RANCANG BANGUN PROTOTYPE KEAMANAN JARINGAN KOMPUTER DENGAN METODE IPS (*INTRUSION PREVENTION SYSTEM)*

(Skripsi)

Oleh

FARISY IDEHAM HANAFI

FAKULTAS TEKNIK

UNIVERSITAS LAMPUNG

BANDAR LAMPUNG

2017

ABSTRAK

RANCANG BANGUN PROTOTYPE KEAMANAN JARINGAN KOMPUTER DENGAN METODE IPS (*INTRUSION PREVENTION SYSTEM)*

Oleh

Farisy Ideham Hanafi

Jaringan komputer adalah jaringan telekomunikasi yang memungkinkan antar komputer untuk saling bertukar data. Belum adanya sebuah sistem untuk melakukan pencegahan tindakan peretasan yang mungkin akan dilakukan, menyebabkan dibutuhkannya suatu sistem untuk melakukan pengawasan dan pencegahan tindakan intrusi dalam jaringan Universitas Lampung yaitu *Intrusion Prevention System.* Snort adalah aplikasi yang digunakan sebagai IPS yang dapat meminimalisasi potensi kerusakan sistem yang akan mengganggu aktivitas akademik. PPDIOO (*prepare, plan, design, implementation, operate, and optimize*) milik CISCO adalah metode yang tepat untuk merancang sebuah sistem keamanan jaringan.

Pada penelitian ini telah berhasil dibangun sebuah *protoype* keamanan jaringan menggunakan Snort dengan *local rules* pada Ubuntu Server dengan *graphical alert system,* BASE (Basic Analysis and Security Engine) untuk melakukan upaya pencegahan intrusi. Dengan tambahan fitur *e-mail notification* dan data analisis menggunakan Splunk.

Hasil pengujian menunjukkan bahwa *Intrusion Prevention System Server* dapat bekerja dengan baik, efisien, dan handal. Hal ini dapat terlihat dengan akuratnya pemblokiran intrusi dengan *local rules* yang telah dibuat dan tidak terjadinya *system crash* pada saat pengujian berlangsung.

Kata kunci : *Intrusion Prevention System,* Snort, PPDIOO, Ubuntu Server, BASE, *e-mail notification,* Splunk, *local rules*.

ABSTRACT

COMPUTER NETWORK SECURITY PROTOTYPE'S DESIGN USING IPS (*INTRUSION PREVENTION SYSTEM)* METHOD

By

Farisy Ideham Hanafi

Computer network is a telecomunications network that allow computers to exchange data. The absence of a system to take preventive action for hacking, cause the need the intrusion prevention system in the network. Snort is used as an Intrusion Prevention Server application that can minimize potential damage to the system, wich is affected academic activities. PPDIOO (prepare, plan, design, implementation, operate and optimize) of CISCO is the proper method for designing a network security system.

This study has been successfully built a protoype network security using Snort with local rules on Ubuntu Server with a graphical alert system, BASE (Basic Analysis and Security Engine) to take steps to prevent intrusion. Some additional features for e-mail notification and data analysis using Splunk are included.

The test results showed that the Intrusion Prevention System Server can work well, efficient, and reliable. It can be seen by accurately blocking intrusions with local rules that have been made and no occurrence of system crashes during the tests.

Key words : Intrusion Prevention System, Snort, PPDIOO, Ubuntu Server, BASE, e-mail notification, Splunk, local rules.

RANCANG BANGUN PROTOTYPE KEAMANAN JARINGAN KOMPUTER DENGAN METODE IPS (*INTRUSION PREVENTION SYSTEM)*

Oleh

FARISY IDEHAM HANAFI

Skripsi

Sebagai Salah Satu Syarat untuk Mencapai Gelar

SARJANA TEKNIK

pada

Jurusan Teknik Elektro

Fakultas Teknik Universitas Lampung

FAKULTAS TEKNIK

UNIVERSITAS LAMPUNG

BANDAR LAMPUNG

2017

Judul Skripsi	:	**RANCANG BANGUN PROTOYPE KEAMANAN JARINGAN KOMPUTER DENGAN METODE IPS (*INTRUSION PREVENTION SYSTEM*)**
Nama Mahasiswa	:	Fariz Ildham Hanafi
Nomor Pokok Mahasiswa	:	1115031030
Program Studi	:	Teknik Elektro
Fakultas	:	Teknik

MENYETUJUI

1. Komisi Pembimbing

Ir. Hery Dian Septama, S.T.	**Raden Arum Setia P, S.Si., M.T.**
NIP. 19850915 200812 1 001	NIP. 19710114 199903 1 003

2. Ketua Jurusan Teknik Elektro

Dr. Ing. Ardian Ulvan, M.Sc.
NIP. 19731128 199903 1 005

MENGESAHKAN

1. **Tim Penguji**

   Ketua : **Ing. Hery Dian Septama, S.T.** .....

   Sekretaris : **Raden Arum Setia P, S.Si., M.T.** .....

   Penguji

   Bukan Pembimbing : **Gigih Forda Nama, S.T., M.T.I.** .....

2. **Dekan Fakultas Teknik Universitas Lampung**

Prof. Dr. Suharno, M.Sc.
NIP. 19620717 198703 100 2

Tanggal Lulus Ujian Skripsi : **10 April 2017**

SURAT PERNYATAAN

Dengan ini saya menyatakan bahwa dalam skripsi ini tidak terdapat karya yang pernah dilakukan oleh orang lain dan sepanjang sepengetahuan saya juga tidak terdapat karya atau pendapat yang ditulis atau diterbitkan oleh orang lain, kecuali secara tertulis diacu dalam naskah ini sebagaimana yang disebutkan di dalam daftar pustaka. Selain itu saya menyatakan pula bahwa skripsi ini dibuat oleh saya sendiri.

Apabila pernyataan saya tidak benar maka saya bersedia dikenai sangsi sesuai dengan hukum yang berlaku.

Bandar Lampung, 26 April 2017

Farisy Ideham Hanafi
NPM. 1115031020

RIWAYAT HIDUP

Penulis dilahirkan di Magelang Jawa Tengah pada tanggal 13 Maret 1993, sebagai anak pertama dari empat bersaudara, dari pasangan Ichromi dan Efi Jariyah. 1 tahun di Sekolah Dasar Negeri 2 Palapa Bandar Lampung lalu pindah ke Sekolah Dasar Negeri 3 Rajabasa Raya diselesaikan pada tahun 2005, Sekolah Menengah Pertama Negeri 29 Bandar Lampung diselesaikan pada tahun 2008, dan Sekolah Menengah Kejuruan Negeri 2 Bandar Lampung pada tahun 2011.

Penulis terdaftar sebagai mahasiswa Jurusan Teknik Elektro Fakultas Teknik Universitas Lampung pada tahun 2011 melalui Seleksi Nasional Masuk Perguruan Tinggi (SNMPTN). Selama menjadi mahasiswa, penulis aktif menjadi anggota Divisi Informasi dan Komunikasi di Himpunan Mahasiswa Teknik Elektro (HIMATRO), anggota Divisi *Marketing and Communication* di AIESEC Universitas Lampung, serta aktif sebagai asisten dan staf Laboratorium Permodelan dan Simulasi di Laboratorium Terpadu Teknik Elektro. Pada tahun 2015, penulis melakukan kerja praktek di CV. Prima Shakti Solusindo.

PERSEMBAHAN

Dengan rasa hormat, cinta dan sayangku

Ku dedikasikan karya sederhana ini untuk

Bapak dan Ibu :

Bapak Ichromi

&

Ibu Efi Jariyah

Terima kasih atas cinta, kasih sayang dan doa-nya

الْحِسَابُ يَقُومُ يَوْمَ وَلِلْمُؤْمِنِينَ وَلِوَالِدَيَّ لِي اغْفِرْ رَبَّنَا

"Ya Tuhan kami, beri ampunlah aku dan kedua ibu bapaku dan sekalian orang-orang mukmin pada hari terjadinya hisab (hari kiamat)". [QS Ibrahim 14:41]

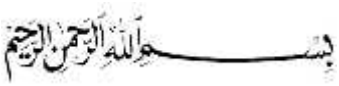
كَمَا ارْحَمْهُمَا رَبِّ وَقُل الرَّحْمَةِ مِنَ الذُّلِّ جَنَاحَ لَهُمَا وَاخْفِضْ صَغِيرًا رَبَّيَانِي

Dan rendahkanlah dirimu terhadap mereka berdua dengan penuh kesayangan dan ucapkanlah: "Wahai Tuhanku, kasihilah mereka keduanya, sebagaimana mereka berdua telah mendidik aku waktu kecil". [QS Al-Isra 16:24]

MOTTO

- Nikmat tuhan manalagi yang engkau dustakan ? (Bersyukurlah dengan apa yang telah diberikan).
- Di manapun kita berada, bagaimanapun keadaan kita, hanya satu yang harus selalu dikedepankan "KEJUJURAN". -Ichromi
- Harta jika diwariskan pasti akan habis namun "ILMU" yang bermanfaat akan kekal selamanya. -Efi Jariyah
- Do'a itu seperti mengayuh sepeda, selambat apapun kau mengayuh pasti akan sampai. - Anonymous
- Hasil tidak akan mengkhianati usaha, apa yang kau perbuat itu yang kau dapatkan. - Anonymous

SANWACANA



Alhamdulillah

Puji syukur ke hadirat Allah SWT, karena atas segala rahmat, hidayah, serta nikmat-Nya, penulis dapat menyelesaikan skripsi ini. Shalawat serta salam tercurah kepada Nabi Muhammad SAW sebagai tauladan umat manusia di dunia.

Skripsi dengan judul **"Rancang Bangun Prototype Keamanan Jaringan Komputer dengan Metode IPS (*Intrusion Prevention System*)"** disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Teknik pada Jurusan Teknik Elektro Fakultas Teknik Universitas Lampung. Ucapan terima kasih kepada **Bapak Ing, Hery Dian Septama, S.T.** dan **R. Arum Setia P., S.Si., M.T.** selaku dosen pembimbing yang telah banyak memberikan arahan, saran serta dorongan semangat dalam penyelesaian skripsi ini.

Dalam Kesempatan ini penulis mengucapkan terima kasih kepada :

1. Bapak Ichromi dan Ibu Efi J. tersayang yang telah memberikan kasih sayang, ilmu, do'a dan dukungan moril maupun materil sepanjang hidup penulis.
2. Adik tersayang Faisal, Farhan dan Faranisa atas dukungan dan do'anya.

3. Bapak Prof. Dr. Suharno, M.Sc., selaku Dekan Fakultas Teknik Universitas Lampung.
4. Bapak Dr. Ing. Ardian Ulvan, M.Sc., selaku Ketua Jurusan Teknik Elektro Universitas Lampung.
5. Bapak Dr. Herman Halomon Sinaga, S.T., M.T., selaku Sekretaris Jurusan Teknik Elektro Universitas Lampung.
6. Bapak Ing. Hery Dian Septama, S.T., selaku Pembimbing yang telah banyak memberikan bimbingan dan saran dalam penyelesaian skripsi ini.
7. Bapak Raden Arum Setia P., S.Si., M.T., selaku Pembimbing Pendamping yang telah banyak memberikan bimbingan dan saran hingga skripsi ini selesai.
8. Bapak Gigih Forda Nama, S.T., M.Ti., selaku Penguji yang telah banyak memberikan saran dan kritik yang membangun untuk skripsi ini.
9. Bu Dr. Dikpride Despa, S.T., M.T., selaku Pembimbing Akademik yang telah memberikan arahan selama penulis menempuh kuliah di Jurusan Teknik Elektro Universitas Lampung.
10. Mbak Ning atas bantuannya dalam mengurus kebutuhan administrasi dalam penulis menjadi mahasiswa.
11. Seluruh Staff dan pengajar di Jurusan Teknik Elektro Universitas Lampung yang telah memberikan ilmu maupun bimbingan selama penulis menjadi mahasiswa.
12. Rekan-rekan di Laboratorium Terpadu Teknik Elektro khususnya Lab Kom.
13. Almarhum Arif Awangga yang telah memberikan canda dan tawa kepada penulis.

14. Teman seperjuangan ElevenEngineer baik SKI, SIE, dan SEE yang selalu sabar menghadapi segala cobaan yaitu : ADHITYA PRATAMA, ADITYA RISKI EFENDI, ALBERTUS BAGUS P, ALFI HERI MADHON, ANANG RESTUNINGRAT, ANDREAS SIREGAR, ANNIDA PUSPA, Alm. ARIEF AWANGGA, CHOIRUDIN DWI JAYA, DARMA SETIAWAN, DENY FIRMANSYAH Z, DWI SATRIO WICAKSONO, ELIZA HARA, FANNY SIMATUPANG, FEKA R, FENTI TRIANI, FRIAN DANIEL PANJAITAN, GUSMAU RADO PRATAMA, HAJAR ALI MAHFUDHI, HAZENDA RENO IRAWAN, IMAM SYUHADA, KHOLIF FAUZI, M YAZIR GUSTARA, MARIYO YOSHUA, MINHAJJUL ABIDIN J, MUHAMAD AJI HILMI ANUGRAH, MUHAMMAD VITO JATI P, NICOLAS GATA JANU P, OCTARINA F, PETRUS PRASETYO, RAHMAT SHOLEH, RANI KUSUMA DEWI, REINHARD HUTABARAT, RESTU PRAYUDI, REZA NAUFAL LIAWAN, RYAN NOFERIAWAN, SUBASTIAN YUSUF P, SYUKUR RAMDHANI .S, YEREMIA LUHUR WIYOTO, YUNITA BAHATI, ADITYA HARTANTO, AGI REZKA PANTRY, AHMAD RIZKY ZARFANI, ALEX MUNANDAR, ALIN ADILAH, ANDI IRAWAN, ANDRIAN RIVANDA, APRIWAN RIZKI, ARROSYIQU BIK, DANI AHMAD FAUZI, DEDEN HASNUL AL ADRI, DIRYA ANDRIYAN, EDI SUPRIYANTO, FADILLAH HALIM R, FEBRY RAMOS SINAGA, FRISKY VOLINO ANDREAS, GRIENDA ELAN EGATAMA M, HABIB SUTRIHARJO, HAJRI TRI SAPUTRA, IDA BAGUS MADE DWIPAKRESNA, JULIAN DWI PRASETIO, M.HAVIF, MIFTAH

FARID, MOHAMAD FIKRI I., MUHAMAD RISKI FIRMANTO, NAJIB AMARO,NURHAYATI, OKA KURNIAWAN S., PRASETIA MUHHARAM, RANDI PRANATA, REINALDY AULIA K, REJANI ERWANDA, REYNOLD TJANDI, RICHARD MANUEL, SIGIT SANTOSO, SURYA PRATAMA, VINA APRILIA, YOGA PUTRA PRATHAMA, YUSUF AFANDI .

15. Para partner DOTA yang tak henti (Fadil, Hajar, Najib, Randi, Ryan a.k.a Peceng, ka Ir, ka Billy, Fandry, Arham, Roviq) kalian semua GGWP.
16. Semua anggota HIMATRO atas pengalaman yang sangat berharga.
17. Semua rekan Teknik Elektro, terima kasih untuk segalanya.
18. Dewi Ninda Wulandari, terima kasih.

Semoga Allah SWT membalas semua amal baiknya dan menghapus dosanya. Penulis menyadari bahwa skripsi ini jauh dari kesempurnaan, namun penulis berharap skripsi ini dapat berguna dan bermanfaat untuk kita semua, aamiin.

Bandar Lampung, Maret 2017

Penulis

Farisy Ideham Hanafi

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR ISTILAH

IDS = *Intrusion Detection System,* sebuah metode yang digunakan untuk mendeteksi sebuah sebuah penyusupan.

IPS = *Intrusion Prevention System,* sebuah metode yang digunakan untuk mendeteksi dan mencegah sebuah penyusupan.

MANET = *Mobile Ad Hoc Network,* sekumpulan *mobile node* yang terdesentralisasi yang mana proses pertukaran informasinya melalui media transmisi nirkabel / *wireless*.

PSO = *Particle Swarm Optimization,* adalah algoritma berbasis kecerdasan buatan (*Artificial Intelligence*) yang digunakan untuk menyelesaikan persoalan optimasi.

DDoS = *Distributed Denial of Service,* adalah sebuah usaha untuk membuat suatu sumber daya komputer menjadi tidak bisa dipakai oleh *user*-nya, dengan menggunakan ribuan *zombie system* yang 'menyerang' secara bersamaan.

Burst Attack = Percobaan *login* berulang-ulang dan terus menerus menggunakan *database* informasi yang telah dikumpulkan melalui *social engineering*.

POSIX = *Portable Operating System Interface for* UNIX, adalah sebuah standar yang dicetuskan oleh *Institute of Electical and Electronics Engineers* (IEEE) yang mendefinisikan sekumpulan layanan dalam sistem operasi.

UNIX = Sebuah sistem operasi komputer yang diawali dari *project Multics* (*Multiplexed Information and Computing Service*) pada tahun 1965 yang dilakukan *American Telephone and Telegraph* (AT&T), *General Electric* (GE), dan *Massachusetts Institute of Technology* (MIT), dengan biaya dari Departemen Pertahanan Amerika (*Departement of Defence Advenced Research Project*, DARPA)

I. PENDAHULUAN

1.1 Latar Belakang

Selama ini keamanan pada jaringan lokal yang ada di sekitar kita kurang diperhatikan dari ancaman yang mungkin saja ada untuk merusak, maupun mencuri data yang ada di lingkungan Universitas Lampung. Banyaknya mahasiswa yang aktif di jaringan Universitas Lampung dengan menggunakan perangkat pribadi, seperti *smartphone* maupun *personal computer* membuka peluang bagi para pelaku tindak kejahatan. Kejahatan yang dilakukan dapat berupa pengiriman paket data secara besar-besaran, atau biasa disebut *flooding* yang bertujuan untuk mengganggu transmisi data di jaringan. *Sniffing,* yaitu tindakan untuk mencari data yang berada di jaringan untuk mendapatkan informasi yang mungkin rahasia atau bersifat *privacy*. Mahasiswa yang terhubung di jaringan lokal juga sering melakukan *folder sharing* untuk memudahkan mereka dalam pengiriman data, yang tanpa disadari telah membuka pertahanan perangkat mereka dengan mematikan *firewall* dan memberikan hak penuh untuk melakukan perubahan pada data mereka. Hal ini pula yang menyebabkan cepatnya penyebaran *virus* ataupun *malware* dalam sebuah jaringan dengan pertahanan terbuka.

Sudah tidak dipungkiri lagi bahwa mahasiswa pada saat ini banyak menggunakan sarana *electronic mail* atau yang biasa disebut *e-mail* dalam kegiatan di dunia maya,

seperti untuk sekedar membuat akun sosial, mengirim tugas kuliah, maupun untuk sekedar bertukar informasi. Tak jarang informasi yang dikirim merupakan informasi penting yang bersifat rahasia seperti hasil penelitian, data pribadi, maupun data laporan. Seperti kasus yang diberitakan oleh laman www.kompasiana.com yang dikutip dari tabloid terbitan Unila yaitu Teknokra bahwa 25 Januari 2011 dosen Pendidikan Fisika, FKIP Unila mengadukan perubahan nilai kepada Ketua Program Studi Pendidikan Fisika serta DDoS *attack* yang pernah menyerang *server* Unila sehingga menyebabkan *system down*. Hal ini mengindikasikan bahwa peretas dapat menyerang berbagai aspek yang ada di dunia maya dengan kemampuan mumpuni yang mereka miliki.

Di dunia maya, banyak sekali tindakan kriminal yang dapat terjadi namun, dengan penanganan yang tepat dan peningkatan dan perawatan yang berkala dapat diminimalisasi kemungkinan buruk yang akan terjadi. IPS dalam dunia keamanan komputer memiliki arti *Intrusion Prevention System* yang berguna untuk melakukan pengawasan terhadap lalu lintas data di jaringan, mendeteksi aktivitas yang mencurigakan dan melakukan pencegahan dini terhadap intrusi atau kejadian yang dapat membuat lalu lintas data di jaringan tidak berjalan semestinya [1].

1.2 Tujuan Penelitian

Tujuan dari penelitian dan penyusunan laporan tugas akhir ini adalah :

Secara Umum

1. Menghasilkan sebuah alternatif sistem keamanan yang dapat digunakan pada jaringan Universitas Lampung

2. Melakukan upaya pembuatan sistem keamanan untuk melakukan pencegahan terjadinya peretasan ilegal pada Universitas Lampung
3. Meningkatan keamanan dalam lalu lintas jaringan Universitas Lampung
4. Melakukan upaya pengawasan lalu lintas data Universitas Lampung

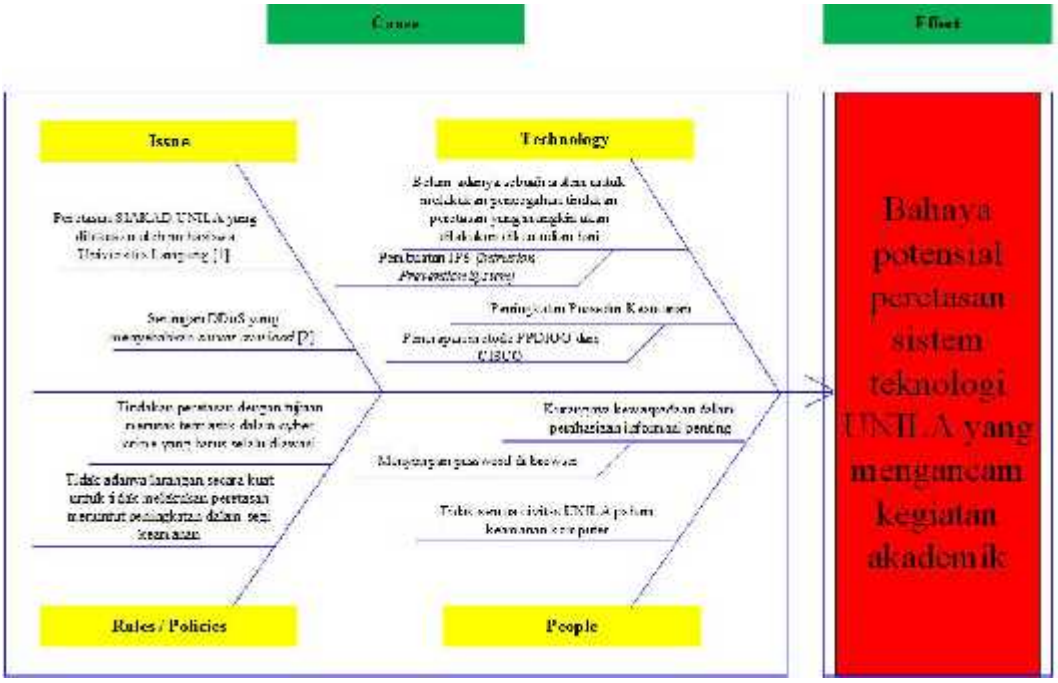
Secara Pribadi

1. Sebagai syarat untuk menyelesaikan studi di Teknik Elektro Universitas Lampung
2. Meningkatkan kemampuan peneliti dalam lingkup *networking.*

1.3 Manfaat Penelitian

Dengan dilakukannya penelitian tugas akhir ini diharapkan dapat dibangun sebuah sistem keamanan yang handal dalam pendeteksian dan pencegahan hal yang mengganggu lalu lintas data di Universitas Lampung sehingga tercipta rasa aman dalam melakukan kegiatan dalam dunia maya.

1.4 Rumusan Masalah



Gambar 1.1 *Fishbone Analysis Diagram*

Akar permasalahan yang didapat setelah dilakukan analisa menggunakan metode *Fishbone Diagram* adalah belum adanya sebuah sistem untuk melakukan pencegahan tindakan peretasan yang mungkin akan dilakukan, menyebabkan dibutuhkannya suatu sistem untuk melakukan pengawasan dan pencegahan tindakan intrusi dalam jaringan Universitas Lampung sehingga dapat meminimalisasi potensi kerusakan sistem yang akan mengganggu aktivitas akademik. Untuk itu dibutuhkan peningkatan keamanan dengan metode tertentu (peneliti menggunakan metode PPDIOO dari CISCO) agar tercipta rasa aman dalam melakukan aktivitas akademik yang menggunakan sistem jaringan Unila.

Pertanyaan yang timbul setelah melakukan analisa :

1. Bagaimana melakukan upaya untuk menghasilkan sebuah sistem keamanan pada lalu lintas jaringan komputer Univeritas Lampung ?
2. Bagaimana melakukan upaya pengawasan pada lalu lintas jaringan komputer di lingkungan Universitas Lampung ?
3. Bagaimana melakukan upaya pencegahan pada lalu lintas jaringan komputer di lingkungan Universitas Lampung ?
4. Bagaimana melakukan upaya peningkatan keamanan pada lalu lintas jaringan komputer di lingkungan Universitas Lampung ?

1.5 Batasan Masalah

Tugas akhir ini membahas perancangan sistem keamanan jaringan dengan batasan masalah sebagai berikut :

1. Peneliti menggunakan IPS (*Intrusion Prevention System*) sebagai metode pengamanan lalu lintas data pada jaringan lokal.
2. Pengamanan hanya di jaringan Laboratorium Teknik Elektro Unila.
3. Tidak membahas keamanan secara fisik.

1.6 Sistematika Penelitian

Penelitian tugas akhir ini disusun secara sistematis dengan urutan sebagai berikut :

Bab I Pendahuluan

Memuat latar belakang masalah, perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitianm sistematika penelitian, dan hipotesis.

Bab II Tinjauan Pustaka

Berisi teori-teori dari berbagai sumber pustaka yang mendukung dalam jaringan komputer, keamanan jaringan, keamanan komputer, dan konfigurasi komputer.

Bab III Metode Penelitian

Berisi tempat dan waktu pelaksanaan penelitian, metode yang digunakan dalam penelitian.

Bab IV Hasil dan Pembahasan

Berisi tentang data-data hasil penelitian dalam jaringan serta analisa terhadap data-data yang diperoleh.

Bab V Kesimpulan dan Saran

Berisi simpulan dari hasil analisa pada bab IV dan saran yang terkait dengan hasil penelitian untuk pengembangan berikutnya.

Daftar Pustaka

Berisi berbagai sumber pustaka yang digunakan untuk dijadikan referensi dalam penelitian tugas akhir ini.

Lampiran

Berisi dokumen-dokumen yang mendukung dalam penelitian.

II. TINJAUAN PUSTAKA

2.1 Keamanan Komputer

Gollmann pada tahun 1999 dalam bukunya "Computer Security" menyatakan bahwa, "Keamanan komputer adalah berhubungan dengan pencegahan dini dan deteksi terhadap tindakan pengganggu yang tidak dikenali dalam sistem komputer". Pencegahan dapat menggunakan *firewall*, sedangkan pendeteksian dapat menggunakan IDS (*Intrusion Detection System*) dan penggabungan dari kedua metode itu adalah IPS (*Intrusion Prevention System*) [2].

2.1.1 *Intrusion Prevention System* (IPS)

Intrusion Prevention System (IPS), adalah pendekatan yang sering digunakan untuk membangun sistem keamanan komputer. IPS mengkombinasikan teknik *firewall* dan metode *Intrusion Detection System* (IDS) dengan sangat baik. Teknologi ini dapat digunakan untuk mencegah serangan yang masuk ke jaringan lokal dengan memeriksa dan mencatat semua paket data serta mengenali paket dengan sensor, di saat serangan telah teridentifikasi, IPS menolak akses (*block*) dan mencatat (*loging*) semua paket data yang teridentifikasi tersebut. Jadi IPS bertindak sepeti layaknya *firewall* yang melakukan *allow* dan *block* yang dikombinasikan seperti IDS yang dapat mendeteksi paket secara detail. IPS menggunakan

signatures untuk mendeteksi *traffic* di jaringan dan terminal, di mana pendeteksian paket yang masuk dan keluar (*inbound-outbound*) dapat dideteksi sedini mungkin sebelum merusak atau mendapatkan akses ke dalam jaringan lokal [3].

2.1.2 *Intrusion Detection System* (IDS)

IDS (*Intrusion Detection System*) adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS digunakan untuk mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS (*Intrusion Detection System*) sendiri mempunyai beberapa pengertian yaitu [3]:

1. Sistem untuk mendeteksi adanya *intrusion* yang dilakukan oleh *intruder* (pengganggu atau penyusup) dalam jaringan. Pada awal serangan, *intruder* biasanya hanya mencari data. Namun, pada tingkat yang lebih serius *intruder* berusaha untuk mendapat akses ke sistem seperti membaca data rahasia, memodifikasi data tanpa permisi, mengurangi hak akses ke sistem sampai menghentikan sistem.
2. Sistem keamanan yang bekerja bersama *firewall* untuk mengatasi *Intrusion*. *Intrusion* itu sendiri didefinisikan sebagai kegiatan yang bersifat *anomaly*, *incorrect*, *inappropriate* yang terjadi di jaringan atau di *host* tersebut. *Intrusion* tersebut kemudian diubah menjadi *rules* ke dalam IDS (*Intrusion Detection System*).
3. Sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan.

Ada dua jenis IDS yaitu :

1. NIDS (*Network Based Intrusion Detection System*)

   Network-based Intrusion Detection System adalah ketika 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.

2. HIDS (*Host Based Intrusion Detection System*)

   Host-based Intrusion Detection System adalah ketika aktivitas sebuah *host* jaringan individual akan dipantau apakah terjadi sebuah percobaan serangan atau penyusupan ke dalamnya atau tidak. HIDS sering diletakkan pada *server* - *server* kritis di jaringan, seperti halnya *firewall*, *web server*, atau *server* yang terkoneksi ke internet.

2.1.3 *Firewall*

Firewall pada dasarnya merupakan suatu alat yang bersifat melindungi, jika seseorang akan berhubungan dengan jaringan komputer dan ingin mendapat hak

akses yang aman, *firewall* merupakan salah satu pelindung yang dibutuhkan. Pada dasarnya ada tiga hal yang perlu dilindungi, di antaranya [4]:

1. Data (Informasi)

   Data merupakan hal yang berharga yang perlu untuk dilindungi, pertukaran data di dunia maya (internet) merupakan hal yang sering dimanfaatkan oleh orang yang tidak bertanggung jawab, sebagai contoh, jika suatu perusahaan mengirim data yang mempunyai rahasia dan dalam pengirimannya disadap atau dihancurkan oleh orang lain, maka rahasia dari perusahaan tersebut akan menjadi milik umum.

2. *Resources* (Sumber Daya)

   Pada organisasi sosial banyak memberikan ruang *hardisk* untuk umum dengan mengharapkan terima kasih dan publisitas, namun bukan berarti mereka aman dari gangguan.

3. *Reputation*

   Hacker biasanya menggunakan identitas orang lain untuk melakukan kejahatan pada jaringan komputer sehingga membuat reputasi dari orang tersebut rusak.

2.1.4 Jenis Serangan pada Sistem Komputer

Ada banyak jenis serangan yang terjadi pada sistem komputer, di antaranya [4]:

1. *Intrusion*

   Serangan yang paling umum pada sistem komputer adalah *intrusion* (penyusup) seorang penyerang dapat menggunakan sistem komputer yang

kita miliki. Sebagian penyerang jenis ini menginginkan akses sebagaimana halnya pengguna yang memiliki hak untuk mengakses sistem dan seolah mereka adalah *user* yang sah.

2. *Denial of Service*

   Merupakan suatu istilah yang diberikan untuk upaya serangan dengan cara menurunkan kinerja susatu sistem komputer secara terus menerus. Serangan seperti ini bertujuan untuk membuat *server* korban menjadi kewalahan dalam melayani permintaan yang terkirim dan berakhir dengan penghentian aktivitas komputer. DoS juga merupakan serangan yang dilancarkan melalui paket tertentu dengan jumlah yang sangat banyak dengan maksud mengacaukan jaringan target.

3. *Information Theft*

   Pada umumnya *information theft* merupakan suatu kejahatan komputer yang bertujuan mencari informasi dari komputer korban.

2.1.5 Jenis Program Pencurian Informasi

Program-program yang berhubungan dengan pencurian informasi ini banyak terdapat di internet seperti [4]:

1. *Sniffer*

   Suatu program yang sifatnya melakukan pencurian atau penyadapan data. Meskipun data tidak dicuri secara fisik (hilang), *sniffer* sangat berbahaya

karena dia dapat digunakan untuk menyadap *password* dan informasi yang sensitive. Ini merupakan serangan terhadap aspek *privacy*.

2. *Intelligence*

   Intelligence merupakan *hacker* atau *cracker* yang merupakan suatu kegiatan mengumpulkan segala informasi yang berkaitan dengan sistem target.

3. *Back Door*

   Merupakan suatu akses yang khusus dibuat oleh seorang *programmer* sehingga dapat masuk ke dalam sistem. Tidak semua *programmer* mengerti perintah dalam sistem operasi, di dalam sistem operasi inilah programmer memasukkan perintah tertentu (yang biasanya disisipkan dalam program yang tidak jelas) namun tidak terlalu mengganggu kinerja sistem pada awalnya. Pada saat dibutuhkan *listing* program ini dijalankan dan dengan menggunakan fasilitas jaringan komputer untuk mendapatkan akses yang sama dengan pemilik yang sah.

4. *Cyber Espionage*

   Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran.

5. *Social Engineering*

   Mencari berbagai informasi yang berhubungan dengan target/korban dari semua detail kehidupannya baik dari dunia maya maupun dunia nyata. Biasanya informasi tersebut digunakan untuk melakukan *brute-forcing* (memasukkan *password* secara acak) untuk mendapatkan hak akses baik *e-mail* maupun akun lainnya.

2.1.6 Jenis Penyerang

Jenis – jenis penyerang yang banyak terdapat di internet seperti [4]:

1. *Joyriders*

   Penyerang yang merasa iseng dan ingin memperoleh kesenangan dengan cara menyerang sistem.

2. *Vandal*

   Penyerang bertujuan untuk merusak sistem yang bertujuan untuk mendapatkan uang, kepopuleran, data penting, dan menghancurkan atau menghapus informasi yang tersisa dalam sistem tersebut.

3. *Scorekeeper / Script Kiddies*

   Penyerang jenis ini hanya bertujuan untuk mendapatkan reputasi dengan cara meng-*crack* sistem sebanyak mungkin.

4. *Cryptanalysis*

   Merupakan bagian dari kriptografi, dan merupakan orang yang mencoba memecahkan kode yang ada.

5. *Developed Kiddie*

   Sebutan untuk kelompok yang masih remaja, mereka membaca metode dan cara *hack* hingga berhasil dan memamerkan keberhasilannya. Pada umumnya masih menggunakan GUI (*Graphic User Interface*) tanpa mampu menemukan lubang pada keamanan sistem operasi.

6. *Hacker*

Seseorang yang mencari kelemahan dan sangat memahami logika pemrogramman dan konsep jaringan komputer. Aktivitas mereka disebut *hacktivism* yang dilakukan untuk mencari simpati tertentu.

2.1.7 Metode Pendeteksian Intrusi

Metode yang banyak digunakan dalam pendeteksian antara lain [4] :

1. *Signature Based Intrusion Detection System*

   Pada metode ini, telah tersedia daftar *signature* yang dapat digunakan untuk menilai apakah paket yang dikirimkan berbahaya atau tidak. Sebuah paket data akan dibandingkan dengan daftar yang sudah ada. Metode ini melindungi sistem dari jenis-jenis serangan yang sudah diketahui sebelumnya. Oleh karena itu, untuk tetap menjaga keamanan sistem jaringan komputer, data *signature* yang ada harus tetap ter-*update*.

2. *Anomaly Based Intrusion Detection System*

   Pada metode ini, terlebih dahulu harus melakukan konfigurasi terhadap IDS dan IPS, sehingga IDS dan IPS dapat mengetahui pola paket seperti apa saja yang akan ada pada sebuah sistem jaringan komputer. Sebuah paket anomali adalah paket yang tidak sesuai dengan kebiasaan jaringan komputer tersebut. Apabila IDS (*Intrusion Detection System*) dan IPS (*Intrusion Prevention System*) menemukan ada anomali pada paket yang diterima atau dikirimkan, maka IDS dan IPS akan memberikan peringatan pada pengelola jaringan (IDS) atau menolak paket tersebut untuk diteruskan (IPS). Untuk metode ini, pengelola jaringan harus terus menerus memberitahu IDS dan

IPS bagaimana lalu lintas data yang normal pada sistem jaringan komputer tersebut, untuk menghindari adanya salah penilaian oleh IDS (*Intrusion Detection System*) atau IPS (*Intrusion Prevention System*).

2.2 Sistem Operasi

Ada beberapa sistem operasi yang umum digunakan salah satunya adalah Linux. Linux adalah suatu sistem operasi yang bersifat multi *user* dan multi *tasking*, yang dapat berjalan di berbagai *platform* termasuk prosesor Intel 386 maupun yang lebih tinggi. Sistem operasi ini mengimplementasikan standar POSIX. Linux dapat berinteroperasi secara baik dengan sistem operasi yang lain, termasuk Apple, Microsoft dan Novell. Nama Linux sendiri diturunkan dari pencipta awalnya, Linus Torvalds, yang sebetulnya mengacu pada suatu kumpulan *software* lengkap yang bersama-sama dengan kernel menyusun suatu sistem operasi yang lengkap. Lingkungan sistem operasi ini mencakup ratusan program, termasuk kompiler, interpreter, editor dan utilitas. Perangkat bantu yang mendukung konektifitas, ethernet, SLIP dan PPP dan interoperabilitas. Produk perangkat lunak yang handal (*reliable*), termasuk versi pengembangan terakhir. Kelompok pengembang yang tersebar di seluruh dunia yang telah bekerja dan menjadikan Linux portabel ke suatu *platform* baru, begitu juga mendukung komunitas pengguna yang memiliki beragam kebutuhan dan juga pengguna dapat turut serta bertindak sebagai tim pengembang sendiri.

Perbandingan Linux Dengan OS Lain

Linux disusun berdasarkan standar sistem operasi POSIX yang sebenarnya diturunkan berdasarkan fungsi kerja UNIX. UNIX kompatibel dengan Linux pada level *system call*, ini berarti sebagian besar program yang ditulis untuk UNIX atau Linux dapat direkompilasi dan dijalankan pada sistem lain dengan perubahan yang minimal. Secara umum dapat dikatakan Linux berjalan lebih cepat dibanding UNIX lain pada *hardware* yang sama. Dan lagi UNIX memiliki kelemahan yaitu tidak bersifat *free*.

MS-DOS memiliki kemiripan dengan Linux yaitu *file system* yang bersifat hirarkis. Tetapi MS-DOS hanya dapat dijalankan pada prosesor x86 dan tidak mendukung multi *user* dan multi *tasking*, serta tidak bersifat *free*. Juga MSDOS tidak memiliki dukungan yang baik agar dapat berinteroperasi dengan sistem operasi lainnya, termasuk tidak tersedianya perangkat lunak *network*, program pengembang dan program utilitas yang ada dalam Linux.

MS Windows menawarkan kemampuan grafis yang ada pada Linux termasuk kemampuan *networking* tetapi tetap memiliki kekurangan yang ada pada MS-DOS. Windows NT yang juga tersedia untuk Digital Alpha selain prosesor x86. Namun Windows NT ini masih juga memiliki beberapa kekurangan yang telah ada pada MS-DOS. Waktu untuk menemukan suatu *bug* dalam suatu system operasi ini tak sebanding dengan harga yang harus dibayar. Sistem operasi Apple untuk Macintosh hanya dapat berjalan di sistem Mac. Juga memiliki kekurangan dari sisi ketersediaan perangkat bantu pengembang (*development tool*) dan juga kurang dapat secara mudah untuk berinteroperasi dengan sistem operasi lainnya. Apple juga telah memungkinkan Linux dapat dijalankan pada PowerMac [5].

2.3 Jaringan Komputer

Jaringan komputer adalah jaringan telekomunikasi yang memungkinkan antar komputer untuk saling bertukar data. Tujuan dari jaringan komputer adalah agar dapat mencapai tujuannya, setiap bagian dari jaringan komputer dapat meminta dan memberikan layanan (*service*). Pihak yang meminta/menerima layanan disebut klien (*client*) dan yang memberikan/mengirim layanan disebut pelayan (*server*). Desain ini disebut dengan sistem *client-server*, dan digunakan pada hampir seluruh aplikasi jaringan komputer.

Dua buah komputer yang masing-masing memiliki sebuah kartu jaringan, kemudian dihubungkan melalui kabel maupun nirkabel sebagai medium transmisi data, dan terdapat perangkat lunak sistem operasi jaringan akan membentuk sebuah jaringan komputer yang sederhana. Apabila ingin membuat jaringan komputer yang lebih luas lagi jangkauannya, maka diperlukan peralatan tambahan seperti *Hub*, *Bridge*, *Switch*, *Router*, *Gateway* sebagai peralatan interkoneksinya.

2.3.1 TCP/IP

Beberapa materi yang digunakan adalah *subnetting* atau pembagian kelas IP. Subnetting adalah suatu proses untuk memecah suatu jaringan IP jaringan ke Sub Jaringan yang lebih kecil atau juga dapat diartikan sebagai metode yang dilakukan untuk membagi blok setiap alamat IP address menjadi beberapa blok IP address.

TCP/IP membagi IP menjadi lima kelas, yaitu:

1. Kelas A

   8 bit pertama merupakan *bit network* sedangkan 24 bit terakhir merupakan *bit host*.

2. Kelas B

   16 bit pertama merupakan *bit network* sedangkan 16 bit terakhir merupakan *bit host*.

3. Kelas C

   24 bit pertama merupakan *bit network* sedangkan 8 bit terakhir merupakan *bit host*.

4. Kelas D

   Kelas D digunakan untuk *multicast address*, yakni sejumlah komputer yang memakai bersama suatu aplikasi. Penggunaan *multicast address* yang sedang berkembang saat ini adalah aplikasi *real-time video conference* yang melibatkan lebih dari dua *host* (*multipoint*), menggunakan *Multicast Backbone* (MBone).

5. Kelas E

   Kelas E (4 bit pertama adalah 1111 atau sisa dari seluruh kelas). Pemakaiannya dicadangkan untuk kegiatan eksperimental.

2.3.2 Topologi Jaringan

Topologi jaringan atau arsitektur jaringan adalah gambaran perencanaan hubungan antar komputer dalam *Local Area Network*, yang umumnya menggunakan kabel sebagai media transmisi, dengan konektor, *ethernet* card dan perangkat pendukung lainnya. Topologi jaringan memberikan gambaran bagaimana komputer-komputer

dan perangkat jaringan komputer lainnya saling dihubungkan. Jaringan yang digunakan di Universitas Lampung adalah jenis topologi *star*.

1. Topologi *Star*

   Karakteristik dari topologi jaringan ini adalah *node* (*station*) berkomunikasi langsung dengan station lain melalui *central node* (*hub/switch*), *traffic data* mengalir dari *node* ke *central node* dan diteruskan ke *node* (*station*) tujuan. Jika salah satu segmen kabel putus, jaringan lain tidak terputus.

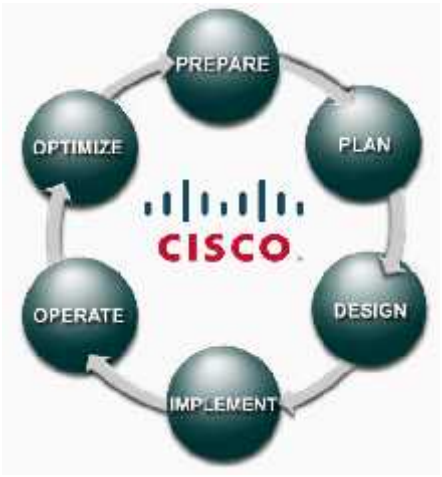
   Keuntungan:

   1. Akses ke *station* lain (*client* atau *server*) cepat
   2. Dapat menerima *workstation* baru selama port di *central node* (*hub*/*switch*) tersedia.
   3. *Hub*/*switch* bertindak sebagai konsentrator.
   4. *Hub*/*switch* dapat disusun seri (bertingkat) untuk menambah jumlah *station* yang terkoneksi di jaringan.
   5. *User* dapat lebih banyak dibanding topologi *bus*, maupun *ring*.

   Kerugian:

   1. Bila *traffic* data cukup tinggi dan terjadi *collision*, maka semua komunikasi akan ditunda, dan koneksi akan dilanjutkan/dipersilahkan dengan cara *random*, apabila *hub*/*switch* mendeteksi tidak ada jalur yang sedang dipergunakan oleh *node* lain. [6].

2.4 PPDIOO (CISCO Lifecycle Service)



Gambar 2.1 PPDIOO Cisco Lifecycle Service [6]

PPDIOO adalah sebuah metode yang digunakan oleh Cisco dalam melakukan pelayanan yang terus menerus. Dalam hal ini peneliti menggunakannya dalam melakukan layanan keamanan jaringan pada Unversitas Lampung. Ada enam tahap yang dilakukan ketika menerapkan metode PPDIOO yaitu *prepare*, *plan, design, implementation*, *operate* dan, *optimize* [6].

2.4.1 Prepare (Persiapan)

Pada fase ini peneliti menetapkan kebutuhan dari jaringan Universitas Lampung pada bagian keamanan sesuai dengan *issue* yang telah terjadi dan dan yang akan terjadi. Dengan merencanakan strategi yang didukung dengan sumberdaya yang tersedia di Universitas Lampung.

2.4.2 Plan (Perencanaan)

Pada fase ini peneliti melakukan identifikasi jaringan berdasarkan tujuan, fasilitas (sumber daya), dan kebutuhan. Perencanaan penelitian untuk tugas yang dikelola, pihak yang bertanggung jawab, *milestones*, dan semua kebutuhan untuk melakukan desain dan implementasi. Fase ini terus diperbarui sesuai dengan siklus yang sedang berjalan.

2.4.3 Design (Desain)

Desain jaringan yang dikembangkan sesuai dengan perencanaan yang telah dibuat. Hasil dari fase ini adalah diagram jaringan dan daftar peralatan yang digunakan. Tahap ini harus disetujui untuk segera melakukan tahap implementasi.

2.4.4 Implementation (Implementasi)

Melakukan instalasi dan konfigurasi sesuai dengan desain. Perangkat mengganti atau menambah sumber daya yang ada, setiap langkah yang dilakukan harus memiliki deskripsi, rincian pelaksanaan, dan perkiraan wakt penyelesaian. Evaluasi dilakukan dan apabila terjadi kegagalan maka dilakukan *rollback* atau pengulangan langkah – langkah dan pencarian informasi sebagai referensi tambahan. Pada tahap ini harus dilakukan pengujian (dengan *penetration test*, maupun penggunaan aplikasi seperti BASE) sebelum dilanjutkan ke fase operasional.

2.4.5 Operate (Operasional)

Pengelolaan dan *monitoring* pada komponen jaringan, pemeliharaan *routing*, *upgrading*, identifikasi dan koreksi jika terjadi kesalahan pada jaringan. Tahap ini adalah pengujian dari desain yang telah dibuat, dengan memantau kinerja, stabilitas, deteksi kesalahan, koreksi konfigurasi, dan pengumpulan data untuk digunakan pada fase optimalisasi.

2.4.6 Optimize (Optimalisasi)

Mempelajari data yang telah ada untuk selanjutnya melakukan identifikasi dan penyelesaian masalah sebelum mengganggu jaringan secara luas. Pada fase ini dimungkinkan untuk melakukan modifikasi desain jaringan jika terlalu banyak masalah yang ditimbulkan, dan melakukan perbaikan pada bagian aplikasi (*software*). Dan jika telah dilakukan modifikasi akan menuntut perkembangan jaringan tersebut ke awal fase pada siklus PPDIOO [6].

2.5 Penelitian Terdahulu

Penelitian yang dilakukan oleh Davood Kheyri dan Mojtaba Karami [7] membahas tentang *Anomaly-Based Intrusion Detection in* MANET *(Mobile Ad Hoc Networks).* Mereka juga melakukan analisa dalam penggunaan teknik yang tepat untuk mengatasi masalah penyusupan di jaringan nirkabel tersebut. *Anomaly-Based Detection* adalah salah satu teknik yang dapat digunakan dalam implementasi IDS *(Intrusion Detection Sysytem)*, lalu melakukan evaluasi untuk memilih teknik yang

tepat untuk diimplementasikan ke dalam MANET, serta keuntungan dan kerugian yang dihasilkan untuk bisa memberikan solusi dalam masalah keamanan maupun penelitian lanjutan.

Dalam penelitian tugas akhir ini dibahas sistem keamanan pada jaringan nirkabel yang ada di Universitas Lampung. Sistem ini menggunakan teknologi IPS (*Intrusion Prevention System*), yang merupakan pengembangan dari IDS. Penelitian dilakukan di dalam sistem operasi Ubuntu Server 16.04 dan fokus terhadap keamanan jaringan komputer pada Unila.

Pada penelitian lain yang dilakukan oleh Ahmed A. Engar, Dowlat A. El A. Mohamed, dan Fayed F. M. Ghaleb [8] yang membahas tentang cara untuk mendapatkan deteksi yang cepat dan akurat pada NIDS (*Network Intrusion Detection System*). Mereka menggunakan algoritma PSO (*Particle Swarm Optimization*) di mana dengan menggunakan algoritma tersebut dapat memaksimalkan akurasi pendeteksian sekaligus meminimalisasi waktu yang digunakan dalam proses deteksi. Metode tersebut mendapatkan hasil peningkatan performa sebesar 99.17 % dan peningkatan waktu sebanyak 11.65 detik. Penelitian ini memberi pengetahuan kepada peneliti bahwa proses pendeteksian dalam skala besar membutuhkan waktu yang cukup banyak sehingga perlu dilakukan optimalisasi dalam prosesnya.

Penelitian selanjutnya, yang dilakukan oleh Daniel Massa dan Raul Valverde [9] yang membahas tentang *A Fraud Detection System Based on Anomaly Intrusion Detection Systems for E-Commerce Applications*. Dalam penelitian ini mereka mengatakan bahwa dengan meningkatnya transaksi barang dan jasa membuat

tingkat penyerangan pada sistem keamanan *online* ikut meningkat. Tempat pelelangan dan jual beli *online* adalah tempat yang paling terlihat tingkat peningkatan kegiatan penipuannya. Banyak transaksi penipuan yang berhasil dilakukan dalam penyusupan komputer walaupun tingkat kesadaran akan hal ini sudah mulai meningkat. Penelitian yang mereka lakukan bertujuan untuk memprediksi penyusupan pada komputer khususnya dalam aplikasi *web*.

Penelitian tersebut banyak membahas metode penipuan yang dilakukan di dunia maya yang sangat dibutuhkan peneliti dalam melakukan pencegahan terhadap tindakan penyusupan, serta bagaimana membangun sebuah sistem yang dapat memprediksi aktifitas penipuan di dunia maya.

Pada penelitian yang dilakukan Tati Ernawati [10] yang melakukan analisis visualiasi data keamanan jaringan membahas tentang aktivitas monitoring keamanan jaringan yang akan menjadi masalah besar apabila data yang diolah sangat banyak sementara analisis dilakuka secara manual. Ia menjelaskan bahwa mayoritas pengguna jaringan tidak memiliki latar belakang dalam dunia keamanan jaringan yang mengakibatkan kelalaian dalam melakukan monitoring dan mengidentifikasi masalah pada jaringan yang kompleks. Banyak pengguna yang terlambat menyadari ketika komputer mereka sudah terserang virus, maupun aplikasi yang tidak diinginkan dan terlihat mencurigakan bermunculan.

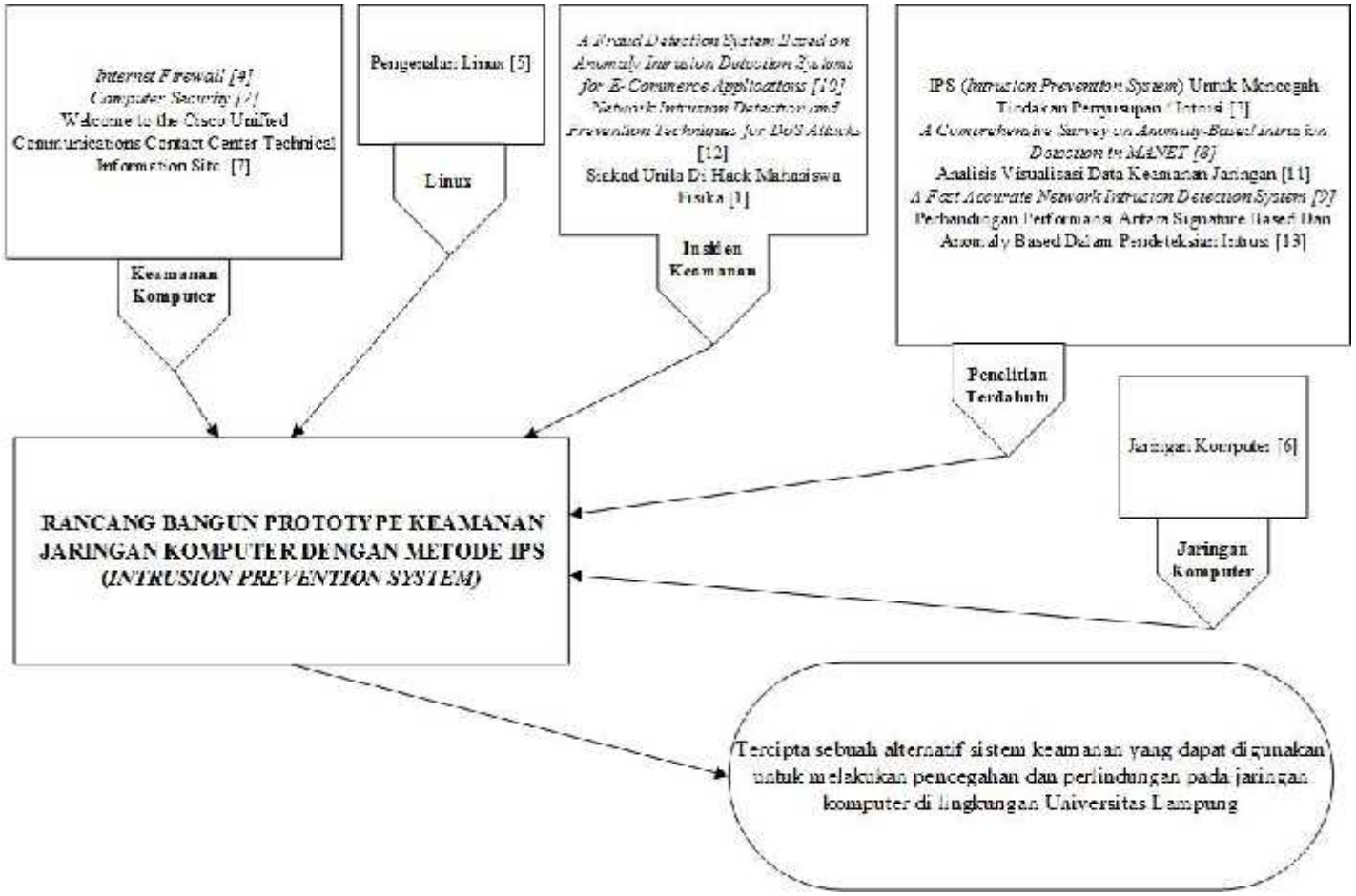
Pada penelitian tersebut menjelaskan tentang bagaimana memvisualisasikan data keamanan jaringan komputer berbasis teks/numerik dan visual. Yang sangat berguna bagi peneliti dalam melakukan pengambilan dan analisis data.

Dan pada penelitian yang dilakukan oleh Suchita Patil dan Dr. B. B. Meshram [11] tentang *Network Intrusion Detection and Prevention Techniques for DoS Attacks* yang membahas tentang apa yang dilakukan sistem pendeteksian dan pencegahan dalam menganalisa paket yang datang dan pergi melalui jaringan. Dalam penelitian ini terdapat ide pendeteksian serangan DoS. Dalam dunia jaringan banyak sekali tipe dari serangan DoS yang datang dan *Services* yang diinterupsi. Penelitian ini memberikan pengetahuan kepada peneliti bagaimana DoS itu bekerja dan cara penangannya.

Pada penelitian yang dilakukan oleh Noviana Sagita, Niken Dwi Cahyani, Fazmah Arif Yulianto [12] tentang Perbandingan Performansi Antara *Signature Based* Dan *Anomaly Based* dalam pendeteksian intrusi, terdapat kesimpulan sebagai berikut:

1. Dari sisi akurasi, IDS *Signature* bisa mendeteksi semua jenis serangan (*port scanning, exploit,* dan *denial of service*), sedangkan IDS *Anomaly* hanya bisa mendeteksi serangan *denial of service*.
2. Dari sisi penggunaan *resource*, IDS Signature menggunakan *resource* RAM yang lebih besar, sedangkan IDS *Anomaly* menggunakan *resource* CPU yang lebih besar.
3. Dari sisi kesalahan deteksi, IDS *Signature* tidak ditemukan *false positive* maupun *false negative*, sedangkan pada IDS *Anomaly* ditemukan *false positive* dan *false negative*.

Sehingga dari penelitian tersebut peneliti dapat menentukan metode pendeteksian mana yang lebih baik digunakan dalam penelitian yang peneliti lakukan yaitu menggunakan *signature based intrusion detection system*.



G**ambar 2.2** *Theoretical Framework*

III. METODE PENELITIAN

3.1 Waktu dan Tempat Penelitian

Tempat : Laboratorium Terpadu Teknik Elektro

3.2 Alat dan Bahan

Ada Beberapa alat dan bahan yang dibutuhkan peneliti dalam melakukan penelitian ini yaitu :

3.2.1 Perangkat Keras

a. Spesifikasi komputer yang digunakan untuk *server* adalah sebagai berikut :

Tabel 3.1 Spesifikasi Komputer

Spesifikasi	Jumlah/Kapasitas	Fungsi
Prosesor Intel Xeon	1	Melakukan olah data pada komputer
RAM	6 GB	Media penyimpanan data sementara sebelum diproses oleh prosesor
Hardisk	500 Gb	Media penyimpanan data dan informasi
LAN *Card*	2	Menghubungkan komputer ke dalam jaringan

b. *Notebook* dengan spesifikasi sebagai berikut :

Tabel 3.2 Spesifikasi *Notebook*

Spesifikasi	Jumlah/Kapasitas	Fungsi
Prosesor Intel Core i3	1	Melakukan olah data pada komputer
RAM	4 GB	Media penyimpanan data sementara sebelum diproses oleh prosesor
Hardisk	500 GB	Media penyimpanan data dan informasi
LAN *Card*	2	Menghubungkan komputer ke dalam jaringan
Wireless Adapter	1	Menghubungkan komputer ke dalam jaringan tanpa kabel

3.2.2 Perangkat Lunak

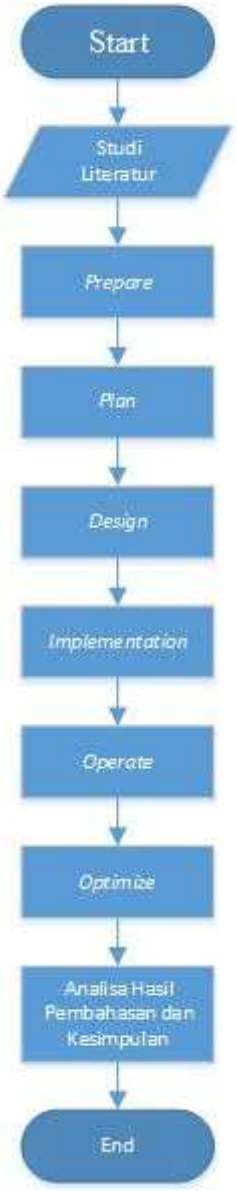
Tabel 3.3 Spesifikasi Perangkat Lunak

Spesifikasi	Jumlah	Fungsi
Ubuntu 16.04	1	Sebagai penghubung antara perangkat keras dan pengguna
SNORT [13]	1	Penyedia layanan keamanan jaringan dan komputer
BASE [14]	1	Menampilkan *alert databases* dalam tampilan grafis dan teks
Splunk [15]	1	Aplikasi pendukung analisa data
Barnyard2 [16]	1	Membaca *output alert file* dari SNORT dan menulisnya ke MySQL

Iaxflood [17]	1	Aplikasi untuk melakukan *flooding*
Kali Linux [17]	1	Untuk melakukan *penetration test*
MySQL	1	Menyimpan *alert databases* untuk ditampilkan BASE
Swatch & Postfix	1	Pengiriman *e-mail notification* secara otomatis
Hydra[15]	1	Digunakan untuk melakukan *brute force SSH login.*
Pulled Pork	1	Digunakan untuk melakukan *rules update* secara otomatis.

3.3 Tahapan Penelitian

Diagram alir tahapan penelitian yang peneliti lakukan adalah seperti ditunjukkan :



Gambar 3.1 Diagram Alir Penelitian

Ada beberapa tahapan yang dilakukan dalam penelitian ini yaitu studi literatur, penerapan PPDIOO yaitu *Prepare, Plan, Design, Implementation, Operate, and Optimize*, lalu dilanjutkan dengan analisa hasil pembahasan dan kesimpulan.

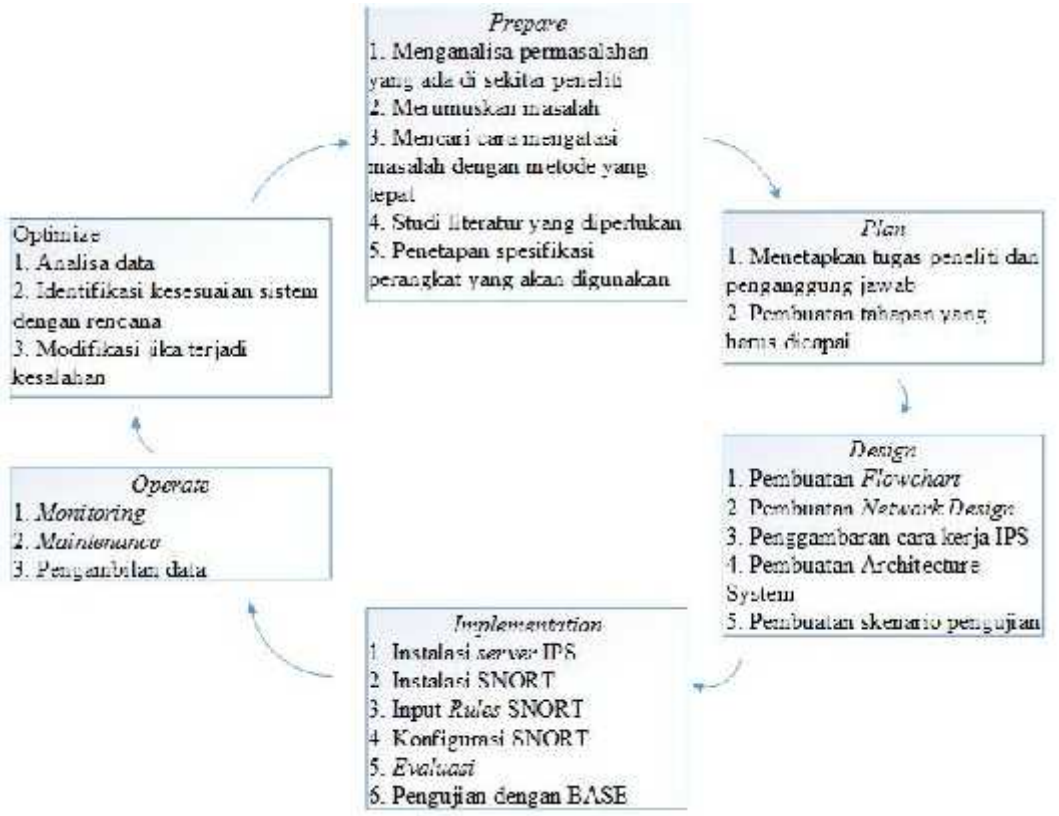
3.3.1 Studi Literatur

Studi literatur dimaksudkan untuk mempelajari berbagai sumber referensi (buku dan internet) yang berkaitan dengan perancangan sistem. Literatur yang dipelajari adalah literatur yang berkaitan dengan :

1. Sistem Operasi (Linux)
2. IDS (*Intrusion Detection System*)
3. IPS (*Intrusion Prevention System*)
4. Keamanan jaringan komputer
5. TCP/IP
6. Insiden *Security*
7. Jurnal penelitian yang berhubungan dengan keamanan dan jaringan

3.3.2 Penerapan Metode PPDIOO (CISCO Lifecycle Service)

Ada enam tahap yang dilakukan ketika menerapkan metode PPDIOO yaitu *prepare, plan, design, implementation, operate* dan, *optimize.*



Gambar 3.2 Ringkasan PPDIOO

3.3.2.1 Prepare (Persiapan)

Pada fase ini peneliti menganalisa permasalahan yang ada di sekitar peneliti dalam lingkup jaringan komputer dan menemukan beberapa masalah yang ada di Unila bersama Kepala Divisi Infrastruktur dan Jaringan yaitu Gigih F.N. Kasus yang pernah terjadi adalah peretasan *database* nilai di *server* Siakad Unila yang menyebabkan seorang mahasiswa dapat mengubah nilai yang tersimpan dalam database siakad. Peneliti menemukan sebuah cara untuk mencoba mengatasi

permasalahan tersebut yaitu dengan menggunakan metode IPS (*Intrusion Prevention System*), yaitu penggabungan antara metode pendeteksian dan *firewall*. Peneliti menganalisa permasalahan yang terjadi dan menerapkan metodologi dari CISCO yaitu PPDIOO yang dirancang untuk melakukan perancangan hingga implementasi dari metode IPS yang digunakan. Dengan menggunakan *fishbone analysis diagram* (Gambar 1.1) peneliti merumuskan masalah dan menemukan sebuah efek yang ditimbulkan dari permasalahan ini yaitu bahaya potensial kerentanan sistem teknologi Unila yang akan mengancam kegiatan akademik. Peneliti melakukan studi literatur untuk menambah wawasan dan panduan untuk mendukung penelitian dengan membaca jurnal, buku, dan mengikuti forum terkait materi penelitian yang telah dipublikasikan baik dalam negeri maupun luar negeri. Peneliti menetapkan spesifikasi perangkat keras dan perangkat lunak yang digunakan pada penelitian. Seperti *virtual machine server* yang digunakan sebagai server IPS dan penggunaan Ubuntu Server sebagai sistem operasi yang digunakan untuk melakukan konfigurasi pengamanan jaringan. SNORT dan kombinasi *firewall* dilakukan untuk melakukan upaya pencegahan peretasan. Dengan perangkat keras yang ada digunakan sebagai media sistem IPS.

3.3.2.2 Plan (Perencanaan)

Peneliti menetapkan tugas yang dilakukan baik oleh peneliti sendiri yaitu melakukan instalasi dan konfigurasi pada *server* di Laboratorium Teknik Eleketro maupun aktor yang berhubungan dengan penelitian ini yaitu penanggung jawab yang memberikan peneliti izin untuk melakukan penelitian di Laboratorium Teknik Elektro dan melakukan penyesuaian dengan sistem yang ada.

Penelitian dilakukan dengan beberapa *milestones* untuk memantau perkembangan, yaitu :

1. Penyelesaian rencana dan desain
2. Pembuatan *server* IPS dengan OS Ubuntu Server
3. Konfigurasi SNORT dan *rules* yang digunakan
4. Pengujian sistem dengan melakukan *penetration test* seperti *burst attack, packet flooding,* dan penggunaan aplikasi BASE.
5. Implementasi

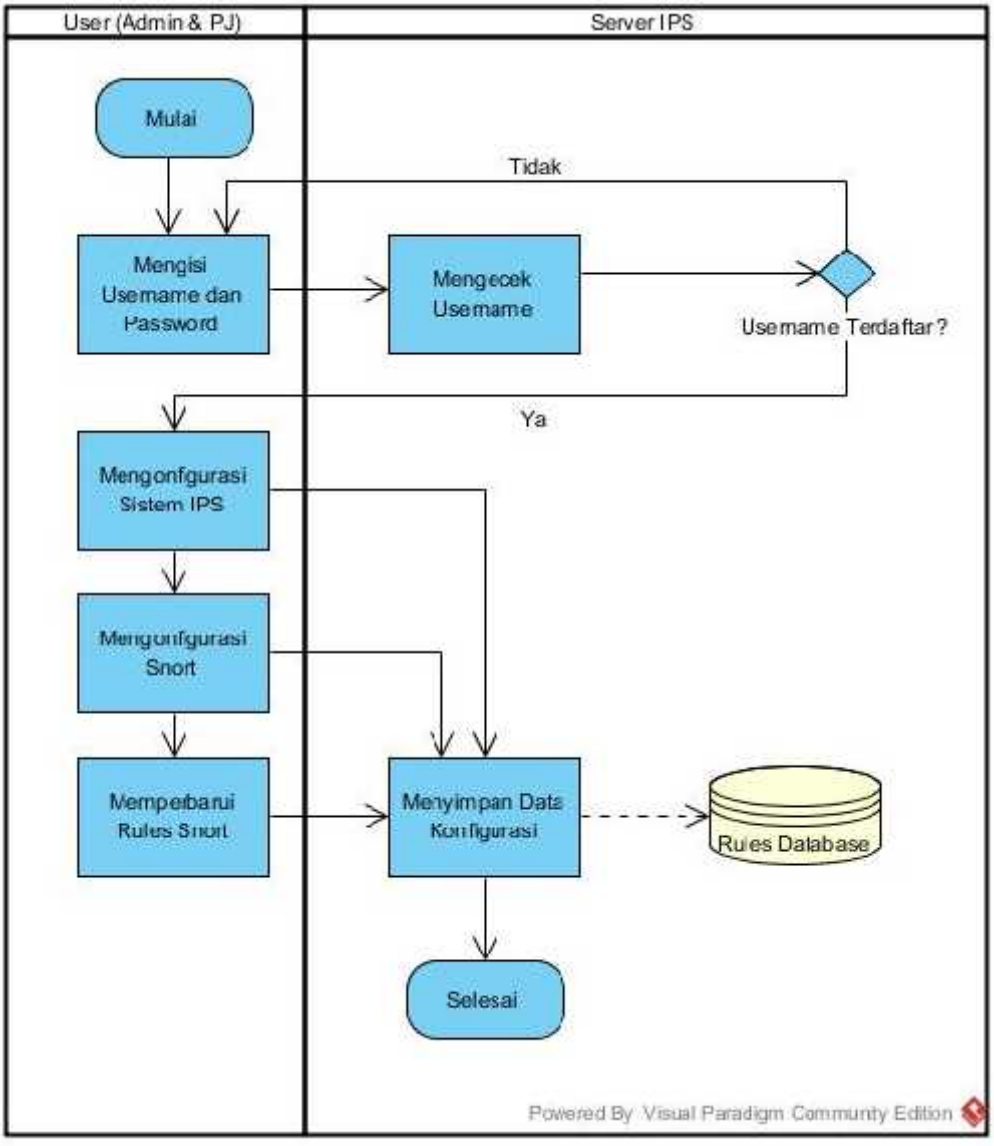
Kebutuhan pada fase ini terus mengalami perubahan sesuai dengan siklus yang sedang berjalan.

3.3.2.3 Design (Desain)

Ada tiga desain yang peneliti buat yaitu *flow chart diagram*, *network design*, Cara Kerja *Intrusion Prevention System,* dan desain skenario pengujian.

1. **Flow Chart**

   Desain aliran diagram menggunakan *flow chart* yang menggambarkan interaksi dari sistem dan pengguna yang digambarkan sebagai berikut :

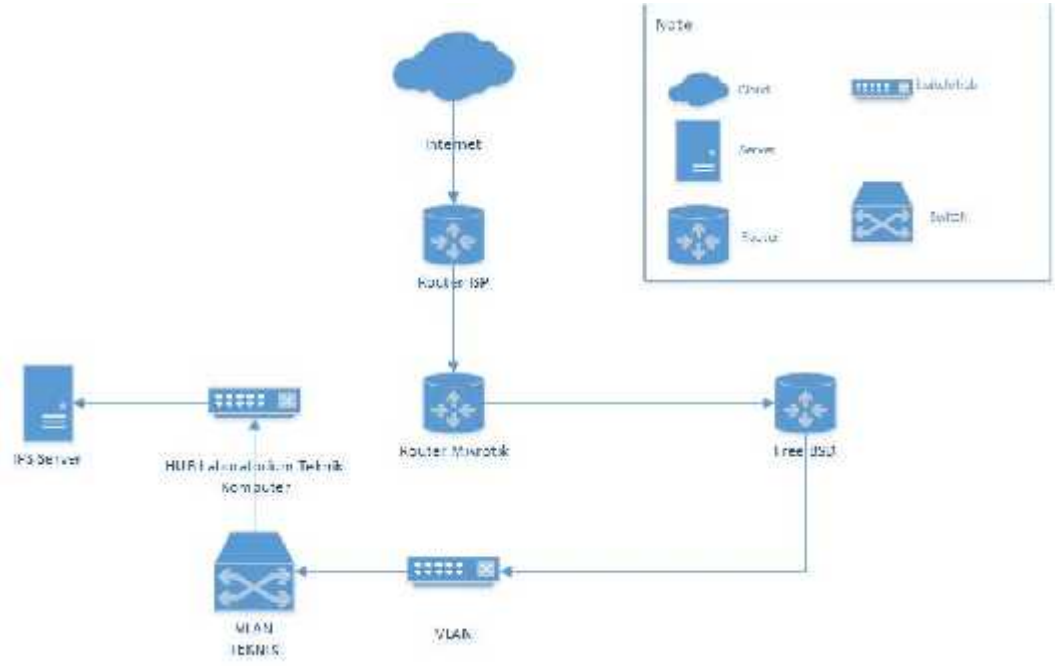


Gambar 3.3 *Flow Chart*

User melakukan *login* ke IPS *server* dan jika terdaftar maka akan diberikan izin untuk masuk ke dalam sistem dan melakukan kofigurasi. Jika salah mengisikan data *login* maka sistem akan meminta untuk memasukkan ulang data. Setelah berhasil melakukan *login* ke dalam sistem maka user dalam melakukan konfigurasi pada sistem IPS dengan melakukan instalasi perangkat lunak yang dibutuhkan dalam melakukan penelitian ini dan semua konfigurasi akan disimpan oleh sistem. Dilanjutkan dengan melakukan konfigurasi pada SNORT dengan mengaktifkan fitur yang diperlukan seperti *data acquisition, rules, configuration file and folder* dan sistem akan menyimpan konfigurasi tersebut dan untuk *rules* akan dituliskan dalam *rules databases*. Aplikasi pengolah *database* yang digunakan adalah MySQL. Ini dapat digunakan ketika SNORT menulis *log* dan menghasilkan sebuah *alert file* yang akan diproses oleh *barnyard2* untuk ditulis ke dalam *database* sehingga dapat ditampilkan pada BASE. *User* yang telah memiliki izin ke sistem juga dapat memperbarui *rules* SNORT jika dibutuhkan.

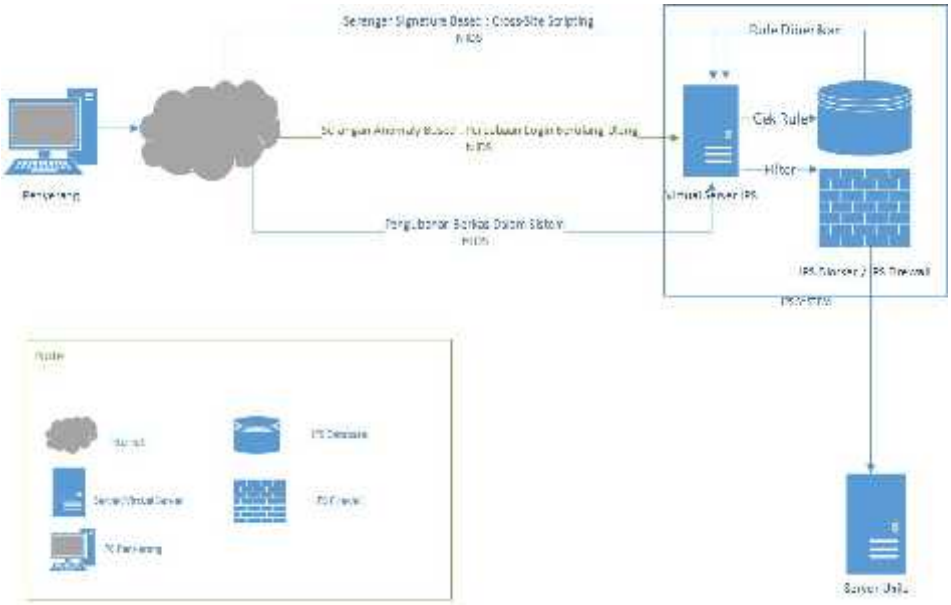
2. Network Design

Setelah melakukan pembahasan pada seminar hasil, dilakukan penyesuaian desain penempatan IPS *server* dengan konfigurasi sebagai berikut :



Gambar 3.4 *Network Design*

3. Cara Kerja *Intrusion Prevention System*

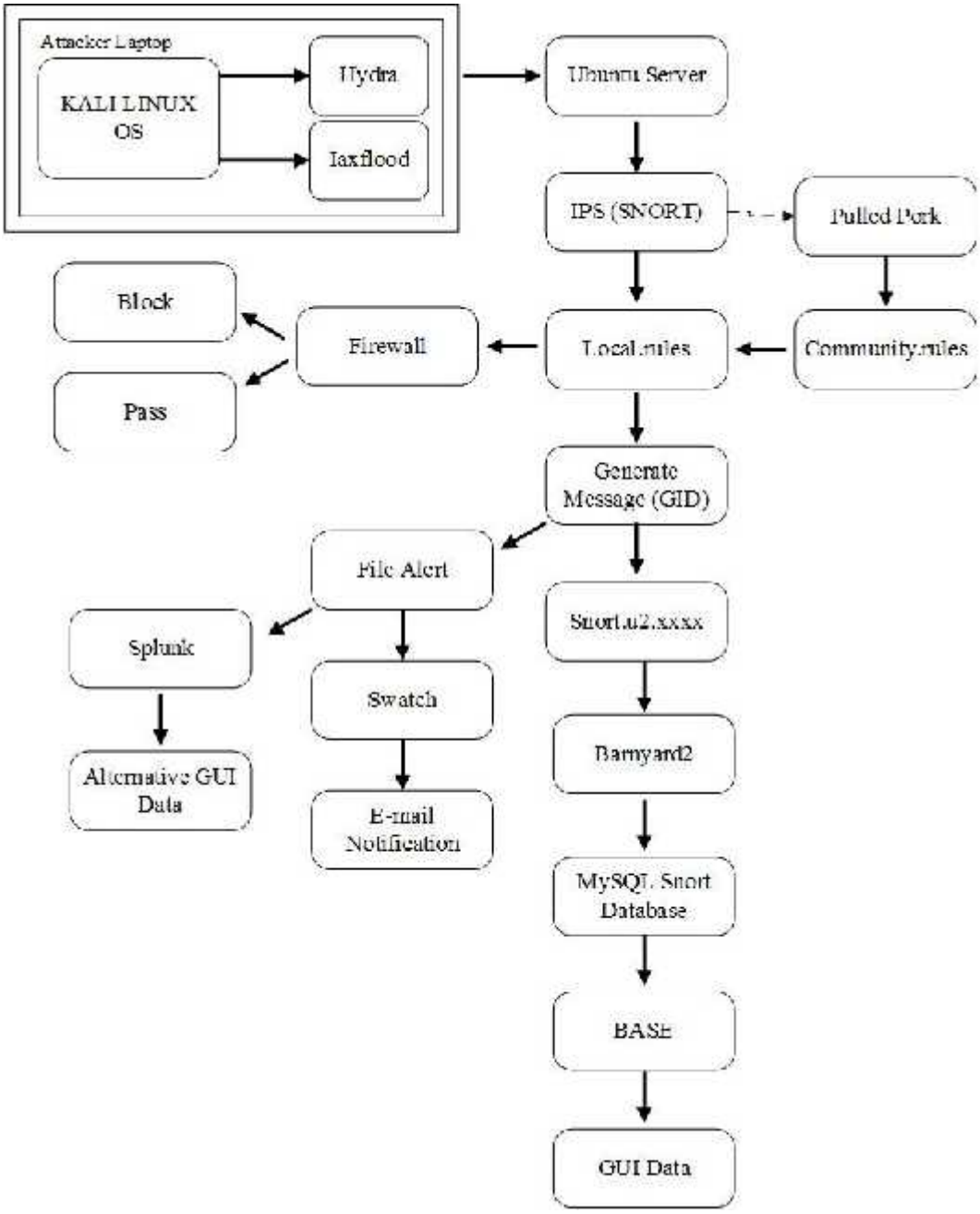


Gambar 3.5 Cara Kerja *Intrusion Prevention System*

Penyerang melakukan penyerangan dengan beberapa metode seperti, *signatured based attack* (bersifat seperti virus), *anomaly based attack* (contohnya percobaan login berkali-kali), dan pengubahan *database* dalam sistem secara ilegal. Sistem IPS mendeteksi lalu lintas jaringan yang melewatinya dan melakukan pemeriksaan kesesuaian dengan *database* yang berada dalam sistem. Ketika paket terindikasi sebagai sebuah serangan, IPS *Firewall* melakukan *blocking* terhadap paket tersebut agar ia tidak diteruskan masuk ke dalam *server* Unila.

4. *Architecture System*

Rencana arsitektur dari sistem SNORT yang akan dibangun adalah sebagai berikut :



Gambar 3.6 *Architecture System*

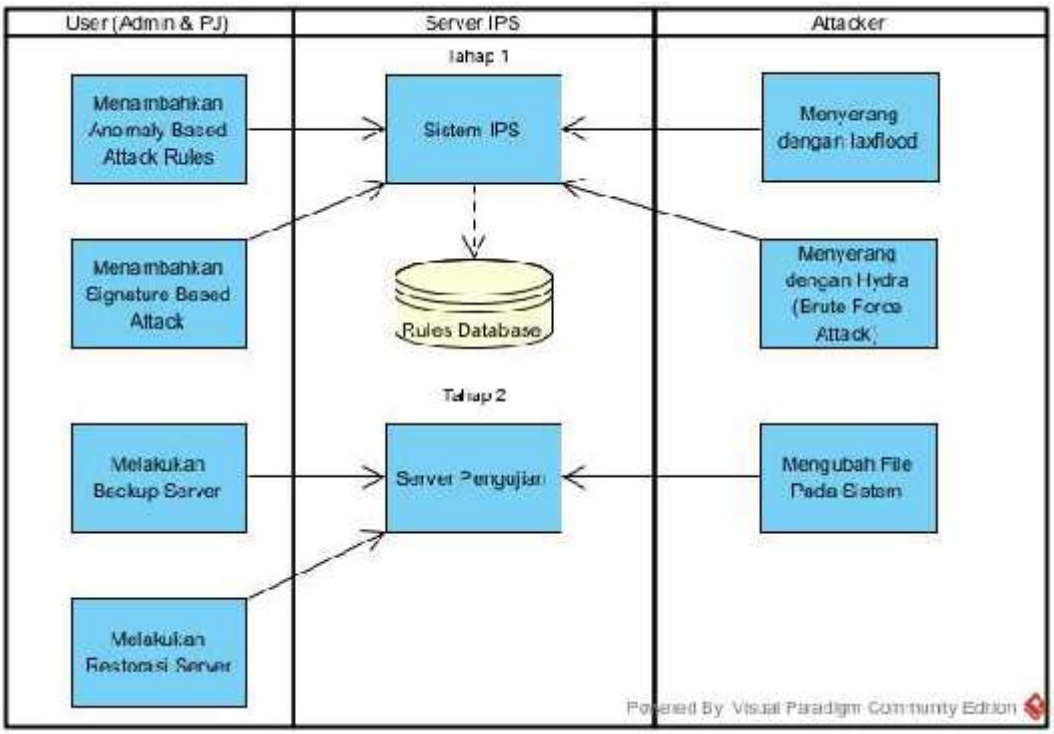
Laptop dengan OS Kali Linux melakukan serangan dengan dua buah *penetration tools* yaitu Hydra dan Iaxflood melakukan serangan ke *server*. SNORT akan bereaksi dengan paket data yang dikirim oleh peretas dengan melakukan identifikasi kesesuaian dengan daftar *rules* yang ada pada *file* local.rules (*rules* yang digunakan mengacu pada community.rules yang didapat dari fitur ekstensi SNORT yaitu Pulled Pork).

Setelah itu akan diteruskan ke *firewall* untuk melakukan tindakan apakah akan di hentikan atau di lewatkan. GID yang dibuat pada *rules* akan mengaktifkan *message generator* dan menghasilkan *file* Alert dan *log* berupa snort.u2.xxxx. Alert dapat digunakan oleh Splunk untuk dapat memberikan tampilan alternatif untuk analisis *data*, dan juga digunakan oleh Swatch yang akan terpicu ketika ada kata kunci yang telah dikonfigurasi untuk selanjutnya dikirim ke *e-mail*.

File snort.u2.xxxx akan digunakan oleh Barnyard2 untuk selanjutnya di-*input* ke dalam snort *databases*. BASE akan menggunakan *tables* yang ada pada snort *databases* untuk selanjutnya ditampilkan sebagai laporan detail kejadian yang dapat digunakan untuk melakukan analisis *data*.

5. Skenario Pengujian

Sebelum melakukan pengujian, disusun skenario sebagai berikut :



Gambar 3.7 Skenario Pengujian

Peneliti berperan sebagai *sysadmin* dan *attacker*, dengan menggunakan 1 buah *notebook* dengan OS KALI Linux dan 1 buah IPS *server* GNU/Linux di Laboratorium Teknik Elektro Universitas Lampung.

Pengujian tahap 1 (*Attacker* belum berhasil masuk ke dalam *system*) adalah sebagai berikut :

1. *Attacker* melakukan metode penyerangan dengan *burst attack/ping flood* pada salah satu *server* yag tersimpan di *server* Laboratorium Teknik Elektro dengan Iaxflood.

2. *Sysadmin* melakukan pengamanan dengan menambahkan *rule anomaly based attack* pada *database* SNORT dari sistem IPS
3. *Attacker* mencoba *penetration test* dengan salah satu perangkat lunak yang ada pada Kali Linux yaitu *brute force login* dengan aplikasi hydra untuk mendapatkan akses ke dalam sistem.
4. *Sysadmin* melakukan pengamanan dengan menambahkan *rule signature based attack* pada *database* SNORT dari sistem IPS.

Pengujian tahap 2 (*Attacker* telah berhasil masuk ke dalam *system*) adalah sebagai berikut :

1. *Sysadmin* melakukan *server backup* dengan memindahkan *alert file* maupun SNORT *folder* yang dilindungi.
2. *Attacker* diposisikan telah berhasil masuk ke dalam sistem dan menghapus *alert file* pada *server* untuk menghilangkan catatan *log*.
3. Sistem IPS memberikan peringatan kepada *sysadmin* dan setelah itu melakukan tindakan yang dibutuhkan yaitu restorasi *server* dan *rules update* sesuai dengan *threat* yang berhasil lolos.

3.3.2.4 Implementation (Implementasi)

Peneliti melakukan instalasi pada server IPS menggunakan Ubuntu Server, pemasangan aplikasi SNORT, pembuatan rules yang digunakan pada SNORT dan melakukan konfigurasi secara keseluruhan dengan dua tahapan implementasi. Pada tahap 1 peneliti melakukan pengujian dengan melakukan instalasi di Fakultas Teknik yang dilanjutkan dengan tahap 2 yaitu instalasi di Laboratorium Teknik

Elektro Universitas Lampung. Penginstalasian dan konfigurasi dilakukan selama 1 bulan. Setelah instalasi selesai dilakukan evaluasi, dan bila terjadi kesalahan dilakukan *rollback* untuk mencari kesalahan dan pencarian informasi tambahan. Setelah sistem berhasil terpasang, peneliti melakukan pengujian dengan melakukan *penetration* test dan penggunaan aplikasi ACID BASE, untuk selanjutnya dapat dilakukan pengoperasian sistem.

3.3.2.5 Operate (Operasional)

Monitoring peneliti lakukan untuk melakukan pemeliharaan jaringan dan perbaikan jika terjadi kesalahan sistem selama 1 minggu (8 – 14 Januari). Peneliti memantau sistem apakah sesuai dengan desain yang telah dibuat dengan memantau kinerja, stabilitas, deteksi kesalahan, konfigurasi, dan pengambilan data yang digunakan untuk penelitian dan optimalisasi.

Tabel 3.4 Parameter *Maintenance*

Kinerja	Stabilitas	Deteksi Kesalahan	Konfigurasi
Kecepatan deteksi *threat*	Apakah terjadi *system crash ?*	Threat berhasil dihentikan	Ubuntu berjalan dengan baik
Apakah terjadi penurunan kecepatan seiring berjalannya waktu sebelum reboot ?	Berapa lama sistem berjalan hingga butuh *clear alert log cache* ?	Tidak ada data aman dihentikan	SNORT berjalan dengan baik
Apakah ada threat yang lolos ?		Pemblokiran sesuai dengan rules	*Rules* telah diperbaharui

3.3.2.6 Optimize (Optimalisasi)

Peneliti menganalisa hasil perolehan data yang ada dan melakukan identifikasi apakah sistem sudah sesuai dengan rencana atau melakukan modifikasi untuk meningkatkan kinerja sistem jika dirasa terlalu banyak masalah yang timbul.

3.4 Analisa Hasil, Pembahasan, dan Kesimpulan

Pada tahapan ini dilakukan analisa hasil dan pembahasan dari kegiatan yang telah dilakukan serta menarik kesimpulan dari hasil dan pembahasan yang dilakukan.

IV. HASIL DAN PEMBAHASAN

4.1 Penerapan Metode PPDIOO (Cisco Lifecycle Service)

4.1.1 *Implementation*

Implementasi dilakukan dengan menggunakan salah satu komputer di LaboratoriumTerpadu Teknik Elektro dengan *ip address* 10.10.13.13.

4.1.1.1 Instalasi *Server* IPS

Sistem operasi yang digunakan pada *server* adalah Ubuntu 16.04 LTS dengan 1 buah ethernet dengan konfigurasi sebagai berikut :

1. auto eno1

   iface eno1 inet static

   address 10.10.13.13

   netmask 255.255.255.0

   network 192.168.1.0

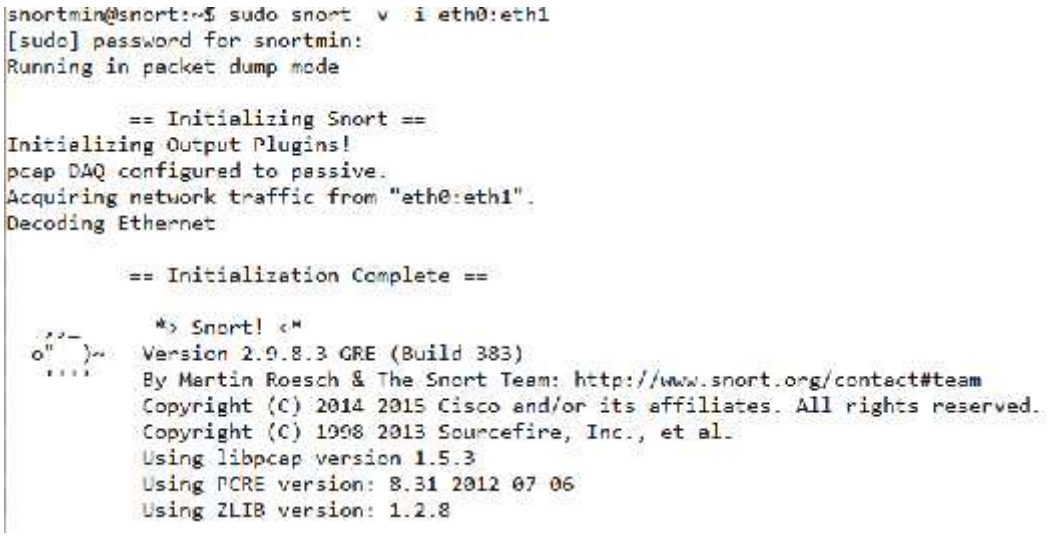
   broadcast 192.168.1.255

   gateway 192.168.1.253

   dns-nameserver 192.168.1.3 192.168.1.253

4.1.1.2 Instalasi Snort

Peneliti menggunakan aplikasi remote ssh server yaitu bitvise. Setelah berhasil masuk ke dalam *server* peneliti melakukan *download* aplikasi dari www.snort.org. Snort yang peneliti gunakan adalah snort versi 2.9.8.3 dengan format tar.gz. Instalasi snort dilakukan dengan perintah "tar –zxvf snort-2.9.8.3.tar.gz". Setelah masuk ke *folder* hasil ekstraksi lalu diketikkan pada terminal instruksi ./configure, make, make install, dan make clean secara bergantian setelah tiap proses selesai. Hasil instalasi berada pada direktori /usr/local/bin/snort. Untuk memastikan snort berjalan, diketikkan perintah "sudo snort –v –i eno1".



Gambar 4.1 Tampilan awal Snort

Di dalam snort ada fitur yang disebut *data acquisition library*, yang digunakan untuk *input* dan *output* paket data yang seterusnya disebut DAQ. Ada beberapa tipe DAQ yaitu :

```
tarisy@ubuntu:~$ snort --daq-list
Available DAQ modules:
pcap(v3): readback live multi unpriv
nfq(v7): live inline multi
ipfw(v3): live inline multi unpriv
dump(v3): readback live inline multi unpriv
afpacket(v5): live inline multi unpriv
```

Gambar 4.2 Daftar DAQ pada Snort

Di sini penulis menggunakan fitur nfq (*net filter queue*) yang berfungsi mengintegrasikan snort dengan *firewall* dan dump yang digunakan untuk melakukan paket *logging*

4.1.1.3 Input Rules Snort

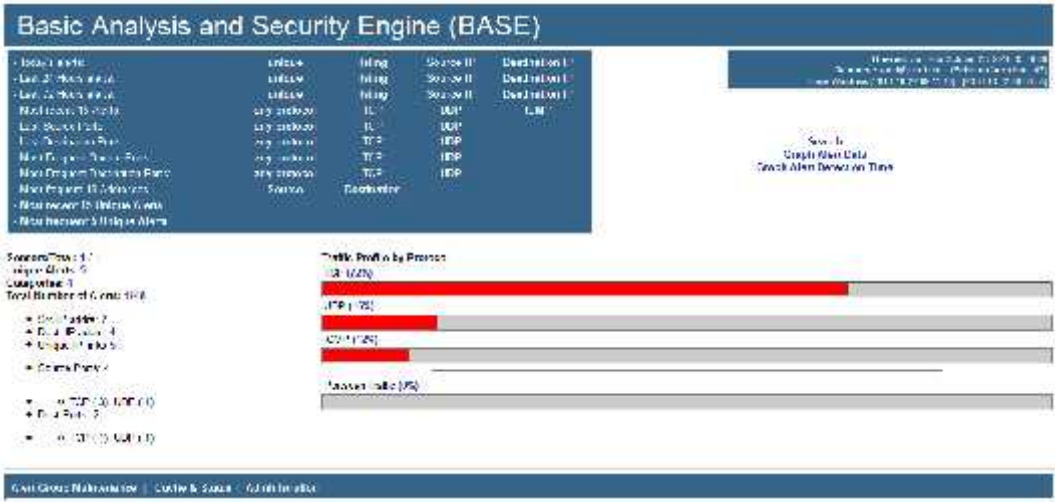
Peneliti menggunakan *rules* dari komunitas snort. *Rules* itu sendiri dapat kita buat sesuai keinginan dan kebutuhan dengan menambahkan *rules* pada file 'local.rules' yang telah peneliti buat di dalam *folder* '/usr/local/etc/snort/rules/'. Contoh *rule* sederhana yang peneliti buat adalah untuk melakukan *block* paket ICMP (*Internet Control Message Protocol*) :

"drop icmp any any -> $HOME_NET any (msg:"Ping Flood detected"; GID:1; sid:10000001; rev:001; classtype:icmp-event;)".

Peneliti juga menggunakan *rules* yang telah disediakan oleh komunitas snort yaitu 'community.rules' yang berisi sekitar 3000 *rules* yang dapat digunakan untuk melakukan pencegahan terhadap berbagai macam serangan. Dari *rules* sebanyak itu yang tepat untuk digunakan sesuai dengan *case* yang pernah terjadi di Unila adalah seperti yang telah peneliti sebutkan pada fase desain local.rules.

4.1.1.4 Instalasi ACID BASE dan barnyard2

Setelah *download* file base-1.4.5.tar.gz ekstrak *file* tersebut dan pindahkan hasil ekstrak ke '/var/www/html/base' agar bisa diakses oleh komputer lain dalam jaringan yang sama. Ketika snort melakukan pendeteksian DAQ dump melakukan *logging* paket ke direktori '/var/log/snort/snort.u2.xxx'. Seperti yang ditunjukkan pada gambar 3.6, snort.u2 dibaca oleh aplikasi barnyard2 untuk segera di-*update* ke dalam *database* snort untuk selanjutnya ditampilkan di halaman utama BASE :

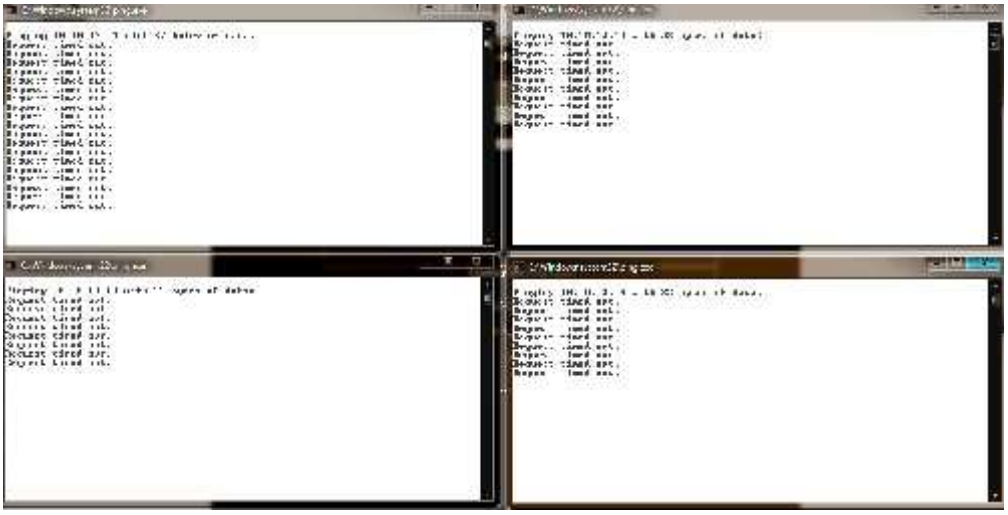


Gambar 4.3 Halaman utama BASE

Setelah berhasil melakukan *logging* paket data peneliti melanjutkan ke tahap pengujian.

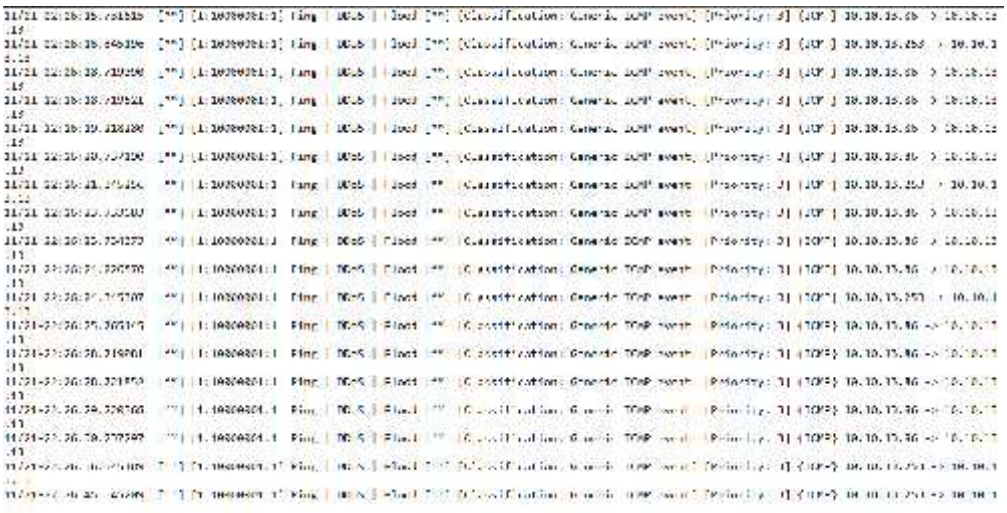
4.1.1.5 Pengujian

Pertama peneliti melakukan pengujian dengan metode *burst attack* / *ping flood* dengan *command prompt* pada windows :



Gambar 4.4 *Ping flood*

Dengan *rules* untuk melakukan *drop* paket ICMP maka ping *flood* yang dilakukan oleh *attacker* di *block* oleh snort yang menyebabkan ping mendapat balasan *request timed out*, hasil *logging* snort:

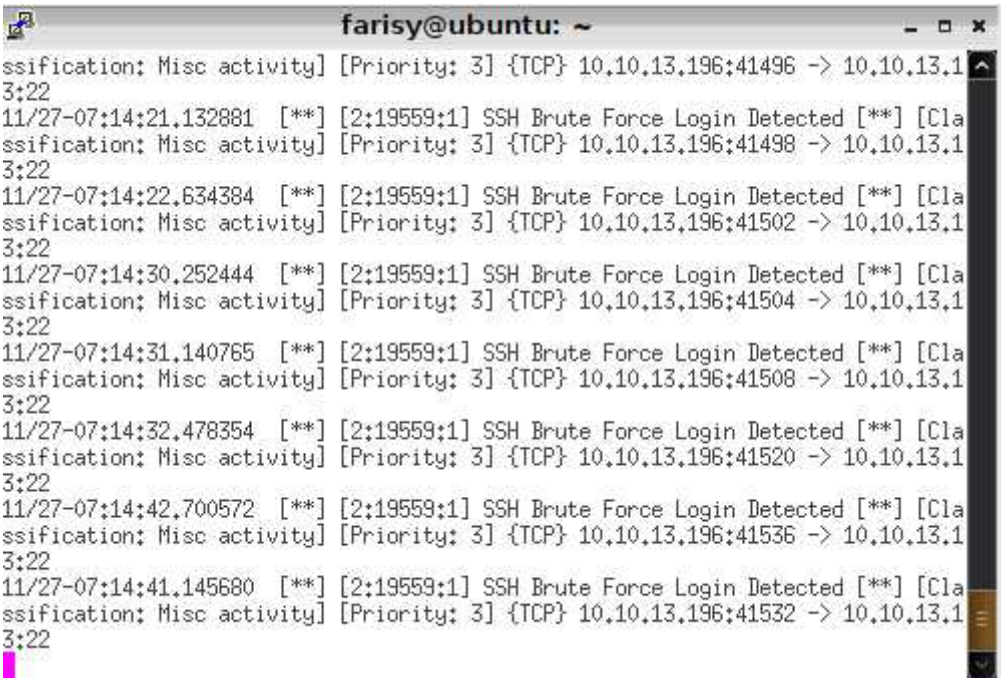


Gambar 4.5 Snort alert

Pengujian kedua dilakukan dengan menggunakan *tools* hydra yang biasa digunakan *hacker* untuk melakukan *brute force login* pada *port* ssh/22 :

Gambar 4.6 Proses pengujian dengan hydra

Dari gambar 4.6 peneliti mengaktifkan *tools* hydra pada terminal, peneliti mencoba login dengna username farisy dan ditambah dengan menggunakan daftar password dari *indonesian wordlist master* dengan tujuan ip 10.10.13.13 pada *port* ssh dengan jumlah percobaan 4 kali. Setelah dijalankan IPS berhasil menghentikan percobaan *brute force login* dengan melihat pesan *error* yang diberikan hydra yaitu *could not connect to* ssh yang disebabkan telah di *block* oleh IPS. Dengan menambahkan *rule* untuk melakukan *drop* paket pada *port* 22, SNORT memberikan peringatan sebagai berikut :



Gambar 4.7 Tampilan *alert* pada IPS *server*

Dari gambar 4.7 terlihat bahwa sistem IPS telah berhasil melakukan *event logging* berupa SSH Brute Force Login Detected dari ip 10.10.13.196.

Peringatan yang dilakukan telah berjalan secara *real time*, dan paket berhasil dihentikan dengan *drop rules* yang telah peneliti buat. Terbukti ada peringatan *ERROR* pada aplikasi hydra yang menyatakan tidak dapat melakukan koneksi ssh ke *port* 22 pada ip 10.10.13.13.

White list dapat digunakan untuk memberikan izin kepada beberapa daftar IP yang diizinkan untuk melakukan *remote server* SSH dengan menambahkan ip yang diizinkan (IP penyerang yaitu 10.10.13.113) pada direktori:

/etc/snort/rules/iplist/whitelist.rules.

Diberikannya izin akses kepada komputer penyerang, sama dengan memberikan celah untuk menghapus isi sistem dari IPS *server*. Setelah berhasil dihapus oleh

penyerang, *sysadmin* melakukan *recovery* dan memperbaiki *rules* (menghapus ip penyerang dari *white list*)

Implementasi tahap kedua pada *server* 192.168.1.138 hanya bisa dilakukan pengujian performa karena *firewall* pada IPS *server* tidak dapat bekerja dengan optimal. Hal ini disebabkan oleh sistem IPS menggunakan *virtual machine server* yang pada saat implementasi *server* dengan 2 buah *virtual ethernet*, tidak sanggup melakukan *filtering packet* pada IP 192.168.1.0/24. Sehingga menyebabkan penumpukan aliran data (*bottle nek*) pada jaringan *server* Unila menyebabkan penurunan kinerja yang signifikan di malam hari tanggal 10 Januari 2017. Untuk berjalan dengan sempurna IPS *server* harus diimplementasikan pada *server firewall* Unila. Namun tidak peneliti lakukan karena dibutuhkan prosedur *maintenance* yang cukup memakan waktu, sedangkan penggunaan jaringan internet di Unila yang tidak pernah berhenti teruatama pada siang hari, membuat peneliti mengurungkan rencana tersebut sehingga dipindahkan ke Laboratorium Terpadu Teknik Elektro.

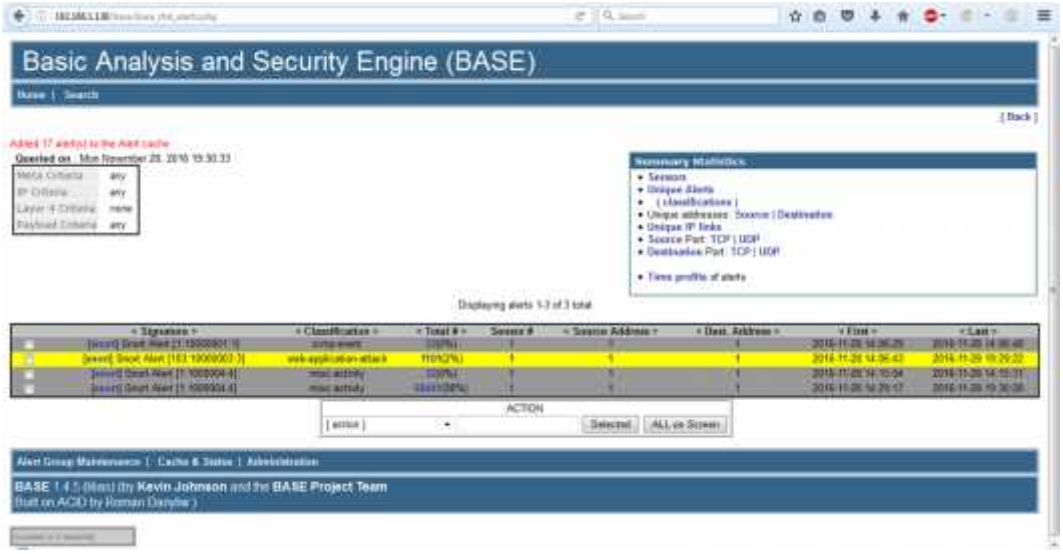
4.1.2 *Operate*

Di tahap ini dilakukan pemantauan, dan perbaikan permasalahan minor untuk segera memperbaiki sistem IPS, seperti kesalahan konfigurasi maupun format *rules*.

4.1.2.1 *Monitoring and Maintenance*

Di fase ini peneliti melihat tampilan GUI dari BASE, dengan menggunakan *browser*, dan membuka URL http://192.168.1.138/base, menjaga kinerja dari IPS

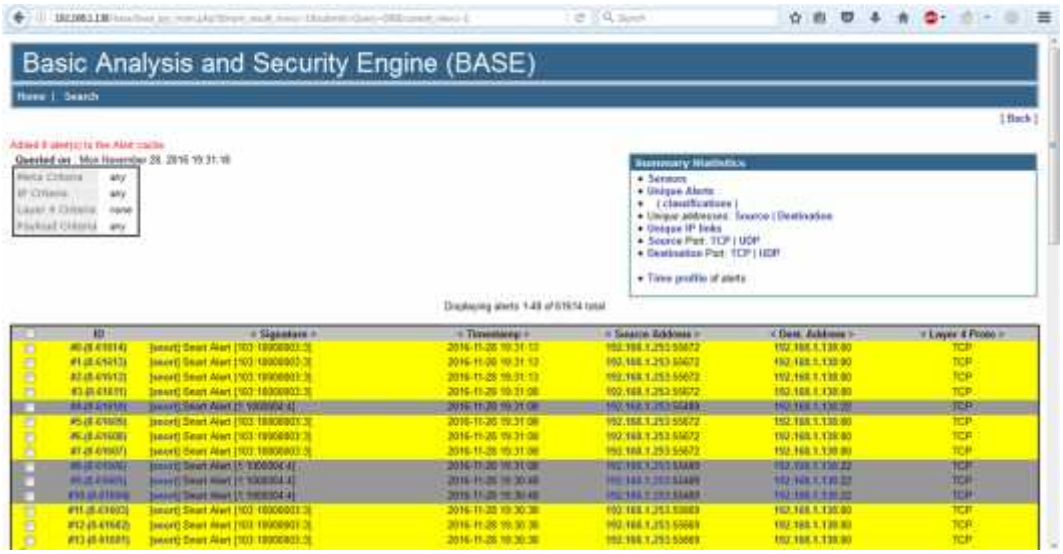
server, dan SNORT. Dengan menggunakan BASE peneliti dapat melihat klasifikasi serangan :



Gambar 4.8 BASE *report* berdasarkan klasifikasi serangan

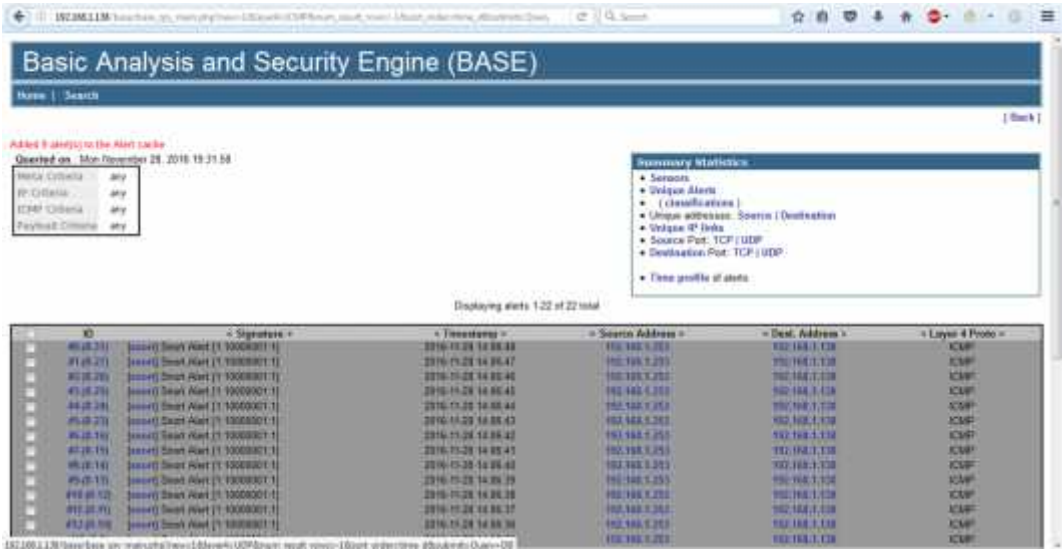
Pada tampilan yang dihasilkan ada tiga klasifikasi serangan yaitu ‘icmp-*event*’, ‘*web-application-attack*’, dan ‘*misc-activity’*. Pada tiap halaman BASE terdapat *live report* yang bertuliskan *text* berwarna merah, pada halaman lain dan warna kuning pada halaman utama BASE dengan kata “*added 17 alert(s) to the alert cache”*.

Base dapat mengelompokkan empat tipe *alert* yaitu TCP, UDP, ICMP, dan *Portscan*, di mana sebagian besar serangan ada pada TCP dan ICMP. Berikut pengelompokkan *alert* berdasarkan TCP :



Gambar 4.9 Tampilan *alert* dengan kategori TCP

Dilihat pada *destination address*, *port* yang diserang adalah TCP *port* 80 (*http port*), dan 22 (*ssh port*). Berikut ini adalah pada protokol ICMP :



Gambar 4.10 Tampilan *alert* dengan kategori ICMP

Pada ICMP tidak terdapat port disebabkan ICMP hanya mengirimkan data berupa pesan, baik itu *echo request* maupun *echo reply*. Alert pada ICMP emberikan pesan

bahwa telah terjadi hubungan atau belum, antara *source address* dan *destination address*.

4.1.2.2 Pengambilan Data

Pengambilan data diambil dari pengamatan langsung oleh peneliti pada sistem IPS *server*, dengan paramater kinerja, stabilitas, deteksi kesalahan, dan konfigurasi.

Tabel 4.1 Kinerja IPS *Server* dan SNORT

Kinerja	Hari Pertama	Hari ke 7
Kecepatan deteksi *threat*	*Real Time* (<1s)	*Real Time* (<1s)
Apakah terjadi penurunan kecepatan seiring berjalannya waktu sebelum *clear alert log cache* ?	Tidak	Ya (Jika *alert* > 1.000.000)
Apakah ada threat yang lolos ?	Tidak	Tidak

Tabel 4.2 Stabilitas IPS *Server* dan SNORT

Stabilitas	Hari Pertama	Hari ke 7
Apakah terjadi *system crash ?*	Tidak	Tidak
Berapa lama sistem berjalan hingga butuh *clear alert log cache* ?	Tidak (*alert* < 10.000)	Ya (Jika *alert* > 1.000.000)

Tabel 4.3 Deteksi Kesalahan SNORT

Deteksi Kesalahan	Hari Pertama	Hari ke 7
Threat berhasil dihentikan	Ya (100%)	Ya (100%)
Tidak ada data aman dihentikan (*false positive*)	Tidak	Ada
Pemblokiran sesuai dengan rules	Ya	Ya

Tabel 4.4 Konfigurasi IPS dan SNORT

Konfigurasi	Hari Pertama	Hari ke 7
Ubuntu berjalan dengan stabil	Ya	Ya
SNORT berjalan dengan baik	Ya	Ya
Rules telah diperbaharui	Ya (*community rules version 2.9.8.3*)	Tidak (Tetap)

4.1.3 *Optimize*

Di tahap ini dilakukan analisa dari hasil yang telah peneliti dapatkan pada tahap *operate,* setelah itu dilakukan identifikasi apakah sistem yang berjalan telah sesuai dengan sistem yang direncanakan. Apabila terjadi ketidaksesuaian pada sistem maka peneliti dilakukan modifikasi pada sistem.

4.1.3.1 Analisa Data

Kinerja dari integrasi antara Ubuntu server 16.04 dan SNORT 2.9.8.3 sangat baik. Dengan kecepatan deteksi threat yang berada pada angka lebih kecil dari 1 detik, dapat dikatakan *real time*. contohnya pada saat peneliti melakukan pengujian dengan hydra, tampilan *console* SNORT yang peneliti aktifkan di IPS *server* seketika memberikan sebuah *alert message* secara bersamaan dengan pendeteksian.

Peneliti memberikan *srcipt* untuk melakukan *ping flood* dan *brute force ssh attack* secara otomatis selama tujuh hari, hingga *alert* yang dihasilkan oleh SNORT lebih dari 1.000.000, dan menghasilkan log file sekitar 14 GB. Membuat *virtual machine server* yang dibangun peneliti pada UPT TIK mengalami penurunan performa yang dapat diketahui dengan melihat kecepatan *website load* dari BASE yang semula 0 *second* menjadi 6 *second*. Ketika dilakukan *remote* dengan ssh terjadi *delay* sekitar 1-3 detik ketika mengetikkan perintah pada *keyboard* dan tampilan yang dihasilkan di aplikasi putty, hal ini memaksa peneliti melakukan *backup alert file* pada /var/log/snort/ ke latop peneliti dan membersihkan BASE *cache* agar dapat berjalan dengan normal kembali. Namun, walaupun terjadi penurunan performa seperti yang

dijelaskan pada sistem IPS, SNORT tetap dapat melakukan pendeteksian, dan tidak ada *threat* yang lolos.

Selama seminggu, peneliti melakukan *monitoring* pada IPS *server* dengan sistem operasi Ubuntu berjalan dengan baik. Pada *virtual machine server* tanpa terjadi *system crash*, yang membuat peneliti tidak perlu melakukan *reboot*. Namun, jika *threat* yang terdeteksi selama seminggu kurang lebih 1.000.000, peneliti hanya perlu melakukan *clear alert log cache* pada sistem dan BASE.

Pendeteksian yang dilakukan snort 100% berhasil dari hari pertama hingga hari ke 7. Namun, terjadi *false positive alert* ketika peneliti melakukan ping dari IPS *server* ke luar jaringan Unila, yang teridentifikasi sebagai "*potentially bad traffic*", namun tidak terlalu berarti. *Droping packet* yang dilakukan snort sesuai dengan *rules* yang peneliti buat, namun terjadi banyak *false positive alert* disebabkan *rules* yang peneliti gunakan dari komunitas SNORT.

Selama peneliti melakukan *monitoring* pada IPS *server* sistem operasi yang peneliti gunakan yaitu Ubuntu server, berjalan dengan baik tanpa terjadi *error* maupun *kernel panic*. SNORT tetap berhasil melakukan pendeteksian ketika *virtual machine* mengalami penurunan performa pada lalu lintas jaringan. Penggunaan *community rules* sudah menggunakan versi terbaru dan belum ada *update* dari halaman resmi SNORT.

4.1.3.2 Identifikasi Kesesuaian Sistem

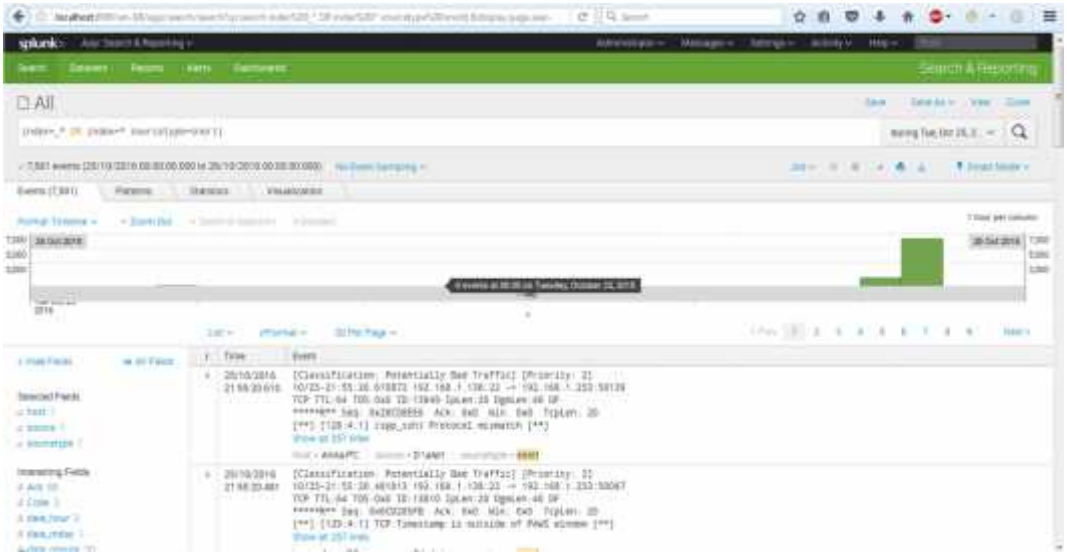
Sejauh ini sistem yang peneliti buat telah memenuhi kebutuhan yang telah direncanakan pada fase *design*. Dengan terpenuhinya parameter yang menjadi

acuan *maintenance* dari IPS *server* dengan kondisi tertentu (melakukan *back up log file* dan *clear alert log cache* sebelum terjadi penurunan performa dengan jumlah alert <1.000.000).

4.1.3.3 Modifikasi

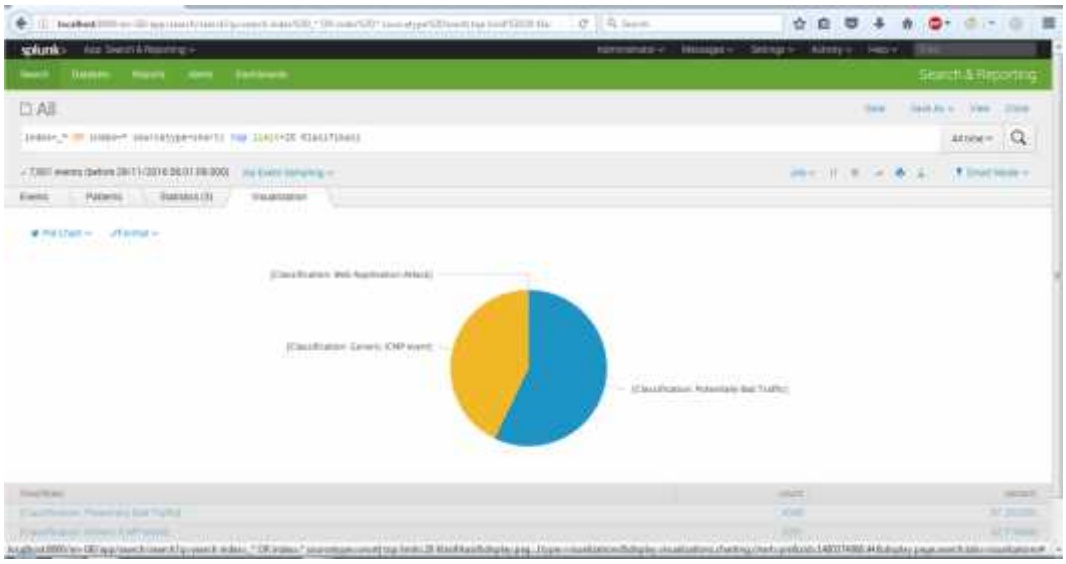
SPLUNK

Penambahan fitur peneliti lakukan pada sisi penyajian data, dengan menggunakan aplikasi ‘splunk’. File output alert yang dihasilkan oleh SNORT dapat langsung diolah oleh splunk tanpa bantuan MySQL dalam melakukan reading file. Ini berguna untuk mengubah data menjadi sebuah grafik yang mudah dipahami seperti pie chart dan bar chart :



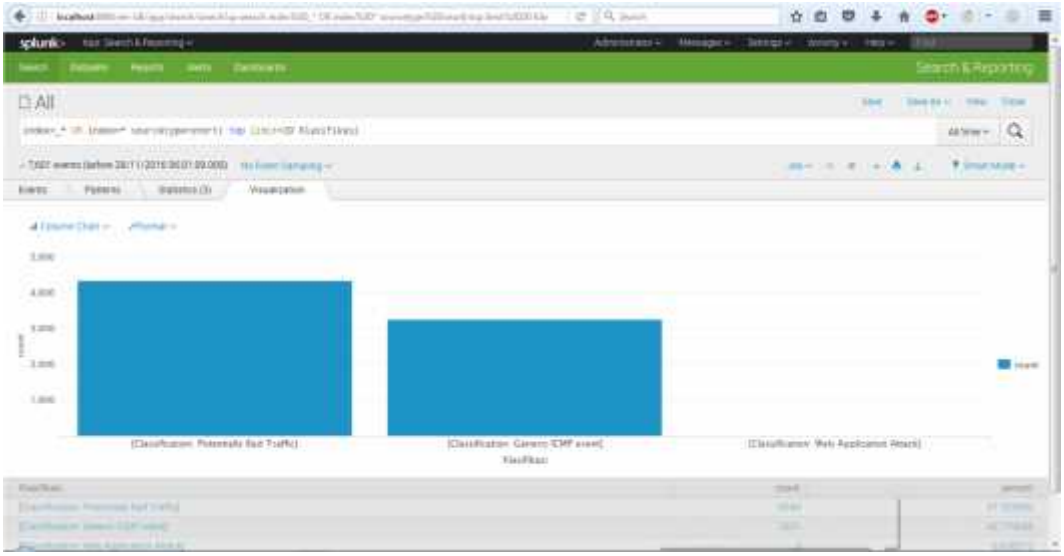
Gambar 4.11 Tampilan halaman utama splunk

Gambar di atas adalah tampilan splunk ketika diberi *input* berupa *alert file* yang dihasilkan saat melakukan *backup* SNORT, berupa pesan notifikasi yang telah diurutkan berdasarkan waktu pendeteksian.



Gambar 4.12 Tampilan splunk *pie chart diagram*

Diagram ini menggambarkan pengelompokkan serangan yang ada dalam *alert file* SNORT berdasarkan klasifikasi serangan, yaitu 1% *web application attack*, 39% *generic* ICMP *event*, dan 60% *pottentially bad traffic*.



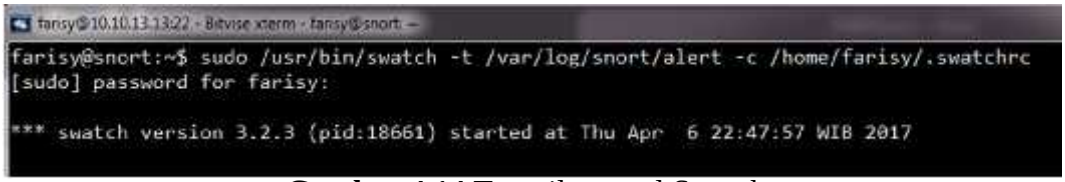
Gambar 4.13 Tampilan splunk *bar chart diagram*

Dan diagram di atas adalah tampilan alternatif yang dapat dihasilkan dari *alert file* SNORT yang sama.

Fitur *e-mail Notification*

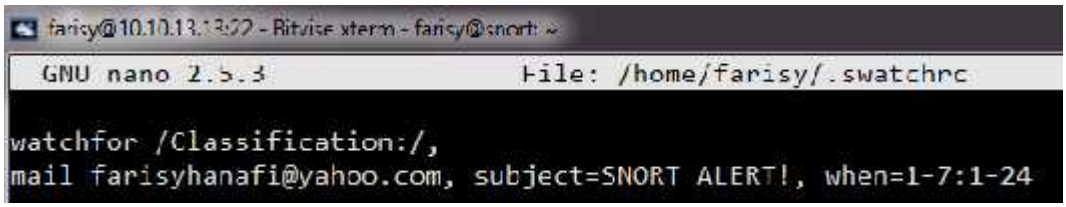
Laporan dari ancaman yang terjadi dapat dikirim menggunakan *e-mail* dengan bantuan aplikasi Swatch yang dapat mengirimkan email secara otomatis ketika kata kunci yang kita inginkan di *generate* oleh SNORT ke dalama *log alert file*. Untuk menjalankan aplikasi ini penulis memberikan perintah di terminal :

sudo /usr/bin/swatch -t /var/log/snort/alert -c /home/farisy/.swatchrc



Gambar 4.14 Tampilan awal Swatch

Sudo untuk menjalankan swatch dengan *privilege* tertinggi –t adalah untuk memberi tahu swatch untuk melakukan pemantauan pada file alert sedangkan –c adalah perintah untuk memberikan swatch konfigurasi sesuai dengan *bash script* yang dibuat di .swatchrc.



Gambar 4.15 Tampilan *bash script* Swatch

Watchfor untuk memberikan perintah untuk memantau kata apa yang akan dikirimkan. Peneliti memilih *classification* dan *address* sebagai kata kunci yang digunakan oleh Swatch untuk digunakan sebagai parameter pemicu untuk mengirim Mail ke email yang dipilih dengan *subject* SNORT ALERT, dan waktu pengiriman 1-7 (senin sampai minggu), 1-24 (jam 01.00 sampai 24.00).

Ketika ada laporan yang masuk dengan kata kunci *clasification* ke *file alert* maka swatch akan mengirim notifikasi ke farisyhanafi@yahoo.com.

Gambar 4.16 Tampilan *e-mail notification*

Waktu pengiriman yang dibutuhkan oleh fitur ini adalah *real-time* setelah terpicunya *alert log* dari SNORT. *Relay host* yang peneliti gunakan adalah smtp.google.com:465. Sistem SMTP gratis yang dapat digunakan dari google

dengan menambahkan *script* pada *file* /etc/postfix/main.cf dan menambahkan relayhost. Peneliti melakukan percobaan dengan mengirimkan ke farisyhanafi@yahoo.com dan farisychemicalromance@gmail.com. Kecepatan pengiriman dengan koneksi yang stabil membutuhkan waktu 1-3 detik untuk sampai ke alamat *e-mail* yang dituju. *E-mail notification* yang peneliti buat dapat diandalkan untuk memberikan laporan secara *real time* untuk dapat segera ditangani.

4.2 Analisa Perbandingan *Rules*

SNORT IPS memiliki sebuah daftar rules yang dapat digunakan secara bebas yang diperbarui oleh aktivis di komunitas SNORT yang bernama community.rules. Namun kita dapat membuat sendiri *rules* yang kita butuhkan dengan nama local.rules. Dengan *rules* tersebut peneliti dapa membuat *rules* sesuai dengan kebutuhan di lingkungan penelitian ini. Berdasarkan wawancara yang peneliti lakukan terhadap M. Taufiq. R. staf Divisi Infrastruktur UPT TIK Universitas Lampung. Jenis serangan yang terjadi dan berpotensial terjadi adalah *defacing, flooding, phising, e-mail exploit,* dan IP *spoofing*. Dan belum pernah terjadi serangan mencurigakan yang tidak teridentifikasi, sehingga peneliti hanya menggunakan local.rules yang peneliti buat secara manual berdasarkan tipikal serangan yang telah disebutkan, beberapa *rules* yang telah peneliti buat adalah sebagai berikut :

Tabel 4.5 Daftar *rules* pada local.rules

Threat	*Rules*	Keterangan
ICMP	drop icmp any any -> $HOME_NET any (msg:"Ping Flood Detected"; GID:1; sid:10000001; rev:001; classtype:icmp-event;)”	Digunakan pada TA
Brute Force SSH Login	drop ssh any any -> $HOME_NET 22 (msg:"Brute Force Attack Detected"; GID:2; sid:10000002; rev:002; classtype:misc-event;)”	Digunakan pada TA
DDoS	drop udp any any -> $HOME_NET any (msg:"DDoS Attack Detected"; GID:3; classtype:attempted-dos; sid:10000003; rev:003;)	Digunakan pada TA
Backdoor	drop tcp any any -> $HOME_NET 666: (msg:"Ada yang mencoba melakukan injeksi SATAN BACKDOOR"; flow:established,from_server; GID:4; classtype:misc-activity; sid:10000004; rev:004;)	Direkomendasikan
Exploit	drop tcp any any -> $HOME_NET 4321 (msg:"String format Disk terdeksi, Exploit Attack Detected"; flow:to_server,established; content:"-soa %p"; reference:bugtraq,3474; reference:cve,2001-0838; classtype:misc-attack; GID:5; sid:10000005; rev:005;)	Direkomendasikan
SQL Injection	drop tcp any any -> $SQL_SERVERS 139 (msg:"ada yang menambah user database menggunakan eksternal script"; flow:to_server,established; content:"s|00|p|00|_|00|a|00|d|00|d|00|u|00|s|00|e|00|r|00|"; depth:32; offset:32; nocase; classtype:attempted-user; GID:6; sid:1000006; rev:006;)	Direkomendasikan
XSS	drop tcp any any -> $HTTP_SERVERS $HTTP_PORTS (msg:"PHP XSS attempt detected"; flow:established,to_server; uricontent:"/modules.php?"; nocase; uricontent:"<script"; nocase; classtype:web-application-attack; GID:7; sid:10000007; rev:007;)	Direkomendasikan

Setelah melakukan analisa, peneliti memilih untuk tidak menggunakan *rules* yang disediakan oleh komunitas berdasarkan :

Tabel 4.6 Perbandingan *community* dan *local rules*

Jenis *rules*	*Community rules*	*Local rules*
Startup Time	50s – 60s	1s - 5s
Blocking threat	Terjadi *false positive block threat*	Tidak terjadi kesalahan *block threat*
Jumlah *rules*	>10.000	Sesuai dengan kebutuhan
Rules update method	*Automatic using* pulled pork *application*	*Manual*
Rules debugging and maintenace	Sulit, dengan begitu banyaknya kata yang sama dalam *rules*	Mudah, tidak banyak *rules* yang menggunakan kata yang sama

Berdasarkan hasil penelitian tersebut *local rules* lebih cepat dan efisien untuk digunakan serta tidak terjadinya *false positive* yang meminimalisasi terjadinya *blocking* aktivitas yang tidak berbahaya seperti *sharing folder* pada jaringan. Berikut adalah tampilan *false positive* dengan *community rules*

Gambar 4.17 *False positive alert*

Metode *update rules* dengan bantuan aplikasi PULLED PORK akan membuat sistem terus menggunakan *rules* yang dibuat berbagai *user* dalam komunitas snort

yang belum tentu Universitas Lampung butuhkan, sehingga *update rules* secara manual adalah pilihan terbaik untuk menjaga efisiensi dan kemudahan dalam *rules maintenance*. Disinilah pentingnya peran *brainware* yaitu staff TI yang ditugaskan untuk menyesuaikan *rule* dengan *threat* yang berpotensi terjadi.

V. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil penelitian yang dilakukan, peneliti menarik kesimpulan bahwa :

1. Telah berhasil dibangun *protoype* IPS *server,* yang bisa dijadikan alternatif solusi dari sistem keamanan pada salah satu jaringan di Universitas Lampung, sehingga meningkatkan keamanan dalam lalu lintas data di jaringan Universitas Lampung.
2. Dengan menggunakan *dropping packet rules,* telah dapat dilakukan upaya pencegahan terjadinya peretasan ilegal.
3. Fitur pcap DAQ (*packet capture data acquisition*), SNORT *console,* dan Basic Analytics and Security Engine telah dapat digunakan sebagai pengawas lalu lintas data pada *prototype* keamanan jaringan komputer terhadap berbagai *threat*.
4. Penggunaan *local rules* pada sistem yang dibuat, lebih efisien daripada penggunaan *community rules.* Dengan berkurangnya *starting time* SNORT dan meminimalisasi *false positive alert.*
5. *E-mail notification* telah bekerja sesuai kebutuhan dengan waktu pengiriman 1-3 detik, dan *relay host* yang digunakan adalah smtp.gmail.com:465.

5.2 Saran

Penelitian lebih lanjut mengenai IPS *server* dapat dilakukan dengan hal berikut :

1. Melakukan perbandingan performa integrasi SNORT dengan sistem operasi lain seperi Clear OS, freBSD, dll.
2. Membuat *real time dynamic graphical alert* untuk SNORT.

DAFTAR PUSTAKA

[1] Gondohanindijo, Jutono. "IPS (Intrusion Prevention System) Untuk Mencegah Tindak Penyusupan / Intrusi," *Majalah Ilmiah INFORMATIKA*, vol. III, no. 3, 2012.

[2] Gollman, Dieter. Computer Security, United States: Wiley, 2006.

[3] Ariyus, Dony. Internet Firewall, Yogyakarta: GRAHA ILMU, 2006.

[4] Raharja, R. Anton., Yunianto, Afri., and Widyantoro, Wisesa. Pengenalan Linux, Bandung: Telematics Indonesia, 2001.

[5] Lukas, Jonathan. Jaringan Komputer, Yogyakarta: GRAHA ILMU, 2006.

[6] CISCO, "Welcome to the Cisco Unified Communications Contact Center Technical Information Site," 2015. [Online]. Available: http://www.cisco.com/cisco/web/docs/iam/unified/ipcc611/pdfs/01home.pdf. [Accessed 3 January 2016].

[7] Kheyri, Davood., and Karami, Mojtaba. "A Comprehensive Survey on Anomaly-based Intrusion Detection in MANET," *Canadian Center of Science and Education,* vol. 5, no. 4, pp. 133-139, 2012.

[8] Elngar, Ahmed A., Mohamed, Dowlat A. El A., and Ghaleb, Fayed F.M."A Fast Accurate Network Intrusion Detection System," *(IJCSIS) International Journal of Computer Science and Information Security,* vol. 10, no. 9, pp. 29-35, 2012.

[9] Massa, Daniel., and Valverde, Raul. "A Fraud Detection System Based on Anomaly Intrusion Detection Systems for E-Commerce Applications," *Canadian Center of Science and Education,* vol. 7, no. 2, pp. 117-140, 2014.

[10] Ernawati, Tati. "Analisis Visualisasi Data Keamanan Jaringan," *Jurnal Teknologi,* vol. 5, no. 1, pp. 53-61, 2012.

[11] Patil, Suchita., and Meshram, B.B. "Network Intrusion Detection and Prevention Techniques for DoS Attacks," *International Journal of Scientific and Research Publications,* vol. 2, no. 7, pp. 1-4, 2012.

[12] Sagita, Noviana., Cahyani, Niken Dwi., and Yulianto, Fazmah Arif. Perbandingan Performansi Antara Signature Based dan Anomaly Based dalam Pendeteksian Intrusi, Bandung: Telkom University, 2011.

[13] Roesch, Martin. "SNORT," [Online]. Available: https://snort.org/downloads#snort. [Accessed 3 January 2016].

[14] Rich, Amy. "Analyzing Snort Data With the Basic Analysis and Security Engine (BASE)," October 2005. [Online]. Available: http://www.oracle.com/technetwork/systems/articles/snort-base-jsp-138895.html. [Accessed 3 January 2016].

[15] Baum, Michael., Das, Rob., and Swan, Erik. "SPLUNK," [Online]. Available: https://www.splunk.com/. [Accessed 3 January 2016].

[16] Smith, Jason. "Barnyard2," [Online]. Available: https://github.com/firnsy/barnyard2/ archive/7254c24702392288fe6be948f88afb74040f6dc9.tar.gz. [Accessed 3 January 2016].

[17] Aharoni, Mati., Kearns, Devon., and Hertzog, Raphael. "Kali Linux," [Online]. Available: http://www.kali.org. [Accessed 3 January 2016].