



NETCLARITY AUDITOR AND OPEN SOURCE NESSUS COMPARISON FOR VULNERABILITY DETECTION ON RANGSIT UNIVERSITY NETWORK

Thanyada Veeraprasit^{1,*}, Sanon Schimmanee¹, Kritsada Sriphaew¹, Aniwat Hemanidhi²

¹M.S.ITM Online, Faculty of Information Technology, Rangsit University, Muang, Pathum Thani 12000, Thailand

²Military Technology Center, The Royal Thai Army Headquarters, Ratchadamnoen Nok Road, Bangkok 10200, Thailand

*e-mail: thanyada.vee@gmail.com

Abstract


Network vulnerability detection is used to determine the weaknesses of the network, risk assessment, and suggestions to resolve the problems. Traditionally, there are 2 types of vulnerabilities detection tools (Hardware and Software), which their cost are different. Thus, this research is a comparison of vulnerability detection tools on Rangsit University Network by using the Hardware i.e., NetClarity Auditor, and Software i.e., Open Source Nessus. There are three features for comparing as follows: 1) the searching ability, 2) the scanning time, and 3) the ability of vulnerability detection. From experiment, it is shown that 1) NetClarity Auditor gives a better searching performance than Nessus 2) the scanning time of Nessus is shorter than NetClarity Auditor, and 3) NetClarity Auditor introduces a better ability of vulnerability detection than Nessus.

Keywords: Vulnerability detection, NetClarity Auditor, Nessus, Network risk

Introduction

Nowadays information technology plays an important role in organization's task-management. It is not only maintains strong advantage over business competitors but also confirm the successful of the organization business. To achieve business goals as mentioned above, the information system of the organization must be provided with high secure condition in order to prevent attackers from exploiting network's vulnerabilities, steal information.

Kanchana (2002) presented a performance comparison of intrusion detection software between SNORT and RealSecure under actual attacks in isolated Local Area Network. This paper has been conducted in various environments using attacks typically found in the real world. The results of this experiments indicated that both software are similar performances and characteristics, as well as, CPU utilization. However, there are slightly differences in response time and accuracy. SNORT can detect faster but RealSecure is more accurate. Moreover, the performances of both systems will be reduced when there are mix of multiple attacks and background data. This results in a high fault alerts.



Jittima and Kwan (2007) developed a computer network security management for Suan Dusit Rajabhat University. This research is the assessment of Suan Dusit Rajabhat University's network system and investigation of user's behavior. The outcomes are as follows: 1) the security audit of Suan Dusit Rajabhat University's network is found at high risk for intrusion and vulnerabilities in every server. Server vulnerabilities could be solved by patching the operating system and other software, but some essential ports that have to provide services at all times could not be patched. So risk is still high; 2) user's behavior on using the internet is found to be inappropriate by some users for lack of understanding or not aware of the appropriate use of the internet, which is impacted network security. In this paper, the PDCA Model was applied to develop a new computer network security management system for Suan Dusit Rajabhat University.

Artit (2010) studied a method to create a baseline security policy for World Study Center Co., Ltd. based on ISO27001/17799 standard. The benefit of this project is to be aware of and to implement IT security policy so that they can deploy IT security systems for improve security of organizations appropriately. Including, performed penetration testing in order to discover vulnerability and to harden the system. The result from the penetration testing and to harden the system shows that the Risk reduction of IT security systems of organizations. The obtained results indicated that the system administrator is efficient for managing the IT security systems of organizations.

G. Corral et al. (2005) discussed the issues related to vulnerability assessment in wireless networks. They proposed a new distributed system to analyze system interactivity, security capability and vulnerability detection in wireless networks. The designs and implementations were also presented. This research was based on international best practices for security, the Open Source Security Testing Methodology Manual (OSSTMM).

G. Corral et al. (2005) reviewed the main topics related to vulnerability assessment in intranets and proposed a new distributed system to analyze security capability and vulnerability detection in intranets. The system design and implementation was also presented. This proposal was based on OSSTMM.

P. Zhang et al. (2007) presented a model of vulnerability detection system based on multi-agent technology, and the distributed network architecture was set up according to this model. By demonstration of the communication mechanism of the agent model, and the simulation of the network node's sending data packages, it is proved that the model can reduce time of detecting network and processes of hosts, and can ensure intranet's security.

Network vulnerability detection is a major component to determine the weaknesses of the network, risk assessment, and suggestions to resolve the problems. Both hardware and software vulnerability detection tools are available but they have significantly difference in cost of investment. The main topic of this research is to comparison between hardware and software tools in three dimensions which are 1) the searching ability, 2) the scanning time, and 3) the ability of vulnerability detection. Hereby, two zones of Rangsit University, intranet and demilitarized zone are discovered as a pilot network for our main goal.

Experimental results show that 1) NetClarity Auditor gives a better searching performance than Nessus 2) the scanning time of Nessus is shorter than NetClarity Auditor, and 3) NetClarity Auditor introduces a better ability of vulnerability detection than Nessus.

Methodology

As shown in a figure 1, Rangsit University Network is separated into 3 zones including: Internet, Intranet, and demilitarized zone. In this paper, two zones are chosen. They are intranet and demilitarized zone.

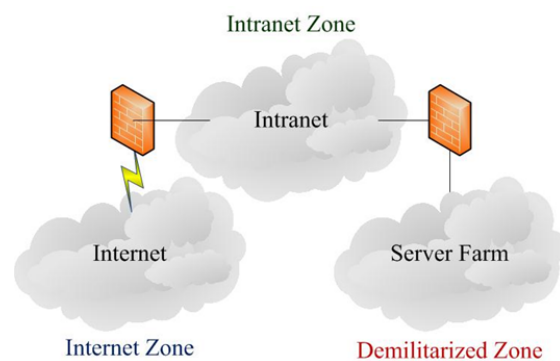


Figure 1 shows the diagram of Rangsit University Network.

Vulnerability Detection on Rangsit University Network uses NetClarity Auditor (Version 8.1.3), and Open Source Nessus HomeFeed (Version 5.0.1) that is installed in a computer notebook called as Nessus notebook in this paper. Experiments are done in demilitarized zone (DMZ) and intranet zone during 2 days of working hours.

Both NetClarity Auditor and Nessus needs to be configured in a proper manner before the vulnerability detection procedure can take place. IP address of the auditor must be set within the same subnet of the target network. Range of investigated IP addresses is required. In this experiment, the target network of DMZ is XXX.YYY.184.0/24 and target network of intranet zone is XXX.YYY.118.0/23. Figure 2 shows the configuration of both vulnerability detection tools.

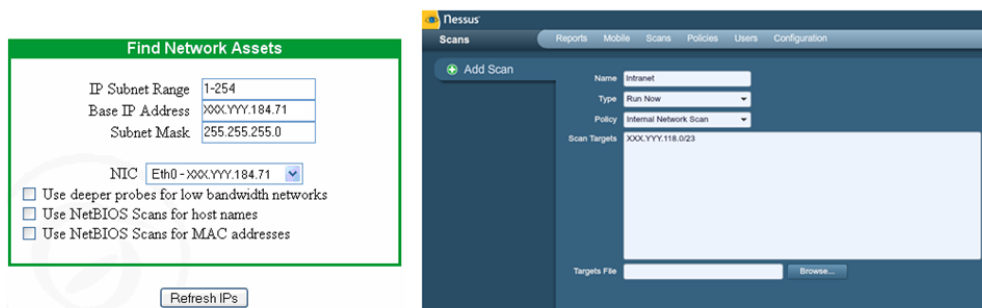


Figure 2 shows the configuration of vulnerability detection with NetClarity Auditor (left) and Nessus (right).

Experimental results can be divided into three features for comparing as follows: 1) the searching ability, 2) scanning time, and 3) the ability of vulnerability detection. Figure 3 (left) displays the outcome of vulnerability detection with NetClarity Auditor. The horizontal axis represents a number of vulnerability. The vertical axis represents hosts. There are 4 colors, which represent 4 levels of risk. Details of risk definition are listed in a table 1.

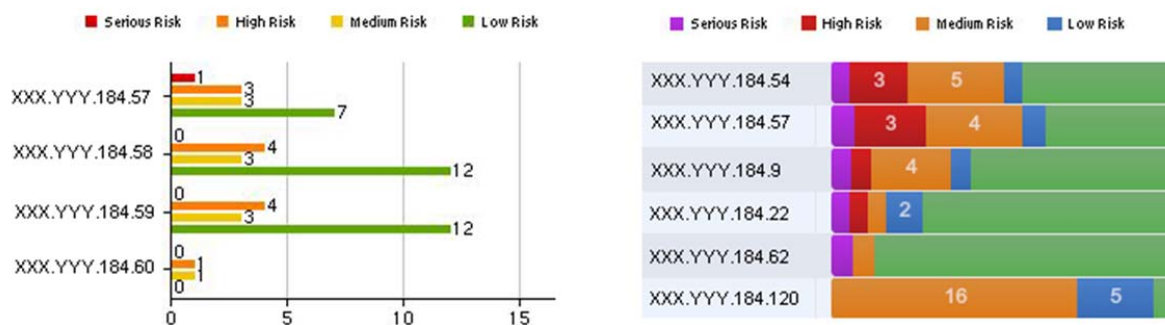


Figure 3 (left) displays the example outcome of vulnerability detection with NetClarity Auditor. Figure (right) shows the example result of vulnerability detection with Nessus.

Table 1 Risk Level Definitions, which there are 4 levels of vulnerability as follows: Serious, High, Medium, and Low (NetClarity, Inc., 2011).

Risk Level	Vulnerability Type
Low	Less important vulnerability - harder to exploit and usually causes little or no damage to your network assets.
Medium	Slightly more important than a Low-level vulnerability but usually hard to exploit. Medium level vulnerabilities might allow an attacker to gain access to your network.
High	Very important vulnerability that may be easy to exploit and allow an attacker to cause serious damage to your network.
Serious	Extremely important vulnerability that may be easy to exploit and allow an attacker to cause critical damage to your network.

Results

There are two main experimental results for DMZ and intranet zones. In DMZ, a summary of the performance comparison is listed in a table 2. More details can be found in a figure 4. It is found that the scanning time of Nessus is shorter than NetClarity Auditor up to 2.632 times. For searching ability, it is shown that the numbers of active hosts are the same. This means that the searching performance of Netclarity Auditor and Nessus are the same approximately. For the ability of vulnerability detection, it is found that NetClarity Auditor has a better performance than Nesuss 3.032 times.

Table 2 A summary of performance comparison of the vulnerability detection on Rangsit University network in DMZ is listed.

Tool	Active Host	Time (h:m:s)	Risk Level			
			Serious	High	Medium	Low
NetClarity Auditor	26	1:36:04	2	98	64	212
Nessus	26	0:36:30	6	22	76	20

NetClarity					Nessus				
Host Address	Serious	High	Medium	Low	Host Address	Serious	High	Medium	Low
XXX.YYY.184.2	0	3	3	19	XXX.YYY.184.1	0	0	0	0
XXX.YYY.184.9	0	0	1	13	XXX.YYY.184.2	0	0	7	0
XXX.YYY.184.11	0	2	4	16	XXX.YYY.184.9	1	1	4	1
XXX.YYY.184.22	0	7	3	7	XXX.YYY.184.11	0	1	5	2
XXX.YYY.184.28	0	8	2	9	XXX.YYY.184.17	0	1	2	1
XXX.YYY.184.51	0	1	0	0	XXX.YYY.184.22	1	1	1	2
XXX.YYY.184.52	0	1	0	0	XXX.YYY.184.28	1	9	14	2
XXX.YYY.184.54	1	9	3	18	XXX.YYY.184.51	0	0	0	0
XXX.YYY.184.55	0	1	1	1	XXX.YYY.184.52	0	0	0	0
XXX.YYY.184.56	0	1	1	0	XXX.YYY.184.53	0	0	0	0
XXX.YYY.184.57	1	3	3	7	XXX.YYY.184.54	1	3	5	1
XXX.YYY.184.58	0	4	3	12	XXX.YYY.184.55	0	0	0	0
XXX.YYY.184.59	0	4	3	12	XXX.YYY.184.56	0	0	0	0
XXX.YYY.184.60	0	1	1	0	XXX.YYY.184.57	1	3	4	1
XXX.YYY.184.61	0	1	1	0	XXX.YYY.184.58	0	1	4	1
XXX.YYY.184.62	0	4	2	5	XXX.YYY.184.59	0	1	4	1
XXX.YYY.184.120	0	6	2	6	XXX.YYY.184.60	0	0	0	0
XXX.YYY.184.123	0	3	5	9	XXX.YYY.184.61	0	0	0	0
XXX.YYY.184.149	0	4	3	6	XXX.YYY.184.62	1	0	1	0
XXX.YYY.184.151	0	3	5	13	XXX.YYY.184.97	0	0	3	0
XXX.YYY.184.152	0	4	3	16	XXX.YYY.184.120	0	0	16	5
XXX.YYY.184.155	0	1	1	5	XXX.YYY.184.123	0	1	6	3
XXX.YYY.184.200	0	1	1	0	XXX.YYY.184.149	0	0	0	0
XXX.YYY.184.231	0	12	6	16	XXX.YYY.184.151	0	0	0	0
XXX.YYY.184.233	0	4	2	7	XXX.YYY.184.152	0	0	0	0
XXX.YYY.184.236	0	10	5	15	XXX.YYY.184.155	0	0	0	0
ToTal	2	98	64	212	Total	6	22	76	20

Figure 4 shows the details of vulnerabilities in individual risk of each Host from NetClarity Auditor (left) and Nessus (right) in DMZ.

In the intranet zone, a table 3 is listed a summary of the performance comparison.

Table 3 A summary of the performance comparison of the vulnerability detection on Rangsit University network in the intranet zone is listed.

Tool	Active Host	Time (h:m:s)	Risk Level			
			Serious	High	Medium	Low
NetClarity Auditor	39	3:19:21	1	42	32	103
Nessus	21	0:52:15	1	3	21	1

From a table 3, the scanning time of Nessus is shorter than NetClarity Auditor 3.815 times but NetClarity Auditor gives a better searching performance than Nessus up to 1.857 times and introduces a better ability of vulnerability detection than Nessus 6.846 times. The vulnerabilities in each risk level of both NetClarity Auditor and Nessus are different because the risk scoring standards are not the same.

A summary of the vulnerability detection tools comparison on Rangsit University Network, by using NetClarity Auditor and Nessus, is shown in a table 4.


Table 4 The comparison of vulnerability detection tools on Rangsit University Network is concluded.

Basis of comparison	Detail
The searching ability	NetClarity Auditor gives a better searching performance than Nessus.
The scanning time	The scanning time of Nessus is shorter than NetClarity Auditor.
The ability of vulnerability detection	NetClarity Auditor introduces a better ability of vulnerability detection than Nessus.

Discussion and Conclusion

NetClarity Auditor has the ability to search and detect vulnerable devices depending on the status of NetClarity Auditor's Firmware. In this paper, NetClarity Auditor's Firmware is updated to the latest version in early 2012. Moreover, there are various standards of the vulnerability detection system depending on what product you have chosen. These standards will affect the analysis of the risk level of vulnerabilities detected.

In DMZ, the scanning time of Nessus is shorter than NetClarity Auditor 2.595 times. In scanning period, both of them could find the same amount of the active hosts. However, NetClarity Auditor gives a better searching performance than Nessus 3.032 times. In the intranet zone, the



scanning time of Nessus is shorter than NetClarity Auditor 3.827 times but NetClarity Auditor gives a better searching performance than Nessus 1.857 times and introduces a better ability of vulnerability detection than Nessus 6.846 times. In summary, NetClarity Auditor has a better performance than Nessus. Thus, NetClarity Auditor should be preferred. Nevertheless, the cost of investment for NetClarity Auditor is significantly higher than Nessus.

References

1. Kanchana Silawarawet. (2002). The comparison of network intrusion detection system between SNORT and RealSecure under attack. Master of Science, Chulalongkorn University.
2. Jittima Tiamboonprasert and Kwan Sitathani. (2007). The development of a computer network security management system for Suan Dusit Rajabhat University, Thailand. Suan Dusit Rajabhat University Research Journal, 3, 110-123.
3. Artit Choongthai. (2010). Developing Security and Baseline Policy: A Case Study at World Study Center Co.,Ltd.. Master of Science, Mahanakorn University of Technology.
4. G. Corral, X. Cadenas, A. Zaballos, and M. T. Cadenas. (2005). A Distributed Vulnerability Detection System for WLANs, IEEE, the First International Conference on Wireless Internet (WICON'05), Hungary, July 2005.
5. G. Corral, A. Zaballos, X. Cadenas, and A. Grane. (2005). A Distributed Vulnerability Detection System for an Intranet, IEEE, the 39th annual 2005 international carnahan conference, 2005.
6. P. Zhang, J. Shang, and Z. Liang. 2007. Application of Multi-Agent Model in Vulnerability Detection System, IEEE, First IEEE International Symposium, 2007.
7. NetClarity, Inc. "NACwall Appliances User Guide Manual", NetClarity, Inc., 2011.