ISSN 2337-6805

SIMULASI JARINGAN VIRTUAL METAROUTER UNTUK MENDETEKSI SERANGAN DENIAL OF SERVICE MENGGUNAKAN WIRESHARK

SIMULATION OF METAROUTER VIRTUAL NETWORK TO DETECT DENIAL OF SERVICE ATTACKS USING WIRESHARK

Novresa Dwi Yudanti[1], Aryo Nur Utomo[2]
Program Studi Teknik Informatika, Fakultas Sains dan Teknologi Informasi
Institut Sains dan Teknologi Nasional
Jl. Moh. Kahfi II, Bhumi Srengseng Indah, Jagakarsa, Jakarta Selatan 12640
yudantinovresa@gmail.com, aryo.nurutomo@istn.ac.id

ABSTRAKSI
Pada penerapannya sehari-hari terkadang pengguna jaringan komputer merasa perlu menambah jumlah router agar memiliki akses langsung penuh, atau memerlukan router dalam jumlah yang banyak. Dengan kemajuan teknologi, saat ini terdapat teknologi MikroTik MetaRouter. MikroTik MetaRouter merupakan fitur yang diberikan oleh MikroTik yaitu sebuah router virtual yang membuat pengguna merasa memiliki router tambahan dengan menggunakan teknik virtualisasi di dalamnya. Serangan Denial of Service merupakan serangan yang sering dilakukan terhadap situs, perangkat atau server. Oleh karena itu, pada penelitian ini dilakukan simulasi serangan Denial of Service pada MetaRouter dengan menggunakan protokol ICMP dan metode live forensic, serta dibantu dengan aplikasi wireshark untuk merekam paket data pada jaringan. Tujuan penelitian ini adalah untuk melakukan simulasi serangan, memperoleh data sebagai bukti, dan mengatasi serangan denial of service pada MetaRouter. Hasil dari pengujian simulasi serangan berupa bukti antara lain, peningkatan yang terjadi Torch Running, Log Acticity, dan IP Address List. Simulasi serangan ini berhasil dilakukan dengan terjadinya perubahan atau peningkatan komunikasi data yang menyebabkan jaringan menjadi down.
Kata kunci: Wireshark, Denial of Service, MikroTik MetaRouter

ABSTRACT
In its daily application, computer network users feel the need to increase the number of routers in order to have full direct access, or require a large number of routers.With technological advances, currently there is MikroTik MetaRouter technology. MikroTik MetaRouter is a feature provided by MikroTik, which is a virtual router that makes users feel like they have an additional router by using virtualization techniques in it. Denial of Service attacks are attacks that are often carried out against sites, devices or servers. Therefore, in this study, a Denial of Service attack simulation on MetaRouter was carried out using the ICMP protocol and live forensics methods, and assisted by the Wireshark application to record data packets on the network. The purpose of this study is to simulate attacks, obtain data as evidence, and overcome denial of service attacks on MetaRouter. The results of the attack simulation test are evidence, among others, the increase in Torch Running, Activity Logs, and IP Address Lists. This attack simulation was successfully carried out with changes or improvements in data communication which caused the network to go down.
Keywords: *Wireshark, Denial of Service, MikroTik MetaRouter*

1. PENDAHULUAN

Seiring dengan berjalannya waktu tidak dapat dipungkiri kemajuan dan perkembangan teknologi pada bidang komputer saat ini terjadi begitu pesat. Pada dasarnya teknologi komputer dan jaringan tidak dapat dipisahkan karena pengguna teknologi komputer yang berbasis jaringan merasakan banyak manfaat yang dihasilkan antara lain pengguna dapat mengirimkan data dengan mudah dan cepat atau hanya sekedar pengguna mengakses internet untuk memperoleh informasi yang diperlukan. Dalam penggunaan teknologi komputer yang berbasis jaringan pengguna membutuhkan sistem yang dapat mendeteksi, menyimpan, memonitor, dan juga merekam kejadian yang terjadi pada sistem jaringan. Hal tersebut dapat digunakan sebagai alat bukti jika terjadi serangan yang dapat merusak sistem secara cepat dan tepat.

Secara umum router merupakan salah satu perangkat keras jaringan komputer yang berfungsi untuk menghubungkan beberapa jaringan sehingga pengguna dapat mentransmisikan data melalui jaringan menuju tujuannya. Mikrotik RouterOS adalah sistem operasi perangkat lunak yang dapat digunakan untuk menjadikan komputer biasa menjadi router network yang handal,

ISSN 2337-6805

mencakup berbagai fitur yang dibuat untuk *IP network* dan jaringan *wireless* (Gustina & Mutiara, 2017). Terkadang pengguna jaringan komputer merasa perlu menambah jumlah router agar bisa langsung mengakses router dengan penuh atau terkadang pengguna membutuhkan jumlah router yang cukup banyak. Hal tersebut tentu saja membuat biaya untuk membangan sebuah jaringan komputer menjadi cukup mahal. Dengan adanya kemajuan teknologi, saat ini terdapat teknologi yang disebut MetaRouter. MetaRouter menggunakan teknik virtualisasi yang terdapat pada mikrotik untuk penerapan virtualisasi ataupun virtualisasi pada topologi jaringan. Teknik Virtualisasi digunakan untuk menciptakan versi virtual atau bukan fisik dari sebuah sistem operasi komputer, sumber daya jaringan komputer, atau perangkat penyimpanan.

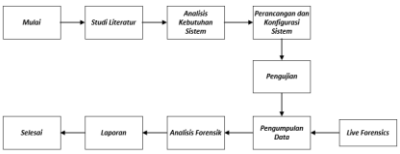
Serangan *Denial of Service* merupakan sebuah serangan yang sering dilakukan untuk menyerang server di jaringan dengan cara menghabiskan sumber yang dimiliki oleh server sehingga menyebabkan server tidak bisa menjalankan fungsinya sebagai penyedia akses ke layanan. Serangan ini bekerja dengan meminta layanan kepada server secara terus menerus sehingga membuat server menjadi *down.*

Dalam penelitian yang dilakukan oleh (Yasin et al., 2021) dengan judul "Identifikasi Bukti Forensik Jaringan Virtual Router Menggunakan Metode NIST" hasil yang didapat dari pengujian forensik dengan menggunakan metode *National Institute of Standard and Technology* (NIST) pada sistem forensik yang telah dibangun dengan objek virtual router, dapat digunakan investigator sebagai identifikasi bukti serangan siber. Pada penelitian yang dilakukan oleh (Firmansyah et al., 2019) dengan judul "Analisis Forensik MetaRouter pada Lalu Lintas Jaringan Klien" menghasilkan bahwa MetaRouter sangat berguna untuk tujuan memecah jaringan jika router yang dimiliki hanya 1 (satu) unit, penelitian tersebut fokus membahas mengenai paket badai ARP yang menyerang MetaRouter untuk mengurangi bandwidth dengan tujuan yang menyerang server. Pada penelitian ini penulis menggunakan protokol ICMP dengan menggunakan *ping* untuk mengetahui respon yang terjadi selama jaringan berlangsung dan terhubung satu sama lain. Berdasarkan latar belakang tersebut, penulis menyusun penelitian ini dengan judul **"**Simulasi Jaringan Virtual MetaRouter Untuk Mendeteksi Serangan *Denial of Service* Menggunakan Wireshark**".**

2. METODOLOGI PENELITIAN

Tahapan Penelitian

Berikut merupakan tahapan penelitian yang digunakan untuk memudahkan proses penelitian ini.



Gambar Tahapan Penelitian

Studi Literatur

Studi literatur merupakan tahap untuk mempelajari referensi teori yang berhubungan dengan kasus atau permasalahan yang ditemukan. Tahap ini dilakukan dengan cara mencari sumber tulisan yang pernah dibuat atau dipublikasi sebelumnya. Melalui studi literatur yang dilakukan dihasilkan beberapa teori yang dapat membantu penelitian ini, seperti teori mengenai MetaRouter, *Denial of Service*, serta teori tentang analisis forensik.

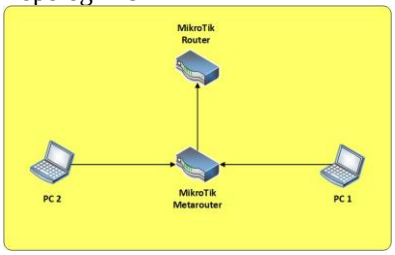
Analisis Kebutuhan Sistem

Tahap analisis kebutuhan sistem merupakan tahap yang diperlukan untuk mengetahui kebutuhan perangkat, baik perangkat keras (*hardware)* atau pun perangkat lunak (*software)* yang diperlukan selama proses penelitian dilakukan dan memutuskan diperlukan atau tidak adanya pengembangan sistem yang baru pada penelitian. Berdasarkan analisis kebutuhan sistem yang dilakukan dapat diketahui bahwa dalam penelitian ini memerlukan satu buah RouterBoard , dua buah laptop, dan beberapa *software* lainnya.

Perancangan dan Konfigurasi Sistem

Perancangan dan konfigurasi merupakan proses yang bertujuan untuk menyusun suatu sistem yang akan dibangun, baik sistem fisik maupun non fisik dengan memanfaatkan informasi yang ada.

Topologi Fisik

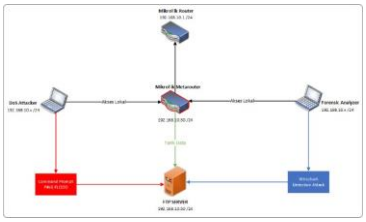


Gambar Topologi Fisik

ISSN 2337-6805

Pada penelitian ini menggunakan satu buah MikroTik Router dengan jenis RB951Ui-2Hnd yang didalamnya terdapat router virtual atau MetaRouter yang berfungsi menghubungkan perangkat. Penelitian ini menggunakan dua buah laptop dengan fungsi berbeda yang saling terkoneksi dengan MetaRouter dalam satu jaringan *Local Area Network* (LAN) dengan menggunakan kabel tunggal sebagai media transfer jenis kabel adalah UTP CAT5E.

Topologi Logik



Gambar Topologi Logik

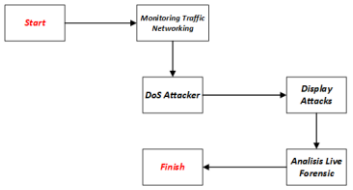
Berdasarkan gambar topologi logik di atas dapat diketahui bahwa PC 1 yang berfungsi sebagai *Forensic Analyzer* terhubung satu jaringan *Local Area Network* (LAN) dengan MetaRouter dan juga PC 2 yang berfungsi sebagai *DoS Attacker*. FTP Server pada MetaRouter digunakan dengan tujuan untuk berbagi data dengan komputer lain. PC 2 melakukan penyerangan *Denial of Service* terhadap FTP Server pada MetaRouter menggunakan protokol ICMP berupa *ping flood.* Kemudian pada PC 1 akan mendeteksi serangan menggunakan aplikasi *Wireshark* dan juga dilakukan analisis dengan menggunakan metode *Live Forensic.*

Tabel Pengalokasian IP Address

Nama Perangkat	IP Address
MikroTik MetaRouter	192.168.10.1 /24
PC1/*Forensic Analyzer*	192.168.10.x /24
PC 2/*DoS Attacker*	192.168.10.x /24

Alur Analisis Serangan DoS Pada MetaRouter

Pada tahap simulasi serangan *Denial of Service* pada MetaRouter bertujuan untuk memperoleh data sebagai bukti terjadinya serangan *Denial of Service* pada jaringan dengan menggunakan metode *Live Forensic* dibantu dengan menggunakan aplikasi *Wireshark.*



Gambar Alur Analisis Serangan DoS Pada MetaRouter

Pengujian

Tahap pengujian merupakan tahapan yang penting dalam sebuah penelitian. Pengujian dilakukan dengan tujuan untuk memastikan kualitas sistem. Proses pengujian dapat dilakukan dengan cara mengevaluasi konfigurasi sistem yang terdiri dari spesifikasi kebutuhan, deskripsi perancangan, dan program yang dihasilkan.

Pada tahap pengujian ini, PC *Attacker* melakukan penyerangan terhadap FTP Server berupa ICMP *PING Flood* dengan menggunakan PsTools. Kemudian PC Analisis Forensik mendeteksi serangan dan melakukan pengambilan data dengan menggunakan aplikasi *Wireshark.*

Pengumpulan Data

Pengumpulan data dilakukan untuk mengumpulkan data atau informasi yang akan dianalisis pada tahap selanjutnya. Pengumpulan data pada penelitian ini dilakukan dengan cara pengamatan dan studi pustaka.

Setelah dilakukan tahap pengumpulan data diperoleh beberapa data antara lain *IP Address List*, Protokol yang digunakan oleh penyerang, MAC Address penyerang dan target, *Source Port, Destination Port*, riwayat CPU dan memori sebelum dan setelah dilakukan serangan *Denial of Service*.

Analisis Forensik

Melalui *Wireshark* dapat diketahui informasi atau data tentang *Log Activity* yang berisikan tentang informasi dari aktivitas apa saja yang terdapat pada router terkait perubahan konfigurasi dan *IP Address List* penyerang yaitu informasi tentang pelaku penyerangan. Data atau informasi yang dapat digunakan sebagai bukti digital dapat meliputi *Log Activity*, *Log Traffic*, *IP Address*, dan *MAC Address*.

Setelah mendapatkan data atau informasi yang dibutuhkan, kemudian dilakukan *monitor system traffic* terhadap serangan *Denial of Service* pada MetaRouter. Hal tersebut dikarenakan adanya proses terhubungnya komputer investigator dengan jaringan dan aktivitas permintaan data yang dilakukan melalui service WinBox pada Router.

Laporan

Dalam tahap ini dilakukan untuk melaporkan data temuan hasil analisis serangan *Denial of Service* terhadap MetaRouter dan menjelaskan apa yang telah dianalisis kemudian dipaparkan barang bukti yang telah ditemukan dan didokumentasikan secara rinci.

ISSN 2337-6805

Instrumen Penelitian

Instrumen penelitian merupakan alat-alat yang digunakan yang bertujuan untuk mengumpulkan data.

Perangkat Keras

1. MikroTik RB951Ui-2HnD

Perangkat ini merupakan router *gateway* pada jaringan komputer yang digunakan untuk membangun jaringan virtual MetaRouter.

2. Laptop ASUS VivoBook X407UF

Perangkat ini digunakan untuk melakukan konfigurasi pada MikroTik dan berfungsi sebagai *Forensc Analyzer*.

3. Laptop Acer Aspire V5-431

Perangkat ini digunakan sebagai *attacker* yang melakukan serangan *Denial of Service* pada jaringan virtual MetaRouter.

Perangkat Lunak

1. Sistem operasi RouterOS
2. Sistem operasi Windows 10 Home Single Language
3. Sistem operasi Windows 8
4. WinBox v3.27 64-bit
5. Wireshark 64-bit

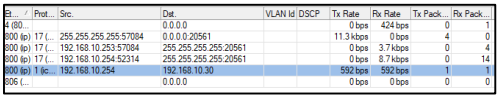
Penerapan *Firewall Rules* Pada MetaRouter

Pada penelitian ini membahas mengenai simulasi serangan *Denial of Service* pada MetaRouter, sehingga diperlukan sebuah sistem yang dapat mencegah akses atau paket data yang tidak diinginkan. Oleh karena itu pada penelitian ini menerapkan *Firewall Rules* pada MetaRouter yang bertujuan untuk mencegah akses atau paket data yang tidak diinginkan. *Firewall Rules* menerapkan *packet filtering* untuk mengatur aliran data. Dengan adanya *firewall rules* data yang masuk atau keluar dapat dikendalikan dan dapat menentukan pada data yang masuk atau keluar untuk dilewati, dijatuhkan, atau ditolak.

3. HASIL DAN PEMBAHASAN

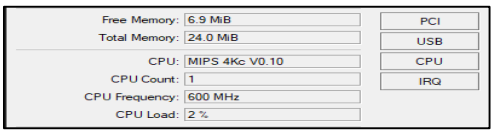
Analisis Komunikasi Data Sebelum Simulasi Serangan

Pada penelitian ini, penulis menggunakan metode *Live Forensic* untuk melakukan pengumpulan data atau bukti. Tahap awal dalam analisis ini adalah melakukan pemeriksaan terhadap keadaan MetaRouter sebelum terjadinya serangan *Denial of Service*. Pemeriksaan tersebut dapat diketahui melalui menu *Torch Running* yang terdapat pada MikroTik RouterOS. Melalui pemeriksaan terhadap *Torch Running* ini dapat diketahui bahwa belum terdapat sebuah serangan yang dapat dilihat melalui indikator *Tx Rate* dan *Rx Rate* pada *Destination Traffic*.



Gambar Tampilan *Torch Running* Sebelum Terjadinya Serangan DoS

Pengujian ini berdampak pada penggunaan CPU dan *memory*. Oleh karena itu, penulis juga melakukan analisis terhadap penggunaan CPU dan Memori pada perangkat jaringan tersebut. Analisis tersebut dilakukan sebelum dan setelah terjadi serangan *Denial of Service*.

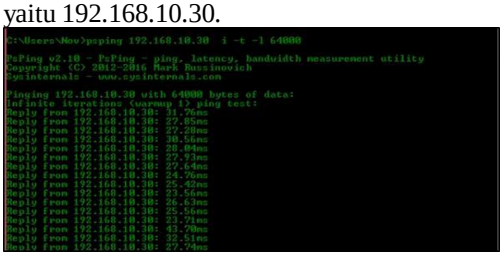


Gambar Tampilan Kondisi CPU dan *Memory* Sebelum Terjadinya Serangan DoS

Gambar di atas menunjukkan bahwa penggunaan CPU dan Memori dalam keadaan normal karena belum terjadi serangan *Denial of Service* yang mempengaruhi performa kinerja pada perangkat.

Pengujian Sistem Menggunakan Aplikasi

Tujuan dari tahap pengujian ini adalah untuk menguji sistem yang telah dibuat apakah berhasil mendeteksi serangan *Denial of Service* terhadap MetaRouter dengan menggunakan metode *Live Forensic*. Pengujian ini dilakukan dengan simulasi serangan DoS melalui PC *attacker* menggunakan aplikasi PsTools dengan protokol ICMP melalui *Command Prompt*. Pengujian dilakukan dengan mengirim serangan *Ping Flooding* ke *IP Address* target yaitu 192.168.10.30.

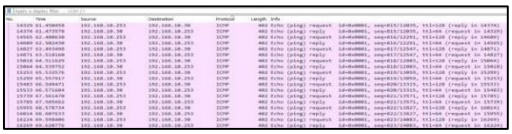


Berdasarkan gambar di atas dapat dilihat bahwa *Ping Flood* berhasil dijalankan dan menyerang jaringan target. Setelah serangan berhasil dilakukan, maka tahap yang perlu dilakukan berikutnya adalah melakukan pengecekan serangan yang masuk melalui aplikasi *Wireshark*.

Pada tahap pengujian ini juga dilakukan *monitoring traffic* dengan menggunakan

ISSN 2337-6805

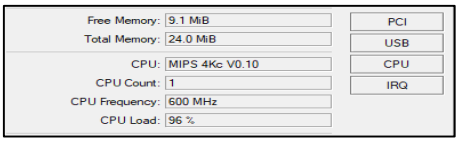
Wireshark kemudian penulis meng-*capture* aktivitas jaringan yang menunjukan adanya serangan *Denial of Service.*



Gambar Tampilan *Wireshark* Mendeteksi Serangan
Denial of Service

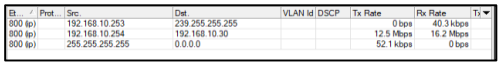
Gambar di atas menunjukkan bahwa trafik yang tidak biasa menunjukan adanya aktivitas serangan *Denial of Service* menggunakan protokol ICMP yaitu *Ping Flood* dari *Source* IP 192.168.10.253 yang melakukan *attack* terhadap target. Pengujian ini dilakukan secara kontinu sehingga menyebabkan MikroTik MetaRouter maupun MikroTik Router menjadi *down*.

Simulasi serangan ini menimbulkan perangkat MikroTik Router melakukan *restart* dengan sendirinya yang dikarenakan kelebihan beban terhadap CPU dan *Memory*.



Gambar Tampilan Kondisi CPU dan *Memory* Setelah Serangan DoS

Gambar di atas menunjukkan bahwa keadaan CPU Load dan *memory* mengalami peningkatan. Hal itu yang menyebabkan *down* pada lalu lintas jaringan dikarenakan adanya aktivitas serangan *Denial of Service.*



Gambar *Traffic Data* Saat Terjadi Serangan DoS Gambar di atas menunjukkan bahwa terjadi

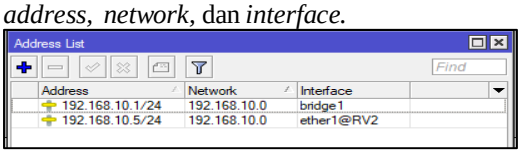
peningkatan pada *Tx Rate* yakni sebesar 12.5 Mbps dan *Rx Rate* menjadi sebesar 16.2 Mbps. Hal tersebut menandakan bahwa serangan *Denial of Service* menyebabkan peningkatan pada *traffic rate*.

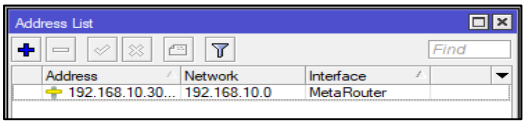
Pemerolehan Data

Pada proses pengujian dilakukan pengambilan data yang dijadikan sebagai bukti bahwa telah terjadi serangan *Denial of Service* terhadap jaringan dengan menggunakan metode *Live Forensic*. Pengambilan data dilakukan dalam kondisi sistem sedang *running*, hal ini disebabkan terdapat beberapa informasi jaringan yang akan hilang jika sistem dimatikan.

IP Address List

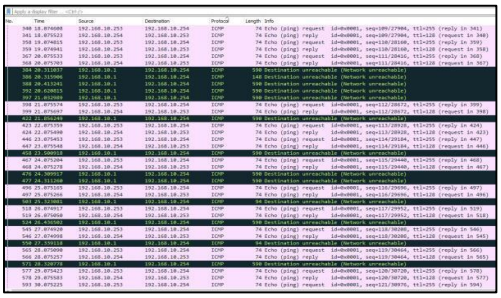
Penelitian ini menggunakan DHCP Server untuk mendistribusikan alamat IP secara otomatis terhadap *client.* IP Address List berguna sebagai penanda atau catatan alamat IP yang terdapat pada suatu jaringan. *IP Address List* yang ditampilkan berisikan *address, network,* dan *interface.*





Log Activity

Log activity diperlukan untuk mengetahui seluruh kegiatan pengguna dalam menggunakan program aplikasi. Melalui *log activity* ini diperoleh beberapa data seperti *Time, Source IP, Destination IP, Protocol,* dan *Info.*

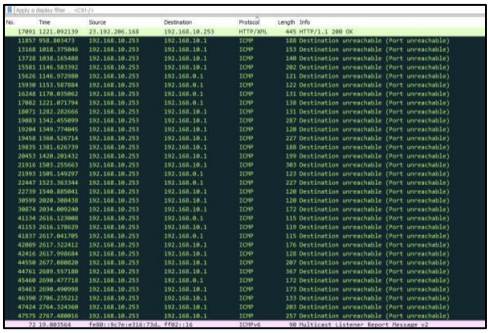


Gambar *Log Activity* Serangan pada MetaRouter

Log activity diatas menunjukan adanya aktivitas serangan DoS terhadap MetaRouter. Hal tersebut dapat diketahui melalui *Time* dan *Message IP Address* 192.168.10.253 yang secara kontinu menyerang pada protokol MetaRouter. Dapat dilihat bahwa target tetap dapat melakukan *request* dan *reply* permintaan ICMP yang berarti sistem tujuan dalam keadaan aktif. namun terdapat beberapa *log unreachable* yang dihasilkan oleh *gateway inbound* untuk menginformasikan bahwa tujuan tidak dapat diakses. Hal ini dapat dilihat bahwa *traffic rate* mulai tidak dapat melakukan *reply* atau memproses permintaan ICMP.

Dalam rentang waktu 18.074608 sampai dengan 30.075225 mulai terlihat terdapat kegagalan login yang cukup banyak sehingga aktivitas ini dicurigai sebagai aktivitas yang tidak wajar dalam sebuah komunikasi data.

ISSN 2337-6805



Gambar Hasil Serangan DoS Saat Target *Down*

Gambar di atas menunjukkan bahwa *traffic* tidak dapat melakukan *reply* terhadap permintaan ICMP sehingga reaksi yang terjadi dikembalikan kepada alamat *gateway*. Hal itu membuktikan bahwa serangan yang terjadi dapat menghambat permintaan data pada tujuan selanjutnya.

Hasil Pengujian Serangan *Denial of Service* Terhadap MetaRouter

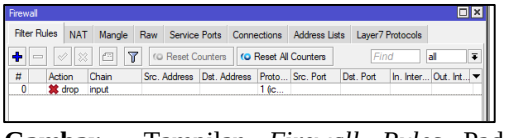
Pengujian ini berhasil melakukan serangan terhadap MetaRouter secara kontinu sehingga mengakibatkan jaringan menjadi down. Setelah dilakukan pengujian pada penelitian ini, maka diperoleh hasil yang dapat dijadikan sebagai laporan 7omputer jaringan sehubung dengan proses analisis 7omputer serangan *Denial of Service* terhadap MetaRouter yang telah dilakukan.

Tabel Hasil Serangan *DoS* Terhadap MetaRouter

No.	Indikator	Sebelum Terjadi Serangan	Setelah Terjadi Serangan
1.	*Tx Rate*	592 bps	12,5 Mbps
2.	*Rx Rate*	592 bps	16,2 Mbps
3.	CPU	2%	96%
4.	*Memory*	6,9 MiB	9,1 MiB

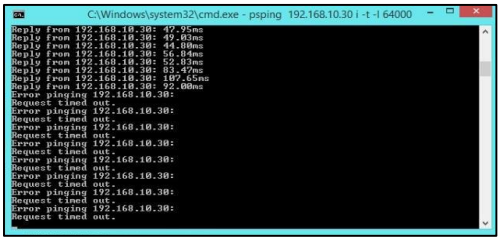
Hasil Penerapan *Firewall Rules*

Pada penelitian ini menerapkan *firewall rules* pada MetaRouter sebagai solusi jika terjadi serangan *Denial of Service*. *Firewall rules* merupakan salah satu fitur yang diberikan oleh MikroTik untuk diterapkan pada sistem keamanan jaringan komputer. Melalui penggunaan *firewall rules* ini *client* dapat membatasi hak akses pada *IP Address* yang dinilai kurang baik atau mencurigakan untuk pengguna jaringan.



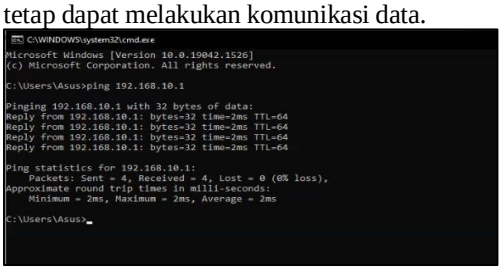
Gambar Tampilan *Firewall Rules* Pada MetaRouter

Penerapan *firewall rules* digunakan dengan *action drop* terhadap alamat IP asal. *Firewall rules* bekerja jika ditemukan *traffic* data pada MetaRouter, maka MetaRouter akan memeriksa paket data tersebut dan mencocokan dengan *rule* atau *filter* yang telah dibuat. Berdasarkan *rule* yang dibuat jika ditemukan paket data yang mencurigakan *action drop* dapat menentukan paket tersebut akan di *drop* atau *allow*. Pada penelitian ini *firewall rules* berhasil diterapkan.



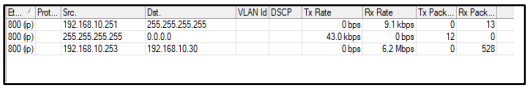
Gambar Tampilan CMD Saat *Firewall Rules* Diterapkan

Gambar di atas merupakan tampilan *command prompt* setelah adanya *firewall rules* pada MetaRouter. Dapat dilihat komputer server tidak merespon atau menjawab kembali permintaan *attacker*. *firewall rules* hanya melakukan *drop* pada alamat IP yang diduga mengirim paket data yang mencurigakan, sehingga dengan adanya *firewall rules* jaringan tetap dapat melakukan komunikasi data.



Gambar Tampilan Komputer *Client* Setelah Diterapkan *Firewall Rules*

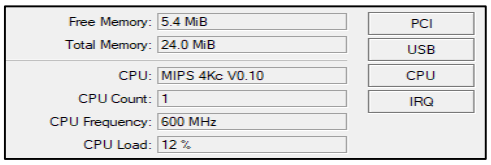
Gambar di atas menunjukkan bahwa computer *client* tetap bisa melakukan komunikasi data, hal ini dibuktikan dengan komputer *client* dapat melakukan *ping* terhadap alamat IP router yakni 192.168.10.1. *Firewall rules* berhasil diterapkan terhadap serangan *Denial of Service* pada MetaRouter, hal itu dibuktikan dengan penurunan nilai *Tx Rate* dan *Rx Rate* pada *Torch Running* yang sebelumnya mengalami peningkatan karena serangan *Denial of Service*.



Gambar Tampilan *Torch Running* Setelah Diterapkan *Firewall Rules*

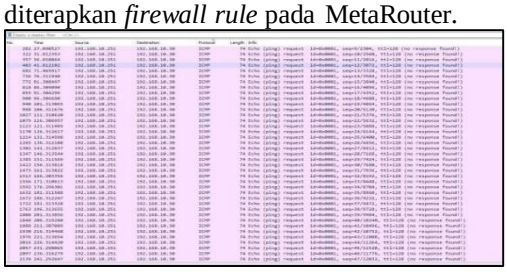
Selain terjadi penurunan pada *Torch Running*, CPU *Load* dan kapasitas memori juga mengalami penurunan.

ISSN 2337-6805



Gambar Tampilan CPU dan Memori Setelah Diterapkan *Firewall Rules*

Kedua gambar di atas menunjukkan bahwa jaringan mulai kembali berjalan normal. Tidak hanya melalui indikator diatas, tetapi perubahan terjadi pada *wireshark* setelah diterapkan *firewall rule* pada MetaRouter.



Gambar Tampilan *Wireshark* Setelah Diterapkan ***Firewall Rules***

Gambar di atas merupakan tampilan *Log Activity* pada *Wireshark*. Melalui gambar diatas dapat dilihat bahwa permintaan *attacker* tidak ditanggapi dengan adanya penerapan *firewall rules* berhasil melakukan *drop* pada protokol ICMP.

4. SIMPULAN

Simpulan

Setelah pengujian simulasi serangan *Denial of Service* pada MetaRouter dilakukan, maka dapat disimpulkan bahwa:

1. Proses pengujian simulasi serangan *Denial of Service* dilakukan menggunakan protokol ICMP yaitu *PING Flood* dan simulasi serangan berhasil dilakukan, hal tersebut dibuktikan dengan adanya perubahan atau peningkatan komunikasi data yang menyebabkan jaringan menjadi *down*.
2. Melalui pengujian yang dilakukan pada penelitian ini, terdapat beberapa data yang dapat dijadikan sebagai bukti digital meliputi protokol yang digunakan, port protocol penyerang, port *destination* target jaringan MetaRouter yang diserang, *Log Activity*, dan *IP Address List* penyerangan yang diperoleh melalui aplikasi *Wireshark*.
3. Penelitian ini berhasil mengatasi simulasi serangan *Denial of Service* pada MetaRouter dengan menggunakan *firewall rules*. *Firewall rules* berhasil melakukan *drop* pada alamat IP yang diduga mengirim paket data yang mencurigakan. Sehingga komputer server tidak merespon atau menjawab kembali permintaan *attacker*, namun komputer *client* tetap dapat melakukan komunikasi data.

Saran

Berdasarkan penelitian yang dilakukan, maka diperoleh beberapa saran atau usulan yang dapat dijadikan penelitian berikutnya, antara lain:

1. Pada penelitian ini analisis yang dilakukan masih cukup sederhana sehingga untuk penelitian selanjutnya dapat dilakukan pengembangan terhadap sistem untuk memperoleh hasil yang lebih baik untuk dijadikan sebagai bukti digital.
2. Penelitian ini hanya menggunakan aplikasi *Wireshark* sebagai alat analisis *traffic* jaringan. Oleh karena itu untuk penelitian selanjutnya akan lebih baik tidak terbatas pada penggunaan aplikasi *Wireshark* dan dapat menggunakan aplikasi lainnya untuk memaksimalkan hasil penelitian.

5. DAFTAR PUSTAKA

[1] Aji, S., Fadlil, A., & Riadi, I. (2017). Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik Jaringan. *Jurnal Ilmiah Teknik Elektro Komputer Dan Informatika*, *3*(1),11. https://doi.org/10.26555/jiteki.v3i1.5665

[2] Asmunin, A., & Hermawan, A. (2016). Penerapan dan Analisis Virtualisasi Router Menggunakan RouterOS. *Multinetics*, *2*(1), 31. https://doi.org/10.32722/vol2.no1.2016.pp31-34

[3] Fatriawans, R. (2017). *Pengertian Jaringan Router*. 1–5.

[4] Firmansyah, F., Fadlil, A., & Umar, R. (2019). Analisis Forensik Metarouter pada Lalu Lintas Jaringan Klien. *Edu Komputika Journal*, *6*(2), 54–59. https://doi.org/10.15294/edukomputika.v6i2.352 21

[5] Gustina, D., & Mutiara, D. (2017). Sistem Penunjang Keputusan Pemilihan Router Mikrotik dengan Menggunakan Metode AHP (Analitycal Hierarchy Process). *Jurnal Ilmiah FIFO*,*9*(1),68. https://doi.org/10.22441/fifo.v9i1.1443

ISSN 2337-6805

[6] Jaya, B., Yuhandri, Y., & Sumijan, S. (2020). Peningkatan Keamanan Router Mikrotik Terhadap Serangan Denial of Service (DoS). *Jurnal Sistim Informasi Dan Teknologi*, *2*, 115– 123. https://doi.org/10.37034/jsisfotek.v2i4.32

[7] Susanto, R. (2020). Rancang Bangun Jaringan Vlan dengan Menggunakan Simulasi Cisco Packet Tracer. *Jurnal Nasional Informatika Dan Teknologi Jaringan*, *4*(2), 1–6.

[8] Yasin, F., Abdul Fadlil, & Rusydi Umar. (2021). Identifikasi Bukti Forensik Jaringan Virtual Router Menggunakan Metode NIST. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *5*(1),91–98. https://doi.org/10.29207/resti.v5i1.2784

[9] Zulkarnain. (2020). Analisis Keamanan FTP server Menggunakan Serangan Man-In-The- Middle Attack. *Telcomatics*, *5*(1), 12–18. https://doi.org/10.37253/telcomatics.v5i1.851