CYBER SECURITY WITH IBM QRADAR

Contents

- Introduction to cybersecurity
- Networking tcp and osi model
- Ports
- Protocols
- Introduction to python

Introduction to cyber security

Cybersecurity is the practice of protecting computer systems, networks, and data from digital threats. It encompasses various technologies, processes, and measures to safeguard against unauthorized access, data breaches, and cyber attacks. Key components include encryption, firewalls, antivirus software, and user education to create a robust defense against evolving cyber threats.

Types of cybersecurity

- **NETwork Security**: Focuses on safeguarding the integrity and confidentiality of data during transmission over networks.
- **Endpoint Security**: Involves protecting individual devices (endpoints) such as computers, smartphones, and servers from cyber threats.
- **Application Security**: Concerned with securing software and applications against vulnerabilities and unauthorized access.
- CLoud Security: Protects data and applications stored in the cloud, ensuring secure cloud computing environmentsenvironments.
- Information Security: Encompasses the protection of sensitive information through measures like encryption, access controls, and data backups.

Essential terminologies

Here are some essential terminologies in cybersecurity:

- **Firewall:** A security barrier between a private internal network and the public internet.
- **Encryption:** The process of converting information into a code to prevent unauthorized access.
- **Virus:** Malicious software that can replicate itself and infect a computer or network.
- **Authentication:** Verifying the identity of a user, system, or device.
- **Authorization:** Granting or denying access rights to users, systems, or devices.
- **Patch:** A software update to fix vulnerabilities and improve security.
- **Incident Response:** The process

Hacker categories

Hackers are broadly categorized based on their intentions and activities. Here are three main categories.

Black Hat Hackers:

- Intent: Malicious and with harmful intentions.
- Activities: Engage in unauthorized and often illegal activities, such as exploiting vulnerabilities, stealing data, and causing damage to systems.
- White Hat Hackers:
- Intent: Ethical and with positive intentions.
- Activities: Work to identify and fix security vulnerabilities.
- Grey Hat Hackers:
- Intent: Ambiguous or undefined intentions.
- Activities: Operate between black hat and white hat roles

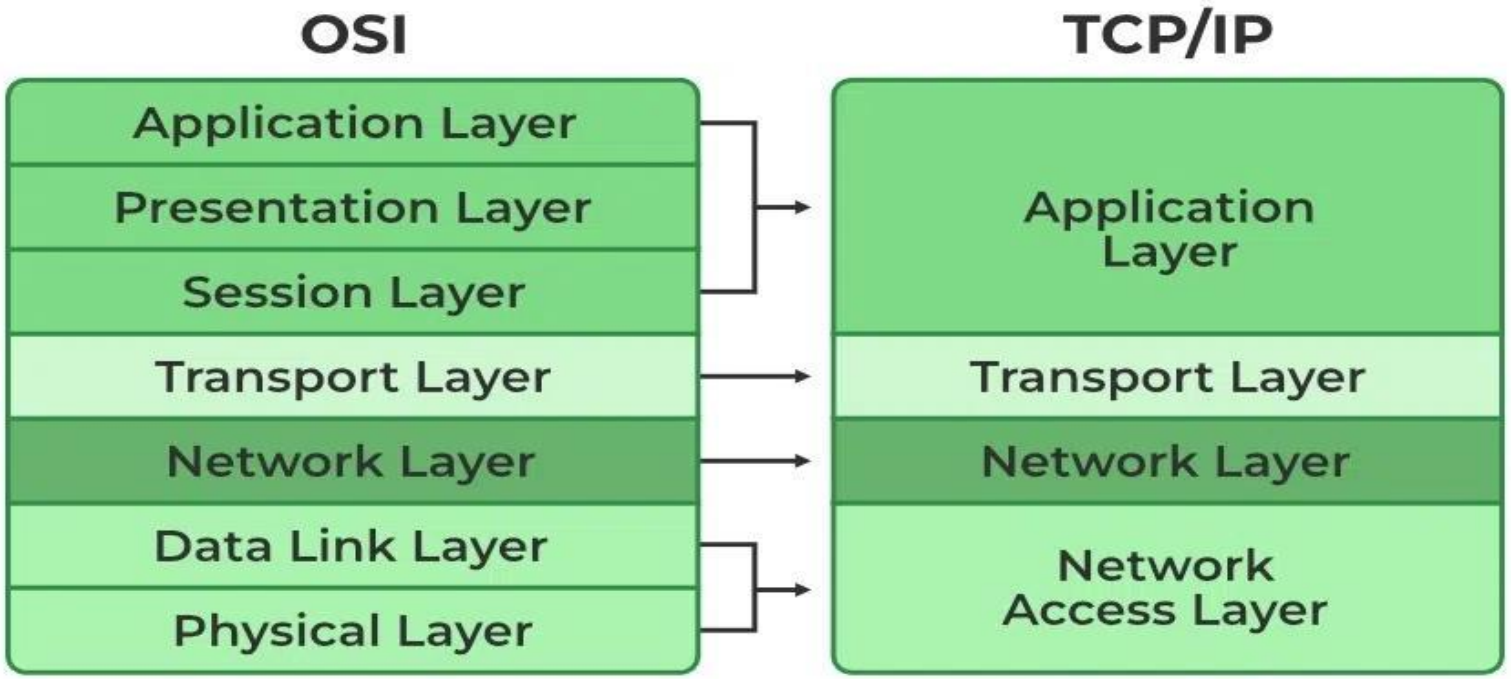
Top 10 Most Notorious Hackers Of All Time In This Internet World:

- Kevin Mitnick
- Adrian Lamo
- Gary McKinnon
- Albert Gonzalez
- Julian Assange
- Lizard Squad
- Anonymous
- Kevin Poulsen
- Robert Tappan Morris
- Jeanson James Ancheta

Phases of hacking

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Analysis
- Covering Tracks

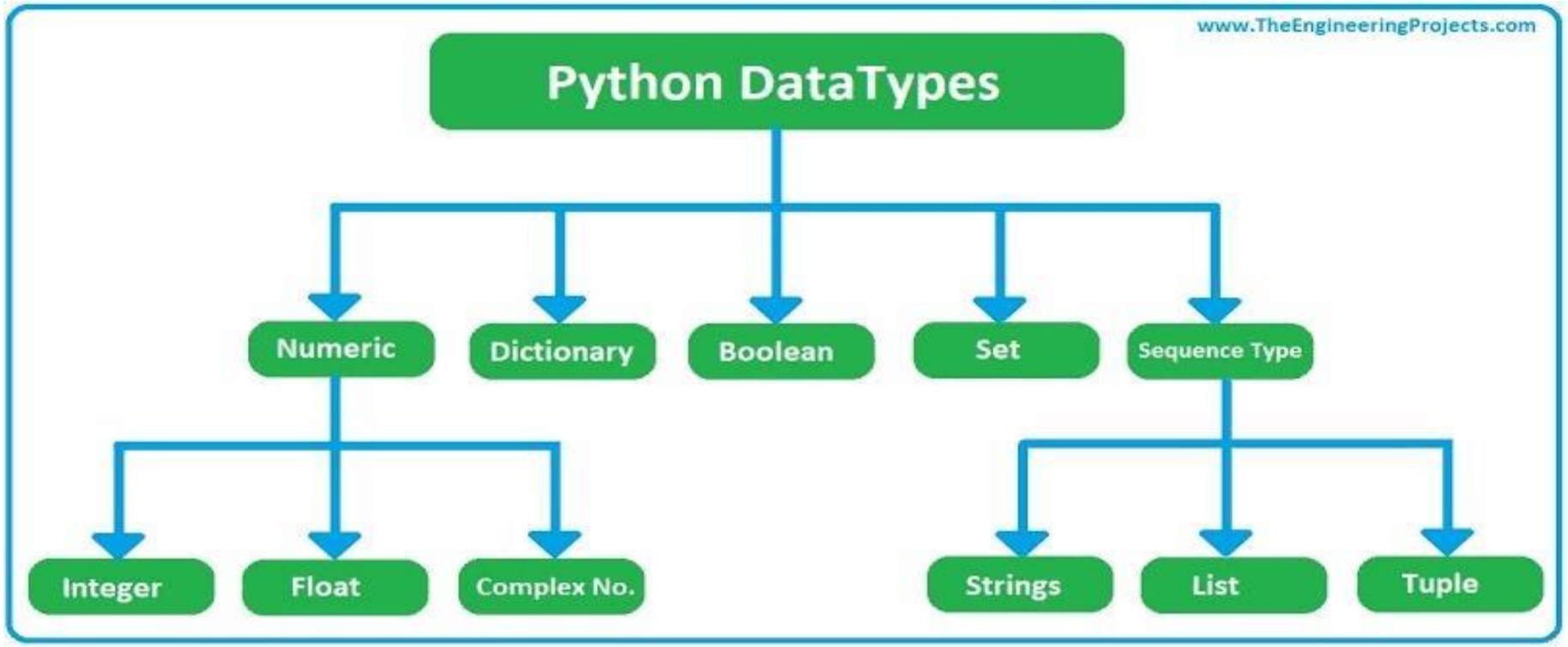
OSI AND TCP/IP MODEL



What is python

Python is a high-level, general-purpose programming language known for its readability and versatility. It supports multiple programming paradigms and is widely used in various domains, including web development, data science, artificial intelligence, automation, and more.

Data types of python



Control structures

- If statements: Used for conditional execution. If, elif (else if), and else are key components
- for loops: Used for iterating over a sequence (such as a list, tuple, or string).
- while loops: Execute a block of code as long as a specified condition is True.
- break and continue: Used within loops. break terminates the loop, and continue skips the rest of the code in the loop for the current iteration.
- try-except blocks: Used for handling exceptions (errors) in code.

Cryptography

- Cryptography involves techniques for secure communication and data protection. In Python, the cryptography library is commonly used for cryptographic operations. Here are some fundamental concepts and operations related to cryptography:
- Hashing:
- Hash functions like SHA-256 (hashlib.sha256()) are used to generate fixed-size hash values from input data. Hashes are often used to verify data integrity.
- Symmetric Encryption:
- Symmetric key algorithms (e.g., AES) use the same key for both encryption and decryption. The cryptography.fernet module provides a simple implementation

PENETRATION TESTING

Penetration testing (or pen testing) is a security exercise where a cyber-security expert attempts to find and exploit vulnerabilities in a computer system. The purpose of this simulated attack is to identify any weak spots in a system's defenses which attackers could take advantage

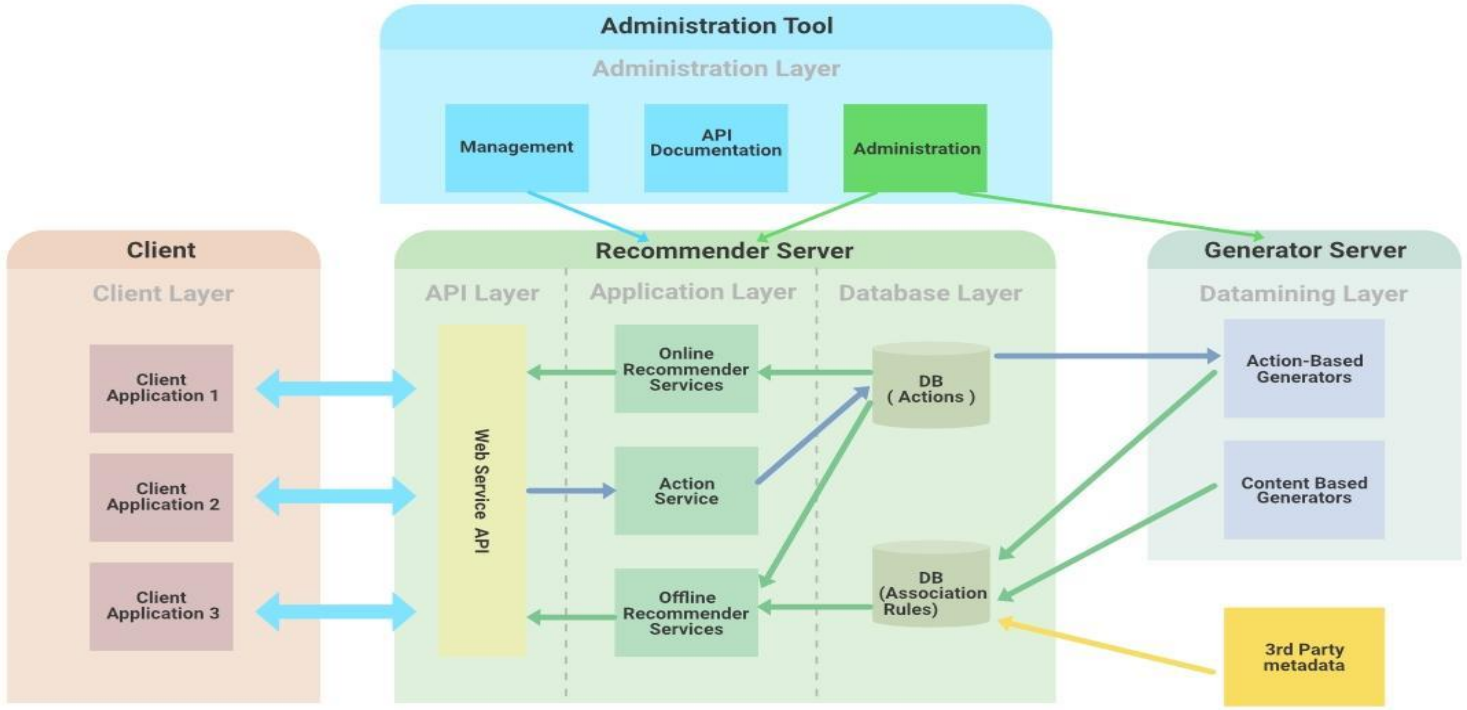
TOP 10 WEB APPLICATION SECURITY RISKS

- Broken access control
- Cryptographic failures
- Injection
- Insecure design
- Security misconfiguration
- Vulnerable and outdated componentS
- Identification and authentication failures
- Software and data integrity failures
- Security logging and monitoring failures
- Server-side request forgery

Introducation To Web Applications…

Web applications are software programs or systems that are accessed and interacted with through web browsers over a network, usually the internet. They play a crucial role in delivering various services and functionalities to users

Web Application Architecture



Web services

Web services are technologies that allow communication and data exchange between different applications over the internet. They often use standard protocols like HTTP or SOAP and are based on XML or JSON for data representation. Web services enable interoperability between diverse systems, facilitating the seamless integration of software components. Common types include RESTful APIs and SOAP-based services.

Vulnerability Stack

Web Application Hacking Methodology

- 1.foot printing web infrastructure
- 2.Attack Authorization schemes
- 3.Attack Access Controls
- 4.Perfor Injection Attacks
- 5.Attack web client