Evaluation and Analysis of Vulnerability Scanners: Nessus and OpenVAS

Sowmyashree A[1], Dr. H S Guruprasad[2]

[1,3]M.Tech, Computer Network Engineering
[2,3]Professor and Dean Student Affairs
[3]Dept. of ISE, B.M.S College of Engineering, Bangalore, Karnataka, India.

---***---

Abstract - *In today's world technology is growing rapidly, the development of software and systems have become more advanced and complex. Because of high speed internet and world communication systems, providing network security is the biggest challenge of any personal or public organization. Their exists additional threats to such organizations so they require top-level network security for securing the company's critical information and it is their responsibility to make sure their products have high security so that the client, may not fall into the victim of data theft. System security is one of the prime concerns when working over the web, LAN and different techniques. Network security safeguards computer systems from unwanted intrusions and reduces the risk of falling victim to data theft. Vulnerability assessments must be performed regularly to make sure the network is stable. Vulnerability scanners detect the security flaws within individual systems. Detecting the vulnerabilities, ensures that information transmission in the network are secure. Vulnerability scanners are used to find the flaws in the network, diagnosis, and provide solutions to solve the problem. This paper focuses on security for Ubuntu OS. To enhance the security of the Linux operating system we have explored a few security tools like Nessus, OpenVAS.*

Key Words: Linux, Network Security, Vulnerability assessment, Vulnerability scanners, Nessus, OpenVAS.

1. INTRODUCTION

With the exponential development of information technology, providing security to those systems and software has become major concern. Most of the software developing corporations don't seem to be conscious of numerous security flaws that automatically exist due to programming languages because their goal is to develop a Software that runs easily and provides expected output, without considering the security imperfections. Not only software developed with flaws make the user vulnerable to attacks, but most often the unsecured network is also an important concern. Analyzing and resolving security flaws or vulnerabilities needs in-depth information for understanding security flaws and vulnerabilities.

As technology is growing quicker, the development of programming and development of software and systems became additional advanced. There's a large risk related to unauthorized access to confidential knowledge and maintaining the integrity of the information. Step by step new hacking activities is found. Therefore, it's very necessary to acknowledge the vulnerabilities and install the safety patches for those vulnerabilities. Since most corporations are increasingly dynamic in nature, their workers are accessing IT resources domestically and remotely, henceforward the necessity for securing the network is important. This action turns into the very best priority for Organizations these days.

Ubuntu is Linux distribution OS. Linux works very well as a server operating system; such huge numbers of organizations may utilize it for this reason. Like other distributions, Ubuntu has limited security. Most network ports are closed by default in Ubuntu to prevent hacking. In order to prevent attackers to gain access to systems through the network, it is important to implement security measures and practices to secure information on the machine. Security is one of the prime concerns during the use of computer systems.

Security is a process of implementing the measures to securely protect and safeguard data. Vulnerability scanners are used to find flaws in network, diagnosis, and provide solutions to resolve the problem. Many security tools are available to discover the vulnerabilities with completely different functionalities and options. There are many scanning tools to discover the vulnerabilities with completely different functionalities and options. This paper focuses on security for Ubuntu OS by using security tools like Nessus, OpenVAS.

1.1 Network Security

Network security is a measure that secures computer systems within network. Network security helps in protecting the computer systems within the network from unwanted intrusions and reduces the chances of falling victim to data theft.

What happens when we don't use these tools?

Vandalism (Misleading of data) can occur: By planting the incorrect data, Customers may feel misled and company's integrity will be questioned. Just in case the client faces any security-related problems, the corporate is going to be accountable for it which might cause revenue loss. Value of the corporate decreases and the company is going to be responsible for security problems faced by purchasers. To provide the product with complete security measures or to enhance the security of the product network security tools are used. By using network security tools, we can find the security holes of the product before the information is misused by hackers. Protecting client data is an integral part of the business.

1.2 Vulnerability Scanning

It is a process that detects and diagnosis weakness on target systems. If an attacker needs to hack your local network, the first process they go for is vulnerability check, next process they go for is a penetration test. There are many scanning tools available to conduct vulnerability test, when they perform vulnerability scan it starts scanning various devices in the network to detect any holes, open ports and software which are outdated with known vulnerabilities or weak passwords on devices. If the attacker found some vulnerabilities with devices, then they go for a penetration test to find a way to exploit. Testing is just a two-step procedure, vulnerability scanning to scan and detect the vulnerabilities, Penetration test verifies the issue is exploitable.

To improve the security features of Ubuntu OS. We are investigating the security tools and detect vulnerabilities on the devices and resolve them.

The below mentioned tools helps in finding security patches, issues, vulnerabilities of the Ubuntu OS. We have performed the security analysis on Ubuntu devices using these tools.

- Nessus is a remote security scanner which scans the devices using IP address, alerts when the vulnerability is discovered.
- OpenVAS is a Vulnerability scanner which detects the vulnerabilities in network and devices.

It is necessary to perform Vulnerability assessment regularly to make sure the network is stable without any security gaps. Vulnerability scanners detect the security flaws within individual systems. Vulnerability scanners are used to find the flaws in the network, diagnosis, and provide solutions to solve the problem. This paper focuses on security for Ubuntu devices. To enhance the security of the Linux operating system we have explored a few security tools like Nessus, OpenVAS.

2. ARCHITECTURE OF VULNERABILITY SCANNER

Vulnerability scanners scan for the security flaws in the network and host devices. The following Fig 1 show the architecture for vulnerability scanning. Both the server and client should be in the same network to perform scanning by providing IP address to server and by configuring scan details on the server-side user interface.

Vulnerability scanner has Four parts such as:

- Scanner's Web UI
- Scan Engine
- Database
- Scan Report

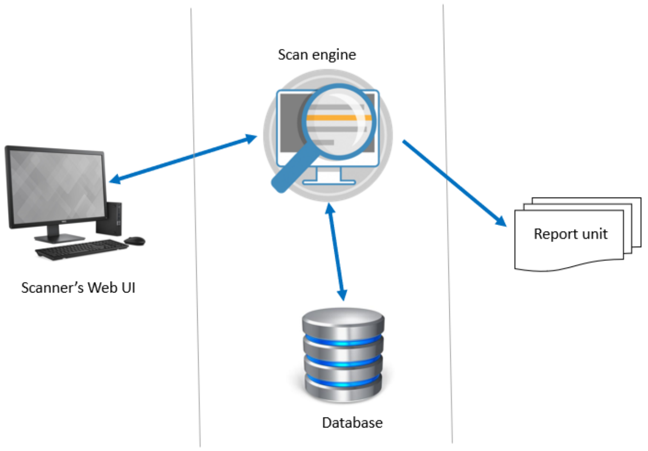


Fig - 1: Represents the Architecture of Vulnerability Scanner

1. ***Scanner's Web UI:*** Both Nessus and OpenVAS have User Interface where the client can interact with scanner system to perform and configure the scan.

2. ***Scan Engine:*** Scan Engine is a vulnerability plugin are installed and user can perform the scan for single host or multiple hosts simultaneously.

3. ***Database:*** It includes previously exposed vulnerabilities to test against given targets. Vulnerability database include all the information related to ports, services and lasted vulnerabilities details with CVE-ID and so on.

4. ***Scan Reports:*** After the scanning is completed the detailed report will be generated in text, pie chart, world cloud and graphical representation showing the severity of vulnerabilities. Reports incudes the procedure to resolve the vulnerability issues.

3. ARCHITECTURE OF VULNERABILITY SCANNER

3.1. Nessus:

It is a Vulnerability Scanner which scans the devices in the network and discovers any vulnerabilities that might be used by attackers to get access to a device which are connected to network. Nessus Attack Scripting Language (NASL) is the language used in Nessus, an easy language that describes security flaws and possible vulnerabilities. Nessus is bought with the aid of Tenable Security. Nessus also performs scanning the Web applications, Mobile devices and so on. It also provides configurating auditing and compliance check. Nessus works on Client-Server Architecture. Nessus is a remote tool because it may not be installed on the device which need to be scanned.

Nessus tool can scan multiple devices simultaneously. The Vulnerabilities which are detected are classified into 4 types based on severity- Informal, Low, Medium and High.

At the Nessus user interface (Client side), before launching the scan we must create and configure the scan details. Nessus Server starts listening to the incoming connections from Client to perform specific scan. Nessus perform its scan by testing the host with plugins to detect vulnerabilities present in the network. Nessus performs its scan by identifying the devices operating system and host discovery, Open ports and software components which are vulnerable to attack. If the Scan is finished, click on Vulnerabilities to see the detailed information. Report will be generated in various formats like pdf, xml, html and so on. The system administration can use the report to resolve security gaps.

3.2. OpenVAS:

The Open Vulnerability Assessment System scanner provides multiple services, provides a remarkable vulnerability management solution. OpenVAS is an open-source scanning tool. OpenVAS works on Client-server architecture. The OpenVAS web UI is the client component where we can configure scan, launch the scan, and review result document. We can perform scan scheduling and managing plugins. The communication is secured through SSL. OpenVAS is a remote scanner because it is not necessary to install on every system, we perform the scan. Instead, it can be installed and configured in one device on a network.

The scanner provides the security testing of IP addresses. Firstly, it will start scanning to find any open ports and services available in the network. After discovering the listening services, these services are scanned against large database which includes more than 53000 NVT checks. The report is generated which includes detailed information related to each vulnerability.

NVT is a Network Vulnerability test. These are directed utilizing modules that are created in the NASL code. The NASL is an inheritance of its unique Nessus code base. Nessus Attack Scripting Language is utilized to perform vulnerability tests originally created in 1998. NVT's are updated to the database on weekly basics whereas others updated when a new vulnerability is discovered.

4. EXPERIMENTAL SETUP TO TEST VULNERABILITY SCANNERS

To perform the security analysis, network setup is made for testing vulnerability scanners. This testing environment consist of Four Client (Ubuntu) devices are used as a host device to perform scan. Both Nessus and OpenVAS are installed in the same Linux device. Both the server and client should be in the same network to perform scanning by providing IP address to server and by configuring scan details on the server-side user interface.

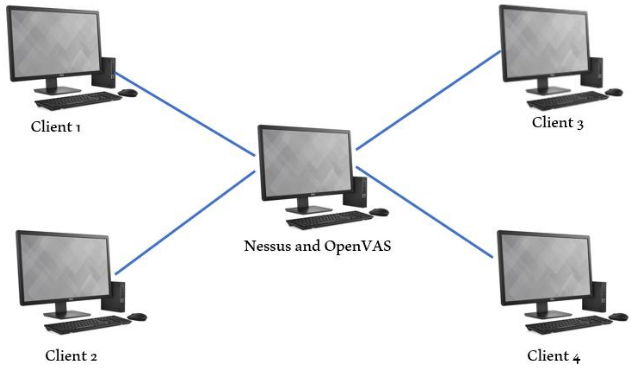


Fig - 2: Represents the Network setup for testing Vulnerability scanners

The Workflow to perform scan through Vulnerability Scanners:

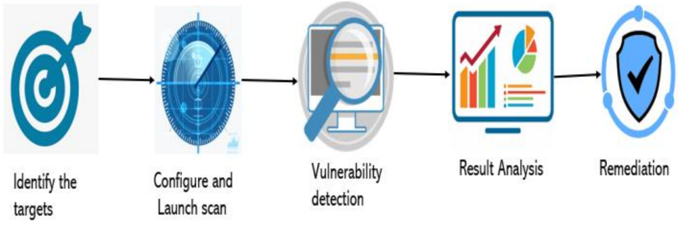


Fig - 3: Workflow of Vulnerability Scanners

1. Identify the host to perform Vulnerability scan in the network.
2. Once the Vulnerability server is ready, Configure the scanning policies and perform the scan.
3. After the scan is completed, if any vulnerability detected it will show on its web UI, admin can see the vulnerabilities which cause flaws.
4. A report will be generated which includes detailed information about Vulnerabilities and the solution to resolve them.
5. Remediation and Implementations made to resolve the vulnerable issues.

5. EXPERIMENT RESULTS AND COMPARATIVE ANALYSIS OF VULNERABILITY SCANNERS

5.1. Nessus

To perform the vulnerability scan, navigate your browser to https://localhost:8834

➢ Steps to perform Scan in Nessus

The steps of scan is shown in the image below.

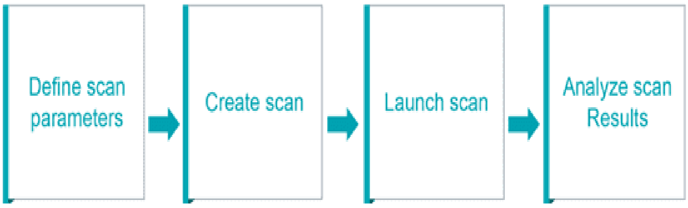


Fig - 4: Steps to Launch scan

The below steps represent the Nessus process.

Step 1: Nessus retrieves scan settings and configure the security policies to perform scan

Step 2: Initially it starts will go for host discovery to find the hosts that are up. The protocols used are UDP, ICMP, ARP and so on.

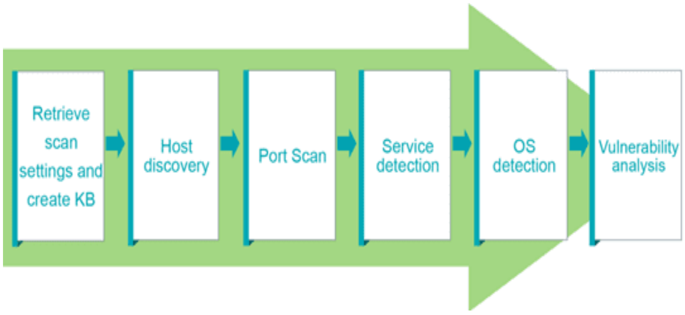


Fig - 5: Series of steps Nessus perform

Step 3: Once host discovery is done, it performs port scanning for each hosts which are up. We can define specifically which ports to be scanned.

Step 4: It perform service detection by running on each port on host.

Step 5: Nessus checks for OS discovery

Step 6: Nessus runs host against a Vulnerability database to detect the vulnerabilities present in the host system. The image above summarizes these steps.

Figure 6 represents the scan details of client using Nessus. It displays all the vulnerabilities detected in the system with their severity levels. Vulnerabilities tab includes the detailed information of Vulnerabilities detected and provides the solution to resolve few vulnerabilities.

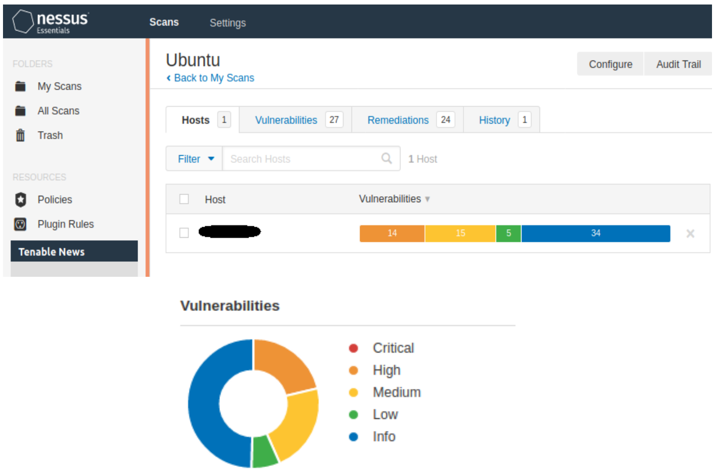
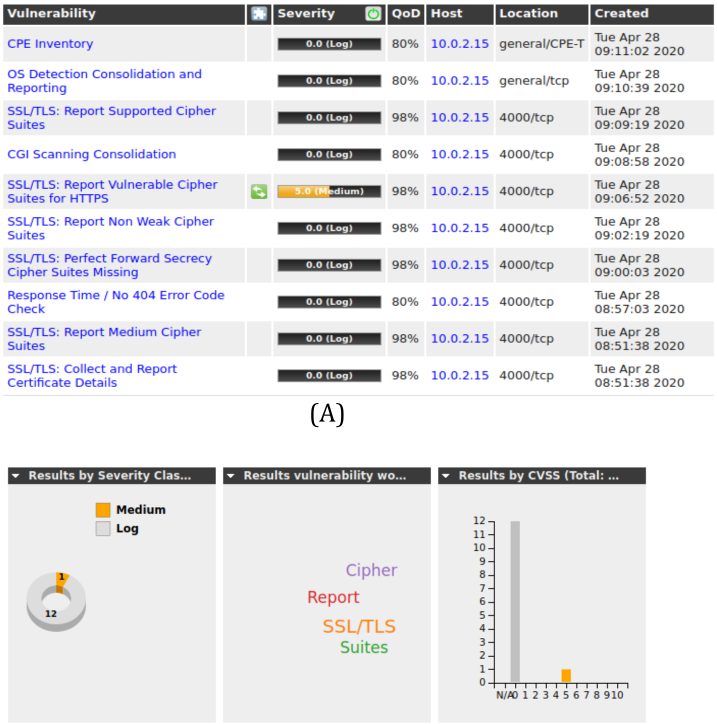


Fig – 6: Scan results using Nessus

5.2. OpenVAS

To perform the vulnerability scan, navigate your browser to https://localhost:4000

Figure 7 represents the Scan details of client using OpenVAS. It displays all the vulnerabilities detected in the system with their severity levels. Vulnerabilities report includes the detailed information of Vulnerabilities detected and provides the solution to resolve few vulnerabilities.



Vulnerability		Severity	QoD	Host	Location	Created
CPE Inventory		0.0 (Log)	80%	10.0.2.15	general/CPE-T	Tue Apr 28 09:11:02 2020
OS Detection Consolidation and Reporting		0.0 (Log)	80%	10.0.2.15	general/tcp	Tue Apr 28 09:10:39 2020
SSL/TLS: Report Supported Cipher Suites		0.0 (Log)	98%	10.0.2.15	4000/tcp	Tue Apr 28 09:09:19 2020
CGI Scanning Consolidation		0.0 (Log)	80%	10.0.2.15	4000/tcp	Tue Apr 28 09:08:58 2020
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS		5.0 (Medium)	98%	10.0.2.15	4000/tcp	Tue Apr 28 09:06:52 2020
SSL/TLS: Report Non Weak Cipher Suites		0.0 (Log)	98%	10.0.2.15	4000/tcp	Tue Apr 28 09:02:19 2020
SSL/TLS: Perfect Forward Secrecy Cipher Suites Missing		0.0 (Log)	98%	10.0.2.15	4000/tcp	Tue Apr 28 09:00:03 2020
Response Time / No 404 Error Code Check		0.0 (Log)	80%	10.0.2.15	4000/tcp	Tue Apr 28 08:57:03 2020
SSL/TLS: Report Medium Cipher Suites		0.0 (Log)	98%	10.0.2.15	4000/tcp	Tue Apr 28 08:51:38 2020
SSL/TLS: Collect and Report Certificate Details		0.0 (Log)	98%	10.0.2.15	4000/tcp	Tue Apr 28 08:51:38 2020

(A)

Results by Severity Clas...
Medium
Log
1
12
Results vulnerability wo...
Cipher
Report
SSL/TLS
Suites
Results by CVSS (Total: ...
12
11
10
9
8
7
6
5
4
3
2
1
0
N/A 0 1 2 3 4 5 6 7 8 9 10

(B)

Fig - 7: Vulnerabilities scan details(A), Results shown in graphical representation(B)

Benefits of OpenVAS is that when the false positive and false negative are discovered, Admin can evaluate the plugin to check why vulnerability is turned into flagged.

Results are shown in pie chart, World Cloud and graph representation. The report generated by these tools will assist the network and system administrator to deal with the Vulnerabilities related to overall network and hosts. Its scanning provides non-stop network evaluation and bridges the security holes.

5.3. Comparative Results

From the table 1, the Scanning of the host is completed by Nessus faster than OpenVAS. Nessus is almost 6 times faster than OpenVAS in terms of Speed.

Table - 1: Scanning time

Vulnerability Scanner	Time hh:mm:ss
Nessus	00:03:32
OpenVAS	00:20:40

Chart 1 shows the comparative chart of vulnerability detection with severity level like info, low, medium and high of both Nessus and OpenVAS tools. Nessus tool has detected more vulnerabilities than OpenVAS. As shown in the Chart 1 the overall security level of the network is medium.

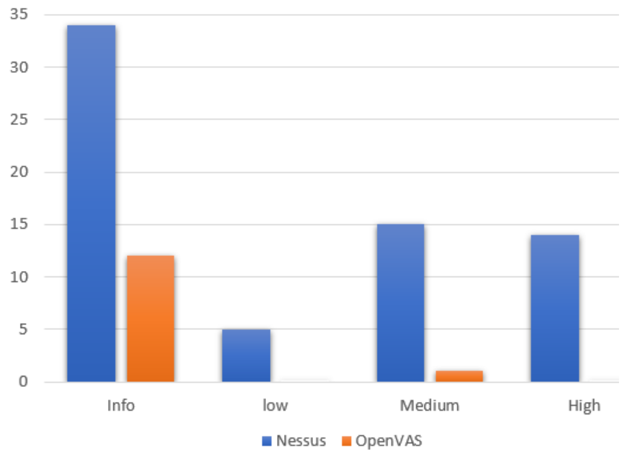


Chart -1: Vulnerability detection of Nessus and OpenVAS

Table 2 shows the list comparative features of Nessus and OpenVAS which includes the working difference of these scanners.

Table - 2: Vulnerability Scanners feature Comparison

Nessus	OpenVAS
CVE Coverage is more than 50,000	CVE Coverage is around 26,000
Nessus is a professional tool	OpenVAS is useful in small businesses
OS platform supports Windows, Linux distributions and so on.	Supports for only Linux platform
Pre-build templates are available for scanning	No Pre-build templates
Easy to install	Complex procedure to install and takes time to sync database
Scanning time is less	Scanning time is more
Vulnerabilities discovered are more	Vulnerabilities detected are less
Scan option is provided with Credential	Scan option does not include Credentials
It can't prevent False positive	Can detect and prevent False positive
Report export formats are available in XML, HTML, PDF, CSV, Nessus DB	Report export formats are available in XML, HTML, PDF and text
Free in Home Version for personal use	Always free because its Open source
Deployment option includes Live USB drive, Traditional install	Deployment option is only Traditional install

Chart 2 represents the graphical representation of Nessus and OpenVAS features like Vulnerabilities detected, scanning time taken to perform scan, Presentation of scan (UI) and report shown, Other Options.

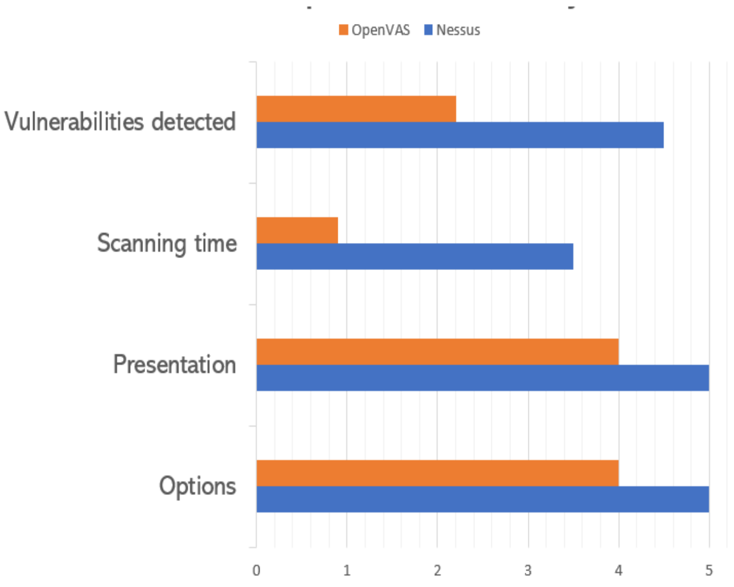


Chart -2: Comparison result of Vulnerability Scanners

6. CONCLUSIONS

This paper presents an Overall performance comparative analysis between the two most used vulnerability scanners: Nessus and OpenVAS. There are many approaches to detect the list of Vulnerabilities within the host system and web application. By undertaking the Vulnerability assessment regularly, helps to stabilize the network. In this paper we examine different Scanners detect different types of vulnerabilities and provide an approach to fix the issues.

Nessus would be a good decision due to its market predominance, accessible documentation and Vulnerability database. Nessus is a proprietary Scanner whereas OpenVAS is an open-source and fork of Nessus project, and OpenVAS can perform nearly what Nessus can do but the primary difference among that two tools is Vulnerability detection of Nessus has a greater number of plugins compared to OpenVAS. The smaller number of Plugins make the tool of a poor choice, but it is probably used as a greater personalized scanner for a selected network. The benefit of OpenVAS is that when the false positive and false negative are discovered, Admin can evaluate the plugin to check why vulnerability is turned into flagged. And it is free to download and audit the code, make changes and get access to a large community of support through the mailing list.

This paper provides different scanning tools with various techniques and performance analysis with their results. The scan report will assist the network and system administrator to deal with the Vulnerabilities related to overall network and hosts. Its scanning provides non-stop network evaluation and bridges the security holes.

REFERENCES

[1] Sandeep Kumar Yadav, Daya Shankar Pandey, Shrikant Lade, May 2017, “A Comparative Analysis of Detecting Vulnerability in Network Systems”, IJARCSSE, Volume 7, Issue 5.

[2] Kushe R, “Comparative Study of Vulnerability Scanning Tools: Nessus Vs Retina”, International Scientific Journal “Security & Future” Polytechnic University of Tirana, Albania.

[3] Ilias Chalvatzis, Dimitrious A. Karras, Rallis C. Papademetriou, “Evaluation of Security Vulnerability Scanners for Small and Medium Enterprises Business Networks Resilience towards Risk Assessment”

[4] Peng Li and Baojiang Cui, “A Comparative Study on Software Vulnerability Static Analysis Techniques and Tools”, IEEE International Conference on Information Theory and Information Security (ICITIS) December 2010.

[5] https://avleonov.com/2016/11/27/fast-comparison-of-nessus-and-openvas-knowledge-bases/

[6] https://www.openvas.org/

[7] https://resources.infosecinstitute.com/a-brief-introduction-to-the-nessus-vulnerability-scanner/

[8] https://382degrees.wordpress.com/2018/09/28/openvas-vs-nessus/

[9] https://www.google.com/search?q=difference+between+nessus+and+openvas&rlz=1C1CHBF_enIN856IN856&oq=differe&aqs=chrome.0.69i59j69i57j69i59l2j0l4.2692j0j7&sourceid=chrome&ie=UTF-8