PERANCANGAN SISTEM PENDETKSI SERANGAN PADA SERVER JARINGAN KOMPUTER MENGGUNAKAN SNORT BERBASIS SMS GETEWAY

Tria Aprilianto[1], Sunu Jatmika[2], Ihsan Wicaksono[3]
Sistem Komputer, STIMIK ASIA Malang
Jln. Soekarno Hatta, Rembuksari 1A, Malang, Jawa Timur
(0341)478877, (0341)4345225
raptorapril@gmail.com, Sunu.srg@gmial.com, ihsan141295@gmail.com

ABSTRACT
Server on a network becomes an important point because its function is to serve all requests required by all clients on a network. For that, maintaining the security of a server is also very important because if the server is experiencing a problem then there is no one the network can serve the request from the client. This makes a server administrator must see traffic to the server at any time. For this reason, it is important to conduct an attack detection system research in order to help the performance of administrators. Detection of attacks directed to the server is an early solution in securing a server from attack. For attack detection systems, SNORT is generally able to detect almost any attack because it has many rules that can be modified. Detection system by configuring and adding the rule first on the server. If there is an incoming attack then SNORT will compare the attack with the existing rule, SNORT will later categorize the attack into 3 types of High, Medium and Low. The design of attack detection system using SNORT and web server is planted on Raspberry Pi. Web server that is planted on Raspberry Pi as information system or container of attack records. In addition, Raspberry Pi also implemented database to store attack log which will be sent via sms gateway. The overall test results of the system built on this final project work well. The admin user can login the web server and do the user creation properly. Among the 6 rule attacks that have been implemented, all rules can read the attack accurately and able to save it into the database. From 75 attacks recorded in the database, only 80% attack detection can be displayed in the web server. And the web server is capable of sending 77.3% of attack notifications to the admin.

Keywords: *Attack Detection System, Computer Network, SNORT, SMS Gateway, Barnyard2, Gammu.*

1. PENDAHULUAN

Server pada sebuah jaringan menjadi poin penting karena fungsinya yaitu melayani semua permintaan yang dibutuhkan seluruh client pada sebuah jaringan. Untuk itu, menjaga keamanan sebuah server juga sangat penting karena jika server mengalami sebuah masalah maka jaringan tersebut maka tidak ada yang melayani permintaan dari client. Pendeteksian serangan yang ditujukan kepada server adalah solusi dini dalam mengamankan sebuah server dari serangan.

Banyaknya serangan yang ditujukan kepada penyedia layanan jaringan membuat seorang administrator jaringan harus dapat mengamankan jaringan tersebut. Serangan – serangan tersebut diantara lain Denial Of Service, Port Scanning dengan menscaning port – port yang aktif atau di jaringan agar bisa menjadi celah masuknya penyusup masuk ke sebuah jaringan, Sniffer menggunakan alat bantuan, IP Spoofing atau penyamaran agar tidak terdeteksi, ICMP Flooding dengan membanjiri perintah Command PING pada sebuah jaringan dan masih banyak lagi. Selain itu pengamanan jaringan cukup penting untuk diajarkan pada mahasiswa jaman sekarang. Untuk itu, maka dibuatlah penelitian ini agar kedepannya dapat menjadi sebuah bahan untuk pengajaran keamanan jaringan di STMIK ASIA Malang.

Ada banyak cara untuk mengamankan sebuah jaringan. Salah satunya dengan menerapkan sistem deteksi penyusupan jaringan atau intrusion detection system (IDS). Ini adalah cara umum yang digunakan oleh para administrator jaringan dalam mengamankan jaringan mereka. Umumnya menggunakan Snort sebagai aplikasi penunjang IDS tersebut untuk mengetahui adanya penyusup yang masuk ke sebuah jaringan.

Di zaman saat ini mobilitas adalah hal yang sangat penting. Pekerjaan tidak harus terpaku pada meja kerja dan ruang kantor. Para admin dan pelaku jaringan lainnya tidak terkecuali, oleh karena itu sistem pendeteksi serangan menggunakan SNORT berbasis SMS gateway merupakan salah satu jalan keluar utama bagi para admin jaringan.

SNORT berbasis SMS gateway memberikan kemudahan kepada para administrator jaringan karena mereka dapat memonitoring jaringan mereka secara mobile, tidak perlu harus berada di depan komputer setiap saat. Dengan ini memungkinkan para admin mendapatkan notifikasi adanya serangan hanya melalui sms.

Berdasarkan permasalahan yang ada tersebut maka dibuatlah perancangan sistem keamanan pada jaringan komputer menggunakan SNORT berbasis sms gateway.

ISSN: 2085-0859
e-ISSN : 2620-4770

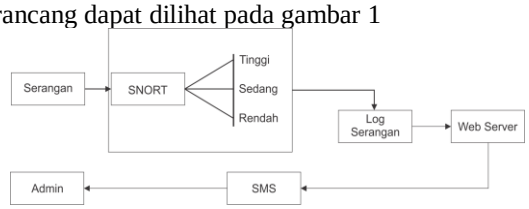
2. METODE

a. Analisa Permasalahan

Saat ini keamanan jaringan menjadi hal yang sangat penting karena merupakan pintu utama ketika terjadi serangan yang ditujukan ke jaringan tersebut. Apalagi jika serangan tersebut ditujukan langsung ke sebuah server sebuah jaringan dimana disana terdapat data – data penting pengguna dan berbagai kebutuhan pengguna jaringan. Tidak adanya pendeteksi serangan membuat sebuah server akan begitu rentan terhadap serangan yang dilakukan secara tersembunyi. Permasalahan ini membuat para administrator harus membuat sistem pendeteksi agar jaringan mereka dapat terjaga dari berbagai serangan yang ada.

b. Arsitektur Jaringan SNORT

Arsitektur keseluruhan jaringan Snort yang akan dirancang dapat dilihat pada gambar 1



Gambar 1 Arsitektur Jaringan SNORT

Secara singkat dapat dijelaskan bahwa arsitektur yang akan dirancang dimulai dari serangan yang masuk menuju server yang telah diimplementasikan SNORT, kemudian SNORT akan membagi serangan tersebut menjadi 3 klasifikasi yaitu Tinggi, Sedang dan Rendah. Setelah diolah oleh SNORT maka akan mendapatkan sebuah log serangan yang akan disimpan pada sebuah database.

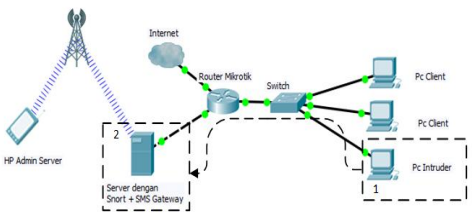
Log serangan tersebut akan diolah dulu agar dapat dipahami dan kemudian akan ditampilkan pada Web Server. Setelah tampil pada web server maka sistem akan membuat sebuah SMS yang berisikan notifikasi serangan dan akan dikirimkan kepada seorang admin.

c. Topologi Jaringan SNORT

Dalam topologi jaringan SNORT yang akan dibahas meliputi Topologi Jaringan secara keseluruhan, Desain Pembagian IP, dan Blok Diagram Sistem.

1) Perancangan Sistem

Dalam perancangan sistem, disini akan dijabarkan perancangan secara keseluruhan sistem yang akan dibangun.



Gambar 2 Desain Topologi Sistem

Pada Gambar 2 bagian 2, didalam server sudah ditanamkan Snort yang berfungsi untuk mendeteksi serangan dibantu dengan ACIDBASE agar log – log yang keluar dari Snort mudah dibaca. Selain itu juga ditambahkan SMS Gateway dengan menginstall Gammu sebagai servicenya. Untuk pengiriman SMS, Server akan dibantu oleh sebuah Modem GSM.

2) Desain Pembagian IP Address

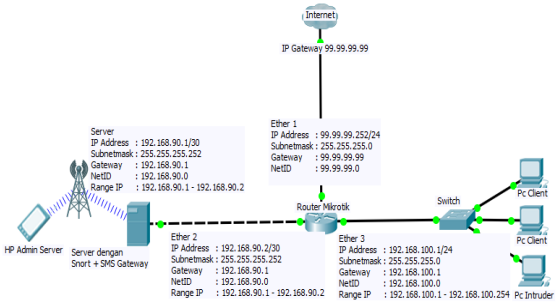
Untuk memudahkan dalam pengaturan IP Address yang digunakan dalam jaringan, maka pembagian IP Address akan menggunakan kelas C yang dinilai efektif jika diterapkan dalam pembangunan jaringan nantinya.

Pembagian IP Address pada perancangan jaringan secara keseluruhan dilakukan di mikrotik. Perancangan pembagian IP Address untuk mikrotik ditunjukkan pada Tabel 1

Tabel 1 Pembagian IP Address Mikrotik

No.	Keterangan	IP *Address*	Subnetmask	Gateway
1.	Ether1 *Router*	99.99.99.252	255.255.255.0	99.99.99.99
2.	Ether2 *Router*	192.168.90.2	255.255.255.252	192.168.90.1
3.	Ether3 *Router*	192.168.100.1	255.255.255.0	192.168.100.1
4.	*Server*	192.168.90.1	255.255.255.252	192.168.90.1
5.	Client	192.168.100.2-192.168.100.254	255.255.255.0	192.168.100.1

Untuk pembagian IP Address secara detail dapat dilihat pada gambar 3.

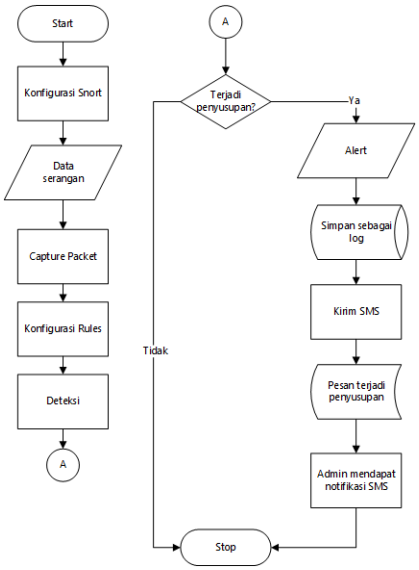


Gambar 3 Desain Pembagian IP

Pada gambar diatas dapat dijelaskan bahwa IP dari server adalah 192.168.90.1/30. Menggunakan prefix 30 agar dapat menghemat ruang IP address yang mempunyai kapasitas sebesar 2 client saja karena hanya digunakan untuk server dan mikrotik saja. IP gateway untuk menuju internet adalah 99.99.99.99. Untuk IP pada jaringan LAN menggunakan IP 192.168.100.1/24. Pada jaringan LAN menggunakan prefix 24 agar mudah dalam penambahan user karena kapasitasnya yang cukup besar yaitu 254 client.

d. Alur Sistem Keamanan Pada Jaringan SNORT

ISSN: 2085-0859
e-ISSN : 2620-4770



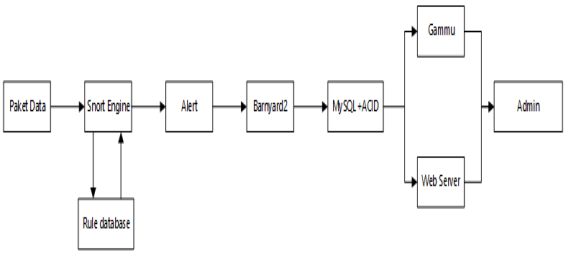
Gambar 4 Alur Sistem Keamanan

Dari Gambar 4 bagian 1 dapat dijelaskan bahwa hal yang pertama kali dilakukan adalah mengkonfigurasi Snort di server yang telah disiapkan. Dimulai dari instalasi SNORT lalu mengkonfigurasinya. Setelah itu mengkonfigurasi rule – rule untuk memfilter paket data yang dikategorikan menyusup atau tidak. Kemudian data serangan yang masuk akan di capture oleh SNORT yang kemudian dicocokkan dengan konfigurasi rule yang telah ditanam di konfigurasi Snort. Disana terjadilah proses pendeteksian apakah paket tersebut termasuk dalam bentuk serangan atau tidak.

Pada Gambar 4 bagian 2, Jika paket tersebut tergolong dalam bentuk serangan maka data tersebut akan diolah menjadi sebuah log alert. Alert tersebut akan dimasukkan oleh Barnyard2 kedalam sebuah database yang nantinya akan diakses oleh ACIDBASE. Alert tersebut masih berbentuk bahasa mesin yang belum bisa diterjemahkan jika orang awan membaca alert tersebut. Untuk itu dibutuhkan ACIDBASE yang berfungsi untuk menerjemahkan alert tersebut agar mudah dibaca. Melalui Gammu, alert tersebut dapat dikirim kepada administrator jaringan berupa informasi/notifikasi telah terjadi serangan didalam jaringannya. Jika data tersebut bukan merupakan bentuk serangan maka akan diteruskan ke dalam jaringan.

e. Komponen – Komponen Sistem Keamanan

Dalam komponen – komponen sistem keamanan akan dijelaskan bahwa sistem Snort akan membutuhkan modul – modul yang membantu dalam pendeteksian segala bentuk serangan.



Gambar 5 Komponen Modul SNORT

f. Perancangan Web Server

Perancangan web server membutuhkan database untuk menampung data – data yang akan ditampilkan nantinya pada web server. Pada database yang akan dirancang adalah tabel user dimana tabel ini akan digunakan untuk web login administrator.

Tabel 2Perancangan Tabel User Database Web Server

Nama	Username	Email	Password
adi	Adi123	Adi123@gmail.com	234qwe
sari	idasw	idasariw@ymail.com	asdida
ihsan	Ihsan1412	Ihsan1412@hotmail.com	Poilkj123

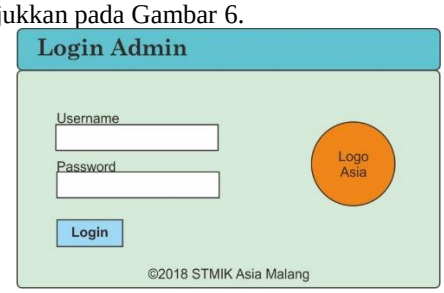
Pada Tabel 2 tabel terdiri dari field nama, username dan password. Field nama digunakan untuk mengetahui nama pemilik dari username. Pembuatan username dan password adalah untuk mengamankan web server agar tidak sembarang orang bisa melihat data – data yang ada.

g. Halaman Web

Halaman web dirancang untuk memudahkan user dalam melakukan login username dan password. Selain itu juga memudahkan admin agar bisa melihat serangan apa saja yang telah terjadi pada jaringannya. Halaman web yang dirancang yaitu web login, halaman catatan serangan dan halaman catatan sms.

1) Halaman Web Login

Halaman web login merupakan halaman pertama yang diakses jika seorang admin hendak melihat aktifitas serangan yang ditujukan kepada jaringannya. Tampilan web login yang dirancang ditunjukkan pada Gambar 6.



Gambar 6 Rancangan Web Login

Pada Gambar 6 terdapat kolom username dan kolom password yang berfungsi untuk memasukkan data username dan password yang

ISSN: 2085-0859
e-ISSN : 2620-4770

dimiliki admin. Tombol login digunakan untuk validasi username dan password. Jika data yang dimasukkan benar maka admin akan langsung masuk dalam halaman catatan serangan.

2) Halaman Register Web Login

Halaman Register web login merupakan halaman yang diakses seorang admin ingin membuat sebuah user web login. Tampilan Register web login yang dirancang ditunjukkan pada Gambar 7.

Gambar 7 Rancangan Register Web Login

Pada Gambar 7 terdapat 4 kolom yang terdiri dari username, email, password dan kolom confirm password yang berfungsi untuk memasukkan data username, email dan password seorang user yang akan admin buat. Tombol register digunakan untuk memvalidasi username, email dan password. Jika data yang dimasukkan benar maka user akan masuk ke dalam database, dan jika terdapat duplikasi maka server akan meminta untuk memperbaiki duplikasi tersebut.

3) Halaman Catatan Serangan

Setelah admin login, halaman yang akan muncul adalah halaman catatan log serangan. Halaman ini berisikan informasi mengenai catatan serangan seperti: IP asal serangan, IP tujuan serangan, jenis serangan dan waktu serangan terjadi. Tampilan halaman catatan serangan yang dirancang ditunjukkan pada Gambar 8.

Gambar 8 Halaman Catatan Serangan

Pada Gambar 8 terdapat beberapa kolom yang berisikan informasi catatan serangan yang terjadi pada jaringan. Pada kolom IP_Source berisikan IP asal serangan. Kolom IP_Destination berisikan IP tujuan serangan dilakukan. Kolom Attack_Type berisikan jenis serangan yang dilakukan oleh penyusup ke target sasaran. Kolom Priority berisikan kode prioritas serangan tersebut dimulai dari angka 1 yang berarti Tinggi, angka 2 yang berarti Sedang dan 3 yang berarti Rendah. Lalu yang terakhir kolom Timestamp berisi waktu kapan penyusup melakukan.

4) Halaman Catatan SMS

Halaman yang akan dibuat selanjutnya adalah halaman catatan SMS. Yang berisikan teks apa saja yang dikirim server kepada administrator jaringan, waktu terkirimnya sms dan status pengiriman sms. Tampilan halaman catatan sms ditunjukkan pada Gambar 9.

Gambar 9 Halaman Catatan SMS

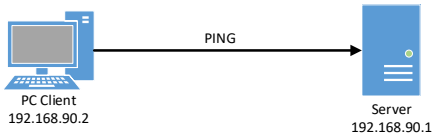
Pada Gambar 9 terdapat beberapa kolom yang berisikan informasi catatan sms yang dikirimkan server ke administrator jaringan. Pada kolom Text_Messages berisikan teks apa saja yang telah dikirimkan server ke administrator jaringan. Pada kolom Messages_Sent berisikan waktu sms terkirim dan yang terakhir kolom Status berisikan status sms apakah terkirim atau tidak.

3. PEMBAHASAN

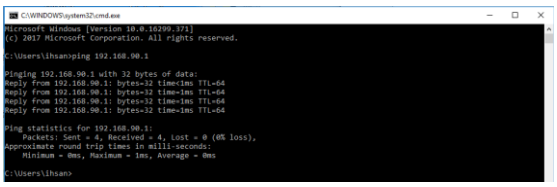
Pada sub bab pengujian ini akan dibahas tentang pengujian sistem yang telah dibangun, diantaranya pengujian sistem snort, sms gateway, halaman login user, halaman pembuatan user, halaman catatan serangan, halaman catatan sms, halaman ACIDBASE, dan Pengujian serangan dari client ke server

a. Pengujian Sistem Snort

Pengujian sistem snort bertujuan untuk mengetahui apakah snort telah benar – benar terimplementasi pada raspberry pi atau tidak. Untuk itu kita dapat membuat ping test dari client menuju server. Sebagai gambaran, simulasi serangan dapat dilihat pada Gambar 10.



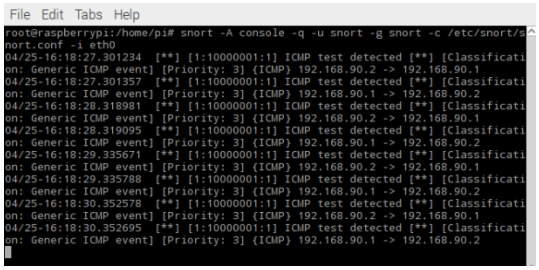
Gambar 10 Simulasi Test Serangan



Gambar 11 Test ping menuju server

Dengan menggunakan perintah ping 192.168.90.1 dari komputer client, kita akan mengetahui apakah rule dapat berjalan dengan baik atau tidak. Untuk itu pada sisi server dilakukan sebuah perintah sudo /usr/local/bin/snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i eth0 maka akan terlihat seperti pada Gambar 12.

ISSN: 2085-0859
e-ISSN : 2620-4770

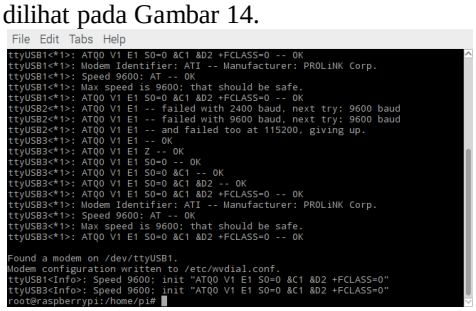


Gambar 13 Snort melakukan scanning serangan

Pada Gambar 13, perintah ping dari client dengan IP Address 192.168.90.2 telah terbaca dengan baik. Maka pengujian Snort dengan satu rule dapat dinyatakan berhasil.

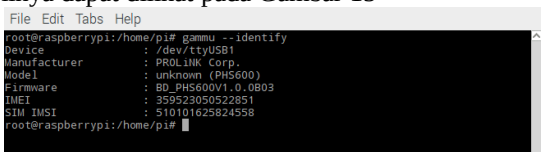
b. Pengujian SMS Gammu

Pengujian SMS gateway disini merupakan pengujian instalasi modem dan gammu berhasil dijalankan dengan baik atau tidak. Hal yang pertama dilakukan adalah memastikan bahwa modem sudah terbaca dengan baik oleh sistem atau tidak dengan melakukan perintah sudo wvdialconf untuk hasilnya dapat dilihat pada Gambar 14.



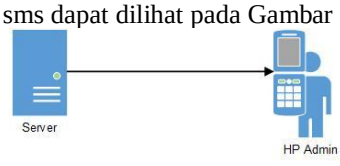
Gambar 14 Scanning Modem oleh Raspberry

Dapat dilihat pada Gambar 14, modem berhasil dibaca oleh raspberry pi pada port /dev/ttyUSB1. Selanjutnya yaitu memeriksa bahwa gammu sudah benar – benar terinstall dengan baik atau belum dengan perintah gammu –-identify hasilnya dapat dilihat pada Gambar 15

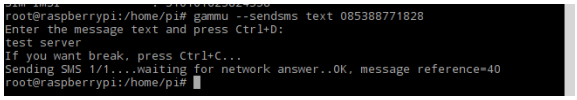


Gambar 15 Memeriksa Instalasi Gammu

Jika terlihat seperti gambar diatas maka dipastikan instalasi gammu pada raspberry pi telah berhasil, selanjutnya yaitu mencoba untuk mengirimkan sebuah sms dari Raspberry menuju Handphone. Sebagai Gambaran, simulasi pengiriman sms dapat dilihat pada Gambar 16.

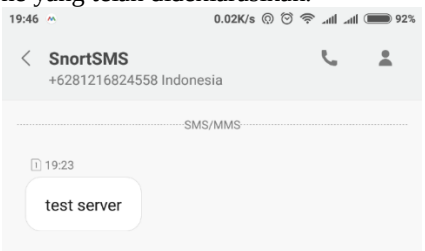


Gambar 16 Simulasi Test SMS menuju Handphone



Gambar 17 Test SMS menuju Handphone

Dengan melakukan perintah gammu --sendsms text (nomor HP tujuan), maka gammu akan segera mengirimkan sebuah sms menuju nomor handphone yang telah dideklarasikan.

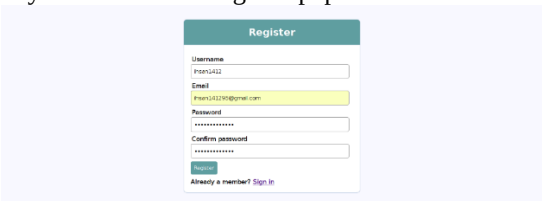


Gambar 18 SMS berhasil diterima oleh Handphone tujuan

Pada Gambar 18 dapat dilihat bahwa sms dari gammu telah berhasil diterima oleh nomor tujuan. Maka pengujian sms gammu dapat dinyatakan berhasil.

c. Pengujian Pembuatan User

Pada pengujian pembuatan user akan diuji apakah web pembuatan user login dapat berjalan baik atau tidak. Untuk membuka web pembuatan user maka pada browser diketikan alamat yaitu snortsystem.com/snort/register.php



Gambar 19 Tampilan Halaman Register Login Web Server

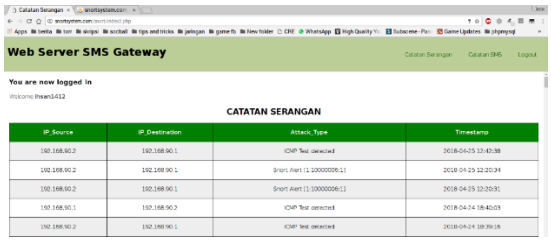
Pada gambar 19, jika admin akan memasuki web server maka diwajibkan untuk mendaftarkan diri agar dapat masuk pada halaman catatan serangan dan halaman catatan sms. Pada halaman register, seorang admin diharuskan untuk menginputkan Username, Alamat Email dan Password, setelah itu tekan tombol register jika ingin mendaftarkan diri.

Tabel 3 Data Create User Admin

Username	Email	Password
Ihsan1412	Ihsan141295@gmail.com	Blackbriar1412

Dari data Tabel 3, data yang diinputkan disimpan dengan mengklik tombol register dan browser secara otomatis akan menampilkan halaman catatan serangan seperti pada Gambar 20

ISSN: 2085-0859
e-ISSN : 2620-4770



Gambar 20 Tampilan Register berhasil

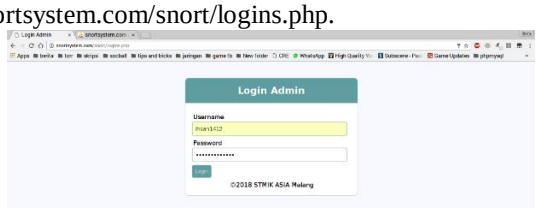
Untuk mengetahui apakah data yang telah diinputkan berhasil masuk database maka dapat dicek snortsystem.com/phpmyadmin kemudian menuju database loginsystem lalu pada tabel users akan terlihat seperti pada Gambar 21.

Gambar 21 Tampilan Database login System

Dapat dilihat pada Gambar 21, user dengan username ihsan1412 berhasil ditambahkan di tabel users pada database loginsystem. Jika telah direcord pada database maka pengujian halaman register user dapat dinyatakan berhasil.

d. Pengujian Login User

Pada pengujian login user akan diuji apakah halaman login user dapat berjalan dengan atau tidak. Untuk membuka halaman login user, pada browser diketikan sebuah alamat yaitu snortsystem.com/snort/logins.php.



Gambar 22 Tampilan Halaman Login Web Server

Jika user admin menginputkan data yang salah, maka akan kembali pada halaman login diikuti dengan peringatan bahwa Username/Password salah. Di halaman login terdapat form yang berisi Username dan Password. Jika diinputkan sesuai dengan data yang tersimpan pada database, browser akan menampilkan halaman catatan serangan seperti pada Gambar 22.

e. Halaman Catatan Serangan

Halaman catatan serangan berisikan informasi mengenai IP address asal serangan, IP tujuan serangan, tipe serangan dan waktu kapan serangan tersebut dilaksanakan. Ditunjukkan pada Gambar 23.

Gambar 23 Tampilan Halaman Catatan Serangan

Selain itu pada halaman ini juga diimplementasikan skrip untuk mengirimkan sebuah sms notifikasi jika ada tambahan atau update mengenai informasi serangan. Oleh karena itu ditambahkan pula sebuah skrip yang bisa merefresh otomatis agar admin bisa mendapatkan sms dengan aktual. Untuk mengaksesnya bisa melalui alamat snortsystem.com/snort/index2.php

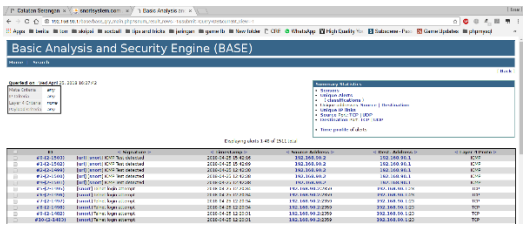
f. Halaman Catatan SMS

Halaman catatan SMS berisikan informasi mengenai pesan sms yang berhasil dikirimkan oleh sistem. Informasi tersebut antara lain pesan sms, kapan sms tersebut berhasil dikirimkan dan status terkirimnya sms. Untuk mengaksesnya melalui alamat snortsystem.com/snort/terkirim.php yang tampilannya dapat dilihat pada Gambar 24.

Gambar 24 Tampilan Halaman Catatan SMS

g. Halaman ACIDBASE

Halaman ACIDBASE merupakan halaman yang akan mempresentasikan log serangan dari Snort agar mudah dipahami. Di dalamnya terdapat berbagai fitur seperti sorting sesuai dengan keinginan, melihat statistik berapa serangan yang telah ditujukan kepada server dan masih banyak lagi. Untuk mengaksesnya melalui snortsystem.com/base/base_main.php seperti pada Gambar 25.



Gambar 25 Tampilan Halaman Catatan SMS

h. Pengujian Serangan dari Client ke Server

Pada pengujian ini adalah pengujian secara keseluruhan sistem apakah sistem dapat bekerja secara maksimal atau tidak. Pada pengujian

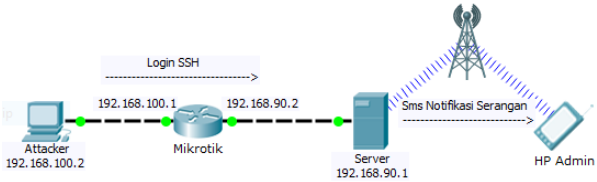
ISSN: 2085-0859
e-ISSN : 2620-4770

ini akan diuji 6 rule yang telah diimplementasikan ke dalam sistem. Rule tersebut antara lain:

1. alert tcp any any -> $HOME_NET 22 (msg:"Remote SSH Connection Attempt"); GID:1; sid:10000002; rev:001; classtype:attempted-admin;)
2. alert tcp any any -> $HOME_NET 21 (msg:"FTP Connection Attempt"); GID:1; sid:10000003; rev:001; classtype:attempted-admin;)
3. alert tcp any any -> $HOME_NET 80 (msg:"WEB-PHP snortsystem.com access"; content:"snort"; http_uri; sid:10000004; rev:001; classtype:attempted-recon;)
4. alert icmp any any -> $HOME_NET any (msg:"Ping of Death"; dsize:>1500; GID:1; sid:10000005; rev:001; classtype:attempted-dos;)
5. alert tcp any any -> $TELNET_SERVERS 23 (msg:"Telnet Login Attempt"); GID:1; sid:10000006; rev:001; classtype:suspicious-login;)
6. alert udp any any -> 192.168.90.1 any (msg:"Nmap UDP Scan"; sid:10000007; rev:001; classtype:network-scan;)

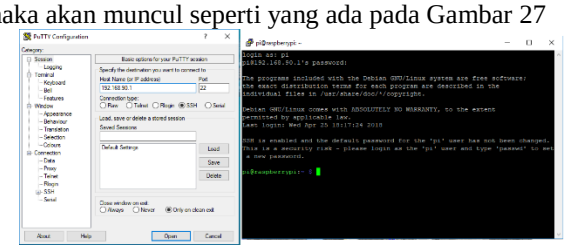
i. Pengujian Remote SSH

Pada tahap ini penulis akan melakukan pengujian dengan mencoba melakukan remote ssh menggunakan aplikasi putty yang ada di PC Client. Sebagai gambaran, pada Gambar 26 akan ditunjukkan simulasi serangan dari pc client menuju pc server.



Gambar 26 Simulasi Serangan

Dengan mengetik IP address server pada kolom Hostname/IP Address lalu memilih port ssh maka akan muncul seperti yang ada pada Gambar 27

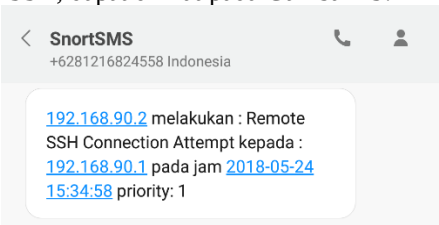


Gambar 27 Tampilan Remote SSH Putty

Setelah jendela telnet terbuka lalu mengetikkan user login pi, maka server akan langsung menanggapi hal tersebut dengan membuat log seperti pada Gambar 28.

Gambar 28 Tampilan Catatan Remote SSH

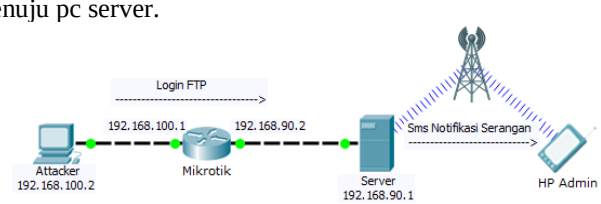
Dan sesaat setelah membuat log catatan, server akan mengirimkan notifikasi berupa sms yang berisikan bahwa ada yang memasuki server melalui Remote SSH, dapat dilihat pada Gambar 29.



Gambar 29 Tampilan SMS Notifikasi Remote SSH

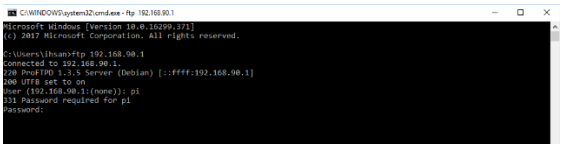
j. Pengujian FTP Connection Attempt

Pada tahap ini penulis akan melakukan pengujian dengan mencoba melakukan koneksi FTP menggunakan aplikasi Command Prompt yang ada di PC Client. Sebagai gambaran, pada Gambar 30 akan ditunjukkan simulasi serangan dari pc client menuju pc server.



Gambar 30 Simulasi Serangan

Dengan mengetik ftp lalu diikuti IP address server maka akan muncul seperti yang ada pada Gambar 31.



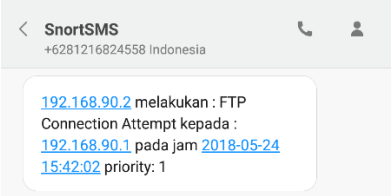
Gambar 31 Tampilan Koneksi FTP

Setelah terkoneksi ftp dengan server kemudian mengetikkan user pi, maka server akan langsung menanggapi hal tersebut dengan membuat log seperti pada Gambar 32.

Gambar 32 Tampilan Catatan Koneksi FTP

ISSN: 2085-0859
e-ISSN : 2620-4770

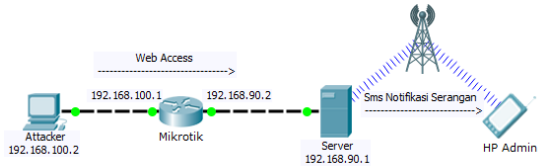
Dan sesaat setelah membuat log catatan, server akan mengirimkan notifikasi berupa sms yang berisikan bahwa ada yang memasuki server melalui koneksi FTP, dapat dilihat pada Gambar 33.



Gambar 34 Tampilan SMS Notifikasi Koneksi FTP

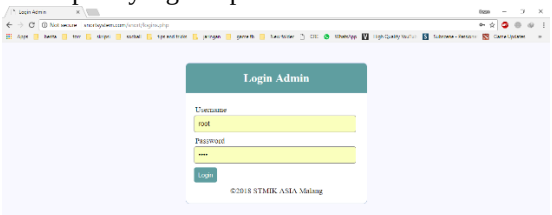
k. Pengujian Web-PHP Access

Pada tahap ini penulis akan melakukan pengujian dengan mencoba membuka web server snortsystem.com melalui browser yang di PC client. Sebagai gambaran, pada Gambar 35 akan ditunjukkan simulasi serangan dari pc client menuju pc server.



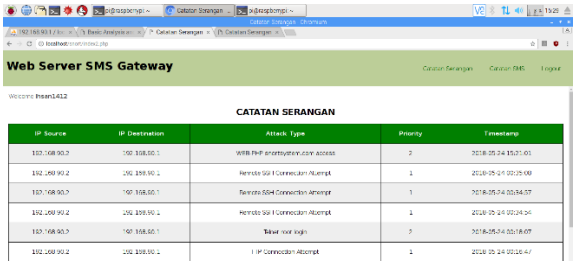
Gambar 35 Simulasi Serangan

Dengan mengetikkan alamat snortsystem.com/snort/logins.php maka akan muncul seperti yang ada pada Gambar 36.



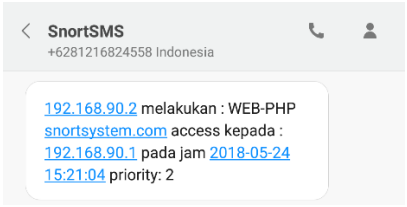
Gambar 36 Tampilan Akses Web Server

Setelah halaman tersebut terbuka pada browser client, maka server akan langsung menanggapi hal tersebut dengan membuat log seperti pada Gambar 37.



Gambar 37 Tampilan Catatan Akses Web Server

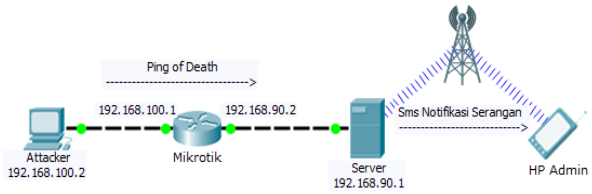
Dan sesaat setelah membuat log catatan, server akan mengirimkan notifikasi berupa sms yang berisikan bahwa ada yang berusaha membuka Web Server, dapat dilihat pada Gambar 38.



Gambar 38 Tampilan SMS Notifikasi Akses Web Server

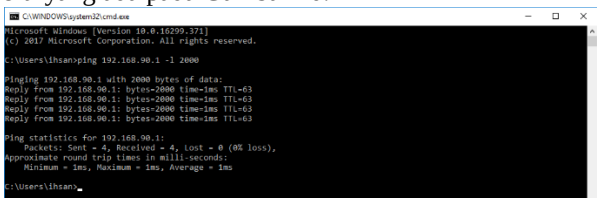
l. Pengujian Ping of Death

Pada tahap ini penulis akan melakukan pengujian dengan mencoba melakukan ping of death dengan Command Prompt yang di PC client. Sebagai gambaran, pada Gambar 39 akan ditunjukkan simulasi serangan dari pc client menuju pc server.



Gambar 39 Simulasi Serangan

Dengan mengetikkan ping diikuti IP Address Server lalu disertai opsi –l 2000, maka akan muncul seperti yang ada pada Gambar 40.

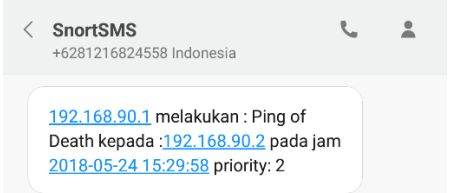


Gambar 40 Tampilan Perintah Ping of Death

Setelah perintah ping berhasil dilaksanakan, maka server akan langsung menanggapi hal tersebut dengan membuat log seperti pada Gambar 41.

Gambar 41 Tampilan Catatan Ping of Death

Dan sesaat setelah membuat log catatan, server akan mengirimkan notifikasi berupa sms yang berisikan bahwa ada yang berusaha melakukan Ping of Death, dapat dilihat pada Gambar 42

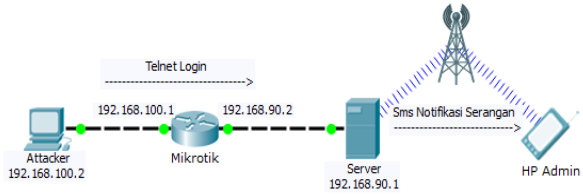


ISSN: 2085-0859
e-ISSN : 2620-4770

Gambar 42 Tampilan SMS Notifikasi Ping of Death

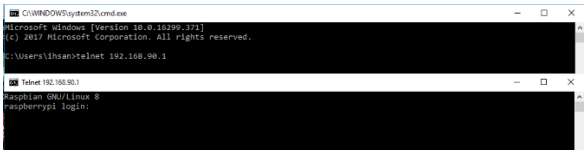
m. Pengujian Telnet Login

Pada tahap ini penulis akan melakukan pengujian dengan mencoba melakukan Koneksi Telnet dengan Command Prompt yang di PC client. Sebagai gambaran, pada Gambar 42 akan ditunjukkan simulasi serangan dari pc client menuju pc server.



Gambar 42 Simulasi Serangan

Dengan mengetikkan telnet diikuti IP Address Server, maka akan muncul seperti yang ada pada Gambar 43.

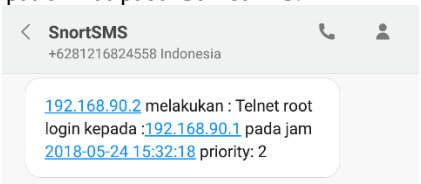


Gambar 43 Tampilan Perintah Telnet

Setelah perintah telnet berhasil dilaksanakan dan muncul jendela telnet, maka server akan langsung menanggapi hal tersebut dengan membuat log seperti pada Gambar 44

Gambar 44 Tampilan Catatan Akses Telnet

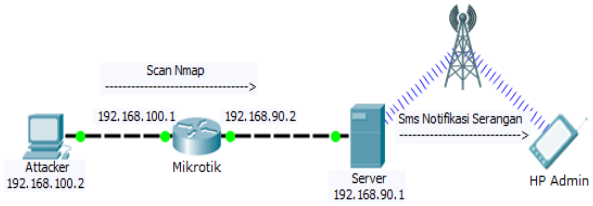
Dan sesaat setelah membuat log catatan, server akan mengirimkan notifikasi berupa sms yang berisikan bahwa ada yang berusaha melakukan login telnet, dapat dilihat pada Gambar 45.



Gambar 45 Tampilan SMS Notifikasi Akses Telnet

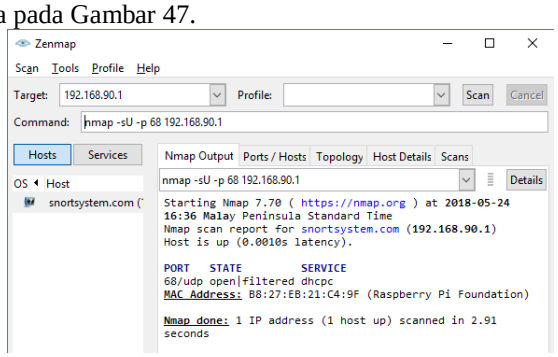
n. Pengujian Nmap UDP Scan

Pada tahap ini penulis akan melakukan pengujian dengan mencoba melakukan Scanning Port dengan program Nmap yang di PC client. Sebagai gambaran, pada Gambar 46 akan ditunjukkan simulasi serangan dari pc client menuju pc server.



Gambar 46 Simulasi Serangan

Dengan mengetikkan nmap –sU –p68 diikuti IP Address Server, maka akan muncul seperti yang ada pada Gambar 47.

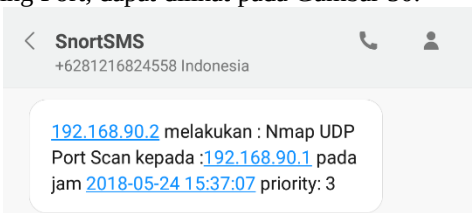


Gambar 47 Scanning Menggunakan Nmap

Setelah proses scanning port berhasil dilaksanakan dan muncul seperti pada Gambar 48, maka server akan langsung menanggapi hal tersebut dengan membuat log seperti pada Gambar 49.

Gambar 49 Tampilan Catatan Scanning Nmap

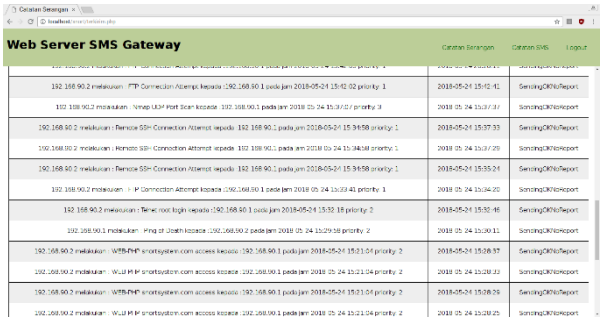
Dan sesaat setelah membuat log catatan, server akan mengirimkan notifikasi berupa sms yang berisikan bahwa ada yang berusaha melakukan Scanning Port, dapat dilihat pada Gambar 50.



Gambar 50 Tampilan SMS Notifikasi Scanning Nmap

Log sms web server dari pengujian diatas dapat dilihat pada gambar dibawah ini:

ISSN: 2085-0859
e-ISSN : 2620-4770



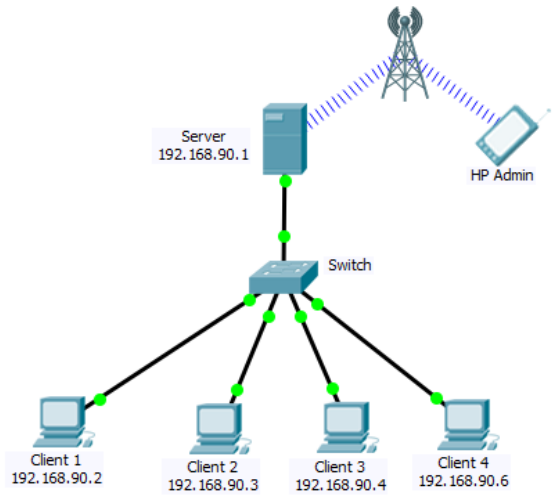
Gambar 51 Tampilan log sms pada web server.

Jika dilihat pada gambar 4.54 rata – rata sms memiliki delay pengiriman 20-30 detik. Hal ini disebabkan oleh proses pengolahan notifikasi yang harus dimasukkan dalam tampilan web server terlebih dahulu kemudian dipanggil oleh service gammu setelah itu barulah notifikasi dikirimkan. Dapat dipengaruhi juga oleh kekuatan signal dari modem itu sendiri.

Dari pengujian – pengujian dapat disimpulkan bahwa sistem mampu mendeteksi serangan dan mengirimkan notifikasi serangan kepada admin. Namun pada pembacaan IP asal serangan hanya terbaca pada IP yang satu jaringan dengan sistem atau IP pada port router yang terhubung pada server.

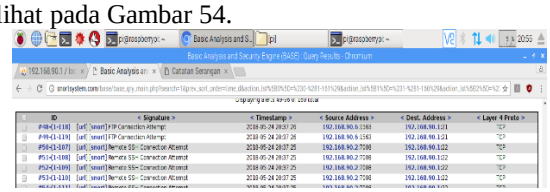
o. Pengujian Sistem Snort Secara Keseluruhan

Pengujian ini dilakukan oleh penulis agar dapat mengetahui performa dari sistem yang telah diimplementasikan. Penulis melakukan pengujian yang dibagi menjadi 2 bagian yaitu: pengujian serangan secara bersamaan dan pengujian serangan secara bertahap. Pengujian serangan dilakukan dengan menggunakan 4 buah pc, sebagai gambaran dapat dilihat pada Gambar 52.



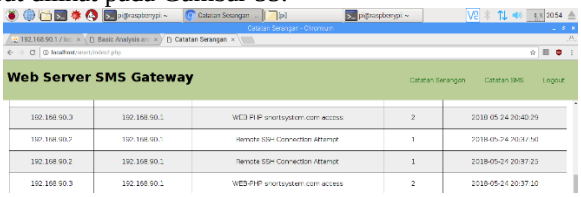
Gambar 53 Pengujian Secara Keseluruhan

Pengujian pertama yaitu pengujian secara bersamaan. Dalam pengujian ini masing-masing pc akan menyerang server secara bersamaan. Peran masing-masing pc antara lain: Client 1 melakukan Akses SSH, client 2 melakukan akses web server, client 3 melakukan login telnet dan client 4 melakukan login ftp server. Setelah melakukan pengujian serangan secara bersamaan, server kemudian mengolah data serangan yang dapat dilihat pada Gambar 54.



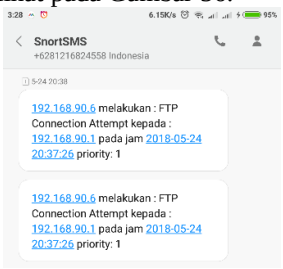
Gambar 54 Tampilan BASE

Pada Gambar 54 dapat dilihat bahwa sistem mampu mendeteksi berbagai serangan secara bersamaan dalam waktu yang berdekatan. Untuk catatan yang dapat dilaporkan dalam web server dapat dilihat pada Gambar 55.



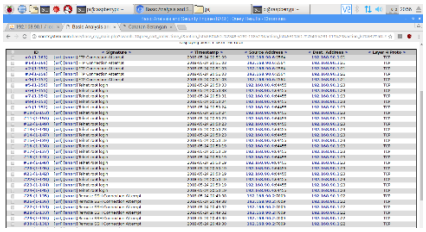
Gambar 55 Tampilan Web Server

Pada Gambar 55 dapat dilihat bahwa web server mencatat hal yang sama seperti pada BASE, namun serangan ftp login tidak tertera pada halaman catatan serangan. Untuk sms yang dikirimkan oleh server dapat dilihat pada Gambar 56.



Gambar 56 Tampilan SMS Notifikasi Serangan

Seperti yang terlihat pada Gambar 56 hanya ada satu serangan yang dapat dikirimkan oleh server sedangkan serangan yang lain tidak dapat dikirimkan. Selanjutnya pada pengujian berikutnya sistem akan diuji secara bertahap. Untuk catatan serangan yang dapat dicatat oleh sistem dapat dilihat pada Gambar 57.



Gambar 58 Tampilan BASE

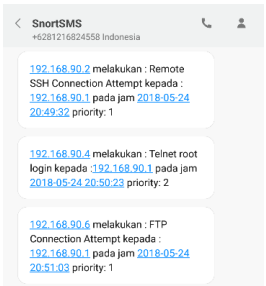
Pada Gambar 58 dapat dilihat bahwa sistem mampu mendeteksi berbagai serangan secara bertahap dalam waktu yang tidak terpaut jauh.

ISSN: 2085-0859
e-ISSN : 2620-4770

Untuk catatan yang dapat dilaporkan dalam web server dapat dilihat pada Gambar 59.

Gambar 59 Tampilan Web Server

Pada Gambar 59 dapat dilihat bahwa web server mencatat hal yang sama seperti pada BASE, semua serangan yang dilaksanakan dapat tercatat dengan baik pada pengujian secara bertahap. Untuk sms yang dikirimkan oleh server dapat dilihat pada Gambar 60.



Gambar 60 Tampilan SMS Notifikasi Serangan

Seperti yang terlihat pada gambar 4.61, server dapat mengirimkan sms notifikasi serangan dari seluruh serangan yang dilakukan secara bertahap sesuai dengan yang tercatat pada web browser.

Dari pengujian sistem secara keseluruhan dapat disimpulkan bahwa sistem ketika diserang secara bersamaan dari IP yang berbeda dalam waktu yang bersamaan, sistem hanya mampu mengirimkan satu notifikasi saja kepada admin. Sedangkan ketika diserang dalam waktu yang tidak bersamaan sistem mampu mengirimkan seluruh notifikasi serangan kepada admin.

Seluruh pengujian pada penelitian ini semuanya terekam pada database Basic Analysis and Security Engine (BASE). Berdasarkan rekaman BASE tercatat ada 227 alert dari 75 kali pengujian yang dilakukan secara sengaja terhadap sistem untuk menguji apakah sistem mampu bekerja secara optimal atau tidak. Pengujian tersebut terdiri dari rule web access sebanyak 6 pengujian, login telnet sebanyak 23 pengujian, login ssh sebanyak 15 pengujian, login ftp sebanyak 17 pengujian, ping of death sebanyak 12 pengujian, dan scan nmap sebanyak 2 pengujian.

Rincian 227 alert terdiri dari rule web access sebanyak 11 alert, login telnet sebanyak 96 alert, login ssh sebanyak 48 alert, login ftp sebanyak 44 alert, ping of death sebanyak 24 alert, dan scan nmap sebanyak 4 alert. Alert diatas diproses didalam web server menjadi hanya 75 notifikasi serangan karena web server yang diimplementasi memiliki algoritma jika timestamp alert sama maka hanya dibaca 1 notifikasi untuk mengurangi beban pengiriman sms.

Sedangkan yang tercatat pada web server terdapat hanya 60 notifikasi. 60 notifikasi tersebut terdiri dari rule web access sebanyak 5 notifikasi, login telnet sebanyak 18 notifikasi, login ssh sebanyak 11 notifikasi, login ftp sebanyak 14, ping of death sebanyak 10 notifikasi, dan scan nmap sebanyak 2 notifikasi. Untuk catatan notifikasi sms tercatat ada 58 notifikasi yang berhasil terkirim.

Angka – angka diatas memiliki arti bahwa sistem mampu mendeteksi seluruh serangan yang ditujukan ke server. Akan tetapi dalam penampilan notifikasi pada web server dan pengiriman notifikasi adanya serangan terdapat beberapa kesalahan atau error. Pada web server hanya tampil sebanyak 60 notifikasi dari 75 serangan yang dilakukan atau memiliki presentase sebesar 80% keberhasilan dalam menampilkan notifikasi dan mampu mengirimkan notifikasi serangan dengan presentase keberhasilan sebesar 77.3%. Hal ini berarti terdapat beberapa kekurangan yang ada di dalam sistem penampilan notikasi serangan dan pengiriman notifikasi serangan.

Terdapat ketidaksamaan jumlah notifikasi antara jumlah yang ada di database BASE dengan yang ada di web server dikarenakan web server memanggil data pada table acid_event tanpa dimasukkan lagi ke dalam sebuah wadah/database sehingga terjadilah kehilangan 15 notifikasi. Untuk jumlah notifikasi yang terkirim, ketidaksamaan terjadi karena web server hanya bisa memproses pengiriman notifikasi jika halaman catatan serangan di-refresh.

4. KESIMPULAN

Dari hasil pengujian yang telah dilakukan didapatkan kesimpulan, sebagai berikut:

1. Sistem telah diimplementasikan rule sebanyak 6 rule serangan yang terdiri dari Deteksi Remote SSH, Remote Telnet, Login FTP, Akses Web-PHP, Ping of Death dan Scan Port UDP.
2. Pendeteksian IP Address asal serangan hanya terlihat pada IP gateway router menuju server di 192.168.90.2
3. Sistem Snort dapat bekerja dengan baik, seluruh serangan dapat terlihat pada sistem pencatatan log serangan yang dicatat oleh BASE. Namun pencatatan web server terkadang ada beberapa catatan yang tidak ditampilkan oleh web server.
4. Berdasarkan hasil pengujian yang dilakukan, dari 75 serangan yang seharusnya ditampilkan hanya 80% notifikasi yang dapat ditampilkan di web server dan hanya 77.3% notifikasi yang dapat dikirimkan oleh sistem.
5. Web login yang telah diimplementasi mampu melindungi web server yang ada. Seorang admin tidak dapat melewati web login jika ingin melihat catatan serangan.
6. Sistem registrasi user admin dapat berjalan dengan baik, hal ini bisa dilihat dari tingkat

kesuksesan pembuatan user yang tersimpan pada database web server.

PUSTAKA

Afrina, Mira dan Ali Ibrahim, Pengembangan Sistem Informasi SMS Gateway Dalam Meningkatkan Layanan Komunikasi Sekitar Akademika Fakultas Ilmu Komputer Unsri. Jurnal Sistem Informasi (JSI), VOL. 7, NO. 2, Okt 2015

A. Masse, Fitriyanti, Andi Nurul Hidayat dan Badriyanto., Penerapan Network Intrusion Detection System Menggunakan SNORT Berbasis database MySql pada Hotspot Kota. Jurnal Elektronik Sistem Informasi dan Komputer STMIK Bina Mulia. Vol. 1., No. 2., 2015

Ariyus, Dony. Intrusion Detection System, Yogyakarta. Penerbit ANDI. 2007.

Dawood, Rahmad., Said Fairuz Qiana, dan Sayed Muchallil, Kelayakan Raspberry Pi sebagai Web Server: Perbandingan Kinerja Nginx, Apache, dan Lighttpd pada Platform Raspberry Pi. Jurnal Rekayasa Elektrika Vol. 11. No. 1. 2014.

Firdaus, PHP & MYSQL dengan Dreamweaver, Palembang, Maxicom, 2007.

Mutaqin, Asep Fauzi. Rancang Bangun Sistem Monitoring Jaringan Prodi Teknik Informatika Melalui SMS Alert dengan Snort. Jurnal Sistem dan Teknologi Informasi (JUSTIN) Vol.1, No.1, 2016

Prastiyanto,Dhidik., Struktur Jaringan Komunikasi Data Paket Berdasar Protokol X.25., Jurnal Teknik Elektro Vol.2, No.2. 2010.

Rafiudin, Rahmat. Mengganyang Hacker dengan SNORT, Yogyakarta. Penerbit ANDI. 2010.

Sofana, Iwan. Teori & Modul Praktikum Jaringan Komputer. Bandung Penerbit Modula. 2011.

Sofana, Iwan. Membangun Jaringan Komputer Mudah Membuat Jaringan Komputer (Wire & Wireless) Untuk Pengguna Linux. Bandung. Penerbit Informatika. 2013.

Sukmaaji, Anjik, dan Rianto, Jaringan Komputer: Konsep Dasar Pengembangan Jaringan dan Keamanan Jaringan. Yogyakarta. Penerbit ANDI. 2008.

Towidjojo, Rendra. Mikrotik Kung Fu Kitab 1. Jakarta . Jasakom. 2016.