Grenze International Journal of Engineering and Technology, June Issue

Analysis Techniques for Network Vulnerability Scanning in Ubuntu Linux Environment

Prof. Vinit A. Sinha[1] and Prof. Dr. Vilas M. Thakare[2]
[1]Department of MCA, PRMITR Badnera- Amravati M.S. India
Email: vinit.sinha84@gmail.com
[2]P.G. Department of Computer Science, SGBAU Amravati M.S. India
Email: vilthakare@yahoo.co.in

***Abstract*—Today's IT world belongs to open-source software, especially Debian class operating system i.e., Ubuntu. However, ubuntu take initiative to protect and stabilize server operating system in terms of providing security services to web hosting platform. With this dramatically change in hosting pattern, many threat actor start their offensive site for gathering information for destructive purpose. Ubuntu 20.04 LTS is launched by canonical for desktop and server platform. But while using this OS on network many high-end intruders intercept these network connections established between server and client system.**

This research work presents a study on analysis of vulnerability scanning using Nessus, Qualys and OpenVAS vulnerability scanner tools. By performing operations using these tools we implement CVSS (Common Vulnerability Scoring System), it is widely used for assessing vulnerability in class of complexity and severity. Research work summarize by calculating vulnerability under six different measures as Access vector, Related complexity, Authentication, Information confidentiality, Availability and Integrity. All these are result out as vulnerability analysis rating and score respectively. Research concluded with evaluation of vulnerability impact under ubuntu Linux environment.

***Index Terms*— Ubuntu, Linux, Nessus, Qualys, OpenVAS, CVSS.**

I. INTRODUCTION

Now a days Internet become widely spread up among the world, which comprehend security aspect according to defender as well as attacker side respectively. Network security had different branches as security point of view. So, security can be breach at any side by internal as well as external intruder. This research work explains the analysis techniques for vulnerability scanning is Linux environment, specially in Ubuntu. As Ubuntu is one of popular Debian class operating system based on open-source system. It has wide variety of flavours [1] (Kubuntu, Lubuntu, Kylin, Mate, Xubuntu etc.) for network administrators and users. For this growing use for application, security scanning is essential in term of vulnerability detection and assessment.

In this paper, we analyze network vulnerability using three popular scanners i.e., Nessus [2], Qualys [3] and OpenVAS [4]. Which result out as vulnerability rating score. We import vulnerability management program to detect, manage and restructure network vulnerability. Basic approach of this program is to scan network vulnerable assets to build strong defendable system in the field of cyber security. Following **Fig. 1** shows structure for network vulnerability assessment.

Grenze ID: 01.GIJET.8.2.507_1

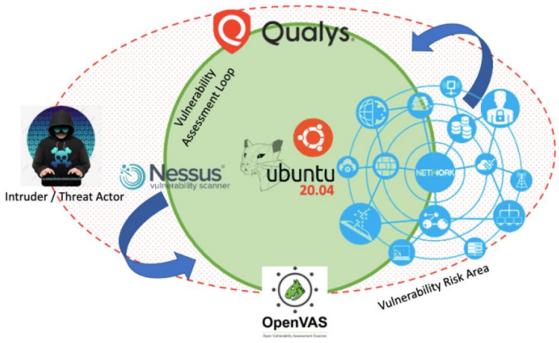

Fig. 1 Network Vulnerability Assessment Structure

It includes involvement of threat actor for searching of vulnerable system in mentioned network. As a part of network Ubuntu operating system supports Nessus, Qualys and OpenVAS scanner tools. Vulnerability assessment loop is continuously scanning any intruder attack using above mentioned tools individually.
This paper is organized as Section 2 represents related work, which gives details information about literature survey and their finding out. Section 3 briefs about methodology and technique used for analysis of vulnerability related to network. Section 4 express implementation technique and measuring terms of vulnerability scanning using three mentioned scanner tools. Section 5 generates evaluation report regarding network vulnerability and Section 6 conclude our research works, which include future scope for scanning vulnerabilities in cloud network.

II. Related Work

For analyzing network vulnerability, we perform survey on different quality literatures as Júnior et. al (2018) [5] described application of distributed firewall for getting solutions on intrusion detection or vulnerability assessment. Ajiya et. al (2019) [6], evaluates performance differences of IPsec network in Debian Linux environment. They use encryption algorithm to encrypt data for protection from intruder or unauthorised person. Levitin et. al (2018) [7] focuses on data vulnerability in cloud network. They suggest use of random server allocation method to get balance data security over network. Pandi et. al (2020) [8], describes threat model STRIDE to detect and analyse threat circumstances around network vulnerabilities, which includes cheating firewall, DDOS attack, Credit card fraud and use of botnet to control over server. Ganji et. al (2018) [9], explains suitable need for Linux infrastructure for security policies regarding network vulnerabilities. They performed analysis of security techniques and evaluates parameter for existing system security. Li et. al (2019) [10], explains network security awareness regarding large scale network exploration. They designed framework into five stages as factor acquisition, model representation, measurement calculation, solution analysis and prediction according to situation. This help to analysis vulnerability in suspected network.

III. Methodology

For analysis of vulnerability scanning, we follow Vulnerability Management Life Cycle (VMLC). As shown in following Fig. 2.

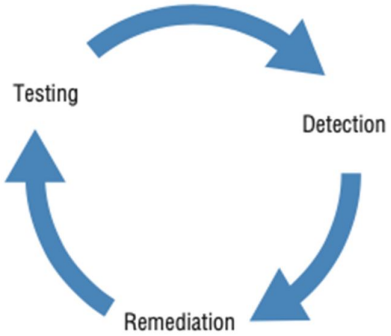

FIG. 2 – VMLC

VMLC describes initial scanning of vulnerability among organization that develops work flow for setting priority of vulnerabilities. We use three dedicated scanners as Nessus, Qualys and OpenVAS at user end side. Following **Fig. 3** shows Nessus vulnerability scan details.

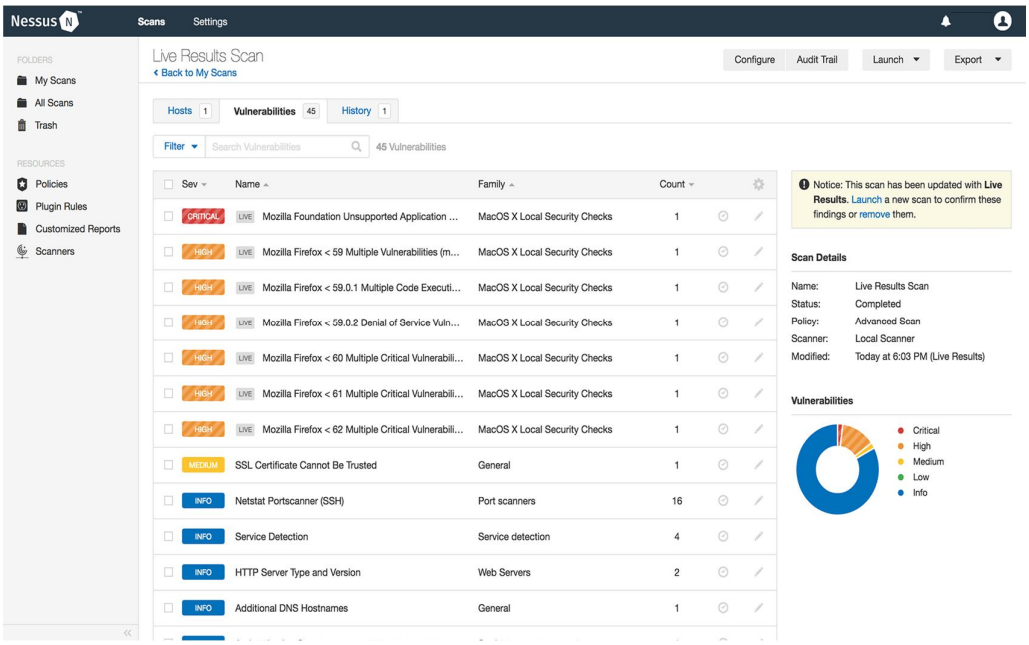

Fig. 3 – Nessus Vulnerability Scan Report

Above figure shows critical details about vulnerability in terms of general category as Low, Medium and High. It also explains SSH services of server that helps to provide support to weak encryption algorithms. By using Nessus scanner, we determine complexity of vulnerability in terms of SSH service support. Final section of vulnerability report generates solution on vulnerability related to information generated and explain how system admin and security professional solve the difficulties surrounded to suspected system.

Same way following **Fig. 4** shows Qualys scan reports regarding Open-Source SSL. Here we use web application management tool for FQDN (Fully Qualified Domain Name) scanning. As per above figure 4 shows, Qualys display status for New, Approved and Rouge domain name, where user can take action as per requirement.

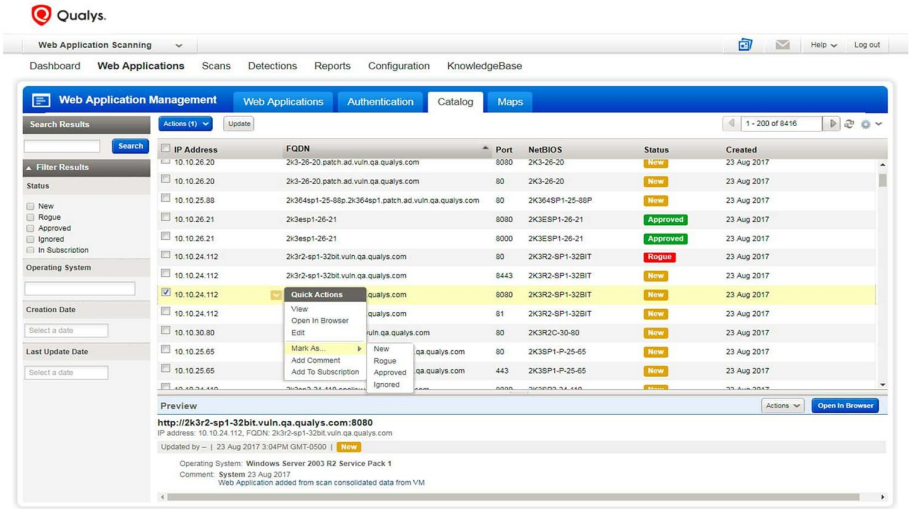

Fig. 4 - Qualys Vulnerability Scan Report

Similarly, we used OpenVAS scanner as Qualys, the details architecture for OpenVAS vulnerability manager is shown in **Fig. 5.** It shows four components of vulnerability assessment system. The first one is OpenVAS server, used for scanning network system also known as target system. This component is primarily used for network traffic initialization. Second component is OpenVAS client, used for establishing GUI connection with server. Third component is OpenVAS Feed (NVT) known for Network Vulnerability Test. Whole work of scanning is based on signature files in the form of Plugins. These are used for updating network from repository sever. The last component is NASL known for Nessus Attack Scripting Language, which is used for importing features from Nessus scanning tool to OpenVAS server.

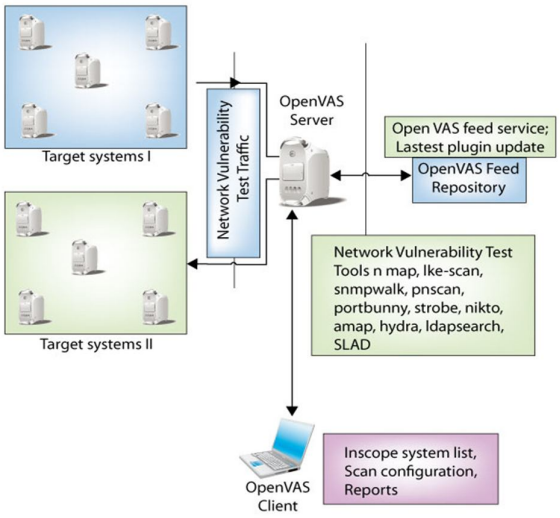

Fig. 5 Architecture Of Openvas

IV. Implementation

For analyzing severity of vulnerabilities, we implement CVSS (Common Vulnerability Scoring System). Purpose behind this approach is to score each vulnerability on different scale factor also known as measures. Following **Table 1.** Shows six different measures scored by CVSS.

TABLE I. CVSS MEASURES DETAILS

SN	Measure details	Purpose
1	Access Vector	This describes the way of attacker to exploit vulnerability.
2	Access Complexity	It describes the hardness of exploit vulnerability
3	Authentication	This describes the obstacles for attacker, which is to be clear for exploitation of vulnerability
4	Confidentially	It describes information type, which is to be disclosed by attacker after successful exploitation.
5	Integrity	This describes the type of information, which is to be altered by attacker after successful attack.
6	Availability Metric	It describes type of interruption occurred when attacker successful exploits vulnerability.

V. Result and Evaluation

We analyze the vulnerability scanning from three different scanners as Nessus, Qualys and OpenVAS on the basis on CVE (Common Vulnerability Exposure). The following **Fig. 6** shows evaluation of these scanning tools related to vulnerability on basis of user reviews up to year 2021.

Above figure explains that how Nessus take much efficient lead as it supports high rated operating system like Ubuntu and others. Nessus has positive side over Qualys and specifically on OpenVAS in the area of setting up and Quality of support. We used Nessus on platform on Ubuntu 20.04 LTS as shown in Fig. 3 for port scanning and it support for cross platform security check also.

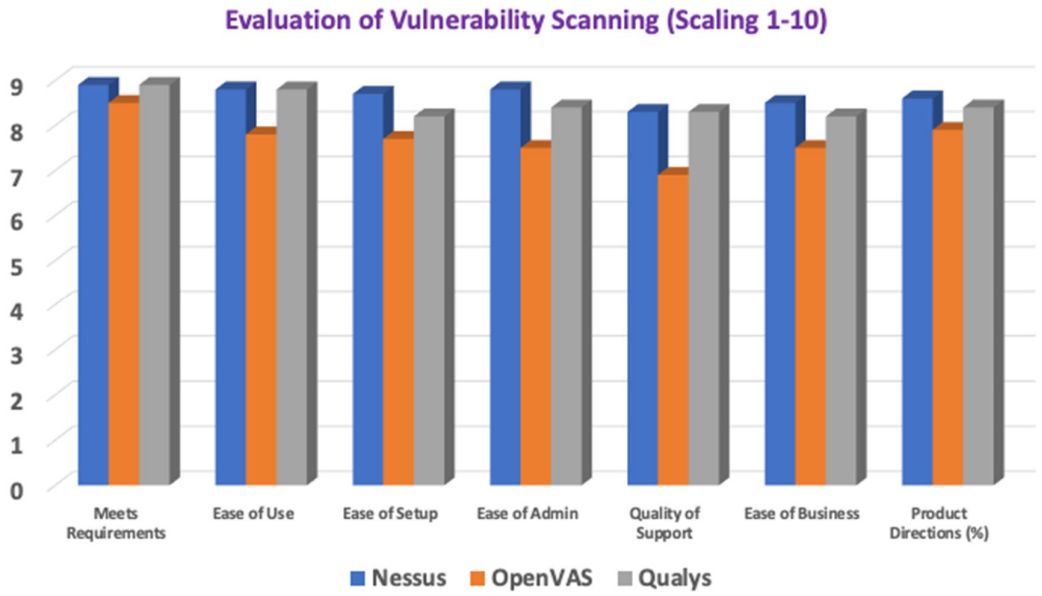

Fig. 6 Evaluation of Vulnerability Scanning (Rating)

VI. Conclusion and Future Scope

In this paper, we focused on different scanning techniques for network vulnerability on Ubuntu 20.04 platform. After performing evaluation of Nessus, Qualys and OpenVAS, we found Nessus scanning technique is more effective for managing network traffic on basis of user reviews. As Nessus support both virtual and physical environment, it become more flawless and harden for intruder as well as threat actor. In future perspective, we plan to build strategy for scanning vulnerabilities on cloud servers using Ubuntu Pro for cloud.

References

[1] Ubuntu. 2022. *Ubuntu flavours | Ubuntu*. [online] Available at: <https://ubuntu.com/download/flavours> [Accessed 9 January 2022].
[2] Tenable®. 2022. *Nessus Product Family*. [online] Available at: <https://www.tenable.com/products/nessus> [Accessed 9 January 2022].
[3] Qualys.com. 2022. *Solutions*. [online] Available at: <https://www.qualys.com/solutions/> [Accessed 9 January 2022].
[4] Openvas.org. 2022. *OpenVAS - Open Vulnerability Assessment Scanner*. [online] Available at: <https://www.openvas.org/> [Accessed 9 January 2022].
[5] Costa Júnior, Edmilson P. da, Carlos Eduardo da Silva, Marcos Pinheiro, and Silvio Sampaio. 'A New Approach to Deploy a Self-Adaptive Distributed Firewall'. *Journal of Internet Services and Applications* 9, no. 1 (December 2018): 12. https://doi.org/10.1186/s13174-018-0083-6.
[6] A., A., U. S., and Jerome M. 'Performance Evaluation of IPSEC-VPN on Debian Linux Environment'. *International Journal of Computer Applications* 181, no. 45 (15 March 2019): 39–44. https://doi.org/10.5120/ijca2019918592.
[7] Levitin, Gregory, Liudong Xing, and Yuanshun Dai. 'Co-Residence Based Data Vulnerability vs. Security in Cloud Computing System with Random Server Assignment'. *European Journal of Operational Research* 267, no. 2 (June 2018): 676–86. https://doi.org/10.1016/j.ejor.2017.11.064.
[8] Pandi (Jain), Gayatri S, Saurabh Shah, and K.H. Wandra. 'Exploration of Vulnerabilities, Threats and Forensic Issues and Its Impact on the Distributed Environment of Cloud and Its Mitigation'. *Procedia Computer Science* 167 (2020): 163–73. https://doi.org/10.1016/j.procs.2020.03.194.
[9] Ganji, Hamid Reza, and Kiarash Aghakhani. 'Provides a New Way to Enhance Security in the Linux Operating System'. *Emerging Science Journal* 2, no. 5 (4 November 2018): 295. https://doi.org/10.28991/esj-2018-01153.
[10] Li, Yan, Guang-qiu Huang, Chun-zi Wang, and Ying-chao Li. 'Analysis Framework of Network Security Situational Awareness and Comparison of Implementation Methods'. *EURASIP Journal on Wireless Communications and Networking* 2019, no. 1 (December 2019): 205. https://doi.org/10.1186/s13638-019-1506-1.