IMPLEMENTASI PENCEGAHAN TERHADAP SERANGAN FLOODING ATTACK TCP DAN UDP DI KANTOR PDAM TIRTA MUSI PALEMBANG

[1]Abriansya Putra,[2]Tamsir Ariyadi
[1]Teknik Komputer, Fakultas Vokasi, Universitas Bina Darma, abriansya.putra@gmail.com
[2]Teknik Komputer, Fakultas Vokasi, Universitas Bina Darma, tamsirariyadi@binadarma.ac.id

Abstract *- Tirta Musi Regional Drinking Water Company (PDAM) Palembang was a Regional-Owned Enterprise (BUMD) which served to provide drinking water supply services to the Citizens. Problems that often occur in computer network security systems in PDAM Tirta Musi Palembang were frequent flooding attacks on devices router in the company. Flooding attacks could be overcome in various ways, especially on the router microtic device, one of the problem was by filtering on the firewall. . Although firewalls couldn't prevent all attacks, at least more firewalls could help make data safer than without firewalls at all. The purpose of the research were: 1. To prevent microtic-based flooding attack in PDAM Tirta Musi Palembang. 2. To increase network security at PDAM Tirta Musi Palembang. This research was held in May 2018 to August 2018 by conducting The research at PDAM Tirta Musi Palembang that was located in Rambutan Ujung Street No.1 Palembang. The conclusion of this study had been conducted a simulation to prevent TCP and UDP flooding attacks by using firewall filter method. Prevention of TCP flooding attack was successfully blocked overall, while the firewall filter in the UDP protocol successfully blocked but not as a whole. With the firewall filter method the threat of attack flooding could be minimized.*

Keywords: *Flooding Attack, Filter Firewall,* TCP, UDP

Abstrak - Perusahaan Daerah Air Minum (PDAM) Tirta Musi Palembang merupakan Badan Usaha Milik Daerah (BUMD) yang befungsi untuk memberikan pelayanan penyediaan air minum kepada masyarakat .Permasalahan yang sering terjadi pada sistem keamanan jaringan komputer di PDAM Tirta Musi Palembang adalah sering terjadi serangan *flooding* pada perangkat *router* di perusahaan tersebut.Serangan *flooding* dapat di atasi dengan berbagai cara khususnya pada perangkat *router mikrotik* salah satunya yaitu dengan memfilter pada *firewall*. Meskipun *firewall* tidak dapat mencegah semua serangan, *firewall* setidaknya lebih dapat membantu membuat data aman daripada tanpa *firewall* sama sekali. Adapun tujuan penelitian yang dilakukan oleh peneliti adalah sebagai berikut :1.Untuk mencegah serangan *flooding attack* berbasis *mikrotik* di PDAM Tirta Musi Palembang.2.Untuk meningkatkan *security* keamanan jaringan di PDAM Tirta Musi Palembang Penelitian ini dilakukan pada bulan Mei 2018 sampai Agustus 2018 dengan melakukan penelitian di PDAM Tirta Musi Palembang yang berlokasi di jalan Rambutan Ujung No.1 Palembang kesimpulan penelitian ini Telah dilakukan simulasi pencegahan serangan *flooding attack* TCP dan UDP menggunakan metode *filter firewall.*Pencegahan serangan *flooding attack* pada *protocol* TCP berhasil di *block* secara keseluruhan, sedangkan *filter firewall* pada protocol UDP berhasil di *block* tetapi tidak secara keseluruhan.Dengan adanya metode *filter firewall* ancaman serangan *flooding attack* dapat diminimalisir.

Kata Kunci: *Flooding Attack, Filter Firewall,* TCP, UDP

1. Pendahuluan

Perusahaan Daerah Air Minum (PDAM) Tirta Musi Palembang merupakan Badan Usaha Milik Daerah (BUMD) yang befungsi untuk memberikan pelayanan penyediaan air minum kepada masyarakat . Jaringan *internet* berperan penting untuk meningkatkan operasional maupun kinerja .Salah satu permasalahan yang sering terjadi pada sistem keamanan jaringan komputer di PDAM Tirta Musi Palembang adalah sering terjadi serangan *flooding* pada perangkat *router*. *Flooding*

adalah sejenis serangan *Denial of Service* (DOS), dimana *flooding* melakukan serangan terhadap sebuah komputer atau *server* di dalam jaringan lokal maupun *internet* [1].

Flooding adalah sejenis serangan *Denial of Service* (DOS), dimana *flooding* melakukan serangan terhadap sebuah komputer atau *server* di dalam jaringan lokal maupun *internet* dengan cara menghabiskan sumber (*resource*) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut [1].

Serangan *flooding* dapat di atasi dengan berbagai cara khususnya pada perangkat *router mikrotik* salah satunya yaitu dengan memfilter pada *firewall* semua *service* TCP dan UDP yang masuk. *Firewall* melakukan *filter* dengan memeriksa data yang diterima dan melacak koneksi yang dibuat untuk menentukan data apakah koneksi tersebut diijinkan atau ditolak. *Firewall* dapat juga bertindak sebagai perantara dan permintaan *proxy host* yang dilindungi, sementara pada saat yang sama menyediakan sarana otentikasi akses untuk lebih memastikan bahwa hanya perangkat akses diberikan. Meskipun *firewall* tidak dapat mencegah semua serangan, *firewall* setidaknya lebih dapat membantu membuat data aman daripada tanpa *firewall* sama sekali.

2. Tinjauan Pustaka

2.1 Implementasi

Implementasi adalah suatu hal yang bermuara pada aksi, aktivitas, tindakan serta adanya mekanisme dalam suatu sistem. Implementasi tidak hanya aktivitas yang monoton namun suatu kegiatan yang terencana dengan baik untuk mencapai tujuan kegiatan tertentu [2].

2.2 Pencegahan

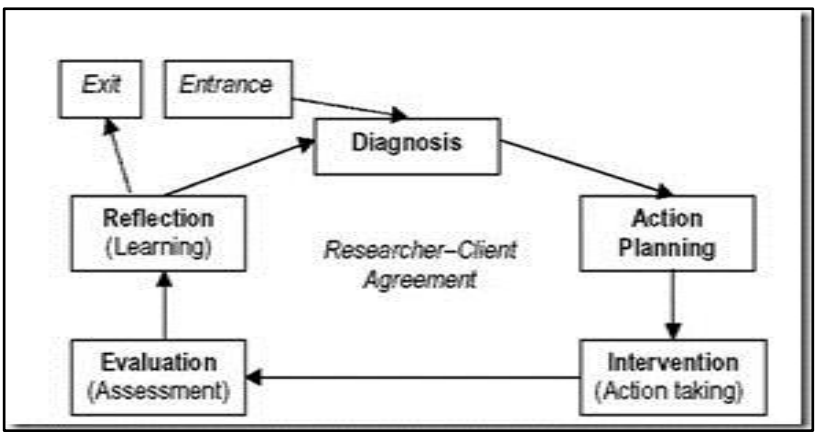
Pencegahan adalah mengambil sesuatu tindakan yang diambil terlebih dahulu sebelum kejadian, dengan didasarkan pada data/keterangan yang bersumber dari hasil pengamatan/ penelitian epidemiologi [3].

2.3 *Flooding Attack*

Flooding adalah sejenis serangan *Denial of Service* (DOS), dimana *flooding* melakukan serangan terhadap sebuah komputer atau *server* di dalam jaringan lokal maupun internet dengan cara menghabiskan sumber *(resource)* yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehinnga secara tidak langsung mecegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut [4].

3. Metodologi Penelitian

3.1 Metode Pengembangan Sistem



Gambar 1. Siklus *Action Research*

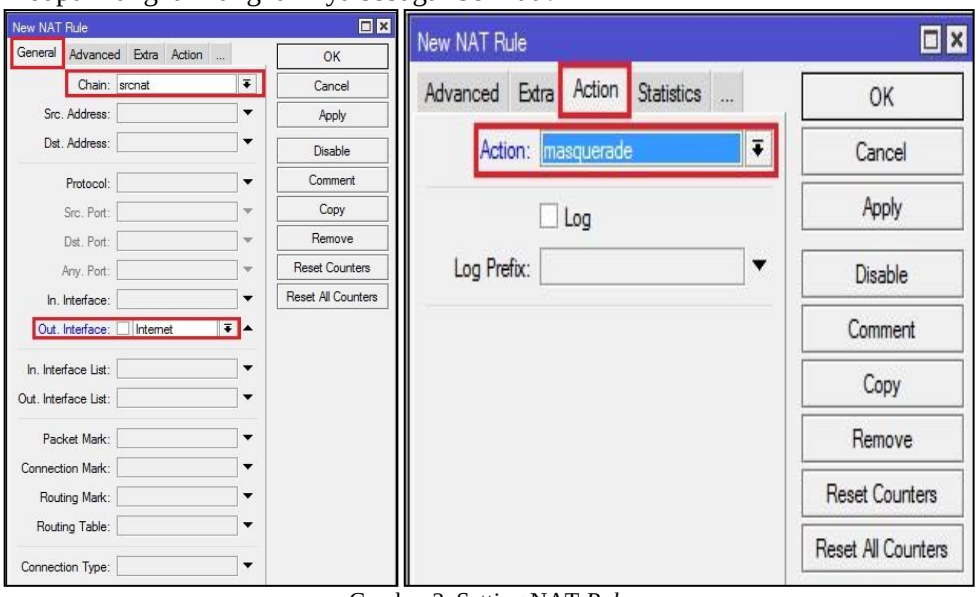
Penelitian tindakan, sebagai sebuah metode penelitian, didirikan atas asumsi bahwa teori dan praktik dapat secara tertutup diintegrasikan dengan pembelajaran dari hasil intervensi yang direncanakan setelah diagnosis yang rinci terhadap konteks masalahnya [5]. Dalam penelitian ini penulis menggunakan metode *Action Research* dibagi dalam beberapa tahapan yaitu :

1. Melakukan Diagnosa (*diagnosing*)
   Melakukan identifikasi masalah-masalah pokok yang ada guna menjadi dasar kelompok atau organisasi sehingga terjadi perubahan. Pada tahap ini peneliti melakukan diagnosa permasalahan yang terdapat pada jaringan *internet* di PDAM Tirta Musi Palembang.
2. Membuat rencana tindakan (*action planning*)
   Memahami pokok permasalahan yang ada kemudian dilanjutkan dengan menyusun rencana tindakan yang tepat. Pada tahap ini peneliti melakukan rencana tindakan yang akan dilakukan yaitu mempersiapkan alat dan bahan serta melakukan perancangan topologi jaringan yang akan dilakukan pencegahan terhadap serangan *flooding attack* di PDAM Tirta Musi Palembang.
3. Melakukan tindakan (*action taking*)
   Pada tahap ini peneliti mengimplementasikan rencana tindakan dengan melakukan konfigurasi pada *mikrotik* untuk mencegah serangan *flooding attack.*
4. Melakukan evaluasi (*evaluating*)
   Peneliti melakukan evaluasi dari hasil implementasi yang telah dilakukan. Pada tahap ini dilihat bagaimana hasil dari konfigurasi pencegahan terhadap serangan *flooding attack* TCP dan UDP di PDAM Tirta Musi Palembang.
5. Pembelajaran (*learning*).

4. Hasil dan Pembahasan

4.1 Konfigurasi Ip pada *Router* Mikrotik

Langkah pertama buka aplikasi *winbox* untuk login ke perangkat *mikrotik.* Ip yang digunakan untuk *login* ke perangkat *mikrotik* yaitu 192.168.10.1 dimana ip ini merupakan ip pada *port* 2 yang terhubung ke laptop, 2 terdapat dua buah *address list, address list* yang pertama dengan ip 192.168.1.12/24 merupakan ip *internet* yang terhubung pada port 1 yang didapat secara dinamis, sedangkan *address list* yang kedua dengan ip 192.168.10.1/24 merupakan ip LAN pada port 2 yang di *setting* secara manual di *mikrotik* yang terhubung ke laptop. Laptop yang pertama hanya berfungsi untuk memantau aktifitas serangan melalui winbox yang nantinya akan dilakukan. Langkah selanjutnya penulis mengaktifkan fitur NAT, agar port 2 dapat terhubung ke jaringan internet. Adapun langkah-langkah nya sebagai berikut :

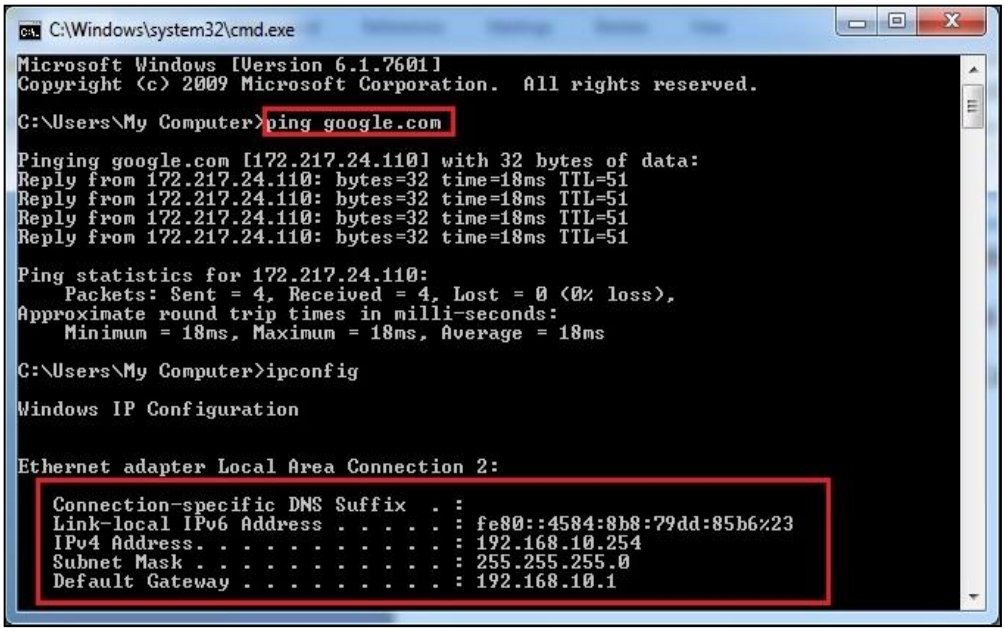


Gambar 2. Setting NAT *Rule*

Berdasarkan gambar 2, pada *tab General* di menu *Chain* pilih *srcnat*, dan di menu *Out Interface* pilih *interface* mana yang terhubung ke jaringan *internet*. Pada tahap ini *port* yang terhubung ke jaringan *internet* terletak di *port* 1 dengan nama *interface* nya yaitu "*Internet*". Oleh karena itu penulis memilih *Out interface* nya yaitu *interface internet*. Kemudian pada *tab Action* pilih *masquerad*e lalu klik Ok.

4.2 Koneksi Pada Laptop

Langkah selanjutnya penulis melakukan uji coba apakah laptop yang terhubung pada port 2 telah dapat melakukan akses ke jaringan internet dengan melakukan ping google.com melalui *command* prompt. Berikut ini hasil screenshoot bahwa port 2 telah berhasil melakukan akses ke jaringan internet.



Gambar 3. Hasil Uji Test Akses Jaringan *Internet*

Berdasarkan gambar 3, *port* 2 telah berhasil terhubung ke akses jaringan *internet*. Adapun ip perangkat laptop yang digunakan yaitu 192.168.10.254 *subnet mask* 255.255.255.0 dan *gateway* nya 192.168.10.1.

4.3 Konfigurasi *Filter Firewall* Pada *Mikrotik*

a. *Filter Firewall* TCP

Langkah pertama klik ip > *firewall* > pada *tab filter rules* klik tanda (+) untuk membuat konfigurasi baru. pada *tab General* di menu *Chain* dipilih *input*, pada menu *Protocol* dipilih tcp, dan pada menu *In.Interface* dipilih *Internet*. Maksudnya adalah semua *protocol* tcp yang masuk yang akan menuju *interface Internet* (nama *interface* pada *port* 1 di mikrotik) akan di *filter*. 7 tujuan pada langkah ini yaitu ketika perangkat *mikrotik* diserang melalui *port* tcp maka secara otomatis ip si penyerang akan di masukkan ke dalam *address list* yang telah diberi nama "TCP FLOODING". Jadi semua ip si penyerang akan ada dalam dalam *address list* tersebut dan akan dihapus jika telah melewati batas waktu 1 hari. Langkah selanjutnya klik Ok. disini penulis membuat rule yang kedua, yang mana pada *tab General* di menu *Chain* dipilih *input*, pada menu *Protocol* dipilih tcp, dan pada menu *In.Interface* dipilih *Internet*. Langkah-langkah nya hampir sama pada *rule* pertama yang dibuat sebelumnya. pada menu *Src. Address List* penulis memasukkan nama *address list* TCP FLOODING yang telah dibuat pada langkah sebelumnya, kemudian pada menu *Action* dipilih *drop*. Jadi penjelasan dari langkah-langkah yang telah

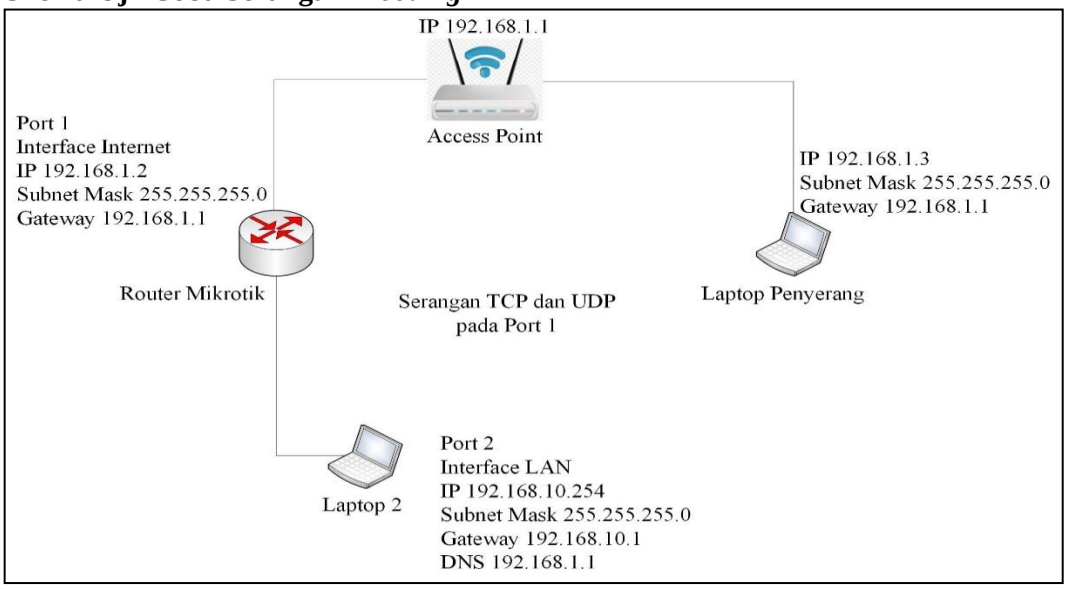
dilakukan yaitu *rule* yang pertama berfungsi secara otomatis menambahkan ip si penyerang ke dalam *address list* yang telah dibuat dengan nama "TCP FLOOODING" dan akan di blokir selama 1 hari, dan *rule* yang kedua fungsinya yaitu daftar ip si penyerang yang telah di dapat pada *address list* yang bernama "TCP FLOODING" tersebut selanjutnya akan di *drop*, sehingga ip tersebut tidak dapat lagi melakukan serangan pada *router mikrotik.*

b. *Filter Firewall* UDP

Pada *tab General* di menu *Chain* dipilih *input*, pada menu *Protocol* dipilih udp, dan pada menu *Interface* dipilih *Internet*. Maksudnya adalah semua *protocol* udp yang masuk yang akan menuju *interface Internet* (nama *interface* pada *port* 1 di *mikrotik*) akan di *filter*. tujuan pada langkah ini yaitu ketika perangkat *mikrotik* diserang melalui *port* udp maka secara otomatis ip si penyerang akan di masukkan ke dalam *address list* yang telah diberi nama "UDP FLOODING". Jadi semua ip si penyerang akan ada dalam dalam *address list* tersebut dan akan dihapus jika telah melewati batas waktu 1 hari. Langkah selanjutnya klik Ok. disini penulis membuat *rule* yang kedua, yang mana pada *tab General* di menu *Chain* dipilih *input*, pada menu *Protocol* dipilih udp, dan pada menu *In.Interface* dipilih *Internet*. Langkah-langkah nya hampir sama pada *rule* pertama yang dibuat sebelumnya. pada menu *Src. Address List* penulis memasukkan nama *address list* UDP FLOODING yang telah dibuat pada langkah sebelumnya, kemudian pada menu *Action* dipilih *drop*. Jadi penjelasan dari langkah-langkah yang telah dilakukan yaitu *rule* yang pertama berfungsi secara otomatis menambahkan ip si penyerang ke dalam *address list* yang telah dibuat dengan nama "UDP FLOOODING" dan akan di blokir selama 1 hari, dan rule yang kedua fungsinya yaitu daftar ip si penyerang yang telah di dapat pada *address list* yang bernama "UDP FLOODING" tersebut selanjutnya akan di *drop*, sehingga ip tersebut tidak dapat lagi melakukan serangan pada *router mikrotik.*

4.4 Uji Coba Serangan *Flooding*

a. Skema Uji Coba Serangan *Flooding*

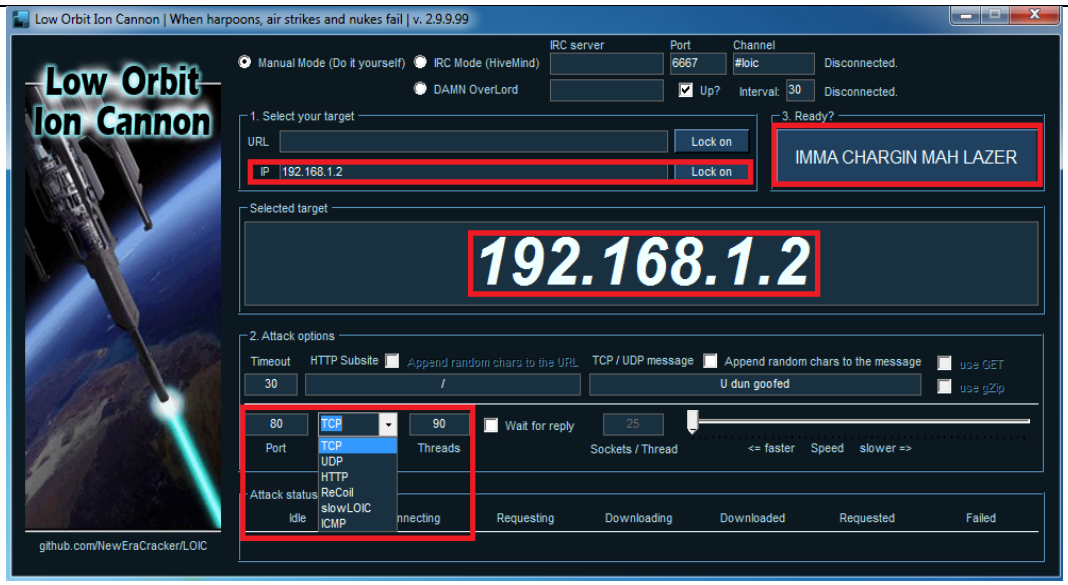


Gambar 4. Skema Serangan *Flooding*

Dalam melakukan uji coba serangan penulis menggunakan 1 *access point wireless*, 1 *router mikrotik*, dan 2 laptop. *Port* 1 di *router mikrotik* adalah jaringan *internet* yang terhubung di *access point*. Sedangkan *port 2 router* mikrotik terhubung pada laptop yang kedua. Laptop yang kedua ini hanya untuk memantau aktifitas serangan yang nantinya akan dilakukan oleh laptop penyerang. Pada laptop penyerang telah terhubung jaringan *internet* pada *access point* melalui *port* 2.

b. Uji Coba Serangan *Flooding* menggunakan *Loic*

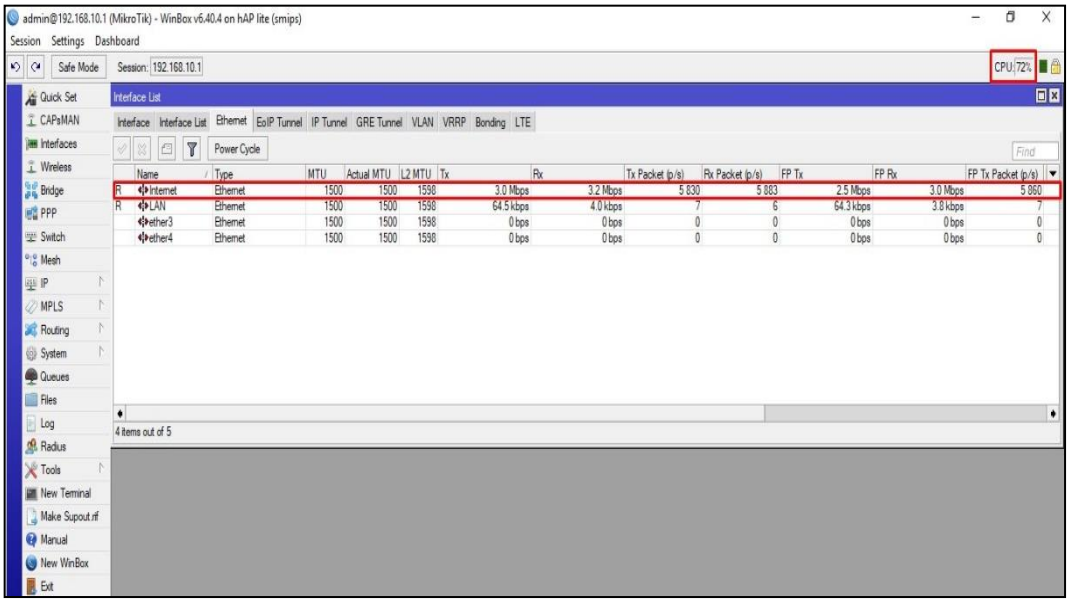
Dalam melakukan uji coba serangan *flooding*, penulis menggunakan aplikasi *Loic* v2.9.9.99 yang akan dilakukan melalui laptop penyerang seperti yang telah dijelaskan sebelumnya.



Gambar 5. Tampilan Aplikasi *Loic*

Serangan *flooding* dapat kita tentukan melalui url atau pun ip. Pada penelitian ini penulis menggunakan serangan pada ip 192.168.1.2 yaitu ip yang terdapat pada *port* 1 di *router* mikrotik. Jenis serangan yang akan dilakukan yaitu TCP dan UDP dengan jumlah 90 *threads*. Maksud dari *threads* disini kita bisa menentukan berapa banyak user yang akan kita gunakan untuk serangan *flooding* tersebut. Untuk melakukan serangan klik *IMMA CHARGIN MAH LAZER*.

4.5 Serangan TCP *Flooding* Sebelum dilakukan *Filter Firewall*

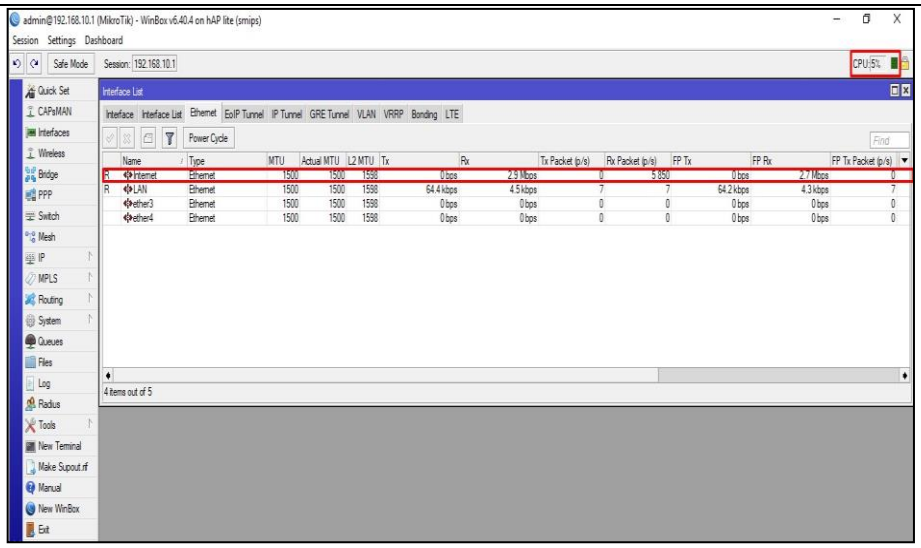


Gambar 6. Tampilan serangan TCP *Flooding* sebelum dilakukan *filter firewall*

Berdasarkan gambar 6, pada *interface internet* di port 1 mengalami peningkatan menjadi 3.0 Mbps (Tx) dan 3.2 Mbps (Rx) dan *resource* CPU meningkat menjadi 72% dikarenakan adanya paket TCP *flooding* yang masuk menuju *interface* tersebut.

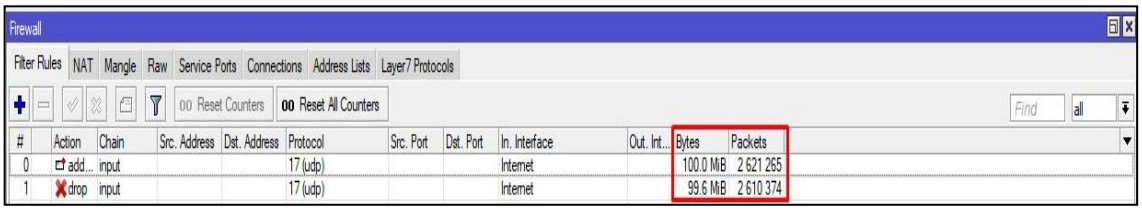
4.6 Serangan TCP *Flooding* sesudah dilakukan *Filter Firewall*

Berikut ini hasil *screenshoot* serangan UDP *Flooding* sesudah dilakukan *filter firewall* pada *mikrotik*.



Gambar 7.Tampilan *Interface Internet*

Berdasarkan gambar 7, Setelah dilakukan *filter firewall* pada *interface internet* di *port* 1 menjadi normal 0 (Tx) dan 2.3 Mbps (Rx). *Resource* CPU pun juga menurun menjadi 5%.



Gambar 8. Koneksi dan Packets UDP Yang Berhasil di *Drop*

Berdasarkan gambar 8, bisa dilihat jumlah koneksi dan *packet* yang berhasil di drop oleh *filter firewall* yaitu sebesar 99.6 MiB dan 2621374 *Packets*.

4.7 Perbandingan Hasil Konfigurasi *Filter Firewall* TCP dan UDP

Filter Firewall TCP : Serangan *flooding attack* pada *protocol* TCP berhasil di *block* secara keseluruhan. Berdasarkan gambar 4.19 setelah dilakukan *filter firewall* pada *protocol* TCP tampilan *interface internet* menjadi 0 bps (Tx) dan 0 bps (Rx). Sedangkan *Filter firewall* UDP : Serangan *flooding attack* pada *protocol* UDP berhasil di *block* tetapi tidak secara keseluruhan. Berdasarkan gambar 4.26 setelah dilakukan *filter firewall* pada *protocol* UDP tampilan *interface internet* menjadi 0 bps (Tx) dan 2.3 Mbps (Rx). Hal ini dikarenakan masih ada sisa *packet flooding* yang masuk sebesar 2.3 Mbps pada *protocol* UDP tersebut.

5. Kesimpulan

Adapun kesimpulan yang penulis dapat dari hasil penelitian yang dilakukan adalah sebagai berikut :

1. Telah dilakukan simulasi pencegahan serangan *flooding attack* TCP dan UDP menggunakan metode *filter firewall.*
2. Pencegahan serangan *flooding attack* pada *protocol* TCP berhasil di *block* secara keseluruhan, sedangkan *filter firewall* pada *protocol* UDP berhasil di *block* tetapi tidak secara keseluruhan.
3. Dengan adanya metode *filter firewall* ancaman serangan *flooding attack* dapat diminimalisir.

Referensi

[1] H. Alfianto, M. V. S. Bria, Y. Saputra, *Analisis Dan Pencegahan Metode Serangan Flooding Pada Jaringan Komputer*, Palembang: STMIK PalComTech, 2017.
[2] A. S. Agusaputra, *Implementasi Sistem Pencegahan Data Flooding Pada Jaringan Komputer*, Palembang: Universitas Bina Darma, 2016.
[3] D. Aprilianto, T. Fadila, M. A. Muslim, *Sistem Pencegahan UDP DNS Flood Dengan Filter Firewall Pada Router Mikrotik*, Semarang: Universitas Negeri Semarang, 2017.
[4] A. H. Hendrawan, *Analisis Serangan Flooding Data Pada Router Mikrotik*, Bogor: Universitas Ibnu Khaldun Bogor, 2016.
[5] J. J. Siregar, *Analisis Exploitasi Keamanan Web Denial Of Service Attack*, Jakarta: Universitas Binus, 2013.