COMPARATIVE STUDY OF VULNERABILITY SCANNING TOOLS: NESSUS vs RETINA

PhD. Kushe R. [1],
Faculty of Information Technology – Polytechnic University of Tirana, Albania [1]
rkushe@fti.edu.al

Abstract: *Detecting vulnerabilities for a network is an important procedure which ensures that all the data, network-based applications and information communicated in this network, is secure. Detection of network vulnerabilities is used to determine weaknesses of the network, the risk evaluation of attacks, the diagnosis and suggestions to solve the problems. There are several types of scanning tools used to detect vulnerabilities, offering different features. In this paper, we will present a performance comparative study between two most used free, software based, network vulnerability scanning tools: Nessus and Retina. The comparison will be based on three main features: The ability to search, Scanning Time, The ability to detect vulnerabilities. In the conclusions of this paper, both scanners performed very well in vulnerability identification. In terms of speed without active Web Application feature, Nessus performed much faster than Retina; (on the other hand, with active Web Application module, Nessus performs much slower than Retina. In terms of scan depth, Nessus has a small advantage, since it includes a web mirroring tool that is very helpful in HTTP.*

Keywords: VULNERABILITY, NESSUS, RETINA, SCANNING TOOL

1. Introduction

Detecting vulnerabilities for a network is an important procedure which ensures that all the data, network-based applications and information communicated in this network, is secure. Detection of network vulnerabilities is used to determine weaknesses of the network, the risk evaluation of attacks, the diagnosis and suggestions to solve the problems. There are several types of scanning tools used to detect vulnerabilities, offering different features. With so many tools available to make penetration testing, it's hard to choose the most effective. There are not many research works on empirical comparison of vulnerability scanning tools that can help security officers to understand which tool to use, in order to have a better performance during the penetration test of a network.

Therefore, the main aim of this paper is to investigate over two most used, free, software based, vulnerability scanning tools, in terms of their performance.

Open source Nessus is defined as the world's most popular vulnerability scanner [1][2]. Additionally, Nessus scanners may be distributed throughout an entire enterprise, inside DMZs, and across physically separate networks [2]. It is free of charge for personal use in a non-enterprise environment [1]. Commercial organizations that deploy the Nessus vulnerability scanner have to purchase a Nessus ProfessionalFeed [2].

Retina CS is also software based scanning tool as Nessus [1][2][3], which is a free vulnerability scanner for up to 256 IPs gives you powerful vulnerability assessment across your entire environment [3].

There are some previous works about Vulnerability Detection by authors. In [4], Thanyada Veeraprasit et al. implemented NetClarity Auditor and Nessus on Rangsit University network in order to find vulnerability of the network and performance comparision. Then, Aniwat Hemanidhi, Sanon Chimmanee, and Prarinya [5] also deployed such vulnerability detection tools on Rangsit University network for finding vulnerability of the network. Network Risk Metric was proposed in order to evaluate a security risk level of the network based on information from such vulnerability detection tools. Consequently, Sanon Chimmanee et al. evaluated performance of such vulnerability detection tools on both Rangsit University and Royal Thai Army network [6]. Aniwat Hemanidhi, Sanon Chimmanee, and Prarinya deployed the proposed Network Risk Metric in order to evaluate security risk level on Royal Thai Army network [7]

In this paper, we will present a performance comparative study between two most used open source, software based, network vulnerability scanning tools: Nessus and Retina. The comparison will be based on three main features: The ability to search, Scanning Time, The ability to detect vulnerabilities. In the conclusions of this paper, both scanners performed very well in vulnerability identification. In terms of speed without active Web Application feature, Nessus performed much faster than Retina; on the other hand, with active Web Application module, Nessus was much slower than Retina. In this paper we have implemented the free open source version). In terms of scan depth, Nessus has a small advantage, since it includes a web mirroring tool that is very helpful in HTTP.

In section II, experiment setup is stated, also in this section, will be presented the tools configuration (Nessus and Retina scanning tools). Section III provides the experimental results and performance evaluation. In section IV are given the conclusions of this work and future work.

2. Experiment Setup and configuration

The following figure (Fig. 1) shows the network which is configured to test the tools. The client machine, which runs the network vulnerability scanning tools, is within the same subnet with other machines. IP address of the auditor must be set within the same subnet of the target network. A range of investigated IP addresses is required. In this experiment, the target network is XXX.YYY.201.0/24.

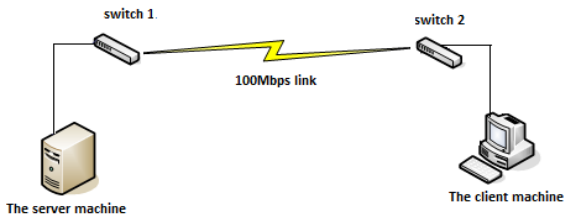

Fig. 1 *The network diagram.*

Nessus [2], by Tenable Network Security, is one of the most popular commercial vulnerability scanners. Vulnerability tests are written using NASL (the Nessus Attack Scripting Language), and

subscriptions to “feeds” of vulnerability checks are available. The “HomeFeed” (the Free version of Nessus we are using) is available for noncommercial home and educational use, while the “ProfessionalFeed” receives updates sooner and can be used in commercial settings. (Nessus Professional (NP) and Nessus Manager (NM), which offer some added features, are available to purchase.). Nessus is based on a client/server architecture, where a client (such as the web interface) connects to the server, which does the scanning. In Fig. 2 and 3 is described the establishment of a secure connection via SSL and also the administrator account setting up.

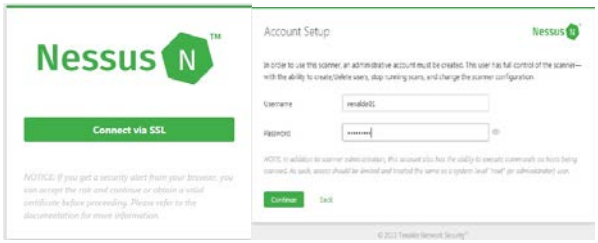

Fig.2 and 3 *The SSL connection and Nessus account setup*

In the Nessus Client side, before starting a scan, must be configured the scanning policies (Fig. 4). In this paper, we will perform a Basic Network Scan.

Results of the scanning can be imported into Metasploit. In addition to vulnerability scanning, Nessus can be used for compliance checks (such as checking the security policies on networked systems by giving Nessus credentials to manage them).

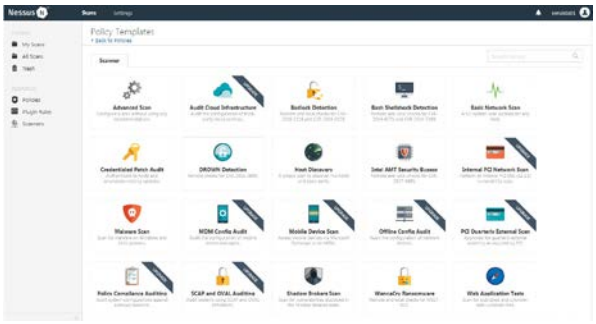

Fig. 4 *Nessus scanning policies*

Retina [3] available as a standalone application or as part of the Retina CS enterprise vulnerability management solution, Retina Network Security Scanner enables you to efficiently identify IT exposures and prioritize remediation enterprise-wide. Retina with its full features integrated is available as Enterprise Edition. For noncommercial and education use, there is Retina free or evaluation version as a Demo also as a Trial. In this paper, we are using the Demo version of Retina, which enable us to use it for 15 days.

In figure 5, is presented Retina Network Security Scanner Interface.

Retina assesses network devices, operating systems, applications, ports and services against a vast, constantly updated vulnerability database. The most innovative feature of it scans the IoT devices and safely checks them for default and hard-coded credentials used with Telnet, SSH, or Basic HTTP Authentication. Also, Retina accurately identifies vulnerabilities with a false positive rate below 1%.

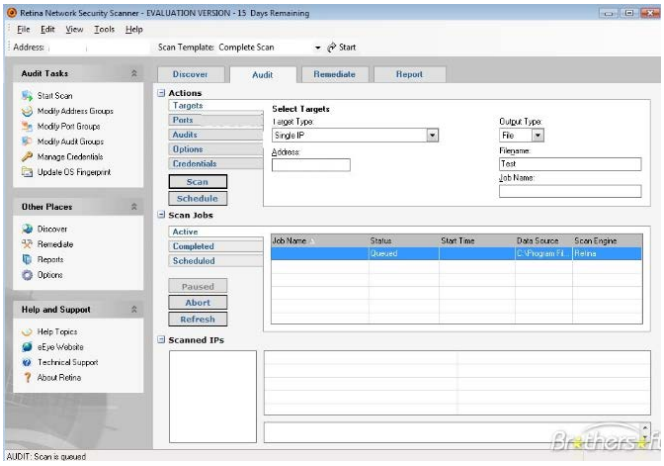

Fig.5 *Retina Network security Scanner Interface*

3. Experimental results

The experimental results will be evaluated upon these features: ability to detect vulnerabilities and the ability to search, also the scanning time.

Nessus also Retina vulnerability scanning tools performed a very good ability to search and to detect vulnerabilities. The considered subnet has five nodes connected to a switch, with the IP address range x.x.201.55-x.x.201.59 and subnet mask /24.

The vulnerabilities classification is based on [8]. The vulnerabilities classification is graded according to the level of risk that they pose to the organization, in terms of severity and exposure. A low rating can be applied to those vulnerabilities that are low in severity and low in exposure. According to this logic, the vulnerability rating 1, 2 and 3 respectively corresponds to low, medium and high risk level. (Table 1).

Table 1: *Vulnerability severity and exposure rating.*

Severity	Rating	Exposure
Minor severity: Vulnerability requires significant resources to exploit, with little potential for loss.	1	**Minor exposure:** Effects of vulnerability tightly contained. Does not increase the probability of additional vulnerabilities being exploited.
Moderate severity: Vulnerability requires significant resources to exploit, with significant potential for loss. Or, vulnerability requires little resources to exploit, moderate potential for loss.	2	**Moderate exposure:** Vulnerability can be expected to affect more than one system element or component. Exploitation increases the probability of additional vulnerabilities being exploited.
High severity: Vulnerability requires few resources to exploit, with significant potential for loss.	3	**High exposure:** Vulnerability affects a majority of system components. Exploitation significantly increases the probability of additional vulnerabilities being exploited.

Figure 6 describes the number of vulnerabilities that Nessus has detected and also the corresponsive risk level of the vulnerability.

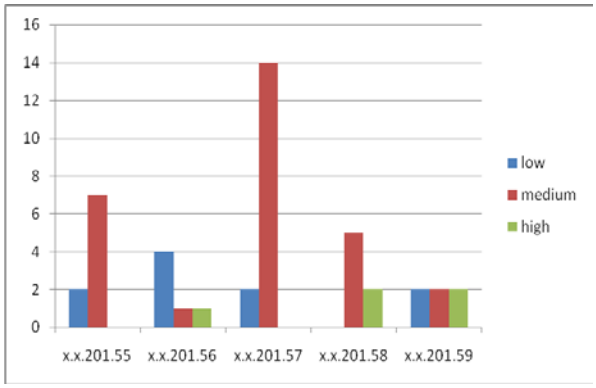

Fig. 6 *Nessus vulnerability detection*

Also figure 7 describes the number of vulnerabilities that Retina has detected and their corresponsive risk level of the vulnerability.

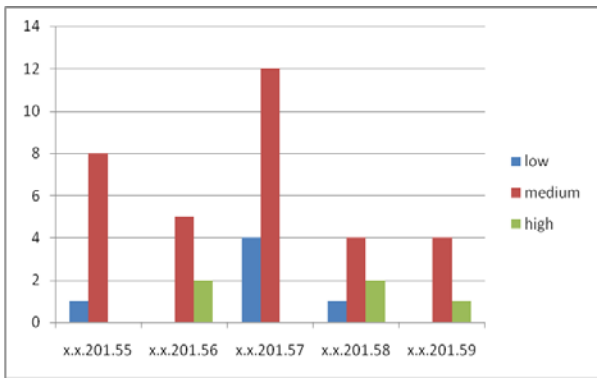

Fig. 7 *Retina vulnerability detection*

In figure 8, is shown a comparative chart according to vulnerability detection ability for these tools. As we can see, Nessus and Retina have almost the same vulnerability detection ability.

As shown on chart (Fig.8), there are much medium vulnerability detected, also some low and very little high vulnerability. The overall security level of this network may be ranked as medium.

In terms of scan depth, Nessus has a small advantage, since it includes a web mirroring tool that is very helpful in HTTP.

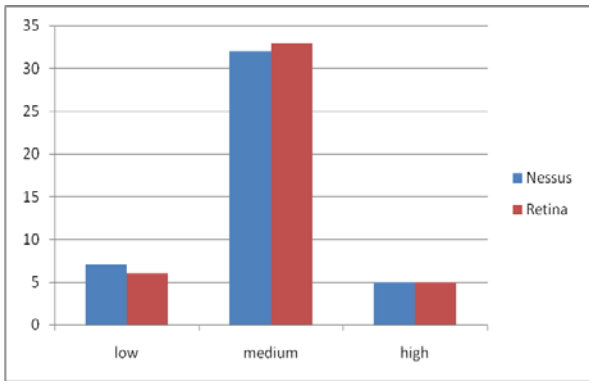

Fig. 8 *Nessus vs Retina vulnerability detection*

In terms of scanning time, (Table 2) Nessus performed much faster than Retina (approximately 6 times faster).

This result initially was a surprise to us. In fact, this result was recorded due to the deactivation of Web Application scanning module in Nessus vulnerability scanning tool.

On the other hand, with active Web application module, Nessus performs much slower than Retina.

Table 2: *Scanning Time*

Tool	Time h:m:s
Nessus	**0:06:01**
Retina	**0:35:49**

Table 2, presents the scanning time for both tools.

4. Conclusion

In this paper, we have presented a performance comparative study between two most used free, software based network vulnerability scanning tools: Nessus and Retina. The comparison is based on three main features: The ability to search, Scanning Time, The ability to detect vulnerabilities. Both scanners performed very well in vulnerability identification. In terms of speed without active Web Application feature, Nessus performed much faster than Retina; on the other hand, with active Web Application module, Nessus performs much slower than Retina In this paper we have implemented the free open source version. In terms of scan depth, Nessus has a small advantage, since it includes a web mirroring tool that is very helpful in HTTP.

The future work will be focused on performance evaluation based on other features, aside from ability to search, Scanning Time, and The ability to detect vulnerabilities. Also, we intend to evaluate other vulnerability scanning tools, not only software based but also hardware based.

Given that there are several types of scanning tools used to detect vulnerabilities, and to perform penetration testing, we aim that with this paper work and with our future work, helping security officers to choose better what tool to implement, in order to have a satisfying performance according to the purpose of use.

References

[1] http://en.wikipedia.org/wiki/Nessus_%28software%29
[2] http://www.tenable.com/products/nessus
[3] https://www.eeye.com/products/retina/community
[4] Veeraprasit Th., Sriphaew K., Chimmanee S. "NetClarity Auditor and Open Source Nessus Comparison for Vulnerability Detection on Rangsit University Network", *The 1st Mae Fah Luang International Conference 2012 (MFUIC 2012)*, Thailand, 2012.
[5] Hemanidhi A., Chimmanee S., Sanguansat P., "Network Risk Evaluation from Vulnerability Detection Tools for IT Department of the Royal Thai Army, *The 1st Mae Fah Luang International Conference 2012 (MFUIC 2012)*, Thailand, 2012.
[6] Chimmanee S., Veeraprasit Th., Sriphaew K, Hemanidhi A. "Performance Comparison of Vulnerability Detection between NetClarity Auditor and Open Source Nessus", WSEAS Proceedings of the 3 rd European Conference of Communications (ECCOM '12), Paris, France, December 2-4, 2012.pp280285.
[7] Hemanidhi A, Chimmanee S, Sanguansat P., "Risk Evaluation by Vulnerability Detection Tools for IT Department of the Royal Thai Army, Proceedings of the 13th WSEAS International Conference on COMPUTERS, Rodos, Greece, July 22-25, 2009, pp.286-292.
[8]https://www.sans.org/reading-room/whitepapers/auditing/overview-threat-risk-assessment-76