
CYBER
SECURITY
WITH IBM
QRADAR
ASSIGNMENT 1

CONTENTS

Inroduction to cybersecurity

Networking tcp and osi model

Ports

Protocols

Introduction to python

INRODUCTION TO CYBERSECURITY

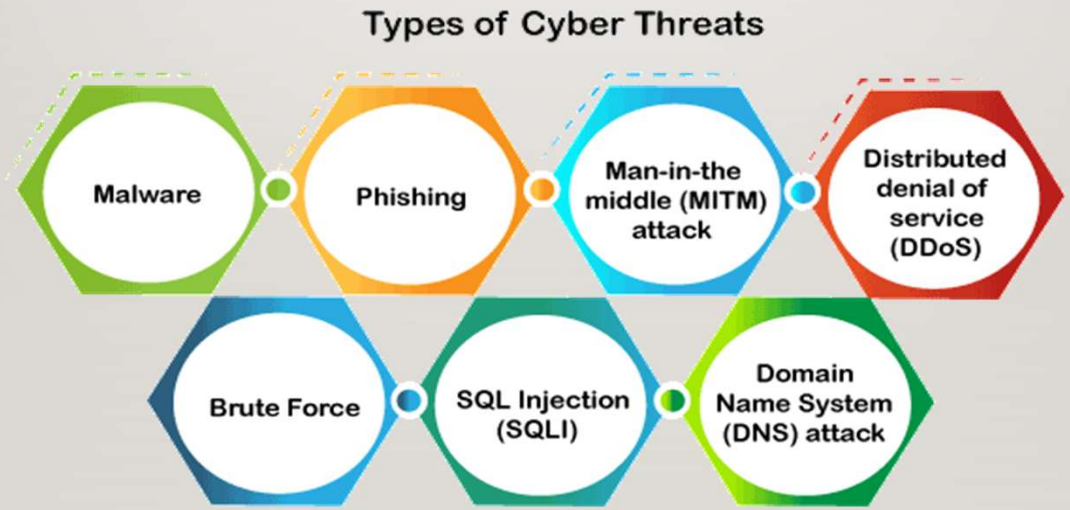
- What is Cyber Security?

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. We can divide cybersecurity into two parts one is cyber, and the other is security. Cyber refers to the technology that includes systems, networks, programs, and data. And security is concerned with the protection of systems, networks, applications, and information. In some cases, it is also called **electronic information security** or **information technology security**.

TYPES OF CYBER SECURITY

- **Information or Data Security:** It involves implementing a strong data storage mechanism to maintain the integrity and privacy of data, both in storage and in transit.
- **Identity management:** It deals with the procedure for determining the level of access that each individual has within an organization.
- **Operational Security:** It involves processing and making decisions on handling and securing data assets.
- **Mobile Security:** It involves securing the organizational and personal data stored on mobile devices such as cell phones, computers, tablets, and other similar devices against various malicious threats. These threats are unauthorized access, device loss or theft, malware, etc.

TYPES OF CYBER SECURITY THREATS



TYPES OF ATTACKS

- ACTIVE ATTACKS
- PASSIVE ATTACKS

PASSIVE ATTACKS

- An **eavesdropping attack** is taken into account as a kind of passive attack. An eavesdropping attack is to steal data transmitted among two devices that area unit connected to the net. Traffic analysis is enclosed in eavesdropping. An eavesdropping attack happens once the attackers insert a software package within the network path to capture future study network traffic. The attackers have to be compelled to get into the network path between the end point and the UC system to capture the network traffic. If their area unit additional network methods and also the network methods area unit longer, it'll be more comfortable for the offender to insert a software package within the network path.
- The **release of messages** is additionally another kind of passive attack. The attackers install a package to the device by using virus or malware to watch the device's activities like a conversation of messages, emails, or any transferred files that contain personal information and knowledge. The attackers will use the data to compromise the device or network.

ACTIVE ATTACKS

- **Denial-of-Service** attacks (DoS) are one in each of the samples of active attack. A denial-of-Service attack happens once the attackers take action to close up a tool or network. This may cause the first user to be unable to access the actual device or network. The attackers can flood the target device or network with traffic till it's not responding or flaming. The services that are affected are emails, websites, or on-line banking accounts. Dos attacks may be performed merely from any location.
- As mentioned on top of, DoS attack includes flooding or flaming the device and network. Buffer overflow attack is one in every of the common DoS attacks. This sort of flooding attack sends a lot and a lot of traffic to the network that exceeds the limit that a buffer will handle. Then, it'll lead to a flaming of the system. What is more, **ICMP flood**, called ping flood, is additionally a kind of flooding attack. The assaulter can send spoofed packets and flood them with ICMP echo requests. The network is forced to reply to all or any claims. This may cause the device not to be accessible to traditional traffic.

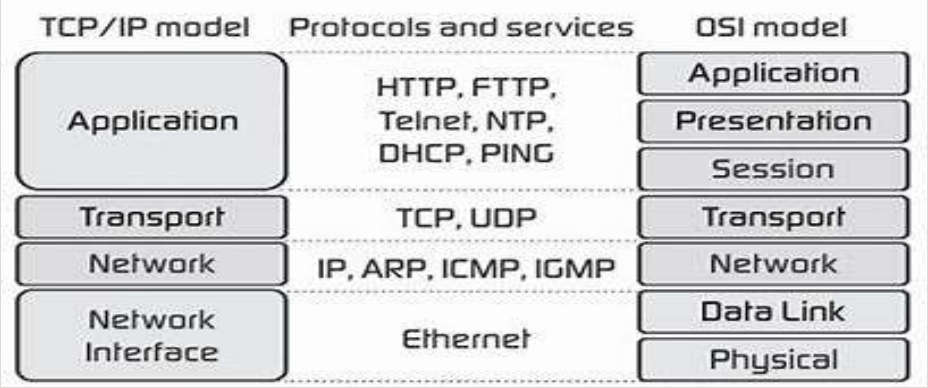
TOP 10 MOST NOTORIOUS HACKERS OF ALL TIME IN THIS INTERNET WORLD

- 1.Kevin Mitnik
- 2.Anonymous
- 3.Adrian Lamo
- 4.Albert Gonzalez
- 5.Matthew Bevan And Richard Pryac
- 6.Jeanson James Ancheta
- 7.Michael Calce
- 8.Kevin Poulsen
- 9.Jonathan James
- 10.Astra

PHASES OF HACKING

NETWORKING OF TCP/IP AND OSI MODEL

- Networking :A computer network is a system that connects numerous independent computers in order to share information (data) and resources. The integration of computers and other different devices allows users to communicate more easily



PORTS

- In computer networking, a Port is an array of communication. It is a 16-bit unsigned integer number from 1 to 65535. With the help of these numbers, multiple programs can use the same IP address. A specific network port is required to transmit or receive data from network devices. There are two primary transport protocols in the networking that uses port numbers. Moreover, the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are used.

WHAT ARE THE DIFFERENT PORT NUMBERS

- **Ports 20 and 21:** FTP, File Transfer Protocol transfers files between a client and a serve and uses port numbers 20 & 21.
- **Network Port 22:** The Protocol Secure Shell (SSH) creates secure network connections.
- **Port 25:** For Email, use Simple Mail Transfer Protocol (SMTP).
- **A Port 80:** Hypertext Transfer Protocol (HTTP) is the protocol that makes the World Wide Web possible.
- **Port 123:** Network Time Protocol (NTP) allows computer clocks to sync. This process is essential for encryption.
- **Port 179:** Border Gateway Protocol (BGP) is essential for establishing efficient routes between the extensive networks that make up the Internet.
- **Port 443:** HTTP Secure (HTTPS) is the secure and encrypted version of HTTP. All HTTPS web traffic goes to port 443.
- **Port 500:** Internet Security Association and Key Management Protocol (ISAKMP) is part of the process of setting up secure IPsec connections.
- **Port 3389:** Remote Desktop Protocol (RDP). RDP enables users to connect to their desktop computers from another device remotely.

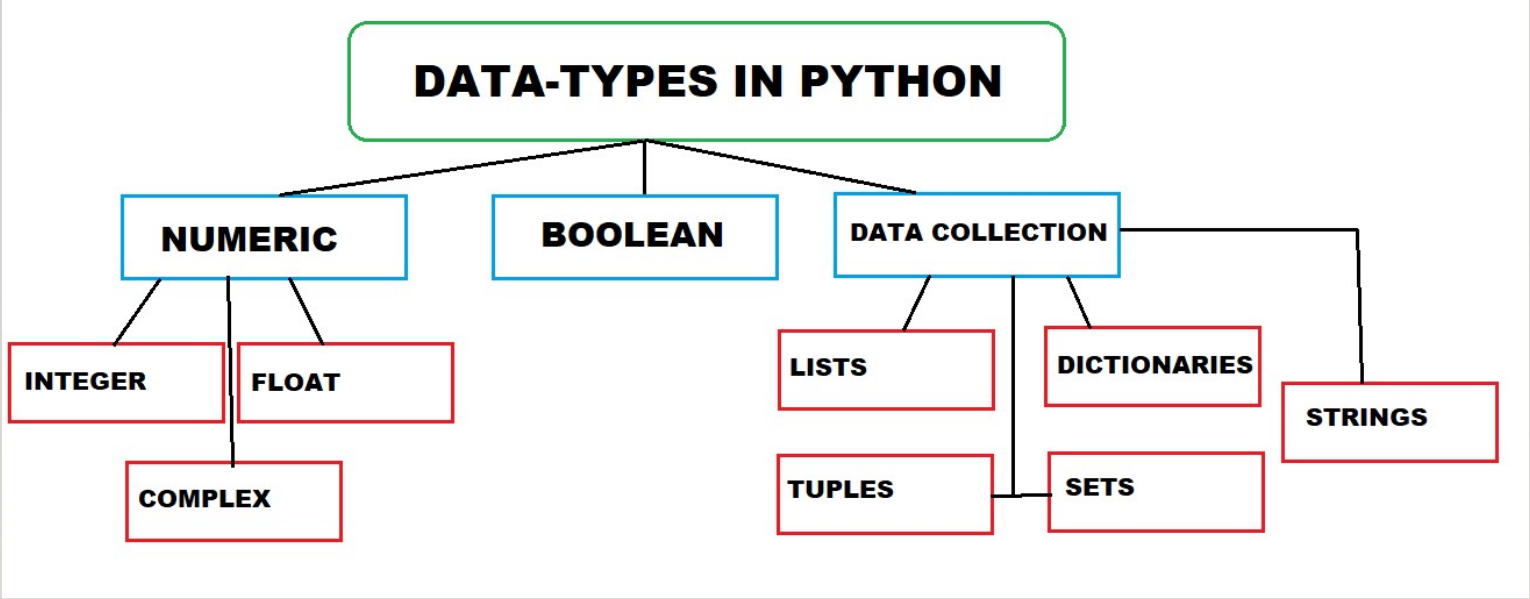
PROTOCOLS

- Standardized protocols are like a common language that computers can use, similar to how two people from different parts of the world may not understand each other's native languages, but they can communicate using a shared third language. If one computer uses the Internet Protocol (IP) and a second computer does as well, they will be able to communicate — just as the United Nations relies on its 6 official languages to communicate amongst representatives from all over the globe. But if one computer uses IP and the other does not know this protocol, they will be unable to communicate.

INTRODUCTION TO PYTHON

- Python is a general-purpose, dynamically typed, high-level, compiled and interpreted, garbage-collected, and purely object-oriented programming language that supports procedural, object-oriented, and functional programming.
- What is Python
- Python is a general-purpose, dynamically typed, high-level, compiled and interpreted, garbage-collected, and purely object-oriented programming language that supports procedural, object-oriented, and functional programming.

DATA TYPES


DATA-TYPES IN PYTHON
NUMERIC
BOOLEAN
DATA COLLECTION
INTEGER
FLOAT
COMPLEX
LISTS
TUPLES
DICTIONARIES
SETS
STRINGS

FUNCTIONS IN PYTHON

- A collection of related assertions that carry out a mathematical, analytical, or evaluative operation is known as a function.
- 1.User defined Function
- 2.Built in Function
- 3.Lambda Function
- 4.Recursion Function

CRYPTOGRAPHY

- In Python, it is possible to encrypt and decrypt files before transmitting to a communication channel. For this, you will have to use the plugin **PyCrypto**. You can installation this plugin using the command given below.
- Symmetric key
- Asymmetric key

➢ Symmetric:In Symmetric key using the same keys to both side of encryption and decryption.

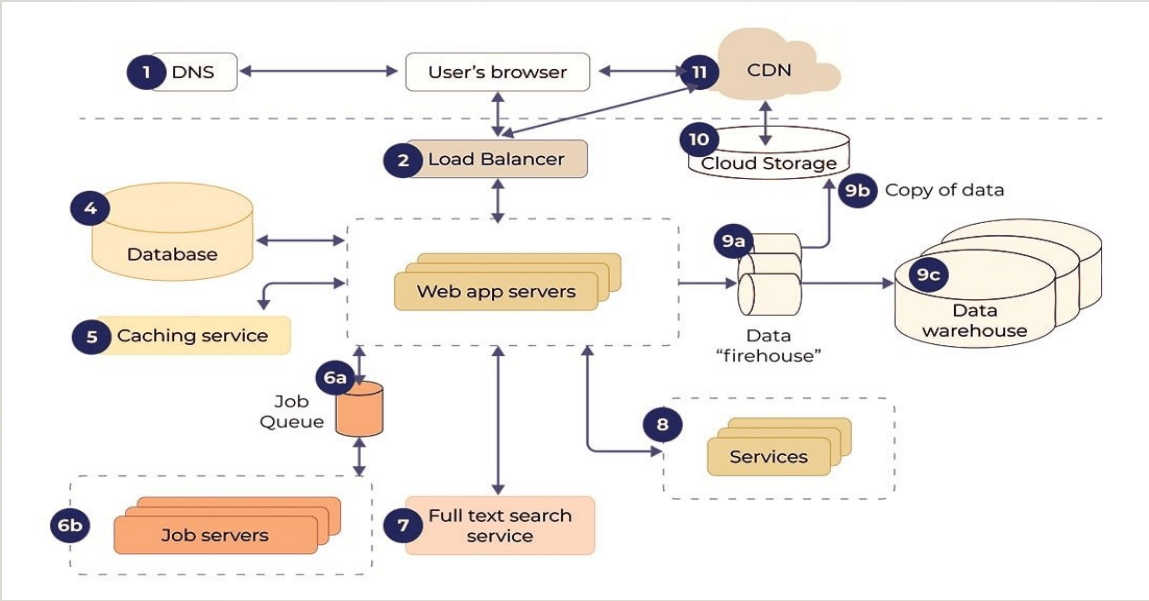
➢ Asymmetric: In Assymetric key using different keys(public&private) of encryption and decryption

INTRODUCTION TO WEB APPLICATIONS

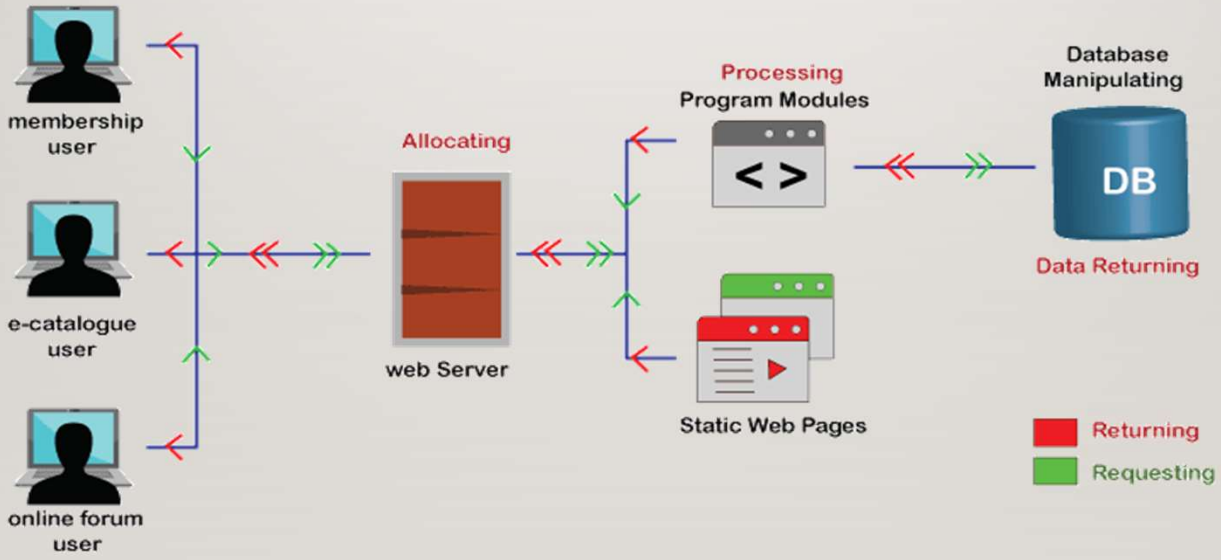
WHAT IS WEB APPLICATION

- A web-application is an application program that is usually stored on a remote server, and users can access it through the use of **Software** known as **web-browser.**
- It is a type of computer program that usually runs with the help of a web browser and also uses many web technologies to perform various tasks on the internet.
- A web application can be developed for several uses, which can be used by anyone like it can be used as an individual or as a whole organization for several reasons.

ARCHITECTURE



HOW DOES IT WORKS



WEB APPLICATION HACKING METHODOLOGY

- 1.foot printing web infrastructure
- 2.analyze web application
- 3.by pass client inside controls
- 4.Attack Authentication mechanism
- 5.Attack Authorization schemes
- 6.Attack Access Controls
- 7.Attack Session Management Mechanism
- 8.Perfor Injection Attacks
- 9.Attack Application Logic Flaws
- 10.Attack Shared Environments
- 11.Attack Database Connectivity
- 12.Attack web client