WLAN Penetration Examination of The University of Pembangunan Panca Budi

Akhyar Lubis[1] , Andysah Putera Utama Siahaan[2]

Faculty of Computer Science, Universitas Pembangunan Panca Budi
Jl. Jend. Gatot Subroto Km. 4,5 Sei Sikambing, 20122, Medan, Sumatera Utara, Indonesia

Abstract–*Hacking and cracking passwords on Wi-Fi in campus location is criminal acts that might approach because it could be considered stealing. Many Wi-Fi SSID are protected. It means that the owner of the Wi-Fi does not allow connections used freely by strangers. The are Many ways to crack it. A penetration test is one of the popular techniques to break the password. This tool directs the user to try to connect to the similar SSID name. However, they do not realize the name they join in is a fake SSID. This moment is used by the attackers to obtain the password. Soon after they try to connect several times, the attacker has been already recorded the SSID password.*

Keywords –*Security, Penetration Test, Hacking, Wi-Fi*

I. INTRODUCTION

Internet connectivity continues to grow up as millions of new devices are connected to the global network [4].Many users do not know the danger of wireless connections [6]. Security is the big problem of information system [3]. The University of Pembangunan Panca Budi has implemented the IS / IT as a supporting system. It triggers business in the world of education. A critical issue for educational institutions is the threat of a rise in attacks against information systems. This problem is due to a combination of increasingly sophisticated attack tools and automated, the growing number of discovered attacks and improved user connectivity. As the system is open to students, staff, faculty and accessible in public, so the network becomes more complex and more vulnerable to security breaches. That is why the problem of information security is one of the most challenging problems faced by companies and educational institutions.The IT administrator keeps trying to improve the the security to protect the data from being stolen.

The first thing before making the attack, we have to do a Reconnaissance. It makes our target is familiar to us [1].Penetration testing is performed on a wireless network in the Faculty of Computer Science to identify the weaknesses and the uncover risk of the system on a wireless network [2][5]. Testing allows use several methods to get into the target tissue, often to penetrate network security system begins at a relatively low priorities parts and then used it to attack sensitive areas. One of them is the attacker will try to get into the network infrastructure. It can easily monitor the activities of the user or users via a wireless network. The attacker must be able to enter into the internal network via wireless LAN.

II. THEORIES

Several models authentication such as MAC address filtering, WEP, WPA, WPA2, SSID filtering and Filtering Protocol can secure LAN and WLAN. The University of Pembangunan Panca Budi uses a cable-based LAN connection and wireless. Almost all users, faculty staff, students and employees take advantage of this technology. They cover several points installing the hotspot in some areas. It makes the signal covers the entire area of the campus location. There are several points of the access point used by employees to access the local network of information systems related to the employee, the financial system and the academy system. The administrator gives the password using WPA2 security system to users who want to access the network.

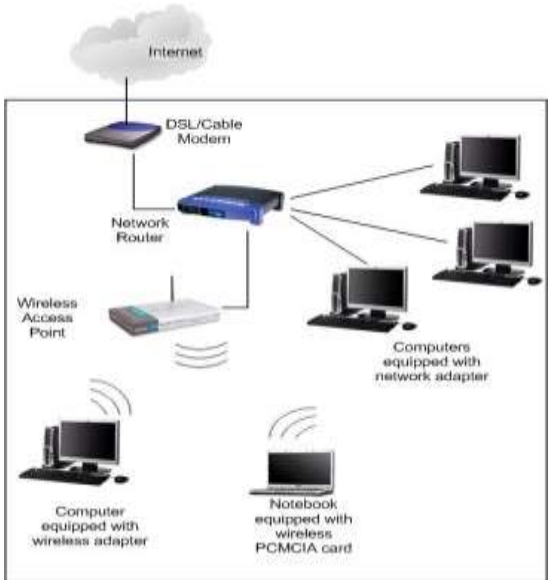

Fig. 1 The network diagram

Figure 1 is the example the network diagram on campus. As we can see, there are various computers connect to the Wi-Fi available. We do not know who, where and when the attackers attack the security. Some of them can use direct cable connection or even

hack the wireless signal. Wireless connection is less secure than cable. We have to strengthen the security to avoid the intruder to breach the firewall.

III. Proposed Work

This research uses both software and hardware. Figure 2 is Leguang LG-N960. It is one of the external wireless that has a penetration module. We use the external wireless USB adapter that supports injection and sniffing. This device has a 23dBi panel antenna. It has 10 meters internal cable. It allows the placement using a pole antenna. This hardware works at 2.4GHz of standard protocol 802.11bgn by using Ralink RT3070 chipset include 30 dBm transmit power. It claims that this hardware can manipulate the Wi-Fi signal stronger than another.

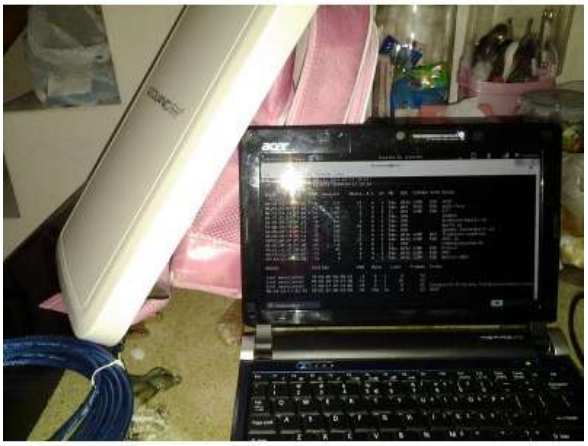

Fig. 2Leguang LG-N960

The software needed is Linset. It is a hacking tool that runs on the Linux Operating System. It allows the attacker retrieve the Wi-Fi password which secured by WPA or WPA2 security type without having to use the brute force wordlist. Linset techniques used on "Evil Twin Attack" which is a technique used attacker to create a wireless network name is the same as the original name of the wireless network. Attackers will interfere and produce a stronger signal than the signal is valid or disable user access point exist. It guides the user by directing a denial of service or creating disturbances surrounding radio frequency. The users do not realize that they are being redirected to the fake SSID. The can always monitor traffic to search for confidential information.

The scope of the assessment of related penetration testing against wireless LAN network by utilizing Linset that runs on the Linux operating system time. Tests conducted on wireless networks on the Faculty of Computer Science to conduct testing on wireless networks including attempting to exploit vulnerabilities using tools Linset application level. In this test, we put the hardware not too far from the targeted Wi-Fi access point. It is to ensure that the penetration test works successfully. In this part, we try to beat the original signal produced. We hope the penetration signal level will replace the position. Moreover, if it happens, the users who want to connect to the network, they will be deceived and attached to the fake SSID provided by the penetration hardware.

IV. Testing and Implementation

First, penetration testing is performed by finding the target against the SSID contained in the computer science faculty. The operating system used is the time the Linux 2.0. After it has successfully booted, the next step is to go into terminal mode. We have to install Linset previously. It will be used as the attacker intended SSID.Then run the program to identify the Access Points exist. Network scanning needs time to accomplish.

Fig.3List of APs Objective

Figure 3 illustrates the SSID list obtained from the scanning. On the results of the above SSID of pancabudi_FILKOM, it is located at number 17. The next steps are more specifically detailing the access point selection to be attacked. The duplication of SSID is created soon after we choose the selected target. Figure 4 shows the step of duplication.

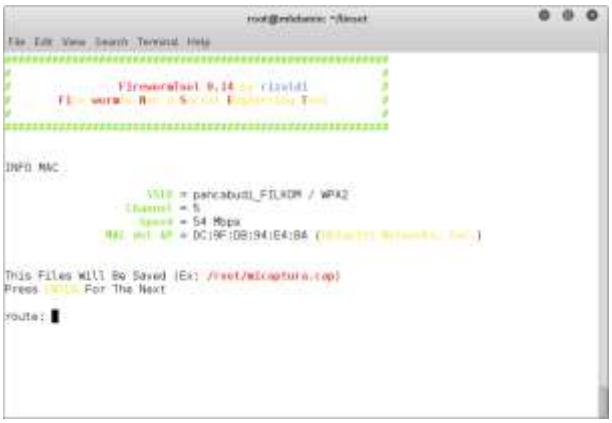

Fig. 4 Duplication of SSID

When we finish this part, there will be two identical SSID where people do not realize the difference between them. It makes the users try to connect to the other SSID when they have failed get attached to the original one.

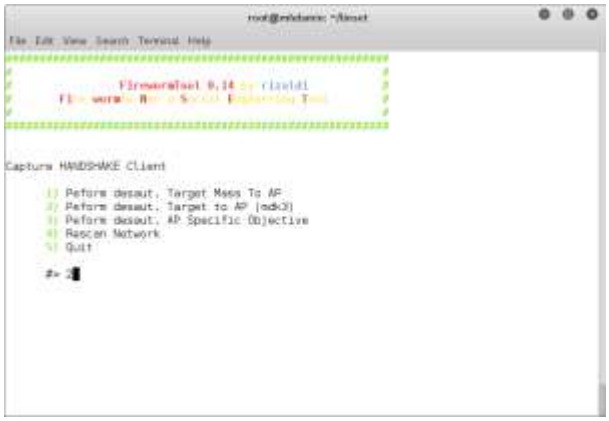

Fig 5 Modes of Attack

Figure 5 shows the modes of attack. There are three modes how to attack the access points. In this section, we use number two, that is the mdk3.

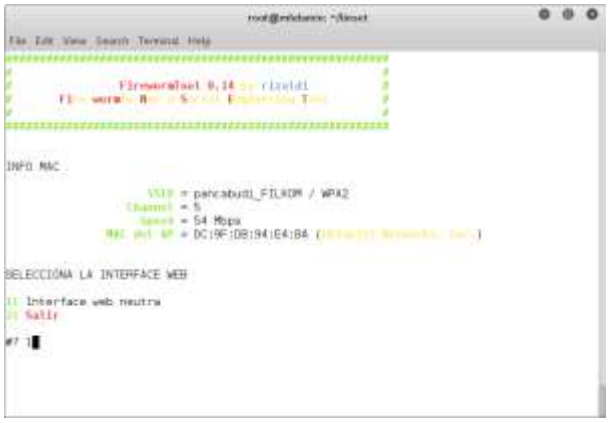

Fig. 6 Interface Web

The above figure explains what the user see on screen. We can change the SSID display by rewrite the text message again. However, in this case, we choose number one to avoid the modification of the SSID name.

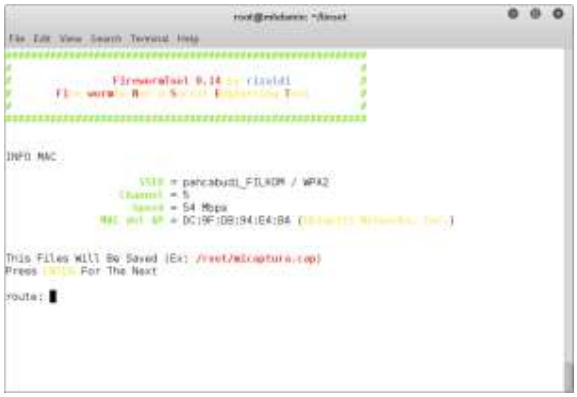

Fig. 7 Save Configuration

Right after we finish and save the configuration as showed in Figure 7, we will be asked whether the configuration is safe. We just press enter to continue to the last step.

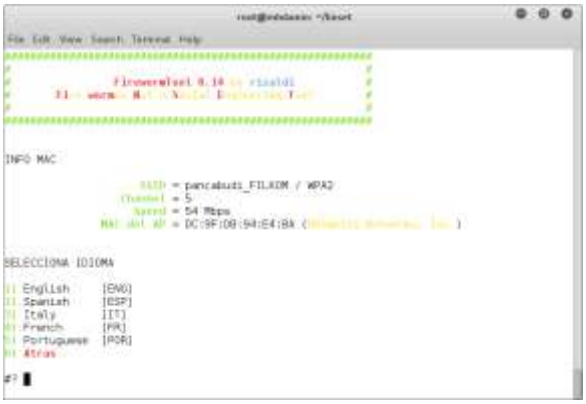

Fig. 8 Language selection

Figure 8 shows the languages available. We can select the appropriate to us. If we want to put it in International, just choose number one as the English language. This section ends the configuration of the penetration test. The test is already on board. We just wait the users try to connect to the fake SSID. Someone who fail to log into the original network, he must be working on the similar name with the exact password. But once he type the wrong password, he will be disconneted and redirected to the fake SSID.

Fig. 9 Obtained SSID password

Figure 9 illustrates the password has been found by the Linset tool. Once we note it on paper, we can disconnect the hardware and try to connect to the original SSID. Finally, we are connected. From now and then we can use the password forever as long as the owner do not change the password. If we just use for the common purpose, maybe it does not matter. However, if we force the Wi-Fi to download much content, they might realize what we have done to their networks.

V. CONCLUSION

In the global network, the security level is very crucial. Maybe we loose our valuable information because of our negligence. Using the penetration test is the best way to measure our safety level. Not all the SSID can be breached by this method. Maybe if the network owners do not have the security knowledge, it will be vulnerable. The debate is still in penetreation test and vulnerability. This tool is not intent to steal confidential information. It helps people to increase the security from gap found using the penetration test.

REFERENCES

[1] R. W. Beggs, Mastering Kali Linux for Advanced Penetration Testing, Birmingham: Packt Publishing, 2014.

[2] A. Gupta, Kavita dan K. Kaur, "Vulnerability Assessment and Penetration Testing," *International Journal of Engineering Trends and Technology*, vol. 4, no. 3, pp. 328-333, 2013.

[3] A. G. Bacudio, 1. Yuan, B.-T. B. Chu dan M. Jones, "An Overview of Penetration Testing," *International Journal of Network Security & Its Applications (IJNSA)*, vol. 3, no. 6, pp. 19-38, 2011.

[4] K. Xynos, I. Sutherland, H. Read, E. Everitt dan A. J. Blyth, "Penetration Testing And Vulnerability Assessments: A Professional Approach," dalam *International Cyber Resilience conference*, Perth, 2010.

[5] B.-H. Kang, "About Effective Penetration Testing Methodology," *Journal of Security Engineering*, vol. 5, no. 5, pp. 425-432, 2008.

[6] A. P. U. Siahaan, "The Weakness of Wireless Networks," in*SEMILOKA*, Medan, 2011.

AUTHORS PROFILE

Akhyar Lubis was born in Medan, Indonesia, in 1983. He received the S.Kom. degree in computer science from Universitas Pembangunan Panca Budi, Medan, Indonesia, in 2006. He is now studying at AMIKOM Yogyakarta for his master degree in computer science. In 2008, he started to join the Faculty of Engineering, Universitas Pembangunan Panca Budi, as a Lecturer, and in 2016 became a Cisco Trainer. He has taught many networking students. He has always had many contributions in journal events.

Andysah Putera Utama Siahaan was born in 1980, Medan, Indonesia. He received the S.Kom. degree in computer science from Universitas Pembangunan Panca Budi, Medan, Indonesia, in 2010, and in 2012, he obtained M.Kom. from the University of Sumatera Utara, Medan, Indonesia. In 2010, he joined as a lecturer at the Department of Engineering, Universitas Pembangunan Panca Budi. He has been a researcher since 2012. He has studied his Ph. D. degree from 2016. He is now active in writing international journals and conferences.