Cyber security

ASSIGNMENT-1

What is cyber security?

- Cyber security is an protecting security. Cyber refers to Technology and security refers to protection .It is all about protecting computers, networks and data from unauthorized access**.**
- **Types Of Cyber Security Attacks:**
- Active Attack & Passive Attack
- **1.Active Attack:** when someone deliberately tries to gain unauthorized access to a computer System or network. They might try to steal information ,distrupt services or even also modify data .
- 1.Man-in-the-middle attack
- 2.spoofing
- 3.Dos attack
- 4.Phishing attack
- 5.Replay attack

Passive Attack

- **Passive Attack :**we can see data what's happening but we cant change it.

1.Computer Surveillance: monitoring of computer systems and activities to ensure security prevent unauthorized access.

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

3.Wire Tapping: interception and monitoring of electronic communications for intelligence gathering or evidence

HACKERS CATEGORIES

1.Black Hat Hacker: These are the bad guys of hacking world.They use their skills to break into computer systems,networks,devices without permission.

2.White Hat Hacker: These are good guys of hacking world .They find vulnerabilities in computer systems,networks devices with permission.They help identitfy weakness.

3.Grey Hat Hacker: Both black hat hackers and white hat hackers.

Essential Terminologies :

1.malware:it can be used to steal sensitive information,damage computer systems,spread to other computers or hold data and systems hostage**.**

2.IP Address: IP address is a unique numerical label used to identify and locate devices on a network.

3.Phishing : Type of social engineering attack where attackers trick individuals into revealing sensitive information.

4.Firewall: System that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

5.Social Engineering: It refers to the use of psychological manipulation and deception tactics to trick individuals into revealing sensitive information.

6.Ransomware: It type of malicious software that encrypts a victims files and demands payment in exchange for the decryption key.

7.Virtual Private Network: It is a secured encrypted connection between a device and a remote server that allows users to securely access the internet and protect their online activity and data from being monitored and intercepted.

8.Pen Testing: To evaluate the security of the system and identify vulnerabilities that could be exploaited by malicious actors.

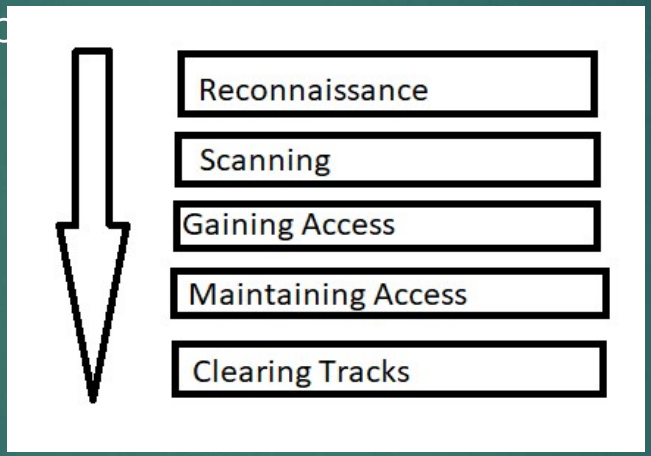
9.Antivirus: Software designed to detect ,prevent and remove malicious software.

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

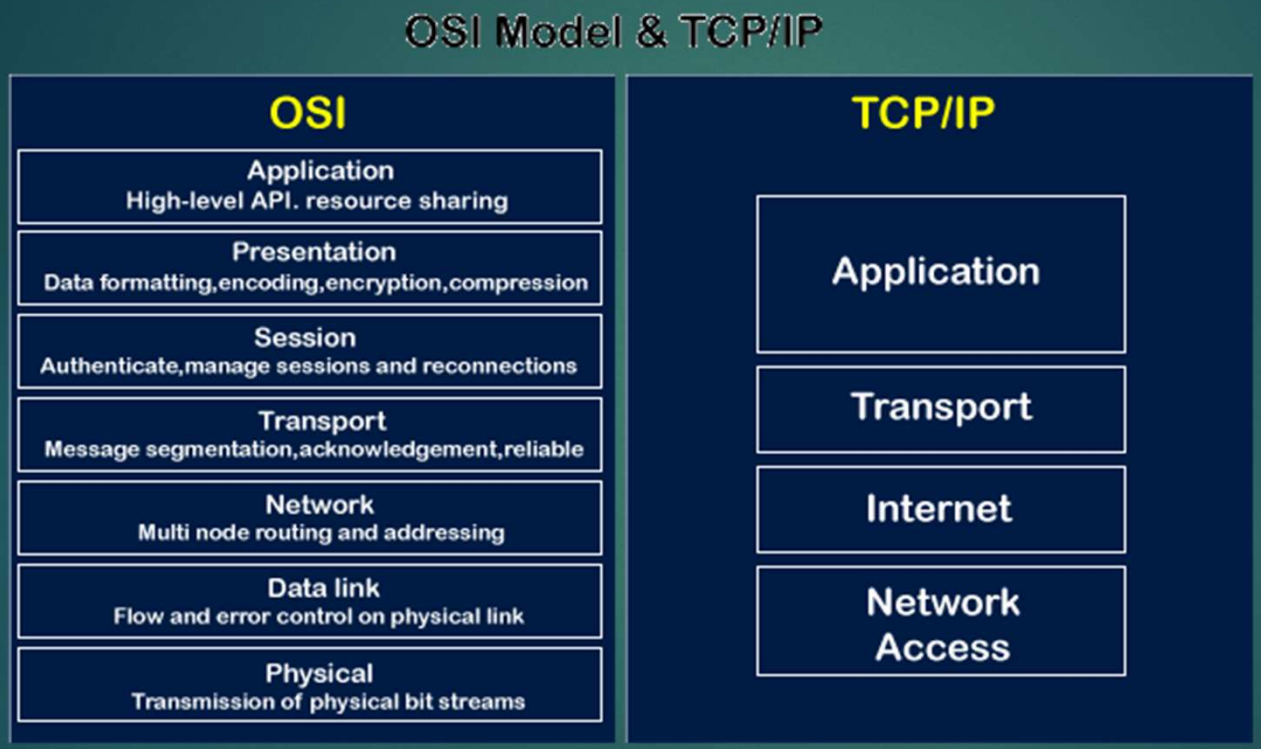
- 1.Kevin Mitnik
- 2.Anonymous
- 3.Adrian Lamo
- 4.Albert Gonzalez
- 5.Matthew Bevan And Richard Pryac
- 6.Jeanson James Ancheta
- 7.Michael Calce
- 8.Kevin Poulsen
- 9.Jonathan James
- 10.Astra

Phases of Hacking

- 1.Reconnaisance/Footp
- 2.Scanning
- 3.Gaining Access
- 4.Maintaining Access
- 5.clearing Tracks

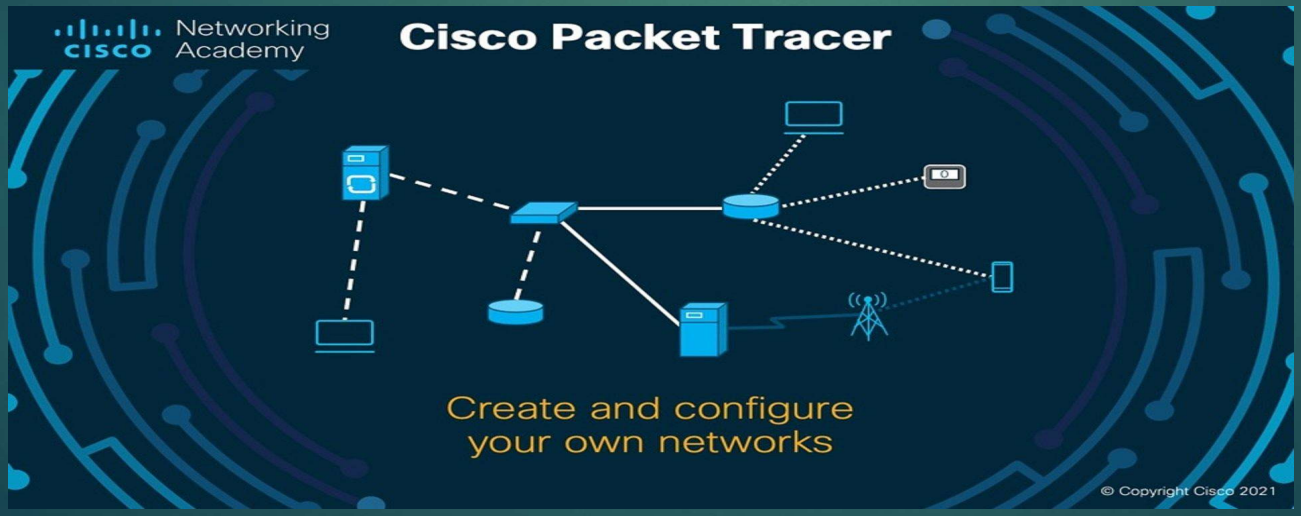


OSI AND TCP/IP MODEL



DASHBOARD OF CISCO PACKET TRACER

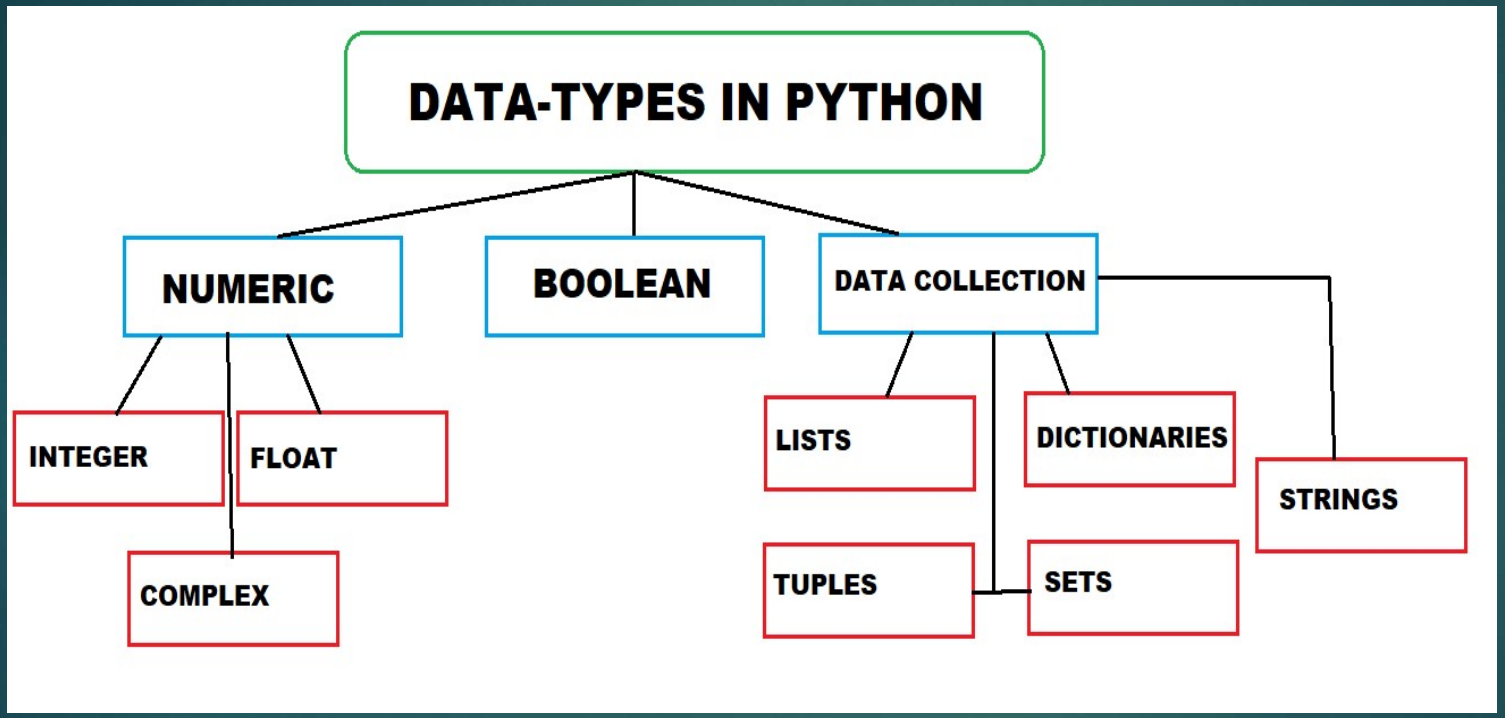
Cisco packet tracer is a network simulation and visualization tool developed by Cisco systems .it allows users to create visual networks and simulate network configuration, devices,and connections.it used for educational purpose,such as teaching networking concepts and practicing network troubleshooting.



What is python

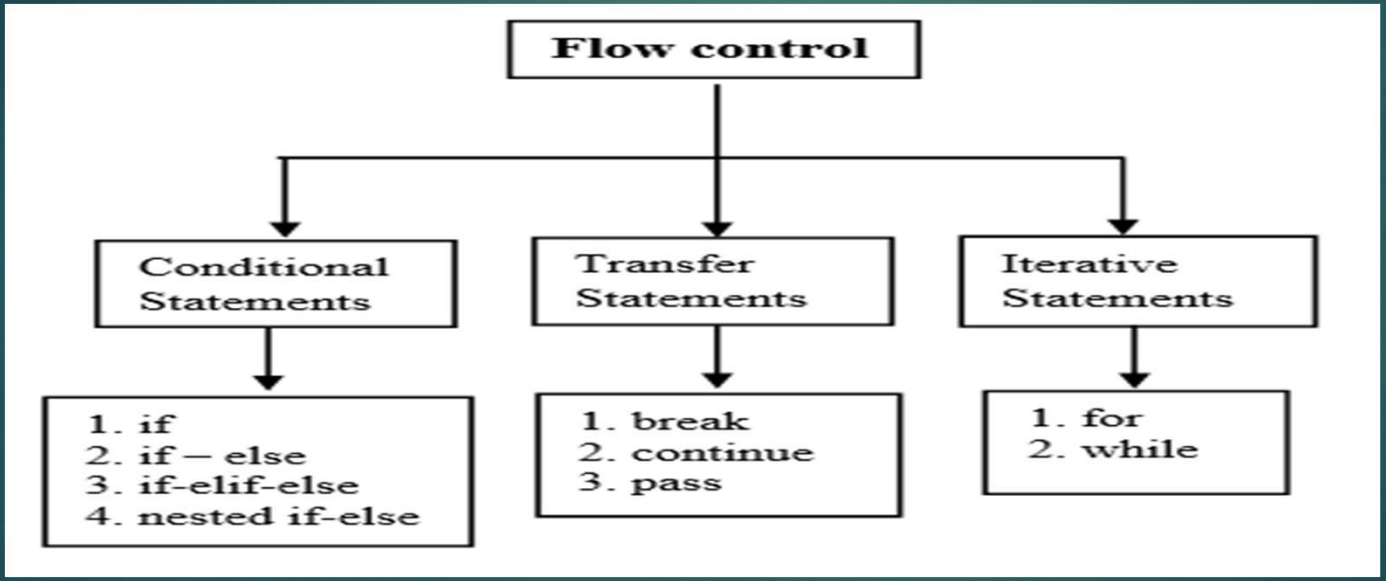
- It is a versatile programming language,is widely used in the field of cybersecurity and hacking due to its simplicity,flexibility and extensive libraries.
- WHY PYTHON ?
- It is offers readability,easy of learning,and a vast ecosystem of libraries,making it ideal for hacking tasks such as penetration testing, network scanning,and automation.

DATA TYPES


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

CONTROL STRUCTURES

It is provides control structures like if-else statements,loops,and exception handling for managing program flow.



FUNCTIONS

- Functions are reusable blocks of code that can be defined and called multiple times promoting code modularity and reusability.
- 1.User defined Function
- 2.Built in Function
- 3.Lambda Function
- 4.Recursion Function

CRYPTOGRAPHY

- Pythons cryptography library provides tools for encryption,decryption hashing,and secure communication,crucial for securing sensitive data.
- Symmetric key
- Asymmetric key
- Symmetric Key:In Symmetric key using the same keys to both side of encryption and decryption.
- Asymetric key: In Assymetric key using different keys(public&private) of encryption and decryption.

PENETRATION TESTING

- Python frameworks like Metasploit and scapy assist in penetration testing by automating tasks like networking scanning,vulnerability assessment and exploitation.
- **WEB APPLICATION SECURITY:**
- Python frameworks like Djangoband flask help secure web applications against common vulnerabilities like SQL injection ,XSS and CSRF.

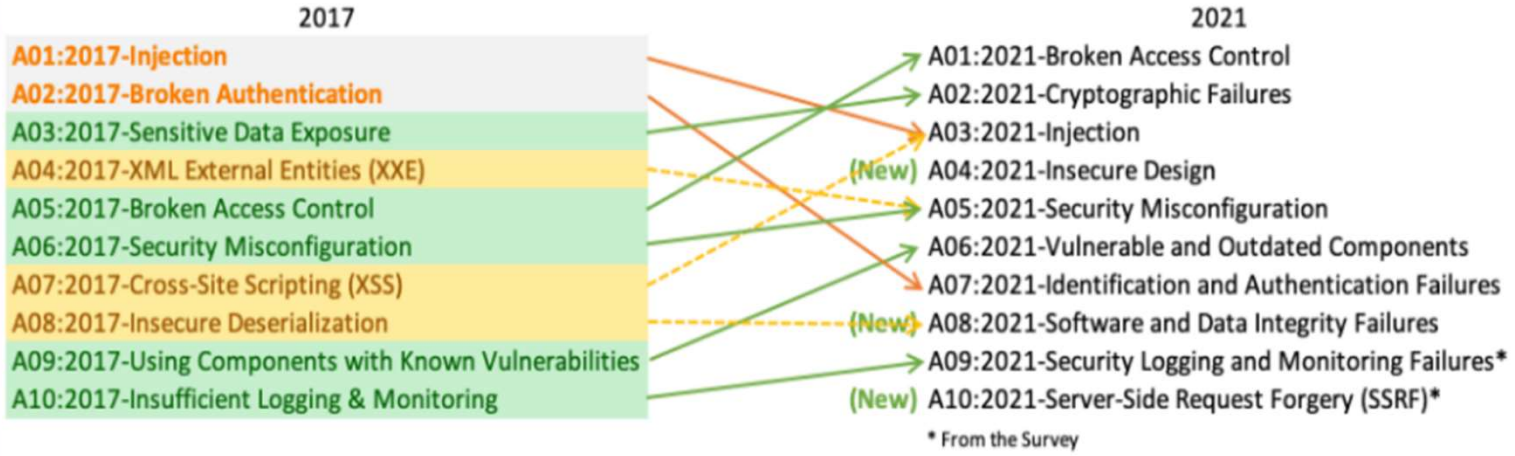
TOP 10 WEB APPLICATION SECURITY RISKS

- A01:2021:Broken Access Control
- A02:2021-Cryptographic Failures
- A03:2021-injection
- A04:2021-Insecure Design
- A05:2021-Security Misconfiguration
- A06:2021-Vulnerable and outdated components
- A07:2021-Identification and Authentication Failures
- A08:2021-Software and Data integrity Failures
- A09:2021-Security Logging and monitoring failures
- A10:Server-side Request Forgery

Top 10 Web Application Security Risks

Open Web Application Security Project (OWASP)

The OWASP Top 10 is a standard awareness document for developers and web application security.

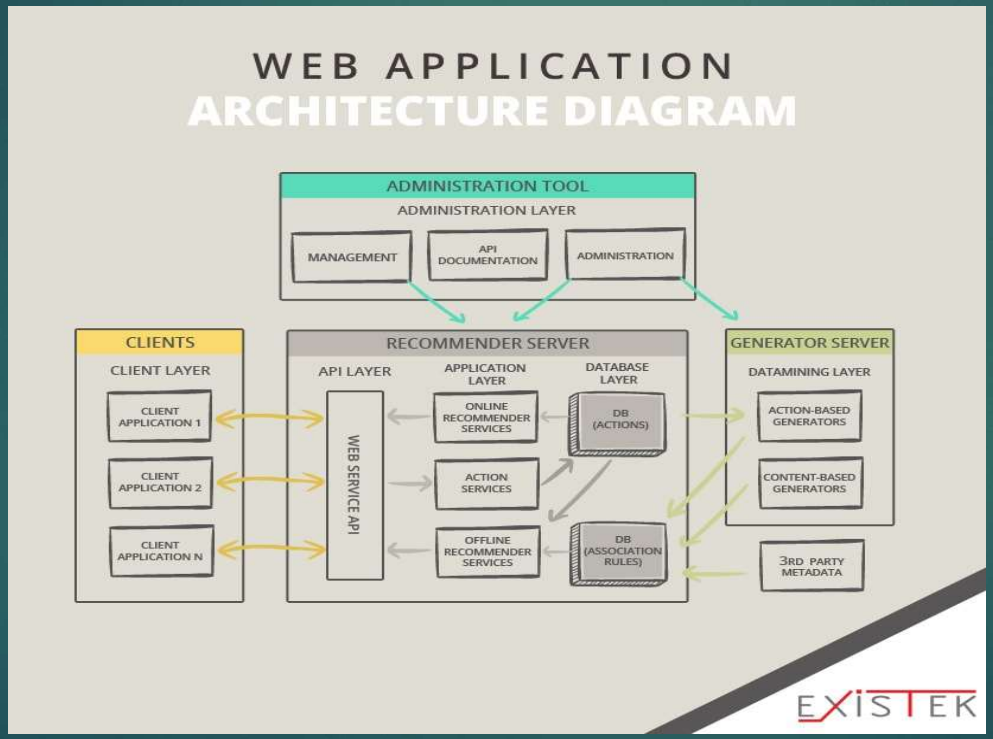


There are three new categories, four categories with naming and scoping changes, and some consolidation in the Top 10 for 2021.

Introducation To Web Applications…

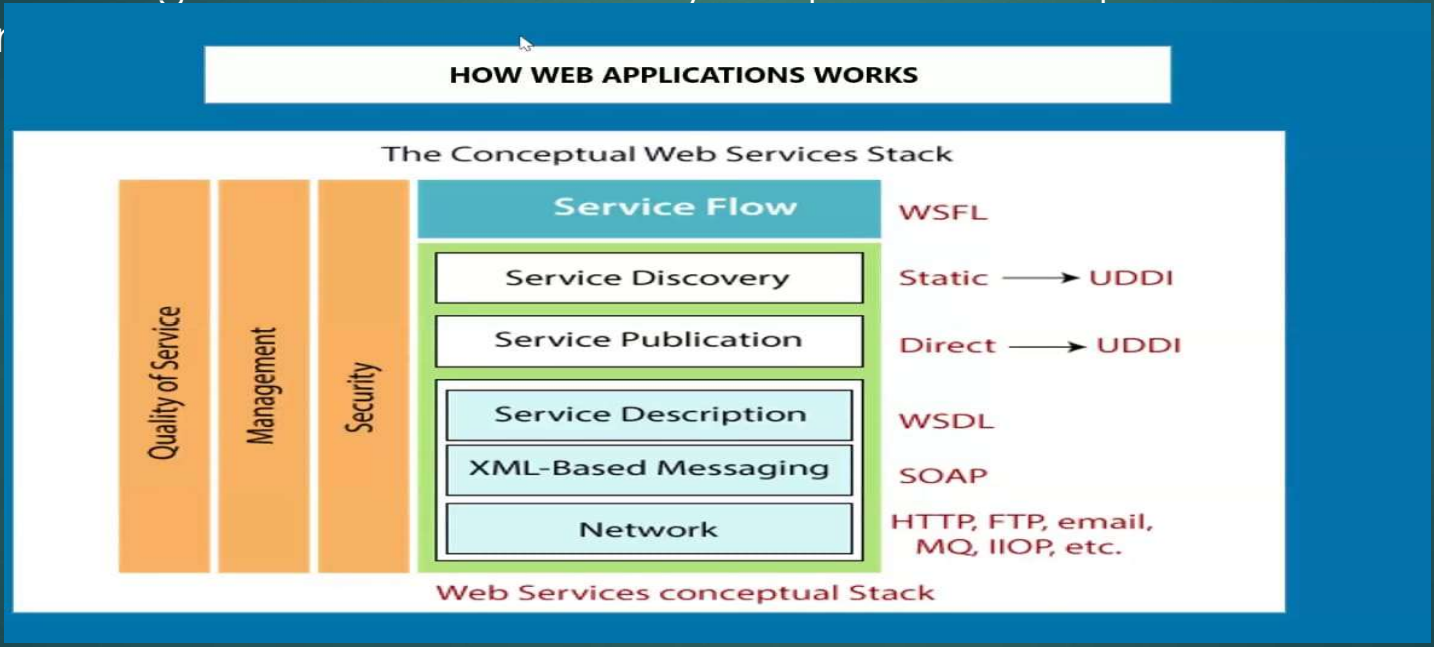
- Web Applications:
- A web Appliaction is a computer program that is accessed through a web browser over a network ,typically the internet. Web Applications are designed to work across different devices and platforms,including desktop computers ,laptops,smartphones and tablets.

Web Application Architecture

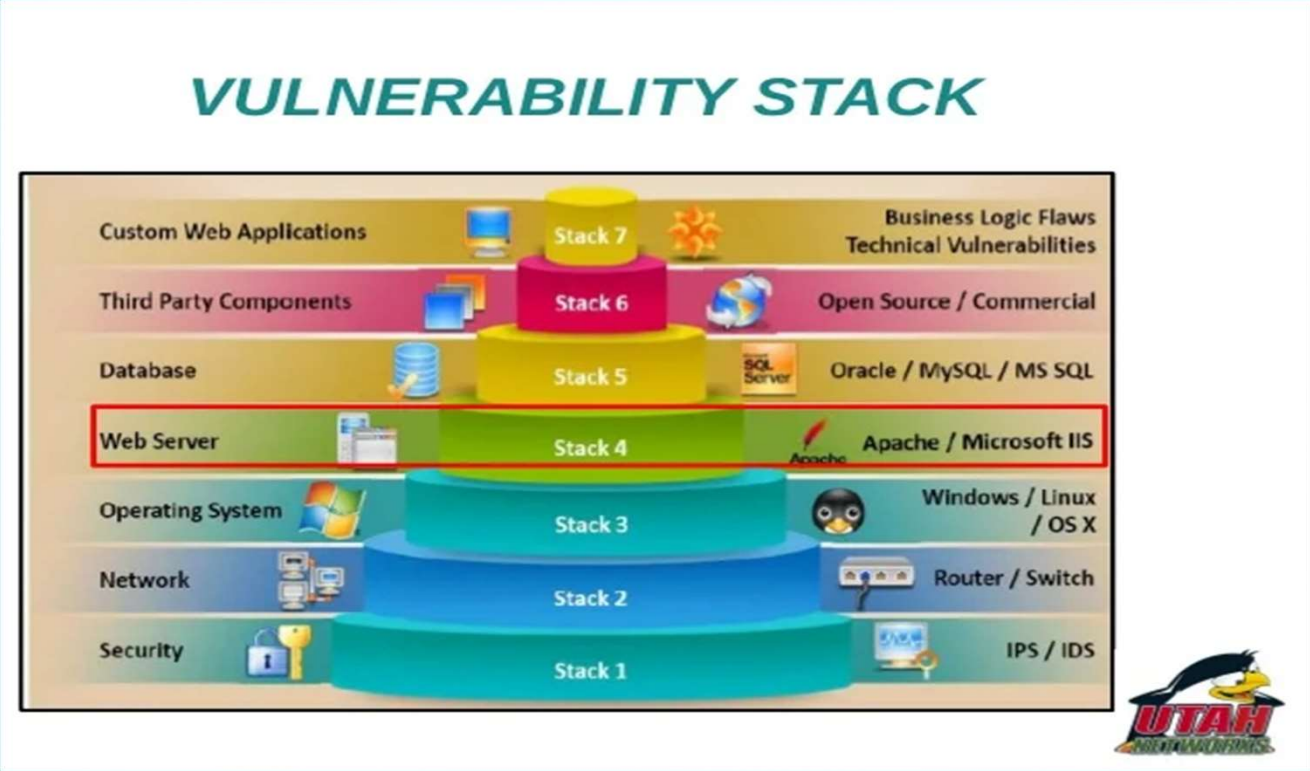


Web services

- Web services is a type of software system that enables communication between different applications /components over the internet.They use standaralized proticols and data formats such as HTTP,XML and JSON to allow different systems to exchange data and functionality in a platform-independent



Vulnerability Stack



OWASP Top 10 Applications security Risks

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entity
- A5:Broken Access Control
- A6: Security Misconfigurations
- A7:Cross-site Scripting(XSS)Attack
- A8:Insecure Deseralization

Components with known vulnerabilities

- Using components with unknown vulnerabilities is a type of security vulnerability that occurs when an application or sytem uses third-party software components,libraries,frameworks that have known security vulnerabilities.This can put the application /system at risk of being exploited by attackers who can take adavantages of these vulnerabilities.

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