Introduction to Cyber Security (Day-1)

Name: T. Mohan Sri Sai

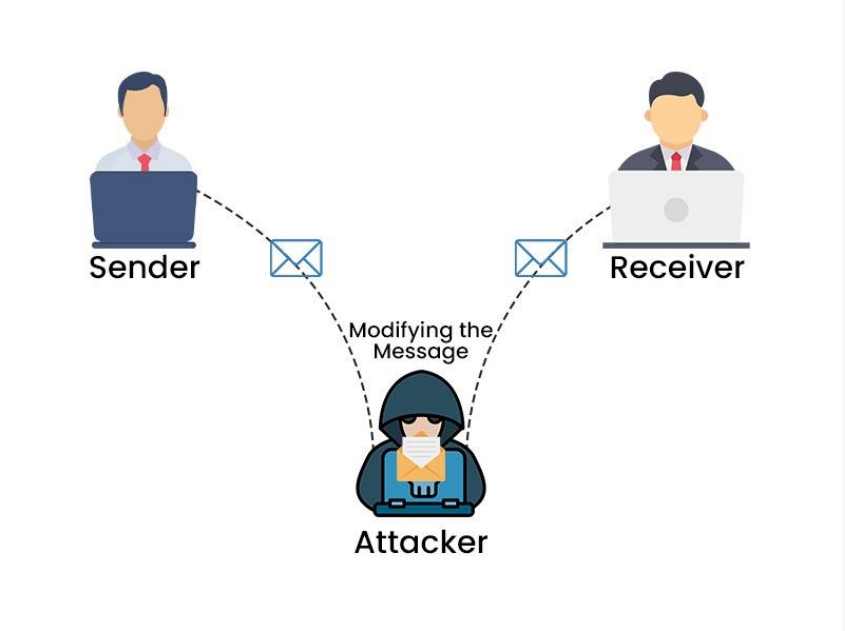
Rollno: 208H1A0540

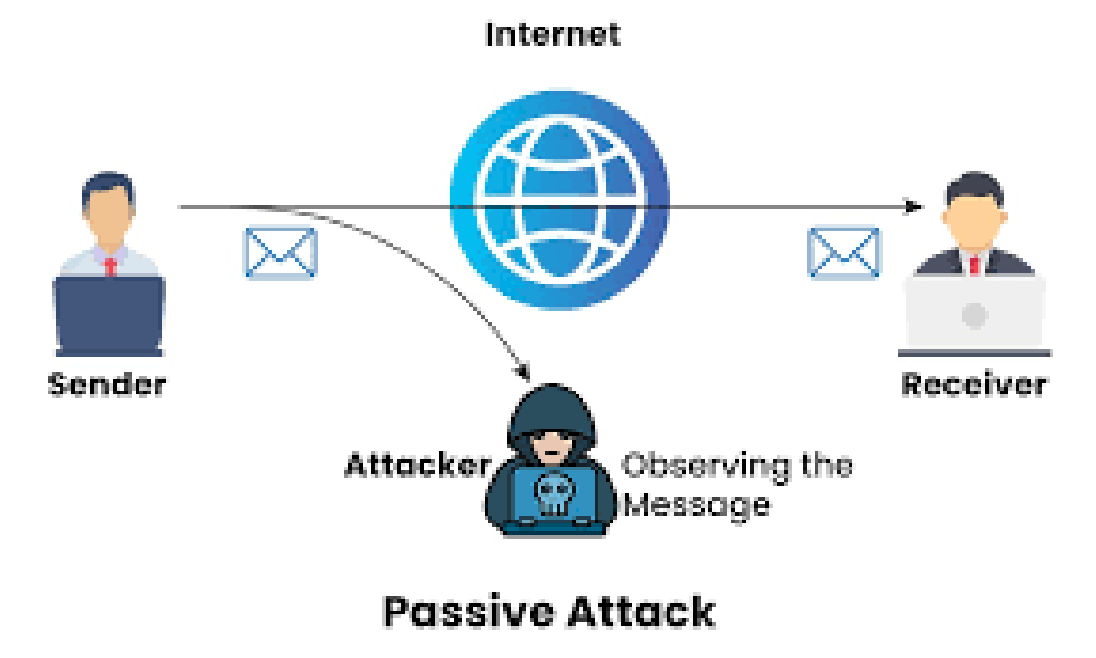
College: MVR College of Engineering & Technology

Types of Cyber Attacks

Active Attacks: These attacks directly target a system or network, aiming to disrupt, damage, or steal data.

- **Man-in-the-middle attack**: Intercepts communication between two parties to steal data or control the flow of information.
- **Spoofing**: Imitates a legitimate user or device to gain unauthorized access.
- **Denial-of-service (DoS) attack**: Overwhelms a system with traffic, making it unavailable to legitimate users.
- **Phishing attack**: Tricks users into revealing personal information or clicking malicious links.
- **Replay attack**: Captures and retransmits legitimate data to gain unauthorized access or manipulate information.





Passive Attacks: These attacks eavesdrop on communication or monitor network activity without directly affecting systems.

- **Computer surveillance**: Monitors a computer's activity to gather information about the user.
- **Network surveillance**: Monitors network traffic to gather information about the network and its users.
- **Wire tapping**: Intercepts communication signals to steal information.

Categories of Hackers

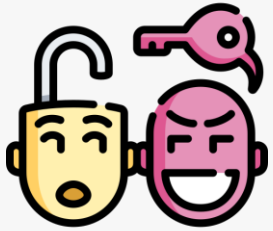
- **Black Hat Hackers:** Malicious actors who exploit vulnerabilities to steal data, disrupt operations, or cause damage.
- **White Hat Hackers:** Ethical hackers who use their skills to identify and fix vulnerabilities in systems with permission from the owner.
- **Gray Hat Hackers:** Operate in a legal gray area, sometimes using their skills for both good and bad purposes.

Essential Cybersecurity Terminology

Malware.

IP Address

Phishing



Social Engineering

Virtual Private Network (VPN)

Antivirus.

Firewall

Ransomware

Penetration Testing (Pentesting)

Phases of Hacking

1

Reconnaissance: Gatherin g information about the target system or network to identify vulnerabilities.

2

Scanning: Using automated tools to identify specific vulnerabilities in the target system.

3

Gaining Access: Exploiting vulnerabilities to gain unauthorized access to the system.

4

Maintaining Access: Establishing methods to maintain access to the system for extended

5

Clearing Tracks: The attacker clears all kinds of logs and malicious malware related to the attack

Introduction to Networking (Day-2)

Name: T. Mohan Sri Sai

Rollno: 208H1A0540

College: MVR College of Engineering & Technology

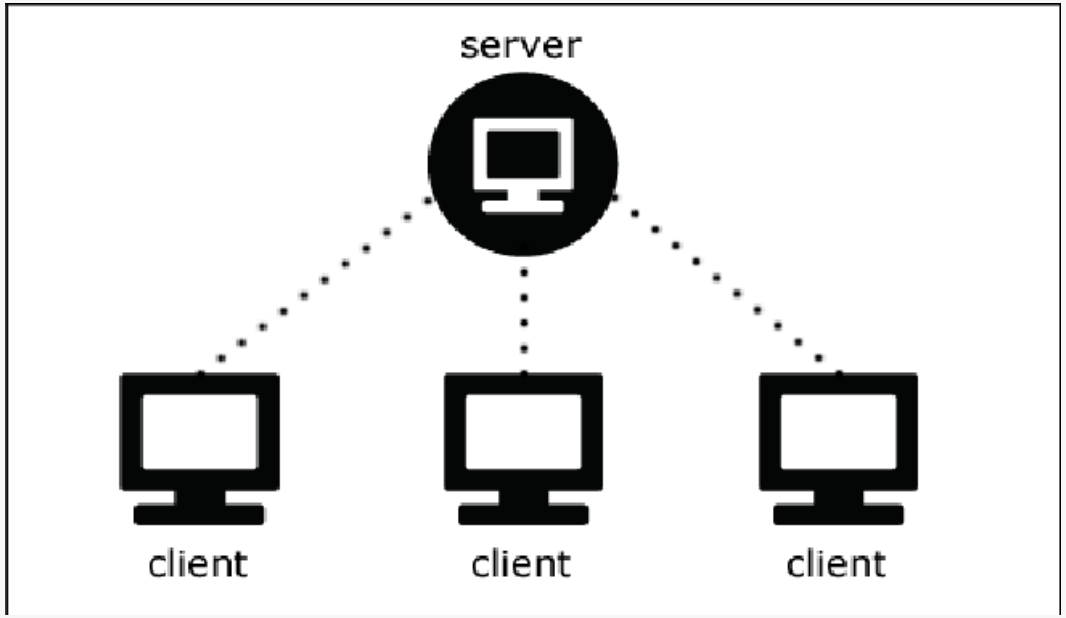
Client-Server Architecture

Client: A computer program or device that requests resources from a server.

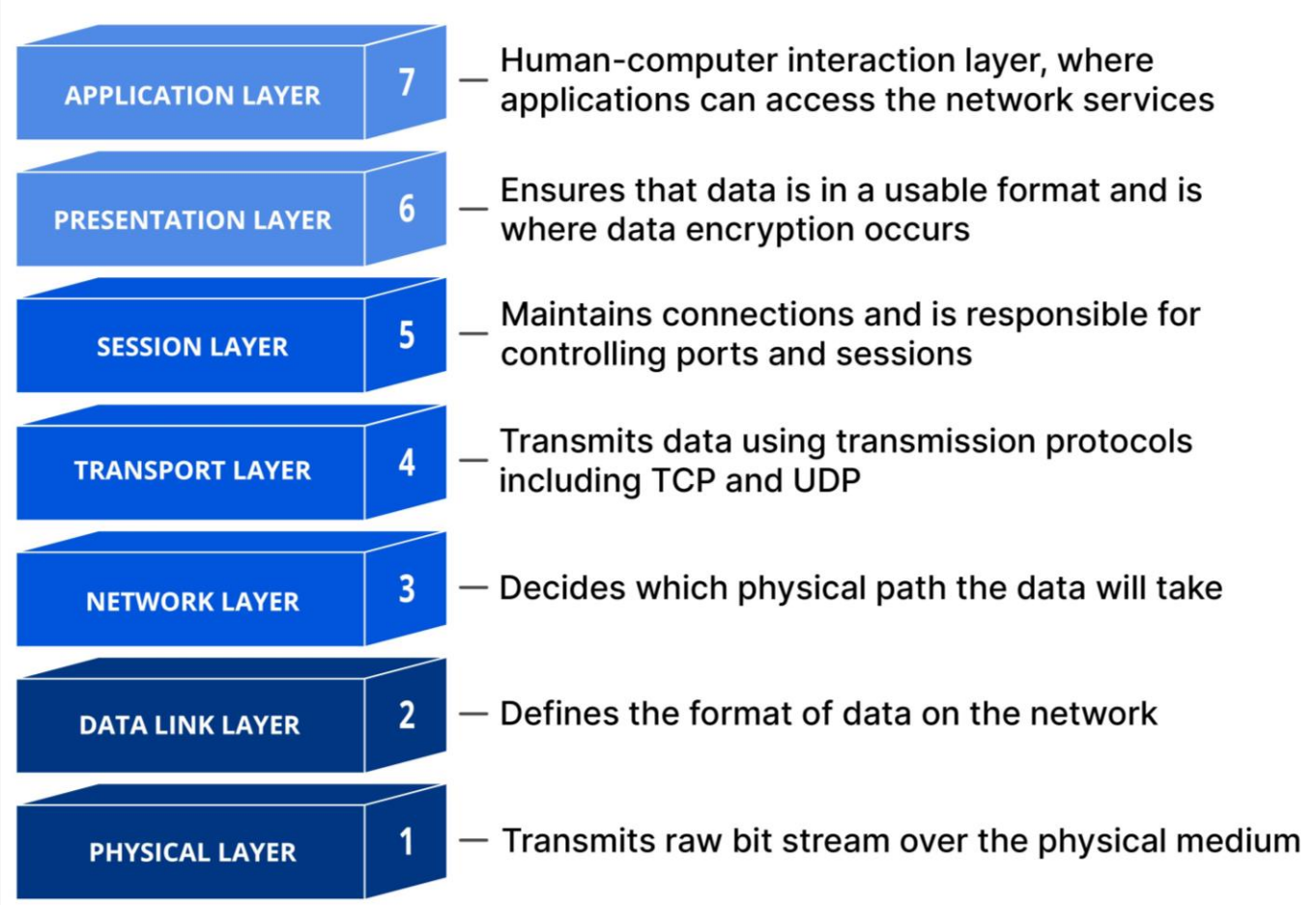
Server: A computer program or device that provides resources to clients.

Benefits:

- Centralized resource management
- Scalability
- Security



OSI Model



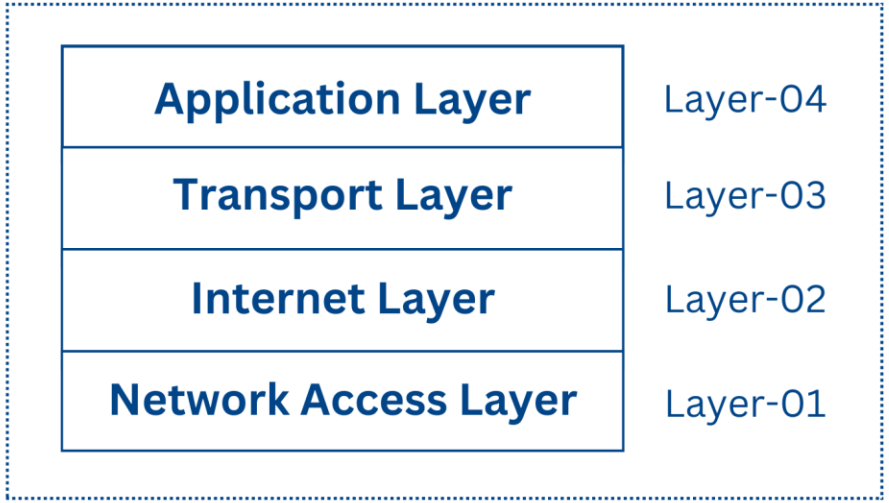
Open Systems Interconnection (OSI) model: A conceptual framework for network communication.

Layers:

- Physical
- Data Link
- Network
- Transpor
- Session
- Presentation
- Application

TCP/IP Protocol

- **Transmission Control Protocol/Internet Protocol (TCP/IP):** A suite of protocols governing communication on the internet.
- **Layers:**
- **Application:** Provides network services to user applications (e.g., HTTP, FTP).
- **Transport:** Provides reliable data transfer (TCP) or datagram service (UDP).
- **Internet:** Handles addressing and routing of data packets (IP).
- **Network Access:** Encapsulates data onto the physical network medium.



IP Address

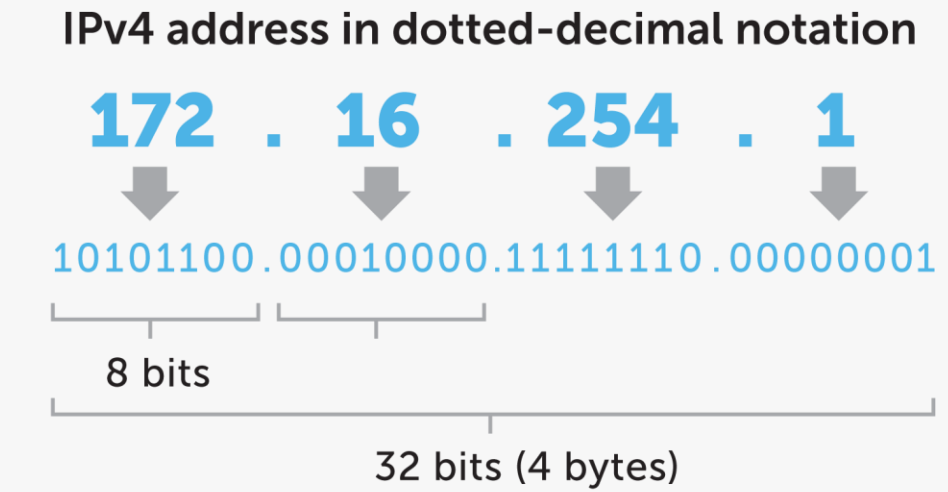
Internet Protocol (IP) address: A unique identifier assigned to a device on a network.

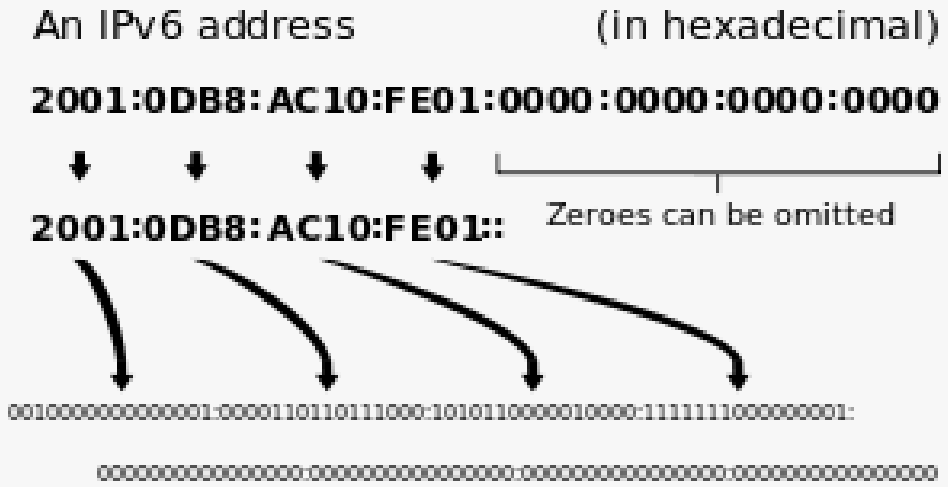
IPv4:

- 32-bit address
- Limited address space (approx. 4.3 billion addresses)
- Dotted decimal notation (e.g., 192.168.1.1)

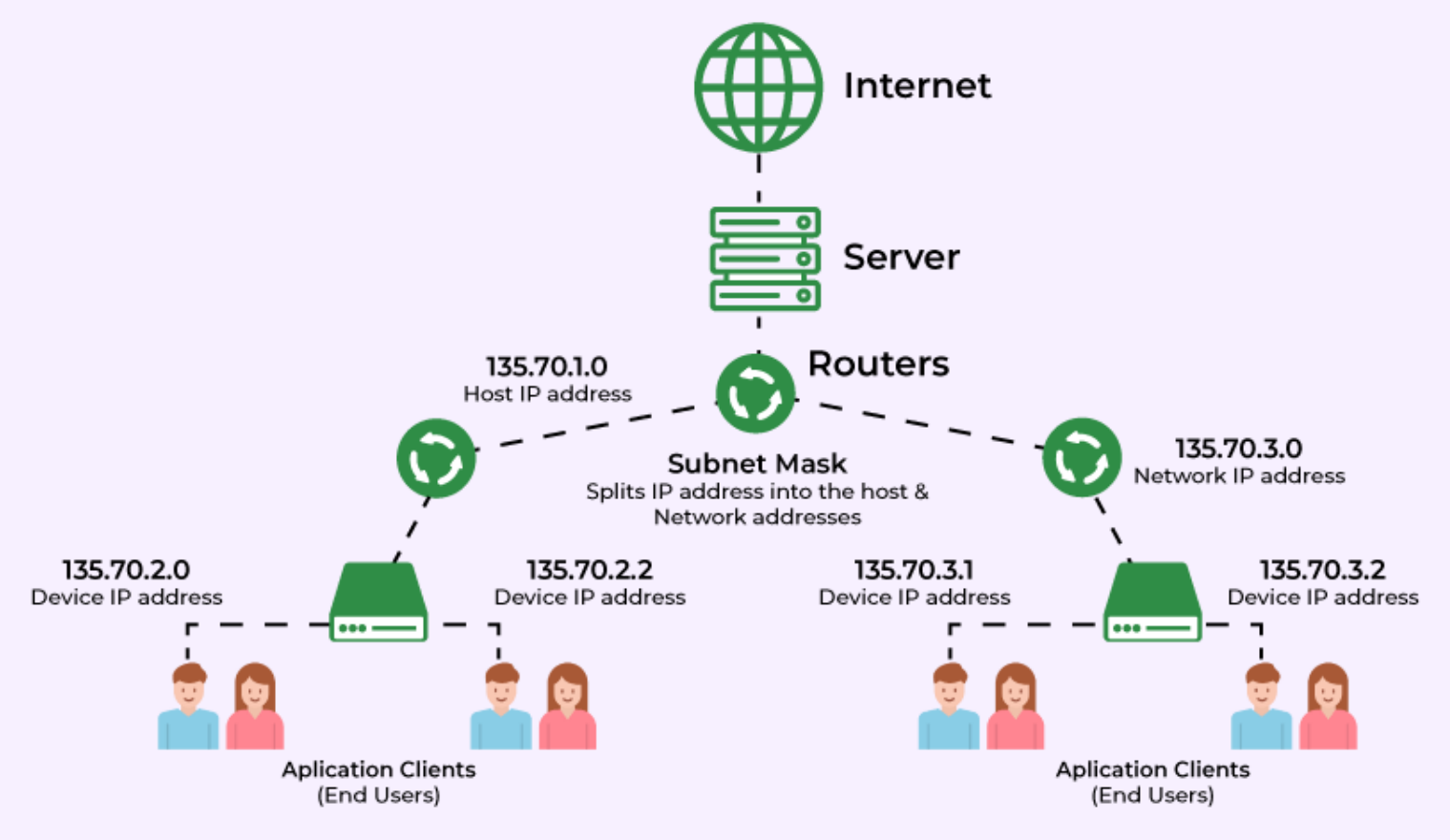
IPv6:

- 128-bit address
- Vastly larger address space (virtually unlimited)
- Hexadecimal notation





Subnetting



- **Subnetting:** Dividing a large network into smaller logical networks called subnets.
- **Benefits:**
- Improved network efficiency
- Enhanced security
- Better network management

Windows Networking Commands

- **Basic Windows Networking Commands:**
- **ipconfig:** Displays information about network adapters, including IP address, subnet mask, default gateway, and DNS server addresses.
- **ping:** Tests connectivity to a specific IP address or hostname.
- **tracert:** Traces the route taken by a packet to reach a destination, showing the hops it takes along the way.
- **nslookup:** Looks up information about a hostname, including its IP address and DNS records.

Cisco Packet Tracer

Cisco Packet Tracer: A network simulation tool.

Features:

- Create and simulate network topologies
- Configure network devices
- Troubleshoot network problems
- Experiment with network concepts

Python for Hacking (Day-3)

Name: T. Mohan Sri Sai

Rollno: 208H1A0540

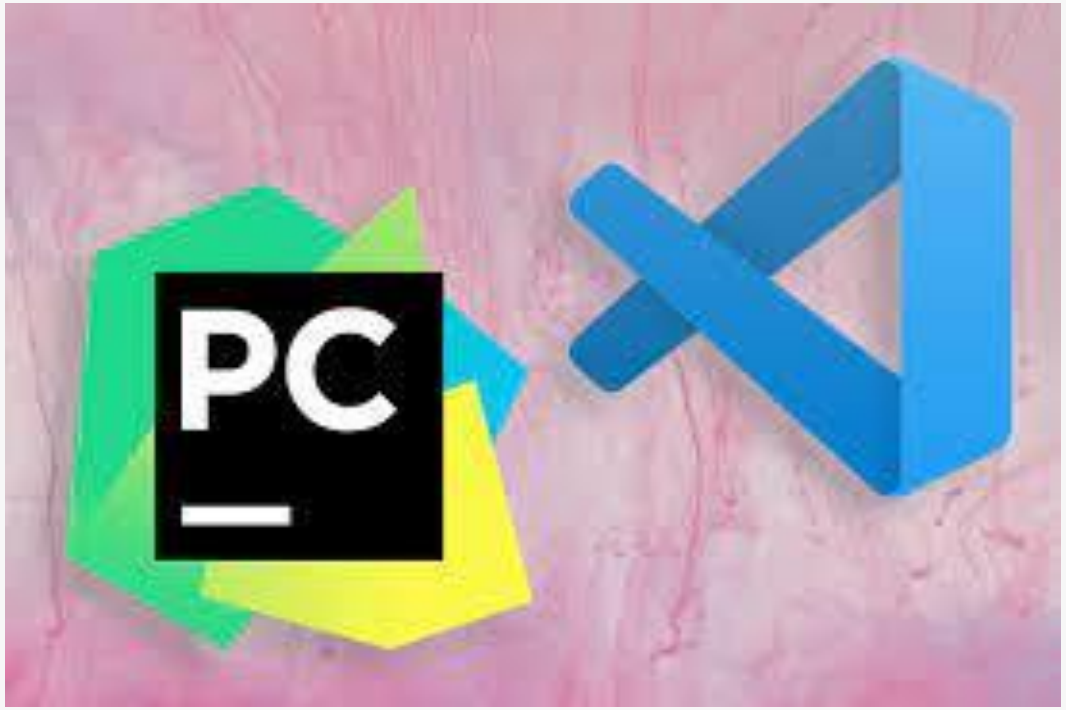
College: MVR College of Engineering & Technology

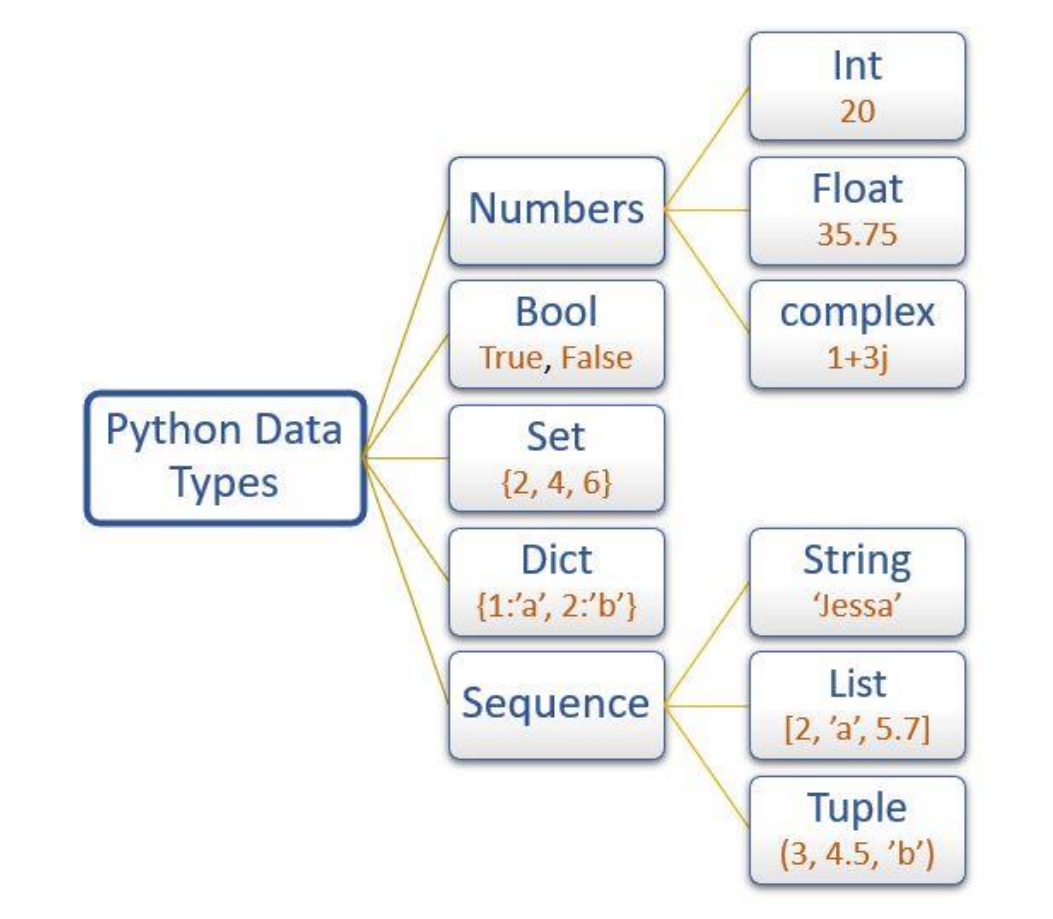
Why Python?

- **Versatility**: Python's flexibility allows for a wide range of hacking tasks.
- **Large community**: Access to numerous libraries and resources for hacking.
- **Ease of learning**: Python's simple syntax makes it accessible to beginners.

Setting up Python

- Download and install Python from python.org.
- Choose an IDE or text editor for coding (e.g., PyCharm, Visual Studio Code).
- Set up a virtual environment for project isolation.





Python Basics

- Data types: Integers, floats, strings, lists, dictionaries, etc.
- Control structures: if statements, loops (for, while), etc.
- Functions: Define reusable blocks of code.
- File handling: Read from and write to files.

Advanced Python Concepts

- **Networking**: Utilize libraries like socket for network communication.
- **Web scraping**: Extract data from websites using libraries like BeautifulSoup.
- **Cryptography**: Implement encryption and decryption algorithms.

Hacking Techniques

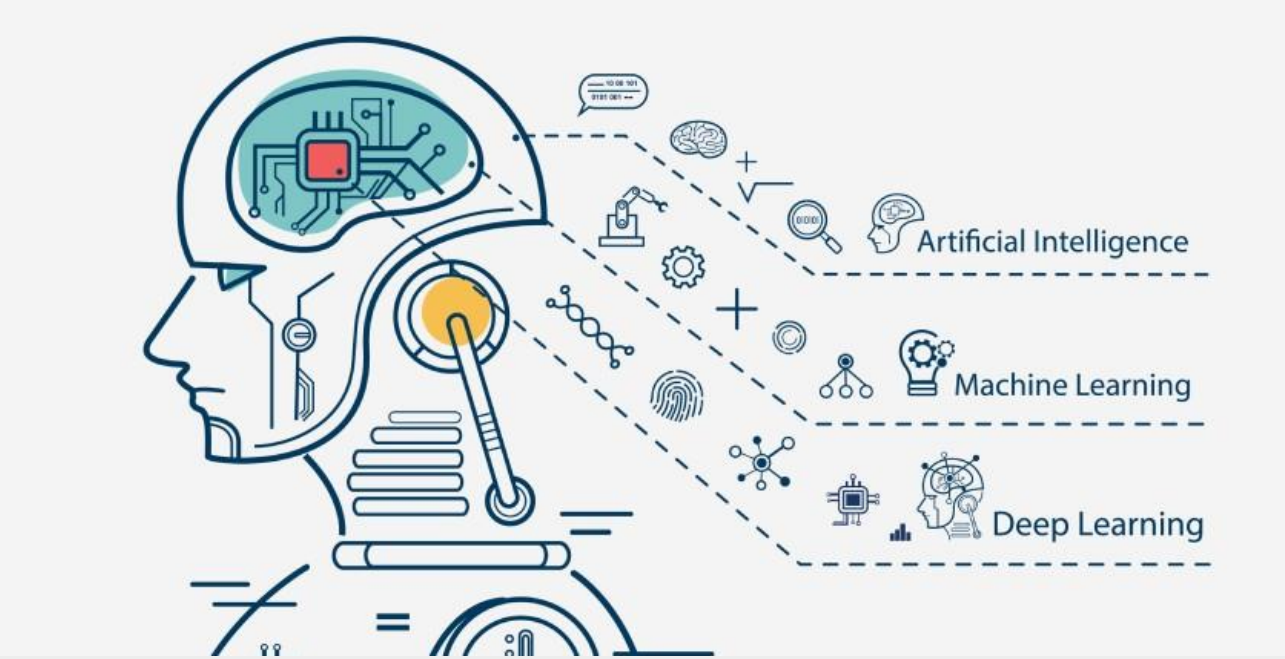
Exploit development: Identify and exploit vulnerabilities in software.

Reverse engineering: Analyze and understand how software works by examining its code.

Penetration testing: Assess the security of systems and networks for vulnerabilities.

Web application security: Test and secure web applications against attacks.

Python and Machine Learning for security



- Utilize machine learning algorithms for anomaly detection and threat analysis.
- Train models to recognize patterns in security data for threat detection.
- Enhance security systems with AI-driven capabilities.

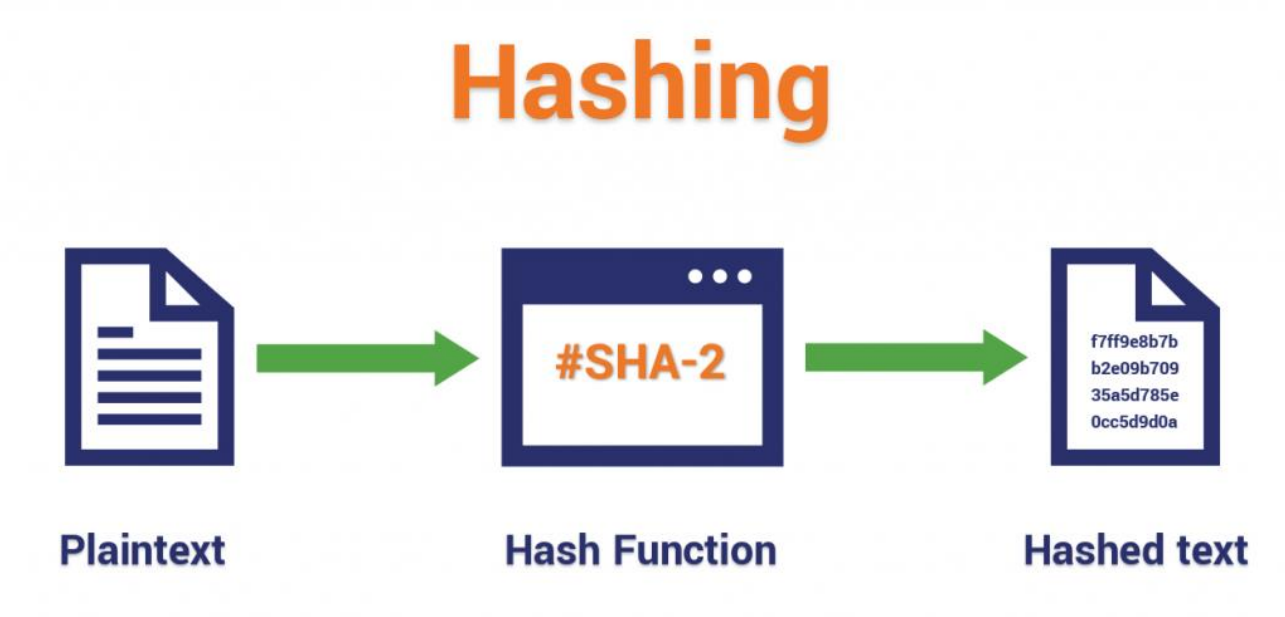
Cryptographic Failures (Day-4)

Name: T. Mohan Sri Sai

Rollno: 208H1A0540

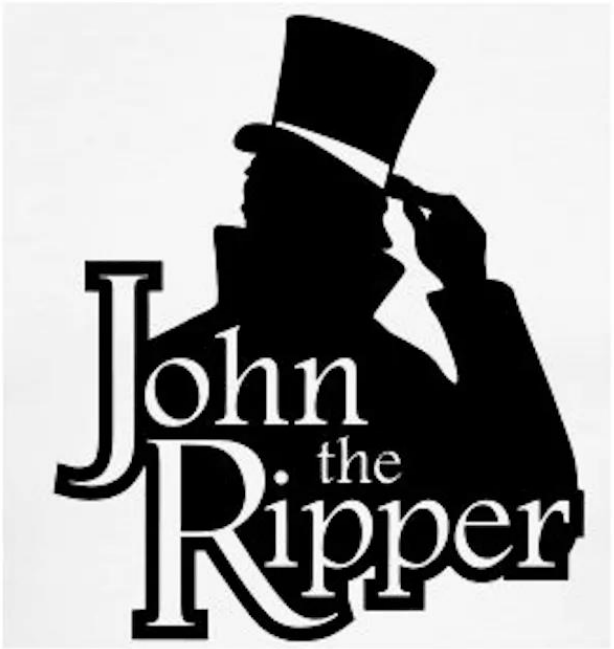
College: MVR College of Engineering & Technology

Cryptography for Hashing



- Hashing algorithms used for data integrity and password storage.
- Examples include MD5, SHA-1, and SHA-256.
- Cryptographic failures occur when weak hashing algorithms are used or when hashes are improperly stored.

Text-Based Hashing



- Tools like Hashcat and John the Ripper used for cracking hashed passwords.
- Weaknesses in hashing algorithms can lead to successful brute force attacks.

Packet Analyzer

- Tools like Wireshark used to capture and analyze network packets.
- Cryptographic failures may occur when sensitive information is transmitted over insecure protocols without encryption

Cryptoforce and Port scanners

1

CryptoForce and port scanners like Nmap used to identify vulnerabilities in cryptographic implementations.

2

Weaknesses such as outdated SSL/TLS versions or misconfigured encryption algorithms can be exploited.

Brute Force, Reverse Shell, and Fuzzers

Brute force attacks attempt to guess passwords or encryption keys through trial and error.

Reverse shell attacks exploit vulnerabilities in cryptographic protocols to gain unauthorized access to systems.

Fuzzers like American Fuzzy Lop (AFL) used to find weaknesses in cryptographic implementations through automated testing.

OWASP Category and API Hacking (Day-5)

Name: T. Mohan Sri Sai

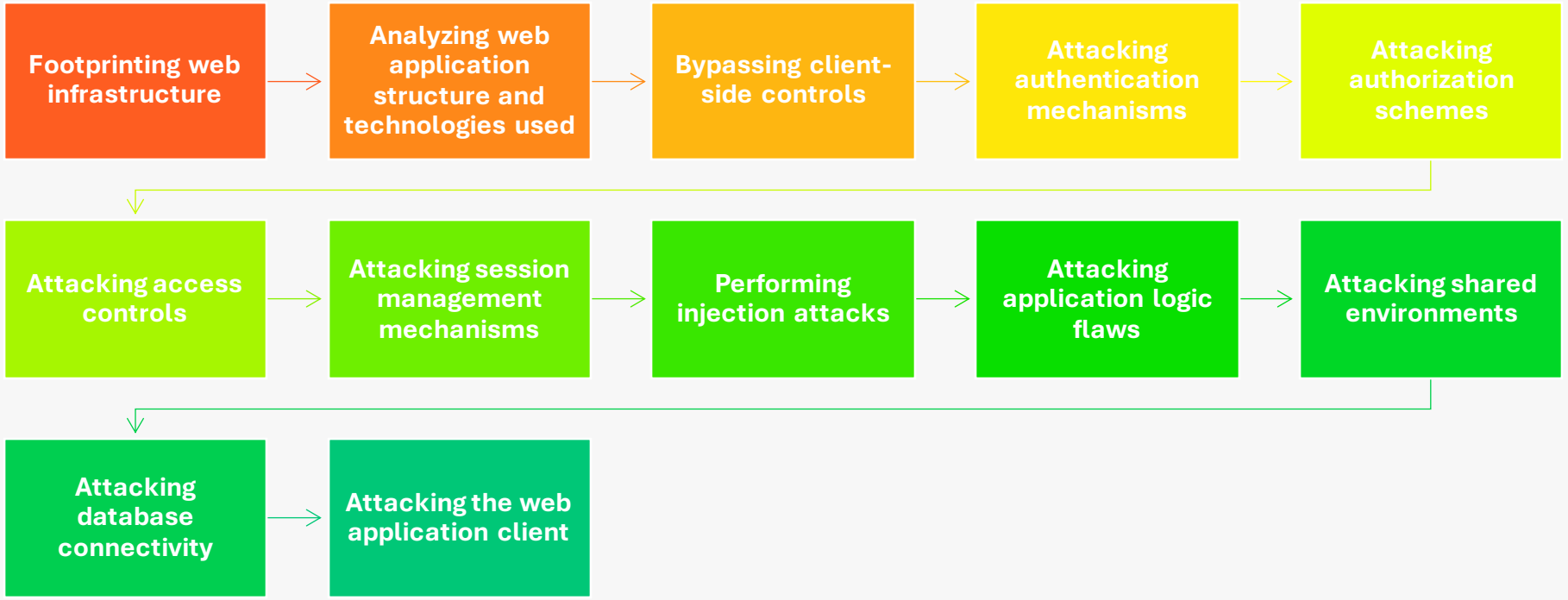
Rollno: 208H1A0540

College: MVR College of Engineering & Technology

Web Application Concepts

- Definition of web applications
- Client-server architecture
- Common technologies used (HTML, CSS, JavaScript, etc.)
- Interaction between client and server

Web Application Hacking Methodology

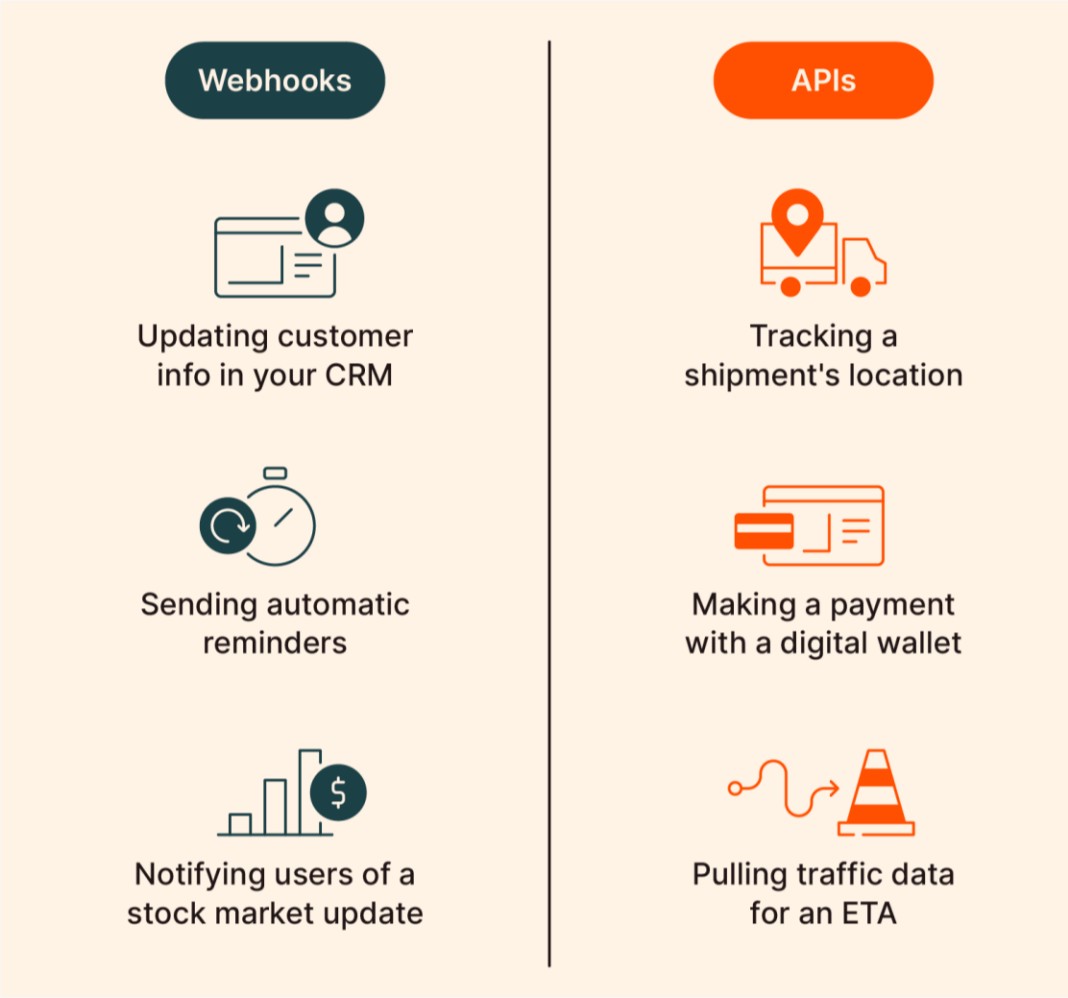


Web Application Threats

- Injection attacks
- Broken authentication
- Sensitive data exposure
- XML external entities (XXE)
- Broken access control
- Security misconfigurations
- Cross-site scripting (XSS)
- Insecure deserialization
- Using components with known vulnerabilities
- Insufficient logging and monitoring

Web API, Web Hooks, and Web Shell

- Introduction to web APIs and webhooks
- Understanding web shells and their usage in attacks
- Risks associated with insecure web APIs and webhooks



OWASP Top 10 Application Security Risks

1. Injection
2. Broken authentication
3. Sensitive data exposure
4. XML external entities (XXE)
5. Broken access control
6. Security misconfigurations
7. Cross-site scripting (XSS)
8. Insecure deserialization
9. Using components with known vulnerabilities
10. Insufficient logging and monitoring