VAPT

In these days of widespread Internet usage, security is of prime importance. The almost universal use of mobile and Web applications makes systems vulnerable to cyber attacks. Vulnerability assessment can help identify the loopholes in a system while penetration testing is a proof-of-concept approach to actually explore and exploit a vulnerability.

Cyber attacks are increasing every day with the increased use of mobile and Web applications. Globally, statistics show that more than 70 per cent of the applications either have vulnerabilities which could potentially be exploited by a hacker, or worse, they have already been exploited. The data losses due to this are typically of two types. Either the data is confidential to the organisation or it is private to an individual. Regardless of the category, data losses result in the loss of money or reputation. This article explores a technical process that can be adopted by industries and organisations to protect their intellectual property, and if implemented correctly, will result in better risk management.

For those who are new to Vulnerability Assessment and Penetration Testing (VAPT), this is a technical assessment process to find security bugs in a software program or a computer network. The network may be a LAN or WAN, while the software program can be a .exe running on a server or desktop, a Web/cloud application or a mobile application. Before we get into the technical aspects of VAPT, let’s look at a few of its benefits.

- Helps identify programming errors that can lead to cyber attacks
- Provides a methodical approach to risk management
- Secures IT networks from internal and external attacks
- Secures applications from business logic flaws
- Increased ROI on IT security
- Protects the organisation from loss of reputation and money

Why are systems vulnerable?

There are primarily two main reasons for systems being vulnerable—misconfiguration and incorrect programming practices. In the case of networks, devices such as routers, switches and servers, as well as firewalls and IPS systems are either misconfigured or, in some cases, not configured at all, thus running default settings. As an example, almost all firewalls have a default built-in user account with the name,‘admin’. Typically, the password for it is also set to ‘admin,’ by default, or something even easier to guess. Looking at the example of servers, installing a database server leaves us with an ‘sa’ account, which has a blank password.

As for programming errors, a user input taken from a Web application form may be directly sent to a backend database server without parsing it. This can lead to a parameter manipulation attack or SQL injection attack. Another example of programming errors would be a Web service accepting requests without performing adequate authentication, thus leaking data inadvertently. This shows us that it is human error that leads to vulnerable systems, which could be exploited easily by attackers, to compromise data confidentiality, integrity and availability.

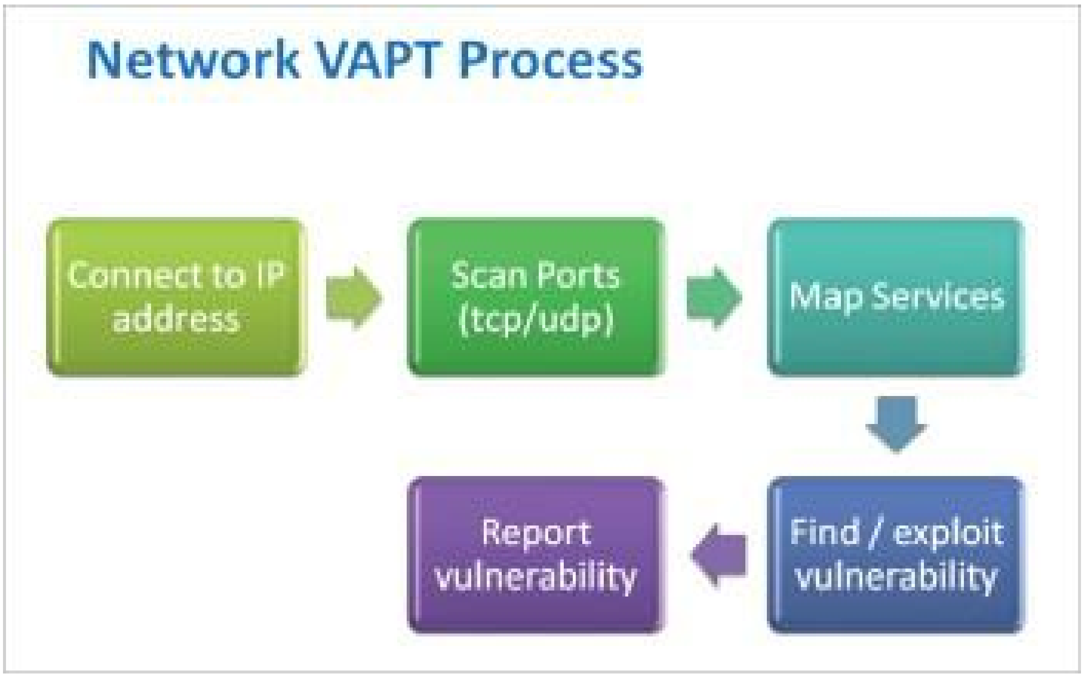

Figure-1: Network VAPT Process

What is vulnerability assessment?

Vulnerability assessment (VA) is a systematic technical approach to find the security loopholes in a network or software system. VA is entirely a process of searching and finding, with the objective that none of the loopholes are missed. It primarily adopts a scanning approach which is done both manually and performed by certain tools. The outcome of a VA process is a report showing all vulnerabilities, which are categorised based on their severity. This report is further used for the next step, which is penetration testing (PT). VA is usually a non-intrusive process and can be carried out without jeopardising the IT infrastructure or application's operations.

What is penetration testing?

A penetration test (PT) is a proof-of-concept approach to actually explore and exploit vulnerabilities. This process confirms whether the vulnerability really exists and further proves that exploiting it can result in damage to the application or network. The PT process is mostly intrusive and can actually cause damage to the systems; hence, a lot of precautions need to be taken before planning such a test. The outcome of a PT is, typically, evidence in the form of a screenshot or log, which substantiates the finding and can be a useful aid towards remediation. As a summary, shown below are the steps involved in the VAPT process.

- Scanning the network or application
- Searching for security flaws
- Exploiting the security flaws
- Preparing the final report of the test

Differences between VA and PT

VA and PT differ from each other in two aspects. The VA process gives a horizontal map into the security position of the network and the application, while the PT process does a vertical deep dive into the findings. In other words, the VA process shows how big a vulnerability is, while the PT shows how bad it is. There is one more subtle difference. Due to the nature of work involved in each process, a VA can be carried out using automated tools, while a PT, in almost all cases, is a manual process. This is because PT essentially simulates what real hackers would do to your network or application. Figures 1 and 2 shows the VAPT process for network and Web applications, respectively.

VAPT tools

While there are multiple tools available in the market, those listed below are well-known for their usability. Although these tools are mentioned as VAPT tools, most of them essentially provide VA only and leave the PT part to the ethical hackers to be done manually. There are a couple of tools, though, which are powerful PT tools, and are mentioned as such in the list below.

- Nmap
- Acunetix
- Nessus
- OpenVAS
- Nexpose
- BurpSuite (PT)
- Metasploit (PT)

There are two important terms that an ethical hacker must know, especially while using these tools. These are: false positive and false negative.

A false positive is when a vulnerability actually does not exist, but it gets reported. A false negative is when a vulnerability actually exists but it is not reported. A false positive can be a nuisance resulting in a waste of time for an ethical hacker, whereas a false negative can be really dangerous, leaving a network or application susceptible to attack, while giving an illusion that everything is alright. It has been observed that automated tools tend to exhibit false positives as well as false negatives. This brings us to the next important question of which method is better—the automated VAPT or manual VAPT?

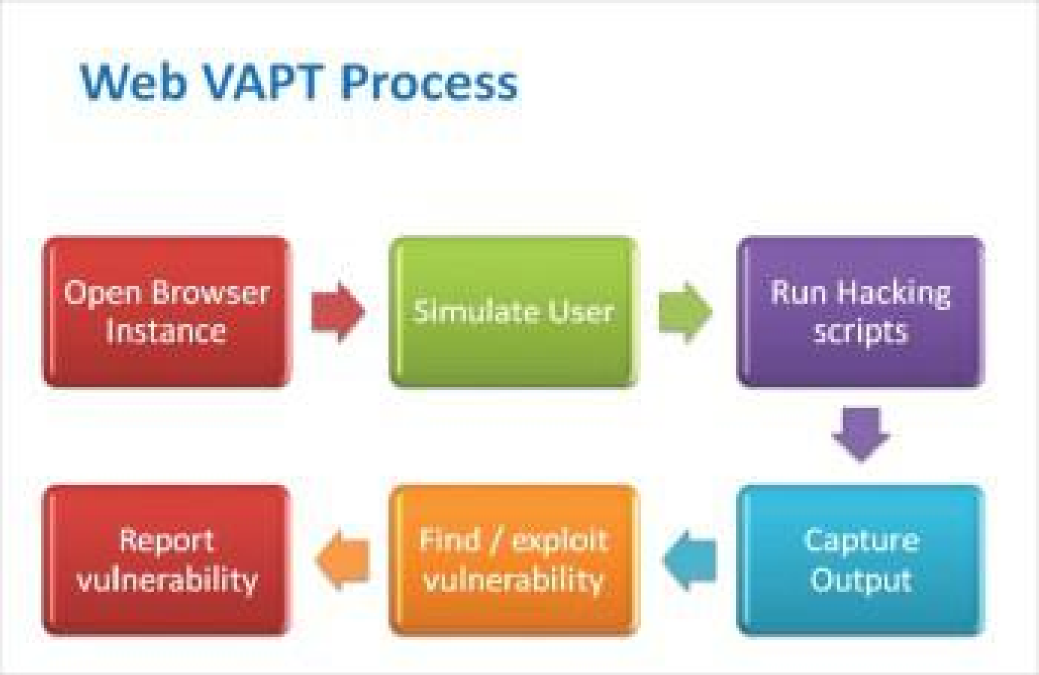

Figure-2: Web VAPT Process

Automated vs manual VAPT

The shortest answer is that the manual VAPT is always better and, hence, is a more widely used approach. This is because the automated tools are based on simple logic, which checks either for signatures or behaviour. To understand this, let’s go to the basic difference between a software program and the human mind. Listed below are the steps a typical ethical hacker performs for a VAPT.

- Enumerates a vulnerability
- Performs an attack manually
- Analyses the results of the attack
- Performs similar or different attacks based on previous findings
- Assimilates the results to create a customised attack
- Exploits the vulnerability further to see if more attacks are possible
- Repeats the above steps for all vulnerabilities

Each network or application is different, resulting in a very wide range of vulnerability scenarios. From the above steps, it becomes clear that there is a lot of complexity involved in VAPT, wherein, the results of one test decide the actions of the next one. This makes VAPT a process of cascaded intelligence, where you cannot predict the next step and also need to apply years of experience to reach a conclusion. No tool can do this, at least, not as of today, and hence it must be performed manually. An ethical hacker’s job can be made less stressful by automating certain tasks of vulnerability assessment; however, the proof-of-concept part in penetration testing mostly relies on manual ways of exploiting the loophole and gathering the required evidence. Given below are the benefits of manual penetration testing.

- Mimics the behaviour of real life hackers
- Brings a great deal of accuracy to the results
- No false positives
- Provides evidence, enabling the replication of problems
- Helps in fixing a product’s security design issues

VAPT is a methodical approach to risk management. CISO’s or IT heads should, as a matter of strategy, incorporate VAPT in their budgets and risk governance processes. It should be a periodically executed process, and the frequency should depend upon the data’s confidentiality and risk impact. While there are multiple tools to perform vulnerability assessment, penetration testing is a manual process, and should be handled by professional and highly experienced ethical hackers. This will ensure genuine cyber security as opposed to an illusion of being secure.