UNIT 1. NEED FOR SECURING A NETWORK

A network means computers, mobiles, servers connected together (like internet, office LAN, Wi-Fi).

Why security is needed?

1. *Protect personal data* – passwords, bank details, Aadhaar, photos
2. *Prevent hacking* – unauthorized access
3. *Avoid financial loss* – online fraud, UPI scams
4. *Ensure privacy* – emails, chats should remain private
5. *Maintain trust* – banks, hospitals, govt websites must be safe

Example:
If a college Wi-Fi is not secure, a hacker can steal students' login IDs and marks.

2. Principles of Security (CIA Triad)

These are the basic rules of cyber security:

A. Confidentiality

- Information should be seen only by authorized persons.
- Achieved by passwords, encryption.

Example:
Only you can read your Gmail because it is password protected.

B. Integrity

- Data should not be changed without permission.

Example:
Marks stored in school database should not be altered by students.

C. Availability

- Information should be available when needed.

Example:
ATM servers should work 24×7.

3. Types of Cyber Attacks

A. Malware Attack

Malicious software like virus, worm, trojan.

Example:
Downloading pirated software installs a virus.

B. Phishing

Fake emails/messages to steal information.

Example:
"You won ₹10 lakh – click here" message.

C. Denial of Service (DoS)

Overloading a website so it stops working.

Example:
Government website crashes during form submission.

D. Man-in-the-Middle Attack

Attacker secretly listens to communication.

Example:
Using public Wi-Fi in a café to steal login details.

4. Introduction to Cyber Crime

Cyber crime means crime done using computer, mobile or internet.

Examples:

- Online fraud
- Hacking bank accounts
- Identity theft
- Cyber bullying
- Spreading fake news

Example:
Someone creates a fake Instagram account in your name.

5. Cyber Law – Indian Perspective

A. IT Act, 2000

India's main cyber law. Provides:

- Legal recognition to e-documents and e-signatures
- Punishment for cyber crimes

B. IT Act Amendment, 2008

Added:

- Data protection
- Cyber terrorism laws
- Stronger punishment

Important Sections:

- Section 43 – damage to computer system
- Section 66 – hacking and fraud
- Section 66F – cyber terrorism

Example:
Hacking a government website can lead to jail and fine.

6. Cyber Ethics

Ethics means moral rules for using internet.

Good Cyber Ethics:

1. Do not hack accounts
2. Do not spread fake news
3. Respect privacy
4. Do not download pirated content

Example:
Not forwarding fake WhatsApp messages.

7. Ethical Hacking

Ethical hacking means legal hacking with permission to find security problems.

Ethical Hacker:

- Works for companies
- Finds weaknesses
- Improves security

Example:
Banks hire ethical hackers to test ATM security.

8. Hacking

Hacking means gaining unauthorized access to systems.

Types:

- White Hat – ethical hacker
- Black Hat – criminal hacker
- Grey Hat – between both

Example:
Breaking into someone's Facebook account.

9. Skimming

Stealing card information using a skimming device.

Example:
ATM card details copied secretly and money withdrawn.

10. Attacker

A person who tries to break security.

Example:
Someone trying multiple passwords to open your email.

11. Phreaker

Person who hacks telephone systems.

Example:
Making free international calls illegally.

12. Hacktivist

Hacker who hacks for political or social cause.

Example:
Defacing a website to protest against government policy.

13. Bluejacking

Sending unwanted messages using Bluetooth.

Example:
Stranger sending messages on your phone in a bus via Bluetooth.

14. Bluesnarfing

Stealing data using Bluetooth without permission.

Example:
Stealing contacts or photos from phone via Bluetooth.

15. iOS Jailbreaking

Removing Apple's restrictions from iPhone.

Purpose:

- Install unauthorized apps
- Customize phone

Risk:

- Security threats
- Warranty loss

Example:
Installing paid apps for free after jailbreaking.

📌 **Quick Exam Tip:**

- Write definition + 1 example
- Use headings & points
- Mention IT Act 2000 & 2008 clearly

This file contains all topics in one document, written in simple layman / Class 12 level language with examples, suitable for:

- Exams
- Quick revision
- Printing or sharing

If you want:

- more examples added,

Introduction to Encryption and Decryption

A. Encryption

Encryption means converting readable data (plain text) into secret code (cipher text) so that no unauthorized person can understand it.

Example:
Message: HELLO
Encrypted form: X7#@9

B. Decryption

Decryption means converting encrypted data back to original form using a key.

Example:
Cipher text X7#@9 → Decrypted to HELLO

Cryptography

Cryptography is the science of securing information using mathematical techniques.

Symmetric Key Cryptography

- Same key is used for encryption and decryption.
- Fast but less secure if key is stolen.

Example:
ATM PIN system
Wi-Fi password

Advantages:

- Fast processing
- Simple

Disadvantages:

- Key sharing is risky

Asymmetric Key Cryptography

- Uses two keys:
    - Public Key (shared)
    - Private Key (secret)

Example:
Email encryption
Digital signatures

Advantages:

- More secure
- No need to share private key

Disadvantages:

- Slower than symmetric encryption

Encryption Algorithms

DES (Data Encryption Standard)

- Symmetric key algorithm
- Uses 56-bit key
- Now considered weak and outdated

Example:
Earlier used in banking systems.

RSA (Rivest–Shamir–Adleman)

- Asymmetric key algorithm
- Uses public & private keys
- Very secure

Example:
Secure email
Online banking login

PGP (Pretty Good Privacy)

- Used for email security

- Combines:
    - Symmetric encryption
    - Asymmetric encryption
    - Hashing

Example:
Secure communication between two people via email.

Introduction to Hashing

Hashing

- Converts data into fixed-length value
- One-way process (cannot be reversed)

Example:
Passwords stored in encrypted form on websites.

MD5 (Message Digest 5)

- Produces 128-bit hash value
- Fast but not secure now

Example:
Earlier used to store passwords.

Secure Communication Protocols

SSL (Secure Socket Layer)

- Encrypts data between browser and server
- Old version of HTTPS

Example:
Online shopping websites.

SSH (Secure Shell)

- Secure way to log into remote computers
- Used by system administrators

Example:
Accessing a server remotely.

HTTPS (Hyper Text Transfer Protocol Secure)

- Secure version of HTTP
- Uses SSL/TLS encryption

Example:
https://www.bank.com

Digital Signature

- Used to verify sender's identity
- Ensures:
    - Authentication
    - Integrity
    - Non-repudiation

Example:
Signing online government documents.

Digital Certificate

- Issued by Certificate Authority (CA)
- Proves website identity

Example:
SSL certificate for e-commerce websites.

IPSec (Internet Protocol Security)

- Provides security at network layer
- Used in VPNs

Example:
Secure office network connection from home.

Quick Revision Table

Term	Meaning
Encryption	Convert data into secret code
Decryption	Convert code into original data
Symmetric	One key
Asymmetric	Two keys
Hashing	One-way encryption
Digital Signature	Verify sender
HTTPS	Secure website

Unit 2. SECURING DATA OVER INTERNET – NOTES

1. Introduction

- Internet is not fully secure
- Data can be:
    - Stolen
    - Modified
    - Misused

data ko secure (safe) banana zaroori hai

- Security is achieved using:
    - Encryption
    - Hashing
    - Secure protocols

2. Encryption and Decryption

Encryption

- Process of converting plain text → secret code (cipher text)
- Makes data unreadable to hackers

Decryption

- Process of converting cipher text → original text

Example:
"HELLO" → (Encryption) → "XJH45"
"XJH45" → (Decryption) → "HELLO"

3. Types of Cryptography

(a) Symmetric Key Cryptography

- Same key used for:
    - Encryption
    - Decryption

Features:

- Fast
- Simple
- Key must be kept secret

Example: Password protected ZIP file

(b) Asymmetric Key Cryptography

- Uses two keys:
    - Public key (shared)
    - Private key (secret)

Features:

- More secure
- Used in internet security

Example: Online banking

4. Overview of Algorithms

(a) DES (Data Encryption Standard)

- Symmetric key algorithm
- Uses 56-bit key
- Old method (less secure now)

(b) RSA

- Asymmetric algorithm
- Uses public + private key
- Widely used for:
    - Secure communication
    - Digital signatures

(c) PGP (Pretty Good Privacy)

- Used for email security
- Combines:
    - Symmetric + Asymmetric encryption

5. Hashing

- Converts data into fixed-length code (hash value)
- Cannot be reversed

Used for:

- Password storage
- Data integrity

MD5

- Produces 128-bit hash
- Fast but now less secure

6. Secure Protocols

SSL (Secure Socket Layer)

- Provides secure communication
- Encrypts data between client and server

SSH (Secure Shell)

- Used for secure remote login
- Protects data during transfer

HTTPS

- Secure version of HTTP
- Uses SSL/TLS
- Used in:
    - Online payments
    - Login pages

7. Digital Signature

- Used to verify identity of sender
- Ensures:
    - Data is not changed
    - Sender is genuine

👉 Like:
Online signature

8. Digital Certificate

- Electronic document that proves identity
- Issued by Certificate Authority (CA)

Example:
Website security certificate

9. IPSec (Internet Protocol Security)

- Provides security at network layer
- Protects IP communication

- Used in:
    - VPN
    - Secure networks

Quick Summary

- Encryption → Hide data
- Decryption → Get original data
- Symmetric → One key
- Asymmetric → Two keys
- Hashing → Fixed code
- SSL/HTTPS → Secure web
- RSA → Secure communication
- IPSec → Network security

UNIT 3. VIRUS, WORMS AND TROJANS

Malware

Malware = Malicious Software designed to damage, steal data or misuse a computer system.

Main types:

- Virus
- Worm
- Trojan
- Ransomware
- Zombie (Bot)

2. Computer Virus

Definition

A computer virus is a malicious program that attaches itself to a file/program and spreads when the file runs.

Key Features

- Needs human action (run file, open USB, email attachment).
- Infects other files.
- Slows system / corrupts data.

Types of Viruses

1. File virus – infects executable files (.exe).
2. Boot sector virus – attacks boot records.
3. Macro virus – infects Word/Excel files.
4. Polymorphic virus – changes its code to avoid detection.

Symptoms

- Slow computer
- Unknown popups
- Files missing or corrupted
- System crashes

3. Computer Worm

Definition

A worm is a self-replicating malware that spreads automatically through networks.

Key Features

- Does NOT need human action.
- Uses internet/network vulnerabilities.
- Spreads very fast.

Example behaviour

- Sends copies of itself to contacts.
- Consumes bandwidth.
- Causes network crash.

4. Trojan Horse

Definition

A Trojan is malware disguised as a useful or genuine program.

Example:

- Fake game
- Fake software crack
- Fake antivirus

What Trojans do

- Steal passwords
- Spy on users
- Open backdoor access
- Install other malware

Important

Trojan does not replicate like virus/worm.

5. Zombie / Bot

Definition

A Zombie is a computer secretly controlled by hackers.

When many zombies are connected → called Botnet.

Uses of Zombie Computers

- Sending spam emails
- Launching DDoS attacks
- Mining cryptocurrency

- Spreading malware

User usually does not know their PC is infected.

6. Ransomware

Definition

Ransomware locks or encrypts files and asks for money (ransom) to unlock them.

Working

1. Enters via email attachment / pirated software.
2. Encrypts all files.
3. Shows message → "Pay money to recover files".

Types

1. Crypto ransomware – encrypts files.
2. Locker ransomware – locks entire computer.

Famous attacks (example)

- WannaCry attack (2017)

Prevention

- Backup data regularly
- Avoid suspicious links
- Update system

7. Preventive Measures Against Malware

A. Access Control

Control who can use the system.

Methods:

- Strong passwords
- User authentication
- Limited user privileges
- Firewall protection

Purpose: Prevent unauthorized access.

B. Checksum Verification

Checksum

A checksum is a value used to check file integrity.

Working

- When file is created → checksum generated.
- Later → checksum rechecked.
- If value changes → file may be infected.

Purpose: Detect file tampering or virus.

D. Process Configuration

System should be configured securely.

Measures:

- Disable unnecessary services
- Close unused ports
- Update OS regularly
- Install security patches

Purpose: Reduce vulnerabilities.

E. Virus Scanners (Signature Based)

Definition

Software that detects viruses using known virus signatures.

Examples:

- Quick Heal
- Windows Defender
- Avast

Working

- Compare files with virus database.
- If match found → virus detected.

Limitation

Cannot detect new unknown viruses.

E. Heuristic Scanners

Definition

Detect unknown viruses by analyzing behaviour.

Working

- Looks for suspicious activities like:

- Self-replication
- File modification
- Unauthorized access

Advantage

Can detect new viruses.

F. Application Level Virus Scanners

Scan specific applications like:

- Email
- Browser downloads
- Office files

Example:

- Email attachment scanning
- Download scanning

Purpose: Stop virus at entry point.

G. Deploying Virus Protection (Full Strategy)

Steps to implement complete protection:

1. Install Antivirus
2. Enable Firewall
3. Update software regularly
4. Backup important data
5. Avoid pirated software
6. Scan USB devices
7. Educate users
8. Enable email filtering

This is called layered security.

8. Virus vs Worm vs Trojan (Comparison)

Feature	Virus	Worm	Trojan
Needs user action	Yes	No	Yes
Self replicate	Yes	Yes	No
Infect files	Yes	No	No

Feature	Virus	Worm	Trojan
Disguised as legit program	No	No	Yes
Spreads via network	Sometimes	Yes	No

9. Conclusion

Malware is a serious cyber threat.
Understanding virus, worms, trojans and ransomware helps us protect systems.

Best protection = Awareness + Antivirus + Updates + Backup.

UNIT 4. FIREWALLS

1. Firewall – Definition and Types

Definition

- A firewall is a network security system that protects a computer or network from unauthorized access.
- It acts as a barrier between a trusted internal network and the internet (untrusted network).
- It monitors incoming and outgoing network traffic.
- It allows or blocks data based on security rules.

Types of Firewall

1. Packet Filtering Firewall – Filters packets based on IP address, port number, and protocol.
2. Stateful Inspection Firewall – Checks packets based on active connections.
3. Proxy Firewall – Works as an intermediary between user and internet.
4. Next Generation Firewall (NGFW) – Advanced firewall with deep packet inspection and intrusion prevention.
5. Hardware Firewall – Installed in routers or network devices.
6. Software Firewall – Installed on individual computers.

2. Firewall Configuration

- Firewall configuration means setting rules and policies to control network traffic.
- Administrators define security policies to allow or block traffic.
- Firewall rules are created using IP address, port number, and protocol.
- Only necessary ports are opened and others are blocked.
- Network Address Translation (NAT) hides internal IP addresses.
- Logging and monitoring track network activities.
- Regular updates and testing are required for better security.

Types of Firewall

1. Packet Filtering Firewall

A **Packet Filtering Firewall** is the most basic type of firewall. It works by checking small pieces of data called **packets** that travel across the network. Each packet contains information such as **source IP address, destination IP address, port number, and protocol**. The firewall

compares this information with predefined security rules. If the packet matches the rule, it is allowed to pass; otherwise, it is blocked.

This firewall works at the **network layer** of the OSI model and is very fast because it only checks packet headers. However, it does not inspect the actual content of the packet, which makes it less secure compared to advanced firewalls.

Advantages

- Fast and simple
- Low cost
- Easy to implement

Disadvantages

- Cannot detect complex attacks
- Does not track connection state

2. Stateful Inspection Firewall

A **Stateful Inspection Firewall** is more advanced than a packet filtering firewall. It monitors the **state of active connections** and keeps a record of them in a **state table**. When a packet arrives, the firewall checks whether it belongs to an existing and trusted connection.

For example, if a user inside the network requests a webpage, the firewall records that request. When the response comes back from the server, the firewall allows it because it recognizes it as part of the existing session.

This firewall provides better security because it understands the **context of network traffic** rather than checking packets individually.

Advantages

- More secure than packet filtering
- Tracks active sessions
- Efficient for modern networks

Disadvantages

- Requires more memory and processing
- Slightly slower than packet filtering

3. Proxy Firewall (Application-Level Gateway)

A **Proxy Firewall** works as an **intermediary between the user and the internet**. Instead of allowing direct communication between a user and a server, the proxy firewall receives the request first. It then checks the request and forwards it to the destination server if it is safe.

Because it operates at the **application layer**, it can inspect the actual content of the data. It can filter specific applications such as **HTTP, FTP, or email traffic**.

This type of firewall also hides the internal network from external users, which improves security.

Advantages

- High level of security
- Hides internal IP addresses
- Can filter application-level traffic

Disadvantages

- Slower performance due to deep inspection
- Requires more configuration

4. Next Generation Firewall (NGFW)

A **Next Generation Firewall (NGFW)** is an advanced firewall that combines traditional firewall features with modern security technologies. It performs **deep packet inspection**, which means it examines both the packet header and the content of the data.

NGFW also includes features such as:

- Intrusion Prevention System (IPS)
- Application awareness and control
- Malware protection
- User identity management

These firewalls are widely used in large organizations because they provide strong protection against modern cyber threats.

Advantages

- Very high security
- Detects advanced attacks
- Supports multiple security features

Disadvantages

- Expensive
- Requires skilled administrators

Whitelisting vs Blacklisting

Whitelisting

- Only approved or trusted programs, websites, or users are allowed.
- Everything else is blocked by default.

- Provides higher security.
- Used in high-security organizations.

Advantages

- Prevents unknown or unauthorized software.
- Reduces risk of malware.

Disadvantages

- Requires frequent updates.
- New trusted applications must be manually added.

Blacklisting

- Blocks known harmful programs, websites, or IP addresses.
- Everything else is allowed.

Advantages

- Easy to manage.
- Only harmful items need to be added to the list.

Disadvantages

- New threats may not be blocked.
- Malware not in the blacklist can still run.

Key Difference

Whitelisting	**Blacklisting**
Allow only trusted items	Block only harmful items
Higher security	Easier to manage
Default action: Block	Default action: Allow

Both techniques are often used together for better system protection.

Limitations of Firewall

- A firewall cannot protect against **internal attacks** within the network.
- It cannot stop malware coming from **USB drives or external devices**.
- Some **new or unknown threats** may bypass firewall rules.
- **Encrypted traffic** may hide malicious content.
- Incorrect **configuration** may create security loopholes.
- Firewall alone is not enough; it should be used with **antivirus and IDS**.

Intrusion Detection System (IDS)

- An Intrusion Detection System (IDS) is like a security guard for a computer network.
- Just like a guard watches who enters a building, an IDS watches the data coming into and leaving a network.
- Its job is to detect suspicious activities, such as:
- Hackers trying to enter the system
- Someone trying to steal data
- Malware attacking the network
- If something suspicious happens, the IDS raises an alert or warning so that the administrator can take action.

Example:
Imagine a CCTV camera in a building. It records and shows if someone suspicious enters. IDS works in the same way for a computer network.

Intrusion Prevention System (IPS)

An Intrusion Prevention System (IPS) is like a security guard who not only watches but also stops criminals.

- While IDS only detects and alerts, IPS can also block the attack immediately.

Example:

- IDS situation
- Someone suspicious enters a building
- Security camera records it
- Guard informs the manager
- IPS situation
- Guard stops the suspicious person at the gate
- So:IDS = Detects attack
  IPS = Detects and stops attack

Types of IDS

- Network Based IDS (NIDS)
- This system monitors the entire network traffic.

Example:

- If a hacker tries to attack the company network from the internet, NIDS can detect it.
- It is usually installed at places like:
- Routers
- Gateways
- Network switches
- It checks all data packets moving in the network.

Host Based IDS (HIDS)

- This system works on individual computers or servers.
- It monitors:
- Files in the computer
- Login attempts
- System activities
- Changes in important files

Example:

- If someone tries to change important system files or access confidential data, HIDS will detect it.

Limitations of IDS

Even though IDS is useful, it has some problems.

1. False Alarm (False Positive)

Sometimes IDS thinks normal activity is an attack.

Example:
A user downloads a large file and IDS thinks it is suspicious.

2. Missed Attacks (False Negative)

Sometimes IDS fails to detect real attacks.

Example:
A new type of hacker attack that the system does not recognize.

3. Encrypted Data Problem

If data is encrypted, IDS may not understand what is inside the packet.

4. Heavy Network Traffic

If the network traffic is very high, IDS may become slow or miss attacks.

5. Teardrop Attack (Simple Explanation)

A Teardrop attack is a type of Denial of Service (DoS) attack.

To understand it simply:

- When data travels on the internet, it is broken into small pieces called packets.
- When these packets reach the destination computer, they are joined again.

In a Teardrop attack:

- The hacker sends corrupted packets.
- These packets overlap incorrectly.
- The computer cannot combine them properly.
- The system crashes or stops working.

Example:

Imagine receiving a puzzle with wrong pieces.
You cannot complete the puzzle, so the process stops.

Old operating systems like:

Windows 95

Windows NT

were vulnerable to this attack.

Counter Measures (How to Stop Teardrop Attack)

To prevent such attacks, we can take several steps.

1. Update Operating System

Always install latest updates and security patches.

2. Use Firewalls

Firewalls can block suspicious packets.

3. Use IDS / IPS

IDS detects abnormal packet behavior and IPS can block the attack.

4. Monitor Network Traffic

Regular monitoring helps identify unusual network activity.

5. Packet Filtering

Network devices can filter invalid or suspicious packets.

7. Host Based IDS Setup (Simple Explanation)

Setting up HIDS means installing security monitoring software on a computer.

Step 1: Install HIDS Software

Examples:

OSSEC

Tripwire

Step 2: Monitor Important Files

The system watches important files such as:

System configuration files

Security settings

If someone changes them without permission, it alerts.

Step 3: Monitor Login Attempts

The system checks:

Who is logging in

How many login attempts are made

If someone tries to log in many times, it is flagged.

Step 4: Generate Alerts

If suspicious activity happens, the system sends alerts such as:

Email notification

Security warning

Log entry

8. Simple Example of IDS in Real Life

Think of bank security.

Bank security includes:

Cameras (monitor activity) → like IDS

Security guards stopping thieves → like IPS

Both together help protect the bank.

Similarly, IDS and IPS help protect computer networks from hackers.

UNIT 5. HANDLING CYBER ASSETS, VPN & DISASTER RECOVERY

1. Handling Cyber Assets

(a) Configuration Policy (as per standards)

- It means **setting rules for system configuration**
- Ensures systems are **secure and properly managed**
- Includes:
  - Password policies
  - Access control rules
  - Software update rules
- Follows **standard security guidelines**
- Helps prevent **unauthorized access**

(b) Disposable Policy

- Policy for **safe disposal of old data and devices**
- Ensures **sensitive data is not leaked**
- Methods:
  - Data wiping
  - Disk formatting
  - Physical destruction of storage devices
- Important for:
  - Old computers
  - Hard disks
  - USB drives

2. Virtual Private Network (VPN)

(a) Basics of VPN

- VPN = **Virtual Private Network**
- Creates a **secure connection over internet**
- Data is **encrypted (hidden)**
- Used for:
  - Secure communication
  - Remote access

(b) Setting of VPN

Steps:

1. Install VPN software
2. Configure server and client
3. Enter username/password
4. Connect to VPN network

(c) VPN Diagram (concept)

- User → Internet → VPN Server → Secure Network
- Data travels in **encrypted tunnel**

(d) Configuration of Required Objects

- IP address
- Authentication settings
- Encryption protocols
- User credentials

(e) Exchanging Keys

- Used for **encryption/decryption**
- Types:
  - Public key
  - Private key
- Ensures **secure communication**

(f) Modifying Security Policy

- Updating security rules as needed
- Includes:
  - Changing passwords
  - Updating encryption methods
  - Adjusting access permissions

3. Disaster and Recovery

(a) Disaster Categories

- Natural disasters (flood, fire)
- Technical failures

- Human errors
- Cyber attacks

(b) Network Disasters

- **Cabling failure** → wires damaged
- **Topology failure** → network design issue
- **Single point of failure** → one device failure stops whole network
- Solution:
  - Backup links
  - Proper design
  - Save configuration files

(c) Server Disasters

- **Power failure** → use UPS
- **Data loss** → use RAID (data duplication)
- **System crash** → use clustering
- **Backup failure** → maintain regular backups

(d) Recovery Techniques

- Restore data from backup
- Restart systems
- Replace damaged hardware
- Use recovery plans

4. Conclusion

- Proper handling of cyber assets ensures **data security**
- VPN provides **secure communication**
- Disaster recovery ensures **system continuity and data protection**