Name	Bharath Prabhakar
Skills Build Email ID:	bharath92002@gmail.com
College Name	Ramachandra College of Engineering Eluru
College State	Andhra Pradesh
Internship Domain	Cyber Security

Introduction to Cyber Security

Cyber Security: Cybersecurity is the practice of protecting internet-connected systems such as hardware, software and data from cyberthreats. It's used by individuals and enterprises to protect against unauthorized access to data centers and other computerized systems.

Types of Cyber Attacks:

1.) Active Attacks
2.) Passive Attacks

1.) Active Attacks: An active attack is a security attack in which the attacker directly communicates with the target system or network.

Types of Active Attacks:

1. Man-In-The-Middle Attack(MITM)
2. Spoofing
3. DoS Attack
4. Phishing Attack
5. Replay Attack

1.) **MITM:** In this attack perpetrator positions himself in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway.

2.) **Spoofing:** Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source.

3.) **DoS Attack:** A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.

4.) **Phishing Attack:** It is a type of attack that attacker manipulate the victim to gain the personal information such as usernames, passwords, credit card numbers, bank account information or other important data in order to utilize or sell the stolen information.

5.) **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.

2.) Passive Attacks: A passive attack is a network attack in which a system is monitored and sometimes scanned for open ports and vulnerabilities. The purpose of a passive attack is to gain information about the system being targeted; it does not involve any direct action on the target.

Types of Passive Attacks:

1.) Computer Surveillance: It is the monitoring of computer activity and data stored locally on a computer or data being transferred over computer networks such as the Internet.

2.) Network Surveillance: Monitoring network traffic to detect and prevent security threats and maintain the confidentiality and security of sensitive information.

3.) Wire Tapping: Wiretapping is the surreptitious electronic monitoring and interception of phone-, fax- or internet-based communications. A typical eavesdropping activity involves connecting to phone lines and using a monitoring device to listen in on phone conversations.

Types of Hackers:

1.) **White Hat Hacker:** 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.

2.) **Black Hat Hacker:** They are often called *Crackers*. Black Hat Hackers can gain the unauthorized access of your system and destroy your vital data.

3.) **Grey Hat Hacker:** 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

5 Stages of Hacking:

1.) **Reconnaissance:** In this stage attacker tries to gather information about the target system.
2.) **Scanning:** In this phase hacker will tries to gather the network information about the target system.
3.) **Gaining Access:** Attacker will exploit the vulnerabilities of the system to gain the access of the target system.
4.) **Maintaining Access:** In this phase attacker maintain access that he gained by exploiting the vulnerabilities of the system.
5.) **Clearing Tracks:** Once the hacker gains access, they cover their tracks to escape the security personnel.

Introduction to Networking

Client Server Architecture:

The client-server architecture refers to a system that hosts, delivers, and manages most of the resources and services that the client requests. In this model, all requests and services are delivered over a network, and it is also referred to as the networking computing model or client server network.

Whenever there is a active communication between client and server, the hacker will interrupt the communication and will modifies the communication between them which is known as sniffing the communication.

OSI Model: OSI stands for **Open System Interconnection** is a reference model that describes how information from a client system moves through a physical medium to the server. There are seven layers in the OSI Model and each layer performs a different task.

7 Layers of the OSI Model:

1.) Application Layer
2.) Presentation Layer
3.) Session Layer
4.) Transport Layer
5.) Network Layer
6.) Data Link Layer
7.) Physical Layer

TCP/IP Model: The TCP/IP Model is a concise version of the OSI model. It contains four layers, unlike the seven layers in the OSI model. The main work of TCP/IP is to transfer the data of a computer from one device to another. The main condition of this process is to make data reliable and accurate so that the receiver will receive the same information which is sent by the sender. To ensure that, each message reaches its final destination accurately, the TCP/IP model divides its data into packets and combines them at the other end, which helps in maintaining the accuracy of the data while transferring from one end to another end.

4 Layers of the TCP/IP Model:

1.) Application Layer
2.) Transport Layer
3.) Internet Layer
4.) Network Layer

Ports

COMMON PORTS :

1. **PORT 20 AND 21:** These Ports are used for FTP (file transfer protocol) connection. FTP uses two TCP connections for communication. Port 21 is used for pass control information. And the other port 20 is used to send the data files between the client and the server. FTP ports 20 and 21 must both be open for successful file transfer on the network.
2. **PORT 22:** The port is used for Secure Shell (SSH) communication and allows remote administration access to the VM. In general, traffic is encrypted using password authentication.
3. **PORT 23:** Port 23 is typically used by the Telnet protocol. Telnet commonly provides remote access to a variety of communications systems. Telnet is also often used for remote maintenance of many networking communications devices including routers and switches
4. **PORT 25:** Port 25 is the default SMTP port that is used to enable communication between the sending and receiving servers when delivering an email message to a recipient. Despite its pedigree, many ISPs (Internet Service Providers) and email providers have started to block incoming connections on port 25 as a security measure.

5. **PORT 53:** The standard port for DNS is port 53. DNS client applications use the DNS protocol to query and request information from DNS servers, and the server returns the results to the client using the same port. Port 53 is used for both TCP and UDP communication.
6. **PORT 67/68:** DHCP servers also use port 67 to initiate communication between the client and server on the network. If port 67 is used by another application, DHCP will fail to function. Clients use port 68.
7. **PORT 80:** Port 80 is the port number assigned to commonly used internet communication protocol, Hypertext Transfer Protocol (HTTP). It is the default network port used to send and receive unencrypted web pages.
8. **PORT 123:** NTP is a built-on UDP, where port 123 is used for NTP server communication and NTP clients use port 1023 (for example, a desktop).
9. **PORT 161,162:** SNMP ports are utilized via UDP 161 for SNMP Managers communicating with SNMP Agents (i.e. polling) and UDP 162 when agents send unsolicited Traps to the SNMP Manager.
10. **PORT 389:** Port 389 is used for TLS connections; TLS establishes a non encrypted connection on port 389 that it 'upgrades' to an encrypted TLS connection as the initial connection proceeds. This allows unencrypted and encrypted connections to be setup and handled by this one port.

1. **IPsec (Internet Protocol Security):** IPsec is like a secret code for internet communication. It makes sure that when computers talk to each other online, their messages are scrambled into unreadable codes, so no one else can understand them. It's commonly used by companies to keep their data safe when employees work from home or when different offices need to connect securely.
2. **SSL/TLS (Secure Sockets Layer/Transport Layer Security):** SSL/TLS is like a secure tunnel for internet browsing. When you visit a website, it sets up a secret language between your browser and the website, so any information you send (like passwords or credit card numbers) is protected from sneaky hackers who might try to listen in.
3. **DTLS (Datagram Transport Layer Security):** DTLS is similar to SSL/TLS, but it's designed for things like video calls or online games that need to be fast and smooth. It makes sure that even in the middle of a fast-paced game or a video chat, your messages stay safe and don't get messed up along the way.
4. **Kerberos:** Kerberos is like a special ticket for getting into a club. When you want to use a computer system or an app, Kerberos checks to make sure you're allowed in. It's like showing your ID at the door, but way more secure. It's often used by big organizations to control who can access their computers and data.

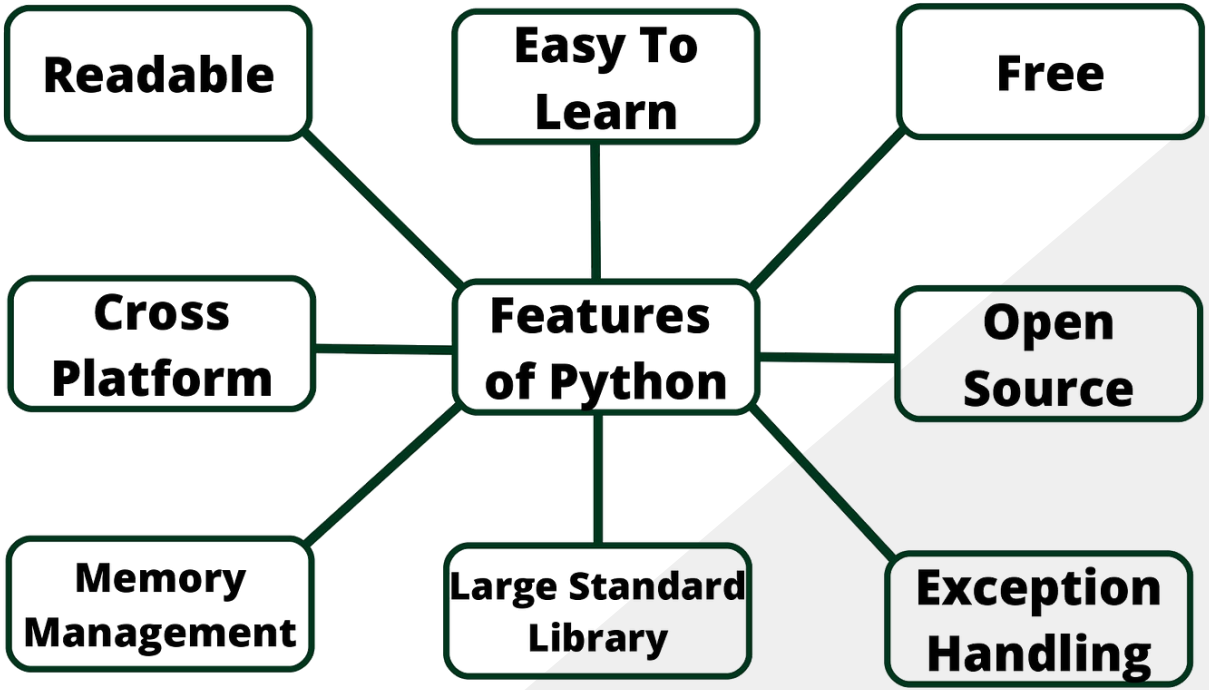
5. **SNMPv3 (Simple Network Management Protocol version 3):** SNMPv3 is like a manager keeping an eye on all the computers and devices in a big office. It checks if everything is working okay and lets you know if something isn't right. But it also makes sure that only authorized people can see this information, so it's like having a security guard for your computer network.
6. **HTTPS (Hypertext Transfer Protocol Secure):** HTTPS is like sending a letter in a locked box instead of on a postcard. When you visit a website with HTTPS, it wraps up all the information you send (like your name or what you're buying) in a locked box, so no one else can read it while it's traveling through the internet. It's an extra layer of protection for your online activities, especially when you're sharing sensitive information.

INTRODUCTION TO PYTHON

INTRODUCTION TO PYTHON

- Python is a popular programming language. It was created by Guido van Rossum, and released in 1991.
- It was designed with an emphasis on code readability, and its syntax allows programmers to express their concepts in fewer lines of code.
- Python is a programming language that lets you work quickly and integrate systems more efficiently.
- There are two major Python versions: Python 2 and Python 3. Both are quite different.

Features of Python:



Role of Python in Cyber Security:

- Python can be used to automate a wide range of tasks in cybersecurity, such as scanning for malware, analyzing network traffic, and performing vulnerability assessments.
- It can also be used to develop custom security tools for specific tasks.
- It is a popular choice for cybersecurity professionals because it is easy to learn and use, and it has a large number of libraries and frameworks that can be used for security tasks.
- It has fantastic libraries that are useful for both developing hacking programs and other kinds of useful programs.

THANK YOU