

Simulasi Sistem Keamanan Jaringan Komputer Berbasis IPS *Snort dan HoneyPot Artillery*

Alja Aminanto¹, Wiwin Sulisty²

^{1,2}Fakultas Teknologi Informasi Universitas Kristen Satya Wacana
Jl. Dr. O. Notohamidjojo 1-10, Salatiga 50711, Indonesia
Email : ¹672015235@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 kewanaman 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 menggunakan 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 keamanan *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. Tinjauan 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 penelitian 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].

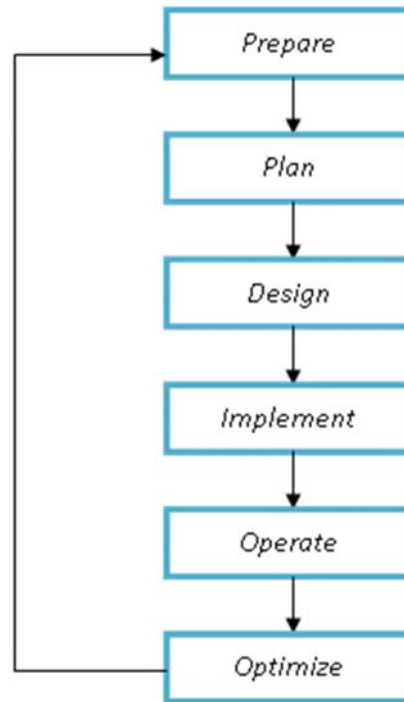
Intrusion Prevention System (IPS), adalah pendekatan yang sering digunakan untuk membangun sistem keamanan komputer. IPS mengkombinasikan teknik firewall dan metode Intrusion Detection System (IDS) dengan sangat baik. Teknologi ini dapat digunakan untuk mencegah serangan yang masuk ke jaringan lokal dengan memeriksa dan mencatat semua paket data serta mengenali paket dengan sensor, di saat serangan telah teridentifikasi, IPS menolak akses (block) dan mencatat (logging) semua paket data yang teridentifikasi tersebut. Jadi IPS bertindak seperti 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 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 referensi yang telah dikumpulkan untuk mengetahui 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.

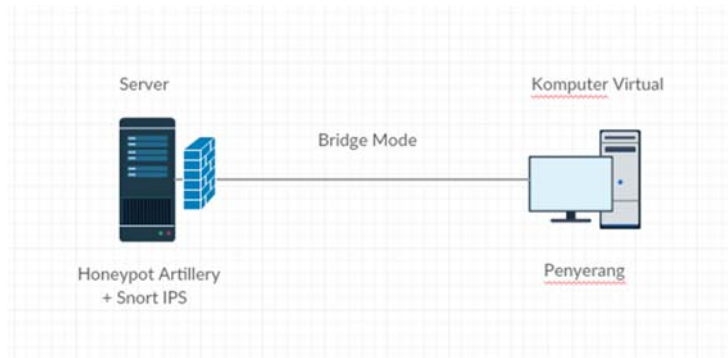
Tabel 1 berisi pemetaan *Software* atau perangkat lunak yang dibutuhkan untuk membangun sistem sebagai berikut :

Tabel 1 Pemetaan perangkat lunak

No	Jenis	Versi	Keterangan
1	Ubuntu server	19.04	Sebagai OS server
2	Snort	2.9.14	Untuk mencatat Alerts 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 Rancangan Topologi Jaringan

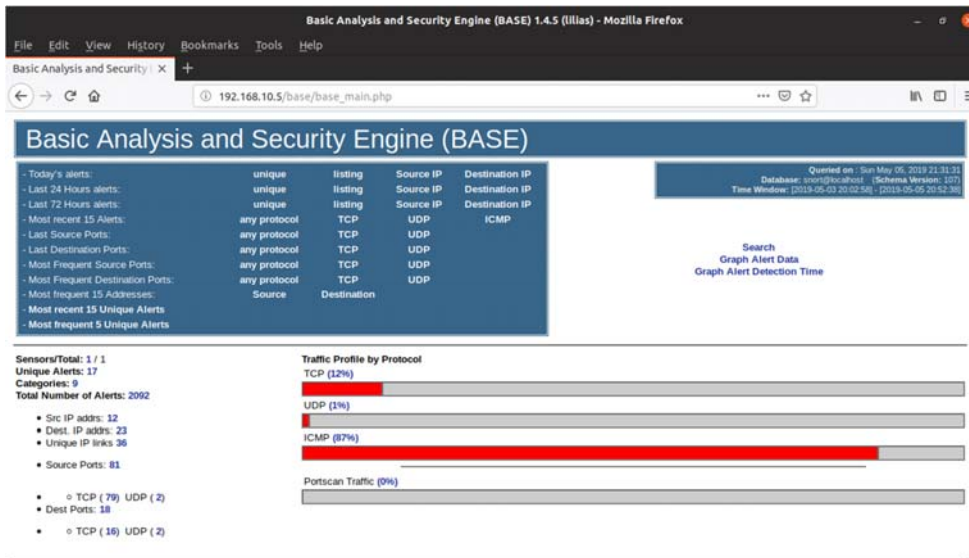
Dalam pembuatan proyek akhir ini penulis menggunakan 1 buah laptop sebagai *server* dan software *Virtual Box* untuk komputer virtual yang digunakan sebagai *client*/penyerang, untuk penghubung antara *server* dan penyerang menggunakan mode *Bridge*. Server dikonfigurasi menggunakan Artillery dan Snort 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 Artillery*" terbagi menjadi dua bagian, yaitu implementasi instalasi sistem keamanan *HoneyPot Artillery* dan *Snort IPS*.



Gambar 4 tampilan Base Snort

Pada gambar 4 menunjukkan 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* menunjukan statistik serangan apa saja yang masuk di *server*.

```

root@server:~# netstat -ntpl | grep python
tcp        0      0 0.0.0.0:5900        0.0.0.0:*        LISTEN    831/python
tcp        0      0 0.0.0.0:110        0.0.0.0:*        LISTEN    831/python
tcp        0      0 0.0.0.0:8080       0.0.0.0:*        LISTEN    831/python
tcp        0      0 0.0.0.0:10000      0.0.0.0:*        LISTEN    831/python
tcp        0      0 0.0.0.0:21        0.0.0.0:*        LISTEN    831/python
tcp        0      0 0.0.0.0:22        0.0.0.0:*        LISTEN    831/python
tcp        0      0 0.0.0.0:1433       0.0.0.0:*        LISTEN    831/python
tcp        0      0 0.0.0.0:25        0.0.0.0:*        LISTEN    831/python
tcp        0      0 0.0.0.0:1337       0.0.0.0:*        LISTEN    831/python
tcp        0      0 0.0.0.0:44443      0.0.0.0:*        LISTEN    831/python
tcp        0      0 0.0.0.0:1723       0.0.0.0:*        LISTEN    831/python
tcp        0      0 0.0.0.0:16993      0.0.0.0:*        LISTEN    831/python
tcp        0      0 0.0.0.0:5060       0.0.0.0:*        LISTEN    831/python
tcp        0      0 0.0.0.0:5061       0.0.0.0:*        LISTEN    831/python
tcp        0      0 0.0.0.0:5800       0.0.0.0:*        LISTEN    831/python

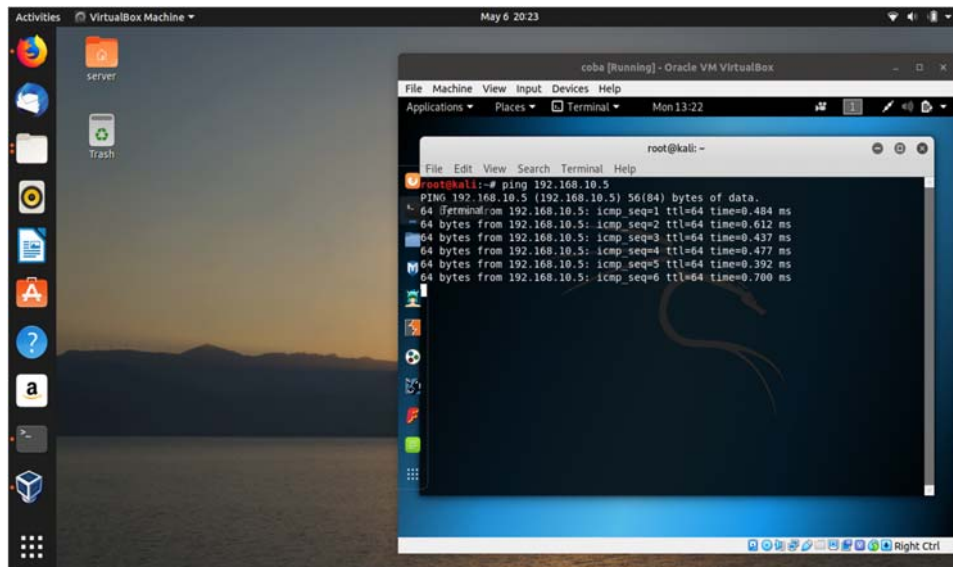
```

Gambar 5 port yang telah dikonfigurasi.

Gambar 5 menunjukkan 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 *setting*.

Skenario Fase *Operate* (Operasional) pengujian untuk Tugas Akhir "Simulasi Sistem Keamanan Jaringan Komputer Berbasis IPS *Snort* dan *Honeypot Artillery*" 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.

ID	Signature	Timestamp	Source Address	Dest. Address	Layer 4 Proto
#0-(1-4597)	[url] [snort] ICMP Test detected	2019-05-06 20:23:09	192.168.10.8	192.168.10.5	ICMP
#1-(1-4595)	[url] [snort] ICMP Test detected	2019-05-06 20:23:08	192.168.10.8	192.168.10.5	ICMP
#2-(1-4593)	[url] [snort] ICMP Test detected	2019-05-06 20:23:07	192.168.10.8	192.168.10.5	ICMP
#3-(1-4591)	[url] [snort] ICMP Test detected	2019-05-06 20:23:06	192.168.10.8	192.168.10.5	ICMP
#4-(1-4589)	[url] [snort] ICMP Test detected	2019-05-06 20:23:05	192.168.10.8	192.168.10.5	ICMP
#5-(1-4587)	[url] [snort] ICMP Test detected	2019-05-06 20:23:04	192.168.10.8	192.168.10.5	ICMP
#6-(1-4586)	[url] [snort] ICMP Test detected	2019-05-06 20:23:03	192.168.10.8	192.168.10.5	ICMP
#7-(1-4578)	[url] [snort] ICMP Test detected	2019-05-06 20:23:02	192.168.10.8	192.168.10.5	ICMP
#8-(1-4576)	[url] [snort] ICMP Test detected	2019-05-06 20:23:01	192.168.10.8	192.168.10.5	ICMP
#9-(1-4569)	[url] [snort] ICMP Test detected	2019-05-06 20:23:00	192.168.10.8	192.168.10.5	ICMP
#10-(1-4567)	[url] [snort] ICMP Test detected	2019-05-06 20:22:59	192.168.10.8	192.168.10.5	ICMP
#11-(1-4560)	[url] [snort] ICMP Test detected	2019-05-06 20:22:55	192.168.10.8	192.168.10.5	ICMP
#12-(1-4558)	[url] [snort] ICMP Test detected	2019-05-06 20:22:54	192.168.10.8	192.168.10.5	ICMP
#13-(1-4556)	[url] [snort] ICMP Test detected	2019-05-06 20:22:53	192.168.10.8	192.168.10.5	ICMP
#14-(1-4054)	[url] [snort] ICMP Test detected	2019-05-06 20:22:52	192.168.10.8	192.168.10.5	ICMP
#15-(1-4547)	[url] [snort] ICMP Test detected	2019-05-06 20:22:51	192.168.10.8	192.168.10.5	ICMP
#16-(1-4222)	[url] [snort] ICMP Test detected	2019-05-06 20:17:26	192.168.10.8	192.168.10.5	ICMP
#17-(1-4215)	[url] [snort] ICMP Test detected	2019-05-06 20:17:25	192.168.10.8	192.168.10.5	ICMP
#18-(1-4213)	[url] [snort] ICMP Test detected	2019-05-06 20:17:24	192.168.10.8	192.168.10.5	ICMP
#19-(1-4211)	[url] [snort] ICMP Test detected	2019-05-06 20:17:23	192.168.10.8	192.168.10.5	ICMP
#20-(1-4209)	[url] [snort] ICMP Test detected	2019-05-06 20:17:22	192.168.10.8	192.168.10.5	ICMP
#21-(1-4207)	[url] [snort] ICMP Test detected	2019-05-06 20:17:21	192.168.10.8	192.168.10.5	ICMP
#22-(1-4206)	[url] [snort] ICMP Test detected	2019-05-06 20:17:20	192.168.10.8	192.168.10.5	ICMP
#23-(1-4198)	[url] [snort] ICMP Test detected	2019-05-06 20:17:19	192.168.10.8	192.168.10.5	ICMP

Gambar 7 hasil alert 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 langsung merespon alert tersebut kemudian menampilkan di base snort.

```

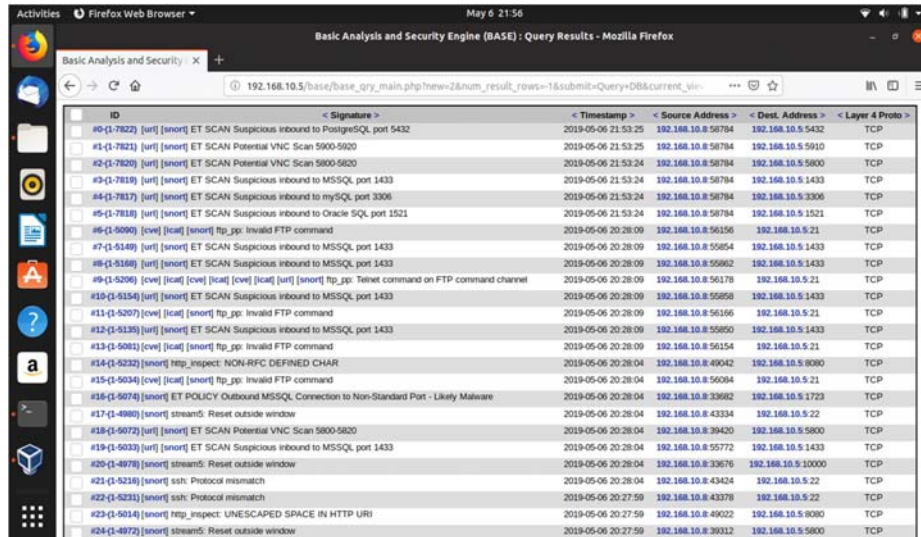
root@kali:~# nmap 192.168.10.5
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-06 14:11 UTC
Nmap scan report for 192.168.10.5
Host is up (0.00020s latency).
Not shown: 894 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
1433/tcp  open  ms-sql-s
1723/tcp  open  ppp
5060/tcp  open  sip
5061/tcp  open  sip-tls
5800/tcp  open  vnc-http
5900/tcp  open  vnc
8888/tcp  open  http-proxy
10000/tcp open  snet-sensor-mgmt
16993/tcp open  smt-smap-https
44443/tcp open  coldfusion-auth
MAC Address: EB:39:DF:85:D8:0D (Askey Computer)

Nmap done: 1 IP address (1 host up) scanned in 13.03 seconds
root@kali:~#

```

Gambar 8 Scanning port.

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

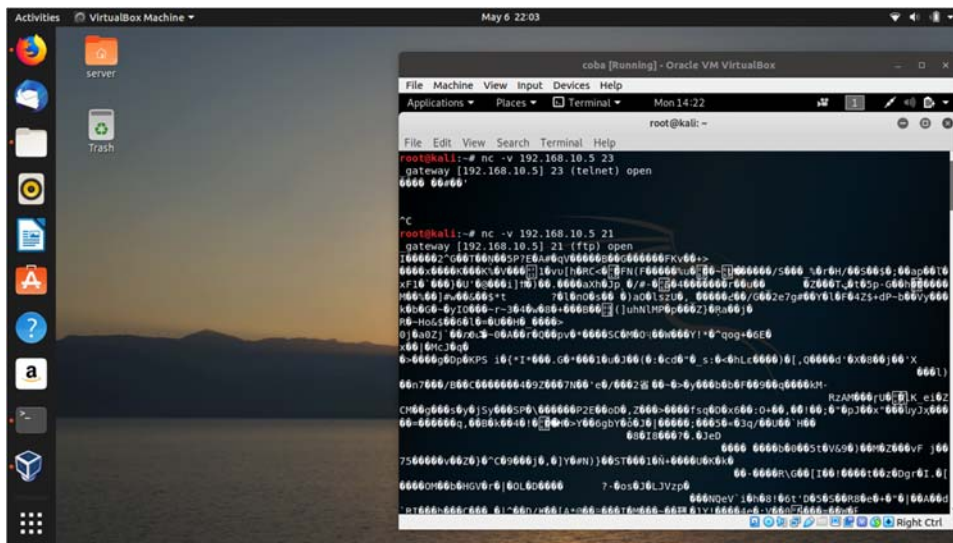


The image shows a screenshot of the Basic Analysis and Security Engine (BASE) interface in Mozilla Firefox. The browser address bar shows the URL: 192.168.10.5/base_gry_main.php?new2&num_result_rows=1&submit=Query+DB¤t_vin. The main window displays a table of snort alert results with the following columns: ID, Signature, Timestamp, Source Address, Dest. Address, and Layer 4 Proto. The table contains 24 rows of alerts, including signatures like 'ET SCAN Suspicious inbound to PostgreSQL port 5432', 'ET SCAN Potential VNC Scan 5900-5920', 'ET SCAN Suspicious inbound to MSSQL port 1433', 'ET SCAN Suspicious inbound to MySQL port 3306', 'ET SCAN Suspicious inbound to Oracle SQL port 1521', 'Invalid FTP command', 'Telnet command on FTP command channel', 'NON-RFC DEFINED CHAR', 'POLICY Outbound MSSQL Connection to Non-Standard Port - Likely Malware', 'Reset outside window', and 'SSH: Protocol mismatch'.

ID	Signature	Timestamp	Source Address	Dest. Address	Layer 4 Proto
#0-(1-7822)	[url] [snort] ET SCAN Suspicious inbound to PostgreSQL port 5432	2019-05-06 21:53:25	192.168.10.8:58784	192.168.10.5:5432	TCP
#1-(1-7821)	[url] [snort] ET SCAN Potential VNC Scan 5900-5920	2019-05-06 21:53:25	192.168.10.8:58784	192.168.10.5:5910	TCP
#2-(1-7820)	[url] [snort] ET SCAN Potential VNC Scan 5900-5920	2019-05-06 21:53:24	192.168.10.8:58784	192.168.10.5:5900	TCP
#3-(1-7819)	[url] [snort] ET SCAN Suspicious inbound to MSSQL port 1433	2019-05-06 21:53:24	192.168.10.8:58784	192.168.10.5:1433	TCP
#4-(1-7817)	[url] [snort] ET SCAN Suspicious inbound to MySQL port 3306	2019-05-06 21:53:24	192.168.10.8:58784	192.168.10.5:3306	TCP
#5-(1-7818)	[url] [snort] ET SCAN Suspicious inbound to Oracle SQL port 1521	2019-05-06 21:53:24	192.168.10.8:58784	192.168.10.5:1521	TCP
#6-(1-9090)	[cve] [icaf] [snort] ftp_gp: Invalid FTP command	2019-05-06 20:28:09	192.168.10.8:56156	192.168.10.5:21	TCP
#7-(1-9149)	[url] [snort] ET SCAN Suspicious inbound to MSSQL port 1433	2019-05-06 20:28:09	192.168.10.8:55954	192.168.10.5:1433	TCP
#8-(1-9148)	[url] [snort] ET SCAN Suspicious inbound to MSSQL port 1433	2019-05-06 20:28:09	192.168.10.8:55962	192.168.10.5:1433	TCP
#9-(1-9209)	[cve] [icaf] [cve] [icaf] [url] [snort] ftp_gp: Telnet command on FTP command channel	2019-05-06 20:28:09	192.168.10.8:56178	192.168.10.5:21	TCP
#10-(1-9154)	[url] [snort] ET SCAN Suspicious inbound to MSSQL port 1433	2019-05-06 20:28:09	192.168.10.8:55958	192.168.10.5:1433	TCP
#11-(1-9207)	[cve] [icaf] [snort] ftp_gp: Invalid FTP command	2019-05-06 20:28:09	192.168.10.8:56166	192.168.10.5:21	TCP
#12-(1-9135)	[url] [snort] ET SCAN Suspicious inbound to MSSQL port 1433	2019-05-06 20:28:09	192.168.10.8:55950	192.168.10.5:1433	TCP
#13-(1-9281)	[cve] [icaf] [snort] ftp_gp: Invalid FTP command	2019-05-06 20:28:09	192.168.10.8:56154	192.168.10.5:21	TCP
#14-(1-9232)	[snort] http_inspect: NON-RFC DEFINED CHAR	2019-05-06 20:28:04	192.168.10.8:49042	192.168.10.5:8080	TCP
#15-(1-9034)	[cve] [icaf] [snort] ftp_gp: Invalid FTP command	2019-05-06 20:28:04	192.168.10.8:56084	192.168.10.5:21	TCP
#16-(1-9074)	[snort] ET POLICY Outbound MSSQL Connection to Non-Standard Port - Likely Malware	2019-05-06 20:28:04	192.168.10.8:33682	192.168.10.5:1723	TCP
#17-(1-4980)	[snort] stream5: Reset outside window	2019-05-06 20:28:04	192.168.10.8:43334	192.168.10.5:22	TCP
#18-(1-9072)	[url] [snort] ET SCAN Potential VNC Scan 5900-5920	2019-05-06 20:28:04	192.168.10.8:39420	192.168.10.5:5900	TCP
#19-(1-9033)	[url] [snort] ET SCAN Suspicious inbound to MSSQL port 1433	2019-05-06 20:28:04	192.168.10.8:55772	192.168.10.5:1433	TCP
#20-(1-4978)	[snort] stream5: Reset outside window	2019-05-06 20:28:04	192.168.10.8:33676	192.168.10.5:10000	TCP
#21-(1-9214)	[snort] ssh: Protocol mismatch	2019-05-06 20:28:04	192.168.10.8:43424	192.168.10.5:22	TCP
#22-(1-9231)	[snort] ssh: Protocol mismatch	2019-05-06 20:27:59	192.168.10.8:43378	192.168.10.5:22	TCP
#23-(1-9014)	[snort] http_inspect: UNESCAPED SPACE IN HTTP URI	2019-05-06 20:27:59	192.168.10.8:49022	192.168.10.5:8080	TCP
#24-(1-4972)	[snort] stream5: Reset outside window	2019-05-06 20:27:59	192.168.10.8:30312	192.168.10.5:5800	TCP

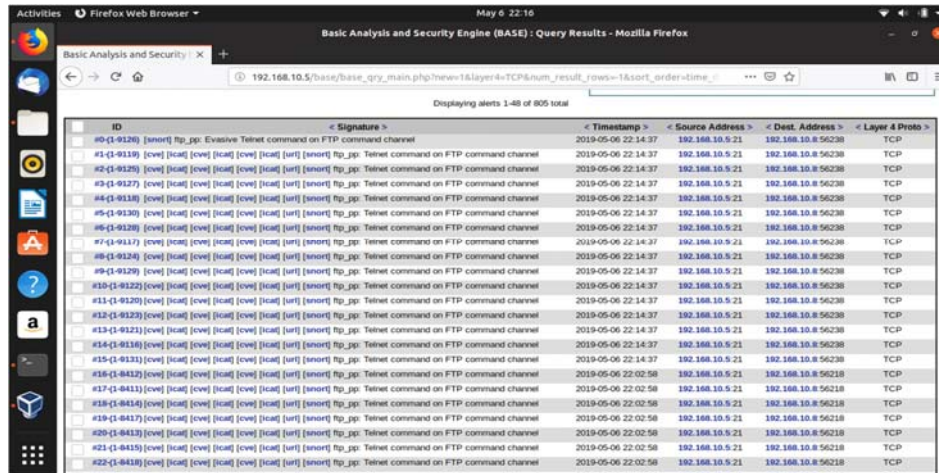
Gambar 9 Hasil alert Scanning port pada Base snort.

Gambar 9 menjelaskan snort base menangkap lagi aktifitas alert 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.

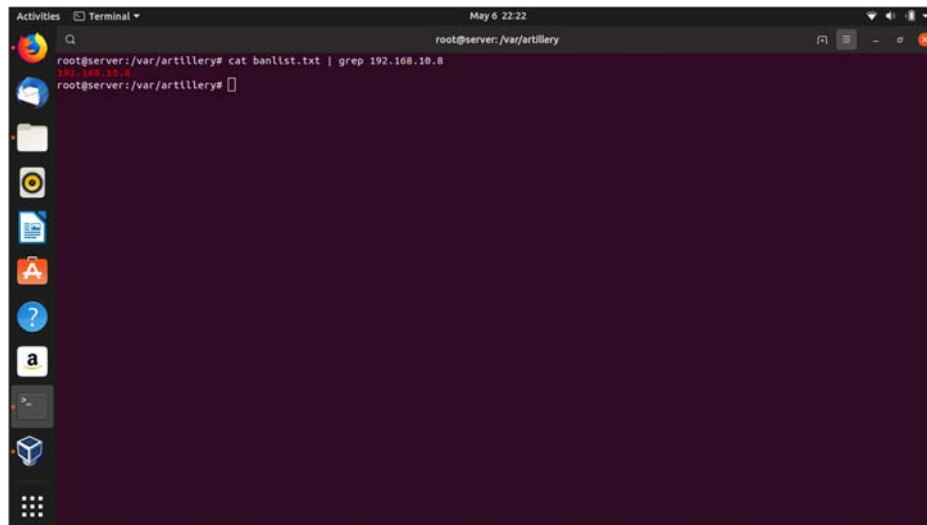


Displaying alerts 1-48 of 805 total

ID	Signature	Timestamp	Source Address	Dest. Address	Layer 4 Proto
#5-(1-9126)	[snort] ftp_sp: Evasive Telnet command on FTP command channel	2019-05-06 22:14:37	192.168.10.5/21	192.168.10.8/56238	TCP
#5-(1-9129)	[snort] [icmp] [icmp] [icmp] [icmp] [icmp] [snort] ftp_sp: Telnet command on FTP command channel	2019-05-06 22:14:37	192.168.10.5/21	192.168.10.8/56238	TCP
#5-(1-9128)	[snort] [icmp] [icmp] [icmp] [icmp] [icmp] [snort] ftp_sp: Telnet command on FTP command channel	2019-05-06 22:14:37	192.168.10.5/21	192.168.10.8/56238	TCP
#5-(1-9127)	[snort] [icmp] [icmp] [icmp] [icmp] [icmp] [snort] ftp_sp: Telnet command on FTP command channel	2019-05-06 22:14:37	192.168.10.5/21	192.168.10.8/56238	TCP
#5-(1-9118)	[snort] [icmp] [icmp] [icmp] [icmp] [icmp] [snort] ftp_sp: Telnet command on FTP command channel	2019-05-06 22:14:37	192.168.10.5/21	192.168.10.8/56238	TCP
#5-(1-9130)	[snort] [icmp] [icmp] [icmp] [icmp] [icmp] [snort] ftp_sp: Telnet command on FTP command channel	2019-05-06 22:14:37	192.168.10.5/21	192.168.10.8/56238	TCP
#5-(1-9128)	[snort] [icmp] [icmp] [icmp] [icmp] [icmp] [snort] ftp_sp: Telnet command on FTP command channel	2019-05-06 22:14:37	192.168.10.5/21	192.168.10.8/56238	TCP
#7-(1-9417)	[snort] [icmp] [icmp] [icmp] [icmp] [icmp] [snort] ftp_sp: Telnet command on FTP command channel	2019-05-06 22:14:37	192.168.10.5/21	192.168.10.8/56238	TCP
#9-(1-9124)	[snort] [icmp] [icmp] [icmp] [icmp] [icmp] [snort] ftp_sp: Telnet command on FTP command channel	2019-05-06 22:14:37	192.168.10.5/21	192.168.10.8/56238	TCP
#9-(1-9129)	[snort] [icmp] [icmp] [icmp] [icmp] [icmp] [snort] ftp_sp: Telnet command on FTP command channel	2019-05-06 22:14:37	192.168.10.5/21	192.168.10.8/56238	TCP
#10-(1-9122)	[snort] [icmp] [icmp] [icmp] [icmp] [icmp] [snort] ftp_sp: Telnet command on FTP command channel	2019-05-06 22:14:37	192.168.10.5/21	192.168.10.8/56238	TCP
#11-(1-9120)	[snort] [icmp] [icmp] [icmp] [icmp] [icmp] [snort] ftp_sp: Telnet command on FTP command channel	2019-05-06 22:14:37	192.168.10.5/21	192.168.10.8/56238	TCP
#12-(1-9123)	[snort] [icmp] [icmp] [icmp] [icmp] [icmp] [snort] ftp_sp: Telnet command on FTP command channel	2019-05-06 22:14:37	192.168.10.5/21	192.168.10.8/56238	TCP
#13-(1-9121)	[snort] [icmp] [icmp] [icmp] [icmp] [icmp] [snort] ftp_sp: Telnet command on FTP command channel	2019-05-06 22:14:37	192.168.10.5/21	192.168.10.8/56238	TCP
#14-(1-9116)	[snort] [icmp] [icmp] [icmp] [icmp] [icmp] [snort] ftp_sp: Telnet command on FTP command channel	2019-05-06 22:14:37	192.168.10.5/21	192.168.10.8/56238	TCP
#15-(1-9113)	[snort] [icmp] [icmp] [icmp] [icmp] [icmp] [snort] ftp_sp: Telnet command on FTP command channel	2019-05-06 22:14:37	192.168.10.5/21	192.168.10.8/56238	TCP
#16-(1-9412)	[snort] [icmp] [icmp] [icmp] [icmp] [icmp] [snort] ftp_sp: Telnet command on FTP command channel	2019-05-06 22:02:58	192.168.10.5/21	192.168.10.8/56218	TCP
#17-(1-9411)	[snort] [icmp] [icmp] [icmp] [icmp] [icmp] [snort] ftp_sp: Telnet command on FTP command channel	2019-05-06 22:02:58	192.168.10.5/21	192.168.10.8/56218	TCP
#18-(1-9414)	[snort] [icmp] [icmp] [icmp] [icmp] [icmp] [snort] ftp_sp: Telnet command on FTP command channel	2019-05-06 22:02:58	192.168.10.5/21	192.168.10.8/56218	TCP
#19-(1-9417)	[snort] [icmp] [icmp] [icmp] [icmp] [icmp] [snort] ftp_sp: Telnet command on FTP command channel	2019-05-06 22:02:58	192.168.10.5/21	192.168.10.8/56218	TCP
#20-(1-9413)	[snort] [icmp] [icmp] [icmp] [icmp] [icmp] [snort] ftp_sp: Telnet command on FTP command channel	2019-05-06 22:02:58	192.168.10.5/21	192.168.10.8/56218	TCP
#21-(1-9415)	[snort] [icmp] [icmp] [icmp] [icmp] [icmp] [snort] ftp_sp: Telnet command on FTP command channel	2019-05-06 22:02:58	192.168.10.5/21	192.168.10.8/56218	TCP
#22-(1-9418)	[snort] [icmp] [icmp] [icmp] [icmp] [icmp] [snort] ftp_sp: Telnet command on FTP command channel	2019-05-06 22:02:58	192.168.10.5/21	192.168.10.8/56218	TCP

Gambar 11 Base Snort menangkap aktifitas telnet.

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



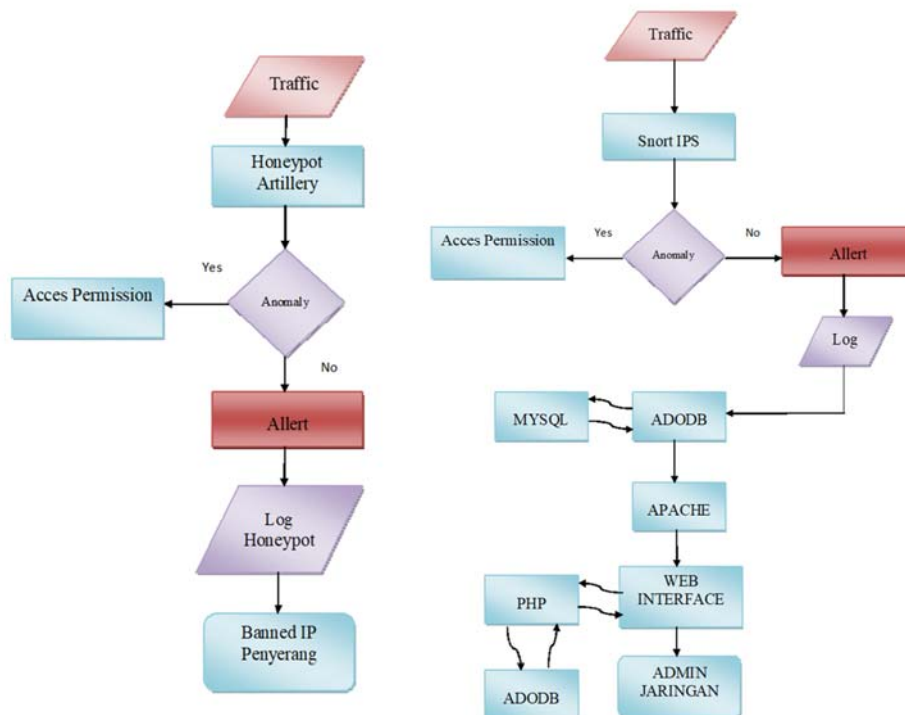
Gambar 12 IP Client/Penyerang yang terkena *banned*.

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

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

1. *Artillery* berbasis *open-source* sehingga dapat dikembangkan 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.



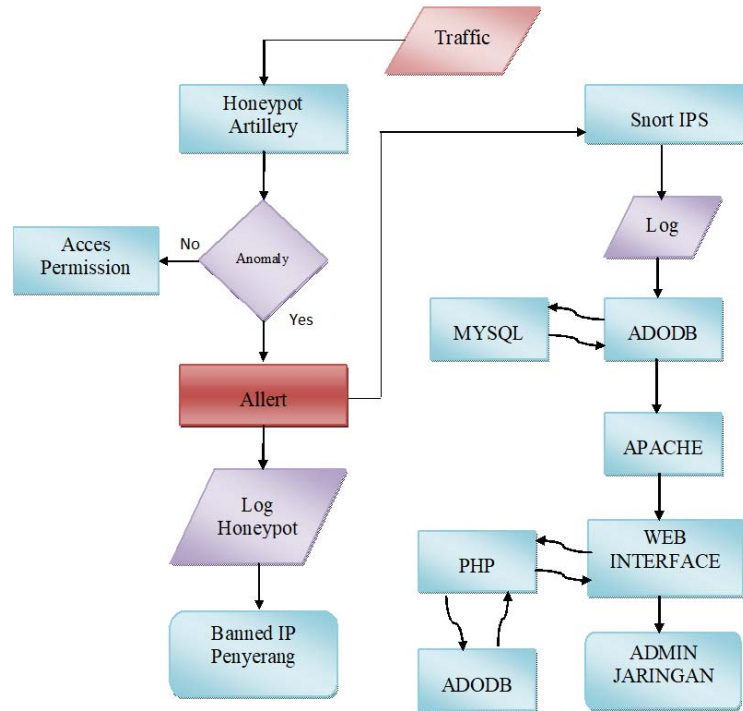
A. Diagram sistem HoneyPot Artillery.

B. Diagram sistem Snort IPS.

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

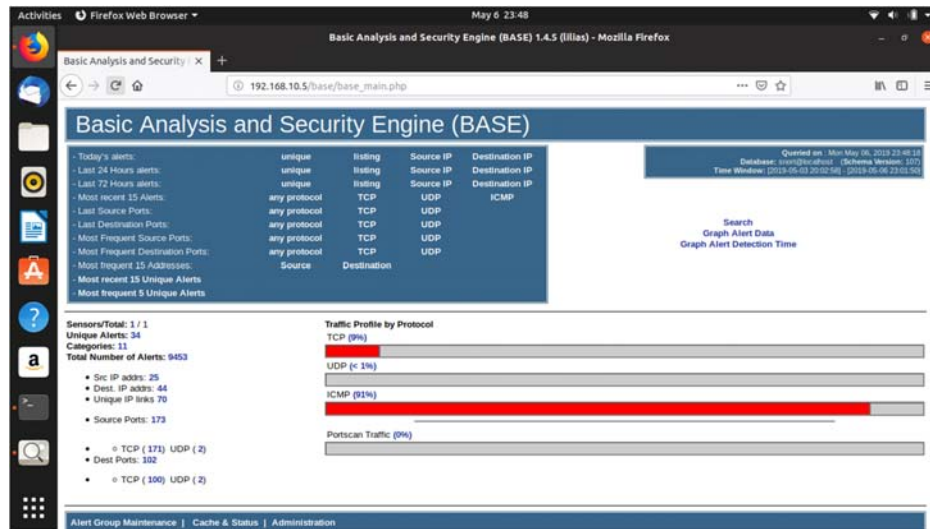
Gambar 13 menunjukkan alur dari setiap sistem yang memiliki kekurangan masing-masing. *HoneyPot Artillery* sendiri hanya dapat memblokir *traffic* yang masuk namun tidak dapat memberikan informasi tentang *traffic* yang masuk tersebut. Pada *snort* sendiri saat ada *traffic* yang masuk hanya memberikan

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



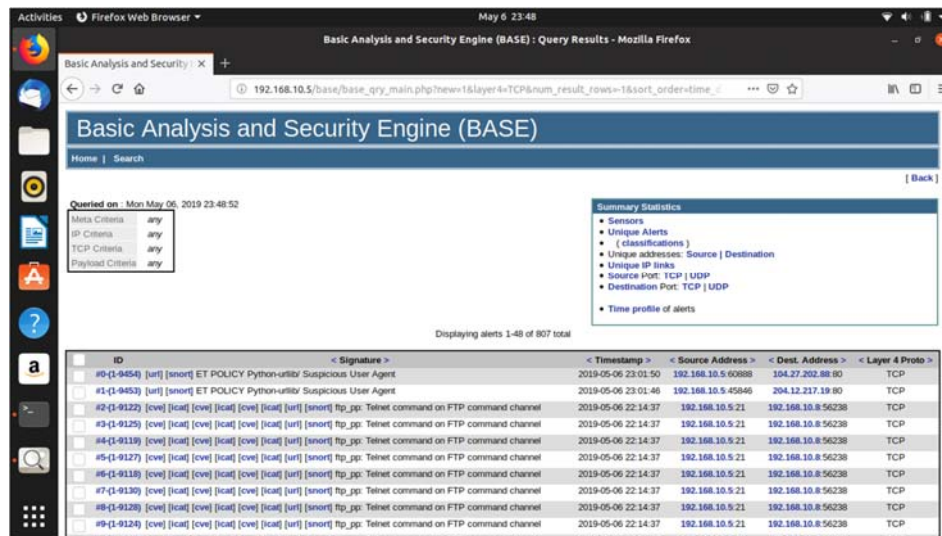
Gambar 14 Diagram penggabungan sistem Honeypot Artillery dan Snort IPS.

Gambar 14 menjelaskan setiap *Traffic* yang masuk ke dua sistem yang telah digabungkan akan langsung direpson dengan alur sistem. Saat *traffic* masuk ke sistem *honeypot alert* akan mencatat *log* dan juga kemudian *alert* 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 *alert traffic* nantinya akan ditampilkan ke *web interface* yang dapat dilihat *admin jaringan* untuk dianalisis.



Gambar 15 Total Number of Alerts sebanyak 9453.

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



Gambar 16 Alert yang tercatat pada tabel TCP.

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

ID	Signature	Timestamp	Source Address	Dest. Address	Layer 4 Proto
#0-(1-1438)	[anort] ET SCAN NMAP OS Detection Probe	2019-05-04 13:41:42	192.168.10.8-47403	192.168.10.5-34031	UDP
#1-(1-855)	[anort] ET SCAN NMAP OS Detection Probe	2019-05-04 13:41:42	192.168.10.8-47403	192.168.10.5-34031	UDP
#2-(1-848)	[anort] ET SCAN NMAP OS Detection Probe	2019-05-04 13:41:40	192.168.10.8-47403	192.168.10.5-34031	UDP
#3-(1-1433)	[anort] ET SCAN NMAP OS Detection Probe	2019-05-04 13:41:40	192.168.10.8-47403	192.168.10.5-34031	UDP
#4-(1-841)	[anort] ET SCAN NMAP OS Detection Probe	2019-05-04 13:41:36	192.168.10.8-47403	192.168.10.5-34031	UDP
#5-(1-1425)	[anort] ET SCAN NMAP OS Detection Probe	2019-05-04 13:41:36	192.168.10.8-47403	192.168.10.5-34031	UDP
#6-(1-835)	[anort] ET SCAN NMAP OS Detection Probe	2019-05-04 13:41:34	192.168.10.8-47403	192.168.10.5-34031	UDP
#7-(1-1418)	[anort] ET SCAN NMAP OS Detection Probe	2019-05-04 13:41:34	192.168.10.8-47403	192.168.10.5-34031	UDP
#8-(1-827)	[anort] ET SCAN NMAP OS Detection Probe	2019-05-04 13:41:32	192.168.10.8-47403	192.168.10.5-34031	UDP
#9-(1-1411)	[anort] ET SCAN NMAP OS Detection Probe	2019-05-04 13:41:32	192.168.10.8-47403	192.168.10.5-34031	UDP
#10-(1-781)	[anort] ET SCAN NMAP OS Detection Probe	2019-05-04 13:39:20	192.168.10.8-56847	192.168.10.5-40177	UDP
#11-(1-1345)	[anort] ET SCAN NMAP OS Detection Probe	2019-05-04 13:39:20	192.168.10.8-56847	192.168.10.5-40177	UDP
#12-(1-755)	[anort] ET SCAN NMAP OS Detection Probe	2019-05-04 13:39:18	192.168.10.8-56847	192.168.10.5-40177	UDP
#13-(1-1339)	[anort] ET SCAN NMAP OS Detection Probe	2019-05-04 13:39:18	192.168.10.8-56847	192.168.10.5-40177	UDP
#14-(1-747)	[anort] ET SCAN NMAP OS Detection Probe	2019-05-04 13:39:15	192.168.10.8-56847	192.168.10.5-40177	UDP
#15-(1-1331)	[anort] ET SCAN NMAP OS Detection Probe	2019-05-04 13:39:15	192.168.10.8-56847	192.168.10.5-40177	UDP
#16-(1-739)	[anort] ET SCAN NMAP OS Detection Probe	2019-05-04 13:39:12	192.168.10.8-56847	192.168.10.5-40177	UDP
#17-(1-1323)	[anort] ET SCAN NMAP OS Detection Probe	2019-05-04 13:39:12	192.168.10.8-56847	192.168.10.5-40177	UDP
#18-(1-1317)	[anort] ET SCAN NMAP OS Detection Probe	2019-05-04 13:39:10	192.168.10.8-56847	192.168.10.5-40177	UDP
#19-(1-733)	[anort] ET SCAN NMAP OS Detection Probe	2019-05-04 13:39:10	192.168.10.8-56847	192.168.10.5-40177	UDP

Gambar 17 Alert yang tercatat pada tabel UDP.

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

ID	Signature	Timestamp	Source Address	Dest. Address	Layer 4 Proto
#0-(1-8452)	[ur] [anort] ICMP Test detected	2019-05-06 22:19:55	192.168.10.8	192.168.10.8	ICMP
#1-(1-8451)	[ur] [anort] ICMP Test detected	2019-05-06 22:19:55	192.168.10.8	192.168.10.8	ICMP
#2-(1-8450)	[ur] [anort] ICMP Test detected	2019-05-06 22:19:55	192.168.10.8	192.168.10.8	ICMP
#3-(1-8449)	[ur] [anort] ICMP Test detected	2019-05-06 22:19:55	192.168.10.8	192.168.10.8	ICMP
#4-(1-8448)	[ur] [anort] ICMP Test detected	2019-05-06 22:19:55	192.168.10.8	192.168.10.8	ICMP
#5-(1-8447)	[ur] [anort] ICMP Test detected	2019-05-06 22:19:50	192.168.10.8	192.168.10.8	ICMP
#6-(1-8446)	[ur] [anort] ICMP Test detected	2019-05-06 22:19:50	192.168.10.8	192.168.10.8	ICMP
#7-(1-8445)	[ur] [anort] ICMP Test detected	2019-05-06 22:19:50	192.168.10.8	192.168.10.8	ICMP
#8-(1-8444)	[ur] [anort] ICMP Test detected	2019-05-06 22:19:50	192.168.10.8	192.168.10.8	ICMP
#9-(1-8443)	[ur] [anort] ICMP Test detected	2019-05-06 22:19:50	192.168.10.8	192.168.10.8	ICMP
#10-(1-8442)	[ur] [anort] ICMP Test detected	2019-05-06 22:19:45	192.168.10.8	192.168.10.8	ICMP
#11-(1-8441)	[ur] [anort] ICMP Test detected	2019-05-06 22:19:45	192.168.10.8	192.168.10.8	ICMP
#12-(1-8440)	[ur] [anort] ICMP Test detected	2019-05-06 22:19:45	192.168.10.8	192.168.10.8	ICMP
#13-(1-8439)	[ur] [anort] ICMP Test detected	2019-05-06 22:19:45	192.168.10.8	192.168.10.8	ICMP
#14-(1-8438)	[ur] [anort] ICMP Test detected	2019-05-06 22:19:45	192.168.10.8	192.168.10.8	ICMP
#15-(1-8437)	[ur] [anort] ICMP Test detected	2019-05-06 22:19:40	192.168.10.8	192.168.10.8	ICMP
#16-(1-8436)	[ur] [anort] ICMP Test detected	2019-05-06 22:19:40	192.168.10.8	192.168.10.8	ICMP
#17-(1-8435)	[ur] [anort] ICMP Test detected	2019-05-06 22:19:40	192.168.10.8	192.168.10.8	ICMP
#18-(1-8434)	[ur] [anort] ICMP Test detected	2019-05-06 22:19:40	192.168.10.8	192.168.10.8	ICMP
#19-(1-8433)	[ur] [anort] ICMP Test detected	2019-05-06 22:19:40	192.168.10.8	192.168.10.8	ICMP
#20-(1-8432)	[ur] [anort] ICMP Test detected	2019-05-06 22:19:35	192.168.10.8	192.168.10.8	ICMP
#21-(1-8431)	[ur] [anort] ICMP Test detected	2019-05-06 22:19:35	192.168.10.8	192.168.10.8	ICMP
#22-(1-8430)	[ur] [anort] ICMP Test detected	2019-05-06 22:19:35	192.168.10.8	192.168.10.8	ICMP

Gambar 18 Alert yang tercatat pada tabel ICMP.

Gambar 18 menunjukkan *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 <i>alert</i> yang masuk langsung dicatat di <i>database</i> dan langsung bisa dilihat statistiknya di <i>BASE page</i> yang telah dibuat.	<i>Rule snort</i> dan konfigurasi <i>Honeypot Artillery</i> harus di- <i>update</i> atau disesuaikan apabila ada pola serangan baru, kemampuan untuk pengamanan tergantung pada <i>rule</i> /aturan yang digunakan.
Dapat mengidentifikasi serangan dan menyimpannya sebagai pola.	Membutuhkan lebih banyak <i>resource</i> untuk menganalisa aktivitas.

5. Simpulan

Berdasarkan penelitian Simulasi Sistem Keamanan Jaringan penggabungan antara *Snort IPS* dengan sistem *alerts*-nya yang responsif dalam menangkap gangguan pada sistem *Alerts* yang tercatat di *database* sebanyak 9453 yang terdiri 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 penelitin 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-ppdiao/