International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 04 | Apr 2021 www.irjet.net p-ISSN: 2395-0072

Vulnerability Management and Analysis Framework

Rutuja Bhoure[1], Shweta Jori[2], Ankit Sarode[3], Prof. Sayali Kokane[4]

[1,2,3]B.E Student, Dept. of Information Technology, Anantrao Pawar College of Engineering and Research, Pune, Maharashtra, India
[4]Professor (Internal Guide), Dept. of Information Technology, Anantrao Pawar College of Engineering and Research, Pune, Maharashtra, India

---

ABSTRACT: *Modern Software Systems are getting bigger and also more complex day by day. This will leads the system to numerous security vulnerabilities, and that will have to be challenging for developers to tackles the consequences. Vulnerability scanning is a fundamental unit in security assessments and risk analysis.*

There are varieties of tools and applications available that can detect vulnerabilities in the system. Vulnerability scanning has different types of applications and tools, it have specific functionality and has specific types of outputs that are particularly heterogeneous which makes further analysis a challenging task.

In this project, we used NMAP scanner. The Network Vulnerability Scanner created in this dissertation scans the active host-identifying network and predicts the remote host's OS and the programs installed in the remote host. They can open the port without identifying the active host and list the services running in the host. Further scanning is done by comparing the information obtained from a network scan and database of vulnerability signatures of vulnerabilities to produce a list of vulnerabilities that are present.

So, Using Network Mapping (NMAP) tool, Common Vulnerability and Exposure (CVE) and Common Vulnerability Scouring System (CVSS). The system will scan the vulnerabilities as well as generate the report automatically.

Key Words: Cyber-Security, Vulnerability Assessment, CVSS, CVE, Report Generation.

1. INTRODUCTION

With the development of technology, information systems are most commonly used in our day-to-day life, and application security tends to be of great concern. The prevalence of software industry to think of how to build quality in it. Software quality is the most related to the knowledge and experience of the developers.

Unfortunately, Because of some mistakes, it leads to vulnerabilities and defects to software. Software Vulnerabilities are defined as a defect in software systems that causes software or system crash or produced invalid output or behaves in an unnecessarily way. With the development of technology, information systems are most commonly used in our day-to-day life, and application security tends to be of great concern. The prevalence of software industry to think of how to build quality in it. Software quality is most related to the knowledge and experience of the developers.

Unfortunately, Because of some mistakes, it leads to vulnerability and defects to software. Software vulnerabilities are defined as defects in a software systems that cause software or system to crash or produced invalid output or behave in an unnecessarily way. Vulnerability Detection is the process of verifying if an error is found in the system or by compromising the security of the platform where the system is running. Comparing the other security approaches, such as Identifying and Preventing Intrusion. Finding faults and ultimately focusing on identifying correcting faults rather than detecting and blocking attacks.

In this system, we build a web application that not only detects the vulnerability from the client system but also automatically generates the report for a client.

2. RELATED DEFINITIONS

A. NMAP: NMAP is a short form of Network Mapper; NMAP is a tool that is free for users and open-source for Vulnerability Scanning and Network Discovery. Network Administrators use NMAP to identify what devices are running on their systems, discovering available hosts and the services they offer, finding open ports, and detecting risks.

B. CVE: The CVE stands for Common Vulnerability and Exposures, It Identifies all vulnerabilities and threats related to the security of the information system. To

do this, a Unique Identifier is assigned to each vulnerability.

C. CVSS: CVSS stands for Common Vulnerability Scoring System. Software security is a free and open-source industry for assigning the seriousness of vulnerabilities and is used in vulnerability management software. CVSS scores vulnerabilities are according to the severity of the threats. Scores are computed considering several metrics. Scores are given in between 0-10.

3. RELATED WORK

Sr. No	Title	Detection
1.	A Vulnerability Risk Assessment Method Based on Heterogeneous Information Network	Using Common Vulnerability Scoring Systems
2.	Automatic Classification Method for Software Vulnerability Based on Deep Neural Network	Using term frequency-inverse document frequency
3.	A Vulnerability Assessment Method in Industrial Internet of Things Based on Attack Graph and Maximum Flow	Based on the attack graph and maximum flow
4.	A Comparative Study of Deep Learning-Based Vulnerability Detection System	Using bidirectional recurrent neural networks
5.	An Intelligent Communication Warning Vulnerability Detection Algorithm Based on IoT Technology	Using CVE Database

Table -1 Reference paper and used Algorithm

4. SYSTEM ARCHITECTURE

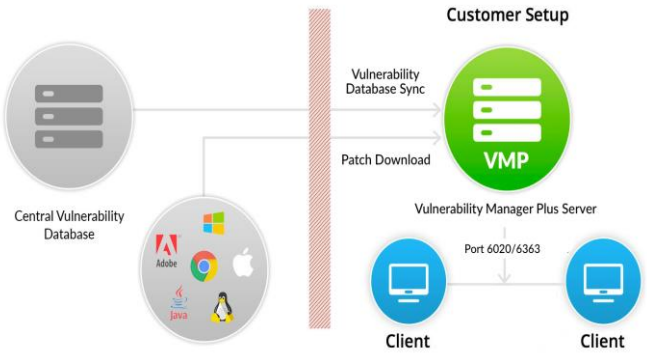

Figure No.: 1 System Architecture

A. Central Vulnerability Database: After analysis, the final aggregated data containing information about vulnerabilities, patches, security configuration, severs hardening, and high-risk software are then hosted in the Central Vulnerability Database(CVDB). The CVDB is a database containing information related to all reported vulnerabilities from publically available vulnerability data sources. Database updates information constantly.

B. Vulnerability Manager Plus Server (VMPS): The Vulnerability Manager Plus Server helps to centralized all vulnerability management tasks in the network endpoint. Tasks are installing a Client-Server, Scanning the client's server for searching vulnerability, etc. This VMP server on the client sites subscribes to the Central Vulnerability Database, from which it compiles the latest information on vulnerabilities and its solutions. Patches are downloaded directly from the vendor site and stored in the center of the server's patch management system.

C. PATCH MANAGEMENT: The ability to keep up-to date software stack on the computer and the network devices and also resist low-level cyber-attacks if there is any software is prone to technical vulnerabilities. Once the vulnerabilities are discovered and shared publically, these can rapidly be exploited by a cyber-criminal.

5. METHODOLOGY

Figure No.: 2 Methodology

A. **Setup:** In this activity, the software required to perform the test is needed to get installed on the base machine or server.

B. **Test Execution:** In this activity, the analyst has to prepare test cases and collect the IP address of the client machine which has to be scan for vulnerability assessment.

C. **Vulnerability Analysis:** It is the process of identifying, quantifying, and prioritizing the security gaps in the system.

D. **Reporting:** In reporting outcome should be Documented for future references. The number of vulnerabilities which are found in Vulnerability Assessment stage, it should be reported for patching purpose.

E. **Remediation:** It is the process of fixing the vulnerabilities in the system which is reported.

6. DESIGNING

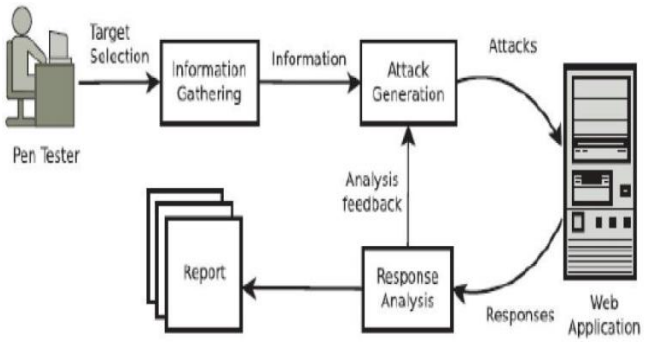

Figure No.: 3 High-Level Designs

In the above figure, Pen-Tester installed a vulnerability scanning tool in the server machine. Then the tester will configure the tool, after the configuration of the tool, the actual scanning process will start where the tool can find out various vulnerabilities in the client machine, and the report will generate automatically.

7. DATA FLOW FOR SCANNING VULNERABILITY

1. Data Flow 0:

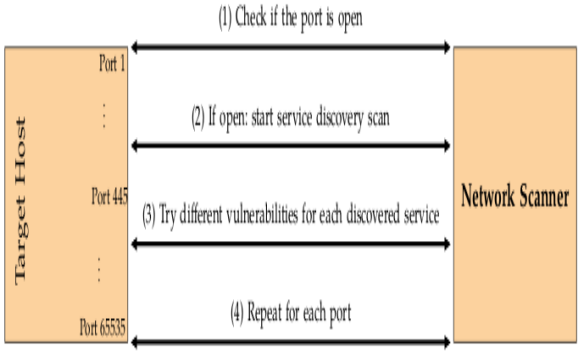

Figure No.: 4 Data Flow 0

The above Figure Shows the Traditional Vulnerability Scanning process. This process is so lengthy; it can take a lot of time to complete the scanning process.

2. Data Flow 1:

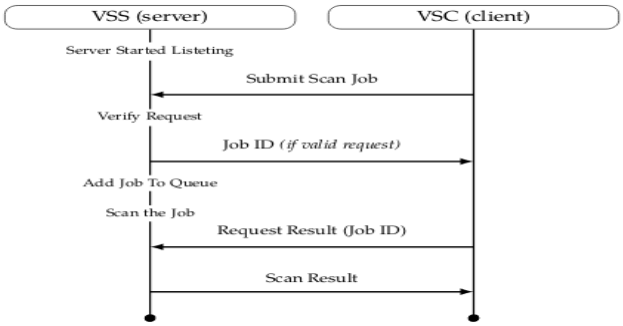

Figure No.: 5. Data Flow 1

The above Figure shows a general overview of the scanning process. This process consists of request/response operation handling so that communication will start in between VSS (server) and VSC(client).

3. Data Flow 2:

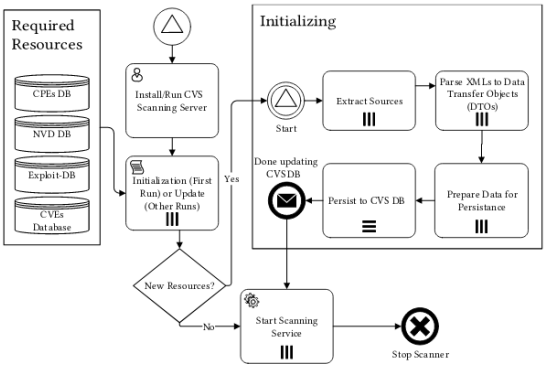

Figure No.: 6 Data Flow 2

The above Figure shows CVS (Common Vulnerability Scanner) server initialization process. The user starts the server by clicking on the web application. The updates are automatically downloaded in the database from multiple sources like exploit-DB, OpenVAS, OSVDB, ScipvulDB, SecurityFocus, SecurityTracker, xforce, etc.

8. IMPLEMENTATION OF APPLICATION

The following images show the overview of the project.

Login Page: This image shows Login Page, which allows the user to access the web application using a token.

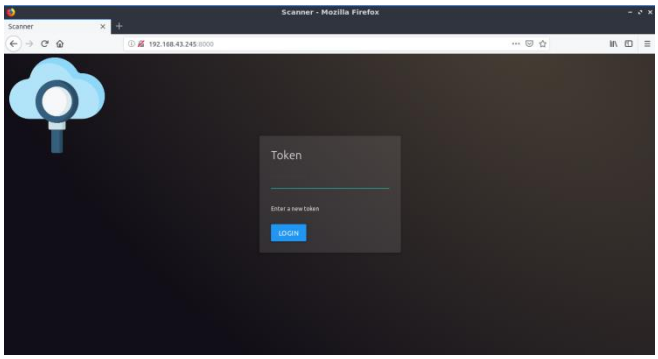

Figure No.: 7 Login Page

Dashboard: The following image shows the dashboard, which relevant information about the scan performed in the web application.

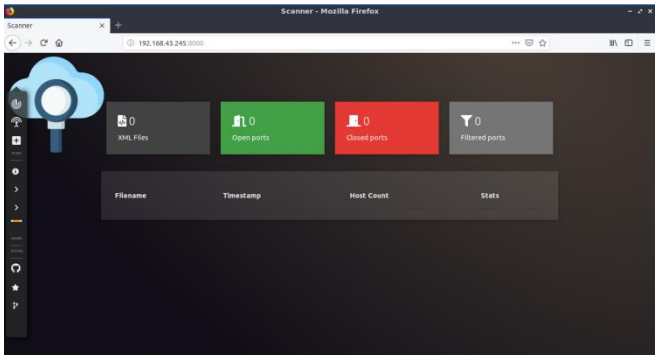

Figure No.: 8 Dashboard

Severity: This image shows the features which are given in the application for assigning the severity of a task.

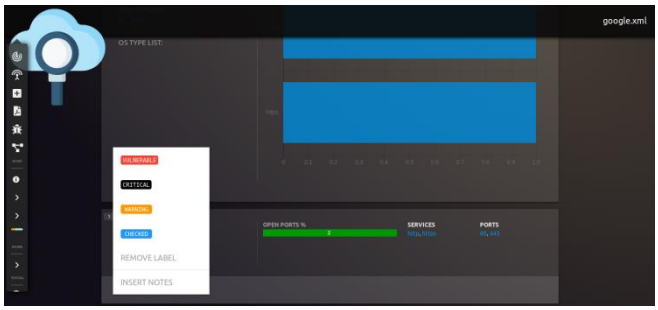

Figure No.: 9 Severity

Report: An entire report will convert into PDF form when the user request a PDF form.

Figure No.: 10 PDF Report

LIMITATIONS

- Not prevent incidents by themselves.
- Administration Required.

FUTURE SCOPES

The features which are mentioned in this project can be implemented in the following products:

A. Next-Generation Firewall
B. Web-Application Firewall
C. Intrusion Detection System
D. Web and Email Gateway
E. Cloud Security

CONCLUSIONS

A vulnerability scanner developed in this project is an application that is used to scan the network and generate a report when the vulnerability is identified. It is a web-based application which deals with important aspects of security i.e. Network Vulnerability Scanning.

In Vulnerability Scanning, the data which are acquired from the network scan and the output will be produced based on raw results. It gathers a list of vulnerabilities from the Network Devises.

The project performs functions with NMAP tool and various open-source of the database like exploit-DB, OpenVAS, OVSDB, ScipvulDB, SecurityFocus, SecurityTracker, xforce, etc., and also web-based GUI develops in python. The scanning can be done automatically or a schedule can fix by the admin. The result will detect the vulnerabilities and generate a report automatically.

ACKNOWLEDGEMENT

We would like to thank our Head of the Department, Prof. Kamlesh Jetha, Our Project Co-ordinate Prof. Ashok Kalal, and our Project Guide Prof. Sayali Kokane for their valuable advice and guidance.

REFERENCES

[1] Wenrui wang College of Electronic Engineering National University if Defense Technology, Hefei, China; Fan Shi; Min Zhang; Chengxi Xu; Jinghua Zheng, "A Vulnerability Risk Assessment Method Based on Heterogeneous Information Network"IEEE Access, 2020

[2] Guoyan Huang; Yazhou Li, Qian Wang; Jiadong Ren; Yongqiang Cheng; Xiaolin zhao, "Automatic Classification Method for Software Vulnerability Based on Deep Neural Network", IEEE Access, Volume:7,2019

[3] Huan Wang; Zhanfang Chen; Jianping Zhao; Xiaoqiang Di;DanLiu; Thar Baker; Sohail Jabbar, "A Vulnerability Assessment Method in Industrial Internet Of Things Based on Attack Graph and Maximum Flow", IEEE Access, Volume: 6, 2018

[4] Zhen Li School of Cyber Security and Computer, Hebei University, Baoding, China; Deqing Zou; Jing Tang; Zhihao Zhang; Mingqian Sun; Hai Jin, "A Comparative Study of Deep Learning-Based Vulnerability Detection System", IEEE Access Volume: 7, 2019

[5] Mao Yi; Xiaohui Xu; Lei Xu,"An Intelligent Communication Warning Vulnerability Detection Algorithm Based on IOT Technology", IEEE Access Volume: 7, 2019