Cyber security

A metaphor of protection

Security

The security is defined as the protection of the system that from the unwanted Users.

User

Security Panel

No data theft

Main motto of Hacking

- Threat actors start cyberattacks for all sorts of reasons, from petty theft to acts of war. They use various tactics, like malware attacks, social engineering scams, and password theft
- The biggest motivation is often financial gain. Hackers can make money by stealing your passwords, accessing your bank or credit card details .
- To corrupt systems, gather information on users, steal data and documents

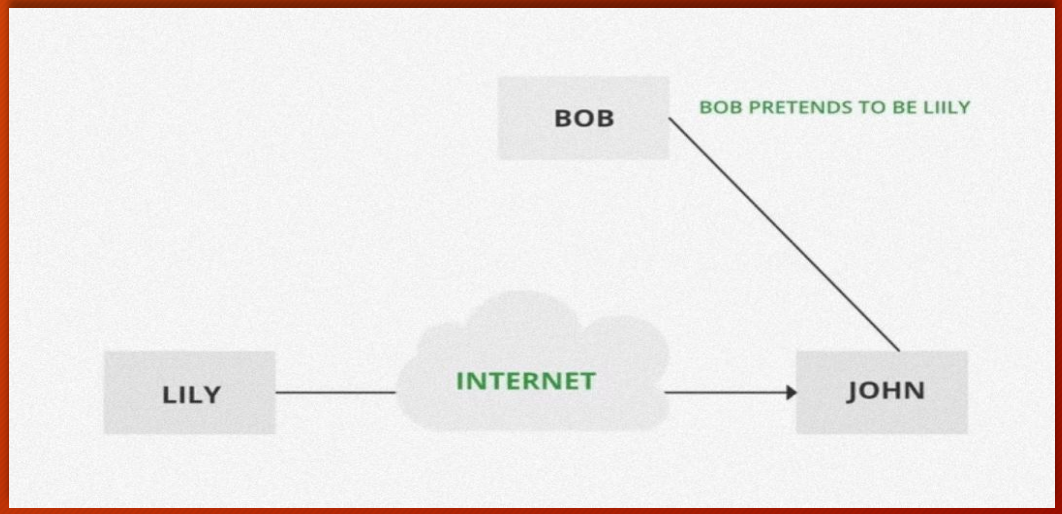
Types of Cyber Attack

Active attack

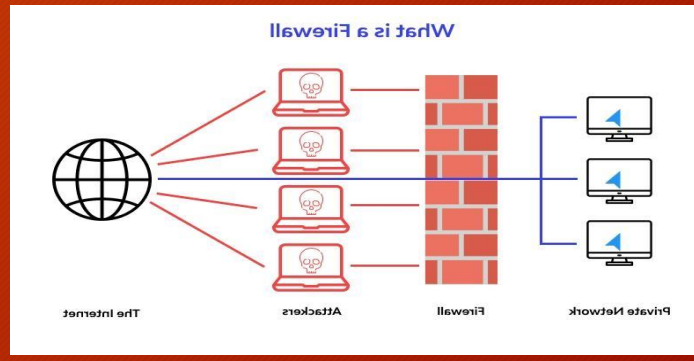
- Man in middle
- Spoofing
- Dos attack
- Phising
- Replay attack
- Ransome ware
- SQL injection

Passive attack

- **A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of eavesdropping on or monitoring transmission.**
  - Computer surveillance
  - Network surveillance
  - Wire tapping
  - Black hat hacker
  - White hat hacker

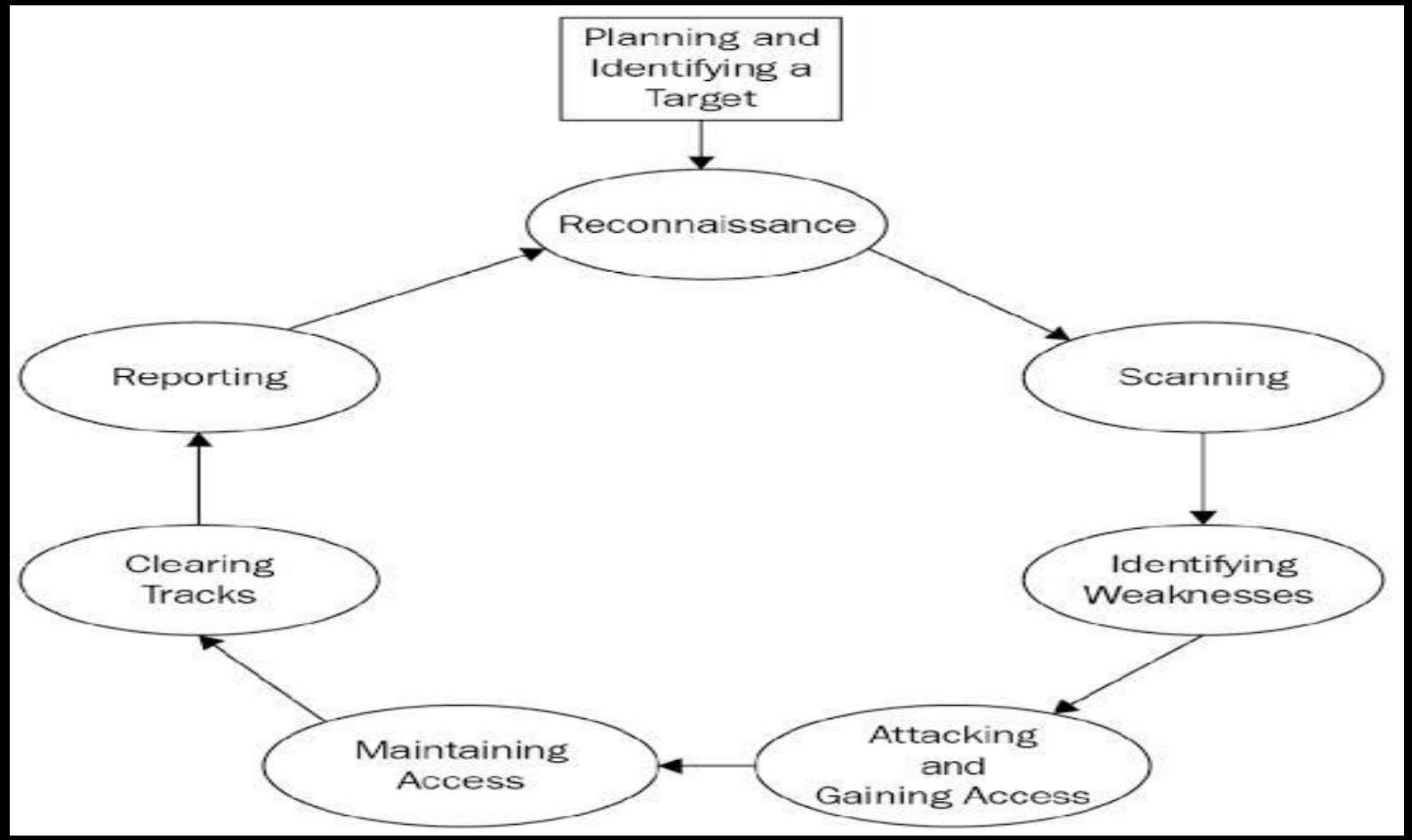


- Malware
- VPN
- Firewall
- Ip Address
- Anti virus
- Phising
- Social engineering



Terminology used in cyber security

Flow chart of phases of hacking



- Reconnaissance
- Sacnning
- Identify weakness
- Gain the acess
- Maintaining acess
- Clearing tracks
- reporting

Networking

- CSA
- OSI
- IP Address
- Types of ports
- Cisco packet tracer
- window network command

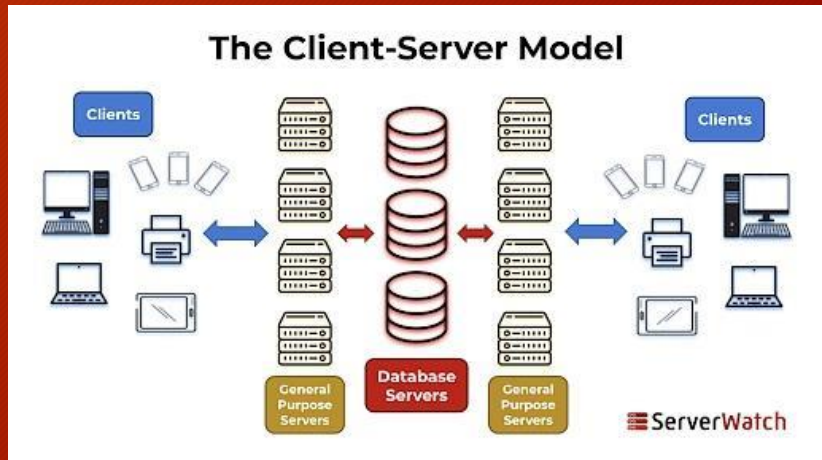
CSA(Client Server Architecture)

- Client-server architecture, alternatively called a client-server model, is a network application that breaks down tasks and workloads between clients and servers that reside on the same system or are linked by a computer network.

Advantages of Client-Server model

- Centralized system with all data in a single place.
- Cost efficient requires less maintenance cost and
- Data recovery is possible

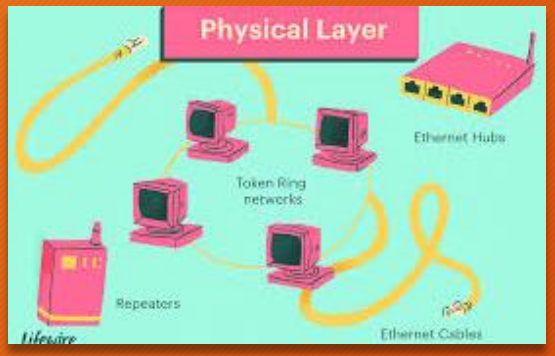
The capacity of the Client and Servers can be done



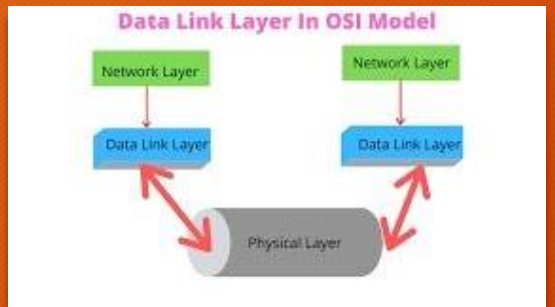
OSI(Open System Interaction model)

The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network. It was the first standard model for network communications, adopted by all major computer and telecommunication companies in the early 1980s

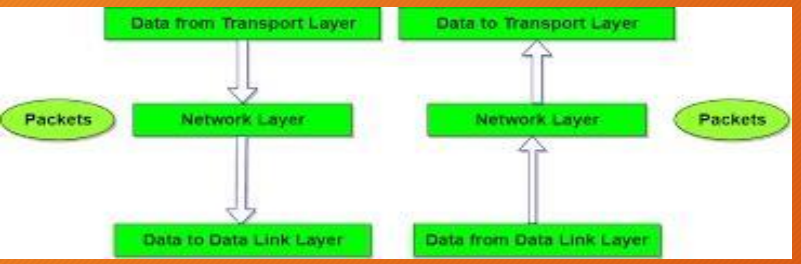
There are 7 layers in OSI model



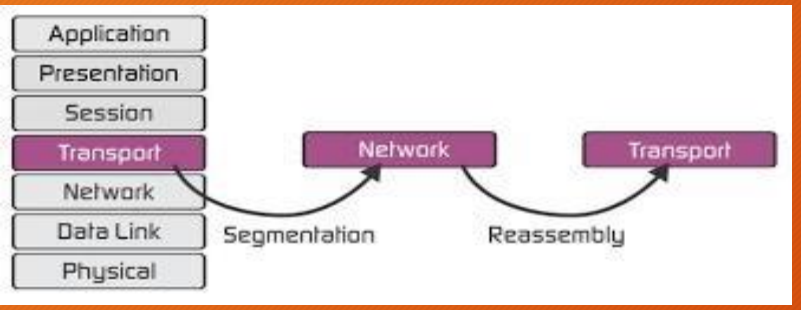
The physical layer's function is to transport data using electrical, mechanical or procedural interfaces



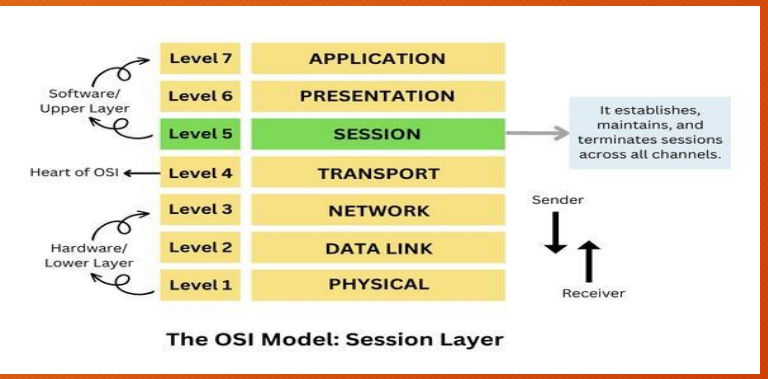
The data link layer is the protocol layer in a program that handles how data moves in and out of a physical link in a network.



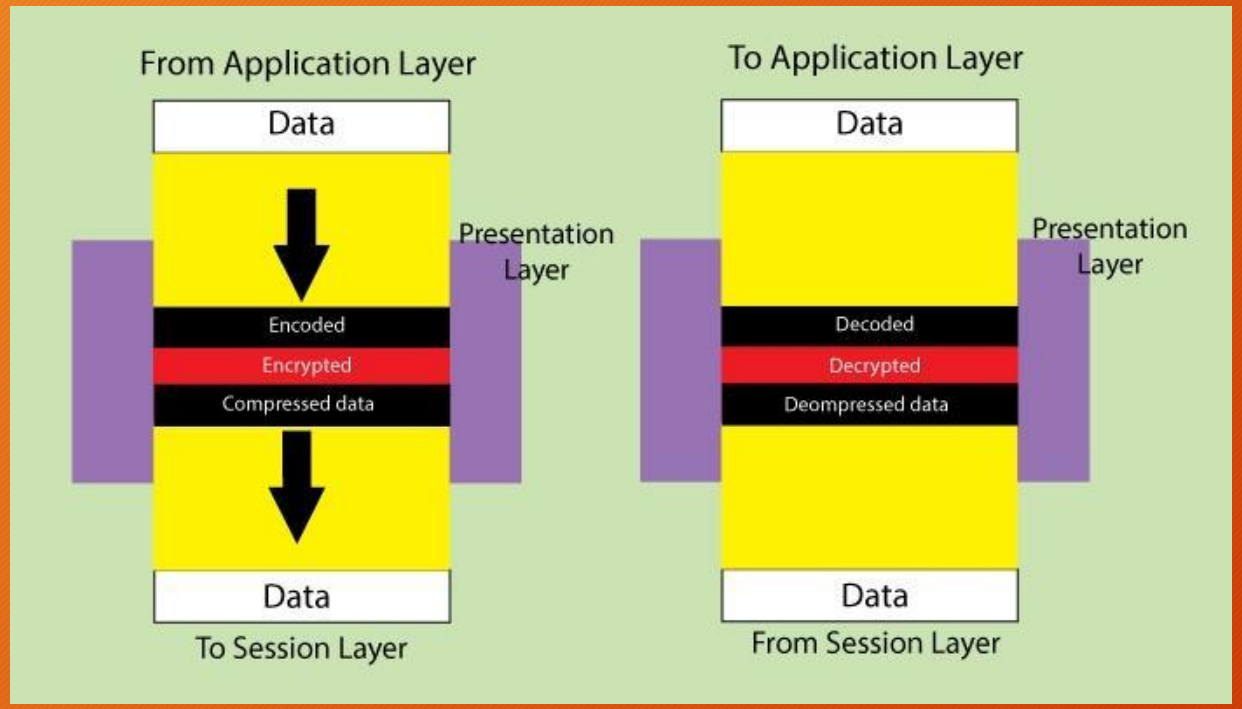
The "network layer" is **the part of the Internet communications process where these connections occur, by sending packets of data back and forth between different network**



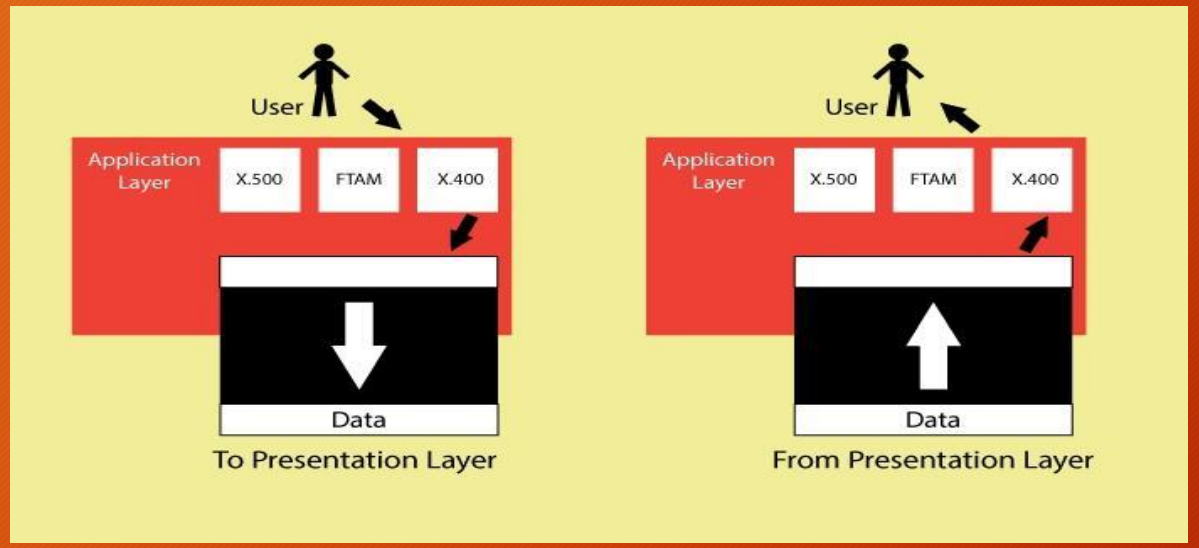
Layer 4 of the OSI model, also known as the transport layer, manages network traffic between hosts and end systems to ensure complete data transfers.



The Session Layer is the 5th layer in the Open System Interconnection (OSI) model. This layer allows users on different machines



presentation layer resides at Layer 6 of the Open Systems Interconnection (OSI) communications model and ensures that communications that pass through it are in the appropriate form for the recipient application.



The application layer sits at Layer 7, the top of the Open Systems Interconnection (OSI) communications model. It ensures an application can effectively communicate with other applications on different computer systems and networks. The application layer is not an application.

IP ADDRESS (internet protocol address)

What Is an IP address

IP address stands intenet protocol address for internet protocol address; it is an identifying number that is associated with a specific computer or computer network. When connected to the internet, the IP address allo

KEY TAKEAWAYS

An internet protocol (IP) address allows computers to sto be sent and received by the correct parties, which means it can also be used to track down a user's physical location in some instances.

IP addresses are generated through a hierarchical system involving the IANA, RIRs and ISPs.

Common IP security threats include hijacking, blacklisting, and DDoS attacks.

Users can protect their IP address by using firewalls, keeping software updated, using VPNs, and enabling two-factor authentication.

Different types of IP addresses include public and private, with public

Types of ports

- Port number is a 16-bit numerical value that ranges from 0 to 65535. Well-known port (0-1023), registered port (1024-49151), and dynamic port is three types of port number space. (49152-65535).

Why is it important to know these ports?

Any security researcher, bug bounty hunter, or anyone working with service configuration would benefit from this. Knowing how to do more thorough scans such as version detection or known vulnerabilities

HTTP, SMTP, FTP, DNS, SSH, Telnet, or VCN) are running and the kind of system being used by the target victim. Here's the list of potential logical ports that are the targets of cybercriminals.

- **15 Netstat**
- **20/21 FTP**
- **22 SSH**
- **23 Telnet**
- **25 SMTP**
- **50/51 IPSec**

OMMON PORTS

Port #	Application Layer Protocol	Type	Description
20	FTP	TCP	File Transfer Protocol - data
21	FTP	TCP	File Transfer Protocol - control
22	SSH	TCP/UDP	Secure Shell for secure login
23	Telnet	TCP	Unencrypted login
25	SMTP	TCP	Simple Mail Transfer Protocol
53	DNS	TCP/UDP	Domain Name Server
67/68	DHCP	UDP	Dynamic Host
80	HTTP	TCP	HyperText Transfer Protocol
123	NTP	UDP	Network Time Protocol
161,162	SNMP	TCP/UDP	Simple Network Management Protocol
389	LDAP	TCP/UDP	Lightweight Directory Authentication Protocol
443	HTTPS	TCP/UDP	HTTP with Secure Socket Layer

Cisco packet tracer

- Cisco Packet Tracer as the name suggests, is a tool built by Cisco. This tool provides a network simulation to practice simple and complex networks.
- The curriculum like CCNA, CCENT where Faculties use Packet Trace to demonstrate technical concepts and networking systems. Students complete assignments using this tool, working on their own or in teams. Engineers prefer to test any protocols on Cisco Packet Tracer before implementing them
- **Logical** – Logical workspace shows the logical network topology of the network the user has built. It represents the placing, connecting and clustering virtual network devices.
- **Physical** – Physical workspace shows the graphical physical dimension of the logical network. It depicts the scale and placement in how network devices such as routers, switches and hosts would look in a real environment.

Key features of Cisco packet tracer

- Unlimited devices
- E-learning
- Customize single/multi user activities
- Interactive Environment
- Visualizing Networks
- Real-time mode and Simulation mode
- Self-paced
- Supports majority of networking protocols
- International language support
- Cross platform compatibility

Window network command

- The Windows operating system provides its user with a powerful tool, i.e., **Command Prompt**, which allows us to access and configure system settings and data. In this article on 'Networking Commands', we will look into some of the most popular network commands.

IPConfig. This ipconfig command is used for finding the IP address and default gateway of your network. ...

IfConfig. The ifconfig command is mainly used: ...

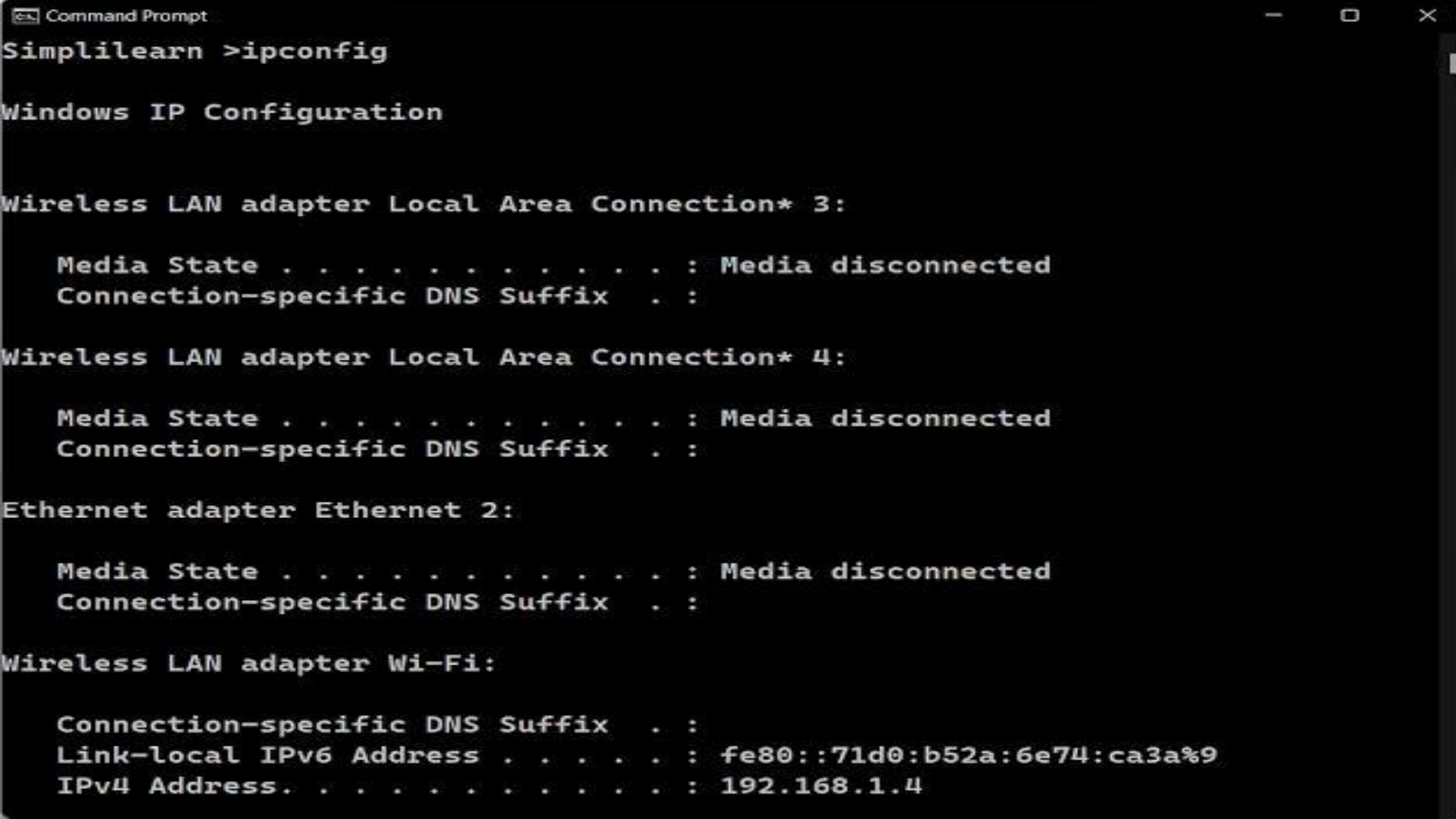
Tracert. ...

Ping. ...

Netstat. ...

Nslookup Command. ...

Getmac


Command Prompt
Simplilearn >ipconfig
Windows IP Configuration
Wireless LAN adapter Local Area Connection* 3:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Local Area Connection* 4:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Ethernet adapter Ethernet 2:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::71d0:b52a:6e74:ca3a%9
IPv4 Address. . . . . : 192.168.1.4

Python for ethical Hacking

Fast and compatible

- Being able to gain access to a system that you're not supposed to have access to is known as Hacking. For example, login into an email account without authorization is considered hacking that account. Gaining access to a remote computer without authorization is hacking that computer. So you can see that there are a large number of ways to hack into a system and the word hacking can refer to a number of things but the main concept is the same

- **Why Python Programming For Hacking**

Python is a widely used general-purpose, high-level programming language. Python is a very simple language yet powerful scripting language, it's open-source and object-oriented and it has great libraries that can be used for both for hacking and for writing very useful normal programs other than hacking programs. In the future and present era python is very popular and it's easy to learn, learning to hack with python will be fun and you will learn python programming in the best way. There is a great demand for python developers in the market.

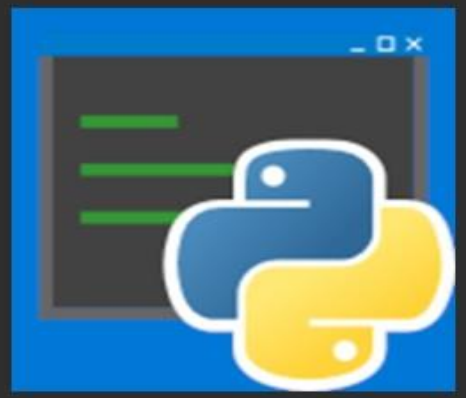
setting up python

Microsoft Store

Home Apps Games Search Cart 43 ...

This product is installed.

Install on my devices ...



Python 3.7

Python Software Foundation

Developer tools > Development kits

★★★★☆ 2 Share

Python is an easy to learn, powerful programming language. It has efficient high-level data structures and a simple but effective approach to object-oriented programming. Python's elegant

More

Wish list

PEGI 3

Visual studio code

- One of the coolest code editors available to programmers, Visual Studio Code, is an open-source, extensible, light-weight editor available on all platforms. It's these qualities that make Visual Studio Code from Microsoft very popular, and a great platform for Python development

How to Install Visual Studio Code

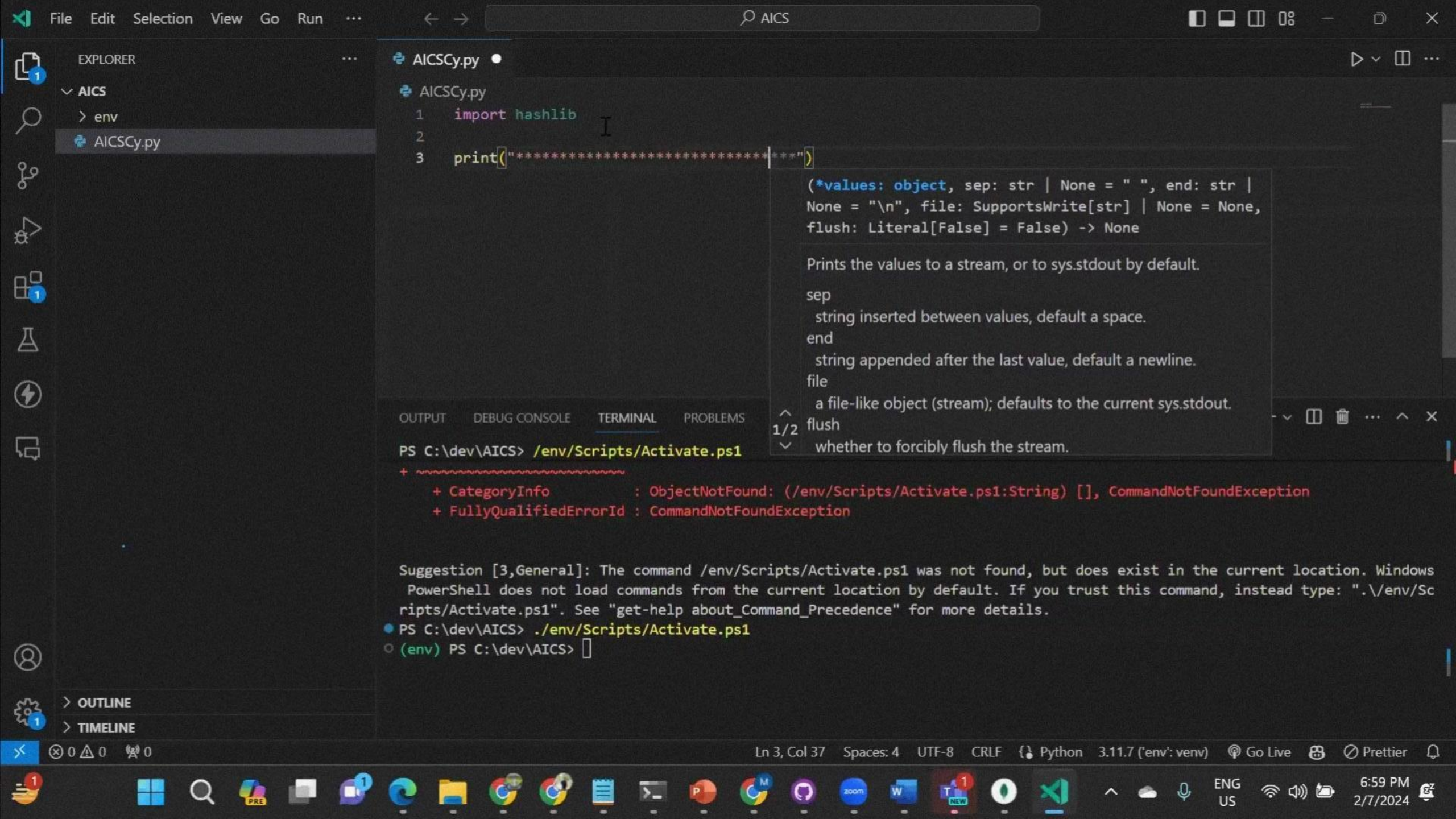
Discover and install extensions that make Python development easy

Write a straightforward Python application

Learn how to run and debug existing Python programs in VS Code

Connect Visual Studio Code to Git and GitHub to share your code with the world

We assume you are familiar with Python development and already have some form of Python installed on your system (Python 2.7, Python 3.6/3.7, Anaconda, or others). Screenshots and demos for Ubuntu

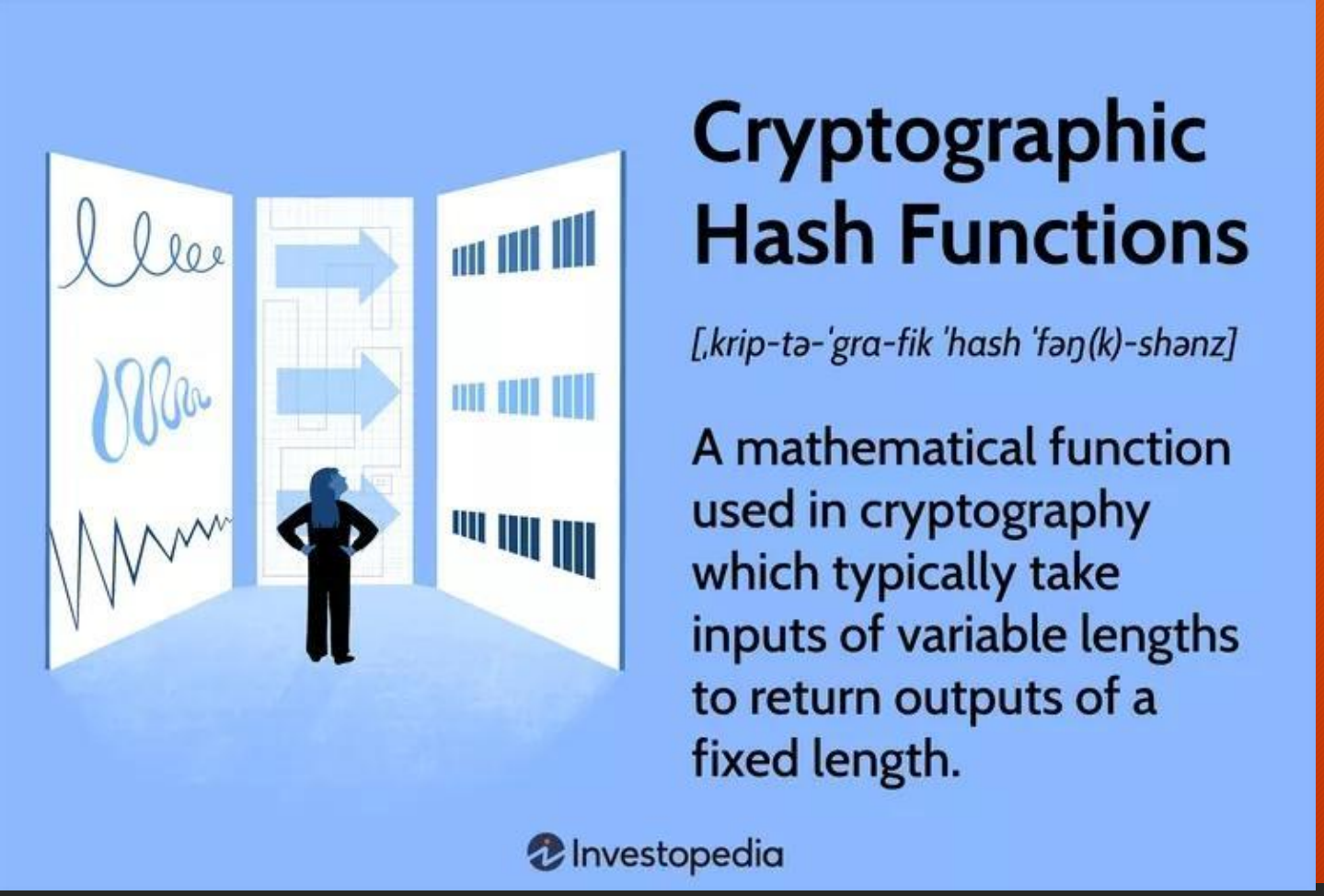

File Edit Selection View Go Run
AICS
EXPLORER
AICS
env
AICSCy.py
AICSCy.py
1 import hashlib
2
3 print("**********")
(*values: object, sep: str | None = " ", end: str | None = "\n", file: SupportsWrite[str] | None = None, flush: Literal[False] = False) -> None
Prints the values to a stream, or to sys.stdout by default.
sep
string inserted between values, default a space.
end
string appended after the last value, default a newline.
file
a file-like object (stream); defaults to the current sys.stdout.
flush
whether to forcibly flush the stream.
1/2
OUTPUT DEBUG CONSOLE TERMINAL PROBLEMS
PS C:\dev\AICS> /env/Scripts/Activate.ps1
+ CategoryInfo : ObjectNotFound: (/env/Scripts/Activate.ps1:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException
Suggestion [3,General]: The command /env/Scripts/Activate.ps1 was not found, but does exist in the current location. Windows PowerShell does not load commands from the current location by default. If you trust this command, instead type: ".\env/Scripts/Activate.ps1". See "get-help about_Command_Precedence" for more details.
PS C:\dev\AICS> ./env/Scripts/Activate.ps1
(env) PS C:\dev\AICS>
OUTLINE
TIMELINE
Ln 3, Col 37 Spaces: 4 UTF-8 CRLF Python 3.11.7 ('env': venv) Go Live Prettier
ENG US
6:59 PM 2/7/2024

Cryptographic Hash fuction (CHF)

- A cryptographic hash function is a mathematical function used in cryptography. Typical hash functions take inputs of variable lengths to return outputs of a fixed length
- A cryptographic hash function combines the message-passing capabilities of hash functions with security properties.

KEY TAKEAWAYS

- Hash functions are mathematical functions that transform or “map” a given data set into a bit string of fixed size, also known as the “hash value.”
- Hash functions are used in cryptography and have variable levels of complexity and difficulty.
- Hash functions are used for cryptocurrency, password security, and message security.a

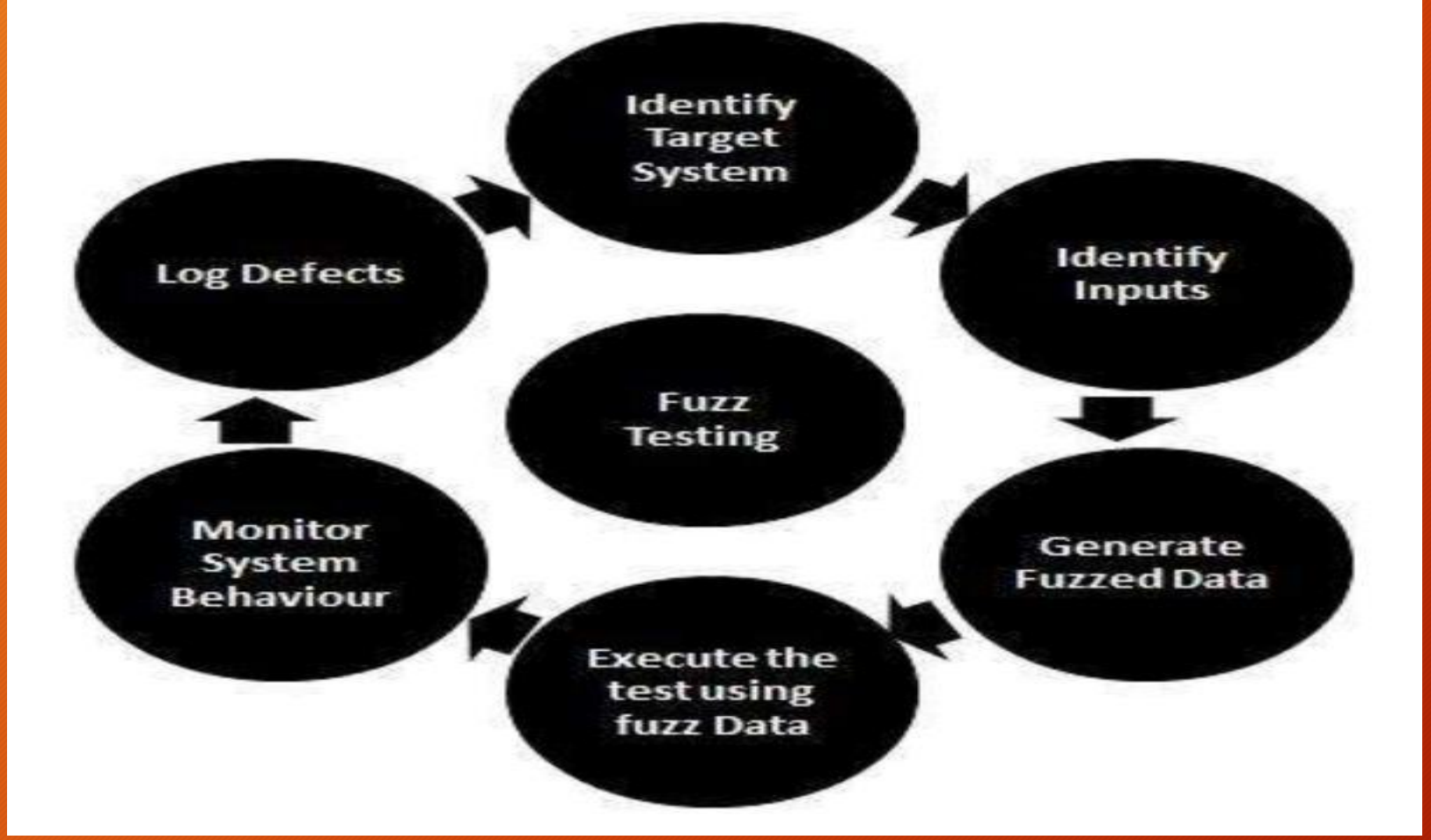


Hash functions are commonly used data structures in computing systems for tasks such as checking the integrity of messages and authenticating information. While they are considered cryptographically "weak" because they can be solved in cryptographies

HOW CRYPTOGRAPHIC HASH FUNCTION WORK

Types of Hashing

- **Types of Hashing in Cybersecurity**
- As a cybersecurity professional, you can select from a wide variety of different types of hashing. Some of the most widely used for decryption are described below:
- **1. MD5**
- The Message Digest hashing algorithm's fifth iteration is MD5, which creates a 128-bit hash function.
- **2. SHA-1**
- SHA-1, the first iteration of the Secure Hash Algorithm, generates a hash function output that is 160 bits long. This SHA is one of the primary hashing algorithms used by professionals in the field of computer science.
- **3. SHA-2**
- SHA-2 is not just one hashing algorithm. Instead, it is a group of four algorithms: SHA-224, SHA-256, SHA-384, and SHA-512. The name of each hashing algorithm is the same as the bit output it generates.
- **4. CRC32**
- The CRC32 hashing algorithm uses a Cyclic Redundancy Check (CRC) as its primary method for identifyin unauthorized changes to data that has been saved. When data is encoded using CRC32, the output hash value will always be of a consistent length. Hashing is performed with the CRC32 method on Zip file formats and File Transfer Protocol (FTP) servers.



FUZZING

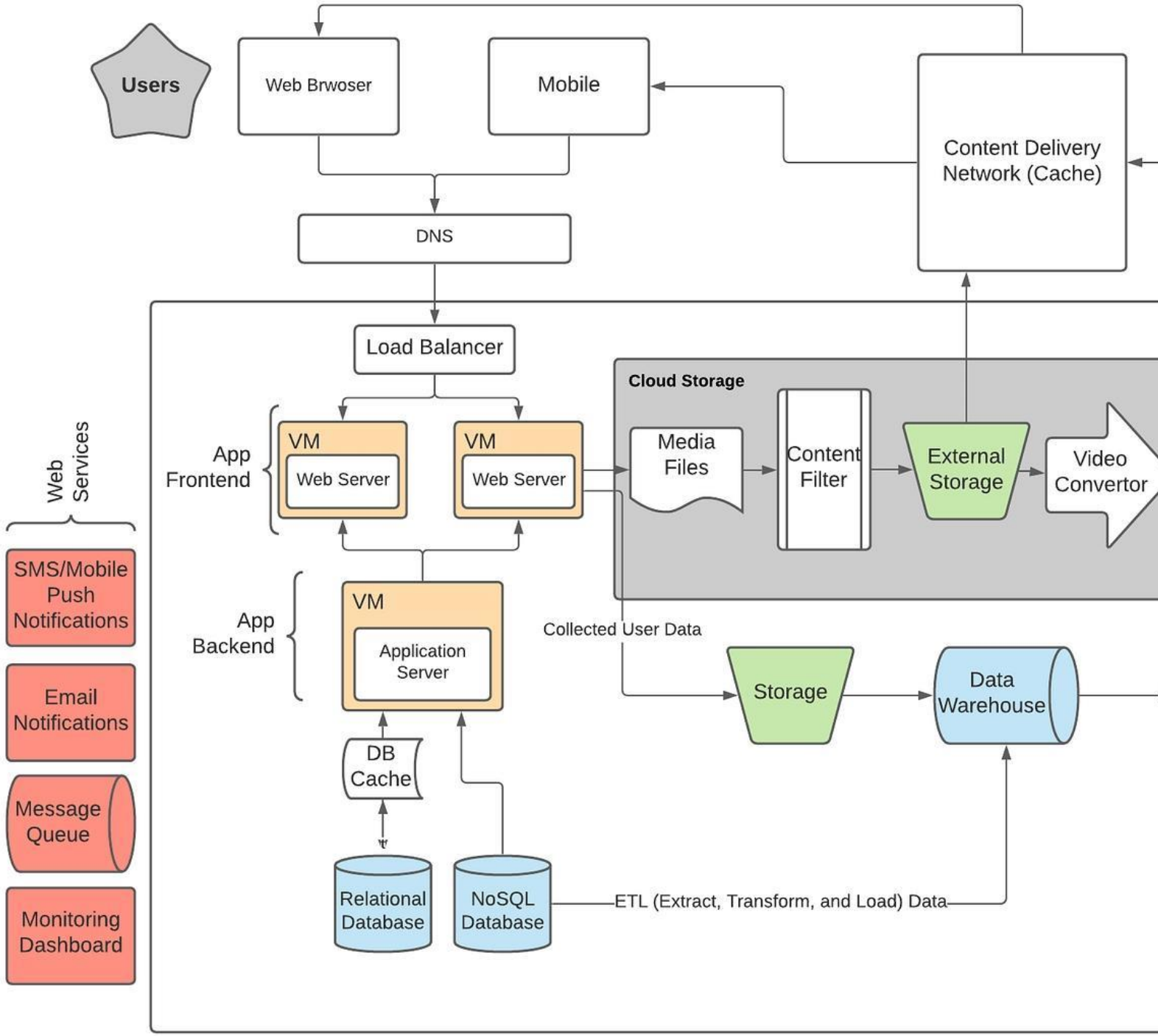
fuzzer is a program which injects automatically semi-random data into a program/stack and detect bugs. The data-generation part is made of generators, and vulnerability identification relies tools

Web Applications

- 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

The application server performs the task that requested by the clients, which also may need a database to store the information sometimes. Application server technologies range from **ASP.NET, ASP**, and **ColdFusion to PHP and JSP**.

Web Application architecture



OWASP

- The oswap stands for open source web application Security project
- The Open Web Application **Security** Project (OWASP) is a non-profit organization founded in 2001, with the goal of helping website owners and security experts protect web applications from cyber attacks.

Web Application Security Risks

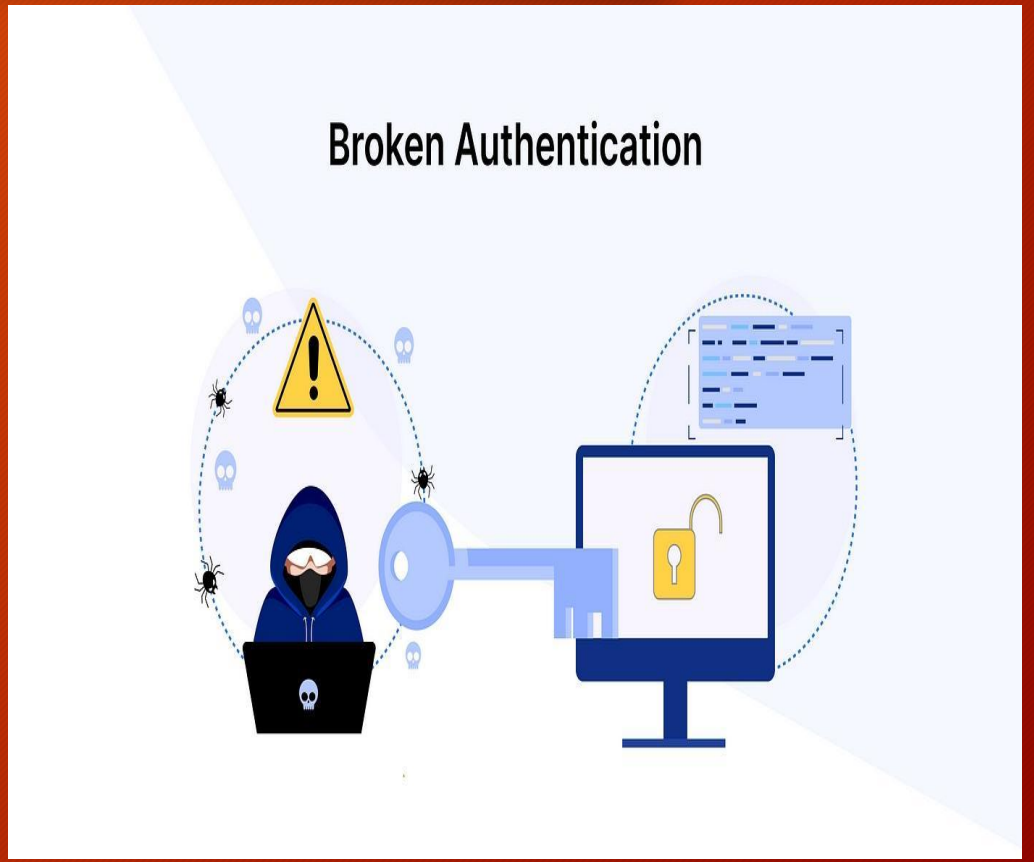
- Injection flaws
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XEE)
- Security Misconfiguration.
- Cross-Site Scripting.
- Insecure Deserialization
- Using components with known vulnerability
- Insufficient logging and Monitoring

Injection flaws

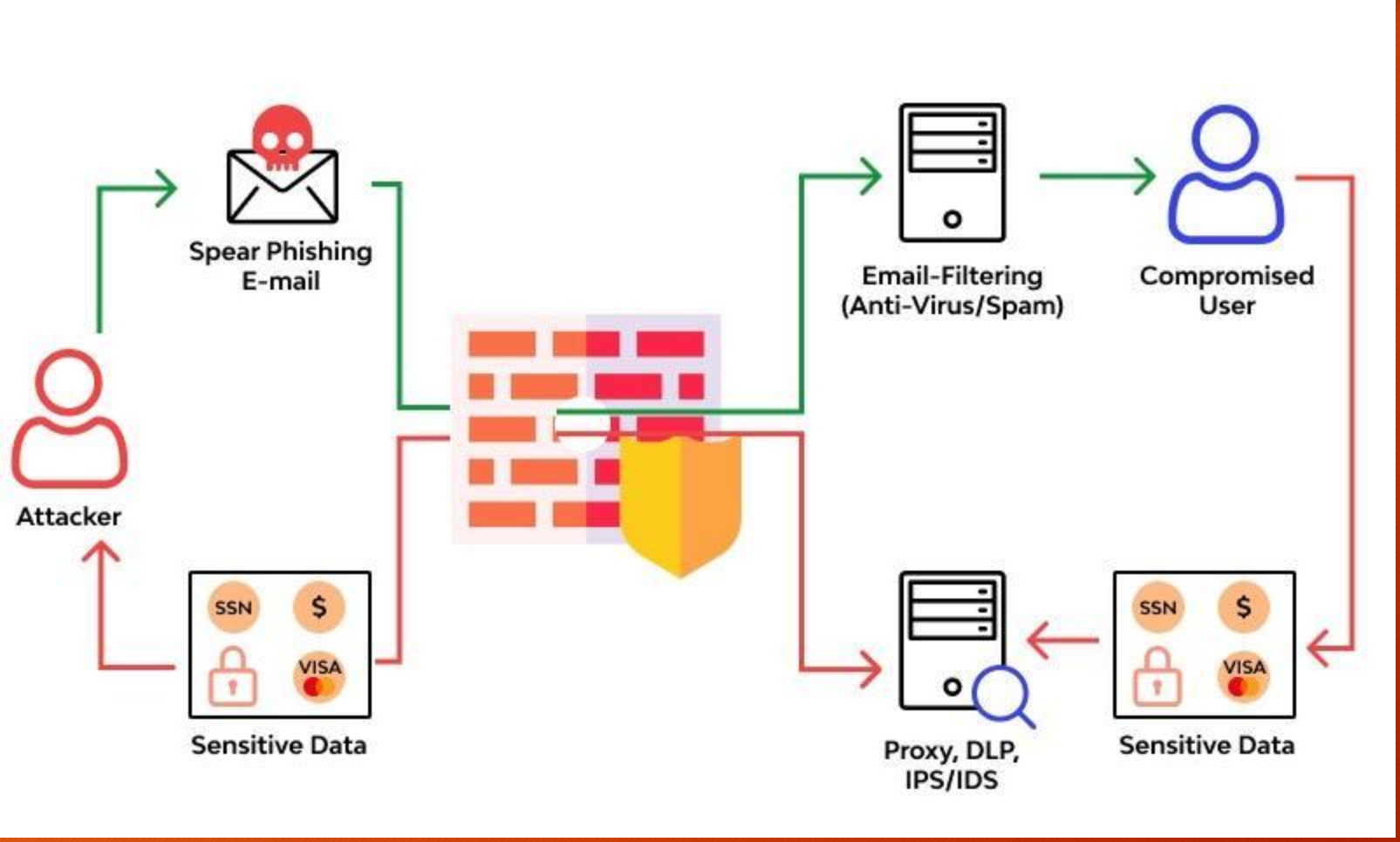
- Injection attacks happen when untrusted data is sent to a code interpreter through a form input or some other data submission to a web application. For example, an attacker could enter SQL database code into a form that expects a plaintext username. If that form input is not properly secured, this would result in that SQL code being executed. This is known as an SQL injection attack.
-
- Injection attacks can be prevented by validating and/or sanitizing user-submitted data. (Validation means rejecting suspicious-looking data, while sanitization refers to cleaning up the suspicious-looking parts of the data.) In addition, a database admin can set controls to minimize the amount of information an injection attack can expose.

Broken Authentication

- Vulnerabilities in authentication (login) systems can give attackers access to user accounts and even the ability to compromise an entire system using an admin account. For example, an attacker can take a list containing thousands of known username/password combinations obtained during a data breach and use a script to try all those combinations on a login system to see if there are any that work.
- Some strategies to mitigate authentication vulnerabilities are requiring two-factor authentication (2FA) as well as limiting or delaying repeated login attempts using rate limiting.



Sensitive Data Exposure

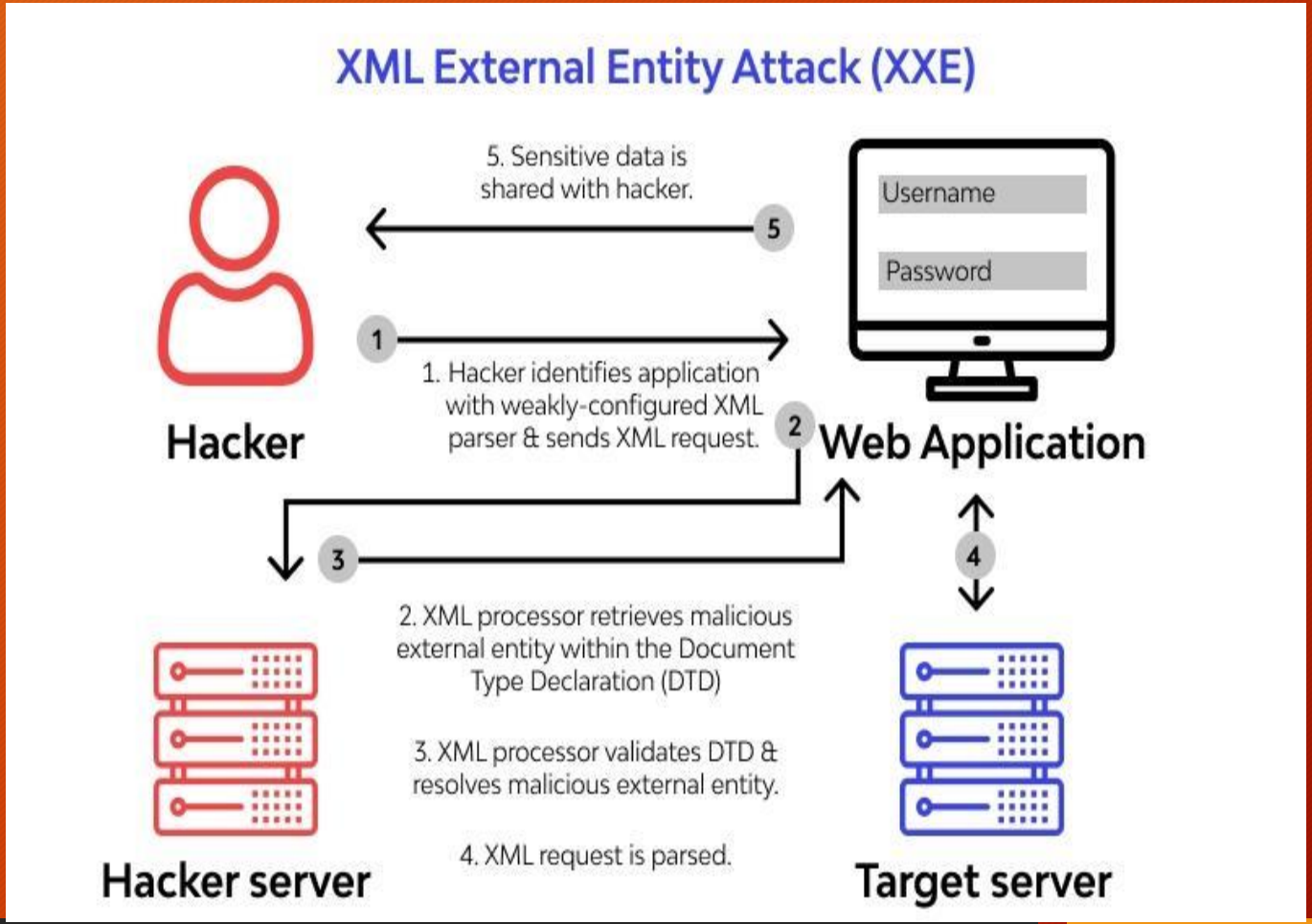


web applications don't protect sensitive data such as financial information and passwords, attackers can gain access to that data and sellor utilize it for nefarious purposes. One popular method for stealing sensitive information is using an on-path attack. Data exposure risk can be minimized by encrypting all sensitive data as well as disabling the caching* of any sensitive information. Additionally, web application developers should take care to ensure that they are not unnecessarily storing any sensitive data.

XML External Entities (XEE)

This is an attack against a web application that parses XML* input. This input can reference an external entity, attempting to exploit a vulnerability in the parser. An 'external entity' in this context refers to a storage unit, such as a hard drive. An XML parser can be duped into sending data to an unauthorized external entity, which can pass sensitive data directly to an attacker.

The best ways to prevent XEE attacks are to have web applications accept a less complex type of data, such as JSON**, or at the very least to patch XML parsers and disable the use of external entities in an XML application.

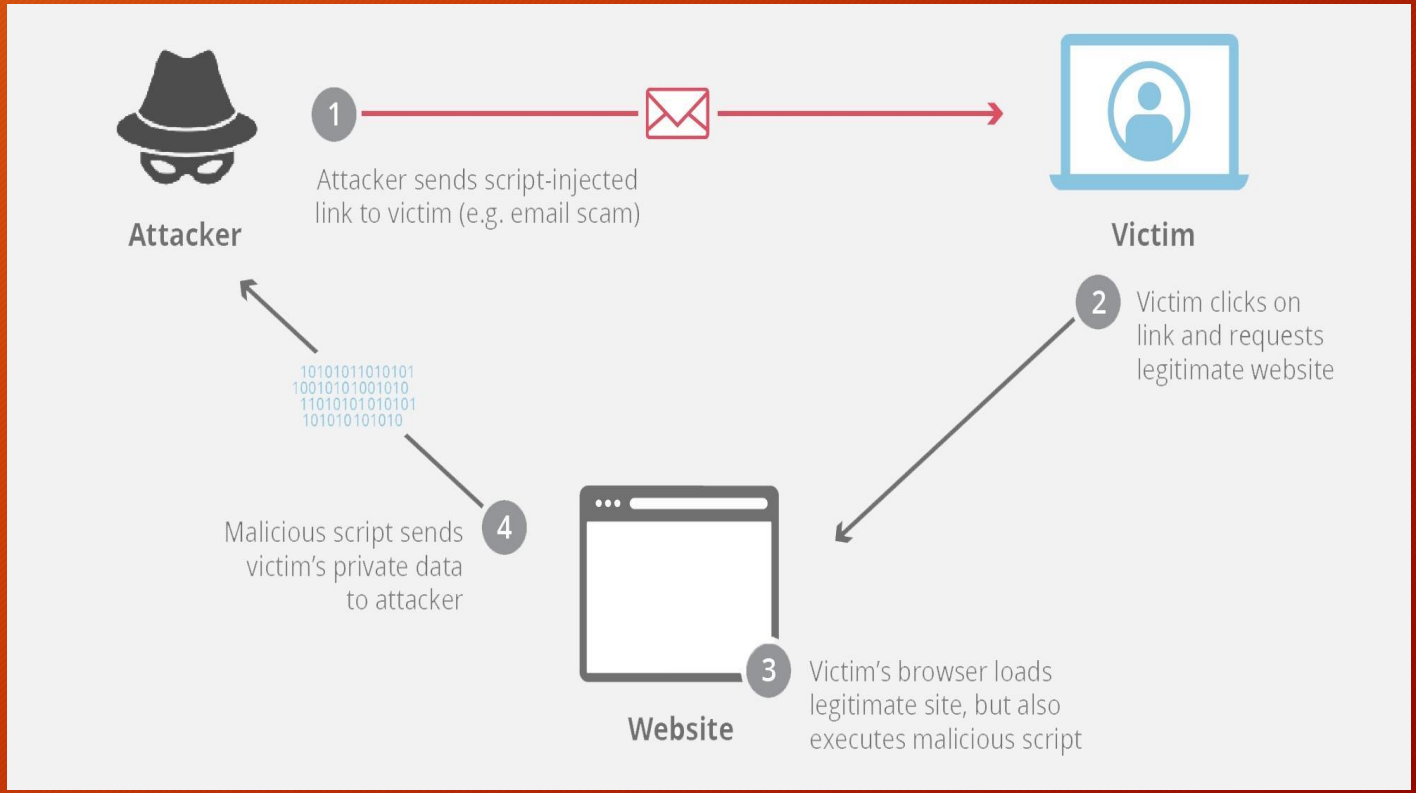


Security Misconfiguration

Security misconfiguration is the most common vulnerability on the list, and is often the result of using default configurations or displaying excessively verbose errors. For instance, an application could show a user overly-descriptive errors which may reveal vulnerabilities in the application. This can be mitigated by removing any unused features in the code and ensuring that error messages are more general.

Cross - site Scripting (Xss)

- Cross-site scripting (XSS) is an exploit where the attacker attaches code onto a legitimate website that will execute when the victim loads the website. That malicious code can be inserted in several ways. Most popularly, it is either added to the end of a url or posted directly onto a page that displays user-generated content. In more technical terms, cross-site scripting is a client-side code injection attack.
-




THANK YOU