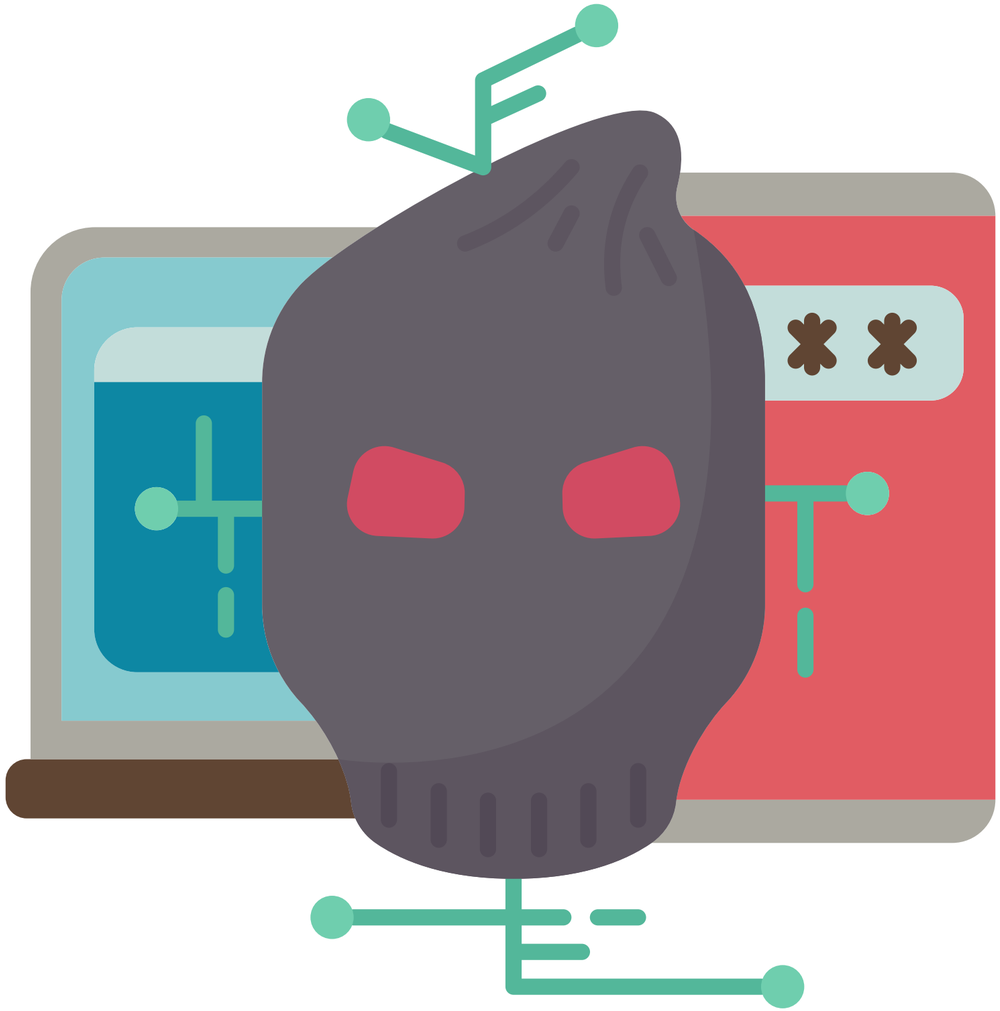
HOW TO DO VULNERABILITY ASSESSMENT STEP-BY-STEP

MOS

A Practical Guide to Vulnerability Assessment

WHAT IS VAPT



VAPT is a security testing process that identifies vulnerabilities in a system and determines whether they can be exploited.

Two Components:

- Vulnerability Assessment (VA): Focuses on identifying known vulnerabilities.
- Penetration Testing (PT): Simulates an actual attack to exploit identified vulnerabilities.

Purpose: To improve the security posture of systems by identifying and fixing security flaws.

TYPES OF VULNERABILITIES

Type	What It Means	Examples
System/OS	Flaws in the operating system.	Unpatched Windows, outdated Linux kernel
Application	Weaknesses in app code.	SQL Injection, Cross-Site Scripting (XSS)
Network	Issues in network setup or services.	Open ports, weak firewall rules
Configuration	Improper security settings.	Default admin password, exposed directory
Authentication	Login/session-related flaws.	Weak passwords, session ID reuse
Business Logic	Misuse of app flow or rules.	Unlimited coupon use, refund abuse
Third-party/Dependency	Vulnerable external components.	Log4j, outdated plugins

VULNERABILITY ASSESSMENT – OVERVIEW

The process of identifying, classifying, and prioritizing security vulnerabilities.

Objective: To detect and highlight potential vulnerabilities before attackers can find and use them.

Common Tools

Nessus – Popular for deep scanning

OpenVAS – Open-source vulnerability scanner

Qualys – Cloud-based scanning

Nexpose – Real-time vulnerability management

PENETRATION TESTING – OVERVIEW

Simulated cyber-attack on a system to evaluate its security.

Goal: To ethically exploit vulnerabilities and assess how far an attacker could go, revealing real-world security risks.

Common Types

- **Black Box:** No prior knowledge of the system; simulates an external attacker.
- **White Box:** Full knowledge of internal architecture, credentials, and code.
- **Gray Box:** Limited information, like an insider or an attacker with some access.

WHY IS VULNERABILITY ASSESSMENT IMPORTANT?

Prevent Breaches

Fix weaknesses before attackers exploit them.

Stay Compliant

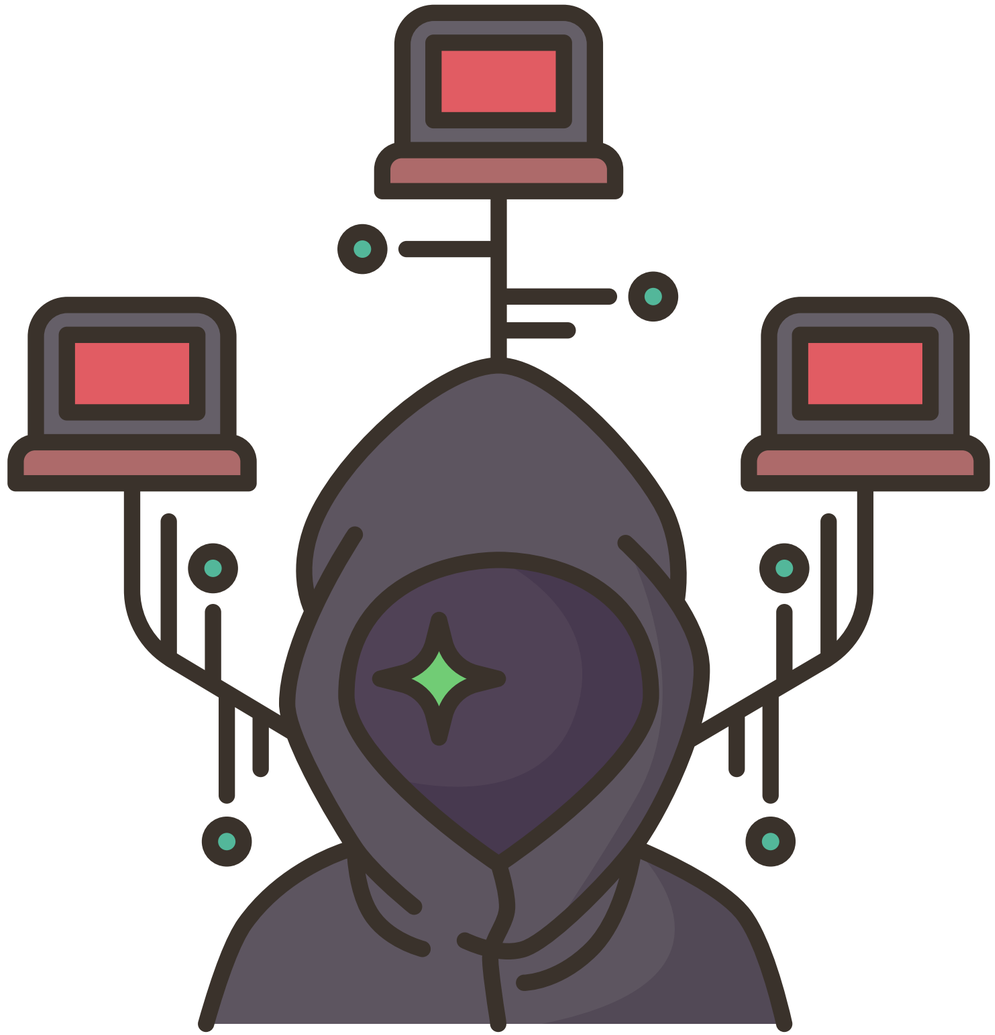
Meet standards like ISO 27001, PCI DSS, HIPAA.

Find Hidden Risks

Detect misconfigurations and outdated systems.

Build Trust

Show customers & stakeholders you prioritize security.



VULNERABILITY ASSESSMENT PROCESS

STEP 1 – DEFINE THE SCOPE

Objective: Understand what you're assessing.

What to Do:

- Identify the assets you want to assess – servers, websites, applications, cloud services, internal networks, etc.
- Decide on scope boundaries: Which systems are in scope and which are out of scope?
- Get permissions: Always take written approval before scanning or testing. Unauthorized scanning can disrupt services or violate policies.
- Clarify goals: Are you doing this for compliance, security hardening, or both?

- **Scanning 10 internal IPs and a public web app**
- **No testing on production database**

STEP 2 – INFORMATION GATHERING

Objective: Learn about the systems before testing.

What to Do:

- Use passive methods: WHOIS lookup, Shodan, Google Dorking, Netcraft
- Use active methods: Nmap or Masscan to detect open ports, running services, and OS info
- Identify:
  - Software versions
  - Open ports & services (e.g., SSH, FTP, HTTP)
  - Technologies used (e.g., Apache, WordPress, Linux)

Why It Matters:

The more you know about the target, the more accurate your scan will be.

Nmap, Netdiscover, WhatWeb, BuiltWith

STEP 3 – VULNERABILITY SCANNING

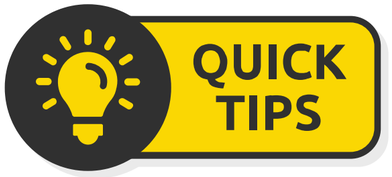
Objective: Use tools to find known weaknesses.

What to Do:

- Run an automated scan using tools like Nessus, OpenVAS, or Qualys
- Perform both:
  - Unauthenticated Scans: Scan like an outsider
  - Authenticated Scans: Scan with credentials for deeper inspection
- Choose scan profiles based on the asset type (e.g., web app scan vs internal server scan)

What You'll Find:

- Missing patches
- Misconfigurations (e.g., open FTP)
- Known CVEs (Common Vulnerabilities & Exposures)



Scans can slow down systems, schedule them wisely!

STEP 4 – VULNERABILITY ANALYSIS

Objective: Understand what the results mean and how serious they are.

What to Do:

- Review scan results: Separate true positives from false positives
- Assign risk levels: Use CVSS (Common Vulnerability Scoring System) or the tool's severity score
  - Critical (9–10)
  - High (7–8.9)
  - Medium (4–6.9)
  - Low (0–3.9)
- Prioritize based on impact: What's easier to exploit or causes the most damage?

Think Like an Attacker:
Could this vulnerability allow access to sensitive data or full system control?

A public-facing login page vulnerable to SQL injection = High Risk

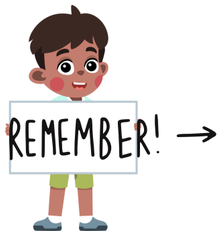
STEP 5 – REPORTING

Objective: Present the findings in a clear, actionable format.

What to Include:

- Executive Summary: A high-level overview for non-technical stakeholders
- Technical Details: Description of each vulnerability, severity, and how it was found
- Screenshots/Proof of Concept (PoC): Where applicable
- Remediation Steps: Clear instructions for fixing each issue
- Risk Ratings: Based on CVSS, tool-based score, or business impact

Use tables, graphs, and color codes to improve readability.



The report is the bridge between discovery and action.

STEP 6 – REMEDIATION SUPPORT

Objective: Help fix the issues found.

<u>What to Do</u>:

- Share the report with relevant teams (IT, DevOps, App Owners)
- Assist with:
  - Patch application
  - Secure configuration guides
  - Code changes (for application vulnerabilities)
- Provide alternate controls if immediate fixes are not possible (e.g., WAF rules)
- Offer timelines based on risk levels (e.g., Critical issues in 7 days)

TIPS

Assign clear ownership for each vulnerability

Some teams may not understand the urgency, make it simple!

STEP 7 – RE-ASSESSMENT

Objective: Make sure everything is actually fixed.

What to Do:

- Re-scan the systems after fixes are applied
- Verify each vulnerability: Has it been patched, blocked, or mitigated?
- Update the report: Mark issues as “Remediated” or “Partially Fixed”
- Close the loop: Confirm with stakeholders and sign off on the assessment

Why It Matters:

No vulnerability assessment is complete without verifying that fixes worked.

Always verify fixes through re-scans or manual validation.

COMMON TOOLS FOR VULNERABILITY ASSESSMENT

Category	Tools
Open Source Tools	OpenVAS, Nikto, Nmap
Commercial Tools	Nessus, Qualys, Burp Suite Pro, Acunetix
Cloud/Container Tools	Prisma Cloud, AWS Inspector

BEST PRACTICES

01 Conduct regular scans (mothly/quarterly)

02 Use authenticated scans

03 Prioritize vulnerabilities via CVSS & business impact

04 Combine with PT for better accuracy

05 Maintain a vulnerability management program

CONCLUSION

- Vulnerability Assessment is not just a scan, it's a security strategy.
- It helps organizations proactively identify, prioritize, and fix weaknesses before attackers can exploit them.

Key Takeaways:

- Regular assessments reduce the risk of breaches and downtime.
- It supports compliance, builds trust, and strengthens your security posture.
- A good assessment combines tools, analysis, and collaboration.
- Always follow through with remediation and re-assessment for lasting impact.

THANK YOU

Authored by : KHUSHI MALHOTRA

WWW.MINISTRYOFSECURITY.CO