CYBER SECURITY

WHAT IS FOOTPRINTING

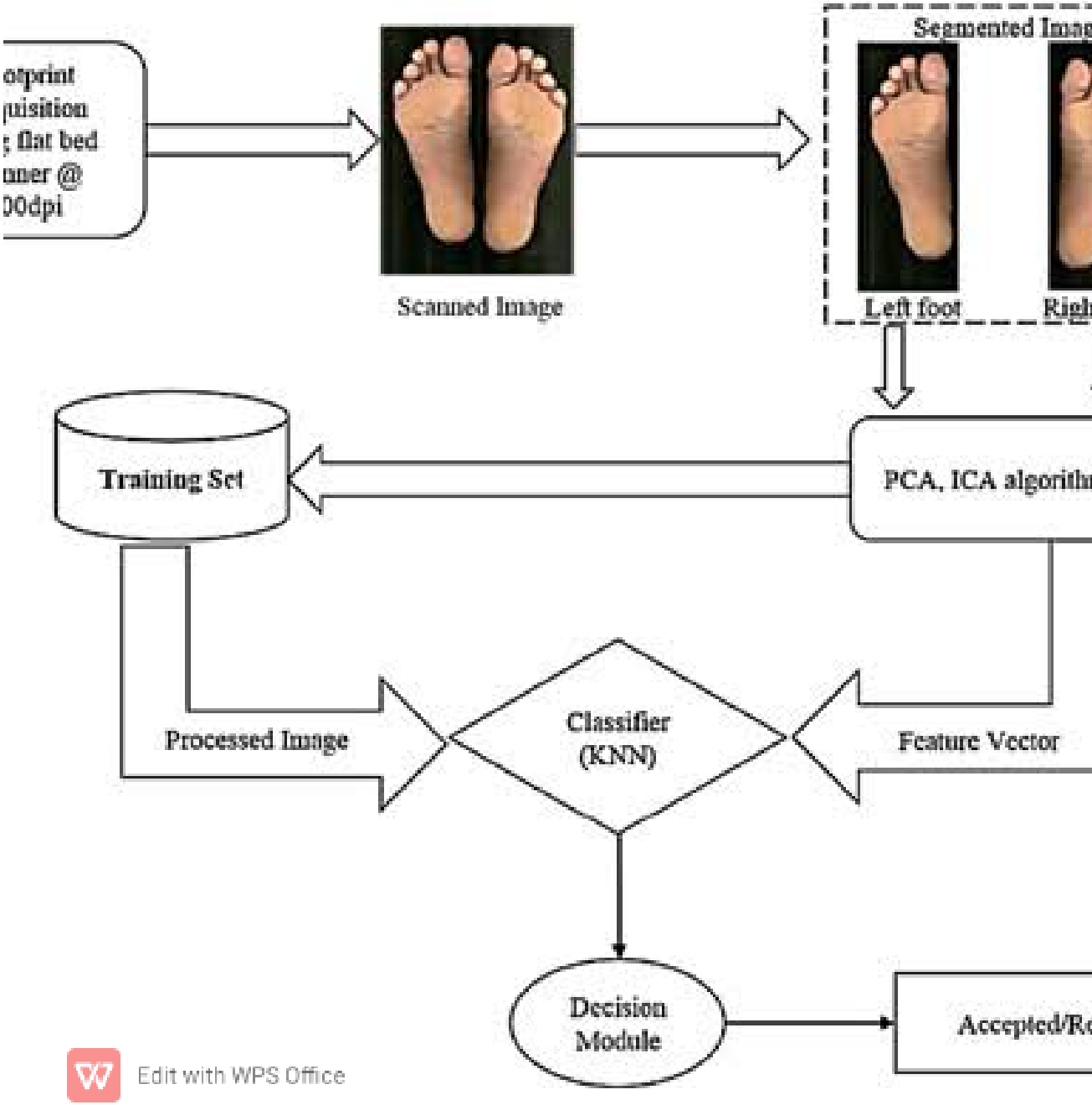
Footprinting, also known as fingerprinting, is a methodology used by penetration testers, cybersecurity professionals, and even threat actors to gather information about a target organization to identify potential vulnerabilities. Footprinting is the first step in penetration testing. It involves scanning open ports, mapping network topologies, and collecting information about hosts, their operating systems, IP addresses, and user accounts. This gathered data helps to generate a comprehensive technical blueprint of the target organization.

TYPE OF FOOTPRINTING

1.Passive Footprinting: Involves collecting information without directly interacting with the target, such as through social media, public records, or WHOIS databases.

2.Active Footprinting: Involves actively engaging with the target to gather information, often using tools like network scanners, DNS interrogation, or social engineering.

ARCHITECTURE OF FOOTPRINTING



WHAT IS DNS FOOTPRINTING

DNS footprinting in cybersecurity refers to the process of gathering information about a target or a network by analyzing its Domain Name System (DNS) records. This technique involves querying DNS servers to obtain details such as domain names, IP addresses, mail server information, and other DNS-related data. Attackers use DNS footprinting to gather intelligence for potential vulnerabilities, target reconnaissance, or planning more sophisticated cyber attacks. It's an essential aspect of cybersecurity to understand and mitigate the risks associated with DNS footprinting.

RECONNAISSANCE

In cybersecurity, reconnaissance refers to the phase where attackers gather information about a target system or network. It involves collecting data on vulnerabilities, network topology, and potential entry points, helping attackers plan and execute their cyber attacks. Reconnaissance can be classified into two types: passive, where attackers gather information without directly interacting with the target, and active, where they engage with the target to collect more specific data.

TYPES OF RECONNAISSANCE

Passive Reconnaissance: Collecting data without directly interacting with the target, such as analyzing publicly available information or monitoring network traffic.

Active Reconnaissance: Actively engaging with the target, often through network scanning, probing, or other methods that may be more detectable.

Social Engineering: Exploiting human interactions to gather information, often through deceptive tactics like phishing or impersonation.

UNDERSTANDING ETHICAL HACKING

Ethical hacking in cybersecurity involves authorized professionals, known as ethical hackers, testing systems for vulnerabilities to strengthen security. They use the same techniques as malicious hackers but with the goal of identifying and fixing weaknesses. It helps organizations preemptively address security flaws and protect against potential cyber threats.

TYPES OF ETHICAL HACKING

Penetration Testing: Simulating cyberattacks to identify vulnerabilities in systems or networks.

Vulnerability Assessment: Identifying and assessing potential weaknesses in a system's security.

Web Application Testing: Focusing on evaluating the security of web applications to prevent attacks like SQL injection and cross-site scripting.

Network Security Testing: Examining the security of network infrastructure to ensure protection against unauthorized access.

THANK YOU