EasyChair Preprint

№ 5425

Auto Vulnerability Assessment and Penetration Testing Tools

Vishal Kumar and Abhay Singh

EasyChair preprints are intended for rapid dissemination of research results and are integrated with the rest of EasyChair.

April 29, 2021

Auto Vulnerability Assessment and Penetration Testing Tools

Mr Vishal Kumar, Mr Abhay Pratap Singh

***Abstract*—The complexity of the system is increasing day by day. This leads to more vulnerability for Systems. The attackers use these being at risk of exploiting the victim's system. It is best to detect this danger ahead of time for the attacker. Attack risk assessment is often underestimated. While Risk Assessment and Entry Test can be used as cyber-defense technology to provide effective cyber protection. In this paper we have shown that Vulnerability Assessment and Penetration Testing (VAPT) as a cyber security technology, on how we can provide effective cyber protection using Vulnerability Assessment and Login test. We have defined the complete life cycle of Vulnerability Assessment and Penetration Testing in systems or networks and actions taken to resolve that risk and to stop potential attacks. In this paper we have explained standard risk assessment strategies and other popular VAPT tools.**

I. INTRODUCTION

Computer use is increasing day by day. System complexity is increasing. Most programs now exist are connected to the Internet. New and sophisticated software is coming to the market. All of these activities are on the rise vulnerability to systems.

Vulnerability is a weakness in the application which may be a launch error or a design error allows the attacker to inflict damage on the system user and gain additional privileges.

Being at risk is what it is potential systemic risk. An attacker uses this risk to exploit the system and gain unauthorized access and knowledge.

Risk is a major flaw in system security and information security. A free risk plan can provide more information and system security. Although it is almost impossible to be 100%
a risk-free system, but by removing as many risks as possible, we can increase system security.

The Need for Injury Test and Entry Test It is often underestimated to date. It's just think of it as a work in progress and used by very few people. By using common and effective vulnerability Testing, we can reduce the risk of serious attacks and have more secure systems.

In this paper we describe the Vulnerability and Testing Penetration testing as an important cyber protection Technology. By using VAPT as a Cyber Defense Technology we can remove the risk from our system as well as reducing the chances of cyber attacks. We have described the various strategies of Vulnerability Assessment and PenetrationTesting. We have described the complete VAPT life cycle of active protection. This will also provide the suitable solution to how to use VAPT as a cyber protection technology.

II. LITERATURE REVIEW

Much research has been done by the researcher in the past on Vulnerability Assessment. Ivan Krsul2 shows that Computer vulnerability data indicate an important event and that can be detected again and again shown with the eyes. Steven E Noel3 et al. find reliance on multiple injuries and single exploitation network and its effects. Stefan Kals4 et al. show the 'SecuBat' web security tool made by them.

Sushil Jajodia5 and Steven Noel described the method of Topical Vulnerability Analysis Analysis. This is analytical dependency dependence and potential attack on a computer network. Christopher Kruegel6 et al. presenting an in-depth study of the "Execution after Redirect" Vulnerability.

Different ways for performing testing:

Static Analysis

In this way we do not commit any criminal offense or exploitation. We analyze code structure and content for

system. In this way we can find all kinds of weaknesses. In this method we do not use the system, so there will be no adverse effect of this test on the system. One of the disadvantages of this approach is that it is slow and requires many hours of practice.

Automated Approach to VAPT

The default method sounds appealing and only requires a tool to be used that works in your area and produces results for you. However, risk testing for networks or systems is done with a tool like Nessus, which is a well-known commercial tool in the security industry that we use in our engagement.

A plugin-based tool that detects risk in terms of environment or system. But in the same login test it is not much to say, the tools can automatically use the risks they find but to what extent; will attempt the Denial of Service (DoS) in the system or provide a return shell to the exploited system; Will be able to use the risk if found, but the payload is restricted to the last resort; will it be able to pinpoint changes in parameters and continue to exploit until exploited?

Let’s talk about some of the disadvantages of automated tools, one thing to look out for is the false positives that use a well-designed tool that may or may not provide the exact output that one expects. The worst case scenario is an automated tool that lowers the entire network or critical system, which not only stops the business but can also cost them a lot of money over leisure time. Using such tools requires a knowledgeable person who can set the settings according to their nature. It also requires a person to understand the report made by the tool and make it a point.

Manual Approach to VAPT

The manual method depends only on the ability of the examiner. From each other the skills may vary. This method is the most common method in the industry, as it exposes more business risks than the general risks that can be generated by automated tools. This method is time consuming and expensive, however, it is very beneficial for the organization in detecting the vulnerability of a business log where any automated tool does not compete with it. In some high-security environments, where the network system may not be connected to the production network; Viewers can be

provided with a new version of the OS for pencil testing or you have limited tools for using it and not the default tools. In such cases, it depends on the skills of the examiner and the years of experience a person has. However, false profits do not concern this approach as they have been verified prior to reporting.

The benefits of this approach are reliable and focused on the level of concern. Also, it can be suspended at any time, the inspector is given clear and concise instructions on how much work will be done. For example: manual pen testing can be stopped at any time or to the extent that the inspector can walk; if the payload is blocked the inspector may try to encrypt it separately where the conclusion may fail to detect and block the upload resulting in the order being executed successfully. Similarly, a zero-day risk can be detected using this method, it is completely critical.

Downsizing an inexperienced inspector may miss out on the risks posed by the client and over time if the client is hacked or does the job for another vendor and gives more results than previously sold, it may tarnish the company's brand and most importantly, give the client a false sense of security. Here the inspector can check according to his / her advanced knowledge and miss out on things. This method is time consuming and not all tests need to be done manually. In today's world, everyone uses the Internet. SECURITY is one of the major problems of the internet. Skilled hackers daily violate security and take advantage of the opportunity to risk access to confidential information. To overcome this problem a single solution was called the Vulnerability Assessment and Penetration Testing (VAPT). Risk Assessment is the ability to find an open door. Entry testing includes a series of activities performed to identify and exploit security threats. Login testing is widely used to help ensure network security. The traditional entry test is done by the inspector manually by the scheme, the process is often complicated which leads to a lot of work and requires the inspector to become familiar with all kinds of tools. It is therefore advisable to use an integrated approach to define a computer-readable system, in which case a computer can be used to install a test site to perform an entry test. This paper provides an overview of VAPT and describes the process and process of VAPT.

Fuzz Testing:

This is also known as paradox. In this case we add invalid or other random data to the system and check for crashes and failure. This is similar to the strength test. This method can be used with very little human communication. This the procedure can be used to determine the risk of a zero day.

All Internet-based programs and applications have security risks. Safety experts around the world address these security risks through Vulnerability Assessment and Pension Testing (VAPT). VAPT is an aggressive approach to protecting an organization's cyber assets. It has two main components, namely Vulnerability Assessment (VA) and Penetration Testing (PT). Risk assessment, including the use of a variety of automated tools and self-assessment techniques to determine the security status of the target system.

At this point all violation points and gaps are available. These areas of lawlessness or gaps where an attacker is found can lead to serious data loss and fraudulent activities. In the login test the tester mimics the activities of a malicious attacker who tries to exploit the dangers of the target system. In this step the visual set of vulnerabilities in the VA is used as an input vector. This VAPT process helps in to evaluate the effectiveness of the safety measures available in the target system. In this page we have describe the entire VAPT process, as well as all methods, models and standards. A set of short lists of useful and popular open source tools that are useful for VAPT and the required monitoring list is provided. The VAPT course conducted in the banking system is also discussed using short-listed tools.

By taking advantage of the vulnerabilities, cyber criminals can easily steal ICT confidential information, resulting in huge losses. Vulnerability Testing Testing and logging is a special way to eliminate various security threats in the web application. With a focus on high-risk resources such as SQL Injection, Cross Site Scripting, Local File Inclusion and Remote File Inclusion, in this paper, we have reviewed the textbooks typical VAPT process and collected tools that can help during the VAPT process.

III . Problem Formulation

There are different types of threats available where the system is always connected to the internet, any system can be attacked using different strategies, and there are always new threats and new types of attacks emerge. Therefore, Everyone needs to identify the risk and take precautionary measures to keep their personal and professional data safe from cyber criminals.

Our project aims to address this by providing people with information on how to attack their system, so that they can fill in the gaps in security of their system and taking precautionary measures such as firefighters, etc. in the event of a possible attack. We have build web tools that will monitor the security of your servers and provide you with a list of risk-taking.

IV . Required tools :

Python:

Python is a translated, high-quality, general-purpose translation language. Created by Guido van Rossum and first released in 1991, Python's design philosophy emphasizes the readability of the code with its remarkable use of white. Its language-building and object-oriented approach aims to assist editors in writing clear, logical code for small and large projects.

Python typed harder and collected garbage. It supports many planning paradigms, including layout (especially, process), object-oriented, and operational planning. Python is often described as a "battery-powered" language because of its standard library

Django:

Django is a free web-based web-based Python based model-view-controller (MVC) architec- tural pattern. It is maintained by the Django Software Foundation (DSF), an American non-profit organization established as a 501 (c) (3) nonprofit organization.

Django's main goal is to facilitate the construction of complex, database-driven websites. The framework emphasizes reuse and “connectivity” of objects, minimal code, low integration, rapid development, and the goal of never repeating them. Python is used everywhere, or in settings files and data models. Django also provides an optional administrative interface for the construction, learning, refurbishment and removal of dynamic and intuitive controls with management models.

Nmap:

Nmap (Network Mapper) is a free and open source scanner for work done by Gordon Lyon (also known as Fyodor Vaskovich).

Nmap provides many features for computer network research, including host and service detection and application detection. These features are expanded with scripts that provide improved service access, risk detection and other features. Nmap can adapt to network conditions including latency and congestion during scanning.

Searchsploit:

searchsploit, an Exploit-DB command line search tool that also allows you to take a copy of the Use Database with you, wherever you go. SearchSploit enables you to perform detailed off-line searches with your local copy. This capability is particularly useful for security checks on isolated or wireless networks without Internet access.

Many exploits contain links to binary files that are not included in the standard repository but can be found in our Exploit Database Binary Exploits repository. If you think you will have internet access to the test, be sure to look at both the caches of the most complete set of data.

NLP:

Natural language processing is a sub-field, computer science, information engineering, and artificial intelligence that affects the interaction between computers and human languages, especially how to configure computers to process and analyze large data of natural language Namely, speech and text. We are surrounded by text.

Think about how much text you see each day:

- Signs
- Menus
- Email
- SMS
- Web Pages
- and so much more. . . .

V. Feasibility Analysis :

In order to predict whether an URL is fully Secured or what is its current level of security.

To predict it we require a URL. Auto VAPT Tool which is used to test penetration testing of any server or system. It generates a list of possible attacks on the server provided to it.

Our input and final result consist of following things:

Inputs:

URL: url of the server to be tested.

Security: Data About different Security Features working on the server.

Goal – To generate a list of possible attacks or security threats.

VI. JUSTIFICATION:

In this section we will show how we can consider risk analysis as cyber protection technology. This usually the attacker does to respect the victim's network and get information about the victim's network. Back to obtain information, the attacker conducts a risk assessment on the victim's network / system and detects exposure or loop holes

After getting the vulnerability list of the victim, the attacker make a plan for the possible attack. With that list

attacker exploit the victim's network or system and compromise his system security and information. But if Victim removes all the vulnerabilities from his system, the attacker would not be able to exploit the

victim's network/system. By applying VAPT technique user can find out the vulnerabilities those can result in

various severe attacks like - DDoS attack, RA flooding, ARP poisoning etc. After finding out the vulnerabilities user can apply counter measures against them. To make the system vulnerability free, Administrator should find out vulnerabilities in his own system/network. The administrator should apply complete vulnerability and penetration testing cycle on the system/network. When the administrator would get the list of available vulnerability in his/her system, he should remove those vulnerabilities. To remove the vulnerabilities, the administrator should apply the necessary patches, updates, install necessary software and other requisite. In this way administrator would remove all vulnerabilities from his system/network.

VII. Complete Work Plan layout:

We plan to build a web-based tool that will capture all the different information about your security flow from your system.

The security measures you used, the servers you visit, your IP address, etc.

We plan to build a website that will be used using HTML and CSS frameworks and web design in advance.

After that we will use the Django frame to wrap our end back and forth.

We are now preparing our dashboard. It will be in the operating phase within a few weeks.

Testing:

For testing our model we will be doing a 4 step testing which includes-

A. Local Development

B. Testing in CI/CD

C. Stage testing / shadow testing

D. A/B test

Local Development :

With this we will train our database into 2-3 models and then determine which model will be suitable for production purpose, which gives us a percentage of high accuracy of how long it will take to produce results.

Testing in CI/CD :

The CI / CD environment has access to a specific external data database that no one in the Science Data group can access. The new model is automatically tested in the same way every time, and the author cannot touch that. testing Download application with a new model can be accepted to join the development branch and proceed to the next step.

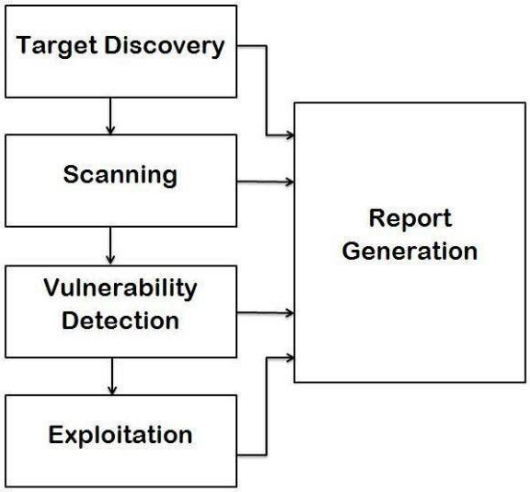
Stage testing / shadow testing:

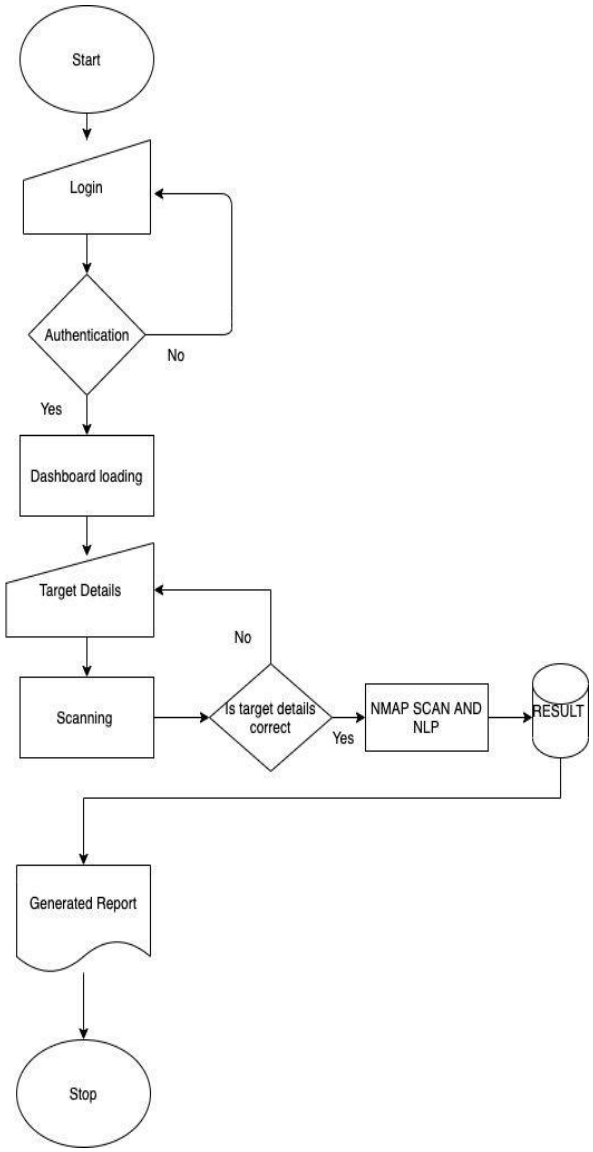
In this we will try to test our environment in the production environment .like if we created a pipeline model for our project does it affect our accuracy or not.

A/B Testing :

For the final test we perform A/B testing ie; to perform statistical test and expected to capture statistical power.

The research paper consists of two figures Fig1 and Fig2 . Fig1 represents the dataset used for this research .





VIII. REFERENCES:

1. Owasp category: Vulnerability. 2015. URL: https://www.owasp.org/index.php/Vulnerability.

2. Krsul, I.. Computer vulnerability analysis: Thesis proposal 1997;.

3. Noel, S.E., O'Berry, B., Hutchinson, C., Jajodia, S., Keuthan, L.M., Nguyen, A.. Combinatorial analysis of network security. In: AeroSense 2002. International Society for Optics and Photonics; 2002, p. 140–149.

4. Kals, S., Kirda, E., Kruegel, C., Jovanovic, N.. Secubat: a web vulnerability scanner. In: Proceedings of the 15th international conference on World Wide Web. ACM; 2006, p. 247–256.

5. Jajodia, S., Noel, S.. Topological vulnerability analysis. In: Cyber Situational Awareness. Springer; 2010, p. 139–154.

6. Doupe´, A., Boe, B., Kruegel, C., Vigna, G.. Fear the ear: discovering and mitigating execution after redirect vulnerabilities. In: Proceedings of the 18th ACM conference on Computer and communications security. ACM; 2011, p. 251–262.

7. Vulnerability assessment and penetration testing (vapt). 2015. URL: http://memorize.com/vulnerability-assessment-and-penetration-te.

8. Nist, usaid mission site vulnerability assessment and remediation. 2015. URL: http://www.nist.gov.

9. Shah, S., Mehtre, B.M.. An overview of vulnerability assessment and penetration testing techniques. Journal of Computer Virology and Hacking Techniques 2014;:1–23.

10. Sectools.org: Top 125 network security tools. 2015. URL: http://sectools.org/. Last Accessed: JAN 2015. 11. Tripathi, N., Mehtre, B.M. Analysis of various arp poisoning mitigation techniques: A comparison. In: Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014 International Conference on. IEEE; 2014, p. 125–132. 12. Goel, J.N., Mehtre, B.M.. Dynamic ipv6 activation based defense for ipv6 router advertisement flooding (dos) attack. In: Computational Intelligence and Computing Research (ICCIC), 2014 IEEE International Conference on. Dec 18-20, 2014, p. 628–632.