

Sistem Keamanan Jaringan Komputer Dengan Firewall dan Intrusion Detection System (IDS)

Saiful Aziz, Bambang Eka Purnama

ABSTRAKSI

Beberapa tahun terakhir, sistem jaringan komputer dan internet telah berkembang pesat pada skala ukuran, kompleksitas dan kerentanan terhadap serangan (*attack*).

Pada saat yang sama, pengetahuan, peralatan, dan teknik yang tersedia bagi penyerang (*attacker*) juga telah berkembang secara proporsional. Sayangnya teknik pertahanan terhadap serangan tidak berkembang cukup cepat. Teknologi keamanan saat ini telah mencapai batasnya dan solusi inovatif selanjutnya diperlukan. Metodologi yang digunakan adalah analisis dan perancangan sistem. Diharapkan dengan rancangan yang dibuat akan dapat diimplementasikan pada pembangunan jaringan yang lebih baik.

A. LATAR BELAKANG MASALAH

Keamanan jaringan saat ini menjadi isu yang sangat penting dan terus berkembang. Beberapa kasus menyangkut keamanan sistem saat ini menjadi suatu pekerjaan yang membutuhkan biaya penanganan dan proteksi yang sedemikian besar. Sistem-sistem vital seperti sistem pertahanan, sistem perbankan dan sistem-sistem setingkat itu, membutuhkan tingkat keamanan yang sedemikian tinggi. Hal ini lebih disebabkan karena kemajuan bidang jaringan komputer dengan konsep open sistemnya sehingga siapapun, di manapun dan kapanpun, mempunyai kesempatan untuk mengakses kawasan-kawasan vital tersebut.

Keamanan jaringan didefinisikan sebagai sebuah perlindungan dari sumber daya daya terhadap upaya penyingkapan, modifikasi, utilisasi, pelanggaran dan kerusakan oleh person yang tidak diijinkan (Mochamad Sarosa, 2000).

Keamanan komputer adalah suatu perlindungan yang diusahakan oleh suatu sistem informasi dalam rangka mencapai sasaran hasil yang bisa diterapkan atau memelihara integritas, kerahasiaan dan ketersediaan sistem informasi sumber daya. Sumber daya informasi meliputi perangkat keras, perangkat lunak, data dan informasi (Nurma Evi, 2003).

Definisi lainnya adalah "*Computer Security is preventing attackers from achieving objectives through unauthorized access or unauthorized use of computers and networks*". (John D. Howard, dikutip oleh Budi Rahardjo, 2000). *Intrusion* adalah usaha untuk masuk dan atau menyalahgunakan sistem yang ada. *Intrusion Detection* adalah proses untuk *monitoring event* yang terjadi pada sistem komputer atau jaringan komputer dan melakukan analisis data tersebut untuk mengetahui adanya *intrusion*, terhadap *confidentiality*, *integrity*, *availability* ataupun melakukan *by-pass* mekanisme pengamanan yang ada (Ivan Suci Firmansyah, 2003).

Sedangkan definisi *firewall* adalah "*A firewall is a system or group of systems that enforces an access control policy between two networks*" (<http://www.clark.net/pub/mjr/pubs/fwfaq/>).

Firewall merupakan suatu cara atau mekanisme yang diterapkan baik terhadap *hardware*, *software* ataupun sistem itu sendiri

dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan atau kegiatan suatu segmen pada jaringan lokal dengan jaringan luar yang bukan merupakan ruang lingkupnya. Segmen tersebut dapat merupakan sebuah *workstation*, *server*, *router*, atau *local area network (LAN)* (Ahmad Muammar, 2004).

Keamanan jaringan komputer sebagai bagian dari sebuah sistem informasi adalah sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunaannya. Sistem harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak berhak dimana usaha tersebut bisa dilakukan baik dari dalam maupun dari luar sistem. Beberapa insinyur jaringan mengatakan bahwa hanya ada satu cara mudah dan ampuh untuk mewujudkan sistem jaringan komputer yang aman yaitu dengan menggunakan pemisah antara komputer dengan jaringan selebar satu inci, dengan kata lain, hanya komputer yang tidak terhubung ke jaringanlah yang mempunyai keamanan yang sempurna. Meskipun ini adalah solusi yang buruk, tetapi ini menjadi *trade-off* antara pertimbangan fungsionalitas dan memasuki kekebalan terhadap gangguan (Mochamad Sarosa, 2000).

Ide dasar dalam membangun sistem keamanan jaringan komputer menggunakan Firewall dan *Intrusion Detection System (IDS)* atau sistem pendeteksi penyusupan jaringan ini adalah semakin maraknya kejahatan di dunia internet atau *Cyber Crime* seperti pencurian password kartu kredit, pembobolan situs *e-commerce*, bobolnya situs Komisi Pemilihan Umum (KPU) dan sebagainya ternyata hanya disebabkan oleh kelemahan dan keteledoran para administrator jaringan dan team IT sistem tersebut yang menganggap remeh tentang masalah-masalah keamanan seperti membiarkan setting sistem yang *default*, membiarkan port – port yang tidak terpakai dan dibiarkan terbuka, jarang melakukan *patch* aplikasi yang digunakan dan membiarkan *vulnerabilities* yang ada pada aplikasi tersebut yang akhirnya dimanfaatkan sebagai pintu masuk kedalam sistem oleh para penyusup jaringan.

B. PERUMUSAN MASALAH

Dari berbagai latar belakang masalah yang ada tentang masalah keamanan jaringan dan sistem penanggulangannya yang dalam penulisan naskah skripsi ini menggunakan Firewall dan *Intrusion Detection System (IDS)* maka dapat dirumuskan suatu perumusan masalah yaitu:

Bagaimana membangun dan mengimplementasikan sistem keamanan jaringan komputer dengan menggunakan *Firewall* dan *IDS (Intrusion Detection System)* secara optimal?

C. BATASAN MASALAH

Masalah keamanan sistem komputer bisa dipandang relatif luas dan rumit. Dalam penulisan naskah skripsi ini yang dilakukan adalah pembangunan sistem keamanan jaringan dengan Firewall dan IDS (*Intrusion Detection System*), Firewall dibatasi pada *Iptables* dan *Ipchains* sedangkan IDS menggunakan *Snort* yang didukung oleh ACID (*Analysys Console For Intrusion Detections*). Setelah sistem selesai dibangun akan dilakukan *penetration test* atau ujicoba sistem keamanan jaringan yang telah dibangun. Diasumsikan pula sistem ini berada pada intranet yang juga sudah tersambung ke internet.

D. TUJUAN PENULISAN

1. Mengimplementasikan sistem keamanan jaringan menggunakan *firewall* dan IDS (*Intrusion Detection System*) atau sistem deteksi penyusupan jaringan
2. Menganalisa performansi sistem deteksi penyusupan jaringan dalam menangani gangguan terhadap sistem
3. Memberikan solusi bagi Administrator jaringan komputer untuk mengamankan jaringan yang telah dibangun dari ancaman para penyusup jaringan
4. Secara umum untuk merancang suatu sistem keamanan jaringan komputer yang dititikberatkan pada penggunaan *Firewall* dan *Intrusion Detection System (IDS)* secara optimal agar supaya sistem yang dibangun terhindar dari berbagai gangguan keamanan yang sering dilakukan oleh *hacker* dan *cracker* serta akses oleh orang yang tidak berhak.

E. METODE PENELITIAN

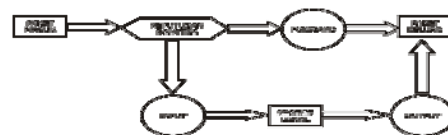
1. Metode *Interview* yaitu Penulis mengadakan wawancara langsung dengan pihak-pihak yang mengetahui dan berpengalaman tentang sistem keamanan jaringan komputer, metode – metode pengamanan jaringan yang digunakan dan sebagainya
2. Metode Observasi. Penulis mengadakan observasi langsung ke beberapa lembaga dan instansi yang memiliki jaringan komputer intranet yang juga sudah terhubung dengan internet.

3. Data Sekunder. Penulis mencari dan mengumpulkan data-data tentang sistem keamanan jaringan, buku-buku literatur dan sumber-sumber pustaka lainnya yang berhubungan dengan pokok permasalahan.
4. Metode Analisis dan Penelitian. Untuk mendapatkan data dan informasi yang valid tentang sistem keamanan jaringan, maka Penulis mengelompokkan data sesuai dengan permasalahannya.
5. Metode Analisis. Yaitu mengadakan kajian analisis terhadap materi atau komponen yang akan dibahas seperti Konsep dasar keamanan jaringan, *Firewall*, IDS (*Intrusion Detection System*), ACID (*Ananlisys Console for Intrusion Detection*), Dan beberapa materi pendukung lainnya
6. Metode Penelitian dan Implementasi. Yaitu penggunaan pendekatan yang paling sesuai dengan urutan-urutan ilmu pengetahuan terhadap tujuan-tujuan dari penulisan Langkah-langkah yang ditempuh dalam penulisan ini adalah
7. Perencanaan. Perencanaan dilakukan dengan tujuan untuk memilah dan memilih sumber-sumber atau data yang paling tepat, kemudian dikaji lebih lanjut untuk kemudian diimplementasikan pada sistem keamanan yang penulis bangun dalam hal ini Server Linux Redhat 9.0. Tahapan dalam perencanaan ini meliputi Pengumpulan informasi, Survey, Analisa data, Perancangan, Implementasi sistem keamanan, Pengelolaan sistem dan *maintenance*
8. Konfigurasi Sistem. Yaitu pengaturan perangkat-perangkat yang diperlukan untuk mengimplementasikan sistem keamanan jaringan dengan Firewall dan *Intrusion Detection System (IDS)*
9. Ujicoba sistem. Yaitu tahapan pengujian sistem yang telah dibangun. Dalam tahapan ini akan diujicoba langsung dengan berbagai *software penetration test* atau perangkat lunak untuk ujicoba sistem yang biasa digunakan dalam proses penyerangan sistem.

F. KEGIATAN IMPLEMENTASI

IPTables

IPTables memiliki tiga macam daftar aturan bawaan dalam tabel penyaringan, daftar tersebut dinamakan rantai *firewall (firewall chain)* atau sering disebut *chain* saja. Ketiga *chain* tersebut adalah INPUT, OUTPUT dan FORWARD.



Gambar 1 Diagram Rantai Firewall (Firewall Chain)

Pada diagram tersebut, lingkaran menggambarkan ketiga rantai atau *chain*. Pada saat sebuah paket sampai pada sebuah lingkaran, maka disitulah terjadi proses penyaringan. Rantai akan memutuskan nasib paket tersebut. Apabila keputusannya adalah DROP, maka paket tersebut akan di-drop. Tetapi jika rantai memutuskan untuk ACCEPT, maka paket akan dilewatkan melalui diagram tersebut.

Sebuah rantai adalah aturan-aturan yang telah ditentukan. Setiap aturan menyatakan "jika paket memiliki informasi awal (*header*) seperti ini, maka inilah yang harus dilakukan terhadap paket". Jika aturan tersebut tidak sesuai dengan paket, maka aturan berikutnya akan memproses paket tersebut. Apabila sampai aturan terakhir yang ada, paket tersebut belum memenuhi salah satu aturan, maka kernel akan melihat kebijakan bawaan (*default*) untuk memutuskan apa yang harus dilakukan kepada paket tersebut. Ada dua kebijakan bawaan yaitu *default* DROP dan *default* ACCEPT.

Jalannya sebuah paket melalui diagram tersebut bisa dicontohkan sebagai berikut:

G. ACID (Analisis Console for Intrusion Detection)

ACID dijalankan lewat Browser web, seperti Internet Explorer, Netscape atau Opera. Misal http://yourhost/acid/acid_main.php. Yourhost diganti dengan IP atau alamat domain sistem yang digunakan. Kemudian akan muncul Message di browser seperti Ketik http://yourhost/acid/acid_main.php pada Address Bar:

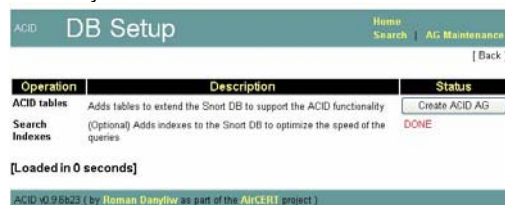
Analysis Console for Intrusion Databases

The underlying database snort@localhost appears to be incomplete/invalid.

The database version is valid, but the ACID DB structure (table: acid_ag) is not present. Use the Setup page to configure and optimize the DB.

Gambar 2 Tampilan Halaman ACID ketika pertama kali dijalankan

Klik pada link "Setup Page" untuk membuat tabel tambahan ke database Snort yang akan dipakai oleh Acid, kemudian akan muncul halaman berikutnya



Gambar 3 Halaman Setup Page ACID

Kemudian klik pada tombol yang bertuliskan

"Create Acid AG". Maka system ACID otomatis akan membuat 4 (empat) tabel baru ke dalam database Snort



Gambar 4 Tabel Acid sukses dibuat

Kemudian klik baris "Goto the Main Page to Use the application", untuk masuk ke halaman depan ACID

Additional DB permissions
In order to support Alert purging (the selective ability to permanently delete alerts from the database) DELETE and UPDATE privilege on the database "snort@localhost"

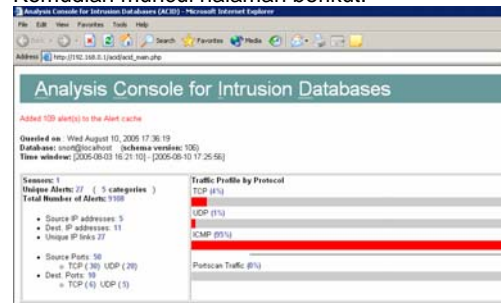
Goto the [Main page](#) to use the application.

[Loaded in 1 seconds]

ACID v0.9.6b23 (by Roman Danyliw as part of the AirCERT project)

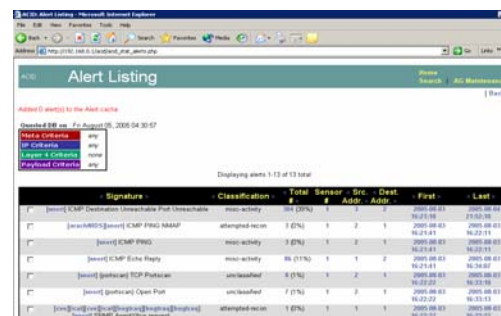
Gambar 5 Link untuk masuk ke halaman utama ACID

Kemudian muncul halaman berikut:



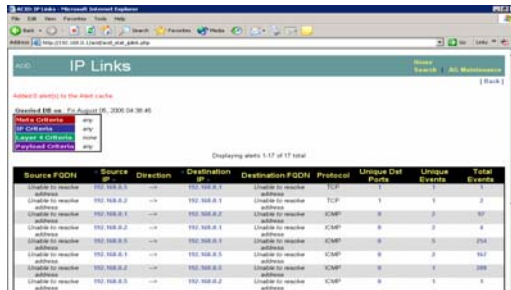
Gambar 6 Halaman ACID setelah pembuatan ACID AG selesai

Misal Untuk melihat daftar hasil *alert* dari Snort, masuk ke http://192.168.0.1/acid/acid_stat_alerts.php



Gambar 7 Melihat daftar Alert Snort

Untuk melihat lalu lintas data IP Address yang masuk dan keluar sistem dan ke port apa saja IP tersebut terhubung bisa di cek dengan masuk ke http://192.168.0.1/acid/acid_stat_iplink.php



Source IP	Source Port	Destination IP	Destination Port	Protocol	Unique Dest Ports	Unique Events	Total Events
192.168.0.1	80	192.168.1.1	80	TCP	1	1	1
192.168.0.1	80	192.168.1.1	80	TCP	1	1	1
192.168.0.1	80	192.168.1.1	80	TCP	1	1	1
192.168.0.1	80	192.168.1.1	80	TCP	1	1	1
192.168.0.1	80	192.168.1.1	80	TCP	1	1	1
192.168.0.1	80	192.168.1.1	80	TCP	1	1	1
192.168.0.1	80	192.168.1.1	80	TCP	1	1	1
192.168.0.1	80	192.168.1.1	80	TCP	1	1	1
192.168.0.1	80	192.168.1.1	80	TCP	1	1	1
192.168.0.1	80	192.168.1.1	80	TCP	1	1	1

Gambar 8 Daftar IP Address yang keluar masuk dan port yang terhubung

H. TINDAK LANJUT IMPLEMENTASI

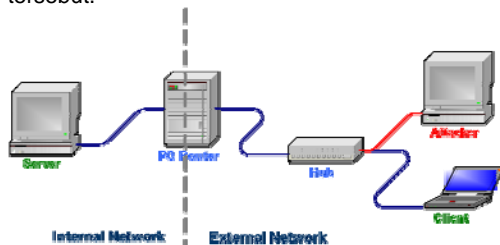
Dalam proses tindak lanjut implementasi sistem keamanan jaringan dengan firewall dan IDS (*Intrusion Detection System*) ini maka akan dilakukan proses pengujian sistem atau *penetration test*. Proses pengujian sistem akan menggunakan beberapa *tools*, *exploits* dan *software* khusus yang biasa dipakai oleh pakar keamanan jaringan untuk melakukan *penetration test*.

Penetration test yang dilakukan dengan beberapa *software*, *tools* dan *exploit* seperti Nmap dan SuperScan untuk *Scanning*, telnet dan Netcat untuk mencoba penyerangan mode *Enumeration* dan untuk mode *Denial of Service Attack* dicoba dengan *ping of death* dan *smurf* dan *Brute force attack* dicoba dengan Brutus dan Unsecure v.20

I. PENGUJIAN SISTEM

Pada implementasi sistem keamanan ini, sistem yang dipakai merupakan PC router linux 2.4.22 distribusi Slackware yang mempunyai 1 buah *network interface card* (NIC). Keseluruhan sistem, baik IDS, monitoring, database, *firewall* maupun notifikasi interaktif, dipasang dalam PC router tersebut. Sistem tersebut dilengkapi dengan paket program Apache Web Server, MySQL Database Server, Iptables serta Snort.

Jaringan yang digunakan dalam lingkungan pengujian sistem adalah sebuah jaringan dengan 2 subnet yang dihubungkan dengan sebuah PC router. Berikut adalah gambar konfigurasi jaringan tersebut.



Gambar 9 Konfigurasi Jaringan Pengujian

Server berada pada *Internal Network* dan diinstalasikan berbagai macam aplikasi server seperti server web, mail, FTP, SMB. Server ini yang nanti akan dijadikan sasaran serangan oleh *attacker*.

Server berada pada *Internal Network* dan menggunakan IP address 192.168.1.2 dengan subnet mask kelas C (255.255.255.0). Server ini diinstalasikan berbagai macam aplikasi server seperti server web, mail, FTP, SMB. Server ini yang nanti akan dijadikan sasaran serangan oleh *attacker*.

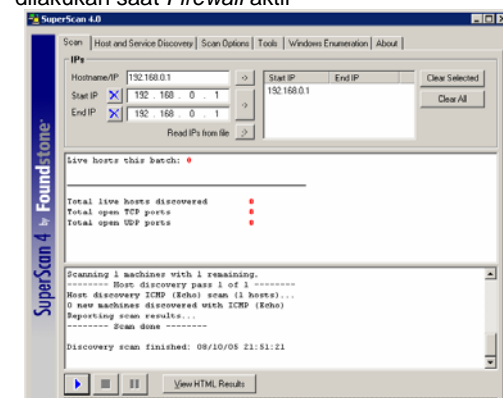
Untuk menghubungkan dua subnet ini digunakan sebuah PC Router berbasis Linux. Router ini mempunyai 2 buah *interface ethernet* dengan konfigurasi IP address 192.168.0.1 untuk jaringan eksternal (*eth0*) dan 192.168.1.1 untuk jaringan internal (*eth1*). Pada router inilah instalasi seluruh sistem *firewall* dan IDS dilakukan.

Pada jaringan eksternal, terdapat dua *host* yang bertindak sebagai *client* dan sebagai penyerang. *Client* berfungsi sebagai titik pengamatan router sekaligus sebagai titik pengirim *flooding data* yang digunakan sebagai simulasi trafik data antara *client* dengan server. IP address yang digunakan adalah 192.168.0.2 dengan subnet mask kelas C. Sistem operasi yang digunakan adalah Linux dengan program pengakses layanan yang disediakan server terinstalasi di dalamnya. Sedangkan untuk *host* yang berfungsi sebagai penyerang (*attacker*), digunakan sebuah PC dengan sistem operasi Linux. IP address yang digunakan adalah 192.168.0.5 dengan subnet mask kelas C. Host ini diinstalasi berbagai program penyerang server seperti *exploit*, *scanner* dan *ping flooder*.

J. HASIL PENGUJIAN

Penetration Test Result

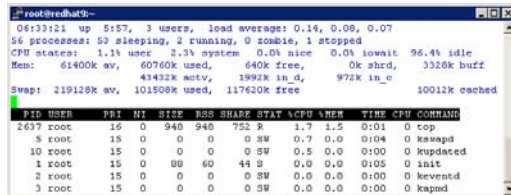
Penetration test yang dilakukan pertama kali adalah *Scanner/Banner Grabbing* dengan Nmap. Ketika dilakukan proses scanning dengan perintah `nmap -sS 192.168.0.1` dari komputer klien dengan Sistem Operasi Windows XP, sistem Firewall dan IDS langsung bereaksi memblokir akses tersebut. Hal yang sama juga terjadi saat pengujian dilakukan dengan Super Scan 4.0. Tampak pada gambar 4.12 pada bagian "Open TCP Ports 0" dan "Open UDP Ports 0", padahal saat *Firewall* tidak aktif akan terdeteksi "Open TCP Ports 6" dan "Open UDP Port 0" itu menunjukkan bahwa proses *Scanning/Banner Grabbing* gagal dilakukan saat *Firewall* aktif



Gambar 10 Tampilan Super Scan 4.0 saat proses scanning gagal

K. Analisa Beban CPU dan Memory

Berikut ini hasil analisa sistem yang menggunakan *Iptables* dan IDS aktif. Pemeriksaan dilakukan dengan command *top* atau *watch free* dari *shell* linux. Sistem menggunakan 61400 KB RAM, total yang terpakai adalah 60760 KB dan sisa 640 KB ketika *Iptables* dan *Snort* aktif.



```

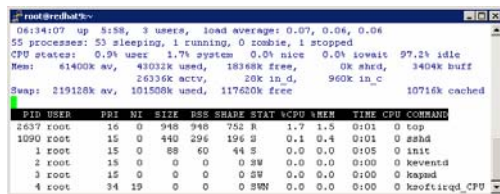
04:33:21 up 5:57, 3 users, load average: 0.14, 0.08, 0.07
55 processes: 53 sleeping, 2 running, 0 zombie, 1 stopped
CPU states: 1.1% user, 2.3% system, 0.0% nice, 0.0% wait, 96.4% idle
Mem: 61400k av, 60760k used, 640k free, 0k shrd, 3320k buff
Swap: 219120k av, 101500k used, 117620k free, 10012k cached

  PID USER      PR  NI  VIRT  RES  SHR  S  %CPU  %MEM     TIME  CPU COMMAND
 2637 root        16   0   948   948   752  R   1.7   1.5   0:01  0 top
    5 root        15   0   0     0   0  SW   0.7   0.0   0:04  0 ksmagd
   10 root        15   0   0     0   0  SW   0.5   0.0   0:00  0 kupdated
    1 root        15   0   0     0   0  SW   0.0   0.0   0:05  0 init
    2 root        15   0   0     0   0  SW   0.0   0.0   0:00  0 keventd
    3 root        15   0   0     0   0  SW   0.0   0.0   0:00  0 ksmagd

```

Gambar 11 Beban CPU dan Memory saat *iptables* dan *Snort* aktif

Ketika *session* *Snort* dihentikan dengan CTRL+C pada keyboard beban CPU dan Memory berkurang drastis menjadi : Total RAM terpakai 43032 KB dari 61400 KB dan sisa memory yang bisa dipakai menjadi 18360KB



```

04:34:07 up 5:58, 3 users, load average: 0.07, 0.04, 0.04
55 processes: 53 sleeping, 1 running, 0 zombie, 1 stopped
CPU states: 0.9% user, 1.7% system, 0.0% nice, 0.0% wait, 97.2% idle
Mem: 61400k av, 43032k used, 18360k free, 0k shrd, 3404k buff
Swap: 219120k av, 101500k used, 117620k free, 10716k cached

  PID USER      PR  NI  VIRT  RES  SHR  S  %CPU  %MEM     TIME  CPU COMMAND
 2637 root        15   0   948   948   752  R   0.1   1.5   0:01  0 top
 1090 root        15   0   440   296   196  S   0.1   0.4   0:01  0 shad
    1 root        15   0   0     0   0  SW   0.0   0.0   0:05  0 init
    2 root        15   0   0     0   0  SW   0.0   0.0   0:00  0 keventd
    3 root        15   0   0     0   0  SW   0.0   0.0   0:00  0 ksmagd
    4 root        34  19   0     0   0  SW   0.0   0.0   0:00  0 ksmagd_CPU

```

Gambar 12 Beban CPU dan Memory saat *iptables* dan *Snort* tidak aktif

Hal ini berarti sistem yang menjalankan *Iptables* dan *Snort* rata – rata menggunakan memory sekitar 17728 KB. Untuk beban CPU tidak terlalu signifikan perbedaannya dari gambar 4.9 dan 4.10 dapat dilihat bahwa ketika sistem keamanan diaktifkan CPU idle pada angka 96,4% atau hanya menggunakan sekitar 3,6% dari kekuatan CPU dan saat sistem keamanan di hentikan angka CPU idle menjadi 97, 2% atau 2,8% dari kekuatan CPU berarti beban sumber daya sistem yang menggunakan sistem keamanan ini hanya membutuhkan sekitar 0,8% berarti kurang dari 1% dari sumber daya CPU yang ada. Lonjakan-lonjakan yang ada terjadi ketika *routing daemon* melakukan *update tabel routing* atau menangani paket-paket yang besar. Selebihnya sumber daya CPU hanya *idle* pada titik tertentu sesuai dengan jenis serta kecepatan prosesor yang digunakan.

Analisa beban CPU dan *memory* diatas bisa berbeda-beda tergantung jumlah paket yang lalu lalang, demikian juga jumlah komputer klien yang terhubung dan *service* apa saja yang dijalankan di sistem komputer yang sedang di uji

L. Analisa Akurasi Deteksi

Seluruh *IP address* yang digunakan untuk menyerang dapat terdeteksi dengan baik.

Demikian juga dengan deteksi jenis serangan yang digunakan terdeteksi dengan benar. Pada gambar 4.7 tercatat *alert* dari 5 (lima) *source IP address* berarti ada 5 alamat IP yang melakukan penyerangan dan 11 (sebelas) alamat IP tujuan (*Destination IP Address*), sedangkan distribusi serangan adalah 4% serangan menggunakan paket TCP, 1% paket UDP dan 95% menggunakan paket ICMP. Log sistem di atas menunjukkan bahwa sistem memiliki akurasi yang cukup tinggi dalam mendeteksi serangan walaupun serangan dilakukan secara simultan dan beruntun. Tercatat pula *Unique Alerts* 27 (5 *Categories*) dan *total Number of Alerts* 9108.

M. KESIMPULAN

1. Membangun sistem keamanan jaringan komputer dengan *Firewall* dan IDS (*Intrusion Detection System*) ini dengan berbagai konfigurasi yang telah dijelaskan pada bab sebelumnya maka sangatlah mudah bagi Administrator jaringan untuk mengamankan sistem yang dibangun, khususnya jaringan yang menggunakan *server* atau *router* dengan sistem operasi Linux, dari usaha-usaha atau akses dari yang tidak berhak yang bertujuan untuk mengambil informasi secara tidak sah, atau bahkan merusak sistem secara keseluruhan.
2. Sistem keamanan jaringan dengan *Firewall* dan IDS ini merupakan kombinasi dua sistem keamanan yang tangguh dan dari berbagai uji coba yang dilakukan dengan berbagai program penyerang *server* seperti *exploit*, *scanner* dan *ping flood* telah terbukti mampu untuk menangkal berbagai upaya *attack* atau serangan yang dilakukan.

N. SARAN

Sistem deteksi penyusupan jaringan yang ada saat ini umumnya mampu mendeteksi berbagai jenis serangan tetapi tidak mampu mengambil tindakan lebih lanjut. Selain itu sistem yang ada pada saat ini tidak memiliki interaktivitas dengan administrator pada saat administrator tidak sedang mengadministrasi sistemnya. Hal ini merupakan suatu hal yang tidak efektif terutama pada saat sistem berada dalam kondisi kritis.

Demikian juga untuk IDS bisa dikembangkan lagi yaitu model sistem deteksi penyusupan jaringan secara otomatis dan interaktif atau biasa disebut dengan AIRIDS (*Automatic Interactive Reactive Intrusion Detection System*). Jika sistem AIRIDS merupakan suatu metode keamanan jaringan yang bertujuan untuk membentuk suatu arsitektur sistem keamanan yang terintegrasi antara *Intrusion Detection System (IDS)*, *Firewall System*, *Database System* dan *Monitoring System*. Sistem keamanan ini bertujuan melindungi jaringan dengan kemampuan merespon sesuai dengan kebijakan keamanan.

Keamanan jaringan adalah suatu keadaan yang harus dijaga terus menerus, karena tidak ada sistem yang bisa dipastikan benar-benar aman. Seperti pendapat Professor Eugene Spafford, pakar keamanan dari Center for Education and Research in Information Assurance and Security, Department of Computer Sciences Purdue University, "The only system which is truly secure is one which is switched off and unplugged. Locked in a titanium lined safe, buried in a concrete bunker, and is surrounded by very highly paid armed guards. Even then, I wouldn't stake my life on it." Maka dari itu upaya pengamanan secara terus – menerus harus selalu dilakukan oleh administrator jaringan komputer untuk melindungi sistemnya. Disarankan juga untuk selalu mengikuti perkembangan terbaru mengenai keamanan jaringan. Informasi bisa didapat dengan selalu aktif mengikuti Mailing List seperti BUGTRAQ, milis keamanan komputer terbesar di dunia atau mereview situs keamanan jaringan yang selalu ter-update dengan informasi terbaru mengenai bug dan vulnerabilities seperti Packet Storm Security packetstormsecurity.com, bisa juga ke website Security Team <http://www.securiteam.com>, dan Insecure <http://www.insecure.org> dan sebagainya.

DAFTAR PUSTAKA

- Brian Laing**, *How To Guide-Implementing a Network Based Intrusion Detection System*, Brain Laing Sovereign House, 2000
- Budi Raharjo**, *Keamanan Sistem Informasi Berbasis Internet*, PT INDOCISC, Jakarta, 1999
- Dani Firman Syah**, *Tip dan Trik Computer Hacking Edisi 1 – 2*, Ardi Publishing, Yogyakarta, 2004
- Firrar Utdirartatmo**, *Analisa Keamanan dan Vulnerabilitas Jaringan Komputer*, Penerbit Gava Media, Yogyakarta, 2005
- Gunawan Adi S.**, *Desain Dan Implementasi Sistem Deteksi Penyusupan Jaringan Secara Otomatis Dan Interaktif*, Institute Teknologi Bandung (ITB), 2004
- Ivan Suci Firmansyah**, *IP Network-Packet Shared Media pada Mesin Cluster Intrusion Detection System*, Institute Teknologi Bandung (ITB), Bandung, 2003
- Jhonsen dan Jhon Edison, ST**, *Membangun Wireless LAN*, PT. Elex Media Komputindo, Jakarta, 2005
- Jogiyanto. HM**, *Analisis dan Desain Sistem Informasi; Pendekatan Terstruktur Teori dan Praktek Aplikasi Bisnis*, Penerbit Andi Yogyakarta, Yogyakarta, 1999
- Kosasih Iskandarsjah dan Onno W. Purbo**, *Hacking dan PC Keamanan*, Majalah Neotek Edisi Agustus 2002
- Muchamad Sarosa dan Sigit Anggoro**, *Jaringan Komputer; Data Link, Network and Issue*, Institute teknologi Bandung, 2000
- Marty Roesch, dkk**, *Snort TM User Manual 2.3.3*, Sourcefire, Inc., 2005
- Nurma Evy Hendrayani, S.Si, M.Kom**, *Intisari Keamanan Komputer*, Magister Informatika Universitas Dian Nuswantoro, Semarang, 2003
- Oskar Andreasson**, *Iptables Tutorial 1.1.0*, Boingworld Organisation, 2001
- Peter L. dan Ronny S**, *Hacker Sebagai Penguji Sistem Keamanan*, <http://students.ukdw.ac.id/~22033120>
- Patrick Harper, CISSP**, *Snort, Apache, PHP, MySQL and Acid Install on RH9.0*, <http://www.InternetSecurityGuru.com>, 2003
- Reza Muhammad**, *Analisa Network dengan TCPDump*, www.ilmukomputer.com, 2003
- Richardus Eko Indrajit**, *Kajian Strategis Cost Benefit Teknologi Informasi*, Andi Offset, Yogyakarta, 2004
- R. Kresno Aji dan Agus Hartanto**, *Panduan Mudah System Administering Redhat Linux*, PT Elex Media Komputindo, Jakarta, 2004
- S'to, MCSE, CCNA**, *Seni Teknik Hacking 1 : Uncensored*, Penerbit Jasakom, Jakarta, 2005
- S. Kent., R. Atkinson.**, *Security Architecture for the Internet Protocol*, RFC 2401, November 1998.