Vulnerability Assessments and Penetration Tests to Secure IT Infrastructure

Mohammed Mustafa Khan

Abstract

Secure systems start with the foundational IT infrastructure, including hardware, software, networking, data centers and cloud services. It is a tremendous aspect to conduct vulnerability assessments and penetration tests (VAPT) to ensure the IT infrastructure meets the security standards. VAPT secures IT infrastructure by keeping the CIA triad in check. CIA triad stands for confidentiality, Integrity, and Availability. The purpose of the CIA triad is to ensure data security by providing a framework that discovers weak points and addresses solutions to strengthen policies and programs used by institutions. Confidentiality refers to the concept of preventing data from unauthorized access; integrity means data must not be modified in case of unauthorized access; and availability refers to the aspect of ensuring data is available at any time to legitimate users. Vulnerability assessments aim to search for potential flaws or weak points inherent in an organization's IT infrastructure, whereas penetration testing discovers the weaknesses or flaws and then attempts to exploit them. This paper discusses the different processes and methodologies of vulnerability assessment and penetration tests and their synergy in securing IT infrastructure.

Keywords: Vulnerability assessment, penetration testing, IT infrastructure, flaws

1.0 Introduction

Today's digital economy has forced organizations to rely completely on complex IT infrastructure to support their workflow operations. This digital transformation has led to exponential growth in cyber threats, and attackers have become relentless in launching threats that exploit flaws and weak points in IT systems. It is critical to efficiently and effectively protect and shield IT infrastructure against different threats and attack vectors. IT infrastructure has become part and parcel of the organizational indispensable asset since it enables the organization to accomplish its strategic vision. IT and security professionals are under high pressure to ensure the security of IT infrastructure is enhanced by conducting vulnerability assessments and penetration testing (VAPT), which stood out as two of the most critical approaches. VAPT serves as an essential tool in identifying and remediating potential threats to IT infrastructure. Vulnerability assessment involves the use of different automated tools and manual testing approaches to identify the security posture of the target system [12]. Extensive scans are performed to identify the loopholes, flaws, and breach points of a system. The discovered loopholes, flaws or breach points can be exploited by an attacker to cause data breach incidents or fraudulent intrusion actions. Penetration testing proceeds by the tester acts as an attacker and simulates malicious activities to exploit vulnerabilities discovered during vulnerability assessment [1]. This process of VAPT aids the IT and security teams in determining the efficacy of the security measures that are inherent in a system, application or network. This paper will discuss the entire process involved in securing IT infrastructure using the VAPT approach. Additionally, the paper will cover ethical and legal issues during VAPT.

2.0 Literature Review

2.1 Overview of Vulnerability Assessments

Vulnerability assessment has been recognized as the premier foundational element in cybersecurity practices. According to Vellani. (2019), vulnerability assessment provides a step-by-step technique for discovering and validating security loopholes in IT systems. These assessments are crucial in maintaining a proactive security posture, thus enabling organizations to stay ahead of the attackers by addressing vulnerabilities inherent in a system prior to exploitation.

Additionally, in a study performed by Humayun et al. (2020), the importance of vulnerability assessments in critical infrastructure is highlighted. The authors discuss the need for regular assessments in sectors like finance, healthcare, and government, where the potential impact of security breaches is high. The study found that organizations that regularly carried out vulnerability assessments were better prepared to shield against cyber threats.

2.2 Penetration Testing in Modern Cybersecurity

Over the past years, penetration testing has become a game changer in helping organizations identify and prioritize security risks. The study conducted by Mahamood et al. (2023) on penetration testing described penetration testing as a prescient approach of security measure that extends to the identification of vulnerability and simulates real attacks on IT infrastructure. This approach offers extensive awareness of how vulnerabilities can be exploited by attackers. The review also highlights the different types of penetration testing, such as black-box, white-box, and gray-box testing, each offering unique advantages depending on the security goals of the organization.

In addition, a study by Basu et al. (2018) expounds on the challenges hobbled by penetration testing in cloud environments. The author points out that traditional penetration testing techniques often fall short when applied to cloud infrastructures due to their dynamic and distributed nature. The study calls for the development of specialized tools and methodologies to address these challenges, emphasizing the need for continuous adaptation of penetration testing practices to keep pace with evolving technologies.

2.3 Ethical Considerations in VAPT

Vulnerability Assessments and Penetration Testing (VAPT) are powerful tools in cybersecurity. However, their implementation raises ethical concerns. One of the primary ethical issues revolves around the concept of "ethical hacking," where IT and security professionals simulate cyberattacks to identify vulnerabilities. According to a study by Mohan & D. (2022), ethical hacking involves a delicate balance between securing systems and respecting privacy. The authors highlight that while the intention is to enhance security, the process often involves accessing sensitive data, raising concerns about the potential misuse of information and the ethical boundaries of such practices.

3.0 Vulnerability Assessment (Vulnerability Analysis)

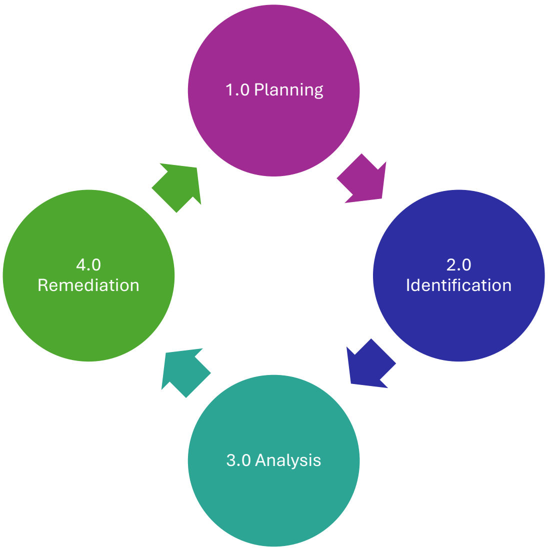
Vulnerability refers to gaps or weaknesses in a security program whereby attackers can unleash threats to exploit by gaining unauthorized access to assets like IT infrastructure. Step-by-step review of security loopholes in an information system. It involves scanning the IT system, applications or networks to locate security flaws and weaknesses [1]. It aids businesses to evaluate if the systems are prone to any known vulnerabilities and also determines the security posture of IT infrastructure. IT infrastructure providing any type of computing services may have vulnerabilities; hence, the purpose of vulnerability assessment is to establish a structured process for identifying vulnerabilities in an IT infrastructure, classifying assets and resources, assigning levels of severity, and developing a mitigation strategy. There are different types of vulnerability assessments that can be used by cybersecurity professionals, including;

- Application assessments review vulnerabilities within the web applications used by organizations [7].
- Host assessments to determine vulnerabilities of critical servers and computers that can cripple operations if not properly tested to ascertain security level.
- Network and wireless assessment needs to review policies and practices that are deployed to prevent unauthorized access and also identify rogue networking devices connected to the corporate network [7].
- Database assessments are used to discover any misconfigurations, unprotected data, and wrong SQL codes and classify sensitive data within the IT infrastructure.

It is crucial for organizations to perform all these types of vulnerability assessments regularly to discover potential vulnerabilities that can impede their IT infrastructure [7]. Fighting with ever-evolving threats needs time, the right tools and expertise. Additionally, cybersecurity professionals need to adapt their practices and policies appropriately to countermeasure the emerging threats.

4.0 Steps for Conducting Vulnerability Assessment

It consists of several steps, including planning, identification, analysis, and remediation.



4.1 Planning

Proper planning helps cybersecurity professionals to get the most out of the entire process [8]. Even though the organization performed the vulnerability assessment of IT infrastructure in the past, it is a crucial factor to plan. The purpose of planning is to determine the following:

- Discover where sensitive data resides.
- Disclose hidden data sources.
- Determine servers that run mission-critical applications.
- Discover which systems and networks to explore.
- Check all IP addresses, ports, and processes, and review for any misconfigurations.
- Locate the entire IT infrastructure, including hardware, software, networks, data centers, and cloud services and identify the communication protocols in use.

4.2 Identification

Perform a vulnerability scan of the IT infrastructure and create a vulnerability assessment checklist of the existing security threats. Vulnerability scanning can be automated or manual [8]. It is crucial to combine automation and manual approach to validate outcomes and minimize false positives.

4.3 Analysis

Successful analysis depends on the superiority of the scanning tools selected to carry out vulnerability assessment. Powerful scanning tools will give a detailed report containing various risk ratings and vulnerability scores [8]. Scanning tools use a CVSS framework that stands for a common vulnerability scoring system to map a numerical score. Proper analysis of these scores will provide insight into which vulnerabilities must be dealt with first. Some factors like urgency, severity, risk, and potential damage will act as a roadmap when prioritizing the scores.

4.4 Remediation

The remediation step proceeds after identifying and analyzing the vulnerabilities. This step involves the procedures and methodologies that will be used to fix the vulnerabilities and prevent exploitation by attackers [8]. Remediation can be accomplished through developing software patches and installation of security tools like SIEM. When conducting remediation, it is crucial to engage with the stakeholders since they are decision-makers. Sometimes, cybersecurity professionals lack a proper fix to the identified vulnerability, but mitigation aids them in minimizing the attack. For instance, cybersecurity personnel can deploy antivirus software to neutralize the malware in a network.

4.6 Vulnerability Assessment (VA) Tools

There are dozens of tools available in the market that are used to conduct vulnerability assessments. Some are open source, while others are licensed. The selection of these tools relies on the organizational budget and the type of IT infrastructure existing in an organization. As a cybersecurity professional, it is essential to familiarize with different tools to gauge their performance [7].

5.0 Table showing Different VA tools

Tool	Functionality
SolarWinds for Network Configuration	SolarWinds provides a powerful network configuration manager that excels in identifying network errors and misconfigurations, which are often overlooked by other tools [7].
Intruder for Cloud-Based Systems	Intruder is a premium tool tailored for cloud storage system security [7]. It offers continuous monitoring and automated scanning to detect vulnerabilities swiftly.
Nikto2 for Web Application Scanning	Open-source solution designed to scan web applications for vulnerabilities [7]. It effectively alerts users to potential security threats within web servers.
Nexpose for Emerging Threats	An open-source tool that offers comprehensive scanning for web apps, devices, and networks. It stays current with daily updates on new vulnerabilities from its active community, making it a reliable option for vulnerability detection [7].

6.0 Penetration Test (Pen Test)

Refers to a security test that launches simulated attacks to identify vulnerabilities in a system, application or network. The purpose of a pen test is to provide a report of information to the IT infrastructure management [1]. The content of the report may cover how penetration testers hacked the critical IT infrastructure and successfully exploited the underlying vulnerabilities. IT administrators responsible for IT infrastructure use the report and give further recommendations besides the suggestions provided by penetration testers. Penetration testers can be hired to carry out pen tests. Pen testers need to exercise their ethical hacking skills without compromising the IT infrastructure later on. The role of penetration testing is to ensure the desired security level of the organizational IT infrastructure is achieved.

7.0 Types of Penetration Tests

There are two main types of penetration testing: physical and virtual. The physical type involves testing tangible systems like routers, servers, data centers, security barriers, switches, computers, CCTV systems, and security guards, to mention a few. The penetration tester may decide to deliberately access these assets physically to determine any gap that exists in accessing these systems [9]. Are the systems easily accessible without any restrictions. If they manage to access the assets, then they can plug in their rogue devices to manipulate the target system. It is a requirement not to allow any unauthorized person to access the data centers, infrastructure and equipment. Proper policies and rules must be established to ensure the security of physical assets. Additionally, it is crucial to ensure the building that hosts IT infrastructure, such as data centers that host core network infrastructure, is proofed. The humidity and cooling of data centers must be properly maintained to avoid anomalies that impact the operation of IT assets.

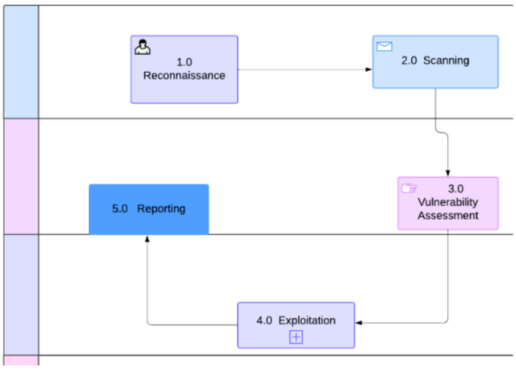
The virtual pen test involves evaluating intangible assets, such as operating systems, web applications, firewalls, databases, and other intangible assets contained in an organization [10]. The OWASP top 10 attacks utilize these virtual assets. Securing virtual assets is more challenging than securing physical assets. A number of advanced technical solutions have been adopted to secure virtual assets. Cybersecurity professionals need to be cognizant of these solutions and implement them appropriately. It is important to note that the classification of penetration testing can vary, so this is one way of categorizing pen tests.

8.0 Pen Test Methodologies

Testing Technique	Description
Black Box Testing	The tester has no prior knowledge of the internal design or structure of the system being tested. The focus is on identifying missing functionalities and interface errors. This approach simulates an external attack, where the tester, like a real attacker, has no information about the network [9].
White Box Testing	Involves full transparency, where the tester has complete access to the internal workings of the system. Testers collaborate with developers, utilizing provided details like paths, credentials, procedures, addresses, and protocols to thoroughly examine the system [9].
Gray Box Testing	This is a middle-ground approach where the tester has partial knowledge of the system's internal structure. Some information is given, but testers must gather additional data on their own before proceeding with the test [9].

In addition to the three pen test methodologies, the pen test can be carried out in two ways: external penetration techniques and internal penetration techniques. External means that the penetration tester is outside the organization settings, whereas internal techniques involve the pen tester being hooked inside the organization environment [10].

9.0 Phases of Penetration Testing



9.1 Reconnaissance

This is the initial stage of conducting a penetration test. The tester collects as much information about the target system as possible. The information may include the network architecture, user accounts, operating system in use, location of the data center and any relevant information that is of use [11]. Gathering information enables the tester to devise the attack strategy they can launch on the target IT infrastructure.

9.2 Scanning

The collected data is scrutinized and analyzed to discover gaps like open ports and the network traffic of the system under inspection. The open ports act as the gateway through which testers can easily gain access to the internal network resources, so many ports are scanned using advanced technical tools [11]. Testers access the network and conduct extensible scans to discover network devices, user accounts, firewall rules, access control and many more. This information will help the testers to perform penetration tests.

9.3 Vulnerability Assessment

The tester utilizes all the obtained in the reconnaissance and scanning phase to discover possible vulnerabilities and determine if they can be exploited. Testers utilize a wide range of resources to evaluate the risks of identified vulnerabilities. One of the resources is the National Vulnerability database, which contains analyzed software vulnerabilities that exist in the Common Vulnerabilities and Exposures database [11].

9.4 Exploitation

Once after discovering the vulnerabilities, exploitation proceeds. The tester tries to access the target system and capitalize on the vulnerabilities discovered using special tools like Metasploit to mock the attacks. This phase is sometimes fragile, so testes need to be cautious of not damaging the computing resources of the target system because the impossible can happen, such as the system may crash [11].

9.5 Reporting

The tester has to document all the outcomes of the process. The report generated can be used to remediate the vulnerabilities discovered in the system and optimize the organization's security posture [11]. The report should cover all the vulnerabilities identified, threats that were launched to exploit the vulnerabilities, recommendations, and declarations by the testing team not to exploit these vulnerabilities.

Basic Pseudocode for Penetration Testing

```
BEGIN PenetrationTest

  // Step 1: Define Scope and Objectives
  DEFINE scope, objectives, and rules of engagement
  OBTAIN necessary authorizations and permissions

  // Step 2: Information Gathering (Reconnaissance)
  TARGET = Identify target systems and networks
  COLLECT information on target systems (e.g., IP addresses, domains, services)
  ENUMERATE open ports and services on target systems

  // Step 3: Vulnerability Assessment
  FOR each target system IN TARGET:
    IDENTIFY vulnerabilities using automated tools (e.g., scanners)
```

```
        ANALYZE identified vulnerabilities for potential exploitation
    END FOR

    // Step 4: Exploitation
    FOR each identified vulnerability:
        IF vulnerability is exploitable:
            EXECUTE exploitation attempts to gain unauthorized access
            DOCUMENT the exploitation process and any access gained
        ELSE
            RECORD that the vulnerability is not exploitable
        END IF
    END FOR

    // Step 5: Post-Exploitation
    IF access was gained:
        ENUMERATE and DOCUMENT sensitive data, system configurations, and further access paths
        ATTEMPT privilege escalation to gain higher-level access
    END IF

    // Step 6: Reporting
    COMPILE findings, vulnerabilities, and exploitation results into a report
    PROVIDE remediation recommendations for each identified vulnerability

    // Step 7: Cleanup
    REMOVE any files, tools, or access methods used during the test
    ENSURE no lasting impact on target systems

END PenetrationTest
```

10.0 Penetration Testing Tools

Tool	Key Features	Platforms
Nmap	Security scanning, network discovery, port scanning, OS detection, free tool with GUI & command line interfaces [1].	All operating systems.
Nessus	Vulnerability scanning, TCP/IP scanning, and PCI DSS audit preparation were initially free but are now paid [1].	Mac OS, Windows, FreeBSD, Linux.
Metasploit Framework	Open-source penetration testing, modular attack libraries, and command prompt access for system control [1].	UNIX, Windows.
Wireshark	Network analysis, TCP stream viewing, supports various protocols and media types, and open-source [11].	Windows, Linux, macOS.

11.0 Synergy Vulnerability Assessment and Penetration Testing

Vulnerability assessments and penetration tests are complementary processes. When integrated, it provides a window of opportunities to shape an organization's security posture. While vulnerability assessments identify and prioritize potential weaknesses, penetration tests determine the impact of these vulnerabilities when exploited. Together, they enable organizations to develop a more effective and targeted approach to cybersecurity [10].

12.0 Ethical and Legal Issues

VAPT augments the process of hacking into the network. However, the disparity that exists is that VAPT is performed legally. VAPT involve ethical and legal challenges, including ensuring informed consent, protecting privacy, and minimizing potential harm during testing. Legally, testers must have proper authorization, comply with data protection laws, and sail through liability issues, especially when handling sensitive data or intellectual property. Ethical concerns also include managing conflicts of interest and responsibly disclosing vulnerabilities. These issues demonstrate the importance of adhering to strict guidelines and maintaining transparency to avoid legal repercussions and ethical breaches during VAPT.

13.0 Conclusion

Vulnerability assessments and penetration testing are essential components of an effective cybersecurity strategy. These processes provide organizations with the cues needed to identify and mitigate security risks, ensuring the protection of critical IT infrastructure. Organizations can stay ahead of emerging threats and maintain a powerful security posture by incorporating these practices into a continuous security strategy.

14.0 Reference:

1. P. Lachkov, L. Tawalbeh, and S. Bhatt, "Vulnerability Assessment for Applications Security Through Penetration Simulation and Testing | River Publishers Journals & Magazine | IEEE Xplore," *ieeexplore.ieee.org*, Oct. 2022. https://ieeexplore.ieee.org/abstract/document/10251051
2. K. H. Vellani, *Strategic Security Management*, 2nd Edition. CRC Press, Sep. 2019, p. (pp. 71-86). Available: https://www.taylorfrancis.com/chapters/edit/10.4324/9780429506611-5/vulnerability-assessments-karim-vellani
3. M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb, and S. Mahmood, "Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study," *Arabian Journal for Science and Engineering*, vol. 45, no. 1, Jan. 2020, doi: https://doi.org/10.1007/s13369-019-04319-2.
4. A. K. Mahamood, M. Malik, A. B. Ruhani, and M. F. Zolkipli, "Cybersecurity Strengthening through Penetration Testing: Emerging Trends and Challenges," *Borneo International Journal eISSN 2636-9826*, vol. 6, no. 1, pp. 44–52, Mar. 2023, Available: http://majmuah.com/journal/index.php/bij/article/view/341
5. S. Basu *et al.*, "Cloud computing security challenges solutions-A survey," *IEEE Xplore*, Jan. 01, 2018. https://ieeexplore.ieee.org/abstract/document/8301700
6. A. Mohan and D. G. A. Swaminathan, "Analysis of Vulnerabilityassessment with Penetration Testing," *papers.ssrn.com*, Feb. 22, 2022. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4040684
7. S. Chamberlain, "How Does Vulnerability Analysis Work?," *Cybersecurity Exchange*, Sep. 06, 2022. https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/conduct-a-vulnerability-analysis/
8. S. Bocetta, "4 steps to conducting a proper vulnerability assessment," *Candid Blog*, Nov. 20, 2020. https://blog.candid.org/post/4-steps-to-conducting-a-proper-vulnerability-assessment/
9. ISACA, "Physical Penetration Testing: The Most Overlooked Aspect of Security," *ISACA*, Sep. 05, 2023. https://www.isaca.org/resources/white-papers/2023/physical-penetration-testing
10. I. Yaqoob, S. Hussain, S. Mamoon, N. Naseer, J. Akram, and A. Ur Rehman, "Penetration Testing and Vulnerability Assessment," *Journal of Network Communications and Emerging Technologies (JNCET) www.jncet.org*, vol. 7, no. 8, Aug. 2019, Available: https://www.jncet.org/Manuscripts/Volume-7/Issue-8/Vol-7-issue-8-M-03.pdf
11. EC-Council, "Understanding the Five Phases of the Penetration Testing Process," *Cybersecurity Exchange*, Mar. 28, 2022. https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/penetration-testing-phases/#:~:text=The%20Five%20Phases%20of%20Penetration

12. Vegesna, Vinod Varma, "Utilizing VAPT Technologies (Vulnerability Assessment & Penetration Testing) as a Method for Actively Preventing Cyberattacks," *Ssrn.com*, Oct. 25, 2023. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4612524