AITI: Jurnal Teknologi Informasi, Volume 16 No. 2 Agustus 2019, 135-150
ISSN 1693-8348 E-ISSN 2615-7128

JURNAL TEKNOLOGI INFORMASI

# Simulasi Sistem Keamanan Jaringan Komputer Berbasis IPS *Snort* dan *Honeypot Artilery*

**Alja Aminanto[1], Wiwin Sulistyo[2]**
[1,2]Fakultas Teknologi Informasi Universitas Kristen Satya Wacana
Jl. Dr. O. Notohamidjojo 1-10, Salatiga 50711, Indonesia
Email : [1]672015235@student.uksw.edu, [2] wiwinsulistyo@uksw.edu

***Abstract***

*The Intrusion Prevention System (IPS) Snort is a server security System that can prevent attacks by examining and recording all data packets as well as recognizing packets with sensors, when the attack has been identified, IPS Snort will deny the access (block) and log of all data packets identified. However by using only IPS Snort which can only check and note the Allert attacks that are incoming in less sense to secure a server by collaborating with the other server's secure system in the sense of being able to make the network security of the server better. Honeypot Artillery chosen which works when there is a Hacker trying to penetrate through open ports can be detected as if hackers can break through the system, then Honeypot Artillery will provide information about who attackers and how the attacker could enter the Snort IPS system for later record in the database that can be viewed on the Web interface, Allert recorded on the experiment that has been done in the database as much as 9453 on TCP protocol as much as 9%, UDP as much as < 1%, and ICMP As much as 91%.*

***Keywords:*** *IPS, Snort, Honeypot Artillery*

**Abstrak**

IPS (*Intrusion Prevention System*) *Snort* merupakan sistem keamanan *server* yang dapat mencegah serangan dengan memeriksa dan mencatat semua paket data serta mengenali paket dengan sensor, disaat serangan telah teridentifikasi, IPS *Snort* akan menolak akses (*block*) dan mencatat (*log*) semua paket data yang teridentifikasi tersebut. Namun dengan hanya menggunakan IPS *Snort* yang hanya dapat memeriksa dan mencatat *Allert* serangan yang masuk dirasa kurang untuk mengamankan sebuah *server* dengan mengkolaborasikan dengan sistem keaman *server* yang lain dirasa dapat membuat kemanan jaringan *server* menjadi lebih baik. Dipilihlah *Honeypot Artillery* yang berfungsi ketika ada *Hacker* mencoba melakukan penetrasi melalui *port* yang terbuka maka dapat terdeteksi seolah olah *Hacker* dapat menembus sistem, lalu *Honeypot Artillery* akan memberikan informasi tentang siapa penyerang dan bagaimana penyerang bisa masuk ke sistem *Snort* IPS untuk kemudian dicatat di *database* yang dapat dilihat di *web interface*, *Allert* yang tercatat pada percobaan yang telah dilakukan di *database* sebanyak 9453 pada protokol TCP sebanyak 9%, UDP sebanyak <1%, dan ICMP sebanyak 91%.

**Kata kunci:** IPS, *Snort, Honeypot Artillery*

## 1. Pendahuluan

Ancaman siber kini mempunyai spektrum yang sangat lebar, salah satu ancaman terbesar adalah *malware*. Sebagai contoh adalah serangan *malware ransomware* yang pernah mengakibatkan dua rumah sakit di Indonesia lumpuh. Dalam laporan tahunan *Honeynet Project* tahun 2018, jumlah total serangan yang menyerang Indonesia pada 21 sensor yang telah terpasang yaitu sebanyak 12.895.554 serangan, dengan jumlah serangan malware sebanyak 513.863 serangan[1]. Berkaca pada kasus tersebut dibutuhkan sistem maupun perangkat yang mumpuni dalam mendeteksi serta malacak serangan-serangan siber, dengan begitu sistem jaringan *server* perlu dilengkapi dengan adanya sistem keamanan yang memadai sehingga mampu mendeteksi aktifitas yang mencurigakan agar bisa diambil tindakan yang sesuai. Salah satunya menggunkan sistem IPS (*Intrusion Prevention System*) *Snort* yang dapat mencegah serangan dengan memeriksa dan mencatat semua paket data serta mengenali paket dengan sensor, disaat serangan telah teridentifikasi, IPS *Snort* akan menolak akses (*block*) dan mencatat (*log*) semua paket data yang teridentifikasi tersebut. Namun dengan hanya menggunakan IPS Snort yang hanya dapat memeriksa dan mencatat *Allert* serangan yang masuk dirasa kurang untuk mengamankan sebuah *server* dan belum cukup untuk menahan, dan melakukan respon balik yang tepat kepada *attacker* pada sebuah jaringan komputer. Maka dari itu kelemahan *Snort* IPS yang ada akan dicoba untuk diminimalisir dengan mengkolaborasikan dengan sistem keaman *server* yang lain. Dipilihlah *Honeypot Artillery* yang berfungsi ketika ada *Hacker* mencoba masuk melalui port yang terbuka maka dapat terdeteksi lalu *Honeypot Artillery* akan memberikan informasi tentang siapa penyerang dan bagaimana penyerang bisa masuk ke sistem *Snort* IPS untuk kemudian dicatat di *database* yang dapat dilihat di *web interface*.

Mengacu pada latar belakang yang ada maka dilakukan penelitian yang bertujuan untuk menerapkan sistem keamanan jaringan berbasis *Intrusion Prevention System* (IPS) menggunakan *snort* dan *Honeypot Artillery*, bisa membantu administrator jaringan dalam mengamankan sistem jaringan (lokal / internet) yang digunakan dari ancaman pencurian dan perusakan data serta dapat mengetahui jenis – jenis serangan yang mengancam sistem.

## 2. Tinjuan Pustaka

Penelitian sebelumnya yang menjadi acuan berjudul " Rancang Bangun Snort Base IPS " *Intrusion Prevention Systems* (IPS) merupakan sistem perangkat lunak, yang digunakan untuk mendeteksi ancaman yang terjadi di suatu jaringan atau sistem jaringan sebagai tindakan perlindungan data yang ada di dalam jaringan. Snort merupakan salah satu *tools* yang digunakan pada IPS yang berfungsi sebagai alert, sehingga *snort* menjadi *tool* pilihan dalam mengamankan jaringan komputer.

Pengaturan IPS pada snort perlu memperhatikan kondisi dan kebutuhan sistem jaringan pada studi kasus[2].

Menurut penelitan selanjutnya "Analisis dan Implementasi Honeypot Menggunakan Dionaea Sebagai Penunjang Keamanan Jaringan " Penelitian selanjutnya disarankan memperhatikan implementasi *honeypot* harus seimbang antara keamanan pada aspek jaringan dengan keamanan pada aspek sistem operasi, karena teknologi selalu berkembang maka tingkat keamanan sistem operasi selalu berkembang dan sistem operasi selalu diperbaharui. Disamping itu honeypot akan lebih baik lagi apabila dikombinasikan[3].

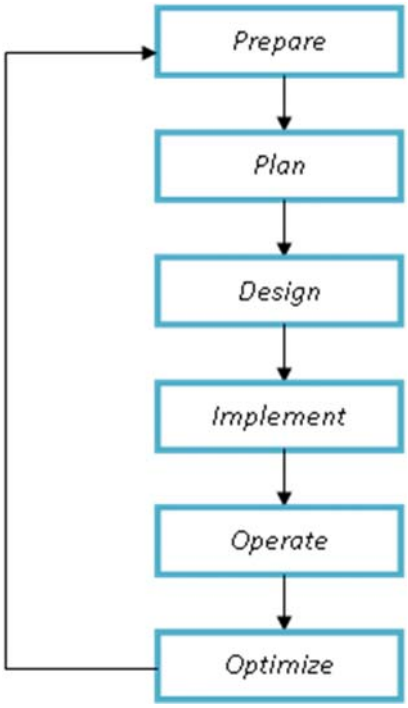
Intrusion Prevention System (IPS), adalah pendekatan yang sering digunakan untuk membangun sistem keamanan komputer. IPS mengkombinasikan teknik firewall dan metode Intrusion Detection System (IDS) dengan sangat baik. Teknologi ini dapat digunakan untuk mencegah serangan yang masuk ke jaringan lokal 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, dimana pendeteksian paket yang masuk dan keluar (inbound-outbound) dapat dideteksi sedini mungkin sebelum merusak atau mendapatkan akses ke dalam jaringan lokal[4].

*Snort* merupakan salah satu *tool* pada IDS dengan komunitas *opensource* sehingga *Snort* menjadi *tool* pilihan dalam mengamankan jaringan komputer. Kemudahan memahami rules pada Snort dan kemudahan dalam membuat signature juga merupakan keunggulan yang dimiliki oleh Snort[5].

Honeypot adalah *security resource* yang yang sengaja dibuat untuk diselidiki, diserang, atau dikompromikan[6]. *Honeypot* merupakan suatu cara untuk membuat sistem palsu atau layanan palsu yang berfungsi untuk menjebak pengguna yang mempunyai tujuan buruk atau menangkal usaha-usaha yang dapat merugikan sistem atau layanan [7].

## 3. Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah model PPDIOO (*Prepare, Plan, Design, Implement, Operate, and Optimize* )[8].




**Gambar 1** Tahapan Penelitian

Model penelitian pada Gambar 1, dijelaskan sebagai berikut:

Tahap perencanaan (*Plan*) dilakukan dengan cara membaca jurnal dan refrensi yang telah dikumpulkan untuk mengtahui cara kerja dan kebutuhan sistem agar berjalan seperti yang diharapkan.Kemudian dilanjutkan ke tahap persiapan seperti memetakan kebutuhan sistem berupa software yang diperlukan untuk mendukung sistem tersebut. Pada tahap Perencanaan (*prepare)* ini bersamaan dengan tahap Persiapan (*plan),* dikarenakan antara persiapan dan perancangan keduanya saling berhubungan dan menjadi dasar yang harus diperhatikan. Sehingga tahap selanjutnya menjadi lebih terarah.

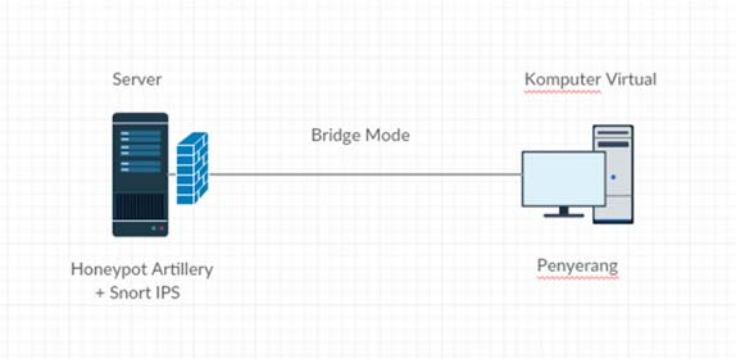
Tabel 1 berisi pemetaan *Software* atau perangkat lunak yang dibutuhkan untuk membangun sistem sebagai berikut :

**Tabel 1** Pemetaan perangkat lunak

| No | Jenis | Versi | Keterangan |
|---|---|---|---|
| 1 | Ubuntu server | 19.04 | Sebagai OS server |
| 2 | Snort | 2.9.14 | Untuk mencatat Allerts yang masuk |
| 3 | Acidbase | 1.4.5 | Untuk mengecek alert jaringan |
| 4 | Honeypot Artillery | 1.5 | Sistem keamanan yang diimplementasikan |

*Hardware* atau perangkat keras yang digunakan untuk membangun sistem adalah Laptop Toshiba Satellite L645 dengan spesifikasi *processor* Intel Core i5 dan RAM 4GB DDR3. Laptop tersebut digunakan sebagai *development server*.

Setelah persiapan *hardware* dan *software* selesai, selanjutnya masuk pada tahapan *design. Design* merupakan tahapan perancangan topologi jaringan yang digunakan.




**Gambar 2** RancanganTopologi Jaringan

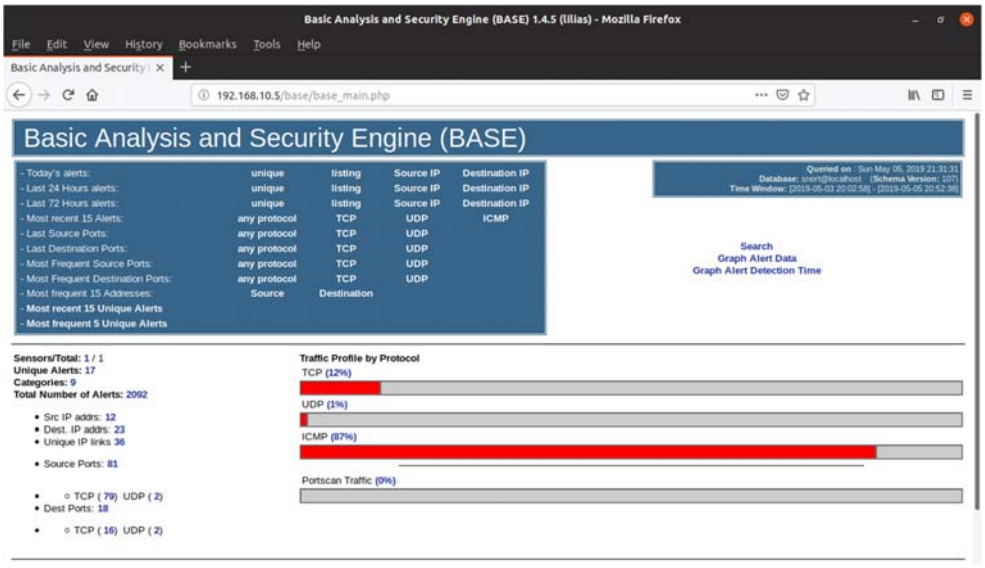
Dalam pembuatan proyek akhir ini penulis menggunakan 1 buah laptop sebagai *server* dan software *Virtual Box* untuk komputer virtual yang digunakan sebagai *client*/penyerang, untuk penghubung antara *server* dan penyerang menggunakan mode *Bridge*. Server dikonfigurasi menggunakan Artillery dan Snort IPS sebagai sistem keamanan. Komputer virtual *client*/Penyerang digunakan untuk melakukan uji coba layanan dan uji coba sistem keamanan.

**Tabel 2** Pengalamatan Perangkat

| No | Perangkat | Alamat Perangkat |
|---|---|---|
| 1 | *Server* | 192.168.10.5/24 |
| 2 | *Client* / Penyerang | 192.168.10.8/24 |

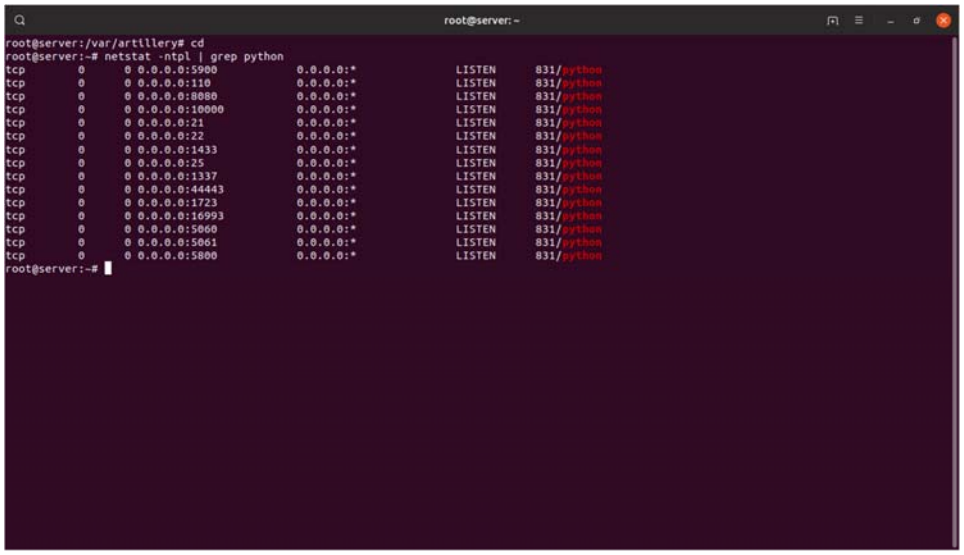
## 4. Hasil dan Pembahasan

Fase Implementasi (*Implement*)"Simulasi Sistem Keamanan Jaringan Komputer Berbasis IPS *Snort* dan *Honeypot Artilery*" terbagi menjadi dua bagian, yaitu implementasi instalasi sistem keamanan *Honeypot Artillery* dan *Snort IPS.*




**Gambar 4** tampilan *Base Snort*

Pada gambar 4 menunjukan instalasi *Snort Base* telah berhasil ditunjukkan dari *Total Number of Alerts* yang bertambah pada saat dilakukan *test ping*. Kemudian pada baris *Traffic Profile by Protocol* menujukan statistik serangan apa saja yang masuk di *server*.




**Gambar 5** *port* yang telah dikonfigurasi.

**Gambar 5** menunjukan instalasi *Honeypot Artillery* telah berhasil ditunjukkan dengan *port* yang dikonfigurasi telah muncul seperti pada **gambar 5.** Maka konfigurasi *port* pada *server* menggunakan *Honeypot Artillery* telah berhasil dan siap untuk menangkap serangan yang masuk pada setiap port yang telah di-*setting*.

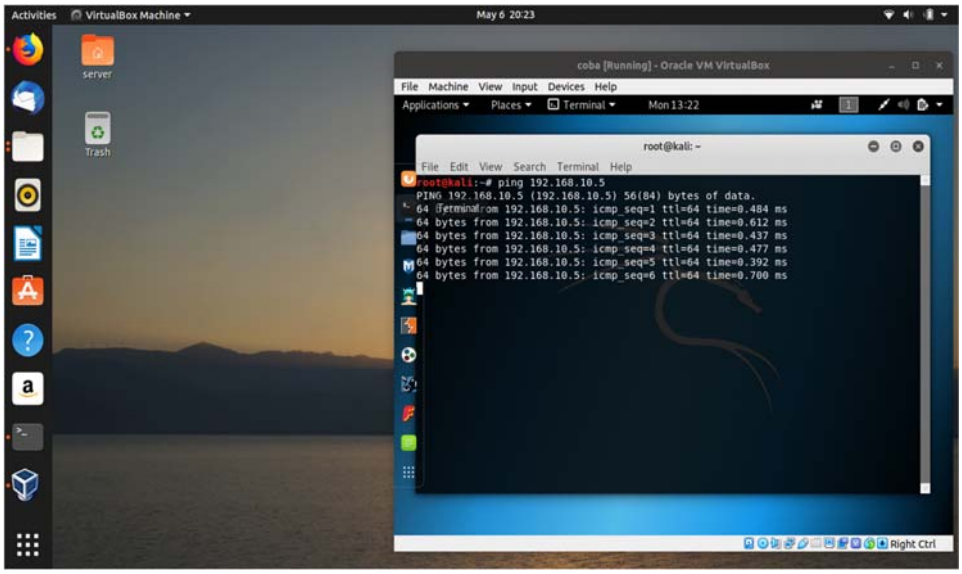
Skenario Fase *Operate* (Operasional) pengujian untuk Tugas Akhir "Simulasi Sistem Keamanan Jaringan Komputer Berbasis IPS *Snort* dan *Honeypot Artilery*" adalah sebagai berikut:

a. *Administrator* akan melakukan konfigurasi pada *Honeypot Artillery* untuk menentukan *port* yang akan diemulasi pada *server*.

b. Setelah *Honeypot Artillery* dikonfigurasi, *Client*/Penyerang akan melakukan koneksi ke *server* dan melakukan *scanning* menggunakan *NMAP*.

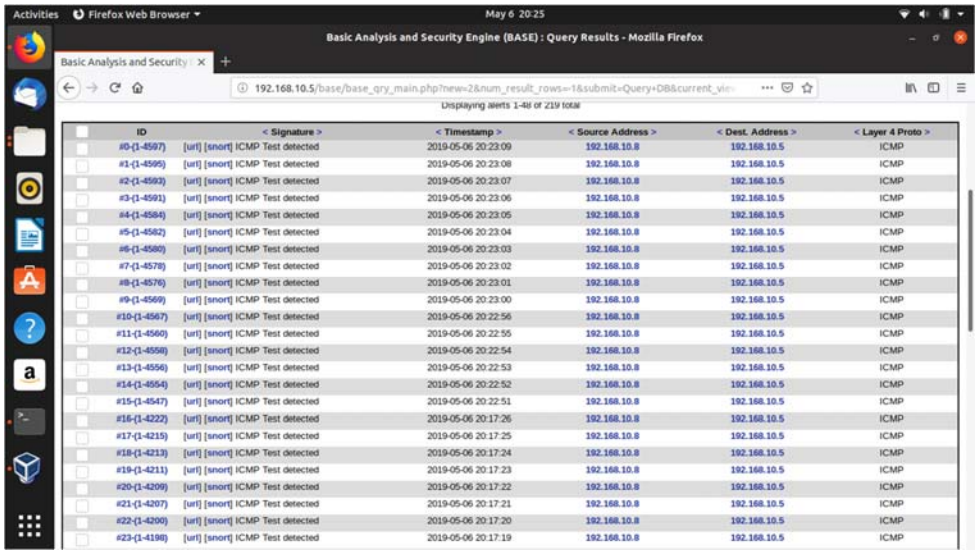
c. Setelah proses *scanning*, *Client*/Penyerang akan melakukan *telnet* ke *port* yang terbuka untuk mencoba masuk kedalam *server*.

d. Jika *Client/Penyerang* melakukan *telnet* ke *port* yang diemulasi oleh *Honeypot Artillery*, maka *Client*/Penyerang tersebut akan terkena larangan akses ke *server* dan terkena *banned*.



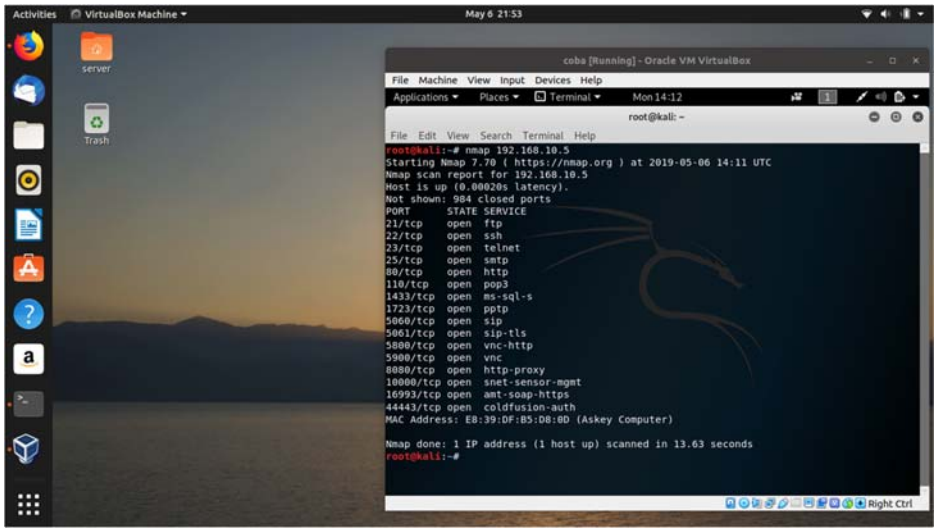

**Gambar 6** koneksi ke *server*.

Pada gambar 6 *Client*/Penyerang melakukan koneksi ke *server* berupa *test ping* pada alamat *IP server* 192.168.10.5.



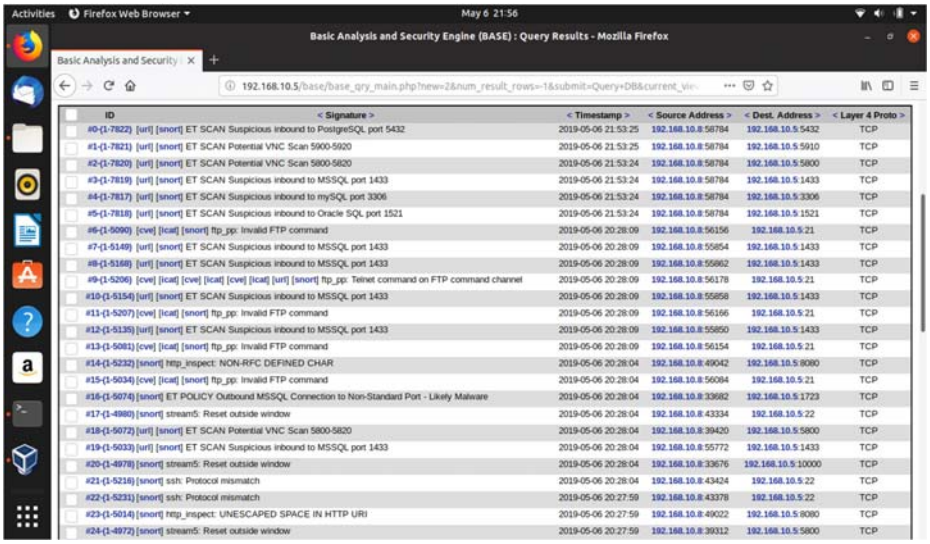

**Gambar 7** hasil *allert* pada *base snort.*

Telihat pada gambar *IP* penyerang yaitu 192.168.10.8 yang tertulis pada baris *Source Address* mencoba melakukan koneksi ke *server* dengan *IP* 192.168.10.5 yang tertulis pada baris *Dest. Address* snort lansung merespon *allert* tersebut kemudian menampilakan di *base snort*.



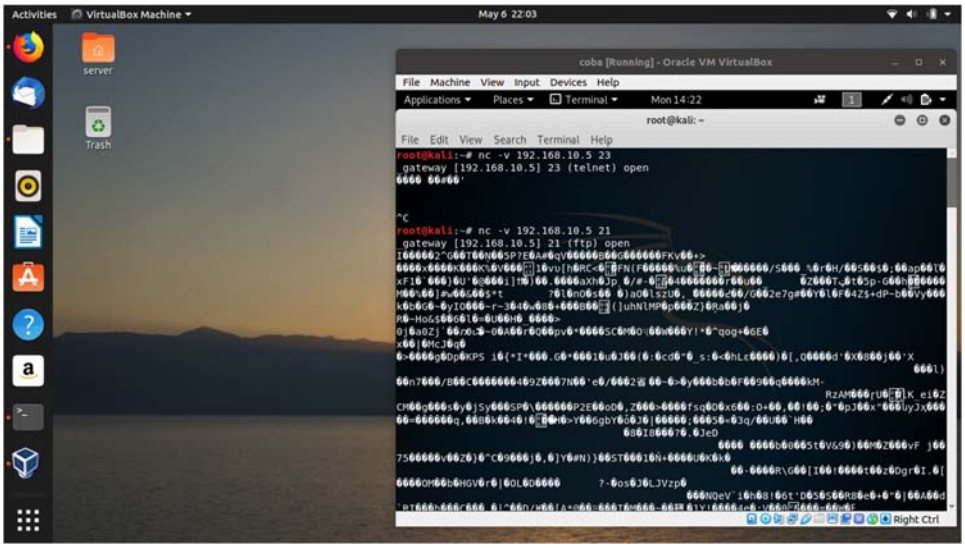

**Gambar 8** *Scanning port.*

Pada gambar 8 *User* melakukan *scanning port* menggunakan aplikasi *nmap* untuk melihat *port* yang terbuka pada *server*.



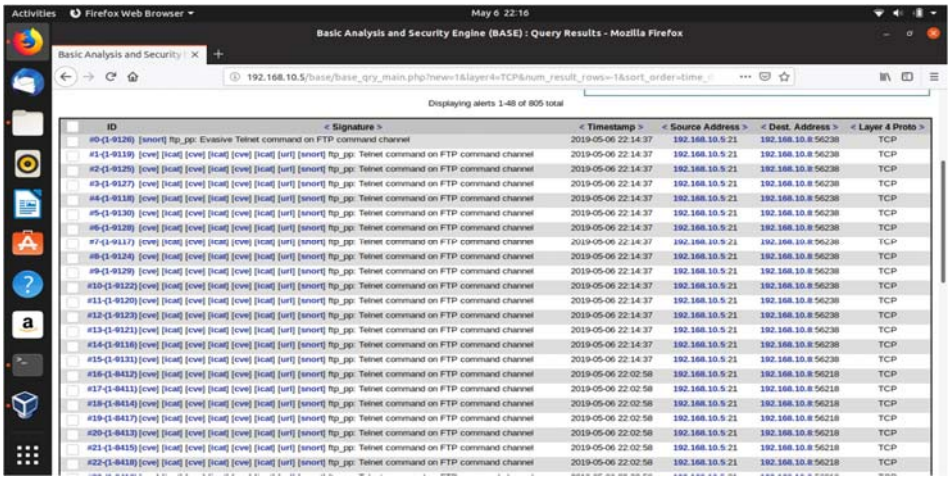

**Gambar 9** Hasil *allert Scanning port* pada *Base snort.*

Gambar 9 menjelaskan snort base menangkap lagi aktifitas allert *Scanning port* yang dilakukan oleh *Client*/Penyerang.



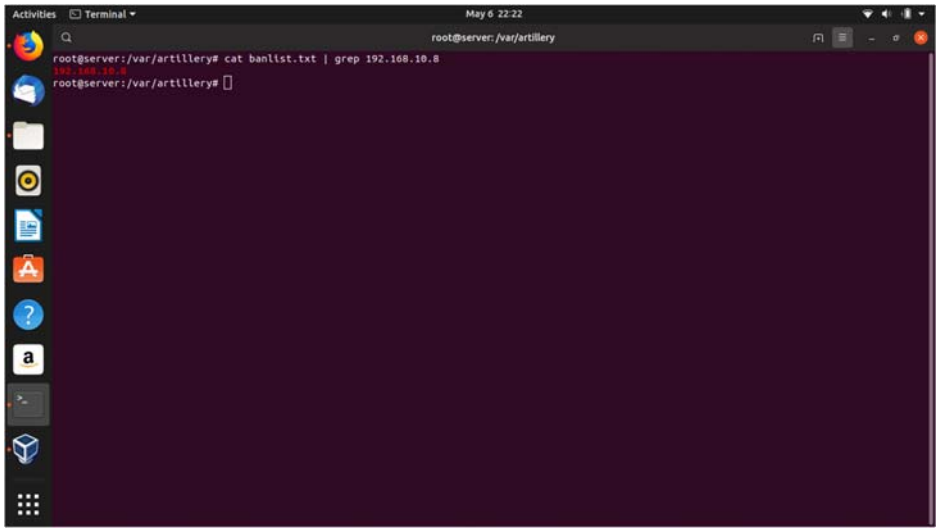

**Gambar 10** *Telnet Testing.*

*Client*/Penyerang melakukan *telnet* pada server dengan tujuan *IP* dan *port* yang terbuka dari *server*. Beberapa *port* yang terbuka merupakan *port* yang diemulasi oleh *Honeypot Artillery*, *Client*/Penyerang akan melakukan *telnet* ke dua *port* tersebut untuk menguji sistem yang telah dikonfigurasi seperti pada gambar 10.




**Gambar 11** *Base Snort* mengangkap aktifitas *telnet.*

Pada gambar 11 menjelaskan usaha *telnet client/*penyerang tetap tercatat pada *base snort*.




**Gambar 12** *IP Client/*Penyerang yang terkena *banned.*

Pada gambar 12 terlihat *IP Client*/Penyerang tercatat di *banlist Honeypot Artilery* yang membuat penyerang tidak dapat melakukan koneksi ke *server* kembali.

Mengoptimalkan sistem keamanan jaringan yang dibuat dengan memonitoring dan memperbaruhi sistem keamanan jaringan yang telah dibuat dengan cara:

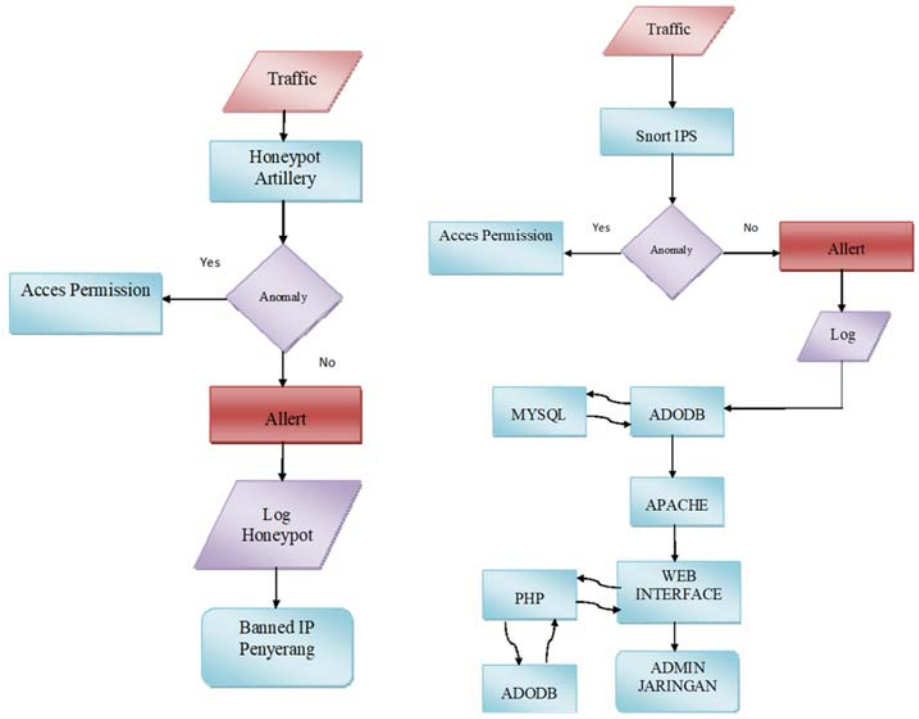
1. *Artillery* berbasis *open-source* sehingga dapat dikembangakan dengan menambahkan fungsi yang dapat disesuaikan dengan kebutuhan.

2. Melakukan *update* pada *snort* jika tersedia. Hal ini dimaksudkan agar database keamanan pada *snort* diperbaharui, sehingga jenis *malware* yang terbaru dapat dideteksi oleh *snort*.

3. Membuat akun di *website* : https://www.snort.org/ untuk mendapat notifikasi *update rules* terbaru dari *snort*.

4. Menambahkan *tools* keamanan jaringan yang kiranya bisa memperketat sistem keamanan pada jaringan.

5. Selalu melakukan *apt-get updated dan upgrade OS Ubuntu* agar sistem berjalan dengan baik dan mendapat versi sistem terbaru. Kiranya itulah beberapa cara dalam mengoptimalkan sistem keamanan jaringan yang telah dibuat, ini dimaksudkan agar sistem keamanan jaringan yang dibuat dapat mengikuti perkembangan jaman yang ada.

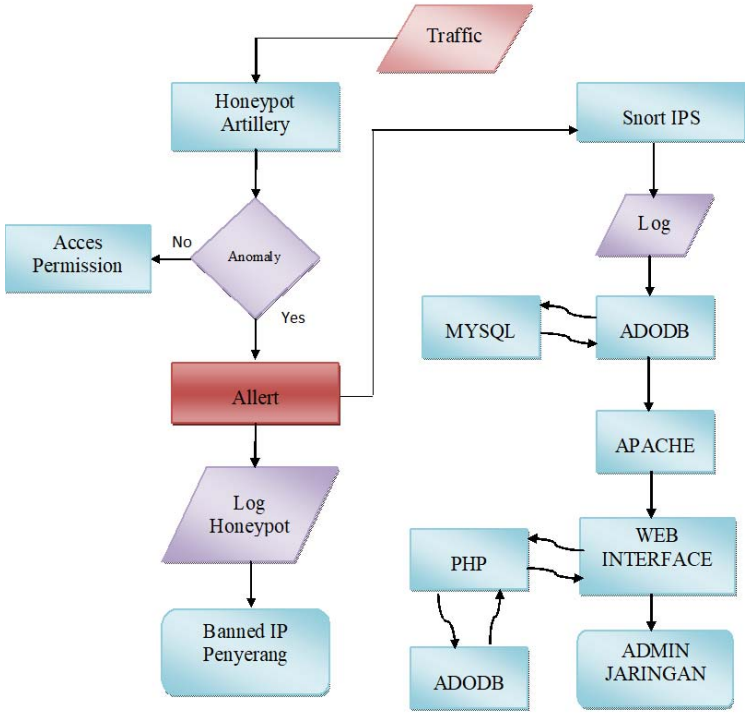



A. Diagram sistem Honeypot Artillery. B. Diagram sistem Snort IPS.

**Gambar 13** Diagram Sistem *Honeypot Artillery* dan *Snort IPS*

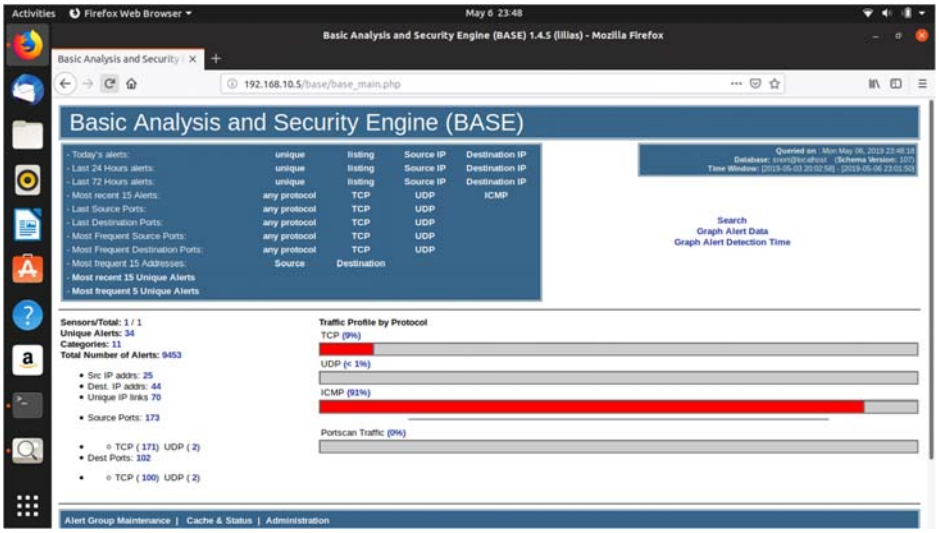
Gambar 13 menunjukan alur dari setiap sistem yang memiliki kekurangan masing-masing. *Honeypot Artillery* sendiri hanya dapat memblokir *traffic* yang masuk namun tidak dapat memberikan informasi tentang *traffic* yang masuk tersebut. Pada *snort* sendiri saat ada *traffic* yang masuk hanya memberikan

*Allert*/peringatan tanpa ada tindakan lebih lanjut pada *traffic* tersebut namun *snort* dapat memberikan informasi tentang *traffic* tersebut yang ditampilkan di *web interface*.



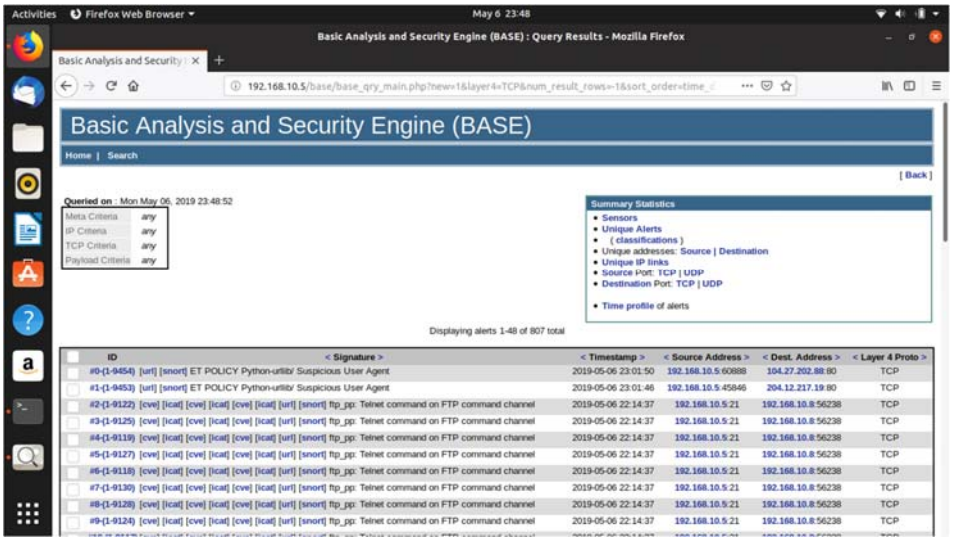

**Gambar 14** Diagram penggabungan sistem Honeypot Artillery dan Snort IPS.

Gambar 14 menjelaskan setiap *Traffic* yang masuk ke dua sistem yang telah digabungkan akan langsung direspon dengan alur sistem. Saat *trafic* masuk ke sistem *honeypot allert* akan mencatat *log* dan juga kemudian a*llert* dikirim ke *Snort IPS* untuk diproses melalui alur sistem Snort IPS kemudian akan di-*input* ke *database* namun sebelumnya *Honeypot Artillery* akan melakukan *Banned IP Client/Penyerang.*Data *allert traffic* nantinya akan ditampilkan ke *web interface* yang dapat dilihat *admin* jaringan untuk dianalisis.



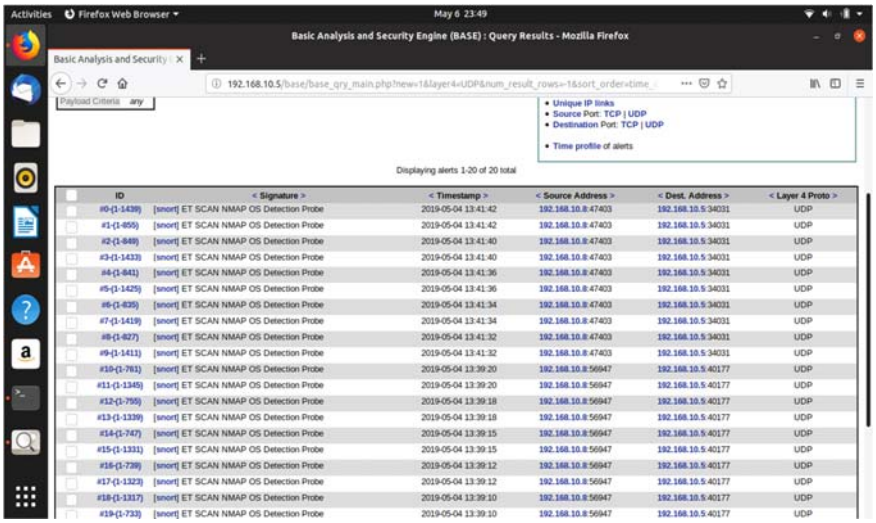

**Gambar 15** Total *Number of Allerts* sebanyak 9453.

Gambar 15 menunjukan banyaknya *Allerts* yang tercatat di *database* sebanyak 9453 pada protokol TCP sebanyak 9%, UDP sebanyak <1%, dan ICMP sebanyak 91%.



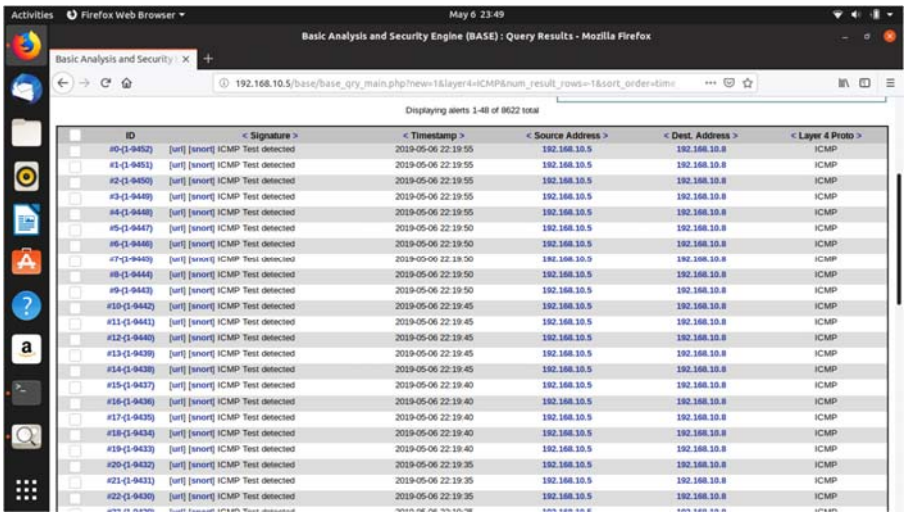

**Gambar 16** *Allert* yang tercacat pada tabel *TCP*.

Gambar 16 menunjukan semua serangan yang menggunakan protokol *TCP* dicatat di tabel ini seperti pada simulasi yang telah dilakukan dan *Allerts* yang diperoleh sebanyak 807 *Allerts.*




**Gambar 17** *Allert* yang tercacat pada tabel *UDP*.

Gambar 17 pada saat dilakukan simulasi serangan *scanning* menggunakan *NMAP Allerts* yang dihasilkan tercatat di tabel *UDP* dan total serangan pada protokol *UDP* sebanyak 20 *Allerts*.




**Gambar 18** *Allert* yang tercacat pada tabel *ICMP*.

Gambar 18 menunjukan *Allerts* pada tabel *ICMP* sebanyak 8622 karena setiap koneksi apapun ke *server* dicatat di tabel ini, seperti pada saat simulasi *test ping* ke *server* setiap koneksi dari penyerang ke *server* dicatat di kolom ini selama *Client*/Penyerang tidak memutuskan koneksi, *Allerts* pada tabel *ICMP* tidak akan berhenti mencatat *Allerts.*

**Tabel 3** Kelebihan dan Kekurangan

| Kelebihan | Kekurangan |
|---|---|
| Akurat dan cepat karena Setiap *allert* yang masuk langsung dicatat di *database* dan lansung bisa dilihat statistiknya di *BASE* page yang telah dibuat. | *Rule snort* dan konfigurasi *Honeypot Artillery* harus di-*update* atau disesuaikan apabila ada pola serangan baru, kemampuan untuk pengamanan tergantung pada *rule*/aturan yang digunakan. |
| Dapat mengidentifiksi serangan dan menyimpannya sebagai pola. | Membutuhkan lebih banyak *resource* untuk menganalisa aktivitas. |

## 5. Simpulan

Berdasarkan penelitian Simulasi Sistem Keamanan Jaringan penggabungan antara *Snort IPS* dengan sistem *allerts*-nya yang responsif dalam menangkap gangguan pada sistem *Allerts* yang tercatat di *database* sebanyak 9453 yang tediri pada *Traffic Profile* yaitu pada protokol TCP sebanyak 9%, UDP sebanyak <1%, dan ICMP sebanyak 91% dan *Honeypot Artillery* yang dapat mendeteksi 1 alamat IP (192.168.10.8) dari mesin virtual box yang dibuat dan melakukan *Block IP* tersebut sebelum memiliki kesempatan lagi untuk menyerang keseluruhan sistem.Sebelum dipasang *Honeypot Artillery dan Snort IPS* pada *server* tidak ada laporan atau data mengenai jenis koneksi apa saja dan dari mana saja koneksi tersebut berasal tanpa adanya proteksi lebih yang membuat tidak amanya *server*, dengan ini *Honeypot Artillery dan Snort IPS* dirasa cukup untuk mengamankan dan menganalisis pola serangan *attackers* yang ingin melakukan intrusi ke sistem jaringan komputer dan dengan memperhatikan kekurangan yang ada dapat membuat penggabungan dua sistem keamanan ini menjadi lebih baik lagi.

Adapun saran dalam penelitain ini yaitu bila diterapkan pada keamanan jaringan dapat ditingkatkan dengan menambahkan *local rules* pada *snort* sesuai dengan kebutuhan yang dibutuhkan dan mengupdate *rule* yang berasal dari *website* resmi *snort*.Meningkatkan performa *Server* dengan melakukan *upgrade hardware*.Dengan *Honeypot Artillery* berbasis *open-source* sehingga memudahkan *Admin* suatu jaringan untuk mengembangkan dengan menambahkan fungsi yang lebih baik lagi.

## Daftar Pustaka

[1] BSSN.(2019,2 Februari).Langkah BSSN dalam melakukan deteksi ancaman siber , https://bssn.go.id/wp-content/uploads/2019/02/Rilis-Forum-Cyber-Corner-Launching-Honeynet-Project-Revisi.pdf.

[2] B. . Octavian, Rancang Bangun *Sort Base IPS*. 2015.

[3] T. A. Cahyanto, H. Oktavianto, and A. W. Royan, "Analisis Dan Implementasi Honeypot Menggunakan Dionaea Sebagai Penunjang Keamanan Jaringan," *J. Sist. Teknol. Inf. Indones.*, vol. 1, pp. 86–92, 2016.

[4] D. Ariyus, *Internet Firewall*. Yogyakarta: Graha Ilmu, 2006.

[5] P. L. Restanti, "Analisis Kolaborasi IDS Snort dan Honeypot," pp. 1–27, 2014.

[6] F. Utdirartatmo, Trik Menjebak *Hacker* Dengan *Honeypot*. Yogyakarta: Andi, 2005.

[7] A. S. Nugroho, "Analisis Dan Implementasi Honeypot Menggunakan Honeyd Sebagai Alat Bantu Pengumpulan Informasi Aktivitas Serangan Pada Jaringan," *Inst. Sains Teknol. AKPRIND*, 2013.

[8] Palcomtech.(2013,23 Desember). Metode Perancangan Jaringan dengan Model PPDIOO. http://www.news.palcomtech.com/metode perancangan jaringan-dengan-model-ppdioo/