ATTACK MONITORING of UMS WIFI USING SNORT

This Final Project Compiled as a Condition to Complete Bachelor Degree Program at the Informatics Department Faculty of Communication and Informatics

Oleh:

MUHAMAD FADLAN WIJAYANTO

L 200 134 016

DEPARTMENT OF INFORMATICS

FACULTY OF COMMUNICATION AND INFORMATICS

UNIVERSITAS MUHAMMADIYAH SURAKARTA

2017

APPROVAL

ATTACK MONITORING of UMS WIFI USING SNORT

PUBLICATION ARTICLE

Submitted By:

MUHAMAD FADLAN WIJAYANTO

L 200 134 016

Has been inspected and approved to be tested by:

Lecturer Supervisor

Dr. Bana Handaga, Ir., M.T.

NIK.793

ACCEPTANCE

ATTACK MONITORING of UMS WIFI USING SNORT

OLEH

MUHAMAD FADLAN WIJAYANTO

L 200 134 016

It has been maintained in front of the Board of Examiners
Faculty of Communication and Informatics
Universitas Muhammadiyah Surakarta
On Saturday, 21 October 2017
And declared eligible

Examiners:

1. **Dr. Bana Handaga, Ir., M.T.** (.....)
   (Chief of Examiner)
2. **Dr. Heru Supriyono, M.Sc.** (.....)
   (Member I of Examiner)
3. **Nurgiyatna, S.T., M.Sc., Ph.D.** (.....)
   (Member II of Examiner)

This publication article has been accepted as one of the requirements
To obtain a bachelor's degree
Date 30 Oktober 2017

Knowing,

Dean of
Faculty of Communication and Informatics

Nurgiyatna, S.T., M.Sc., Ph.D.
NIK : 881

Head of Department
Informatics

Dr. Heru Supriyono, M.Sc.
NIK:970

DECLARATION

I declare that this final project does not contain works that have been proposed to obtain degree in college and throughout my knowledge also does not contain work or opinions that ever written or published by another person, except being revered to in the text and mentioned in the bibliography.

If it is proven later that there is untruth in my statement above, I will fully responsible.

Surakarta, 30 Oktober 2017

Author

MUHAMAD FADLAN WIJAYANTO

L 200 134 016

UNIVERSITAS MUHAMMADIYAH SURAKARTA
FAKULTAS KOMUNIKASI DAN INFORMATIKA
PROGRAM STUDI INFORMATIKA
Jl. A Yani Tromol Pos 1 Pabelan Kartasura Telp. (0271)717417, 719483 Fax (0271) 714448
Surakarta 57102 Indonesia. Web: http://informatika.ums.ac.id. Email: informatika@ums.ac.id

SURAT KETERANGAN LULUS PLAGIASI

371/A.3-II.3/INF-FKI/X/2017

Assalamu'alaikum Wr. Wb

Biro Skripsi Program Studi Informatika menerangkan bahwa :

Nama	:	Muhamad Fadlan Wijayanto
NIM	:	L200134016
Judul	:	Attack Monitoring of UMS Wifi Using Snort
Program Studi	:	Informatika
Status	:	**Lulus**

Adalah benar-benar sudah lulus pengecekan plagiasi dari Naskah Publikasi Skripsi, dengan menggunakan aplikasi Turnitin.

Demikian surat keterangan ini dibuat agar dipergunakan sebagaimana mestinya.

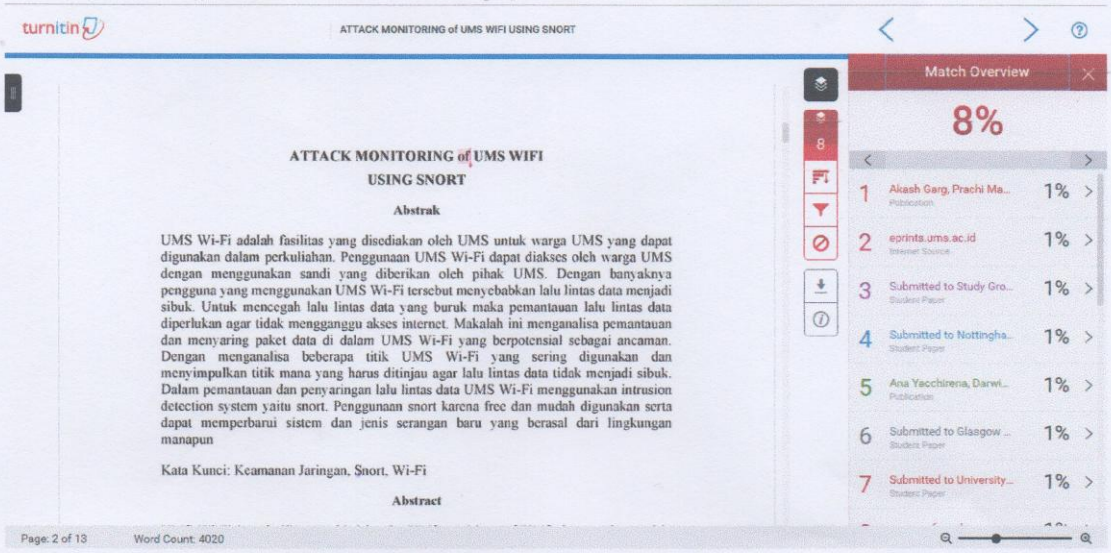
Wassalamu'alaikum Wr. Wb

Surakarta, 31 Oktober 2017

Biro Skripsi Informatika

Ihsan Cahyo Utomo, S.Kom., M.Kom.

UNIVERSITAS MUHAMMADIYAH SURAKARTA
FAKULTAS KOMUNIKASI DAN INFORMATIKA
PROGRAM STUDI INFORMATIKA
Jl. A Yani Tromol Pos 1 Pabelan Kartasura Telp. (0271)717417, 719483 Fax (0271) 714448
Surakarta 57102 Indonesia. Web: http://informatika.ums.ac.id. Email: informatika@ums.ac.id



ATTACK MONITORING of UMS WIFI USING SNORT

Abstrak

UMS Wi-Fi adalah fasilitas yang disediakan oleh UMS untuk warga UMS yang dapat digunakan dalam perkuliahan. Penggunaan UMS Wi-Fi dapat diakses oleh warga UMS dengan menggunakan sandi yang diberikan oleh pihak UMS. Dengan banyaknya pengguna yang menggunakan UMS Wi-Fi tersebut menyebabkan lalu lintas data menjadi sibuk. Untuk mencegah lalu lintas data yang buruk maka pemantauan lalu lintas data diperlukan agar tidak mengganggu akses internet. Makalah ini menganalisa pemantauan dan menyaring paket data di dalam UMS Wi-Fi yang berpotensial sebagai ancaman. Dengan menganalisa beberapa titik UMS Wi-Fi yang sering digunakan dan menyimpulkan titik mana yang harus ditinjau agar lalu lintas data tidak menjadi sibuk. Dalam pemantauan dan penyaringan lalu lintas data UMS Wi-Fi menggunakan intrusion detection system yaitu snort. Penggunaan snort karena free dan mudah digunakan serta dapat memperbarui sistem dan jenis serangan baru yang berasal dari lingkungan manapun

Kata Kunci: Keamanan Jaringan, Snort, Wi-Fi

Abstract

UMS Wi-Fi is a facility provided by the UMS to citizen of UMS that can be used in coursework. UMS Wi-Fi can be accessed of UMS citizen by using password that given by UMS. Because of a number of users UMS Wi-Fi caused traffic data being busy. To prevent this bad traffic data, monitoring of data traffic is needed to speed up of accessing to the internet. This paper analyzes the monitoring and filtering of data packages in UMS Wi-Fi as a threat. By analyzing some points of UMS Wi-Fi which is frequently used and concluding the points which should be reviewed so that traffic data will not being busy. In the monitoring and filtering of traffic data UMS Wi-Fi using intrusion detection system called snort. The use of snort because it is free and easy to use as well as can updating system and a new type of attack from any environment.

Keyword: Network Security, Snort, Wi-Fi

1. INTRODUCTION

In the era of technological advancement, Wi-Fi is one of the most sought after thing when working on assignments with friends or simply to enjoy a cup of coffee at a cafe. Wi-Fi comes into existence mandatory facility as in restaurant, coffee shop, campus, even as the government creates space public by having a public Wi-Fi access. UMS Wi-Fi is one of the facilities provided by the campus to support the activities of on-Campus lectures by both professors and students. Currently installed Wi-Fi UMS in 3 areas, whereas campus UMS itself has 5 areas. In one area there are several lecturing buildings and each floor of the building there are some wireless access point connected by a switch that is centered in the floor. There are several access points there are installed in every classroom so

learning time can be optimally used by lecturers and students. In one access point has already been set with the maximum number of users and speed for downloading, uploading so as not to cause the data traffic in the network. This led to a busy switch even to the center can not optimal network. Because of security in receiving packets has not been filtered. The standard security of network in UMS Wi-Fi can lead Wi-Fi not optimal and distracted.

UMS is very large and spacious area that divides into 5 sections, the 3 of them are already affordable Wi-Fi facility. It makes the students who has not activities, off class, no organization activity can also linger on the campus by using Wi-Fi. Lecturing activities start from 7 am until evening, depending on the schedule, UMS Wi-Fi can be accessed from 5 am to 10 pm. When students work on tasks that requires Wi-Fi access could to the campus in the lid until 01.00. Because accessing to UMS Wi-Fi is very open that everyone easily use it and when users are wearing with a need to access the internet is different then your package is sent through a device that will connect Wi-Fi more and more. Since the number of packages are not filtered and could lead to full traffic data or with threats which could interfere in the Wi-Fi network.

A threat in the Wi-Fi can interfere and uncontrolled traffic data. Kadam et al. (2016) say penetration testing is a method used to test the Wi-Fi network. With a variety of penetration test as testers in a Wi-Fi network security system whether the Wi-Fi security has a safe defense or just a standard security. A firewall is the most basic security standard within an operating system.

Yacchirena et al. (2016) says that the intrusion detection systems are systems that monitor traffic from a host or network for abnormal traffic and if it is considered as an attack issues alerts. In addition to network security that collaborate with firewalls, intrusion detection systems is helpful in filtering package that will pass and give warnings at admin. Intrusion detection systems being used is snort.

Intrusion detection systems used snort because according to Garg & Maheshwari (2016) snort rules that may be written in any language, its models is in addition under stable and it can be easily read and rules can be modified. In the buffer overflow attack, snort can noticed the anomalies by the preceding identical prototype of anomalies and then will take suitable act to avoid from these anomalies.

Snort is an open-source, free and lightweight network intrusion detection system (NIDS) software for Linux and Windows to detect emerging threats (Garg & Maheshwari, 2016). Snort can perform real-time analysis of traffic packets on the IP network and can analyze protocol and can

search for content that matches so with ability to detect threats to the network by using a rule that can be customize as desired.

Hping3 is a packet generator and analyzer for the TCP/IP protocol that is derived from the unix command so that it can be described and analyzed by the programmer (Dar et al., 2016). Hping3 is free software, you can write scripts any license, so it will be possible to build products based on hping3.

2. METHOD

Before this research was conducted, the selection method is the most basic and important from a case. For this study, phases that will be used is object research, design and implementation.

2.1 Object research

At this stage, the research will be conducted in one of the faculty building in UMS. In one faculty building consisting of two floors up to four floors. Faculty building that will become a place of research is building with four floors. Each floor consists of four access point located at a distance of every two class. This was done because in order not to intersect the signal between access point. Each access point in one floor connected by a central switch on the floor. From each floor of the switch then leads to a switch of each building before entering the router as the gateway to be able to access the internet.

The use of the UMS Wi-Fi in hours of lectures as a media student learning and information retrieval of the material is very high. Even in some cases, professors are using the internet to give you an example so that students become clear and the granting of duty directly should use an internet connection. Provider network in several floors to use the internet rather difficult, because the students use UMS Wi-Fi to simply update the latest news via smartphone. Because the number of students in using UMS Wi-Fi within hours of learning is quite high, and caused the busy traffic on the network. The increase in network traffic be the cause of slow response in connect between users with UMS Wi-Fi. For network depictions that UMS Wi-Fi needed in order to know the layout and line from the access point to the gateway router towards UMS Wi-Fi

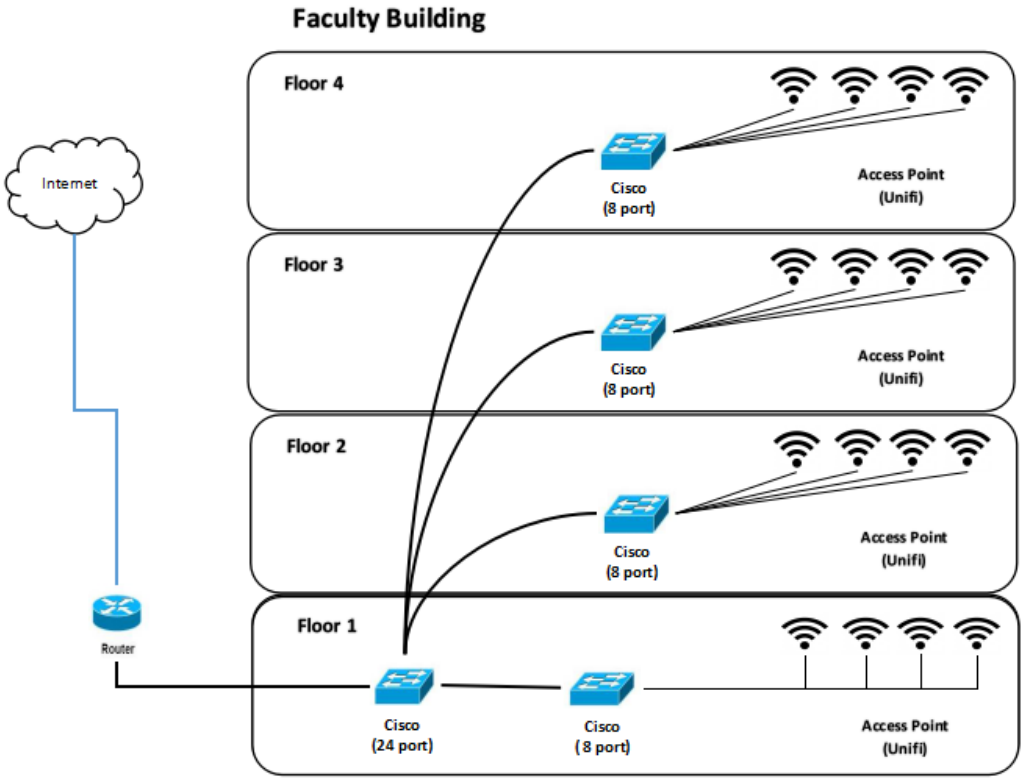


Figure 1. Topology

2.2 Design

After the stages of research object gets information that will be used in research, the next stage is configuration intrusion detection system that are used in a simulated attack on the research.

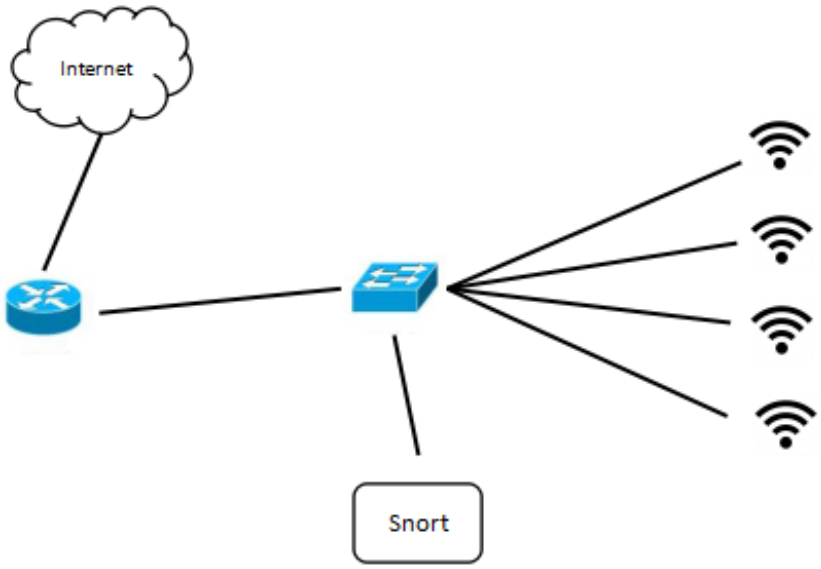


Figure 2. Simulation

Figure 2, for installation intrusion detection system can be done anywhere on the network, depending on its purpose. Because of intrusion detection system snort can do Sniffer, Packet Logger Mode, Intrusion Detection Mode. The sniffer is used to view the incoming data traffic to the network. Packet Logger Mode is used to record the passing packets and analyzing it in the future. Intrusion Detection Mode is useful for detecting data passes that could pose a threat to the network. For the case using intrusion detection mode because monitoring and detecting data passes which can analyzing a threat to the network

After installation of intrusion detection system at one point in the network and do tests with penetration testing against snort. During penetration testing done and testing where snort suitable for UMS Wi-Fi.

2.3 Implementation

To implement intrusion detection system on computer, first is install snort at the computer and in this case using the operating system ubuntu server 16.04 lts. After installation snort, then change the default directory to configure snort.

/snort/snort.conf

Set ipvar $HOME_NET to home network IP address range that will be protected. After that customize the rule set on the directory rules. It's a simple snort rule to be written, but not yet powerful enough to medeteksi the threat of suspicious traffic on the network. Snort rule base itself has split into two, namely the rule header and the rule options. The rule header itself consists of Rule Action, Protocols, IP Address, Port Number, The Operator, and the SE Active/Dynamic Rules. While the rule action function of supplementing the rule header separated by semicolon and specify that the rule can run or not. The basis of Snort that can be used when a packet matches the rule is pass, logs, and alerts. Rule pass will drop only the package, while the rule log will write down all the activities that occur on the snort when it detects packets that match the rule. Rule alert will produce a notification to the user with a mode that is used when running the user on snort. In this case, the rule that will be used is the rule alert, because in monitor network UMS Wi-Fi and do a penetration test that requires a response from the speed detection using snort alerts. As an example of how a simple rule-writing:

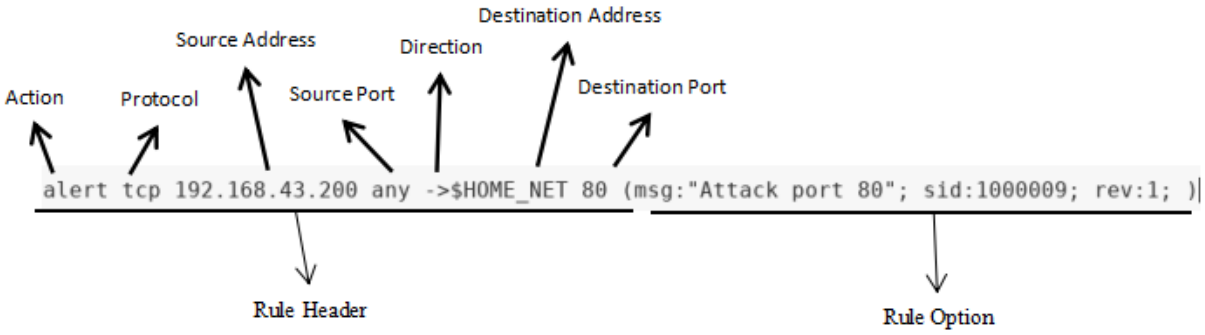


Figure 3. Example Rule

Figure 3, show an example rule of snort. This rule will show the alert action is with TCP protocol packets originating source IP address 192.168.43.200 with source port any towards the destination address $HOME_NET is a protected IP address with destination port 80 i.e. HTTP. Rule option shows the message “Attack port 80” and sid is a special number of snort itself.

After writing a few simple rules that are stored in the folder rules, then running the below command to check if the rule in accordance with the rules of the snort.

snort -T -c /etc/snort/snort.conf -I enp0s3

The next step after the rule was no problem, run the command below to console mode

snort -A console -q -c /etc/snort/snort.conf -I enp0s3

Then snort console mode will show the detection of penetration test that emerged from the rule written in snort rule.

Then after the good installation topology where configuration intrusion detection system does not the case the density the traffic data and can give warnings to admin for a package that passes is not appropriate or even brought threats on the network to immediately anticipated. Who is expected to supervise the then detects a threat could reduce traffic density to be smooth and controlled.

3. PENETRATION AND RESULT

As from figure 2, the installation of intrusion detection system applied to faculty building (figure 1). Penetration testing would have done simulated on snort to detect the rule's written work and analyse the attacks and response to attack against snort.

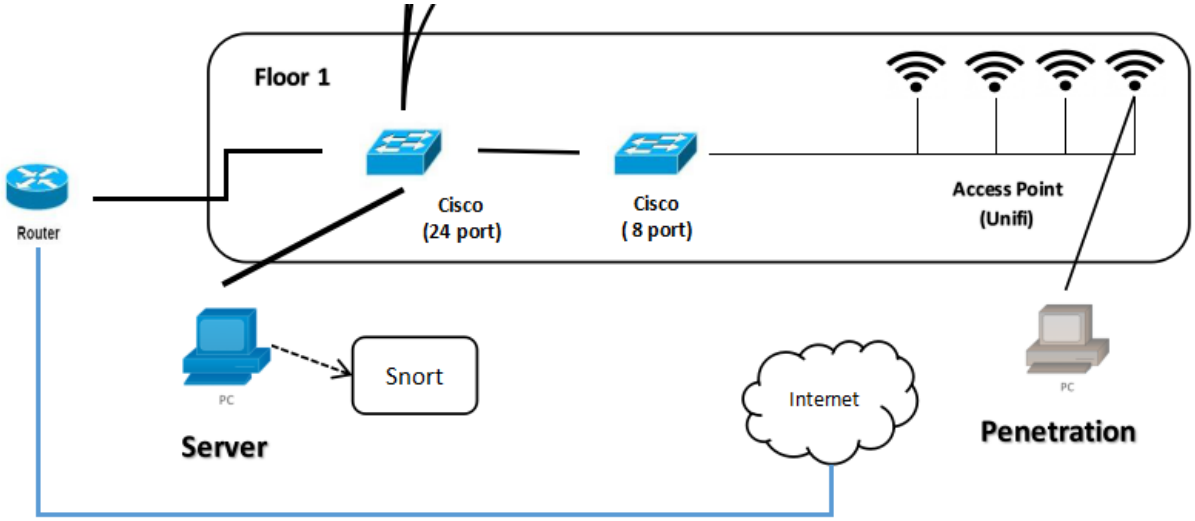


Figure 4. Penetration Test

Figure 4, shows the simulation of penetration test with the location on the 1st floor of the faculty building. Placement of servers already installed snort on switches that will go to the router because it will monitor the data traffic on the network UMS Wi-Fi. For penetration attacks using tools from Kali linux is hping3 and IP address in ubuntu is 192.168.43.100. When monitoring in progress, do penetration and attack list simulation are:

Ping flood

A denial of service attacks that flood a target with an icmp protocol that aims to overload system in large numbers. The attack sent a package of requests to find out the network responds with the same package. The effect of these attacks is to target experienced slow response and may also experience down. Hping3 is a command is:

hping3 -1 192.168.43.100 --flood

TCP syn flood

This attack can be also called syn flood attack is utilizing from the three-way handshake of tcp with exploiting resources on the target server. Basically this attack sends a TCP connection request (syn flag) faster server so as not to allow the server to give an answer (syn-ack flag) to the sender so that the traffic on the server contains only the SYN flag with the number of overload and cause the server start down. For a TCP syn flood attack is using hping3 with the command:

hping3 -S --flood -V 192.168.43.100

UDP flood

Send a UDP packet to the target system via UDP port overload and resulting in slowed the response of the target system. UDP flooding by itself can be found on the denial of service due to the delivery of the target port on the target system so that UDP packets which were received and responded to be overwhelmed and becomes unresponsive. UDP protocol itself more vulnerable because it doesn't need a handshake to make connections, and traffic sent over UDP channel without any protection to limit UDP flood denial of service. The impact of these attacks in the network is making a saturated network internet firewall and attack because this protocol have access to firewall and will be overwhelmed if flooded the connection very quickly. For this attack are still using following command hping3:

hping3 192.168.43.100 --udp --flood

Smurf attack

An attack in order to create fake ping delivery network traffic is busy. This attack is similar to a ping flood which sends ICMP packets to the target but this attack sends icmp to the broadcast IP address in the network. The utilization of these attacks use IP broadcast network that must respond to a request from a fake ping by the number of different magnitude so that network traffic can not be used because of the confusion at the network in responding to icmp request and answer icmp replies to the target. This attack will cause high network traffic and collided in response to the request of icmp. This attack can use hping3 with command:

hping3 -1 --flood --spoof 192.168.43.100 192.168.43.255

DNS flood

The attack is targeting the domain name system (DNS) in a specific zone that aims to hinder the receipt of a request from the source zone and other zone. This type of attack is a variant with a UDP flood attack because the DNS server depend on Protocol UDP. A result of this attack by meeting the network by lambar respond more to a legitimate DNS requests. This attack command using hping3 is:

hping3 192.168.43.100 -I enp0s3 -q -n --udp -d 110 -p 53 --flood

Use the list of attacks and begin to simulate the attack to the server. Attacks executed using Kali linux connect to UMS Wi-Fi available on the 1st floor of the faculty building. Once connected to a network with a server, then the server running snort with console mode to monitor traffic on Wi-Fi. From simulate penetration testing and give a result:

Table 1. Simulation Result

Simulation	Detection Time (seconds)	Attack List				
		TCP syn flood	Smurf Attack	UDP flood	Ping flood	DNS flood
1		10	5	1	26	60
2		120	7	10	15	5
3		5	3	2	9	3
4		3	2	1	2	15
5		2	2	2	15	2
6		10	20	150	20	1
7		40	2	1	13	1
8		2	1	2	1	2
9		1	2	1	2	5
10		1	1	1	2	30
Average		19	5	17	11	12

Table 1, shows result of simulation with penetration testing and produce different snort detection. TCP syn flood attack, snort detects an average of 19 seconds with several times the penetration test. At the time of the attack TCP syn flood, snort detects many different kinds-in responding to the attack. The time needed to detect a TCP syn flood attack is the longest is 120 seconds while the fastest is 1 second. With the number of times TCP syn flood attack is done, snort to detect quickly because of some of the attacks are having quite a long detection response are 120 and 40 seconds. The next penetration test with a Smurf Attack is detected by snort with an average of 5 seconds. Smurf attack is detected by snort faster because it wasn't until the 10 seconds. The next test of penetration is UDP flood detected has an average of 17 seconds. In recent times the penetration test with results of detection is very fast because it is about 10 seconds but this attack was detected 150 seconds while in UDP flood attacks monitoring, often detected by snort. Then ping flood attack by an average of 11 seconds of detection with multiple times the penetration test results have a detection medium because the detection time is more than 10 seconds. A ping flood attack is also often occurs when monitoring network traffic. The last attack with DNS flood attacks detection with an average of 12 seconds. The attack was initially detected by snort 60 seconds after that attack detection response more quickly. Snort detection results in various penetration tests, detection of the longest 150 seconds with UDP flood attacks detected 120 seconds later by a TCP syn flood attack.

When it detects to the time long enough and snort are experiencing slow response. It can also be affected by the busy network traffic or from some previous attacks resulting in communication in the network is compromised but just moments later the traffic on the network back to normal.

When Wi-Fi network monitoring, detection snort through manifold length response. The responses are categorized as follows:

Table 2. Categories Detection

Detection Time	Category
≤ 10 seconds	Fast
11 to 30 seconds	Medium
≥ 31 seconds	Slow

Table 2, shows the categories response detection snort when penetration tests. The first category, the response in detecting attacks snort is very fast because it only takes ≤ 10 seconds so that potential attacks on the server can be known quickly. The next snort detects an attack category in between 11 to 30 seconds. The response can lead to busy network traffic can interfere with another user in internet usage on the network. The last category, a response to attacks on the server with the detection time ≥ 30 seconds can cause a server experiencing slow response to does not respond to network monitoring activity. Attacks that can lead to the detection of snort does not respond is very likely to develop as a threat because network traffic is very busy to the detriment of other users when connected to the network.

After seeing the results of penetration test and response detection snort, UMS Wi-Fi very vulnerable if in attack using flooding. Because flooding one of the types of denial of service attacks that used to overwhelm a target so that network traffic becomes busy and can paralyze services. For prevention of an attack flooding, should the installation snort is located very close to the host so that detection and block threats at the network traffic UMS Wi-Fi can be efficient. However, because the installation of snort that close to the host causes congestion because of dealing with the volume of packets originating from the flooding attacks so that network traffic UMS Wi-Fi will slow response. Therefore installation of snort is only done on the switch before the faculty building heading to the Center and snort will only monitoring UMS Wi-Fi and with the rules contained in the snort just checking of data packets passing on UMS Wi-Fi. However, to monitor UMS Wi-Fi from possible attack flooding takes should be in front of the screen. To use real-time systems by telling someone if there is any attack would be very helpful but in traffic UMS Wi-Fi always detected from the snort

rules and in case of attack very fast as well as flooding if give notification to someone will as spam. Because of the results of penetration on UMS Wi-Fi after detection snort does not respond in quite a long time after waiting a while then any network traffic back to normal. Therefore in this paper does not use the notification system and the snort detection as an attack after giving a response when performed penetration tests are still running normally.

Some observations of penetration tests that have been done, there is a type of attack that is very dangerous for the network and also the server. Viewed from the results of the simulation, TCP syn flood attacks including a dangerous attack because one of the Distribution Denial of Service (DDoS) attack that is documented to the public (Čandrlić, 2016). One of prevention with the installation of intrusion detection system in the server is a step that will be enough but for very large networks such as the UMS Wi-Fi this is very not yet adequate. Protection with blocking such attacks already is considered enough, and for configuration snort be more complicated and more sophisticated computer specification so as not to interfere with traffic on the network UMS free Wi-Fi. Because computer specifications of this research and cases taken is the network monitoring. To help the intrusion detection system in detecting attacks, certainly need to merge the firewall to monitor network traffic. Firewalls also have in common the workings with a snort that is able to filter package that will go to the server and checked against the new type of connection which had been the previous connection.

4. CONCLUSION

This paper analyzes the results of monitoring the use of Wi-Fi networks using intrusion detection system is snort. In detecting attacks using snort rules and test it with denial of service attacks and resulting high data traffic that could potentially become a threat in the Wi-Fi network can interfere with the use of the network. Through monitoring of UMS Wi-Fi use snort, traffic data that often arises is because UDP protocol does not restrict the connection to communicate and harm possibilities for shipping requests can happen continuously. Snort should be able to block the package can be a potential threat in the network. Update the snort rule must often be done to recognize the type of new attacks. And to do this, the computer specifications will be in install snort should also be sufficient so as not to hinder traffic network UMS free Wi-Fi. With the analysis of this research, UMS Wi-Fi good enough when facing an attack because just wait a while the network was back to normal.

References

Čandrlić, G (2016, June). *15 Most Dangerous DDoS Attacks That Ever Happened*. Retrieved from http://www.globaldots.com/15-most-dangerous-ddos-attacks-that-ever-happened/

Dar, A. H., Habib, B., Khurshid, F. Mrs., and Banday, M. T. (2016, Sept). *Experimental Analysis of DDoS Attack and it's Detection in Eucalyptus Private Cloud Platform*. Paper presented at Intl. Conference on Advances in Computing, Communications and Informatic. doi: 10.1109/ICACCI.2016.7732295

Grag, A. and Maheshwari, P. (2016, Jan). *Performance Analysis of Snort-based Intrusion Detection System.* Paper presented at International Conference on Advanced Computing and Communication Systems. doi: 10.1109/ICACCS.2016.7586351

Kadam, S. P., Mahajan, B., Patanwala, M., Sanas, P., and Vidyarthi S. (2016, March). *Automated Wi-Fi Penetration Testing*. Paper presented at International Conference on Electrical, Electronics, and Optimization Techniques. doi: 10.1109/ICEEOT.2016.7754855

Trabelsi, Z. and Alketbi, L. (2013, July). *Using Network Packet Generators and Snort Rules for Teaching Denial of Service Attacks*. Paper presented at the Proceedings of the 18th ACM conference on Innovation and technology in computer science education. doi: 10.1145/2462476.2465580

Yacchirena, A., Alulema, D., Aguilar, D., Morocho, D., Encalada, F., and Granizo, E. (2016, Oct). *Analysis of Attack and Protection Systems in Wi-Fi Wireless Networks under the Linux Operating System*. Paper presented at International Conference on Automatica. doi: 10.1109/ICA-ACCA.2016.7778423