ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 6, Issue 1, July 2016

Integrating ticketing system for Vulnerability management

Siva guru. G. S
Professional Diploma in Cyber Investigation and Laws

Abstract*— The latest threat report reveals that business is struggling to keep up with rapid changes in techniques by cyber criminals as they switch to increasingly malicious campaigns. Vulnerability is a flaw to a system that allows an attacker to suppress a system's information assurance in computer security. Hence vulnerability assessment is performed for defining, identifying, and classifying the vulnerabilities or security loop holes in a computer, network, or other communications infrastructure. Nessus is a comprehensive proprietary vulnerability scanning tool which scans a computer network and raises an alert if it detects any vulnerabilities. This paper deals with bug tracking with Nessus, where Nessus doesn't have bug tracking with blocker, critical and major report it to cyber security team in any organizations. This proposed system is a novel approach which gives an established idea that all organizations needs an automated bug/issue/defect tracking system and significance of a bug tracking system in cyber security team. This proposed tool is a bug tracking tool integrated with Nessus and Bugzilla which can used for automated ticketing in many organizations.

***Index Terms*— Bug, Bugzilla, Nessus, Vulnerability**

I. INTRODUCTION

Network security is most important to computer users, organizations and in the military. Security is essential for networks and applications. Existence of communication gap between developers of networks and the developers of security technology has to be considered in part of network security. Network security is a concern about computers at each end of the communication chain. There is a possibility that the communication channel is vulnerable to attack when transmitting data. Hackers could intend the communication channel, acquire the data, decrypt, and re-insert a false data [2].

Nessus is a comprehensive proprietary vulnerability scanning tool which scans a computer network and raises an alert if it detects any vulnerabilities. After scanning, Nessus clients typically provides means to analyze the result, wherein client itself list each of the vulnerability found, determining its level of severity and suggesting how the problem could be fixed to the user [1] . Ticketing is a technique to track the detection, reporting, and resolution of some type of vulnerabilities. Unfortunately, Nessus only provides reports on vulnerability but do not support ticketing. Hence we present a novel approach which takes in the output of Nessus and render it to the Selenium Web driver which performs ticketing by considering only the high and critical vulnerabilities using Bugzilla. The drawback of Nessus is replaced by this approach, by using the Nessus capabilities. Selenium web driver is used for its advantage of being open source automation tool and direct interaction with the browser. This exploits the communication gap by sending vulnerability report

II. GENERATION OF VULNERABILITY REPORT

Nessus is vulnerability scanner developed by Tenable Network Security. Nessus is a powerful tool to help keep the domains free of vulnerabilities that viruses and hackers commonly target to exploit in any computer (or group of computers) connected to the internet. . Nessus is a tool which does not actively prevent attacks but scans the computer network for any vulnerability that hackers try to exploit.

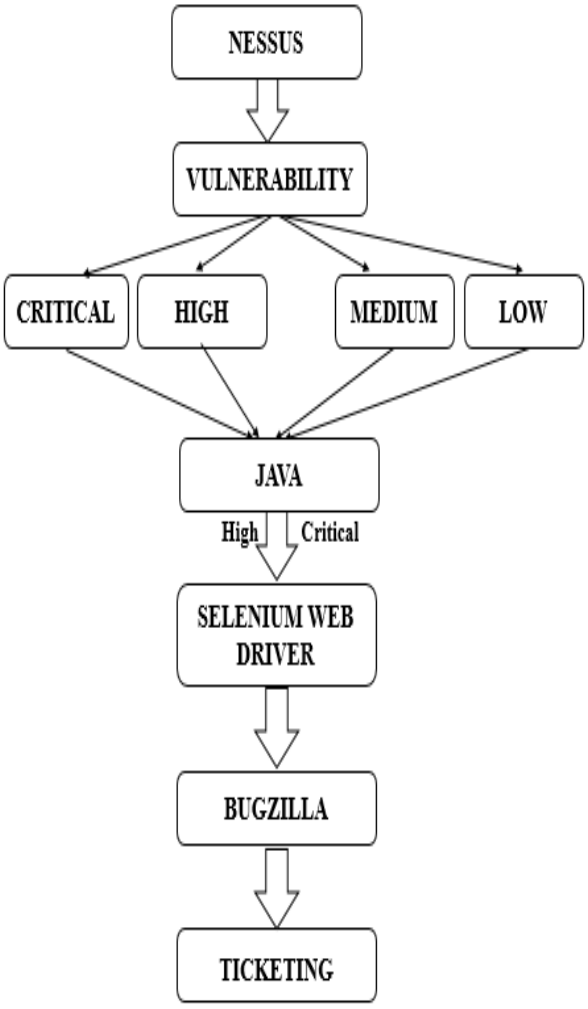

Fig 1. Block Diagram of the Automation tool

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 6, Issue 1, July 2016

After running a scan, Nessus client itself will list each vulnerability found, reporting its level of severity and suggesting how this problem could be fixed. Nessus categorises the vulnerabilities of risk as Low, Medium, High and Critical as in Fig. 1 by generating report. Nessus does not make assumptions about the server configuration unlike other scanners which leads the scanners to miss real vulnerabilities. Nessus clients generate more elaborative and graphical reports in a variety of different formats about the vulnerabilities. The formats in which the report can be exported are, .nessus - This format uses an expanded set of XML tags to make extracting and parsing information. This report does not allow chapter selection

HTML - A report generated using standard HTML that allows chapter selection and opens in a new tab in your browser.

PDF - A report generated in PDF format that allows chapter selection.

Nessus DB - A proprietary encrypted database format that contains all the information from a scan, including the results and audit trials.

CSV- A comma-separated values (CSV) report that can be used to be imported into many external programs like spreadsheets, databases and more. This report does not allow chapter selection.

III. VULNERABILITIES REFINEMENT USING SELENIUM WEBDRIVER

We prefer using Selenium WebDriver out of the Selenium suite because of its ability to control the browser from the OS level [3] and composed of simple architectureas represented in Fig 2 .Selenium WebDriver accepts commands and pass them to the browser. The CSV report format from the Nessus is passed as an input to the Selenium WebDriver using Java. This format is taken as it contains vast information about the vulnerabilities compared to other formats. Then the elements from the report are refined for further processing using Bugzilla.

The significant elements to be extracted from the report comprises of Common Vulnerabilities and Exposures (CVE), Common Vulnerability Scoring System (CVSS), name and description from the high risk vulnerability. CVE system is maintained by MITRE Corporation that defines CVE identifiers as common, unique identifiers for publicly known information-security vulnerabilities [5]. CVSS is free and industry standard for estimating the severity of computer system security vulnerabilities [6]. This attempts to assign scores ranging from 0-10 for the severity of vulnerabilities which is calculated by formula depending on metrics that approximates the impact and ease of exploit. We are taking the vulnerability scores above 7, which represents high and critical in the severity scale. Name and description gives the name and description of the vulnerability.

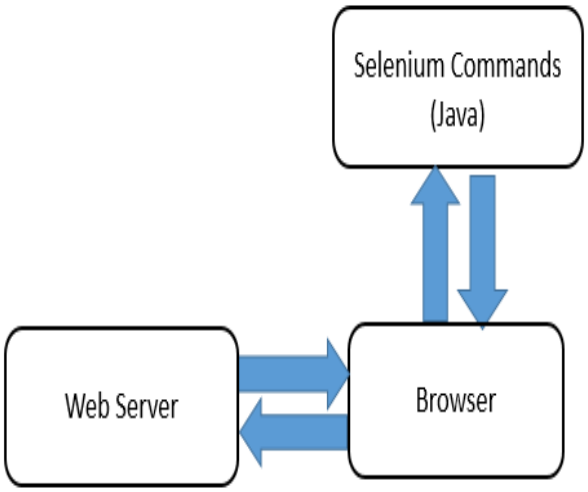

Fig 2. Architecture of Selenium Web driver

IV. TICKET CREATION USING BUGZILLA AND AUTOMATION

Bugzilla version 4 is an open source product, used as a bug-tracking/defect-tracking system which allows an individual or groups of developers to have track on critical bugs effectively in their product [4]. Our automation tool utilizes Bugzilla in order to perform ticketing, as Bugzilla does ticketing by requiring a person to assign bug manually. It is initiated by connecting through localhost and feeding the input from the previous stage which extracted CVE, CVSS, name and description from Nessus. Our tool manages to send a report about the bug one by one through e-mail to the group of people concerned in networking department without the need of a person to assign tickets manually.

V. CONCLUSION

Nessus reports all categories of vulnerabilities by scanning a network. Our tool refines only the major vulnerabilities using Selenium Web Driver. Bugzilla on the other hand, reports the bug and performs ticketing by manually assigning bug. This tool overcomes that by an automation process by which it takes only the critical vulnerabilities significant elements produced from Nessus and using Bugzilla to create tickets and produce bug report to the employees. This tool has been developed for the vulnerability issue tracking using Bugzilla. This will help to improve Strong link between review and bugs and commit queue integration and Comments are emailed out automatically. Tracking bugs improves communication, ensures accountability and increases security. The employees can review the report in a formatted way which would help minimizing the time to solve the bug. We can check the employees work accordingly.

VI. FUTURE WORK

The future work is to implement ticketing metric in this defect login tool, so that it can track performances in real

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 6, Issue 1, July 2016

time and respond to tickets before they can emerge as crisis.

ACKNOWLEDGMENT

I sincerely acknowledge Dr. B. Muthumuran, HTC ITMR for his guidance and supervision in this project. His care and concern has been the driving force for me all through this work. I am thankful for his constant advice and encouragement.

REFERENCES

[1] Dan Wendlandt, " Nessus: A security vulnerability scanning tool", http://www.cs.cmu.edu/~dwendlan/personal/nessus.html.

[2] Daya, Bhavya. "Network security: History, importance, and future", University of Florida Department of Electrical and Computer Engineering (2013).

[3] Gojare, Satish, Rahul Joshi, and Dhanashree Gaigaware. "Analysis and Design of Selenium WebDriver Automation Testing Framework." Procedia Computer Science 50: 341-346, 2015.

[4] Rocha, Henrique, et al. "NextBug: a Bugzilla extension for recommending similar bugs." Journal of Software Engineering Research and Development 3.1: 1-14, 2015.

[5] Rohse, Michael. "Vulnerability naming schemes and description languages: CVE, Bugtraq, AVDL and VulnXML." Sans Gsec Practical (2003).

[6] Scarfone, Karen, and Peter Mell. "An analysis of CVSS version 2 vulnerability scoring." Proceedings of the 2009 3rd International Symposium on Empirical Software Engineering and Measurement. IEEE Computer Society, 2009.