REMOTE IPTABLES DAN *INTRUSION DETECTION SYSTEM* (*IDS*)DENGAN *SNORT* BERBANTUAN *SMS GATEWAY* PADA JARINGAN FAKULTAS TEKNIK UNIVERSITAS IBN KHALDUN BOGOR

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

[1,2),3)]Jurusan/Program Studi Teknik Informatika
[4)]Jurusan/Program Studi Teknik Elektro
Fakultas Teknik, Universitas Ibn Khaldun Bogor
Jl. Sholeh Iskandar km.2, Kedung Badak, Tanah Sareal,Kota Bogor 16162 Telpon:0251-8356884
Email: apriana517@gmail.com

Abstrak . *Telah dilakukan Remote Iptables dan Intrusion Detection System (IDS) dengan Snort berbantuan SMS Gateway. Jaringan komputer di Fakultas Teknik UIKA Bogor saat ini sering terdapat keluhan berkaitan dengan penurunan kinerja jaringan Internet, karena sejumlah serangan ping of death dan SYN flooding attack yang berimbas ke semua komputer yang terhubung pada jaringan tersebut. Berdasarkan hal itu, dibutuhkan sistem pendeteksian serangan dan pencegahannya secara tepat agar dapat membantu administrator dalam pengamanan jaringan. Pembuatan Remote Iptables dan Intrusion Detection System dengan Snort berbantuan SMS GatewayI, sehingga diperoleh alert serangan secara real time melalui SMS, sejumlah syntax permblokiran dengan remote iptables berbantuan SMS Gateway, dan pemblokiran secara real time. Tahapan yang digunakan untuk pencapaian tujuan penelitian, adalah identifikasi masalah, design kebutuhan sistem, implementasi sistem, dan testing. Hasil pendeteksian berupa 4 (empat) jenis informasi, yaitu waktu serangan, jenis serangan IP tujuan, dan IP sumber. Deteksi dan pemblokiran serangan berdasarkan sejumlah syntax yang dilakukan dengan cara pembandingan packet terhadap rules berupa pengintegrasian melalui SMS Gateway untuk kemudahan administator dalam pengeksekusian pemblokiran. Pemblokiran serangan berupa 3 (tiga) jenis informasi, yaitu IP sumber, jenis serangan, dan kebijakan (ditolak atau diterima). Berdasarkan hasil tersebut disimpulkan, berupa serangan dapat terdeteksi secara real time terhadap 4 jenis informasi, pemblokiran serangan diintegrasikan melalui SMS Gateway berupa pembandingan packet terhadap rules, dan pemblokiran serangan berupa Remote Iptables dengan 3 (tiga) jenis informasi.*

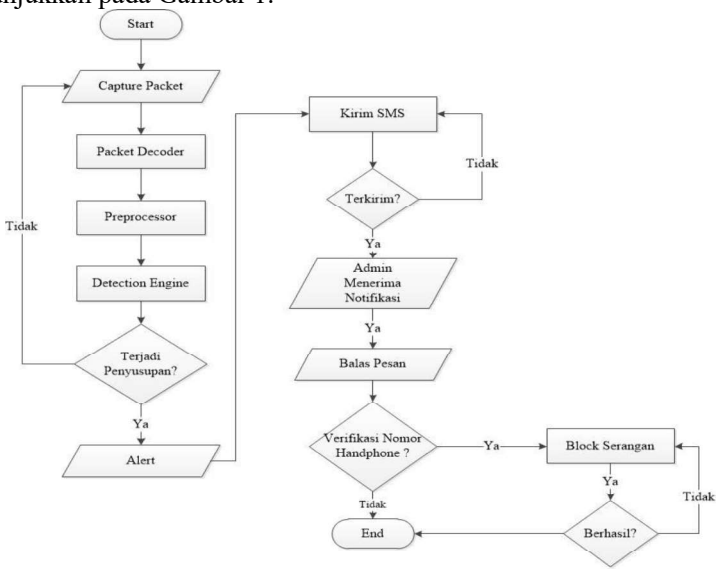
Kata kunci: *Remote Iptables, Intrusion Detecion System, SMS Gateway.*

1. Pendahuluan

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]. Jaringan komputer di Fakultas Teknik Universitas Ibn Khaldun Bogor saat ini sering terdapat keluhan, seperti penurunan kinerja jaringan *Internet* yang melemah dan dapat berimbas ke semua komputer yang berhubungan pada jaringan tersebut.

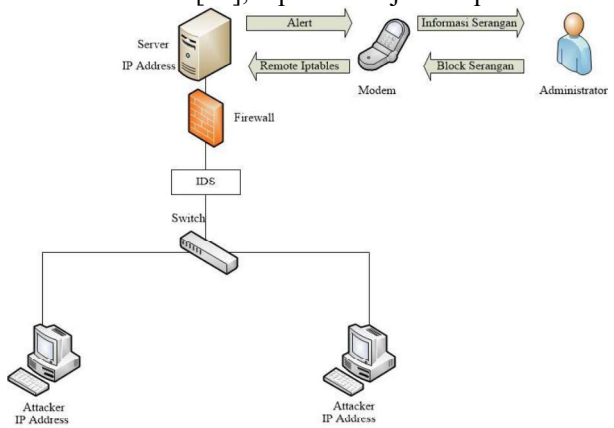
Kebutuhan sistem pendeteksi serangan yang dapat membantu administrator dalam pemantauan (*monitoring*) jaringan, sehingga administrator dapat menanggulangi ancaman secara cepat dan jaringan dapat beroperasi kembali secara optimal [5]. Penerapan sistem pengamanan jaringan yang mampu mendeteksi serangan 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 *Internet* 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* berbantuan *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

Tujuan penelitian ini, yaitu 1) memperoleh tahapan pembuatan sistem dan 2) pengukuran kinerja sistem. Untuk pencapaian tujuan tersebut, diperlukan metode penelitian. 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*.

2. Pembahasan

2.1. 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
iptables -N icmp_flood
iptables -A INPUT -p icmp -j icmp_flood
iptables -A icmp_flood -j DROP

# block Syn_flood
iptables –N syn_flood
iptables –A INPUT –p tcp --syn -j syn_flood
iptables –A syn_flood –j DROP
```

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

```
port = /dev/ttyUSB0
connection = at115200
PIN = 1234
service = sql
driver = native_mysql
logfile = /var/log/smsdlog

debuglevel = 1
user = root
password = root
database = gammu
pc = localhost
```

Scripts untuk memanggil *database gammu* terdapat pada *directory* /var/www/shell/conn.php

```
<?php
        mysql_connect("localhost","root","root");
        mysql_select_db("gammu");
        date_default_timezone_set("Asia/Bangkok"); ?>
```

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")
{file_put_contents("snort.txt", $count2);
echo $msg;          else echo "0"; ?>
```

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
{    $data=mysql_fetch_object(mysql_query("SELECT * FROM inbox
WHERE ID=".$ID));
        exec('sudo '.$data->TextDecoded); }
```

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/apriana/iptables.sh yaitu sejumlah *syntax* pemblokiran serangan.

2.2. 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*, sehingga sistem dapat dikatakan beroperasi optimal. Pengetesan dilakukan dengan 2 (dua) *Operating System* yaitu *Ubuntu Desktop* 16.04 LTS dan *Windows* 7 *Professional* 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.

Hasil Pengetesan Ping of Death Hasil Pengetesan SYN Flooding Attack

Gambar 3 Tampilan hasil pengetesan terhadap system

Berdasarkan Gambar 3 ditunjukkan, bahwa penjelasan terhadap hasil pengetesan terhadap sistem. Penjelasan hasil pengetesan terhadap sistem, seperti ditunjukkan pada Tabel 1.

Tabel 1 Penjelasan hasil pengetesan terhadap sistem

Attacker	*Operating System*	Serangan	*Tools*	*IDS*	*Iptables*
192.168.1.2	*Ubuntu Desktop* 16.04 LTS	*Ping of Death*	*Hping3*	✓	✓
		SYN Flood	*Hping3*	✓	✓
192.168.1.3	*Windows* 7 *Professional* 32 *bit*	*Ping of Death*	*Command prompt*	✓	✓
		SYN Flood	*Digital Blaster*	✓	✓

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

3. Simpulan

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 sistem dengan 2 (dua) jenis serangan, yaitu *ping of death* dan *SYN flooding attack*, *attacker* (192.168.1.2) menggunakan *Operating System Ubuntu Desktop* 16.04 LTS melakukan kedua serangan tersebut dengan *tools hping3* serangan dapat terdeteksi oleh *Intrusion Detection System* dan terblokir oleh *iptables*. *Attacker* (192.168.1.3) menggunakan *Operating System Windows* 7 *Professional* 32 *bit* melakukan kedua serangan tersebut dengan *tools command prompt* dan *digital blaster* serangan dapat terdeteksi oleh *Intrusion Detection System* dan terblokir oleh *iptables*.

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.