International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Vulnerability Analysis of Wi-Fi System Using Nessus Scanner

Hengky Satria Putra S.T, M.T[1]
[1] Department of Information Technology, Gunadarma University, Jakarta, Indonesia, 10440

Abstract— *A wireless attack may occur even before the users realize it. It is not easy to state that wireless is safe from attack. If a hacker can break the password, he/she will be able to access that network easily. In order to find out the wireless vulnerability, Nessus vulnerability scanner can be used. Based on the result of the study, it was found that the lab's wireless security contains 1 medium vulnerability and 18 informal. The result of the study can be useful information for the user.*

Keywords— *Wireless, Penetration Test, Vulnerability Analysis, Vulnerability Report.*

I. Introduction

In this digital era, it is difficult to protect data privacy security. Wi-Fi is one of the accesses to connect to internet. Wireless network security systems should gain attention, considering that a hacker has many ways to attack the wireless network, such as Denial of Services Attacks, Man-in-the-middle, etc. To anticipate data theft done by the hacker, it is necessary to find the security hole through a vulnerability scanner.

A vulnerability scanner is capable of detecting a security hole in the wireless system. By scanning wireless system vulnerability, unprotected aspects of vulnerability can be found. Scanning vulnerability may lower the risk of the system. There are many software developed for scanning Wi-Fi system vulnerability, such as Nessus, Retina, among other software. In the journal "Wi-Fi Network Vulnerability Analysis and Risk Assessment in Lebanon", using kismet and Acrylic Wi-Fi Professional. The researchers currently focus on testing wireless vulnerability systems using Nessus scanner. Using such software, the wireless system vulnerability can be detected. The report can be generated in several formats. This vulnerability analysis may help IT auditor and compliance to close all holes in the system.

II. Literature Review

A. Wireless Fidelity (Wi-Fi)

Wi-Fi stands for wireless fidelity. Wi-Fi is the abbreviation of a trademarked phrase that means IEEE 802.11x. It is a short-distance wireless transmission technology [1]. It reaches about 100 meters. By using Wi-Fi, users do not need to use LAN cable to connect to the internet. Users are connected to Wi-Fi through high-frequency electromagnetic waves.

Currently, Wi-Fi has experienced significant improvement. It has broader coverage and faster data transfer speed. Wi-Fi is often used in the office area, residential area, cafe, hotel, and many other places. To access the internet is a human necessity nowadays, through Wi-Fi, this necessity is satisfied easier. Regarding cost, the use of Wi-Fi is affordable from some internet providers.

Wireless was once connected to LAN cable in transmitting data, nowadays, many users switch to fiber-optic cable since the latter is considered faster than LAN cable. Fiber-optic cable can be considered as new and fast in data transmission. However, its expensive cost is viewed as a burden by some users.

B. Penetration Test

Penetration testing, or usually called pentesting, or ethical hacking, refers to a practice of testing a system of computer, network, or web application to find out the security vulnerability that may be exploited by an attacker [2]. Penetration testing is crucial for a company. It is helpful for the company to increase its security system. Some steps should be carried out in pen testing, such as information gathering, vulnerability analysis, and reporting.

Pentesting is usually done by the Cyber Red Team (CRT). CRT imitate the thinking and action pattern of the attacker to improve the organization's security [3]. Pentesting requires NDA containing the scope of the test. In pen testing, not all penetrations succeed. Some of them fail, meaning that the system is secure. Nowadays, there has been some certification relating to pen testing, such as CEH (Certified Ethical Hacker), OSCP (Offensive Security Certified Professional), among others. The followings are the steps of pen testing in general.

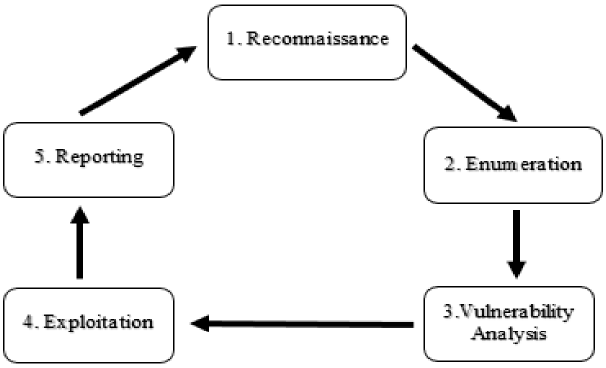


Fig. 1. Penetration Test Cycle.

C. Vulnerability Analysis

Vulnerability analysis refers to an action where a tester seeks and finds the system vulnerability in the test target to be analyzed. Based on the result, the tester finds the weakness of the system, such as user's misconfiguration, open port, unprotected access. Vulnerability Analysis is divided into two, active and passive. After finding the weaknesses in an active and passive form, the findings are validated.

D. Vulnerability Report

A vulnerability scan was conducted to reveal the security hole of the wireless. Once the scanning process completes, the next step is to generate report in the determined format such as pdf, csv, or html. This report is important for the IT audit party or pentester to find out the data on vulnerability.

III. Research Methodology

In analyzing the vulnerability of the Wi-Fi, Nessus software with interface display (GUI) was employed. This method was selected since it is suitable to find the vulnerability of the Wi-Fi. Nessus will scan IP 192.168.8.238 on wireless.

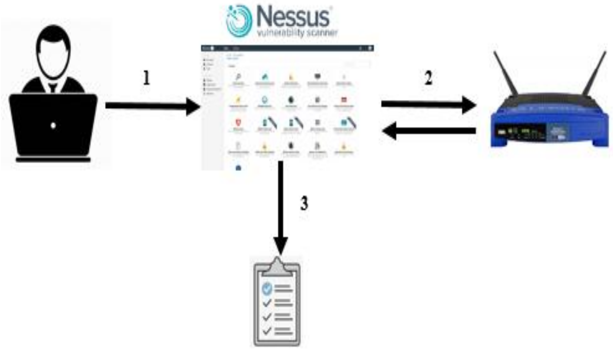


Fig. 2. Flow of Scanner using Nessus

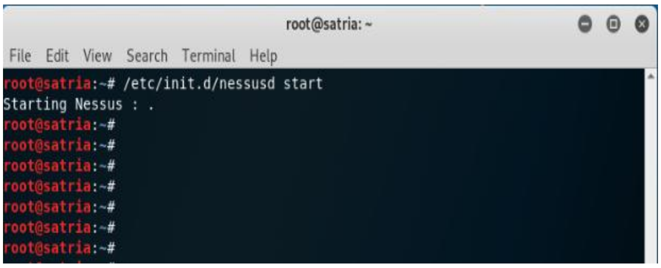
Information:
1. Vulnerability Analysis
2. The tester scans the wireless target using Nessus
3. The tester generates scan result report

IV. Discussion

A. Vulnerability Analysis

Vulnerability analysis conducted in the present study analyzes the vulnerability of the wireless system by using Nessus. The followings are steps of the test using Nessus.

1. Before using Nessus, it is required to run service Nessus; if service Nessus is not activated, Nessus will not open. To activate Nessus service, the following comment is used.
   # /etc/init.d/nessus start



```
root@satria:~# /etc/init.d/nessusd start
Starting Nessus : .
root@satria:~#
root@satria:~#
root@satria:~#
root@satria:~#
root@satria:~#
root@satria:~#
root@satria:~#
```

Fig. 3. Start Nessus Services.

2. The next step is to enter Nessus's web portal using a web browser. To open Nessus web portal, that link can be used Then, log in to Nessus Essentials. https:/localhost:8834/

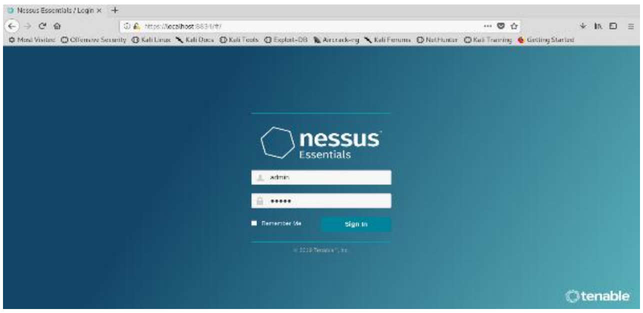


Fig. 4. Nessus Web portal

3. After logging in, the web shows its homepage. To run the wireless vulnerability scan, click 'new scan' in the 'my scans' tab.
4. Enter the scan template. Here some scan templates are displayed. Since we use the free trial version, the scan template was limited. Then, select 'advanced scan'.

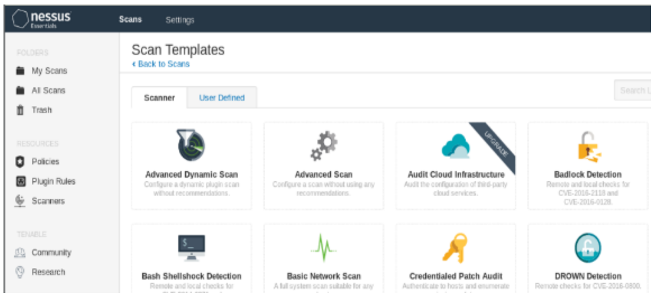
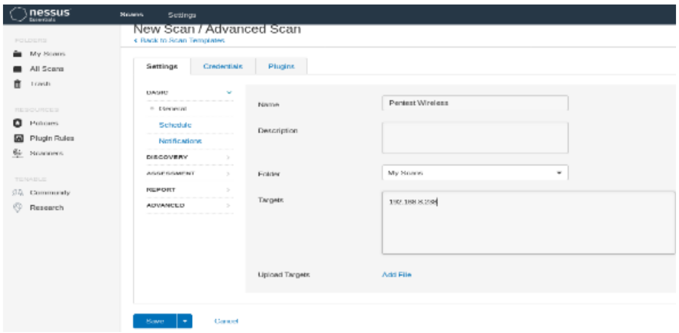


Fig. 5. Advanced Scan

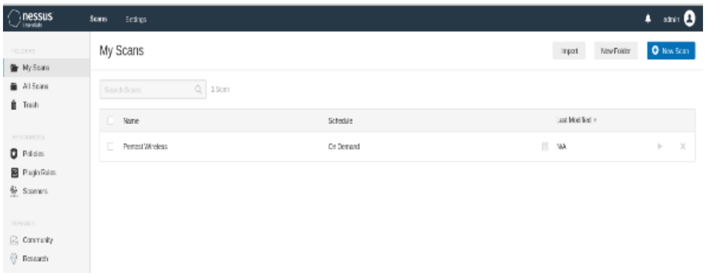
5. In general setting, there are some setting options, I used default scan by setting the target's IP, and click save.



Name: Pentest Wireless
Description:
Folder: My Scans
Targets: 192.168.8.238

Fig. 6. Target IP Setting

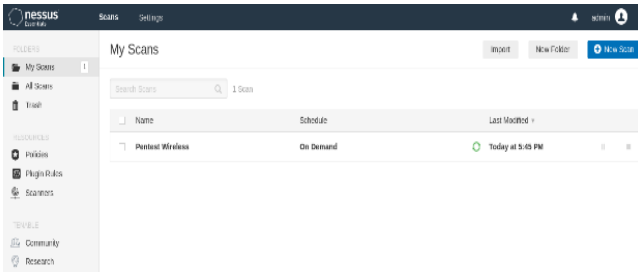
6. After entering target's IP, the next step is run the scanner by clicking play/start button.



Name	Schedule	Last Modified
Pentest Wireless	On Demand	N/A

Fig. 7. Start scanning

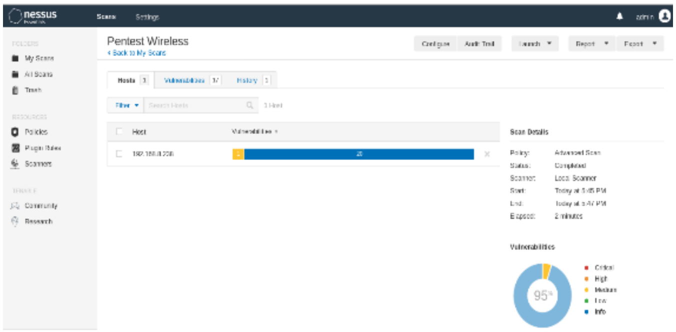
7. The Scanning process is running, wait until it is completed. This process takes about 10 minutes. However, it depends on the target and the setting.



Name	Schedule	Last Modified
Pentest Wireless	On Demand	Today at 5:45 PM

Fig. 8. Scanning Process

8. Once the scanning is completed, the data on vulnerability is displayed, it is shown in host, vulnerabilities, and history tabs. The chart in this beginning indicate vulnerabilities found in the scanning process.

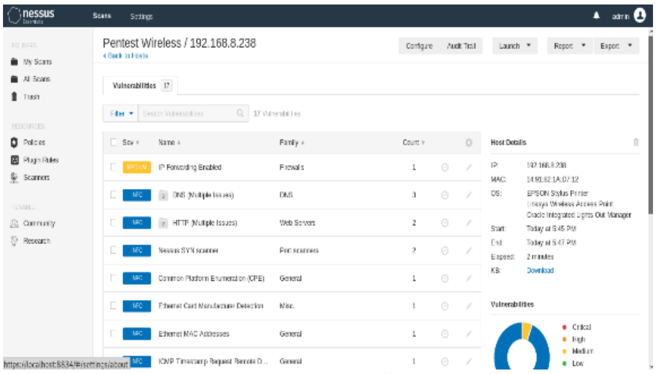


Scan Details

Policy: Advanced Scan
Status: Completed
Scanner: Local Scanner
Start: Today at 5:45 PM
End: Today at 5:47 PM
Elapsed: 2 minutes

Fig. 9. Info Host in Nessus

9. In the vulnerability tab, there is a list of severity, ranging from critical, high, medium, low, or info. It was found that there was only 1 medium vulnerability, namely IP Forwarding Enabled on firewall, while the rests contain only severity info.



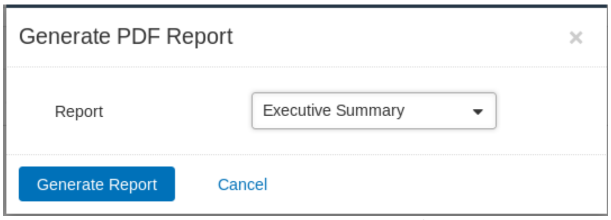
Sev	Name	Family	Count
MEDIUM	IP Forwarding Enabled	Firewalls	1
INFO	DNS (Multiple Issues)	DNS	3
INFO	HTTP (Multiple Issues)	Web Servers	2
INFO	Nessus SYN scanner	Port scanners	2
INFO	Common Platform Enumeration (CPE)	General	1
INFO	Ethernet Card Manufacturer Detection	Misc.	1
INFO	Ethernet MAC Addresses	General	1
INFO	ICMP Timestamp Request Remote D...	General	1

Host Details

IP: 192.168.8.238
MAC: 14:91:82:1A:07:12
OS: EPSON Stylus Printer
Linksys Wireless Access Point
Oracle Integrated Lights Out Manager
Start: Today at 5:45 PM
End: Today at 5:47 PM
Elapsed: 2 minutes
KB: Download

Fig. 10. Vulnerability Info in Nessus

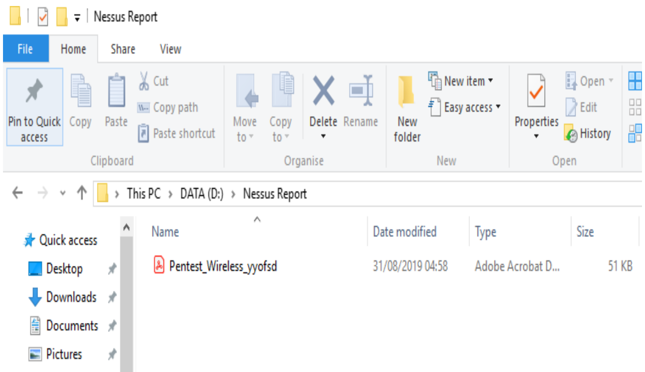
10. To show the report in Nessus web portal, click report, then select the format (csv,pdf, or html). After selecting the format, select the report template. We used executive summary, wait until the report generating process is finished.


Generate PDF Report

Report: Executive Summary

Fig. 11. Generate report pdf

11. Once the report is generated in pdf, it becomes more concise due to the selected template.

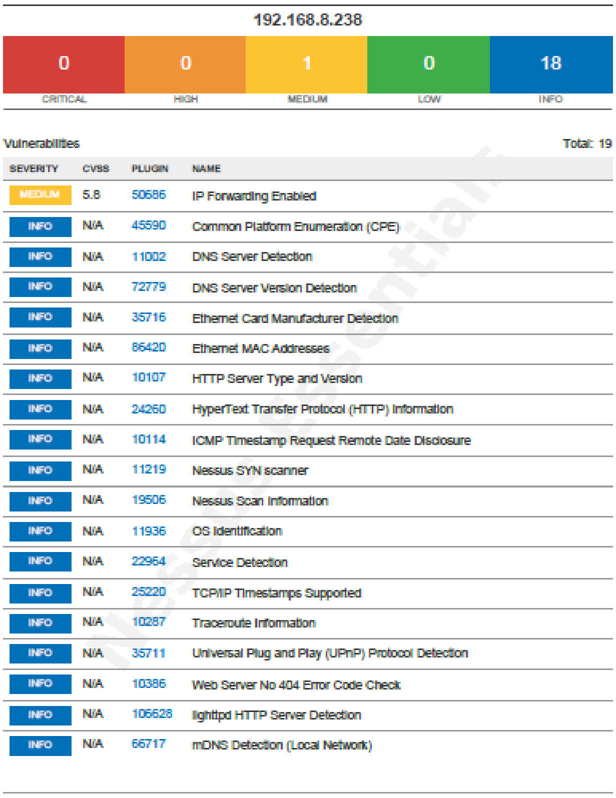


Name	Date modified	Type	Size
Pentest_Wireless_yyofsd	31/08/2019 04:58	Adobe Acrobat D...	51 KB

Fig. 12. Nessus Report Folder

V. Result

After scanning the Wi-Fi vulnerability, the report will explain some vulnerabilities of the Wi-Fi system. The result of vulnerability scanning of the Wi-Fi system is as follow:


192.168.8.238

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	1	0	18

Vulnerabilities Total: 19

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	5.8	50686	IP Forwarding Enabled
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	11002	DNS Server Detection
INFO	N/A	72779	DNS Server Version Detection
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11936	OS Identification
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	10287	Traceroute Information
INFO	N/A	35711	Universal Plug and Play (UPnP) Protocol Detection
INFO	N/A	10386	Web Server No 404 Error Code Check
INFO	N/A	106628	lighttpd HTTP Server Detection
INFO	N/A	66717	mDNS Detection (Local Network)

Fig. 13. Nessus Scanning Result

VI. Conclusion

In this study, we focused on wireless scanning by using an open source version. Vulnerability scanner software, namely, Nessus. This open source software has some limitations in some features. Based on the test conducted in our lab, it could be concluded that the wireless had 1 medium vulnerability and 18 informal. Using Nessus for vulnerability scan is helpful for users to make them more aware of security system of a wireless. Future works should focus on evaluating performance based on other features to detect wireless vulnerabilities

References

[1] Adel Ismail Al-Alawi "WiFi Technology: Future Market Challenges and Opportunities" Journal of Computer Science, 2006.

[2] Pawan Kesharwani, Sudhanshu Shekhar Pandey, Vishal Dixit, Lokendra Kumar Tiwari "A study on Penetration Testing Using Metasploit Framework" International Research Journal of Engineering and Technology (IRJET), 2018.

[3] Pascal Brangetto, Emin Çalişkan, Henry Rõigas "Cyber Red Teaming" NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) Tallinn, Estonia, 2015.

[4] Sheetal Bairwa1, Bhawna Mewara2, Jyoti Gajrani3 "Vulnerability scanners : A Proactive Approach to Asses Web Application Security" International Journal, 2014.