

VULNERABILITY ASSESSMENT ON THE COMPUTER NETWORK SECURITY

Firkhan Ali B. Hamid Ali, ¹Maziah Bt. Na'man@Na'aman

¹Fakulti Teknologi Maklumat dan Multimedia,
Kolej Universiti Teknologi Tun Hussein Onn,
Beg Berkunci 101, 86400 Parit Raja, Johor Darul Takzim.
Tel: 07-4538030, Fax: 07-4532199
E-mail: firkhan@kuittho.edu.my

ABSTRACT

Nowadays, miscellaneous towards computer network can always be read through newspaper and be seen or hear via electronic media. This problem is happen because of lack of effort on computer network security system. Even the network security system or application is good, but vulnerability towards the computer network has to be implied regularly. So, vulnerability assessment is important to be done in the computer network.

Vulnerability assessment had done towards computer network at Computer Networking Lab, Fakulti Teknologi Maklumat dan Multimedia (FTMM), Kolej Universiti Teknologi Tun Hussein Onn (KUiTTTHO). Security Life Cycle Methodology was used as a guideline to execute Vulnerability assessment by using software, Nessus which is based on client server model.

The result of this vulnerability assessment is there's a lot of vulnerability exists inside the computer network nodes at FTMM Networking Technology Lab. The vulnerabilities that had found were such as open port, useless application, bugs in the operating system and others. Therefore, a few steps had been taken such as doing patching, update the application version and operating system that have been used, close the port that is not needed and others. When reevaluation had made, it can be minimize the amount of vulnerabilities inside the computer network.

Keywords: attacks, computer network, exploits, network security, security, vulnerability, vulnerability-scanning.

INTRODUCTION

Malaysian organization has face very tough time including FTMM, KUiTTTHO according to the issues, statistic and news of the computer network security that had provided by Malaysian Computer Emergency Response Team (MyCERT). MyCERT had claimed that most of the system or network administrators in Malaysia are not practice proactive action to secure the computer system before the attacks are exist and breach into one of the server or computer network. So, these things will make Information and Communication Technology (ICT) facilities become slowly the process or usable use. Then, it will be affected to the quality and quantity of productions and business strategy in the organizations. [1]

Vulnerability Assessment is proactive action which mean tahat the process to show and report the existing vulnerabilities inside the computer network. It will provide scanning computer network to detect the existing vulnerabilities and suggest the action that should be take on it before it use by irresponsible person. It also provide the level of security for that vulnerabalities such as low, medium and high level. [2]

So, the purpose of this study is to do vulnerability assessment inside the computer network system that will permit the possible exploits. Then, provide general useful tips and guidelines from the report to manage and minimize those weaknesses in the computer network system at FTMM, KUiTTTHO.

MATERIALS AND METHODS

Open source vulnerability scanning tool, Nessus had used as a tool to detect and capture information about the vulnerabilities that exist inside the nodes of the computer network. Nessus is the client-server application. [3]

Security Life Cycle or SLC had used as a methodology to do the vulnerability assessment inside the computer lab. [4] The phases of this methodology can be view inside the figure 1 below.

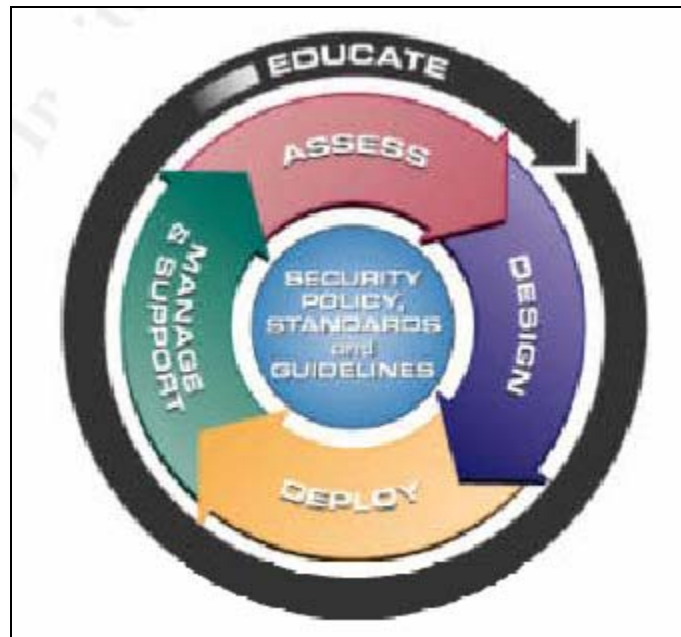


Figure 1 :Security Life Cycle (Lee, Wan Wai.(2001)). “Security Life Cycle – 1. DIY Assessment.” SANS Institute 2001.

In the first phase or assess’s phase, vulnerability scanning had done by using Nessus to determine the existing holes that have inside the computer networking lab. Assessment had done over 30 nodes inside the lab.

Then, in second phase, the result of the vulnerability that had in phase one will be analyse for designing of proper configuration according to the standard of CVE or Common Vulnerabilities and Exposures. In this phase, planning to design the proper solution to overcome existing vulnerabilities had done. It’s very important to understand in detail on each existing vulnerability for the designing the best solution. [5]

The next phase is the process to deploy the solution that had be designed on the each vulnerability such as closed unneeded port, update the patch, deploy security fix and others.

The last phase is very important to be sure all the configuration or solution that had be done can be done in functionally and it also can become problem identifier. In this phase, vulnerability scanning and assessment will be done severally to be sure the vulnerabilities are in the minimum level or none.

RESULTS AND ANALYSIS

The result from this vulnerability scanning task by using Nessus can be categorized into two types which it including the result of the vulnerability scanning on the phase 1 of SLC and the result of vulnerability scanning on the phase 4 of SLC.

In the phase 1, the result of the vulnerability scanning can be view from the Figure 2 and Table 1. In this result, the vulnerability had categorized by its type of security such as security notes, security warning and security holes. [6]

Security note is information about the open ports or available services that exist inside the hosts. Security warning is information about available open ports or services too but it can be vulnerable into possible attack.

Security hole is information about open ports or available services that already vulnerable in the computer network system and available use by an attacker to launch an exploit.

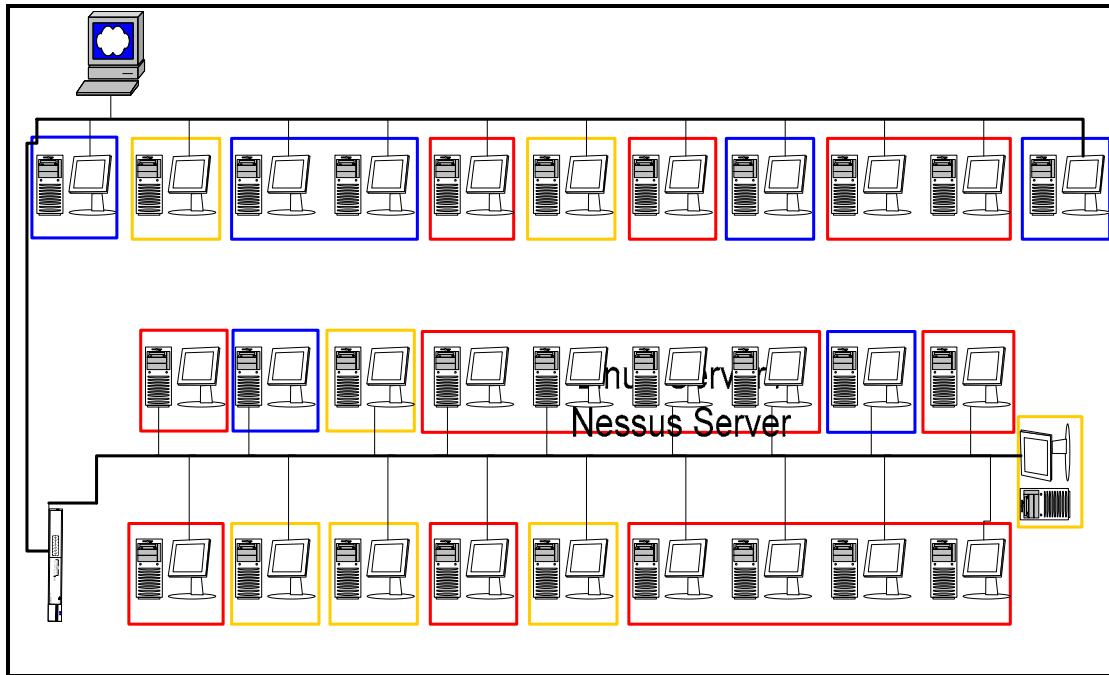


Figure 2: Reference nodes that available of vulnerability in the lab

Table 1: the result of vulnerability on the phase 1 of SLC

Lab	Security holes	Security warning	Security notes
Networking Technology	71	141	501

There is around 7774 of plug-ins that is very specific type of vulnerability that are located inside the Nessus application server to use for checking security hole or vulnerability. Then, all this plug-ins is classify into 33 types of family plug-in.

From the Table 1, there were 71 of the security holes, 141 of the security warnings and 501 of the security notes that exist over the 30 hosts inside the networking technology lab in the phase 1 of SLC.

The result in the phase 1 will be analyzed for doing the tasks in phase 2 and phase 3 of SLC in this vulnerability assessment study.

In the phase 4, the result of the vulnerability scanning can be view from the Table 2. In this result, the vulnerability had also categorized by its type of security such as security notes, security warning and security holes.

Table 2: the result of vulnerability on the phase 4 of SLC

Lab	Security holes	Security warning	Security Notes
Networking Technology	17	29	144

From the Table 2, there were 17 of the security holes, 29 of the security warnings and 144 of the security notes that exist over the 30 hosts inside the networking technology lab in the phase 4 of SLC.

The result in the phase 4 will be analyzed for doing again all the phases in the SLC to minimize or remove all the vulnerabilities. It also shown the result in the phase 2 and 3, whether the solution that had be take in action is success or fail in this vulnerability assessment study.

In the 30 available and alive hosts at the lab's computer network, there is possibly having open ports within the available services. So, Nessus application had scan all over that open ports and available services that exist on it. In the Nessus's report, security holes are referring to the weaknesses or possible exploits that are very important to analysis in this study. [7]

From the result, this study had found that more than 80% of the security holes are categorize on the Windows's vulnerability and the others are categorized on Gain Root Remotely, CGI abuses and Miscellaneous by referring it to the types of family for Nessus plug-in.

For example in the non-server application, software that run under the Window's environment like Internet Explorer, Macromedia Flash, Microsoft Visual Basic and others is full of lack in the security aspects because of bugs and viruses. So, the installation, configuration and maintenance for all the software that run under Window's environment must be doing properly with full of awareness on its security aspect like patching, configuration setting and others. [8]

DISCUSSION

At the end of this study, there are several of recommendations, practices and actions that are need to be revised for solving and minimize the problems of possible exploits or vulnerabilities from the Nessus report as soon as possible.

There are two types of action that should be taken which it in technical overview and management overview. In the management overview, continuously actions that should be needed to consider are provide a proper, suitable and practice security policy in the organizations and provide education program to educate the staff on using IT facilities in wellness and secure.

In the technical overview, continuously actions that should be needed to consider are (1) proper installing and configuration the applications or software, operating system and hardware base items like firewall, router and other that need to revise its patching, bug and security fix, (2) close all unneeded ports and services on every node or hosts in the computer network system, (3) keep regularly perform the practice of security audits and security assessments, (4) keep regularly update the patching, bug and security fix in any software, application, operating system and network components and (5) avoid the practices in default installation. All this actions are for the better practices of computer network security in the future.

CONCLUSION

In this vulnerability assessment the number of vulnerabilities and the number of possible vulnerabilities had reduced more rather than before. However, the process of vulnerability assessment is needed more time and efforts to make it zero vulnerability.

Then, the vulnerability assessment must have done regularly due to expanding of exploit, vulnerability or threat that is always changing and reform.

All the most valuable information of this security holes or possible vulnerability regarding to the weaknesses in the computer network security in this study had produced by powerful of Nessus. The weaknesses or security holes are the same situation with the improperly lock or close the doors or windows in the house. So, that condition can be possibly compromise in the security aspect to allow unauthorized person to hack in that house. Within the lack of practices like that situation, it may invite the most dangerous of threats or attacks into the computer system.

Today, computer network security is involves in very tough area that needs to meet any level of risks that are acceptable. But, the main key to practice effectively in the computer network security is it must meet the organization missions, goals, security policies and security practices at the preliminary action. [9]

The lack of this study is the vulnerability assessment had done in certain selected vulnerability and possible vulnerability only in the lab because of the limitation time and effort. However, the contribution of this study is more valuable that can increase the level of sensitivity, awareness and knowledge regarding to the computer network security among the staffs at FTMM. Then, this study and network security assessment can be done to the overall computer network system at FTMM in the future in continuously within the proper practices.

REFERENCES

- [1] 'Awat! Pencerobohan laman web besar-besaran', http://www.mycert.org.my/news/2004_01_28_01.html [30 May 2004]
- [2] Bauer, M. (2001). "Paranoid Penguin: Checking Your Work with Scanners, Part I (of II): nmap" *Linux Journal. Volume* 2001 , Isu 85 (Mei 2001).
- [3] Bauer, M. (2001). "Paranoid Penguin: Seven Top Security Tools" *Linux Journal. Volume* 2004 , Isu 118 (Februari 2004).
- [4] Lee, Wan Wai. "Security Life Cycle – I. DIY Assessment." (Versi 1.0, November 13, 2001), *SANS Institute* 2001.
- [5] Blaha, K. D. and Murphy, L. C. (2001). "Targeting assessment: how to hit the bull's eye" *Journal of Computing Sciences in Colleges. Volume* 17 , Isu 2 (Disember 2001).
- [6] Deraison, R., Haroon Meer, Temmingh, R., Walt, C., Raven Alder, Alderson, J., Johnston, A., Theall, G. A. (2004). "Nessus Network Auditing." *Syngress*.
- [7] Bauer, M. (2001). "Paranoid Penguin: Checking Your Work With Scanners, Part II: Nessus" *Linux Journal. Volume* 2001 , Isu 86 (Jun 2001).
- [8] Whitman, M. E. (2003). "Enemy at the gate: threats to information security" *Communications of the ACM. Volume* 46 , Isu 8 (Ogos 2003).
- [9] Firkhan Ali, H. A. , " An Analysis of Possible Exploits in the Computer Network's Security " in ISC 2005 : Proceedings of the International Science Congress 2005. PWTC, Kuala Lumpur, 2005. pp.338.