CYBERSECURITY WITH QRADAR

By

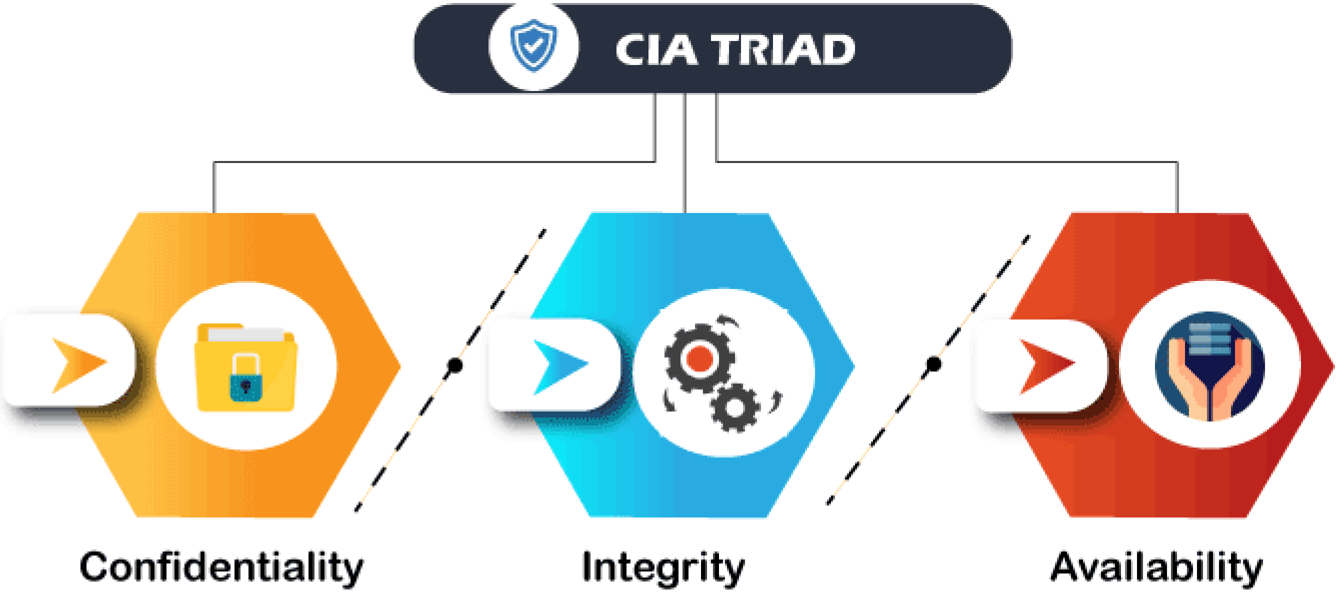
KUPPALA BHARGAVI PRIYA

208X1A4224

INTRODUCTION TO CYBERSECURITY

- The technique of protecting internet-connected systems such as computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks is known as cybersecurity
- 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**. The CIA model is designed to guide policies for an organization's information security infrastructure. When any security breaches are found, one or more of these principles has been violated.

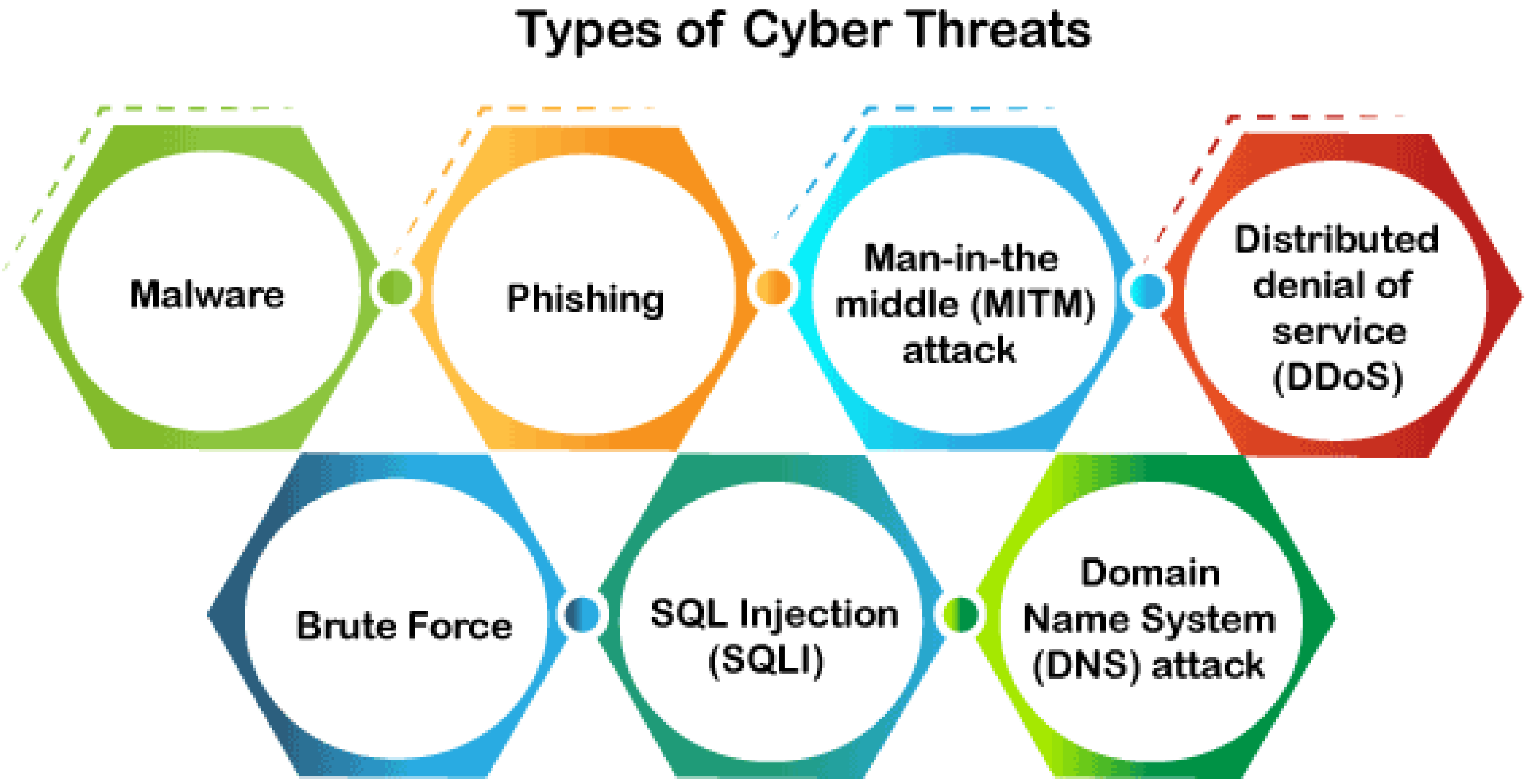
CIA TRAID



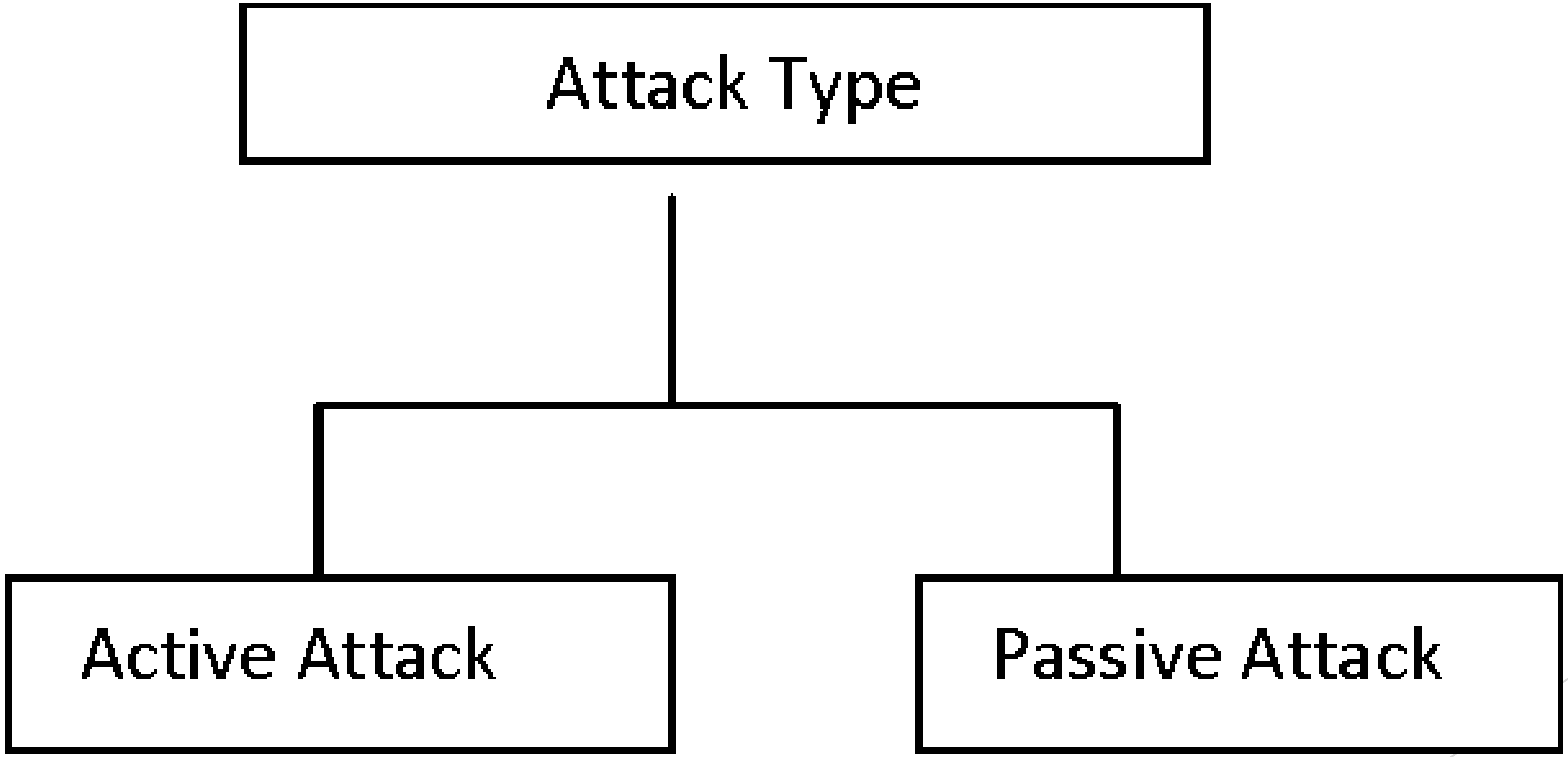
CIA TRAID

- **Confidentiality**
- Confidentiality is equivalent to privacy that avoids unauthorized access of information. It involves ensuring the data is accessible by those who are allowed to use it and blocking access to others.**Data encryption** is an excellent example of ensuring confidentiality.
- **Integrity**
- This principle ensures that the data is authentic, accurate, and safeguarded from unauthorized modification by threat actors or accidental user modification. If any modifications occur, certain measures should be taken to protect the sensitive data from corruption or loss and speedily recover from such an event.
- **Availability**
- This principle makes the information to be available and useful for its authorized people always. It ensures that these accesses are not hindered by system malfunction or cyber-attacks.

Types of Cyber Security 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

TYPES OF ATTACKS



Attack Type

Active Attack

Passive Attack

TYPES OF ATTACKS:

1.Active Attacks:

- Active attacks are a type of cybersecurity attack in which an attacker attempts to alter, destroy, or disrupt the normal operation of a system or network. Active attacks involve the attacker taking direct action against the target system or network, and can be more dangerous than passive attacks, which involve simply monitoring or eavesdropping on a system or network.
- Types of active attacks are as follows:
- Masquerade
- Modification of messages
- Repudiation
- Replay
- Denial of Service

TYPES OF ATTACKS

- ## 2.Passive Attack:

- A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of eavesdropping on or monitoring transmission.
- The goal of the opponent is to obtain information that is being transmitted.
- Examples of passive attacks include eavesdropping, where an attacker listens in on network traffic to collect sensitive information, and sniffing, where an attacker captures and analyzes data packets to steal sensitive information.
- Types of Passive attacks are as follows:
- The release of message content
- Traffic analysis

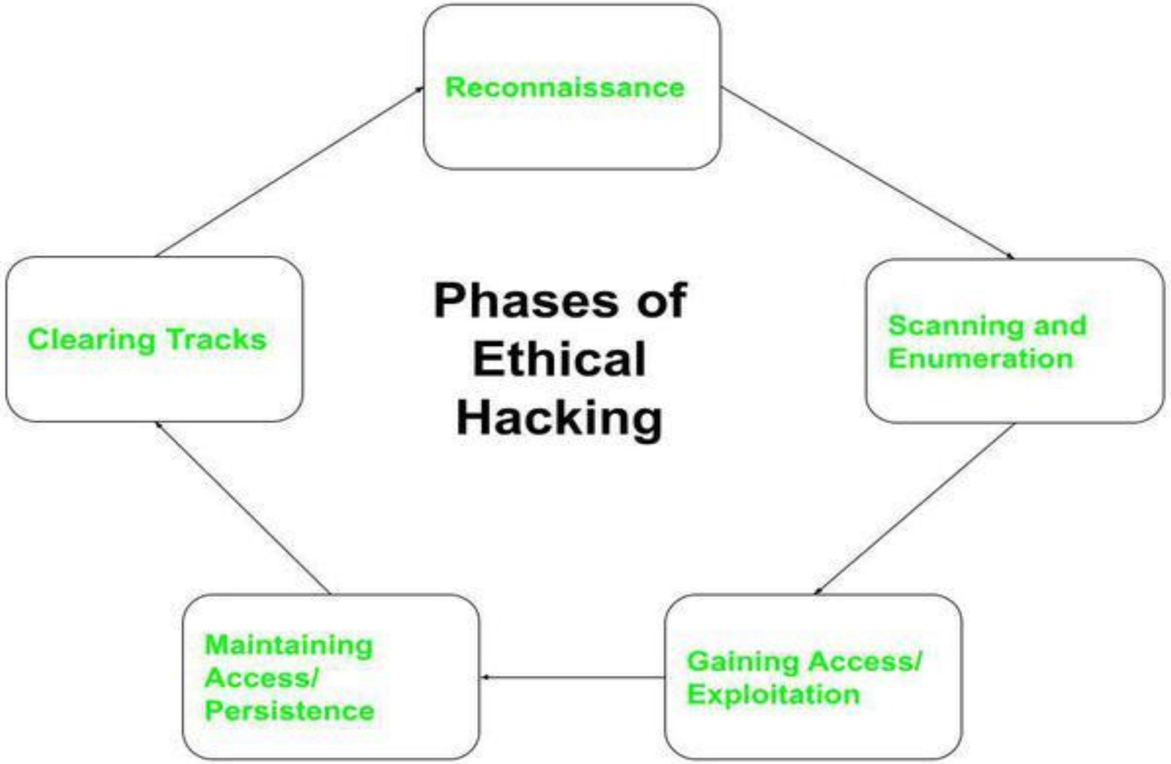
Passive Attack:

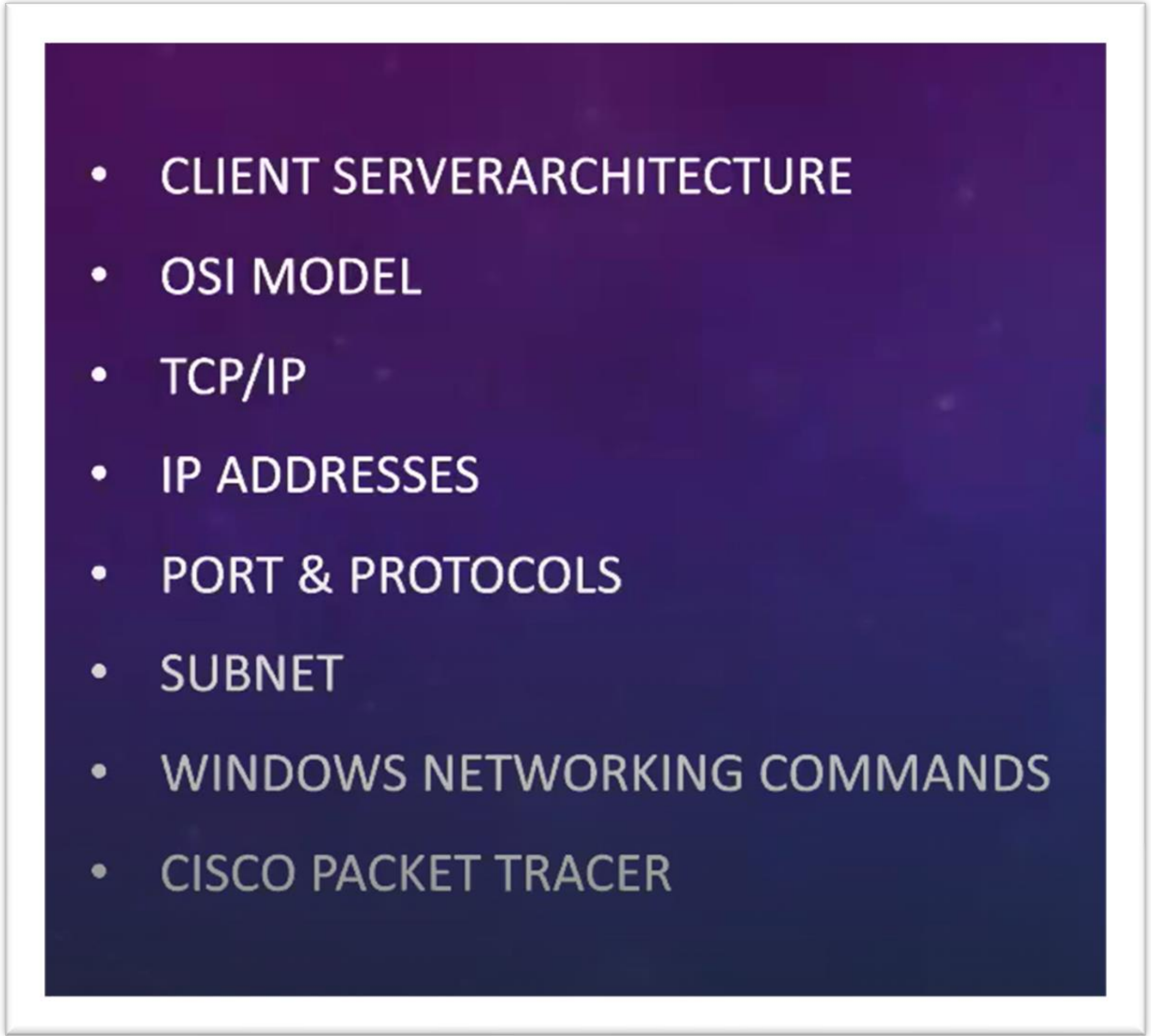
- Computer Surveillance: Computer surveillance involves monitoring the activities and data on a computer system or device without the user's knowledge or consent.
- Network Surveillance: Network surveillance is the monitoring of data traffic within a network to gain insights into the communication patterns and potentially capture sensitive information.
- Wire Tapping: Network surveillance is the monitoring of data traffic within a network to gain insights into the communication patterns and potentially capture sensitive information.

TYPES OF HACKERS

- **White Hat Hackers**: White hat hackers are the one who is authorized or the certified hackers who work for the government and organizations by performing penetration testing and identifying loopholes in their cybersecurity.
- **Black Hat Hackers:** They are often called *Crackers*. Black Hat Hackers can gain the unauthorized access of your system and destroy your vital data.They are considered to be as criminals and can be easily identified because of their malicious actions.
- **Gray Hat Hackers:** Gray hat hackers fall somewhere in the category between white hat and black hat hackers. They are not legally authorized hackers. They work with both good and bad intentions; they can use their skills for personal gain. It all depends upon the hacker. If a gray hat hacker uses his skill for his personal gains, he/she is considered as black hat hackers.

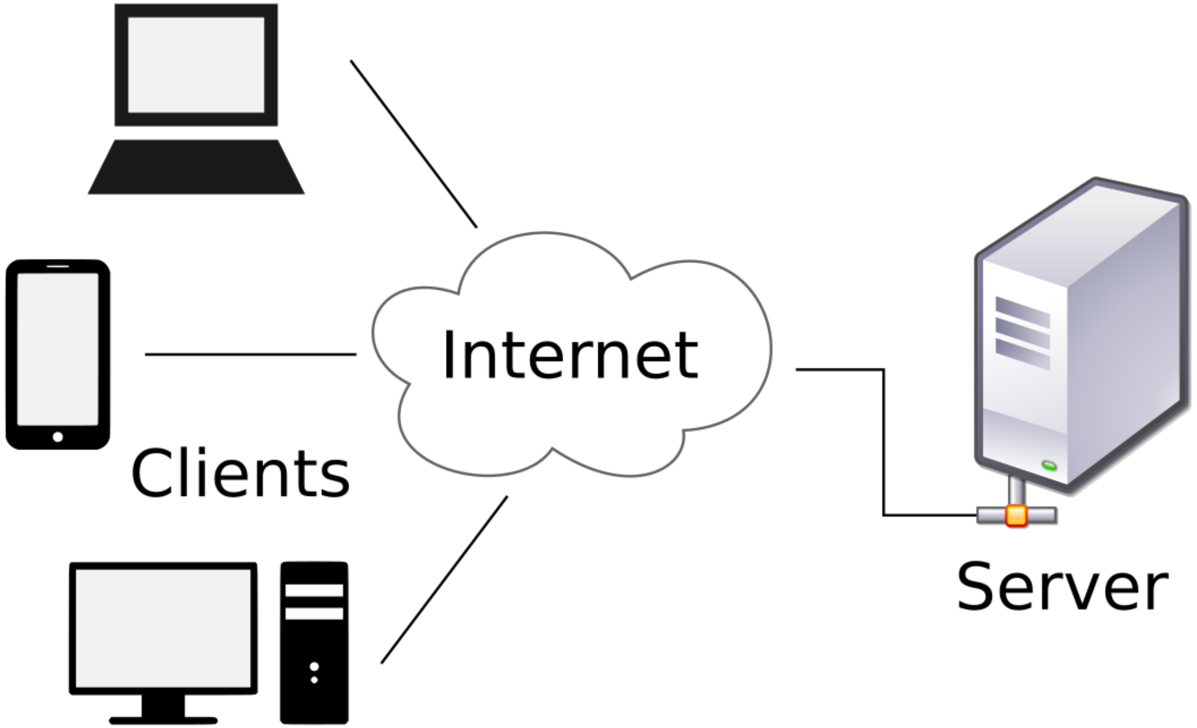
PHASES OF HACKING


Reconnaissance
Scanning and Enumeration
Gaining Access/ Exploitation
Maintaining Access/ Persistence
Clearing Tracks
Phases of Ethical Hacking

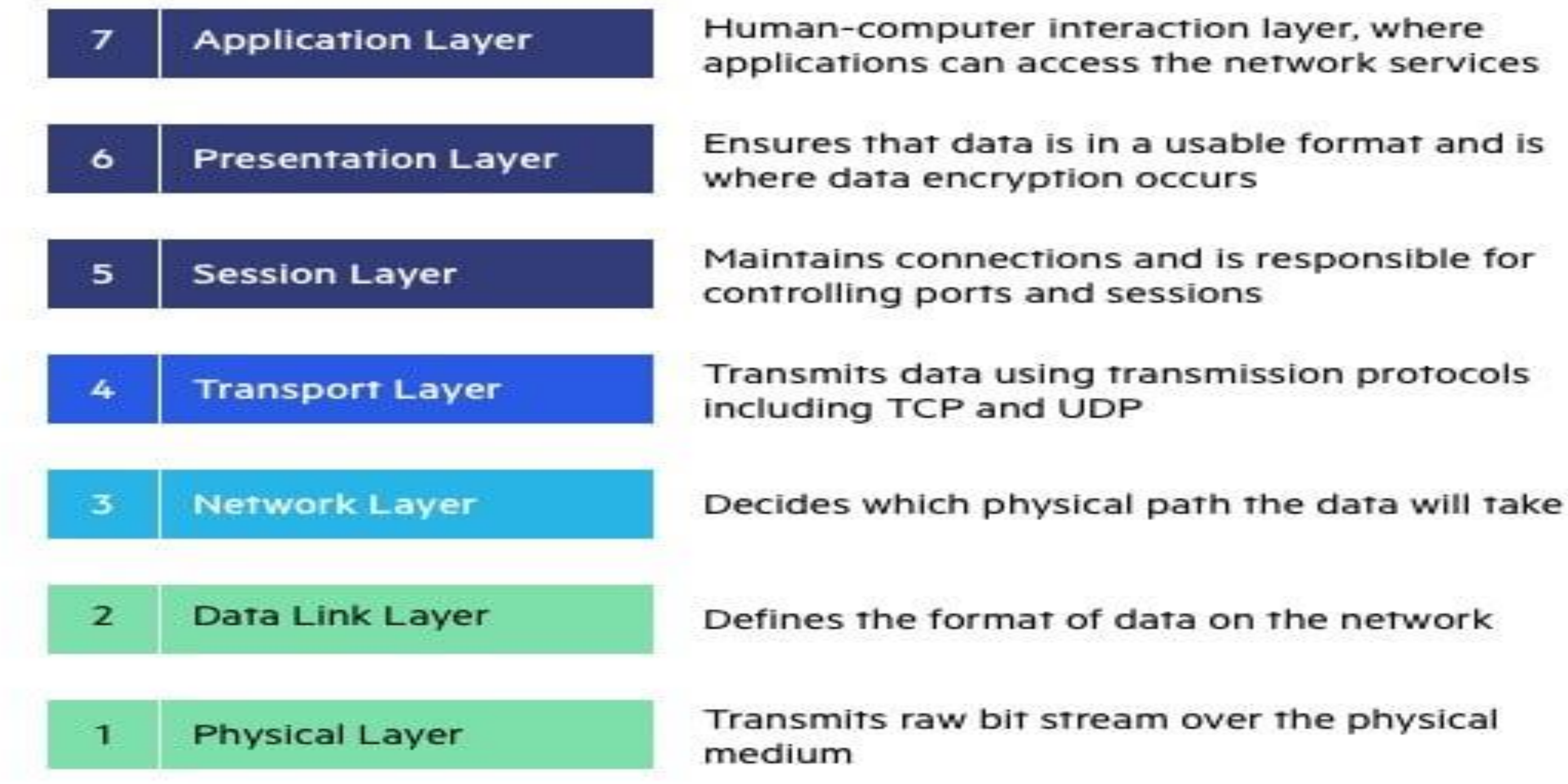


- CLIENT SERVERARCHITECTURE
- OSI MODEL
- TCP/IP
- IP ADDRESSES
- PORT & PROTOCOLS
- SUBNET
- WINDOWS NETWORKING COMMANDS
- CISCO PACKET TRACER

CLIENT SERVER ARCHITECTURE

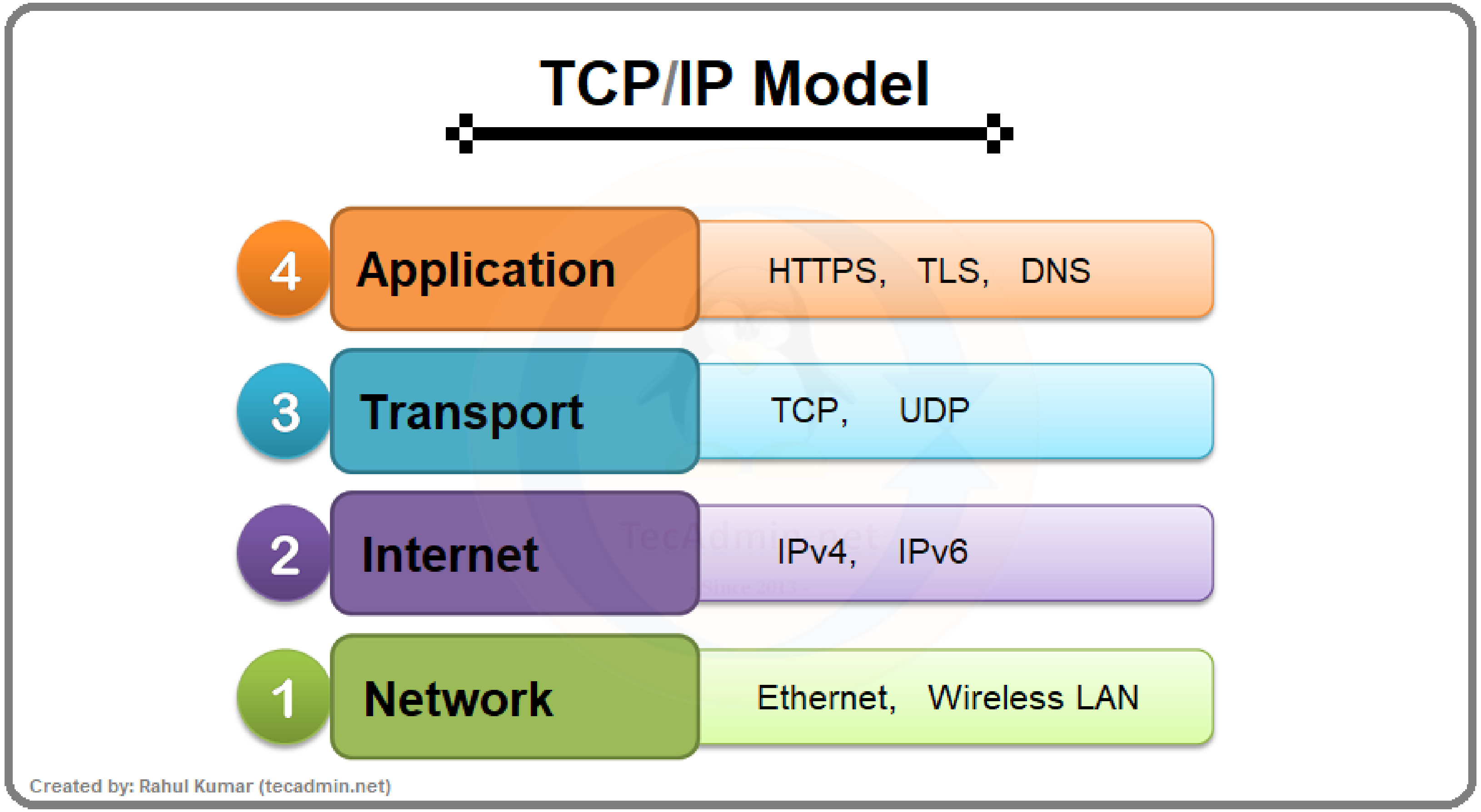


OSI MODEL



7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

TCP/IP MODEL

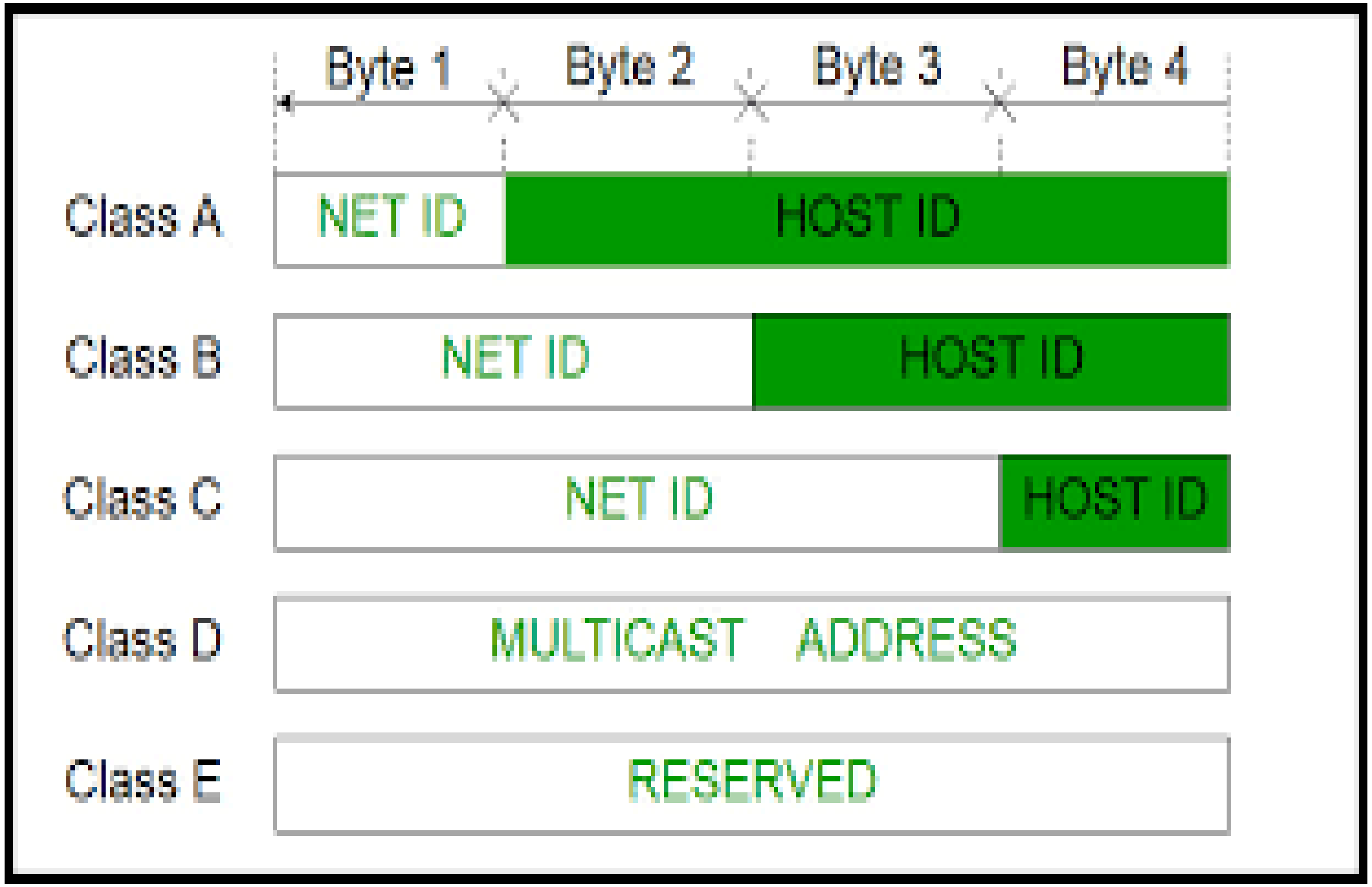


TCP/IP Model

4	Application	HTTPS, TLS, DNS
3	Transport	TCP, UDP
2	Internet	IPv4, IPv6
1	Network	Ethernet, Wireless LAN

Created by: Rahul Kumar (tecadmin.net)

IP Address Classes



Byte 1 Byte 2 Byte 3 Byte 4

Class A NET ID HOST ID

Class B NET ID HOST ID

Class C NET ID HOST ID

Class D MULTICAST ADDRESS

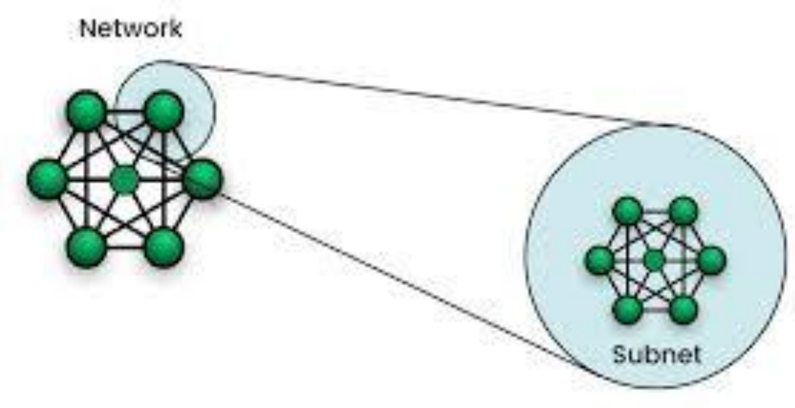
Class E RESERVED

Port and Protocols

- **Port:**
  - A port is a logical endpoint for communication in an operating system.
  - Ports are identified by a 16-bit number, allowing for a total of 65,536 possible ports.
  - Ports are used to distinguish between different services or processes running on a device.
- **Protocol:**
  - A protocol is a set of rules that governs how data is transmitted and received over a network.
  - Common protocols include TCP (Transmission Control Protocol), UDP (User Datagram Protocol), HTTP (Hypertext Transfer Protocol), and FTP (File Transfer Protocol).

SUBNET

- A subnet, or subnetwork, is a network inside a network.
- Subnets make networks more efficient.
- Through subnetting, network traffic can travel a shorter distance without passing through unnecessary routers to reach its destination.



Window Networking Commands

- 1. **PING** : Used for Troubleshooting network connection issues and to check whether the device is online or not
- 2. **IPCONFIG** Used for: Quickly finding your IP address
- 3. **GETMAC** Used for: Quickly finding your MAC address
- 4. **ARP** Used for: Troubleshooting network connection issues
- 5. **HOSTNAME** Used for: Quicking finding your hostname
- 6. **NSLOOKUP** Used for: Troubleshooting network connection issues
- 7. **NBTSTAT** Used for: Troubleshooting NetBIOS issues
- 8. **NET** Used for: Displaying available Net switches
- 9. **NETSTAT** Used for: Displaying network statistics
- 10. **NETSH** Used for: Displaying and configuring network adapters
- 11. **TASKKILL** Used for: Ending processes
- 12. **TRACERT** Used for: Troubleshooting network connection issues
- 13. **PATHPING** Used for: Troubleshooting network connection issues

Cisco Packet Tracer

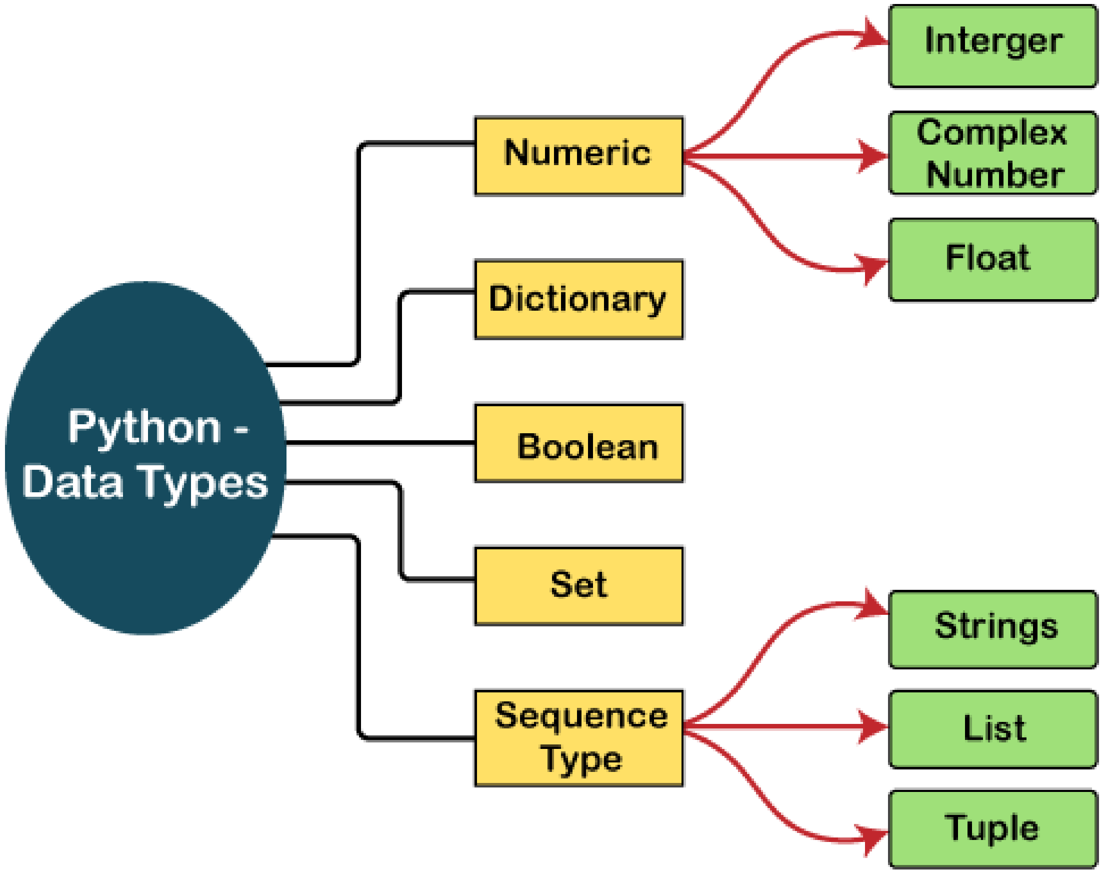
- Cisco Packet Tracer is a free and powerful network simulation software designed for teaching and learning.
- It features a realistic simulation that will help you visualise and assess experiences.
- You can use unlimited devices available in the packet tracer to practice networking labs.
- It supports the majority of networking protocols…. And many more.

Python

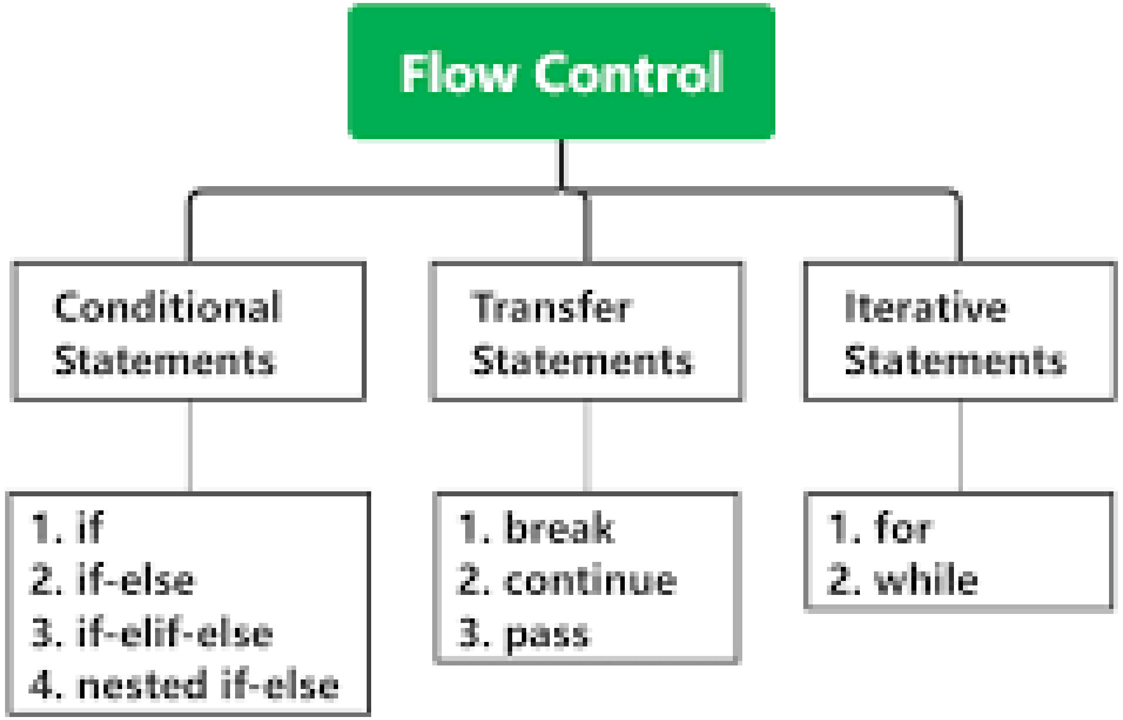
- Python is a high-level, general-purpose, and interpreted programming language that finds extensive use in various domains, including:

- Machine Learning: Python is a popular choice for developing machine learning models due to its simplicity and powerful libraries like TensorFlow and PyTorch.
- Artificial Intelligence: Python’s readability and versatility make it a preferred language for AI research and development.
- Data Analysis: Analysts and data scientists use Python for data manipulation, visualization, and statistical analysis.
- Web Development: Python frameworks like Django and Flask simplify web application development.
- Automation and Scripting: Python serves as an excellent scripting language for automating repetitive tasks.
- Scientific Computing: Scientists and researchers use Python for numerical simulations and data processing.

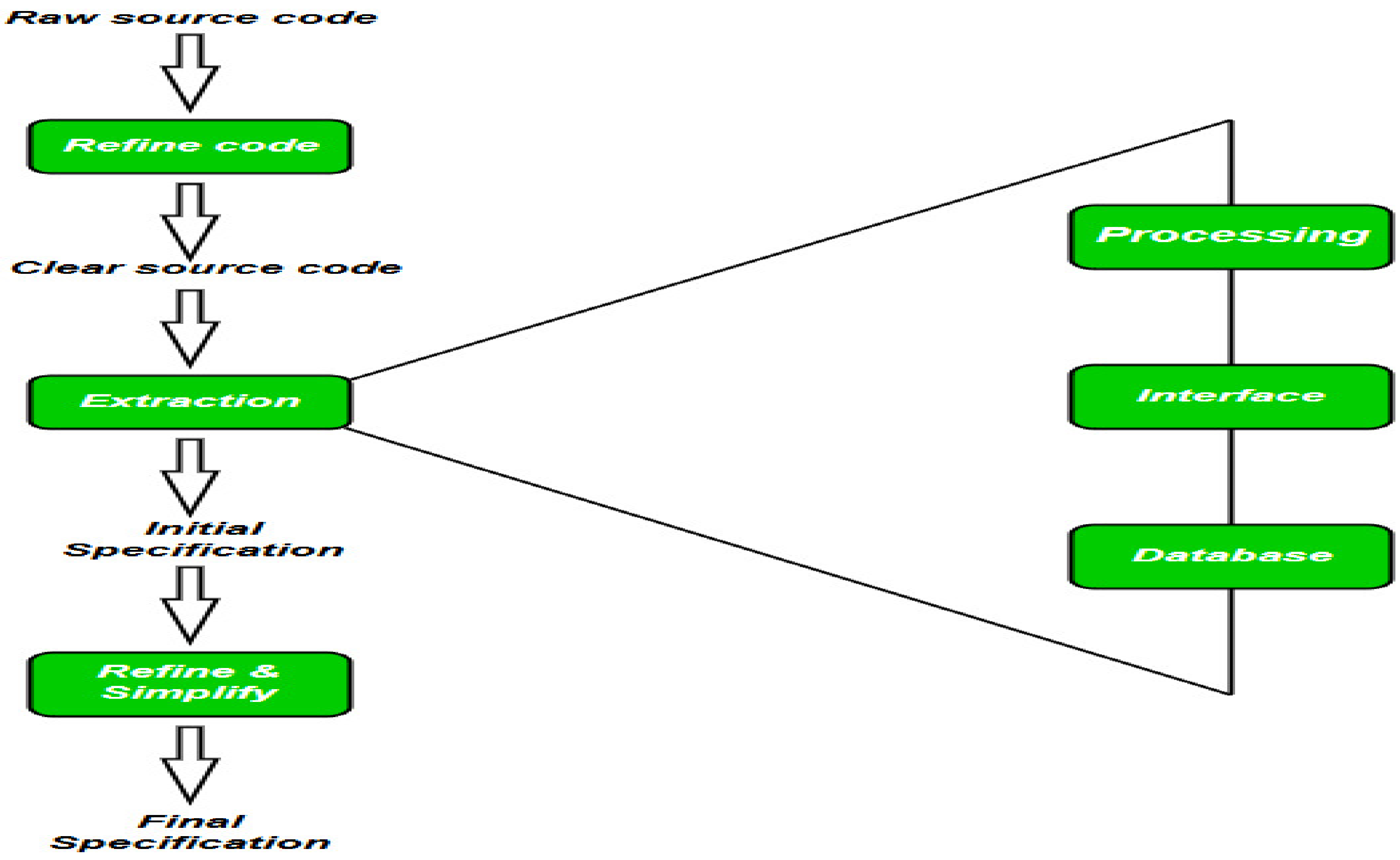
Data Types In Python



Control Structures



Python along with tools like ‘IDA Pro’ and ‘Ghidra’,aids in reverse engineering tasks such as analyzing and understanding binary executables.



Password Cracking

- Finding the password by using some techniques like brute force attack, rainbow attack etc.

Thank You