Wireless Penetration Testing Method To Analyze WPA2-PSK System Security And Captive Portal

Erfan Wahyudi[1], Emha Taufiq Luthfi[2], Muhammad Masjun Efendi[3]
STMIK Mataram[1]
Universitas Amikom Yogyakarta[2]
Universitas Islam Indonesia[3]
erfan.wahyudie@gmail.com

Abstract – One of the major changes in the telecommunications sector is the use of wireless technology. But many problems that must be faced when implementing this wireless network, one of which is a security problem. Many people are still questioning about wireless security, and many others believe that wireless security systems using WPA2-PSK are more secure than other wireless security systems. However, based on the results of literature studies conducted, a wireless security system that really can provide more secure security is to use the system security Remote Authentication Dial-In User Servers (RADIUS) server. While at present, many parties still use WPA2-PSK as their wireless security system to avoid the possibility of unauthorized use of internet access by unauthorized people. This study aims to analyze the comparison of the two wireless network security systems above. The test was performed using wireless penetration testing method, and the result stated that 80% of Security Captive Portal system is more secure than WPA2-PSK.

Keywords: ***Wireless, RADIUS, Penetration, Security, Captive, Portal***

1. INTRODUCTION

Information and communication at this time absolutely becomes a basic requirement that must be met, even for some people, they need information whenever and wherever they are. And the technology that is able to meet these needs is wireless technology.

Wireless offers a variety of conveniences, freedom, mobility, and high flexibility. Wireless technology has enough advantages over existing cable technologies (Stallings, 2011). The ease with which wireless LANs offer their own pull data for computer users in using this technology to access a network of computers or the Internet (Habibi, 2009). The problem that will be faced when implementing wireless network is the issue of its security. Many people are still questioning about wireless security, and many others believe that wireless security systems that use WPA2-PSK are more secure than other wireless security systems (Tariq, 2011).

Based on the results of literature studies conducted, the wireless security system that is actually able to provide more secure security is to use the security system Remote Authentication Dial-In User Servers (RADIUS) server using Captive Portal authentication (Choi, 2011). But at the moment, many people still use WPA2-PSK as their wireless security system to avoid the possibility of unauthorized use of internet access by people who do not have access rights (xiao, 2009).

2. LITERATURE REVIEW

The authors found previous research on the topic of wireless network security analysis using server radius, which describes the RADIUS Server security analysis to find out ways attackers damage the facility. After knowing the weakness at a certain point, then done penetration testing on the RADIUS Server to ensure weaknesses found (Boukerche, 2002).

Wifi signal interference is a common problem in wireless networks, this interference will occur if the frequency or wifi channel is equal or close to other frequencies (Kumar, 2014). This problem arises when a room or location has 2 or more routers emitting wifi signals, so the router can not specify a fixed and irregular frequency (Farooq, 2017). For example, such as wifi networks in offices and hotels that have 2 routers in one room and if the frequency settings on the router are not set well, then most likely wifi signal will encounter problems (Lii, 2005).

A. Captive Portal

Captive portal is an authentication and data security technique that makes a user or user of a network must go through a special web page, (usually as authentication) before being able to access the internet. The captive portal is actually a router or gateway machine that utilizes a web browser as a means or a secure and controlled authentication device in protecting and allowing traffic until the user registers (Sen, 2009).

This is done to prevent the delivery of all packets of data in any form to unauthorized users until the user opens a web browser and tries to access the

internet. At that point, the browser will be redirected to a specified page specified to authenticate, or simply display the applicable policy page and require the user to approve it. Captive portals are often used on wireless networks (wifi, hotspot) and can also be used for wired networks.

B. Captive Portal Works

Here is how Captive Portal works (Goeritno, 2017):

1. Users with wireless clients are allowed to connect to wireless to obtain DHCP IP address.
2. Before authenticating, all DHCP IPs propagated by the previous server are redirected to the Captive portal (web-based authentication).
3. Users connected to the network will pass the Captive portal.
4. After the user finished logging or registration, then the user can use the internet network provided by the server.

C. Penetration Testing

Penetration testing or more familiar with penetration testing is a method to evaluate the security of a computer system or computer network by simulating attacks from attackers (people who have no authority to access a system). These proses involve active analysis of the system for vulnerabilities that can result from misconfiguration or lack of knowledge in the security sector in terms of hardware or software. This analysis is carried out from the attacker's or attacker's position and involves exploitation of system flaws.

Penetration testing is considered necessary as an effort to test the security of information systems for an organization or company. A security assessment is a great first step for an organization that takes into account the importance of understanding security on their networks. A highly recommended practice is that individuals outside your organization carry out security assessments annually. Therefore, there is an objective and transparent evaluation of your security, and because vulnerability is always found, your network will often be evaluated to determine its effectiveness.

D. Wifi Protected Access (WPA and WPA2)

Addressing the weaknesses owned by WEP has developed a new security technique called WPA (WiFi Protected Access). The WPA technique is a model compatible with IEEE 802.11i standard specifications. This technique has several objectives in its design, that is solid, interoperable, capable of being used to replace WEP, can be implemented on a home or corporate user, and available to the public as soon as possible. Some say WPA has a stronger encryption mechanism. However, some are pessimistic because the communication path used is not secure, where man-in-the-middle techniques can be used to outsmart the data transmission process. To achieve WPA goals, at least two major security developments are underway. The WPA technique was established to provide the development of data encryption that became WEP's weak point, as well as providing user authentication that seems to be missing on the development of the WEP concept.

The WPA technique is designed to replace the WEP security method, which uses static security keys, using a TKIP (Temporal Key Integrity Protocol) that is able to dynamically change after 10,000 data packets are transmitted. The TKIP protocol will take the primary key as a starting point which is then regularly changed so that no encryption key is used twice. The background process is automatically unnoticed by the user. By regenerating encryption keys approximately every five minutes, wifi networks that use WPA have slowed down the work of hackers trying to crack passwords.

Although using 64 and 28-bit encryption standards, such as those of WEP technology, TKIP makes WPA more effective as an encryption mechanism. But the problem of decrease throughput as complained by the wireless network users such as not meeting the answers to the standard documents sought. Because, the problem associated with throughput is very influential on the hardware owned, more specifically is the chipset used

3. RESEARCH METHODS

To perform penetration testing, the author refers to Wireless Network Penetration Testing Methodology as written on the site www.rapid7.com. The following authors describe the method of penetration testing in figure 1.

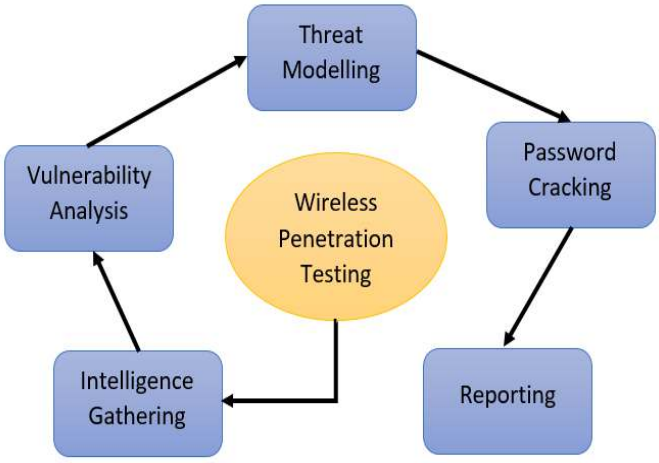

Figure 1. The Proposed Methodology

1) Intelligence Gathering

This stage is the stage of collecting information on the network, application services, searching information about the object of attack or footprinting on a predetermined scope. During this stage, testers try to identify the existing protection mechanisms in the system.

2) Vulnerability Analysis

At this stage, the tester looks for and sets the security level. Analysis of possible vulnerabilities will result in technical reports such as open ports, etc. [12].

3) Threat Modelling

Based on the information obtained from earlier stages, at this stage, the tester will determine an effective attack method..

4) Password Carcking

At this stage, the testers will directly crack the password based on the information already obtained by using the method specified in the stage of threat modeling.

5) Reporting

Reporting is the end result of system testing. Testers tell you what they have done and what they find during the system test. The testers then tell how the system owner fixes and closes the vulnerability.

4. ANALYSIS AND RESULT

A. Intelligence Gathering

Observed from the logical side, there are several types of attacks that can occur in a wireless network, such as Brute force attack, MAC address spoofing, Sniffing to Eavesdrop, Man in the Middle Attack, Ping of Death and Deauthentication Attack.

B. Vulnerability Analysis

To determine the vulnerability point on the Captive Portal, the author uses the help of Nessus Scanner tool version 6 on BackBox Linux. After scanning, I found some vulnerability detected on Captive Portal server after scanning done.

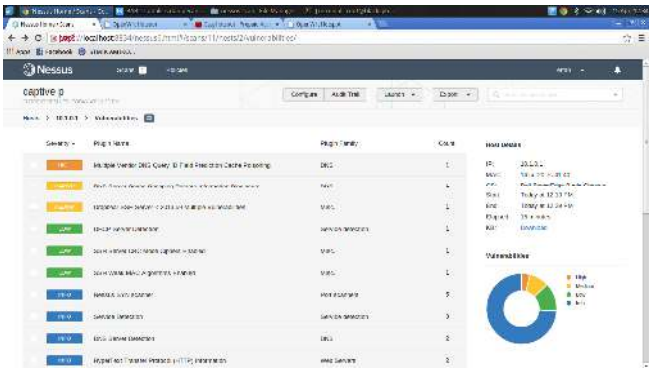

Figure 2. List Vulnerability Captive Portal

From the figure 2 shows, there is some vulnerability found, there is a low value, medium, and high. A vulnerability is orange (high) there is 1 fruit, yellow color (medium) there are 2 pieces, and green (low) 3 pieces. To know the details of the vulnerability is double-click on the vulnerability that wants to open, it will appear display showing recommendation from an existing problem.

As for searching for vulnerability on wireless networks that use WPA2-PSK security system, the author uses aircrack-ng software. Aircrack-ng will be used to search information from wireless networks, the information sought in the form of security used, target SSID, MAC Address access point, MAC address host connected to the target wireless network.

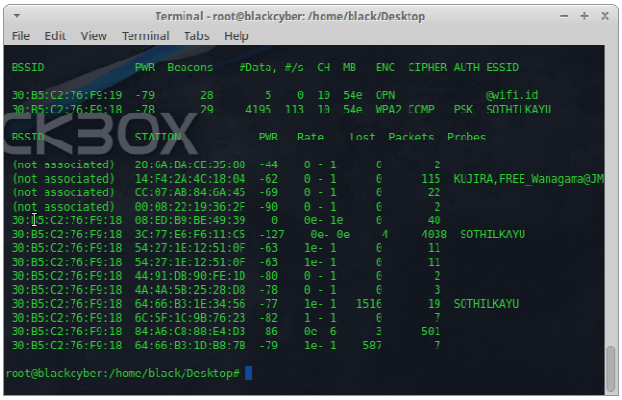

Figure 3. Finding wireless information

In the figure 3 we can see that the target to be tested using WPA2-PSK security system and its SSID is displayed or not in hidden, in the picture it looks the target SSID is SOTHILKAYU and located on channel 10. MAC address of target access point is 30: B5: C2: 76: F9: 18 and there are 2 hosts connected to the network with 3C MAC addresses: 77: E6: F6: 11: C5 and 64: 66: B3: 1E: 34: 56Threat Modelling.

There are 6 test variables determined through the information and vulnerability that have been found and will be performed on each wireless network security system.

1) Brute Force
2) MAC Address Spoofing
3) Sniffing to Eavesdrop
4) Man in the Middle Attack (MITM)
5) Ping of Death (PoD)
6) Deauthentication Attack

C. Password Cracking

1) Brute Force Attack

One of the known weaknesses in WPA2-PSK is when the client connects to the access point where the handshake process occurs. By getting a handshake package, hackers can perform a Brute Force that will try one by one the existing password with information obtained from the package handshake.

The problem is doing hacking by means of Brute Force this takes a very long time so that the most feasible method is Brute Force based dictionary file. That is, it takes a file containing the passphrase that will be tried one by one with the handshake package to find the key used. Here are some ways or steps to get WPA2-PSK password using dictionary file. When the password is found, it will be seen the phrase "KEY FOUND!" Which is accompanied by key information or password from WPA2-PSK is like in the following figure 4:

Figure 4. WPA2-PSK Password found

While on the captive portal, brute force attack is failed to be done as in the following picture:

Figure 5. Brute force captive portal failed

From the figure 5 can be seen that the process of password cracking on captive portal failed, this is because Captive Portal does not use security encryption when wifi connected, but captive portal using AAA authentication system in the web browser.

2) MAC Address Spoofing

MAC address is a unique hardware and can not be changed but can be manipulated. In this test, the author tries to manipulate MAC address with MAC address client connected to the network by using mac changer in BackBox Linux.

Figure 6. MAC Address Spoofing WPA2-PSK succeeded

In the figure 6 shows that the MAC address interface wlan0 has been successfully changed with the MAC address client connected to the WPA2-PSK wireless network, and successfully ping the google.com site and can access the Internet without the need to enter a wireless password. MAC Address Spoofing attack is also successfully performed on wireless networks that use RADIUS or Captive Portal security system.

3) Snifing to Eavesdrop

The Sniffing to Eavesdrop attack on this test is to prove whether sensitive information such as usernames and email passwords or other accounts connected to the internet using wireless networks

with WPA2-PSK security systems can be captured and analyzed by attackers using sniffing software such as Wireshark.

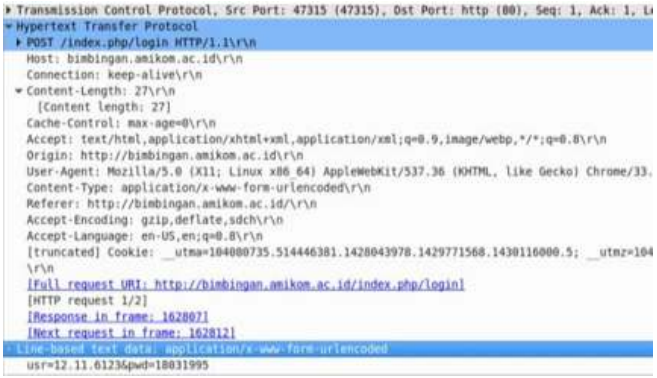

Figure 7. Sniffing to Eavesdrop WPA2-PSK succeeded

From the figure 7, Wireshark captures client activities that open the site http://bimbingan.amikom.ac.id/index.php/login1 then login to the site, Wireshark also managed to get the username and password used to log in. Based on the analysis of the obtained package, it can be known that username used is 12.11.6123 and password 18031995 and can be concluded that sniffing to eavesdrop on WPA2-PSK successfully done.

The same attack is also done on the captive portal, but it does not work. This attack can not be done on a wireless network that uses the captive portal security system as shown in figure 8 below.

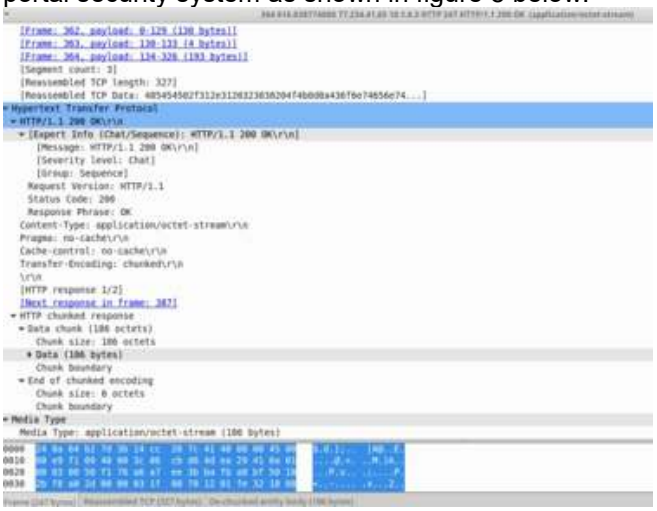

Figure 8. Sniffing to Eavesdrop Captive Portal Failed

The above picture is the contents of one of the captured HTTP packages, in this case, the author tries to login to amikom.ac.id using the client computer but none of the packages obtained using Wireshark can display the information of the opened site address and the username and password used to login to the site. So the conclusion of this attack testing is Sniffing to Eavesdropping failed to be done on captive portal using this technique.

4) Man in the Middle Attack

The type of MITIM attack to be used in this test is ARP Spoofing using Ettercap tool in Backbox Linux ARP Spoofing is a third-party tapping technique performed in a LAN or WLAN network. With this method, the attacker can tap data transmission, traffic modification, to stop communication traffic between two machines connected to the network. To perform ARP spoofing, please note first the required data is the IP and MAC address gateway and client or target as in the following table 1.

Table 1. IP and MAC target

Device	IP Address	MAC Address
Gateway	192.168.1.1	3C:1E:04:2F:6B:DF
Target	192.168.1.53	40:F0:2F:E2:A2:58
Attacker	192.168.1.50	08:ED:B9:BE:49:39

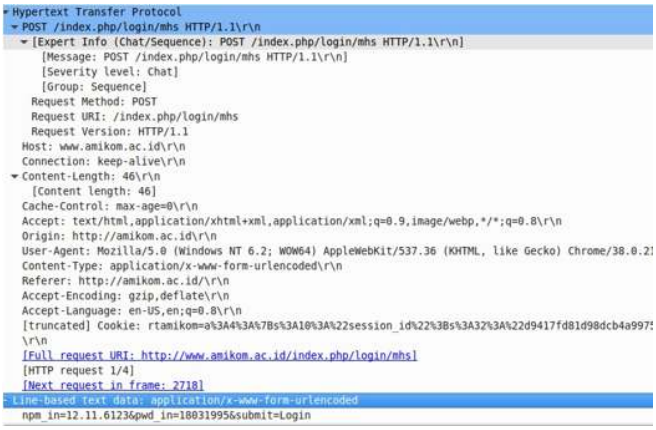

Figure 9. ARP Spoofing WPA2-PSK succeeded

In figure 9, Based on the analysis of the obtained package, it can be known that username used is 12.11.6123 and password 18031995 and can be concluded that Man in the Middle Attack with ARP Spoofing technique using Ettercap and Wireshark on WPA2-PSK successfully done. While the Captive Portal ettercap cannot get the host connected to the network, this is because of the working principle of Radius server and WPA2-PSK different. So the conclusion obtained is ARP Spoofing cannot be done on Captive Portal using this technique.

5) Ping of Death

The Ping of death attack is actually the exploitation of a ping program by providing a large-size package to the target system. Some UNIX systems turn out to hang when attacked in this way.

This Ping of death attack has actually existed for a long time, and it is called ping of death because in general ping utility on windows sends a maximum ping package of 65,536 bytes while Ping of death can send more than that, for example sending 70.000 bytes and cause the server to be down.

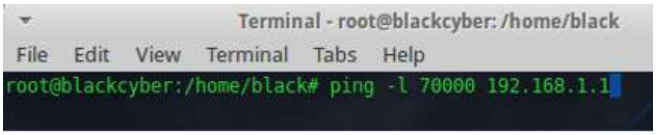

Figure 10. Ping of Death WPA2-PSK

In the figure 10, it can be seen that ping attack is done simply by running ping -l 70000 192.168.1.1, also can be seen that 70000 is the number of packets sent to the target, and the picture below is the process of sending the ping packets to the target. Ping of Death attacks are also successfully performed on wireless networks that use RADIUS or Captive Portal security system.

6) Deauthentication Attack

When the above deauthentication attack is launched on the target, automatically the connection between the target and the access point will be disconnected, but when the deauthentication attack is stopped, the target connection with the access point will be normal again as shown below.

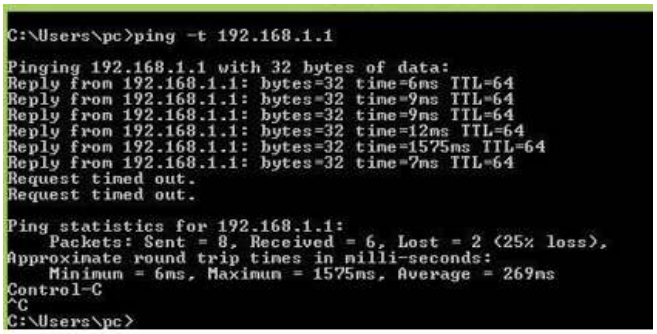

Figure 11. Deauthentication WPA2-PSK Succeeded

From the figure 11 above can be seen that the ping to 192.168.1.1 initially successful, but after the attack, automatically appear response Request Time Out on the screen. Attack Deauthentication Attack is also successfully done on a wireless network that uses RADIUS security system or Captive Portal.

7) Reporting

Based on the test results in the previous stage, the results of the authors' tests summarized in the following comparison table.

Table 2. Table of Findings

Type of Attack	Attack Status	
	WPA2-PSK	Captive Portal
Brute Force	Succeeded	Failed
MAC Address Spoofing	Succeeded	Succeeded
Sniffing to Eavesdrop	Succeeded	Failed
Man in the Middle Attack	Succeeded	Failed
Ping of Death	Succeeded	Succeeded
Deauthentication Attack	Succeeded	Succeeded

Table 2 shows that brute force, sniffing to eavesdrop attacks and man in the middle attack failed to occur on networks using RADIUS servers with Captive Portal authentication. From the attacks that have been accomplished with the wireless penetration testing method, an analysis can be generated that using RADIUS server with Captive Portal authentication as a wireless network security system can prevent unauthorized users from joining the network.

As for the reasons why brute force, sniffing to eavesdrop attacks and man in the middle attack failed to occur on networks using RADIUS servers with Captive Portal authentication are as follows:

1. Brute force attacks by dictionary files fail on a captive portal because aircrack-ng packets can only be used on wireless networks that use security encryption such as WEP, WPA, and WPA2. While Captive Portal does not use any of the three security encryption, it is Open Network and uses authentication through a web browser.
2. Sniffing to eavesdrop attacks and man in the middle attack with ARP spoofing technique failed to be performed on captive portal due to the different way of working with WPA2-PSK, where the captive portal uses a remote system which has to go through 3 methods ie AAA to connect to the internet. So before the user connects to an external network, the user will bypass the authentication on the RADIUS internal network first.

5. CONCLUSION

From the results of research conducted on wireless with WPA2-PSK security system and Captive Portal OpenWrt, it can be concluded that there are problems found in wireless networks such

as password theft and username, illegal access, and man in the middle attack. MAC filtering techniques can be tricked easily because the MAC address can be changed virtually using the tool mac changer. And Data security on WPA2-PSK is still relatively low because sensitive data such as username and password can be known by doing sniffing on the network. While the captive security portal data is guaranteed because based on the results of sniffing tests failed to be done on the captive portal.

WPA2-PSK has strong encryption, but when using a weak passphrase it is possible to do password cracking process using a dictionary attack. The RADIUS server security system with a captive portal using OpenWRT offers a secure alternative to powerful wireless LAN networks, as well as user-controlled management. From the test results show that this system is very difficult to break down using ARP attack techniques Spoofing, brute force and sniffing to eavesdrop.

6. REFERENCES

William Stallings. *Network Security Essentials: Application and Standard Fourt Edition.* Prentice Hall. 2011.

Habibi Lashkari, Arash & Danesh, Mir & Samadi, Behrang. (2009). A survey on wireless security protocols (WEP, WPA and WPA2/802.11i). 10.1109/ICCSIT.2009.5234856.

Tariq, Muhammad. (2011). Wireless Security and Threats.

Choi, Jihyuk & Chang, Sang-Yoon & Ko, Diko & Hu, Yih-Chun. (2011). Secure MAC-Layer Protocol for Captive Portals in Wireless Hotspots. 1-5. 10.1109/icc.2011.5963508.

Xiao, Yang & Chen, Hui & Yang, Shuhui & Lin, Yi-Bing & Du, Ding-Zhu. (2009). Wireless Network Security. EURASIP J. Wireless Comm. and Networking. 2009. 10.1155/2009/532434.

Boukerche, Azzedine. (2002). Security and Fraud Detection in Mobile and Wireless Networks. 309 - 323. 10.1002/0471224561.ch14.

Kumar, Umesh & Gambhir, Sapna. (2014). A Literature Review of Security Threats to Wireless Networks. International Journal of Future Generation Communication and Networking. 7. 25-34. 10.14257/ijfgcn.2014.7.4.03.

Farooq Ahmed, Zain ul Abedin Butt, Ahmed Waqas, “Educational Roaming”. International Journal of Computer Science and Information Security (IJCSIS), Vol. 15, No.1, January 2017

Iii, Guillermo & Phuong, Le & Kilaru, Aditya. (2005). Wireless Security Tools.. 562-568.

Sen, Jaydip. (2009). A Survey on Wireless Sensor Network Security. International Journal of Communication Networks and Information Security. 1. 59 – 82.

Goeritno, Arief & Aprianto, Yuggo & Basri, Hasan & , Ritzkal. (2017). PENERAPAN INTEGRASI CAPTIVE PORTAL DENGAN SINGLE SIGN ON (SSO) PADA LAYANAN HOTSPOT DAN SISTEM INFORMASI AKADEMIK.