Literature Survey Report on VAPT (Vulnerability Assessment and Penetration Testing)

Introduction

VAPT stands for Vulnerability Assessment and Penetration Testing. In simple words, it's like a health check-up for your computers, networks, websites, or apps to find weak spots (vulnerabilities) before bad guys (hackers) can use them to break in.

- **Vulnerability Assessment (VA)**: This is the "scanning" part. Tools automatically check for known weaknesses, like outdated software or mis-configurations. It gives a list of problems but doesn't try to break in.
- **Penetration Testing (PT)**: This is the "hacking" part (done ethically). Testers act like real attackers to exploit the weaknesses found in VA, showing how much damage could happen.

The idea of penetration testing started in the 1960s-1970s when governments and big companies began testing their systems against attacks. In the 1990s, as the internet grew, companies like Netscape launched the first **bug bounty programs** in 1995 – paying ethical hackers to find bugs in their browsers. This evolved into modern bug bounties.

Bug bounty programs became popular in the 2010s with platforms like **HackerOne** (launched 2012) and **Bugcrowd** (2013). Companies like Google, Facebook, Microsoft, and even the U.S. Department of Defense ("Hack the Pentagon" in 2016) started them. Open Bug Bounty (2014) is a free, non-profit platform for anyone to report web vulnerabilities responsibly.

Today, VAPT is a key part of cybersecurity. It's required for compliance like PCI-DSS, ISO 27001, GDPR, and helps prevent data breaches. Literature shows VAPT as a "proactive defense" – find and fix issues before attacks happen.

Cyber Attack Life Cycles

To understand why VAPT is needed, we look at how real cyber attacks happen. There are models that break attacks into steps (like a "kill chain" – a term from military).

1. **Lockheed Martin Cyber Kill Chain (2011)**:

   The classic model with 7 phases:

   - Reconnaissance: Hacker researches the target (e.g., Google employees, check LinkedIn).
   - Weaponization: Build a malicious tool (e.g., phishing email with malware).
   - Delivery: Send it (email, USB, website drive-by).
   - Exploitation: Trigger the vulnerability.
   - Installation: Install backdoor for persistent access.
   - Command & Control (C2): Hacker controls the system remotely.
   - Actions on Objectives: Steal data, ransom, destroy.

   VAPT helps break this chain early – VA finds weaknesses in reconnaissance/exploitation, PT simulates delivery to installation.

2. **MITRE ATT&CK Framework (2013 onward)**:

   More detailed and modern. It's a big matrix of real-world attacker tactics (why they do it) and techniques (how).

   - Tactics (14+ for enterprise): Recon, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command & Control, Exfiltration, Impact.
   - Based on real attacks (e.g., from APT groups like Russian or Chinese hackers).
   - Better than Kill Chain because attacks aren't always linear – insiders skip steps, or attacks are "living off the land" (using normal tools).

3. **Comparison of Models**:

    - Kill Chain: Linear, good for traditional malware attacks. Weak for insider threats or quick web attacks.
    - MITRE ATT&CK: Non-linear, post-compromise focus, used for red teaming and detection.
    - Other models: Mandiant Attack Lifecycle (adds loops for internal movement), Unified Kill Chain (combines both).

VAPT aligns with these: Testers follow similar phases to simulate attacks and recommend defenses at each stage.

VAPT Methodologies

There are standard ways to do VAPT properly:

- **PTES (Penetration Testing Execution Standard)**: 7 phases – Pre-engagement, Intelligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post-Exploitation, Reporting.
- **OSSTMM (Open Source Security Testing Methodology Manual)**: Scientific, covers physical/human/wireless too. Focuses on operational security.
- **NIST SP 800-115**: Government guide – Planning, Discovery, Attack, Reporting.
- **OWASP Testing Guide**: Best for web apps, detailed checks for top risks.
- **Others**: ISSAF, PCI-DSS guidelines.

Most VAPT follows a mix: Start with rules of engagement, scan (tools like Nessus, OpenVAS), manual exploit (Metasploit, Burp Suite), report with fixes.

Literature (papers from ResearchGate, IEEE) shows combining automated VA + manual PT is best. AI is emerging for faster testing.

Existing Bug Reports and Real-World Vulnerabilities (from Bug Bounty Platforms)

Bug bounty programs give real data on what vulnerabilities exist today.

- **HackerOne (2024/2025 Report)**:
  - Over 580,000 valid vulnerabilities reported total.
  - $81 million bounties paid in the last year (13% increase).
  - Top issues shifting from simple XSS to systemic ones: Insecure Direct Object References (IDOR) up 29%, Improper Access Control up 18%.
  - AI vulnerabilities exploding: Prompt injection up 540%.
  - Critical bugs common in finance, crypto, tech.
- **Bugcrowd**: Runs programs for Tesla, Twilio, etc. Focus on crowdsourced, continuous testing. Many reports on APIs, mobile apps.
- **Open Bug Bounty**: Free platform, over 488,000 fixed vulnerabilities (as of recent data), mostly XSS on websites. 862,000+ disclosures coordinated.

Common trends (2024-2025):

- CVE numbers exploding: Over 29,000 in 2024, 21,500+ in first half 2025.
- OWASP Top 10 evolving (2025 draft/release): Broken Access Control still #1, Injection #5, new entries like Software Supply Chain Failures (e.g., Log4Shell style), AI-specific risks.
- Most exploited: Misconfigurations, outdated components, IDOR, API bugs.

Real reports show web apps have lots of XSS, SQLi, but high-impact are RCE (remote code execution), privilege escalation.

Current Trends and Future

- Shift to continuous VAPT (not yearly) via bug bounties or PTaaS (Penetration Testing as a Service).
- AI in VAPT: Tools for faster scanning, but also new bugs in AI systems.
- Supply chain attacks rising (e.g., third-party libraries).

- Bug bounties vs Traditional PT: Bounties find more unique/rare bugs over time, cheaper long-term; PT is structured, better for compliance.

Literature concludes: Manual PT + crowdsourced bounties = best defense. Organizations using both avoid more breaches.

Conclusion

VAPT is essential in today's world where attacks follow clear life cycles like Kill Chain or ATT&CK. Starting from early bug bounties (Netscape 1995) to platforms like HackerOne/Open Bug Bounty, we've seen millions of real bugs fixed. Common issues are access control flaws, injections, and now AI/supply chain risks.

In simple words: Do regular VAPT, combine scanning with ethical hacking (or bounties), and fix fast. This turns defense from reactive to proactive. As per 2025 data, companies ignoring this pay millions in breaches – better to pay ethical hackers a little!