Jurnal KomtekInfo

https://jkomtekinfo.org/ojs

2024 Vol. 11 No. 4 Hal: 247-255 e-ISSN: 2502-8758

Penerapan Metode Live Forensik untuk Analisis Serangan DoS pada Router Mikrotik

Afriadi Syahputra✉, Y. Yuhandri, Syafri Arlis

Fakultas Ilmu Komputer, Universitas Putra Indonesia YPTK, Padang, 25221, Indonesia

Afriadi.bkt@gmail.com

Abstract

Denial of Service attacks on router devices can cause damage to the network and hinder connectivity. Denial of Service attacks are one of the attacks on sites, networks, firewall routers, and servers that often occur. The type of attack that is often used by hackers is sending several packets through the internet protocol continuously which can disrupt the organization of the computer network to paralyze the server. The purpose of this study is to provide a solution or alternative to prevent DoS attacks on Mikrotik router devices. The application of the Live Forensic method can be used to analyze DoS attacks on router devices. Live forensics is a state or process of Forensic analysis that is carried out when the computer network system is operating. This is because digital evidence information can only be obtained when the system is running, and the information can be lost if the network system is turned off. This method includes stages such as data analysis, investigation, and presentation of results. From the attack process that was analyzed, the Denial-of-Service attack used the Hping3 application from the Kali Linux Operating System by sending messages repeatedly so that the Router network went Down. The data used is data from network devices and activity logs of the Mikrotik Router of the Communication and Informatics Service of Bukittinggi City. The results of the study obtained evidence of digital Denial of Service attacks in the form of IP Addresses and attacker activity logs. Improving router security in terms of software by using Firewall Filter and Firewall Raw has proven effective in preventing attacks. The application of the Live Forensics method can be used to analyze DoS attacks on router devices and assist in taking action to prevent further attacks.

Keywords: DoS (Denial of Service) Attack, Live Forensics, Router, Hping3, firewall

Abstrak

Serangan *Denial of Service* pada perangkat router dapat menyebabkan kerusakan pada jaringan dan menghambat konektivitas. Serangan *Denial of Service* merupakan salah satu serangan terhadap situs, jaringan, router firewall dan server yang sering terjadi. Jenis serangan yang sering digunakan oleh hacker adalah yang bersifat mengirimkan sejumlah paket melalui *internet protocol* secara terus menerus yang dapat mengganggu organisasi dari jaringan komputer dengan tujuan melumpuhkan server. Tujuan dari penelitian ini adalah untuk memberikan solusi atau alternatif pencegahan terjadinya serangan DoS terhadap perangkat router mikrotik. Penerapan metode *Live Forensik* dapat digunakan untuk menganalisis serangan DoS pada perangkat router. *Live forensics* merupakan keadaan atau proses analisis Forensik yang dilakukan ketika sistem jaringan Komputer sedang beroperasi. Hal ini dikarenakan informasi bukti digital hanya bisa didapatkan pada saat sistem berjalan dan informasi tersebut bisa hilang jika sistem jaringan dalam keadaan mati. Metode ini meliputi tahap-tahap seperti analisis data, investigasi dan presentasi hasil. Dari proses penyerangan yang di analisa bahwa serangan *Denial of Service* menggunakan aplikasi Hping3 dari Sistem Operasi Kali Linux dengan cara mengirim pesan secara bertubi-tubi sehingga membuat jaringan Router menjadi Down. Data yang digunakan adalah data dari perangkat jaringan dan log aktivitas Router Mikrotik Dinas Komunikasi dan Informatika Kota Bukittinggi. Hasil penelitian diperoleh bukti digital serangan *Denial of Servic* berupa *IP Address* dan *log activity* penyerang. Peningkatan keamanan *router* dari segi *software* dengan menggunakan *Firewall Filter* dan *Firewall Raw* terbukti efektif dalam mencegah terjadinya serangan. Penerapan metode *Live Forensik* digunakan untuk menganalisis serangan DoS pada perangkat router dan membantu dalam mengambil tindakan mencegah serangan selanjutnya.

Kata Kunci: Serangan *DoS (Denial of Service), Live Forensik ,Router, Hping3, Firewall*

1. Pendahuluan

Perkembangan teknologi informasi telah mengubah cara manusia berinteraksi, berkomunikasi, dan bekerja. Teknologi informasi telah menjadi tulang punggung dari hampir semua aspek kehidupan kita, termasuk komunikasi, bisnis, pendidikan, dan administrasi pemerintahan. Namun, seiring dengan manfaat besar yang ditawarkan oleh teknologi ini, muncul pula ancaman keamanan pada teknologi informasi seperti

Diterima: 25-08-2024 | Revisi: 27-09-2024 | Diterbitkan: 31-12-2024 | doi: 10.35134/komtekinfo.v11i4.555

Serangan malware, worm, DoS, ransomware, dan trojan horse yang dapat menginfeksi sistem dan merusak data atau mencuri informasi penting.

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 [1].

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 [2]. 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 [3].

Tujuan dari penelitian ini adalah untuk mengetahui dan menganalisis serangan *Denial of Service* secara teknis dapat mengganggu operasional jaringan dan sistem informasi dan untuk memberikan solusi atau alternatif pencegahan terjadinya serangan terhadap perangkat router mikrotik. 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 bertanggung jawab.

Banyaknya terjadi serangan DoS maka banyak peneliti melakukan penelitian terhadap serangan DoS oleh Naik S mengusulkan sebuah model forensik jaringan yang mengintegrasikan network forensics dan live forensics untuk mendeteksi serangan DoS pada perangkat Internet of Things (IoT). Model ini mampu mengumpulkan dan menganalisis data jaringan serta data dari memori dan proses sistem secara real-time untuk mengidentifikasi pola serangan DoS secara efektif [4]. Sementara itu, Olusula menekankan pentingnya melakukan investigasi forensik pada perangkat jaringan seperti router untuk mencegah dan merespons serangan DoS. Penelitian ini menyajikan sebuah kerangka kerja forensik router dengan menggunakan teknik *memory forensics* dan *network forensics*. Kerangka kerja ini divalidasi pada router Mikrotik dan terbukti efektif dalam mengumpulkan bukti digital dari aktivitas jaringan dan sistem router [5]. Budi J menyimpulkan bahwa *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 packet data tidak wajar pada jaringan router [6].

Pham et al. Mengusulkan kerangka kerja baru yang disebut DDOS-TL untuk deteksi serangan DDoS dan investigasi forensik langsung (*live forensic*) .Kerangka kerja ini dapat digunakan untuk mendeteksi serangan DDoS pada router dan melakukan investigasi forensik secara real-time. Hasil evaluasi menunjukkan bahwa DDOS-TL memiliki tingkat deteksi yang tinggi dan mampu mengumpulkan bukti forensik yang berguna terkait serangan DDoS pada router [7]. Mabanza dan Hamid Melakukan survei komprehensif terhadap berbagai teknik dan alat forensik jaringan untuk pengumpulan dan analisis bukti digital. Membahas teknik yang relevan untuk investigasi serangan DoS pada router, seperti packet capture, flow analysis, dan analisis log. Mengidentifikasi tantangan dan peluang dalam forensik jaringan, termasuk investigasi serangan DoS pada router [8].

Analisis forensik adalah proses mengumpulkan, menganalisis, dan melestarikan bukti-bukti digital terkait insiden keamanan siber. Proses ini membantu mengidentifikasi asal serangan, memahami motifnya, dan mengevaluasi dampak yang ditimbulkan. Dengan analisis yang komprehensif, penyelidikan terhadap insiden dapat dilakukan secara efektif [9].

Network forensic merupakan cabang ilmu forensik digital yang berfokus pada pengumpulan, analisis, dan investigasi trafik jaringan untuk mendeteksi aktivitas ilegal atau penyalahgunaan jaringan[10]. Live forensic adalah proses analisis sistem atau perangkat saat masih dalam kondisi aktif (*live*). Tujuannya adalah untuk mengumpulkan bukti digital tanpa mengganggu integritas data yang ada. Dengan metode ini, data dapat diperoleh secara *real-time* sebelum sistem dimatikan atau diubah. [11]. Pada penelitian ini penulis akan menggabungkan metode network forensik dan live forensik dibagian analisa sistemnya agar hasil yang didapatkan lebih maksimal dan dapat dipertanggung jawabkan, inilah yang menjadi keterbaruan dari penelian ini dari penelitian sebelumnya.

2. Metodologi Penelitian

Penelitian ini menggunakan metode *live forensic* untuk menganalisis serangan Denial of Service (DoS) pada router MikroTik. Live forensic adalah pendekatan yang melibatkan analisis langsung pada sistem yang masih aktif, yang memungkinkan pengumpulan bukti digital secara real-time tanpa mengganggu operasional sistem. Dalam konteks ini, penerapan live forensic pada router MikroTik bertujuan untuk mendeteksi, mengidentifikasi, dan menganalisis pola serangan DoS dengan tepat.

Tahap pertama dalam metodologi ini adalah persiapan lingkungan forensik. Router MikroTik yang menjadi target serangan akan dipersiapkan dengan pengaturan khusus untuk memfasilitasi monitoring trafik jaringan secara real-time. Tools yang digunakan dalam proses ini mencakup software monitoring jaringan yang kompatibel dengan MikroTik serta tools forensik untuk menangkap dan menganalisis log jaringan. Langkah ini penting untuk memastikan bahwa setiap aktivitas yang mencurigakan dapat dideteksi dan dicatat secara akurat.

Selanjutnya, selama serangan DoS berlangsung, data yang diperoleh melalui tools monitoring akan dianalisis menggunakan teknik live forensic. Proses ini melibatkan pengumpulan data langsung dari memori sistem, log jaringan, dan informasi konfigurasi router tanpa mematikan perangkat. Analisis ini bertujuan untuk mengidentifikasi sumber serangan, memahami metode yang digunakan oleh penyerang, dan mengevaluasi dampak yang ditimbulkan pada router MikroTik. Hasil dari analisis ini akan memberikan wawasan mendalam tentang bagaimana serangan DoS mempengaruhi jaringan dan bagaimana langkah mitigasi dapat diterapkan secara efektif.

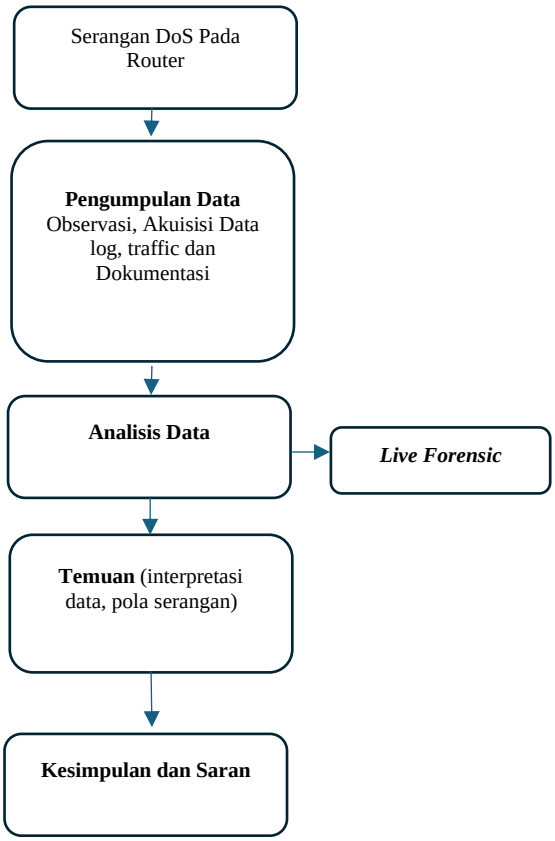
2.1 *Live Forensik*

Live forensic adalah proses analisis sistem atau perangkat saat masih dalam kondisi aktif (live). Tujuannya adalah untuk mengumpulkan bukti digital tanpa mengganggu integritas data yang ada. Dengan metode ini, data dapat diperoleh secara real-time sebelum sistem dimatikan atau diubah [12].

alur proses penerapan metode live forensic dalam menganalisis serangan Denial of Service (DoS) pada router, khususnya router MikroTik. Tahapan ini dimulai dengan identifikasi serangan DoS yang ditujukan pada router, di mana serangan tersebut bertujuan untuk membanjiri jaringan dengan trafik yang sangat tinggi, menyebabkan gangguan atau bahkan penghentian layanan. Serangan ini menjadi titik awal analisis forensik untuk mengidentifikasi sumber, motif, dan dampaknya terhadap infrastruktur jaringan.

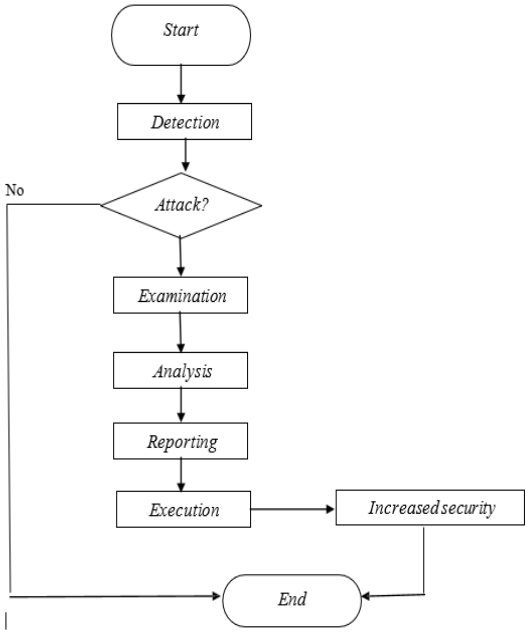
Setelah serangan teridentifikasi, tahap berikutnya adalah pengumpulan data yang relevan. Data ini diperoleh melalui berbagai metode, termasuk observasi langsung, akuisisi log jaringan, pemantauan trafik, dan dokumentasi sistematis dari aktivitas yang mencurigakan. Pengumpulan data dilakukan dengan cermat untuk memastikan bahwa semua bukti terkait serangan dapat direkam dan disimpan tanpa mempengaruhi integritas sistem. Pengumpulan data ini menjadi landasan penting untuk analisis lebih lanjut, memastikan bahwa setiap aspek serangan dapat ditelusuri dan dianalisis secara mendalam.

Tahap analisis data merupakan inti dari metode live forensic, di mana data yang telah dikumpulkan dianalisis secara real-time saat sistem masih aktif. Analisis ini bertujuan untuk mengidentifikasi pola serangan, teknik yang digunakan oleh penyerang, dan dampaknya terhadap router MikroTik. Dari hasil analisis ini, akan dihasilkan temuan yang memberikan wawasan mendalam tentang karakteristik serangan dan metode mitigasi yang efektif. Temuan tersebut kemudian dirangkum dalam kesimpulan dan saran yang mencakup rekomendasi teknis dan strategis untuk mencegah terjadinya serangan serupa di masa depan, serta meningkatkan ketahanan jaringan terhadap ancaman serupa seperti terlihat pada Gambar 1 [13].



Gambar 1. Flowchart Alur Proses Penelitian

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.



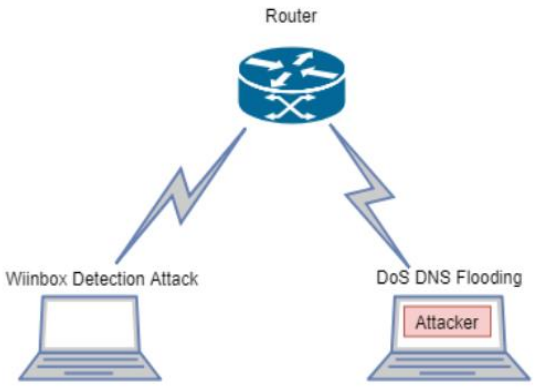
Gambar 2. Flowchart *Live Forensics*

Flowchart *live forensics* dimulai dari tahapan deteksi, pencarian informasi, analisa, laporan hasil temuan, eksekusi dan peningkatan keamanan router 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.
6. 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 [12].

2.2 Skema Serangan DoS Pada Router

Serangan terhadap router yang dilakukan melalui dua metode: *Winbox Detection Attack* dan *DoS DNS Flooding*. *Winbox Detection Attack* melibatkan deteksi dan eksploitasi kerentanan pada Winbox, yang merupakan antarmuka manajemen untuk router MikroTik. Sementara itu, *DoS DNS Flooding* adalah serangan yang berfokus pada membanjiri DNS server dengan *trafik* berlebihan untuk mengganggu layanan jaringan, dimana pelaku serangan menggunakan metode ini untuk menyebabkan gangguan atau penghentian layanan pada router seperti pada Gambar 3.

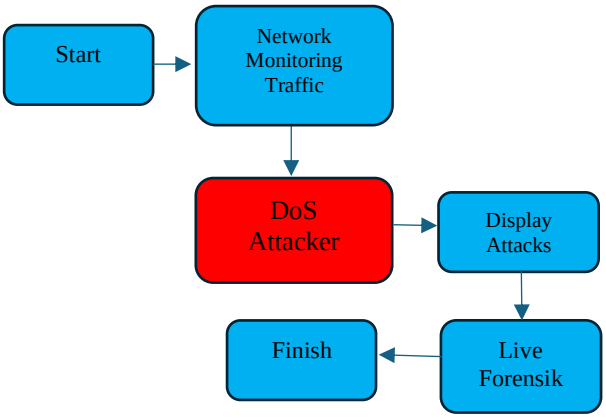


Gambar 3. Skema Serangan DoS Pada *Router*

Skema serangan DoS Pada Router seperti gambar 3 marupakan tahapan simulasi serngan DoS dengan tujuan untuk menguji apakah aplikasi wireshark mampu mendeteksi aktivitas serangan DoS pada router.[13]

2.3 Analisis Serangan DoS Pada Router

Gambaran alur proses penanganan serangan DoS menggunakan pendekatan *live forensic*. Proses dimulai dengan monitoring *trafik* jaringan untuk mendeteksi adanya aktivitas mencurigakan atau anomali, yang mengarah pada identifikasi serangan DoS. Setelah serangan terdeteksi, informasi terkait serangan tersebut ditampilkan untuk dilakukan analisis lebih lanjut melalui metode live forensic, yang bertujuan untuk mengumpulkan dan menganalisis bukti digital tanpa mengganggu integritas data. Tahap akhir adalah penyelesaian proses setelah serangan berhasil dianalisis dan langkah-langkah mitigasi diambil. Analisis serangan DoS pada router terlihat pada alur analisis serangan seperti pada Gambar 4 dimana saat *network administrator* melakukan Analisa dengan melihat traffic monitoring network, jika ada serangan DoS maka akan dianalisa pelaku serangan menggunakan metode *live forensic* dapat dilihat pada Gambar 4.



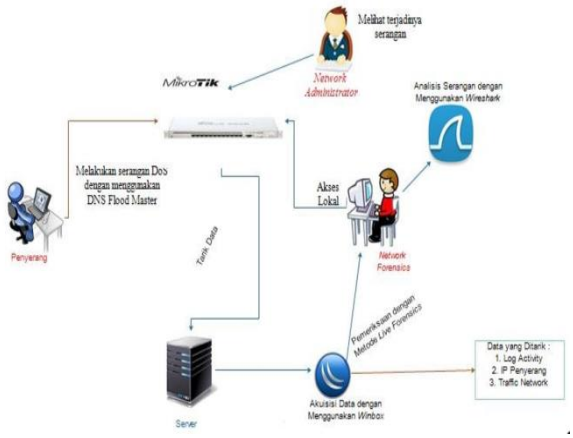
Gambar 4 Analisa *Live Forensik*

Analisis serangan DoS pada router terlihat pada alur analisis serangan seperti pada Gambar 4 dimana saat network administrator melakukan Analisa dengan melihat traffic monitoring network, jika ada serangan DoS maka akan dianalisa pelaku serangan menggunakan metode live forensic.

2.4 Skema Akuisisi Data Forensik

Saat melakukan simulasi DNS Flooding terdiri dari 3 bagian yaitu penyerang yang mengirim serangan pada jaringan *router*, administrasi jaringan sebagai user dari jaringan *router*, serta *network forensics* yang menganalisis serangan, melakukan akuisisi data, dan peningkatan keamanan pada perangkat router. [14] Peran dari masing-masing bagian serta fungsi perangkat dalam penelitian ini yaitu:

1. 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.
2. Administrasi Jaringan 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.
3. 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 [15] seperti terlihat pada Gambar 5.

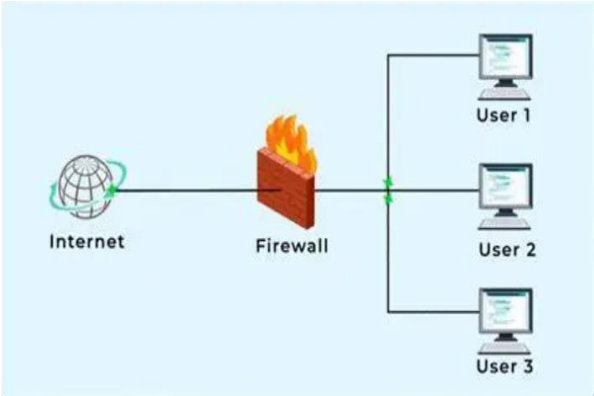


Gambar 5. Skema Akuisisi Data Forensik

Diagram tersebut menggambarkan interaksi antara berbagai komponen dan pengguna dalam sistem.
Di bagian kiri atas, terdapat seorang pengguna yang digambarkan sedang menggunakan komputer, kemungkinan untuk memasukkan atau mengakses data. Data ini kemudian disimpan dalam server yang digambarkan di bagian bawah. Server ini terhubung ke berbagai komponen lain dalam sistem.
Di bagian kanan atas, terdapat representasi manajer yang memiliki akses ke laporan dan informasi penting. Hal ini menunjukkan bahwa sistem memungkinkan manajemen tingkat atas untuk melihat dan menganalisis data.

2.5 Firewall

Firewall merupakan mekanisme yang melakukan filtering terhadap paket yang masuk maupun keluar dari jaringan. 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. Umumnya, sebuah Firewall diimplementasikan dalam sebuah mesin terdedikasi, yang berjalan pada pintu gerbang (gateway) antara jaringan lokal dan jaringan lainnya [16]. Firewall umumnya juga digunakan untuk mengontrol akses terhadap siapa saja yang memiliki akses terhadap jaringan pribadi dari pihak luar. Saat ini, istilah Firewall menjadi istilah generik yang merujuk pada sistem yang mengatur komunikasi antar dua jaringan yang berbeda, dapat dilihat pada Gambar 6.



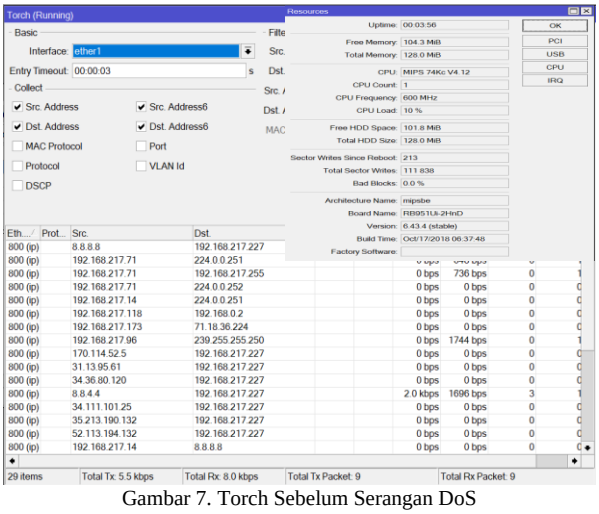
Gambar 6. Skema Firewall

Untuk memblokir IP address yang dicurigai melakukan serangan DoS, kita dapat menggunakan fitur Firewall RAW. Firewall RAW memungkinkan kita untuk memproses atau memblokir paket data sebelum mereka mencapai tahap koneksi. Dengan cara ini, serangan dapat dicegah secara lebih efektif, karena paket data berbahaya dihentikan pada tahap awal.

3. Hasil dan Pembahasan

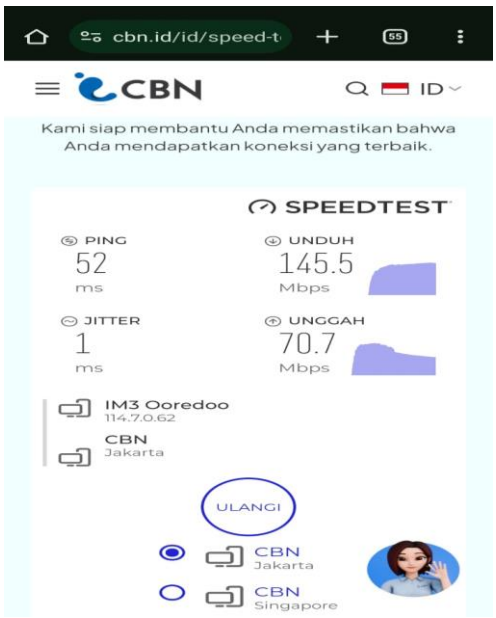
3.1 Serangan DoS Pada Router

Langkah pertama yang dilakukan dalam proses Analisa serangan DoS adalah dengan melakukan pengecekan kondisi jaringan pada Winbox Router Mikrotik melalui menu Torch Running. Jika ada serangan maka penyerang berusaha melumpuhkan router agar tidak bisa diakses oleh user lain. Pada Gambar 8 terlihat kondisi router mikrotik dalam normal hal dan mampu malayani koneksi intranet dan internet. Terlihat Load CPU masih kondisi 10%, Memory yang digunakan adalah 104MiB dari 128MiB dan koneksi yang ada dalam keadaan normal dengan IP Address Router 192.168.217.227 tersaji pada Gambar 7.



Gambar 7. Torch Sebelum Serangan DoS

Sebelum terjadinya serangan DoS, kecepatan internet diukur menggunakan situs cbn.id menunjukkan hasil yang cukup tinggi. Kecepatan unduhan (download) mencapai 145 Mbps, sementara kecepatan unggahan (upload) berada di angka 70 Mbps. Angka ini mencerminkan kinerja jaringan yang optimal dan stabil. Namun, kinerja ini bisa terganggu jika terjadi serangan DoS yang dapat menyebabkan penurunan kecepatan secara signifikan.

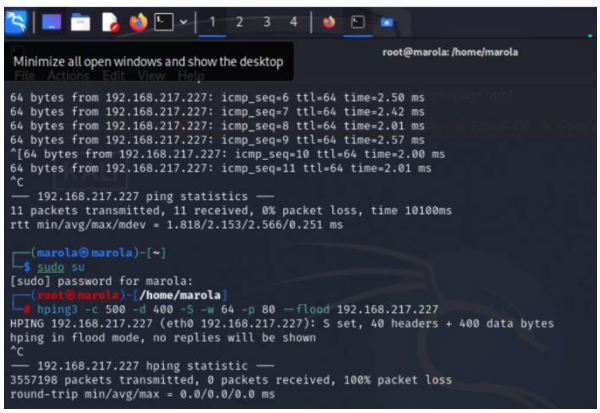


Gambar 8. Tampilan Speed Test Sebelum Terjadi Serangan Dos

Gambar 8 menunjukkan hasil tes kecepatan internet dari layanan CBN. Hasil tes menampilkan ping 52 ms, kecepatan unduh 145.5 Mbps, jitter 1 ms, dan kecepatan unggah 70.7 Mbps. Terdapat juga informasi bahwa koneksi menggunakan IM3 Ooredoo dan CBN Jakarta.

3.2 Serangan DoS Menggunakan *Kali Linux*

Serangan dilakukan menggunakan DNS Flooding Hping3 dari Kali Linux seperti terlihat pada gambar 8 dimana pengiriman paket data secara terus-menerus berhasil dilakukan kejaringan router IP 192.168.217.227 pada port 80, dapat dilihat pada Gambar 9.



Gambar 9. Tampilan Serangan DoS

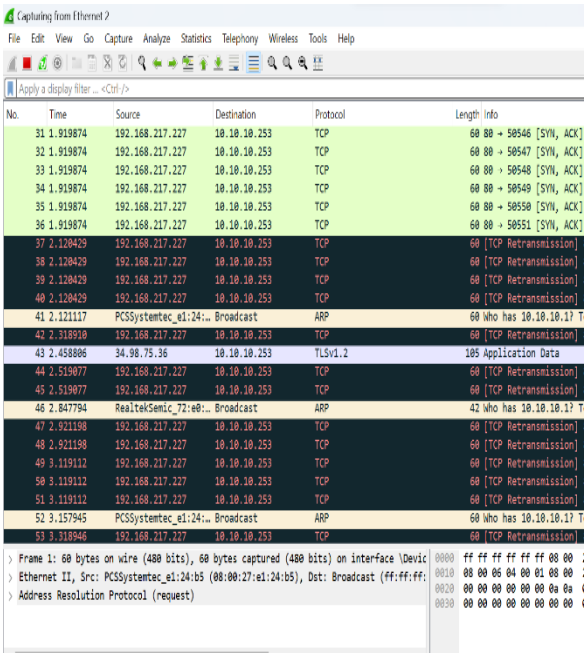
Gambar diatas menampilkan sebuah terminal atau command line interface pada sistem operasi berbasis

Linux. Terlihat beberapa perintah yang dijalankan, terutama terkait dengan aktivitas jaringan dan pengujian koneksi.

Yang paling menonjol adalah penggunaan perintah "ping" untuk menguji konektivitas ke alamat IP 192.168.217.227. Hasilnya menunjukkan bahwa ping berhasil dengan waktu respons sekitar 2-3 milidetik. Selain itu, ada juga penggunaan perintah "hping3" yang merupakan alat pengujian jaringan yang lebih canggih. Perintah ini digunakan untuk melakukan flood ping ke alamat IP yang sama, mengirimkan sejumlah besar paket dalam mode flood.

3.3 Akuisisi Data Forensik

Menggunakan aplikasi wireshark terlihat pada gambar 9 traffic aktivitas pada jaringan router dimana terjadi pengiriman data secara tidak wajar terus-menerus yang dilakukan IP 10.10.10.253 kepada IP router 192.168.217.227 pada Port 80 dapat dilihat pada Gambar 10.

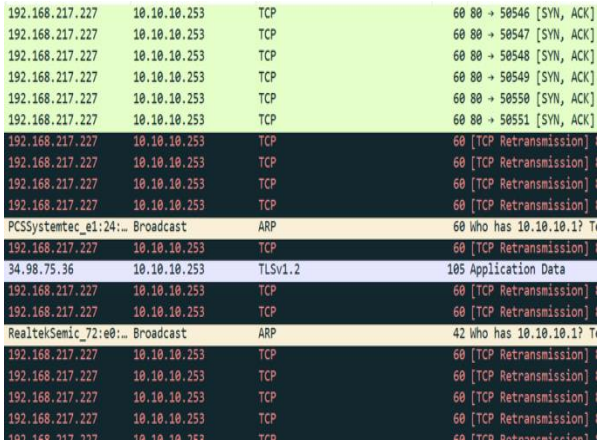


Gambar 10. *Wireshark* Deteksi Serangan DoS

Pada gambar 10 terlihat ada IP 10.10.10.253 melakukan serangan secara bertubi-tubi menyerang Protocol Port router yaitu 192.168.217.227. Aktivitas ini dicurigai sebagai aktivitas yang tidak wajar dalam komunikasi data.

3.4 *Log Aktivity*

Pada gambar 10 terlihat ada IP 10.10.10.253 melakukan serangan secara bertubi-tubi menyerang Protocol Port router yaitu 192.168.217.227. aktivitas ini dicurigai sebagai aktivitas yang tidak wajar dalam komunikasi data, dilihat pada Gambar 11.

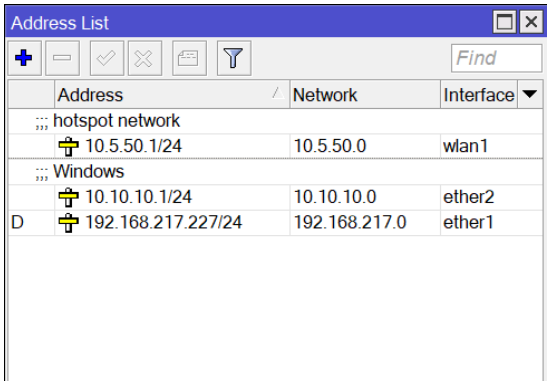


Gambar 11. Data Log Serangan DoS

Gambar 11 menampilkan output dari alat analisis jaringan, kemungkinan besar Wireshark, yang menunjukkan lalu lintas paket antara dua alamat IP: 192.168.217.227 dan 10.10.10.253. Sebagian besar lalu lintas menggunakan protokol TCP dengan beberapa paket ARP dan ICMP juga terlihat. Warna-warna berbeda pada baris menunjukkan jenis paket yang berbeda, dengan warna hijau menandakan paket TCP normal dan warna merah mungkin mengindikasikan paket yang bermasalah atau ditandai untuk perhatian khusus.

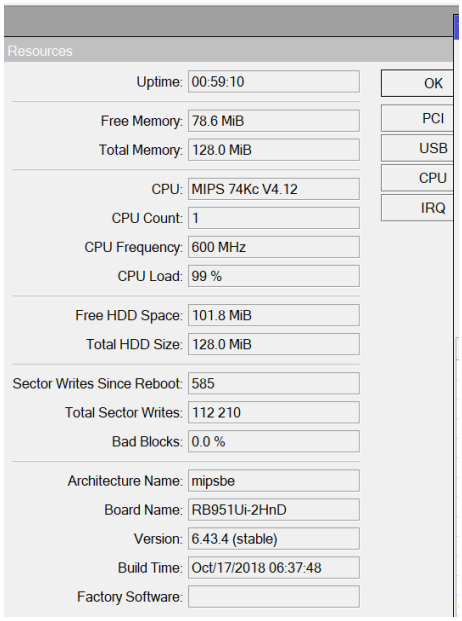
3.5 *IP Address List*

Pada Gambar 12 terlihat konfigurasi address list dari router mikrotik. IP Address pada suatu port router bisa juga berarti gateway pada network segment. IP gateway biasa digunakan sebagai target dari suatu aktivitas serangan pada jaringan.



Gambar 12. IP Address Penyerang

Saat serangan DoS terjadi maka bisa dilihat tambilan *resource* mikrotik dari sebelumnya adalah 10% menjadi 99% artinya kalua tidak cepat ditindak lanjuti maka mikrotik akan segera down karena tidak sanggup menahan serangan secara terus-menerus. Kemudian *speed test* internet mengalami penurunan dari sebelumnya 145 Mbps menjadi 0.1 Mbps.



Gambar 13. Kondisi *Resource Mikrotik* Saat Serangan DoS Berlangsung

Gambar 13 ini menampilkan informasi sistem dari sebuah perangkat, menunjukkan uptime, penggunaan memori, dan spesifikasi CPU. Perangkat ini memiliki total memori 128.0 MB dengan 78.6 MB memori bebas, CPU MIPS 74Kc V4.12 dengan frekuensi 600 MHz, dan beban CPU 99%. Informasi tambahan mencakup ukuran HDD, jumlah penulisan sektor, dan detail arsitektur perangkat.

3.6 *Peningkatan* Keamanan *Router*

Langkah awal yang dilakukan penulis adalah membuat rule pada *firewall filter* dengan menggunakan action "drop". Rule ini bertujuan untuk memblokir alamat IP asal yang disebut "doser". Alamat IP tersebut diarahkan ke tujuan tertentu, yaitu alamat IP "dosed". Proses ini dilakukan melalui Command Line Interface (CLI) menggunakan script yang telah ditentukan.

/ip firewall filter

add chain=forward connection-state=new src-address-list=ddoser dst-address-list=ddosed

action=drop

Langkah berikutnya, maka kita akan menangkap semua koneksi "*new*" dan membuat *chain* baru yaitu "*detect-dos*".

/ip firewall filter

add chain=forward connection-state=new action=jump jump-target=detect-ddos

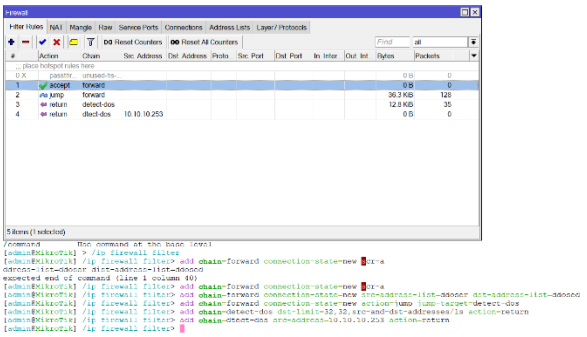
Kemudian kita akan membuat rule firewall sebagai berikut :

/ip firewall filter

add chain=detect-ddos dst-limit=32,32,src-and-dst-addresses/1s action=return

add chain=detect-ddos src-address=10.10.10.253 action=return

Dengan *rule firewall* diatas, maka ketika terdapat paket *new* yang tidak wajar, misalnya diatas 32 paket selama satu detik, maka *firewall* akan melakukan penandaan terhadap alamat asal dan alamat tujuan menggunakan *address list*. Sebagai contoh untuk alamat IP penyerang maka akan dilakukan grouping dengan nama "*doser*", kemudian untuk alamat IP target maka akan dilakukan grouping dengan nama "*dosed*" seperti terilaht pada Gambar 14.



Gambar 14. *Firewall Filter*

Setelah dilakukan peningkatan keamanan maka kondisi router mikrotik dan akses internet dan intranet menjadi normal seperti terlihat pada gambar

3.7 Analisa Hasil

Berdasarkan pengujian terhadap serangan DoS yang penulis lakukan pada perangkat *router mikrotik*, maka diperoleh hasil penelitian menggunakan metode *Live Forensic*. Hasil analisis ini penulis rangkum dalam Tabel 2.

Tabel 2. Hasil Analisis Serangan DoS pada router mikrotik

No	Analisa	Keterangan
1	Serangan pada router menggunakan Hping3 Kali Linux	Serngan berhasil dilakukan secara terus-menerus sehingga membuat router down dan tidak bisa bekerja secara maksimal lagi
2	Protokol	Protokol yang diserang adalah Port 80
3	Kondisi CPU sebelum serangan	CPU Load 10%
4	Kondisi CPU setelah Serangan	CPU Load 99%
5	Kondisi Memory sebelum serangan	104MiB/128MiB
6	Kondisi Memory setelah terjadi serangan	78MiB/128MiB
7	IP Addres: IP Mikrotik IP Penyerang	 192.168.217.227 10.10.10.253
8	Peningkatan Keamanan	Menggunakan *Firewall Filter* dan *Firewall RAW*
9	Kondisi Router Setelah menggunakan filter firewall	CPU Load 12% 101/128MiB

Load CPU	98Mbps
Memory	
Akses Internet	
Kondisi IP Penyerang setelah menggunakan *Firewall Raw*	IP Penyerang Langsung Diblok

Tabel 2 menampilkan hasil analisis serangan DoS (*Denial of Service*) yang dilakukan pada router Mikrotik menggunakan alat "*Hping3*" pada sistem operasi Kali Linux. Serangan ini berhasil dilakukan secara terus-menerus, menyebabkan router mengalami *downtime* dan tidak dapat berfungsi secara optimal. Protokol yang diserang adalah Port 80.

Sebelum serangan, beban CPU (CPU Load) router adalah 10%, sementara setelah serangan, beban CPU meningkat tajam menjadi 99%. Pada sisi penggunaan memori, sebelum serangan, router menggunakan memori sebesar 104MiB dari total kapasitas 128MiB. Namun, setelah serangan terjadi, penggunaan memori menurun menjadi 78MiB dari total 128MiB.

Router Mikrotik yang diserang memiliki IP Address 192.168.217.227, sedangkan IP Address penyerang adalah 10.10.10.253. Untuk meningkatkan keamanan router, digunakan fitur "Firewall Filter" dan "Firewall RAW". Setelah fitur keamanan ini diterapkan, kondisi router menunjukkan peningkatan dengan CPU Load menurun menjadi 12%, penggunaan memori mencapai 101MiB dari total 128MiB, dan kecepatan akses internet mencapai 98Mbps. Selain itu, fitur "Firewall RAW" juga berhasil memblokir IP penyerang secara langsung.

4. Kesimpulan

Berdasarkan hasil analisis serangan DoS (Denial of Service) terhadap router Mikrotik, dapat disimpulkan bahwa serangan DoS secara signifikan membebani performa router, yang terlihat dari peningkatan beban CPU hingga 99% dan perubahan dalam penggunaan memori. Namun setelah dilakukan peningkatan keamanan dengan menerapkan fitur "*Firewall Filter*" dan "*Firewall RAW*", performa router menunjukkan pemulihan yang signifikan. CPU load turun menjadi 12%, dan memori yang digunakan menjadi lebih stabil, sementara IP penyerang berhasil diblokir secara langsung. Ini menunjukkan bahwa penggunaan fitur keamanan firewall sangat efektif dalam menangkal serangan DoS dan menjaga kestabilan serta keamanan jaringan router. Oleh karena itu, untuk melindungi jaringan dari ancaman serangan DoS, penting bagi administrator jaringan untuk menerapkan langkah-langkah keamanan yang memadai, termasuk penggunaan fitur firewall yang tersedia pada perangkat router.

Daftar Rujukan

[1] Haris, A. I., & Ryanto, B. (2022). Analisis Pengamanan Jaringan Menggunakan Router Mikrotik dari Serangan DoS dan Pengaruhnya terhadap Performansi. Komputika: Jurnal Sistem Komputer, 11(1), 67-76. https://doi.org/10.34010/Komputika.v11i1.5227

[2] Mitro, S., & Sukma, D. (2023). Penerapan Metode Network Forensik Untuk Analisis Serangan DoS Pada Perangkat Router. POLEKTRO: Jurnal Power Elektronik, 12(1).

[3] 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

[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.

[5] Olusola, A. A., Akinyemi, B. A., & Taofeek, A. A. (2022). Router forensics framework for mitigating DoS/DDoS attacks. International Journal of Computing and Digital Systems, 11(2), 179-189.

[6] Pham, T. V., Nguyen, D. N., & Lee, Y. K. (2023). DDOS-TL: A Novel Framework for Distributed Denial of Service Attack Detection and Live Forensic Investigation. IEEE Access, 11, 45567-45583.

[7] Mabanza, N., & Hamid, K. A. (2022). Network Forensics Techniques and Tools for Evidence Collection and Analysis: A Survey. IEEE Access, 10, 28907-28928.

[8] Muria, R. M., & Muntasa, A. (2023). Studi Literatur: Peningkatan Kinerja Digital Forensik dan Pencegahan Cyber Crime. Jurnal Aplikasi Teknologi Informasi dan Manajemen, 3(1).

[9] Budi, J. (2020). Peningkatan Keamanan Router Mikrotik Terhadap Serangan Denial of Service (DoS). e-ISSN: 2686-3154.

[10] Wireshark. (2023). About Wireshark. https://www.wireshark.org/about.html

[11] Wu, Z., Qu, P., & Zhang, H. (2022). Network forensics Visualization and Analysis System Based on Packet Capture and Log Analysis. In 2022 IEEE 4th International Conference on Data Science and Machine Learning Applications (DSMA) (pp. 222-226).

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

[13] Endace. (2023). Network forensics with Endace. Retrieved from https://www.endace.com/solutions/network-forensics.pdf

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

[15] Central Data Teknologi. (2022). Serangan DoS. Retrieved from https://centraldatatech.com/id/blog-news/serangan-denial-of-service-dos-terus-meningkat-ini-solusinya/

[16] Casey, E. (2011). Digital Evidence and Computer Crime (3rd ed.). Elsevier. Montasari, R. (2016). Review and Assessment of the Existing Digital Forensic Investigation Process Models. International Journal of Computer Applications, 147(7), 41–49. https://doi.org/10.5120/ijca2016911194