A Performance Evaluation of Vulnerability Detection: NetClarity Audito, Nessus, and Retina

Sanon Chimmanee, Thanyada Veeraprasit, and Chetneti Srisa-An

Rangsit University, Pathumthani, Thailand

Summary

Network vulnerability detection is used to determine the weaknesses of the network, risk assessment, and suggestions to resolve the problems. Basically, there are 2 types of vulnerability detection tools (Hardware and Software), which their cost are different. Thus, this paper is a performance comparison of vulnerability detection tools on the Rangsit University network and the Royal Thai Army network by using the hardware i.e., NetClarity Auditor, and software i.e., Open Source Nessus and Retina Network Security Scanner . There are three features for comparison 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 the best in searching performance, 2) the scanning time of Nessus is the shortest, and 3) NetClarity Auditor is also the best in the ability of vulnerability detection.

Key words:

Vulnerability detection, NetClarity Audito, Nessus, Retina Network Security Scanner.

1. Introduction

Network vulnerability detection is an important procedure to ensure that the organization network is secured. In information security for web-based applications, the detection and diagnosis of software vulnerabilities are important tasks for the user [1]. However, there are often significant differences in the content, organization, and format of different vulnerability reports [1-2]. CVSS is an open framework developed by National Institute of Standards and Technology for assessing vulnerabilities criticality across many disparate hardware and software platforms [3]. G. Corral et al. [4-5] proposed the distributed vulnerability detection system for wireless and intranet networks based on international best practices for security, the Open Source Security Testing Methodology Manual (OSSTMM). P. Zhang et al. [6] introduced a model of vulnerability detection system based on multi-agent technology, and distributed network architecture was set up according to this model.

Nessus, Retina, Snort, and other software-based are important tools for testing and monitoring or other components that are quite wide-spread these days [7].

Zhihong Tian et al [8] presented a Vulnerability-driven Active Alert Verification (VAAV) approach that performs real-time verification of attack detected by IDS. Kanchana [9] presented a performance comparison of intrusion detection software between SNORT and RealSecure under actual attacks in isolated Local Area Network. In [10], testing and comparing web vulnerability scanning tool for SQL injection and XSS attacks was presented. N. Antunes, and M. Vieira [11] proposed the comparing the effectiveness of penetration testing and static code analysis on the detection of SQL injection vulnerability in web services. A comparative study on software vulnerability static analysis techniques and tools was introduced by P. Li, and B. Cui [12].

Both hardware and software vulnerability detection tools are available but they have significantly difference in cost of investment. Thanyada Veeraprasit et al [13] introduced a performance comparison of NetClarity Auditor and Open Source Nessus Vulnerability Detection on Rangsit University Network. Sanon Chimmanee et al [14] investigated the performance comparison of these vulnerability detections on an additional site that is Royal Thai Army network. The main topic of this research is to compare between hardware and software tools in three dimensions, which are 1) the searching ability, 2) scanning time, and 3) the ability of vulnerability detection. There are two network sites for testing. First is the Rangsit University network and the other is the Royal Thai Army network. Each site consists of two zones (demilitarized zone and intranet zone). This paper adds another vulnerability detection that is Retina Network Security Scanner V.5.17.1.2570. Additional experiment is done on MTC zone 2 of Royal Thai Army network.

From experiment, it is found that NetClarity Auditor is the best for the searching ability. Nessus is better than Retina Network Security Scanner for this feature. For scanning time, it can be seen that Nessus is the best performance. NetClarity Auditor has a better performance than Retina. For the ability of vulnerability detection, NetClarity Auditor is also the best performance. Retina is better than Nessus. From overall, NetClarity Auditor should be preferred. However, the cost of investment for NetClarity Auditor is the highest.

The rest of this paper is organized as follows. Section II provides related works. In section III, experiment setup is stated. Section IV provides the performance evaluations. Section V gives conclusions and future work.

Manuscript received March 5, 2014
Manuscript revised March 20, 2014

2. Related Works

There are two major experiments: First is done at Rangsit University and the other is done at the Royal Thai Army.

2.1 Vulnerability Detection Tools

Typically, there are two types of the vulnerability detection tool: Hardware-based, and Software-based. NetClarity Auditor based on hardware is one of popular vulnerability detection tool [13]. However, its cost is high. Open source Nessus based on software is the world's most popular vulnerability scanner, which is needed to install on the computer [15],[16]. Additionally, Nessus scanners may be distributed throughout an entire enterprise, inside DMZs, and across physically separate networks [16]. It is free of charge for personal use in a non-enterprise environment [15]. Commercial organizations that deploy the Nessus vulnerability scanner have to purchase a Nessus ProfessionalFeed [16]. Retina CS is also software-base, which is a free vulnerability scanner for up to 256 IPs gives you powerful vulnerability assessment across your entire environment [17].

2.2 Literature Review

Snort is one of popular Intrusion Detection systems (IDS) since it is open-source software. IDS has been considered the second line of defense for computer and network systems along with prevent-based techniques e.g., access control [8]. Kanchana [9] evaluated a performance of IDS between Snort and RealSecure under actual attacks in isolated Local Area Network. From experiments, it is found that both IDS tools 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. Zhihong Tian et al [8] presented a Vulnerability-driven Active Alert Verification called as “VAAV” approach that performs real-time verification of attack detected by IDS. The proposed VAAV attempts to address the aforementioned shortcomings in current IDSs. It can be considered as a finite state machine. The role of VAAV is designed on base of Snort.

Nessus, Retina, Snort, and other are important tools for testing and monitoring or other components that are quite wide-spread these days [7]. Pavel Vachek [18] proposed the developed e-mail interface that allows users to perform basic host security audits simply and securely for Nessus running on a PC sever under Linux operating system. G. Corral et al. [4],[5] 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). P. Zhang et al. [6] 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.

2.3 Previous work

There are four previous works about Vulnerability Detection by authors. In [13], 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 [19] 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 [14]. Aniwat Hemanidhi, Sanon Chimmanee, and Prarinya. deployed the proposed Network Risk Metric in order to evaluate security risk level on Royal Thai Army network [20].

3. Experimental Setup

There are two major experiments: First is done at Rangsit University and the other is done at the Royal Thai Army.

3.1 Rangsit University Network

As shown in a Fig. 1, Rangsit University Network is separated into three zones including: internet, intranet, and demilitarized zones. In this paper, two zones are chosen, demilitarized zone (DMZ) and intranet zone.

There are two vulnerability detections on Rangsit University Network: NetClarity Auditor (Version 8.1.3), and Open Source Nessus HomeFeed (Version 5.0.1) installed in a computer notebook called as Nessus notebook in this paper. The experiments were done in the DMZ and the intranet zone during two days of working hours.

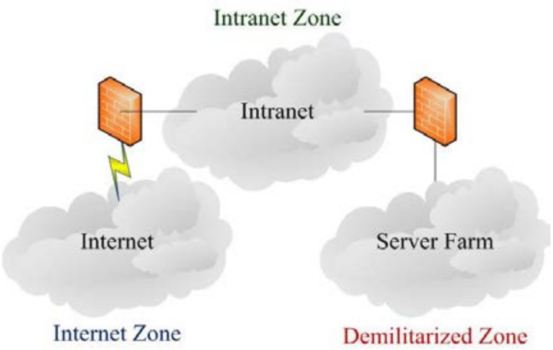
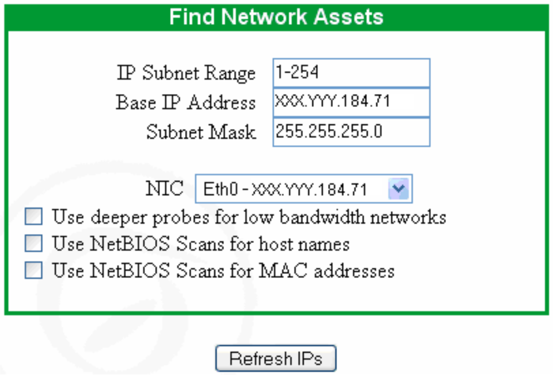


Fig. 1 Network Diagram of Rangsit University.

NetClarity, Nessus, and Retina need 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. A range of investigated IP addresses is required. In this experiment, the target network of DMZ is XXX.YYY.184.0/24 and the target network of intranet zone is XXX.YYY.118.0/23. Fig. 2, Fig.3 and Fig. 4 show the configuration of these vulnerability detection tools, respectively.



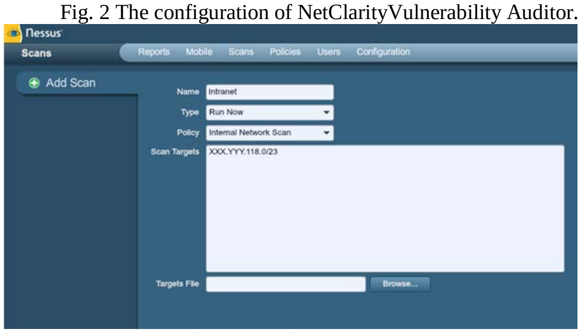
Find Network Assets

IP Subnet Range: 1-254
Base IP Address: XXX.YYY.184.71
Subnet Mask: 255.255.255.0

NIC: Eth0 - XXX.YYY.184.71

☐ Use deeper probes for low bandwidth networks
☐ Use NetBIOS Scans for host names
☐ Use NetBIOS Scans for MAC addresses

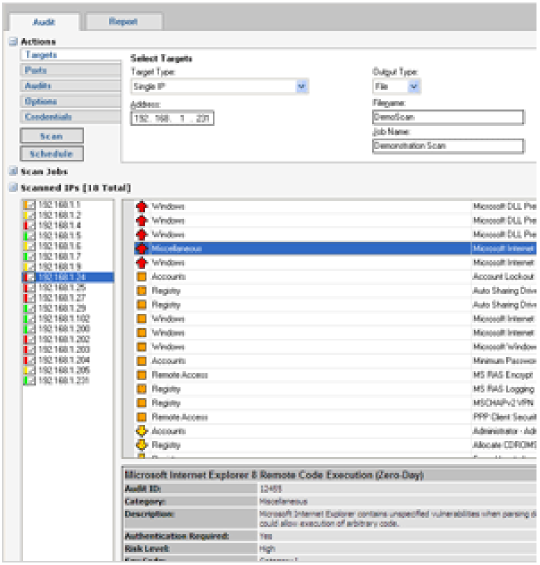
Fig. 2 The configuration of NetClarityVulnerability Auditor.



Name: Intranet
Type: Run Now
Policy: Internal Network Scan
Scan Targets: XXX.YYY.118.0/23
Targets File:

Fig. 3 The configuration of vulnerability detection with Nessus.

For comparison, experimental results are divided into three features including: 1) the searching ability, 2) the scanning time, and 3) the ability of vulnerability detection. Fig. 5, 6 and Fig. 7 display the outcome of the vulnerability detection with NetClarity Auditor, Nessus and Retina, respectively. The horizontal axis represents a number of the vulnerability. The vertical axis represents hosts. There are four colors which represent four levels of risk. Details of risk definition are listed in Table 1.



Select Targets
Target Type: Single IP
Address: 192 . 168 . 1 . 231
Output Type: File
Filename: DemoScan
Job Name: Demonstration Scan

192.168.1.1
192.168.1.2
192.168.1.4
192.168.1.5
192.168.1.6
192.168.1.7
192.168.1.9
192.168.1.24
192.168.1.25
192.168.1.27
192.168.1.29
192.168.1.102
192.168.1.200
192.168.1.202
192.168.1.203
192.168.1.204
192.168.1.205
192.168.1.231

Windows Microsoft DLL Pre
Windows Microsoft DLL Pre
Windows Microsoft DLL Pre
Miscellaneous Microsoft Internet
Windows Microsoft Internet
Accounts Account Lockout
Registry Auto Sharing Drive
Registry Auto Sharing Drive
Windows Microsoft Internet
Windows Microsoft Internet
Windows Microsoft Window
Accounts Minimum Passwo
Remote Access MS RAS Encrypt
Registry MS RAS Logging
Registry MSCHAPv2 VPN
Remote Access PPP Client Securit
Accounts Administrator - Adi
Registry Allocate CDROMS

Microsoft Internet Explorer 8 Remote Code Execution (Zero-Day)

Audit ID:	12455
Category:	Miscellaneous
Description:	Microsoft Internet Explorer contains unspecified vulnerabilities when parsing d could allow execution of arbitrary code.
Authentication Required:	Yes
Risk Level:	High

Fig. 4 The configuration of vulnerability detection with Retina Network Security Scanner referred from (http://www.beyondtrust.com/Products/RetinaNetworkSecurityScanner/)

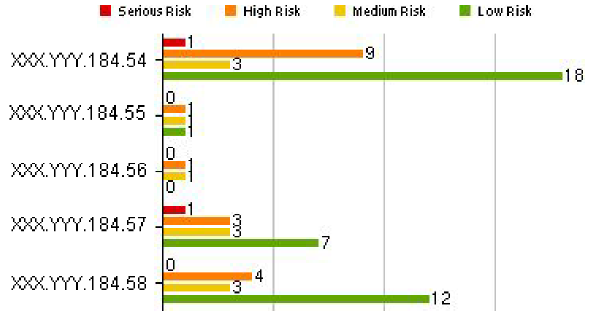


Fig. 5 Example of the outcome of vulnerability detection with NetClarity Auditor.

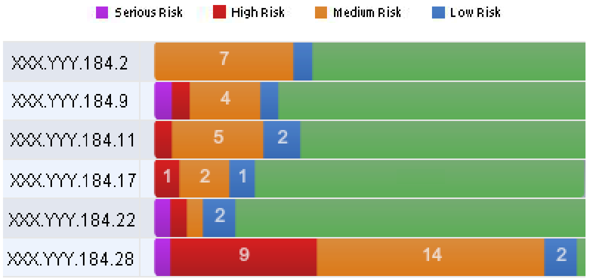


Fig. 6 Example of the outcome of vulnerability detection with Nessus.

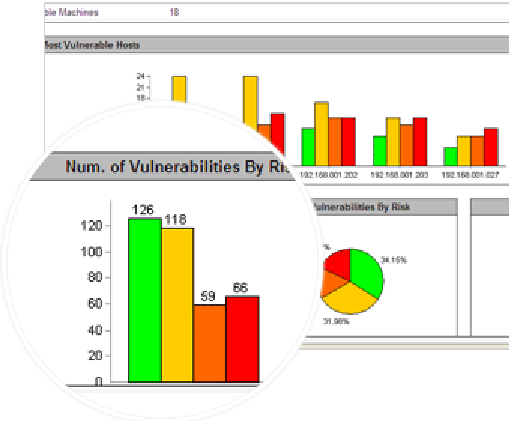


Fig. 7 Example of the outcome of vulnerability detection with Retina Network Security Scanner referred from (http://www.beyondtrust.com/Products/RetinaNetwork SecurityScanner/)

Table 1: Risk level of each vulnerability types classifies by NetClarity [12].

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.

3.2 The Royal Thai Army Network

There are many types of data communication networks in the RTA. The MTC has responsible on several major networks including gateway that link to the internet/extranet. For security reason, the network diagram of the RTA will not be described in depth on this paper. Nevertheless, it is necessary to show some details of the MTC network diagram used in this research. In the overview, there are three main network zones connected to the CISCO Core Switch-L3. They are MTC network zone 0, 1, and 2 as shown in Fig. 8.

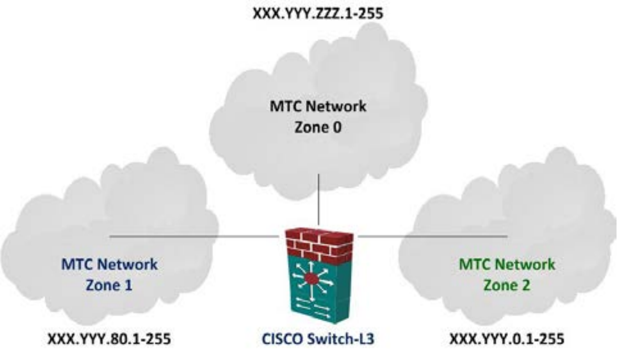


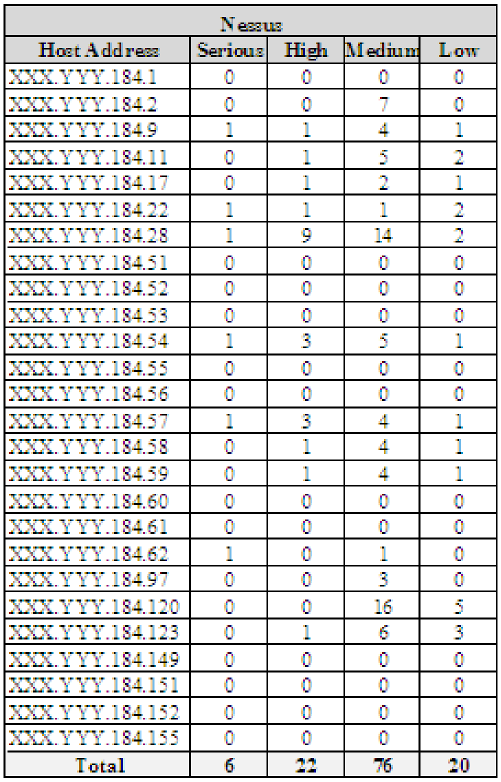
Fig. 8 Network Diagram of the Military Technology Center (MTC).

The Thai Army network configuration is the same direction as the Rangsit University network configuration in subsection 3.1. There are two vulnerability detections on MTC zone 1 like on the Rangsit University network. Additionally, there are three vulnerability detections on MTC zone 2: NetClarity Auditor (Version 8.1.3), Open Source Nessus HomeFeed (Version 5.0.1), and Retina Network Security Scanner V.5.17.1.2570 installed in the HP desktop call as Retina Computer in this paper.

4. Performance Evaluation

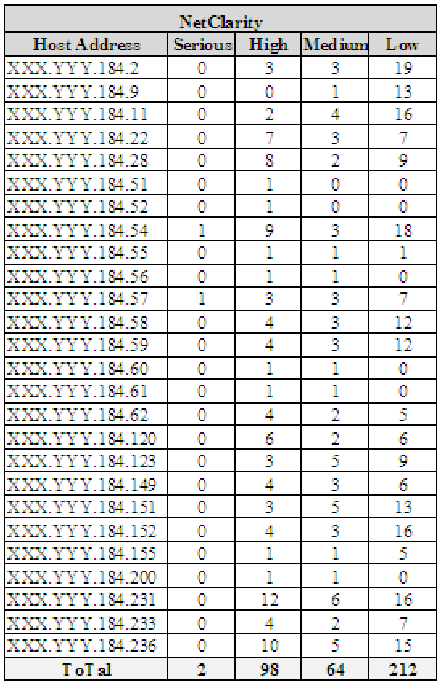
4.1 Experimental Result of Rangsit University Network

There are two main experimental results for DMZ and intranet zones. In DMZ, a summary of the found active hosts and scanning time are shown in a Table 2. Also, the total detected vulnerabilities are represented in Fig. 9 and 11. It is found that the scanning time of Nessus is shorter than NetClarity Auditor up to 2.632 times. For the searching ability, it is shown that the number of active hosts is the same for both NetClarity Auditor and Nessus. This means that the searching performance of NetClarity Auditor and Nessus are approximately the same. For the ability of vulnerability detection, it is found that NetClarity Auditor has a better performance than Nessus 3.032 times.



Nessus				
Host Address	Serious	High	Medium	Low
XXX.YYY.184.1	0	0	0	0
XXX.YYY.184.2	0	0	7	0
XXX.YYY.184.9	1	1	4	1
XXX.YYY.184.11	0	1	5	2
XXX.YYY.184.17	0	1	2	1
XXX.YYY.184.22	1	1	1	2
XXX.YYY.184.28	1	9	14	2
XXX.YYY.184.51	0	0	0	0
XXX.YYY.184.52	0	0	0	0
XXX.YYY.184.53	0	0	0	0
XXX.YYY.184.54	1	3	5	1
XXX.YYY.184.55	0	0	0	0
XXX.YYY.184.56	0	0	0	0
XXX.YYY.184.57	1	3	4	1
XXX.YYY.184.58	0	1	4	1
XXX.YYY.184.59	0	1	4	1
XXX.YYY.184.60	0	0	0	0
XXX.YYY.184.61	0	0	0	0
XXX.YYY.184.62	1	0	1	0
XXX.YYY.184.97	0	0	3	0
XXX.YYY.184.120	0	0	16	5
XXX.YYY.184.123	0	1	6	3
XXX.YYY.184.149	0	0	0	0
XXX.YYY.184.151	0	0	0	0
XXX.YYY.184.152	0	0	0	0
XXX.YYY.184.155	0	0	0	0
Total	6	22	76	20

Fig. 9 shows the details of vulnerabilities in individual risk of each Host from NetClarity Auditor in DMZ.



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

Fig.10 shows the details of vulnerabilities in individual risk of each Host from Nessus in DMZ.

Table 2: A summary of performance comparison of the vulnerability detection on Rangsit University network in DMZ.4.2 Experimental Result of Rangsit University Network.

Tool	Active Host	Time (h:m:s)
NetClarity Auditor	26	1:36:04
Nessus	26	0:36:30

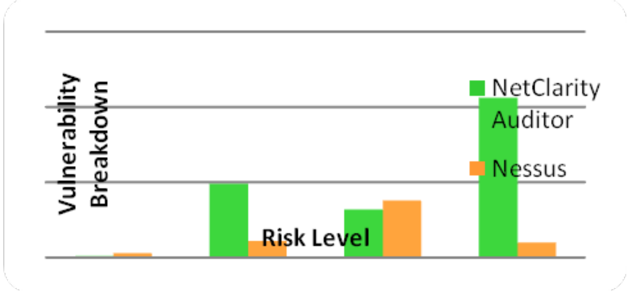


Fig.11 The total detected vulnerabilities on Rangsit University network in DMZ.

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

Tool	Active Host	Time (h:m:s)
NetClarity Auditor	39	3:19:21
Nessus	21	0:52:15

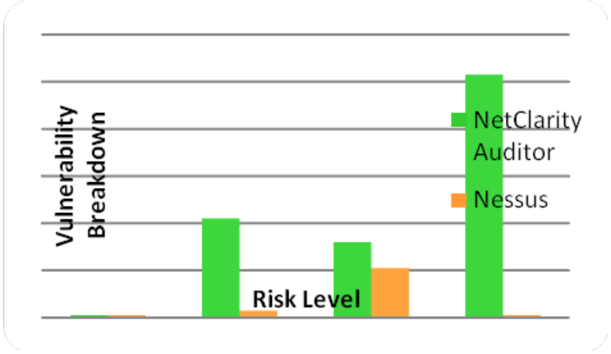


Fig. 12 The total detected vulnerabilities on Rangsit University network in Intranet zone.

The found active hosts and scanning time on the intranet zone of Rangsit University network is listed in Table 3 and the total detected vulnerabilities are shown in the Fig. 10 and 12. It is show that Nessus uses shorter time to detect actives host and vulnerabilities than NetClarity Auditor about 3.815 times. Somehow, NetClarity Auditor shows a better searching performance than Nessus up to 1.857 times since it can find more host than Nessus. Finally, NetClarity implies better ability of vulnerability detection over Nessus about 6.846 times by the total number of detected flaws. From this point of view, NetClarity and Nessus represent different number of found vulnerabilities in each risk level because they tied their detecting ability among various different standards.

4.2 Experimental Result of the Royal Thai Army Network

In this experiment, two network zones of the MTC are discovered as the representative network of the Royal Thai Army (RTA). From the MTC zone 1, the found active hosts and scanning time are listed in Table 4 and the total detected vulnerabilities are represented in Fig. 13. It is found that scanning time of Nessus is shorter than NetClarity Auditor up to 2.143 times. NetClarity Auditor shows better searching performance than Nessus up to 1.077 times and implies better ability of vulnerability detection over Nessus about 2.054 times.

Table 4: A summary of performance comparison of the vulnerability detection on the MTC zone 1 of the Royal Thai Army Network.

Tool	Active Host	Time (h:m:s)
NetClarity Auditor	14	1:37:06
Nessus	13	0:45:18

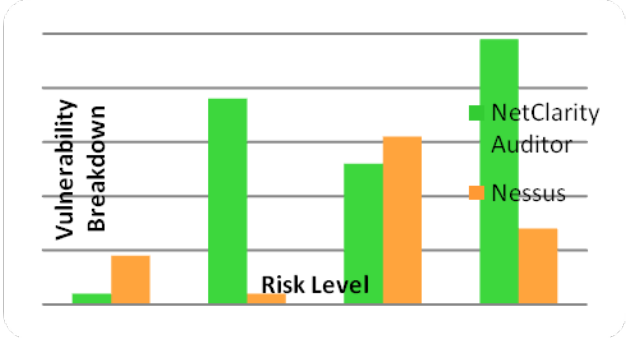


Fig. 13 The total detected vulnerabilities on the MTC zone 1 of the Royal Thai Army network.

Next shown in Table 5 is the performance comparison of the vulnerability detection on the MTC zone 2.

Table 5: A summary of performance comparison of the vulnerability detection on the MTC zone 2 of the Royal Thai Army Network.

Tool	Active Host	Time (h:m:s)
NetClarity Auditor	26	1:34:55
Nessus	11	0:22:09
Retina Network Security Scanner	10	7:34:53

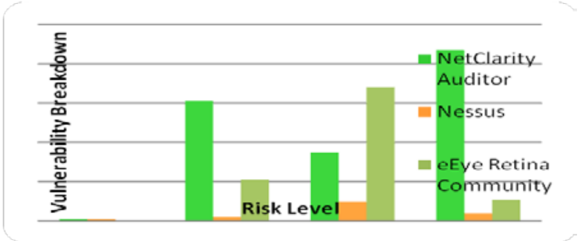


Fig. 14 The total detected vulnerabilities on the MTC zone 2 of the Royal Thai Army network.

From the Table 5, it is found that Nessus is the best for the scanning time. It uses a shorter time to detect actives host and vulnerabilities than NetClarity Auditor about 4.285 times. NetClarity Auditor is better than Retina Network Security Scanner up to 4.792 times. For searching ability, it can be seen that NetClarity Auditor is the best performance. It is better than Retina Network Security Scanner up to 2.6 times. Nessus has a better performance than Retina up to 1.1 times.

For the ability of vulnerability detection as shown in Fig.8, NetClarity Auditor is also the best performance. It is better than Retina Network Security Scanner up to 1.84 times and better than Nessus up to 5.882 times. From this point of view, NetClarity Auditor, Nessus, and Retina Network Security Scanner represent different number of found vulnerabilities in each risk level because they tied their detecting ability among various different standards.

The comparison of vulnerability detection from NetClarity and Nessus on the Rangsit University networkis and the Royal Thai Army network are shown in the following Table 6.

Table 6: The comparison of two vulnerability detection tools, NetClarity Auditor and Nessus, on Rangsit University and the Royal Thai Army.

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.
Ability of vulnerability detection	NetClarity Auditor introduces a better ability of vulnerability detection than Nessus.

5. CONCLUSION

In DMZ of the Rangsit University network, the scanning time of Nessus is shorter than NetClarity Auditor 2.632 times. During the scanning, both of them could find the same amount of active hosts. However, NetClarity Auditor gives a better searching performance than Nessus 3.032 times. In intranet zone, the scanning time of Nessus is shorter than NetClarity Auditor 3.815 times but NetClarity Auditor gives a better searching performance than Nessus 1.857 times. It also introduces a better ability of vulnerability detection than Nessus 6.846 times.

From the MTC zone 1 of the Royal Thai Army Network, the scanning time of Nessus is shorter than NetClarity Auditor up to 2.143 times. NetClarity Auditor shows better searching performance than Nessus up to 1.077 times and implies better ability of vulnerability detection over

Nessus about 2.054 times. In the MTC zone 2, Nessus uses shorter time to detect actives host and vulnerabilities than NetClarity Auditor about 4.285 times. NetClarity Auditor shows better searching performance than Nessus up to 2.364 times and implies better ability of vulnerability detection over Nessus about 10.824 times. From MTC zone 2 of the Royal Thai Army Network, it is found that NetClarity Auditor is the best for the searching ability. Nessus is better than Retina Network Security Scanner for this feature. For scanning time, it can be seen that Nessus is the best performance. NetClarity Auditor has a better performance than Retina Network Security Scanner. For the ability of vulnerability detection, NetClarity Auditor is also the best performance. Retina Network Security Scanner is better than Nessus. In summary, NetClarity Auditor has a better performance than Nessus and Retina Network Security Scanner. However, the cost of investment for NetClarity Auditor is significantly higher than Nessus and Retina Network Security Scanner.

The security metric of evaluation the vulnerability from several tools will be studied in the future work.

Acknowledgments

Author thanks Aniwat Hemanidhi for his supports.

References

[1] Peter KokKeongLoh, and Deepak Subramanian, “Fuzzy Classification Metrics for Scanner Assessment and Vulnerability Reporting”, IEEE *Transaction on Information Forensics and Security, Vol. 5, No. 4*, December 2010.

[2] DHS National Security Division, NIST, Web Application Vulnerability Scanners [Online]. Available: https://samet.nist.gov/index.php/Web_Application_Vulnerability_Scanners

[3] GolnazElahi, Eric Yu, and Nicola Zannone, “Security Risk Management by Qualitative Vulnerability Analysis”, IEEE, *Third International Workshop on Security Measurements and Metrics*, 2011.

[4] G. Corral, X. Cadenas, A. Zaballos, and M. T. *Cadenas, “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, “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, “Application of Multi-Agent Model in Vulnerability Detection System”, *IEEE, First IEEE International Symposium*, 2007.

[7] MIROSLAV VOZNAK, FILIP REZAC,"SIP Threats Detection System", 9th WSEAS International Conference on DATA NETWORKS, COMMUNICATIONS, COMPUTERS (DNCOCO'10), Universtiy of Algarve, Faro, Portugal, November 3-5, 2010

[8] Zhihong Tian, Binxing Fang, Bin Li, Hongli Zhang, “A Vulnerability-Driven Approach to Active Alert Verification for Accurate and Efficient Intrusion Detection”, WSEAS TRANSACTIONS on COMMUNICATIONS", Issue 10, Volume 4, October 2005, pp. 1002-1009, ISSN 1109-2742.

[9] Kanchana Silawarawet, “The comparision of network intrusion detection system between SNORT and RealSecure under attack”, *Thesis*, Master of Science, Chulalongkorn University, Thailand, 2002.

[10] J. Fonseca, M. Vieira, and H. Madeira, “Testing and comparing web vulnerability scanning tools for SQL injection and XSS attacks”, *IEEE, 13th IEEE International Symposium on Pacific Rim Dependable Computing*, 2007.

[11] N. Antunes, and M. Vieira, “Comparing the effectiveness of penetrating testing and static code analysis on the detection of SQL injection vulnerabilities in web services”, *IEEE, 15th IEEE Pacific Rim International Symposium on Dependable Computing*, 2009.

[12] P. Li, and B. Cui, “A comparative study on software vulnerability static analysis techniques and tools”, *IEEE, Information Theory and Information Security (ICITIS), 2010 IEEE International Conference*, 2010.

[13] Thanyada Veeraprasit, Kritsada Sriphaew, and Sanon Chimmanee “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.

[14] Sanon Chimmanee, Thanyada Veeraprasit, Kritsada Sriphaew, and Aniwat Hemanidhi “Peformance Comparisionof Vulnerability Detection betweenNetClarity Auditor and Open Source Nessus”, WSEAS Proceedings of the 3rd European Conference of Communications (ECCOM ’12), Paris, France, December 2-4, 2012.pp280-285.

[15] http://en.wikipedia.org/wiki/Nessus_%28software%29

[16] http://www.tenable.com/products/nessus

[17] https://www.eeye.com/products/retina/community

[18] Pavel Vachek, "CESNET Audit System", Proceedings of the 13th WSEAS International Conference on COMPUTERS, Rodos, Greece, July 22-25, 2009

[19] Aniwat Hemanidhi, Sanon Chimmanee, Prarinya Sanguansat, “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.

[20] Aniwat Hemanidhi, Sanon Chimmanee, Prarinya Sanguansat, “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.

Sanon Chimmanee received B.Eng. degree in Electrical Engineering, Rangsit University, Thailand in 1996 and M.S. degree in Telecommunications Science and Computer Network Engineering, South Bank University, London in 1998 and Ph.D. degree in Sirindhorn International Institute of Technology (SIIT), Thammasat University, Thailand in 2006. He is now with Rangsit University, Thailand as Assistant Professor in Faculty of Information Technology. He is also Director of MSITM-online program.

Thanyada Veeraprasit received B.Eng. degree in Telecommunication Engineering, Suranaree University of Technology, Thailand in 2004 and M.S. degree in Master of Science Program in Information Technology Management, Rangsit University, Thailand in 2012. She is now with Samart Communication Services Co., Ltd. in Thailand as Network Engineer.

Chetneti Srisa-An received B.Eng. degree in Electrical Engineer, Chiangmai University, Thailand and MBA (Finance) Loyola University of Chicago, USA. He got MSCS (Computer Science) and Ph.D. (Computer Science) lllinois Institute of Technology, USA. He is now with Rangsit University, Thailand as Assistant Professor in Faculty of Information Technology.