IMPLEMENTASI *SIMPLE NETWORK MANAGEMENT PROTOCOL* (SNMP) PADA APLIKASI MONITORING JARINGAN BERBASIS *WEBSITE*(STUDI KASUS UNIVERSITAS MUHAMMADIYAH BENGKULU)

Diana[1], Fadel Maulana[2]

[1,2] Program Studi Teknik Informatika, Fakultas Teknik, Universitas Muhammadiyah Bengkulu
Jl. Bali PO.BOX 118 Telp.(0736) 227665, Fax (0736) 26161, Bengkulu 38119
[1]anaiboel@gmail.com
[2]xdcyber@gmail.com

Abstract:

Network management is the ability to monitor, control and planning a computer network and system components. Monitoring the network is part of network management. Simple Network Management Protocol (SNMP) is an application protocol on TCP / IP network that can be used for management and monitoring of computer network system. An application built with web-based will be able to provide advantages in ease of access, has a display in the form of a Graphical User Interface (GUI) to the administrator to read the conditions of a network of value provided by SNMP.The purpose of this study was to find a web-based monitoring system can be implemented using SNMP, as well as to determine the completion of the disruption of the network. From the research results can be shown that the monitoring system of web-based has been successfully implemented using the SNMP protocol as a data collection monitoring and database Round Robin (RRDtool) for the analysis of monitoring data and displays the data results of monitoring in the form of graphs and data obtained in the event of a network interruption enough accurate and sufficient information about the complete disruption.

Keyword: *network management,Simple Network Management Protocol*(SNMP), *website*

Abstrak:

Manajemen jaringan adalah kemampuan untuk memonitor, mengontrol dan merencanakan suatu jaringan komputer dan komponen sistem. Monitoring jaringan merupakan bagian dari manajemen jaringan. *Simple Network Management Protocol* (SNMP) adalah protokol aplikasi pada jaringan TCP/IP yang dapat digunakan untuk pengelolaan dan pemantauan sistem jaringan komputer. Sebuah aplikasi yang dibangun dengan berbasis web akan dapat memberikan kelebihan dalam kemudahan akses, memiliki tampilan dalam bentuk *Graphical User Interface* (GUI) yang dapat memudahkan administrator dalam membaca kondisi jaringan dari nilai yang diberikan oleh SNMP. Tujuan dari penelitian ini adalah untuk mengetahui sistem monitoring berbasis *web* dapat diimplementasikan dengan menggunakan SNMP, serta untuk mengetahui penyelesaian dari gangguan yang terjadi pada jaringan. Dari hasil penelitian dapat ditunjukan bahwa sistem monitoring berbasis *web* ini telah berhasil diimplementasikan dengan menggunakan SNMP sebagai protokol pengumpul data *monitoring* dan *databaseRound Robin* (RRDtool) untuk analisis data *monitoring* dan menampilkan data hasil monitoring dalam bentuk grafik serta data yang diperoleh ketika terjadi gangguan jaringan cukup akurat dan informasi mengenai gangguan tersebut cukup lengkap.

Kata Kunci: Monitoring Jaringan, *Simple Network Management Protocol*(SNMP), *website*

I. PENDAHULUAN

Peningkatan ukuran dan jumlah perangkat jaringan akan meningkatkan masalah yang ada pada jaringan tersebut. Hal tersebut tentunya membutuhkan pengawasan secara terus-menerus terhadap seluruh perangkat jaringan untuk menjamin ketersediaan atau *availability* layanan. Terdapat banyak kesulitan yang dihadapi oleh administrator jaringan jika harus memantau seluruh jaringan berkaitan dengan performa, analisis dan kontrol beberapa komponen secara manual, terutama jika jaringan tersebut semakin berkembang.

Jaringan yang terdapat pada Universitas Muhammadiyah Bengkulu belum memiliki sistem untuk mengetahui adanya gangguan sehingga admin jaringan tidak dapat segera menangani permasalahan yang ada. Selainitu admin juga tidak dapat melakukan antisipasi terhadap kegagalan yang berulang pada jaringan tesebut.

Simple Network Management Protocol (SNMP) adalah protokol aplikasi pada jaringan TCP/IP yang dapat digunakan untuk pengelolaan dan pemantauan sistem jaringan komputer [1]. Hampir semua peralatan jaringan telah mendukung penggunaan SNMP untuk pemantauannya. Namun informasi yang didapat dengan menggunakan SNMP hanya dapat diakses melalui tampilan *command prompt* atau terminal, sehingga dalam penggunaannya menjadi tidak efektif. Hasil yang diberikan SNMP itu sendiri masih memiliki kekurangan, yaitu hasil yang ditampilkan hanya sebatas informasi kondisi jaringan pada saat itu dan masih belum ada sistem untuk menyimpan dan mengolah nilai SNMP lebih lanjut.

Untuk mengatasi hal tersebut maka dibangun sebuah aplikasi berbasis *web*. Aplikasi ini dapat memberikan kelebihan dalam kemudahan akses, memiliki tampilan dalam bentuk *Graphical User Interface* (GUI) yang dapat memudahkan *administrator* dalam membaca kondisi jaringan dari SNMP, membaca hasil dari perangkat yang dimonitoring yaitu *agent* sehingga melakukan penanganan secara dini terhadap gangguan yang terjadi di jaringan. Dengan menggunakan *web browser*, *admin* dapat membuka aplikasi tersebut dimana saja selama terhubung dengan jaringan.

II. LANDASAN TEORI

A. Manajemen Jaringan

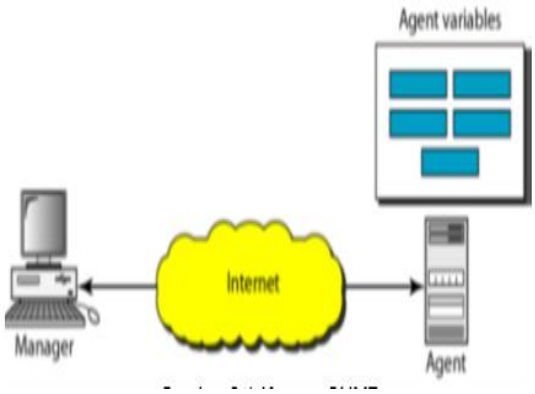
Manajeman jaringan merupakan kemampuan untuk mengontrol dan memonitor sebuah jaringan komputer dari sebuah lokasi. *The International Organization for Standardization* (ISO) mendefinisikan sebuah model konseptual untuk menjelaskan fungsi manajemen jaringan, antara lain [2]: 1) Manajemen kesalahan (*Fault Management*), ditujukan agar administrator dapat mengetahui

kesalahan (*fault*) pada perangkat, sehingga dapat diambil tindakan perbaikan; 2) Manajemen konfigurasi (*Configuration Management*), mencatat informasi konfigurasi jaringan, sehingga dapat dikelola dengan baik; 3) Pelaporan (*Accounting*), mengukur penggunaan jaringan dari pengguna; 4) Manajemen Performa (*Performance Management*), mengukur performansi jaringan dan melakukan pengumpulan dan analisis data statistik; 5) Manajemen Keamanan (*Security Management*), mengatur akses ke resource jaringan sehingga informasi tidak dapat diperoleh tanpa izin.

B. *Simple Network Management Protocol* (SNMP)

Simple Network Management Protocol (SNMP) adalah sebuah protokol yang dirancang untuk memberikan kemampuan kepada pengguna untuk memonitor dan mengatur suatu jaringan komputer dari jarak jauh (secara remote) atau dalam satu pusat kontrol saja. Dengan menggunakan protokol ini bisa didapatkan informasi tentang status dan keadaan dari suatu jaringan. Protokol ini menggunakan transport UDP pada port 161. Pengolahan ini dijalankan dengan mengumpulkan data dan melakukan penetapan terhadap variabel-variabel dalam elemen jaringan yang dikelola [3].

Dalam aplikasinya, Elemen SNMP terdiri dari tiga bagian, yaitu manager, agent, dan MIB [4]. Manager merupakan software yang berjalan di sebuah host di jaringan, yang merupakan suatu proses atau lebih yang berkomunikasi dengan agent dalam jaringan. Agent merupakan perangkat lunak yang dijalankan disetiap elemen jaringan yang dikelola. Agent terdapat pada, workstation, repeater, router, switch, dan personal computer, bertugas untuk merespon dan memberikan informasi sesuai permintaan manager SNMP. Manager Information Base (MIB) merupakan struktur database variabel dari elemen jaringan yang dikelola [5]. Pendefinisian MIB dalam SNMP menggunakan diagram pohon, dan menempatkan setiap Object Identifier (OID) pada suatu lokasi unik pada pohon.



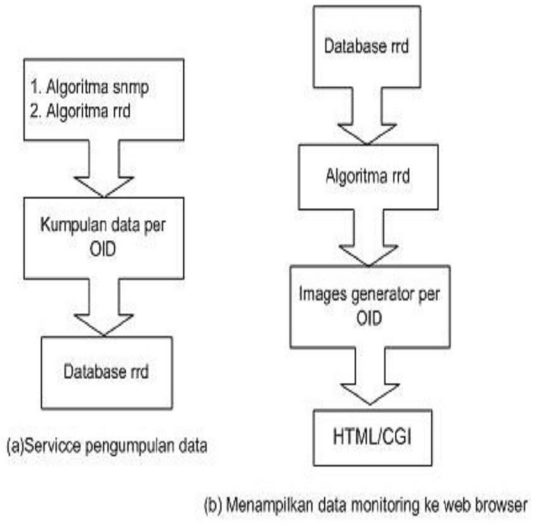
Gambar 1. Konsep SNMP

III. METODELOGI PENELITIAN

Monitoring sistem ini dikembangkan dengan menggunakan SNMP (*Simple Network Management Protocol*). Untuk itu

pada perancangan sistem dibutuhkan *agent* SNMP untuk memperoleh data yang dibutuhkan kemudian data tersebut akan dikumpulkan ke dalam suatu *database* dan dibuat grafiknya dengan menggunakan *RRDtool* (*Round Robin Database*), dimana perangkat lunak ini akan bertindak sebagai *database* untuk mengumpulkan data *monitoring*.

Hubungan antara pengambilan data melalui SNMP, pengumpulan *database* dengan *RRDtool* hingga ditampilkan dalam bentuk grafik pada *web browser* dapat dilihat pada Gambar 2 dibawah ini :



Gambar 2. Perancangan SNMP dan *RRDTool*

1. *Service*pengumpulan data

a. Algoritma SNMP

"Pesan SNMP v 2c + self_host + "-c" + self_password + OID"

b. Algoritma RRD.Pada tahapan ini algoritma rrd yang digunakan adalah *create* dan *update.*

1) Tahap 1 : *create rrdtool (rrd_name, item_type, interval)*

Command create = *"rrdtool create" + self_RRD_DIRS_DATA + rrd_name + ".rrd" + "-step" + interval \DS :item_name :item_type : interval*2 :u:u RRA:AVERAGE:0.5:1*

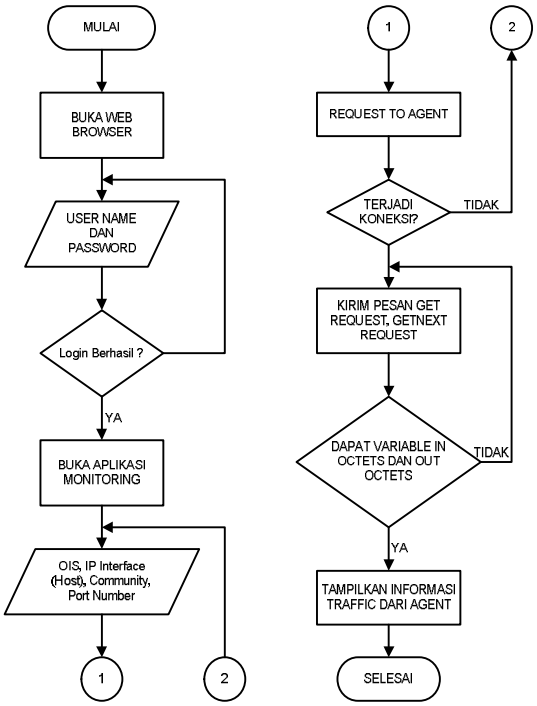
2) Tahap 2 : *update rrdtool (rrd_name)*

Command update = *"rrdtool update"+self.__RRD_DIRS_DATA +rrd_name + ".rrd N"*

2. Menampilkan data *Monitoring*ke*web browser* Pada proses menampilkan data *monitoring* ke*web browser* dibuat dalam bentuk grafik .*Algoritm arrd* pada tahapan ini :*rrdtool graph (name_rrd)*

Command rrdtoolgraph : *"rrdtool graph" + self.__RRD_DIRS_IMAGE + rrd_name + ".png" + *

Berdasarkan desain sistem yang dibuat, maka diagram alir dari aplikasi monitoring traffic intranet adalah sebagai dapat dilihat pada Gambar 3.

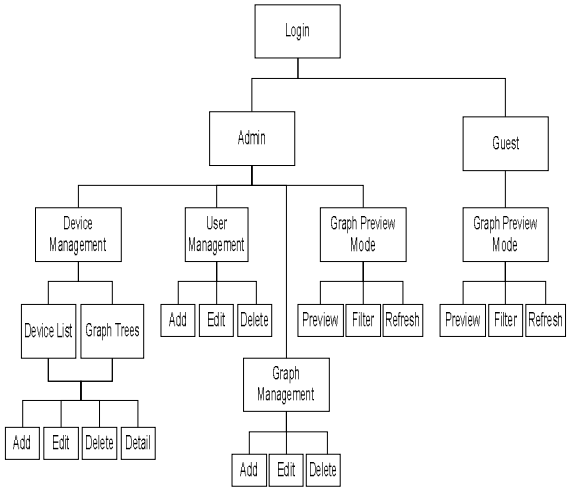


Gambar 3. Flowchat aplikasi monitoring

IV. HASIL DAN PEMBAHASAN

A. Struktur Menu Aplikasi

Secara umum struktur menu aplikasi dapat dilihat pada Gambar 3, dimana proses *login* pada struktur menu implementasi sistem *monitoring jaringan* terdiri atas dua *user* yaitu *login* sebagai *user* tamu (*guest user*) dan *login* sebagai administrator (*adminuser*). *User* tamu adalah *user* yang hanya dapat melihat grafik dari *device* yang sudah diatur oleh admin, sedangkan administrator adalah pihak pengelola sistem.



Gambar 4. Implementasi Struktur Menu

B. Uji Coba Sistem

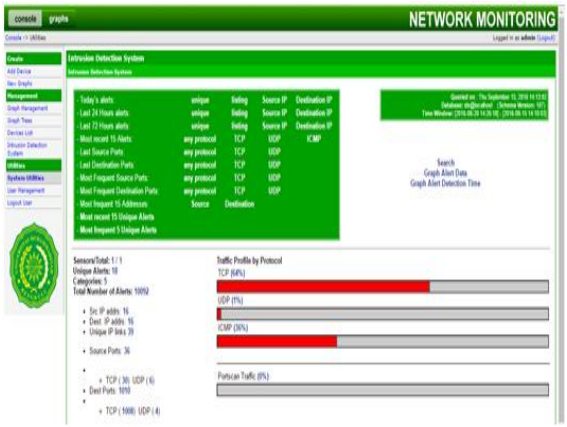
Sistem ini dibangun dengan menggunakan dua buah komputer dan satu mesin virtual dengan aplikasi *Oracle VM VirtualBox*, dimana mesin virtual tersebut sebagai *web server* sekaligus server *Intrusion Detection System* (IDS) dan dua komputer lainnya sebagai *client*. Ketiga komputer ini dihubungkan dengan mengunakan jaringan nirkabelsehingga membentuk jaringan LAN (*Local Area Network*). Kedua komputer *client* juga sebagai *agent* SNMP yang akan dimonitoring. Ujicoba dilakukan selama kurang lebih 5 (lima) jam mulai dari pukul 02:00 WIB hingga pukul 7:00 WIB.

C. AnalisisSistem

1. nalisissistempendeteksigangguan.Penelitianinimenggunakanaplikasi BASE (*Basic Analysis and Security Engine*) sebagai hasil dari pantauan *Snort*.

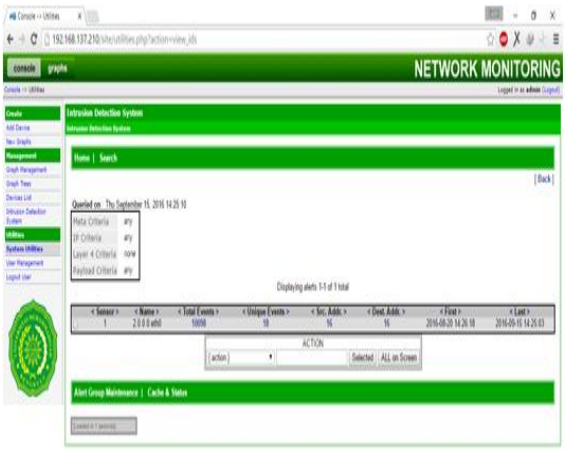
a. Tampilanutama*Intrusion Detection System*

Pada halaman utama *Intrusion Detection System*, disajikan dengan tampilan *traffic protocol* dengan tampilan grafik bar agar mempermudah administrator membaca hasil keseluruhan dari data yang di proses oleh *Snort*.



Gambar 5.*Interface* Halaman Utama

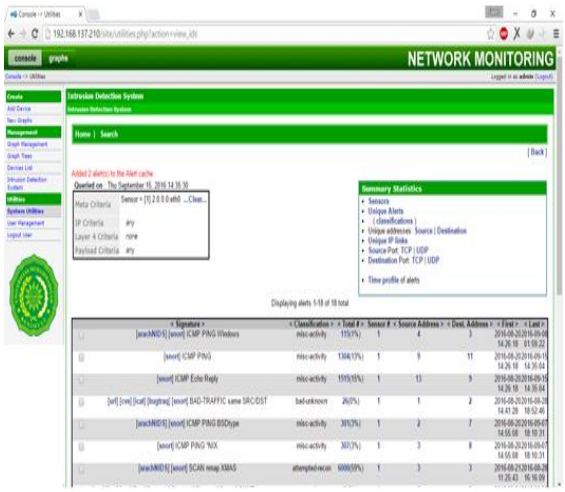
b. TampilanSensor*Interface*



Gambar 6.*Interface* Halaman Sensor

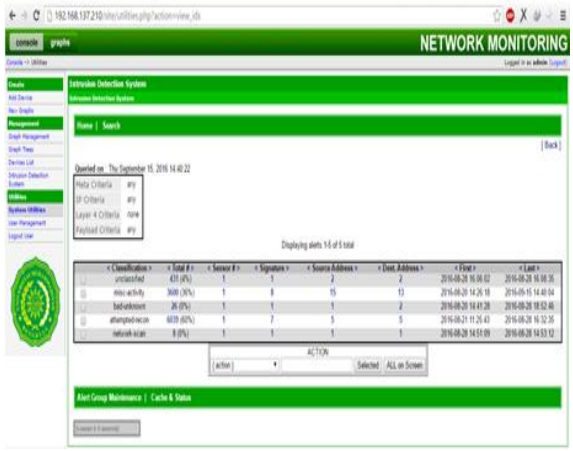
c.

d. Tampilan*Unique Alerts*



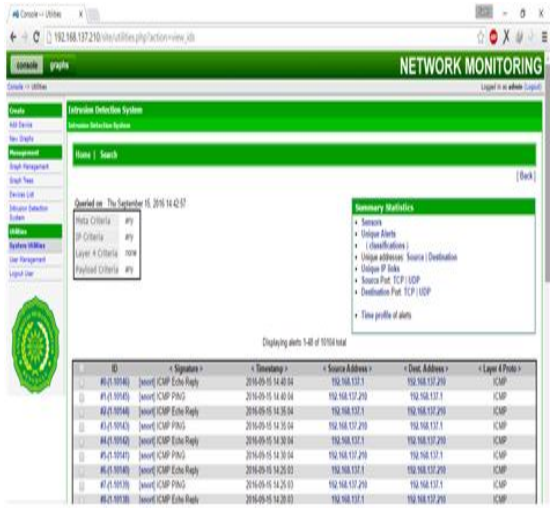
Gambar 7.*Interface* Halaman *Unique*

e. Tampilan*Category dan Unique Alerts*

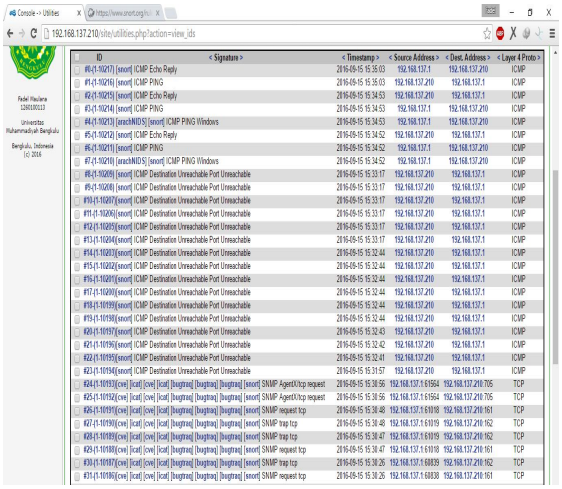


Gambar 8.*Interface* Halaman

f. Tampilan*DisplayAlerts*



Gambar 9.*Interface* Halaman *Display Alerts*



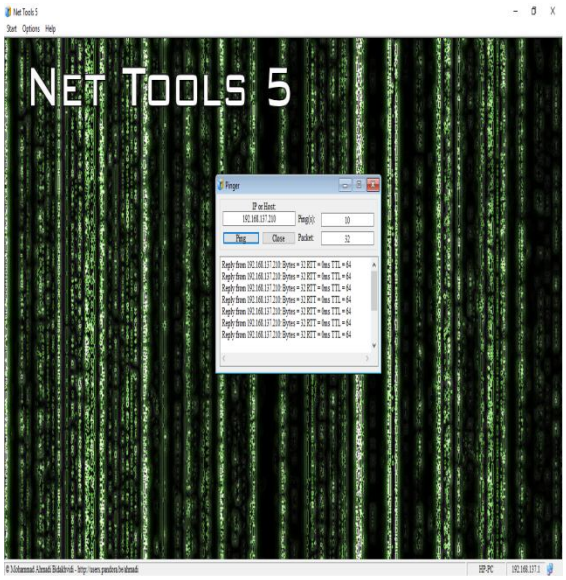
Gambar 10.*Interface* Halaman *Display Alerts*

Pada Gambar 10 terlihat bahwa *IPAddress* 192.168.137.1 mencoba melakukan *scan* ICMP. ICMP utamanya digunakan oleh sistem operasi komputer jaringan untuk mengirim pesan yang menyatakan bahwa komputer tersebut dapat dijangkau atau tidak. *Alert* merupakan *alert* ketika paket data dalam ukuran besar yang berasal dari *ip address* 192.168.137.1 ke *IP Addres*s 192.168.137.210 yang dianggap sebagai serangan oleh snort karena pola serangan tersebut terapat pada *rule snort.* Serangan tersebut dapat dikategorikan sebagai DOS yaitu serangan dengan mengunakan paket tertentu dengan jumlah yang sangat besar dengan maksud mengacau kan keadaan jaringan target dalam hal ini disebut *ping attack.*

Pada Gambar 10 juga terdapat *SNMP trap*, dan *SNMP Request* yang di akses melalui protokol TCP. Ini dikenali sebagai gangguan karena terdaftar pada tabel *snort* sebagai jenis gangguan, pada bagian ini bermaksud informasi rinci *SNMP tarp daemon* biasanya mendengarkan pada port 162, TCP atau UDP.Seorang penyerang mungkin mencoba untuk mengirim permintaan ini untuk menentukan apakah perangkat menggunakan SNMP.

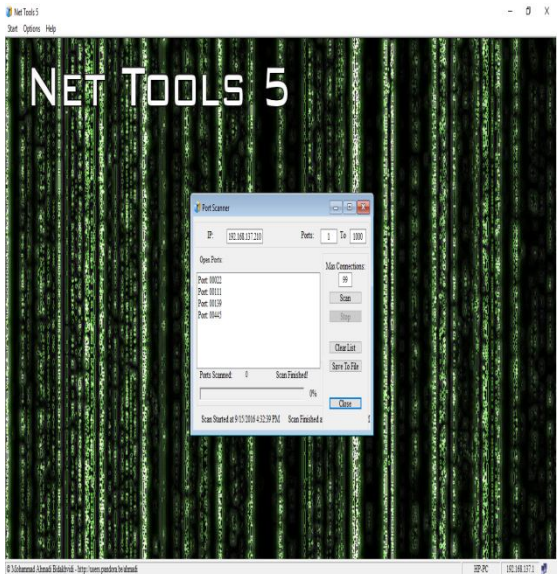
2. engujiansistempendeteksigangguan

Pengujian sistem ini menggunakan berbagai aplikasi sebagai simulasi serangan yang umumnya terjadi pada jaringan komputer.



Gambar 11.*Interface ping attack*

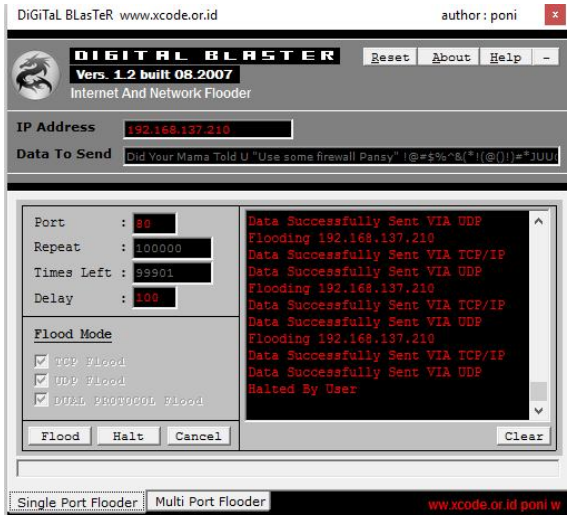
Gambar 11 penyerangan dilakukan oleh penyusup dengan mengirimkan paket data dengan kapasitas 32 *byte* dan melakukan proses ping sebanyak 10x pada *ip server* yaitu 192.168.137.210.



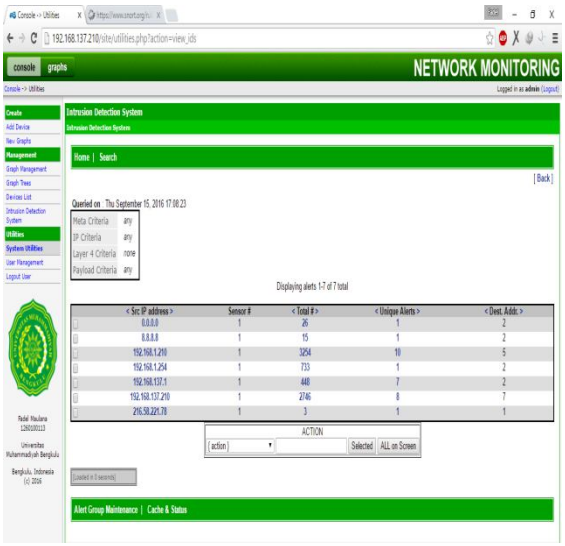
Gambar 12*Interface Scan Port*

Gambar 12*nettools* mencoba mencari informasi pada *IP Address*192.168.137.210 dengan mencoba mens*can port-port* yang terbuka. Pada *server* dengan membuat range port 1 sampai dengan 1000, kemudian klik *scan*, sehingga kita dapat mendapatkan *port* yang terbuka pada pada ip 192.168.137.210, yaitu *port* 22, dan *port* 80. *Port* 22 merupakan *port protocol tcp* yang melayani *service remote ssh (secure shell)* dan *port* 80 merupakan *port protocol tcp* yang berfungsi mengelola *web server (apache)*

Pada Gambar 13, penyerangan dilakukan oleh penyusup dengan melakukan *flooding* terhadap port 80 *ip address server* 192.168.137.210 yang berfungsi menbanjiri paket jaringan dengan menggunakan aplikasi *digiblast* yang membuat sistem *server* menjadi *hang*.



Gambar 13.*Interface Flooding Protocol TCP*dan *UDP*



Gambar 14Daftar *IP Address* yang Melakukan Serangan

3. KelemahandanKeunggulanSistem

Beberapa keunggulan sistem adalah :

a. Apikasi system *monitoring* ini dapat diakses dengan menggunakan *web browser* baik itu *platform windows* atau*linux.*

b. Aplikasi ini memungkinkan *admin* dengan mudah untuk mengamati permasalahan atau kondisi beban yang terlalu berat yang dialamimasing-masing*device*.

c. Kemudahan untukmengaksessistem*monitoring*. *Admin* yang menggunakan aplikasi ini dapat memilih sendiri sumber daya *jaringan*yang ingindimonitor.

d. Kemudahanuntukmenambah, mengubah atau mengurangi *item monitoring*, *device*, *agent,* yang semuanya diatur dalam manajemen jaringan sehingga jika ada penambahan tidak perlu mengubah *source code* (perangkatlunak) sistem*monitoring.*

e. Kemampuan mendeteksi gangguan yang terjadipadajaringan.

f. Sistem *monitoring* ini dikembangkan dengan beberapa tools sehingga kinerja masing-masing tools juga sangat dibutuhkan.

1) Dengan menggunakan SNMP memungkin kan kita untuk memperoleh data *monitoring* mengenai jaringan pada komputer.

2) Dengan menggunakan Snort sebagai induk system deteksi gangguan.

Kelemahan yang dimiliki sistem adalah:

a. Sistem hanya dapat di akses melalui perangkat yang terhubung pada jaringan yang sama dengan *server*.

b. Karena database sistem*monitoring* hanya menggunakan *file* maka data yang dapatdisimpanjugaterbatas.

c. *Loading* untukpengaktifan*agent* snmp ketika menambahkan *device* baru memerlukan waktu yang sedikit lama diawal inisialisasi. Karena diperlukan koneksi ke *device* untuk mengetahui apakah terdapat *agent* snmpatautidak.

d. Sistempendeteksigangguanhanya dapat mengenalibeberapajenisgangguan.

e. PengenalandanPenangananmasalah masih menggunakan database dariluarjaringan.

V. PENUTUP

Berdasarkan hasil penelitian, pengujian, implementasi serta pembahasan pada Implementasi *Simple Network Management Protocol* (SNMP) Pada Aplikasi Monitoring Jaringan Berbasis *Website* (Studi Kasus Universitas Muhammadiyah Bengkulu), maka didapatkan kesimpulan sebagai berikut:

1. Sistem monitoring berbasis web initelahberhasildiimplementasikandenganmenggunakan SNMP sebagaiprotokolpengumpul data *monitoring*dan*databaseRound Robin* (RRDtool) untukanalisis data *monitoring*danmenampilkan data hasil*monitoring* dalambentukgrafik.
2. Dari hasilujicoba, data yang diperolehketikaterjadigangguanjaringancukupakuratdaninformasimengenaigangguantersebutcukuplengkap. Akan tetapi terdapat kelemahan yaitu masih menggunakan data dariluar*server*, dan hanya dapat mengenali beberapa fitriajenisgangguan. Hal inibisasajadisebabkankarenaadanya*l oss* jaringansaatpengiriman data atau tidak semua data dapat dikirim kembali.
3. Dari segi *performance* memori dan CPU, terlihat jelas bahwa spesifikasi *hardware* sangat berpengaruh dalam kestabilan kerja prosesornya. *Server* dengan spesifikasi *hardware* dua kali lebih bagus dari *agent* hasilnya lebih stabil dan lebih optimal.

REFERENSI

[1] Behrouz A. Forouzan. 2007. *Data Communications and Networking*, 4th Edition, McGraw Hill.

[2] Teare, Diane. Paquet, Chaterine. 2006. "*Campus Network Fundamentals*". Indianapolis : Cisco Press.

[3] Case, J., ed., "*About SNMP, SNMP Architecture, Protocol Specification*", RFC 1157, The Internet Society, Mei 1990.

[4] Harrington, D, "*An Architecture Describing SNMP Management Frameworks*". RFC 3411, The Internet Society, Desember 2002.

[5] McCloghrie, K., "*Management Information Base for Network Management of TCP/IP-based internets: MIB-II*", RFC 1213, Hughes LAN Systems, Inc., Maret 1991.