APLIKASI MONITORING KEAMANAN JARINGAN DENGAN MENGGUNAKAN IDS DAN ROUTER MIKROTIK

Pidie wiyanto[1], Amir Hamzah[2], Mohammad Sholeh[3]

[1,2,3] Teknik Informatika, institut Sains & Teknologi AKPRIND Yogyakarta
[1]Pidi1101@gmail.com, [2]Muhash@akprind.ac.id, [3]Miramzah@yahoo.co.id

ABSTRACT

This study is aimed at making security application of computer network by using snort detection system method and mikrotik. Combining IDS method and IPTables mikrotik is to avoid intruder furthrmore, using web to make admin easily to monitor .This application aims to make system of network computer security easier, based on web and to be analyzed as well as controlled by administrator . this application is made to block ip address that is suspected bringing. The system is capable to processing output data from mikrotik, and it can also recognize all activities an intruder in attempt to infiltrate into the system by using port scanner, the ssh, ftp,then do the bloking of ip address that are considered as intruder after that the system will provide a report to the administrator through webserver of the presence of an intruder who trying to get into the system.

Keywords *:security system, intruder,Instrusion detection system, Mikrotik*

INTISARI

Tugas Akhir ini merancang aplikasi keamanan jaringan komputer dengan menggunakan metode dari *Snort Intrusion Detection System* dan mikrotik. Penggabungan metode *IDS* dan *IPTables* mikrotik merupakan sistem pencegahan penyusup. Selain itu juga menggunakan web untuk mempermudah admin untuk monitoring. aplikasi ini bertujuan untuk menciptakan sistem keamanan jaringan computer yang ringan, berbasiskan web dan mudah dianalisa serta diatur oleh administrator. Sistem ini dirancang akan memberikan *blocking* pada alamat *IP* yang diketahui mengirimkan paket penyusup.

Sistem mampu memperoleh data output dari mikrotik serta dapat mengenali segala aktifitas yang dilakukan intruder dalam usaha untuk menyusup kedalam sistem dengan menggunakan *Port scanner, shh, ftp*, kemudian dilakukan proses *blocking* terhadap *ip address* yang dianggap sebagai *intruder* setelah itu sistem akan memberikan laporan kepada administrator melalui webserver mengenai adanya serangan yang mencoba masuk kedalam system

Kata Kunci : Sistem Keamanan, Penyusup, *IDS*, Mikrotik

PENDAHULUAN

Jaringan komputer bukanlah sesuatu yang baru saat ini. Hampir disetiap perusahaan terdapat jaringan komputer untuk memperlancar arus informasi dalam perusahaan tersebut. Internet adalah suatu jaringan komputer raksasa yang saling terhubung dan dapat saling berinteraksi.

Kecepatan upload maupun download merupakan hal yang sangat penting bagi jaringan yang terhubung dengan internet untuk memperlancar transmisi data. Banyak hal yang dapat mempengaruhi kecepatan dua proses tersebut, diantaranya yaitu besarnya bandwidth yang digunakan jaringan tersebut dan seberapa efektifnya bandwidth tersebut bisa dimanfaatkan.

Masalah adalah kebebasan mengakses internet membuat seseorang tidak dapat mengontrol diri dan lupa akana apa yang harusnya dikerjakan. Contoh pada jaringan komputer sebuah perusahaan itu memungkinkan setiap client bebas mengakses situs-situs yang seharus nya tidak boleh diakses pada jam-jam tertentu atau bahkan tidak boleh diakses sama sekali, karena dapat mengganggu proses bisnis dan kinerja karyawan dalam perusahaan tersebut. Dan juga pada jaringan sebesar internet banyak hancker / cracker yang kita tidak ketahui dari mana datangnya yang dapat mengganggu atau bahkan merusak jaringan. Untuk itu diperlukan

sebuah system keamanan pada jaringan tersebut untuk membatasi akses setiap client dan mencegah hacker / cracker masuk ke dalam jaringan.

Mikrotik dapat membantu kita dalam mengelola jaringan komputer, mulai dari pengelolaan *bandwidth* dan penerapan *firewall* untuk membatasi aktifitas *client* dan keamaan jaringan dari ancaman *local* maupun luar.

Intrusion detection (ID) singkatnya adalah usaha mengidentifikasi adanya penyusup yang memasuki system tanpa otorisasi (misalnya cracker) atau seorang user yang sah tetapi menyalahgunakan (*abuse*) privilege sumber daya system (missal *insider threat*). *Intrusion Detection System* (IDS) atau system deteksi penyusupan adalah system computer (bisa merupakan kombinasi software dan hardware). Yang berusaha melakukan deteksi penyusupan. IDS akan melakukan pemberitahuan saat pendeteksian sesuatu yang dianggap sebagai mencurigakan atau tindakan illegal. IDS tidak melakukan pencegahan terjadinya penyusupan.

TINJAUAN PUSTAKA

Penelitian ini disusun berdasarkan beberapa penelitian yang telah dilakukan sebelumnya yang berjudul "Analisa performansi implemantasi intrusion *detection system* berbasis *snort, honeypot honeyd* pada PT X surabaya" (Prasetyo, 2010). Pada penelitian tersebut pemberitahuan adanya serangan masih melalui web, tindak penyerangan masih belum fokus pada jaringan yang ingin diserang. Selain itu, belum ada notifikasi seperti melalui SMS dan media lainnya yang lebih efektif.

Adapun jurnal lain yang membahas tentang *Intrusion Detection System* yaitu "Nagois Untuk Monitoring *Server* Dengan Pengiriman Notifikasi Gangguan *Server* Menggunakan Email dan SMS *Gateway*" (Asri, 2013). Menjelaskan tentang monitoring *server* mengenai masalah notifokasi *error* dan gangguan servis. Belum ada hal spesifik yang mengarah kepada keamanan dari jaringan tersebut

Jurnal public yang membahas tentang *Intrusion Detection System* yaitu "Implementasi *Intrusion Detection System* (IDS) Menggunakan Snort Pada Jaringan Wireless" (Putri, 2011). Fokus penyerangan pada penelitian tersebut pada jaringan *wireless* namun notifikasi kepada *administrator* jaringan masih mengunakan *interface website*.

Jurnal diatas merupakan acuan dari penelitian ini untuk dilakukan pengembangan selanjutnya. Studi kasus ini berfokus pada keamanan jaringan komputer yang mendeteksi serangan dengan menggunakan sistem ids, sistem deteksi serangan jaringan dapat dilakukan secara efektif dan selanjutnya melakukan penanganan terhadap tindakan yang mencurigakan terhadap jaringan. *Tools* yang digunakan pada merupakan gabungan dari beberapa *tools* yang bersifat *open source* seperti Linux Ubuntu, Acidbase, *Router* dan Web*server* serta menggunakan sistem operasi berbasis *Open Source* yang difungsikan khusus untuk penetrasi keamanan jaringan yaitu menggunakan Linux.

METODOLOGI PENELITIAN

Dalam penelitian ini metode pengumpulan data digunakan adalah sebagai berikut :

1. Metode Studi Pustaka
   Melakukan pendalaman terhadap teori-teori yang berkaitan dengan studi kasus. Selain itu juga menggunakan beberapa jurnal yang digunakan sebagai acuan dalam menulis penelitian ini.
2. Metode Penelitian Tindakan / *Action Research*
   Dalam rangka penyelesaian penelitian ini maka digunakan metode penelitian tindakan dalam analisa, perancangan sistem, instalasi perangkat dan pengujian sistem.

Dalam tahap ini, akan dibahas tentang alur penelitian dilakukan, hingga tahapan akhir yaitu analis, desain, simulasi, implementasi, monitoring.

1. Analisis
   Pada tahap ini akan dilakukan pengumpulan data dan materi yang berguna untuk memulai desain dan merancang sebuah desain dari masalah yang akan dibahas.

2. Desain
   Desain dirancang setelah menyelesaikan tahap analisis, pada desain menerangkan tentang gambar dari interface jaringan serta desain keamanan *Intrusion Detection System.*
3. Simulasi
   Dimulainya perancangan sistem yang akan dibuat, termasuk didalamnya instalasi perangkat yang akan digunakan.
4. Implementasi
   Implementasi dilakukan setelah semua perangkat pendukung telah terinstall dan melakukan percobaan awal dari *Intrusion Detection System.*
5. Monitoring
   Tahap ini dilakukan untuk menguji apakah keamanan jaringan telah benar sesuai yang diinginkan. Serta melakukan pengamatan pada perangkat yang digunakan untuk meminimalisir kesalahan.

Pada penelitian ini, dapat beberapa bahan dan alat yang digunakan selama penelitian adalah sebagai berikut :

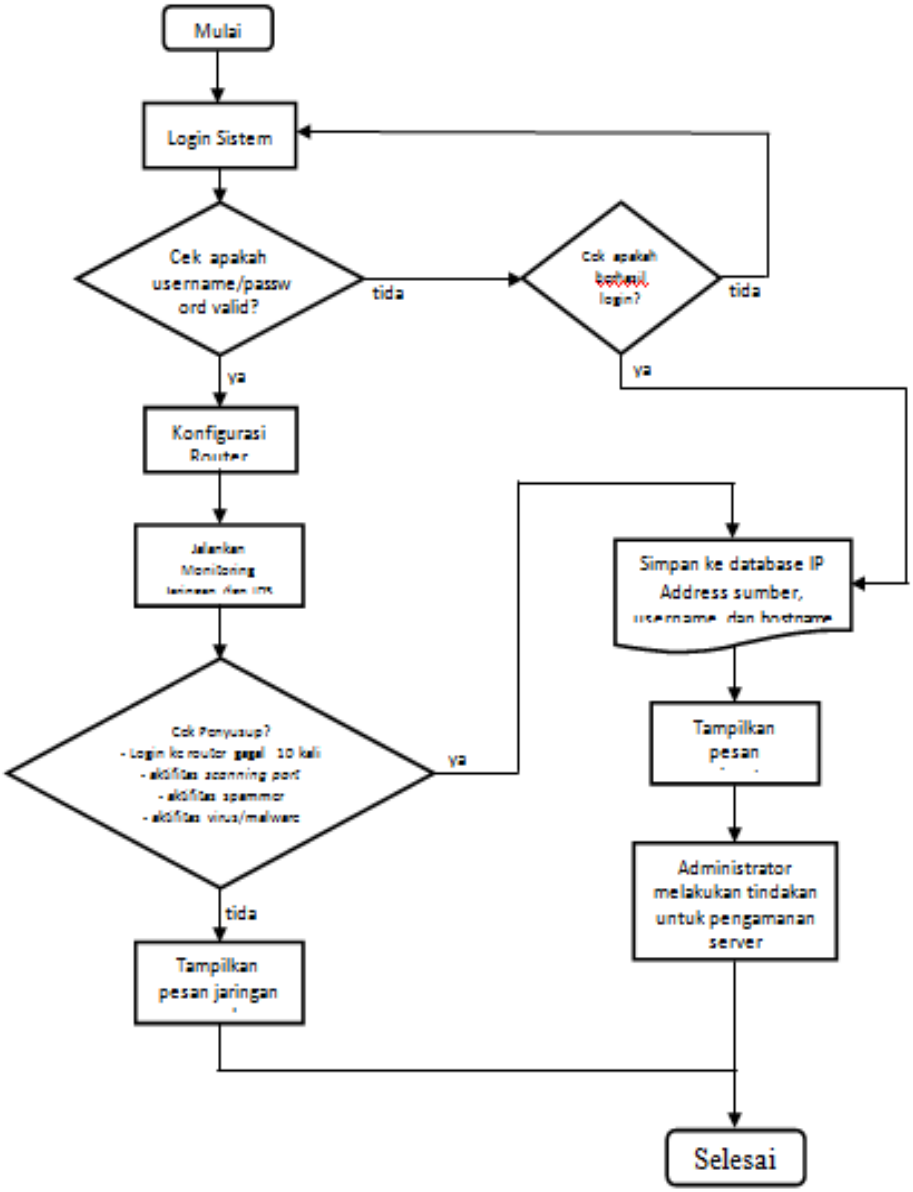
Perangkat Keras :

1. Komputer *Server*
   Komputer *server* bertugas melayani permintaan klien terhadap akses dalam suatu jaringan. Komputer server dalam penelitian ini menggunakan sistem operasi Linux Ubuntu 14.04 LTS.
   - *Processor Intel Dual Core P6200*
   - *RAM 3 GB*
   - *Hard disk 500 GB*
   - *1 Ethernet Card (LAN Card)*
2. Router Mikrotik (RB 450 R)
   Mikrotik merupakan sebuah system operasi perangkat lunak yang diperuntukkan sebagai *router network.*
3. Switch
   adalah sebuah alat jaringan yang melakukan penjembatan taktampak (penghubung penyekatan (segmentation) banyak jaringan dengan pengalihan berdasarkan alamat MAC).
4. Perangkat Klien
   Perangkat klien yang digunakan yaitu komputer *laptop* dan *smartphone* yang mendukung konektifitas nirkabel akan dihubungkan dengan jaringan *WiFi Hotspot* melalui *access point*.
5. Kabel UTP
   Kabel UTP *(Unshielded Twisted Pair)* merupakan kabel yang digunakan untuk menghubungkan antar perantala yang berhubungan dengan jaringan komputer.

Dalam beberapa *software opensource* yang akan digunakan untuk infrastruktur jaringan yang akan dibuat yaitu:

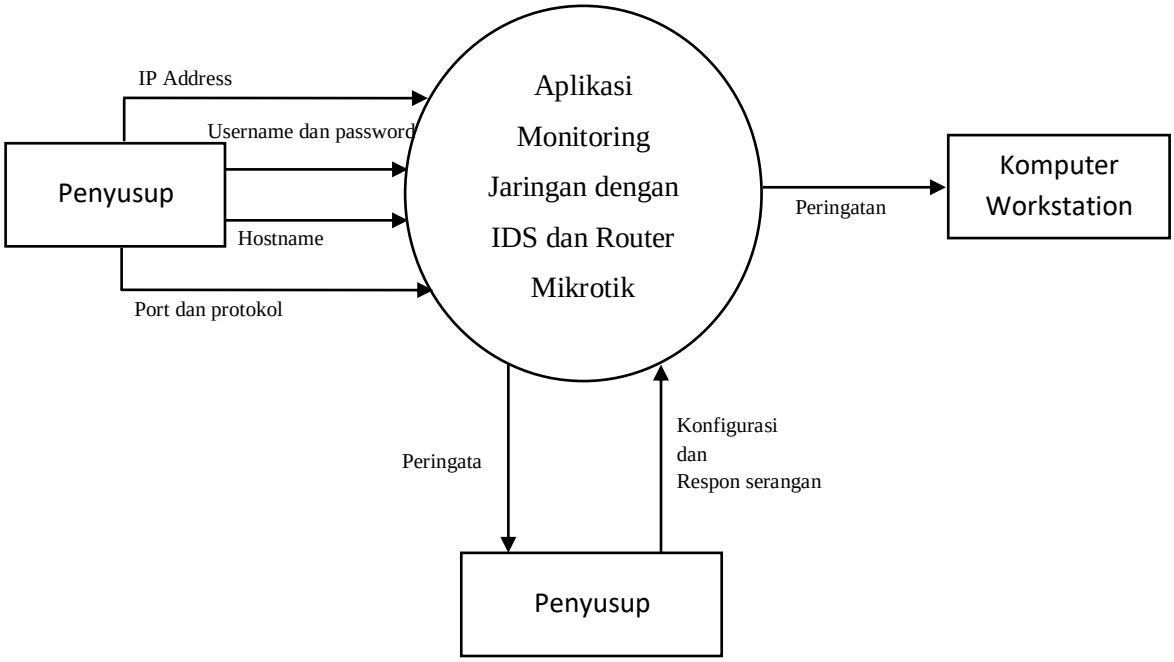
1. Mikrotik OS
   Mikrotik OS adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer manjadi router network yang handal,
2. Apache
   web server yang bertanggung jawab pada request-response HTTP dan logging informasi secara detail.
3. PHP
   PHP berfungsi unutk membuat script server-side yang didesain untuk pengembangan web .
4. MySQL
   MySQL adalah sebuah perangkat lunak sistem manajemen basis data SQL atau DBMS yang multithread, multi-user,

Perancangan infastruktur pada penelitian ini dengan berupa flowchart pada sistem keamanan jaringan dapat digambarkan seperti pada gambar 1 berikut ini.



Gambar 1. Flowchart keamanan jaringan

Perancangan schema serangan pada sistem keamanan jaringan dapat digambarkan seperti pada gambar 2 berikut ini.



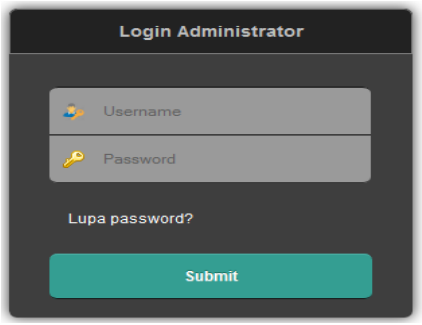
Gambar 2. Schema pengujian keamanan

PEMBAHASAN

Hasil desain sistem merupakan pembahasan hasil pembuatan program berdasarkan perancangan yang dilakukan implementasi sistem merupakan tahap akhir dari proses desain sistem yang telah di buat. Setelah proses perancangan dilakukan dengan membuat keamanan jaringan dengan mikrotik dan desain *interface* sistem, maka penelitian berlanjut dengan implementasi dilakukan serangkaian proses uji coba guna mengetahui apakah sistem tersebut dapat berfungsi seperti tujuan yang di harapkan. Pada pembahasan implementasi sistem ini diuraikan bagian-bagian sistem sebagaimana yang telah didesain pada bagian perancangan.

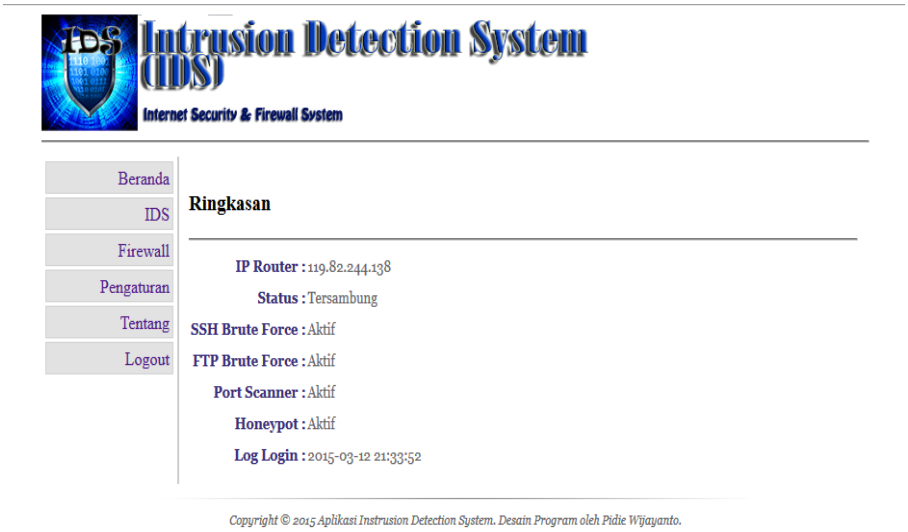
Dalam pembentukan sebuah sistem monitoring keamanan jaringan, langkah-langkah yang digunakan adalah menentukan alur serangan dengan menggunakan metode – metode serangan seperti, *ssh burce force, ftp burce force, port scanner*. Melalui hasil implementasi dapat diketahui evaluasi jalannya sistem dan mendapatkan alasan-alasan kemungkinan perlunya perbaikan, pengembangan ataupun langkah-langkah lebih lanjut yang diperlukan.
IDS akan menampilkan menu-menu monitoring jaringan diantaranya:

1. Halaman login
   Pada gambar 3. dapat dilihat tampilan halaman login berisi tentang direktori / page pada website untuk administrator.



Gambar 3. login admin

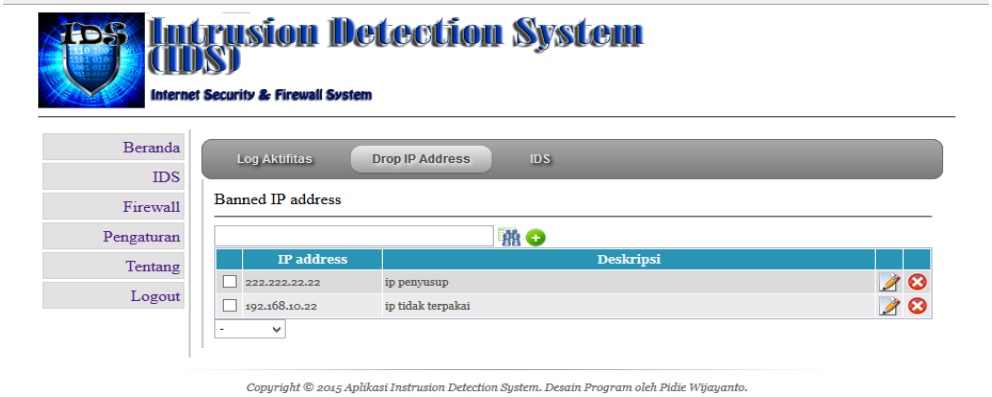
2. Beranda admin
Menu home berisi tentang penjelasan system dan menu-menu yang terdapat didalam system. Berikut tampilan pada gambar 4.



Gambar 4.beranda admin

3. IDS
Didalam tabel ids terdiri diri log aktifitas dan drop ip address yang dapat dilihat pada gambar.5 dan gambar 6.

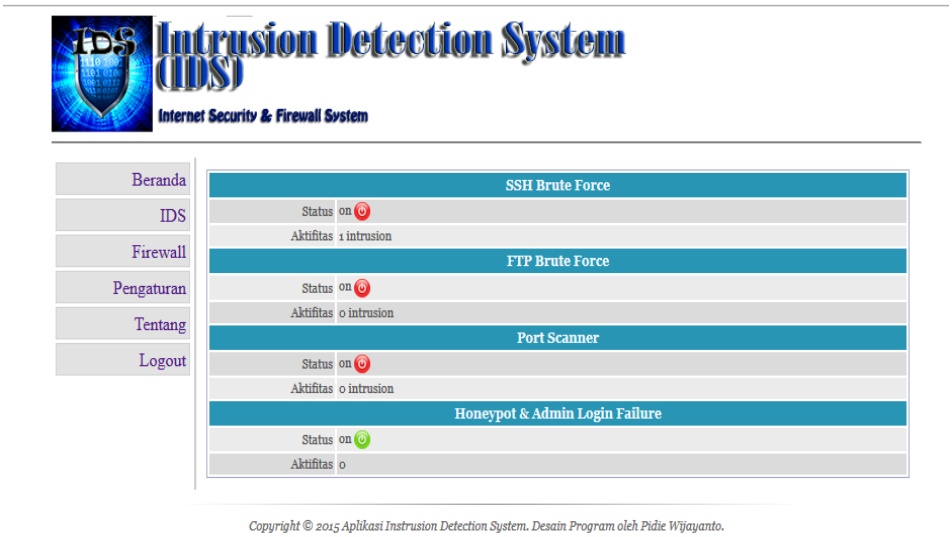
Gambar 5. log aktitas



Gambar 6 drop ip address

4. Firewall

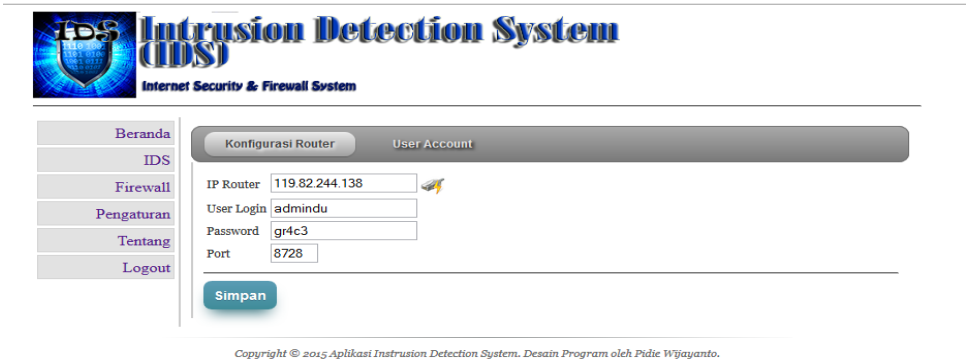
Pada gambar .7 dapat dilihat tampilan halaman firewall berisi informasi aktifitas serangan dengan skema *seperti SSH Brute Force, FTP Brute Force, Port Scanner* dan *Login failure*



Gambar 7. Tampilan Firewall

5. Pengaturan

Pada gambar.8 dan gambar.9 dapat dilihat tabel pengaturan terdiri dari konfigurasi router dan konfigurasi username / password.



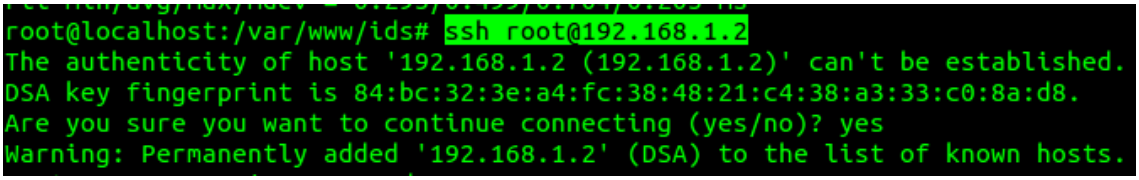
Gambar.8 Konfigurasi router

Gambar .9 konfigurasi username / password

Pengujian sistem ini diharapkan bisa mendeteksi serangan-serangan pada jaringan, Metode pengujian menggunakan penetration testing seperti uraian sebelumnya. Proses pengujian keamanan jaringan LAN melalui beberapa tahap sebagai berikut (Rathore, 2006):

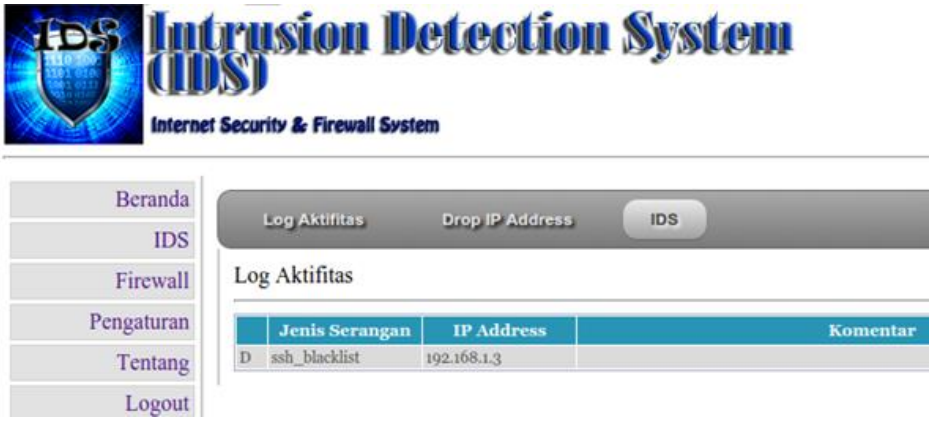
1. Information gathering
   Sebelum melakukan tindakan pengujian dibutuhkan data-data access point yang terpasang di objek pengujian seperti network, ESSID, channel, MAC address dan IP address dalam jaringan.
2. Analisis
   Setelah mengetahui karakter jaringan selanjutnya dilakukan analisis untuk menentukan jenis tindakan dan kebutuhan pengujian dengan penetrasi.
3. Attacking
   Tahap ini dilakukan tindakan penetrasi jaringan dengan berbagai macam serangan seperti SSH brute force, Port scanner, FTP brute force.

Pada gambar .11 dilakukan Pengujian SSH Brute Force melalui terminal ubuntu untuk login dengan cara paksa ke dalam sistem ,



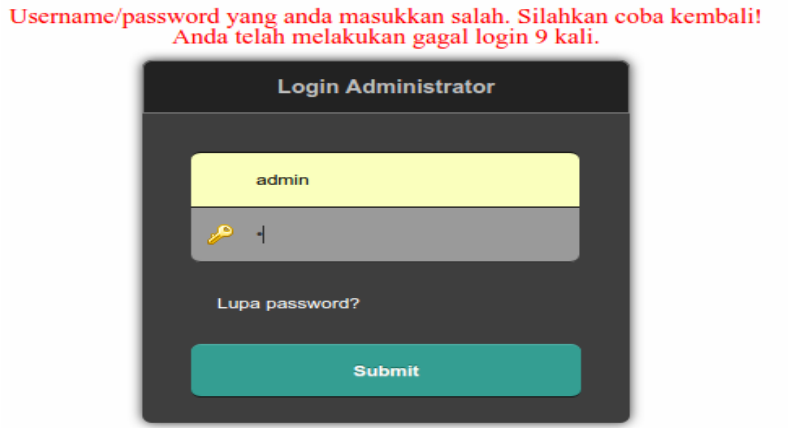
Gambar.11 Serangan SSH Brute Force

Pada gambar.12 system mendeteksi serangan ssh brute force dengan ip address penyerang 192.168.1.3, untuk lebih jelasnya bisa digambar berikut



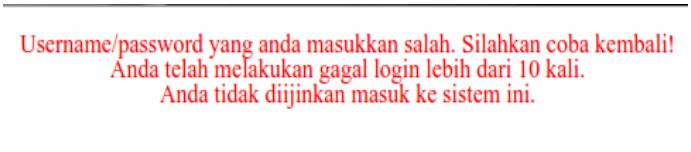
Gambar.12 Gambar SSH brute Force

Pada gambar.13 dilakukan Pengujian Ancaman login failure melalui web login dengan salah login lebih dari 10 kali, dan sistem membaca ancaman, bisa dilihat digambar berikut.



Gambar.13 Login Failure

Setelah administrator gagal login lebih dari 10 kali maka system akan memblokir ip address user, bisa dilihat pada gambar.14



Gambar.14 Ancaman Login Failure

KESIMPULAN

Pada proses pengujian yang dilakukan dapat diketahui kemampuan dari system yang dibuat mampu mengenali segala aktifitas yang dilakukan intruder dalam usaha untuk menyusup

ke dalam sistem dengan menggunakan SSH brute force, Ftp brute force ,Port scanner ,kemudian diproses blocking terhadap IP address yang dianggap sebagai intruder selain itu system akan memberikan laporan kepada administrator melalui web untuk mempermudah administrator untuk mengelola atau mengawasi jaringan tersebut.

Kategori serangan yang paling tinggi didalam sistem adalah serangan SSH, bila intruder dapat mengetahui username dan password sebuah system maka intruder dapat melakukan apa saja terhadap system tersebut. Untuk serangan FTP dapat dikategorikan kedalam tingkat menengah, karena tidak mendapat hak akses secara penuh kedalam server. Sedangkan port scanner dikategorikan serangan paling rendah karena intruder hanya mengetahui port yang terbuka.

DAFTAR PUSTAKA

Prasetyo, 2010, Analisa performansi implemantasi intrusion *detection system* berbasis *snort, honeypot honeyd,skripsi*, Jurusan Teknik Informmatika, Universitas Islam Indonesia, Yogyakarta

Dwiyono, Aswin. 2008. Pengenalan Firewall dan IPTables pada Jaringan Komputer, Tugas Akhir, Teknik Informatika, Universitas Sriwijaya, Indralaya.

Asri, 2013, Nagois Untuk Monitoring *Server* Dengan Pengiriman Notifikasi Gangguan *Server* Menggunakan Email dan SMS *Gateway,* Jurusan Teknik Informmatika, Universitas Islam Indonesia, Yogyakarta

Handriyanto, Dwi Febrian. 2009. Kajian Penggunaan Mikrotik Router OSTM Sebagai Router pada Jaringan Komputer, Jurnal, Fakultas Teknik

Herlambang. 2008. Panduan Lengkap Menguasai Router Masa Depan Menggunakan MikroTik RouterOSTM . ANDI Publisher : Yogyakarta.

Purbo, O. W. 2000, Linux Untuk Warung Internet, Jakarta: Elex Media Komputindo.

Putri, 2011, Implementasi *Intrusion Detection System* (IDS) Menggunakan Snort Pada Jaringan Wireless, Jurusan Teknik Informatika, Universitas Islam Indonesia, Yogyakarta