ASSIGNMENT 1

SALAVUDDIN SHAIKMOTHAD

UCEN JNTUK

TYPES OF CYBER ATTACKS:

1)Active attacks
2)Passive attacks

1)ACTIVE ATTACKS: Active attacks" in the context of cybersecurity refer to malicious activities that involve the unauthorized access, modification, or disruption of computer systems, networks, or data. Unlike passive attacks, which involve eavesdropping or monitoring without altering data, active attacks aim to directly impact or manipulate the targeted system.

A) Man-in-the-Middle (MitM) Attacks:
Intercepting and potentially altering communication between two parties, allowing the attacker to eavesdrop or manipulate data.

B)Denial of Service (DoS) Attacks:
Overloading a system, network, or website with excessive traffic to make it unavailable to legitimate users.

C)Phishing Attacks:
Deceptive attempts to trick individuals into revealing sensitive information, such as passwords or financial details, often through fraudulent emails or websites.

2)PASSIVE ATTACKS:
*involves unauthorized monitoring or observation of communication, data, or systems without altering or disrupting them.

A) Wiretapping:
Illegally tapping into telephone or data communication lines to intercept and listen to conversations or data transmissions.
B)Network Reconnaissance:
Collecting information about a target system or network to identify potential vulnerabilities or weaknesses without actively exploiting them.

1.HACKERS CATEGORY:

A)White Hat Hackers:

Also known as ethical hackers or penetration testers, white hat hackers use their skills to identify and fix security vulnerabilities in systems. They work to improve cybersecurity, often employed by organizations to conduct authorized penetration testing.

B)Black Hat Hackers:

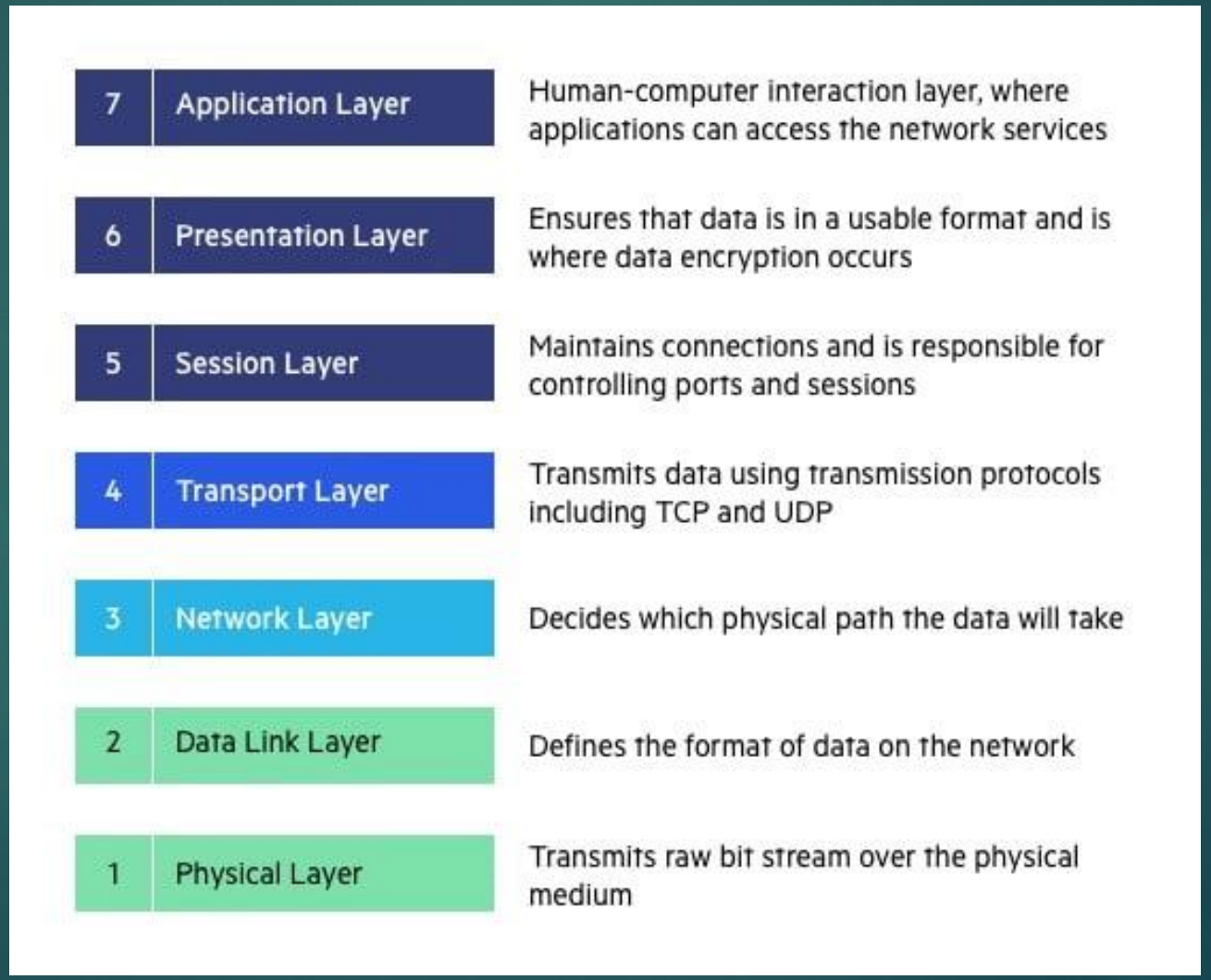
Black hat hackers engage in malicious activities with the intent of causing harm. They may steal data, compromise systems, launch cyber attacks, or engage in other illegal activities for personal gain, financial motives, or just for the thrill of it.

C)Grey Hat Hackers:

Grey hat hackers fall somewhere between white hat and black hat hackers. They may exploit vulnerabilities without authorization but with good intentions, intending to alert the system owner to the weaknesses. However, their actions are still considered unauthorized.

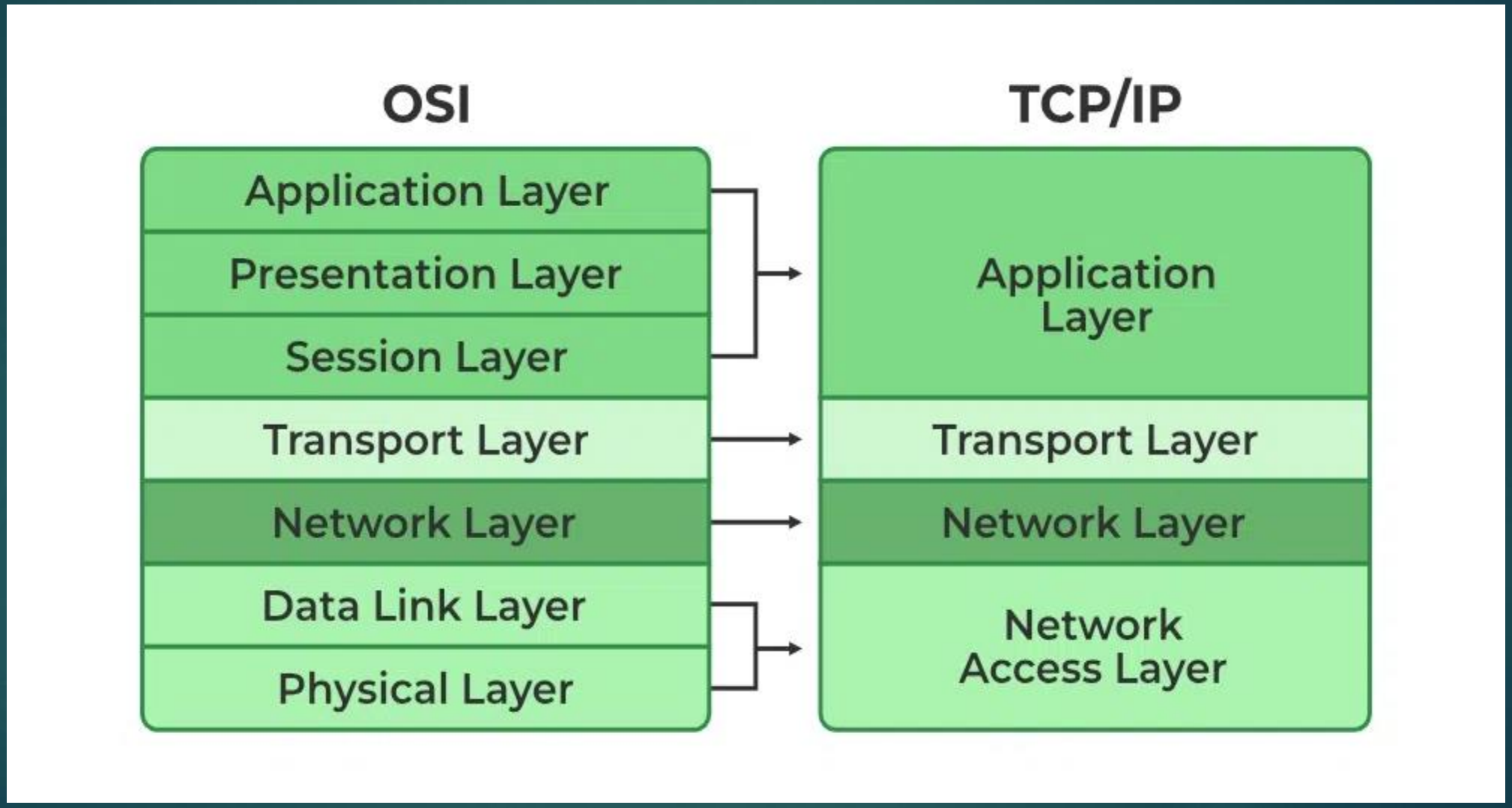
Open Systems Interconnection (OSI) model:

The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network.



TCP/IP Model:

It stands for Transmission Control Protocol/Internet Protocol. The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike the seven layers in the OSI model.

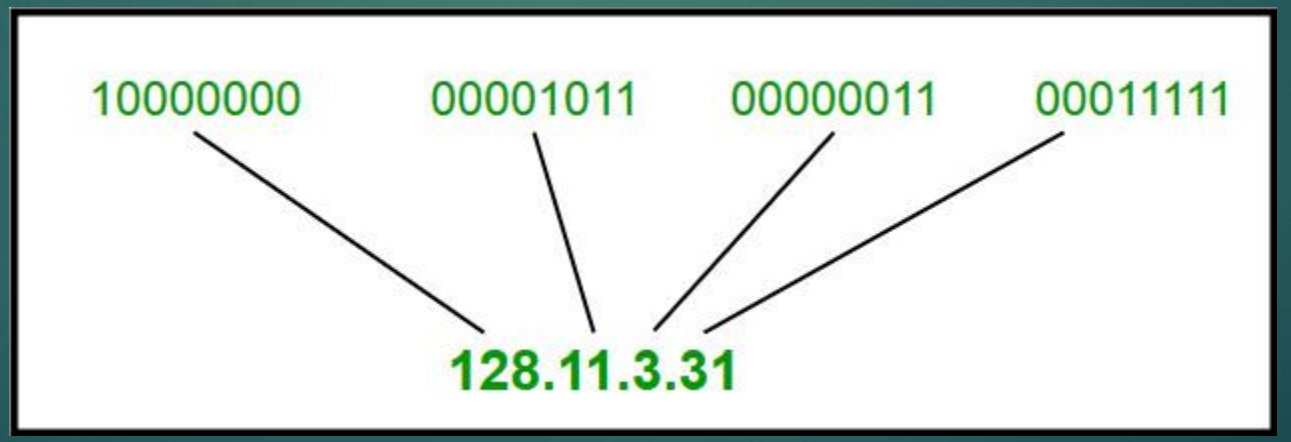


Types of IP Addresses

IPv4 (Internet Protocol Version 4):

IPv4 address consists of two things that are the network address and the host address. It stands for **Internet Protocol version four**

IPv4 addresses are 32-bit integers that have to be expressed in Decimal Notation. It is represented by 4 numbers separated by dots in the range of 0-255, which have to be converted to 0 and 1, to be understood by Computers. For Example, An IPv4 Address can be written as **189.123.123.90.**



IPv6 (Internet Protocol Version 6)

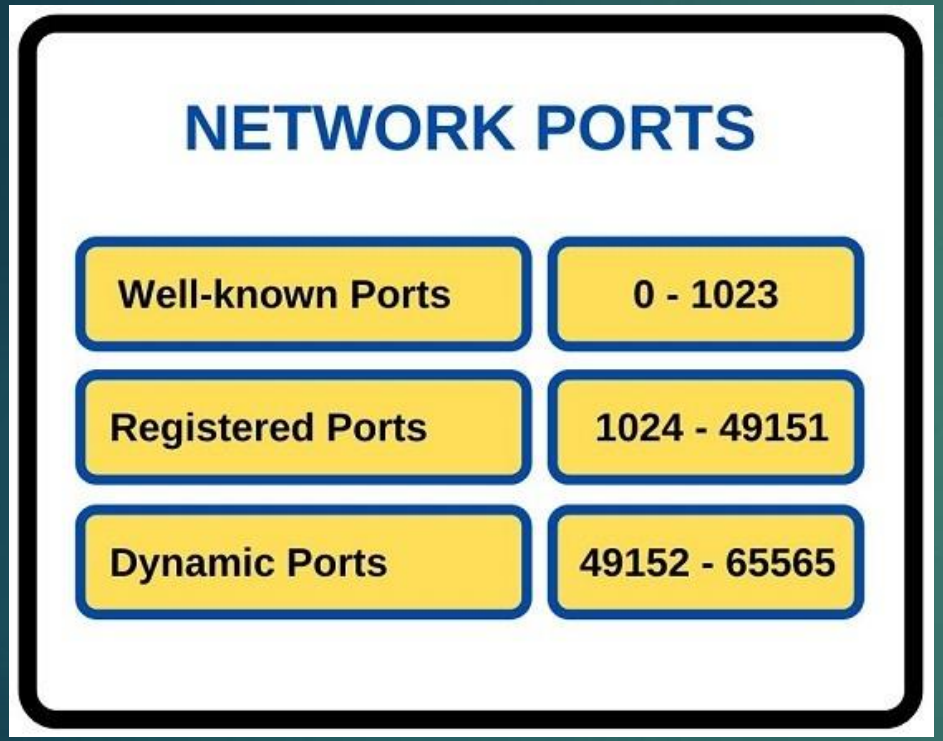
IPv6 is based on IPv4 and stands for Internet Protocol version 6. It was first introduced in December 1995 by Internet Engineering Task Force. IP version 6 is the new version of Internet Protocol, which is way better than IP version 4 in terms of complexity and efficiency. IPv6 is written as a group of 8 hexadecimal numbers separated by colon (:). It can be written as 128 bits of 0s and 1s.

IPv6 Address Format

IPv6 Address Format is a 128-bit IP Address, which is written in a group of 8 hexadecimal numbers separated by colon (:).

Types of Ports:

Ports are virtual places within an operating system where network connections start and end. They help computers sort the network traffic they receive.



Port Number	Process Name	Protocol Used	Description
20	FTP-DATA	TCP	File transfer---data
21	FTP	TCP	File transfer---control
22	SSH	TCP	Secure Shell
23	TELNET	TCP	Telnet
25	SMTP	TCP	Simple Mail Transfer Protocol
53	DNS	TCP & UDP	Domain Name System
69	TFTP	UDP	Trivial File Transfer Protocol
80	HTTP	TCP & UDP	Hypertext Transfer Protocol
110	POP3	TCP	Post Office Protocol 3
123	NTP	TCP	Network Time Protocol
143	IMAP	TCP	Internet Message Access Protocol
443	HTTPS	TCP	Secure implementation of HTTP

SCALER Topics

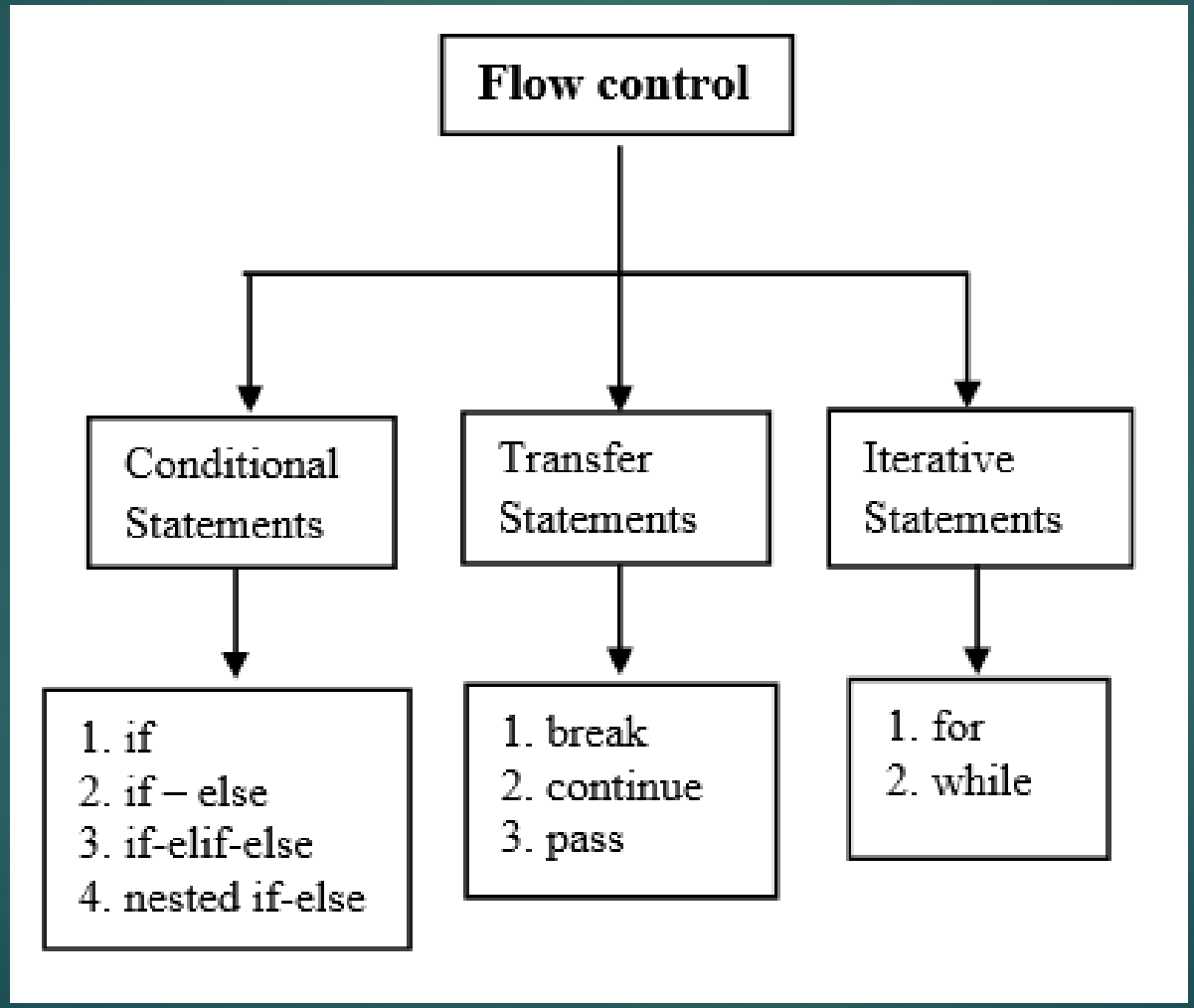
•**Python Data Types**

Data types are the classification or categorization of data items. It represents the kind of value that tells what operations can be performed on a particular data. Since everything is an object in Python programming, data types are classes and variables are instances (objects) of these classes. The following are the standard or built-in data types in Python:

1.**Numeric**
2.**Sequence Type**
3.**Boolean**
4.**Set**
5.**Dictionary**
6.**Binary Types**

Control Statements

Control statements in Python are used to manage the flow of execution of a program based on certain conditions.



Web Services

Web services are a type of internet software that use standardized messaging protocols and are made available from an application service provider's web server for use by a client or other web-based programs.