# CYBER SECURITY

Assignment -1

# WHAT IS CYBER SECURITY

Cybersecurity involves protecting computer systems, networks, and data from digital attacks, unauthorized access, and damage to ensure confidentiality, integrity, and availability of information. It encompasses various measures, such as firewalls, encryption, and authentication, to safeguard against cyber threats like malware, phishing, and hacking.

# PASSIVE AND ACTIVE ATTACKS

Passive attacks involve unauthorized monitoring or eavesdropping on data without altering it, while active attacks involve manipulating or disrupting data, like through unauthorized access or modification. Examples of passive attacks include sniffing and traffic analysis, while active attacks include malware, denial of service (DoS), and injection attacks. Cybersecurity measures aim to prevent and mitigate both types of attacks.

# HACKER CATEGORIES

Black Hat Hackers: Malicious hackers who exploit vulnerabilities for malicious purposes, such as stealing data, spreading malware, or causing damage.

White Hat Hackers: Ethical hackers employed to identify and fix security vulnerabilities. They work to improve systems' security.

Grey Hat Hackers: Individuals who fall between black hat and white hat hackers. They may exploit vulnerabilities without authorization but without malicious intent, often notifying the organization afterward

# ESSENSHIYAL TERMINOLOGIES

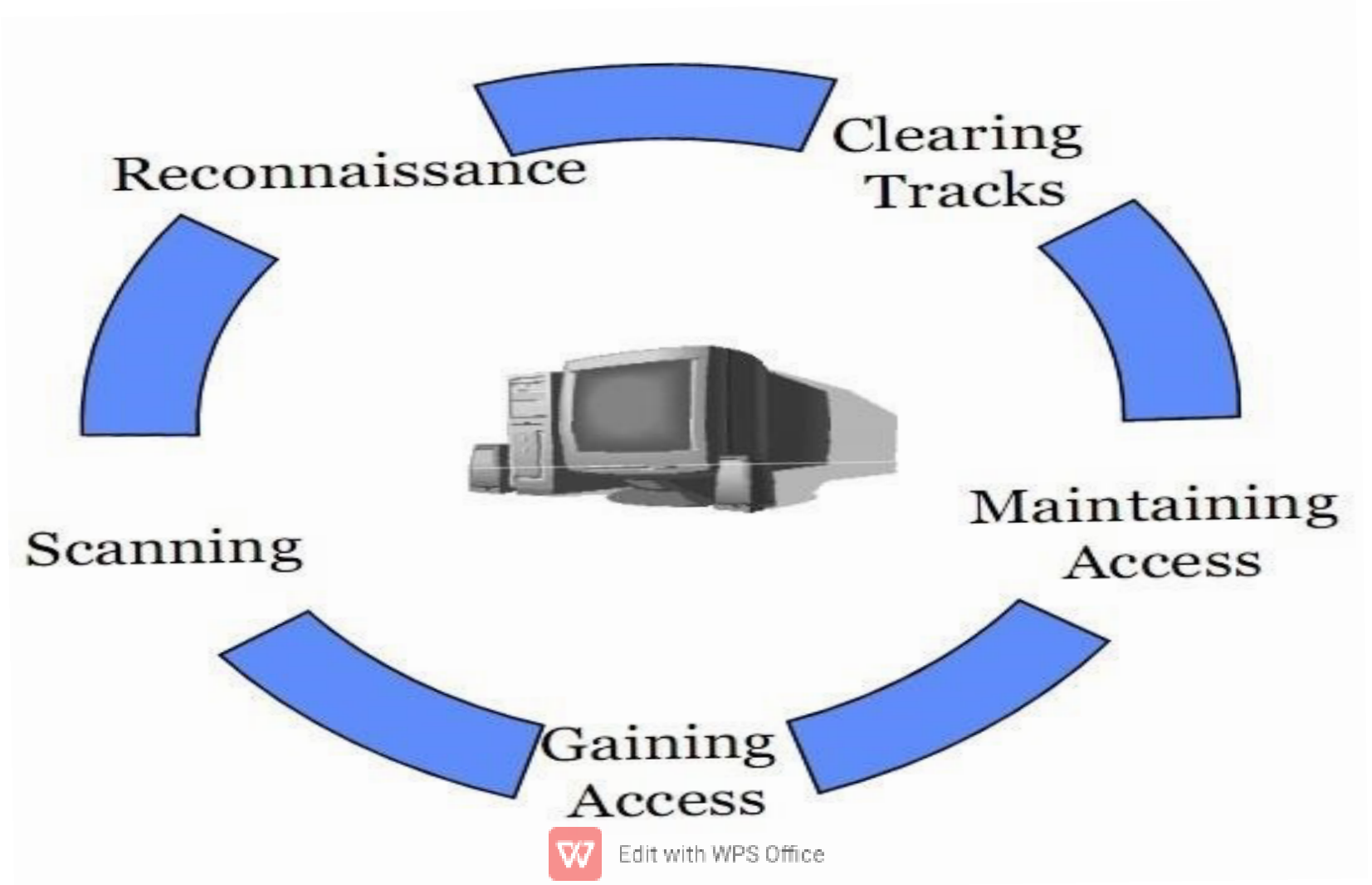
Firewall: A security barrier that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

Encryption: The process of converting information into a code to prevent unauthorized access, protecting data confidentiality.

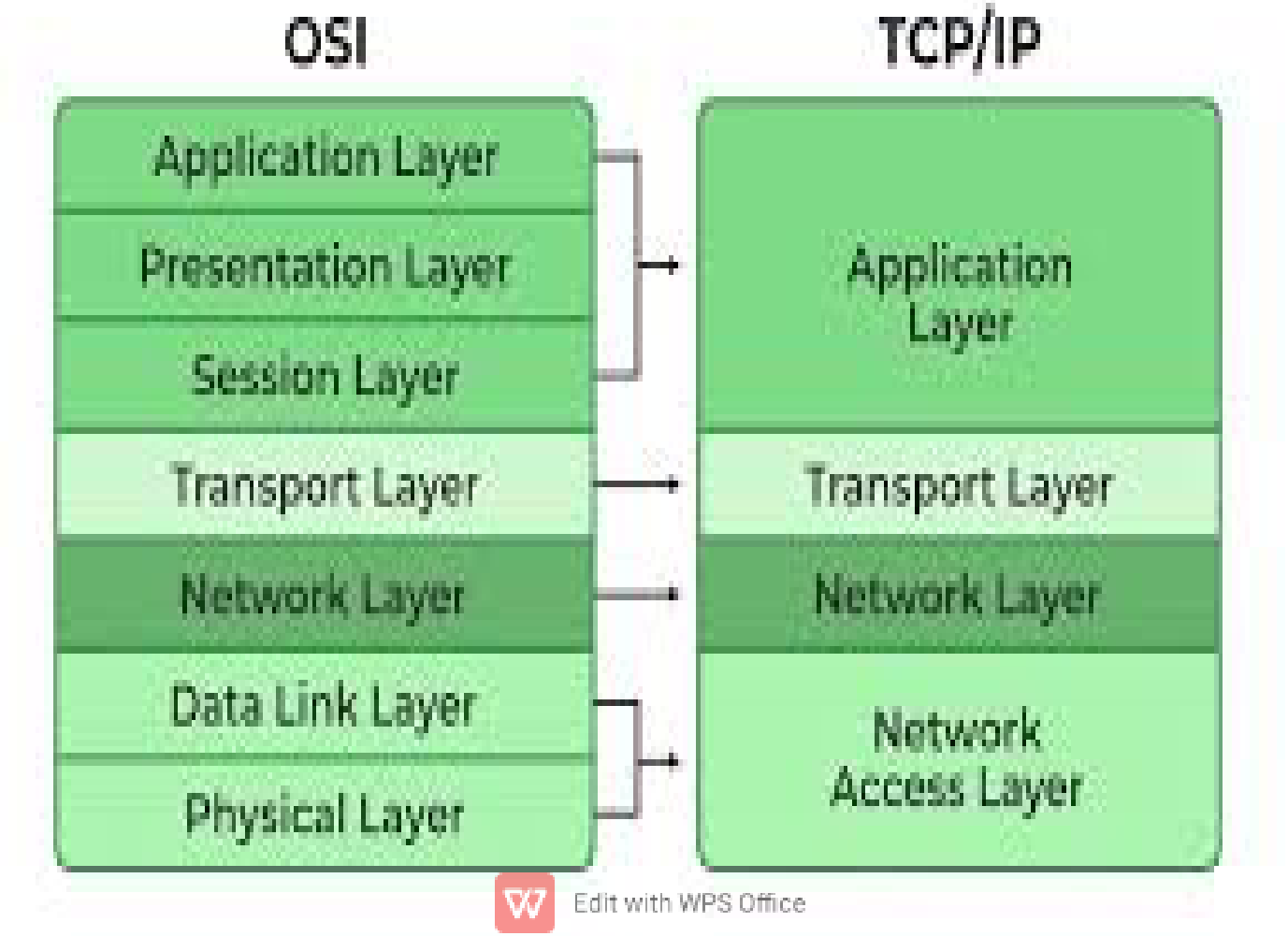
Malware: Malicious software, including viruses, ransomware, and spyware, designed to harm or exploit computer systems.

Phishing: A fraudulent attempt to obtain sensitive information, such as usernames, passwords, and credit card details, by disguising as a trustworthy entity.

# PHASES OF HACKEING



# OSI AND TCP/IP MODEL



# DATABASE OF CISCO PACKET TRACER

Cisco Packet Tracer is a simulation tool primarily used for networking scenarios and not specifically designed for storing databases related to cybersecurity. However, you can use external databases or tools for managing cybersecurity-related data and integrate them with your Packet Tracer network simulations. Consider using dedicated cybersecurity tools and databases for tasks like logging, monitoring, and analyzing security events.

# CONTROL STRUCTURES

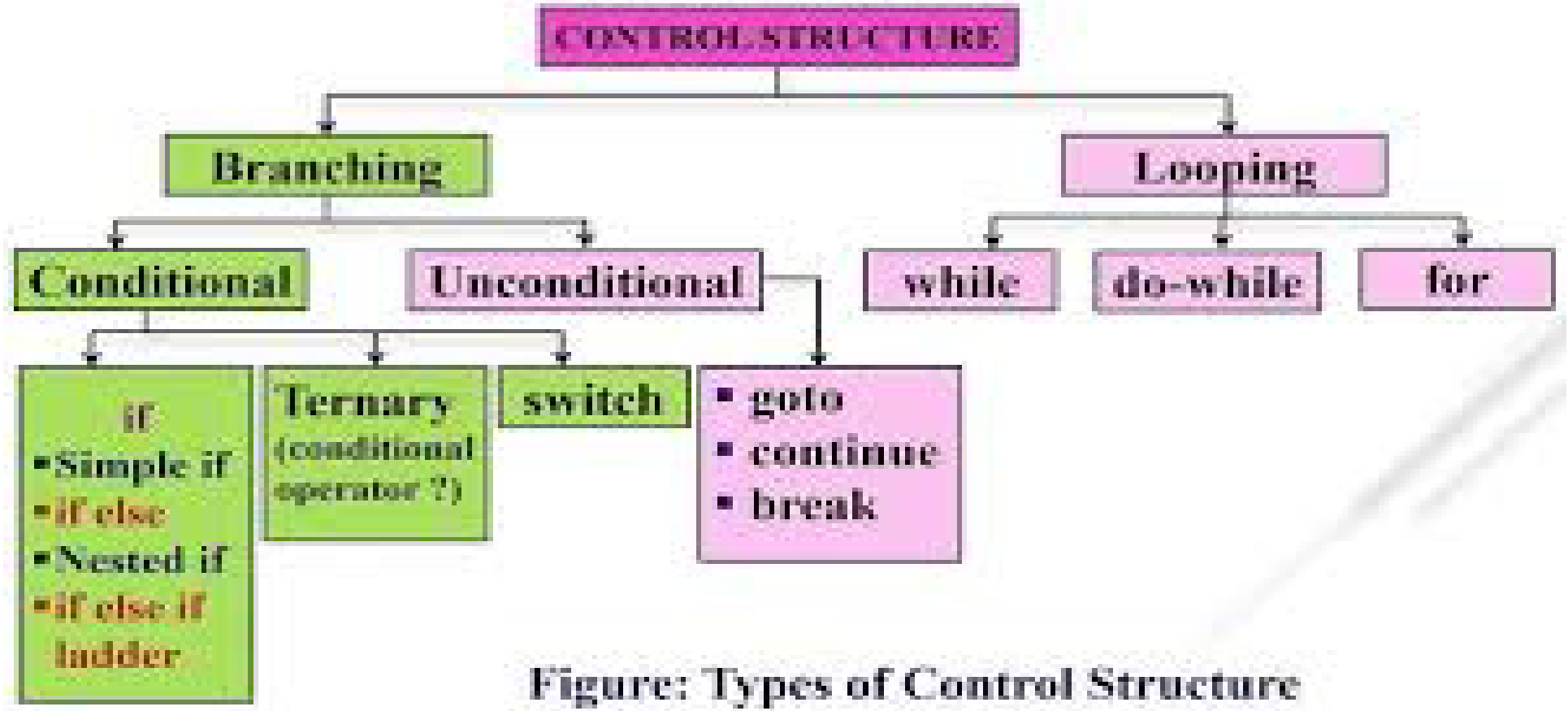


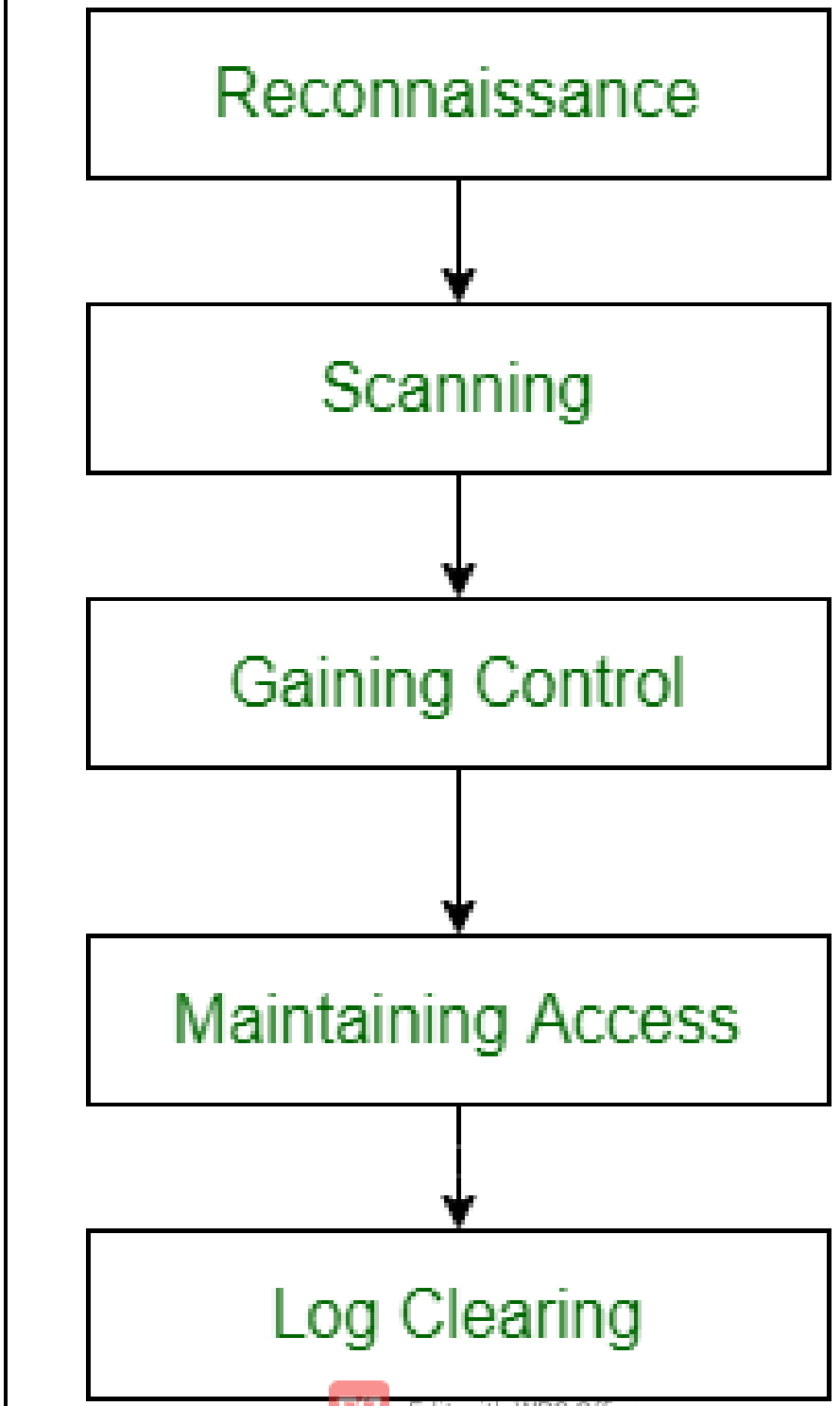

Figure: Types of Control Structure

# CRYPTOGRAPHY

Cryptography plays a crucial role in cybersecurity by securing communication, data, and identities. It involves techniques for encrypting and decrypting information, ensuring confidentiality, integrity, and authenticity in digital transactions and communications.

# What is a Web Application

- Web Application simply means the application or software that usage a web browser as a client .
- Web Application is mainly coded in browser-supported programming language like HTML, PHP, Javascript, XML, Perl, Python.
- It is popular due to its fast update without updating any software or any and due to convenience of using a web browser



# THANK YOU