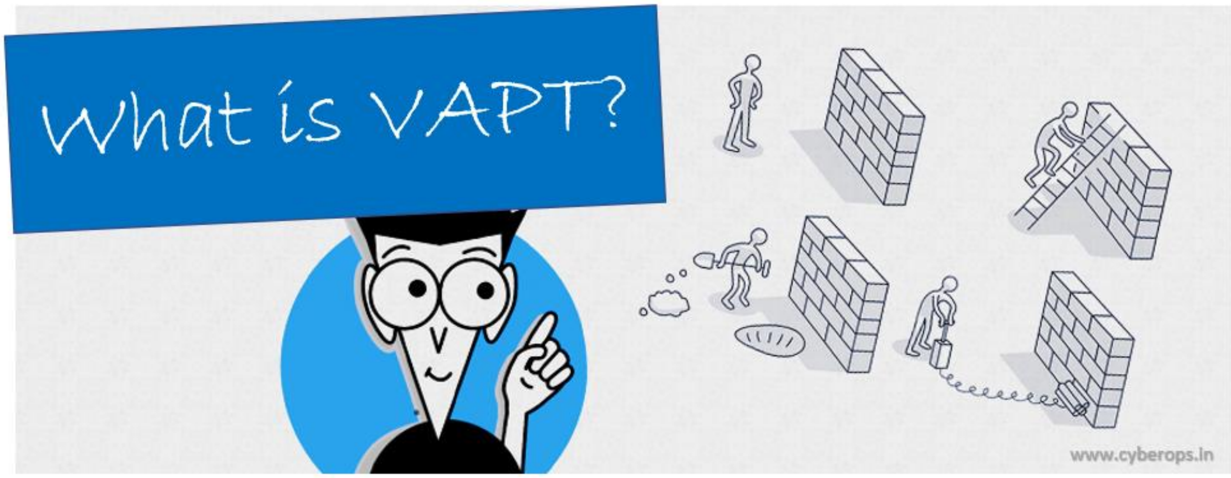
What is VAPT and Why would your Organization need it?



Purpose

The purpose of the document is to highlight the basic concepts of vulnerability assessment, the reader should have some basic technical knowledge in the field of information technology in order to understand the content of the article, however, this document does not go deep into deep technical knowledge.

What is it?

In computer security, the term "vulnerability" is used to denote a system flaw that allows an attacker to disrupt the integrity of the system. Vulnerabilities can be the result of weak passwords, software errors, incorrect software settings, a computer virus, or another type of malicious script injection or SQL injection.

Security risk is classified as a vulnerability if it is recognized that as a result of its presence an attack can be made. Security risk, combined with one or more well-known examples of workable and fully completed attacks, is classified as an exploit. Constructs in programming languages that are difficult to use correctly can be a major source of vulnerabilities.

Vulnerabilities existed at all times, but when the Internet was at an early stage of development, they were not used and exploited so often. The media did not report news about hackers who were sent to jail for hacking servers and stealing valuable information. At that time, all nodes on the network were trusted, secure protocols (SSH, SCP, SSL) did not exist yet, however, telnet, FTP and plain text HTTP were used to transfer important data. Then no one even thought about sniffing (passive listening on the network) and ARP spoofing (an attack technique that allows you to intercept traffic between hosts).

A vulnerability assessment can be performed on many objects, not just computer systems / networks. For example, physical buildings may be evaluated, the results of which will make it clear which parts of the building are flawed. If a burglar can bypass the guard at the front door and get inside the building through the back door - this is definitely a vulnerability. If he actually does this - this is an exploit. Physical security is one of the most important aspects that you need to attach importance to. If the attacker gets physical access to the server - the server is no longer yours! Because if a server is stolen, an attacker does not need to bypass IDS (intrusion detection system), does not need to bypass IPS (intrusion prevention system), does not need to think about the way in which you can transfer 10 TB of data - they are already here on the server . Full disk encryption may help, but usually it is not used on servers. Make sure that all your laptops have FDE (Full Disk Encryption, Full Disk Encryption), also known as WDE (Whole Disk Encryption, full disk encryption).

Statements like "your systems/networks" are vulnerable - they do not provide any valuable information. A vulnerability assessment without a comprehensive report is no good. With the use of automatic tools for scanning networks, you can create utility reports and distribute them, but all this is not of great value since a report can easily consist of thousands of pages. It is much better to get the “top 10” vulnerabilities from all the existing ones and create a report based on them.

Penetration Testing vs. Vulnerability Assessment

It is known that in the security industry there is a certain amount of confusion about the differences between penetration testing and vulnerability assessment, they are often classified as one and the same, although in reality this is not so. Penetration testing sounds more exciting, but most people actually need a vulnerability assessment, not penetration testing; Many projects are marked as penetration tests, although in fact they are a 100% vulnerability assessment. Penetration testing, as a rule, includes an assessment of vulnerability, but this is only one of the additional steps of such tests. Penetration testing is a method of assessing the security of a computer system or network by simulating an attacker's attack. This process includes an active analysis of the system for any deficiencies, technical flaws or vulnerabilities. This analysis is carried out from the perspective of a potential intruder, and will include the active exploitation of security vulnerabilities. Any security issues found will be presented to the system owner along with an assessment of their seriousness and often with a risk reduction plan or technical solution. Vulnerability assessment is what most companies usually do, as the systems they test are in an active production process and their work cannot be disrupted by active exploits that can disable the system. Vulnerability assessment is the process of identifying and qualifying system vulnerabilities. The system being studied may be physical equipment, such as a nuclear power plant, a computer system or a larger system (for example, communication system infrastructure or district water infrastructure). Vulnerability assessment contains many things in conjunction with risk assessment. Assessment usually contains the following steps:

1. Cataloging capabilities and system performance (resources)

2. Quantifying the value and importance of resources
3. Identification of vulnerabilities or potential threats for each resource
4. Reducing or eliminating most serious vulnerabilities for most valuable resources

Who conducts VAPT?

Someone may say that the best candidate will be a security officer of the organization who knows the system from the inside, its strengths and weaknesses, but not everything is so simple. If a penetration test is carried out by a specialist with a minimum level of knowledge about the constructed protection system, he is more likely to find so-called “blind spots” missed by developers when building and organizing protection levels. It is for this reason that third-party contractors specializing in this field are usually ordered for VAPT.

This role is also suitable for hackers, "ethical" hackers (also referred to as white hat). These guys have a lot of experience, which is used in good intentions, with the aim of improving security.

There is no better candidate to find, since everything is done individually, it all depends on the strategy and the type of pentest that representatives of the organization wish to fulfill.

What does VAPT include?

- Network penetration test:

1. detection of network and system level vulnerabilities;
2. identification of incorrect configurations and settings;
3. identify the vulnerability of the wireless network;
4. fraudulent services;
5. lack of strong passwords and the presence of weak protocols.

- Application penetration test:

1. identification of application level deficiencies;
2. fake requests;
3. the use of malicious scripts;
4. violation of session management;
5. etc.

- Physical penetration test:

1. breaking physical barriers;
2. checking and breaking locks;
3. malfunctions and sensor bypass;
4. disabling CCTV cameras;
5. etc.

- Device Penetration Testing (IoT):

1. detection of hardware and software deficiencies of devices;
2. brute force weak passwords;
3. identifying insecure protocols, APIs, and communication channels;
4. configuration violation and more.

What are the types of pentest (penetration tests)?

- Pentest "white box" - in this penetration test, the pentesters will be provided with some information about the implemented security structure of the organization. Also, this method can be implemented in conjunction with the organization's IT team and the penetration testing team;
- Pentest "black box" (or "blind test") - in this case, simulates the actions of a real attacker, because the specialist or team does not provide any relevant information, except the name and basic data for a general understanding of the company;
- Hidden pentest (also known as "double-blind") - in this situation, only a small part of the organization's staff (1-2 people), including IT specialists and security specialists who will respond to attacks do not have information about the existing verification. For this type of test, it is very important for the pentesters or team to have the appropriate document in order to avoid problems with law enforcement agencies in the event of a proper response from the security service;
- External Pentest is an attack by an "ethical" hacker, which is carried out against external servers or devices of the organization, such as their website and network servers. The goal is to determine if an attacker can penetrate the system remotely and how far if he can;
- Internal Pentest - an imitation of an attack is carried out by an authorized user with standard access rights, which allows you to determine how much damage an employee who has some personal accounts with respect to the management can do.

What are the stages of VAPT?

---

1. Collecting information - searching for information about the organization and employees in open sources, social networks, forums and blogs;
2. Search technical base - identification of existing resources, applications and hardware for the enterprise;
3. Analysis of vulnerabilities and threats - detection of vulnerabilities in security systems and applications using a set of tools and utilities, both commercial and directly developed in the company of pentesters;
4. Operation and data processing - imitation of a real cyber-attack to obtain information about any vulnerabilities with further analysis;

5. Formation of the report - design and presentation of the findings made pentest with suggestions for improving the existing security system.

Why is pentest needed?

Penetration testing shows a real picture of the existing security threat and identifies an organization’s vulnerabilities to manual attacks. Pentesting on a regular basis will allow defining technical resources, infrastructure, physical and personnel arsenal containing weak aspects that require development and improvement.

It is for the same reason that you go to the doctor for an annual health check, it makes some sense to contact highly qualified security consultants to conduct safety testing. Of course, it can be said that you are absolutely healthy; nevertheless, a specialist can conduct tests to detect hazards of which you may not even know.

Ultimately, penetration testing is an element necessary to ensure the security of your organization.