Cyber Security with IBM QRadar

CHITTALA SWATHI
B. TECH
20ME1A4612
RCEE

INTRODUCTION:

- Cybersecurity refers to any technology, measure or practice for preventing cyberattacks or mitigating their impact. Cybersecurity aims to protect individuals' and organizations' systems, applications, computing devices, sensitive data and financial assets against computer viruses, sophisticated and costly ransomware attacks, and more.

Types of cyber Attacks:

Active attacks
Passive attacks

ACTIVE ATTACKS

- Man-in-the-middle attacks
- Spoofing
- Dos attack
- Phishing attack
- Replay attack

Man-in-the-middle attacks: A man-in-the-middle (MitM) attack is a type of cyber attack in which the attacker secretly intercepts and relays messages between two parties who believe they are communicating directly with each other. The attack is a type of eavesdropping in which the attacker intercepts and then controls the entire conversation.

Spoofing: spoofing: Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source. Spoofing can apply to emails, phone calls, and websites, or can be more technical, such as a computer spoofing an IP address, Address Resolution Protocol (ARP), or Domain Name System (DNS) server.

Dos attack: A denial-of-service (DoS) attack is a type of cyber attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning.

Phishing attack: “Phishing” refers to an attempt to steal sensitive information, typically in the form of usernames, passwords, credit card numbers, bank account information or other important data in order to utilize or sell the stolen information.

Replay attack: A replay attack is a type of network attack in which an attacker captures a valid network transmission and then retransmit it later. The main objective is to trick the system into accepting the retransmission of the data as a legitimate one.

PASSIVE ATTACKS

- Computer Surveillance
- Network Surveillance
- Wire Tapping

Computer Surveillance: Computer surveillance refers to the monitoring of computer activities, data, and communications to gather information, track activities, or ensure security. Surveillance can be conducted for various purposes, ranging from legitimate and legal activities such as network security and employee monitoring to more controversial and potentially intrusive practices.

Network Surveillance: Network surveillance involves monitoring and analyzing data traffic on computer networks to ensure their security, performance, and integrity. This process helps detect and prevent various security threats, unauthorized access, and suspicious activities. Network surveillance is crucial for maintaining the overall health and functionality of computer networks

Wire Tapping: Wiretapping refers to the interception of telephone or electronic communications, often for the purpose of surveillance or gathering information. It involves the monitoring of conversations or data transmitted over communication networks without the knowledge or consent of the parties involved.

TYPES OF HACKERS

- White Hat
- Black Hat
- Grey Hat

White Hat: Ethical hackers who use their skills to improve cybersecurity, often employed by organizations to identify and fix vulnerabilities legally.

Black Hat: Malicious hackers who exploit vulnerabilities for personal gain or to cause harm, engaging in illegal activities such as data theft, fraud, and system disruption.

Grey Hat: Hackers whose actions and motivations fall between white hat and black hat, sometimes disclosing vulnerabilities but without explicit authorization, resulting in ethically ambiguous behavior.

PHASES OF HACKING

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Clearing Tracks

Reconnaissance: Gathering information about the target, including vulnerabilities, network architecture, and key personnel.

Scanning: Actively probing the target's network to identify potential entry points and vulnerabilities.

Gaining Access: Exploiting vulnerabilities to gain unauthorized entry into the target system or network.

Maintaining Access: Ensuring continued, persistent access to the target system or network for prolonged malicious activities.

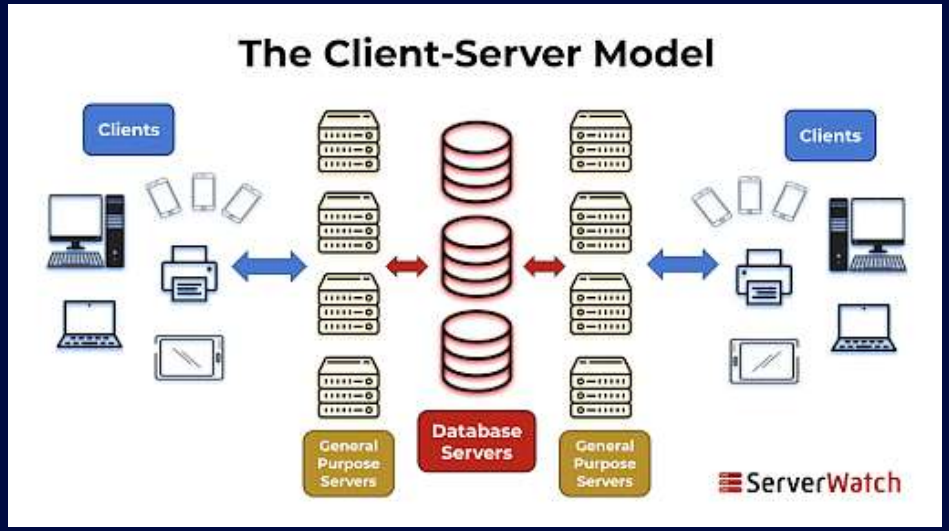
Clearing Tracks: Erasing or altering evidence of the attack to evade detection and attribution.

INTRODUCTION TO NETWORKING

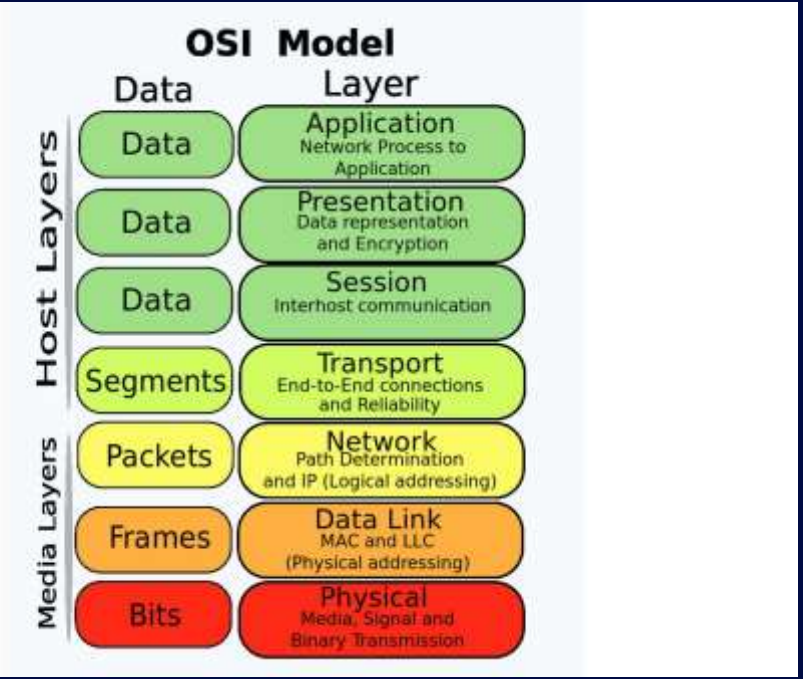
- Client ServerArchitecture
- OSI Model
- TCP/IP
- IP Addresses
- Port & Protocols
- Subnet
- Windows Networking Commands
- CISCO Packet Tracer

CLIENT SERVERARCHITECTURE:

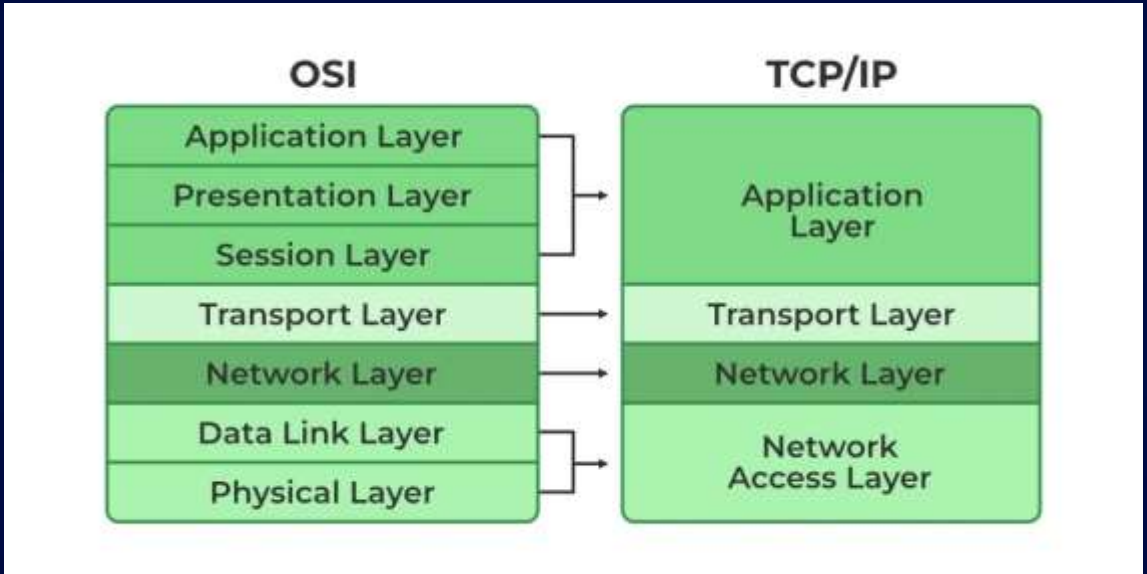
- Client-Server Architecture is a computing model where tasks or processes are divided between "clients" and "servers." This architecture is commonly used in networking and distributed computing. In a client-server model, the client and server devices or software applications interact with each other to accomplish a specific task.



OSI MODEL


OSI Model
Data
Layer
Host Layers
Media Layers
Data
Application
Network Process to Application
Data
Presentation
Data representation and Encryption
Data
Session
Interhost communication
Segments
Transport
End-to-End connections and Reliability
Packets
Network
Path Determination and IP (Logical addressing)
Frames
Data Link
MAC and LLC (Physical addressing)
Bits
Physical
Media, Signal and Binary Transmission

TCP/IP


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

- **IP ADDRESSES**

  An Internet Protocol (IP) address is the unique identifying number assigned to every device connected to the internet. An IP address definition is a numeric label assigned to devices that use the internet to communicate.

- **PORT & PROTOCOLS**

  PORTS

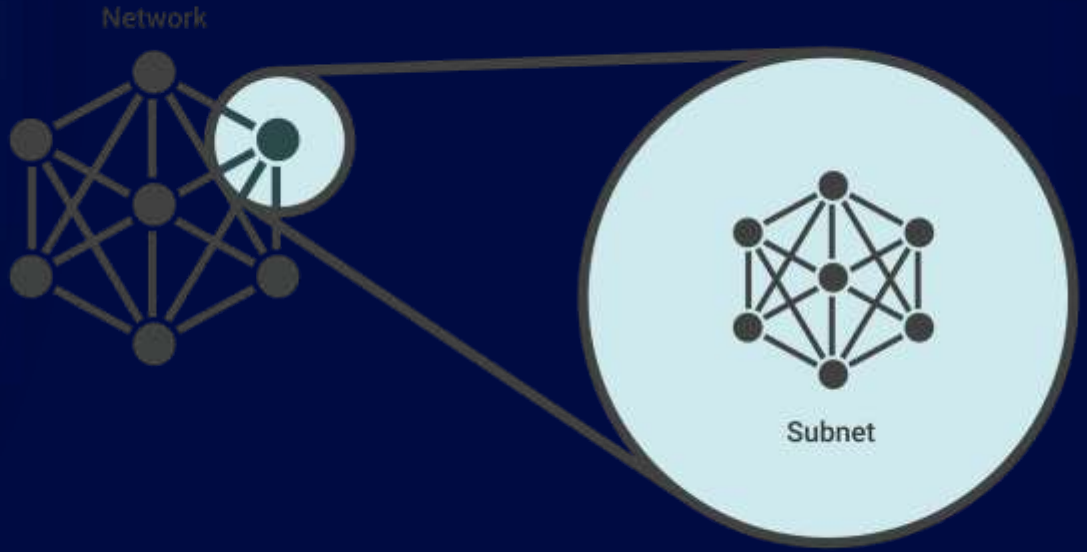
  - A port is a logical endpoint for communication in an operating system.
  - Ports are identified by a 16-bit number, allowing for a total of 65,536 possible ports.
  - Ports are used to distinguish between different services or processes running on a device.

  PROTOCOLS:

  - 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: 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

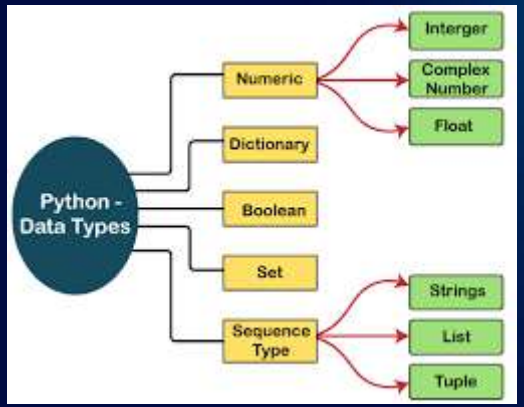
CISCO PACKET TRACER

- 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.

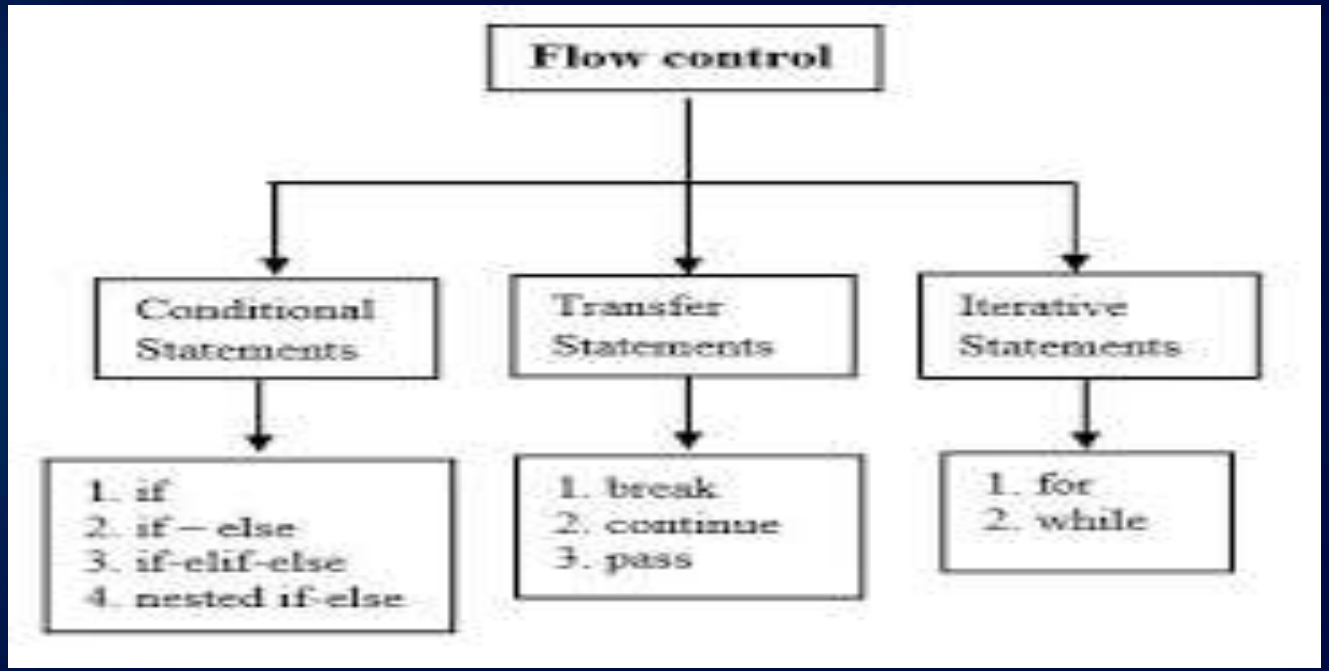
PYTHON

- Python is a high-level, general-purpose programming language known for its readability, simplicity, and versatility. It was created by Guido van Rossum and first released in 1991. Python has gained widespread popularity in the software development community due to its emphasis on code readability, ease of use, and support for multiple programming paradigms.

- **DATA TYPES:** Python has several built-in data types, including numeric types (int, float, complex), string (str), boolean (bool), and collection types (list, tuple, dict, set). Each data type has its own set of properties, methods, and behaviors that allow programmers to manipulate and process data effectively in their programs.



Control structures:

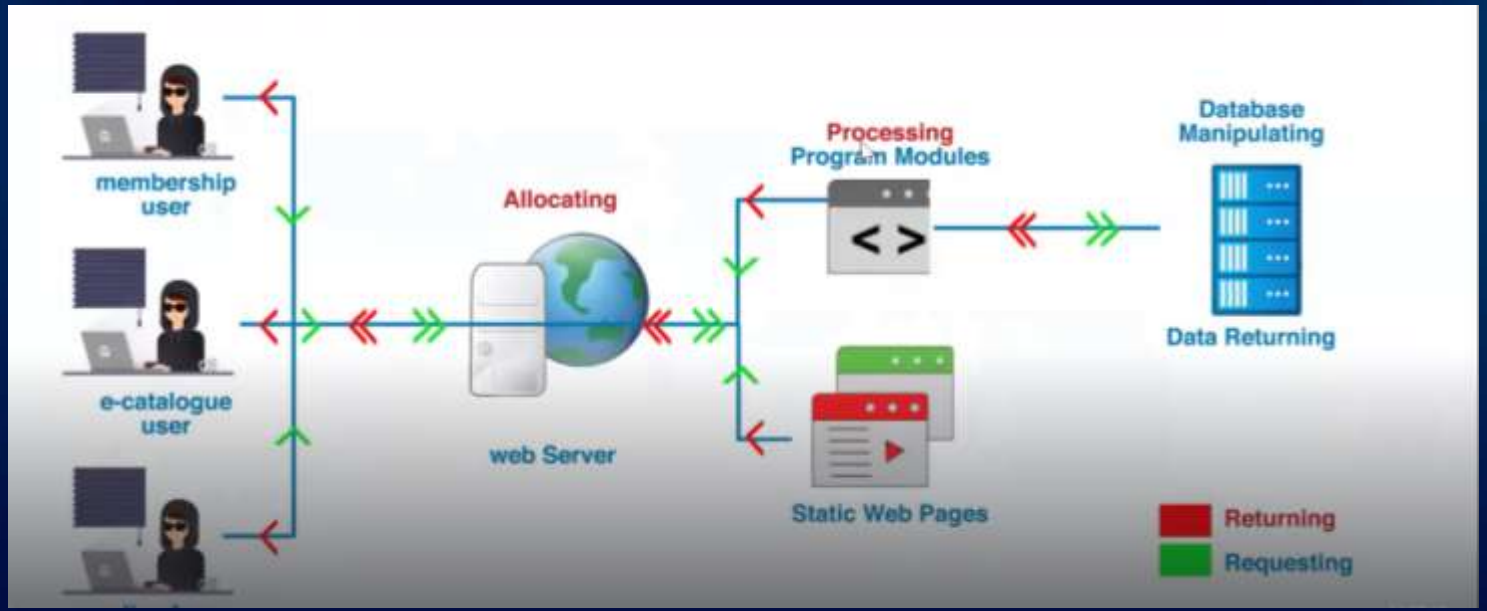


PYTHON FOR HACKERS:

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

WEB APPLICATION

- A web application is a computer program that is accessed through a web browser over a network, typically the internet. Web applications are designed to work across different devices and platforms, including desktop computers, laptops, smartphones, and tablets.



WEB SERVICES:

- A web service is a software system that supports interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically, web Service Definition Language, or WSDL). web services fulfill a specific task or a set of tasks.

VULNERABILITIES STACK: