JURSIMA
Jurnal Sistem Informasi & Manajemen
ISSN : 2338-1523, E-ISSN: 2541- 576X

RANCANG BANGUN *INTRUSION DETECTION SYSTEM (IDS)* MENGGUNAKAN *SNORT* (STUDI KASUS PT PLN BATAM)

Sunarsan Sitohang[1)], Hotma Pangaribuan[2)]
[12]Universetas Putera Batam, Batam
ssunarsan@gmail.com

ABSTRAK

Keamanan merupakan aspek penting dalam membangun sebuah jaringan. Penggunaan dan pemanfaatan teknologi informasi bagi PT PLN Batam sudah menjadi salah satu komponen penting untuk aktifitas pegawai sehari-hari dalam meningkatkan kinerja perusahaan. Penelitian ini dilakukan untuk membantu administrator jaringan dalam pengawasan *traffic* dan pengawasan terhadap aktifitas yang mencurigakan pada PT PLN Batam. Untuk pengawasan terhadap aktifitas yang mencurigakan pada PT PLN Batam maka sistem deteksi penyusup yang penulis gunakan adalah *Snort* yang berjalan pada Sistem Operasi *Linux* yaitu *Debian*, karena *Snort* bersifat *open source* dan dapat mendeteksi pola serangan sesuai dengan *rules* yang telah ada. Penulis menggunakan *Snort* yang dibantu oleh *interface Snorby* agar memudahkan seorang *administrator* jaringan dalam hal *monitoring*. Hasil *Log* atau *Alert* dari *Snort* disajikan dalam bentuk *Graphichal User Interface (GUI)* menggunakan aplikasi *Snorby* sebagai sistem *monitoring* berupa *Line Chart* dan *Pie Chart*. *Snort* juga dapat menampilkan *Log* atau *Alert* berdasarkan tingkat keparahan yang dibedakan menjadi 3 warna, yaitu *High severity* dengan warna merah yang dikategorikan serangan berbahaya, *Medium severity* dengan warna kuning yang dikategorikan serangan dengan tingkat sedang, dan *Low severity* dengan warna hijau yang dikategorikan sebagai serangan tidak berbahaya atau lemah. Secara umum *Snort* hanya bekerja sebagai pendeteksi dan tidak mampu menahan serangan. Diharapkan kedepannya dapat dikembangkan *Snort* yang mampu mencegah serangan secara otomatis.
Kata Kunci*: Snort*, *Snorby*, *IDS*, Keamanan, Jaringan

ABSTRACT

Security is an important aspect in building a network. The use and utilization of information technology for PT PLN Batam has become an important component for the daily activities of employees in improving company performance. This research was conducted to assist network administrators in monitoring traffic and supervising suspicious activities at PT PLN Batam. For monitoring of suspicious activities at PT PLN Batam, the intruder detection system that the author uses is Snort which runs on the Linux Operating System, namely Debian, because Snort is open source and can detect attack patterns in accordance with existing rules. The author uses Snort which is assisted by the Snorby interface to make it easier for a network administrator in terms of monitoring. Log or Alert results from Snort are presented in the form of a Graphical User Interface (GUI) using the Snorby application as a monitoring system in the form of Line Charts and Pie Charts. Snort can also display Logs or Alerts based on the severity level which is divided into 3 colors, namely High severity in red which is categorized as a dangerous attack, Medium severity in yellow which is categorized as an attack with a moderate level, and Low severity in green which is categorized as an attack that is not dangerous or weak. In general, Snort only works as a detector and is unable to withstand attacks. It is hoped that in the future Snort can be developed which is able to prevent attacks automatically.

Keywords: Snort,Snorby, IDS, Security, Network

JURSIMA
Jurnal Sistem Informasi & Manajemen
ISSN : 2338-1523, E-ISSN: 2541- 576X

PENDAHULUAN

Keamanan merupakan aspek penting dalam membangun sebuah jaringan. Pada dasarnya keamanan yang ada pada sistem operasi belum cukup untuk mengamankan suatu jaringan computer (Sitohang & Setiawan Agus, 2018). Penggunaan dan pemanfaatan teknologi informasi berbasis *internet* bagi PT PLN Batam sebagai Pemegang Izin Usaha Ketenagalistrikan Untuk Umum (PIUKU) dengan wilayah kerja Batam, Rempang dan Galang, sudah menjadi salah satu komponen penting untuk aktifitas pegawai sehari-hari dalam meningkatkan kinerja perusahaan.

Berdasarkan penelitian (Mutaqin, 2016) diperoleh fakta bahwa gangguan keamanan dapat dibagi menjadi dua kategori, gangguan internal dan gangguan eksternal atau keamanan dari luar jaringan. Gangguan dari dalam jaringan terjadi dari pihak yang sudah mengetahui kondisi jaringan, dan gangguan dari luar jaringan terjadi dari pihak yang sengaja ingin melakukan percobaan terhadap sistem keamanan jaringan dari luar.

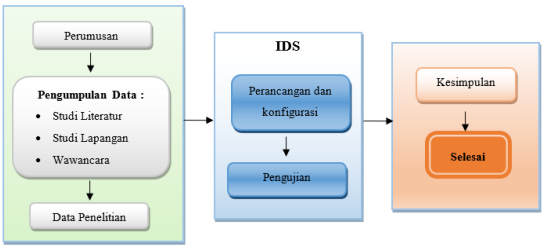
Potensi serangan tersebut bisa memberikan beberapa ancaman bagi pengguna, seperti *Flooding* yaitu serangan yang mengakibatkan suatu sistem akan dibanjiri oleh data-data secara terus menerus dalam waktu yang singkat, yang mengakibatkan lalu lintas jaringan menjadi sangat padat sehingga lalu lintas jaringan yang datang dari pengguna yang terdaftar menjadi tidak dapat masuk ke dalam sistem jaringan, serta menyebabkan penurunan peforma pada sistem jaringan s*erver* yang ada di PT PLN Batam. Pentingnya peranan dan tugas PT PLN Batam perlu menerapkan suatu sistem keamanan jaringan yang handal dan mempunyai kemampuan yang tinggi agar tidak dapat ditembus oleh pihak-pihak yang tidak berhak.

Untuk pencegahan serangan serta meningkatkan kinerja pegawai instansi maka perlu diterapkan *Intrusion Detection System (IDS)* yang dapat membantu *administrator* jaringan dalam pengawasan *traffic* jaringan dan pengawasan terhadap aktifitas yang mencurigakan baik dari lingkungan dalam maupun lingkungan luar perusahaan. *Intrusion Detection System (IDS)* merupakan penghambat semua serangan yang akan mengganggu sebuah jaringan.(Akhyar, 2018); (Aprianto, 2023; Taufikurrahman et al., 2015)

Hasil penelitian (Wijayanto et al., 2015) merancang aplikasi keamanan komputer dengan menggunakan metode dari *Snort Instrusion Detection System* dan mikrotik. Aplikasi ini bertujuan untuk menciptakan sistem keamanan jaringan komputer yang ringan, berbasiskan *web* dan mudah dianalisa serta diatur oleh *administrator*.

Berdasarkan hal tersebut di atas, maka tujuan penelitian ini adalah melakukan perancangan *Intrusion Detection System (IDS) Snort*, sehingga *Snort* dapat mendeteksi dan memberikan *alert* atau pesan peringatan kepada *administrator* ketika ada serangan serta menciptakan sistem pengawasan *traffic* jaringan dan pengawasan jaringan terhadap serangan dari *malware, adware* yang dikirimkan oleh penyusup dan serangan yang disebabkan oleh pengiriman *packet data* secara terus-menerus oleh komputer yang digunakan oleh pegawai.

METODE PENELITIAN



Gambar 1. Desain Penelitian

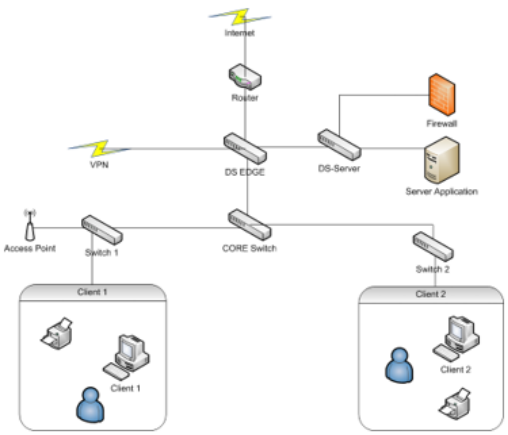
Berikut adalah pembahasan dari gambar 1 sesuai alur desain penelitian dari mulai hingga selesai:

1. Perumusan masalah, merupakan dasar dalam penelitian ini yang sudah dibahas pada pendahuluan

JURSIMA
Jurnal Sistem Informasi & Manajemen
ISSN : 2338-1523, E-ISSN: 2541- 576X

2. Pengumpulan data, yang dibutuhkan dalam penelitian ini adalah, studi literatur, dan wawancara.
3. Data penelitian, data yang sudah diperoleh dengan tiga cara yaitu:,
   a. Studi literatur dengan cara menelusuri sumber-sumber tulisan yang pernah dibuat sebelumnya,
   b. Studi Lapangan yaitu berdasarkan keluhan *user* yang terjadi selama ditempat penelitian.
   c. Wawancara yaitu melakukan wawancara kepada *Network Administrator* terkait keadaan jaringan pada saat melakukan penelitian.
2. Perancangan dan konfigurasi, merupakan melakukan perancangan dan konfigurasi terhadap sistem yang akan dibangun.
3. Pengujian, yaitu melakukan pengujian di tempat penelitian dengan sistem yang sudah dirancang dan dikonfigurasi.
4. Kesimpulan, yaitu menarik kesimpulan atas hasil penelitian, baik data yang didapat, maupun hasil pengujian.
5. Selesai

Sebelum melakukan rancang bangun dilakukan, terlebih dahulu melakukan kajian pemahaman tentang jaringan yang sedang berjalan gambar 2. merupakan gambaran topologi jaringan di PT. PLN Kota Batam.



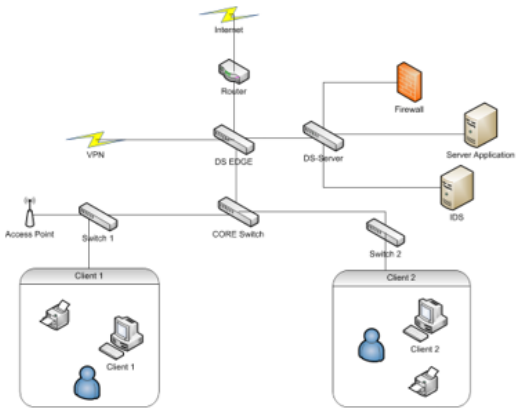
Gambar 2. Topologi Jaringan PT. PLN Batam

Berikut deskripsi singkat tentang jaringan PT. PLN Batam

1. *Provider* yang digunakan di PT PLN Batam adalah Telkom.
2. *DS-Server* atau *Distribution Switch* merupakan tempat semua *Server Application* terhubung ke *Switch*.
3. *Firewall* yang digunakan adalah *Check Point Software Technologies*.
4. *Server Application* merupakan ruangan yang terdiri dari sekumpulan *Server* Aplikasi yang digunakan untuk keperluan pekerjaan sehari-hari, diantaranya: *Server Proxy*, *Server Kaspersky*, AP2T (Aplikasi Pelayanan Pelanggan), *Info* PLNBatam, *BMap* (Aplikasi Distribusi Jaringan Listrik di Kota Batam), *CRM*, *IT360*.
5. *Switch* yang digunakan untuk klien adalah *CISCO Catalyst 3750-X Series*.
6. *CORE-Switch* merupakan tempat terhubungnya DS-EDGE dan Switch untuk klien disetiap lantai.
7. *Access Point* yang digunakan adalah *CISCO WAP121 Wireless-N*.

HASIL DAN PEMBAHASAN

Berdasarkan Analisis yang dilakukan berikut gambar 3 rancangan topologi yang disarankan.



Gambar 3. Usulan Topologi Jaringan

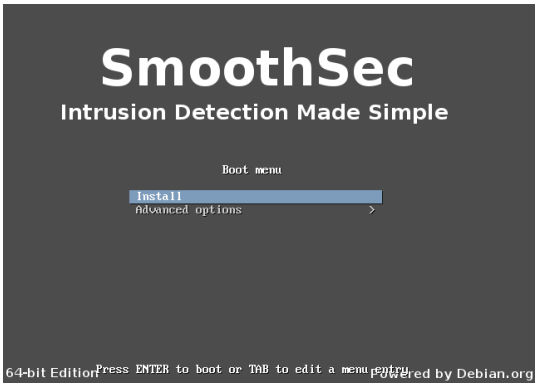
JURSIMA
Jurnal Sistem Informasi & Manajemen
ISSN : 2338-1523, E-ISSN: 2541- 576X

Berdasarkan usulan topologi gambar 3 diatas, IDS ditempatkan diantara DS EDGE dan server application tepatnya di DS server.

Persiapan Tools Snort

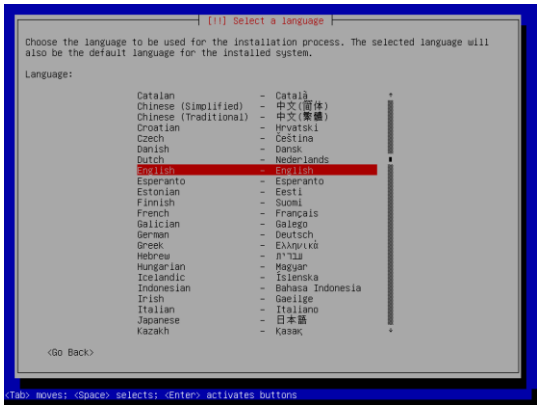
Instalasi *Snort* kedalam komputer *server*. Disini peneliti melakukan instalasi menggunakan media *CD* yang sudah dijadikan *bootable Linux*.

1. Masukkan *CD Installer Linux* kedalam komputer, dan jadikan *CD* tersebut sebagai *bootable* pertama.
2. Tampilan pertama pada saat *booting*, dan pilih *Install* seperti gambar 4.



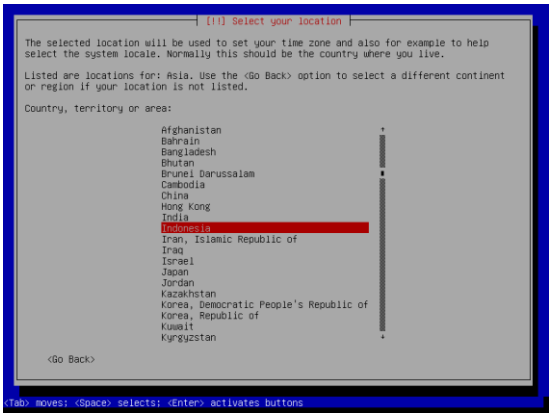
Gambar 4. Tampilan awal

3. Selanjutnya, pilih bahasa yang akan digunakan. Disini peneliti menggunakan bahasa inggris seperti gambar 5, maka pilih *English* dan tekan *Enter*.



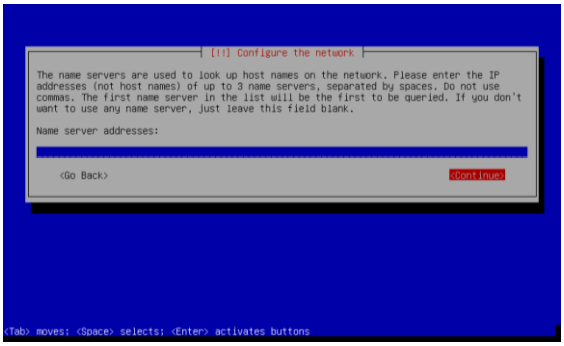
Gambar 5. Bahasa Instalasi

4. Selanjutnya pemilihan lokasi yang akan digunakan untuk *Time-Zone* seperti Gambar 6, disini peneliti memilih Indonesia.



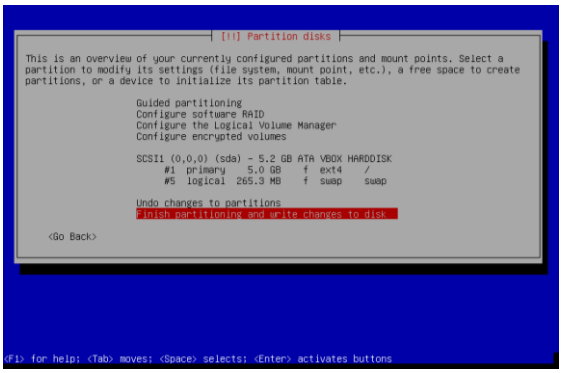
Gambar 6**.** Lokasi dan *Time-Zone*

5. Pada tahap *name server*, peneliti tidak mengisi dan memilih ke tahap selanjutnya dengan cara menekan opsi *Continue* seperti gambar 7.



Gambar 7. *Name servers*

6. Selanjutnya partisi *harddisk*, peneliti menggunakan partisi *harddisk* yang telah disediakan otomatis oleh *Linux*, lalu pilih *"Finish partitioning and write changes to disk"* dan pilih *"Yes"* seperti gambar 8.



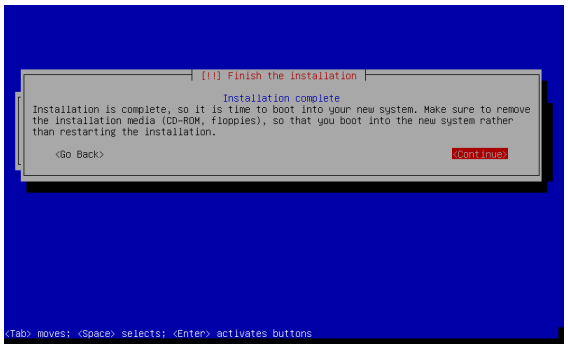
Gambar 8. Partisi *Harddisk*

JURSIMA
Jurnal Sistem Informasi & Manajemen
ISSN : 2338-1523, E-ISSN: 2541- 576X

7. Proses *copy file* ke dalam *harddisk*, tunggu hingga 100%.
8. Selanjutnya *GRUB boot loader*, pilih *Yes* lalu enter seperti gambar 9.

Gambar 9. *GRUB Boot Loader*

9. Instalasi selesai, pilih *Continue*, dan sistem akan *restart.*

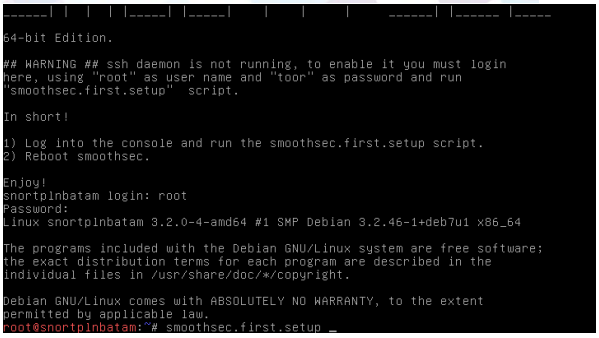


Gambar 10. Instalasi selesai

10. Setelah komputer hidup, maka akan muncul tampilan seperti gambar 11 yaitu tahap konfigurasi awal, kemudian ketikkan *Username : root* dan *Password : toor.*

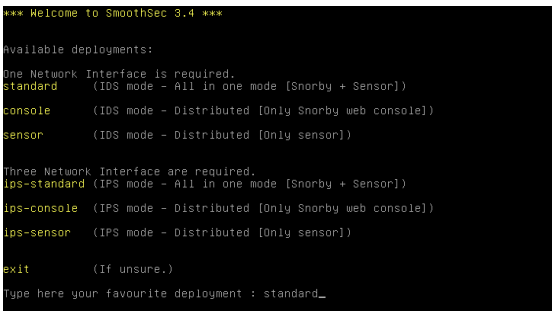
Gambar 11. Tampilan setelah *restart*

11. Setelah *login* berhasil, maka akan tampil seperti gambar 12, dan ketikkan ”*smoothsec.first.setup”* dan *Enter*.



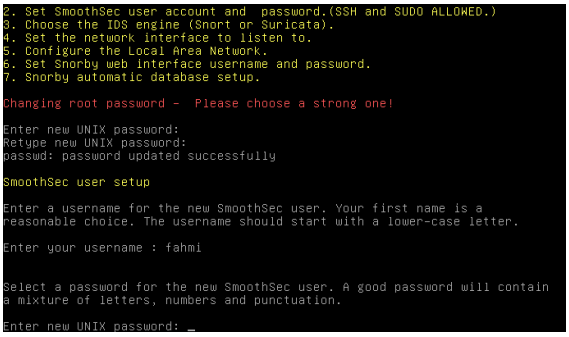
Gambar 12. Tahap Setup Awal

12. Selanjutnya, peneliti memilih *IDS mode*, dan memilih *Snort* sebagai sensor, peneliti mengetikkan “*standard”* lalu *enter* seperti gambar 13.



Gambar 13. *Deployments*

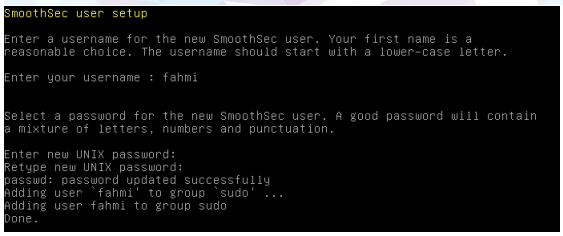
13. Selanjutnya, proses penggantian *password root*, biasa disebut *Administrator* pada *Windows. Password* yang diketikkan tidak akan tampil seperti gambar 14, tetapi tetap terbaca pada *Linux*, dan tekan *enter* untuk tahap selanjutnya.



Gambar 14. Penggantian *Password root*

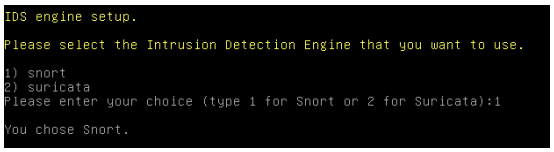
14. Selanjutnya, akan diminta memasukkan *user SmoothSec*, kemudian ketikkan *password* untuk *user* tersebut seperti gambar 15.

JURSIMA
Jurnal Sistem Informasi & Manajemen
ISSN : 2338-1523, E-ISSN: 2541- 576X



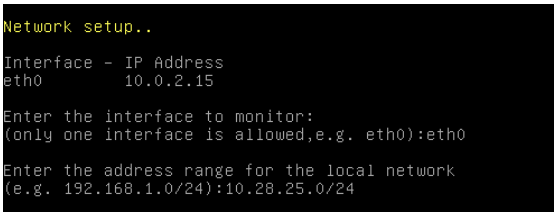
Gambar 15. *SmoothSec user setup*

15. Selanjutnya, disini peneliti memilih *Snort* sebagai *IDS engine.* Maka ketikkan angka 1 seperti gambar 16, lalu *enter*.



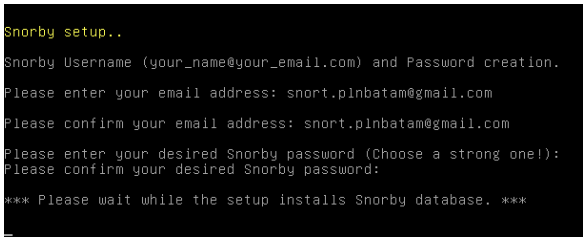
Gambar 16. *IDS engine setup*

16. Selanjutnya *Network setup, server IDS* menggunakan "eth0" sebagai *network interfaces.* Dan menggunakan *ip address range* 10.28.25.0/24 seperti gambar 17.



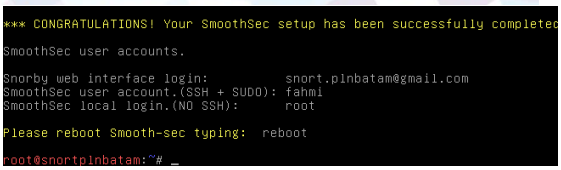
Gambar 17. *Network setup*

17. Selanjutnya *Snorby setup*, yang akan digunakan untuk *login* kedalam sistem (*Web interface)* dari *Snorby*.



Gambar 18. *Snorby setup*

18. Selanjutnya akan ditampilkan informasi dari yang telah dibuat seperti gambar 19. Lalu ketik *reboot* untuk merestart sistem. Dan sistem telah berhasil dikonfigurasi.

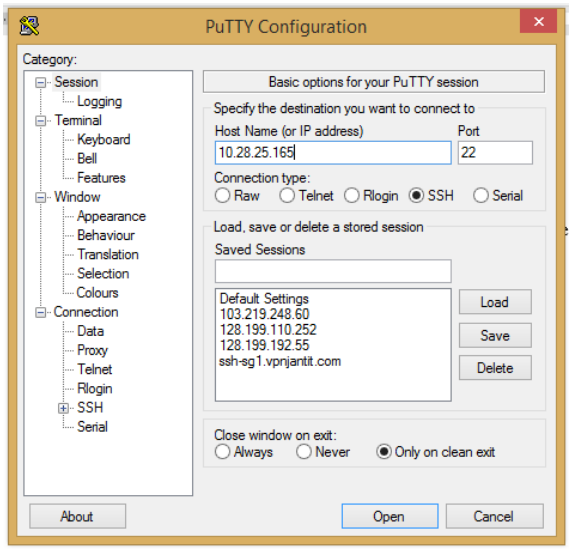


Gambar 19. Konfigurasi selesai

Pembahasan

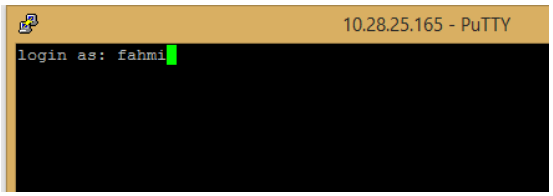
Untuk melakukan *remote server*, peneliti menggunakan *software putty*, dengan cara sebagai berikut :

1. Unduh *software putty* pada *link* http://www.putty.org/
2. Buka *putty*, lalu pada kolom *Host Name* ketikkan *IP Address* (10.28.25.165) dari *server Snort* dan gunakan *port 22* seperti gambar 20.



Gambar 20. Halaman awal *Putty*

3. Klik *Open* untuk memulai sesi *remote.*
4. Ketikkan *username* yang digunakan seperti gambar 21, lalu *Enter* pada *keyboard.*

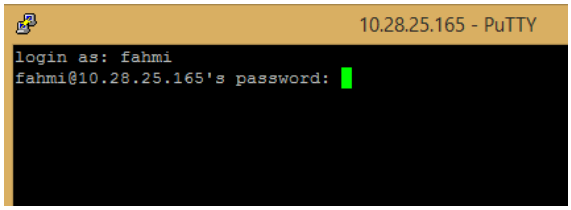


Gambar 21. *Input username*

5. Selanjutnya ketikkan *password*, pada saat mengetikkan password tidak muncul karakter apapun jangan panik,

JURSIMA
Jurnal Sistem Informasi & Manajemen
ISSN : 2338-1523, E-ISSN: 2541- 576X

tidak ada yang salah, memang seperti itu prosesnya seperti gambar 22.

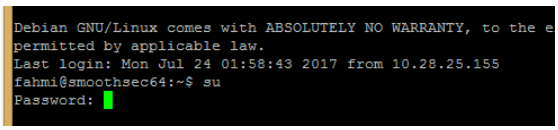


Gambar 22. *Input password*

6. Jika berhasil *Login*, maka akan tampil seperti gambar 23

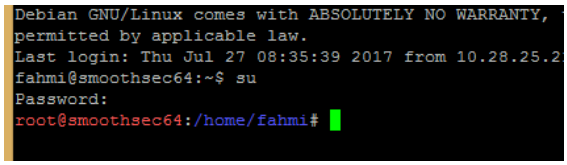
Gambar 23. Berhasil login *user*

7. Jika ingin menggunakan akses *Root*, ketikkan perintah "*su*" (tanpa tanda kutip) kemudian *Enter*.



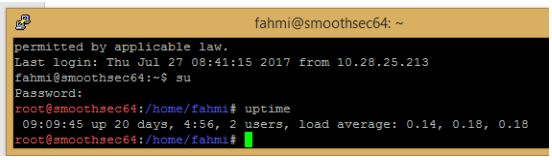
Gambar 24. *Login Root*

8. Ketikkan *password Root*, kemudian *Enter*.
9. Jika berhasil, maka akan tampil seperti gambar 25.



Gambar 25. Berhasil *login root*

10. Untuk melihat sudah berapa lama *server* menyala, ketikkan perintah *uptime* kemudian *Enter*.
Pada gambar 26 *server* sudah menyala selama 20 hari.



Gambar 26. *Uptime Server*

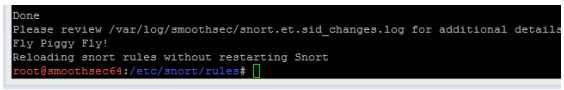
Update Rules

Untuk melakukan *update rules* :

1. Ketikkan perintah "*smoothsec.snort.rules.update*" (tanpa tanda kutip) kemudian *enter* seperti gambar 26.

Gambar 26. *Update Rules*

2. Jika berhasil, maka akan tampil seperti gambar 27.



Gambar 27. Berhasil *update rules*

3. Kemudian ketikkan perintah *"/etc/init.d/snort restart*" (tanpa tanda kutip) untuk melakukan *restart* pada *snort* agar *rules* yang baru bisa diterapkan.

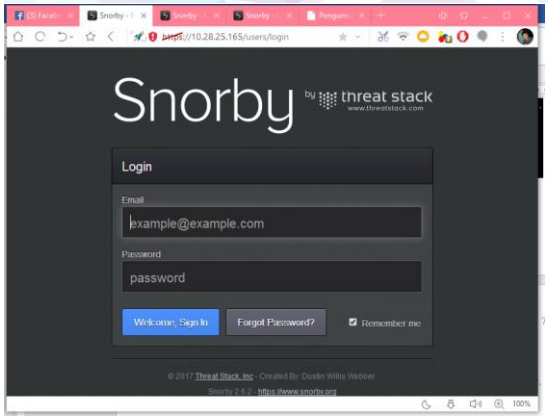
Gambar 28 *Restart service snort*

Snorby Web Interface

Mengoperasikan *Snort* pada *browser*

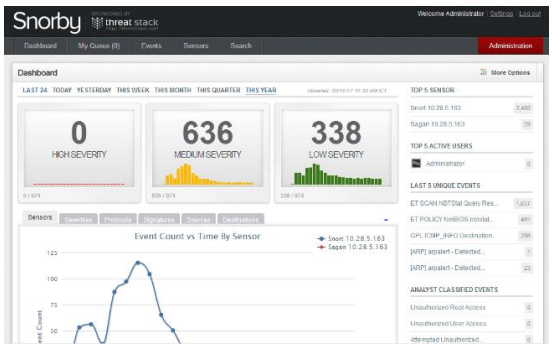
1. Buka *browser*, kemudian ketikkan 10.28.25.165 pada *address bar* dan *enter* seperti gambar 29.

JURSIMA
Jurnal Sistem Informasi & Manajemen
ISSN : 2338-1523, E-ISSN: 2541- 576X



Gambar 29. Halaman *Login*

2. Ketikkan *Email* dan *Password* yang sudah di daftarkan untuk *Login Snorby*
3. Jika berhasil *login*, maka akan tampil *dashboard snorby* seperti gambar 30. Terlihat pada gambar 30, menunjukkan angka 636 pada *medium severity* dan 338 pada *low severity*, ini artinya *snort* telah berhasil meng-*capture packet* pada saat sebelum melakukan *login.*



Gambar 30. Halaman *Dashboard*

Hasil Pengujian

Dari hasil pengujian di peroleh hasil seperti gambar 31.

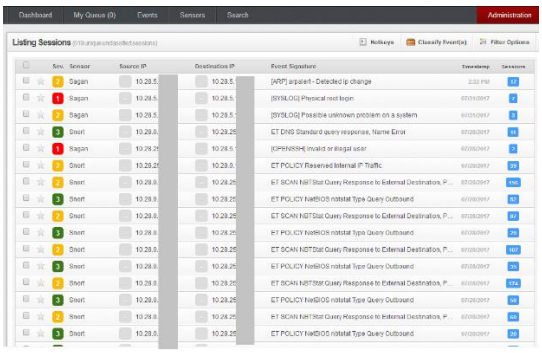
Gambar 31**.** Hasil Pengujian

Dari hasil gambar 30 dan gambar 31 terlihat bahwa telah terjadi perubahan grafik yang signifikan, hal ini menunjukan sensor *IDS* dapat mendeteksi dengan baik.

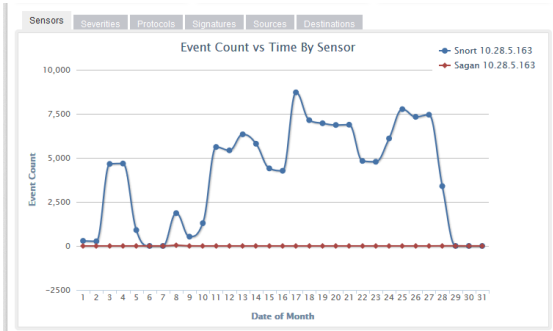
Pada kolom disebelah kanan terdapat *Last 5 Unique Events* juga teridentifikasi beberapa jenis serangan diantaranya *arpalert-Detected ip change*, *Physical root login*, *Possible unknown problem on a system*, *GPL SCAN Same SRC/DST*, *ET DNS Standard query response name error*.

Pada menu tab *events* akan menampilkan detail jenis serangan, *ip source dan ip destination* dengan label merah (1), kuning (2), hijau (3) yang menunjukan *level* prioritas serangan seperti gambar 32.

Snorby menyajikan data-data dalam bentuk *Line Chart* seperti pada gambar 32 dan *Pie Chart* seperti pada gambar 33.



Gambar 32. Menu *Events Snorby*



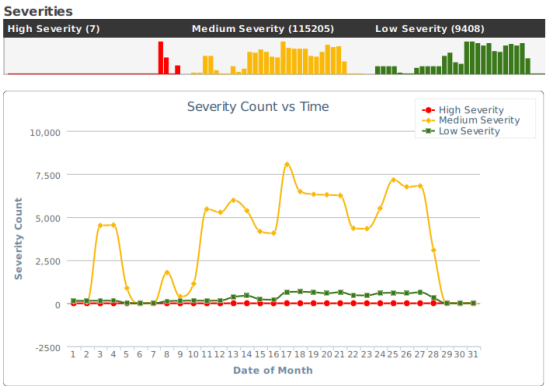
Gambar 33. Tampilan *Line Chart* Pada *Sensors*

Pada gambar 31 terdapat *tab severities*, *snorby* menampilkan data dalam bentuk *Line Chart* yang terdiri dari:

JURSIMA
Jurnal Sistem Informasi & Manajemen
ISSN : 2338-1523, E-ISSN: 2541- 576X

1. *High Severity* (7) berwarna merah, yaitu tingkat serangan yang dianggap berbahaya.
2. *Medium Severity* (115205) berwarna kuning, yaitu tingkat serangan yang dianggap sedang
3. *Low Severity* (9408) berwarna hijau, yaitu tingkat serangan yang dianggap tidak berbahaya atau lemah.

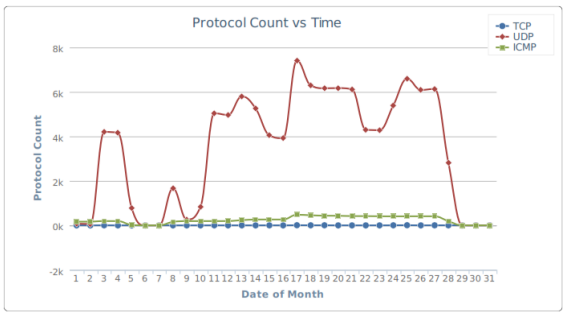
Pada gambar 34 dapat dilihat *Snort* menampilkan data dari tanggal 1 hinggal 31 Juli, yang terdiri dari 35 protokol *TCP*, 108841 protokol *UDP*, dan 7535 protokol *ICMP*.



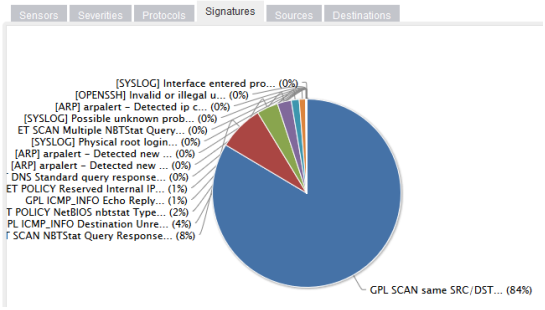
Gambar 34. Tampilan *Line Chart* Tingkat Keparahan

Protocols

TCP Count	UDP Count	ICMP Count	Total
35	108841	7535	124620



Gambar 35. Tampilan *Line Chart* Jenis *Protocol*



Gambar 36. Tampilan *Pie Chart* Jenis Serangan

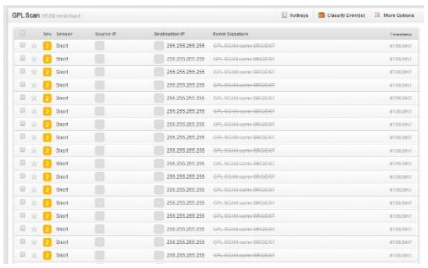
Tabel 1. Serangan

Signature Name	Percentage	Event Count
GPL SCAN same SRC/DST	83.56%	104132
ET SCAN NBTStat Query Response to External Destination, Possib...	7.76%	9671
GPL ICMP_INFO Destination Unreachable Port Unreachable	3.66%	4559
ET POLICY NetBIOS nbtstat Type Query Outbound	2.38%	2969
GPL ICMP_INFO Echo Reply	1.36%	1689

Dari tabel 1 di atas terdapat pada *Signature name GPL SCAN same SRC/DST* terdapat *Event Count* 104132, ini dimaksudkan bahwa yang terdeksi dan berpotensi *bad traffic* sekitar 104132 *packet*.

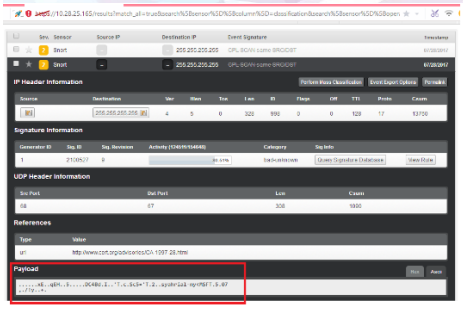
Setelah melihat pada tab *Event*, *Snort* tidak menampilkan *Source IP* seperti gambar 36, tetapi jika di klik akan terlihat informasi jelas pada bagian *Payload* seperti gambar 37.

Ditemukan *Payload* pada gambar 37 yang merujuk pada *Computer Name* SYAHRIAL-MY, yang artinya *Source IP* adalah SYAHRIAL-MY.



Gambar 37. GPL SCAN same SRC/DST

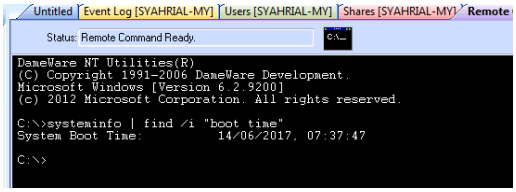
JURSIMA
Jurnal Sistem Informasi & Manajemen
ISSN : 2338-1523, E-ISSN: 2541- 576X



Gambar 38**.** *Payload* pada *Event*

Pada tanggal 21 Juli 2017 Pukul 23:19 WIB, penulis menggunakan *Software DameWare Utilities* yang biasa digunakan untuk mengontrol komputer jarak jauh pada PT PLN Batam, penulis menggunakan *Remote Command* untuk mengetahui berapa lama komputer SYAHRIAL-MY menyala.

Didapat hasil bahwa komputer tersebut sudah menyala sejak tanggal 16 Juni 2017 Pukul 07:37 WIB seperti gambar 39, inilah yang salah satu penyebab *Snort* mendeteksi banyaknya *Event bad traffic.*



Gambar 39. *Remote Command*

SIMPULAN

Berdasarkan hasil pengujian yang telah dilakukan, maka dapat diambil kesimpulan bahwa :

1. Sistem deteksi penyusup yang digunakan adalah *Snort* dan dapat mendeteksi pola serangan sesuai dengan *rules* yang telah ada.
2. Secara umum *Snort* bekerja hanya sebagai sistem deteksi dan tidak mampu menahan serangan, sehingga memerlukan tindakan pencegahan serangan.

UCAPAN TERIMA KASIH

Terimakasih kepada seluruh rekan akedemisi yang telah memberikan kontribusi dalam penelitian ini. Baik kontribusi langsung maupun tidak langsung. Demikian pula kepada staff PLN Batam, khususnya departemen IT.

DAFTAR PUSTAKA

Akhyar, Z. (2018). *Rancang Bangun Sistem Pengiriman Alert Instrusion Detection System Suricata Melalui Telegram*. *2*(1).

Aprianto, M. (2023). Desain Dan Implementasi Intrusion Detection System Menggunakan Debian 7 Dan Snort. *Teknologipintar.Org*, *3*(3). www.aprianto.com,

Mutaqin, A. F. (2016). Rancang Bangun Sistem Monitoring Keamanan Jaringan Prodi Teknik Informatika Melalui SMS Alert dengan Snort. *Jurnal Sistem Dan Teknologi Informasi (JUSTIN)*, *1*(1).

Sitohang, S., & Setiawan Agus, S. (2018). Implementasi Jaringan Fiber To The Home (Ftth) Dengan Teknologi Gigabit Passive Optical Network (Gpon). *Jurnal SIMETRIS*, *9*(2).

Taufikurrahman, A., Syamsul, L. A. A. I., & Widiartha. (2015). Intrusion Prevention System Pada Server Fakultas Teknik Universitas Mataram Intrusion Prevention System On Mataram University Server. *Dielektrika*, *2*(1), 27–31.

Wijayanto, P., Hamzah, A., & Sholeh, M. (2015). *Aplikasi Monitoring Keamanan Jaringan Dengan Menggunakan Ids Dan Router Mikrotik*. *2*(2), 6–15.