ASSIGNMENT 1

CONTENTS:

INTRODUCTION TO CYBER SECURITY

NETWORKING TCP AND OSI MODEL

PORTS

PROTOCOLS

INTRODUCTION TO PYTHON

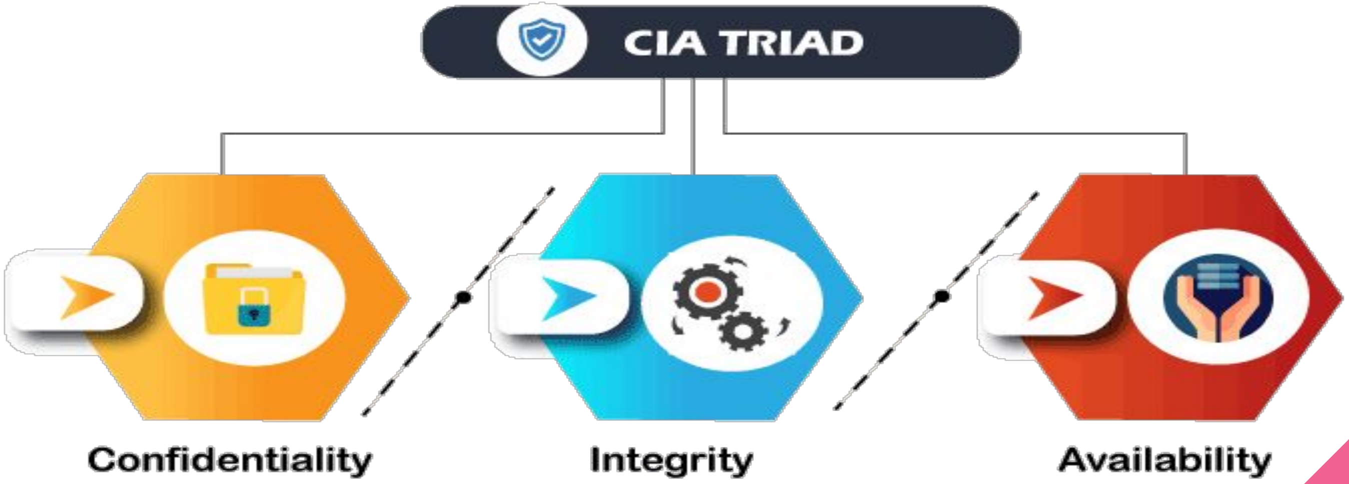
KRISHNA SATHVIKA GANNI
4TH YEAR, B.TECH
RCEE

INTRODUCTION TO CYBER SECURITY

- ➔ Cybersecurity is the practice of protecting networks, devices, and data from unauthorized access or criminal use. It also involves ensuring the confidentiality, integrity, and availability of information.
- ➔ Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks.
- ➔ These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users via ransomware; or interrupting normal business processes.
- ➔ Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

CIA TREND

- ➔ Cyber Security's main **objective is to ensure data protection**.
- ➔ The security community provides a triangle of three related principles to protect the data from cyber-attacks. This principle is called the **CIA triad**.



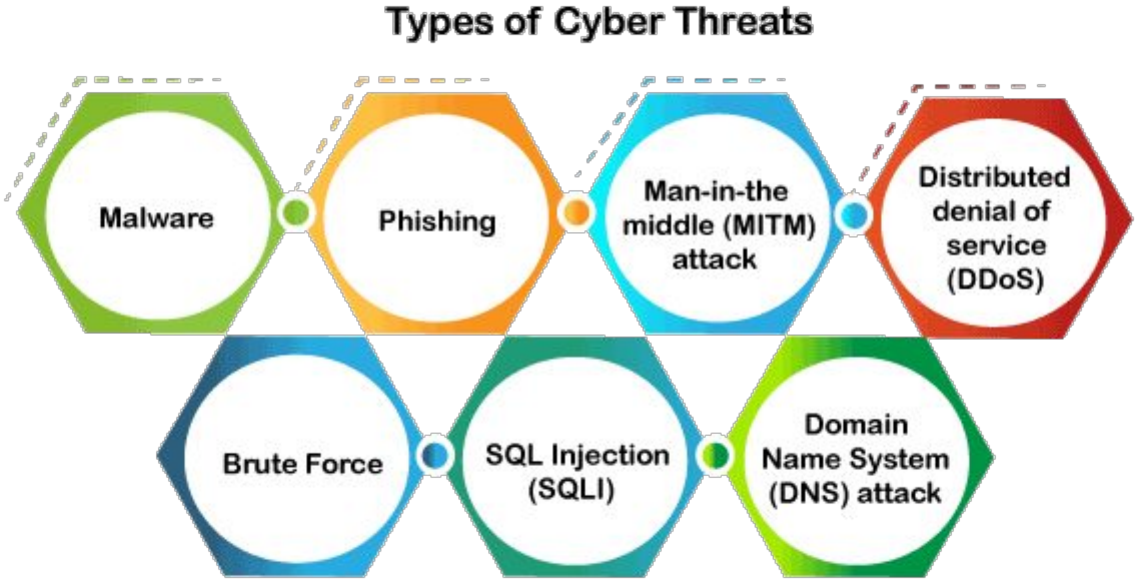
CIA TRIAD

Confidentiality

Integrity

Availability

TYPES OF CYBER THREATS


Types of Cyber Threats
Malware
Phishing
Man-in-the middle (MITM) attack
Distributed denial of service (DDoS)
Brute Force
SQL Injection (SQLI)
Domain Name System (DNS) attack

NETWORKING IN TCP MODEL

- ➔ The TCP/IP model is a suite of protocols that defines how devices transmit data between them.
- ➔ The TCP/IP protocol is divided into two layers: the Transport layer and the Internet layer. The Transport layer is responsible for ensuring that data is transmitted reliably from one device to another. This layer is comprised of two protocols: the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP). TCP is used for reliable data transmission, while UDP is used for fast transmission of data that can tolerate some packet loss.
- ➔ The Internet layer is responsible for transmitting data packets between devices. This layer is comprised of two protocols: the Internet Protocol (IP) and the Address Resolution Protocol (ARP). IP is responsible for routing data packets between devices, while ARP is used to map IP addresses to physical addresses.
- ➔ TCP/IP also includes a number of application layer protocols that are used to provide services to end-users. These include protocols such as HTTP (Hypertext Transfer Protocol) for web browsing, FTP (File Transfer Protocol) for file transfer, and SMTP (Simple Mail Transfer Protocol) for email.

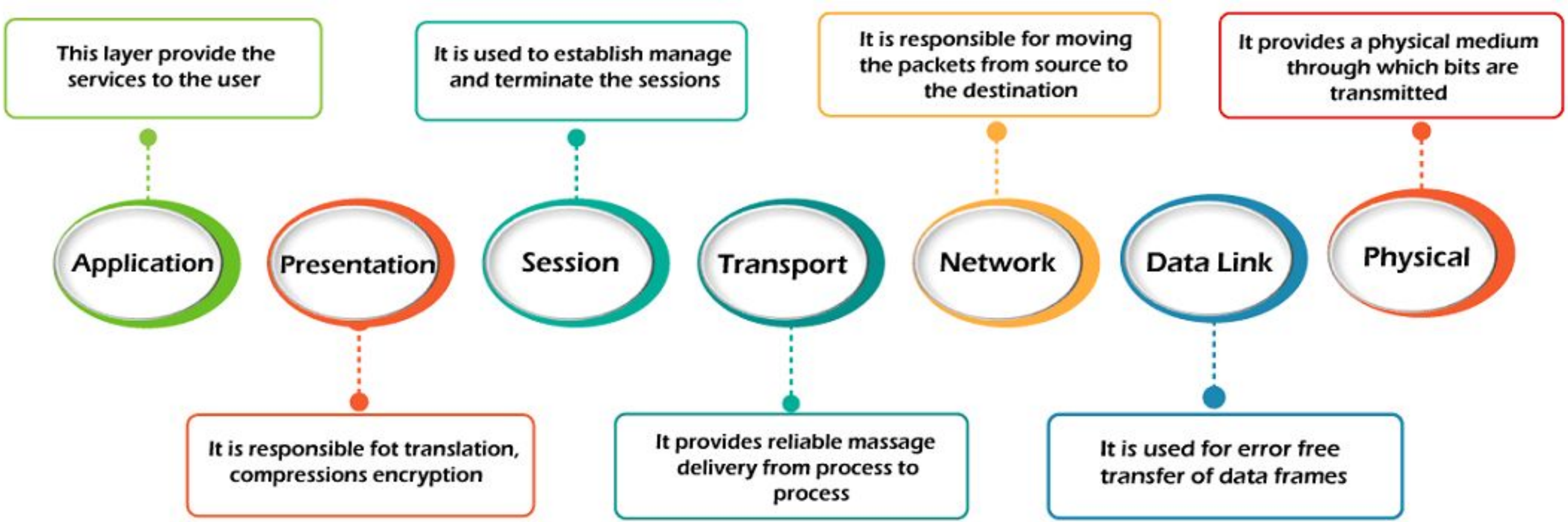
WORKING OF TCP/IP

- TCP/IP employs the client-server demonstration of communication in which a client or machine (a client) is given a benefit (like sending a webpage) by another computer (a server) within the network.
- Collectively, the TCP/IP suite of conventions is classified as stateless, which suggests each client request is considered new since it is irrelevant to past requests. Being stateless liberates up network paths so they can be utilized continuously.
- The transport layer itself, is stateful. It transmits a single message, and its connection remains open until all the packets in a message have been received and reassembled at the destination.
- The TCP/IP model differs from the seven-layer Open System Interconnection (OSI) model designed after it.

NETWORKING IN OSI MODEL

- ➔ The Open Systems Interconnection (OSI) model is a framework that describes the functions of a networking system. The model is based on the idea of splitting up a communication system into seven abstract layers.
- ➔ The OSI model is divided into two layers: upper layers and lower layers.
- ➔ The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.
- ➔ The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software.
- ➔ The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium.

7 LAYERS OF OSI MODEL



Application

This layer provide the services to the user

Presentation

It is responsible fot translation, compressions encryption

Session

It is used to establish manage and terminate the sessions

Transport

It provides reliable massage delivery from process to process

Network

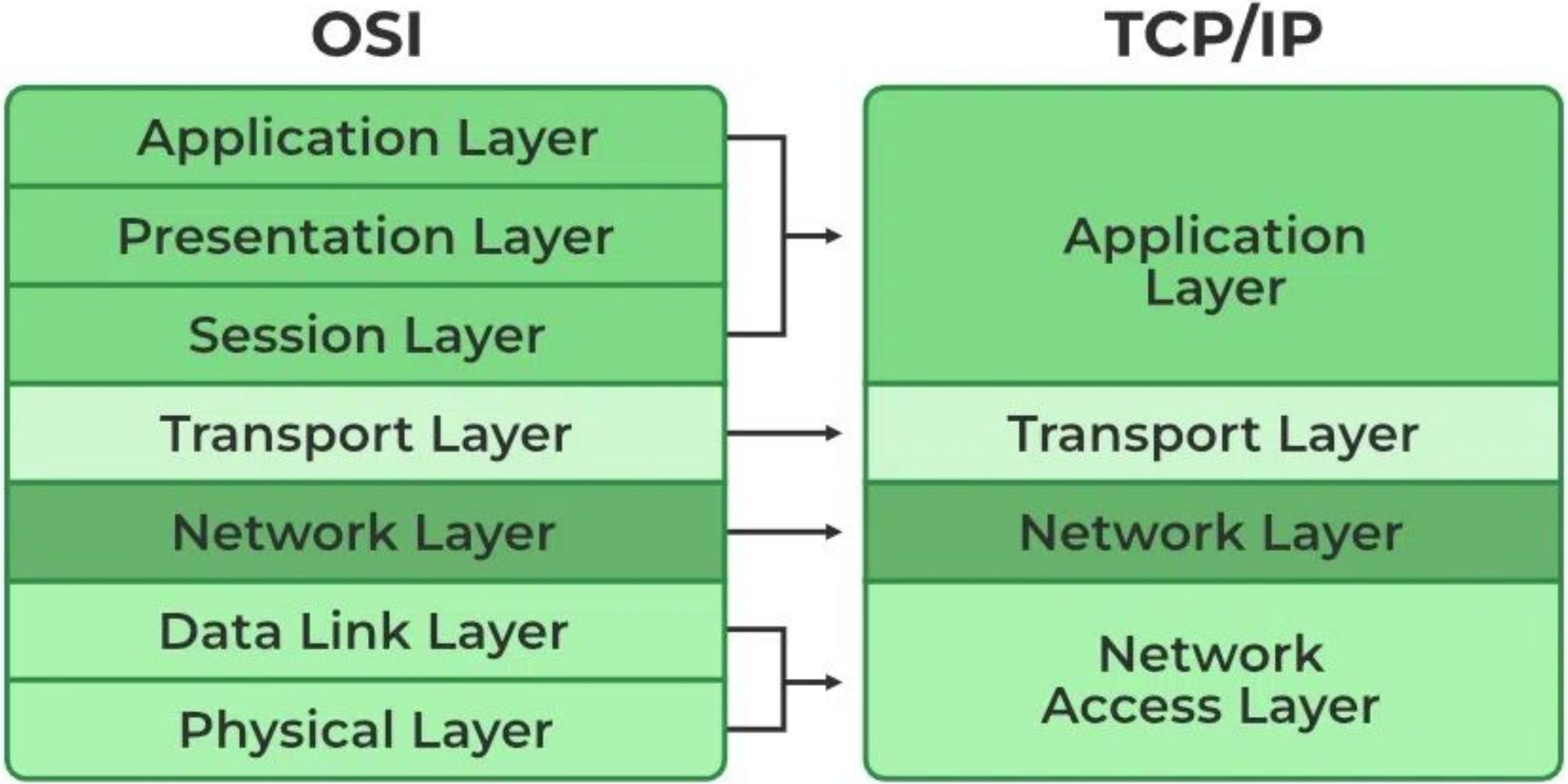
It is responsible for moving the packets from source to the destination

Data Link

It is used for error free transfer of data frames

Physical

It provides a physical medium through which bits are transmitted



OSI
TCP/IP
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer
Application Layer
Transport Layer
Network Layer
Network Access Layer

COMMON PORTS

1. **PORT 20 AND 21:** These Ports are used for FTP (file transfer protocol) connection. FTP uses two TCP connections for communication. Port 21 is used for pass control information. And the other port 20 is used to send the data files between the client and the server. FTP ports 20 and 21 must both be open for successful file transfer on the network.

2. **PORT 22:** The port is used for Secure Shell (SSH) communication and allows remote administration access to the VM. In general, traffic is encrypted using password authentication.

3. **PORT 23:** Port 23 is typically used by the Telnet protocol. Telnet commonly provides remote access to a variety of communications systems. Telnet is also often used for remote maintenance of many networking communications devices including routers and switches.

1. **PORT 25:** Port 25 is the default SMTP port that is used to enable communication between the sending and receiving servers when delivering an email message to a recipient. Despite its pedigree, many ISPs (Internet Service Providers) and email providers have started to block incoming connections on port 25 as a security measure.

2. **PORT 53:** The standard port for DNS is port 53. DNS client applications use the DNS protocol to query and request information from DNS servers, and the server returns the results to the client using the same port. Port 53 is used for both TCP and UDP communication.

3. **PORT 67/68:** DHCP servers also use port 67 to initiate communication between the client and server on the network. If port 67 is used by another application, DHCP will fail to function. Clients use port 68.

4. **PORT 80:** Port 80 is the port number assigned to commonly used internet communication protocol, Hypertext Transfer Protocol (HTTP). It is the default network port used to send and receive unencrypted web pages.

1. **PORT 123:** NTP is a built-on UDP, where port 123 is used for NTP server communication and NTP clients use port 1023 (for example, a desktop).

2. **PORT 161,162:** SNMP ports are utilized via UDP 161 for SNMP Managers communicating with SNMP Agents (i.e. polling) and UDP 162 when agents send unsolicited Traps to the SNMP Manager.

3. **PORT 389:** Port 389 is used for TLS connections; TLS establishes a non encrypted connection on port 389 that it 'upgrades' to an encrypted TLS connection as the initial connection proceeds. This allows unencrypted and encrypted connections to be setup and handled by this one port.

4. **PORT 443:** Port 443 is a web browsing port used to secure web browser communication or HTTPS services. Over 95% of secured websites use HTTPS via port 443 for secure data transfer. It will provide encryption and transport over secure ports.

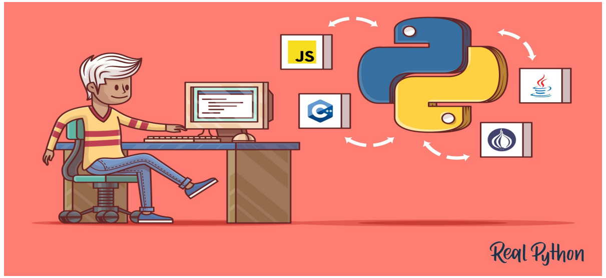
PROTOCOLS

1. **IPsec (Internet Protocol Security):** IPsec is like a secret code for internet communication. It makes sure that when computers talk to each other online, their messages are scrambled into unreadable codes, so no one else can understand them. It's commonly used by companies to keep their data safe when employees work from home or when different offices need to connect securely.
2. **SSL/TLS (Secure Sockets Layer/Transport Layer Security):** SSL/TLS is like a secure tunnel for internet browsing. When you visit a website, it sets up a secret language between your browser and the website, so any information you send (like passwords or credit card numbers) is protected from sneaky hackers who might try to listen in.
3. **DTLS (Datagram Transport Layer Security):** DTLS is similar to SSL/TLS, but it's designed for things like video calls or online games that need to be fast and smooth. It makes sure that even in the middle of a fast-paced game or a video chat, your messages stay safe and don't get messed up along the way.

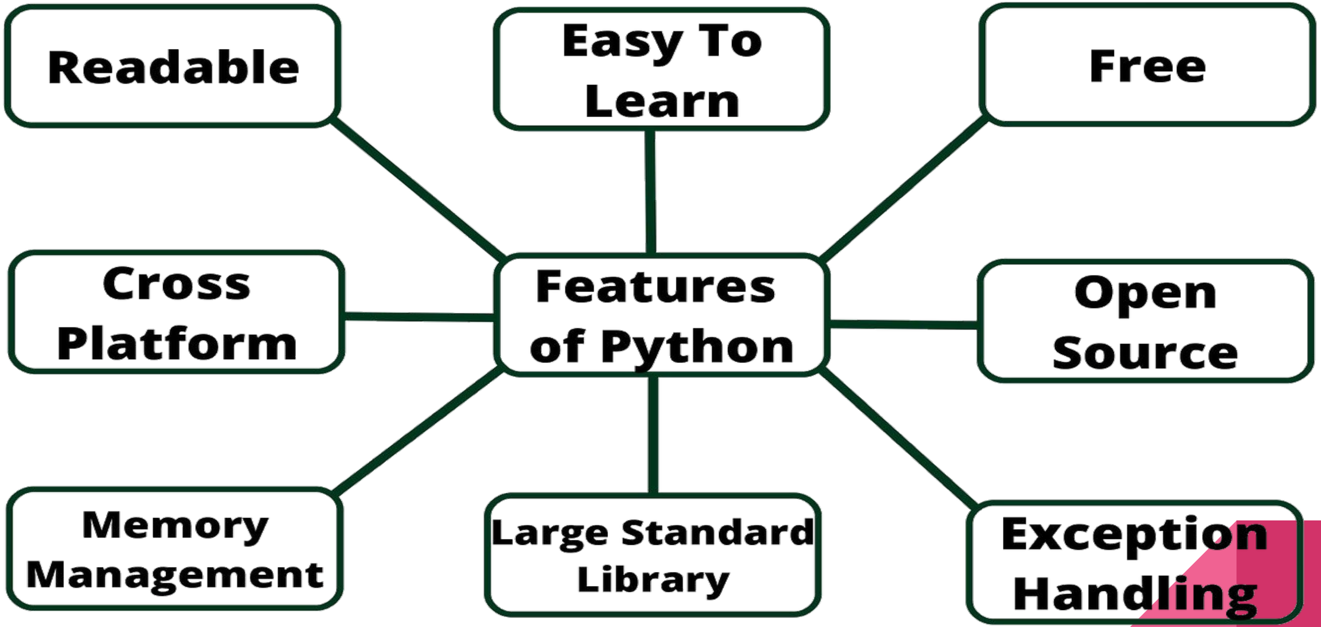
1. **Kerberos:** Kerberos is like a special ticket for getting into a club. When you want to use a computer system or an app, Kerberos checks to make sure you're allowed in. It's like showing your ID at the door, but way more secure. It's often used by big organizations to control who can access their computers and data.
2. **SNMPv3 (Simple Network Management Protocol version 3):** SNMPv3 is like a manager keeping an eye on all the computers and devices in a big office. It checks if everything is working okay and lets you know if something isn't right. But it also makes sure that only authorized people can see this information, so it's like having a security guard for your computer network.
3. **HTTPS (Hypertext Transfer Protocol Secure):** HTTPS is like sending a letter in a locked box instead of on a postcard. When you visit a website with HTTPS, it wraps up all the information you send (like your name or what you're buying) in a locked box, so no one else can read it while it's traveling through the internet. It's an extra layer of protection for your online activities, especially when you're sharing sensitive information.

INTRODUCTION TO PYTHON

- Python is a popular programming language. It was created by Guido van Rossum, and released in 1991.
- It was designed with an emphasis on code readability, and its syntax allows programmers to express their concepts in fewer lines of code.
- Python is a programming language that lets you work quickly and integrate systems more efficiently.
- There are two major Python versions: **Python 2 and Python 3**. Both are quite different.



FEATURES OF PYTHON



Features of Python

Readable

Easy To Learn

Free

Cross Platform

Open Source

Memory Management

Large Standard Library

Exception Handling

ROLE OF PYTHON IN CYBER SECURITY

➔ Python can be used to automate a wide range of tasks in cybersecurity, such as scanning for malware, analyzing network traffic, and performing vulnerability assessments.

➔ It can also be used to develop custom security tools for specific tasks.

➔ It is a popular choice for cybersecurity professionals because it is easy to learn and use, and it has a large number of libraries and frameworks that can be used for security tasks.

➔ It has fantastic libraries that are useful for both developing hacking programmes and other kinds of useful programmes.