Devise A Methodology To Conduct VAPT on IoT Devices and IoT Network

[1]Vipul Kumar, [2]Pritish Kshetre, [3]Naman Richhariya, [4]Naresh Kumawat, [5]Divya Kumar Patel
PG-DITISS CDAC, Bangalore.
Guide By: Dr. Sanjay Adiwal

Abstract

Complexity of systems is increasing day by day. This leads to more and more vulnerabilities in Systems. Attackers use these vulnerabilities to exploit the victim's system. It is better to find out these vulnerabilities in advance before the attacker finds them. Vulnerability Assessment and Penetration Testing can be used as a cyber-defence technology. Life cycle of Vulnerability Assessment and Penetration Testing on systems or networks

Penetration testing, also known as Pen testing is usually performed by a testing professional in order to detect security threats involved in a system. Penetration testing can also be viewed as a real-time cyber Security attack, done in order to see whether the system is secure and free of vulnerabilities. Penetration testing is widely used for testing both Network and Software, but somewhere it fails to make IoT more secure. In IoT the security risk is growing day-by-day, due to which the IoT networks need more penetration testers to test the security.

- **Key Words:** Vulnerability Assessment, Penetration testing, IoT devices, IoT networks.

● Introduction

VAPT (Vulnerability Assessment and Penetration Testing)

- With increasing world-wide connectivity of Information systems, and growth in accessibility of data resources, the threat to the Integrity and Confidentiality of Data and Services has also increased. Every now and then cases of Hacking and Exploitation are being observed.
- So in order to remain immune and minimize such threats, the Organizations conduct regular Vulnerability Assessment and Penetration Testing (VAPT) on their Technical Assets which will help the Organizations to assess their Application/Services and analyze their Security Posture. Apart from these it detects the SQL Injection vulnerabilities and reports all the Identified vulnerable links on the Target.
- Further the tool can also exploit the identified SQLI vulnerable links and grab confidential information from Target. With the growing interconnectivity of systems and advancement in Cyber Services, the level of Cyber Attacks has also increased. The major factors responsible for any malicious Act over the Internet includes Lack of Awareness and Inefficiency/Lack of Defensive Measures. Today the Organizations are required to be well aware of the possible threats and should keep auditing their services and other security measures periodically to ensure the safety of their valuable resources.

- ## Vulnerability:-

  -A vulnerability is any mistakes or weakness in the system security procedures, design, implementation or any internal control that may result in the violation of the system's security policy.

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

- ## Classification Of Vulnerability:-

1. **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.

2. **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.

3. **Design Flaws –** It refers to the design of software, hardware or any process in which any mistake is made by the developer of 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.

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

5. **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.

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

7. **Default password –** Nowadays using default passwords is like inviting hackers to 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:-

  Vulnerability Assessment is a process to evaluate the security risks in the software system in order to reduce the probability of a threat. It is also called Vulnerability Testing.

- ## Penetration Testing:-

  -It is a process of hacking the system with the permission of the owner of the system, through which we can evaluate security, attacks, exploits and other components which are harming the system.
  -Penetration testing investigates and abuses the system to determine whether a vulnerability exists.

- ## Types Of Penetration Testing:-

- White-Box Testing in VAPT:

  -In VAPT, white-box testing may involve a detailed examination of the internal code, architecture, and configurations of the target system.

-It helps identify vulnerabilities that can be discovered through a thorough analysis of the system's internal workings.

-White-box testing can be particularly useful for identifying vulnerabilities related to code flaws, misconfigurations, and other issues that require knowledge of the system's internals.

- Black-Box Testing in VAPT:

  -Black-box testing is a crucial aspect of VAPT, especially when the goal is to simulate real-world attack scenarios from an external perspective.

  -It involves testing the system without prior knowledge of its internal structure, focusing on assessing vulnerabilities that can be exploited without detailed information about the system's internals.

  -External penetration testing, web application testing, and network vulnerability assessments often fall under the black-box testing category in VAPT.

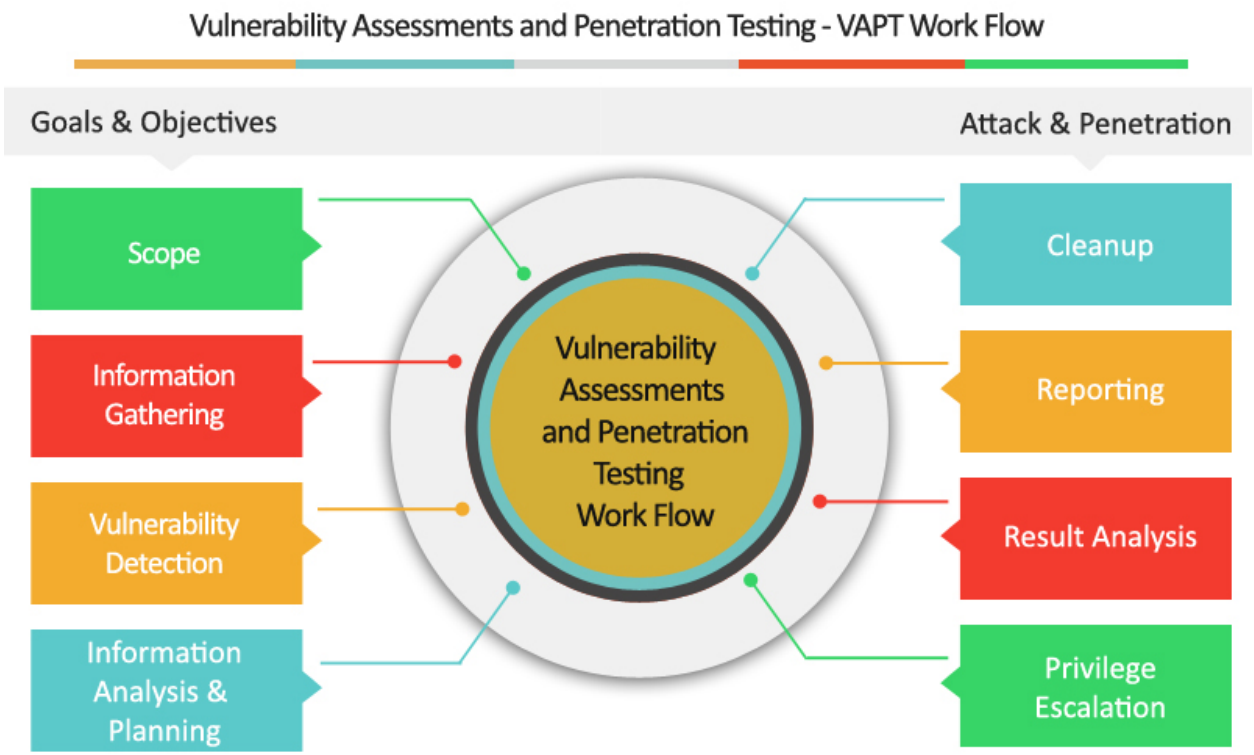
- Gray-Box Testing in VAPT:

  -Gray-box testing in VAPT involves a combination of both white-box and black-box testing elements.

  -Testers may have partial knowledge of the system's internals, allowing them to blend insights from both perspectives for a more comprehensive assessment.

  -This approach is often used when some information about the system is available, but not complete, and a more nuanced testing strategy is required.

- **Vulnerability Assessment and Penetration Testing Process**



- (Scope)Planning and Preparation:-
  - Scope Definition: Define the scope of the assessment, the systems, networks, and applications to be tested.
  - Rules of Engagement: Establish rules and guidelines for the testing process, including any limitations on testing activities.
  - Resource Identification: Identify the resources required for testing, such as tools, personnel, and documentation.
- Reconnaissance:
  - Information Gathering: Collect information about the target environment, including network infrastructure, IP addresses, domain names, and employee details.
  - Network Scanning: Perform scanning to discover live hosts, open ports, and services running on target systems.

- Vulnerability Analysis:
    - Vulnerability Scanning: Use automated tools to scan for known vulnerabilities in the target systems.
    - Manual Testing: Conduct manual testing to identify vulnerabilities that automated tools may miss.
    - Risk Assessment: Evaluate the identified vulnerabilities based on their potential impact and likelihood of exploitation.
- Information Analysis and Planning:
    - It will analyze the identified vulnerabilities, to devise a plan for penetrating into the network and systems.
- Exploitation:
    - Penetration Testing: Attempt to exploit the identified vulnerabilities to gain unauthorized access or privileges.
    - Privilege Escalation: If initial access is achieved, attempt to escalate privileges to simulate an attacker's progression.
- Post-Exploitation:
    - Persistence: Test the ability to maintain access to the target environment over an extended period.
    - Data Exfiltration: Simulate the extraction of sensitive data to assess the impact of a successful attack.
- Reporting:
    - Documentation: Document all findings, including vulnerabilities, exploited paths, and recommendations for remediation.
    - Risk Assessment: Provide a risk assessment that prioritizes vulnerabilities based on their severity and potential impact.
    - Executive Summary: Create an executive summary that communicates the overall security posture and recommendations to stakeholders.

- Remediation:
    - Mitigation Planning: Collaborate with the organization to develop a plan to address and immediately identify vulnerabilities.
    - Follow-up Testing: Conduct follow-up testing to ensure that remediation efforts have been effective.
- Verification:
    - Reassessment: Verify that the previously identified vulnerabilities have been successfully remediated.
    - Validation: Ensure that the implemented security measures do not introduce new vulnerabilities.
- Documentation and Closure:
    - Final Report: Provide a final report summarizing the entire VAPT process, including initial findings, remediation steps, and verification results.
    - Non-Disclosure Agreements (NDAs) are legally binding contracts that require the signer to keep information confidential. They are typically one-page documents that are electronically signed.
    - Closure Meeting: Conduct a meeting with relevant stakeholders to discuss the findings, remediation efforts, and any additional recommendations.

- **VAPT on IoT Devices and network**

- **Steps to Follow In General for Vulnerability Assessment:-**

1. Identify the assets and resources in your system.

   Create a comprehensive list of the elements your system relies on, such as data, software, and equipment. In vulnerability assessment, this step involves recognizing what requires safeguarding.

2. Assign the monetary and contextual value to the resources.

   Figure out how much each item on your list is worth in terms of money (monetary value) and how crucial it is for your system's operation (contextual value). This helps prioritize what needs more protection in vulnerability assessment.

3. Determine any security flaws or potential dangers to each resource.

   Identify any weaknesses or risks that could harm the things on your list. In vulnerability assessment, this involves finding potential entry points for attackers, software bugs, or any other issues that could compromise security.

4. Reduce or eliminate the most serious threats to important resources.

   -Take steps to make the important things on your list safer. In vulnerability assessment, this means addressing and fixing the identified weaknesses and risks to prevent them from being exploited by attackers.

   -A Vulnerability Assessment should be performed once a year or after making significant changes to your application.

- **VA vs PT :-**

Parameters	Vulnerability Assessment	Penetration Testing
Working	Discover Vulnerabilities	Identify and Exploit Vulnerabilities
Mechanism	Discovery & Scanning	Simulation
Focus	Breadth over Depth	Depth over Breadth
Coverage of Completeness	High	Low
Cost	Low- Moderate	High
Performed By	In-house Staff	An attacker or Pen Tester
Tester Knowledge	High	Low
How often to Run	After each equipment is loaded	Once in a year
Result	Provide Partial Details about Vulnerabilities	Provide Complete Details of Vulnerabilities

A VAPT tool performs a VA to identify areas of weakness and a PT to exploit those areas of weakness to get access. For instance, a VA might help identify weak encryption while the PA works to decipher it.

The VAPT tools do a vulnerability scan, provide a PA report, and sporadically execute code or payloads.

OWASP(Open Web Application Security Project)

OWASP TOP 10 INTERNET OF THINGS 2018

1 Weak, Guessable, or Hardcoded Passwords

Use of easily bruteforced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed systems.

2 Insecure Network Services

Unneeded or insecure network services running on the device itself, especially those exposed to the internet, that compromise the confidentiality, integrity/authenticity, or availability of information or allow unauthorized remote control...

3 Insecure Ecosystem Interfaces

Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering.

4 Lack of Secure Update Mechanism

Lack of ability to securely update the device. This includes lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changes due to updates.

5 Use of Insecure or Outdated Components

Use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms, and the use of third-party software or hardware components from a compromised supply chain.

6 Insufficient Privacy Protection

User's personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission.

7 Insecure Data Transfer and Storage

Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing.

8 Lack of Device Management

Lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring, and response capabilities.

9 Insecure Default Settings

Devices or systems shipped with insecure default settings or lack the ability to make the system more secure by restricting operators from modifying configurations.

10 Lack of Physical Hardening

Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device.

- ## Types of a vulnerability scanner:

1. **Host Based**

- Identifies the issues in the host or the system.
- The process is carried out by using host-based scanners and diagnosing the vulnerabilities.
- The host-based tools will load a mediator software onto the target system; it will trace the event and report it to the security analyst.

2. **Network-Based**

- It will detect the open port, and identify the unknown services running on these ports. Then it will disclose possible vulnerabilities associated with these services.
- This process is done by using Network-based Scanners.
-

3. **Database-Based**

- It will identify the security exposure in the database systems using tools and techniques to prevent SQL Injections. (SQL Injections: – Injecting SQL statements into the database by the malicious users, which can read the sensitive data from a database and can update the data in the Database.)

AUTOMATED VAPT vs MANUAL 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 robots 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.

● Advantages of VAPT on IoT :

1) **Hardware Security:**

   Physical Security: Protecting IoT devices from physical tampering, theft, or unauthorized access.

   Device Authentication: Implementing secure methods for device identification and authentication.

   Secure Boot: Ensuring that only authenticated and authorized firmware is loaded during the device boot process.

   Hardware Encryption: Employing encryption mechanisms at the hardware level to safeguard data in transit and at rest.

2) **Firmware Security:**

   Code Integrity: Verifying that the firmware code has not been altered or tampered with.

   Update Mechanisms: Implementing secure over-the-air (OTA) update processes for firmware.

   Authentication and Authorization: Ensuring that only authorized entities can modify or update firmware.

3) **Network Security**:

   Secure Communication Protocols: Implementing encryption protocols (such as TLS/SSL) to secure data transmitted between devices and backend systems.

   Firewall and Intrusion Detection Systems: Deploying protective measures to monitor and control network traffic.

   Device Isolation: Preventing unauthorized access by segmenting and isolating devices within the network.

4) **Application Security:**

   API Security: Ensuring that APIs used by IoT devices are secure and properly authenticated.

   Secure Coding Practices: Implementing coding practices that prevent common vulnerabilities such as injection attacks and buffer overflows.

   Access Controls: Implementing proper access controls to restrict unauthorized access to sensitive functionalities.

5) **Data Security:**

   Encryption: Implementing end-to-end encryption to protect data both in transit and at rest.

   Data Integrity: Ensuring the accuracy and reliability of data collected by IoT devices.

   Privacy Measures: Implementing measures to protect user privacy, including anonymization and pseudonymization of data.

- # Types of VAPT Assessments:

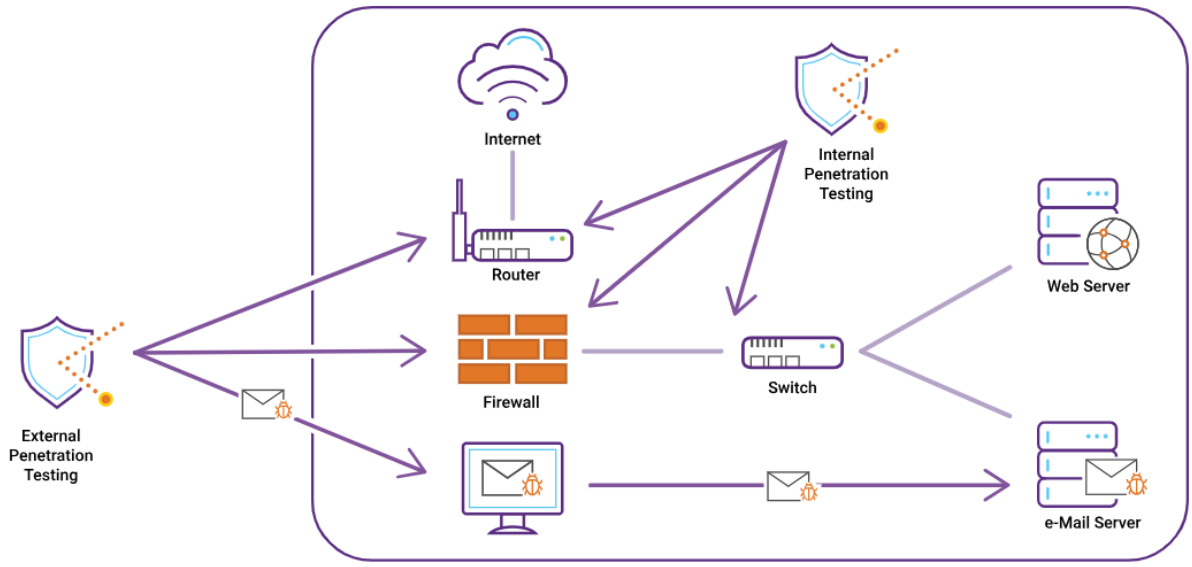
Vulnerability Assessment and Penetration Testing (VAPT), different types of assessments are conducted to identify and address security vulnerabilities in a system or network.

- **Vulnerability Assessment (VA):**
    - Purpose: Identifies and classifies security vulnerabilities in a system, network, or application.
    - Methodology: Automated tools are often used to scan the target environment for known vulnerabilities. This phase focuses on discovering weaknesses that could be exploited by attackers.
- **Penetration Testing (PT):**
    - Purpose: Simulates real-world attacks to exploit vulnerabilities and assess the effectiveness of security controls.
    - Methodology: Manual testing by ethical hackers (penetration testers) who attempt to exploit vulnerabilities to gain unauthorized access. This phase goes beyond automated scanning and involves a more hands-on approach.

- **Web Application Security Testing:**
    - Purpose: Focuses specifically on identifying vulnerabilities in web applications.
    - Methodology: Includes testing for common web application vulnerabilities such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and other security issues unique to web applications.
- **Network Security Assessment:**
    - Purpose: Evaluates the security of the network infrastructure, including routers, switches, firewalls, and other network devices.
    - Methodology: Involves scanning for open ports, assessing network architecture, and identifying potential weaknesses in network configurations.
- **Wireless Network Assessment:**
    - Purpose: Assesses the security of wireless networks to identify vulnerabilities and weaknesses.
    - Methodology: Involves scanning for open wireless networks, testing encryption protocols, and identifying potential security risks associated with wireless communication.

- **Mobile Application Security Testing:**
    - Purpose: Evaluates the security of mobile applications on various platforms.
    - Methodology: Similar to web application testing but focuses on vulnerabilities specific to mobile apps, such as insecure data storage, insufficient encryption, and insecure authentication mechanisms.
- **Social Engineering Assessment:**
    - Purpose: Assesses the effectiveness of security awareness training and policies by simulating social engineering attacks.
    - Methodology: Involves attempts to manipulate individuals within the organization through phishing emails, phone calls, or other methods to gather sensitive information.
- **Red Team vs. Blue Team Exercises:**
    - Purpose: Simulates a real-world attack scenario (Red Team) and assesses the defensive capabilities of the organization (Blue Team).
    - Methodology: Red Team actively tries to breach security, while the Blue Team defends and responds to the simulated attacks. The goal is to enhance incident response capabilities.

- **Types of Network VAPT:**



Internal VAPT:-

This only applies to the internal network. In terms of vulnerability screening, internal servers, firewalls, and data components such as database servers or file servers are crucial. Only vulnerability assessment is performed because the test is to be run from within the network; penetration testing is not. Internal security audits can be conducted either physically within the network premises or remotely within the network.

External VAPT:-

This type monitors the internet for the external perimeter. Because the testing is done from outside the premises, thorough penetration testing is probably certainly performed after the vulnerability assessment. The former use vulnerability scanning to detect security flaws or vulnerabilities, whilst the latter attempts to exploit those holes.

- **Vulnerabilities Assessment & Penetration Testing Tools**

Category	Tool	Description
Host Based	STAT	Scan multiple systems in the network.
	TARA	Tiger Analytical Research Assistant.
	Cain & Abel	Recover password by sniffing the network, cracking HTTP password.
	Metasploit	Open source platform for developing, testing and exploiting 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.
	Burp Suite	Burp Proxy allows penetration testers to conduct man-in-the-middle (MitM) attacks between a web server and a browser.

Database-Based	SQL diet	Dictionary Attack tool for SQL server.
	Secure Auditor	Enable users to perform enumeration, scanning, auditing, and penetration testing and forensic on OS.
	DB-scan	Detection of Trojan of a database, detecting hidden Trojan by baseline scanning.
Application Based	IoT Inspector	Automated testing tool for identifying common IoT vulnerabilities.
	ChipWhisperer	Analyzes firmware and hardware vulnerabilities using side-channel attacks.
	Bus Pirate	Versatile tool for interacting with embedded systems through various protocols.