RANCANG BANGUN APLIKASI DETEKSI DAN PENANGANAN SERANGAN DDOS DAN *PORT SCANNING* MEMANFAATKAN SNORT PADA JARINGAN KOMPUTER

Rizkial Achmad[(1)], Evanita Veronica Manullang[(2)], Emha Rizal Sanmas[(3)]

iky.mtech@gmail.com
eva.manullang@gmail.com
rizalsanmas6@gmail.com

[1)] Staf Pengajar Pada Program Studi Sistem Informasi
[2)] Staf Pengajar Pada Program Studi Teknik Informatika
Fakultas Ilmu Komputer dan Manajemen
Universitas Sains dan Teknologi Jayapura

Abstraksi - *Keamanan dalam jaringan komputer merupakan hal yang wajib diperhatikan khususnya pada komputer server. Mengingat fungsi server sebagai penyedia layanan dan pusat dari jaringan komputer maka tidak jarang menjadi sasaran dari berbagai macam serangan cyber seperti DDoS, Port Scanning, SQL Injection dan lain-lain. Serangan-serangan tersebut memiliki dampak yang berbahaya bahkan sampai mengakibatkan down pada layanan server. Penerapan Intrution Detection System (IDS) berupa sistem deteksi dini sangat dibutuhkan untuk dapat meminimalisir serangan yang terjadi sekaligus membantu seorang administrator untuk dapat mengenali serangan maupun ancaman yang terjadi. Penelitian ini bertujuan untuk membuat sebuah sistem yang dapat mendeteksi serangan DDoS dan Port Scanning dengan menggunakan Snort dan juga melakukan penanganan terhadap serangan-serangan tersebut. Hasil dari penelitian yang dilakukan yaitu sistem yang dibangun dapat mendeteksi serangan DDoS dan Port Scanning dengan memanfaatkan Snort sebagai tool pendeteksi serangan. Sistem juga dapat mengirimkan notifikasi peringatan kepada administrator melalui SMS dengan menggunakan layanan SMS Gateway Nexmo SMS Application Programming Interface (API) berdasarkan serangan yang terdeteksi dan mampu melakukan penanganan serangan dengan memanfaatkan IPTables berdasarkan analisa yang dilakukan oleh administrator.*

Keyword **: Keamanan Komputer, *Intrution Detection System* (IDS), Snort, *Port Scanning,* DDoS, Nexmo SMS API, IPTables**

1. PENDAHULUAN

Jaringan komputer merupakan suatu sistem yang sangat berperan penting didalam perkembangan teknologi pada zaman ini dimana fungsi dari jaringan komputer itu sendiri diantaranya melayani hubungan antar komputer sehingga dapat saling terkoneksi dan mampu melakukan aktivitasnya seperti *sharing file*, *printer*, akses data dan banyak hal lainnya. Dengan adanya jaringan komputer sangat mempermudah penggunanya dalam memenuhi kebutuhan selama menjalankan pekerjaannya. Mengingat peran *vital* jaringan komputer sebagai penghubung setiap komputer, maka jaringan komputer menjadi sasaran utama dari berbagai macam jenis serangan baik yang mengarah pada setiap komputer maupun sistem jaringan secara langsung. Serangan-serangan yang terjadi pada jaringan komputer dapat membebani trafik jaringan sehingga koneksi maupun aksesbilitas menjadi terhambat. Berdasarkan penjelasan tersebut maka penelitian yang dilakukan yaitu dengan membangun sebuah sistem yang dapat mendeteksi adanya anomali yang terdapat di dalam jaringan komputer dengan memanfaatkan *Intrusion Detection System (IDS)* menggunakan *Snort* sebagai *tool* nya. Sistem yang akan dibangun dapat mengirimkan *message* atau notifikasi dan dapat melakukan pencegahan serangan.

Untuk menghindari meluasnya pembahasan penelitian ini, maka penelitian ini dibatasi pada :

1. Sistem yang dibangun memanfaatkan *tool* Snort sebagai pendeteksi dan pemberi *warning* terhadap suatu serangan.
2. Sistem menyimpan *alert* serangan memanfaatkan *tool* Barnyard2 untuk menampilkan *log* Snort ke dalam *Database*.
3. Sistem dapat melakukan penanganan terhadap serangan memanfaatkan *tool Firewall* pada Linux yaitu IPTables.
4. Sistem akan memberikan notifikasi kepada administrator dengan memanfaatkan SMS *Gateway* berupa informasi jenis serangan dan alamat IP penyerang.
5. Sistem menggunakan 5 *rules* Snort untuk mendeteksi serangan berikut ini :
   a. ICMP (*Internet Control Message Protocol*) *Attack .*
   b. *Ping Of Death Attack*.
   c. UDP *Flood Attack*.
   d. TCP *Scanning Port*.
   e. UDP *Scanning Port*.
6. Sistem yang dibangun menggunakan bahasa pemograman PHP.
7. Sistem SMS *Gateway* yang digunakan yaitu SMS *Notification* dengan memanfaatkan Nexmo SMS API.
8. Sistem operasi yang digunakan pada *server* yaitu Ubuntu 16.04.
9. Skema jaringan menggunakan topologi *STAR* pada jaringan Smart Campus USTJ.

2. TINJAUAN PUSTAKA

Parningotan Panggabean (2018), *Analisis Network Security SNORT Menggunakan Metode Intrusion Detection System (IDS) Untuk Optimasi Keamanan Jaringan Komputer.* Penelitian ini dilakukan dengan tujuan untuk mendeteksi serangan *Denial of Service (DoS)* pada jaringan *internal* dan *external* Dinas Lingkungan Hidup Pemerintah Kota Batam. Penelitian ini dapat mendeteksi serangan DoS dengan metode TCP *Flooding*, UDP *Flooding* dan *HTTP Flooding*.

Novi Kezia Kawiyan (2017), *Rancang Bangun Aplikasi Server Monitoring Untuk Deteksi Dini Serangan DDOS Dan Backodoor Pada Server Berbasis Windows*. Didalam penelitian ini, peneliti melakukan perancangan dan pembangunan sebuah aplikasi *monitoring* yang bertujuan untuk mendeteksi serangan DDoS dan *Backdoor* dengan menggunakan Snort untuk memantau paket data yang mengandung serangan-serangan tersebut. Penelitian ini dilakukan pada *server* berbasis Window dan mampu mendeteksi serangan bentuk serangan DDoS baik menggunakan *TCP* maupun *UDP* serta dapat mendeteksi serangan *Backdoor*.

Asep Fauzi Mutaqin (2016), *Rancang Bangun Sistem Monitoring Keamanan Jaringan Prodi Teknik Informatika Melalui SMS Alert Dengan Snort.* Didalam penelitian ini dibangun sebuah sistem yang mampu memonitoring keamanan jaringan Prodi Teknik Informatika dengan menggunakan Snort dan memberikan notifikasi melalui SMS *Gateway*. Sistem Snort yang dibangun mampu mendeteksi serangan Dos *Attack* dan *Ping Attack*.

Muhammad Anif dan Mohammad Daman Huri (2015), *Penerapan Intrusion Detection System (IDS) Dengan Metode Deteksi Port Scanning Pada Jaringan Komputer Di Politeknik Negeri Semarang*. Pada penelitian tersebut dilakukan penerapan sistem deteksi intrusi dengan menggunakan metode *Port Scanning* dengan Portsentry sebagai *software* IDS.

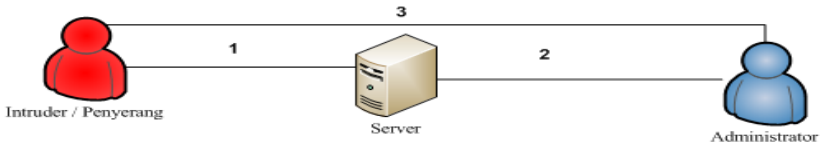
Mohammad Affandi dan Sigit Setyowibowo (2015), *Implementasi Snort Sebagai Alat Pendeteksi Intrusi Menggunakan Linux*. Penelitian ini mengimplementasikan *Intrusion Detection System (IDS)* pada sistem operasi berbasis Linux Ubuntu 10.04 untuk mendeteksi serangan berupa *ping, nmap port scan, SQL injection* dan pengaksesan *database*.

Berdasarkan tinjauan pustaka yang telah dijabarkan diatas, terdapat perbedaan antara beberapa penelitian tersebut dengan penelitian yang akan dilakukan. Penelitian yang akan dilakukan yaitu dengan membangun sebuah aplikasi yang akan mendeteksi serangan DDoS dan *Port Scanning.* Perbedaan selanjutnya yaitu sistem yang dibangun akan melakukan tindakan penanganan terhadap serangan-serangan tersebut dan akan memberikan *alert* atau notifikasi melalui SMS *Gateway* kepada administrator jaringan. Penelitian yang akan dilakukan dengan penelitian yang terdahulu memiliki persamaan yaitu dengan memanfaatkan Snort sebagai alat deteksi serangan.

3. HASIL DAN PEMBAHASAN

3.1 Sistem Berjalan

Pada jaringan yang ada saat ini, proses dari sistem yang terjadi selama ini adalah sebagai berikut :



Gambar 1 : Sistem Berjalan

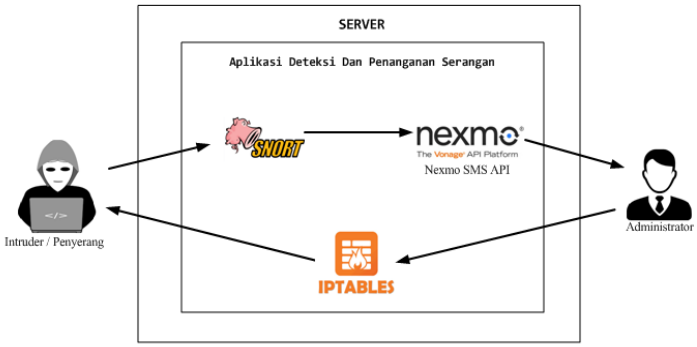
Berikut ini penjelasan dari sistem berjalan tersebut :

1. *Intruder* atau penyerang melakukan usaha penyerangan langsung terhadap *server* yang berada pada jaringan.
2. Dengan adanya serangan yang masuk ke dalam *server*, maka *server* akan menerima serangan yang terjadi tanpa dapat menginformasikan kepada administrator jaringan.
3. Adminstrator jaringan mendapati adanya serangan setelah melihat langsung ke dalam *server* yang menjadi sasaran serangan Intruder.

Situasi sistem yang ada seperti di atas masih terdapat kekurangan dan dianggap kurang efektif, karena serangan yang masuk ke dalam *server* tidak secara langsung dapat diketahui oleh administrator jaringan. Serangan dapat diketahui oleh administrator apabila berhadapan langsung pada *server*.

3.2 Perancangan Sistem

Berdasarkan penjelasan sistem yang berlangsung saat ini, maka sistem usulan yang dirancang sebagai berikut :



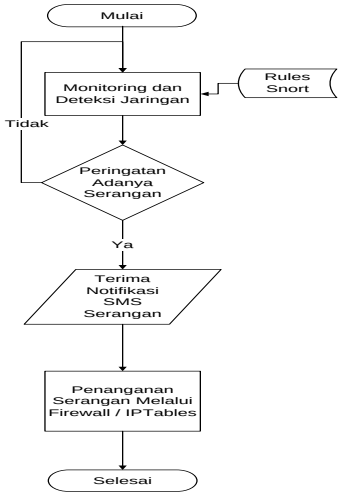
Gambar 2 : Sistem Usulan

Berikut ini penjelasan dari sistem yang diusulkan :

1. *Intruder* melakukan upaya serangan terhadap *server* yang berada pada jaringan.
2. Aktivitas yang tak lazim yang mengarah ke *server* terdeteksi aplikasi pendeteksi yang oleh Snort dianggap sebagai sebuah serangan berdasarkan *rules* yang telah dibuat pada Snort.
3. Aplikasi mengirimkan dua notifikasi berdasarkan *alert* yang dikeluarkan oleh Snort kepada administrator berupa *pop up alert* pada program dan melalui sebuah SMS dengan memanfaatkan Nexmo SMS API.
4. Administrator menerima notifikasi berupa adanya penyerangan melakukan analisa terhadap serangan yang terdeteksi tersebut untuk melakukan tindakan pengangan lebih lanjut.
5. Aplikasi melakukan eksekusi perintah berupa tindakan pencegahan melalui *Firewall* dengan memanfaatkan IPTables berdasarkan analisa yang dilakukan oleh administrator.

a. *Flowchart*

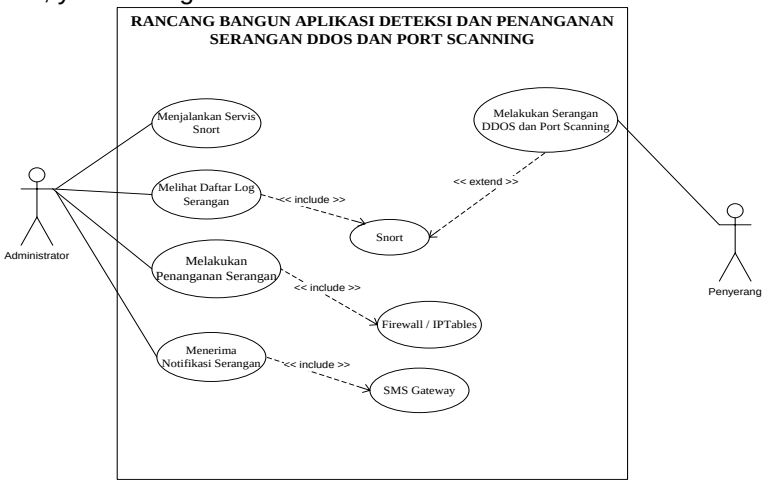
Berikut ini *flowchart* s*ystem* yang digunakan dalam penelitian :



Gambar 3 : *Flowchart System*

b. *Use Case Diagram*

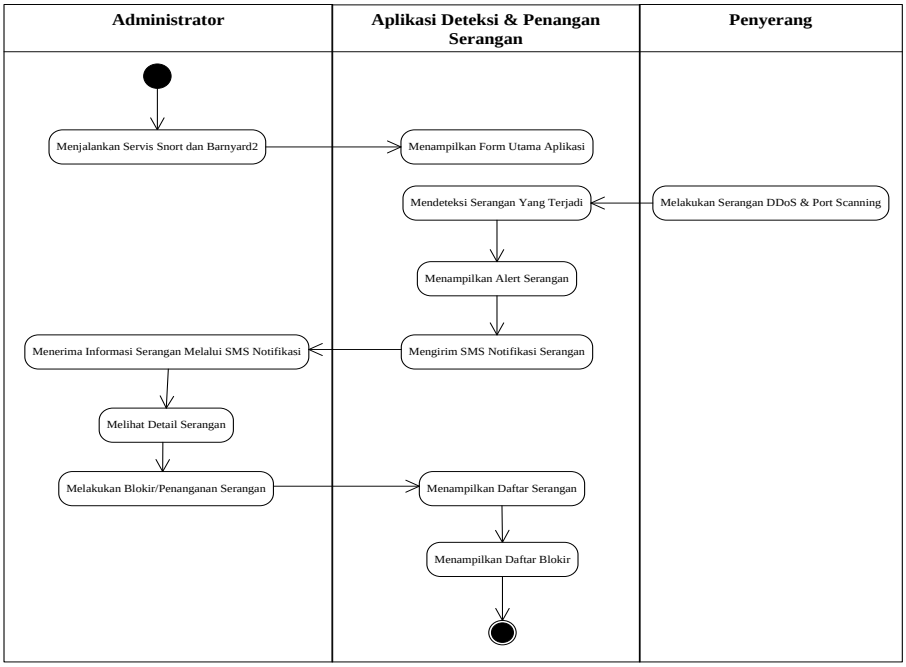
Pada perancangan *Aplikasi Deteksi dan Penanganan Serangan DDoS dan Port Scanning* mempunyai 2 aktor, yaitu sebagai berikut :



Gambar 4 : *Use Case Diagram*

c. ***Activity Diagram***

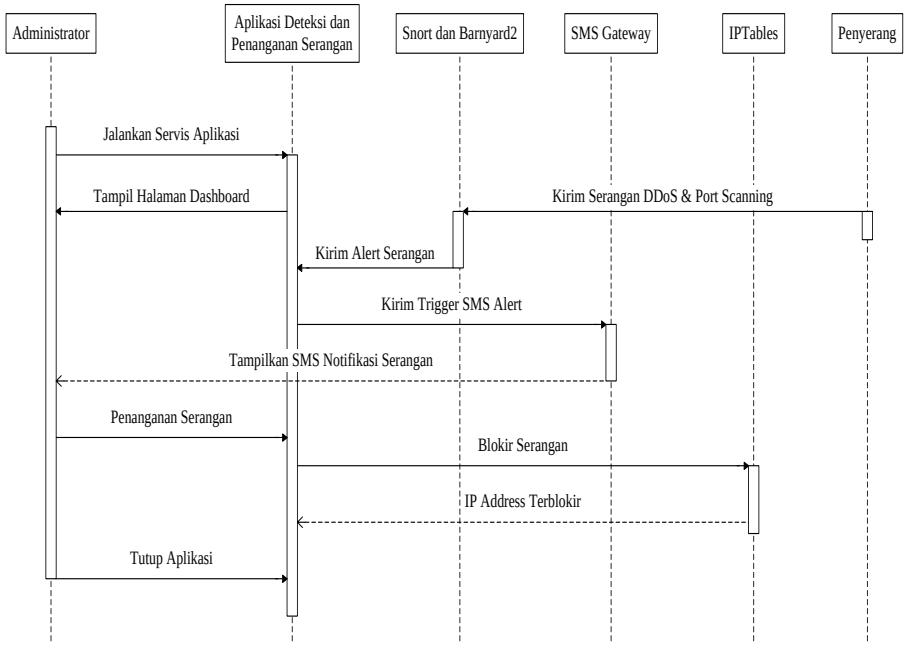
Berikut ini rancangan diagram aktivitas yang akan digunakan :



Gambar 5 : ***Acitivity Diagram***

d. ***Sequence Diagram***

Berikut ini rancangan diagram sekuen yang digunakan :

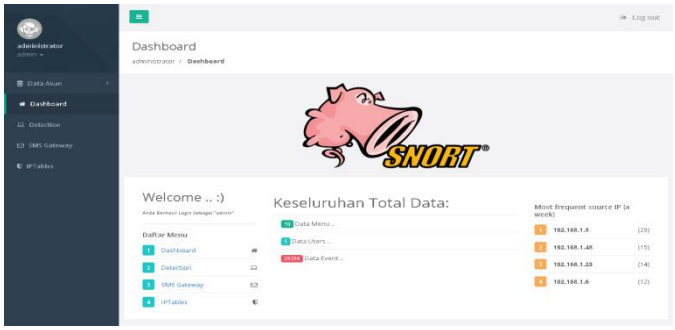


Gambar 6 : ***Sequence Diagram***

3.3 Hasil

a. Halaman Utama Sistem

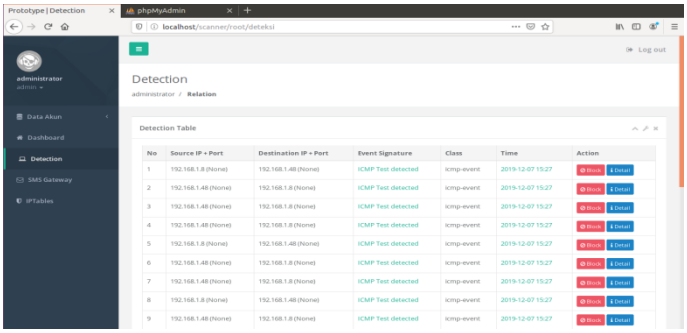
Pada halaman ini terdapat beberapa menu dan daftar alamat IP yang tercatat sering melakukan serangan.



Gambar 7 : Halaman Utama Sistem

b. *Form Detection*

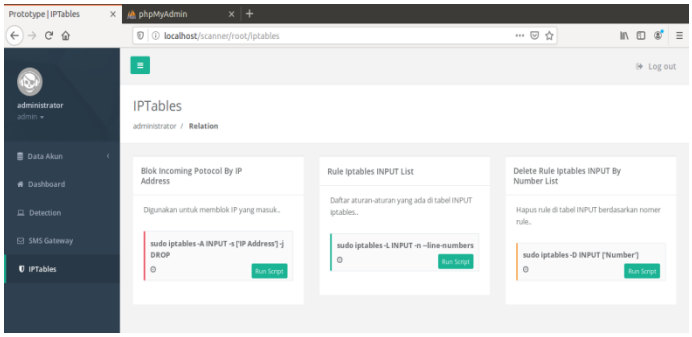
Form detection berfungsi untuk menampilkan riwayat serangan dan detail rincian data serangan yang mengarah ke *server*. Data serangan yang ditampilkan antara lain *source* IP *address*, *destination* IP *address* beserta *port* yang digunakan untuk melakukan penyerangan maupun *port* tujuan serangan dan waktu terjadinya serangan.



Gambar 8 : *Form* Deteksi

c. *Form* IPTables

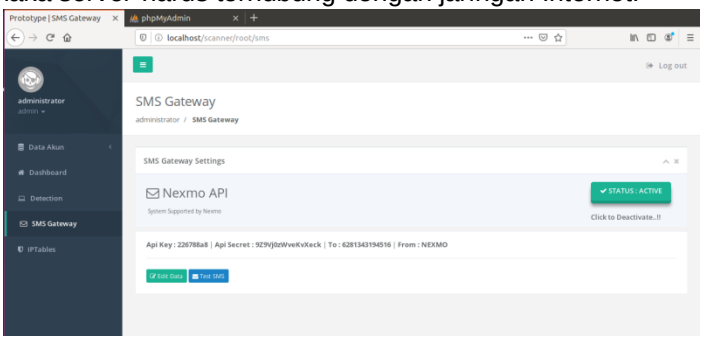
Penanganan terhadap serangan berada pada *form* IPTables. Dalam *form* ini terdapat menu yang berfungsi untuk melakukan blok alamat IP secara manual, menampilkan daftar IP yang telah terblok dan menghapus daftar blokir yang telah tercatat oleh IPTables linux. Dalam prosesnya perintah yang dieksekusi pada *form* ini memanfaatkan tools IPTables pada Linux.



Gambar 9 : *Form* IPTables

d. *Form* SMS *Gateway*

Pada *form* SMS *Gateway* memiliki beberapa fungsi yaitu merubah nomor tujuan SMS dikirimkan. Sistem SMS API yang digunakan pada program membutuhkan API *key* dan API *secret* yang diperoleh dari penyedia layanan tersebut. Sehingga agar notifikasi SMS dapat terkirim maka *server* harus terhubung dengan jaringan Internet.



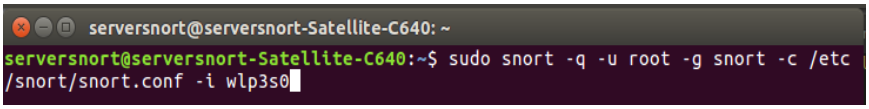
Gambar 10 : *Form* SMS *Gateway*

3.4 Pembahasan

a. Persiapan Server

1. Menjalankan Servis Snort

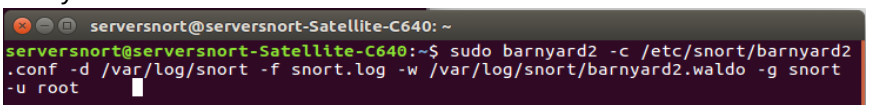
Untuk dapat mendeteksi serangan yang masuk perlu mengaktifkan servis dari Snort.



Gambar 11 : *Syntax Service Snort*

2. Menjalanakan Servis Barnyard2

Untuk dapat merekam dan menyimpan *alert* serangan yang terjadi pada *server* ke dalam *database* sehingga dapat ditampilkan oleh sistem maka perlu dijalanakan servis Barnyard2.

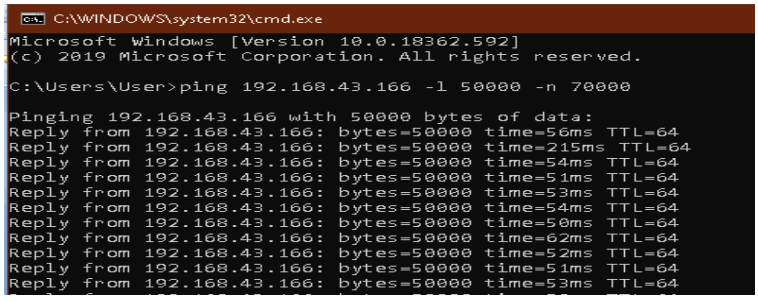


Gambar 12 : *Syntax Service B*arnyard2

b. Pengujian Server

1. Serangan DDoS

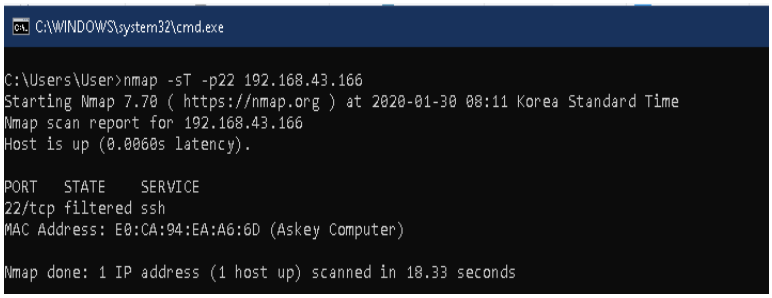
Serangan dilakukan melalui *command prompt* pada komputer penyerang. Pengujian serangan dilakukan dengan mengirimkan *buffer* sebesar 50000 *bytes* dengan paket yang dikirim sebanyak 7000 *request*.



Gambar 11 : Pengujian Serangan DDoS

2. Serangan *Port Scanning*

Serangan ini dilakukan menggunakan aplikasi Nmap. Proses pengujian *port scanning* dilakukan melalui *command prompt*.



Gambar 12 : Pengujian Serangan *Port Scanning*

3. Notifikasi Serangan

Notifikasi serangan yang diberikan kepada administrator berupa SMS serangan. SMS tersebut berisi informasi IP yang digunakan penyerang untuk melakukan serangan.

Gambar 13 : Notifikasi SMS

4. Penanganan Serangan

Penanganan terhadap serangan yang telah terdeteksi dilakukan dengan menggunakan *Firewall* dengan memanfaaatkan IPTables Linux. Tindakan yang dilakukan berupa blokir alamat IP yang tercatat melakukan serangan berdasarkan informasi yang diperoleh dari *form detection* dan SMS notifikasi.

Gambar 14 : Blokir IP Penyerang

4. Penutup

4.1 Kesimpulan

1. Sistem yang dibangun dapat mendeteksi adanya intrusi berupa serangan DDoS yang diakukan oleh *Intruder* menggunakan PING melalui *command prompt* dan serangan *Port Scanning* yang dilakukan menggunakan *tools* Nmap.
2. Pemanfaatan Snort sebagai pendeteksi intrusi dan Barnyard2 sebagai perekam *log* Snort ke dalam *database* sangat membantu administrator dalam melakukan analisa dan membaca jenis serangan yang terjadi.
3. Penggunaan SMS *Gateway* pada sistem mempermudah administrator dalam mendapatkan peringatan dini terhadap keamanan *server.*
4. Penanganan serangan dengan memanfaatkan IPTables juga sangat penting sebagai tindakan preventif dalam pengamanan *server*.

4.2 Saran

1. Menambahkan fitur untuk dapat menambah dan menghapus *rules* Snort sehingga tidak perlu mengakses file konfigurasi Snort secara manual.
2. Penanganan serangan yang dilakukan agar dapat dilakukan secara jarak jauh atau *remote*, sehingga administrator tidak perlu datang langsung melihat *server*.

5. REFERENSI

[1] Aditya, A. N., 2013, *30 Menit Mahir Membuat Jaringan Komputer*, Dunia Komputer, Jakarta

[2] Affandi, M., Setyowibowo, S., 2015, Implementasi Snort Sebagai Alat Pendeteksi Intrusi Menggunakan Linux, *Jurnal Teknologi Informasi*, Oktober 2013. http://ejurnal.stimata.ac.id/index.php/TI/article/view/109/149, diakses pada tanggal 12 Mei 2019

[3] Anif, M., Huri, M. D., 2015, Penerapan Intrusion Detection System (IDS) Dengan Metode Deteksi Port Scanning Pada Jaringan Komputer Di Politeknik Negeri Semarang, *Jurnal TELE*, Maret 2015 https://jurnal.polines.ac.id/index.php/tele/article/view/158/150, diakses pada tanggal 12 Mei 2019

[4] Enterprise, J., 2014, *MySQL Untuk Pemula*, PT. Elex Media Komputindo, Jakarta

[5] Kadir, A., 2017, *Dasar Logika Pemograman Komputer*, PT. Elex Media Komputindo, Jakarta

[6] Kawiyan, N. K., 2017, Rancang Bangun Aplikasi *Server* Monitoring Untuk Deteksi Dini Serangan DDOS Dan Backodoor Pada *Server* Berbasis Windows, *Skripsi Teknik Informatika, Universitas Sains dan Teknologi* Jayapura.

[7] Maulana, S., 2015, *5 Proyek Populer SMS Gateway*, PT. Elex Media Komputindo, Jakarta.

[8] Mutaqin, A. F., 2016, Rancang Bangun Sistem Monitoring Keamanan Jaringan Prodi Teknik Informatika Melalui SMS Alert Dengan Snort, *Jurnal Sistem dan Teknologi Informasi* http://jurnal.untan.ac.id/index.php/justin/article/download/12537/11376, diakses pada tanggal 11 Mei 2019

[9] Panggabean, P., 2018, Analisis Network Security SNORT Menggunakan Metode Intrusion Detection System (IDS) Untuk Optimasi Keamanan Jaringan Komputer, *Jurnal Sistem Informasi dan Manajemen*. Mei 2018 https://ejournal.stmikgici.ac.id/index.php/jursima/article/download/107/55, diakses pada tanggal 12 Mei 2019.

[10] Purbo, O. W., 2018, *Internet-TCP/IP: Konsep & Implementasi*, Penerbit Andi, Yogyakarta

[11] Rafiudin, R., 2010, *Mengganyang Hacker Dengan Snort*, Penerbit Andi, Yogyakarta

[12] Rosa, A. S., Salahuddin, M., 2018, *Rekayasa Perangkat Lunak Terstruktur dan Berorientasi Objek*, Edisi 2, Informatika, Bandung

[13] Sugeng, W., 2010, *Jaringan Komputer dengan TCP/IP*, Penerbit Modula, Jakarta

[14] Zam, E., 2011, *Buku Sakti Hacker*, Mediakita, Jakarta

[15] https://www.nexmo.com diakses pada tanggal 22 Mei 2019