Deteksi serangan maya pada komputer server berbasis SMS Gateway

Supardinata[1#] , Nur Cahyono K, S.Si., M.Sc[2#]

1# Politeknik Negeri Batam
Program Studi Teknik Informatika
Parkway Street, Batam Centre, Batam 29461, Indonesia
E-mail: supardinataa@gmail.com

2# Politeknik Negeri Batam
Program Studi Teknik Informatika
Parkway Street, Batam Centre, Batam 29461, Indonesia
E-mail: anung@polibatam.ac.id

Abstrak

Seiring komputer server terhubung dengan jaringan internet maka diperlukan proteksi yang lebih protektif guna menghindari dari ancaman serangan dari penyusup. Sering kali kendala yang dihadapi oleh para administrator jaringan adalah keterlambatannya penanggulangan langkah responsif untuk mencegah terjadinya serangan pada komputer server. Sistem deteksi ini memanfaatkan aplikasi Snort dengan mode IDS (intrusion detection system) dan SMS gateway yaitu Gammu dengan tujuan untuk mendeteksi terjadinya serangan maya secara *realtime*, mengirimkan SMS kepada Administrator secara automatis jika terdapat aktivitas jaringan yang mencurigakan, dan mencegah aksi terlalu jauh bagi penyusup. Akhirnya, administrator jaringan tidak perlu berada didepan komputer server seharian karena sistem deteksi ini dapat memonitoring selama sistem berjalan.

Kata kunci: Komputer server, administrator, serangan maya, *monitoring,* sms gateway

Abstract

A computer server connected to the Internet network will require more protection protective order to avoid the threat of attacks from intruders. Often the constraints faced by the network administrator is the response delay a response action to prevent attacks on the server computer. The detection system utilizes application Snort with mode IDS (intrusion detection system) and SMS gateway that Gammu with the aim to detect the occurrence of cyber attacks in real time, send a SMS to the administrator automatically if there is a suspicious network activity, and prevent the action too much for intruders. Finally, the network administrator does not need to be in front of the server computer all day because of this detection system can monitor for system running.

Keywords : Computer server, administrator, cyber attacks, monitoring, sms gateway

1 Pendahuluan

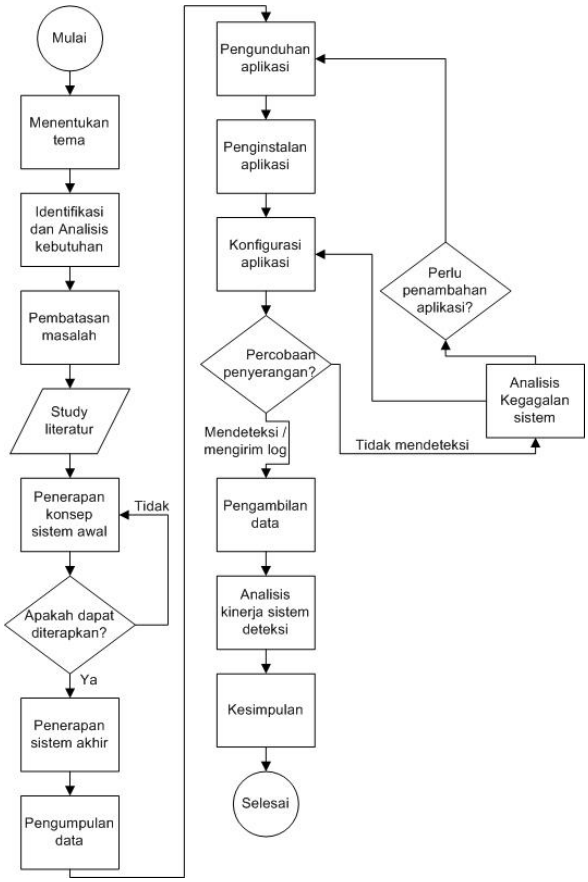
Komputer server merupakan elemen penting dalam sebuah jaringan. Jika komputer server tidak memiliki perlindungan yang maksimal maka akan mudah diserangan oleh penyusup (*cyber attack*). Mengingat di Indonesia kian tahun meningkat kasus penyerangan oleh penyusup yaitu sekitar 36,6 juta serangan terhitung agustus 2015[1]. Maka diperlukan sebuah sistem yang dapat memantau kondisi komputer server secara real-time sehingga penyusupan kedalam jaringan dapat diketahui sedini mungkin dan dapat

menimalisir aksi penyusupan. Untuk itu kegiatan ini membahas metode deteksi serangan pada komputer server tanpa harus administrator didepan komputer server dengan memanfaatkan fitur SMS *gateway* sebagai media notifikasi.

Berbeda pada penelitian sebelumnya[2] yang menggunakan jejaring sosial dan aplikasi *intrusion detection system* (IDS) yaitu Snort[3]. Pada penelitian sebelumnya memanfaatkan jejaring sosial sebagai media notifikasi yang menurut penulis kurang efisien, dikarenakan memiliki titik lemah pada ketergantungan pada akses internet maka untuk menutupi kekurangan tersebut dibuatlah sistem yang dapat mengirimkan pemberitahuan serangan yang sedang terjadi secara cepat dan efisien dengan memanfaatkan SMS sebagai media notifikasinya. SMS hanya memerlukan sinyal operator seluler yang digunakan saja tidak seperti media jejaring sosial yang harus memerlukan akses internet.

2 Metodologi

Metodologi pada kegiatan ini dapat dilihat pada gambar diagram alir dibawah ini.



Gambar 1: diagram alir

A. Menentuan tema

Menentukan tema merupakan langkah awal yang akan diambil untuk menentukan rancangan yang akan diterapkan. Dalam perancangan ini memiliki tema tentang suatu "**sistem deteksi serangan yang mampu mengirimkan hasil deteksi melalui sms**".

B. Identifikasi dan analisis kebutuhan

Sistem deteksi yang akan diterapkan nanti mampu memenuhi syarat sebagai berikut :

1. Mampu mengenali, mendeteksi, dan mengirimkan sms serangan.
2. Mampu menampilkan hasil serangan kedalam database dan dapat diakses melalui web base.
3. Sistem dapat bekerja secara real-time.

TABEL I

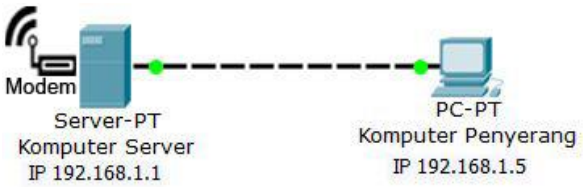
PERANGKAT KERAS YANG DIGUNAKAN

No.	Hardware
1	Laptop (komputer server)

2	Modem (vodafone K3565 – Rev 2)
3	Simcard (kartu operator seluler)
4	Kabel LAN (UTP)
5	Laptop (Komputer penyerang)

C. Pembatasan masalah

Sistem yang akan diimplementasikan hanya sebagai simulasi yang terdiri dari komputer server dan komputer penyerang dimana komputer server dipasangi modem yang telah dipasangi *sim card* dan komputer penyerang bersistem operasi Kali Linux.



Gambar 2: rancangan percobaan

D. Study literatur

Study literatur digunakan hanya untuk memahami teori dasar tentang cara kerja aplikasi IDS dan sms gateway. Sehingga mampu memberikan gambaran dalam penerapan sistem deteksi serangan ini.

E. Penerapan konsep sistem awal

Penerapan konsep sistem awal yaitu ide-ide tentang bagaimana fungsi aplikasi pada masing-masing aplikasi dapat terintegrasikan sehingga menjadi sistem yang dapat mendeteksi serangan dan mengirimkan hasil *log* deteksi serangan.

F. Penerapan sistem akhir

Penerapan sistem akhir yaitu setelah sistem awal dianalisis melalui berbagai uji coba sehingga dapat diimplementasikan menjadi suatu sistem yang diharapkan.

G. Pengumpulan data

Mendaftar apa-apa saja yang menjadi komponen penting dan pendukung dalam penerapan sistem deteksi serangan ini. Seperti mendata aplikasi yang dibutuhkan, konfigurasi, jenis serangan yang akan diuji cobakan dan perangkat keras yang digunakan.

TABEL II

SERANGAN YANG AKAN DIUJI COBAKAN

No.	Jenis Serangan
1.	Ping
2.	Port Scanning
3.	SQL Injection
4.	Akses URL Rahasia
5.	DoS Attack

H. Pengunduhan dan penginstalan aplikasi

Langkah ini melakukan pengunduhkan dan penginstalan aplikasi yang berperan penting dalam sistem deteksi serangan.

TABEL III

APLIKASI YANG DIGUNAKAN

No.	Aplikasi
1.	Snort ver. 2.9.7.0
2.	Gammu ver. 1.33.0
3.	Pcap
4.	PCRE
5.	Libdnet
6.	DAQ
7.	Barnyard2
8.	BASE (*Basic Analysis and Security Engine*)
9.	ADODB 5.18

I. Konfigurasi aplikasi

Melakukan segala konfigurasi pendukung meliputi aplikasi dan maupun perangkat keras agar sistem dapat saling terintegrasi.

TABEL IV

KONFIGURASI RULE SNORT

No.	serangan	Rule Snort
1.	Ping	Alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"Penyusup mencoba PING Server";threshold: type both, track by_src, count 20, seconds 60; sid:10000001; rev:001;)
2.	Port Scanning	alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"SCAN nmap XMAS"; flow:stateless; flags:FPU,12; reference:arachnids,30; classtype:attempted-recon; sid:1228; rev:7;)
3.	SQL Injection	alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"SQL Injection Paranoid ";flow:to_server,established;uricontent:".php ";pcre:"/(\%27)|(\')|(\-\-)|(%23)|(#)/i";classtype:Web-application-attack; sid:9099; rev:5;)
4.	Akses URL Rahasia Admin	alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (sid:1002354;rev:2;msg:"Akses url rahasia admin"; uricontent:"/home";classtype:web-application-activity;)
5.	DoS Attack	alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (flags: S; msg:"Possible TCP DoS"; flow: stateless; threshold: type both, track by_src, count 70, seconds 60; sid:1000003;rev:1;)

J. Analisis kegagalan

Jika dalam konfigurasi sistem belum dapat bekerja dengan semestinya maka kegagalan ini akan dianalisis guna memperbaiki sistem yang gagal.

K. Pengambilan data

Mengumpulkan data serangan yang dapat dideteksi untuk tujuan analisis.

L. Analisis kinerja sistem deteksi

Serangan yang dapat dideteksi dan berhasil dikirim melalui sms ke administrator akan dianalisis seberapa akurat sistem dapat mendeteksi serangan dan dapatkah fungsi sistem bekerja sesuai dengan harapan.

M. Kesimpulan

Setelah melakukan berbagai percobaan maka didapatkan suatu kesimpulan yang bisa diambil berdasarkan pengujian.

4 Implementasi dan Hasil

A. Implementasi Deteksi Serangan

Adapun persiapan yang dilakukan pada komputer server dalam menjalankan sistem deteksi yaitu :

1. Komputer server IP 192.168.1.1
2. Menjalankan service apache2 sebagai web server serta service mysql
3. Menjalankan perintah diterminal

```
- sudo service snort start
- sudo service barnyard2 start
- firefox localhost/php/realtime.php
- firefox localhost/base
- gammu-smsd
```

4. sekarang sistem deteksi sedang berjalan (*running*)

B. Implementasi Serangan

Adapun perintah serangan yang dilancarkan dikomputer penyerang yaitu :

1. Ping ip target

```
ping 192.168.1.1
```

2. Scanning port

```
Port scanning 22 :
      nmap –sX –p 22 192.168.1.1
Port scanning 80 :
      nmap –sX –p 80 192.168.1.1
```

3. SQL injection berupa memasukkan username dan password ke halaman yang memiliki login page diwebsite target.

```
Username : admin'/*
Password : hancurkan')*/ OR ('1'='1
```

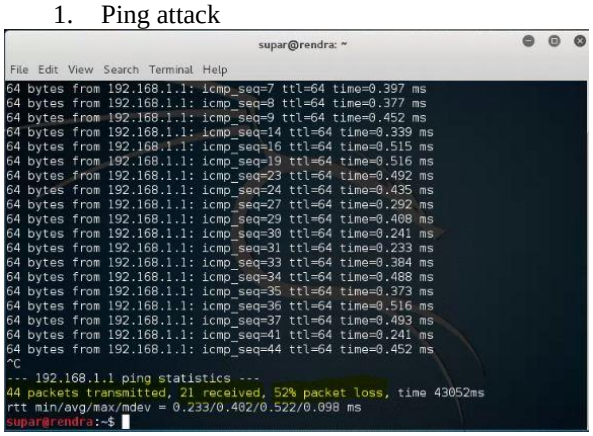
4. Pada contoh kasus ini dibuat website sederhana yang memiliki halaman rahasia "**home**". Perintah akses URL rahasia yaitu hanya mengklik link "**home**" yang merupakan halaman rahasia diwebsite target.
5. Perintah DoS attack

```
nping –tcp-connect -rate=100 -c 300 -q 192.168.1.1
```

C. Hasil Deteksi serangan

Adapun hasil dari implementasi serangan yang dilakukan komputer penyerang dapat dilihat pada gambar dibawah ini.

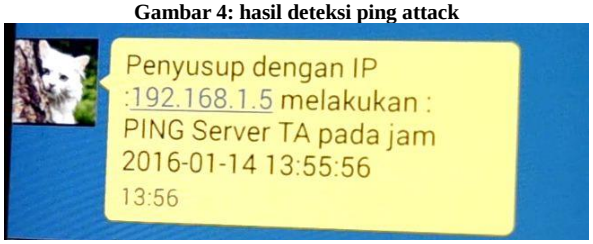
1. Ping attack



Gambar 3: ping attack dikomputer penyerang

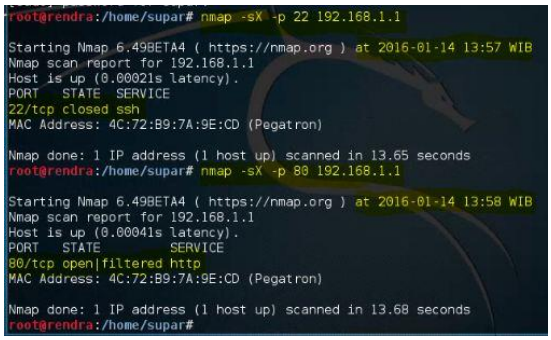
IP Asal	IP Tujuan	Jenis Alert	Waktu
192.168.1.5	192.168.1.1	PING Server TA	2016-01-14 13:55:56

Gambar 4: hasil deteksi ping attack



Gambar 5: hasil ping attack telah terkirim melalui sms

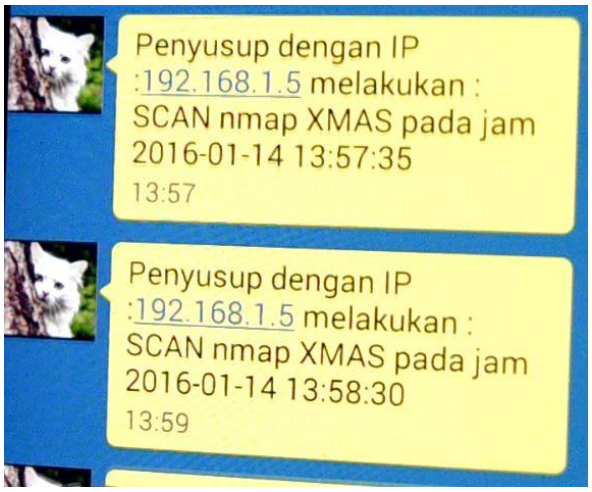
2. *Port Scanning*



Gambar 6: port scanning dikomputer penyerang

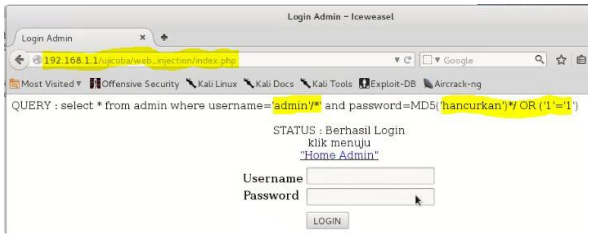
IP Asal	IP Tujuan	Jenis Alert	Waktu
192.168.1.5	192.168.1.1	SCAN nmap XMAS	2016-01-14 13:58:30
192.168.1.5	192.168.1.1	SCAN nmap XMAS	2016-01-14 13:57:35

Gambar 7: hasil deteksi *port scanning*



Gambar 8: hasil *port scanning* telah terkirim melalui sms

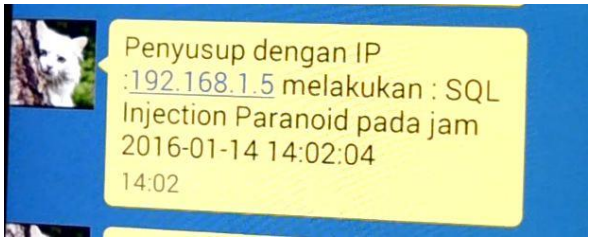
3. SQL Injection



Gambar 9: SQL *Injection* dikomputer penyerang

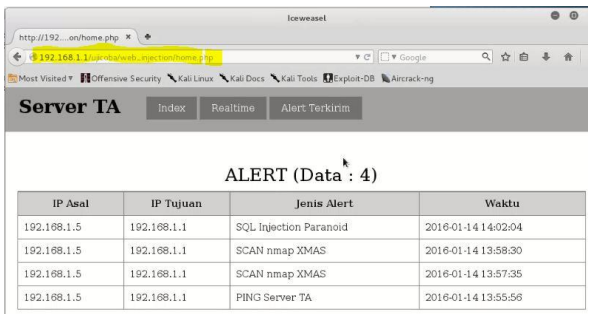
IP Asal	IP Tujuan	Jenis Alert	Waktu
192.168.1.5	192.168.1.1	SQL Injection Paranoid	2016-01-14 14:02:04

Gambar 10: hasil deteksi SQL *Injection*



Gambar 11: hasil SQL *Injection* telah terkirim melalui sms

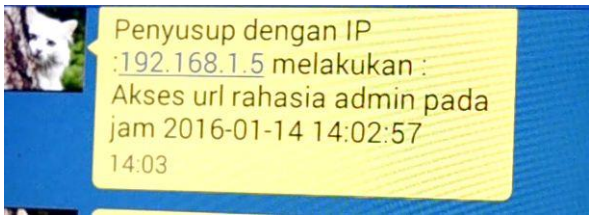
4. Akses URL Rahasia



Gambar 12: akses url rahasia dikomputer penyerang

IP Asal	IP Tujuan	Jenis Alert	Waktu
192.168.1.5	192.168.1.1	Akses url rahasia admin	2016-01-14 14:02:57

Gambar 13: hasil deteksi akses url rahasia



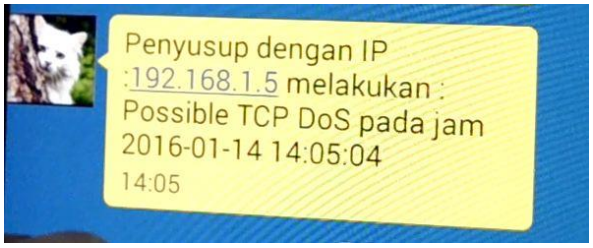
Gambar 14: akses url rahasia telah terkirim melalui sms

5. DoS attack

Gambar 15: DoS attack dikomputer penyerang

IP Asal	IP Tujuan	Jenis Alert	Waktu
192.168.1.5	192.168.1.1	Possible TCP DoS	2016-01-14 14:05:04

Gambar 16: hasil deteksi DoS attack



Gambar 17: DoS attack telah terkirim melalui sms

5 Kesimpulan

Dari hasil implementasi dan pengujian kegiatan "**Deteksi serangan maya pada komputer server berbasis sms gateway**" dapat ditarik kesimpulan:

1. Sistem dapat mendeteksi serangan secara *realtime* dan automatis mengirimkan pesan jika terjadi serangan.
2. Aplikasi IDS (*Intrusion Detection System*) Snort dapat diintegrasikan dengan aplikasi sms gateway yaitu gammu, sehingga menjadi sistem yang dapat mendeteksi serangan atau aktivitas jaringan yang mencurigakan dan mengirimkan pesan secara automatis melalui sms ke *handphone* administrator dengan waktu yang relatif cepat yaitu kurang dari 30 detik.
3. Sistem deteksi serangan maya pada komputer server ini telah berfungsi dua arah yaitu komputer server mengirimkan pesan serangan ke *handphone* administator dan administrator dapat mengirimkan sms yang

fungsinya untuk memutuskan koneksi jaringan agar penyerang tidak leluasa dalam mengeksploit komputer server ataupun mencegah aksi terlalu jauh kedalam sistem.

4. Aplikasi IDS (*Intrusion Detection System*) Snort dapat mendeteksi berbagai serangan yang sudah didefinisikan dalam rules snort dan menginputkan hasil deteksi serangan ke dalam database.

Kata Sambutan

Penulis ucapkan puji syukur atas limpahan rahmat Allah SWT yang senantiasa memberi kemudahan dalam penyelesaian tugas akhir ini. Tidak luput jua kedua orang tua yang selalu mendukung baik materil maupun doa. Bapak Nur Cahyono K., S.Si, M.Sc. selaku pembimbing, dan seluruh orang yang turut andil dalam membantu penulis dalam menyelesaikan tugas akhir ini yang tidak dapat disebutkan satu per satu.

Referensi

[1] Oni, 2015, Serangan Hacker Rugikan Negara Rp33,29Miliar, http://nasional.harianterbit.com/nasional/2015/08/25/39345/43/25/Serangan-Hacker-Rugikan-Negara-Rp3329-Miliar , diakses pada 28 agustus 2015.

[2] Catur Sahid, dkk, 2014. *Implementasi intrusion detection system (IDS) menggunakan jejaring sosial sebagai media notifikasi*. FTI, IST AKPRIND, Yogyakarta

[3] Kaur, T., & Kaur, S. (1930). *Comparative Analysis of Anomaly Based and Signature Based Intrusion Detection Systems Using PHAD and Snort*. School of Mathematics and Computer Science Applications,Thapar University.