Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 3, No. 4, August 2022, Page 247−256
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v3i4.2037

Mengoptimalkan Keamanan Jaringan Komputer Menggunakan Snort dan Telegram Bot yang Terintegrasi dengan Mikrotik

I Putu Gede Abdi Sudiatmika[*], I Putu Yesha Agus Ariwanta, I Gusti Ayu Sri Melati

Informatika dan Komputer, Sistem Komputer, Institut Teknologi dan Bisnis STIKOM Bali, Denpasar, Indonesia
Email: [1,*]gede_abdi@stikom-bali.ac.id ,[2]yeshaagus_ariwanta@stikom-bali.ac.id, [3]melati@stikom-bali.ac.id
Submitted: **03/08/2022**; Accepted: **10/08/2022**; Published: **30/08/2022**

Abstrak−Penerapan IDS (*Intrusion Detection System*) snort dan telegram bot yang dapat terintegrasi dengan router mikrotik pada jaringan komputer Uppala Villa Nusa Dua digunakan untuk mendeteksi aktivitas penyerangan atau penyusupan pada jaringan komputer Uppala Villa Nusa Dua serta memberikan notifikasi secara real-time log aktivitas yang mencurigakan pada jaringan komputer. Metode penelitian yang digunakan adalah metode SPDLC (Security Policy Development Life Cycle) yang memiliki enam tahapan yaitu : Identifikasi, Analisis, Desain, Implementasi, Pengujian dan Evaluasi. Perangkat lunak yang di gunakan pada komputer server adalah Snort, WinPcap, Xampp dan BASE (Basic Analysis and Security Engine) sedangkan untuk pengujian sistem keamanan jaringan komputer menggunakan tools Nmap, Loic dan Brutus. Hasil penelitian yang didapat implementasi IDS (*Intrusion Detection System*) Snort dan telegram bot telah berhasil diimplementasikan dan dapat saling terintegrasi dengan router mikrotik. Berdasarkan pengujian yang dilakukan setelah implementasi sistem baru didapat hasil bahwa 95% penggunaan snort dan telegram bot dapat mengoptimalkan sistem keamanan jaringan komputer di Uppala Villa Nusa Dua.

Kata Kunci: Keamanan; Jaringan Komputer; Snort; Telegram Bot; Router Mikrotik

Abstract−The implementation of IDS (*Intrusion Detection System*) snort and telegram bot that can be integrated with a microtic router on the Uppala Villa Nusa Dua computer network is used to detect attack activities and suspicious activity on the Uppala Villa Nusa Dua computer network and to provide notification in real-time logs of suspicious activity on computer network. The research method used is the SPDLC (Security Policy Development Life Cycle) method which has six stages: Identification, Analysis, Design, Implementation, Testing and Evaluation. The software used on the server computer is Snort, WinPcap, Xampp and BASE (Basic Analysis and Security Engine) while for testing a computer network security system using Nmap, Loic and Brutus tools. The results obtained by the implementation of the IDS (*Intrusion Detection System*) Snort and telegram bot have been successfully implemented and can be integrated with the microtic router. Based on testing conducted after the implementation of the new system, it was found that 95% of the use of snort and telegram bot can optimize the computer network security system at Uppala Villa Nusa Dua.

Keywords: Security; Computer Network; Snort; Telegram Bot; Microtic Router

1. PENDAHULUAN

Uppala Villa Nusa Dua terletak di wilayah kampial yang merupakan kawasan bukit tertinggi di Nusa Dua. Uppala Villa Nusa Dua mulai beroperasi sejak akhir january 2017 dengan jumlah bangunan sebanyak 110 villa. Dalam *operational* villa diatur oleh Uppala *Hospitality Management* (UHM) yang berkantor tepat di sebelah bangunan *lobby* Uppala Villa Nusa Dua. Kantor Uppala *Hospitality Management* (UHM) memiliki beberapa komputer di masing-masing *department* yang saling terhubung dan membentuk jaringan komputer menggunakan sebuah router mikrotik. *Administrator* jaringan komputer pada uppala villa nusa dua beberapa kali menemukan *log* data percobaan serangan atau penyusupan ke router mikrotik dengan melakukan *login* ke router mikrotik dengan mengacak *user* dan *password* hingga menemukan *user* dan *password* yang cocok atau biasa disebut teknik *bruteforce attack*.

Pada *log* data router mikrotik juga ditemukan bahwa penyusup atau penyerang memanfaatkan port terbuka yang ada pada router mikrotik. Sehingga keamanan data dan informasi merupakan salah satu masalah terbesar pada jaringan komputer Uppala Villa Nusa Dua, jika saja percobaan penyusupan atau penyerangan tersebut berhasil dan tanpa diketahui oleh *administrator* jaringan komputer tentu data – data yang berisi informasi perusahaan dapat dicuri dan disalah gunakan. Saat ini *administrator* jaringan komputer Uppala Villa Nusa Dua dalam melakukan *monitoring* jaringan komputer masih menggunakan sistem secara manual yaitu melakukan *login* ke router mikrotik dan saat terjadinya percobaan penyusupan atau penyerangan *administrator* tidak dapat mengetahui secara *real time* sehingga dalam melakukan analisa dan mengambil tindakan keamanan jaringan komputer agak terlambat. Setelah meninjau masalah tersebut maka muncul solusi untuk mengoptimalkan keamanan jaringan komputer dengan menambahkan sistem yang dapat memonitoring, menganalisa, dan melakukan tindakan terhadap aktivitas yang mencurigakan di dalam jaringan komputer secara *real time*.

Sistem keamanan jaringan komputer yang belum optimal tentu akan berdampak buruk bagi penyedia maupun pengguna system, Oleh sebab itu, perlu adanya *monitoring* keamanan jaringan komputer dengan tujuan untuk meminimalisir aktivitas percobaan penyusupan oleh pihak yang tidak bertangggung jawab [1]. IDS (*Intrusion Detection System*) adalah sebuah sistem yang digunakan untuk memonitor dan mengidentifikasi aktivitas pada suatu host atau network untuk dijadikan informasi apakah host atau network tersebut terdapat aktivitas yang mencurigakan [2]. Penerapan IDS (*Intrusion Detection System*) diusulkan sebagai salah satu solusi

Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 3, No. 4, August 2022, Page 247−256
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v3i4.2037

yang dapat digunakan untuk membantu melakukan proses *monitoring* dan menganalisa keamanan jaringan komputer. Snort merupakan jenis *software* IDS (*Intrusion Detection System)* yang digunakan oleh peneliti karena mendukung beberapa macam *platform* dan sistem operasi termasuk linux dan windows, snort merupakan *software* jenis IDS (*Intrusion Detection System*) yang bersifat *open source* dan juga memiliki *support system* di internet sehingga dapat dengan mudah melakukan *update rule* snort yang ada dibandingkan *software* IDS (*Intrusion Detection System*) yang lain. Snort merupakan aplikasi *open source* yang memiliki kemampuan mendeteksi adanya aktivitas penyusupan terhadap sistem keamanan jaringan komputer yang sesuai dengan aturan (*rule*) yang telah ditetapkan didalam IDS (*Intrusion Detection System*) [3].

Penerapan IDS (*Intrusion Detection System*) Snort tentu memerlukan beberapa *software* pendukung diantaranya ialah WinPcap yang memiliki fungsi untuk menangkap paket-paket dari kabel jaringan dan melemparnya ke *system* Snort [3]. Hasil *log* yang dicatat oleh *system* snort disimpan dalam *database* sehingga memudahkan *administrator* jaringan komputer Uppala Villa Nusa Dua dalam menganalisa log yang dicatat oleh snort untuk memudahkan dalam melihat hasil *log* yang dicatat oleh snort dengan menggunakan tambahan *system* dari BASE (*Basic Analysis and Security Engine)* yang memiliki fungsi untuk menghasilkan sebuah *interface web* yang digunakan dalam menganalisa *log* yang dihasilkan snort [4].

Administrator jaringan komputer di Uppala Villa Nusa Dua tidak selalu berada di depan layar komputer untuk melakukan pengawasan, sebuah notifikasi diperlukan untuk memberikan laporan secara *real-time* saat serangan terjadi sehingga pada penelitian ini telegram digunakan untuk mengirim notifikasi *log* snort secara *real-time* dikarenakan menyediakan Bot yang dapat digunakan untuk pengiriman notifikasi dan pengiriman perintah oleh *administrator* jaringan [5].

Pengujian pada penerapan IDS (*Intrusion Detection System)* snort dan telegram bot menggunakan beberapa *tools* yaitu Nmap, LOIC dan Brutus. Nmap digunakan untuk melakukan *network scanning port* yang terbuka pada router mikrotik. LOIC (*Low Orbit Ion Cannon)* digunakan untuk melakukan pengujian jenis *DDOS Attack* pada router mikrotik. Brutus digunakan untuk melakukan pengujian jenis *Brute Force Attack* pada router mikrotik [6]. Hasil penelitian ini membantu administrator jaringan komputer Uppala Villa Nusa Dua untuk mengimplementasikan snort dan telegram bot yang dapat terintegrasi dengan router mikrotik, tidak hanya mengimplementasikan penelitian ini juga menguji apakah implementasi snort dan telegram bot untuk mengoptimalkan keamanan jaringan komputer Uppala Villa Nusa Dua dapat mendeteksi penyusup jaringan komputer dan mendapatkan notifikasi laporan penyerangan secara realtime menggunakan bot yang terdapat di aplikasi telegram serta dapat melakukan tindakan awal pengamanan jaringan komputer sehingga sistem keamanan baru yang dibangun dapat saling terintegrasi untuk membantu administrator jaringan komputer Uppala Villa Nusa Dua.

2. METODOLOGI PENELITIAN

2.1 Metode Pengumpulan Data

Pengumpulan data adalah usaha untuk memperoleh data yang dibutuhkan dalam perekayasaan. Pengumpulan data merupakan langkah yang sangat penting dalam metode ilmiah karena pada umumnya data yang dikumpulkan akan digunakan untuk menguji hipotesa yang telah dirumuskan. Dengan memenuhi prosedur yang sistematik dan standar yang diperlukan maka diharapkan memperoleh hubungan antara metode pengumpulan data dengan masalah yang akan dipecahkan. Pada penelitian ini metode pengumpulan data menggunakan metode observasi dan studi literatur.

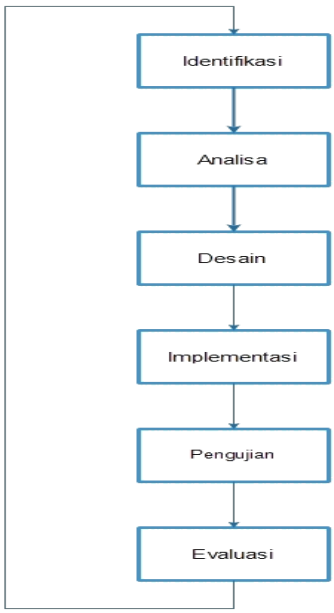
2.2 Metode Pengembangan Sistem

Pada penelitian ini memiliki lingkup penelitian yang akan dibahas yaitu keamanan jaringan komputer pada Uppala Villa Nusa Dua, sehingga metode atau model pengembangan sistem yang peneliti gunakan dalam penelitian ini adalah Security Policy Development Life Cycle (SPDLC). Dalam metode pengembangan sistem Security Policy Development Life Cycle (SPDLC) terdapat enam tahapan yaitu Identifikasi, Analisa, Desain, Implementasi, Pengujian, dan Evaluasi yang dapat dilihat pada bagan gambar 1 [9]:

2.3 Analisa Sistem Berjalan

Pada jaringan komputer Uppala Villa Nusa Dua semua paket yang akan masuk atau keluar dari sistem harus melalui router mikrotik. Dapat dianalogikan bahwa router mikrotik adalah pemisah antara internet dan sistem. Fungsi dari router mikrotik adalah untuk mengatur lalu lintas jaringan dan berfungsi sebagai firewall di jaringan komputer. *Firewall* yang ada di router mikrotik memiliki kelemahan yaitu tidak dapat memberikan peringatan kepada administrator apabila akan terjadi sebuah serangan. Firewall hanya mampu melakukan pencatatan (logging) dan blocking berdasarkan rule firewall tanpa mampu melakukan deteksi apabila paket yang berisi serangan telah masuk ke dalam sistem. Berdasarkan permasalahan tersebut diusulkanlah penggunaan *Intrusion Detection System* (IDS) Snort dan telegram bot untuk mengoptimalkan keamanan jaringan komputer Uppala Villa Nusa Dua.

Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 3, No. 4, August 2022, Page 247−256
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v3i4.2037



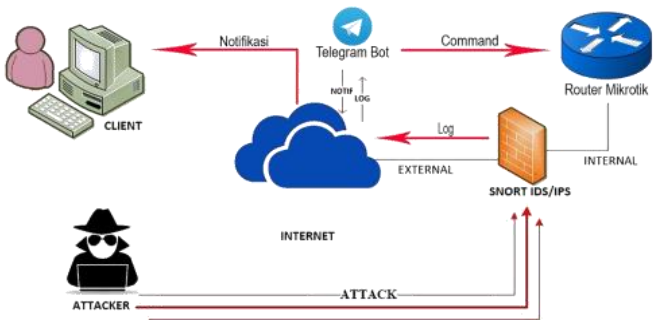
Gambar 1. Bagan Metode Pengembangan SPDLC

2.4 Desain Sistem Baru

Desain atau perancangan sistem keamanan jaringan komputer yang akan diterapkan di Uppala Villa Nusa Dua yaitu penambahan server untuk *Intrusion Detection System* (IDS) Snort dan script untuk menjalankan telegram bot. Tahap desain atau perancangan ini juga akan menjelaskan alur sistem keamanan jaringan yang akan dibangun, serta menjelaskan kebutuhan sistem baik dari software maupun hardware dalam membangun sistem keamanan jaringan tersebut. Pemasangan *Intrusion Detection System* (IDS) diletakkan berdampingan dengan router mikrotik, sehingga semua paket yang memasuki sistem dapat dicatat (logging) pada *Intrusion Detection System* (IDS). Setelah dilakukan pencatatan, *Intrusion Detection System* (IDS) memberikan peringatan kepada network administrator dengan mengirimkan notifikasi melalui telegram bot apabila terdapat paket data yang mencurigakan. Di dalam *Intrusion Detection System* (IDS) terdapat rules yang akan digunakan sebagai dasar pencatatan (logging) serta alert yang dikirimkan kepada network administrator.

2.5 Kerangka Berpikir Sistem

Penelitian yang akan di buat berupa implementasi dan penerapan snort sebagai (*Intrusion Detection System*) IDS dan telegram bot untuk mengoptimalkan keamanan jaringan yang dikelola oleh sebuah router mikrotik. Snort akan mendeteksi aktifitas jaringan yang mencurigakan dan akan mengirimkan notifikasi melalui telegram bot. Telegram bot tidak hanya memberikan notifikasi log aktifitas jaringan yang mencurigakan, telegram bot juga dapat memberikan perintah atau tindakan terhadap aktifitas jaringan yang mencurigakan tersebut. Penyusunan laporan penelitian ini mengacu pada hasil kajian penelitian penulis dilapangan guna bisa diterapkan sebagaimana fungsinya dengan baik. Dalam kerangka berpikir sistem, snort digambarkan dengan alur posisi dari snort ids, penyerang (*attacker*), dan router mikrotik.



Gambar 2. Kerangka Berpikir Sistem

Pada Gambar 2 terlihat ketika penyerang atau *attacker* yang ingin melakukan serangan ke router mikrotik terhalang dalam firewall snort, kemudian ketika action tersebut terjadi maka snort akan mengirimkan notifikasi melalui telegram bot. dan administrator jaringan dapat menggunakan telegram bot untuk memberikan command perintah untuk pengamanan router mikrotik.

Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 3, No. 4, August 2022, Page 247−256
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v3i4.2037

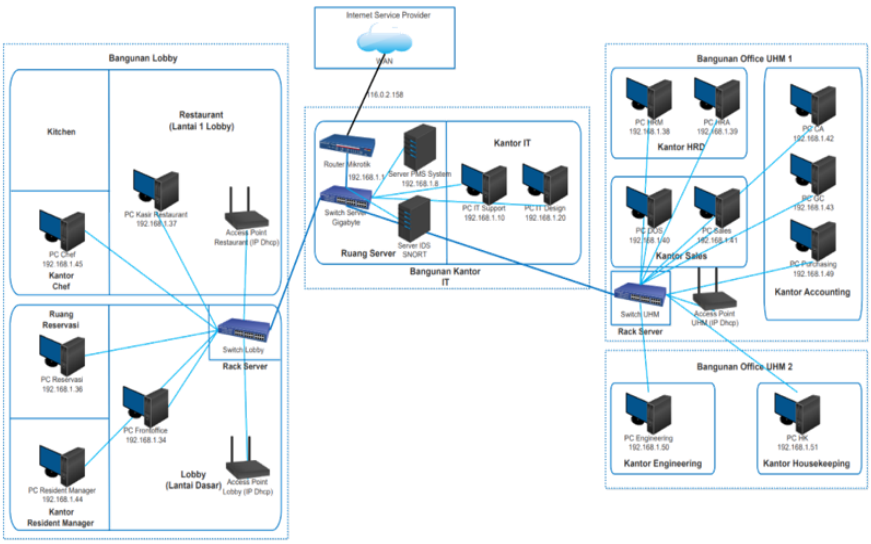
3. HASIL DAN PEMBAHASAN

3.1 Sistem

Setelah melakukan analisa sistem yang sedang berjalan pada Uppala Villa Nusa Dua dan merancang desain sistem baru yang akan diterapkan, maka tahap selanjutnya adalah implementasi sistem sehingga selanjutnya sistem baru yang akan dirancang dapat berjalan sesuai dengan desain yang sudah dibuat. Pada tahap implementasi atau penerapan rancangan sistem keamanan jaringan komputer, detail rancangan atau desain akan digunakan sebagai intruksi atau panduan tahap implementasi agar sistem yang dibangun dapat sesuai dengan sistem yang sudah dirancang atau didesain. Proses implementasi terdiri dari instalasi dan konfigurasi.

3.1.1 Topologi Jaringan

Pada implementasi tapologi jaringan peneliti mengumpulkan seluruh perangkat yang dibutuhkan. Perangkat ini meliputi *hardware* dan *software*, Selanjutnya peneliti menempatkan seluruh perangkat sesuai dengan topologi yang sudah dirancang. Setelah semua perangkat terhubung satu sama lain, selanjutnya adalah mengkonfigurasi setiap perangkat agar dapat berkomunikasi satu dengan lainnya.



Gambar 3. Topologi Jaringan Komputer Uppala Villa Nusa Dua

3.1.2 Konfigurasi Komputer *Server* Snort

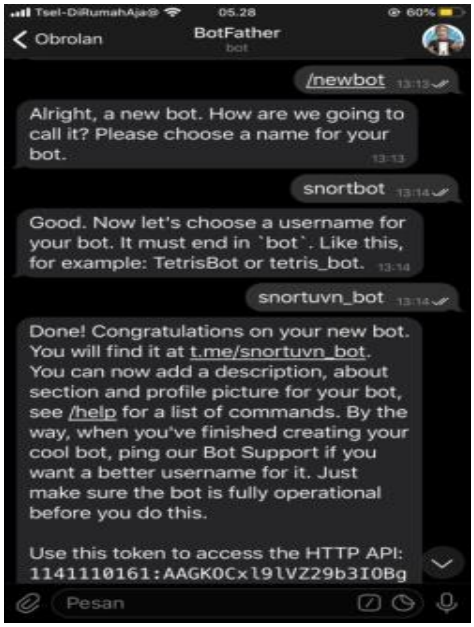
Komputer server *Intrusion Detection System* (IDS) yang peneliti bangun dengan menggunakan beberapa komponen utama, yaitu :

a. Implementasi dan Konfigurasi Snort
   Implementasi dan konfigurasi snort sebagai komponen utama komputer *server Intrusion Detection System* (IDS) dengan melakukan instalasi sistem snort dan melakukan penyesuaian pengaturan di file snort.conf pada sistem snort.
b. Implementasi dan Konfigurasi WinPcap
   Implementasi dan konfigurasi WinPcap sebagai komponen utama komputer *server Intrusion Detection System* (IDS) berfungsi untuk membantu snort untuk menangkap paket – paket jaringan yang lewat pada sistem jaringan komputer.
c. Implementasi dan Konfigurasi Xampp
   Implementasi dan konfigurasi Xampp sebagai komponen utama komputer *server Intrusion Detection System* (IDS). Pada penelitian ini xampp digunakan untuk menjalankan BASE dan *script program* php telegram bot.
d. Implementasi dan Konfigurasi BASE
   Implementasi dan konfigurasi Base sebagai komponen utama komputer *server Intrusion Detection System* (IDS)**.** Pada penelitian ini BASE ditambahkan fungsinya agar *log* snort dapat diterima *administrator* jaringan melaluli telegram bot.

3.1.3 Konfigurasi Telegram Bot di BASE

Implementasi dan konfigurasi telegram bot pada tahap ini memiliki fungsi sebagai media notifikasi secara *real-time* ke *administrator* jaringan, jadi jika ada *log database* snort yang masuk otomatis bot akan memberikan notifikasi secara *real-time*. Pada gambar 3.2 dibawah ini merupakan tampilan awal dalam proses pembuatan telegram bot.

Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 3, No. 4, August 2022, Page 247−256
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v3i4.2037



Gambar 4. Tampilan Pembuatan Telegram Bot

Pada gambar 4. dibawah ini merupakan *script bot_engine.php* yang peneliti buat untuk menjalankan bot telegram yang dibuat sebelumnya agar dapat mengirim *log data* snort secara *real-time* ke *administrator* jaringan. Untuk *$token key* nya didapat saat mendaftarkan *bot* pada *BotFather*. Untuk *$chatid* dapat kita lihat menggunakan "https://api.telegram.org/bot1141110161:AAGURRLF7FIIlNiZzSW 3GLEqEBxz4c_HG4/getUpdates" pada *web browser*.

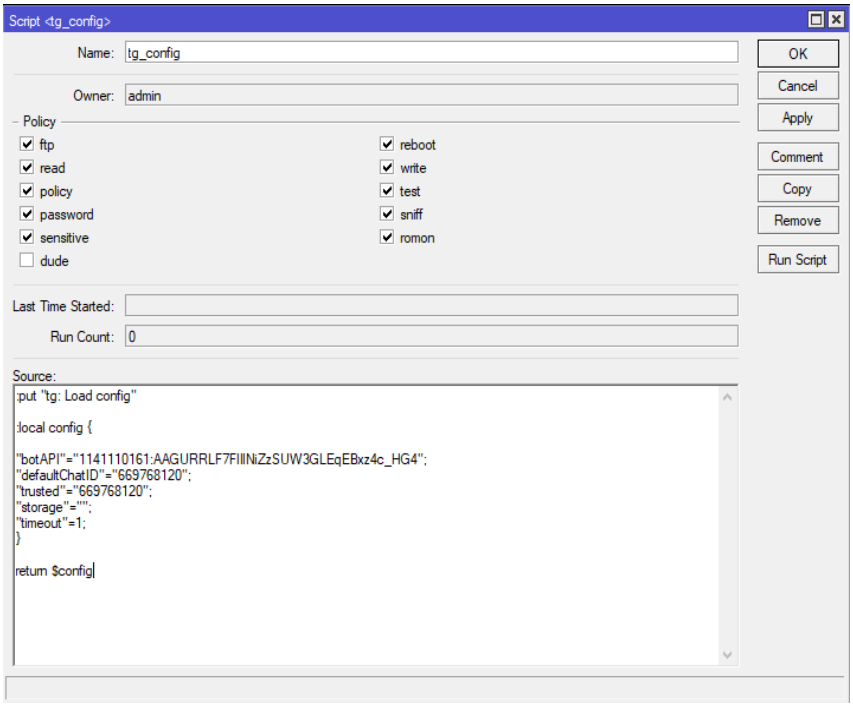
```php
<?php
require_once('bot_config.php');
require_once('bot_functions.php');

$query = mysqli_query($conn, "SELECT sig_name, timestamp, ip_src, inet_ntoa(ip_src) vip_src, ip_dst, inet_ntoa(ip_dst)
vip_dst, status FROM acid_event ORDER BY timestamp DESC");
$count = mysqli_num_rows($query);
$token = "bot1141110161:AAGURRLF7FIIlNiZzSUW3GLEqEBxz4c_HG4";
$chatid = "669768120";

if(!empty($count)) {
    while($row = mysqli_fetch_array($query, MYSQLI_ASSOC)) {
        if($row['status'] == 0) {
            $content = " Terjadi serangan " . $row['sig_name'] . " dari " . $row['vip_src'] . " ke " . $row['vip_dst'] .
            " pada tanggal " . $row['timestamp'];
            sendMessage($chatid, $content, $token);
            $update = mysqli_query($conn, "UPDATE acid_event SET status = '1' WHERE sig_name = '$row[sig_name]' AND
            timestamp = '$row[timestamp]' AND ip_src = '$row[ip_src]' AND ip_dst = '$row[ip_dst]'");
        }
    }
}
?>
```

Gambar 5. Konfigurasi Script Engine Telegram Bot

3.1.4 Konfigurasi Telegram Bot di Mikrotik

Implementasi dan konfigurasi telegram bot pada tahap ini memiliki fungsi agar telegram bot dan router mikrotik saling terintegrasi dan telegram bot dapat memberikan perintah untuk Memblock *IP Address* dan *Port* yang ada di mikrotik, jadi jika ada *intrusion* yang terdeteksi dan notifikasi dikirim melalui telegram bot *administrator* jaringan dapat dengan cepat melakukan langkah pengamanan. Pada gambar 3.4 dibawah ini merupakan *script mikrotik tg_config* yang memiliki fungsi agar *router* mikrotik dan telegram bot dapat saling berkomunikasi. *Script* ini memerlukan *API key* dan *Chat id* telegram bot.

Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 3, No. 4, August 2022, Page 247−256
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v3i4.2037



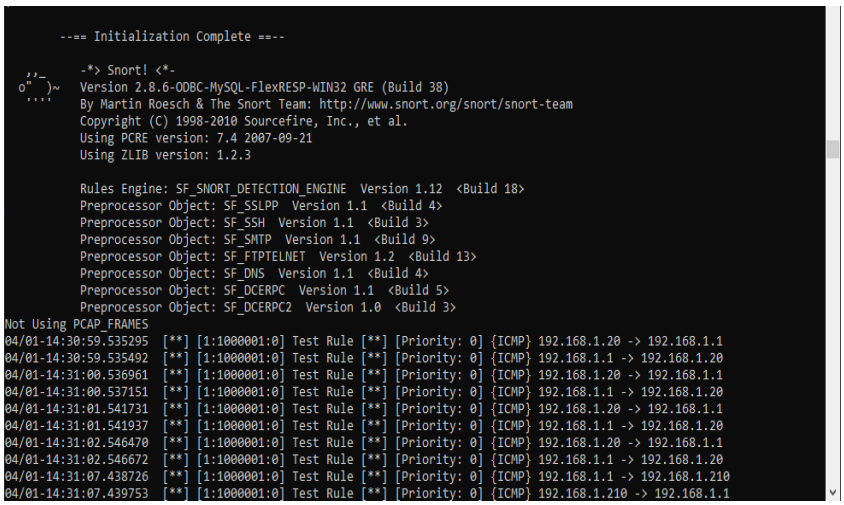
Gambar 6. Script tg_config Telegram Bot di mikrotik

3.2 Pengujian Sistem

Aktivitas pengujian yang dilakukan dalam penelitian ini adalah pengujian pada *system Intrusion Detection System* (IDS), pengujian pada telegram bot dan pengujian bersifat fungsionalitas dimana pengujian tersebut menghasilkan output yang valid atau yang tidak valid.

3.2.1 Pengujian *Intrusion Detection System* (IDS) Snort

Pengujian snort dilakukan pada sensor deteksi, pengujian ini menggunakan *rules* sederhana (untuk mendapatka data dari sebuah jenis serangan tertentu) dan memastikan *Instrusion Detection System* (IDS) Snort dapat mendeteksi *rules* tersebut. *Intrusion Detection System* (IDS) Snort diaktifkan dengan perintah berikut ini : *snort -A console -i1 -c c:\snort\etc\snort.conf -l c:\snort\log -K ascii*. Perintah tersebut akan menampilkan notifikasi atau alert pada layar *console command prompt*.

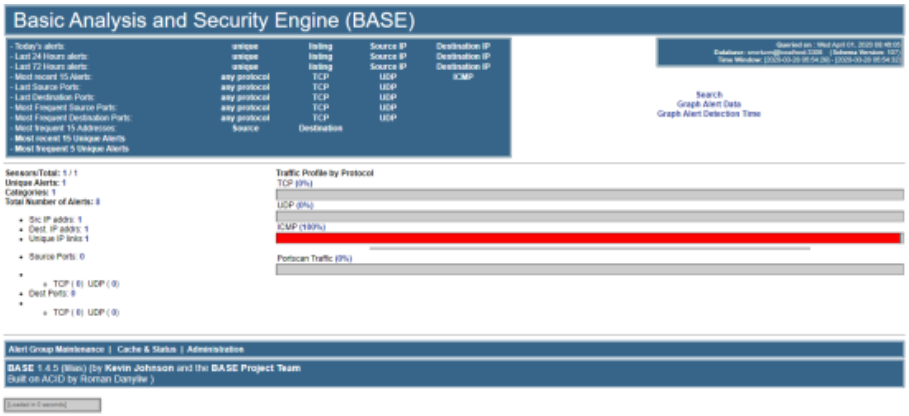


Gambar 7. Pengujian Snort

3.2.2 Pengujian BASE (Basic Analysis and Security Engine)

Dalam menampilkan *log* snort pada system BASE (*Basic Analysis and Security Engine*) saat melakukan pengaktifan snort menggunakan perintah berikut ini : *snort -c c:\snort\etc\snort.conf -l c:\snort\log -i1*. Hasilnya dapat dilihat pada gambar dibawah ini, BASE (*Basic Analysis and Security Engine*) dapat menampilkan *log* snort.

Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 3, No. 4, August 2022, Page 247−256
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v3i4.2037

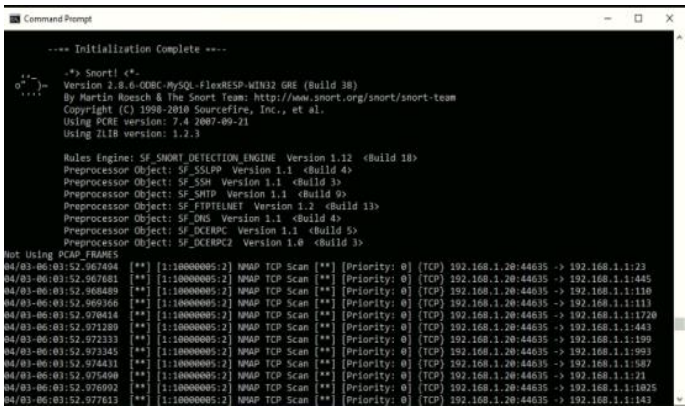


Gambar 8. Pengujian BASE (*Basic Analysis and Security Engine*)

3.2.3 Pengujian Fungsionalitas *Intrusion Detection System* (IDS) Snort

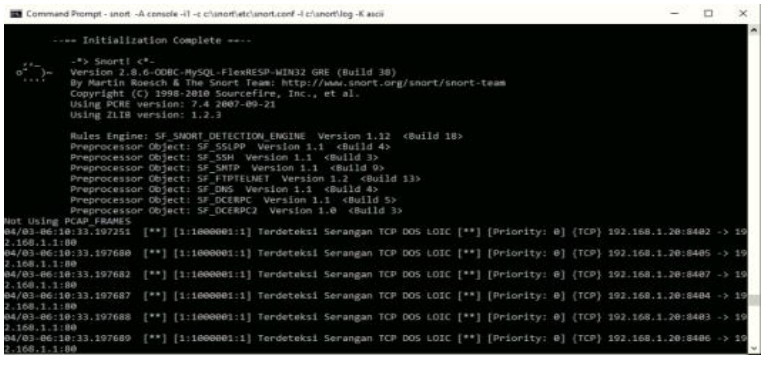
Pada tahap pengujian ini peneliti akan menguji keefektifan dari fungsionalitas *Intrusion Detection System* (IDS) Snort secara keseluruhan. *Intrusion Detection System* (IDS) Snort merupakan sebuah sistem yang berfungsi untuk mendeteksi aktivitas *intrusi* atau penyerangan.

a. Nmap *Port Scanning Attack*
Pada tahap simulasi penyerangan Nmap *Port Scanning attack* peneliti akan mensimulasikan dan menganalisis aktivitas *port scanning* dengan menggunakan *tools* NMAP yang akan dilakukan di komputer *client* sebagai *attacker*. Berikut adalah *rules* yang peneliti gunakan untuk mendeteksi Nmap *Port Scanning Attack* : *alert tcp any any -> 192.168.1.1 any (msg:"NMAP TCP Scan";sid:10000005;rev:2;).*



Gambar 9. *Log* Snort Mendeteksi *Port Scanning*

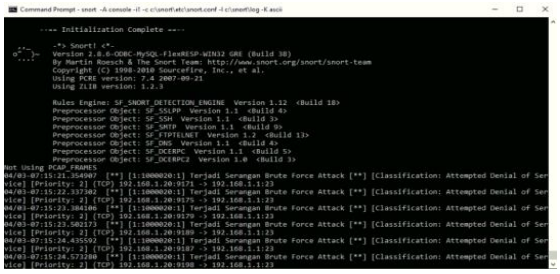
b. LOIC *DDOS Attack*
Pada tahap simulasi penyerangan LOIC *DDOS Attack* peneliti akan mensimulasikan dan menganalisis aktivitas *DDOS Attack* dengan menggunakan *tools* LOIC yang akan dilakukan di komputer *client* sebagai *attacker*. Berikut adalah *rules* yang peneliti gunakan untuk mendeteksi serangan *DDOS attack* menggunaan *protocol TCP* dan *UDP* : *alert tcp any any -> 192.168.1.1 any (msg:"Terdeteksi Serangan TCP DOS LOIC"; sid:1000001;rev:1;)* dan *alert udp any any -> 192.168.1.1 any (msg:"Terdeteksi Serangan UDP DOS LOIC"; sid:1000003;rev:1;).*



Gambar 10. *Log* Snort Mendeteksi *TCP DDOS Attack*

Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 3, No. 4, August 2022, Page 247−256
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v3i4.2037

c. Brutus Brute Force Attack
Pada tahap simulasi penyerangan Brutus *Brute Force Attack* peneliti akan mensimulasikan dan menganalisa aktivitas *Brute Force Attack* dengan menggunakan *tools* Brutus yang akan dilakukan di komputer *client* sebagai *attacker.* Berikut adalah *rules* yang peneliti gunakan untuk mendeteksi serangan *Brute Force Attack* : *alert tcp any any -> 192.168.1.1 any (msg:"Terjadi Serangan Brute Force Attack";flow:to_server; flags:A; threshold:type threshold, track by_src, count 15, second 60; classtype:attempted-dos;sid:1000020;rev:1;).*

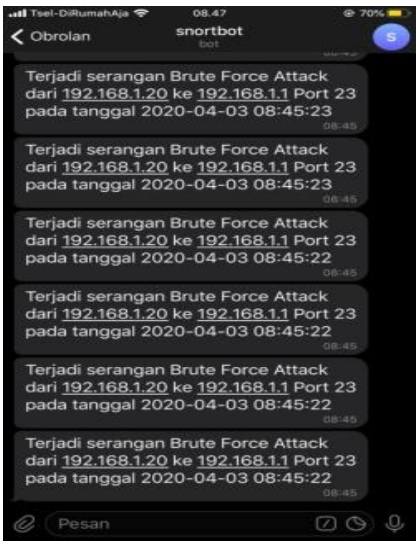


Gambar 11. *Log* Snort Mendeteksi *Brute Force Attack*

3.2.4 Pengujian Integrasi Telegram Bot Dengan Snort dan Mikrotik

Pengujian integrasi Telegram bot dengan Snort dan Mikrotik peneliti melakukan uji coba saat snort mendeteksi serangan *brute force attack* dengan perintah : *snort -c c:\snort\etc\snort.conf -l c:\snort\log -i1* Hasilnya dapat dilihat pada gambar berikut ini.

Gambar 12. *Log* Snort di *Database* Snortuvn



Gambar 13. *Log* Snort di Telegram Bot

3.3 Evaluasi Hasil Pengujian Sistem

Pada tahap evaluasi hasil pengujian sistem terdapat beberapa hal hasil pengujian yang akan dievaluasi untuk mengetahui tingkat efektifitas dari penerapan sistem keamanan jaringan komputer tersebut.

Tabel 2. Hasil Pengujian Sistem Monitoring Keamanan Jaringan Komuter

No	Tipe Serangan	Tools	Sistem Baru	Sistem Lama	Kesimpulan
1	*Port Scanning*	Nmap	Terdeteksi	Tidak Terdeteksi	Sistem baru yang di terapkan berhasil mendeteksi serangan jenis Port

Journal of Computer System and Informatics (JoSYC)
ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 3, No. 4, August 2022, Page 247−256
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v3i4.2037

No	Tipe Serangan	Tools	Sistem Baru	Sistem Lama	Kesimpulan
					Scanning.
2	*DDOS Attack*	Loic	Terdeteksi	Tidak Terdeteksi	Sistem baru yang di terapkan berhasil mendeteksi serangan jenis *DDOS Attack*.
3	*Brute Force Attack*	Brutus	Terdeteksi	Terdeteksi	Sistem baru yang di terapkan berhasil mendeteksi serangan jenis *Brute Force Attack*.

Tabel 3. Hasil Pengujian Efektivitas Waktu Sistem

No	Pengujian	Sistem Baru	Sistem Lama	Kesimpulan
1	Pencatatan notifikasi ke *log* sistem keamanan jaringan komputer	Terdeteksi 08:28:30 Pencatatan *log* sistem 08:28:30	Terdeteksi 08:28:30 Pencatatan *log* sistem 08:28:30	Tidak ada selisih waktu yang didapat baik menggukanan sistem lama atau sistem baru yang telah diterapkan.
2	Notifikasi keamanan jaringan komputer secara *real-time* ke *administrator* jaringan komputer	Terdeteksi 08:28:30 Pengiriman notifikasi ke administrator 08:28:40	Belum adanya notifikasi keamanan secara *real-time*	Selisih waktu sistem baru dari terdeteksi sampai pengiriman notifikasi yaitu 10 detik pada sistem lama belum ada notifikasi secara *real-time*
3	Tindakan pengamanan sistem jaringan komputer secara *real-time*	Terdeteksi 08:35:18 Pengiriman perintah tindakan pengamanan ke sistem 08:35:28	Belum adanya tindakan pengamanan secara *real-time*	Selisih waktu sistem baru dari terdeteksi sampai notifikasi sukses saat melakukan pengamanan jaringan yaitu 10 detik pada sistem lama belum adanya tindakan pengamanan secara *real-time*

Tabel 4. Hasil Pengujian Telegram Bot

No	Uji Coba	Hasil Pengujian	Kesimpulan
1	Notifikasi *Alert* Snort ke Telegram Bot Secara *Real Time*	Terdeteksi	Berhasil
2	Memblock *IP Address Attacker*	Terdeteksi	Berhasil
3	Memblock *Port* Terbuka Pada Router Mikrotik	Terdeteksi	Berhasil

Pada pengujian sistem monitoring keamanan jaringan komputer didapat bahwa sebelum sistem baru menggunakan snort di terapkan sistem lama hanya dapat mendeteksi serangan jenis *brute force attack* saat sistem baru diterapkan sistem keamanan jaringan komputer dapat lebih aman dan optimal dikarenakan dapat mendeteksi jenis serangan lain yaitu *Port Scanning, DDOS Attack* dan *Brute Force Attack.* Pada tahap pengujian efektifitas waktu sistem baru keamanan jaringan komputer didapat bahwa terdapa selisih waktu sekitar 10 detik saat pengiriman notifikasi dan melakukan tindakan pengamanan jaringan komputer. Namun selisih waktu tersebut lebih baik dari sistem keamanan sebelumnya yang tidak memiliki notifikasi secara *real-time* dikarenakan masih menggunakan sistem manual, yang dimaksud secara manual ialah pengecekan secara terjadwal atau tidak setiap waktu oleh administrator ke log mikrotik. Pengujian terakhir yaitu pengujian Telegram Bot didapat bahwa seluruh pengujian berhasil dilakukan dan sistem berjalan dengan baik. Berdasarkan hasil dari pengujian dan tersebut didapat bahwa sistem keamanan jaringan komputer di Uppala Villa Nusa Dua saat sistem baru yang menggunakan snort dan telegram bot diterapkan dapat mengoptimalkan sistem keamanan jaringan komputer sebesar 95% angka ini didapat dikarenakan ada beberapa hal yang perlu dievaluasi seperti selisih waktu untuk pengiriman dan penerimaan notifikasi atau alert snort ke telegram bot yang masih memiliki selisih waktu 10 detik.

4. KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan yang telah diuraikan maka dapat disimpulkan sebagai berikut : *Intrusion Detection System* (IDS) Snort dapat di implementasikan pada jaringan komputer Uppala Villa Nusa Dua dengan baik dan seluruh sistem pendukung snort bekerja sesuai fungsinya, Implementasi telegram bot telah berhasil diimplementasikan dan dapat saling terintegrasi dengan snort dan router mikrotik sehingga seluruh sistem baru keamanan jaringan komputer Uppala Villa Nusa Dua berhasil diimplementasikan. Pengujian yang dilakukan didapat bahwa setelah pemasangan sistem snort dapat mendeteksi tiga jenis serangan yaitu *Port Scanning, DDOS Attack* dan *Brute Force Attack* dari yang sebelumnya sistem keamanan jaringan komputer

ISSN 2714-8912 (media online), ISSN 2714-7150 (media cetak)
Volume 3, No. 4, August 2022, Page 247−256
https://ejurnal.seminar-id.com/index.php/josyc
DOI 10.47065/josyc.v3i4.2037

Uppala Villa Nusa Dua hanya mendeteksi jenis serangan *Brute Force Attack*. Penambahan sistem notifikasi secara *real-time* dengan memanfaatkan Telegram Bot berhasil membantu *administrator* jaringan komputer untuk memonitoring jaringan komputer dikarenakan sistem sebelumnya belum memiliki sistem notifikasi secara *real-time*. Berdasarkan hasil pengujian pemasangan sistem baru menggunakan snort dan telegram bot pada Uppala Villa Nusa Dua dapat mengoptimalkan sistem keamanan jaringan komputer sebesar 95%. Berikut beberapa saran-saran yang diberikan pada penelitian ini adalah sebagai berikut : Pada pengembangan selanjutnya sebaiknya menggunakan lebih banyak aplikasi atau *tools Penetration Testing* sehingga dapat meningkatkan akurasi *rules* snort dalam mendeteksi sebuah serangan. Sebaiknya menambah *rules* serangan agar snort tidak hanya sebatas mendeteksi jenis serangan *port scanning*, *DDOS Attack* dan *Brute force Attack* sehingga dapat mencegah jenis serangan lain pada jaringan komputer. Telegram bot hanya digunakan oleh satu orang *administrator* jaringan saja, sebaiknya telegram bot tersebut dapat ditambahkan di sebuah grup telegram agar memudahkan dalam proses monitoring. Sebaiknya selisih waktu dalam pengiriman dan penerimaan notifikasi atau alert snort ke telegram bot dapat lebih di optimalkan lagi dengan memperbaiki koneksi internet di server dan kode program yang ada di sistem BASE (*Basic Analysis and Security Engine*).

REFERENCES

[1] Danang Tri Atmaja, Eka Budhy Prasetya, Priadhana Edi Kresnha, "Notifikasi Adanya Serangan Pada Jaringan Komputer dengan Mengirim Pesan Melalui Aplikasi Telegram dan Kontrol Server," Jurnal Seminar Nasional Sains dan Teknologi 2018, Vol. 5, No. 1, 2-3, Oktober 2018.

[2] Azaim. Haikal, "Mengenal *Intrusion Detection System* (IDS)", 12 January 2017, [Online]. Tersedia: https://netsec.id/intrusion-detection-system/ [Diakses: 21 Oktober 2019].

[3] Sutarti, Adi Putranto Pancaro, Fembi Isnanto Saputra, "Implementasi IDS (*Intrusion Detection System* Pada Sistem Keamanan Jaringan SMAN 1 Cikeusal," Jurnal Prosisko, Vol. 5, No. 1, 2-3, Maret 2018.

[4] Bangun Saputra, Setia Juli Irza Ismail, Mochamad Fachru Rizal, "Perancangan dan Implementasi NIDS (Network *Intrusion Detection System*) Menggunakan Snort dan BASE Pada Freebsd 10," Jurnal e-Proceeding of Applied Science, Vol. 1, No. 2, Agustus 2015.

[5] Agung Sulistyo, Felix Andreas Sutanto, " Warning System Gangguan Konektivitas Jaringan Pada BMKG Semarang Dengan Telegram Bot," Prosiding SINTAK 2018, Oktober 2018.

[6] Fauzi. Yusuf, "Mengenal Berbagai Jenis Serangan Pada Jaringan Komputer", 20 January 2017, [Online]. Tersedia: https://netsec.id/jenis-serangan-jaringan-komputer/ [Diakses: 21 Oktober 2019].

[7] Yudhi Arta, Abdul Syukur, Roni Kharisma, "Simulasi Implementasi Intrusion Prevention System (IPS) Pada Router Mikrotik," IT Journal Research and Development, Vol. 3, No.1, 105-106, Agustus 2018.

[8] I Gusti Komang Oka Mardiyana, "Keamanan Jaringan Dengan Firewall Filter Berbasis Mikrotik Pada Laboratorium Komputer STIKOM Bali," Konferensi Nasional Sistem & Informatika 2015, Oktober 2015.

[9] Muh. Sadam Husain S.S, LM. Fid Aksara, Natalis Ransi, "Implementasi Keamanan Server Pada Jaringan Wireless Menggunakan Metode Intrusion Detection and Prevention System (IDPS) (Studi Kasus : Techno's Studio)" Journal semanTIK, Vol. 4, No.2, pp. 11-20, Jul-Des 2018.