Peningkatan Keamanan Router Mikrotik Terhadap Serangan *Syn Flood* dengan Menggunakan *Firewall Raw* (Studi kasus : Sekolah Menengah Kejuruan Negeri 3 Bengkalis)

Mhd.Fakhmi[1], Lipantri Mashur Gultom[2]
Teknik Informatika Politeknik Negeri Bengkalis
JL.Bathin Alam, Sungai Alam Bengkalis-Riau, Indonesia 28714
Email: fakhmitkj3@gmail.com[1] , lipantri@polbeng.ac.id[2]

Abstract

Internet services provide many benefits that are public, this is the cause of many people using the internet. Of the many benefits provided, there are many shortcomings in the internet network that can be exploited by hackers to do damage such as data theft and others. The attack that often occurs is a DoS (Denial of Service) attack which is carried out to flood the target with packets sent to the target continuously. Syn attack is a type of DoS (Denial Of Service) attack that implements the TCP/IP protocol by sending SYN request packets into the ports on the router with the aim of absorbing all available resources on the server so that the server becomes too busy and cannot control network traffic well. It can even result in a system crash (hang). MikroTik Router is one type of router that has a complete range of features to support network security such as a firewall. The firewall will filter the data received and track the connections made to determine whether the connection is allowed or denied.

Keywords: *Internet, DoS, TCP/IP, Syn Attack, Mikrotik, Firewall.*

1. PENDAHULUAN

Perkembangan jaringan internet saat ini sangat pesat, hal ini dilihat dari manfaat internet yang sangat berdampak dalam kehidupan masyarakat. Fitur-fitur yang disediakan oleh jaringan internet juga begitu banyak, mulai dari *web server*, *file transfer Protocol* (ftp), *E-mail*, maupun layanan transaksi publik seperti *E-Commerce*, *E-Banking*, *E-Government* dan sebagianya. Layanan internet kini sudah banyak digunakan oleh berbagai kalangan baik itu perusahaan, instansi pemerintahan, perkantoran, perumahan, universitas dan lain-lain. Penggunaan internet ini disebabkan oleh dengan didapatkannya kemudahan dalam hal komunikasi dan transfer data. Dengan menggunakan jaringan komputer berbasis *Local Area Network* dan *Wireless Local Area Network*, topologi yang sering diterapkan adalah topologi *star* dengan satu titik terpusat pada *device*, lebih seringnya menggunakan *device router*.

Router adalah sebuah *tool* yang menggunakan sistem operasi *Linux Base.* Yang diperuntukkan sebagai *Network Router* yang dapat menghubungkan dua atau lebih jaringan komputer yang berbeda. Ukuran kinerja *router* sangat penting untuk memadai kapasitas pengguna dengan pengiriman data yang banyak. Apabila suatu jaringan terjadi *transfer* data dalam jumlah yang besar maka akan terjadi kebanjiran data atau *Flooding* melalui *Internet Protocol* (IP) *address* atau *mac address.* Hal tersebut membuat banyak *hacker* menjadikan *Router* sebagai target serangan utama karena *Router* merupakan perangkat penting dalam sebuah jaringan.

Jenis serangan yang kerap terjadi pada jaringan yaitu serangan DoS (*Denial of Service*). Adalah serangan yang dilakukan secara individual dengan menggunakan mesin komputer yang digunakan sebagai media penyerang. Serangan ini dijalankan komputer penyerang yang lebih kuat dari targetnya sehingga penyerang mampu membanjiri targetnya dengan paket-paket yang dikirim pada target.

Syn attack adalah salah satu jenis serangan DoS (*Denial Of Service*) yang mengimplementasi potokol *TCP/IP* dengan mengirimkan paket-paket *SYN request* kedalam *port-port* pada *router* sasaran dengan maksud menyerap seluruh sumber daya yang ada pada *server* sehingga server menjadi terlalu sibuk dan tidak dapat mengontrol lalu lintas jaringan dengan baik. Bahkan dapat berakibat macetnya sistem (*hang*).

MikroTik Routerboard merupakan salah satu jenis *router* yang memiliki berbagai fitur yang lengkap dalam mendukung keamanan jaringan seperti *firewall*. *Firewall* akan memfilter data yang diterima dan melacak koneksi yang dibuat untuk menentukan data apakah koneksi tersebut diizinkan atau ditolak. Meskipun *firewall* tidak dapat mencegah serangan secara keseluruhan, setidaknya *firewall* lebih dapat membantu membuat data menjadi lebih aman daripada tanpa *firewall* sama sekali. *Firewall* yang digunakan pada penelitian ini adalah *firewall raw*. Merupakan fitur baru pada *MikroTik RouterOS* yang memungkinkan kita untuk melewatkan atau mendrop suatu koneksi sebelum masuk ke proses *connection-tracking*, oleh karena itu maka penggunaan *firewall raw* bisa mengurangi beban *CPU* secara signifikan.

Lembaga Pendidikan di Indonesia yang berada dibengkalis yang dimana didalamnya terdapat informasi tentang sekolah tersebut. Selama ini sistem keamanan yang diterapkan di SMKN 3 Bengkalis hanya melakukan keamanan pada segi *gateway* saja karena menganggap tidak akan ada penyerangan yang demikian. Hal tersebut tidaklah benar, serangan bisa terjadi kapanpun, dimanapun, dan kepada siapapun. Oleh karena itu Penelitian ini bertujuan untuk memberikan pemahaman saat terjadi serangan terhadap perangkat *router mikrotik* terutama terhadap serangan *DoS/DDoS* yaitu *Syn Flood Attack* dengan melakukan penigkatan keamanan jaringan menggunakan fitur pada *mikrotik router* yaitu *firewall*.

2. TINJAUAN PUSTAKA

Dasar atau acuan berupa teori-teori melalui hasil dari penelitian sebelumnya merupakan hal yang sangat penting dan dapat digunakan sebagai data pendukung pembuatan melakukan penelitian. Salah satu data pendukung yang dapat dijadikan sumber tersendiri adalah kajian terdahulu yang berhubungan dengan permasalahan yang sedang dibahas dalam penelitian ini. Penelitian terdahulu dikumpulkan oleh penulis untuk membuat perbandingan antara penelitian terdahulu dengan penelitian yang dilakukan oleh penulis untuk melengkapi dan menjadi landasan dalam melakukan penelitian ini. Oleh karena itu, penulis mengambil referensi dari beberapa jurnal penelitian terdahulu. Berikut hasil perbandingan penelitian tersebut.

Penelitian terdahulu yang dilakukan oleh Aprilianto Doni dkk., (2019) yang berjudul ”Sistem Pencegahan *UDP DNS Flood* Dengan *Filter Firewall* Pada *Router Mikrotik*” menjelaskan bahwa *firewall* yang dikonfigurasi dalam sistem keamanan *Router MikroTik* melakukan pemeriksaan data yang diterima dan melacak koneksi tersebut diizinkan atau ditolak. Penggunaan *Firewall* digunakan untuk menyaring *user* yang terkoneksi dan melakukan penghalangan akses dari *user* yang diblokir.

Penelitian terdahulu yang dilakukan oleh Putra Baytar (2020) dengan judul "Pemanfaatan *Mikrotik Routerboard* Sebagai Keamanan Jaringan Dari *UDP Flood* Dengan Menggunakan *Firewall* Di Dinas Pendidikan Kabupaten Bengkalis" menjelaskan bahwa *mikrotik routerboard* sebagai keamanan jaringan dari *UDP Flood* dengan menggunakan *firewall* bekerja dengan baik. Dengan menggunakan *routerboard mikrotik* sebagai media pengamanan jaringan sangat membantu meningkatkan perlindungan pada lalu lintas jaringan internet di dinas pendidikan Bengkalis.

3. PERANCANGAN

3.1 Data dan Alat Penelitian

Tujuan dari peningkatan keamanan *router mikrotik* terhadap serangan *syn flood* dengan menggunakan *firewall raw* adalah untuk mengoptimalkan keamanan jaringan dari serangan *syn flood* yang bisa mengganggu kinerja jaringan. Demi mewujudkan semua itu dibutuhkan beberapa perangkat yang bisa mendukung. Beberapa hal yang perlu diperhatikan untuk melakukan keamanan jaringan antara lain :

3.1.1 Data Penelitian

Data yang digunakan dalam melakukan analisa keamanan jaringan dari serangan *syn flood* pada *mikrotik* yaitu berupa data-data bukti digital dari serangan yang telah dilakukan pada penelitian yang lalu. Dari data tersebut dapat diketahui bagian sistem mana yang berdampak setelah dilakukan penyerangan dan bagaimana tindakan pertama yang dilakukan untuk menanggulangi serangan tersebut.

3.1.2 Peralatan *Software*

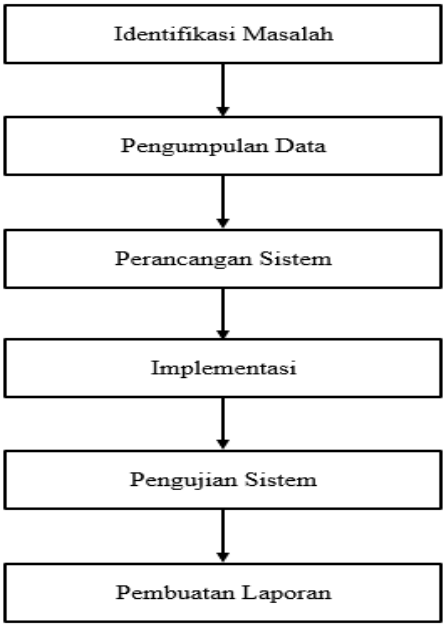
1. *Winbox*
2. *Microsoft Windows 10 sebagai Client*
3. *Kali Linux*

i. Peralatan *Hardware*

1. Laptop
2. *Routerboard Mikrotik*
3. Kabel UTP

3.2 Prosedur Penelitian

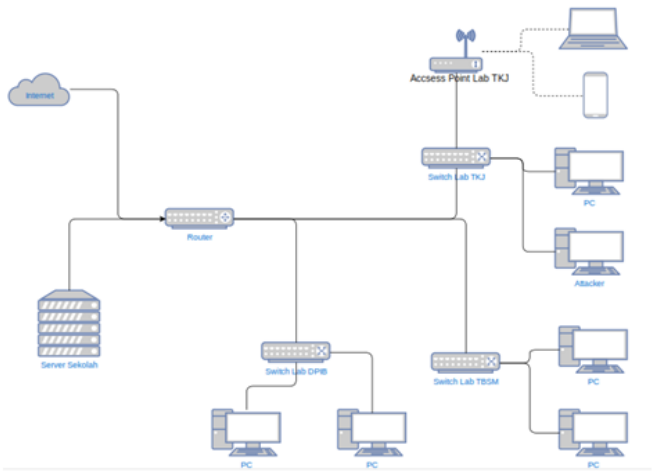
Dalam melakukan penelitian tentang peningkatan keamanan *router mikrotik* terhadap serangan *syn flood* dengan menggunakan *firewall raw*, kemudian melakukan pengumpulan data tentang pengamanan jaringan setelah itu melakukan Evaluasi Data yang telah di dapatkan untuk mendapatkan data-data penggunaan jaringan atau konten-konten yang di akses oleh pengguna internet dan memisahkan konten yang bisa di akses dengan yang tidak perlu. Dalam perancangan sistem ini peneliti membuat mekanisme *filtering* dan titik-titk yang akan ditempati *firewall*. Dan instalasi Perangkat Keras dan Perangkat Lunak dari sistem yang dirancang.



Gambar 3.7 Alur Penelitian)

3.3 Perancangan

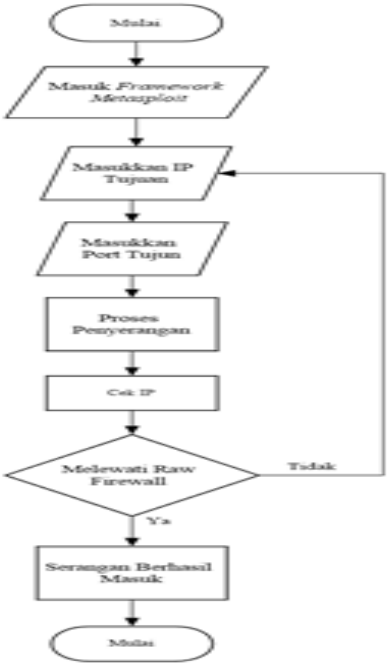
Perancangan adalah proses setelah dilakukan evaluasi. Perancangan tahap pertama yang dilakukan adalah setting jaringan menggunakan *mikrotik routerboard* susuai dengan topologi yang telah dirancang. Perancangan tahap selanjutnya yaitu melakukan *setting firewall* pada *routerboard mikrotik* untuk melakukan proteksi jaringan yang ada pada *server* dari serangan *syn flood*. Kemudian melakukan pengujian dengan melakukan penyerangan menggunakan *syn flood* pada *routerboard mikrotik*. Adapun topologi yang akan dibuat untuk menggambarkan perangkat-perangkat (*devices*) yang digunakan yaitu :



Gambar 3.8 Topologi yang digunakan

3.4 Skema Penyerangan

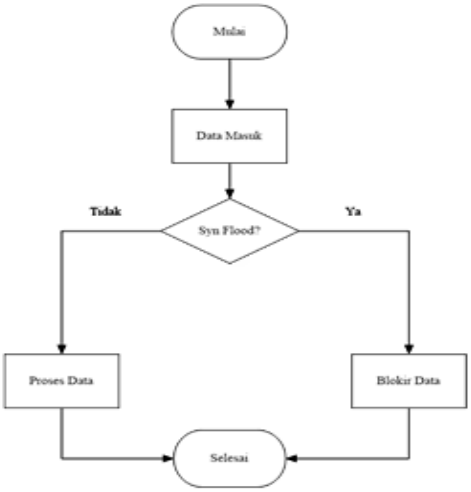
Skema penyerangan yang digunakan dalam pengujian ini yaitu menggunakan *Framework Metasploit* pada sistem operasi *Kali Linux*. Pada proses ini *Framework Metasploit* akan melancarkan serangan *Syn Flood* langsung ke target jaringan *Router* yang diserang. Dengan memasukkan IP target dan *port* yang akan dilakukan penyerangan. Jika penyerangan berhasil menembus sistem keamanan pada *Router* maka serangan berhasil dilakukan. Jika tidak maka ulangi proses yang sama yaitu dengan memasukkan alamat *ip* dan *port* dari target yang akan dilakukan penyerangan. Seperti dijelaskan pada *FlowChart* dibawah ini.



Gambar 3.10 *Flow Chart* Penyerangan Menggunakan *Metasploit*

3.5 Skema Penanganan

Langkah penanganan terhadap serangan yang dilakukan yaitu dengan menggunakan *Firewall Raw* sebagai sistem keamanan yang diterapkan dalam melakukan pencegahan terjadinya serangan *Syn Flood*. *Firewall Raw* akan memeriksa data yang diterima dan melacak koneksi yang dibuat untuk menentukan data apakah koneksi tersebut diizinkan atau ditolak. Data yang ditolak adalah data yang dikirimkan *port* yang telah diblokir aksesnya oleh *Firewall Raw*. Lalu *firewall* akan memblokir alamat *ip* yang tidak dizinkan tersebut jika mencoba melakukan *request*. Data yang diizinkan masuk kedalam jaringan yaitu data yang dikirimkan oleh *port* yang tidak diblokir oleh *Firewall Raw*. Adapun skema penanganan menggunakan *Firewall Raw* dapat dilihat pada *FlowChart* berikut.



Gambar 3.11 *FlowChart* Penanganan Menggunakan *Firewall Raw*

4. HASIL PENELITIAN DAN PEMBAHASAN

Pada penelitian ini akan menjelaskan beberapa hal yang diperoleh dari proses penelitian yang telah dilakukan berdasarkan rumusan masalah, batasan masalah dan tujuan penelitian yang telah diajukan sebelumnya.

4.1 Konfigurasi pada *MikroTik Router*

Tahap pertama yang harus dilakukan sebelum melakukan serangkaian pengujian yaitu melakukan konfigurasi pada *Router* dengan menggunakan aplikasi *winbox* supaya bisa terkoneksi ke internet serta tidak lupa menerapkan rancangan yang sudah dibuat sebelumnya. Berikut adalah detail konfigurasi yang dirancang.

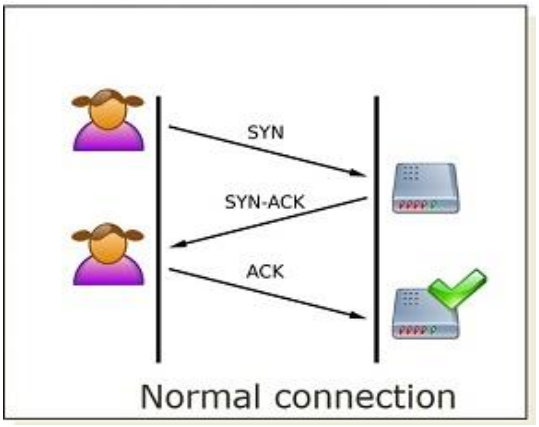
4.2 Persiapan Skenario Pengujian Serangan *Syn Flood.*

4.2.1 Gambaran Simulasi Serangan pada *Router*

SYN Flood adalah merupakan salah satu bentuk serangan *Denial Of Service (DOS)* dimana penyerang akan mengirimkan *SYN request* kepada mesin sasaran dengan tujuan mengkonsumsi sumber daya dari *server* yang bertujuan untuk membanjiri *connection limit* tersebut, jika berhasil memenuhi *connection limit*, maka user yang lainnya akan kehabisan dan tidak dapat terkoneksi ke dalam *Server*, karena koneksi sudah penuh. Pada dasarnya ketika suatu *computer* terhubung kepada *server* maka akan terjadi yang namanya koneksi TCP ke *server*, kemudian *client* dan *server* saling bertukar Informasi yang pada umumnya berlaku seperti ini:

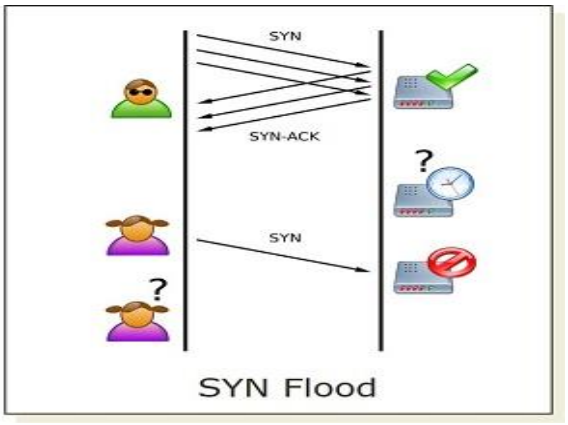
1. *Client* meminta koneksi ke *server* dengan mengirimkan kode *SYN (Synchronize)* ke *server.*
2. *Server* mengenali atau mengakui (*acknowledges*) *request* ini dengan mengirimkan kode *SYN-ACK* kembali ke *client.*
3. *Client* merespon kembali dengan mengirimkan kode *ACK* dan hasilnya koneksi terjalin antara *client* dan *server*.

Ini yang dikenal dengan nama *TCP Three Way Handshake*, yang merupakan dasar dari semua koneksi yang menggunakan protokol TCP. Seperti gambar berikut.



Gambar 4.20 *TCP Three Way Handshake*

Namun didalam kasus *SYN Flood*, kode *ACK* (Fase 3) tidak pernah di kirimkan kembali kepada *server* malah justru mengulangi *SYN request* ke *server*. *Client* membuat semua *SYN request* tampak valid namun karena IP yang dikirim adalah IP palsu maka tidaklah mungkin *server* untuk kemudian mengakhiri koneksi tersebut. Akibatnya koneksi masih tetap terbuka (setengah terbuka) sehingga koneksi tidak juga terjalin (tertutup) antara *client* dan *server*. Demikian seterusnya, lama kelamaan *server* akan menjadi sangat sibuk untuk merespon *resquest* yang tidak berujung, bahkan pada akhirnya *client* yang sah pun akan kesulitan masuk untuk terhubung ke *server*.



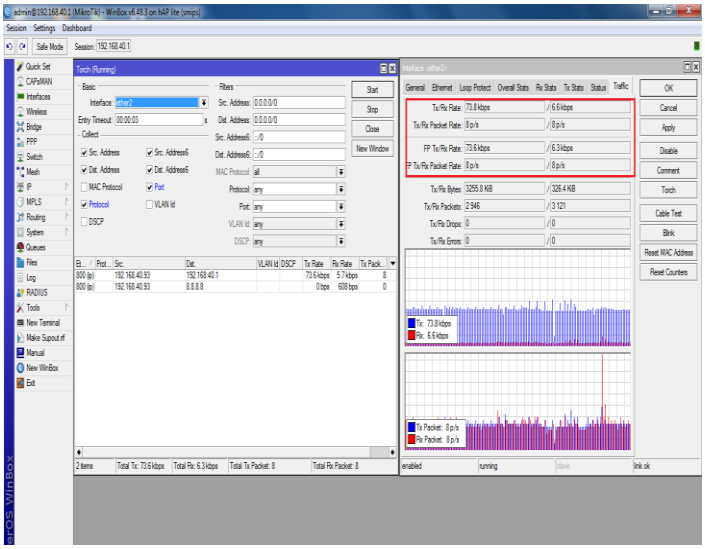
Gambar 4.21 *SYN Flood*

4.2.2 Analisis Serangan *Syn Flood* pada *Router*

Proses awal untuk analisis apakah *Router* masih dalam keadaan normal atau belum ada serangan DoS, dapat dilakukan pemantauan menggunakan menu yang tersedia pada *WinBox*, yaitu seperti menu *Trafic, Torch,* dan *Resources*. menu *Trafic* adalah alat untuk memonitor berbagai parameter *Router* dari waktu ke waktu dan menempatkan data yang dikumpulkan kedalam bentuk grafik. Hal ini dapat dilihat pada grafik yang dikategorikan menjadi *Tx (Transmitted Rate)* dan *Rx (Received Rate). Transmitted Rate* ini diartikan sebagai jumlah data yang keluar dari *Router* melalui *interface.* Sedangkan *Received Rate* adalah data yang diterima / masuk ke *Router* melalui *interface.* Menu *Torch* merupakan *tools Realtime Traffic Monitor* yang digunakan untuk pemantauan lalu lintas yang akan melalui sebuah *interface*.

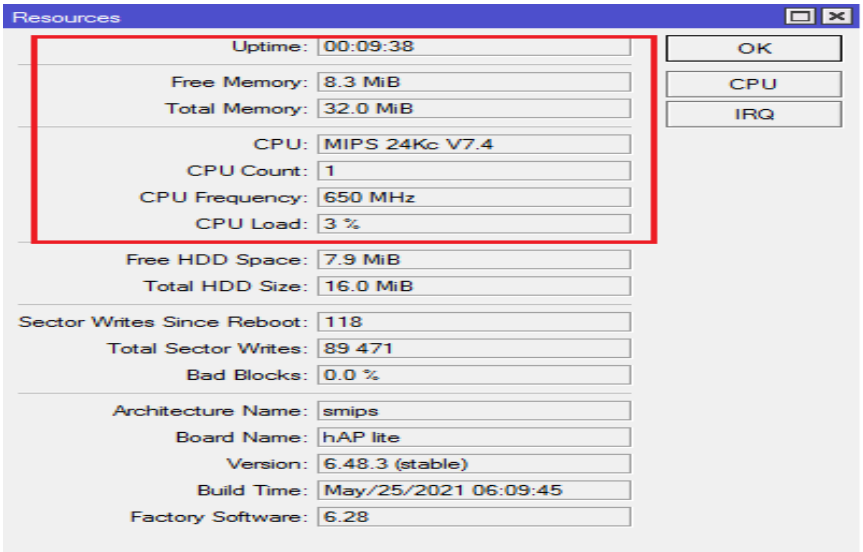
Anda dapat memonitor trafik berdasarkan protokol, IP Sumber, IP tujuan, dan *port*. Sehingga dari *tools*nya dengan mudah kita mendapatkan informasi perihal trafik yang ada dari IP mana saja dan menuju ke IP mana dengan *port* berapa dan protokol apa beserta besaran nilai Rx/Txnya. Menu *Resources* berfungsi untuk melihat semua informasi mengenai sistem yang kita gunakan pada *OS Mikrotik* itu sendiri mulai dari versi OS yang dipakai, model *Hardware* yang dipakai, Load Cpu yang digunakan, kapasitas HDD dan *memory* dan informasi lainnya yang sangat kita butuhkan. Berikut adalah tampilan keadaan *Router* sebelum dilakukan penyerangan.

Tampilan sebelum dilakukan penyerangan :



Gambar 4.22 Tampilan *Trafic* Sebelum Terjadi Serangan

Dari gambar, dapat dilihat pada menu *Trafic* bahwa kodisi grafik data yang masuk ke *router* dalam keadaan normal dan belum ada serangan yang masuk dan mengganggu lalu-lintas jaringan pada *Router*. Seperti terlihat pada grafik yang tampak normal dimana nilai *Tx/Rx Rate* yaitu 73.8 kbps 6.6 kbps dan nilai *Tx/Rx Packet* yaitu 8 p/s / 8 p/s. Ini menunjukkan adanya komunikasi antara *client* dengan *Router* yang berjalan normal. Sedangkan pada menu *Torch* yang digunakan untuk memantau arus lalu lintas terlihat normal. Dan pada menu *resource* terlihat persentase *Cpu Load* adalah 1 % dan *Free Memory* 7.0 MiB belum bergerak secara signifikan karena belum terjadi transaksi serangan *DoS* yang dapat mempengaruhi kinerja atau *Load* pada jaringan *router*, seperti terlihat pada gambar berikut.



Gambar 4.23 Tampilan *Resources* Sebelum Terjadi Serangan

4.2.3 Pengujian Menggunakan Aplikasi

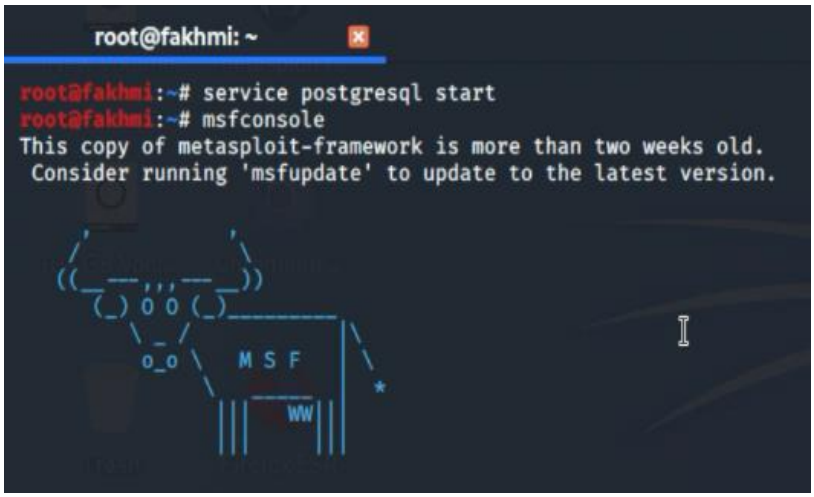
Proses pengujian dilakukan menggunakan *Framework Metasploit* pada sistem operasi *Kali Linux*. Pada proses ini *Framework Metasploit* akan melancarkan serangan *Syn Flood* langsung ke target jaringan *Router* yang diserang. Adapun langkah-langkah yang dilakukan untuk melakukan serangan adalah sebagai berikut.

```
root@fakhmi:~# service postgresql start
root@fakhmi:~# msfconsole
msf6 > search synflood
msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > show options
msf6 auxiliary(dos/tcp/synflood) > set RHOST 192.168.40.1
msf6 auxiliary(dos/tcp/synflood) > set RPORT 53
msf6 auxiliary(dos/tcp/synflood) > set TIMEOUT 1000
msf6 auxiliary(dos/tcp/synflood) > show options
msf6 auxiliary(dos/tcp/synflood) > exploit
```

Exploit code script

1. Menjalankan *Framework Metasploit*.

Proses awal yang dilakukan yaitu dengan menjalankan *framework metasploit* dengan menggunakan perintah ***service postgresql start*** untuk menjalankan *database postgresql* pada *metasploit* dan perintah ***msfconsole*** untuk menjalankan *framework metasploit*, seperti pada gambar berikut.



Gambar 4.24 Tampilan Menjalankan *Metasploit*

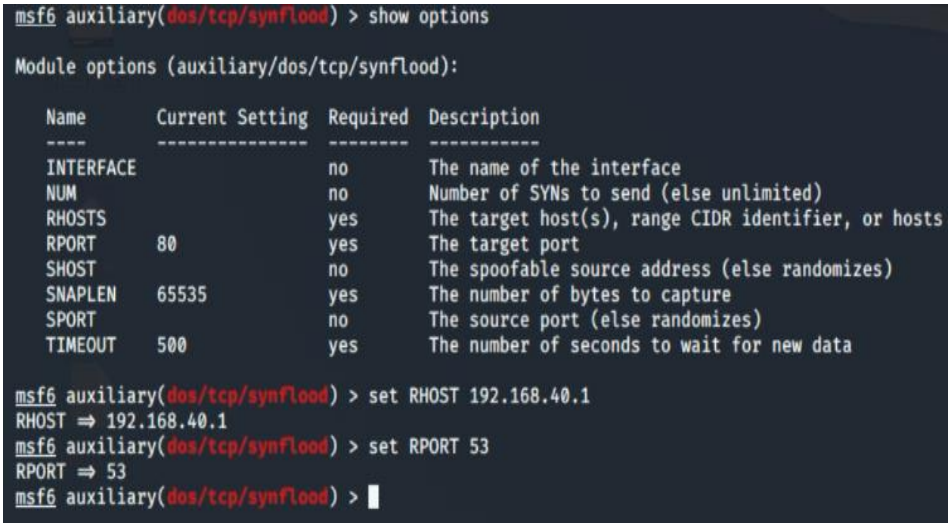
2. Mencari *Module*

Tahap selanjutnya yang dilakukan yaitu mencari lokasi *module syn flood* pada *metaslpoit* dengan menggunakan perintah ***search synflood***, dan perintah ***use*** untuk menentukan *module* yang digunakan. seperti terlihat pada gambar berikut. Perintah ini digunakan.

Gambar 4.25 Tampilan Mencari *Module*

3. Melihat pilihan pada *Module*

Untuk melihat pilihan *module* atau *exploit* yang tersedia dapat menggunakan perintah ***show options*** kita bisa menggunakan seluruh menu yang disediakan. Tapi pada uji coba ini penulis hanya menggunakan **RHOST** untuk menentukan ip target dan **RPORT** untuk menentukan *port* taget yang akan dilakukan penyerangan. Untuk menentukan Ip dan *port* target menggunakan perintah ***set***, seperti pada gambar berikut.



Gambar 4.26 Tampilan Menentukan Target

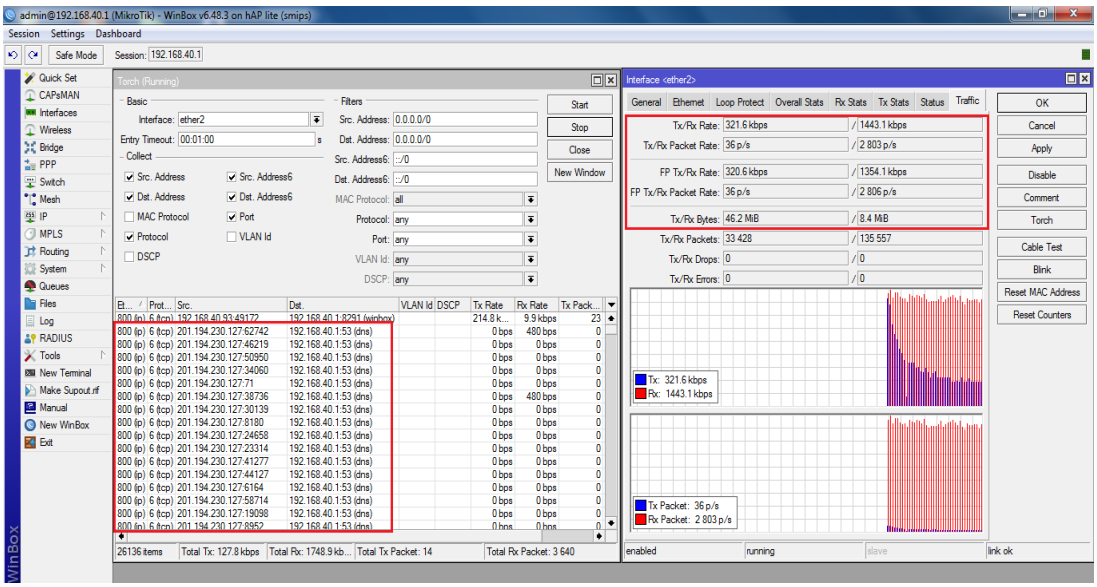
4. Melancarkan Penyerangan

Selanjutnya adalah melancarkan serangan setelah dilakukan pengaturan pada menu-menu yang tersedia. Untuk melakukan penyerangan dapat menggunakan perintah ***exploit***, seperti pada gambar berikut.

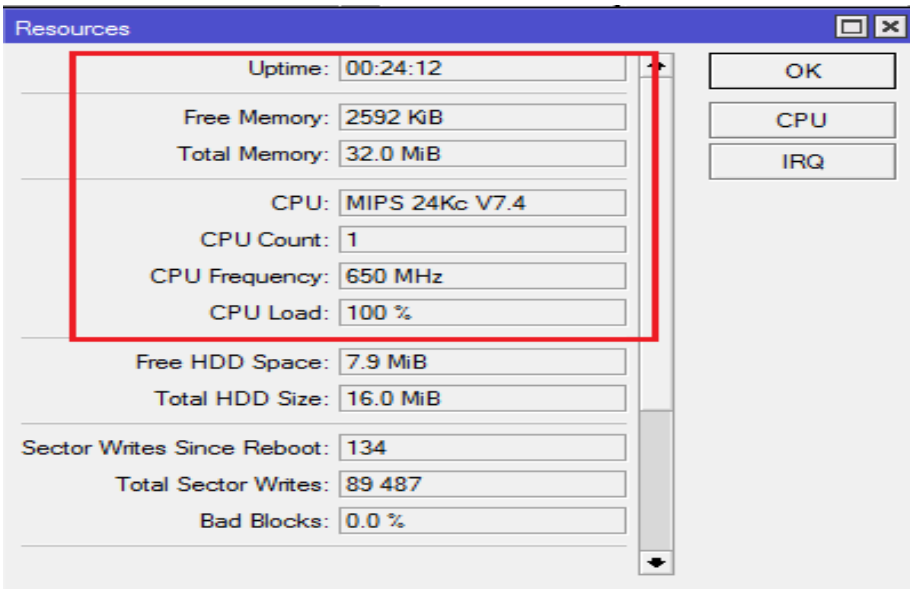
Gambar 4.27 Tampilan Melancarkan Serangan

Setelah melakukan penyerangan langkah selanjutnya adalah melihat keadaan *trafic* seperti pada gambar 4.25, terlihat bahwa *Trafic* yang terlihat tidak normal dimana nilai *Tx/Rx Rate* yaitu 321.6 kbps / 1443.1 kbps dan nilai *Tx/Rx Packet* yaitu 36 p/s / 2803 p/s. Hal ini dapat diartikan bahwa perangkat *router* dari segi *interfaces* maksimal hanya mampu melewatkan data yang *direques*t oleh *user* sebesar 100 Mbps pada *interface router* tersebut. Sedangkan dampak serangan DoS ini menyebabkan *interface* sudah melewatkan data sebesar 46.2 Mbps. Ini menandakan bahwa *traffic* sudah tidak bisa lagi melewatkan permintaan akses *user* terhadap *server* yang melalui *router* tersebut.

Tampilan *Trafic* saat dilakukan penyerangan:



Ketika terjadi serangan DoS yang masuk pada jaringan *router*, *Load CPU* dan *memory* meningkat. meningkat. Berdasarkan hasil *Traffic Monitor System* setelah terjadi serangan DoS diketahui *Traffic System Monitor Packet* data *CPU Load* meningkat menjadi 100% dan *Memory* 2592 KiB naik secara signifikan. Hal ini yang menyebabkan *down* pada *Network Traffic* akibat serangan *DoS* pada *router*. Dapat dilihat pada gambar berikut.

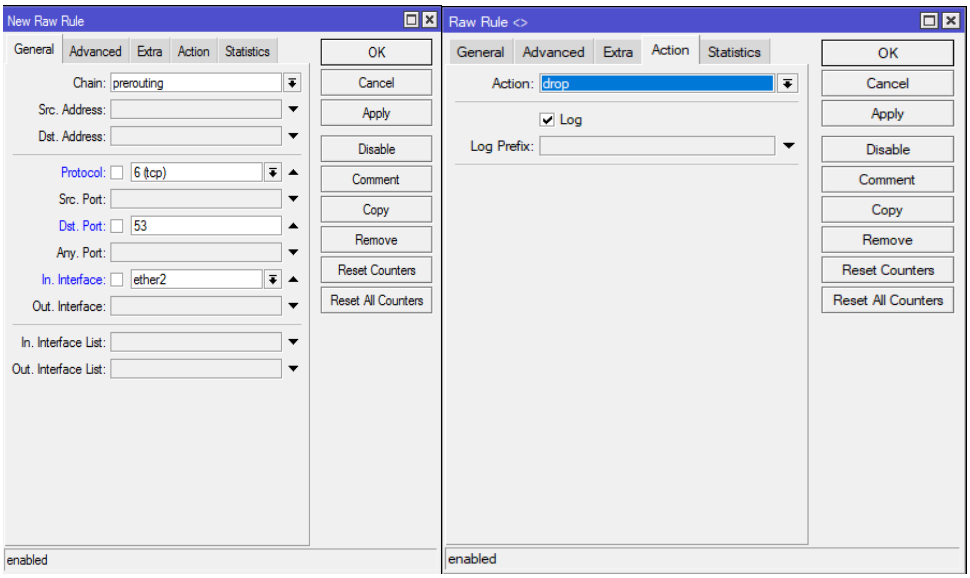


Gambar 4.29 Tampilan Menu *Resources* Saat Penyerangan

4.2.4 Peningkatan Keamanan *Router MikroTik*

Dari permasalahan diatas penulis mengambil tindakan untuk melakukan peningkatan keamanan terhadap *Router* yaitu dengan menggunakan fitur *Firewall Raw* pada *Router MikroTik*. *RAW* merupakan tabel *firewall* yang mirip dengan tabel filter yakni menangani *filtering* paket. Namun *Raw* memiliki keunggulan yaitu tidak memakan *resource* cpu sebanyak pada *firewall filter*. *Firewall Raw* sangat efektif dalam melakukan pengamanan pada serangan yang terjadi pada *Router MikroTik*. Berikut adalah hasil dari pengujian serangan *Syn Flood* setelah menggunakan fitur *Firewall Raw*.

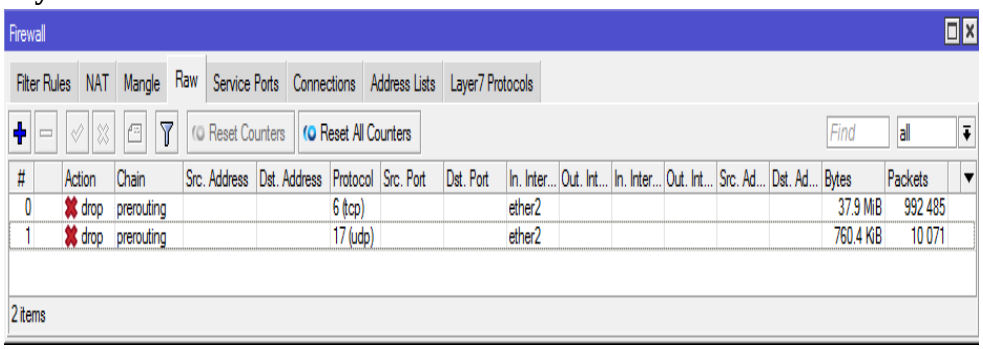
Adapun Langkah-langkah untuk menjalankan *tools Firewall Raw* yaitu dengan menuju ke menu *IP* > *Firewall* > *Raw*, seperti gambar berikut, untuk konfigurasinya bisa dilihat pada gambar berikut.



Gambar 4.30 Tampilan Pengaturan *General* pada *New Raw Rule*

Lakukan pengaturan yang sama pada protokol yang lainnya. Dan setelah beberapa parameter telah di-*input*, maka akan menghasilkan *Firewall Raw* seperti yang terlihat pada gambar berikut.

Hasilnya :

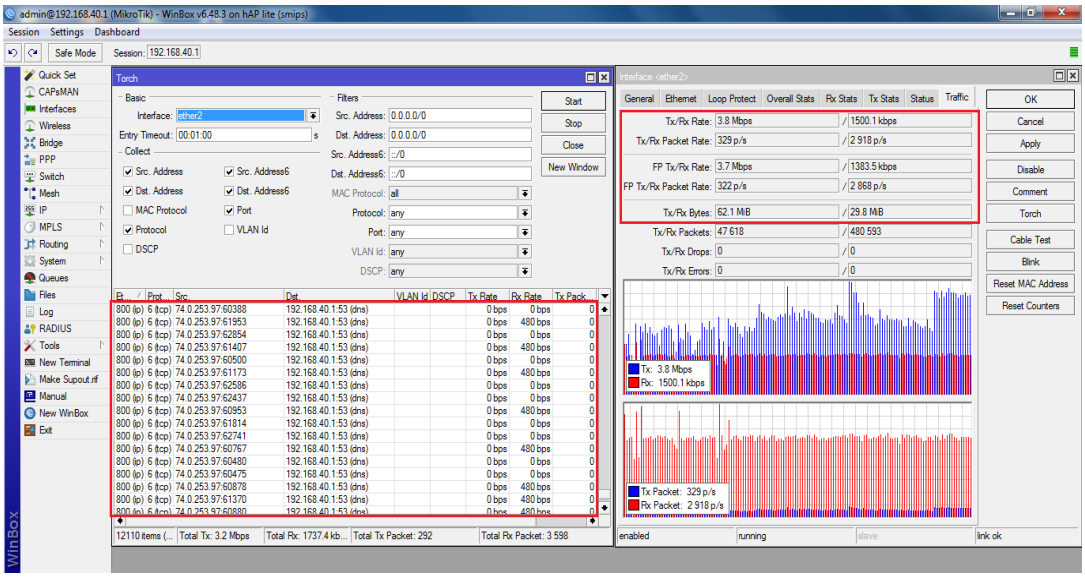


Gambar 4.31 Tampilan Paket Data yang Diblokir *Firewall Raw*

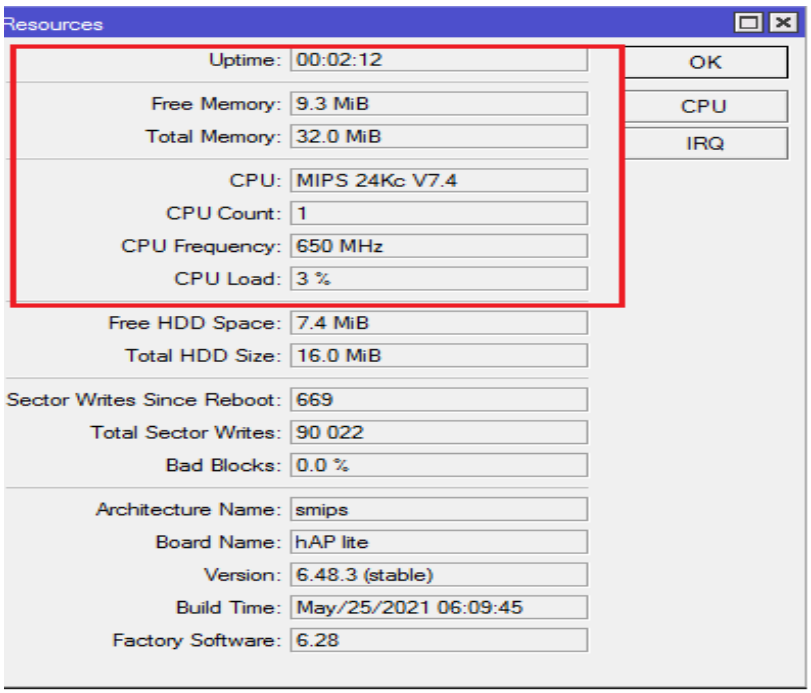
Terlihat pada gambar diatas bahwa penulis mengkonfigurasi 2 jenis protokol yang di blokir oleh *Firewall Raw*, yaitu protokol tcp dan protokol udp. Hal ini berarti, ketika penyerang mengirim paket data secara bertubi-tubi, *Firewall Raw* dapat mencegah serangan tersebut dengan cara memblokir *IP Address* yang dicurigai sebagai penyerang sehingga koneksi jaringan penyerang terputus terhadap *Router*.

Selanjutnya dilakukan pengujian setelah menggunakan *Firewall Raw* pada gambar 4.28 dapat dilihat bahwa pada menu *Trafic* yang memang terlihat tidak normal dimana nilai *Tx/Rx Rate* yaitu 3.8 Mbps / 1500.1 kbps dan nilai *Tx/Rx Packet* yaitu 329p/s / 2918p/s. Hal ini disebabkan karena serangan yang dilakukan tetap tercatat masuk kedalam grafik tetapi *request* yang dilakukan tidak diterima oleh *Router* karena protokol yang masuk yaitu protokol *tcp* dan *udp* yang sudah di-*drop* oleh *Firewall Raw* tersebut merupakan data yang ditolak untuk masuk ke jaringan *Router*.

Tampilan setelah menggunakan *Firewall Raw*:



Hal ini membuktikan bahwa *Firewall Raw* mampu memblok data-data yang dicurigai dikirim oleh penyerang pada jaringan *Router*. Sehingga jaringan *Router* tidak mengalami *down* seperti sebelum menggunakan *Firewall Raw*. Perubahan yang terjadi pada jaringan *Router* ketika menggunakan *Firewall Raw* dapat dilihat pada gambar berikut.



Gambar 4.33 Tampilan Setelah Menggunakan *Raw Firewall*

Pada gambar 4.30, terlihat *CPU Load* dari 100% turun menjadi 3% setelah menggunakan *Firewall Raw*. Dapat disimpulkan bahwa *Firewall Raw* dapat mencegah serangan DoS dalam hal ini adalah serangan *Syn Flood* sehingga tidak terjadi *Router down*.

4.2.5 Analisa Hasil

Berdasarkan hasil pengujian yang telah dilakukan yaitu melakukan serangan DoS serta peningkatan keamanan pada *Router Mikrotik* menggunakan *Firewall Raw*, maka hasil penelitian tersebut disajikan dalam bentuk tabel berdasarkan proses yang telah dilakukan. Hasil analisis dirangkum pada tabel 4.1 berikut.

Tabel 4.1 Hasil Analisis Serangan DoS dan Peningkatan Keamanan pada *Router Mikrotik*

No.	Analisis	Keterangan
1	Serangan *Syn Flood* pada router menggunakan *Framework Metasploit* pada *Kali Linux.*	Berhasil melakukan serangan pada jaringan *router* secara bertubi-tubi hingga membuat jaringan menjadi *down*.
2	Protokol serangan yang berhasil tembus	Protokol *TCP* dan *UDP*
3	*Port Destination* target	Port 53
4	Kondisi CPU dan *Memory* perangkat jaringan sebelum diserang	*CPU Load* 3% *Memory* 8.3 Mib

No.	Analisis	Keterangan
5	Kondisi *CPU* dan *Memory* perangkat jaringan setelah diserang .	*CPU Load 100% Memory 2592 Kib*
6	*Log Activity*	Terdapat kegagalan *login* yang cukup banyak. Aktivitas ini dicurigai sebagai aktivitas yang tidak wajar yang melakukan komunikasi data pada *Protocol* DNS dengan IP 201.194.230.12 terhadap *Router* dengan IP jaringan lokal 192.168.40.1
7	a. *IP Address List* Penyerang *b. IP Router Mikrotik* *c. IP Network Administrator* *d. IP Router to ISP (Internet Services Provider)* *f. IP Gateway Internet to ISP*	a. 201.194.230.12 b. 192.168.40.1 c. 192.168.1.0 d. 192.168.1.2 f. 192.168.1.1
8	Peningkatan Keamanan *Router Mikrotik*	Menggunakan *Firewall Raw*.
9	Kondisi *CPU* dan *Memory* perangkat jaringan setelah menggunakan *Firewall Raw*	*CPU Load* turun menjadi 3% Memory 9.3 Mib

5. KESIMPULAN DAN SARAN

5.1 KESIMPULAN

Berdasarkan hasil pengujian dari pemanfaatan *Router MikroTik* sebagai media keamanan jaringan dari *Syn Flood* dengan menggunakan *Firewall Raw* dapat disimpulkan bahwa penggunaan *Firewall Raw* pada *RouterBoard MikroTik* sangat efektif dalam melakukan pengamanan sistem jaringan dari serangan-serangan salah satunya seperti *Syn Flood* yang melakukan serangan dengan melakukan pengiriman paket *SYN request* kepada mesin sasaran dengan tujuan mengkonsumsi sumber daya dari *server* yang bertujuan untuk membanjiri *connection limit* pada *router* target. *Firewall Raw* berfungsi untuk memblokir *IP* yang dicurigai mengirim *pack*et data tidak wajar pada jaringan *router*. Hal ini tentu sudah mencapai tujuan dari penulis yaitu meningkatkan sistem keamanan jaringan dengan menggunakan *Router MikroTik* yang membantu dalam mengamankan dan meningkatkan perlindungan pada jaringan di Sekolah Menengah Kejuruan Negeri 3 Bengkalis.

5.2 SARAN

Adapun saran dari penulis mengenai peningkatan keamanan *Router MikroTik* terhadap serangan *Syn Flood* dengan menggunakan *Firewall Raw* adalah sebagai berikut :

1. Peningkatan keamanan *Router MikroTik* terhadap serangan *Syn Flood* dengan menggunakan *Firewall Raw* di Sekolah Menengah Kejuruan Negeri 3 (SMKN 3) Bengkalis ini hanya mencangkup jaringan kecil yang berada dilingkup SMKN 3 Bengkalis saja. Kedepan diharapkan agar dapat dikembangkan lingkup penelitiannya.
2. Penigkatan keamanan *Router MikroTik* terhadap serangan *Syn Flood* dengan menggunakan *Firewall Raw* di Sekolah Menengah Kejuruan Negeri 3 (SMKN 3) Bengkalis ini hanya mengatasi satu jenis serangan saja yaitu serangan *Syn Flood.* Kedepan diharapkan bisa diterapkan metode penyerangan yang lain agar bisa meningkatkan sistem keamanannya pula.
3. Penigkatan keamanan *Router MikroTik* terhadap serangan *Syn Flood* dengan menggunakan *Firewall Raw* di Sekolah Menengah Kejuruan Negeri 3 (SMKN 3) Bengkalis ini pada proses penyerangannya hanya menggunakan 1 (satu) jenis *port* penyerangan saja yaitu *port* 53, diharapkan untuk penelitian selanjutnya dapat menggunakan jenis port yang lain.

6. DAFTAR PUSTAKA

Aprilianto, Doni, Triyana, F. dan Muslim, A. (2017). Sistem pencegahan UDP DNS Flood dengan filter Firewall pada router Mikrotik. *Jurnal Techno.COM,* 16(2).

Ariyus, D. (2005). *Kamus Heacker.* Andi, Yogyakarta

Astari, A. (2018). Implementasi Keamanan Jaringan Dengan Metode Firewall Filtering Menggunakan Mikrotik. *Jurnal Universitas Nusantara PGRI Kediri.*

Baytar, P. (2020). Pemanfaatan Mikrotik Routerboard sebagai keamanan jaringan dari UDP Flood dengan menggunakan Firewall di Dinas Pendidikan Kabubaten Bengkalis. *Politeknik Bengkalis.*

Hendrawan, A. (2016). Analisis serangan Flooding data pada Router Mikrotik. *Jurnal Kreatif,* 04(01).

Jaya, Budi dan Yuhandri, Y. (2020). Peningkatan keamanan Router Mikrotik terhadap serangan Denial Of Service (DoS).. *Jurnal Universitas Padang.*

Kennedy, O'gorman, Kearns, dan Aharoni. (2011). *Metasploit: The Penetration Tester's Guide.* New York: s.n.

Mardiyana, Oka. (2015). Keamanan Jaringan Dengan Firewall Filter Berbasis Mikrotik Pada Laboratorium Komputer STIKOM Bali. *E JURNAL.*

Putra, A. dan Ariyadi. (2019). Implementasi Pencegahan terhadap serangan Flooding Attack TCP dan UDP di Kantor PDAM Tirta Musi Palembang. *Jurnal Universitas Bina Darma.*

Rahmadani Addy, dan M.Fahru Rizal. (2017). *Implementasi Hacking Wireless dengan Kali Linux Menggunakan Kali Nethunter*. e-Proceeding of Applied Science, 03(03), p. 1768.

Santoso, Dwi. (2020). Analisis Perbaningan Metode Queue. *Jurnal Pseudocode,* VII(1).

Shaifullah dan M. Syarif. (2018). *Desain Firewall Terhadap Serangan DDOS Pada Router Mikrotik*. Yogyakarta

Solikin, Suryayusra dan Ulfa. (2019). *Pengembangan Sistem Keamanan Jaringan Komputer Berbasis Mikrotik Pada SMK Negeri 1 Indralaya*. Indralaya Utara.

Susianto. (2016). IMPLEMENTASI QUEUE TREE UNTUK MANAJEMEN BANDWIDTH MENGGUNAKAN. *Jurnal Cendikia*, 12(01), p. 1.

YasinK, (2018). *niagahoster*.[Online]
Available at: https://www.niagahoster.co.id/blog/ddos-adalah/