages.	**03**	**COe**
	(b) Explain Digital Forensic Investigation method in detail.	**07**	**COe**
	OR		
Q.3	**(a)** Differentiate: Malware Forensics V/s Malware Analysis.	**03**	**COe**
	(b) Explain Digital Evidence preservation methods in detail.	**07**	**COe**

★★★