Detection of Denial of Service on Website With Wireshark Using the Anomaly-Based IDS Method

Finandito Adhana[a1], I Ketut Gede Suhartana[a2]

[a]Informatics Engineering, Udayana University
Unud Campus Street, Indonesia
[1]dito.iwan@gmail.com

Abstract

Denial of Service (DoS) attacks are increasingly dangerous. This DoS attack works by sending data packets continuously so that the target being attacked cannot be operated anymore. DoS attacks attack the most websites, thus making the website inaccessible. An anomaly based intrusion detection system (IDS) is a method used to detect suspicious activity in a system or network on the basis of anomaly pattern arising from such interference. Wireshark is software used to analyze network traffic packets that have various kinds of tools for network professionals.

Keywords: *Denial of Service, Wireshark, Intrusion Detection System, Website, Network Traffic*

1. Introduction

The use of websites now has a very rapid development. All fields that help in every aspect of life almost 90 percent certainly have a website, such as hospitality, government, military, and others. The use of websites in these fields is inevitable and has become a major need to support their activities.

Over time, the development of technology is increasingly rapid and the crackers are even more aggressive in launching various attacks on many websites where DoS attacks are the most common type of attacks launched by crackers. This DoS attack can cause several negative impacts for the website including abnormal network communication where there is no reply to the packet in the data exchange process, shutting down the work of the website, and even worse if the target is the server is able to cause damage to the server . Based on the above problems the authors conducted a study with the title "Detection of DoS Attacks on the Website With Wireshark Using Anomaly-Based IDS Methods".

The tools used in this study are Wireshark. Wireshark is software used to analyze computer networks, where these tools are also very useful for professionals working in the field of networking, academics, and even beginners who want to learn to use and know computer network analysis. Wireshark can capture packets that run on a network. Not infrequently also information - very important information such as passwords from a social media account can be captured easily.

Anomaly-Based IDS (Intrusion Detection System) is a network security system that functions to detect interference on a computer network by detecting interference based on anomalous patterns that are caused. Denial of Service (DoS) is an example of a type of attack that damages network infrastructure, DoS attacks themselves have a unique pattern, that is, every time an attack is carried out, a continuous packet of data is sent to its target.

With the Anomaly-Based IDS method, DoS attacks can be detected by identifying the anomalous patterns that are generated. Although the error rate of the Anomaly-Based IDS method is quite large, it can detect new types of attacks.

2. Related Works

Website security is any action or application taken to ensure website data is not exposed to cybercriminals or to prevent exploitation of websites in anyway. There are many examples of attacks on a website such as DoS (Denial of Service), Spoofing, Clickjacking, *etc*.

DoS (Denial of Service) attack is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting service of a host connected to the internet.

Wireshark is a software that have purpose to analyze the computer network traffic which has very useful functions for network professionals, network administrators, researchers, and software developer [1].

The impact of a DDOS attack will cause bandwidth used by the victim will be exhausted resulting in a disconnection between servers, If DDOS attacks are not dealt with immediately they can cause damage permanent against the victim's hardware and software [2].

IDs can inspect inbound and outbound traffic in a system or network, conduct analysis, and look for evidence of intrusion attempts [3].

3. Theoretical Basis

3.1. Web Security

Security of computer networks as part of an information system is very important to maintain data validity and integrity as well guarantee the availability of services for users. A network is designed as communication data highway with the aim of increasing access to computer system, while security is designed to control access. Network supply security is a balancing act between open access with security.

According to a security expert, security computer or computer security covers some aspects such as [4] :

3.1.1. Privacy

The privacy aspect is related to confidentiality of information. The main aspect of privacy is how to protect information from people who have no right to access.

3.1.2. Integrity

This aspect is related to wholeness information. The main point of the integrity aspect is how information should not be changed without permission information owner.

3.1.3. Authentication

The authentication aspect is related to identity or identity or ownership The system must know that a information created or accessed by the owner who legitimate.

3.1.4. Availability

The availability aspect is related to information availability.

3.2. Attack

Attack against security or security attack is all of intrusion form against information system security. There are some possibility of attack against security aspect such as [4] :

3.2.1. Interruption

This type of attack is aimed at availability (aspect availability) of information. System can be damaged, both software and hardware, in such a way that information cannot accessed again.

3.2.2. Interception

This type of attack is aimed at aspects privacy and authentication. Parties who do not authorized to access information.

3.2.3. Modification

This type of attack is aimed at aspects privacy, authentication, and integrity not authorized to access and change information.

3.2.4. Fabrication

This type of attack is aimed at aspects privacy, authentication, and integrity is not authorized to insert fake objects into in systems such as computer networks.

3.3. Type of Computer Attack

There are some type of computer attack such as :

3.3.1. Packet Interception

Read the package when the package on the way is called with packet sniffing this is a way attacker get existing information in the package.

3.3.2. ICMP Flood

System exploits which aims to make the target hang / down by sending ICMP / Ping packets with a large size that causes network performance decreases.

3.3.3. DoS (Denial of Service)

An attack which is done individually using one computer machine. This attack is carried out the attacker computer is stronger than the target, so the attacker is able flooding the target with packages he sent.

3.4. Intrusion Detection System (IDS)

IDS (Intrusion Detection System) is a software application system or hardware that can detect activity suspicious in a system or network. IDS is used to detect activity suspicious in a system or network [6]. There are three type of IDS, such as :

3.4.1. Signature-Based Detection

This method is done by comparing signature of each packet to identify possible intrusion. This method is effective when IDS detects known threats, but it is not effective if the threat is new or not known by IDS.

3.4.2. Anomaly-Based Detection

This method is used by comparing activities are being monitored with activities that are considered normal to detect any deviations. In this method, IDS has profile that represents normal behavior from user, host, network connection and application. Profile these are obtained from the results of monitoring characteristics of an activity in an interval of time certain. The advantages of this method are effective in detecting unknown threats, for example when a network is attacked by an intrusion type the new one.

3.4.3. Stateful Protocol Analysis

This method actually resembles anomaly-based, that is comparing existing profiles with ongoing activities for identify irregularities. However, no like anomaly-based detection which is using the host profile, stateful protocol analysis use a broader profile that can detailing how a protocol is special can be used or not. Meaning stateful here is a system in this IDS that you can understand and track the situation on the network protocol, transport and application.

3.5. Tools

In this research, we use one attacking tools and one packet analyzer. There are :

3.5.1. Slowloris

Slowloris is a type of denial of service attack tool invented by Robert "RSnake" Hansen which allows a single machine to take down another machine's web server with minimal bandwidth and side effects on unrelated services and ports. Slowloris tries to keep many connections to the target web server open and hold them open as long as possible. It accomplishes this by opening connections to the target web server and sending a partial request. Periodically, it will send subsequent HTTP headers, adding to—but never completing—the request. Affected servers will keep these connections open, filling their maximum concurrent connection pool, eventually denying additional connection attempts from clients.

3.5.2. Wireshark

Wireshark is one of many Network Analyzer tools used by network administrators for analyze network performance including protocol inside it. Wireshark is much liked because the interface that uses Graphical Users Interface (GUI) or graphical display. Wireshark able to capture packets of data or information that passes through the network. all kinds of information packages in various protocol formats too will be with easily captured and analyzed.

3.6. Flowchart

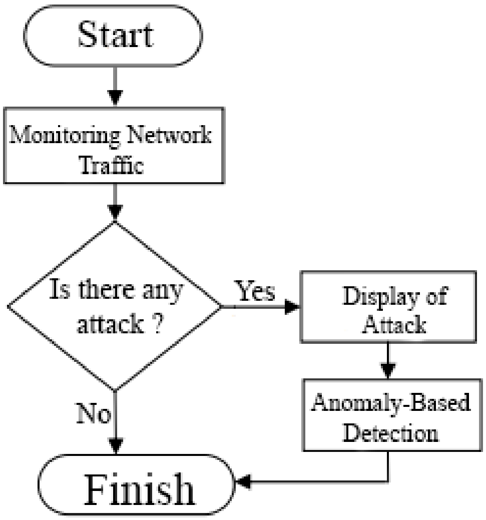


Figure 1. Research Flowchart

For the explanation of the stages of the anomaly detection process is as the following:

1. The initial process is the system will catch and record any data communication in and out of each network.
2. Any information obtained will be seen on the list in the application Whether an attack has occurred or not.
3. If "Yes" there is an attack it will be carried out anomaly detection and complete, if "No" detection will be finished.

4. Research Methods

This research was completed by using the order method as the following:

1. Literature Study
   Gather data or information from various sources such as books and searches data via the internet.
2. Literature Study
   Study related information with computer networks, anomaly-based methods, and all relate matters with the network model.
3. Trial and Evaluation
   At this stage a network trial is conducted to look for problems that might arise, and evaluate.

5. Result and Discussion

5.1. Implementation

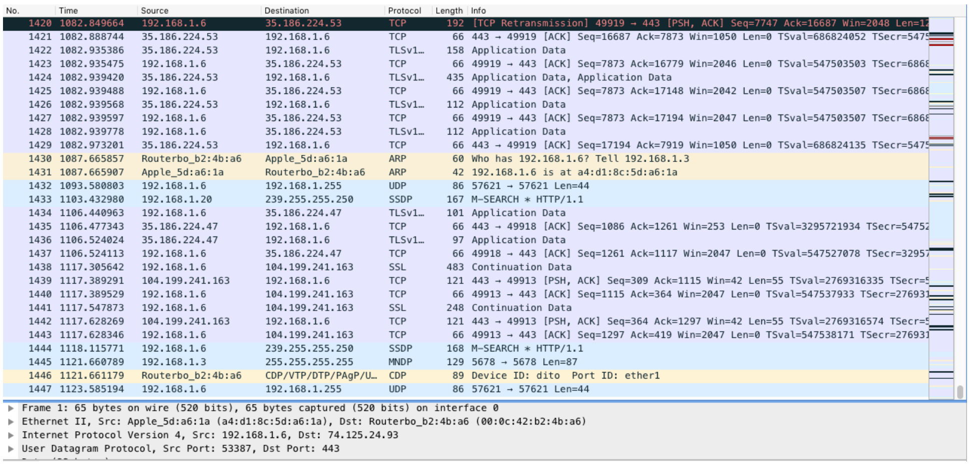
Implementation of attack detection systems computer network using the method anomaly-based, then the application is installed Wireshark on a computer that uses a system Mac OS operations, for monitoring network. For DoS attacks, the Slowloris application is used. The IP of the attack sender is 192.168.1.6 and the target itself is a website that is pudihomestay.com with an IP address of 156.67.212.136. Time for testing phase in this research is 10 minutes.

5.2. Testing

The testing phase is divided into two, namely when the attack has not been carried out and when the attack has been done.

5.2.1. Without DoS Attack

With an estimated time of 10 minutes, there are 1447 network traffic, and in the source and destination tables on figure 2., there is no packet sending from 192.168.1.6 to the destination that is 156.67.212.136. The packet sending phase indicate that the DoS attack from attackers to the destination, which is the website, pudihomestay.com.



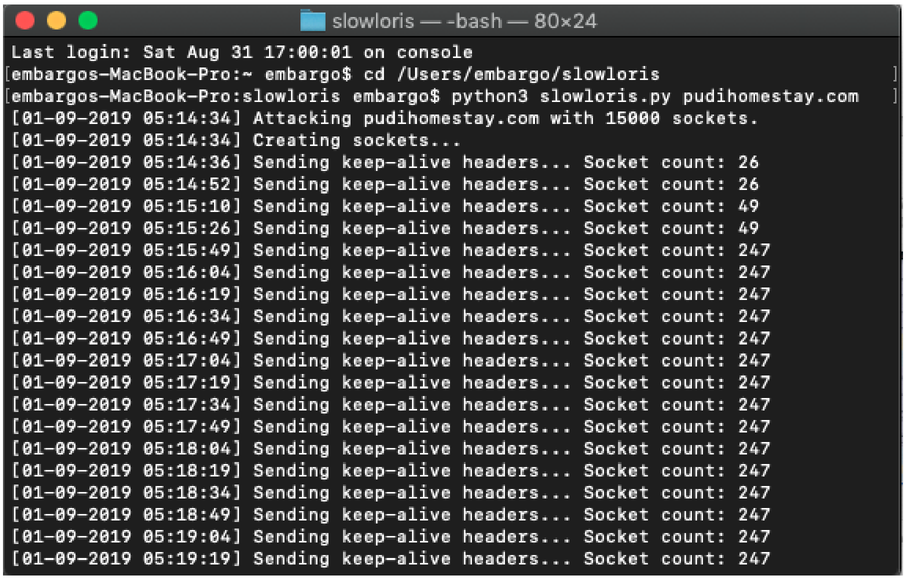
```
No.   Time         Source              Destination          Protocol  Length Info
 1420 1082.849664  192.168.1.6         35.186.224.53        TCP        192 [TCP Retransmission] 49919 → 443 [PSH, ACK] Seq=7747 Ack=16687 Win=2048 Len=12
 1421 1082.888744  35.186.224.53       192.168.1.6          TCP         66 443 → 49919 [ACK] Seq=16687 Ack=7873 Win=1050 Len=0 TSval=686824052 TSecr=5475
 1422 1082.935386  35.186.224.53       192.168.1.6          TLSv1…     158 Application Data
 1423 1082.935475  192.168.1.6         35.186.224.53        TCP         66 49919 → 443 [ACK] Seq=7873 Ack=16779 Win=2046 Len=0 TSval=547503503 TSecr=6868
 1424 1082.939420  35.186.224.53       192.168.1.6          TLSv1…     435 Application Data, Application Data
 1425 1082.939488  192.168.1.6         35.186.224.53        TCP         66 49919 → 443 [ACK] Seq=7873 Ack=17148 Win=2042 Len=0 TSval=547503507 TSecr=6868
 1426 1082.939568  35.186.224.53       192.168.1.6          TLSv1…     112 Application Data
 1427 1082.939597  192.168.1.6         35.186.224.53        TCP         66 49919 → 443 [ACK] Seq=7873 Ack=17194 Win=2047 Len=0 TSval=547503507 TSecr=6868
 1428 1082.939778  192.168.1.6         35.186.224.53        TLSv1…     112 Application Data
 1429 1082.973201  35.186.224.53       192.168.1.6          TCP         66 443 → 49919 [ACK] Seq=17194 Ack=7919 Win=1050 Len=0 TSval=686824135 TSecr=5475
 1430 1087.665857  Routerbo_b2:4b:a6   Apple_5d:a6:1a       ARP         60 Who has 192.168.1.6? Tell 192.168.1.3
 1431 1087.665907  Apple_5d:a6:1a      Routerbo_b2:4b:a6    ARP         42 192.168.1.6 is at a4:d1:8c:5d:a6:1a
 1432 1093.580803  192.168.1.6         192.168.1.255        UDP         86 57621 → 57621 Len=44
 1433 1103.432980  192.168.1.20        239.255.255.250      SSDP       167 M-SEARCH * HTTP/1.1
 1434 1106.440963  192.168.1.6         35.186.224.47        TLSv1…     101 Application Data
 1435 1106.477343  35.186.224.47       192.168.1.6          TCP         66 443 → 49918 [ACK] Seq=1086 Ack=1261 Win=253 Len=0 TSval=3295721934 TSecr=54752
 1436 1106.524024  35.186.224.47       192.168.1.6          TLSv1…      97 Application Data
 1437 1106.524113  192.168.1.6         35.186.224.47        TCP         66 49918 → 443 [ACK] Seq=1261 Ack=1117 Win=2047 Len=0 TSval=547527078 TSecr=32957
 1438 1117.305642  192.168.1.6         104.199.241.163      SSL        483 Continuation Data
 1439 1117.389291  104.199.241.163     192.168.1.6          TCP        121 443 → 49913 [PSH, ACK] Seq=309 Ack=1115 Win=42 Len=55 TSval=2769316335 TSecr=5
 1440 1117.389529  192.168.1.6         104.199.241.163      TCP         66 49913 → 443 [ACK] Seq=1115 Ack=364 Win=2047 Len=0 TSval=547537933 TSecr=276931
 1441 1117.547873  192.168.1.6         104.199.241.163      SSL        248 Continuation Data
 1442 1117.628269  104.199.241.163     192.168.1.6          TCP        121 443 → 49913 [PSH, ACK] Seq=364 Ack=1297 Win=42 Len=55 TSval=2769316574 TSecr=5
 1443 1117.628346  192.168.1.6         104.199.241.163      TCP         66 49913 → 443 [ACK] Seq=1297 Ack=419 Win=2047 Len=0 TSval=547538171 TSecr=276931
 1444 1118.115771  192.168.1.6         239.255.255.250      SSDP       168 M-SEARCH * HTTP/1.1
 1445 1121.660789  192.168.1.3         255.255.255.255      MNDP       129 5678 → 5678 Len=87
 1446 1121.661179  Routerbo_b2:4b:a6   CDP/VTP/DTP/PAgP/U…  CDP         89 Device ID: dito  Port ID: ether1
 1447 1123.585194  192.168.1.6         192.168.1.255        UDP         86 57621 → 57621 Len=44

▶ Frame 1: 65 bytes on wire (520 bits), 65 bytes captured (520 bits) on interface 0
▶ Ethernet II, Src: Apple_5d:a6:1a (a4:d1:8c:5d:a6:1a), Dst: Routerbo_b2:4b:a6 (00:0c:42:b2:4b:a6)
▶ Internet Protocol Version 4, Src: 192.168.1.6, Dst: 74.125.24.93
▶ User Datagram Protocol, Src Port: 53387, Dst Port: 443
```

Figure 2. Wireshark Intercept The Condition of Network Without DoS Attack Anomaly

5.2.2. With DoS Attack

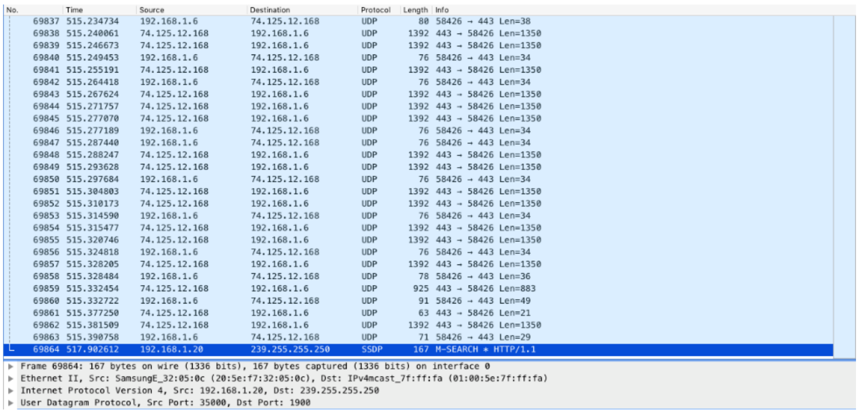
In this phase, launch the Slowloris application to send the DoS attack to the destination, pudihomestay.com that is shown on figure 3.



```
Last login: Sat Aug 31 17:00:01 on console
[embargos-MacBook-Pro:~ embargo$ cd /Users/embargo/slowloris                  ]
[embargos-MacBook-Pro:slowloris embargo$ python3 slowloris.py pudihomestay.com ]
[01-09-2019 05:14:34] Attacking pudihomestay.com with 15000 sockets.
[01-09-2019 05:14:34] Creating sockets...
[01-09-2019 05:14:36] Sending keep-alive headers... Socket count: 26
[01-09-2019 05:14:52] Sending keep-alive headers... Socket count: 26
[01-09-2019 05:15:10] Sending keep-alive headers... Socket count: 49
[01-09-2019 05:15:26] Sending keep-alive headers... Socket count: 49
[01-09-2019 05:15:49] Sending keep-alive headers... Socket count: 247
[01-09-2019 05:16:04] Sending keep-alive headers... Socket count: 247
[01-09-2019 05:16:19] Sending keep-alive headers... Socket count: 247
[01-09-2019 05:16:34] Sending keep-alive headers... Socket count: 247
[01-09-2019 05:16:49] Sending keep-alive headers... Socket count: 247
[01-09-2019 05:17:04] Sending keep-alive headers... Socket count: 247
[01-09-2019 05:17:19] Sending keep-alive headers... Socket count: 247
[01-09-2019 05:17:34] Sending keep-alive headers... Socket count: 247
[01-09-2019 05:17:49] Sending keep-alive headers... Socket count: 247
[01-09-2019 05:18:04] Sending keep-alive headers... Socket count: 247
[01-09-2019 05:18:19] Sending keep-alive headers... Socket count: 247
[01-09-2019 05:18:34] Sending keep-alive headers... Socket count: 247
[01-09-2019 05:18:49] Sending keep-alive headers... Socket count: 247
[01-09-2019 05:19:04] Sending keep-alive headers... Socket count: 247
[01-09-2019 05:19:19] Sending keep-alive headers... Socket count: 247
```

Figure 3. Launching The Slowloris

After launch the attack to the destination, Launch the Wireshark to analyze the network traffic. And the result is shown on figure 4.

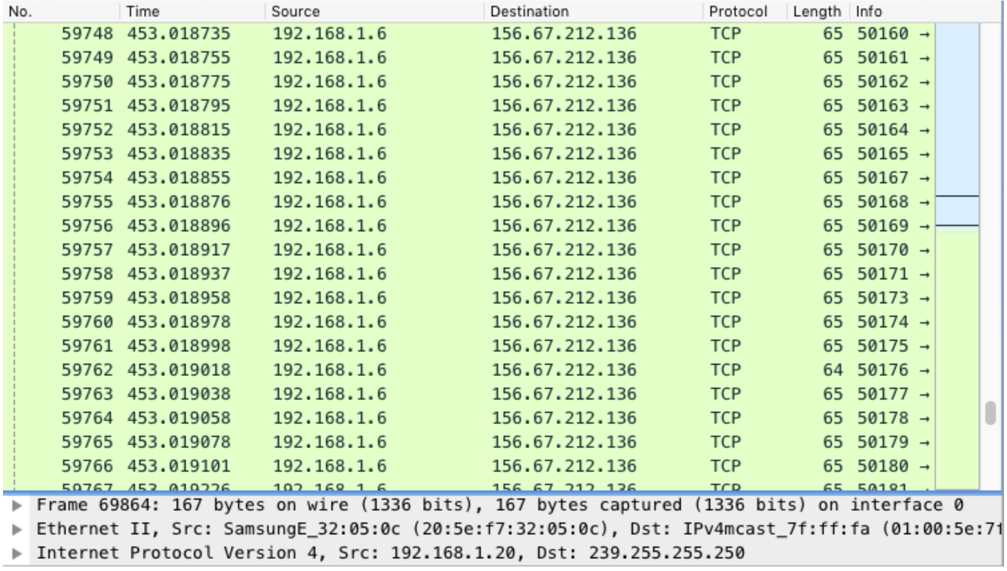


```
No.    Time        Source           Destination       Protocol  Length Info
 69837 515.234734  192.168.1.6      74.125.12.168     UDP         80 58426 → 443 Len=38
 69838 515.240061  74.125.12.168    192.168.1.6       UDP       1392 443 → 58426 Len=1350
 69839 515.246673  74.125.12.168    192.168.1.6       UDP       1392 443 → 58426 Len=1350
 69840 515.249453  192.168.1.6      74.125.12.168     UDP         76 58426 → 443 Len=34
 69841 515.255191  74.125.12.168    192.168.1.6       UDP       1392 443 → 58426 Len=1350
 69842 515.264418  192.168.1.6      74.125.12.168     UDP         76 58426 → 443 Len=34
 69843 515.267624  74.125.12.168    192.168.1.6       UDP       1392 443 → 58426 Len=1350
 69844 515.271757  74.125.12.168    192.168.1.6       UDP       1392 443 → 58426 Len=1350
 69845 515.277070  74.125.12.168    192.168.1.6       UDP       1392 443 → 58426 Len=1350
 69846 515.277189  192.168.1.6      74.125.12.168     UDP         76 58426 → 443 Len=34
 69847 515.287440  192.168.1.6      74.125.12.168     UDP         76 58426 → 443 Len=34
 69848 515.288247  74.125.12.168    192.168.1.6       UDP       1392 443 → 58426 Len=1350
 69849 515.293628  74.125.12.168    192.168.1.6       UDP       1392 443 → 58426 Len=1350
 69850 515.297684  192.168.1.6      74.125.12.168     UDP         76 58426 → 443 Len=34
 69851 515.304803  74.125.12.168    192.168.1.6       UDP       1392 443 → 58426 Len=1350
 69852 515.310173  74.125.12.168    192.168.1.6       UDP       1392 443 → 58426 Len=1350
 69853 515.314590  192.168.1.6      74.125.12.168     UDP         76 58426 → 443 Len=34
 69854 515.315477  74.125.12.168    192.168.1.6       UDP       1392 443 → 58426 Len=1350
 69855 515.320746  74.125.12.168    192.168.1.6       UDP       1392 443 → 58426 Len=1350
 69856 515.324818  192.168.1.6      74.125.12.168     UDP         76 58426 → 443 Len=34
 69857 515.328205  74.125.12.168    192.168.1.6       UDP       1392 443 → 58426 Len=1350
 69858 515.328484  192.168.1.6      74.125.12.168     UDP         78 58426 → 443 Len=36
 69859 515.332454  74.125.12.168    192.168.1.6       UDP        925 443 → 58426 Len=883
 69860 515.332722  192.168.1.6      74.125.12.168     UDP         91 58426 → 443 Len=49
 69861 515.377250  74.125.12.168    192.168.1.6       UDP         63 443 → 58426 Len=21
 69862 515.381509  74.125.12.168    192.168.1.6       UDP       1392 443 → 58426 Len=1350
 69863 515.390758  192.168.1.6      74.125.12.168     UDP         71 58426 → 443 Len=29
 69864 517.902612  192.168.1.20     239.255.255.250   SSDP       167 M-SEARCH * HTTP/1.1

▶ Frame 69864: 167 bytes on wire (1336 bits), 167 bytes captured (1336 bits) on interface 0
▶ Ethernet II, Src: SamsungE_32:05:0c (20:5e:f7:32:05:0c), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
▶ Internet Protocol Version 4, Src: 192.168.1.20, Dst: 239.255.255.250
▶ User Datagram Protocol, Src Port: 35000, Dst Port: 1900
```

Figure 4. Network Analyzer Result With DoS Attack Using Slowloris

From the Wireshark analyze result, from 10 minutes time of testing phase, the total of network traffic is 69864. And there is package sent continuously from attacker with IP address 192.168.1.6 to the destination, pudihomestay.com, with IP address 156.67.212.136, which is shown on Figure 5.



```
No.     Time        Source        Destination      Protocol  Length Info
  59748 453.018735  192.168.1.6   156.67.212.136   TCP           65 50160 →
  59749 453.018755  192.168.1.6   156.67.212.136   TCP           65 50161 →
  59750 453.018775  192.168.1.6   156.67.212.136   TCP           65 50162 →
  59751 453.018795  192.168.1.6   156.67.212.136   TCP           65 50163 →
  59752 453.018815  192.168.1.6   156.67.212.136   TCP           65 50164 →
  59753 453.018835  192.168.1.6   156.67.212.136   TCP           65 50165 →
  59754 453.018855  192.168.1.6   156.67.212.136   TCP           65 50167 →
  59755 453.018876  192.168.1.6   156.67.212.136   TCP           65 50168 →
  59756 453.018896  192.168.1.6   156.67.212.136   TCP           65 50169 →
  59757 453.018917  192.168.1.6   156.67.212.136   TCP           65 50170 →
  59758 453.018937  192.168.1.6   156.67.212.136   TCP           65 50171 →
  59759 453.018958  192.168.1.6   156.67.212.136   TCP           65 50173 →
  59760 453.018978  192.168.1.6   156.67.212.136   TCP           65 50174 →
  59761 453.018998  192.168.1.6   156.67.212.136   TCP           65 50175 →
  59762 453.019018  192.168.1.6   156.67.212.136   TCP           64 50176 →
  59763 453.019038  192.168.1.6   156.67.212.136   TCP           65 50177 →
  59764 453.019058  192.168.1.6   156.67.212.136   TCP           65 50178 →
  59765 453.019078  192.168.1.6   156.67.212.136   TCP           65 50179 →
  59766 453.019101  192.168.1.6   156.67.212.136   TCP           65 50180 →
  59767 453.019226  192.168.1.6   156.67.212.136   TCP           65 50181
▶ Frame 69864: 167 bytes on wire (1336 bits), 167 bytes captured (1336 bits) on interface 0
▶ Ethernet II, Src: SamsungE_32:05:0c (20:5e:f7:32:05:0c), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7
▶ Internet Protocol Version 4, Src: 192.168.1.20, Dst: 239.255.255.250
```

Figure 5.DoS Attack Detected Using Wireshark

5.3. Result

In carrying out some of these tests above, the advantages of Wireshark can detect attacks carried out by intruders by looking information from the results of data packet capture done, from the start of the IP used attacker, and what protocol is used. Lack of this product can't prevent attacks that occur, but can only monitor suspected data packets as intruders who carry out attacks on computer network.

And with those two type of testing phase, we can conclude that DoS attack can cause of massive traffic of data. And those massive traffic of data can cause of bad service in website service.

6. Conclusion

a. Wireshark can be used well by applying anomaly-based methods IDS.
b. Security of data or information on a computer security can be guaranteed from intruder attack. By knowing from data packets captured by Wireshark, and analyze each of these packages.

References

[1] M. Junaidi Putra, Ilham Faisal, S.T, M.Kom, and Arief Budiman, S.T, M.Kom, "Deteksi Serangan Pada Jaringan Komputer Dengan *Wireshark* Menggunakan Metode *Anomally-Based* IDS" *STTH Medan,* vol. 1375, Page Number, 2017.

[2] Rudi Hermawan, "Analisis Konsep Dan Cara Kerja Serangan Komputer Distributed Denial of Service" *Unindra,* vol.5, Page Number, 2015.

[3] Khairil, Toibah Umi Kalsum, "Implementasi *Intrusion Detection System* Sebagai Keamanan *Website Server* Universitas Dehasen Bengkulu" *Jurnal Pseudocode,* vol. 1, Page Number 1, 2014.

[4] Iwan Sofana, Membangun Jaringan Komputer, 1 Edition., Bandung: Informatika, 2008.

[5] Dony Ariyus, Intrusion Detection System, 1 Edition., Yogyakarta: Andi, 2007.

[6] Jutono Gondohanindijo, Sistem Untuk Mendeteksi Adanya Penyusup (IDS : Intrusion Detection System), 1 Edition., Semarang:Universitas AKI, 2011.