PERANCANGAN SISTEM REMOTE IP TABLE DAN INSTRUSION DETECTION SYSTEM (IDS) DENGAN SNORT PADA JARINGAN LAN

Bayu Adhi Prakosa, A. Hendri Hendrawan, Windi Apriana
Unversitas Ibn Khaldun Bogor
Jln. K.H Sholeh Iskandar Km. 2 Bogor
bayu.adhi@ft.uika-bogor.ac.id, hendri@ft.uika-bogor.ac.id

Abstract- The design of Remote Iptables and Intrusion Detection System (IDS) system with Snort has been done. Local Area Network Model Network is widely applied to various customer segments. Problems of decreasing LAN network performance, due to a number of ping of death attacks and SYN flooding attacks that affect all computers connected on the LAN network. Based on that, we need a proper attack detection and prevention system to help the administrator in LAN network security. Remote Iptables and Intrusion Detection System with Snort, warning system of real-time attacks will be sent via SMS, a number of syntax with iptables remote using SMS Gateway, and blocking in real time. Stages used for the achievement of research objectives, is the identification of problems, design system requirements, system implementation and testing. Detection results are 4 (four) types of information, ie attack time, type of destination IP attack, and IP source. Detection and blocking of attacks based on a number of syntax is done by comparing the packet to the rules in the form of integration through SMS Gateway for the ease of the administrator in the execution of blocking. Blocking attacks in the form of 3 (three) types of information, the source IP, the type of attack, and security policy. Based on these results, some attacks can be detected in real time against 4 types of information, blocking attacks integrated via SMS Gateway in the form of packet comparisons to rules, and blocking attacks in the form of Remote Iptables with 3 (three) types of information.
Keywords: *LAN Network, Remote Iptables, Intrusion Detecion System, SMS Gateway.*

1. PENDAHULUAN

A. Latar Belakang

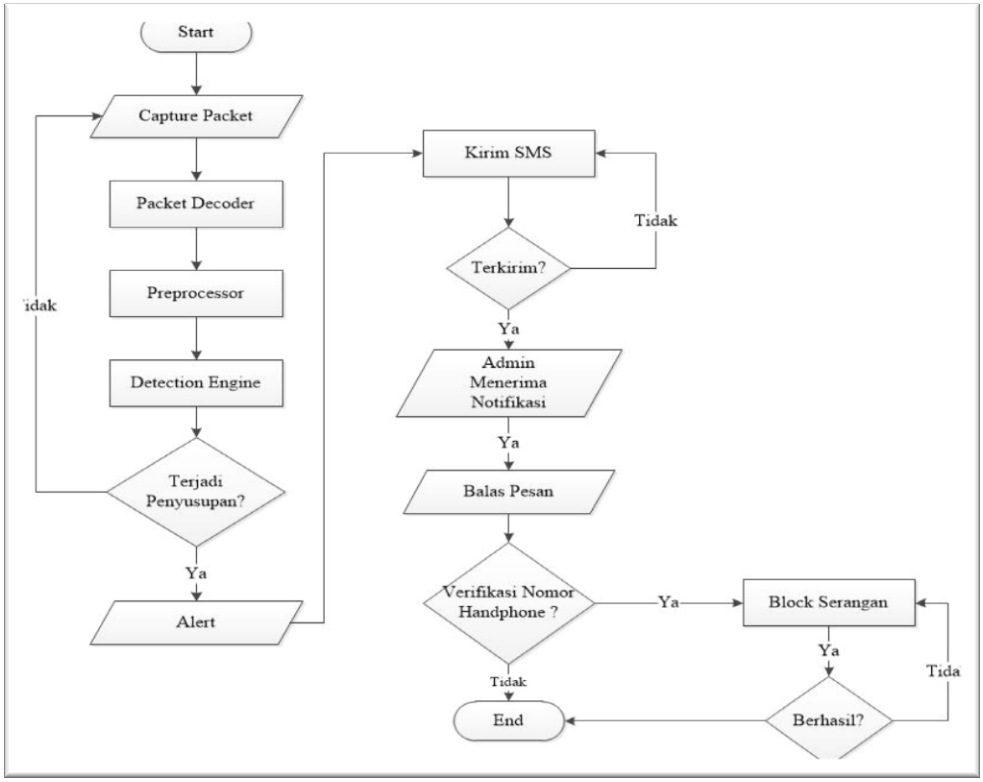
Teknologi informasi telah berkembang dengan pesat pada saat ini, terutama dengan adanya jaringan internet yang dapat memudahkan dalam melakukan komunikasi dengan pihak lain [1]. Dua dekade terakhir, jaringan komputer telah menjadi bidang revolusioner untuk berimprovisasi [2]. Keamanan jaringan merupakan tugas penting yang harus serius dipertimbangkan ketika merancang jaringan. Keamanan jaringan didefinisikan sebagai kebijakan dan prosedur diikuti oleh administrator jaringan untuk melindungi perangkat jaringan dari ancaman, hal ini sangat penting bahwa mekanisme keamanan dari suatu sistem yang dirancang untuk mencegah akses tidak sah [3-6]. Model Jaringan Local Area Network paling

banyak digunakan oleh berbagai segmen pelanggan dimana saat ini terdapat beberapa masalah, seperti penurunan kinerja jaringan *Internet* yang melemah dapat berimbas ke semua komputer *client* jaringan *LAN* tersebut.

Kebutuhan sistem pendeteksi serangan yang dapat membantu administrator dalam pemantauan (*monitoring*) jaringan, sehingga administrator dapat menanggulangi ancaman secara cepat dan jaringan dapat beroperasi kembali secara optimal [5]. Penerapan sistem pengamanan jaringan yang mampu mendeteksi serangan dapat dilakukan melalui pembuatan *Intrusion Detection System* (*IDS*) dan pelaksanaan pencegahan dengan *filtering firewall*, sehingga administrator dengan mudah dapat menganalisis dan melakukan penangulangan terhadap serangan pada jaringan. *Instrusion Detection System* (*IDS*) melakukan pendeteksian serangan berdasarkan *rules* yang ditentukan, sedangkan *Remote Iptables* melakukan pencegahan dengan cara pemutusan terhadap serangan tersebut[1-3].

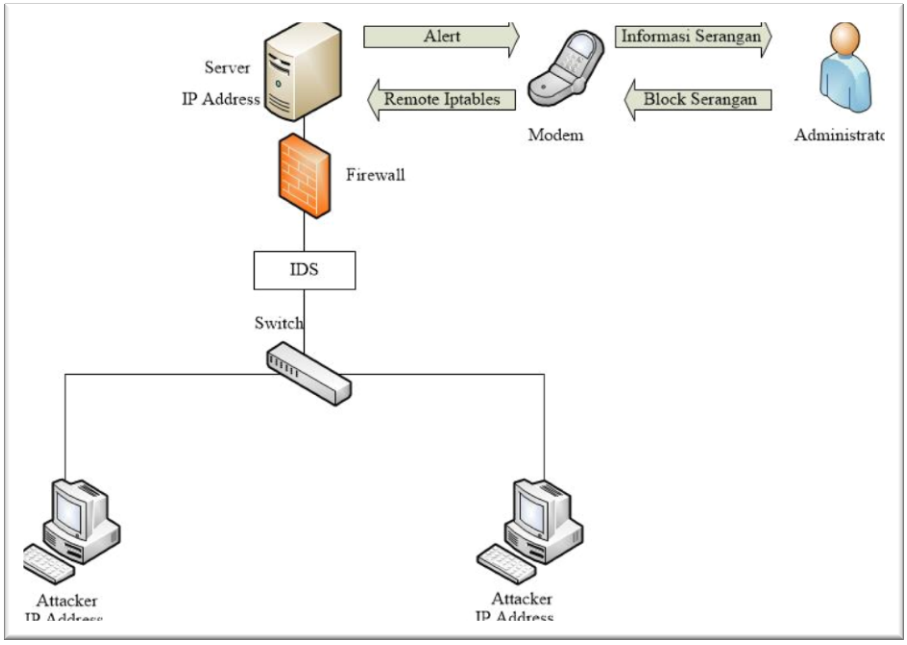
Berdasarkan latar belakang tersebut, perlu dilakukan identifikasi masalah dan rancangan kebutuhan sistem. Identifikasi masalah adalah tahapan awal dalam analisis suatu permasalahan dan cara pemecahan masalah tersebut. Identifikasi masalah pada penelitian ini terletak pada penurunan kinerja jaringan *LAN* yang disebabkan oleh serangan, sehingga perlu pembuatan *Intrusion Detection System* yang terintegrasi dengan *database* dan terkoneksi dengan *SMS gateway*[7-10]. Berdasarkan hal itu, administrator dapat memperoleh informasi serangan dan cara penanggulangan apabila terjadi serangan dengan melakukan *remote iptables*

Berbantuan *SMS gateway*. Diagram alir identifikasi masalah, seperti ditunjukkan pada Gambar 1.



Gambar 1 Diagram alir identifikasi masalah

Rancangan kebutuhan sistem yang diimplementasikan, disesuaikan dengan kebutuhan yang bertujuan untuk optimasi sistem yang dibangun dan untuk kemudahan proses pengembangan sistem. *Remote Iptables* dan *Intrusion Detection System* dengan *Snort* menggunakan *SMS Gateway* meliputi perancangan perangkat keras (*hardware*) dan perangkat lunak (*software*) untuk keluaran (*output*) yang diinginkan. Rancangan kebutuhan sistem secara umum[11], seperti ditunjukkan pada Gambar 2.



Gambar 2 Rancangan kebutuhan sistem secara umum

B. Tujuan

Tujuan penelitian ini, yaitu

1) Memperoleh tahapan pembuatan sistem dan

2) Pengukuran kinerja sistem. Untuk pencapaian tujuan tersebut, diperlukan metode penelitian.

II. METODOLOGI

Tahapan pembuatan sistem dilakukan dengan langkah-langkah:

i) Pembuatan konfigurasi *snort*,

ii) Pembuatan *rules snort*,

iii) Pembuatan *syntax* pemblokiran,

iv) Pembuatan konfigurasi *gammu* agar modem terdeteksi dan terkoneksi dengan *database*, dan

v) Pembuatan sejumlah *scripts* agar saling terintegrasi. Tahapan pengukuran kinerja sistem dilakukan melalui pengetesan dengan pemberian 2 (dua) jenis serangan yaitu: *Ping of Death* dan *SYN Flooding Attack*.

III. HASIL DAN BAHASAN

A. Hasil

a) Tahapan pembuatan sistem

Implementasi sistem yaitu penerapan sistem agar berjalan dengan optimal melalui installasi *software* yang dibutuhkan dan konfigurasi *hardware* dan *software* agar saling terintegrasi. Pada penelitian *Remote Iptables* dan *Intrusion Detection System* (*IDS*) dengan *Snort* berbantuan *SMS Gateway*, yaitu

Intrusion Detection System (*IDS*) terintegrasi dengan *database*, *alert* serangan tersebut akan diambil oleh *gammu* untuk dikirimkan kepada administrator. Administator dapat memblokir serangan dengan cara *Remote Iptables* dengan *SMS Gateway*, yaitu pesan masuk tersimpan di *database gammu* tabel *inbox* yang nantinya akan diproses oleh *PHP* untuk memanggil *iptables* yang akan mengeksekusi pemblokiran serangan.

Konfigurasi *snort* yang terdapat pada *directory* /etc/snort/snort.conf

```
# setup the network addresses you are protecting
ipvar HOME_NET 192.168.1.1
# set up the external network addresses
ipvar EXTERNAL_NET $HOME_NET
# Path to your rules files (this can be a relative path)
var RULE_PATH /etc/snort/rules
var SO_RULES /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules
# Configure output plugins
output database: alert, mysql, user=root, password=root, dbname=snort, host=localhost
```

Pembuatan *rules snort* yang terdapat pada *directory* /etc/snort/rules/local.rules

```
#Rules deteksi Ping of Death
alert icmp any any -> any any (msg:"ping of death now"; dsize:>65536;sid:1000001rev:1)
#Rules deteksi SYN Flooding Attack
alert tcp any any -> $HOME_NET any (msg:"SYN Flooding";flow:stateless;ack:0 flags:S;ttl:>10;reference:arachnids,439;classtype:attempted-recon;sid:10000002;rev:2;)
```

Syntax pemblokiran terdapat pada *directory* /home/apriana/iptables.sh, *iptables* diintegrasikan dengan *shell scripting*, sehingga dapat mempercepat pemblokiran karena dengan satu kali eksekusi dapat melakukan beberapa perintah.

```
#!/bin/bash
# block Ping of Death
# block Syn_flood
iptables -N icmp_flood
iptables –N syn_flood
iptables -A INPUT -p icmp -j icmp_flood
iptables –A INPUT –p tcp --syn -j syn_flood
iptables -A icmp_flood -j DROP
iptables –A syn_flood –j DROP
```

Konfigurasi *gammu* agar modem terdeteksi dan terkoneksi dengan *database*, terdapat pada directory /etc/gammu-smsdrc

```
port = /dev/ttyUSB0                    debuglevel = 1
connection = at115200                  user = root
PIN = 1234                             password = root
service = sql                          database =
```

gammu terdapat pada *directory* /var/www/shell/conn.php

```
<?php
        mysql_connect("localhost","root","root");
        mysql_select_db("gammu");
```

Scripts untuk mengirim *alert* kepada administrator, terdapat pada *directory* /var/www/shell/fungsi2.php

```
<?php
mysql_connect("localhost","root","root");
mysql_select_db("snort");
$qry=mysql_query("SELECT * FROM
signature INNER JOIN event ON
signature.sig_id=event.signature INNER
JOIN iphdr ON event.sid=iphdr.sid ORDER
BY event.timestamp DESC LIMIT 10");
$data=mysql_fetch_object($qry);
$count2="";
$msg="";
while($data=mysql_fetch_object($qry))
{$src=long2ip($data->ip_src);
$dst=long2ip($data->ip_dst);
$count2=$data->timestamp;
$count=$data->timestamp;
$msg=$data->timestamp." - ".$data-
>sig_name." Attack to ".$src." from ".$dst;
}
$count = file_get_contents("snort.txt");
if(strcmp($count2,$count)=="1")
```

Scripts hanya satu nomor telepon yang dapat mengeksekusi perintah, terdapat pada *directory* /var/www/html/shell/fungsi.php

```
if($data->ID>$count)
   {          if          ($data2-
>SenderNumber=="+6289637464253")
          {    file_put_contents("count.txt",
$data->ID);
           execute($data->ID); }
    else mysql_query("DELETE FROM
inbox WHERE id=".$data->ID); }
```

Scripts untuk dapat *remote iptables*, terdapat Pada *directory* /var/www/html/shell/fungsi.php

```
function execute($ID) //eksekusi di shell
{
$data=mysql_fetch_object(mysql_query("
SELECT * FROM inbox WHERE
```

Hasil tahapan pembuatan sistem, yaitu *Intrusion Detection System* yang dapat mendeteksi serangan yang menghasilkan *alert* berupa *text file* dengan 4 (empat) jenis informasi waktu serangan, jenis serangan, IP tujuan, dan IP sumber yang disimpan pada *database* yang kemudian diambil oleh *gammu* untuk diproses dan dikirimkan kepada administrator berupa *SMS*. Pendeteksian yaitu membandingan *packet* dengan *rules* dimana *rules* telah ditentukan. Pemblokiran serangan dengan cara *remote iptables*, yaitu membalas *SMS* dengan kata /home/apriana/iptables.sh pesan tersebut akan masuk ke dalam database *gammu* tabel *inbox* yang nantinya akan diproses oleh *PHP* untuk mengeksekusi dengan *iptables*. Dimana *file* /home/adhia/iptables.sh yaitu sejumlah *syntax* pemblokiran serangan.

b) Pengukuran Kinerja Sistem

Pengukuran kinerja sistem berupa pengetesan yang dilakukan terhadap komputer yang didalamnya telah tertanam *Remote Iptables* dan *Intrusion Detection System* (*IDS*) dengan *Snort* berbantuan *SMS Gateway*. Pengetesan sistem dilakukan dengan penyerangan terhadap *server*, apabila administrator menerima *alert* berupa *SMS* dari *Intrusion Detection System* (*IDS*) dan

administrator dapat memblokir serangan tersebut dengan cara *remote iptables* dengan *SMS Gateway*, maka sistem dapat dikatakan beroperasi dengan optimal. Pengetesan dilakukan dengan 2 (dua) *Operating System* yaitu *Ubuntu Desktop* 16.04 LTS dan *Windows* 7 *Ultimate* 32 *bit* dengan 2 (dua) jenis serangan yaitu: *Ping of Death* dan *SYN Flooding Attack*. Tampilan hasil pengetesan terhadap sistem, seperti ditunjukkan pada Gambar 3.

Gambar 3 Tampilan Hasil Pengetesan *Ping Of Death Attack* Terhadap Sistem

Gambar 4 Tampilan Hasil Pengetesan *SYN Flooding Attack* Terhadap Sistem

Berdasarkan Gambar 3 ditunjukkan, bahwa serangan *ping of death* dan *SYN flooding attack* dapat terdeteksi oleh *Intrusion Detection System* (*IDS*), *alert* serangan tersebut dikirimkan kepada administrator berupa *SMS* dengan 4 (empat) jenis informasi, yaitu waktu serangan, jenis serangan, *IP* tujuan, dan *IP* sumber. Administrator memblokir serangan tersebut dengan membalas *SMS*, pesan tersebut akan memanggil *iptables* untuk memblokir serangan. Hasil pengetesan *ping of death*, seperti ditunjukkan pada Gambar 3(a). Hasil pengetesan *SYN flooding attack*, seperti ditunjukkan pada Gambar 3(b). Penjelasan hasil pengetesan terhadap sistem , seperti ditunjukkan pada Tabel 1.

Tabel 1 Penjelasan hasil pengetesan terhadap sistem

Attacker	*Operating System*	Serangan	*Tools*	*IDS*	*Iptables*
192.168.1.1	*Ubuntu Desktop* 17.04	*Ping of Death*	*Hping3*	✓	✓
		SYN Flood	*Hping3*	✓	✓

192.168.1.2	*Windows 7 Ultimate 32 bit*	*Ping of Death*	*Command prompt*	✓	✓
		SYN Flood	*Digital Blaster*	✓	✓

Keterangan: ✓ terdeteksi (untuk *IDS*), terblokir (untuk *Iptables*)

Berdasarkan Tabel 1. ditunjukkan, bahwa pengetesan terhadap sistem dengan 2 (dua) jenis serangan, yaitu *ping of death* dan *SYN flooding attack*, dengan 2 (dua) *Operating System* dan *tools* berbeda, sistem berhasil mendeteksi dan memblokir serangan, maka sistem dapat dikatakan berjalan secara optimal.

IV. PENUTUP

Berdasarkan pembahasan, ditarik simpulan sesuai tujuan penelitian.

1) Hasil dari penerapan *Intrusion Detection System* (*IDS*) berhasil mendeteksi serangan melalui 5 (lima) tahapan, yaitu : konfigurasi *snort*, pembuatan *rules snort*, pembuatan *syntax* pemblokiran, konfigurasi *gammu* dan pembuatan sejulah *scripts* agar saling terintegrasi satu sama lain, sehingga menghasilkan *alert* berupa *SMS* dengan 4 (empat) jenis informasi, yaitu: waktu serangan, jenis serangan, *IP* tujuan, dan *IP* sumber.
2) Hasil pengetesan terhadap pengetesan terhadap sistem dengan 2 (dua) jenis serangan, yaitu *ping of death* dan *SYN flooding attack*, *attacker* (192.168.1.2) menggunakan *Operating System Ubuntu Desktop* 17.04 melakukan kedua serangan tersebut dengan *tools hping3* serangan dapat terdeteksi oleh *Intrusion Detection System* (*IDS*) dan terblokir oleh *iptables*. *Attacker* (192.168.1.1) menggunakan *Operating System Windows* 7 *Ultimate* 32 *bit* melakukan kedua serangan tersebut dengan *tools command prompt* dan *digital blaster*, kedua serangan dapat terdeteksi oleh *Intrusion Detection System* (*IDS*) dan terblokir oleh *iptables* .

V. DAFTAR PUSTAKA

[1] Taluja, Sachin, Pradeep Kumar Verma, Rajeshwar Lal Dua, 2012, "Network Security Using IP firewalls" in *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 2 Issue 8, August 2012, pp. 348-354.

[2] Ur Rehman, Rafeeq, 2003, *Intrusion Detection Systems with Snort*, Prentice Hall PTR, pp. 23-73.

[3] Boob, Snehal, Priyanka Jadhav, 2010, "Wireless Intrusion Detection System" in *International Journal of Computer Applications*, Volume 5– No.8, August 2010, pp. 9-13.

[4] Gunasekhar, T., K.Thirupathi Rao, P.Saikiran, P.V.S. Lakshmi, 2014, "A Survey on Denial of Service Attacks" in *International Journal of Computer Science and Information Technologies* (*IJCSIT*), Vol. 5 (2), 2014, pp. 2373-2376.

[5] Vijayarani, S., Maria Sylviaa.S, 2015, "Intrusion Detection System – A Study" in *International Journal of Security, Privacy and Trust Management* (IJSPTM), Vol 4, No 1, February 2015, pp. 31-44.

[6] Nemade, Sonali, Madhuri, A. Darekar, Jyoti Bachhav, 2016, "Intrusion Detection System in Wireless LANs: A Review" in *International Journal of Innovative Research in Computer and Communication Engineering*, Vol. 4, Issue 9, September 2016, pp. 16358-16361.

[7] Katherine Booth Wellington, 2013, "Cyberattacks on Medical Devices and Hospital Networks: Legal Gaps and Regulatory Solutions" in *Santa Clara High Technology Law Journal*, Vol. 30, Issue 2, January 2013, pp. 142.

[8] Rao, Udai Pratap, Dhiren R. Patel, 2011,"Design and Implementation of Database Intrusion Detection System for Security in Database" in *International Journal of Computer Applications,*Vol. 35-No. 9, December 2011,pp. 33.

[9] Mehra, Pritika, 2012, "A brief study and comparison of Snort and Bro Open Source Network Intrusion Detection Systems" in *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 1, Issue 6, August 2012, pp. 383.

[10] Junita Juwita Siregar, Rubil, 2014, "The Prototype Design Academic Information For Management Of Exams Quiz University Stundent Based On SMS Gateway" in *Journal of Theoretical and Applied Information Technology*, Vol. 65 No.1,10th July 2014, pp. 248-249.

[11] Tejvir Kaur, Vimmi Malhotra, Dr. Dheerendra Singh, 2014, "Comparison of network security tools- Firewall Intrusion Detection System and Honeypot" in *International Journal of Enhanced*

Research in Science Technology & Engineering, Vol. 3 Issue 2, February 2014, pp. 201-202.

[12] *Windi Apriana[1)], Bayu Adhi Prakosa[2)], Ade Hendri Hendrawan[3)], Arief Goeritno[4)]*

Remote Iptables dan *Intrusion Detection System* (*IDS*) dengan *Snort* Berbantuan *SMS Gateway* pada Jaringan Fakultas Teknik Universitas Ibn Khaldun Bogor Seminar Nasional Inovasi Dan Aplikasi Teknologi Di Industri 2017 ITN Malang, 4 Pebruari 2017