Volume 7, Issue 5, May 2017 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Comparative Analysis of Detecting Vulnerability in Network Systems

Sandeep Kumar Yadav*
M.Tech. Scholar Dept. of CSE
RKDFIST Bhopal (M.P.), India

Daya Shankar Pandey
Asst. Professor, Dept. of CSE
RKDFIST Bhopal (M.P.), India

Shrikant Lade
Asst. Professor, Dept. of CSE
RKDFIST Bhopal (M.P.), India

Abstract— In the age of fast internet and global communication systems, computer security is a big challenges for any public or private organization. There exists many more threats to such organization and required some top level of security in the organization for securing company's critical information. Therefore each individual computer system is very important to secure them because a single system is responsible to compromise whole organizations network. To verify the security checks and strengthen the organizations network, a vulnerability assessment of the whole organizations network must be performed regularly. Vulnerability scanners are useful to discover security flaws within each individual system as well as whole network also. If already known security flaws are not fixed then an attacker might try to exploit vulnerability and gain information what they wants. This paper focuses on the different vulnerability scanners and their methods to discover various vulnerabilities available in the networks or remotely connected host system and make a comparative analysis on the bases of their ability to detect different flaws.

Keywords— Threat, Vulnerability, Vulnerability Scanners, Security flaw, Port scanning.

I. INTRODUCTION

With exponential growth of advancement in information technology, the security of those system has more serious concern. Commonly most of the software developing industries are not aware of various security misconception that is automatically exist in the system due to programming languages because their intention to make the good software that runs smoothly and gives desired output without considering the security flaws; to provide the safety and security of each individual, it is very much significant to plan new strategies and methodologies [01] that will consider the security breaches to which the user is prone to. Not only the software developed with flaws makes the user vulnerable to attacks, most often network also becomes a key factor by compromising the security aspect of the users.

Assessing and eliminating the vulnerabilities requires the knowledge and deep understanding of these vulnerabilities or security flaws. A vulnerabilities in a system's security that can lead to attackers exploiting the system in a different manners that the designer intended [02]. Many more methods have been implemented to identify these vulnerabilities and different approaches to fix these vulnerability as well. Some of them are attack graph generation method, static analysis methods to discover the vulnerabilities is quite popular and prominent today. They play a major role to design the safety model and generate the attack graphs [03-07].

In this paper involves the study of various vulnerability scanners, scanning the organization's network, applications and host systems on the remote locations as well. Also analysing the results of various scanners on the bases of their capability to detect potential vulnerabilities.

Section 2 shows the basic structure of vulnerability scanner and division of major components existed in vulnerability scanners and further Section 3 shows the study of two most popular vulnerability scanners such as Nessus [04] and OpenVAS [05] and in Section 4 presents the study of comparative analysis of Nessus and OpenVAS scanning results and try to develop an idea that will help to provide the secure network for an organization.

II. ARCHITECTURE OF VULNERABILITY SCANNERS

Vulnerability scanning means scanning of the systems, network devices and applications which works on front to external worlds or scanning the internally hosted system to find the security flaws on them. There are number of different approaches to understand the basic framework of Vulnerability scanners [6]. Vulnerability scanners have a database of already exposed vulnerabilities; with reference to known vulnerability, vulnerability scanner performs the security verification on remote host.

Vulnerability scanner is break down into four major modules; such as user interface, scan engine, scan databases, report generation module.

- **User Interface:** This is the part where user interact with scanner system to execute or configure their scan. This interface can be a Graphical user interface (GUI) or a command line interface (CLI) or both.
- **Scan Engine:** The scan engine part performance the security validation based on latest installed plug-ins and payloads. User can perform the single system scan or multiple host scan at a single time also.

- **Scan database:** The vulnerabilty database stores all the scan results prviously performed. The scan database contains all the information related to port, packet type, services, a potential path to exploit, latest attack techniques etc. This may also contain the different techniques to patch the vulnerabilites and have detailed information of CVE-ID mapping(Common Vulnerability and Exposures)[08].

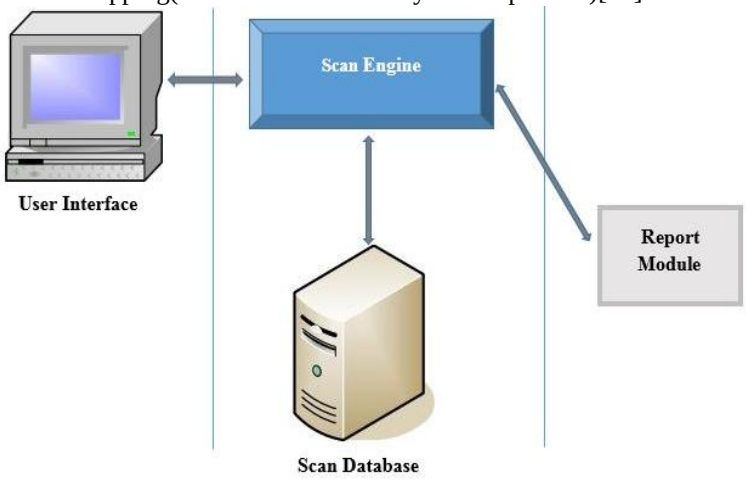

Figure 1: Components of vulnerability scanner

- **Report Module:** The report module generate the different types of report such as a detailed report, a list of vulnerabilities, a graphical report with their recommendation to mitigate the detected vulnerabilities.

III. VULNERABILITY SCANNERS

A. NESSUS

Nessus is one of the most popular vulnerability scanners. It is used for both authenticated and unauthenticated vulnerability scans. It is suitable for both internal and external network scans. It is also performed the scanning of web applications. The main advantage of this tool is to perform the multiple host scanning at once. The detected vulnerability is categories into four types based on their severity levels- High, Medium, Low and Informal.

A detail scan result is automatically saved as the scanning of desired host is completed. The results are expressed into two different forms- first is vulnerabilities by plug-ins and second is vulnerabilities by host. Firstly classifies the all detected vulnerabilities during scan, and then it shows the list of all hosts affected by these vulnerabilities. By using the detailed generated scan report, issues can be addressed easily. Then afterward finds the all host in scanning phase and their existed vulnerabilities.

This report will help the security administrator to address the distinct issues associated with individual host and overall networks. Its real time active scanning provides continuous network evaluation and bridges the security gaps. Nessus scan result can be exported in different formats which you desired like PDF, HTM, and CSS etc. Nessus is works on the principle of client-server architecture. Each scan session is managed by client and scan test is done on the servers.

Figure 2 shows the scan results for host system with IP address 192.168.1.3 using Nessus. It shows the all the vulnerability present on the system according to their severity levels as high, medium and low.

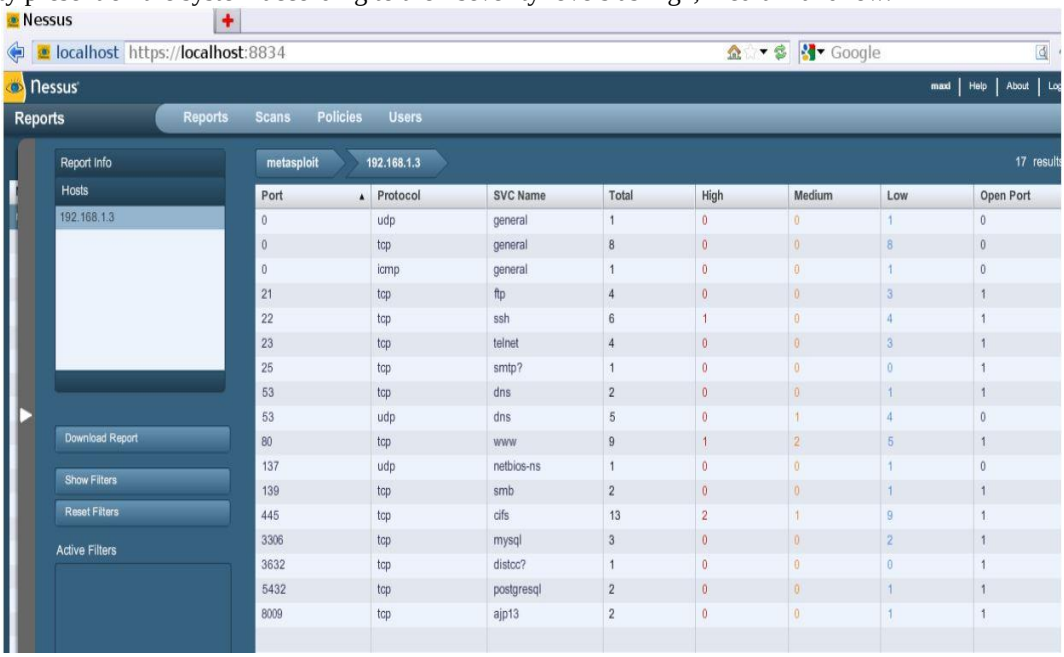

Figure 2: Nessus vulnerability scanning details for host with IP adress 192.168.1.3

B. OpenVAS

The Open Vulnerability Asssessment System(OpenVAS) have the features of sevral services and tools makes it very powerfull to scanning and provides the significant vulnerability managemnt solution. OpenVas is freely available as it is open source. OpenVAS have a web interface and also works on the principle of clien-server architecture. The client component is responsible for configuring the scan and access the report while server component is used for scheduling the scan and managing the plugins.

There are some important features of OpenVAS inclues:

- **Authenticated scan:** In authenticated scan user can supply a user id and password of target host to perform the scan after log in and list the vulnerabilities of installed components such as Adobe reader, wireshark etc.
- **Compatible for customized plugin:** The OpenVAS is fully compatible with customized plugins where user can create a plugin and configure the scan for Nessus Attack scripting Language (NACL).
- **Export of report:** The OpenVAS scanner have the features to export the scan result in different formats as like in HTML, XML, TXT, and PDF.
- **Act as port scanner:** The OpenVAS scanner have also the options for port scanning [11]. It performs TCP scan, SYN scan, IKE-scan to locate IPSec, VPN scan etc.
- **Safe checks:** OpenVAS have also the safe checks options. In the safe check mode, the scanner will depends on the banners of the remote host instead of sending all the payloads to the remote host. This option is useful in case where old host crash during the default scan.

Figure 3 shows the scan result using OpenVAS with same target address. OpenVAS detect the total 48 vulnerabilities and also there is 25 vulnerability with very high risk and 23 have moderate risk.

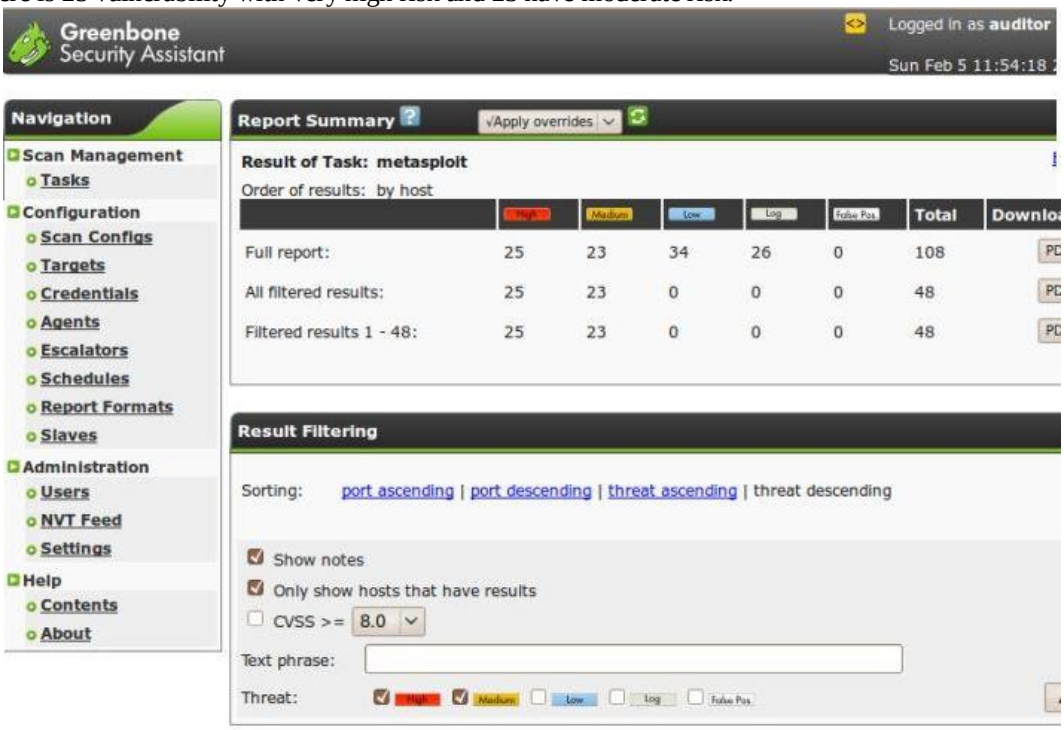

Figure 3: Vulnerability detcted by using OpenVAS

IV. COMPARATIVE ANALYSIS OF VULNERABILITY SCANNERS

In this section, two vulnerability scanning tool are analyzed on the basis of their specific fetures. Table 1 shows the list of specific features of Nessus and OpenVAS and clearly it gives the idea how Nessus working differs from the OpenVAS tool [10].

Table I Features comparision of Nessus and OpenVAS

Nessus	OpenVAS
Increased number of plugins	Lowest number of plugins
Ease of installation (on All in Windows)	Installing Multiple Components And, therefore, more difficult
Clear environment, good Aspect (flash environment)	Surroundings with too many Elements, lousy aspect
Configuration with few Options, limited	Configuration with many Options, custom-made

Unscheduled scans	Scans can be programmed
Reduced equipment scanning	Scan unlimited computers
It can not prevent and correct false positives	It prevents false positives and Serves to add annotations
Can not find all Vulnerabilities on the prepared equipment	Find virtually all Vulnerabilities in the Equipment prepared
Scan with credentials Better than without them (whitebox)	Do not see the scan option with Credentials
Very complete reports With reference to the BD vulnerabilities, Dates, patches, exploits, etc.	Reports less colourful, but very Effective and with all the details, Dates, patches, exploits, etc.
Export formats of High results Compatibility (metasploit, Excel), NBE, XML	Identical export formats to Nessus (pdf, NBE, XML, etc.) More Options
Prepared for audits PCI-DSS	Prepared for ISO 27001 and PCI-DSS audits credit)
No event escalation	Has event escalation Configurable
Free for personal use, Limited version	Free always full version

In figure 2 we observe that Nessus detcted the total 53 vulnerabilities, where 4 are very critical with associated high risk and also 4 are moderate risk and 45 are just informational; while in case of OpenVAS figure 3 depicts that after excluding logs and and false positive, OpenVAS detected total 48 vulnerabilities, where it categoriese 25 are critical and 23 are moderate level for a particular host system. Table 2 shows the comparative outputs to detect the vulnerability after using Nessus and OpenVAS.

Table 2 Comparision Of Scan Results

	Nessus	**OpenVAS**
Total vulnerabilities detected	53	48
Vulnerabilities with high severity level	4	25
Vulnerabilities with medium severity level	4	23
Vulnerabilities with low severity level	45	0

V. CONCLUSIONS

There are number of techniques available to present the list of vulnerabilities present in the web application or remote host system. Regular vulnerability assessment of organization plays a significant role to secure the network. Our observation in this paper shows that different scanners detect so many other types of vulnerabilities and collective approach is very useful to fix the issues. This paper addressed the various techniques with different tools and analyses their results. We come to a conclusion that a tool have the capability to detect the vulnerabilities and shows their level of severity.

Nessus has so many features exist within it and hence it can be integrated with the other tool that work differently and produces more efficient results. These steps may more beneficial for network administrator to fix the overall issues. In future our work is to integrate more scanning tools to gives the better performance and takes less time.

REFERENCES

[1] 1. P. Zhang, J. Shang, and Z. Liang, "Application of Multi-Agent Model in Vulnerability Detection System", IEEE, First IEEE International Symposium, 2007.

[2] 2. Golnaz Elahi, Eric Yu, and Nicola Zannone, "Security Risk Management by Qualitative Vulnerability Analysis", IEEE, Third International Workshop on Security Measurements and Metrics, 2011.

[3] 3. Xia Yiming, 2006. "Security Vulnerability Detection Study Based on Static Analysis," Computer Science, 33(10), pp. 279-283, Symposium, 18-22 May 2008, pp. 143-157.

[4] Nessus Open source vulnerability scanner project, http://en.wikipedia.org/wiki/Nessus (software), 10-07-2016.

[5] Open Vulnerability Assessment System (OpenVAS), http://www.openvas.org/about.html, 10-04-2017.

[6] R. Yadav, R.N. Verma and A.K. Solanki, "An Improved Model for Analysis of Host Network Vulnerability", International Journal of Computer Applications (IJCA), pp. 12-16, Vol. 148, No.13, August 2016.

[7] Peng Li and Baojiang Cui, December, 2010, "A Comparative Study on Software Vulnerability Static Analysis Techniques and Tools", in Proceedings of the IEEE International Conference on Information Theory and Information Security (ICITIS), IEEE International conference, 2010.

[8] Common Vulnerabilities and Exposures (CVE), https://cve.mitre.org, 15-03-2017.
[9] http://www.tenable.com/products/nessus-vulnerability-scanner, 10-04-2017.
[10] Nilima R. Patil and Nitin N. Patil, April, 2012. "A comparative study of network vulnerability analysis using attack graph", in Proceedings of National Conference on Emerging Trends in Computer Technology (NCETCT-2012.
[11] J. Padhye, V. Firoiu, and D. Towsley, "A stochastic model of TCP Reno congestion avoidance and control," Univ. of Massachusetts, Amherst, MA, CMPSCI Tech. Rep. 99-02, 1999.
[12] Fyodor, Port scanning techniques, http://nmap.org/book/man-port-scanning-techniques.html, 18-12-2016.

