Jurnal Sistim Informasi dan Teknologi
https://jsisfotek.org/index.php
2020 Vol. 2 No. 4 Hal: 115-123 e-ISSN: 2686-3154

Peningkatan Keamanan *Router Mikrotik* Terhadap Serangan *Denial of Service* (DoS)

Budi Jaya[1]✉, Yuhandri Yunus[2], Sumijan[3]
[1,2,3]Universitas Putra Indonesia YPTK Padang
budi_jaya01upiyptk@yahoo.com

Abstract

Denial of Service (DoS) attacks are one of the most common attacks on website, networks, routers and servers, including on router mikrotik. A DoS attack aims to render a network router unable to service requests from authorized users. The result will disrupt the operational activities of the organization and cause material and non-material losses. In this study, a simulation and analysis of DoS attacks using the Live Forensics method were carried out and the router security enhancement from rectangular software and hardware. From the research results obtained digital evidence of DoS attacks in the form of IP addresses and attacker activity logs. In addition, the increase in router security in terms of software by using Firewall Filter and Firewall Raw has proven effective in preventing attacks. While improving router security in terms of hardware by setting a reset button on the router and firewall devices is also very necessary so that the router can avoid physical attacks by irresponsible persons.

Keywords: Router Mikrotik, DoS, Live Forensics, Security, IP Address.

Abstrak

Serangan *Denial of Service* (*DoS*) merupakan salah satu serangan terhadap situs, jaringan, *router* dan *server* yang sangat sering terjadi termasuk pada *router mikrotik*. Serangan *DoS* bertujuan untuk membuat jaringan *router down* sehingga tidak mampu melayani permintaan *user* yang memiliki hak akses yang sah. Akibatnya akan mengganggu aktivitas operasional organisasi dan menimbulkan kerugian material maupun nonmaterial. Dalam penelitian ini dilakukan simulasi dan analisis serangan *DoS* dengan menggunakan metode *Live Forensics* serta peningkatan keamanan *router mikrotik* dari segi *software* dan *hardware*. Dari hasil penelitian diperoleh bukti digital serangan *DoS* berupa *IP Address* dan *log activity* penyerang. Selain itu peningkatan keamanan *router* dari segi *software* dengan menggunakan *Firewall Filter* dan *Firewall Raw* terbukti efektif dalam mencegah terjadinya serangan. Sedangkan peningkatan keamanan *router* dari segi *hardware* dengan menonaktifkan tombol *reset* pada router dan menggunakan perangkat *Hardware Firewall* juga sangat diperlukan agar *router* bisa terhindar dari serangan fisik oleh oknum yang tidak bertanggung jawab.

Kata kunci: *Router Mikrotik*, *DoS*, *Live Forensics*, Keamanan, IP Address.

1. Pendahuluan

Keamanan teknologi informasi menjadi suatu hal yang sangat penting saat ini [1]. Hal ini dimaksudkan guna menjamin keamanan terhadap seluruh informasi yang dikirim ataupun disimpan melalui internet tidak bisa diakses sembarangan oleh pihak yang tidak bertanggung jawab. *Internet* diakses oleh banyak orang tanpa terkecuali *hacker* dan *cracker*. Dengan alasan tertentu mereka melakukan penyusupan yang dapat merugikan para pemilik *server* dan jaringan komputer. Mereka menggunakan berbagai macam serangan jaringan komputer dengan *tools* yang dibuat secara mandiri ataupun yang telah ada di pasar. Kecanggihan serangan dan *tools* pada jaringan komputer berbanding terbalik dengan pengetahuan tentang penyusupan pada jaringan komputer [2].

Jumlah serangan-serangan pada dunia *internet* telah mengalami peningkatan yang signifikan dalam beberapa tahun ini. Target dan pola serangannya bermacam-macam dan sangat banyak. Munculnya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), Peraturan pemerintah nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik dan *Telecom Act* menjadi angin segar bagi pengelola sistem karena pelaku dapat dijerat hukum. Penggunaan teknologi komputer berbasis jaringan telah banyak memberikan kemudahan kepada para penggunanya untuk melakukan aktivitas secara *online* dengan tujuan mengirim data atau hanya sekedar mengakses media *online* [3].

Salah satu perangkat yang paling penting pada suatu jaringan dengan cakupan yang luas adalah *router*. *Router* dapat menyimpan identitas lalu lintas data berdasarkan tabel-tabel yang tersedia melalui *router*. Pesatnya kemajuan teknologi *router* membuktikan bahwa *router* adalah perangkat yang paling dibutuhkan khususnya pada penyedia jasa *internet* dalam membangun sebuah jaringan maupun keamanannya. Target utama *attacker* sebelum masuk pada sistem utama atau pusat data adalah dengan mematikan kinerja *router* [4]. Serangan *Distributed Denial of Services* (*DDoS*) terus menjadi salah satu ancaman paling menantang ke Internet. Intensitas dan frekuensi

Diterima: 05-09-2020 | Revisi: 15-09-2020 | Diterbitkan: 31-12-2020 | DOI: 10.37034/jsisfotek.v2i4.32

serangan ini meningkat dengan kecepatan yang mengkhawatirkan [5]. Peningkatan level serangan *DoS* dengan melakukan pengubahan pada data *size* yang dikirimkan ke target *DoS* menyebabkan *router* yang dilewatinya mengalami peningkatan konsumsi daya listrik dan beban kerja *CPU*.

Forensik jaringan merupakan proses mendeteksi, menangkap, mencatat dan menganalisa aktivitas jaringan guna menemukan bukti digital dari suatu serangan atau kejahatan yang dilakukan melalui jaringan komputer sehingga pelaku kejahatan dapat dituntut sesuai hukum yang berlaku. Bukti digital dapat diidentifikasi dari pola serangan yang dikenali melalui metode *Live Forensic*. Metode *Live Forensic* adalah situasi atau proses analisis forensik yang dilakukan ketika sistem jaringan komputer beroperasi. Hal ini disebabkan oleh informasi bukti digital yang hanya dapat diperoleh saat sistem berfungsi dan informasi tersebut dapat hilang jika sistem jaringan mati.

Karena serangan *DoS* merupakan serangan yang sangat sering kali dilakukan, maka banyak peneliti yang melakukan simulasi serta pencegahan serangan DoS baik terhadap situs, perangkat keras, maupun server. Nita Hildayanti dan Imam Riadi [6] melakukan analisis serangan *Netcut* dengan menggunakan *Wireshark* sebagai detektor serangan. Hasil penelitian ini menyimpulkan bahwa dengan menemukan data di *router* forensik, membantu menyediakan informasi tentang penggunaan *internet* yang dilakukan oleh pengguna lain, sehingga penggunaan *internet* tidak disalahgunakan untuk tujuan buruk.

Potensi kejahatan dengan menggunakan perangkat *smart router* sebagai media *file sharing* sangat mungkin terjadi dan sulit untuk mendapatkan bukti digital. Membutuhkan pengembangan lebih lanjut mengenai teknik ataupun metode yang digunakan dalam menginvestigasi perangkat *smart router*, dikarenakan semakin beragamnya perangkat *smart router* dari berbagai *vendor* dan sistem operasi yang ada di dalamnya. Serta membutuhkan pengujian lebih lanjut dari metode *Live Forensics acquisition* terhadap kasus *cybercrime* yang terjadi [7].

Firmansyah, et.al [8] menyimpulkan bahwa analisis forensik *metarouter* pada lalu lintas jaringan klien, *metarouter* sangat berguna untuk tujuan memecah jaringan jika *router* yang dimiliki hanya 1 (satu) unit. Kasus yang terjadi membuktikan bahwa *router* sangatlah penting untuk membagi atau mendistribusikan *IP address*, baik secara statik maupun dinamik. Forensik jaringan berfungsi untuk merekam kejadian atau aktivitas lalu lintas data pada jaringan komputer, dengan melakukan analisa dari hasil investigasi yang didapat, sehingga menemukan sebuah bukti aliran paket yang mencurigakan.

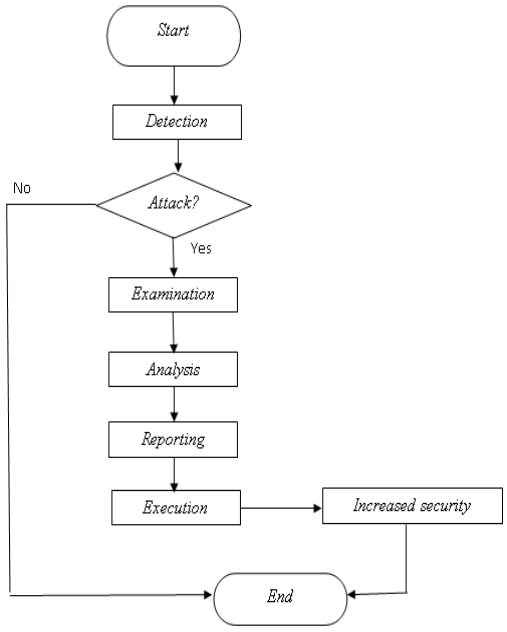
Begitu seringnya serangan *DoS* terjadi menyebabkan banyak peneliti yang melakukan penelitian tentang serangan DoS di antaranya yaitu serangan pada sistem fisik [9], *survey* dan *mitigasi* serangan *DoS* pada *Named Data Networking* [10], eksplorasi bukti digital pada smart router [11], mitigasi serangan DoS yang efisien [12], deteksi DoS pada penerapan jaringan sensor nirkabel [13], deteksi serangan *DDoS* berbasis *multiple autonomous systems* [14], dan *DDoS bandwidth flooding* [15].

Penelitian ini bertujuan untuk memberikan solusi atau alternatif pencegahan terjadinya serangan terhadap perangkat *router mikrotik* terutama terhadap serangan *DoS* melalui peningkatan keamanan perangkat *router* dari segi *software* dan *hardware*. Sehingga organisasi yang menggunakan perangkat *router mikrotik* dalam aktivitas operasionalnya dapat terhindar dari kerugian material dan nonmaterial akibat kondisi jaringan *router* yang *down* karena serangan dari orang yang tidak bertanggungjawab.

2. Metodologi Penelitian

2.1 Live Forensics

Live forensics dilakukan untuk mencari informasi dan barang bukti dalam sebuah jaringan lokal, artinya kita menghadapi keadaan di mana komputer atau alat bukti yang ditemui di tempat kejadian perkara terhubung pada sebuah jaringan komputer dan dalam keadaan *Power On* [16]. Hal ini memberikan keuntungan dari kekurangan proses forensik tradisional yang tidak dapat menganalisa sebuah jaringan komputer untuk mencari barang bukti serta informasi di dalamnya [17]. Adapun tahapan yang dilakukan dalam penelitian ini dapat dilihat pada Gambar 1.



Gambar 1. *Flowchart Live Forensics*

2.2 Perangkat yang Digunakan Dalam Simulasi

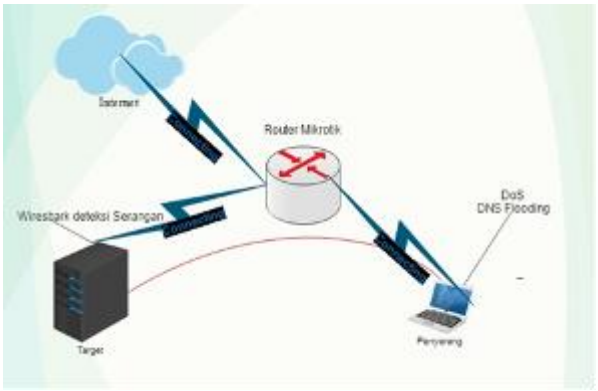
Dalam penelitian ini dibutuhkan perangkat *hardware* dan *software* untuk melakukan simulasi serangan *DoS* dan peningkatan keamanan pada *router mikrotik*. Perangkat yang digunakan dapat dilihat pada Tabel 1.

Tabel 1. Perangkat yang digunakan dalam Penelitian

	Nama Alat	Keterangan
Hardware	*Router Mikrotik* RB51Ui Versi 6	Alat manajemen jaringan serta mengatur *traffic* jaringan baik koneksi *internet* maupun *intranet*. *Router* ini merupakan objek yang diserang.
	Hub/ Switch	Terminal pembagi koneksi pada jaringan.
	Access Point	Alat koneksi jaringan dengan menggunakan *wifi*.
	Modem	Alat penghubung jaringan internet ke jaringan lokal.
	Laptop Core i7, RAM 4GB	Sebagai media untuk melakukan serangan
	Laptop Client jaringan	Sebagai media untuk melakukan monitoring terjadinya serangan.
Software	*Winbox*	Aplikasi *remote* pada *router* yang digunakan untuk monitoring dan konfigurasi jaringan.
	Kali Linux	Sistem operasi yang berbasis *open source*, digunakan untuk melakukan serangan. Sistem operasi ini sering digunakan oleh para *hacker* untuk melakukan *hacking* atau *attacker*.
	Tools DNS Flood Master	Perintah untuk melakukan serangan.
	Wireshark	Aplikasi yang digunakan untuk melihat *traffic* jaringan.
	Firewall Filter dan *Firewall Raw*	Aplikasi yang digunakan untuk melakukan peningkatan keamanan pada *router*.

2.3 Skema Serangan *DoS* pada *Router*

Rancangan simulasi serangan DoS pada *rou*ter menggunakan *DNS Flooding*, dan analisis serangan pada *router* menggunakan aplikasi *Wireshark* terdapat pada Gambar 2.



Gambar 2. Skema Serangan DoS pada Router

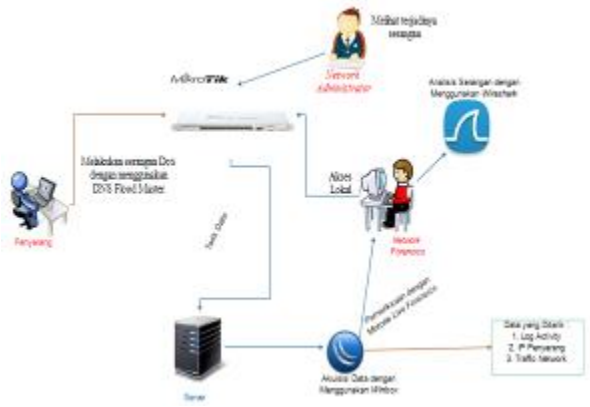
2.4 Analisis Serangan *DoS* pada *Router*

Tahapan simulasi serangan pada Gambar 2 bertujuan untuk menguji apakah aplikasi *Wireshark* mampu menampilkan beberapa aktivitas dari usaha serangan *DoS* pada *router*. Gambar 3 merupakan skema alur analisis serangan *DoS* pada *router* berdasarkan metode *Live Forensics*.

Gambar 3. Alur Analisis Serangan DoS pada *Router*

2.5 Skema Akuisisi Data Forensik

Simulasi kasus terdiri dari simulasi serangan *DoS* pada perangkat *router mikrotik*, akuisisi data forensik, serta simulasi peningkatan keamanan *router mikrotik*. Skema akuisisi data forensik pada penelitian ini dapat dilihat pada Gambar 4.



Gambar 4. Skema Serangan *DoS* dan Akuisisi Data Menggunakan Metode *Live Forensics*

Simulasi serangan DoS terdiri dari 3 *actor* yaitu penyerang yang mengirim serangan pada jaringan *router*, *network administrator* sebagai *user* dari jaringan *router*, serta *network forensics* yang menganalisis serangan, melakukan akuisisi data, dan peningkatan keamanan pada perangkat *router*. Peran dari masing-masing *actor* serta fungsi perangkat dalam penelitian ini yaitu :

a. Penyerang melakukan serangan *DoS* dengan cara membanjiri lalu lintas jaringan dengan mengirim banyak data sehingga menyebabkan *traffic* data yang sangat tinggi pada *interface router*. Hal ini akan mengakibatkan sehingga *user* lain yang terhubung pada *router* tersebut tidak bisa menggunakan layanan jaringan, teknik ini di sebut dengan serangan *traffic flooding*. Aplikasi yang digunakan untuk melakukan serangan yaitu *DNS Flood Master* dan *Hping3*.
b. *Network Administrator* melihat terjadinya serangan terhadap jaringan ketika sudah terhubung dengan jaringan. Hal ini ditandai dengan traffic jaringan dalam kondisi yang tidak biasanya, cenderung sangat tinggi, terjadi peningkatan *resources* pada *CPU Load Router*. Dalam kondisi normal,

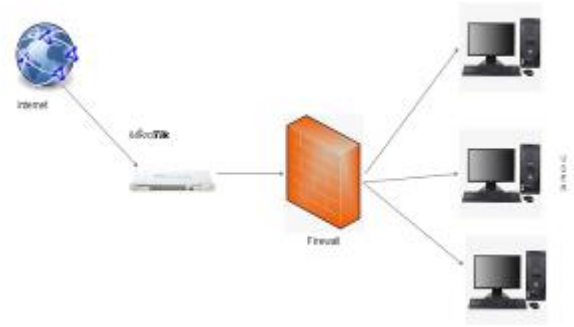
resources CPU Load berada antara 3-9%. Namun pada saat terjadi serangan, *CPU Load* pada *router* bisa mencapai 80-100% sehingga mengakibatkan *router down* dan tidak bisa melayani request user lainnya.

c. Setelah mendapat laporan atau pengaduan terjadinya serangan, *Network Forensics* masuk pada jaringan melalui akses lokal dan melakukan analisa serangan yang terjadi dengan menggunakan aplikasi *Wireshark*. Kemudian Network Forensics menggunakan metode *Live Forensics* dengan bantuan aplikasi Winbox untuk memperoleh data serangan berupa *Log Activity*, *IP address penyerang*, dan *traffic network* yang terdapat pada *interface* jaringan lokal tersebut.

2.6 Firewall Filter

Peningkatan keamanan perangkat *router* dari segi *software* dapat dilakukan dengan menggunakan aplikasi *Firewall Filter*. *Firewall Filter* bertujuan untuk menyaring *packet* data yang masuk pada perangkat *router* agar *router* tidak mengalami kondisi *down*. Sedangkan Firewall melakukan filter terhadap data yang diterima dan melacak koneksi yang dibuat untuk menentukan data apakah koneksi tersebut diizinkan atau ditolak [18].

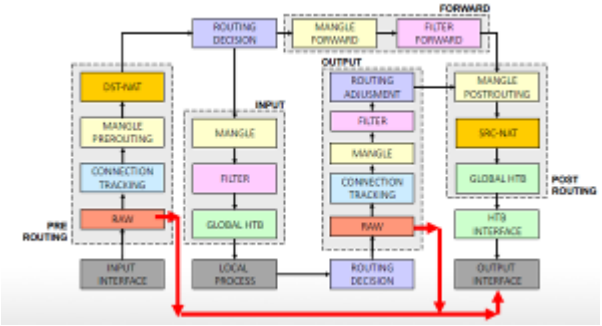
Meskipun firewall tidak dapat mencegah semua serangan firewall setidaknya lebih dapat membantu membuat data aman daripada tanpa firewall sama sekali Skema peningkatan keamanan router mikrotik dengan menggunakan Firewall terdapat pada Gambar 5.



Gambar 5. Peningkatan Jaringan dengan Menggunakan *Firewall Filter Router*

2.7 Firewall Raw

Firewall Raw berfungsi untuk memblokir *IP Address* yang dicurigai sebagai penyerang atau tidak memiliki hak yang sah untuk mengakes jaringan. *Firewall RAW* memungkinkan kita memilih untuk melewatkan atau mendrop *packet* data sebelum *connection tracking*, sehingga menghemat *load CPU*. Hal ini sangat berguna untuk serangan *DoS* dan hanya bisa dilakukan pada *chain prerouting* dan *output*, sebelum *connection tracking*. Pada Gambar 6 merupakan alur dari penggunaan *Firewall Raw*.



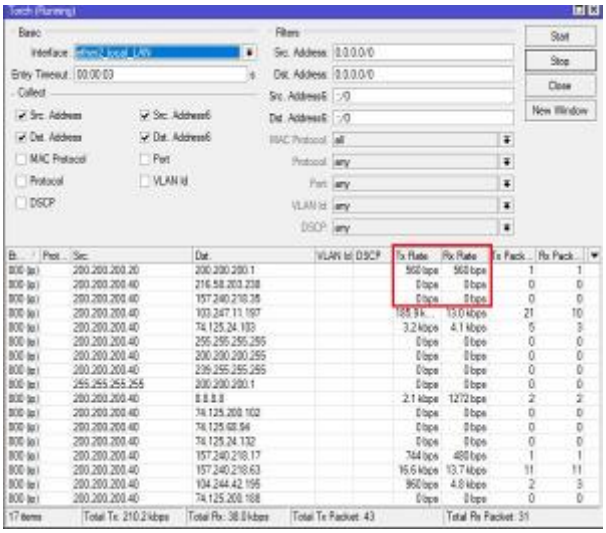
Gambar 6. Skema *Firewall Raw*

3. Hasil dan Pembahasan

3.1 Serangan *DoS* pada *Router Mikrotik*

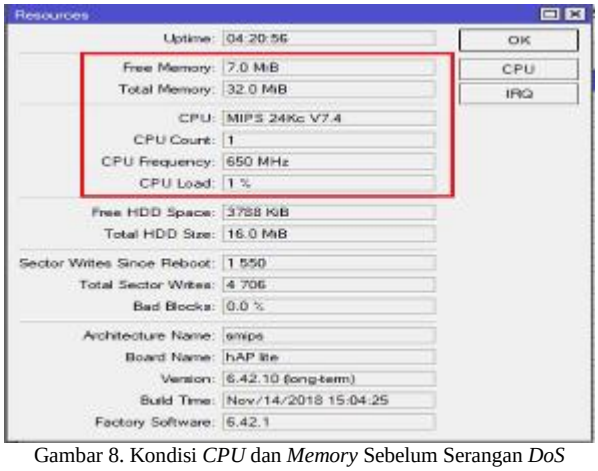
Proses pertama untuk menganalisis apakah *r*outer masih dalam keadaan normal atau ada serangan *DoS*, dapat dilakukan melalui pengecekan pada menu *WinBox* yaitu melalui menu *Torch Running*. Setelah dilakukan pengecekan, diketahui belum ada serangan masuk *DoS*, hal ini terlihat pada *Traffic Destination*, *Tx Rate* dan *Rx Rate*.

Berdasarkan Gambar 7, dapat disimpulkan belum terjadinya serangan yang masuk dan dapat mengganggu *traffic* jaringan. Hal ini terlihat Hal ini dapat dilihat pada baris *Source* dan *Destination*, terdapat IP dari masing-masing komputer dalam melakukan komunikasi satu sama lain secara normal.



Gambar 7. Tampilan *Tourch* Sebelum Serangan *DoS*

Berikut pada Gambar 8, merupakan hasil analisis pada *Traffic Monitor System* sebelum terjadi serangan *DoS*, diketahui bahwa keadaan *Traffic System* sebelum terjadi serangan menunjukkan Presentase *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*.



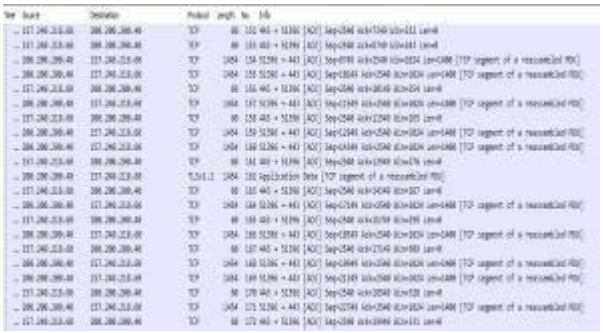
Gambar 8. Kondisi *CPU* dan *Memory* Sebelum Serangan *DoS*

3.2 Serangan Dos dengan Menggunakan Kali Linux

Pada Gambar 9, peneliti menggunakan Port 53 UDP dan 443 ICMP. Aplikasi *DNS Flooding* di *Kali Linux* dengan menggunakan *Hping3* berhasil dijalankan dan siap melancarkan serangan ke jaringan *router* yang menjadi target serangan. Setelah serangan dilancarkan, proses selanjutnya melakukan pengecekan serangan yang masuk pada *router* melalui aplikasi *Wireshark*.

Gambar 9. Tampilan Serangan DoS pada Kali Linux

3.3 Akuisisi Data Forensik

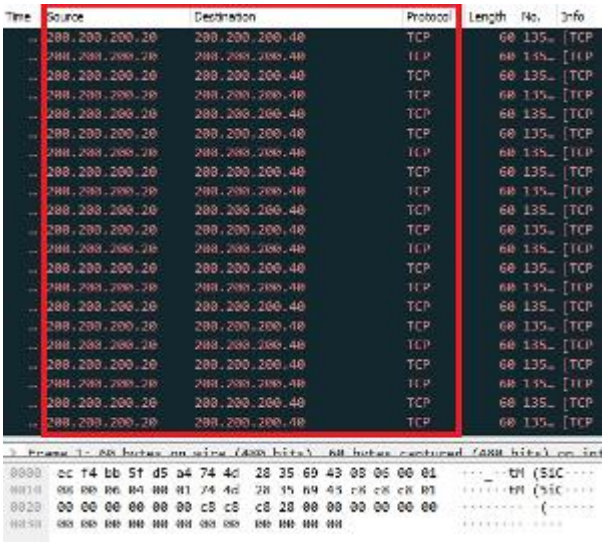


Gambar 10. Tampilan *Wireshark* Deteksi Serangan *DoS* pada *Protocol DNS*

Pada Gambar 10, merupakan trafik yang tidak biasa yang menunjukkan terjadinya aktivitas serangan *Port Scanning*, dari *Source Row* terdapat IP komputer penyerang yaitu 192.168.1.20 yang melakukan *attact*, dan pada *Destination Row* adalah IP 192.168.1.2 yang merupakan komputer target. Protokol yang digunakan adalah DNS dan di *Info Row* menyatakan bahwa *Port* penyerang sedang memindai ke semua *Port Komputer* target. Di sana kita bisa melihat di *Port Protocol* (penyerang) adalah 8291 di depan ke *Port* 49167 atau *Port* (53) sebagai (target). Artinya P*ort* 49167 (53) dalam keadaan terbuka dengan mengirimkan umpan balik ke komputer penyerang dan siap menerima koneksi dari luar.

3.4 Log Activity

Pada Gambar 11, terlihat bahwa *IP Address* 200.200.200.20 secara bertubi-tubi menyerang *Protocol Port Router*, yaitu 200.200.200.40. Aktivitas ini dicurigai sebagai aktivitas yang tidak wajar dalam melakukan komunikasi data.



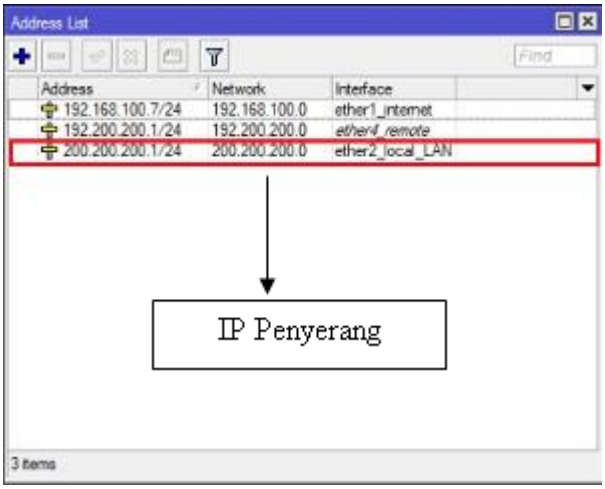
Gambar 11. Data *Log Activity* Serangan pada *Router*

3.5 IP Address List

IP Address List yang ditampilkan adalah hasil konfigurasi melalui kolom *Segmentasi Network* tersebut yang biasa diakhiri dengan angka 0. Sedangkan pada kolom *Interface* dapat dilihat nama *Interface* atau *Ether LAN Port* fisik ataupun *WLAN Port* dari *RouterBoard*.

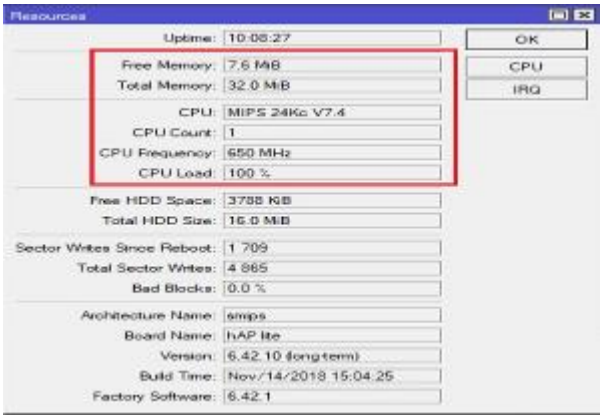
IP Address pada suatu *Port Router* bisa juga dapat berarti *Gateway* pada *Network Segment*. *IP Gateway* biasa dijadikan sebagai target dari suatu aktivitas serangan pada jaringan. Berdasarkan tab informasi *IP Address List.*

Pada Gambar 12, dapat dilihat bahwa *packet-packet* yang dikirimkan melintasi masing-masing data *Link* dengan cara *Enkapsulasi packet* ke dalam *Frame* menggunakan pengenal data *Link* agar *Frame* dapat dikirimkan dari sumber ke tujuan di dalam *Protocol Link Network* yang lebih rendah.



Gambar 12. Tampilan IP Address List Penyerang

Pada Gambar 13, ketika terjadi serangan DoS yang masuk pada jaringan *router*, *Load CPU* dan *Memory* meningkat. Berdasarkan hasil *Traffic Monitor System* setelah terjadi serangan DoS diketahui *Traffic System Monitor Packet* data *CPU Load* meningkat menjadi 100 % dan *Memory* 7.6 MiB naik secara signifikan. Hal ini yang menyebabkan *down* pada *Network Traffic* akibat serangan *DoS* pada *router*.



Gambar 13. *Traffic Monitor System* Setelah Terjadi Serangan *DoS*

Pada Gambar 14, terlihat bahwa *traffic Tx/Rx Rate* 94.9 Mbps dan *Tx/Rx Packet Rate* 24 270 p/s. Hal ini dapat diartikan bahwa perangkat *router* dari segi *interface* maksimal hanya mampu melewatkan data yang *direquest* oleh *user* sebesar 100 Mbps pada *interface router* tersebut. Sedangkan dampak serangan DoS ini menyebabkan *interface* sudah melewatkan data sebesar 94.9 Mbps. Ini menandakan bahwa *traffic* sudah tidak bisa lagi melewatkan permintaan akses user terhadap *server* yang melalui *router* tersebut.

Gambar 14. Traffic Data Ketika Terjadi Serangan DoS

3.6 Peningkatan Keamanan *Router Mikrotik*

Berdasarkan uraian pada penyerangan serta akuisisi data, maka langkah selanjutnya adalah melakukan peningkatan kemanan *Router Mikrotik* dari segi *software* dan segi *hardware*.

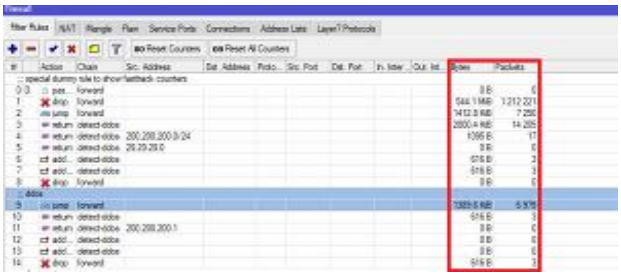
3.6.1. Keamanan dari segi *software*

a. Firewall Filter

Firewall Filter ini berfungsi menyaring (filter) *packet* data yang masuk dan keluar dari jaringan dalam (*local*) atau dari jaringan luar (*internet*). Maka *router* akan menyaring data apa saja yang boleh masuk atau keluar. *Script Firewall Filter* ini di-*input* melalui CLI pada terminal *Router Mikrotik*. Tampilan input CLI dapat dilihat pada Gambar 15.

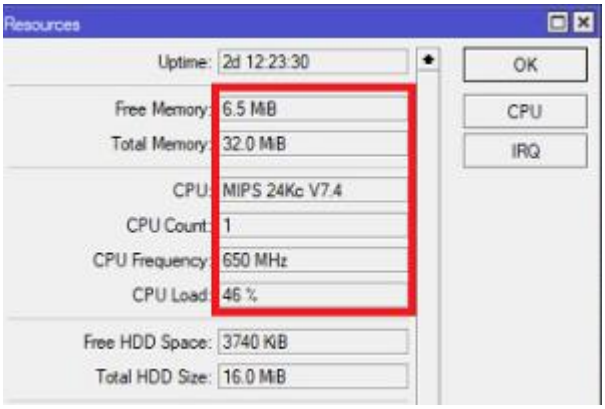
Gambar 15. *Command Line Interface* (CLI)

Setelah *script* di-*input*, akan menghasilkan *Firewall Filter* seperti yang terlihat pada Gambar 16.



Gambar 16. *Firewall Filter DoS* pada *Router Mikrotik*

Dari Gambar 16, dapat dilihat pada kolom *Bytes* dan *Packets* yang di *filter* oleh *Firewall* saat penyerang melakukan serangan. Terdapat data yang di-*drop* dan di-*forward*. Hal ini menandakan data yang di-*drop* dan *foward* tersebut merupakan data yang ditolak untuk masuk ke jaringan *router*. Hal ini membuktikan bahwa *Firewall Filter* mampu membatasi serta menolak data-data yang dicurigai dikirim oleh penyerang pada jaringan *router*. Sehingga jaringan *router* tidak mengalami *down* seperti sebelum menggunakan *Firewall Filter*. Perubahan yang terjadi pada jaringan *router* ketika menggunakan *Firewall Filter* dapat dilihat pada Gambar 17 berikut ini :



Gambar 17 Tampilan Resources CPU Load Setelah Menggunakan Firewall Filter

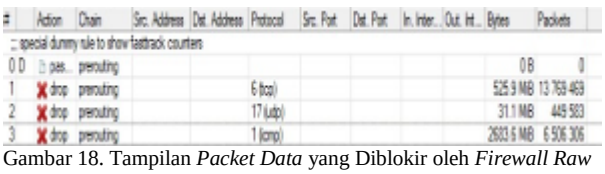
Pada Gambar 17, terlihat *CPU Load* dari 100% turun menjadi 46% setelah menggunakan *Firewall Filter*. Dapat disimpulkan bahwa *Firewall Filter* dapat mencegah serangan *DoS* sehingga tidak terjadi *router down*.

b. Firewall Raw

Berikut merupakan *script Firewall Raw* yang digunakan untuk melakukan *bloking IP* penyerang. *Script* ini di-*input*-kan ke dalam terminal CLI pada *Router Mikrotik*.

```
/IP firewall raw
add action=drop chain=prerouting disabled=yes protocol=tcp
add action=drop chain=prerouting disabled=yes protocol=udp
add action=drop chain=prerouting disabled=yes protocol=icmp
```

Pada Gambar 18 di bawah ini terlihat bahwa ada 3 *packet* data yang diblokir oleh *Firewall Raw*. Hal ini berarti, ketika penyerang mengirim *packet* 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*.

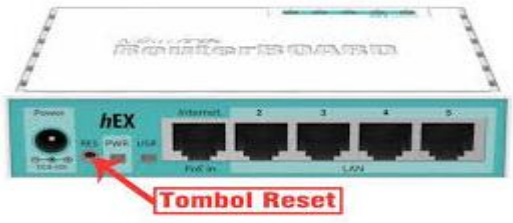


Gambar 18. Tampilan *Packet Data* yang Diblokir oleh *Firewall Raw*

3.6.2. Keamanan dari segi *hardware*

Selain pada sisi *software*, peningkatan keamanan terhadap serangan *DoS* pada jaringan *Router Mikrotik* dapat juga dilakukan dari segi h*ardware* agar keamanan jaringan *Router Mikrotik* tersebut lebih sempurna sehingga tidak mudah bagi penyerang untuk mencoba melakukan serangan kembali terutama untuk serangan *DoS*. Peningkatan keamanan dari segi *hardware* diperuntukkan pada serangan yang dilakukan secara fisik terhadap perangkat *Router Mikrotik* yang dilakukan oleh oknum yang tidak bertanggung jawab.

Serangan fisik yang dimaksud dapat berupa sengaja menekan tombol *reset* pada perangkat *router* sehingga *router* kembali pada pengaturan *default* pabrik. Hal ini berakibat perangkat *router* tidak bisa digunakan sesuai dengan kebutuhan organisasi yang menggunakannya sehingga organisasi dalam hal ini LLDIKTI Wilayah X terpaksa melakukan pengaturan kembali sesuai dengan kebutuhannya dan bisa menimbulkan biaya yang cukup material serta terganggunya aktivitas operasional pada organisasi tersebut. Berikut pada Gambar 19, merupakan salah satu contoh letak tombol router pada perangkat router.



Gambar 19. Tombol Reset pada Perangkat Router

Untuk menghindari serangan fisik pada tombol *reset router*, maka pada terminal CLI dapat di-*input*-kan *script* untuk mengunci tombol *reset* agar tidak berfungsi. Hal ini berguna agar tombol *reset* tidak berfungsi apabila ada oknum yang sengaja atau tidak menekan tombol *reset* tersebut. *Script* yang dimaksud ialah sebagai berikut :

```
klik terminal CLI pada router mikrotik

ketik
/system routerboard setting enable-jumper-reset=no
```

Selain menonaktifkan tombol *reset* pada *router*, alternatif lain untuk meningkatkan keamanan jaringan *router* ialah dengan menggunakan perangkat *Hardware Firewall*. Jenis *firewall* ini menggunakan alat fisik yang bertindak dengan cara yang mirip dengan *router* lalu lintas. Cara kerjanya mencegat *packet* data dan permintaan lalu lintas sebelum mereka terhubung ke *server* jaringan. *Firewall* berbasis alat fisik seperti ini unggul pada keamanan perimeter dengan memastikan lalu lintas berbahaya dari luar jaringan di stop sebelum

titik akhir jaringan terpapar risiko. Namun perlu diperhatikan bahwa kemampuan tiap *firewall* perangkat keras bervariasi tergantung pabrikan. Pada Gambar 20 merupakan salah satu bentuk perangkat *Hardware Firewall*.

Gambar 20. Perangkat *Hardware Firewall*

3.7 Analisis Hasil

Berdasarkan hasil pengujian analisis serangan DoS serta peningkatan keamanan pada *Router Mikrotik*, maka hasil penelitian tersebut disajikan dalam bentuk laporan *Network Forensic* berdasarkan proses yang telah dilakukan. Hasil analisis dirangkum pada Tabel 2.

Tabel 2. Hasil Analisis Serangan DoS dan Peningkatan Keamanan pada Router Mikrotik

No.	Analisis	Keterangan
1	Serangan *DoS* pada *router* menggunakan aplikasi *DNS Flooding Hping3* pada *Kali Linux*.	Berhasil melakukan serangan pada jaringan *router* secara bertubi-tubi hingga membuat jaringan menjadi *down*.
2	Aplikasi *Wireshark* berhasil menangkap aktivitas lalu-lintas yang mencurigakan melalui *Protocol DNS*.	Diperoleh informasi adanya serangan *DoS* pada *router* mulai dari proses penyerang mengirim *Ping* untuk me-*request* akses masuk pada *router*.
3	*Protocol* serangan yang berhasil ditembus.	*Protocol TCP* dan *ICMP*
4	*Port Protocol* yang diserang.	*Port* 443 dan *Port* 53
5	*Port Destination* target.	49167 atau *Port* 53
6	Kondisi *CPU* dan *Memory* perangkat jaringan sebelum diserang.	*CPU Load* 1% *Memory* 7.0 Mib
7	Kondisi *CPU* dan *Memory* perangkat jaringan setelah diserang .	*CPU Load* 100% *Memory* 7.6 Mib
8	*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* 200.200.200.20 terhadap *router* dengan *IP* jaringan lokal 200.200.200.40
9	a. *IP Address List* Penyerang *b. IP Router Mikrotik* *c. IP Network Administrator* *d. IP Network Foorensics* *e. IP Router to ISP (Internet Services Provider)* *f. IP Gateway Internet to ISP*	a. 200.200.200.20 b. 200.200.200.1 c. 200.200.200.40 d. 192.200.200.20 e. 192.168.100.7 f. 192.168.100.1
10	Peningkatan Keamanan *Router Mikrotik*	1. Segi *software* menggunakan *Firewall Filter* dan *Firewall Raw*. 2. Segi *hardware*, nonaktifkan tombol *reset* dan menggunakan *Hardware Firewall.*
11	Kondisi *CPU* dan *Memory* perangkat jaringan setelah menggunakan *Firewall Filter*	*CPU Load* turun menjadi 46% Memory 6.5 Mib
12	Kondisi perangkat *router* setelah menggunakan *Firewall Raw*	Koneksi terputus dengan *IP Address* penyerang yang diblokir adalah **200.200.200.20**, *netmask* **255.255.255.0**, dan *IP broadcast* **200.200.200.255**.

4. Kesimpulan

Firewall Filter dan *Firewall Raw* terbukti efektif dalam mencegah terjadinya serangan *DoS* pada *router mikrotik*. *Firewall Filter* berfungsi menyaring *packet* data yang masuk pada jaringan *router*, sedangkan *Firewall Raw* berfungsi untuk memblokir *IP* yang dicurigai mengirim *pack*et data tidak wajar pada jaringan *router*. Pencegahan serangan fisik pada perangkat *router* bisa dilakukan dengan cara menonaktifkan tombol *reset* pada *router* serta menggunakan perangkat tambahan salah satunya *Hardware Firewall*.

Daftar Rujukan

[1] Dwiyatno, S., Sari, A. P., Irawan, A., & Safig, S. (2019). Pendeteksi Serangan Ddos (Distributed Denial of Service) Menggunakan Honeypot di PT. Torini Jaya Abadi. *Jurnal Sistem Informasi dan Informatika (SIMIKA)*, *2*(2), 64-80. DOI: https://doi.org/10.47080/simika.v2i2.606 .

[2] Fadlil, A., Riadi, I., & Aji, S. (2017). Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik Jaringan. *Jurnal Ilmu Teknik Elektro Komputer dan Informatika (JITEKI)*, *3*(1), 11-19.

[3] Zulkifli, M. A., Riadi, I., & Prayudi, Y. (2018). Live Forensics Method for Analysis Denial of Service (DOS) Attack on Routerboard. *International Journal of Computer Applications*, 180(35), 23-30. DOI: http://doi.org/10.5120/ijca2018916879 .

[4] Yudhana, A., Riadi, I., & Ridho, F. (2018). DDoS Classification Using Neural Network and Naïve Bayes Methods for Network Forensics. *International Journal of Advanced Computer Science and Applications (IJACSA)*, *9*(11), 177-183. DOI: http://dx.doi.org/10.14569/IJACSA.2018.091125 .

[5] Liang, X., & Znati, T. (2019). On The Performance Of Intelligent Techniques For Intensive And Stealthy DDos Detection. *Computer Networks*, *164*. DOI: https://doi.org/10.1016/j.comnet.2019.106906 .

[6] Hildayanti, N., & Riadi, I. (2019). Forensics Analysis of Router On Computer Networks Using Live Forensics Method. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, *8*(1), 74-81. DOI: http://dx.doi.org/10.17781/P002559 .

[7] Supriyono, A. R., Sugiantoro, B., & Prayudi, Y. (2018). Live Forensics Acquisition File Sharing Samba Pada Mikrotik Routeros. *Cyber Security dan Forensik Digital, 1*(1), 7-13.

[8] Firmansyah, F., Fadlil, A., & Umar, R. (2019). Analisis Forensik Metarouter pada Lalu Lintas Jaringan Klien. *Edu Komputika Journal*, *6*(2), 54-59. DOI: http://dx.doi.org/10.15294/edukomputika.v6i2.35221 .

[9] Al-Sharif, Z. A., Al-Saleh, M. I., Alawneh, L. M., Jararweh, Y. I., & Gupta, B. (2020). Live Forensics of Software Attacks on Cyber Physical Systems. *Future Generation Computer Systems*, *108*, 1217-1229. DOI: http://dx.doi.org/10.1016/j.future.2018.07.028 .

[10] Rai, S., Sharma, K., & Dhakal, D. (2018). A Survey on Detection and Mitigation of Distributed Denial-of-Service Attack in Named Data Networking. *Advances in Communication, Cloud, and Big Data*. DOI: https://doi.org/10.1007/978-981-10-8911-4_18 .

[11] Supriyono, A. R., Sugiantoro, B., & Prayudi, Y. (2019). Eksplorasi Bukti Digital Pada Smart Router Menggunakan Metode Live Forensics. *Jurnal Infotekmesin*, *10*(2), 38-45. DOI: https://doi.org/10.35970/infotekmesin.v10i2.48 .

[12] Liu, G., Quan, W., Cheng, N., Zhang H., & Yu, S. (2019). Efficient DDoS Attacks Mitigation for Stateful Forwarding In Internet of Things. *Journal of Network and Computer Applications*, *130*, 1-13. DOI: https://doi.org/10.1016/j.jnca.2019.01.006 .

[13] Krishnan, S. S. N.. (2019). Denial of Service (DoS) Detection in Wireless Sensor Networks Applying Geometrically Varying Clusters. *International Conference on Computer Networks and Communication Technologies*, *15*. DOI: https://doi.org/10.1007/978-981-10-8681-6_93 .

[14] Singh, K., Dhindsa, K. S., & Nehra, D. (2020). T-CAD: A Threshold Based Collaborative DDoS Attack Detection In Multiple Autonomous Systems. *Journal of Information Security and Applications*, *51*. DOI: https://doi.org/10.1016/j.jisa.2020.102457 .

[15] Furfaro, A., Pace, P., & Parise, A. (2020). Facing Ddos Bandwidth Flooding Attacks. *Simulation Modelling Practice and Theory*, *98*. DOI: https://doi.org/10.1016/j.simpat.2019.101984 .

[16] Casey, E. (2009). Handbook of Digital Forensics and Investigation. *1st ed. London: Elsevier Inc. eBook.*

[17] Dimaio, V. J., & Dimaio, D. (2001). Forensics Pathology. *2nd ed. London: CRC Press*.

[18] Aprilianto, D., Fadila, T., & Muslim, M. A. (2017). Sistem Pencegahan UDP DNS Flood dengan Filter Firewall Pada Router Mikrotik. *Techno.COM*, *16*(2), 114-119. DOI: https://doi.org/10.33633/tc.v16i2.1291