VARIABLE RESEARCH JOURNAL
Volume 01, Number 02, July 2024
E-ISSN: 3032-4084
Open Access

PENERAPAN METODOLOGI *LIVE FORENSIC* PADA ROUTER MIKROTIK TERHADAP SERANGAN *DOS (DENIAL OF SERVICE)* (STUDI KASUS DI DINAS KOMUNIKASI DAN INFORMATIKA KOTA BUKITTINGGI)

APPLICATION OF LIVE FORENSIC METHODOLOGY ON MIKROTIK ROUTERS AGAINST DOS (DENIAL OF SERVICE) ATTACKS (CASE STUDY IN THE COMMUNICATION AND INFORMATICS DEPARTMENT OF BUKITTINGGI CITY

Afriadi Syahputra
Magister Teknik Informatika, Universitas Putra Indonesia YPTK Padang, Padang, Indonesia
Email: afriadi.bkt@gmail.com

ARTICLE INFO

Article history:
Received May 16, 2024
Revised June 16, 2024
Accepted July 15, 2024
Available online July 15, 2024

Kata Kunci:
Serangan DoS (Denial of Service), Router, Network Forensics, router dan Fastream Web Stress Tester

Keywords:
Denial of Service (Denial of Service), Router, Network Forensics, router dan UDP Fastream Web Stress Tester

ABSTRAK

Serangan *Denial of Service* (DoS) pada perangkat *router* dapat menyebabkan kerusakan pada jaringan dan menghambat konektivitas. Penerapan metode Network Forensik dapat digunakan untuk menganalisis serangan DoS pada perangkat router. Metode ini meliputi tahap-tahap seperti perangkat *router*. Metode ini meliputi tahap-tahap seperti analisis data, investigasi dan presentasi hasil. Dari proses penyerangan yang di analisa bahwa serangan DoS menggunakan aplikasi *Fastream Web Stress Tester* dengan cara mengirim pesan secara bertubi-tubi sehingga membuat jaringan *Router* menjadi *Down.* Penerapan metode *Live Forensik* dapat digunakan untuk menganalisis serangan DoS pada perangkat router dan membantu dalam mengambil tindakan untuk mencegah serangan selanjutnya. Namun, metode ini memerlukan pengalaman dan keahlian khusus dalam bidang jaringan dan forensik..

ABSTRACT

Denial of Service (DoS) attacks on router devices can cause damage to the network and hinder connectivity. The application of the Network Forensic method can be used to analyze DoS attacks on router devices. This method includes stages such as preparation, incident handling, data collection, preservation, data analysis, investigation and presentation of results. From the attack process, it is analyzed that the DoS attack uses the Fastream Web Stress Tester application by sending messages repeatedly so that the router network goes down. The application of the Network Forensic method can be used to analyze DoS attacks on router devices and assist in taking action to prevent further attacks. However, this method requires special experience and expertise in networking and forensics

PENDAHULUAN

Salah satu tantangan keamanan yang paling serius yang dihadapi oleh organisasi dan institusi pemerintahan adalah serangan *DoS (Denial of Service)*. Serangan *DoS (Denial of Service)* merupakan salah satu serangan terhadap situs, jaringan, *router firewall* dan *server* yang sangat sering terjadi. Serangan *DoS (Denial of Service)* bertujuan untuk membuat jaringan *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* (Arief Indriarto et al., 2022).

Denial of Service (DoS) adalah jenis serangan yang dilakukan dengan cara membanjiri lalu lintas jaringan pada aplikasi pada *server*, sistem, atau *website*. Umumnya serangan ini dilakukan

untuk membuat lalu lintas server berjalan dengan beban yang berat sampai tidak bisa lagi menampung koneksi dari *user* lain atau overload. (Central Data Teknologi 2022)

Serangan *DoS (Denial of Service)* menyebabkan kerugian besar dalam hal gangguan operasional, kerugian finansial, dan kerusakan reputasi bagi organisasi yang menjadi sasaran, dan juga dapat digunakan sebagai serangan pengalihan perhatian yang memungkinkan penyerang untuk mengeksploitasi celah keamanan lainnya (Singgih Mitro S dan Dadan Sukma 2023)

Terkait Ancaman Digital di Indonesia Semester II-2023, terdapat rata-rata 155.292 serangan siber per jam di Indonesia sepanjang paruh kedua tahun 2023 atau sekitar 43 serangan siber per detik. Serangan siber meningkat 97,53 persen pada semester II (Juli-Desember)-2023, atau hampir dua kali lipat dari semester I (Januari hingga Juni)-2023, dengan jumlah serangan siber mencapai 347.172.666 atau 22 serangan siber per detik dengan total serangan mencapai 685.772.501 serangan atau hampir dua kali lipat dari semester sebelumnya, menunjukkan Indonesia sebagai sasaran favorit penjahat dunia maya. (awanpintar.id)

Pusat Operasi Keamanan Badan Siber dan Sandi Negara (BSSN) mencatat jumlah serangan siber yang terjadi di Indonesia antara Januari hingga Juli 2021 sebanyak 741.441.648 kali (GOV-CISRT 2021) Jumlah serangan itu mengalami peningkatan hampir dua kali lipat dibandingkan seluruh anomali trafik yang dideteksi oleh lembaga siber tersebut selama tahun sebelumnya yang mencapai kurang lebih 495 juta kali.

Kategori serangan siber atau anomali trafik yang terbanyak dideteksi di Indonesia, antara lain berupa perangkat lunak jahat (malware), *DoS (Denial of Service)* yang mengganggu aplikasi berbasis *web* dengan banjir permintaan palsu ke *server* dan ketiga aktivitas trojan. (Aldhyani & Alkahtani, 2023)

Diantara banyaknya serangan yang sering terjadi di Internet adalah serangan *DoS (Denial of Service)* merupakan jenis serangan jaringan komputer yang dapat mengakibatkan server tidak mampu melayani permintaan *User,* hingga menyebabkan jaringan komputer menjadi *down*.(Mitro & Sukma, n.d.-b)

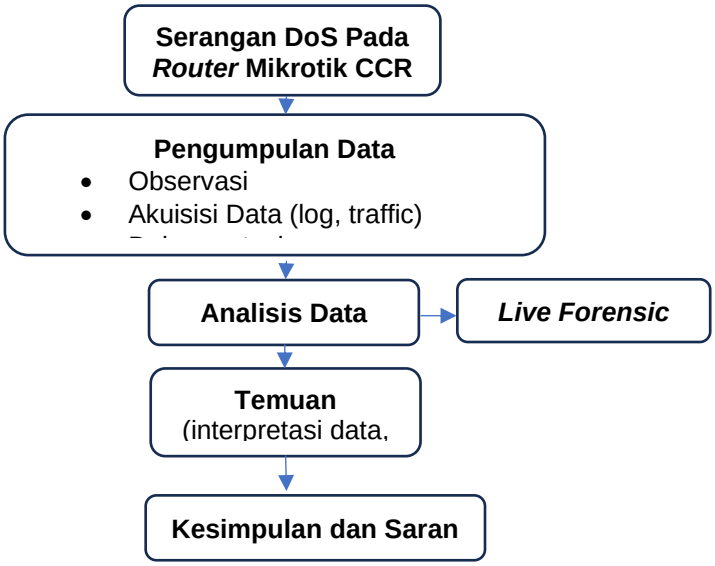
Penyebab utama dari masalah forensik jaringan adalah tindak penyalahgunaan teknologi oleh orang-orang yang tidak bertanggung jawab dengan tujuan memanfaatkan fasilitas jaringan pihak lain untuk kepentingan pribadi maupun kelompok.(Aldhyani & Alkahtani, 2023)

METODE

Kerangka Pemikiran

Kerangka pemikiran ini menggambarkan alur proses penelitian yang akan dilakukan, dimulai dari insiden serangan DoS pada *router* Mikrotik CCR 1072 di Dinas Komunikasi dan Informatika Kota Bukittinggi. Selanjutnya, akan dilakukan pengumpulan data melalui berbagai teknik seperti observasi, akuisisi data log dan bukti digital, serta studi dokumentasi terkait.

Data-data yang telah dikumpulkan kemudian akan dianalisis menggunakan dua pendekatan utama, yaitu *network forensic* dan *live forensic*. Analisis *network forensic* meliputi filtering data, rekonstruksi kejadian, analisis jejak, dan interpretasi temuan. Sementara analisis *live forensic* meliputi pemeliharaan lingkungan *live*, akuisisi data live, analisis data *live*, dan korelasi temuan dengan hasil *network forensic*.



Gambar 2.1 Alur proses penelitian

Dari hasil analisis metode tersebut, akan dilakukan korelasi temuan untuk mendapatkan gambaran yang komprehensif tentang pola serangan DoS yang terjadi, motif, dan dampaknya. Selanjutnya, akan diberikan rekomendasi mitigasi untuk mencegah serangan serupa di masa mendatang.

Teknik Pengumpulan Data

Teknik pengumpulan data pada penelitian ini menggunakan teknik sebagai berikut:

1. Observasi
   Observasi akan dilakukan pada router Mikrotik CCR 1072 yang menjadi sasaran serangan DoS. Hal ini bertujuan untuk mengamati secara langsung kondisi perangkat, konfigurasi, dan mengidentifikasi potensi bukti digital yang terkait dengan serangan tersebut.

2. Akuisisi Data
   Teknik ini dilakukan untuk mengumpulkan data-data penting seperti log router, data lalu lintas jaringan (*network traffic*), dan bukti digital lainnya yang relevan dengan kasus serangan DoS. Akuisisi data dapat dilakukan dengan menggunakan tools forensik yang sesuai, *seperti packet sniffer*, *disk imaging*, dan lain-lain.

3. Studi Dokumentasi
   Mempelajari dokumentasi terkait seperti kebijakan keamanan jaringan, prosedur operasional standar (SOP), laporan insiden, dan dokumentasi teknis lainnya yang relevan dengan kasus serangan DoS pada *router* Mikrotik CCR 1072.

Dalam proses pengumpulan data, peneliti akan memperhatikan prinsip-prinsip forensik seperti menjaga integritas bukti digital, meminimalkan perubahan pada sistem yang dianalisis, dan mendokumentasikan setiap langkah yang dilakukan dengan baik. Selain itu, peneliti juga harus mempertimbangkan aspek hukum dan etika dalam proses pengumpulan data tersebut.

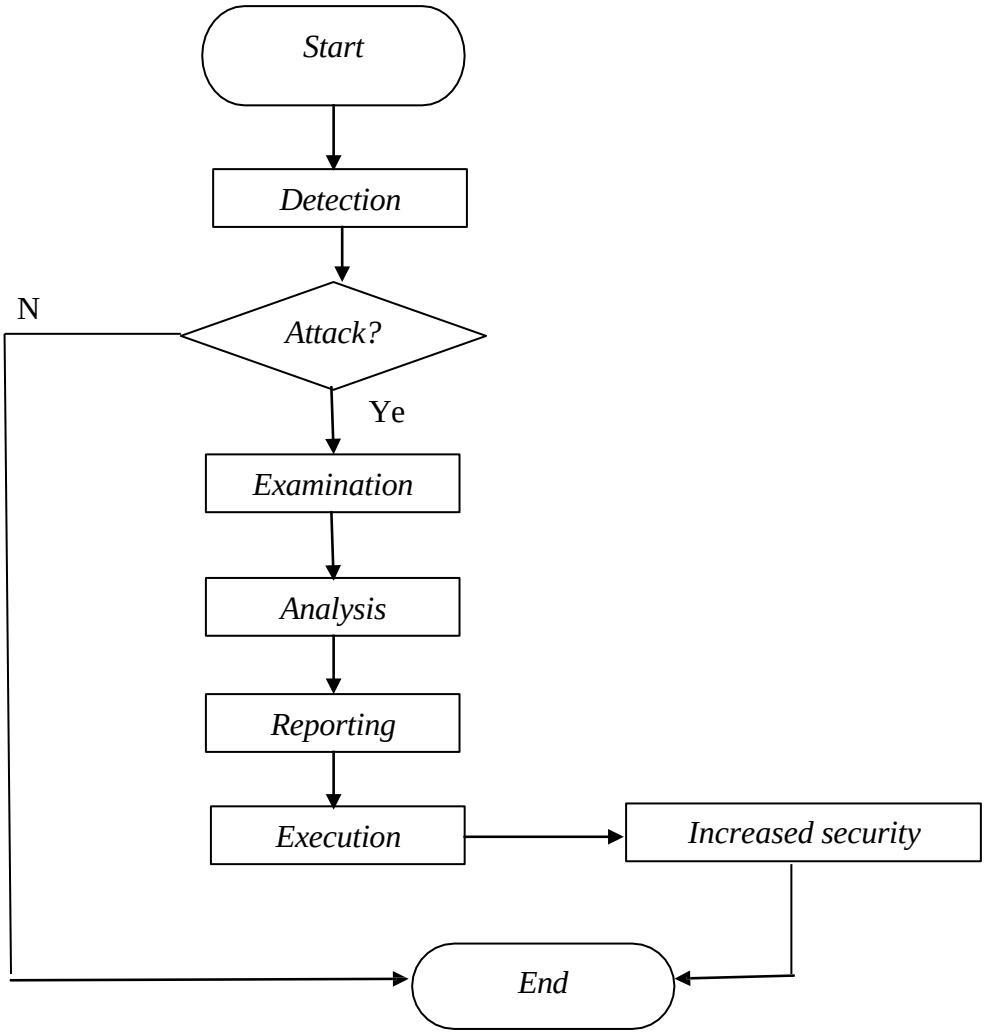
Analisis Live forensic

Pada bagian ini, penulis akan melakukan analisis forensik secara *live* atau langsung pada router Mikrotik CCR 1072 yang diserang. Tahapan analisis *live forensic* dapat meliputi:

1. Pemeliharaan lingkungan live (*live environment preservation*) untuk Memastikan kondisi *router* dan lingkungannya tidak berubah selama proses akuisisi dan analisis data.
2. Akuisisi data *live* (*live data acquisition*) untuk mengumpulkan data dari memori, proses, koneksi jaringan, dan komponen sistem lainnya pada router saat masih dalam keadaan hidup/menyala.
3. Analisis data *live* (*live data analysis*) untuk menganalisis data-data yang diperoleh dari akuisisi live, seperti proses yang berjalan, koneksi aktif, dan potensi indikator serangan DoS pada sistem *router*.
4. Korelasi temuan untuk mengaitkan dan mengkorelasikan temuan dari analisis *live forensic* dengan hasil analisis *network forensic* untuk mendapatkan gambaran yang lebih komprehensif.

Metode *Live Forensic* pada penelitian ini ada 6 tahapan yaitu: *Detection, Examination, Analysis, Reporting Execution dan increased security.*

Live Forensics memainkan peran yang penting selama pemeriksaan sistem karena potensi ketersediaan bukti digital yang mudah hilang, seperti proses yang sedang berjalan, koneksi jaringan, *Port*, yang terbuka dan kunci enkripsi, dan lainnya. Tahapan metode *Live Forensics* dalam penelitian ini dapat digambarkan dalam bentuk *flowchart* agar terlihat lebih jelas dan terarah. *Flowchart Live Forensics* yang dimaksud dapat dilihat pada Gambar 2.2 berikut ini:



Gambar 2.2 *Flowchart Live Forensics*

Keterangan dari gambar 3.2 tentang *flowchart live forensics* adalah :

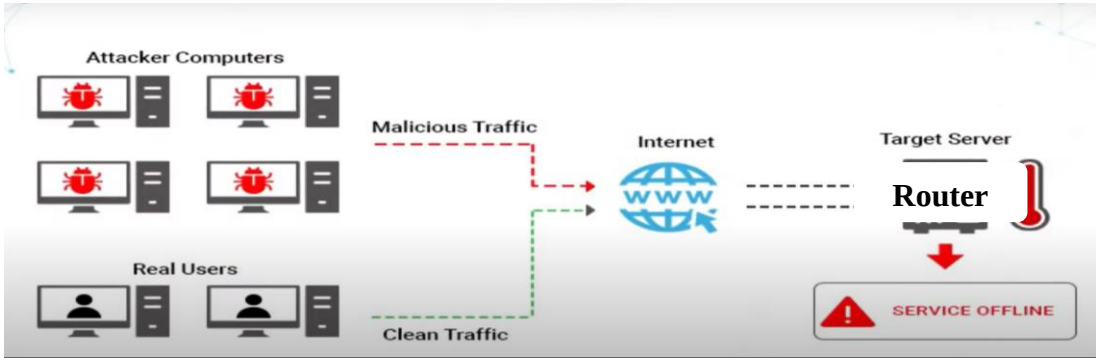
1. *Detection,* tahap ini merupakan langkah awal dalam mendeteksi apakah terjadi serangan *DoS* pada *Router Mikrotik* atau tidak. Pada tahap ini yang dilakukan adalah mendeteksi dan mencari bukti-bukti, pengenalan terhadap bukti-bukti penyusupan, dan pengumpulan bukti.
2. *Examination,* Pada tahap ini pencarian informasi yang tersembunyi dan mengungkapkan dokumentasi yang relevan. Pemeriksaan menggunakan *software Winbox RouterOS* semisal memeriksa urutan *packet*, jumlah *packet* data, dan lain-lain.
3. *Analysis*, dilakukan untuk menjawab pertanyaan forensik yaitu apa yang terjadi, *IP Address* siapa yang melakukan serangan, kapan serangan tersebut terjadi, dimana serangan tersebut terjadi, dan bagaimana serangan tersebut terjadi. Analisis bisa dilakukan dengan menggunakan *software Wireshark.*
4. *Reporting,* Berdasarkan hasil temuan dengan menggunakan aplikasi *Wireshark* berupa informasi mengenai *IP* penyerang, *log activity*, dan *traffic network*, maka selanjutnya dilakukan akuisisi data.
5. *Execution,* bukti dan hasil analisis forensik jaringan yang sudah diperoleh, kemudian bisa dijadikan rujukan dalam melakukan peningkatan keamanan pada *Router Mikrotik* terutama dari serangan *DoS.*

Increased Security, Peningkatan keamanan jaringan *Router Mikrotik* bisa dilakukan dengan menggunakan *Firewall*. *Firewall* merupakan sebuah sistem atau perangkat yang mengizinkan lalu lintas jaringan yang dianggap aman untuk melaluinya dan mencegah lalu lintas jaringan yang tidak aman.

HASIL DAN PEMBAHASAN

Simulasi Serangan Dos Pada *Router*

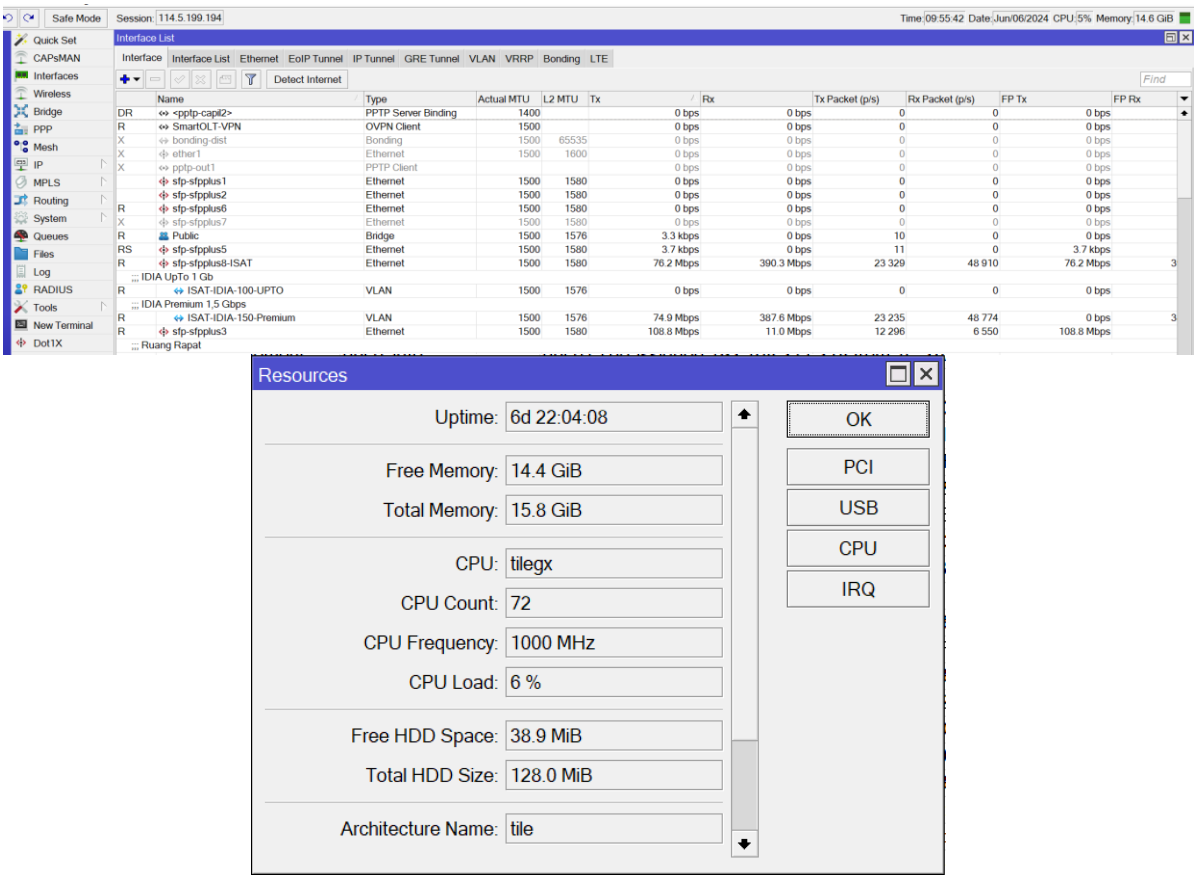
DoS dapat dilakukan dengan menyalah gunakan perangkat, memanipulasi perangkat lunak dan aplikasi, atau mengganggu saluran komunikasi. Salah satu serangan DoS adalah serangan gangguan di mana saluran komunikasi mampu menonaktifkan saluran komunikasi sensor dari membawa sinyal dengan menghasilkan tabrakan. Tabrakan akan menyebabkan pesan komunikasi terganggu. Berikut rancangan simulasi serangan DoS pada *Router* menggunakan DNS *Flooding*, dan analisis serangan pada *Router* menggunakan aplikasi *Winbox.*



Gambar 3.1 Desain Analisis Serangan DoS pada *Router*

Pengujian Menggunakan Aplikasi

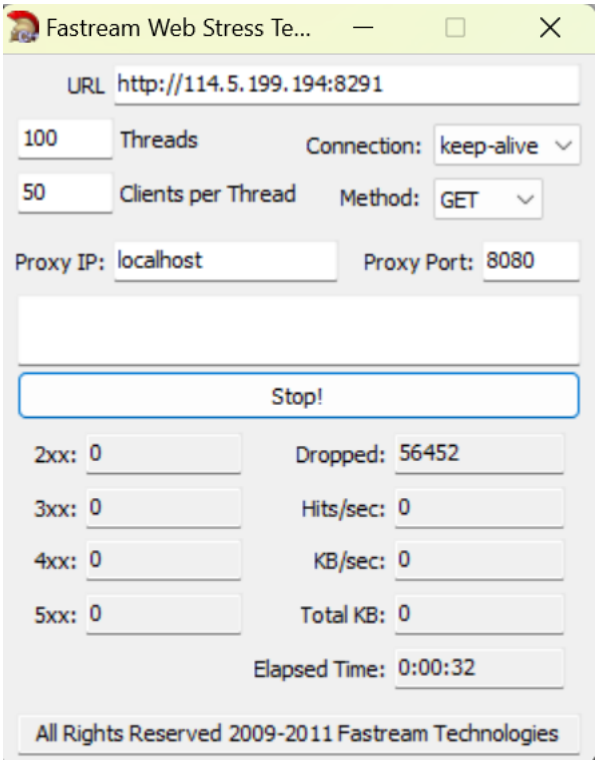
Proses awal untuk analisis apakah *Router* masih dalam keadaan normal atau sudah ada serangan DoS, dapat dilakukan melalui pengecekan pada menu *WinBox*.



Gambar 3.2 Tampilan Sebelum Ada Serangan DoS

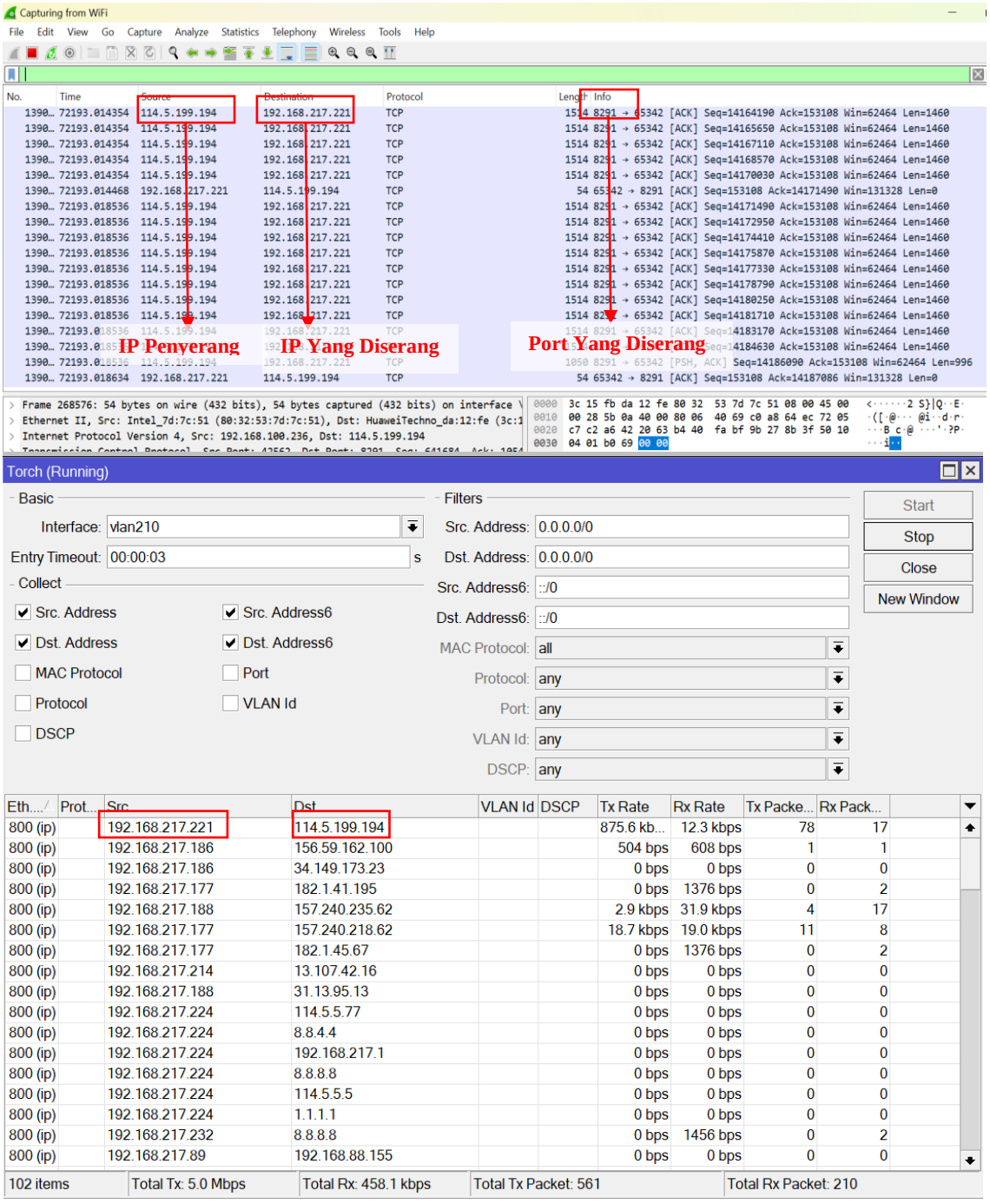
Berdasarkan tampilan Proses awal pengecekan seperti gambar di atas , dapat disimpulkan belum ada serangan yang masuk dan menganggu lalu-lintas jaringan pada *Router*. Hal inid apat dilihat

pada kolom merah CPU & *Memory* masih normal. Langkah berikutnya adalah mulai melakukan simulasi serangan DoS pada Router menggunakan aplikasi *Fastream Web Stress Tester* untuk mengetahui apakah serangan DoS yang diluncurkan berhasil menembus jaringan *Router*. Setelah melakukan pengujian pengecekan awal terhadap lalu-lintas jaringan Router, maka selanjutnya dilakukan pengujian menggunakan aplikasi. Pada proses ini aplikasi *Fastream Web Stress Tester* dijalankan *windows* untuk melancarkan serangan.



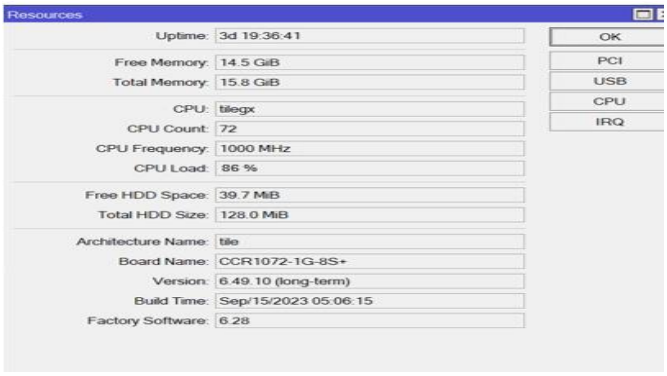
Gambar 3.3 Aplikasi Fastream Web Stress Tester untuk Serangan

DoS Berdasarkan tampilan Gambar di atas, dapat dijelaskan bahwa aplikasi *Fastream Web Stress Tester* berhasil dijalankan dan siap melancarkan serangan ke jaringan *Router* yang menjadi target serangan. Setelah dilakukan serangan, proses selanjutnya melakukan pengecekan serangan yang masuk pada *Router* melalui aplikasi *Winbox* dan analisa serangan menggunakan aplikasi *wireshark*. Setelah dicek percobaan simulasi serangan ini sudah berhasil masuk, sehingga dapat dilakukan *Monitoring Flooding* untuk melakukan serangan pada *Router*. Penyerangan DoS menggunakan *Fastream Web Stress Tester* langsung menuju ke target jaringan *Router* yang diserang, seperti tampilan pada Gambar berikut :



Gambar 3.4 Tampilan Monitoring Saat Serangan DoS Berlangsung

Pada gambar diatas dijelaskan terjadi serangan oleh IP 192.168.217.221 pada Port 8291 dengan *bandwith* yang dikirim terus menerus oleh ke IP 114.5.199.194 sampai *router down*.



Gambar 3.5 Resources Setelah Serangan Dos

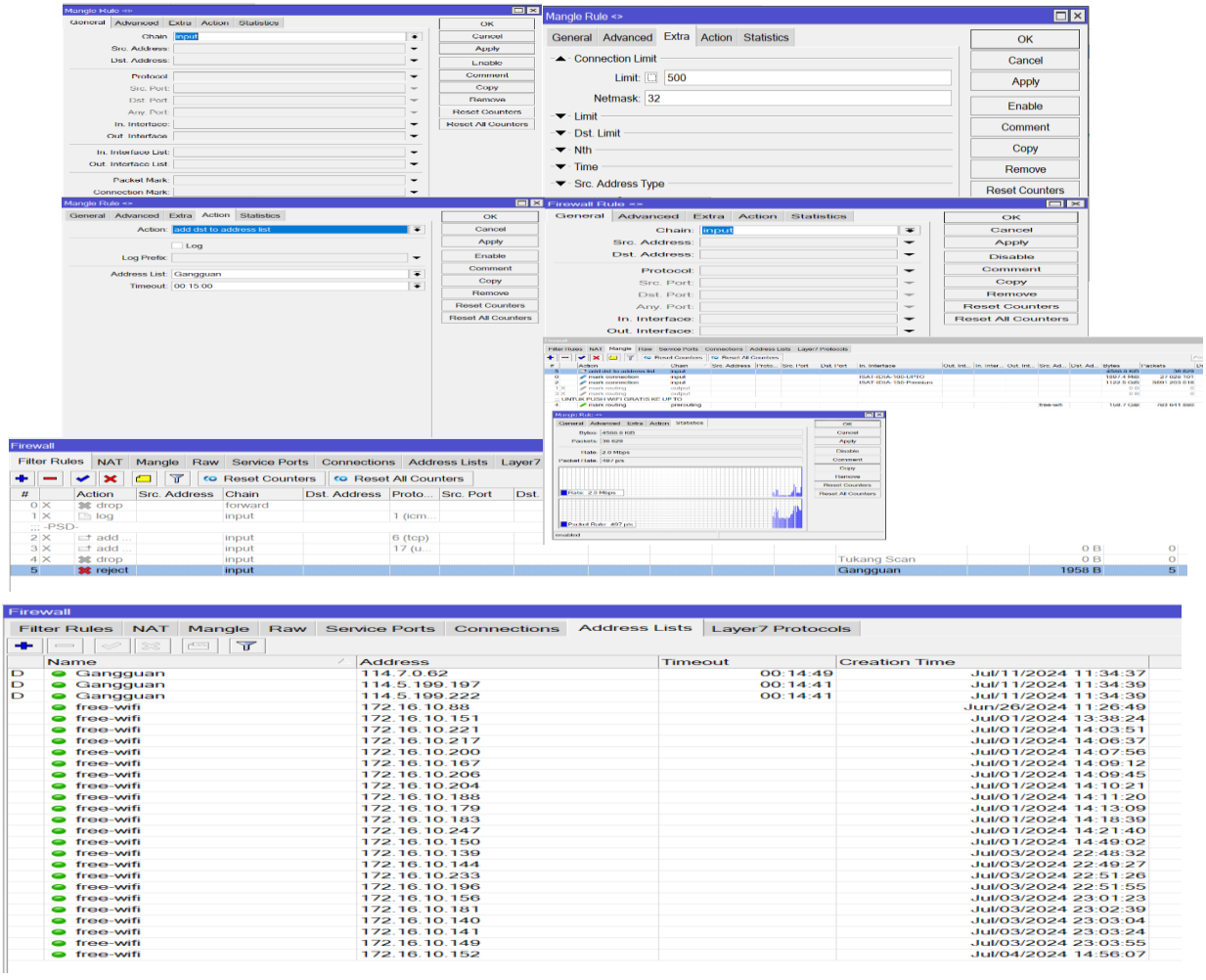
Pada gambar diatas terlihat *resource* dari *router* mikrotik CCR 1072 yang sebelumnya CPU *Load* normal menjadi 86%.

Peningkatan Keamanan Router Mikrotik

Berdasarkan uraian pada penyerangan serta akuisisi data, maka langkah selanjutnya adalah melakukan peningkatan kemanan *Route*r Mikrotik dari *software*.

Untuk pengamanan dari *software* maka digunakan *firewall filter* dari perangkat lunak mikrotik. *Firewall Filter* ini berfungsi menyaring (*filter*) paket data yang masuk dan keluar dari jaringan dalam (*local*) atau dari jaringan luar*)*. Maka *router* akan menyaring data apa saja yang boleh masuk atau keluar.

Adapun tampilan pengaturan pada *firewall* filter seperti yang terlihat pada gambar 3.6 dibawah ini.



Gambar 3.6 *Filter Firewall*

Dari gambar diatas terlihat bahwasanya *filter firewall* difungsikan sebagai bloking serangan DoS dimana bisa setiap paket DoS yang dikirimkan akan langsung diblokir oleh *filter firewall*. Dapat dilihat pada kolom *Bytes* dan *Packets* yang *di filter oleh Firewall* saat penyerang melakukan serangan. Terdapat data yang di-*drop* dan di-*forward* dan dikirimkan ke *adresslist* yang untuk dilakukan pemblokiran sementara sampai waktu yang ditentukan. 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*.

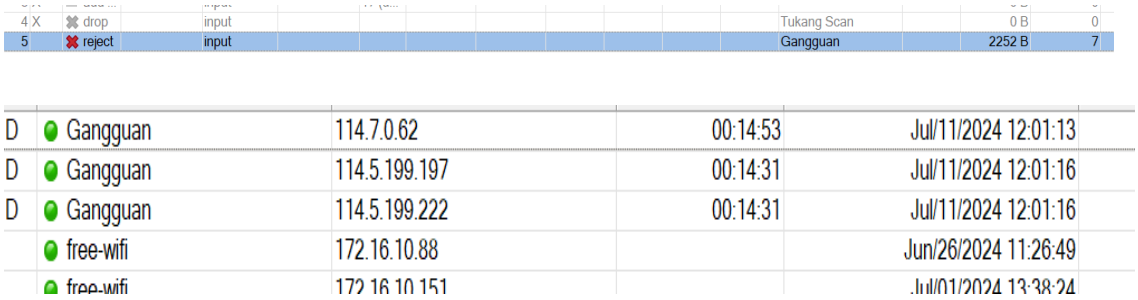
HASIL

Pada hasil pengujuan diperoleh hasil analisa sebelum dan sesudah terjadi serangan DOS dimana Sebelum terjadi serangan Kondisi CPU 6% dan setelah terjadi serangan kondisi CPU menjadi 86% menyebabkan *router* menjadi down atau tidak bisa menjalankan fungsi sebagaimana mestinya seperti yang terlihat pada tabel berikut ini :

Tabel 1 Hasil Analisis Serangan DOS di *Router*

Analisis	Keterangan
IP Addres Penyerang	192.168.217.221
Kondisi CPU perangkatjaringan yang belum diserang	6 %
Kondisi CPU perangkatjaringan yang sudah diserang	86 %
Serangan DoS pada*Router* menggunakan aplikasi Web Stress Tester	Berhasil melakukanserangan

Namun setelah dilakukan filter *firewall* dapat terlihat bahwa serangan DoS yang masuk akan langsung direject oleh *router* dan melakukan pemblokiran ip sehingga ip tersebut tidak bisa lagi melakukan serangan DoS ke *Router* Mikrotik CCR 1072 Dinas Komunikasi dan Informatika Kota Bukittinggi seperti terlihat pada gambar 3.7 dibawah ini.



Gambar 3.7 Reject IP Gangguan

KESIMPULAN

Setelah melakukan simulasi serangan DoS pada *Router*, makadapat ditarik beberapa temuan penelitian sebagai kesimpulan. Berikut kesimpulan penelitian ini :

1. Dari proses penyerangan yang di analisa bahwa serangan DoS menggunakan aplikasi *Fastream Web Stress Tester* dengan cara mengirim pesan secara bertubi-tubi sehingga membuat jaringan *Router* menjadi *Down*.
2. Semua Teknik yang dilakukan berdasarkan metode yang digunakan memiliki keberhasilan 100% untuk mendeteksi serangan DOS di *Router*.
3. Penggunakan *Filter Firewall* sangat ampuh digunakan untuk melakukan pertahanan pada *router* CCR 1072 dimana menggunakan *filter firewall* ini maka *router* mampu melakukan bloking paket-paket data DoS yang dapat mengganggu kinerja dari jaringan *router* mikrotik.

Firewall Filter terbukti efektif dalam mencegah terjadinya serangan DoS pada *router* mikrotik. *Firewall Filter* berfungsi menyaring paket data yang masuk pada jaringan *router*, sedangkan *Firewall Mangle* berfungsi untuk memblokir IP yang dicurigai mengirim paket data tidak wajar pada jaringan router.

DAFTAR PUSTAKA

Aldhyani, T. H. H., & Alkahtani, H. (2023). *Cyber Security for Detecting Distributed Denial of Service Attacks in Agriculture 4.0: Deep Learning Model. Mathematics*, 11(1). https://doi.org/10.3390/math11010233

Arief Indriarto Haris, Budhi Ryanto (2022) Analisis Pengamanan Jaringan Menggunakan Router Mikrotik dari Serangan Dos dan Pengaruhnya terhadap Performansi “Komputika : Jurnal Sistem Komputer Vol 11 No 1 April 2022 Hal 67-76 DOI:10.34010/Komputika v11i1.5227

BSSN (2020) Panduan Menghadapi Serangan Denial of *Service Retrieved from* https://www.bssn.go.id/panduan-menghadapi-serangan-denial-of-service-untuk-badan-usaha-kecil-dan-menengah/

Central Data Teknologi (2022) Serangan Dos Retieved from https://centraldatatech.com/id/blog-news/serangan-denial-of-service-dos-terus-meningkat-ini-solusinya/

Cisco. (2023). *Network forensics* Using Cisco NetShark. https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-netflow/network-forensics.html

Dolan-Gavitt, B., Hulin, M., Srivastava, A., & Giffin, J. (2022). Bridging the Gap Between Memory and Disk Forensics. In The Art of Memory Forensics (pp. 521-546). Wiley.

Koochaki, J., Sani, A. M., Qureshi, H. S., & Sobhi, S. S. (2020). Anomaly detection with meta-heuristic algorithms. IEEE Access, 8, 193344-193359.

Kuzmanovic, A., & Knightly, E. W. (2018). Low-rate TCP-targeted denial of service attacks and counter strategies. IEEE/ACM Transactions on Networking, 16(4), 1203-1216.

Lashkari, A. H., Danesh, A. S., & Samadi, H. (2022). Towards deep packet inspection for *Network forensics* using natural language processing. IEEE Access, 10, 24085-24102.

Louw, T., Wilkins, S., & Cichonski, P. (2023). Memory Forensics with Volatility and WinPmem. In The Official Volatility Commander's Reference (pp. 37-56). Apress, Berkeley, CA.

Mhd. Fakhmi, Lipantri Mashur Gultom (2021) Peningkatan Keamanan Router Mikrotik Terhadap Serangan Syn Flood dengan Menggunakan Firewall *Mangle* “Seminar Nasional Industri dan Teknologi (SNIT) Politeknik Negeri Bengkalis Oktober 2021

MikroTik. (2023). CCR1072-1G-8S+ Cloud Core Router. https://mikrotik.com/product/ccr1072-1g-8s_plus

Mitro, S., & Sukma, D. (n.d.-a). Penerapan Metode Network Forensik Untuk Analisis Serangan DOS Pada Perangkat Router. Jurnal POLEKTRO: Jurnal Power Elektronik, 12(1), 2023.

Mitro, S., & Sukma, D. (n.d.-b). PENERAPAN METODE NIJ UNTUK ANALISIS SERANGAN DOS PADA PERANGKAT IOT. Jurnal POLEKTRO: Jurnal Power Elektronik, 12(2), 2023.

Muhammad Adam, Erick I*Mangle*adi Alwi dan Ihwana As’ad (2022) Analisis Forensik Terhadap Serangan DDoS Ping Of Death Pada Server “Cybersecurity dan forensic digital Vol 5 No 1 Mei 2022 Hlm 23-31 e-ISSN : 2615-8442

Muhammad Alim Zulkifli, Imam Riadi dan Yudi Prayudi (2018) *Live forensics* Method for Analysis Denial of Service (DOS) Attack on Routerboard “International Jurnal of Computer Application (0975-8887) Volume 180 – No 35 April 2018

Munish, A., & Anil, S. (2020). Password Attack: A Theoretical Study. International Journal of Computer Applications, 176(19), 1-4.

Naik, S., Binu, D., & Nagaraju, V. (2023). DoS attack detection in IoT network using an integrated network and live forensics model. IEEE Internet of Things Journal, 10(1), 1-12.
Naik, S., Binu, D., & Nagaraju, V. (2023). DoS attack detection in IoT network using an integrated network and live forensics model. IEEE Internet of Things Journal, 10(1), 1-12.
Rizky Mezi Muria, Arif Muntasa (2023) Studi Literatur : Peningkatan Kinerja Digital Forensik dan Pencegahan Cyber Crime “Jurnal Aplikasi Teknologi Informasi dan Manajemen Vol 3 No 1 April 2023 ISSN : 2722-435X
Shamsolmoali, P., & Wang, J. (2020). Deep argmax network for network traffic data stream processing and abnormal event mining. Future Generation Computer Systems, 107, 1053-1064.
Sitompul Josua. (2012). Cyberspace, Cybercrimes, Cyberlaw Tinjauan Aspek Hukum Pidana. Jakarta:Tatanusa. Retrieved from http://www.tatanusa.co.id/index.php/produk-buku/buku-referensi/160-cyberspace-cybercrimes-cyberlaw.html
Wireshark. (2023). About Wireshark. https://www.wireshark.org/about.html
Zulkifli, M. A., Riadi, I., & Prayudi, Y. (2018). *Live forensics* Method for Analysis Denial of Service (DOS) Attack on Routerboard. In International Journal of Computer Applications (Vol. 180, Issue 35).