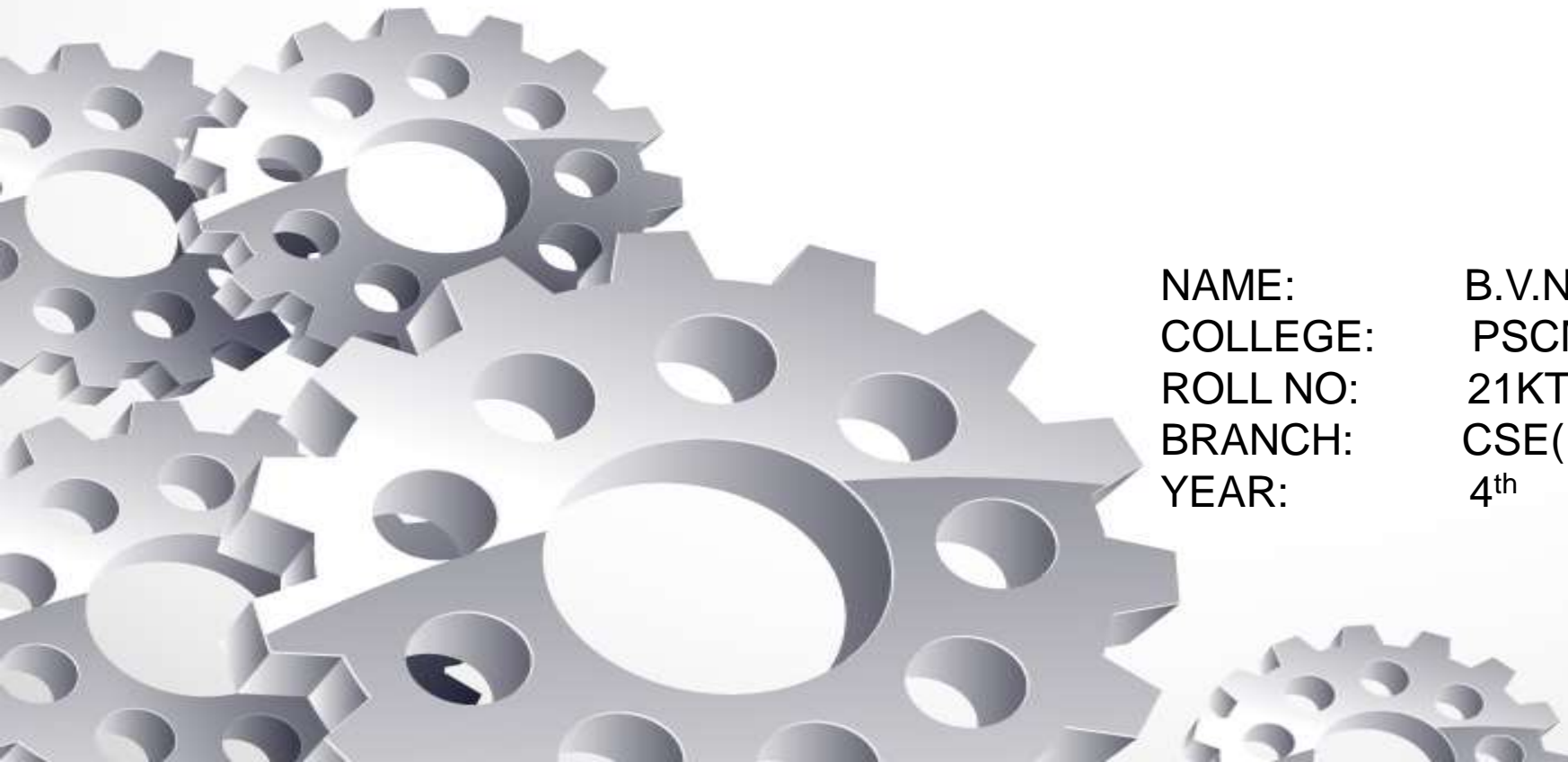



# Cyber Security with QRadar

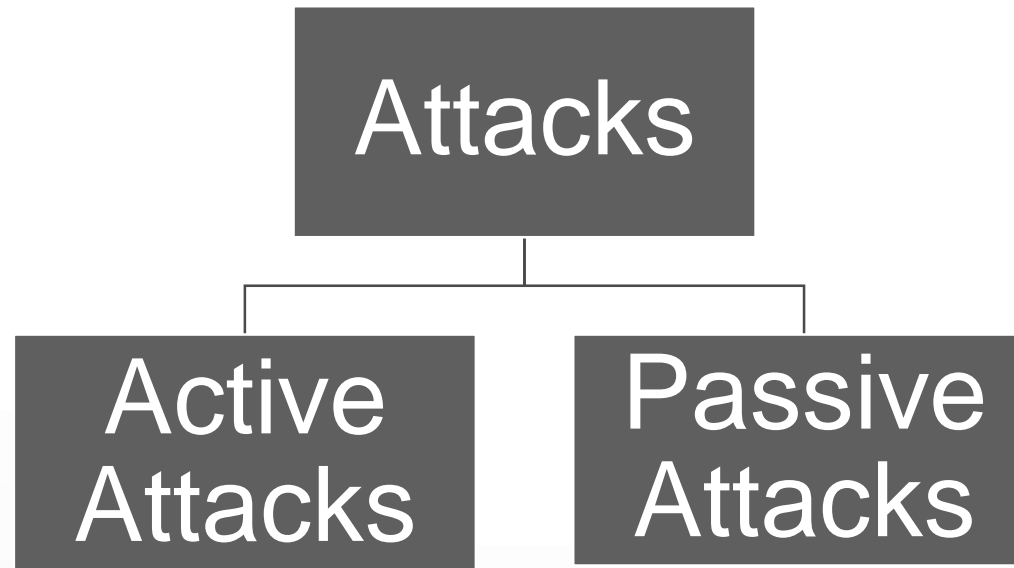


NAME:	B.V.N.VIJAYA DURGA
COLLEGE:	PSCMRCET
ROLL NO:	21KT5A4703
BRANCH:	CSE(IoT & CS incl BCT)
YEAR:	4 <sup>th</sup>



**Introduction :** Providing security to the devices of users and their data/information in the cyber medium from unethical hackers and their attacks is called Cybersecurity. Cyber means the medium where information, resources are being shared in the network or through internet.

### Types of attacks



## Active attacks

Man in the Middle Attack : The attacker positions themselves between the communicating entities, allowing them to eavesdrop on or manipulate the data being exchanged.

Spoofing Attack : A spoofing attack involves the creation of a fake or deceptive identity to manipulate or deceive others.

Dos Attack : A Denial-of-Service (DoS) attack is a malicious attempt to disrupt the normal functioning of a targeted server, service, or network by overwhelming it with a flood of illegitimate requests or traffic. The primary goal of a DoS attack is to make the targeted system or network unavailable to its intended users, causing a denial of service.

Phishing Attack : Phishing is a type of cyberattack where attackers use deceptive tactics to trick individuals into divulging sensitive information, such as login credentials, personal details, or financial information.

Replay Attack : The attacker captures a legitimate data exchange and then replays or resends that data to the target system, tricking it into accepting the duplicated information as if it were legitimate.

## Passive Attacks



### 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

Wiretapping involves the interception of electronic communications, such as phone calls, emails, or data transmissions, by tapping into the communication lines.

## Types of Hackers



### White Hat

- A white hat hacker is an ethical computer security expert or cybersecurity professional who focuses on securing systems and networks.

### Black Hat

- A black hat hacker is an individual who engages in computer security breaches and malicious activities for personal gain, financial profit, or other malicious intentions.

### Grey Hat

- A grey hat hacker is an individual who falls between the ethical boundaries of white hat hackers and the malicious intent of black hat hackers.

## Phases of hacking




Reconn  
aissance

Informati  
on  
Gatherin  
g

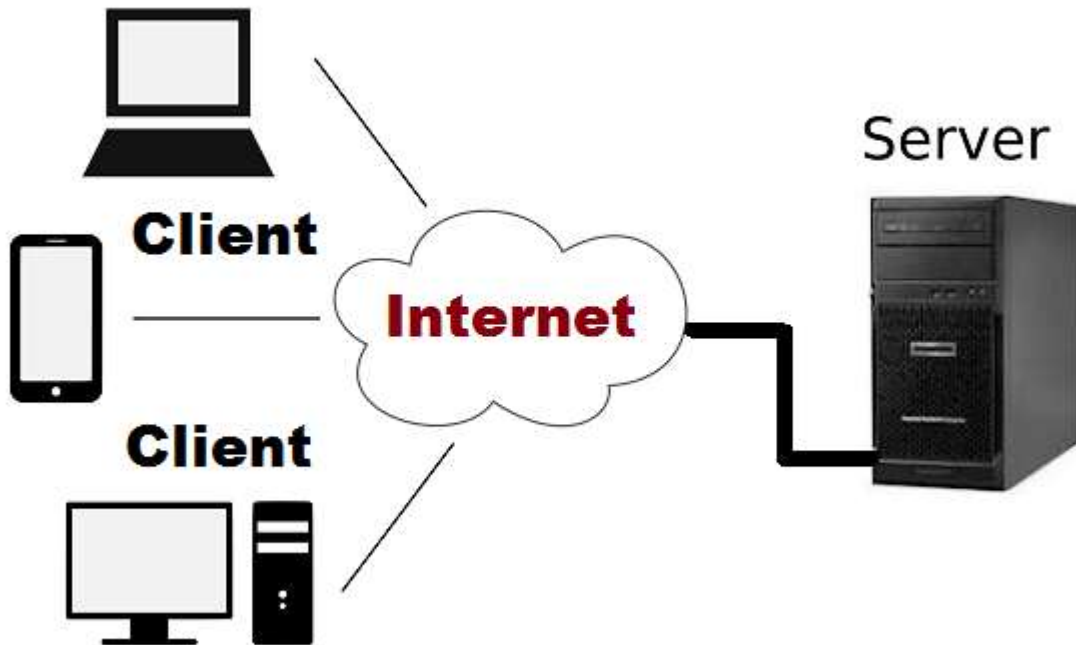
Gaining  
Access

Maintain  
ing  
Access

Removin  
g Tracks

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

## Client Server Architecture



- ✓ A server is the one who provides requested services.
- ✓ Clients are the ones who request services.
- ✓ computing model in which the server hosts, delivers, and manages most of the resources and services requested by the client
- ✓ Examples:
  - Mail servers
  - File servers
  - Web servers

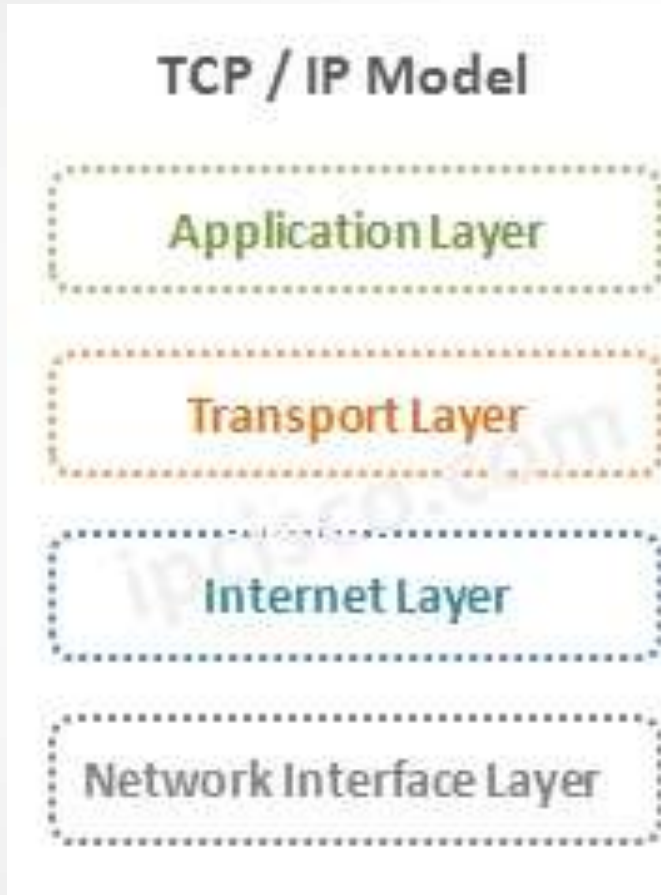


# OSI Model



- ❖ OSI stands for Open Systems Interconnection.
- ❖ Application Layer is the topmost layer and provides several ways for manipulating the data which actually enables any type of user to access the network with ease.
- ❖ Presentation Layer is the 6th layer. This layer is also known as the Translation layer, as this layer serves as a data translator for the network.
- ❖ The Session Layer is the 5th layer. This layer allows users on different machines to establish active communication sessions between them.
- ❖ The Transport Layer is the fourth layer. It is an end-to-end layer used to deliver messages to a host.
- ❖ The Network Layer is the third layer in the OSI model of computer networks. Its main function is to transfer network packets from the source to the destination.
- ❖ The data link layer is the second layer. It is responsible for the node-to-node delivery of data.
- ❖ The physical Layer is the bottom-most layer in the **OSI Model** which is a physical and electrical representation of the system. It consists of various network components such as power plugs, connectors, receivers, cable types, etc.

# TCP/IP model



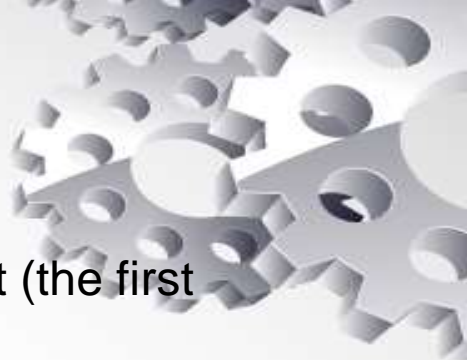
- The main work of TCP/IP is to transfer the data of a computer from one device to another.
- The Application Layer is the topmost layer and provides several ways for manipulating the data which actually enables any type of user to access the network with ease.
- The Transport Layer is the fourth layer. It is an end-to-end layer used to deliver messages to a host.
- It transmits data packets to the link layer.
- It routes each of the data packets independently from the source to the destination, using the optimal route.
- The Network Interface layer is the combination of the data link layer and Physical layer. responsible for the node-to-node delivery of data as well as performing physical layer operations

# IP Addresses

IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.

## IP Address Classes

	8 bits	8 bits	8 bits	8 bits
<b>Class A:</b>	Network	Host	Host	Host
<b>Class B:</b>	Network	Network	Host	Host
<b>Class C:</b>	Network	Network	Network	Host
<b>Class D:</b>	Multicast			
<b>Class E:</b>	Research			



IP addresses are typically divided into classes based on the range of values in their first octet (the first segment of the address).

The classes are:

1. Class A: IP addresses in the range 1.0.0.0 to 126.255.255.255. The first octet is used to identify the network, and the remaining three octets are used to identify hosts on that network.
2. Class B: IP addresses in the range 128.0.0.0 to 191.255.255.255. The first two octets are used to identify the network, and the remaining two octets are used to identify hosts on that network.
3. Class C: IP addresses in the range 192.0.0.0 to 223.255.255.255. The first three octets are used to identify the network, and the last octet is used to identify hosts on that network.
4. Class D (multicast): IP addresses in the range 224.0.0.0 to 239.255.255.255. These addresses are reserved for multicast groups.
5. Class E (reserved): IP addresses in the range 240.0.0.0 to 255.255.255.255. These addresses are reserved for future use or experimental purposes.

Note that the concept of IP address classes has been largely deprecated with the introduction of Classless Inter-Domain Routing (CIDR), which allows for more flexible allocation of IP addresses.

# Port and Protocols



## ✓ Port:

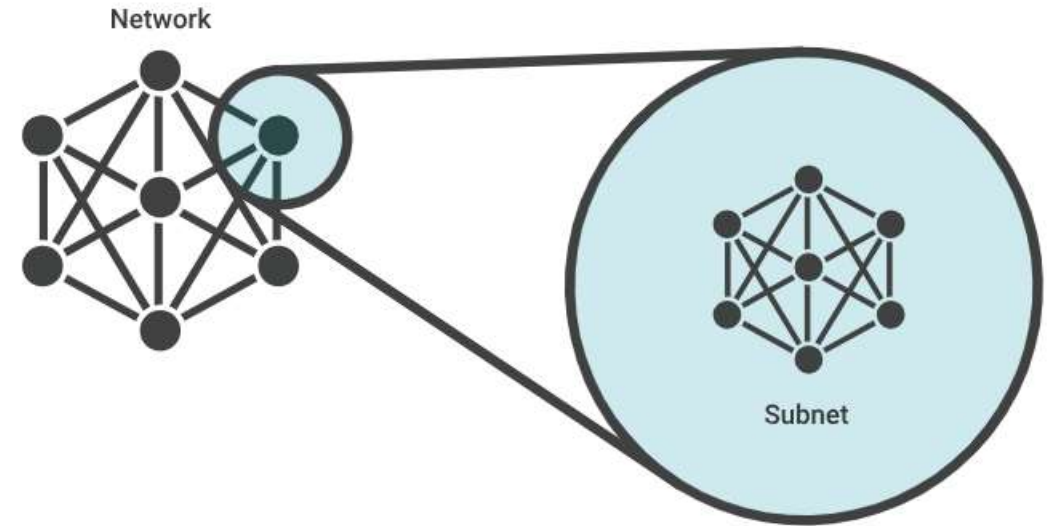
- ✓ A port is a logical endpoint for communication in an operating system.
- ✓ Ports are identified by a 16-bit number, allowing for a total of 65,536 possible ports.
- ✓ Ports are used to distinguish between different services or processes running on a device.

## ✓ 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.





# Windows 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: Quickly 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.

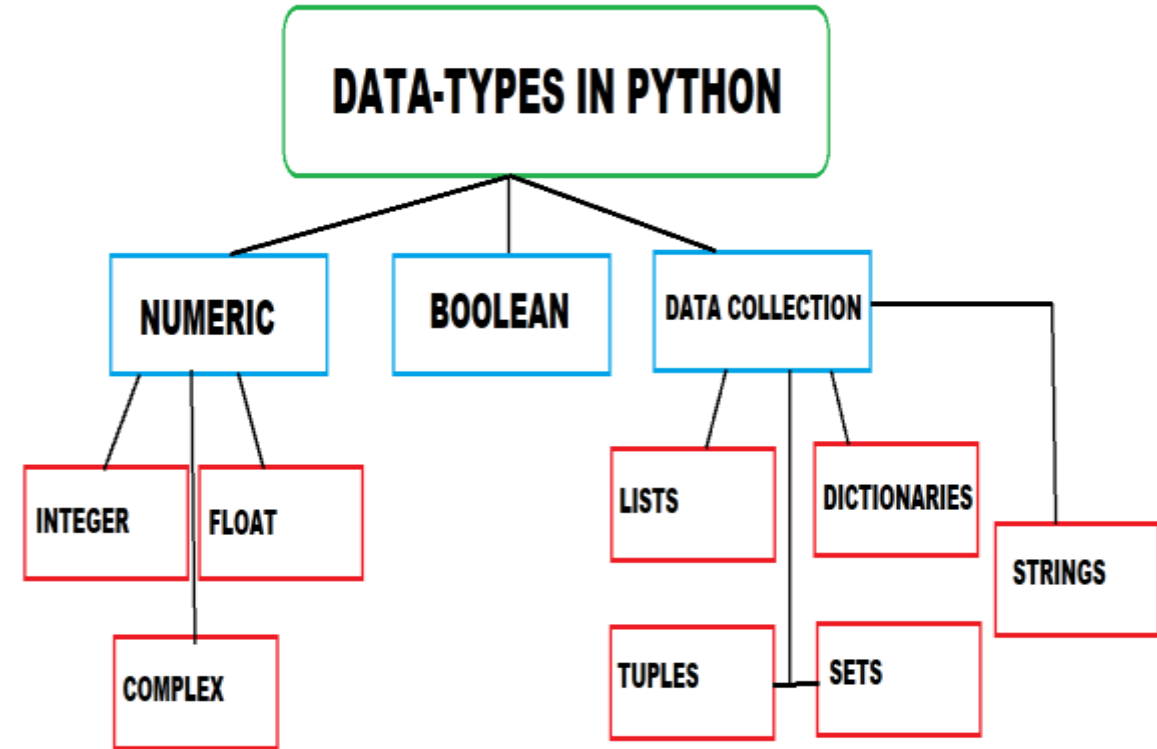




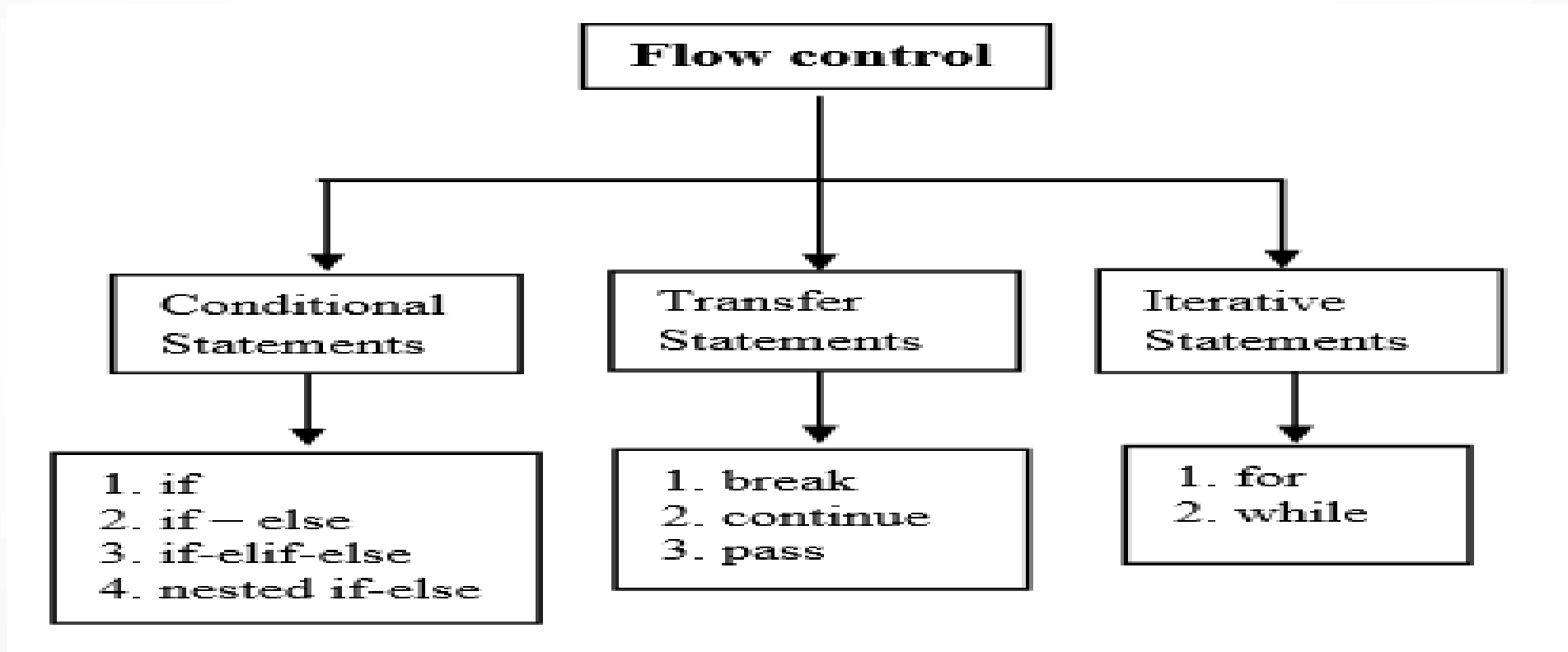
# Python

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

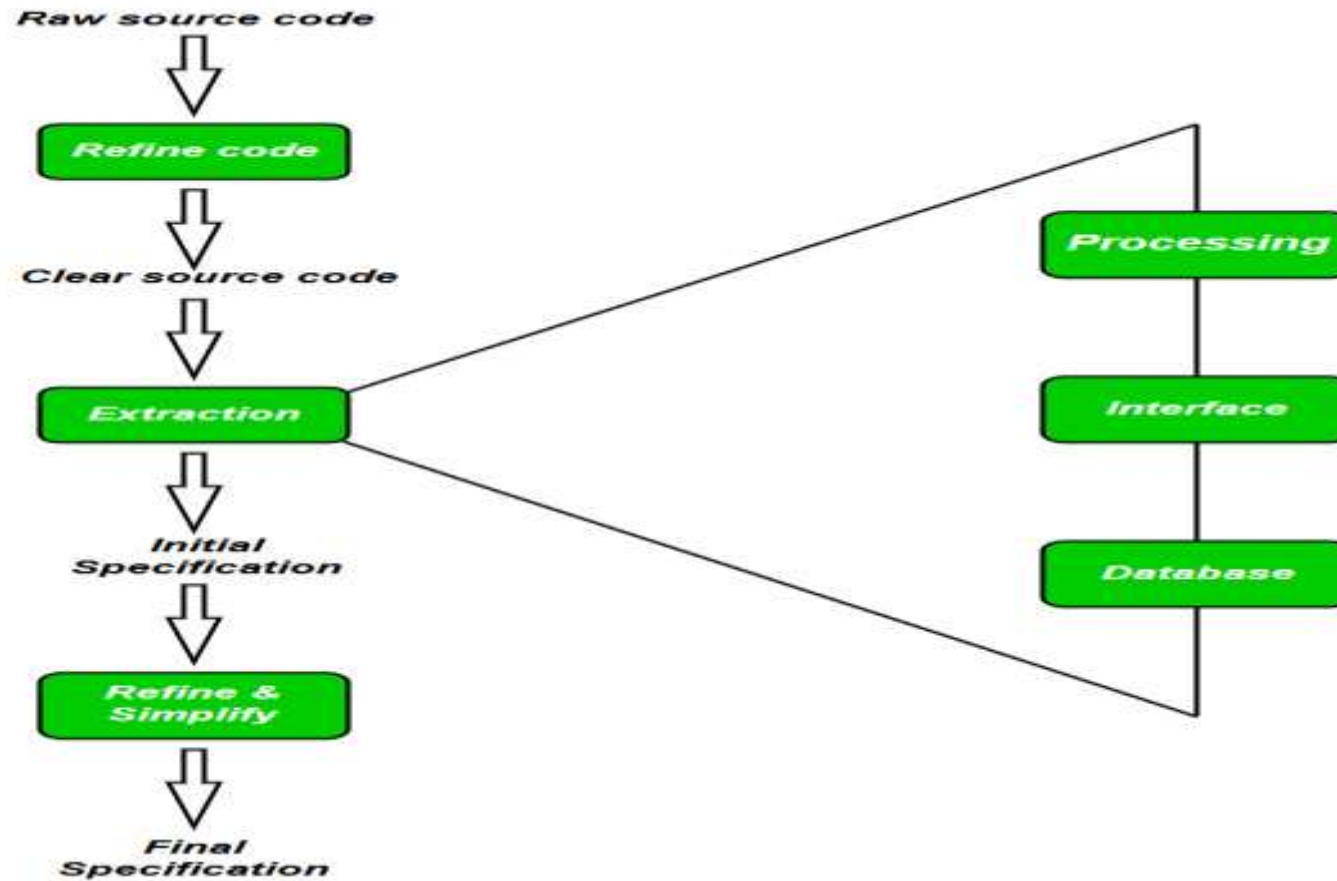
- Machine Learning: Python is a popular choice for developing machine learning models due to its simplicity and powerful libraries like TensorFlow and PyTorch.
- Artificial Intelligence: Python's readability and versatility make it a preferred language for AI research and development.
- Data Analysis: 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.



It provides control structures like if-else statements, loops and exception handling for managing program flow.



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.



Password cracking is the process of attempting to gain unauthorized access to a computer system or online account by guessing or systematically trying different passwords until the correct one is found. This is often done using specialized software or tools that automate the process of trying different combinations of characters to find the correct password.

