International Journal of Computer and Information System (IJCIS)
Peer Reviewed – International Journal
Vol : Vol. 03, Issue 02, June 2020
e-ISSN : 2745-9659
https://ijcis.net/index.php/ijcis/index

Campus Website Security Vulnerability Analysis Using Nessus

1st Muhammad Abdul Muin, 2ndKapti, 3thTri Yusnanto
[1]Informatics, STMIK Bina Patria,[2]Informatics, STMIK Bina Patria,[3]Informatics Managenent, STMIK Bina Patria
[1,2,3]Magelang, Jawa tengah, Indonesia
[1]muin@stmikbinapatria.ac.id, [2]tensmart18@stmikbinapatria.ac.id, [3]yusnanto@stmikbinapatria.ac.id

***Abstract*—** *Security is a concept of securing data from hacker attacks, Agencies or organizations are competing to create websites for their agencies, where this website to make work easier or disseminate information to the public in this study is a college or campus website. With this website, many people access it, so there is a possibility of security holes, which can be exploited by irresponsible people. So that data can be manipulated, retrieved or otherwise to the detriment of one-sided or several parties. For this reason, we tried to analyze the vulnerability of a website using a software called Nessus. From the results of the scan, it was found that several vulnerabilities were found from each website with different vulnerability levels. Of the 3 websites that have the most vulnerabilities, web 1 is 14. Meanwhile, the vulnerability at the medium level is on web 2, which is 22%. For the vulnerability lies in a weak DNS Server*.

Keywords : Vulnerability, Nessus, Website.

I. INTRODUCTION

With advances in technology for now agencies or organizations are competing to create websites for their agencies. [1] In recent years, human work has become easier with the existence of a website. According to Nick Huss on his website [2] in the world of existing websites (05/04/2022) there are 1,179,448,021 active websites and 200,756,193 websites. Which will always increase every day for today the addition of about 252000 websites or about 3 websites every second globally. [3] A website is basically a collection of documents containing data and information that can be accessed via the internet. One of them is a university website which is carried out for the academic interest of the university.

STMIK Bina Patria is one of the universities that utilizes the website, which has several websites and web-based applications. Among them are campus portals, PMB (New Student Admissions) website, Siakad, e-learning, journals, CDC (Career Development Center). This website has been accessed through the internet network, so anyone can access it. Websites that are connected to the internet without being equipped with an adequate system will have attacks on the website intended to steal data/information, change data, or also intended to disable the services provided by the website [3]. Web-based applications allow users to share and manipulate information using various platforms. [4] A weakness in a computer network system is often ignored, so that if there is a threat or destructive attack on the system, the impact will be worse and very detrimental. Considering the dangers and disadvantages of misuse of services on local networks and all internet-based applications today, it is imperative that businesses and organizations implement first-step strategies to mitigate them. So it is necessary to analyze the vulnerability of a website.

In his research [5] showed that nessus to detect vulnerabilities faster than Netclarity. Additionally [6] In terms of speed without the Web App feature on, Nessus works much faster than Retina; on the other hand, with the Web App module active, Nessus performance is much slower than Retina. In terms of scan depth, Nessus has a slight advantage, as it includes a very helpful web mirroring tool in HTTP. From both research, nessus makes the scanning process faster. According to [3] Vulnerability analysis is a process that defines, identifies, classifies security vulnerabilities (vulnerabilities) in computers, networks, or communications infrastructure. For this reason, researchers want to examine the maturity level of campus websites using Nessus

II. RESEARCH METHODS

This research was conducted at STMIK Bina Patria. The data collection methods used to obtain the data are as follows:

1. Interview

In this case, the researcher conducted an interview with the website manager under the auspices of STMIK Bina Patria.

2. Observation

In this case, the researcher conducted an interview with the website manager under the auspices of STMIK Bina Patria.

We hereby scan the STMIK Bina Patria website. In this case, there are 3 websites that we are trying to analyze for maturity. Because of the existing websites, there are only 3 servers, so we tried to do a sample that is often used by the STMIK Bina Patria academic community, as many as 3 websites, which we call web1, web2, web3. For the analysis of maturity, the researcher uses security scanner software, namely Nessus version 8.13.1 free trial, which we can download for free on the tenable.com website. For which for severity base using CVSS v2.0.

2.1 Vulnerability

The Vulnerability Scanner consists of four main modules: user interface, scan engine, vulnerability database and report module. There are many Vulnerability scanners, some of which are free and Open Source (or have a free version with limitations) while others can be very expensive. For our purposes, a key requirement is the ability to create custom tests and custom reports by combing the results with our own metrics and formulas to generate a summary of the total network security.

Alternatively, the report must be exportable in such a way that the data can be retrieved by an external program if we wish to perform the generation of overall security flags and externally proposed stochastic models.

Vulnerability is a point of weakness where a system is vulnerable to attack. [8]. [3] Explains that Vulnerability assessment is a process that defines, identifies, classifies security holes in a computer, network, or communication infrastructure. In addition, vulnerability analysis can estimate the effectiveness of the proposed countermeasures and evaluate their actual effectiveness once they are implemented. The results of the vulnerability assessment activity can be used to determine the security maturity level of a website. In this case, the researcher is to find out the security gap or what can be called the Vulnerability Assessment of a website by scanning it using a software called Nessus.

2.2. Nessus

Nessus is a software, maintained by Tenable.sc. which we can use by way of subscription and or can use the free version. [7] Nessus has become one of the most popular vulnerability scanners mainly due to the fact that it was originally Open Source and Free until 2005 when they closed the source code in 2005 and removed the free version in 2008. From its usefulness Nessus is a piece of software that works to help organizations or industry as a security scanner that will audit the intended network, then determine the weaknesses of the intended network. for example in this study is the STMIK Bina Patria website. In addition, scanning with Nesuss requires a faster time than Netclarity [5].

Nesssus managed by Tenable provides vulnerability levels ranging from Critical, high, medium, low, and finally info based on CVSSv2 Severity Base [9]. Which can be seen in table 1 below:

Tabel 1. Range CVSSv2

Severity	*CVSSv2 Range*
Critical	Skor CVSSv2 kerentanan tertinggi *plugin* adalah 10.0.
High	Skor CVSSv2 kerentanan tertinggi *plugin* adalah antara 7,0 dan 9,9.
Medium	Skor CVSSv2 kerentanan tertinggi *plugin* adalah antara 4.0 dan 6.9.
Low	Skor CVSSv2 kerentanan tertinggi *plugin* adalah antara 0,1 dan 3,9..
Info	Skor CVSSv2 kerentanan tertinggi *plugin* adalah 0, atau bisa disebut *Plugin* tidak rentan.

An example of the Nessus application can be seen in the following image:

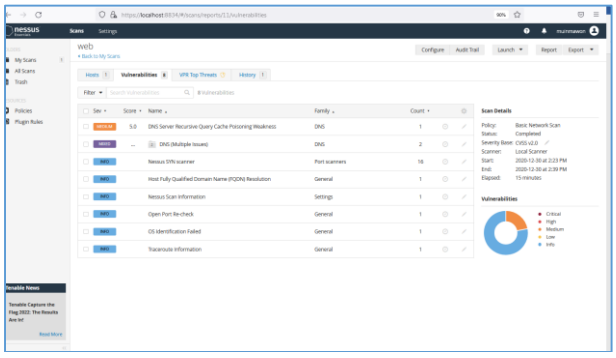

Figure 1. Example screenshot of the nessus application

III. RESULT AND ANALYSIS

In this discussion contains the concept of implementing system security. Nessus will audit or assess the targeted website, by scanning the website and then determining the weaknesses of the STMIK Bina Patria website. Among the 3 websites there are security holes, which can be seen in table 2.

Table 2. Scanning Recap Results Using Nessus

	Vulnerabilities	*Critical*	*high*	*medium*	*low*	*info*
Web 1	14			14%		86%
Web 2	8			22%		78%
Web 3	13			13%		87%

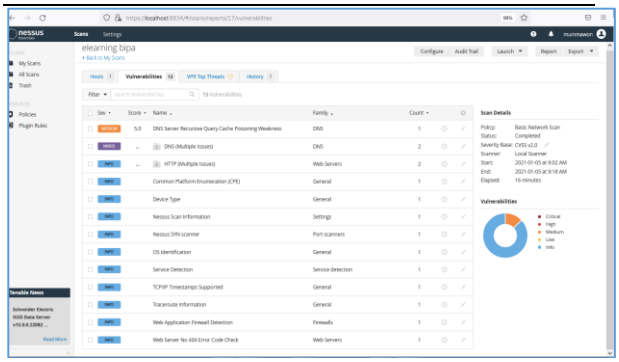

Figure 2. Scan capture results with Nessus

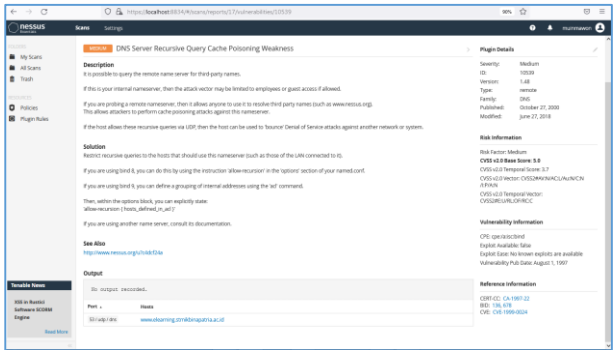

Figure 3. The results of the scan capture with nessus at medium level

From the scans using the Nessus Scanner that the researchers did from 3 websites, we found several vulnerabilities. Where that has the most vulnerabilities is web1, as many as 14. Meanwhile, the vulnerability at the medium level lies in web2, which is 22% and, according to the severity base, uses CVSS v2.0. the range is in the range of 4.0 to 6.9. colored in orange.

All websites have vulnerabilities categorized by medium, either web1, web2, web3. For the medium vulnerabilities, everything lies in the weak DNS Server which can be seen in Figure 4. While the others are only at the info level. With this scan, it is hoped that later weaknesses can be corrected and reduce the risks that occur on the website.

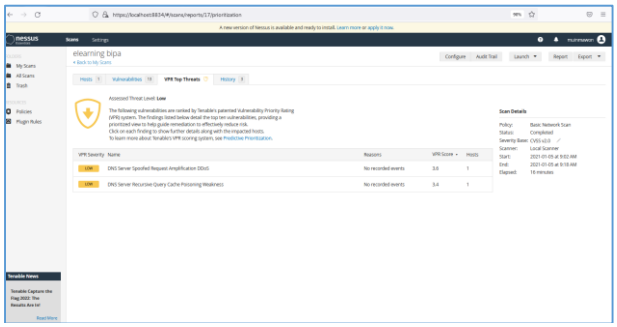

Figure 4. Vulnerability Priority Rating

In Figure 5 the scan results for range info are explained that Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to collect one or more fingerprints from a remote system. Unfortunately, Nessus currently doesn't know how to use it to identify the system as a whole

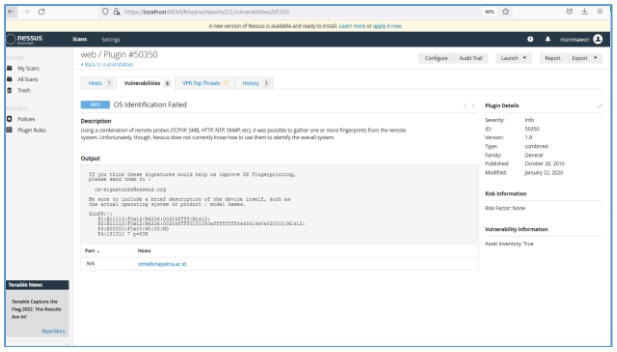

Figure 5. Capture Scan for info

IV. CONCLUSION

From the results of testing the STMIK Bina Patria campus website by scanning it using a software called Nessus. Found several vulnerabilities from each website with different vulnerability levels. Of the 3 websites that have the most vulnerabilities, web 1 is 14. Meanwhile, the vulnerability at the medium level is on web 2, which is 22%. For the vulnerability lies in a weak DNS Server. The final result of this research is the formation of an application program that can monitor the system for system security.

REFERENCES

[1] W. Wardana, A. Almaarif, and A. Widjajarto, "Vulnerability assessment and penetration testing on the xyz website using NIST 800-115 standard," *J. Ilm. Indones.*, vol. 7, no. 1, pp. 520–529, 2022.

[2] N. Huss, "How Many Websites Are There in the World?," *siteefy.com*, 2022. [Online]. Available: https://siteefy.com/how-many-

websites-are-there/#:~:text=Currently%2C there are around 1.18 billion websites in the World.

[3] I. G. N. Mantra, M. S. Hartawan, H. Saragih, and A. A. Rahman, "Web vulnerability assessment and maturity model analysis on Indonesia higher education," in *Procedia Computer Science*, 2019, vol. 161, pp. 1165–1172.

[4] S. Ariyani, "ATCS System Security Audit Using Nessus," *J. Inf. Eng. Appl.*, vol. 7, no. 3, pp. 24–27, 2017.

[5] S. Chimmanee, T. Veeraprasit, K. Sriphaew, and A. Hemanidhi, "A Performance Comparison of Vulnerability Detection between Netclarity Auditor and Open Source Nessus," *Recent Adv. Commun. Circuits Technol. Innov.*, pp. 280–285, 2012.

[6] R. Kushe, "COMPARATIVE STUDY OF VULNERABILITY SCANNING TOOLS: NESSUS vs RETINA," *Int. Sci. J. "Security Futur.*, vol. YEAR I, no. 2, pp. 69–71, 2017.

[7] I. Chalvatzis, "Reproducible modelling and simulating security vulnerability scanners evaluation framework towards risk management assessment of small and medium enterprises business networks," *Indian J. Sci. Technol.*, vol. 13, no. 37, pp. 3910–3943, Oct. 2020.

[8] I. Kamilah and A. Hendri Hendrawan, "Analisis Keamanan Vulnerability pada Server Absensi Kehadiran Laboratorium di Program Studi Teknik Informatika," in *Prosiding Semnastek*, 2019, vol. 16, no. 0, pp. 1–9.

[9] Tenabel, "Nessus 8.14.x User Guide," 2022. [Online]. Available: https://docs.tenable.com/nessus/8_14/Content/PDF/Nessus_8_14.pdf.