DESAIN DAN IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) BERBASIS LINUX PADA JARINGAN LAN

SKRIPSI

Disusun Oleh:

RINO JIWANDANU
08.18.902

PROGRAM STUDI TEKNIK INFORMATIKA S-1
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL MALANG

2013

LEMBAR PERSETUJUAN

DESAIN DAN IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) BERBASIS LINUX PADA JARINGAN LAN

SKRIPSI

Disusun dan diajukan untuk melengkapi dan memenuhi persyaratan guna mencapai gelar Sarjana Komputer

Disusun Oleh :

RINO JIWANDANU

08.18.902

Diperiksa dan Disetujui,

Dosen Pembimbing I	Dosen Pembimbing II
Joseph Dedy Irawan, ST., MT.	**Sonny Prasetio, ST., MT.**
NIP. 19740416 2005011002	**NIP.P. 1031000433**

Mengetahui

Kepala Jurusan Teknik Informatika S-1

Joseph Dedy Irawan, ST., MT.

NIP. 19740416 2005011002

INSTITUT TEKNOLOGI NASIONAL MALANG
FAKULTAS TEKNOLOGI INDUSTRI
PROGRAM STUDI TEKNIK INFORMATIKA S-1
2013

DESAIN DAN IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) BERBASIS LINUX PADA JARINGAN LAN

Rino Jiwandanu (NIM. 0818902)

Teknik Informatika S-1, Institut Teknologi Nasional Malang
e-mail : rinojiwandanu@gmail.com

Dosen Pembimbing : I. Joseph Dedi Irawan, ST, MT
II. Sonny Prasetio, ST, MT

Abstrak

Teknologi jaringan komputer selain memberikan kemudahan dalam berkomunikasi, ternyata terdapat pula beberapa kelemahan pada segi kemanannya. Keamanan jaringan bergantung pada kecepatan pengatur jaringan dalam menindaklanjuti sistem saat terjadi gangguan. IDS disarankan karena.IDS mampu mendeteksi paket-paket berbahaya pada jaringan dan memberikan peringatan kepada admin tentang keadaan jaringan saat itu. Dalam proses pengerjaannya menggunakan IDS Snort, dilakukan pengujian dengan dua cara dan sebanyak 5 intruder yaitu pengujian pertama dilakukan scan port pengujian yang kedua menggunakan DDOS, setelah di lakukan pengujian maka didapat hasil 100% karena pengujian pertama dan kedua dari kelima IP tersebut *masing – masing* semua berhasil terdeteksi.

Kata Kunci : IDS, Snort, Intrusion Detection System

Abstract

Computer networking technology in addition to providing ease of communication, it turns out there are also some disadvantages in terms kemanannya. Network security depends on the speed of the network control system to follow up when an interruption occurs. IDS suggested because IDS able to detect malicious packets on the network and alert the administrator about the state of the network at that time. In the course of the work using Snort IDS, tested in two ways and as much as 5 intruder is the first test performed port scans using DDOS second test, after test done then obtained test results of 100% for the first and second of these IP fifth respectively - each all successfully detected

Keyword : IDS, Snort, Intrusion Detection System

PROGRAM STUDI TEKNIK INFORMATIKA S-1
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL
MALANG

PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan di bawah ini:

Nama	:	Rino Jiwandanu
Nim	:	08.18.902
Program Studi	:	Teknik Informatika S-1
Fakultas	:	Teknologi Industri

Menyatakan dengan sesungguhnya bahwa Skripsi saya yang berjudul:

"DESAIN DAN IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) BERBASIS LINUX PADA JARINGAN LAN"

Adalah bukan duplikat atau mengutip dan tidak memuat seluruhnya karya orang lain kecuali dari sumber aslinya.

Malang, 11 Maret 2013

Yang membuat pernyataan

Rino Jiwandanu

KATA PENGANTAR

Alhamdulillah Puji syukur penulis panjatkan ke hadirat Allah SWT atas karunia, rahmat dan hidayahNya, sehingga penulis dapat menyelesaikan penelitian yang berjudul "**DESAIN DAN IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) BERBASIS LINUX PADA JARINGAN LAN**".

Skripsi ini dapat terselesaikan tidak terlepas dari dukungan berbagai pihak. Penulis mengucapkan terima kasih yang sebesar-besarnya kepada :

1. Bapak Ir. Soeparno Djiwo, MT selaku Rektor Institut Teknologi Nasional Malang.
2. Bapak Ir. H. Anang Subardi, MT selaku Dekan Fakultas Teknologi Industri Institut Teknologi Nasional Malang.
3. Bapak Joseph Dedy Irawan, ST, MT selaku Kepala Jurusan Teknik Informatika S-1 Institut Teknologi Nasional Malang dan selaku Dosen Pembimbing I yang telah memberikan saran dan bimbingannya dalam penyusunan laporan ini.
4. Bapak Sonny Prasetio, ST, MT selaku Dosen Pembimbing II yang telah memberikan saran dan bimbingannya dalam penyusunan laporan ini.
5. Bapak dan Ibu Dosen yang telah mengajar penulis selama studi di Institut Teknologi Nasional Malang.
6. Ayahanda Drs.Herman Suhargo, MM dan Ibunda Muntianah yang selalu memberikan do'a restu, dorongan dan semangat.
7. Rekan-rekan yang turut membantu dalam penyelesaian laporan ini.

Semoga apa yang telah disajikan dapat memberikan manfaat dan pengetahuan bagi para pembaca. Segala kritik dan saran yang bersifat membangun, diterima dengan senang hati sebagai tambahan ilmu pengetahuan.

Malang, 11 Maret 2013

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB II LANDASAN TEORI

BAB III PERANCANGAN SISTEM

BAB IV IMPLEMENTASI DAN PENGUJIAN


INSTITUT TEKNOLOGI NASIONAL
ITN
MALANG

BAB I
PENDAHULUAN

1.1. Latar Belakang

Keamanan jaringan komputer sebagai bagian dari sebuah sistem sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunanya. Sistem harus dilindungi dari segala macam serangan dan usaha penyusupan atau pemindaian oleh pihak yang tidak berhak.

Keamanan jaringan bergantung pada kecepatan pengatur jaringan dalam menindaklanjuti sistem saat terjadi gangguan. Penerapan IDS diusulkan sebagai salah satu solusi yang dapat digunakan untuk membantu pengatur jaringan dalam memantau kondisi jaringan dan menganalisa paket-paket berbahaya yang terdapat dalam jaringan tersebut. IDS diterapkan karena sistem ini mampu mendeteksi 'paket-paket berbahaya pada jaringan dan langsung memberikan peringatan kepada pengatur jaringan tentang kondisi jaringannya saat itu.

Pada dasarnya IDS terbagi menjadi dua jenis yaitu *rule based* dan *adaptive system*. Sistem rule based mendeteksi suatu serangan berdasarkan aturan-aturan yang sudah didefinisikan pada kumpulan data aturan, sedangkan sistem adaptive dapat mengenali jenis serangan baru dengan cara membandingkan kondisi saat ini dengan kondisi normal suatu sistem.

Terdapat banyak software IDS seperti Snort yang merupakan open source IDS yang juga digunakan dalam penelitian ini. Namun belum terdapat sistem antar muka yang membantu para pengguna dalam mengatur sistem sehingga penerapan IDS ini masih sulit dilakukan. Oleh karena itu diusulkan untuk membuat sebuah sistem IDS lengkap dengan tampilan antarmuka berbasiskan web dengan beberapa fitur tambahan yang diharapkan dapat membantu administrator dalam memonitor kondisi jaringannya serta meningkatkan mutu keamanan jaringan tersebut.

1.2. Rumusan Masalah

Bagaimana mendesain dan mengimplementasikan IDS dalam mendeteksi serangan pada sistem jaringan komputer .

1.3. Tujuan

Mengimplementasikan IDS dalam mendeteksi serangan pada sistem jaringan komputer.

1.4. Batasan Masalah

Agar permasalahan mengarah sesuai dengan tujuan yang diharapkan, maka pembahasan dibatasi oleh hal-hal sebagai berikut:

1. Menggunakan Snort IDS (Intrusion Detection System)
2. Melakukan pengujian dengan serangan port scanning dan ddoss.
3. Menampilkan hasil serangan melalui tampilan Web.

1.5. Metodologi Penelitian

Adapun metode penelitian yang digunakan adalah sebagai berikut:

1. Studi Literatur

   Pengumpulan data dilakukan dengan mencari bahan-bahan referensi dari berbagai sumber sebagai landasan teori yang berhubungan dengan permasalahn yang dijadikan objek penelitian.

2. Analisa Kebutuhan Sistem

   Data dan informasi yang telah diperoleh akan dianalisa agar didapatkan suatu kerangka yang digunakan untuk acuan perancangan sistem.

3. Implementasi

Implementasi IDS dalam mendeteksi serangan pada sistem jaringan LAN diimplementasikan dengan menggunakan Snort berbasis Open Source dan hasil serangan ditampilan melalui tatap muka Web.

4. Eksperimen dan Evaluasi

Merupakan tahap pengujian terhadap system yang telah dibuat. Tahap pengujian ini akan menggunakan 1 komputer target, 1 komputer yang di install Snort dan 1 komputer intruder.

1.6. Sistematika Penulisan

Untuk mempermudah dan memahami pembahasan penulisan skripsi ini, maka sistematika penulisan disusun sebagai berikut :

Bab I PENDAHULUAN

Berisi Latar Belakang, Rumusan Masalah, Tujuan Penelitian, Batasan Masalah, Metode Penelitian dan Sistematika Penulisan.

Bab II LANDASAN TEORI

Berisi tentang landasan teori mengenai permasalahan yang berhubungan dengan penelitian yang dilakukan.

BAB III PERANCANGAN SISTEM

Membahas tentang tahapan perancangan dan rekayasa perangkat lunak maupun perangkat keras yang dibutuhkan dalam sistem ini, serta konfigurasi.

BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM

Membahas tentang pengujian sistem serta analisis dari hasil pengujian sistem tersebut

BAB V PENUTUP

Memberikan kesimpulan yang diperoleh dari hasil pengujian sistem yang dibutuhkan untuk kesempuranaan sistem.


INSTITUT TEKNOLOGI NASIONAL
ITN
MALANG

BAB II
LANDASAN TEORI

2.1 Jaringan Komputer

Jaringan komputer merupakan sekumpulan komputer berjumlah banyak yang terpisah-pisah akan tetapi saling berhubungan dalam melaksanakan tugasnya. Dua buah komputer misalnya dikatakan terkoneksi bila keduanya dapat saling bertukar informasi. Bentuk koneksi dapat melalu : kawat tembaga, serat optic, gelombang mikro, satelit komunikasi. Sebuah jaringan komputer pada dasarnya dibentuk oleh lapisan jaringan dalam model Open System Infastruktur atau yang dikenal sebagai model OSI.

2.1.1 Jenis-Jenis Jaringan Komputer

Berdasarkan luas areanya maka jaringan komputer dapat dibedakan menjadi:

a. LAN (Local Area Network)

Adalah sebuah jaringan komputer yang hanya mencakup area kecil seperti kantor atau bangunan. Semua komputer individu harus memiliki lapisan protocol umum untuk konektivitasnya dengan fungsionalitas dasar yang terjadi pada lapisan jaringan. Secara umum, LAN didasarkan pada teknologi Ethernet.

b. MAN (Metropolit Area Network)

Merupakan kombinasi dua atau lebih individual Lokal Area Networks tetapi dengan criteria dari batas jaringan kecil dan tidak melebihi dari batas kota, sehingga dapat di asumsikan jaringan dalam sebuah kota. Apabila dihitung dengan jarak sekitar 10.000-1000.000 meter.

c. WAN (Wide Area Network)

Ukuran jaringannya lebih besar dari MAN. Menurut perhitungan jarak, jarak yang dapat dijangkau adalah 100.000-1000.000.000 meter. Atau dapatmencakup sebuah Negara atau benua.

2.1.2 Arsitektur Jaringan

Standar yang paling populer untuk menggambarkan arsitektur jaringan adalah model referensi Open System Interconnect (OSI) yang dikembangkan oleh International Organization for Standarization (ISO) pada tahun 1977 dan diperkenalkan pada tahun 1984. Pada model referensi OSI terdapat 7 buah lapisan yang setiap lapis-nya mengilustrasikan fungsi – fungsi jaringan. Pembagian fungsi – fungsi jaringan ini antara lain :

Lapisan ke-	Nama lapisan	Keterangan
7	*Application layer*	Berfungsi sebagai antarmuka dengan aplikasi dengan fungsionalitas jaringan, mengatur bagaimana aplikasi dapat mengakses jaringan, dan kemudian membuat pesan-pesan kesalahan. Protokol yang berada dalam lapisan ini adalah HTTP, FTP, SMTP, dan NFS.
6	*Presentation layer*	Berfungsi untuk mentranslasikan data yang hendak ditransmisikan oleh aplikasi ke dalam format yang dapat ditransmisikan melalui jaringan. Protokol yang berada dalam level ini adalah perangkat lunak redirektor (*redirector software*), seperti layanan *Workstation* (dalam Windows NT) dan juga Network shell (semacam *Virtual Network Computing* (VNC) atau *Remote Desktop Protocol* (RDP)).
5	*Session layer*	Berfungsi untuk mendefinisikan bagaimana koneksi dapat dibuat, dipelihara, atau dihancurkan. Selain itu, di level ini juga dilakukan resolusi nama.
4	*Transport layer*	Berfungsi untuk memecah data ke dalam paket-paket data serta memberikan nomor urut ke paket-paket tersebut sehingga dapat disusun kembali pada sisi tujuan setelah diterima. Selain itu, pada level ini juga membuat sebuah tanda bahwa paket diterima dengan sukses (acknowledgement), dan mentransmisikan ulang terhadp paket-paket yang hilang di tengah jalan.

3	*Network layer*	Berfungsi untuk mendefinisikan alamat-alamat IP, membuat *header* untuk paket-paket, dan kemudian melakukan routing melalui *internetworking* dengan menggunakan *router* dan *switch layer-3*.
2	*Data-link layer*	Befungsi untuk menentukan bagaimana bit-bit data dikelompokkan menjadi format yang disebut sebagai ***frame***. Selain itu, pada level ini terjadi koreksi kesalahan, *flow control*, pengalamatan perangkat keras (seperti halnyaMedia Access Control Address (MAC Address)), dan menetukan bagaimana perangkat-perangkat jaringan seperti*hub*, *bridge*, *repeater*, dan *switch layer 2* beroperasi. Spesifikasi IEEE 802, membagi *level* ini menjadi dua level anak, yaitu lapisan *Logical Link Control* (LLC) dan lapisan *Media Access Control* (MAC).
1	*Physical layer*	Berfungsi untuk mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur jaringan (seperti halnya Ethernet atau Token Ring), topologi jaringan dan pengabelan. Selain itu, level ini juga mendefinisikan bagaimana *Network Interface Card* (NIC) dapat berinteraksi dengan media kabel atau radio.

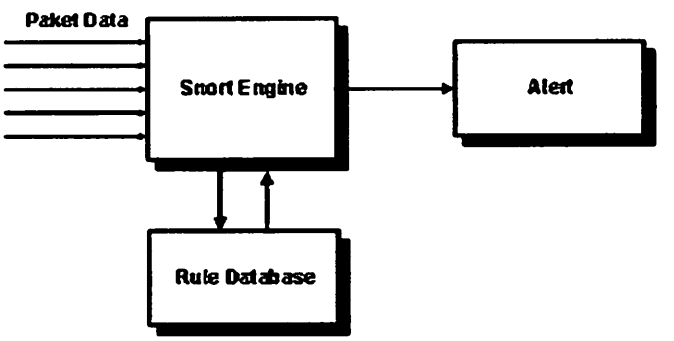
2.2 Keamanan Jaringan

Keamanan jaringan secara umum adalah komputer yang terhubung ke network, mempunyai ancaman keamanan lebi besar daripada komputer yang tidak terhubung kemana – mana. Dengan pengendalian yang teliti, resiko tersebut dapat dikurangi. Namun network security biasanya bertentangan dengan network access, dimana bila network access semakin mudah, maka network security semakin rawan, dan bila network security semakin baik, network access semakin tidak nyaman. Suatu network didesain sebagai komunikasi data highway dengan tujuan meningkatkan akses ke sistem komputer, sementara security didesain untuk mengontrol akses. Penyediaan network security adalah sebagai aksi antara penyemimbang antara open access dengan security.

2.3 IDS (Intrusion Detection System)

Intrusion Detection System (disingkat IDS) adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS dapat melakukan inspeksi terhadap lalu lintas inbound dan outbound dalam sebuah sistem atau jaringan, melakukan analisis dan mencari bukti dari percobaan intrusi (penyusupan).

Suatu Intrusion Detection System (IDS) dapat didefinisikan sebagai tool, metode, sumber daya yang memberikan bantuan untuk melakukan identifikasi, memberikan laporan terhadap aktivitas jaringan komputer. Intrusion Detection System (IDS) berfungsi sebagai proteksi secara keseluruhan dari sistem yang telah diinstal IDS. IDS tidak berdiri sendiri dalam melindungi suatu sistem.



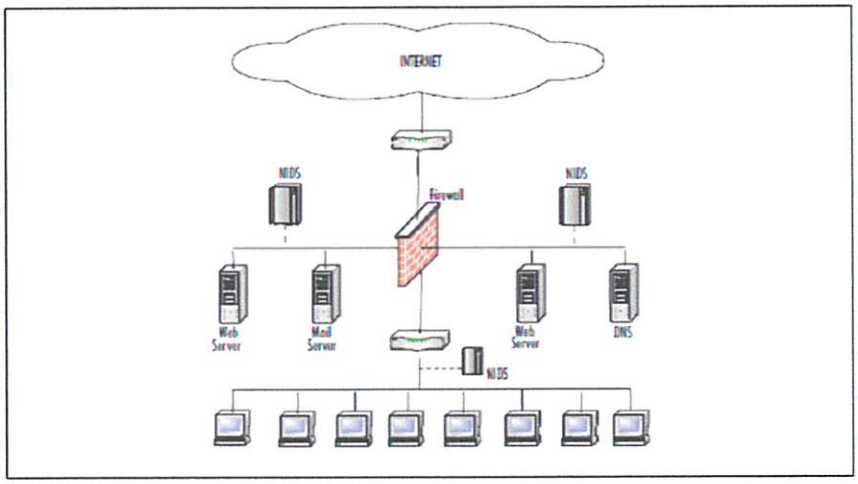
Gambar 2.1. Bagian bagian IDS

2.3.1 Tipe Intrusion Detection System (IDS)

Pada dasarnya terdapat dua macam IDS yaitu :

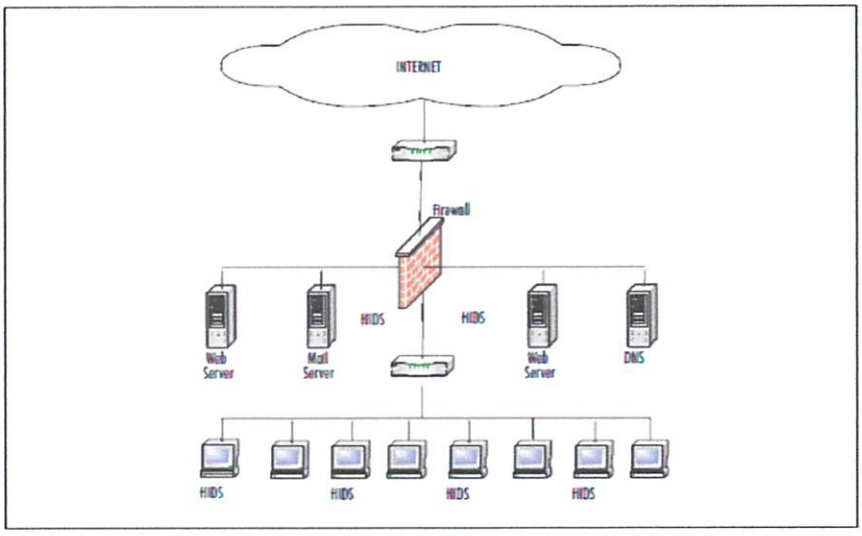
1. Network-based Intrusion Detection System (NIDS): Semua lalu lintas yang mengalir ke sebuah jaringan akan dianalisis untuk mencari apakah ada percobaan serangan atau penyusupan ke dalam sistem jaringan. NIDS umumnya terletak di dalam segmen jaringan penting di mana server berada atau terdapat pada "pintu masuk" jaringan. Kelemahan NIDS adalah bahwa NIDS agak rumit diimplementasikan dalam sebuah jaringan yang menggunakan switch Ethernet, meskipun beberapa vendor switch

Ethernet sekarang telah menerapkan fungsi IDS di dalam switch buatannya untuk memonitor port atau koneksi.



Gambar 2.2. NIDS

2. Host-based Intrusion Detection System (HIDS): Aktivitas sebuah host jaringan individual akan dipantau apakah terjadi sebuah percobaan serangan atau penyusupan ke dalamnya atau tidak. HIDS seringnya diletakkan pada server-server kritis di jaringan, seperti halnya firewall, web server, atau server yang terkoneksi ke Internet.



Gambar 2.3. HIDS

2.3.2 Cara kerja IDS

1. Knowledge-based atau misuse detection
2. Behavior-based atau anomaly based

2.4 Snort

Snort merupakan suatu perangkat lunak untuk mendeteksi penyusup dan mampu menganalisis paket yang melintasi jaringan secara real time traffic dan logging ke dalam database serta mampu mendeteksi berbagai serangan yang berasal dari luar jaringan. Snort tersedia gratis di internet. Snort bisa digunakan pada platform sistem operasi Linux, BSD, solaris, Windows dan sistem operasi lainnya.

Gambar 2.4. Snort

2.4.1 Mode - Mode Snort

Snort diopersikan dalam tiga mode, yaitu:

1. Paket sniffer : untuk melihat paket yang lewat di jaringan.
2. Paket logger : untuk mencatat semua paket yang lewat di jaringan untuk di analisis di kemudian hari.
3. NIDS, deteksi penyusup pada network : pada mode ini snort akan berfungsi untuk mendeteksi serangan yang di lakukan melalui jaringan komputer. Untuk menggunakan mode IDS ini diperlukan setup dari berbagai rules atau aluran yang akan membedakan sebuah paket.

2.4.2 Paket Sniffer

Untuk menjalankan Snort pada Sniffer Mode, berikut beberapa contoh perintahnya:

1. # snort –v
2. # snort –vd
3. # snort –vde
4. # snort –v –d –e

2.4.3 Paket logger

Berikut beberapa yang dapat digunakan untuk mencatat paket yang ada:

1. # snort –vde –h 192.168.0.1/24 ./log
2. # snort -l /var/log/snort/snortlog -b
3. # snort -l ./log –b
4. # snort –vder packet.log
5. # snort –dvr packet.log icmp

2.4.4 NIDS

1. # snort –dev -l ./log –h 192.168.0.1/24 –c snort.conf
2. # snort –d –h 192.168.0.1/24 -l ./log –c snort.conf
3. # snort –c snort.conf -l ./log –s –h 192.168.0.1/24
4. # snort –c snort.conf –s –h 192.168.0.1/24
5. #/usr/local/bin/snort –d –h 192.168.0.1/24 -c /root/snort/snort.conf –A full –s –D

2.4.5 Snort Rules

Snort Rules adalah sebuah folder yang berisikan tentang berbagai aturan-aturan yang dibuat.

2.5 Linux Ubuntu

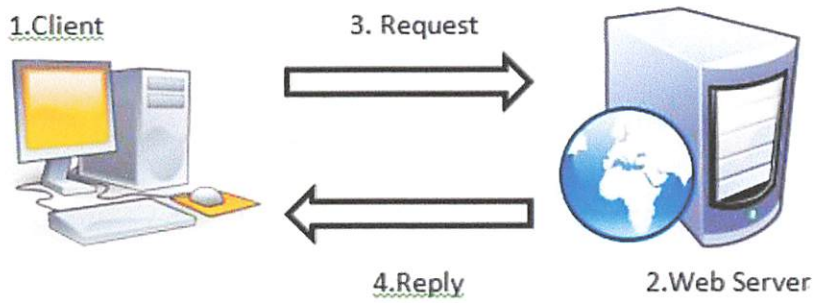
Merupakan salah satu distribusi Linux yang berbasiskan Debian dan didistribusikan sebagai software bebas. Nama Ubuntu berasal dari filosofi dari Afrika Selatan yang berarti "Kemanusiaan kepada sesama"[7]. Ubuntu didesain untuk kepentingan penggunaan personal, namun versi server Ubuntu juga tersedia, dan telah dipakai secara luas.

2.6 Apache

Server HTTP Apache atau Server Web/WWW Apache adalah server web yang dapat dijalankan di banyak sistem operasi (Unix,BSD, Linux, Microsoft Windows dan Novell Netware serta platform lainnya) yang berguna untuk melayani dan memfungsikan situs web. Protokol yang digunakan untuk melayani fasilitas web/www ini menggunakan HTTP.

Beberapa paket nya adalah:

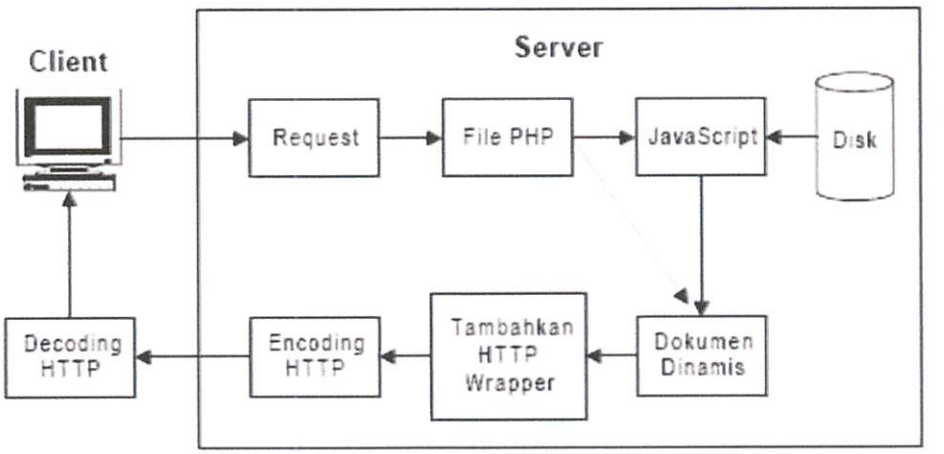
1. Apache2
2. PHP5
3. MySQL



Gambar 2.5. Sistem kerja Apache

2.7 PHP

PHP: Hypertext Preprocessor adalah bahasa skrip yang dapat ditanamkan atau disisipkan ke dalam HTML.PHP banyak dipakai untuk pemrogram situs web dinamis. PHP dapat digunakan untuk membangun sebuah CMS.



Gambar 2.6. Sistem kerja PHP

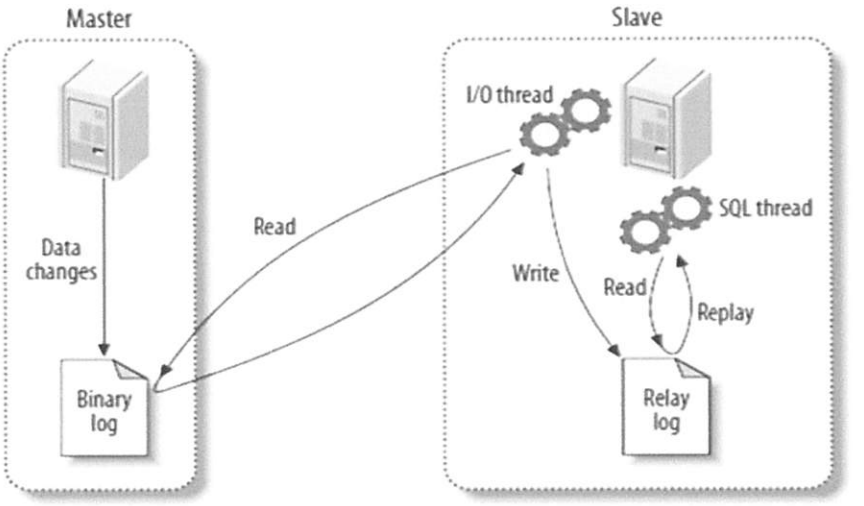
2.8 PhpMyAdmin

phpMyAdmin adalah perangkat lunak bebas yang ditulis dalam bahasa pemrograman PHP yang digunakan untuk menangani administrasi MySQL melalui Jejaring Jagat Jembar (World Wide Web). phpMyAdmin mendukung berbagai operasi MySQL, diantaranya (mengelola basis data, tabel-tabel, bidang (fields), relasi (relations), indeks, pengguna (users), perijinan (permissions), dan lain-lain).

Gambar 2.7 Page Login phpMyAdmin

2.9 MySQL

MySQL adalah sebuah perangkat lunak sistem manajemen basis data SQL (bahasa Inggris: database management system) atau DBMS yang multithread, multi-user, dengan sekitar 6 juta instalasi di seluruh dunia. MySQL AB membuat MySQL tersedia sebagaiperangkat lunak gratis dibawah lisensi GNU General Public License (GPL), tetapi mereka juga menjual dibawah lisensi komersial untuk kasus-kasus dimana penggunaannya tidak cocok dengan penggunaan GPL.



Gambar 2.8 Cara kerja MySql

2.10 Nmap

Nmap (Network Mapper) adalah sebuah aplikasi atau tool yang berfungsi untuk melakukan port scanning. Nmap dibuat oleh Gordon Lyon, atau lebih dikenal dengan nama Fyodor Vaskovich. Aplikasi ini digunakan untuk meng-audit jaringan yang ada. Dengan menggunakan tool ini, kita dapat melihat host yang aktif, port yang terbuka, Sistem Operasi yang digunakan, dan feature-feature scanning lainnya. Pada awalnya, Nmap hanya bisa berjalan di sistem operasi Linux, namun dalam perkembangannya sekarang ini, hampir semua sistem operasi bisa menjalankan Nmap

2.11 Distributed Denial of Service (DDOS)

Distributed Denial of Service (DDOS) adalah jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber (resource) yang dimiliki.

2.12 Port Scanning

Port scanning adalah sebuah aktivitas untuk mendapatkan informasi yang menyeluruh mengenai status port (biasanya *port* TCP) pada sebuah host. Dengan port scanning, seseorang dapat mengetahui port-port mana saja yang terbuka pada sebuah host.


INSTITUT TEKNOLOGI NASIONAL
ITN
MALANG

BAB III
PERANCANGAN SISTEM

3.1 Identifikasi Masalah

Pada bab ini akan di jelaskan mengenai desain dan perancangan sistem intrusi, dan menjelaskan jaringan yang biasanya di tanam sistem intrusi atau *intrusion detection system*. Dalam sebuah jaringan DMZ *(Demilitarized Zone)* terdapat beberapa PC Server yang meliputi DNS Server, Mail Server, Database Server, FTP Server, Web Server serta beberapa perangkat lainnya. Desain juga meliputi perancangan web interface sebagai sistem monitoring.

3.2 Identifikasi Masalah Jaringan

Penempatan IDS pada lokasi untuk melindungi *demilitarized zone* (DMZ) yang meliputi Web Server, Mail Server, Database Server, SMTP Server, external DNS server dan host yang di akses oleh external user. Sensor *IDS* netwok tidak akan menganalisis lalu lintas jaringan jika tidak melewati zona yang dikontrol oleh suatu *IDS*, karena *IDS* juga mempunyai keterbatasan. Oleh karena itu setelah meletakkan sensor antara firewall dan router sebaiknya ditambahkan sensor pada DMZ.

Meletakkan sensor network untuk DMZ bisa di letakkan di belakang firewall dan bersebelahan dengan LAN. Karena sebuah jaringan DMZ berada di belakang firewall. Karena biasanua semua lalu lintas jaringan melintasi firewall. Sensor network harus bisa mengontrol konfigurasi firewall secara efisien sehingga serangan terhadap jaringan bisa dideteksi sebelum dan sesudah firewall.

Dengan penempatan seperti itu administrator bisa mengontrol semua lalu – lintas inbound dan outbound pada demilitarized zone, karena semua lalu lintas jaringan akan berputar pada segment LAN sebagai gateway jaringan.

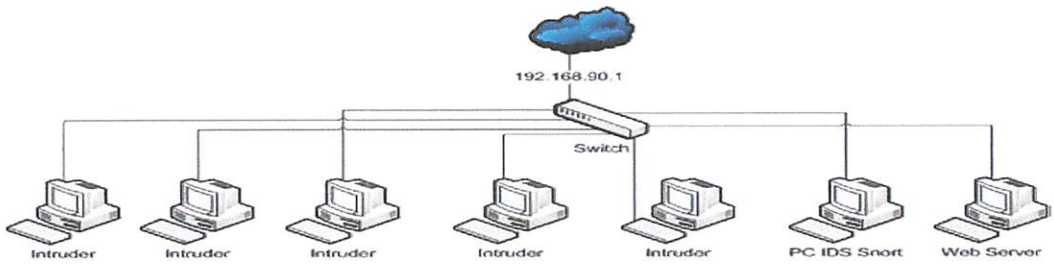
Proses mendeteksi intrusi, membutuhkan monitoring yang fleksibel. Yaitu dapat melakukan monitoring pendeteksian intrusi secara user friendly. Untuk mendukung hal tersebut di perlukan aplikasi yang bisa menampilkan hasil intrusi agar mudah di pahami dan lebih mendetail.

3.3 Prinsip Kerja Sistem

Dalam implementasi skripsi ini akan digunakan 1 laptop dan beberapa komputer yang dihubungkan dengan kabel LAN, pada laptop yang pertama akan di gunakan intruder. 1 komputer akan di install Sebagai Intrusion Detection System-Network based (NIDS). Sedangkan 1 komputer yang kedua sebagai webserver.

3.4 Perancangan Sistem

Gambar 3.1 merupakan rancangan sistem yang akan dibangun pada jaringan LAN



Gambar 3.1 Sistem intrusi dan monitoring pada jaringan LAN

Pada sisi server menggunakan sistem operasi LINUX, Ubuntu versi 12.04 yang akan bertindak sebagai webserver dan sebagai victim. Pada sisi komputer yang terinstall sistem intrusi dan laptop sebagai Intruder menggunakan sistem operasi LINUX Ubuntu 10.04. Kemudian IDS tersebut menjalankan sistem pendeteksi penyusup dan menampilkan hasil intrusi via web base. Sehingga dari hasil intrusi dapat di ambil tindakan sesuai serangan yang telah di terima oleh sistem.

3.4.1 Spesifikasi Hardware

a. Berikut spesifikasi PC yang di gunakan sebagai komputer IDS :
    1. *Processor* Intel(R) Pentium(R) CPUG630@2.70Ghz
    2. *Memory* 2 GB
    3. *Network Interface Card* 10/100 Mbits/s
    4. Sistem Operasi Linux Ubuntu 10.04

b. Berikut spesifikasi PC yang digunakan sebagai web server :

1. *Processor* Intel Pentium ® 4CPU 2.66GHz
2. *Memory* 1Gb
3. *Network Interface Card* 10/100 Mbits/s
4. Sistem Operasi Linux Ubuntu 12.04

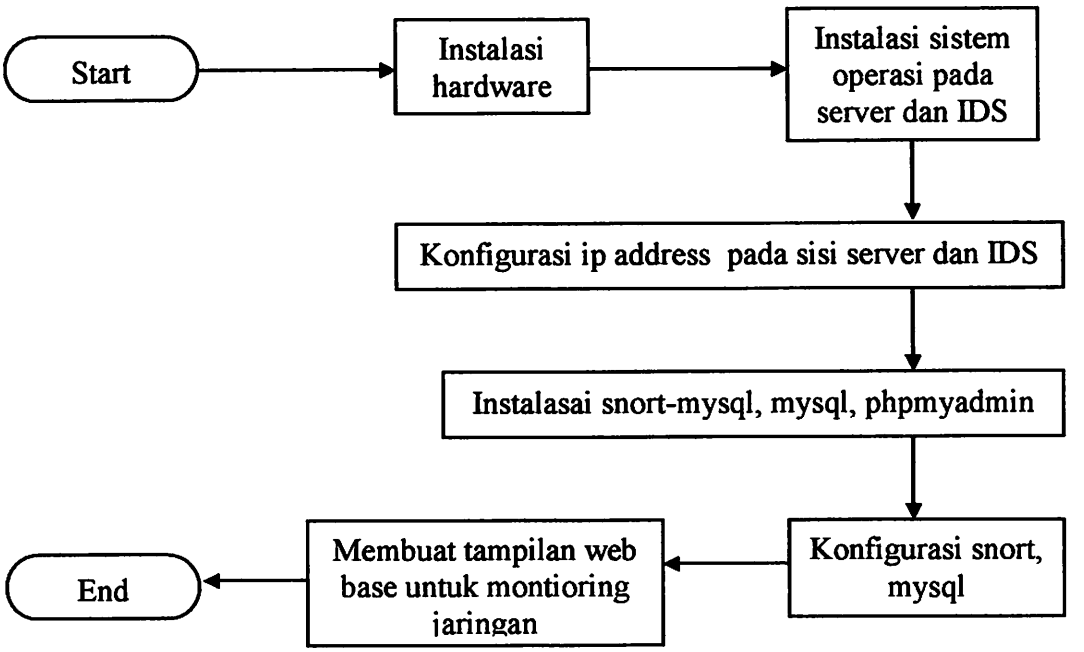
c. Berikut spesifikasi Laptop yang digunakan sebagai intruder :

1. *Processor* Intel(R) Pentium(R) Dual CPU T2390 1.86Ghz
2. *Memory* 1536Mb
3. *Network Interface Card* 10/100 Mbits/s
4. Sistem Operasi Linux Ubuntu 10.04

3.4.5 Spesifikasi Software

1. OS Linux Ubuntu 10.04
2. OS Linux Ubuntu 12.04
3. snort-mysql
4. snort-rules
5. snort-common-libraries
6. snort-common
7. oinkmaster
8. mysql
9. apache2
10. phpmyadmin
11. phpshell

3.5 Diagram Alir Rancang Bangun Sistem



Gambar 3.2 Diagram Alir Rancang Bangun Sistem Monitoring

Langkah pertama seperti yang dapat dilihat dalam gambar 3.2 yang dilakukan adalah instalasi perangkat keras *hardware* yang meliputi PC *server*, PC *client* dan NIC, hub sehingga tercipta sebuah jaringan yang mendukung sistem monitoring deteksi intrusi. Selanjutnya dilakukan instalasi sistem operasi (OS), dimana pada *server* menggunakan sistem operasi Linux Ubuntu 12.04 dan pada sisi *IDS* menggunakan Ubuntu 10.04. Kemudian melakukan konfigurasi IP Address pada *server* dan *IDS*. Selanjutnya langkah berikutnya instalasi pada sisi *IDS* dengan pengistalan aplikasi yang dibutuhkan untuk monitoring intrusi dan *web server.*

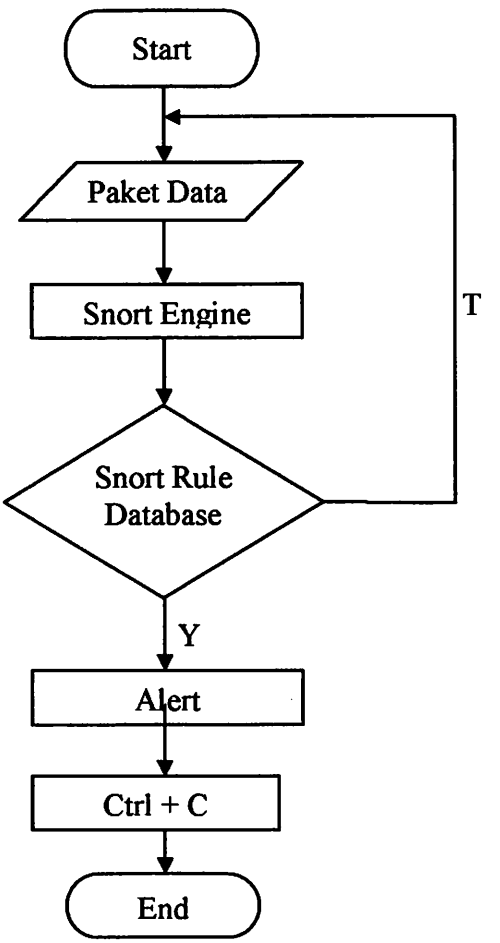
Pada web server sebuah server membutuhkan Apache, lalu diikuti instalasi PHP, *web-base* yang digunakan dibut menggunkan fungsi-fungsi PHP, lalu pengistalan MySQL dengan MySQL ini log data yang sudah disimpan pada database aplikasi snort dipindahkan ke database yang dibuat sendiri. Sehingga dapat dengan mudah mengambil data-data tersebut. Setelah penginstalan telah dilakukan dan tanpa error dilanjutkan melakukan konfiguras-konfigurasi yang diperlukan. Konfigurasi yang dilakukan meliputi konfigurasi awal Apache,

MySQL, Snort. Karena aplikasi tersebut tidak dapat bekerja apabila tanpa setting ulang sesuai kebutuhan. Setelah instalasi dan konfigurasi selesai, maka dilakukan pembuatan web interface untuk sistem monitoring jaringan. Pembuatan web tersebut disesuaikan dengan kebutuhan yang akan menampilkan data-data maupun gambar-gambar yang dihasilkan dari aplikasi monitoring sistem intrusi. Web juga mengambil data-data yang telah dipindahkan ke database web sendiri.

Langkah-langkah secara detail mengenai instalasi dan konfigurasi Snort, Linux, Apache, Sedangkan instalasi dan konfigurasi aplikasi monitoring deteksi intrusi dapat dilihat pada Lampiran.

3.6 Diagram alir Sistem IDS Snort

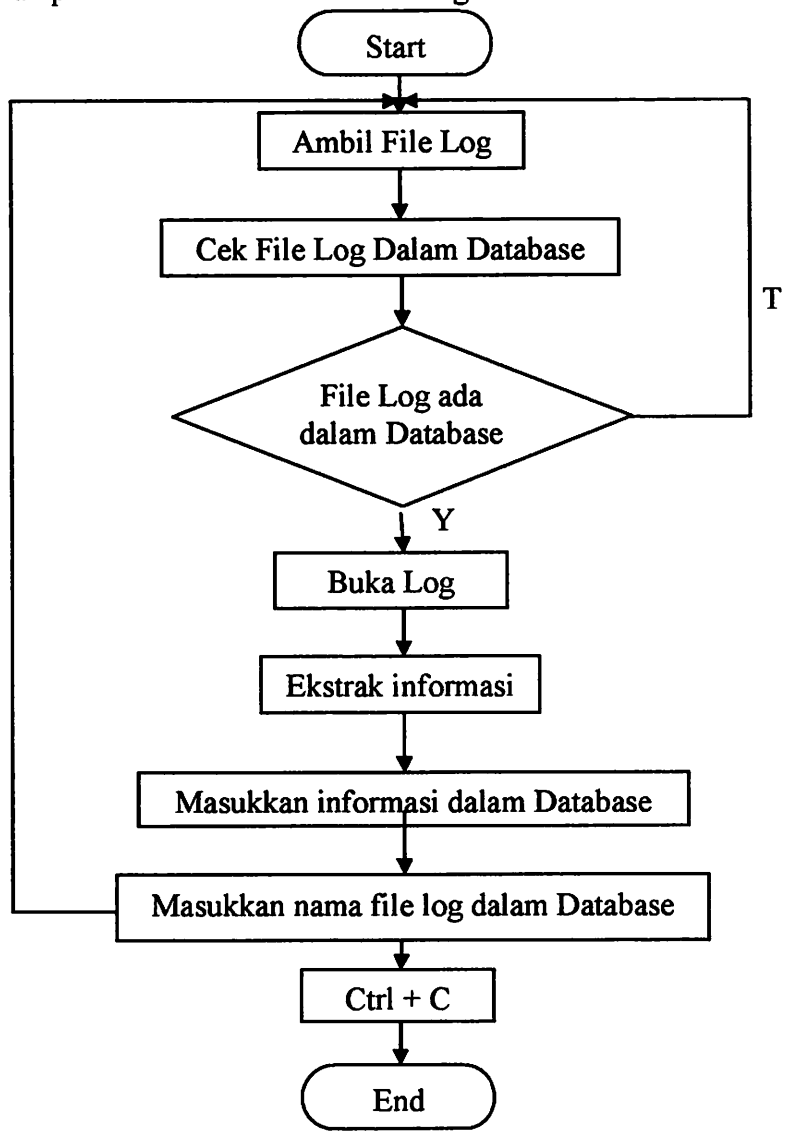
Gambar 3.3 akan menggambarkan cara kerja sistem IDS snort dalam mendeteksi intrusi dan menampilkan alert.



Gambar 3.3 Diagram alir sistem snort

3.7 Diagram Alir Sistem Olah Data

Berikut ini akan digambarkan cara sistem monitoring dalam memperolah data sampai menampilkan ke dalam web monitoring.



Gambar 3.4 Diagram alir sistem olah data

Langkah pengambilan data seperti dalam gambar 3.4 yaitu:

a. Mengkonfigurasi semua sistem deteksi intrusi

b. Setelah konfigurasi berhasil maka akan didapatkan data-data yang diinginkan yang tersimpan dalam tcpdump.log.xxx

c. Agar data-data tersebut dapat masuk ke dalam web monitoring dilakukan pemisahan data-data yang dapat dengan mudah dibaca

d. Karena data yang diambil dilakukan setiap detik dan membuat sistem terbebani maka dilakukan penjadwalan setiap 10 menit sekali.

e. Setelah dilakukan penjadwalan data yang diambil akan dimasukkan ke dalam database yang sudah dibuat pada sistem web monitoring.

f. Dan selanjutkan data dapat ditampilkan ke dalam web monitoring dan selanjutkan dapat melakukan monitoring.

3.8 Perancangan Perangkat (PC IDS)

Untuk membuat sistem deteksi intrusi dibutuhkan PC yang digunakan sebagai IDS. PC IDS yang akan dirancang adalah sebuah PC yang di install IDS Snort dilakukan pada sistem operasi Linux Ubuntu. Konfigurasi pembuatan PC IDS di Linux Ubuntu tergolong mudah. Karena hanya mensetting alamat IP address PC IDS. Peralatan yang digunakan dalam perancangan PC *IDS* ini adalah sebagai berikut:

Peralatan yang digunakan dalam perancangan PC *IDS* ini adalah sebagai berikut:

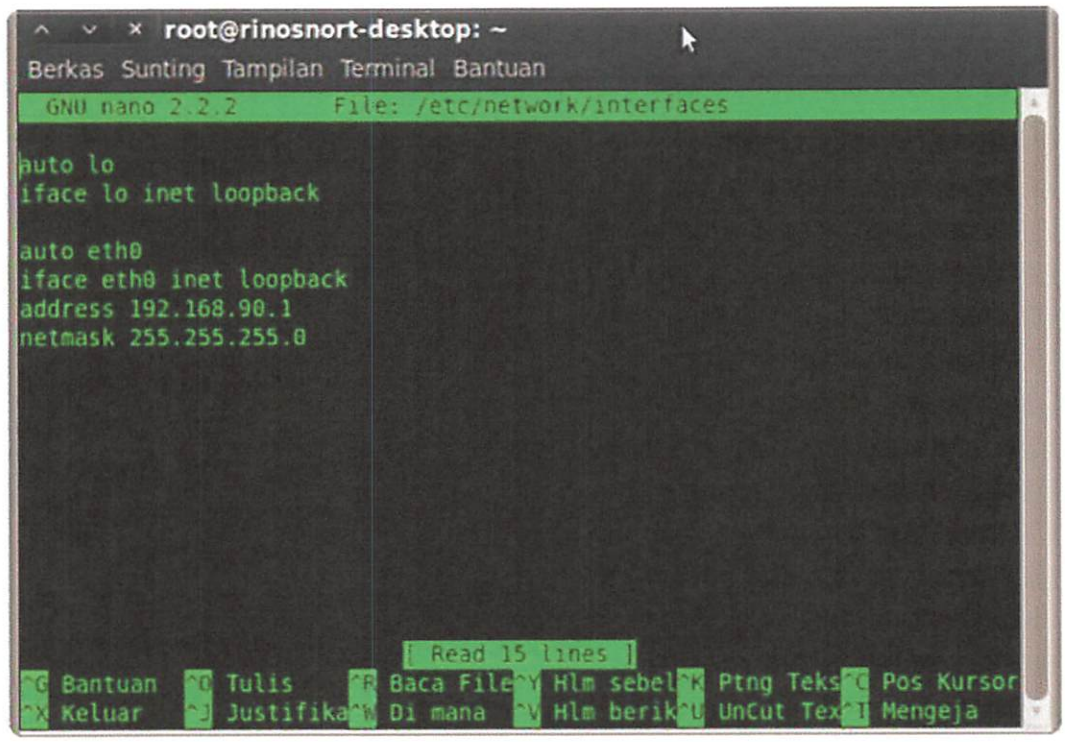
1. 1 buah *Ethernet card*
2. 1 buah *switch*

Berikut langkah-langkah membuat PC IDS

1. Konfigurasi kartu jaringan secara statik dengan mengkonfigurasi pada file /etc/network/interfaces seperti dalam gambar 3.5

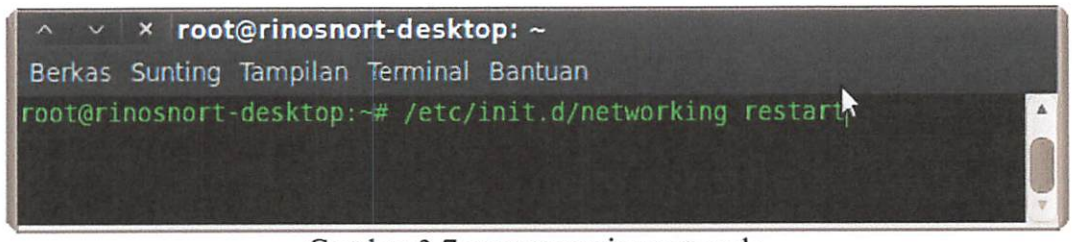
Gambar 3.5 nano

2. Konfigurasi IP statik seperti pada gambar 3.6 :



Gambar 3.6 konfigurasi IP statik

3. Selesai mengkonfigurasi, lakukan restart seperti gambar 3.7 :



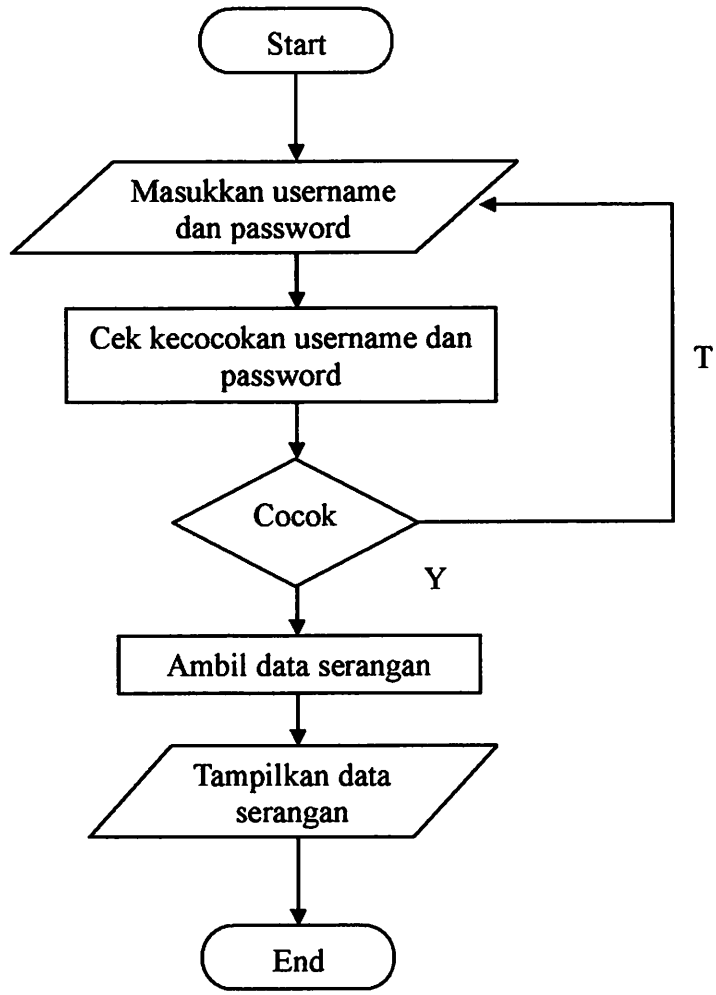
Gambar 3.7 restart service network

3.9 Perancangan Web Interface untuk Sistem Monitoring

Untuk kegiatan monitoring sistem deteksi intrusi, diperlukan suatu sarana untuk mempermudah administrasi jaringan dalam memonitoring jaringan. Web-base yang dibuat harus memiliki sifat *user friendly*, navigasi yang digunakan harus dapat dioperasikan secara mudah. Web tersebut dapat dioperasikan pada platform berbeda beda, serta dapat menampilkan segala macam informasi yang dibutuhkan.

3.9.1 Flowchart Sistem pada Web

Flowchart seperti terlihat pada gambar 3.8 menggambarkan alur pada sistem web ini. Menunjukkan langkah-langkah apa yang akan dilakukan sebuah administrator menggunakan web monitoring.



Gambar 3.8 Flowchart sistem web

Langkah menampilkan data serangan via web seperti pada gambar 3.8 :

a. Administrator memasukkan username dan password untuk agar bisa mengakses

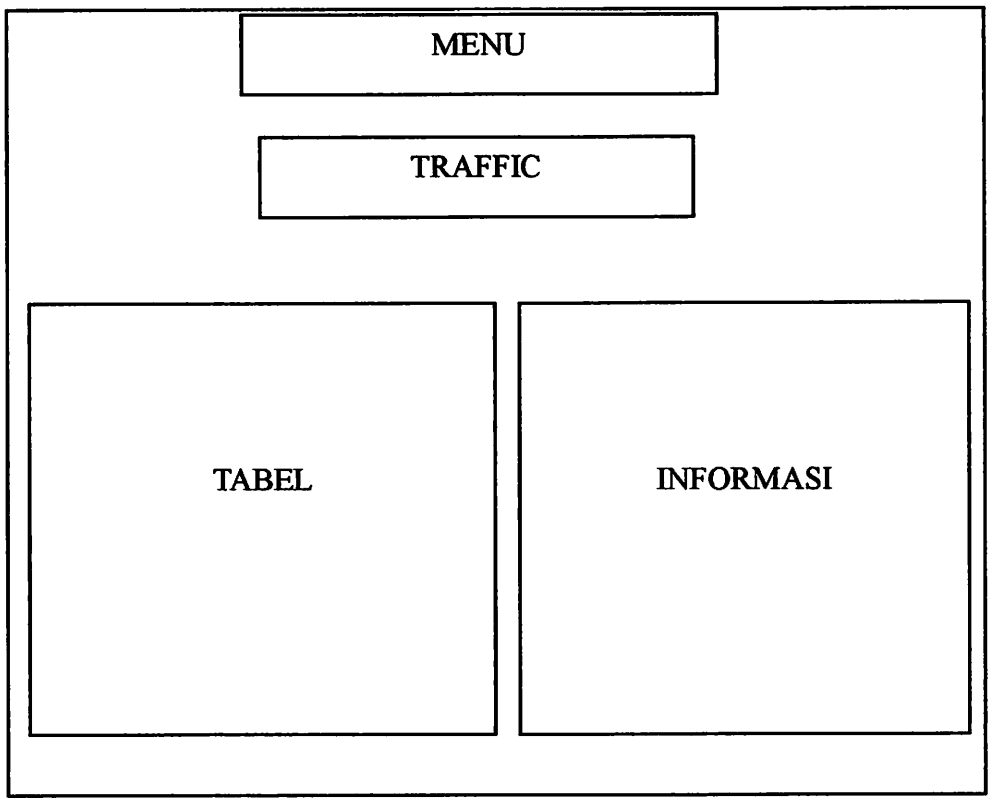
b. Jika username dan password cocok maka dilakukan pengambilan log dan menampilkan data serangan via interface web jika tidak cocok maka kembali ke halaman login

c. Akses Monitoring digunakan untuk menampilkan hasil-hasil monitoring yang didapat dari hasil intrusi. Hasil berupa , IP Address, Tanggal, Waktu, jenis serangan, port dan traffic serangan.

3.9.2 Desain Interface Web

Berikut ini merupakan desain dari *Interface* halaman aplikasi web yang terdiri dari beberapa komponen. Rancangan desain digunakan untuk seluruh halaman-halaman yang ada di web monitoring tersebut, yang membedakan hanya konten isinya. Web ini hanya digunakan untuk administrator jaringan.

Gambar 3.9 merupakan tampilan awal sistem monitoring berbasis web:



Gambar 3.9 Desain interface web


INSTITUT TEKNOLOGI NASIONAL
MALANG
ITN

BAB IV
IMPLEMENTASI DAN PENGUJIAN SISTEM

Setelah melakukan tahap perancangan sistem, maka tahap selanjutnya adalah tahap pengujian program monitoring interface web dan hasil konfigurasi rancang bangun IDS. Pengujian ini bertujuan untuk mengimplementasikan rancangan yang telah di bangun. Hasil implementasi tersebut adalah sebagai berikut :

4.1 Persiapan Lingkungan Implementasi sistem

Sebelum implementasi sistem monitoring penyusup dapat dilakukan, maka perlu disiapkan lingkungan yang mendukung pengembangan sistem
Pada komputer IDS memerlukan perangkat pendukung yaitu:

1. LAN Card
2. Kabel UTP

Pada komputer yang dipergunakan sebagai IDS telah ter-install:

1. Sistem Operasi Linux yaitu Ubuntu 10.04,
2. Web server dan telah dikonfigurasi untuk mendukung pemrograman web.
   Ada beberapa element yang harus ada dalam penginstallan yaitu :
   1. Apache2
   2. MySQL
   3. PHPMyAdmin
   4. Php5
   5. Snort
3. Sistem pendeteksi penyusup, Snort digunakan untuk mendeteksi sebuah intrusi dan menampilkan data intrusi.

Pada komputer yang dipergunakan sebagai target telah ter-install :

1. Sistem Operasi Linux yaitu Ubuntu 12.04
2. Web Server dan telah dikonfigurasi untuk sharing repository.

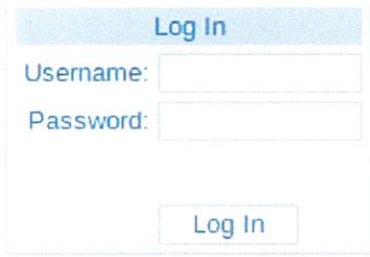
Pada komputer yang dipergunakan sebagai intruder telah ter-install :

1. Sistem Operasi Linux yaitu Ubuntu 10.04
2. Nmap untuk melakukan port scanning
3. Script untuk melakukan DDOS

4.2 Implementasi Tampilan Web Monitoring

Dari rancangan yang telah dibuat pada bab perancangan, maka tahap selanjutnya yaitu mengimplementasikan menjadi sebuah tampilan. Terdapat beberapa element dari web monitoring.

4.2.1 Halaman Login



Gambar 4.1 Halaman login

Sebelum dapat mengakses bagian inti dari web monitoring, administrator jaringan diharuskan login kedalam web monitoring tersebut. Gambar 4.1 merupakan halaman login admin. Dalam halaman tersebut admin dapat memonitoring hasil intrusi.

Form yang terdapat di halaman login adalah:

a. *Username*, digunakan sebagai identitas berupa karakter.
b. *Password*, digunakan sebagai kata kunci dari identitas yang terjaga kerahasiannya terhadap orang lain.

Berikut ini merupakan listing program untuk otentikasi halaman web monitoring:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">
<title>Untitled Page</title>
<meta name="generator" content="WYSIWYG Web Builder 8 -
http://www.wysiwygwebbuilder.com">
<style type="text/css">
body
{
  background-color: #FFFFFF;
  color: #000000;
}
</style>
<style type="text/css">
p, span, div, ol, ul, li, td, button, input, textarea, form
{
  margin: 0;
  padding: 0;
}
a
{
  color: #C8D7EB;
  outline: none;
  text-decoration: underline;
}
a:visited
{
  color: #C8D7EB;
}
a:active
```

```
{
  color: #C8D7EB;
}
a:hover
{
  color: #376BAD;
  text-decoration: underline;
}
</style>
<style type="text/css">
.loginform_table
{
  background-color: #EDF2F8;
  border-color:#BBCEE6;
  border-width:1px;
  border-style: solid;
  color: #376BAD;
  border-spacing: 4px;
  font-family: Arial;
  font-size: 13px;
  text-align: right;
}
.loginform_header
{
  background-color: #BBCEE6;
  color: #376BAD;
  text-align: center;
}
.loginform_text
{
  background-color: #FFFFFF;
  border-color: #BBCEE6;
```

```
  border-width: 1px;
  border-style: solid;
  color: #376BAD;
  font-family: Arial;
  font-size: 13px;
}
.loginform_button
{
  background-color: #FFFFFF;
  border-color: #BBCEE6;
  border-width: 1px;
  border-style: solid;
  color: #376BAD;
  font-family: Arial;
  font-size: 13px;
}
</style>
</head>
<body>
<a href="http://www.wysiwygwebbuilder.com" target="_blank"><img
src="images/builtwithwwb8.gif" alt="WYSIWYG Web Builder"
style="position:absolute;left:453px;top:735px;width:88px;height:31px;border-
width:0;z-index:250"></a>
<div id="wb_Login1"
style="position:absolute;left:3px;top:0px;width:183px;height:129px;text-
align:right;z-index:1;padding:0;">
<form name="loginform" method="post" action="" id="loginform">
<input type="hidden" name="form_name" value="loginform">
<table class="loginform_table" style="width:183px;height:129px;">
<tr>
  <td class="loginform_header" colspan="2" style="height:19px;">Log In</td>
</tr>
```

```
<tr>
  <td style="height:20px;width:69px">Username:</td>
  <td style="text-align:left"><input class="loginform_text" name="username"
type="text" id="username" style="width:100px;height:18px;"></td>
</tr>
<tr>
  <td style="height:20px">Password:</td>
  <td style="text-align:left"><input class="loginform_text" name="password"
type="password" id="password" style="width:100px;height:18px;"></td>
</tr>

<tr>
  <td> </td><td style="text-align:left;vertical-align:bottom"><input
class="loginform_button" type="submit" name="login" value="Log In"
id="login" style="width:70px;height:20px;"></td>
</tr>
</table>
</form>
</div>
<?
    if(isset($_POST['username']) && isset($_POST['password'])){
        include "../konfigurasi.php";
        if($_POST['username']==$user && $_POST['password']==$password){
            header("location: ../view.php");
            session_start();
            $_SESSION['login']="true";
        }
    }
?>
</body>
</html>
```

4.2.2 Halaman Monitoring

Gambar 4.2 Halaman monitoring

Dalam halaman monitoring proses yang berlangsung secara otomatis sesuai dengan data yang sudah data. Pada awal mula halaman akan kosong seperti dalam gambar 4.2

Hasil monitoring menampilkan semua data yang tertangkap oleh IDS Snort. Dan tampil sesuai tabel yang tersedia.

Isi dalam tabel yang terdapat dalam halaman ini adalah:

a. Time : Menampilkan waktu tanggal bulan dan tahun serangan

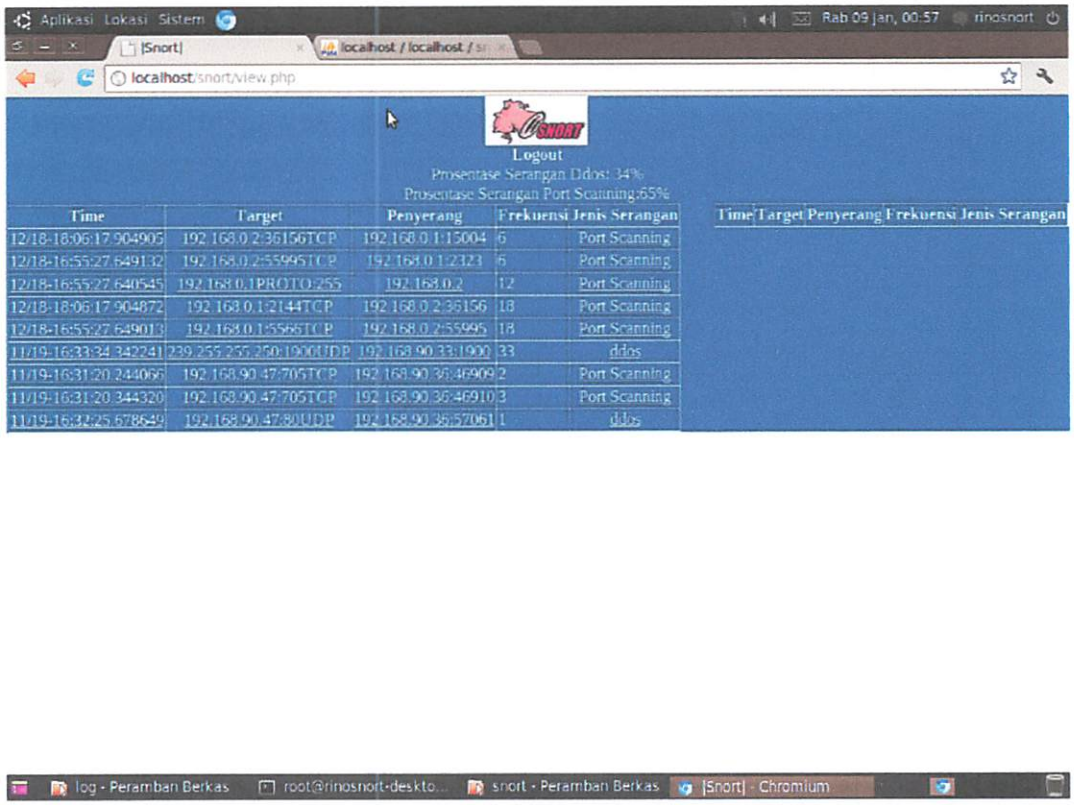
b. Target : Menampilkan IP yang di serang

c. Penyerang : Menampilkan IP intruder

d. Frekuensi : Menampilkan jumlah serangan

e. Jenis Serangan: Menampilkan jenis serangan.

Setelah semua data log serangan diisikan maka akan ditampilkan dalam sebuah tabel. Saat tabel di tampilkan juga langsung dapat dilihat jenis serangan dan alamat IP penyerang yang dapat dilihat pada gambar 4.3.



Gambar 4.3 Hasil Intrusi

Berikut ini merupakan listing program untuk menampilkan hasil intrusi :

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<html>
<head>
        <title>|Snort|</title>

        <?
        session_start();
        if($_SESSION['login']!="true"){
                header("location: login/index.php");
```

```
        }
        $tersambung=mysql_connect("localhost","root","r1n0l4r45");        //login
database
        $tersambungDb=mysql_select_db("snortInfo",$tersambung);//sambung
database
        ?>
</head>

<body style="padding:0px;margin: 0px;">

<div style=" float: left;width: 100%;background: #376488">
        <?
        $ddos=mysql_num_rows(mysql_query("select * from dataAttack where
jenisSerangan='ddos'"));
        $portScan=mysql_num_rows(mysql_query("select * from dataAttack
where jenisSerangan='Port Scanning'"));
        $total=$ddos+$portScan;
        $prosenDdos=floor($ddos/$total*100);
        $prosenPortScan=floor($portScan/$total*100);
        //$prosenPortScan=(($total/100)*$portScan)*100;
        echo "<center style='color:white'><img width=100px
src='logo.jpg'><br><a style='color:white;text-decoration:none'
href='logout.php'><b>Logout</b></a><div>Prosentase Serangan Ddos:
".$prosenDdos."%<br>"."Prosentase Serangan Port
Scanning:".$prosenPortScan."%"."</div></center>";
        ?>
        <div style="margin-left:1;margin-right:auto">
    <table border=1 style="float:left;border: white;color: white;border-
collapse:collapse">
        <tr>
          <td>
            <center><b>Time</b></center>
```

```
        </td>
        <td>
          <center><b>Target</b></center>
        </td>
        <td>
          <center><b>Penyerang</b></center>
        </td>
        <td>
          <center><b>Frekuensi</b></center>
        </td>
        <td>
          <center><b>Jenis Serangan</b></center>
        </td>
      </tr>
      <?
            //echo "select time,ipTarget,ipAsal,count(ipAsal) as
jumlahSerangan,jenisSerangan from dataAttack group by ipAsal";
        $res=mysql_query("select time,ipTarget,ipAsal,count(ipAsal) as
jumlahSerangan,jenisSerangan from dataAttack group by ipAsal") or die
(mysql_error()); // query untuk mengumpulkan data serangan
        while($data=mysql_fetch_array($res)){
          $time=$data['time']; // ambil data waktu
          $target=$data['ipTarget']; //ambil target
          $asal=$data['ipAsal'];// ambil penyerang
          $frek=$data['jumlahSerangan'];//frekuensi serangan
          $jenis=$data['jenisSerangan'];//ambil jenis serangan
              $timePetik="'$time'";
              $targetPetik="'".$target."'";
              $asalPetik="'$asal'";
              $jenisPetik="'$jenis'";
          echo " <tr>
        <td>
```

```
            <center><a                                    style='color:white'
href='?kolom=time&val=$time'>$time</a></center>
            </td>
            <td>
              <center><a                                  style='color:white'
href='?kolom=ipTarget&val=$target'>$target</a></center>
            </td>
            <td>
              <center><a                                  style='color:white'
href='?kolom=ipAsal&val=$asal'>$asal</a></center>
            </td>
            <td>
              $frek
            </td>
            <td>
              <center><a                                  style='color:white'
href='?kolom=jenisSerangan&val=$jenis'>$jenis</a></center>
            </td>
          </tr>";
            }
          ?>

      </table>

<table     border=1     style="float:right;border:     white;color:     white;border-
collapse:collapse">
          <tr>
            <td>
              <center><b>Time</b></center>
            </td>
            <td>
              <center><b>Target</b></center>
```

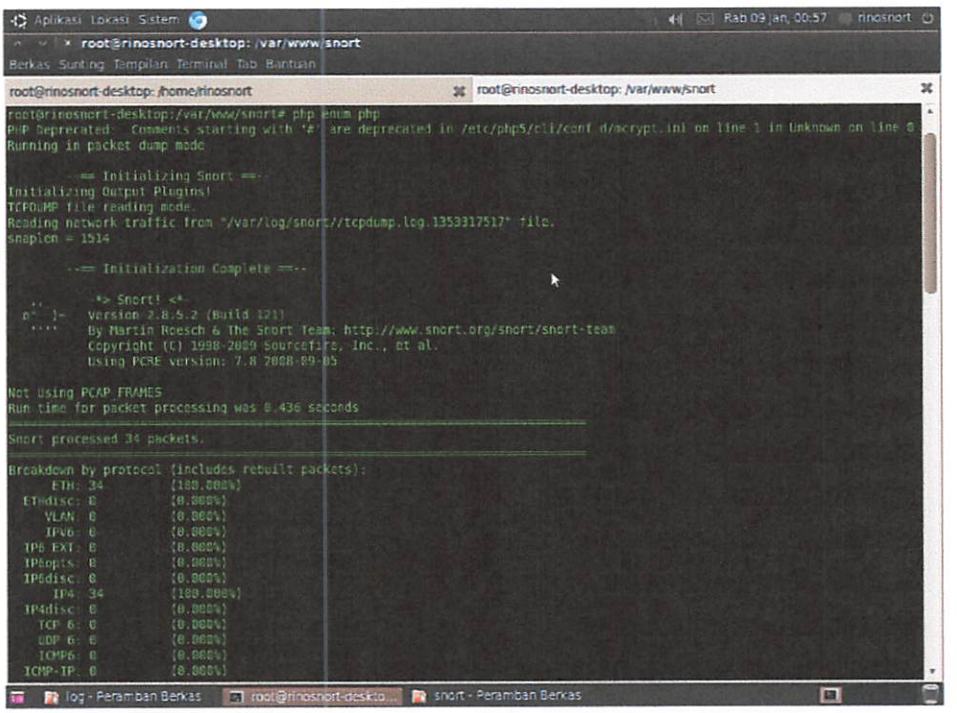
```
        </td>
        <td>
          <center><b>Penyerang</b></center>
        </td>
        <td>
          <center><b>Frekuensi</b></center>
        </td>
        <td>
          <center><b>Jenis Serangan</b></center>
        </td>
      </tr>
      <?
      $kolom=$_GET['kolom'];
      $val=$_GET['val'];

      $query=mysql_query("select * from dataAttack where $kolom='$val'");
      while($data=mysql_fetch_array($query)){
            $time=$data['time']; // ambil data waktu
        $target=$data['ipTarget']; //ambil target
        $asal=$data['ipAsal'];// ambil penyerang
        //$frek=$data['jumlahSerangan'];//frekuensi serangan
        $jenis=$data['jenisSerangan'];//ambil jenis serangan
            echo " <tr>
        <td>
          <center><a                                    style='color:white'
href='?kolom=time&val=$time'>$time</a></center>
        </td>
        <td>
          <center><a                                    style='color:white'
href='?kolom=ipTarget&val=$target'>$target</a></center>
        </td>
        <td>
```

```
            <center><a                                    style='color:white'
href='?kolom=ipAsal&val=$asal'>$asal</a></center>
            </td>
            <td>
              $frek
            </td>
            <td>
              <center><a                                  style='color:white'
href='?kolom=jenisSerangan&val=$jenis'>$jenis</a></center>
            </td>
          </tr>";

          }

          ?>
<?php

?>
</table>
          </div>
</body>
</html>
```

4.2.3 Input Data Log

Untuk menampilkan data intrusi di dalam halaman monitoring perlu di lakukan input data log kedalam database, dan dilakukan enumerasi yaitu mengumpulkan data log snort dan dimasukan kedalam database yang sudah dibuat.

Proses enumerasi seperti pada gambar 4.4 :



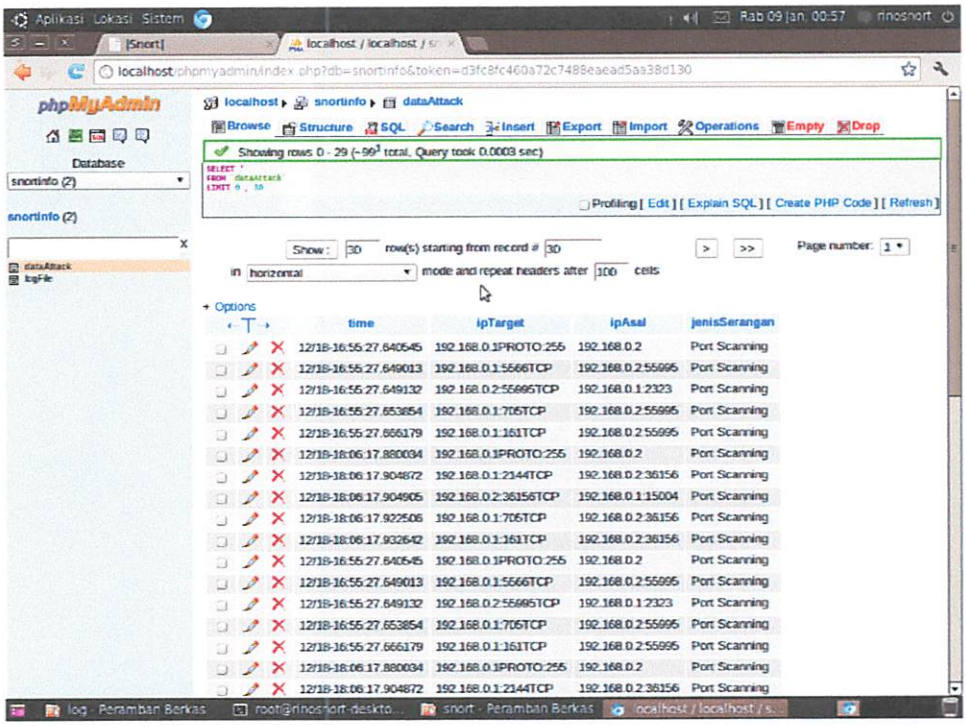
Gambar 4.4 Proses enumerasi

Berikut ini merupakan listing program untuk memasukkan data log kedalam database :

```
<?php
include "index.php";
$folderLog="/var/log/snort/";
$tersambung=mysql_connect("localhost","root","r1n0l4r45");
$tersambungDb=mysql_select_db("snortInfo",$tersambung);
while(true){
    if ($handle = opendir($folderLog)) {
        while (false !== ($entry = readdir($handle))) {
            if(substr($entry,0,3)=="tcp"){
                $kueri=mysql_query("select * from logFile where name='$entry'");
                $jumlahFileMysql= mysql_num_rows($kueri);
                if($jumlahFileMysql==0){
                //pengolahan Data
```

```
                    olahData($folderLog,$entry);
                    mysql_query("insert into logFile values('$entry')");
                }
            }
        }

        closedir($handle);
    }
}
?>
```

Setelah di lakukan proses enumerasi dicek ke dalam database apakah data log sudah masuk ke database seperti gambar 4.5 :

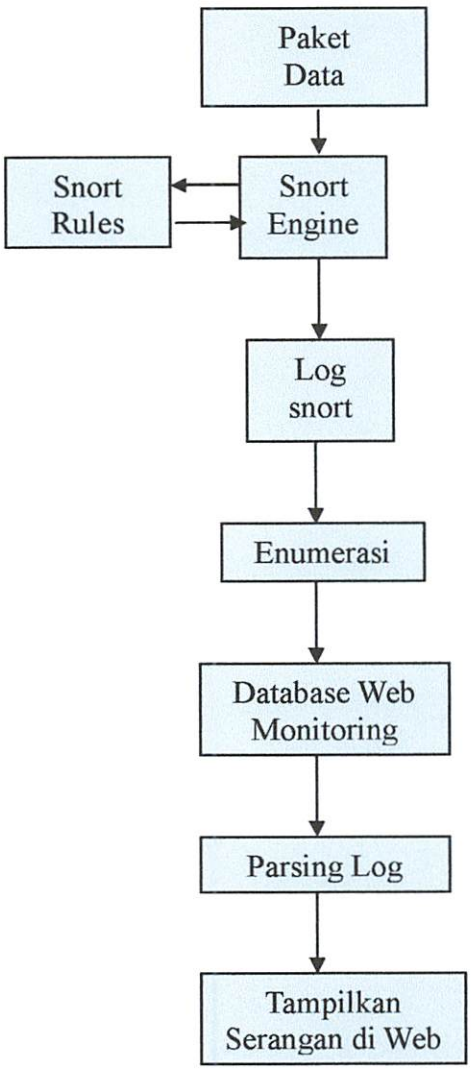


Gambar 4.5 Hasil proses enumerasi

4.3 Pengujian Sistem

Pengujian sistem dibagi menjadi 2. Yang pertama adalah dilakukan *port scanning* untuk mengetahui port yang terbuka, yang kedua dilakukan serangan *DDOS*. Pengujian dilakukan dengan menggunakan 5 intruder dengan IP yang berdeda masing – masing intruder melakukan dua serangan yaitu port scanning dan ddos. Kenapa menggunakan serangan *port scanning* terlebih dahulu, karena awal dari sebuah serangan atau proses hacking adalah dengan mengetahui port – port yang terbuka, setelah mengetahui port yang terbuka baru bisa dilakukan serangan selanjutny. Serangan selanjutnya kali ini yaitu dengan teknik *DDOS*.

4.3.1 Alur Pengujian



Gambar 4.6 Alur Pengujian Sistem

Seperti alur pada gambar 4.6 yaitu paket data yang masuk akan di deteksi oleh snort lalu snort engine mencocokan dengan rule snort jika rule cocok maka dianggap sebagai serangan dan log serangan snort tersimpan di directory /var/log/snort/, maka dilakukan proses enumerasi yaitu mengumpulkan dan memasukkan data log ke database web monitoring selanjutnya dilakukan parsing lalu hasil parsing di tampilkan di web untuk melihat hasil serangan.

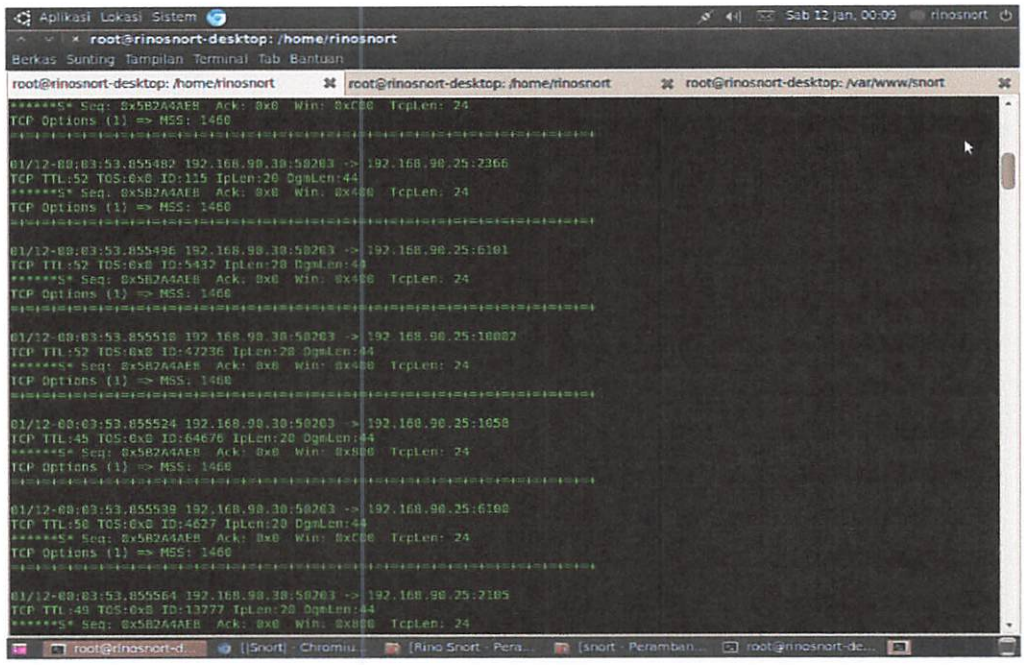
a. Port Scanning

Pengujian dengan cara port scanning dilakukan menggunakan dan memanfaakan utilitas aplikasi nmap yang sudah diinstall di komputer yang digunakan sebagai intruder. Karena menggunakan Operating System Ubuntu maka pengujian lewat terminal atau command prompt seperti pada gambar 4.7 :

```
~# nmP -sS 192.168.90.25
```

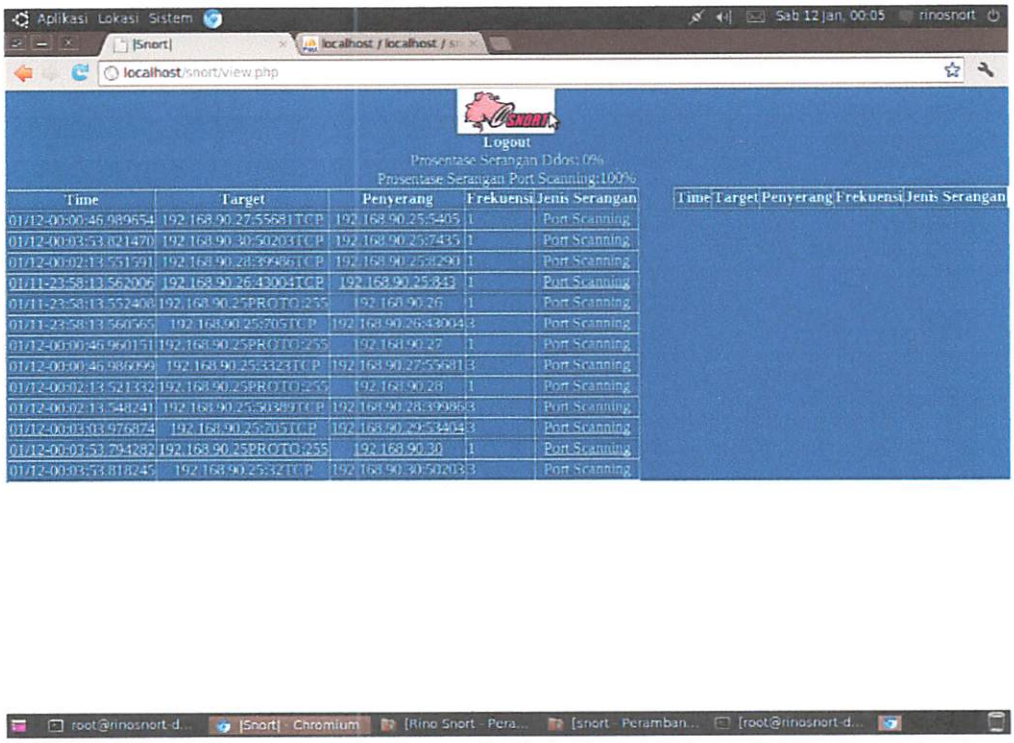
Gambar 4.7 Perintah menggunakan Nmap

IDS Snort akan menampilkan hasil intrusi port scanning via terminal atau command prompt seperti gambar 4.8 :



Gambar 4.8 Hasil intrusi port scanning di Snort

Hasil intrusi yang ditampilkan di snort sulit di baca karena muncul di terminal dan bergerak cepat dan jumlah data yang banyak. Pengamatan di lakukan menggunakan web browser google chrome. Maka untuk mempermudah pembacaan ditampilkan via web seperti pada gambar 4.9 :



Gambar 4.9 Tampilan serangan port scanning

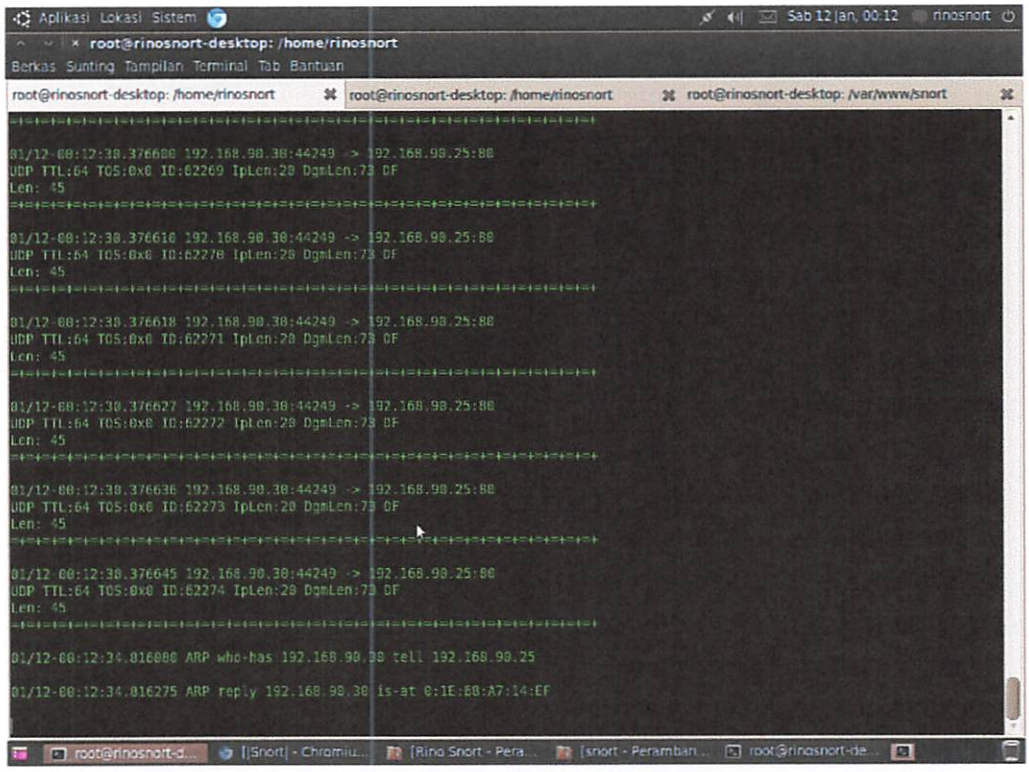
b. DDOS

Pengujian menggunakan DDOS dengan memanfaatkan sebuah script DDOS yang dibuat dengan menggunakan bahasa pemrograman C. Dan di jalankan lewat terminal atau command prompt pada gambar 4.10 :

```
~# ./tembak 192.168.90.25 80
```

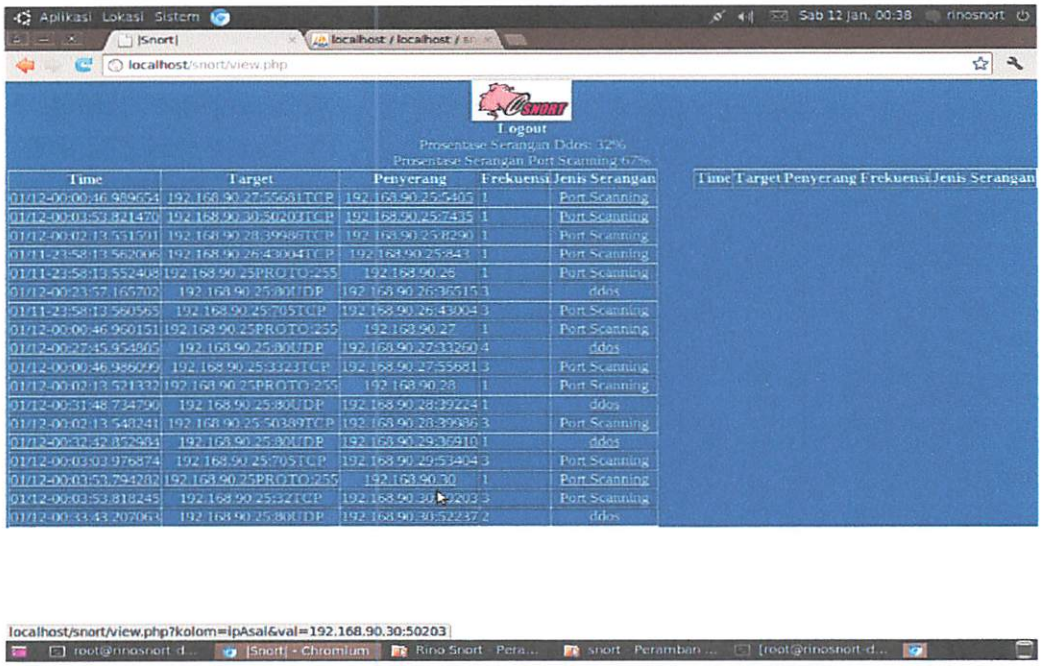
Gambar 4.10 Perintah DDOS

Angka 80 adalah port yang dituju, karena yang diserang adalah web server sedangkan port 80 adalah untuk protokol HTTP. Seperti yang di tunjukkan pada gambar 4.11 :



Gambar 4.11 Hasil intrusi DDOS

Hasil intrusi maka ditampilkan via web seperti pada gambar 4.12 :



Gambar 4.12 Tampilan serangan DDOS

Pada gambar 4.9 dan 4.12 adalah tampilan monitoring dari sistem IDS Snort sendiri dan pada gambar 4.9 dan 4.12 merupakan tampilan monitoring web yang dibuat dan ditujukan untuk mempermudah pembacaan sebuah intrusi. Dari hasil monitoring tersebut bisa dilakukan pencegahan sesuai serangan yang terdeteksi oleh sistem IDS yaitu Snort.

4.4 Hasil Pengujian Sistem

Berdasarkan pengujian yang telah di lakukan sesuai dengan langkah – langkah pengujian sistem didapatkan hasil pengujian pada tabel 4.1 :

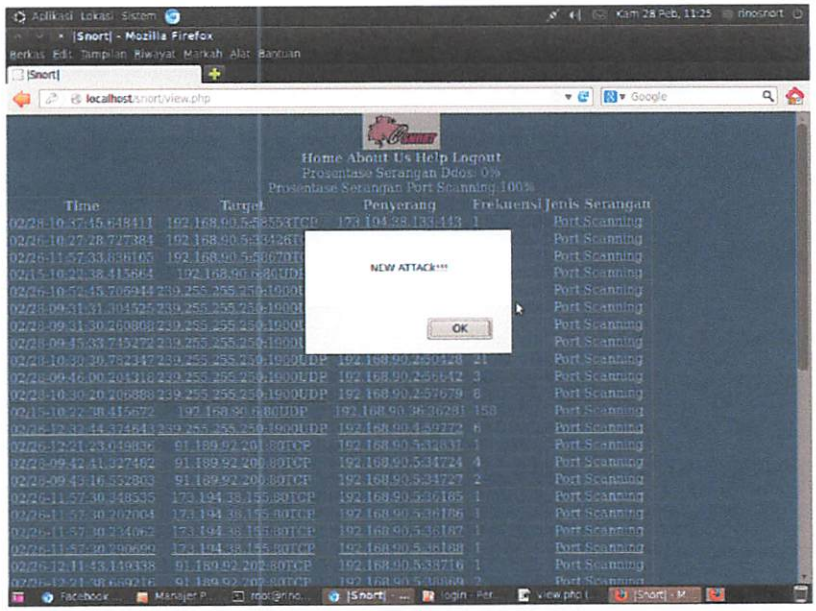
Tabel 4.1 Hasil Pengujian

NO	IP Address	Serangan	Status Serangan
1.	192.168.90.26	PortScanning	Terdeteksi
		DDOS	Terdeteksi
2.	192.168.90.27	PortScanning	Terdeteksi
		DDOS	Terdeteksi
3.	192.168.90.28	PortScanning	Terdeteksi
		DDOS	Terdeteksi
4.	192.168.90.29	PortScanning	Terdeteksi
		DDOS	Terdeteksi
5.	192.168.90..30	PortScanning	Terdeteksi
		DDOS	Terdeteksi

Dari tabel 4.1 didapatkan hasil pengujian yang mengacu pada gambar 4.9 dan 4.12, pengujian tersebut melibatkan 5 intruder dengan IP address yang berbeda dan masing – masing intruder melakukan dua serangan yaitu serangan pertama *Port Scanning* dan serangan kedua *DDOS*, hasil pengujian tersebut berhasil 100 %. Perhitungan persentase status serangan dari 5 komputer (penyerang) adalah 5/5 x 100% = 100 %.

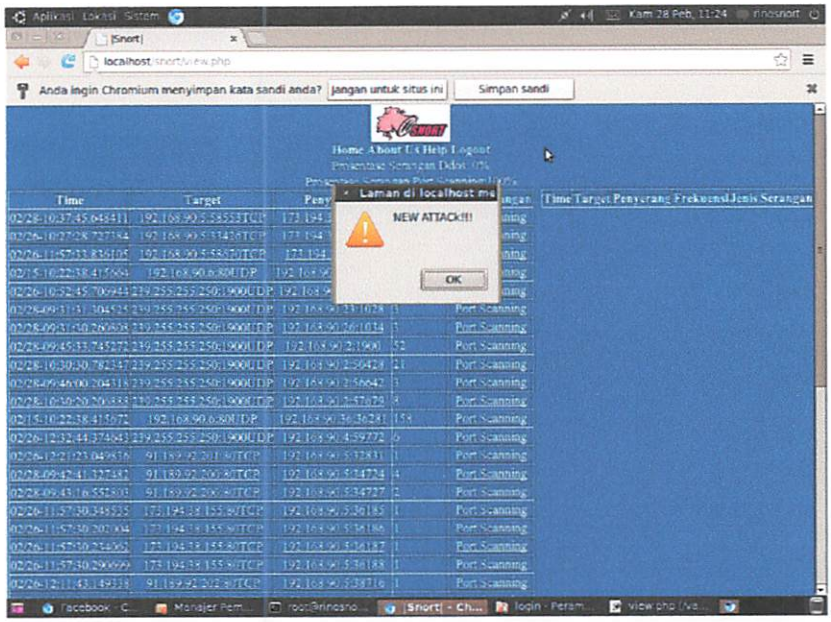
4.5 Hasil Pengujian di Browser

a. Mozilla Firefox



Gambar 4.13 Pengujian di browser Mozilla Firefox

b. Google Chrome



Gambar 4.14 Pengujian di browser Google Chrome

Dari hasil pengujian di kedua browser pada gambar 4.13 dan gambar 4.14 dihasilkan hasil pengujian di browser google chrome tampilan nya lebih baik.


INSTITUT TEKNOLOGI NASIONAL
MALANG
ITN

BAB V
PENUTUP

5.1 Kesimpulan

Dari hasil perancangan dan pengujian sistem Desain dan Implementasi Intrusion Detection System (IDS) berbasis Linux pada jaringan LAN dapat disimpulkan bahwa :

1. IDS snort dapat mendeteksi banyak serangan seperti DDOS dan Port scanning.
2. Paket data yang dianggap serangan tersimpan di log dan digunakan untuk melakukan monitoring sistem melalui web.
3. Sistem monitoring bisa melakukan monitoring dengan cukup baik, saat dilakukan pengujian hasilnya 100%, karena dari semua pengujian berhasil terdeteksi semua.
4. Snort dapat di implementasikan dengan 1 blok alamat jaringan atau beberapa IP address.

5.2 Saran

Ada beberapa saran yang disampaikan berkaitan implementasi IDS sebagai berikut :

1. Rule snort yang digunakan merupakan rule snort default, rule snort bisa dikonfigurasi sesuai kebutuhan untuk mengidentifikasi bermacam - macam serangan .
2. Aplikasi sistem web monitoring perlu dikembangkan kearah tampilan yang lebih segar dan ditambahkan menu seperti traffic protocol dan graph alert
3. Perlu ditambahkan menu untuk mengetahui jenis Operating System intruder.


INSTITUT TEKNOLOGI NASIONAL
ITN
MALANG

DAFTAR PUSTAKA

1. M.kom,Dony Ariyus, 2007 " *Instrusion Detection System* ", Penerbit Andi, Yogyakarta.
2. Rahmat Rafiudin, 2010 " *Mengganyang Hacker Dengan Snort* ", Penerbit Andi, Yogyakarta.
3. http://id.wikipedia.org/wiki/Nmap diakses tanggal 07 November 2012
4. Anggiat, Yogha, Gareca, 2011 " *Tutorial-IDS-menggunakan-Snort-danAcidbase.pdf* ", Indonesia.
5. http://id.wikipedia.org/wiki/MySql diakses tanggal 07 November 2012
6. http://id.wikipedia.org/wiki/Apache_HTTP_Server diakses tanggal 07 November 2012
7. http://id.wikipedia.org/wiki/Phpmyadmin diakses tanggal 07 November 2012


INSTITUT TEKNOLOGI NASIONAL
MALANG
ITN

LAMPIRAN

Langkah – langkah menginstall snort

1. apt-get install snort
2. Tekan **Any** dan **OK**
3. Tekan **OK**
4. Set up a database tekan **NO**

Masuk MySQL

1. Ketik : **mysql –u root –p** lalu masukkan password user root **r1n0l4r45**
2. Ketik : create database snort;
3. Ketik : **grant all on snort.* to snortuser@localhost identified by 'r1n0l4r45'**
4. Ketik : **flush privileges;**
5. Ketik : **Exit**

Mengimpor table ke dalam MySQL

1. Ketikkan : **mysql –u snortuser –p** (untuk password masukkan **r1n0l4r45**) <- masuk mysql menggunakan user yang bernama **snortuser**
2. Ketik : **show databases;**
3. Ketik : **use snort;**
4. Ketik : **show tables;**
5. Ketik : **exit**

Konfigurasi SNORT

1. Ketik : **pico /etc/snort/snort.conf**
2. Gunakan search yaitu **CTRL+W** lalu ketikkan **dbstart**
3. Diantara **(#DBSTART#)** dan **(#DBBEND#)**, ketik : **output database: log, mysql, user=snortuser password=r1n0l4r45 dbname=snort host=localhost**
4. Masih di file yang sama, search kata-> **redalert** Hilangkan tanda comment **(#)** dari bagian **ruletype redalert{}** Ganti bagian **output**

database dari **ruletype redalert{}** dengan : **output database: log, mysql, user=snortuser password=r1n0l4r45 dbname=snort host=localhost**

5. Save dan exit
6. Jalankan Snort dengan perintah : **snort –u snort –c /etc/snort/snort.conf**
7. Tekan **CTRL + C** untuk mengakhiri
8. Buka file crontab dan edit Ketik : **pico /etc/crontab** tambahkan perintah dibawah ini di baris paling akhir. ketikkan : **@reboot root snort -u snort -c /etc/snort/snort.conf >> /dev/null**
9. **Reboot** lagi, maka pesan error tetap akan tampil ketik : **rm /etc/snort/db-pending-config**
10. Ketik : **pico /etc/default/snort,** pada bagian paling bawah, ubah nilai bagian ALLOW_UNAVAILABLE dari **no** menjadi **yes**
11. Save dan Exit
12. Ketik : **pico /etc/snort/snort.conf** cari bagian **eth0** di (var HOME_NET **$eth0**_ADDRESS) hilangkan tanda comment (#).
13. Ketik : **dpkg –configure –pending**
14. Ketik : **dpkg-reconfigure snort-mysql**
15. Pilih **Boot** lalu **Ok**
16. Pilih **Ok**
17. Kalau muncul **eth0** langsung **Ok**
18. Tekan **Any**
19. Disable pilih **No** dan Testing pilih **No**
20. Selanjutnya biarkan kosong
21. Email pilih **No** selanjutnya pilih **Ok**
22. Set up a database pilih **No**

INSTITUT TEKNOLOGI NASIONAL MALANG
Fakultas Teknologi Industri
Program Studi Teknik Informatika S1
Jl. Raya Karanglo Km. 2 Malang

BERITA ACARA UJIAN SKRIPSI
FAKULTAS TEKNOLOGI INDUSTRI

Nama : Rino Jiwandanu
NIM : 08.18.902
Jurusan : Teknik Informatika S-1
Judul : Desain Dan Implementasi Intrusion Detection System Berbasis Linux Pada Jaringan LAN

Dipertahankan dihadapan Majelis Penguji Skripsi Jenjang Strata Satu (S-1) pada :
Hari : Jumat
Tanggal : 15 Februari 2013
Nilai : 89,73(A)

Panitia Ujian Skripsi :

Ketua Majelis Penguji

Joseph Dedy Irawan, ST., MT.
NIP. 197404162005011002

Anggota Penguji :

Dosen Penguji I	Dosen Penguji II
Ali Mahmudi, BEng, PhD.	**Sandy Nataly Mantja, Skom.**
NIP.P. 1031000429	**NIP.P. 1030800418**

INSTITUT TEKNOLOGI NASIONAL MALANG
Fakultas Teknologi Industri
Program Studi Teknik Informatika S1
Jl. Raya Karanglo Km. 2 Malang

FORMULIR PERBAIKAN SKRIPSI

Nama : Rino Jiwandanu
NIM : 08.18.902
Prodi : Teknik Informatika S-1
Judul : Desain Dan Implementasi Intrusion Detection System Berbasis Linux Pada Jaringan LAN

Tanggal	Penguji	Uraian	Paraf
15 Februari 2013	I	- Tambahkan menu About Us - Tambahkan pengujian Browser - Tambahkan Alert/Pop Up jika ada serangan	
15 Februari 2013	II	- Tidak boleh menggunakan button karena penulisan ilmiah - Saran no. 1 di tambahkan - Daftar Pustaka dan diagram alir - Tambahkan menu Help / Bantuan	

Anggota Penguji :

Dosen Penguji I

Ali Mahmudi, BEng, PhD.
NIP.P. 1031000429

Dosen Penguji II

Sandy Nataly Mantja, Skom.
NIP.P. 1030800418

Mengetahui

Dosen Pembimbing I

Joseph Dedy Irawan, ST, MT.
NIP. 197404162005011002

Dosen Pembimbing II

Sonny Prasetio, ST, MT.
NIP. 1031000433

INSTITUT TEKNOLOGI NASIONAL MALANG
Fakultas Teknologi Industri
Program Studi Teknik Informatika S1
Jl. Raya Karanglo Km. 2 Malang

FORMULIR BIMBINGAN SKRIPSI

Nama : Rino Jiwandanu
Nim : 08.18.902
Masa Bimbingan : 15 Oktober 2012 s/d 15 April 2013
Judul Skripsi : Desain Dan Implementasi Intrusion Detection System (IDS) Berbasis Linux Pada Jaringan LAN

NO	TANGGAL	URAIAN	PARAF PEMBIMBING
1	23-1-2013	Acc Seminar Hasil	
2	11-2-2013	Acc Makalah (Laporan)	
3	11-2-2013	Acc Kompre	
4			
5			
6			
7			
8			
9			
10			

Malang, 11 Februari 2013
Dosen Pembimbing I

Joseph Dedy Irawan, ST., MT.
NIP. 197404162005011022

Form S-4b

INSTITUT TEKNOLOGI NASIONAL MALANG
Fakultas Teknologi Industri
Program Studi Teknik Informatika S1
Jl. Raya Karanglo Km. 2 Malang

FORMULIR BIMBINGAN SKRIPSI

Nama : Rino Jiwandanu
Nim : 08.18.902
Masa Bimbingan : 15 Oktober 2012 s/d 15 April 2013
Judul Skripsi : Desain Dan Implementasi Intrusion Detection System (IDS) Berbasis Linux Pada Jaringan LAN

NO	TANGGAL	URAIAN	PARAF PEMBIMBING
1	30-11-2012	Revisi Bab III	
2	1-12-2012	Revisi Bab III	
3	5-12-2012	Acc Bab III	
4	12-1-2013	Revisi Bab IV	
5	15-1-2013	Acc Bab IV Revisi makalah seminar hasil	
6	22-1-2013	Acc Bab I dan II Revisi Makalah seminar hasil	
7	23-1-2013	Acc Makalah seminar hasil	
8	11-2-2013	Acc Kompre	

Malang, 11 Februari 2013
Dosen Pembimbing II

Sonny Prasetio, ST, MT
NIP. 1031000433

Form S-4b