Leveraging Vulnerability Assessment And Penetrattion Testing (Vapt) As An Internal Control Tool

Introduction

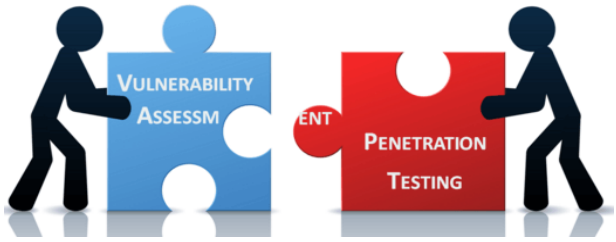
Vulnerability Assessment and Penetration Testing (VAPT) is a security testing method used by organizations to test their applications and IT networks.

A Vulnerability Assessment (VA) examines, discovers, and discloses known vulnerabilities by generating a report that details the vulnerability's categorization and priority whereas Penetration Test (PT) seeks to exploit vulnerabilities to identify the level of entrance. It assesses the level of defense. The VA is similar to approaching a door, assessing it, and examining its potential flaws. The VA is usually automated, but a PT is generally done by a security expert.

Purpose

Vulnerabilities exist in all levels of a computing system- both on premises and cloud regardless of the organization's size. There's a big misconception that small and medium-sized businesses are spared by cyber attackers. As the security of small businesses is usually relaxed, attackers incline towards them. Many times, organizations say they don't require vulnerability risk assessments because they are such a small organization. But this false belief could prove very costly for a business whether big or small.

It is important to monitor the organization's cyber security frequently as hackers' tools, strategies, and processes for breaching networks are constantly improving.



VAPT assists in the security of your organization by offering insight into security flaws as well as advice on how to remedy them. For organizations wishing to comply with standards such as the ISO 27001; control objective A12.6 (Technical Vulnerability Management) states that 'information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk', VAPT is becoming increasingly crucial.

The security loopholes in your IT infrastructure are:

1. Poor hardware and software design
2. Complex software and hardware
3. Poor authentication system
4. Misconfigured systems
5. Unsecured network
6. Vulnerable endpoints

Benefits of performing VAPT

1. It will provide you with a thorough assessment of your application.
2. It will assist you in identifying security flaws or faults that might lead to catastrophic cyber-attacks.
3. VAPT provides a more complete picture of the dangers posed to your network or application.
4. It assists businesses in defending their data and systems from harmful assaults.
5. Compliance standards necessitate the use of VAPT.
6. Defends your company against data loss and unwanted access.
7. It will assist you in safeguarding your data from both external and internal dangers.

Effects of Data Breach

A data breach can have a tangible impact on your company. It can cost you money in the form of legal fees and fines, your customers in terms of loss of trust, reduced sales and loss of reputation.
When people use your product or service, they want to know they can trust you with their personal information and that you will keep it safe. And if a company is breached, then that trust is broken. This is the reason why security is a top priority for any company.

Vulnerability Assessment and Penetration Testing tools

There are a number of vulnerability assessment and penetration tools that are available in the market. The key issue is to ensure that a needs assessment is done to ensure that the tool procured addresses your specific needs.

Vulnerability Assessment and Penetration Testing audit

A VAPT audit is designed to test the overall security of a system by performing an in-depth security analysis of its various elements. It is about the verification and assessment of the security posture of your organization.

The goal of a VAPT audit is to identify the overall vulnerabilities present in the software, which hackers can exploit. VAPT security audit is carried out through a

systematic process involving various tools, techniques, and methodologies.

In addition, VAPT testing also enables data security compliance for storing customer data in networks and applications and protecting it against any compromise attempt by hackers.