Bit-Tech

Vol.5, No.3, April 2023
Available online at: http://jurnal.kdi.or.id/index.php/bt

Network Security Analysis with SnortIDS Using ACID (Analysis Console for Intrusion Databases

Ruruh Wuryani[1)*], Indah Fenriana[2)], Dicky Surya Dwi Putra[3)], Desiyanna Lasut[4)], Susanto Hariyanto[5)]

[1)2)4)5)]Buddhi Dharma University
Jl. Imam Bonjol No. 41 Karaci Ilir Tangerang, Indonesia
[3)]Binus University
Jl. Jalur Sutera Barat Kav. 21, Alam Sutera, Tangerang, Indonesia
[1)]ruruh.wuryani@ubd.ac.id
[2)]indah.fenriana@ubd.ac.id
[3)]dicky.surya@binus.ac.id
[4)]desiyanna.lasut@buddhidharma.ac.id
[5)]susanto.hariyanto@buddhidharma.ac.id

Article history:

Received 18 March 2023;
Revised 25 March 2023;
Accepted 4 April 2023;
Available online 28 April 2023

Keywords:

ACID
IPTables
Network Security
Ntop
Snort IDS

Abstract

The use of Wi-Fi and Ethernet is increasing in today's computer networks due to the advancement of technology. The development of networks today is characterized by the need for low-latency and high-bandwidth technology. The technology has also introduced 5G and Wi-Fi 6 which support high-speed internet surfing. The introduction of Network File System (NFS) in this era sparked the demand for Ethernet. NFS also increased the use of UNIX in education and professional computing in the 1980s. Then, in 1982, Token Ring Topology emerged as an alternative to the internet and was only standardized in 1985. Network security is an important factor in ensuring data is not stolen or damaged. With the increasing knowledge of hacking and cracking, and the availability of tools that can be easily used to launch attacks or intrusions, it is important to investigate when an attack occurs. One network forensic method for monitoring attacks on the network is using Snort IDS and Ntop to facilitate the logging process for monitoring the network system. Based on the results obtained from designing a network security with Snort Intrusion Detection System (IDS) using ACID (Analysis Console for Intrusion Databases) with the utilization of IPTables on Ubuntu Server can stop attackers. In this research, the researcher used IPTables on Ubuntu as a firewall to anticipate attacks. To prevent port scanning attacks conducted by the attacker, the author created a firewall using IPTables where the IPTables rules aim to block the IP address of the attacker.

I. INTRODUCTION

Computer networks are the most important elements in the modern era. With computer networks, connections between devices are made possible by using LAN (Local Area Networks) and WAN (Wide Area Networks). The existence of computer networks can enable interaction and information sharing between devices. Since we use computer networks all the time and they help us in various computer activities, we need to know why computer networks are so essential today. Let's trace the development of computer networks from the 1960s[1].

Peer to Peer is a computer networking model in which each computer can give and receive resources (such as printers, disks, drives, etc.). There is no central computer for the other computers. Each computer can receive or give access to or from other computers[2].

This decade has also successfully introduced wireless technology. In 1997, the Wi-Fi standard was born with a speed of 2Mbps that could reach transmission rates of up to 25Mbps and used a frequency of 5GHz.

Computer networks connected to the internet provide a lot of convenience in accessing information from all over the world. However, connecting a network to the internet actually increases the possibility of disruptions to the security of the system. A computer becomes easily accessible and at risk of being infiltrated by parties who

* Corresponding author

ISSN 2622-2728 (online) 2622-271X (print)
doi: 10.32877/bt.v5i3.728

want to access the computer. As a result, computer systems are at risk of threats or attacks. This is very dangerous for company computer systems that contain confidential data and can only be accessed by certain people. The possible forms of threats are eavesdropping or theft of confidential data. Other forms of threats are discussed in research[3] and also in attacks from malware[4]. Therefore, computer network systems must be equipped with a system that can detect any intrusions. This system is known as an Intrusion Detection System (IDS).

Based on the background of the problem that has been described, connecting computer networks to the internet will increase the possibility of security breaches. Therefore, there is a need for a network security monitoring system to anticipate such attacks.

By implementing a network security system with Snort Intrusion Detection System (IDS) using ACID (Analysis Console for Intrusion Databases) by utilizing IPTables on Ubuntu Server to be used as a firewall.

II. RELATED WORKS/LITERATURE REVIEW

The following table reviews literature from 3 journals used in related research. The components used in the literature review are the name of the researcher, the name of the journal along with the ISSN, the year of publication of the journal, the institution, the title and method used and the conclusion.

TABLE 1
LITERATUR REVIEW

Researcher	1. Harjono Harjono[4] 2. Agung Purwo Wicaksono	1. Randy Mentang[5] 2. Alicia A.E. Sinsuw 3. Xaverius B.N. Najoan	1. Bambang Sugiantoro[6] 2. Jazi Eko Istianto
Journal Name	JUITA ISSN:2086-9398	Jurnal Teknik Elektro dan Komputer ISSN: 2301-8402	UPN "Veteran" Yogyakarta ISSN: 1979-2328
Year	2013	2015	2010
Institution	Universitas Muhammadiyah Purwokerto.	Universitas Sam Ratulangi	UPN "Veteran" Yogyakarta
Title and Method	Using Honeyd to Detect Network Attacks at Muhammadiyah Purwokerto University	Design and Security Analysis of Wireless Network Using Wireless Intrusion Detection System	Analysis of Security System with Intrusion Detection System (IDS), Firewall System, Database System, and Monitoring System using Mobile Agent
Conclusion	The conclusion that can be drawn from the research results are as follows: 1. By using VLAN, network segmentation based on functionality can be done without physical location limitations. 2. Dividing the network into several network segments can improve network performance and security. 3. To connect between VLANs with router on a stick inter-VLAN routing, only one interface is required.	The summary conclusion of the entire research process that has been conducted from the discussions that have been presented can be formulated as follows: The IDS system detects attacks by scanning a number of sources and the traffic that occurs within the network. The mechanism of snort and BASE system operation has been successfully implemented. The system testing was conducted on snort and ACID by using Ping attack and Digital Blaster. The prevention that can be done against attacks is by using iptables. To overcome attacks from intruders, such as ping attacks to a server, a configuration of an iptable rule is implemented. The rule is used to block based on the IP Address. The analysis of the attack, detection, and response is carried out by describing the process that	The integrated system is designed to be executed as a single entity in order for the programs in each system to run synchronously. Another reason is for user convenience. Therefore, the execution of supporting system programs is included in the automatic firewall program. The system administrator can interact with this AIRIDS system through the one-way ACID monitoring system or the two-way SMS notification system. The above system design provides system administrators with flexibility in maintaining their systems. Thus, the efficiency of the administrator's work improves, while increasing the system's

		occurs in testing the interconnection between applications and sensor machines. After various processes in implementing IDS, there is ease in its implementation. The results obtained from the implementation of IDS are that a computer network can be monitored through only one machine or computer that acts as a sensor in the network and can see all the events that are happening in it.	reliability in addressing security risks in the network. One clear disadvantage of this system is the delay that arises in the packet forwarding process. Therefore, this system must be implemented in such a way that it has high efficiency in both algorithms and the use of system resources.

III. METHODS

The Open Systems Interconnection (OSI) is a collection of protocols that allows two different systems to communicate without regard to the underlying architecture of those systems. The purpose of the OSI model is to show how to facilitate communication between two different systems without requiring changes to the logic of hardware and software. The OSI model is not a protocol but a model for understanding and designing a network architecture that is flexible, robust, and easy to operate. The OSI model is a layered framework for designing a network system that enables communication between all types of computers[7].

Network topology is the representation of the relationship between computers within the scope of a Local Area Network, which generally uses cables (transmission media) with RJ45 connectors, Ethernet cards, and other supporting devices[8].

In this research design, the author found several shortcomings or issues in the current running network system. Therefore, with various considerations, the criteria for the network system will be established as follows:

- Can anticipate attacks on computer networks.
- Can monitor the security of computer networks.
- The system can analyze all network traffic and detect various types of intrusion or attacks within a network.

Based on the problem identification and problem formulation, it can be concluded that the network system requirements in this research emphasize the need for a network system that can monitor network traffic and store it in a database, so that no network traffic is missed and can be analyzed. The database used in this research is MariaDB. MySQL is one of the database servers that has grown in the open source environment and is distributed for free under the GPL license. MySQL is an RDBMS (Relational Database Management System) server. RDBMS is a program that allows database users to create, manage, and use data on a relational model. Therefore, the tables in the database have relationships between one table and another[9].

By monitoring the network properly, it is hoped that the security of the network system can be improved by anticipating attacks that occur on the network system.

In this research, an attempt was made to create a network system with supporting tools to monitor the network system, such as Snort IDS (Intrusion Detection System), ACID (Analysis Console for Intrusion Databases), and Ntop.

Fig 1 Installation Process of Snort

The use of Snort IDS (Intrusion Detection System) aims to detect intruders and able to analyze packets passing through the network in real-time traffic, and with the additional module of ACID (Analysis Console for

Intrusion Databases) for analysis and alerting purposes, so it can be stored in a database, and to view the packets passing through the network, the Ntop application is used.

The proposed network system procedure already includes packet monitoring and detection sensors in the network system, where every request or packet sent from outside will be recorded as real-time traffic and stored in the database. If a threat is detected, it will trigger an alert and the firewall will block the traffic.

The proposed network system is designed based on the block diagram reflected by the author as follows:

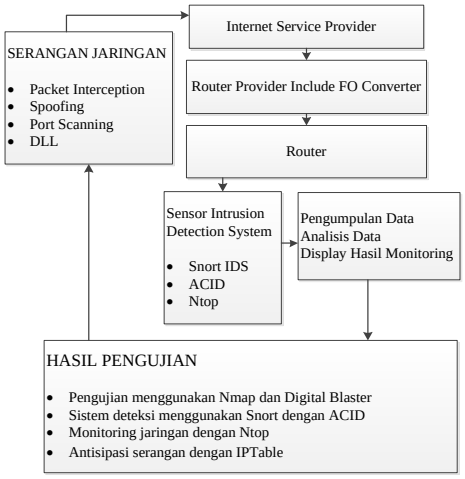

Fig 2 Block Diagram of the Proposed Network System

"Intrusion detection is the process of detecting unauthorized usage or attacks on a computer network." Intrusion Detection Systems (IDS) are designed and used to help prevent or reduce threats, damages that may result from hacking activities. IDS is a combination of software or hardware devices that can perform intrusion detection on a network[10].

The proposed network system by the researcher can be depicted from the block diagram above. Every incoming packet will be detected by the IDS sensor system and analyzed to estimate whether the packet is dangerous or not. In this research, testing will be carried out using Nmap and Digital Blaster applications to simulate network attack forms such as packet interception, spoofing, port scanning, and others, in order to anticipate possible attacks. Firewall will be implemented using IPTable.

IV. RESULTS

The detailed topology of the proposed new network system is a diagram that explains the relationship between one network device and another network device in detail, including the IP addresses used. Here is the detailed topology of the new network system.

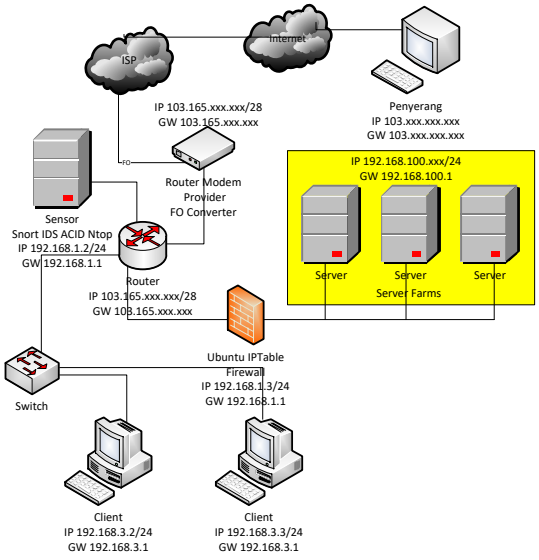

Fig 3 Details of the New Network System Topology

An IP Address is an identifier used to provide an address for each computer on a computer network. The IP Address format is a 32-bit number with each 8 bits separated by a dot, and theoretically, it can address up to 4 billion computers, or more precisely 4,294,967,296 computers worldwide. This number is obtained from 256x256x256x256, so the maximum value of an IPv4 address is 255.255.255.255, with values counted from zero, allowing for 256x256x256x256=4,294,967,296 hosts[11].

Nmap (Network Mapper) is an open-source program that is useful for exploring networks. Nmap is designed to be able to scan large networks, and can also be used to scan single hosts. Nmap uses IP packets to determine active hosts on a network, open ports, the operating system being used, and the type of firewall being used[12].

The new network system topology illustrates a attacker with IP address 103.xxx.xxx.xxx attempting to launch attacks using Nmap and Digital Blaster applications against the public IP address range 103.168.xxx.xxx/28, which serves as the internet source from the provider for the new network system. Every packet transmitted and received will be monitored by the Snort IDS sensor and recorded in the MariaDB database, managed by ACID for easy viewing of logs. Ntop application is also used for monitoring data traffic that may be considered a threat to the server farms located at IP address 192.168.2.xxx/24. If such traffic is detected, Ubuntu IPTable, acting as the firewall, will block it. Additionally, the topology includes two client computers with a gateway at 192.168.3.1.

The following is the configuration process of the snort IDS sensor server. The operating system used for the snort IDS sensor server is Ubuntu 18.04 server. Here are the installation and configuration processes for Ubuntu 18.04 server.

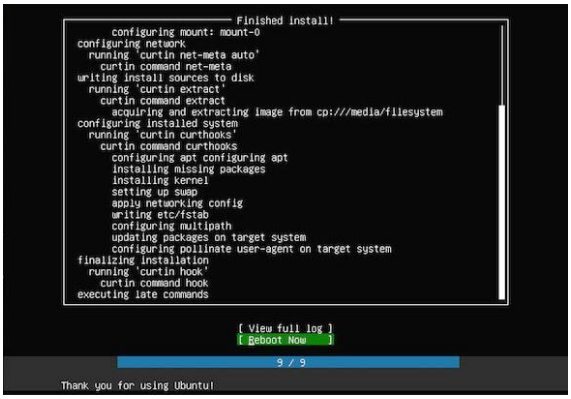

Fig 4 Proses Finished Install Ubuntu Server 18.04

After the successful installation of the Ubuntu server 18.04 operating system, the next step is to install the Snort IDS. Snort is a software used to detect intruders and analyze packets passing through the network in real-time traffic and logging them into a database. It is also capable of detecting various attacks coming from outside the network. Snort can be used on various operating system platforms, such as Linux, BSD, Windows, and other operating systems[13].

- sudo apt-get update && sudo apt-get dist-upgrade –y
- sudo apt install build-essential libpcap-dev libpcre3-dev libnet1-dev zlib1g-dev luajit hwloc libdnet-dev libdumbnet-dev bison flex liblzma-dev openssl libssl-dev pkg-config libhwloc-dev cmake cpputest libsqlite3-dev uuid-dev libcmocka-dev libnetfilter-queue-dev libmnl-dev autotools-dev libluajit-5.1-dev libunwind-dev
- sudo mkdir snort-source-files
- cd snort-source-files
- git clone https://github.com/snortadmin/snort3.git
- ./configure_cmake.sh --prefix=/usr/local --enable-tcmalloc
- cd build
- make
- sudo make install
- cd etc/snort
- sudo nano rules/local.rules
- alart icmp any any -> $HOME_NET any (msg:”ADA PERCOBAAN PING”;sid:1000001;rev:0001)
- snort –A console –i lo –u snort –g snort –c /etc/snort/snort.conf
- ping 192.168.100.11

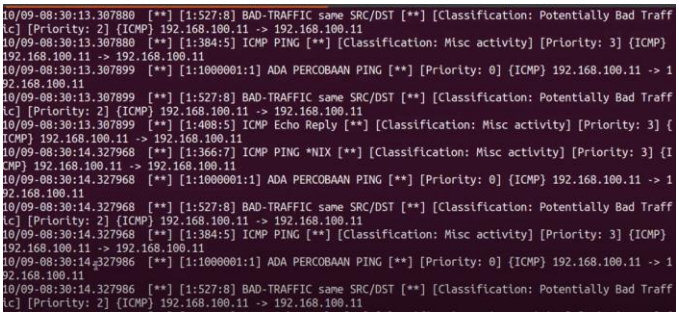

Fig. 5 Alert Snort display

After the installation process of Snort IDS is completed, the next step is to add the ACID (Analysis Console for Intrusion Database) module. Here is the process of adding the ACID module.

- sudo apt-get install mariadb-server mariadb-client –y
- sudo systemctl status mariadb
- sudo mysql_secure_installation
- sudo mysql –u root –p
- sudo nano etc/snort/snort.conf
- var RULE_PATH /etc/snort/rules
- output database: log, mysql, user=usersnort password:snort123! Dbname=snort host=localhost
- var PREPROC_RULE_PATH /etc/snort/preproc_rules
- output database: log, mysql, user=usersnort password:snort123! Dbname=snort host=localhost
- sudo mysql –u root –p
- CREATE DATABASE snort;
- GRANT CREATE, INSERT, SELECT, DELETE, UPDATE ON snort.* TO root@localhost;
- SET PASSWORD FOR root@localhost=PASSWORD('123456');
- cd /usr/local/snort-2.8.4.1/schemas
- sudo mysql –u root –p snort < create_mysql
- sudo mysql –u root –p
- use snort;
- show tables;
- cd /var/www
- sudo tar zxfv jpgraph-1.27.1
- sudo apt-get install apache2 –y
- sudo ufw allow 'Apache'
- sudo /etc/init.d/httpd start
- sudo apt-get install python-software-properties
- sudo add-apt-repository ppa:ondrej/php5-oldstable
- sudo apt-get update
- sudo apt-get install -y php5
- sudo apt-get install mysql-server php5-mysql
- /etc/init.d/apache2 restart
- cd /var/www
- sudo tar zxfv adodb411.tgz
- sudo tar zxfv acid-0.9.6b23.tar.gz.gz
- cd /var/www/acid
- sudo nano acid_conf.php
- $DBlib_path = "/var/www/adodb";
  /* Alert DB connection parameters
  * - $alert_dbname : MySQL database name of Snort alert DB
  * - $alert_host : host on which the DB is stored
  * - $alert_port : port on which to access the DB
  * - $alert_user : login to the database with this user
  * - $alert_password : password of the DB user
  *
  * This information can be gleaned from the Snort database
  * output plugin configuration.

```
 */
$alert_dbname = "snort";
$alert_host = "localhost";
$alert_port = "";
$alert_user = "usersnort";
$alert_password = "snort123!";
/* Archive DB connection parameters */
$archive_dbname = "snort";
$archive_host = "localhost";
$archive_port = "";
$archive_user = "usersnort ";
$archive_password = "snort123!";
$ChartLib_path = "/var/www/jpgraph-1.27/src";
```

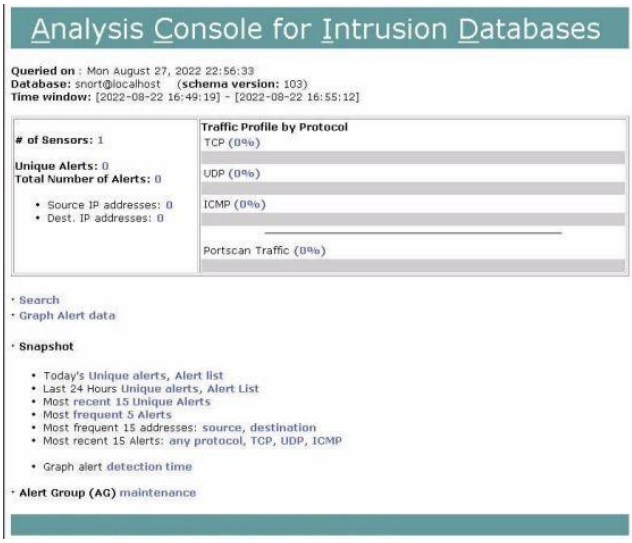

Fig. 6 ACID Homepage

After the installation process of Snort IDS and ACID (Analysis Console For Intrusion Database) module is completed, the installation process of Ntop will be continued. Ntop application will be used to facilitate the process of displaying logging for network system monitoring. NTOP is a tool to view traffic on a network and display it in an incredible way. NTOP is claimed to be the most reliable open-source network probing tool, at least according to me[14].

- sudo yum install epel-release –y
- sudo dpkg -i apt-ntop.deb
- sudo apt-get update -y sudo apt-get install pfring-dkms nprobe ntopng n2disk cento –y
- sudo nano /etc/ntopng/ntopng.conf
- sudo nano /etc/ntopng/ntopng.start
- sudo systemctl start ntopng
- sudo systemctl enable ntopng
-

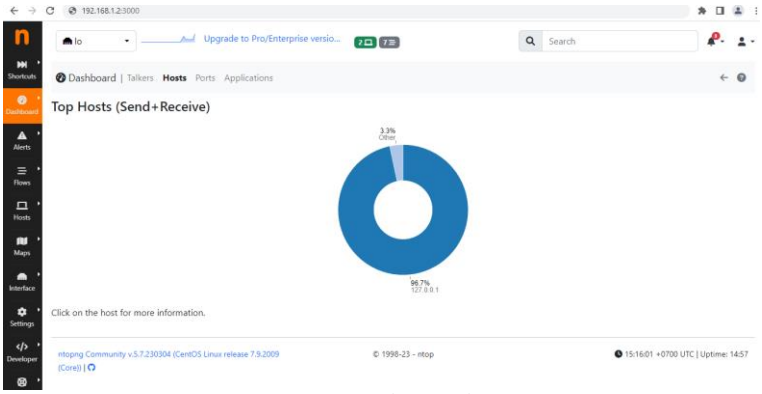

Fig. 7 Initial View of Ntop After Login

The digital blaster can send packets to an IP address and specify the target port determined by the attacker.

In this research, the use of digital blaster is aimed to analyze port scanning activities that will be conducted through the attacker's machine. In this experiment, the attacker's machine attempts to conduct port scanning on one of the servers located in the server area with IP 192.168.100.2 and port 80.

The following is the display shown by ACID during the port scanning process carried out by the attacker using digital blaster. The ACID application shows that there is detected activity on the UDP protocol.

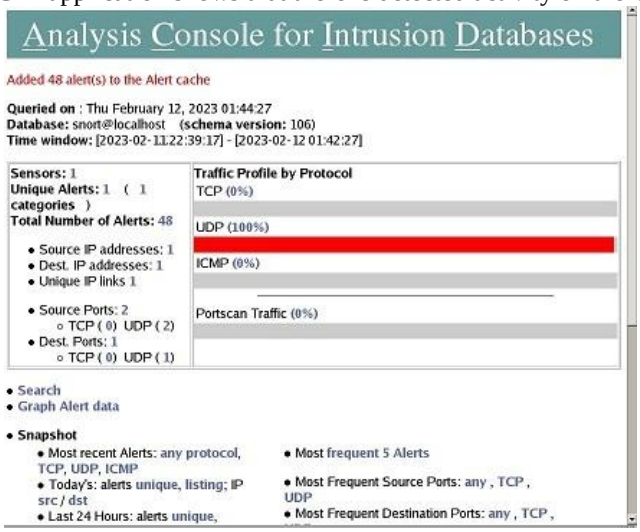

Fig. 8 ACID Display When Port Scanning Occurs

V. DISCUSSION

In this research, the researcher used IPTables on Ubuntu as a firewall to anticipate attacks. To prevent port scanning attacks conducted by the attacker, the author created a firewall using IPTables where the IPTables rules aim to block the IP address of the attacker. A firewall is a way or mechanism applied to hardware, software, or systems with the aim of protecting them[15].

- sudo apt-get install iptables iptables-persistent
- sudo iptables –nvL
- sudo iptables -A INPUT -p icmp -j ACCEPT
- sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
- sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
- sudo iptables –nL

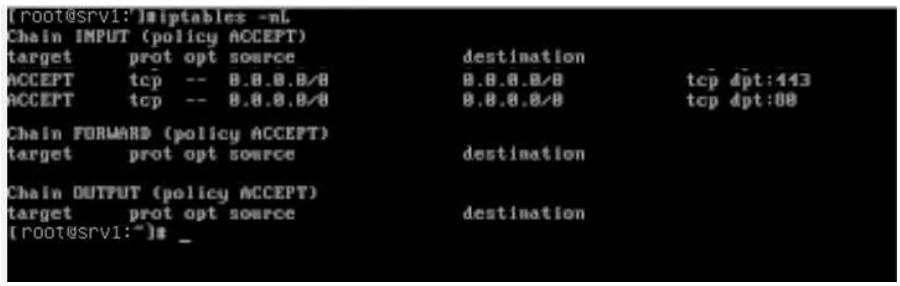

Fig. 9 Display IPTables After Setting Accept Port 80 And 443

VI. CONCLUSIONS

Based on the results obtained from the network security design with Snort Intrusion Detection System (IDS) using ACID (Analysis Console for Intrusion Databases) and utilizing IPTables on Ubuntu Server, the following conclusions were obtained:

1. The Snort IDS is capable of performing an early detection when the network system is being attacked with port scanning.
2. By using the ACID (Analysis Console for Intrusion Databases) module in Snort IDS, it can display alerts if there is an attack on the network system.
3. By using Ntop, every packet traffic that occurs on the network system can be easily monitored.
4. In this research, IPTables tool on Ubuntu Server was utilized to block the IP address of the attacker and stop the attack.

After securing the network with Snort intrusion detection system (IDS) using ACID (analysis console for intrusion databases) and utilizing IPTables on Ubuntu Server, there are also some recommendations for further development of this research to make it better and more effective in the future.

1. In the next research, it is expected to use other Intrusion Detection System (IDS) applications to detect network attacks on the system.
2. The use of other applications besides Nmap and Digital Blaster for conducting network attacks.
3. The system can be improved by implementing an automatic security system to block attackers.

REFERENCES

[1] N. Shiba, "Perkembangan Jaringan Komputer," *STMIK Indo Daya Suvana*, 2022. https://ids.ac.id/sejarah-dan-perkembangan-jaringan-komputer/
[2] Stallings and William, *Komunikasi data dan komputer: dasar-dasar komunikasi data*. Jakarta: Salemba Teknika, 2000.
[3] Pinandita and Harjono, "Deteksi Malware di Jaringan Lokal Universitas Muhammadiyah Purwokerto Menggunakan Dionaea," 2012.
[4] Harjono and A. P. Wicaksono, "Honeyd untuk Mendeteksi Serangan Jaringan di Universitas Muhammadiyah Purwokerto," *JUITA ISSN:2086-9398*, vol. 2, no. 4, 2013.
[5] R. Mentang, A. A. E. Sinsuw, and X. B. N. Najoan, "Perancangan Dan Analisis Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System," *J. Tek. Elektro dan Komput. ISSN 2301-8402*, vol. 4, no. 7, pp. 35–44, 2015.
[6] B. Sugiantoro and J. E. Istianto, "ANALISA SISTEM KEAMANAN INTRUSION DETECTION SYSTEM (IDS), FIREWALL SYSTEM, DATABASE SYSTEM DAN MONITORING SYSTEM MENGGUNAKAN AGENT BERGERAK," *UPN "Veteran" Yogyakarta ISSN 1979-2328*, pp. c21–c29, 2010.
[7] N. S. J. Abraham, Harianto, Agus, and Alexander, "Perancangan dan Implementasi Intrusion Detection System pada Jaringan Nirkabel BINUS University," Universitas Bina Nusantara, 2009.
[8] Abdul and Kadir, *Pengenalan Sistem Informasi Edisi Revisi*. Yogyakarta : Andi, 2014.
[9] D. D. Prasetyo, *Aplikasi Database Client/Server Menggunakan PHP dan MySQL*. Jakarta: PT.Elex Media Komputindo, 2004.
[10] R. A. Wibowo, "Analisis dan Implementasi IDS menggunakan Snort pada cloud server di jogja digital valley," AMIKOM YOGYAKARTA, 2014.
[11] M. Syafrizal, *Pengantar Jaringan Komputer*. Yogyakarta: Andi, 2005.
[12] Setiawan and Thomas, "Analisis Keamanan Jaringan Internet Menggunakan Hping, Nmap, Nessus, dan Ethereal.," Institut Teknologi Bandung, 2004.
[13] D. Ariyus, *Intrusion Detection System*. Yogyakarta: C.V. Andi Offset, 2007.
[14] T. Gregory, *Melihat Lalu Lintas di Network Dengan NTOP*. IlmuKomputer.Com, 2007.
[15] A. Sukamaaji and Rianto, *Jaringan Komputer : Konsep Dasar Pengembangan Jaringan dan Keamanan Jaringan*. Yogyakarta : Andi, 2008.