Turkish Journal of Computer and Mathematics Education Vol.12 No.13 (2021), 1959-1964

Research Article

Auto Vulnerability Assessment and Penetration Testing Tools

Mr Vishal Kumar, Mr Abhay Pratap Singh

B.Tech.(CSE), Galgotias University

B.Tech.(CSE), Galgotias University

abhay.satyam.singh@gmail.com, Vishalkumar6404338@gmail.com

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 4 June 2021

Abstract— The complexness of the system is increasing day by day. This results in a lot of vulnerability for Systems. The attackers use these being in danger of exploiting the victim's system. it's best to sight this danger earlier than time for the assailant. Attack risk assessment is usually under estimated. While Risk Assessment and Entry check will be used as cyber-defense technology to supply effective cyber protection. during this paper we've got shown that Vulnerability Assessment and Penetration Testing (VAPT) as a cybersecurity technology, on however we are able to give effective cyber protection penetration Vulnerability Assessment and Login check. we've got outlined the entire life cycle of Vulnerability Assessment and Penetration Testing in systems or networks and actions taken to resolve that risk and to prevent potential attacks. during this paper we've got explained customary risk assessment methods and alternative in style VAPT tools.

Index Terms—*About four key words or phrases in alphabetical order, separated by commas.*

INTRODUCTION

Computer use is increasing day by day. System complexness is increasing. Most programs currently exist square measure connected to the web. New and complex code is coming back to the market. All of those activities square measure on the increase vulnerability to systems. Vulnerability may be a weakness within the application which can be a launch error or a style error permits the assaulter to impose harm on the system user and gain further privileges.

Being in danger is what it's potential general risk. associate degree assaulter uses this risk to take advantage of the system and gain unauthorized access and data.

Risk could be a major flaw in system security and knowledge security. A free risk set up will offer a lot of info and system security. though it's nearly not possible to be 100% a unhazardous system, however by removing as several risks as potential, we will increase system security. The Need for Injury take a look at and Entry take a look at it's typically underestimated thus far. It's simply consider it as a piece ongoing and employed by only a few folks. By victimization common and effective vulnerability Testing, we will scale back the chance of significant attacks and have safer systems. In this paper we have a tendency to describe the Vulnerability and Testing Penetration testing as a crucial cyber protection Technology. By victimization VAPT as a Cyber Defense Technology we will take away the chance from our system still as reducing the probabilities of Cyber Attacks. we've represented the assorted methods of Vulnerability Assessment and Penetration Testing. we've represented the whole VAPT life cycle of active protection. this may conjointly offer the appropriate answer to a way to use VAPT as a Cyber security technology.

I. LITERATURE REVIEW

Much analysis has been done by the man of science within the past on Vulnerability Assessment. Ivan Krsul shows that pc vulnerability knowledge indicate a vital event which is detected once more and once more shown with the eyes. Steven E Christmas realize reliance on multiple injuries and single exploitation network and its effects. Stefan Kals show the 'SecuBat' internet security tool created by them. Sushil Jajodia and Steven Christmas represented the strategy of Topical Vulnerability Analysis. this is often analytical dependency dependence and potential attack on a electronic network. Saint Christopher Kruegel presenting Associate in Nursing in-depth study of the "Execution when Redirect" Vulnerability.

Different ways for performing testing:

Static Analysis

In this method we tend to don't commit any criminal offense or exploitation. we tend to analyze code structure and content for system. during this method we are able to realize all types of weaknesses. during this technique we tend to don't use the system, thus there'll be no adverse impact of this take a look at on the system. one in every of the disadvantages of this approach is that it's slow and needs several hours of apply.

Automated Approach to VAPT

The default methodology sounds appealing and solely needs a tool to be used that works in your space and produces results for you. However, risk testing for networks or systems is completed with a tool like Nessus, that could be a we tend toll-known industrial tool within the security business that we use in our engagement. A plugin-based tool that detects risk in terms of setting or system. However within the same login take a look at it's not a lot of to mention, the tools will mechanically use the dangers they notice however to what extent; can try the Denial of Service (DoS) within the system or offer a comeback shell to the exploited system; are going to be ready to use the risk if found, however the payload is restricted to the last resort; can or not it's ready to pinpoint changes in parameters and still exploit till 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 methodology depends solely on the power of the examiner. From one another the talents could vary. This methodology is that the most typical methodology within the trade, because it exposes a lot of business risks than the overall risks which will be generated by automatic tools. This methodology is time overwhelming and expensive. however, it's terribly useful for the organization in police work the vulnerability of a business log wherever any automatic tool doesn't vie with it. In some high-security environments, wherever the network system might not be connected to the assembly network; Viewers is given a replacement version of the OS for pencil testing otherwise you have restricted tools for exploitation it and not the default tools. In such cases, it depends on the talents of the examiner and also the years of expertise someone has. However, false profits don't concern this approach as they need been verified before news. The benefits of this approach square measure reliable and targeted on the extent of concern. Also, it is suspended at any time, the inspector is given clear and elliptic directions on what quantity work are going to be done. For example: manual pen testing is stopped at any time or to the extent that the inspector will walk; if the payload is blocked the inspector could attempt to write it on an individual basis wherever the conclusion could fail to notice and block the transfer leading to the order being dead with success. Similarly, a zero-day risk is detected exploitation this methodology, it's fully crucial. Downsizing associate degree inexperienced inspector could miss out on the risks exhibit by the shopper and over time if the shopper is hacked or will the employee of the vender and provides more results than antecedently sold-out, it should tarnish the company's complete and most significantly, provide the shopper a false sense of security. Here the inspector will check in line with his / her advanced data and miss out on things. This methodology is time overwhelming and not all tests have to be compelled to be done manually. In today's world, everybody uses the net. SECURITY is one amongst the main issues of the net. sure-handed hackers daily violate security and profit of the chance to risk access to counsel. to beat this drawback one answer was referred to as the Vulnerability Assessment and Penetration Testing (VAPT). Risk Assessment is that the ability to search out associate degree open door. Entry testing includes a series of activities performed to spot and exploit security threats. Login testing is wide accustomed facilitate guarantee network security. the normal entry check is finished by the inspector manually by the theme, the method is commonly sophisticated that results in tons of labor and needs the inspector to become accustomed to every kind of tools. it's thus well to use associate degree integrated approach to outline a computer-readable system, during which case a pc is accustomed install a check web site to perform associate degree entry check. This paper provides an outline of VAPT and describes the method and processes of VAPT.

Fuzz Testing:

This is additionally called contradiction. during this case we have a tendency to add invalid or different random information to the system and check for crashes and failure. this can be almost like the strength check. This methodology is used with little human communication. This the procedure is wont to confirm the chance of a zero day.

All Internet-based programs and applications have security risks. Safety consultants round the world address these security risks through Vulnerability Assessment and Pension Testing (VAPT). VAPT is associate aggressive approach to protective associate organization's cyber assets. it's 2 main parts, particularly Vulnerability Assessment (VA) and Penetration Testing (PT). Risk assessment, as well as the utilization of a range of automatic tools and self-assessment techniques to work out the protection standing of the target system.

At now all violation points and gaps area unit offered. These areas of lawlessness or gaps wherever associate wrongdoer is found will result in serious information loss and fallacious activities. within the login check the tester mimics the activities of a malicious wrongdoer WHO tries to take advantage of the hazards of the target system. during this step the visual set of vulnerabilities within the VA is employed as associate input vector. This VAPT method helps in to judge the effectiveness of the security measures offered within the target system. during this page we've describe the complete VAPT process, moreover as all ways, models and standards. a group of short lists of helpful and standard open supply tools that area unit helpful for VAPT and also the needed observation list is provided. The VAPT course conducted within the industry is additionally mentioned exploitation short-listed tools.

By taking advantage of the vulnerabilities, cyber criminals will simply steal ICT tip, leading to vast losses. Vulnerability Testing and work could be a special thanks to eliminate numerous security threats within the internet application. With a spotlight on risky resources like SQL Injection, Cross website Scripting, native File Inclusion and Remote File Inclusion, during this paper, we've reviewed the textbooks typical VAPT process and picked up tools that may facilitate throughout the VAPT process.

III. PROBLEM FORMULATION

There are differing types of threats out there wherever the system is usually connected to the net, any system are often attacked victimization completely different methods, and there square measure continually new threats and new forms of attacks emerge. Therefore, everybody must determine the danger and take preventative measures to stay their personal and skilled knowledge safe from cyber criminals.

Our project aims to handle this by providing individuals with data on the way to attack their system, in order that they'll fill within the gaps in security of their system and taking preventative measures like firefighters, etc. within the event of a potential attack. we've designed internet tools which will monitor the protection of your servers and supply you with an inventory of risk-management tools.

IV. REQUIRED TOOLS:

1. **Python**: Programming language used for implementation of backend code.
2. **Django**: Web-Framework of python language for backend development of product.
3. **Nmap**: Tool used for generating list of services being used on the network to be tested.
4. **Searchsploit**: python Library for Data analytics
5. **NLP**: Natural Language processing, a Advance machine learning tool for convert generated risks into a user readable pdf file.

V. FEASIBILITY ANALYSIS:

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 In 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.
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-

Local Development
Testing in CI/CD
Stage testing / shadow testing
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.

Fig1

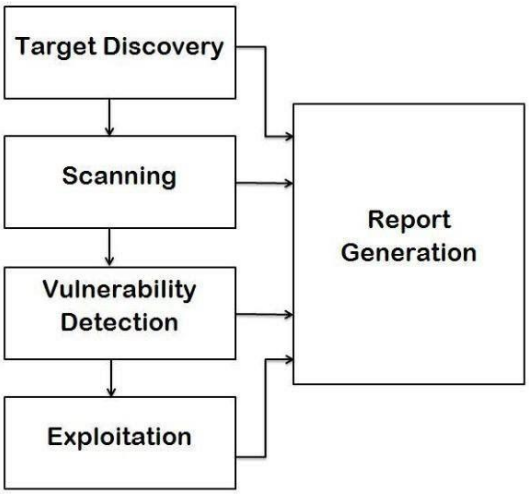
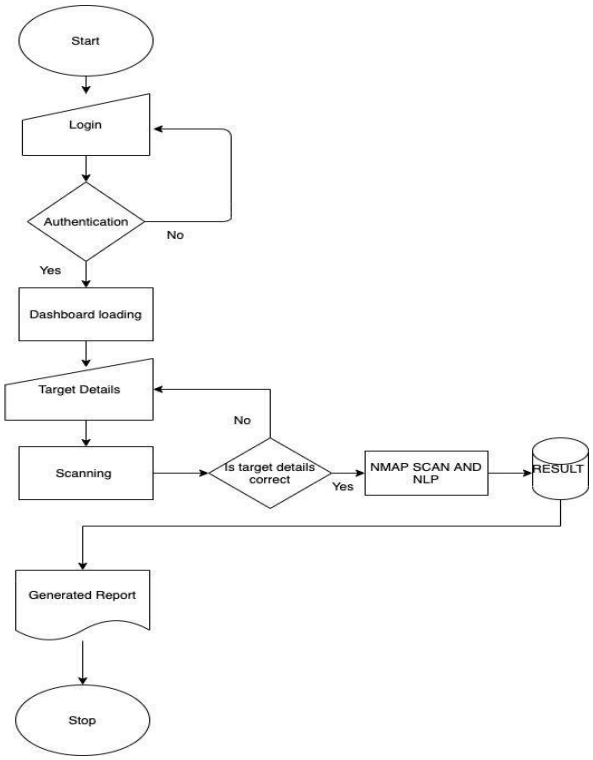

Target Discovery
Scanning
Vulnerability Detection
Exploitation
Report Generation

Fig2


Start
Login
Authentication
No
Yes
Dashboard loading
Target Details
No
Scanning
Is target details correct
Yes
NMAP SCAN AND NLP
RESULT
Generated Report
Stop

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.