VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT)

CENTRE FOR DEVLOPEMENT OF ADVANCE COMPUTING (C-DAC)

Group No – 01

Group members

Vipul Kumar

Naman Richhariya

Pritish Prakash Kshetre

Kumawat Naresh Ramanand

Patel Divyakumar Harshadbhai

Guided by : - Dr. Sanjay Adiwal

Associate Director of CDAC Bangalore

CONTENT:-

- What is Vulnerability.?
- Classification of Vulnerability
- Vulnerability Assessment
- Penetration Testing and their types
- Types of Scanning in VAPT
- Phase in penetration Testing
- Workflow Diagram
- Process of VAPT in detail
- How VAPT is performed in IT Network (Automated & Manual)
- Few tools in VAPT

WHAT IS VULNERABILITY ..?

- It is like a gap or a weak spot in a computer system, network, software, or process . It's a potential entry point that hacker could use to break into or harm the security of the system and steal sensitive information.

  e.g:

CLASSIFICATION OF VULNERABILITY

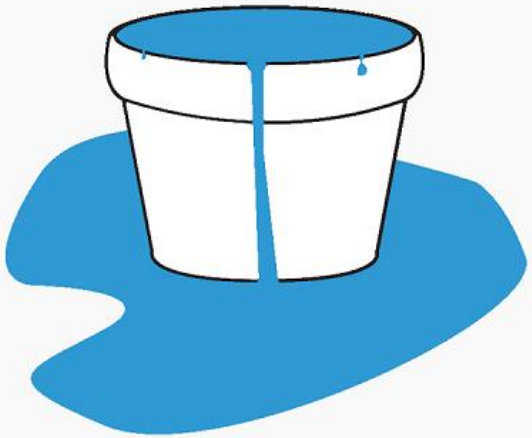
- **Misconfiguration** – It refers to the incorrect setup of software, hardware, or systems, often due to human error or oversight. It can lead to security vulnerabilities, unauthorized access, and data exposure. e.g. include weak passwords, default settings, and improperly configured access controls.

CLASSIFICATION OF VULNERABILITY

- **Default Installation** – It is a type of vulnerability in a computing device that most commonly affects devices having some default application(pre installed apps) and administrative credentials to access all configuration settings.

CLASSIFICATION OF VULNERABILITY

- **Buffer Overflow –** It is buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer.



CLASSIFICATION OF VULNERABILITY

- **Unpatched server –** It is the security flaws or weaknesses in software, hardware, or systems that have not yet been addressed through an update or patch.

  eg- proxynotshell & proxylogon in Microsoft.

CLASSIFICATION OF VULNERABILITY

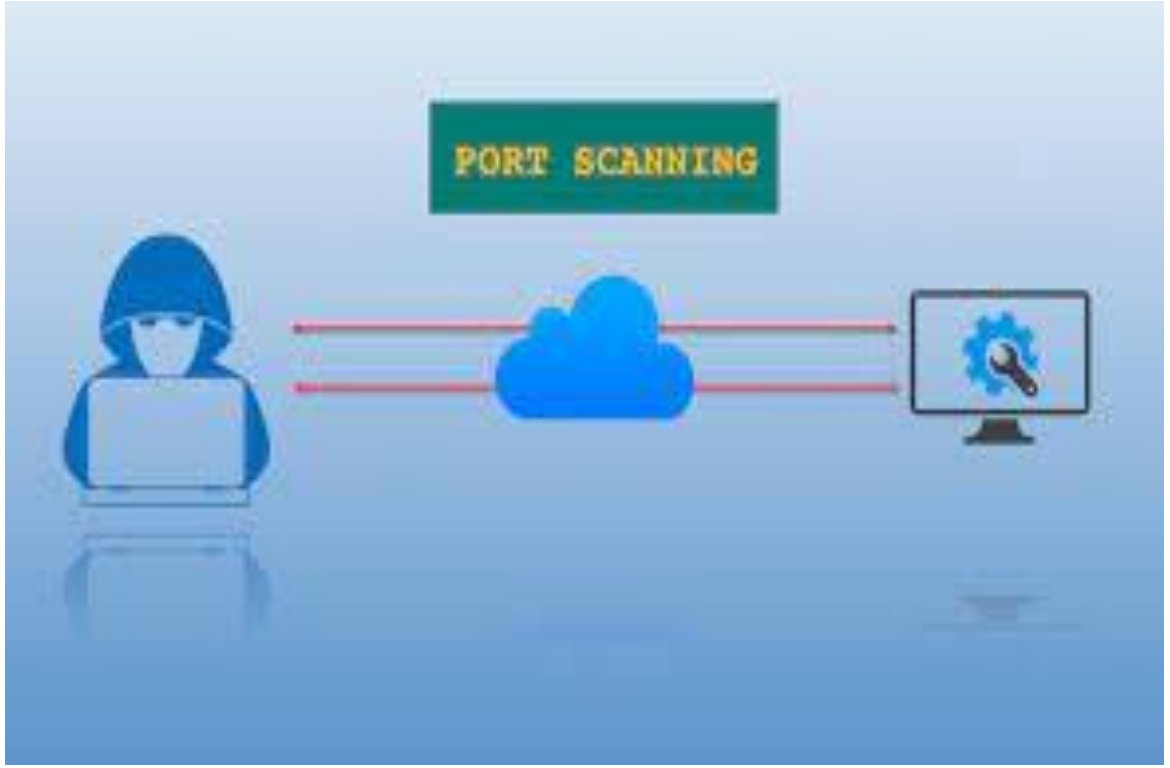
- **Design Flaws –** It refers to design of software, hardware or any process in which any mistake done by developer a web application or web site. a weakness or opportunity in an information system that cybercriminals can exploit and gain unauthorized access to a computer system.

CLASSIFICATION OF VULNERABILITY

- **OS flaws –** These vulnerabilities are exposures within an OS that allow hackers to cause damage on that device where the OS is installed .

CLASSIFICATION OF VULNERABILITY

- **Open Ports** – It is as doors in a house; if these doors are unlocked or unguarded, They can exploit these unprotected entry points to gain unauthorized access to your computer or network.



CLASSIFICATION OF VULNERABILITY

- **Application Flaws** – Thes are like cracks in a digital wall. if not fixed, hackers can use them to break in and compromise your data. You need to updates and remove the flaws in the apps always.

CLASSIFICATION OF VULNERABILITY

- **Default password** – Now a days using default passwords is like inviting hackers know these defaults and can easily t in. Always change default passwords to strong, unique ones, preventing unauthorized access and protecting your data from potential breaches.

VULNERABILITY ASSESSMENT

- A vulnerability assessment is the part of scanning process. It is the process of discovering, identifying, and classifying the loopholes, weakness or backdoor in any device.

PENETRATION TESTING

- **Definition** – It is a process of hacking the system with the permission of owner of system, through which we can evaluate *security, attacks, exploits* and other components which is harming the system.

TYPES OF PENETRATION TESTING

- **Black Box –** It is also called as blind testing, which means the tester does not know any info about thee particular device

- **Gray Box –** In this, the tester have limited information about the device such as *ip address or any port no* .

- **White Box –** In this process of testing, the tester have whole information about the system such as *system password, ip , ports, operating system details* etc.

White Box Penetration Testing

White Box penetration testing is also known as open box penetration testing.

Complete knowledge of Code and Infrastructure.

Black Box Penetration Testing

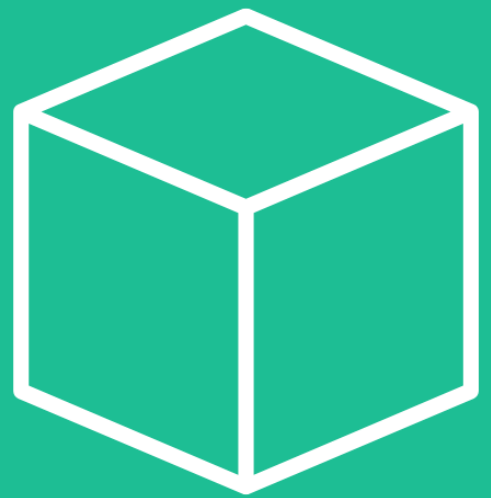
Black Box penetration testing is also known as close box penetration testing.

No knowledge of Codebase and Infrastructure.

Gray Box Penetration Testing

Gray Box penetration testing is a combination of Black Box and White box testing.

Some knowledge of Code and Infrastructure



astra

TYPES OF SCANNING IN VAPT

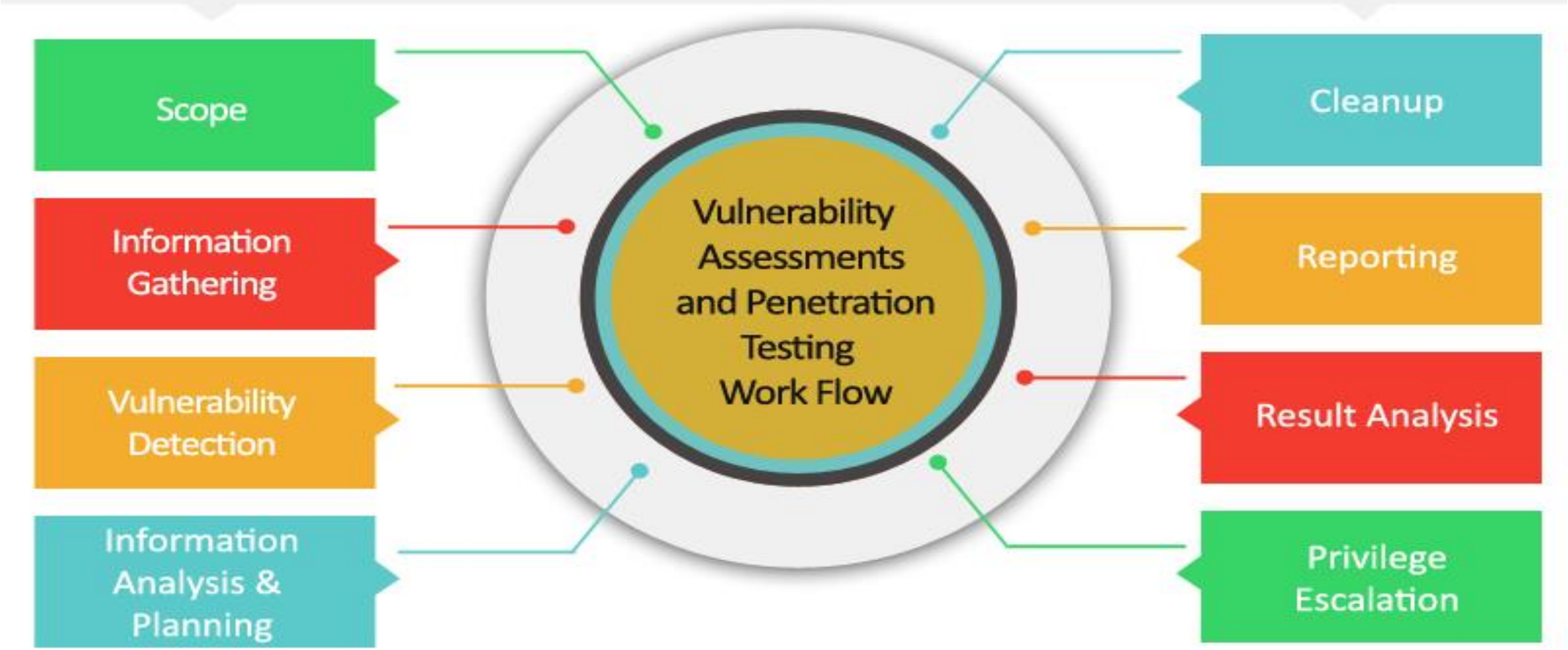
1. **Host Based – It** helps to identifies the issues in the host or the system and process is carried out by using host-based scanners which helps us to find the vulnerabilities. The host-based tools will load a mediator software onto the target system, which trace the event and report it to the security analyst.
2. **Network-Based** - This process is done by using Network-based Scanners which will detect the open ports, and identify the unknown services running on these ports. Then it will disclose possible vulnerabilities associated with these services.
3. **Database-Based** - It will identify the security exposure in the database systems using tools and techniques to prevent from SQL Injections (Injecting SQL statements into the database by the malicious users, which can take the root access of the system)

Category	Tool	Description
Host Based	STAT	Scan multiple systems in the network.
	Cain & Abel	Recover password by sniffing network, cracking HTTP password
	Metasploit	Open source platform for developing, testing and exploit code.
Network-Based	Cisco Secure Scanner	Diagnose and Repair Security Problems.
	Wireshark	Open Source Network Protocol Analyzer for Linux and Windows.
	Nmap	Free Open Source utility for security auditing.
	Nessus	Agentless auditing, Reporting and patch management integration.
Database-Based	SQL diet	Dictionary Attack tool door for SQL server.
	DB-Scan	Detection of Trojan of a database, detecting hidden Trojan by baseline scanning.

PHASES IN PENETRATION TESTING

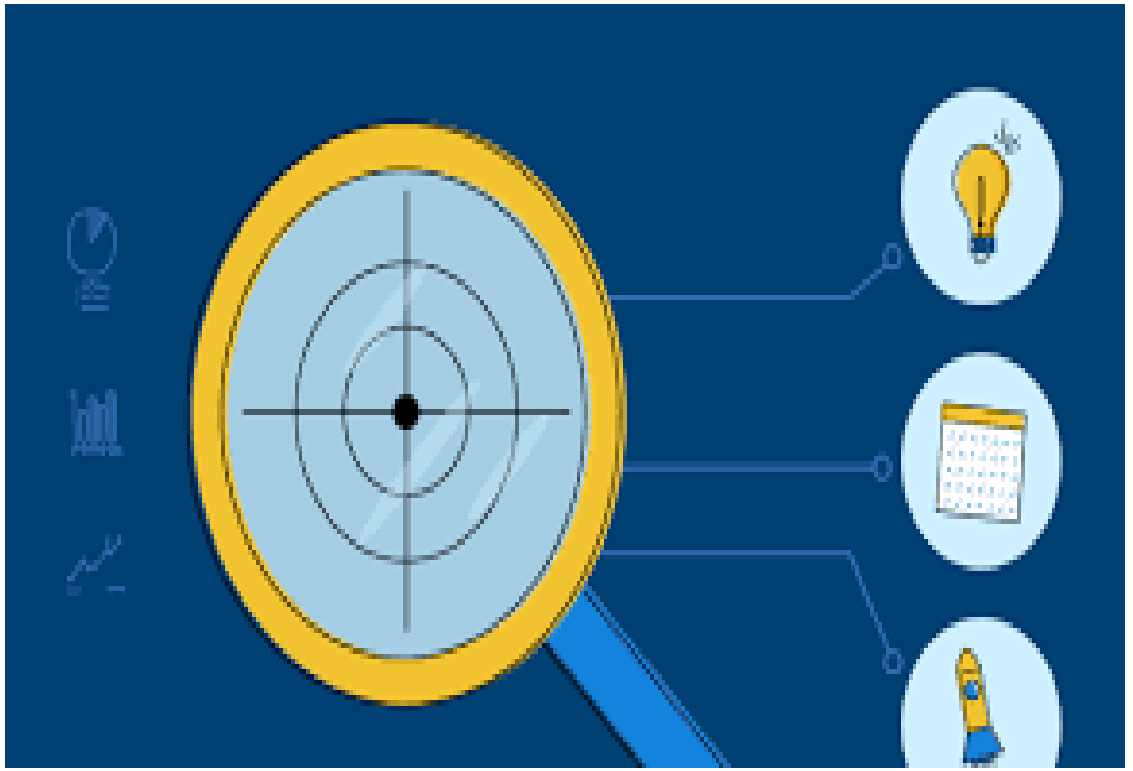
- **Pre Attack Phase** - It involves gathering information about a system, understanding its weak points, and preparing strategies for potential cyberattacks. This phase is groundwork for cybersecurity experts to anticipate and defend against threats effectively.
- **Attack Phase** – In this, hackers attempt to break into a system by exploiting its weaknesses. It's like a testing the system's defenses and revealing the vulnerabilities that need fixing.
- **Post Attack Phase** - This phase involves analyzing the results of the Pen Test, identifying vulnerabilities and weaknesses in the system or network, and providing recommendations for improving security.

WORKFLOW OF VULNERABILITY ASSESSMENT & PENETRATION TESTING.



SCOPE

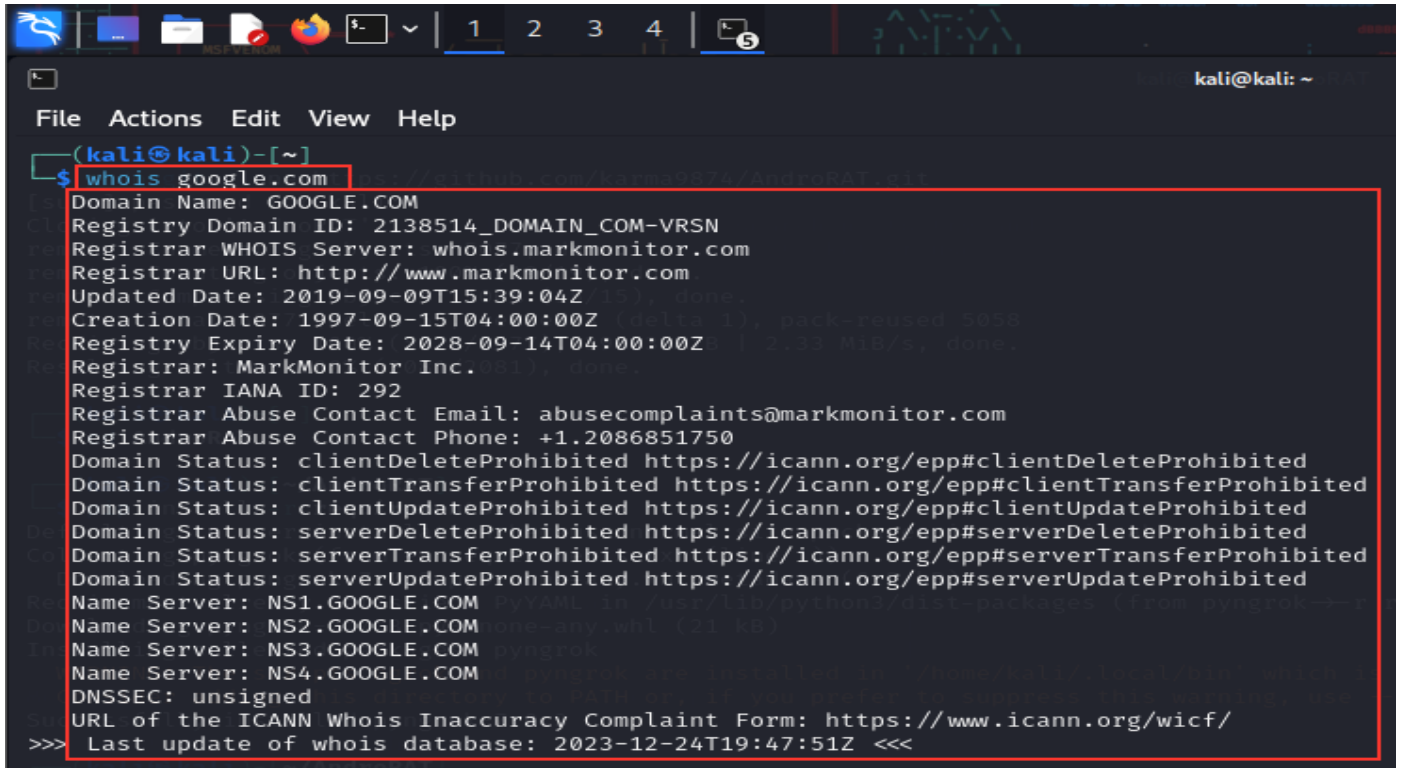
- VAPT is a crucial process for securing IoT devices and networks. It proactively identifies vulnerabilities in networks, devices, apps, and wireless protocols, simulates real-world attacks to assess risks, and ensures compliance with regulations. By addressing unique challenges of IoT security, VAPT plays a vital role in protecting devices, data, and entire IoT ecosystems from cyberattacks.



PROCESS OF VAPT IN DETAIL

- **Information Gathering** – It is the first step in VAPT, where we gather information about target device, network.

  Imp tools are – Nmap. Google dorks, whois, Shodan etc.



PROCESS OF VAPT IN DETAIL

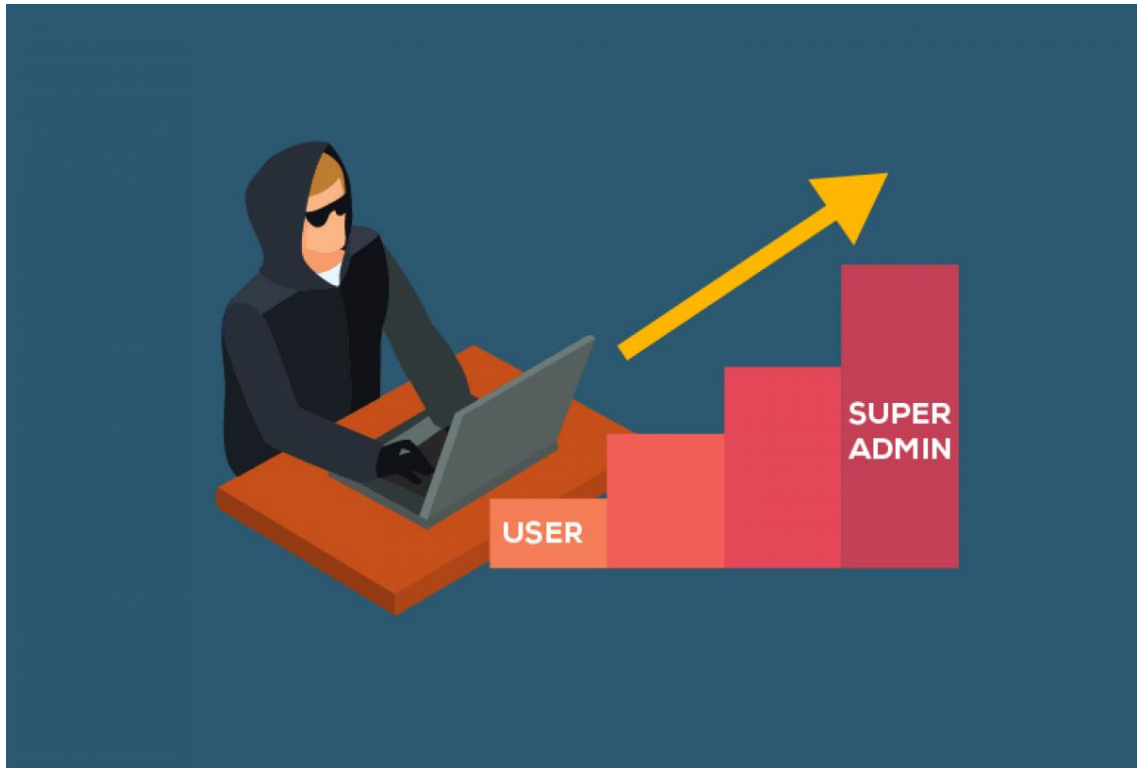
- **Vulnerability Detection** - It involves using tools and techniques to find weaknesses in a device or network. By identifying these vulnerabilities, cybersecurity experts can then address and fix them, enhancing the overall security and reducing the risk of potential cyberattacks.

PROCESS OF VAPT IN DETAIL

- **Information Analysis & Planning -** It involves understanding the target system, In this phase helps cyber security experts develop a strategy to address vulnerabilities systematically.

PROCESS OF VAPT IN DETAIL

- **Privilege Escalation** – It is cyber technique in which hackers gains unauthorized access to higher privilege of a device or network.



PROCESS OF VAPT IN DETAIL

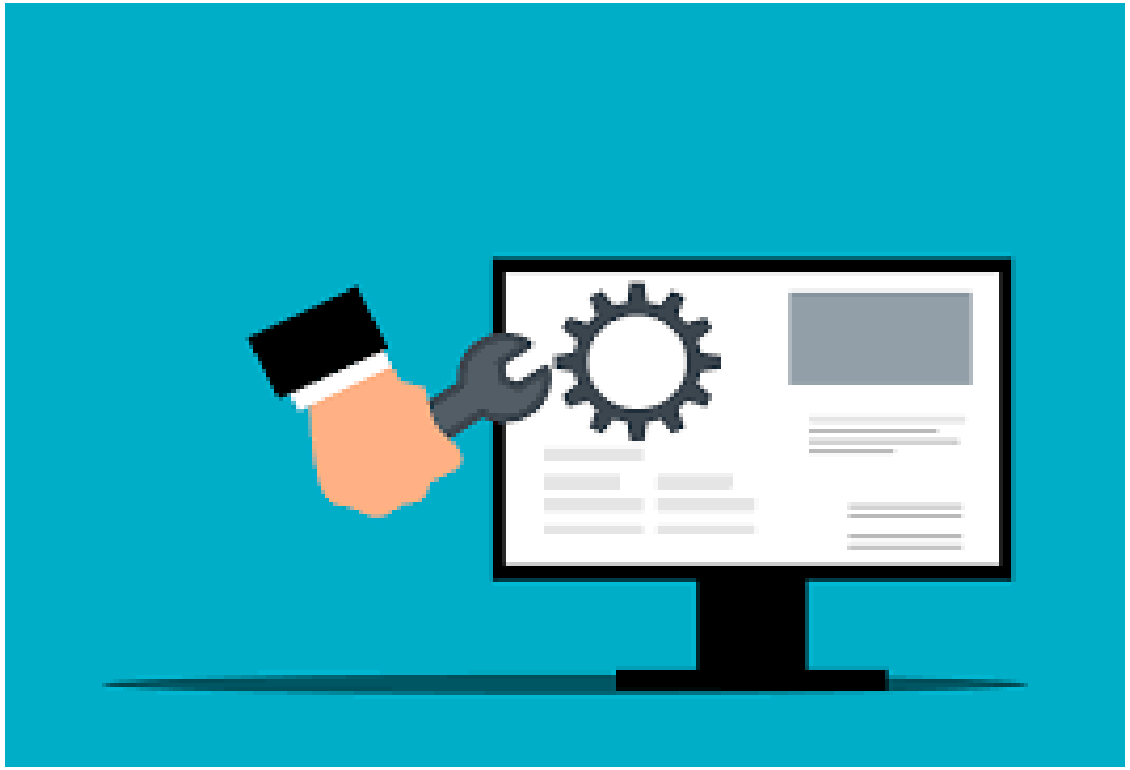
- **Result Analysis** – It is a review on security-relevant issues that either moderately or severely impact the security of the product or system which we got after scanning the device.

PROCESS OF VAPT IN DETAIL

- **Report -** This document include the vulnerabilities found, explains their potential impact, and provides solution for increasing the system security. It's a guide for improving digital defenses and reducing the risk of cyber threats.

PROCESS OF VAPT IN DETAIL

- **Cleanup** – It is a process in which, finding security weaknesses, cybersecurity experts work to patch and strengthen the system, making necessary changes to strengthen the system's defenses.



AUTOMATED VS. MANUAL APPROACH TO VULNERABILITY ASSESSMENT, PENETRATION TESTING (VAPT)

- **Automated VAPT** is like using a smart robot to find and test weaknesses in your computer systems. It quickly scans for potential security issues, like open doors, and even tries to see if they can be exploited. But it is important that robot might not catch all the vulnerabilities which a human expert can, and it's crucial to interpret its findings carefully to ensure a strong defense against cyber threats

- **Manual VAPT** is like having a skilled detective inspect your home for security gaps. A human expert carefully examines your computer systems, looking for vulnerabilities that automated tools might miss. This hands-on approach involves thinking like an attacker to uncover potential risks and provides a deeper understanding of the security.

FEW TOOLS FOR VULNERABILITY ASSESSMENT AND PENETRATION TESTING

- Metasploit.
- Nessus
- Burp Suite
- Wireshark
- Aircrack-ng
- Nmap
- Nikto
- SQL Map.

THANK YOU