Panthera : Jurnal Ilmiah Pendidikan Sains dan Terapan
E-ISSN 2808-246X; P-ISSN 2808-3636
Volume 5, Issue 3, July 2025; Page, 570-592
Email: pantherajurnal@gmail.com

ANALISA PENERAPAN FITUR *FIREWALL* PADA MIKROTIK UNTUK MENGAMANKAN DARI SERANGAN *DENIAL OF SERVICE* (DoS)

Frederico Indra Wijaya[1]*, Muhammad Innuddin[2], & Kurniadin Abd. Latif[3]
[1,2,&3]Program Studi Ilmu Komputer, Fakultas Teknik, Universitas Bumigora, Jalan Ismail Marzuki Nomor 22, Mataram, Nusa Tenggara Barat 83127, Indonesia
**Email: 2001010044@universitasbumigora.ac.id*
Submit: 23-06-2025; Revised: 30-06-2025; Accepted: 03-07-2025; Published: 21-07-2025

ABSTRAK: Kejahatan siber seperti serangan *Denial of Service* (DoS) merupakan ancaman serius bagi stabilitas jaringan komputer, khususnya pada jaringan yang tidak memiliki perlindungan memadai. Penelitian ini bertujuan untuk menganalisis implementasi fitur *firewall* pada *router* Mikrotik sebagai upaya meningkatkan keamanan jaringan terhadap serangan DoS. Metode yang digunakan mengacu pada pendekatan *Network Development Life Cycle* (NDLC), yang meliputi tahapan analisis, perancangan, simulasi, implementasi, dan pengujian. Hasil penelitian menunjukkan bahwa konfigurasi *firewall* berhasil menutup sejumlah *port* yang rentan (FTP, SSH, Telnet, dan HTTP), serta mempertahankan *port* operasional yang penting (DNS dan *Winbox*). Selain itu, beban CPU pada *router* menurun drastis dari 100% menjadi 3-4% setelah implementasi yang mengindikasikan keberhasilan dalam memitigasi lalu lintas berbahaya. Temuan ini menegaskan bahwa fitur *firewall* pada Mikrotik dapat meningkatkan ketahanan jaringan terhadap serangan DoS secara signifikan.

Kata Kunci: *Denial of Service*, *Firewall*, Mikrotik, *Port Scanning*.

ABSTRACT: *Cybercrimes such as Denial of Service (DoS) attacks pose a serious threat to the stability of computer networks, especially those without adequate protection. This study aims to analyze the implementation of firewall features on Mikrotik routers as an effort to improve network security against DoS attacks. The method used refers to the Network Development Life Cycle (NDLC) approach, which includes the stages of analysis, design, simulation, implementation, and testing. The results show that the firewall configuration successfully closed several vulnerable ports (FTP, SSH, Telnet, and HTTP) while maintaining critical operational ports (DNS and Winbox). Furthermore, the CPU load on the router decreased dramatically from 100% to 3-4% after implementation, indicating success in mitigating malicious traffic. These findings confirm that the firewall feature on Mikrotik can significantly increase network resilience against DoS attacks.*

Keywords: *Denial of Service, Firewall, Mikrotik, Port Scanning.*

How to Cite: Wijaya, F. I., Innuddin, M., & Latif, K. A. (2025). Analisa Penerapan Fitur *Firewall* pada Mikrotik untuk Mengamankan dari Serangan *Denial of Service* (DoS). *Panthera : Jurnal Ilmiah Pendidikan Sains dan Terapan, 5*(3), 570-592. https://doi.org/10.36312/panthera.v5i3.546

PENDAHULUAN

Kejahatan siber selalu berkaitan dengan teknologi informasi dan komputer. Tindakan ini dilakukan dengan cara memasuki sistem jaringan komputer secara ilegal atau tanpa sepengetahuan pemilik jaringan. Serangan siber, terutama *Denial of Service* (DoS), merupakan jenis serangan yang paling sering ditemukan dalam dunia maya (Zukhruf *et al.*, 2023). Menurut Nurilahi *et al.* (2022) yang merujuk pada berbagai jurnal ilmiah, kejahatan siber terus terjadi, termasuk di Indonesia.

Panthera : Jurnal Ilmiah Pendidikan Sains dan Terapan
E-ISSN 2808-246X; P-ISSN 2808-3636
Volume 5, Issue 3, July 2025; Page, 570-592
Email: pantherajurnal@gmail.com

Data dari Pusat Operasi Keamanan Siber Nasional (PUSOPSKAMSINAS) Badan Siber dan Sandi Negara mencatat sebanyak 88.414.296 serangan siber terjadi selama periode 1 Januari hingga 12 April 2020 (BSSN, 2020). Jenis serangan siber yang umum terjadi antara lain *port scanning*, *brute force*, *metasploit*, dan *Denial of Service* (DoS) (Marta *et al.*, 2020). Penelitian oleh Romadhan *et al.* (2020) menunjukkan bahwa serangan *port scanning* terjadi sebanyak 2.053 kejadian, *brute force* sebanyak 606 kejadian, dan serangan DoS sebanyak 428 kejadian. Syaftahan (2024) juga melaporkan bahwa jumlah serangan *Distributed Denial of Service* (DDoS) mengalami peningkatan sebesar 46% dibandingkan periode yang sama tahun sebelumnya, dengan total 445.000 serangan pada kuartal kedua 2024, naik 34% dibandingkan kuartal ketiga dan keempat tahun 2023.

Berbagai upaya telah dilakukan dalam penelitian terdahulu untuk mengatasi serangan DoS, khususnya dengan memanfaatkan fitur *firewall* pada perangkat Mikrotik. Putra *et al.* (2023) meneliti penggunaan *firewall filtering* dan *port knocking* sebagai metode perlindungan. *Firewall filtering* digunakan untuk memeriksa setiap paket berdasarkan aturan tertentu, sedangkan *port knocking* digunakan untuk menyembunyikan *port* yang biasanya terbuka. Syahputra *et al.* (2024) juga meneliti penggunaan *firewall filtering* sebagai pemblokir serangan DoS, dimana setiap paket berbahaya langsung diblokir oleh sistem. Tambunan & Neyman (2024) mengombinasikan *firewall filtering* dan IP *tables*, *firewall filtering* berfungsi menyaring lalu lintas mencurigakan, sementara IP *tables* memberikan kontrol granular atas kebijakan keamanan. Penelitian lain oleh Irwinsyah & Sianipar (2017) mengkaji penggunaan *firewall raw*, *port knocking*, dan *tarpit firewall*. Dalam penelitian tersebut, aturan *firewall* dikonfigurasi pada bagian *chain* untuk mengatur koneksi masuk dan keluar *router*. Salah satu aturan yang diterapkan adalah pemblokiran semua paket TCP dengan tujuan *port* 80 (HTTP) agar tidak diproses lebih lanjut oleh *firewall*.

Berdasarkan permasalahan dan tinjauan pustaka yang telah disampaikan, peneliti mengusulkan ide penelitian dengan judul "Analisis Penerapan Fitur *Firewall* pada Mikrotik untuk Mengamankan Jaringan dari Serangan DoS". *Firewall* merupakan teknologi keamanan jaringan yang digunakan untuk mengontrol, membatasi, atau menolak lalu lintas data dari jaringan luar yang berpotensi berbahaya (Wicaksono & Widiasari, 2022). Salah satu fitur *firewall*, yaitu *firewall raw* berfungsi untuk memblokir IP *address* yang mencurigakan atau tidak sah. Fitur ini memungkinkan sistem memilih untuk melewatkan atau memblokir paket data sebelum memasuki proses *connection tracking*, sehingga dapat menghemat beban CPU. Hal ini sangat efektif untuk memitigasi serangan DoS karena proses pemblokiran dilakukan sejak awal, tepatnya pada *chain prerouting* dan *output* (Jaya *et al.*, 2020). Dengan demikian, penelitian ini bertujuan untuk menganalisis efektivitas penerapan *firewall* Mikrotik, khususnya fitur *raw* dalam memitigasi serangan DoS.

METODE

Penelitian ini menggunakan pendekatan pengembangan sistem berbasis *Network Development Life Cycle* (NDLC) yang terdiri dari enam tahapan utama, yaitu Analisis, Perancangan, Simulasi, Implementasi, dan Pengujian. Penelitian ini

Panthera : Jurnal Ilmiah Pendidikan Sains dan Terapan
E-ISSN 2808-246X; P-ISSN 2808-3636
Volume 5, Issue 3, July 2025; Page, 570-592
Email: pantherajurnal@gmail.com

difokuskan pada penerapan fitur *firewall* pada Mikrotik untuk mengamankan jaringan dari serangan *Denial of Service* (DoS).

Analisis (*Analysis*)

Tahap ini diawali dengan pengumpulan data melalui studi literatur dari jurnal ilmiah, buku, dan laporan penelitian terdahulu yang relevan mengenai serangan DoS, fitur *firewall* Mikrotik, serta metode pertahanan jaringan. Informasi ini digunakan untuk menyusun dasar teori serta merancang langkah-langkah pengamanan jaringan yang diterapkan.

Perancangan (*Design*)

Pada tahap ini dilakukan desain topologi jaringan yang terdiri atas tiga *router* Mikrotik dan beberapa klien. Penentuan IP *Address*, konfigurasi jaringan *Wireless Distribution System* (WDS), serta identifikasi peran setiap perangkat (*admin*, *client*, dan *attacker*) menjadi fokus utama.

Simulasi Prototipe (*Simulation Prototyping*)

Simulasi dilakukan dengan skenario uji coba jaringan dan pengamanan menggunakan *firewall* Mikrotik. Aktivitas yang dilakukan antara lain: 1) pengujian koneksi dan fungsi dasar jaringan; 2) konfigurasi *firewall* pada Mikrotik; 3) simulasi serangan *port scanning* dan DoS; dan 4) pencatatan dan analisis terhadap kondisi jaringan sebelum dan sesudah penerapan *firewall*.

Implementasi (*Implementation*)

Pada tahap implementasi dilakukan konfigurasi *firewall* pada masing-masing *router*, meliputi: 1) *firewall filter*, yaitu mengatur dan memblokir koneksi mencurigakan melalui *chain input*, *forward*, dan *output*; 2) *firewall raw*, yaitu menurunkan beban CPU dengan memblokir paket sebelum melalui *connection tracking*; 3) pembuatan aturan *firewall* menggunakan metode "*add src to address list*" dan "*drop*"; dan 4) penutupan *port* yang rentan (FTP, SSH, Telnet, HTTP) serta pembatasan akses hanya untuk *port* penting, seperti DNS (53) dan *Winbox* (8291).

Pengujian Sistem (*Testing*)

Pengujian dilakukan melalui dua skenario, yaitu sebelum dan sesudah penerapan *firewall*. Pada skenario pertama, dilakukan serangan *port scanning* menggunakan NMAP dan serangan *Denial of Service* (DoS) menggunakan LOIC. Hasil menunjukkan bahwa banyak *port* dalam kondisi terbuka dan penggunaan CPU mencapai 100%. Setelah penerapan *firewall* (skenario kedua), *port-port* berbahaya berhasil ditutup, dan penggunaan CPU menurun drastis menjadi 2–4% meskipun serangan tetap berlangsung. *Log* pada aplikasi *Winbox* juga menunjukkan bahwa *firewall* berhasil memblokir lalu lintas jaringan yang mencurigakan yang mengindikasikan efektivitas konfigurasi dalam memitigasi serangan DoS.

Metode Pengembangan Sistem

Dalam penelitian ini, penulis menggunakan metode pengembangan *Network Development Life Cycle* (NDLC). pengembangan jaringan dilakukan melalui enam tahapan, yaitu sebagai berikut:

Analisis (Analysis)

Pada tahap ini penulis melakukan analisis untuk mendukung penelitian ini mengenai analisa penerapan fitur *firewall* pada Mikrotik untuk mengamankan dari serangan *Denial of Service* dengan melakukan pengumpulan data melalui studi

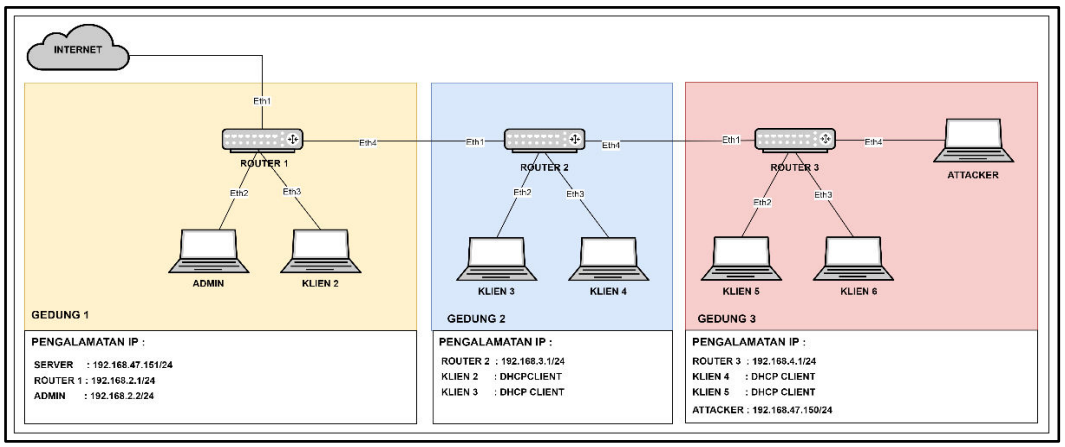
Panthera : Jurnal Ilmiah Pendidikan Sains dan Terapan
E-ISSN 2808-246X; P-ISSN 2808-3636
Volume 5, Issue 3, July 2025; Page, 570-592
Email: pantherajurnal@gmail.com

literatur dari berbagai sumber terpercaya, seperti jurnal ilmiah dan buku. Data yang dikumpulkan kemudian dianalisis untuk memahami mekanisme kerja *firewall* pada Mikrotik, khususnya dalam mendeteksi dan memitigasi serangan *Denial of Service* (DoS).

Perancangan (Design)

Pada tahap desain, penulis akan melakukan rancangan uji coba jaringan dengan admin yang melakukan konfigurasi jaringan berserta keamanan fitur *firewall*. lalu ada *attacker* sebagai penyerang jaringan tersebut, kemudian dilanjutkan dengan pengalamatan IP. Berikut adalah rancangan ujicoba jaringan yang sudah dibuat:

1) Topologi Jaringan *Wireless Distribution System*



Gambar 1. Topologi Jaringan.

2) Pengalamatan IP

Desain pengalamatan IP pada analisa penerapan *firewall* pada Mikrotik. Untuk pengalamatan IP menggunakan kelas C dengan 3 mikrotik, untuk keterangan penegalamatan yang digunakan pada jaringan ini, dapat dilihat pada Tabel 1.

Tabel 1. Pengalamatan IP.

Pengalamatan IP					
Lokasi	**Perangkat**	***Hostname***	***Interface***	**Ip *Address***	***Gateway***
G1	*Router* 1	*Router1*	*Ether* 1	192.168.1.6/24	192.168.1.1
			Bridge 1	192.168.2.1/24	
	Laptop 1	Admin	*Ethernet*	192.168.2.2/24	
	Laptop 2	klien2	*Ethernet*	DHCP *Client*	
G2	*Router* 2	Router2	*Ether* 1	192.168.2.253/24	192.168.2.1
			Bridge 2	192.168.3.1/24	
	Laptop 3	klien 3	*Ethernet*	DHCP *CLIENT*	
	Laptop 4	klien 4	*Ethernet*	DHCP *CLIENT*	
G3	*Router* 3	Router3	*Ether* 1	192.168.3.253/24	192.168.3.1
			Bridge 3	192.168.4.1/24	
	Laptop 5	klien 5	*Ethernet*	DHCP *Client*	
	Laptop 6	klien 6	*Ethernet*	DHCP *Client*	
	Laptop 7	*Attacker*	*Ethernet*	192.168.47.150/24	

Panthera : Jurnal Ilmiah Pendidikan Sains dan Terapan
E-ISSN 2808-246X; P-ISSN 2808-3636
Volume 5, Issue 3, July 2025; Page, 570-592
Email: pantherajurnal@gmail.com

Simulasi Prototipe (Simulation Prototyping)

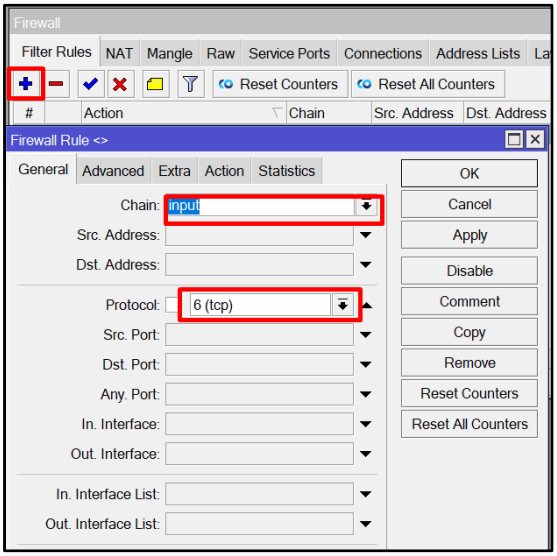
Pengujian dilakukan dengan menguji apakah jaringan sudah terkoneksi dengan internet. Hal ini diawali dengan mencoba utilitas *ping* ke semua *router*. Kemudian, untuk memastikan keandalan jaringan, dilakukan serangkaian tahapan pengujian sebagai berikut: 1) dilakukan konfigurasi terhadap mikrotik untuk kebutuhan *firewall* sesuai dengan topologi yang telah ditetapkan oleh penulis; 2) melakukan *setting* jaringan dan menerapkan *firewall* di dalamnya untuk menambah lapisan keamanan; 3) setelah konfigurasi selesai, penulis melakukan ujicoba serangan menggunakan *port scanning* dan DoS untuk menguji ketahanan jaringan; dan 4) terakhir akan dilakukan analisis hasil uji coba dari semua teknik serangan yang telah dilakukan. Analisis tersebut mencakup kondisi jaringan sebelum dan setelah penerapan keamanan *firewall*, termasuk perbandingan performa jaringan, respons sistem terhadap serangan, serta efektivitas *firewall* dalam memblokir akses tidak sah. Dengan demikian, dari hasil analisis tersebut diharapkan dapat diperoleh simpulan apakah keamanan tersebut dapat menjaga keamanan dari berbagai serangan yang telah diuji coba.

Impelementasi (Impelementation)

Pada tahap ini dilakukan instalasi dan konfigurasi, terbagi menjadi empat tahap, yaitu instalasi dan konfigurasi pada komputer admin, *Router* 1, *Router* 2, dan *Router* 3, dan komputer penyerang.

1) Hasil Konfigurasi

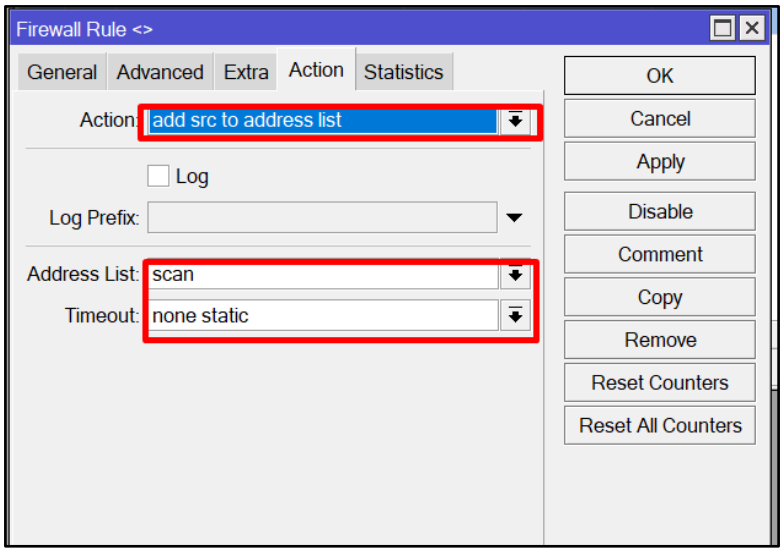
Pada tahap ini dilakukan konfigurasi *firewall* yang pertama masuk ke tab IP, pilih *firewall*, kemudian lakukan konfigurasi seperti pada Gambar 2.



Gambar 2. *Firewall Rule General.*

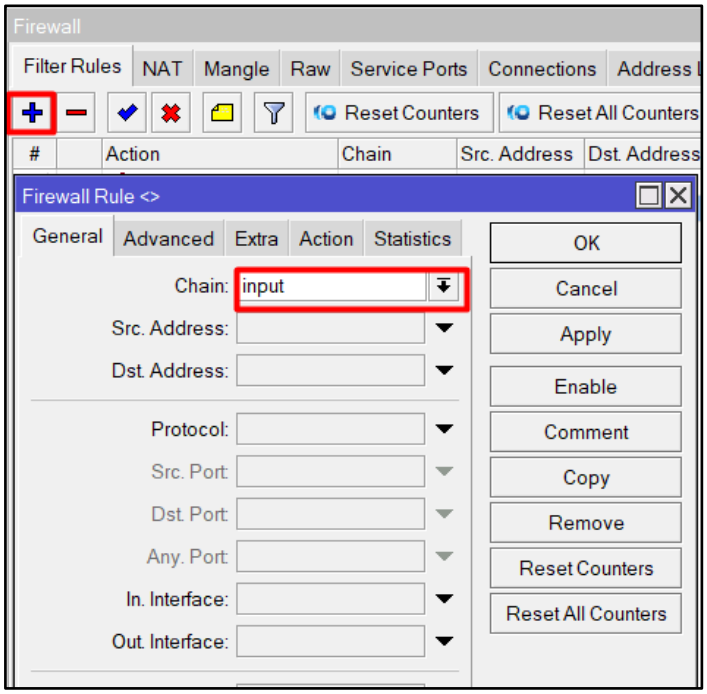
Pada Gambar 2 ditampilkan menu *General Firewall Rule*. Pada tahap ini, konfigurasi *firewall* dilakukan untuk mendeteksi IP penyerang, yang kemudian akan ditampilkan pada *Address List*. Caranya adalah dengan memilih *Chain* "*input*" dan *Protocol* "TCP". Setelah itu, lanjutkan ke *tab action* seperti yang ditunjukkan pada Gambar 3.

Panthera : Jurnal Ilmiah Pendidikan Sains dan Terapan
E-ISSN 2808-246X; P-ISSN 2808-3636
Volume 5, Issue 3, July 2025; Page, 570-592
Email: pantherajurnal@gmail.com



Gambar 3. *Firewall Rule Action*.

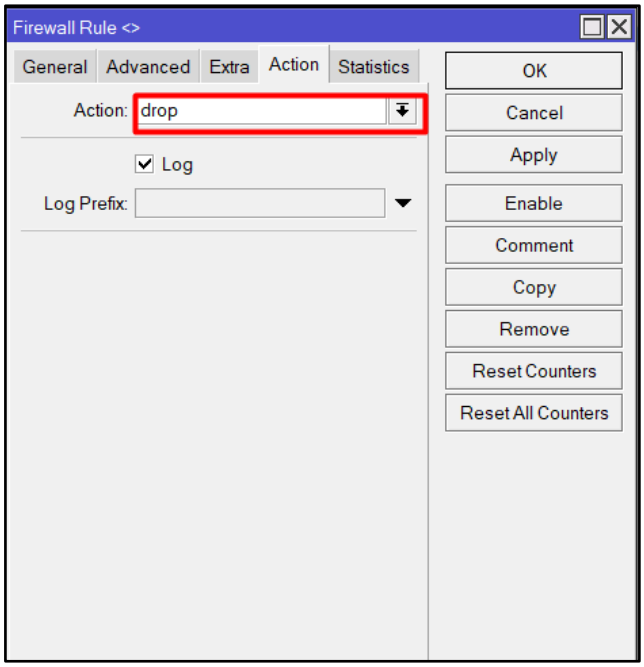
Pada Gambar 3 ditampilkan menu *action* pada aturan *firewall*. Pada tahap ini digunakan opsi *action* "*add src to address list*" dengan *address list* bernama *scan*, serta pengaturan *timeout* diatur pada *none* atau *static*. Opsi ini berfungsi untuk menambahkan alamat IP sumber yang terdeteksi oleh aturan *firewall* ke dalam daftar alamat *scan* yang dapat digunakan untuk keperluan pemantauan atau pemblokiran terhadap sumber berbahaya. Pengaturan *timeout* dengan nilai *none/static* memastikan bahwa alamat IP tersebut tetap berada dalam daftar hingga dihapus secara manual, sehingga memungkinkan pemantauan jangka panjang terhadap aktivitas jaringan yang mencurigakan.



Gambar 4. *Firewall Block General*.

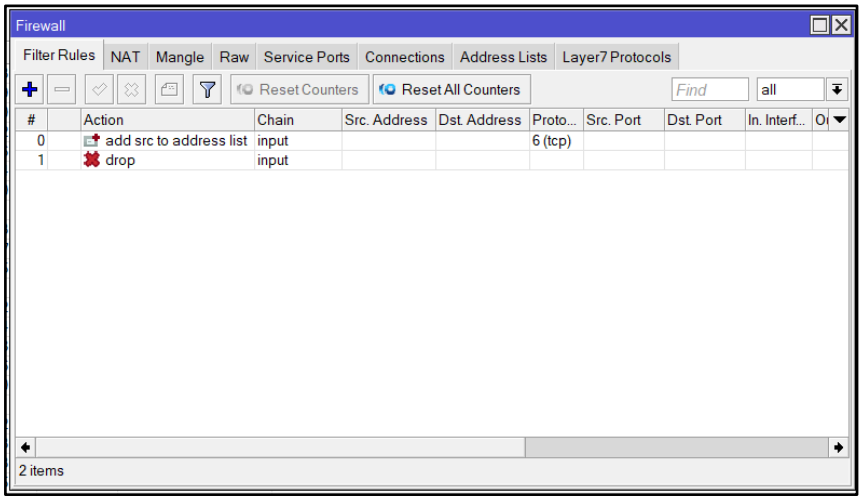
Panthera : Jurnal Ilmiah Pendidikan Sains dan Terapan
E-ISSN 2808-246X; P-ISSN 2808-3636
Volume 5, Issue 3, July 2025; Page, 570-592
Email: pantherajurnal@gmail.com

Pada Gambar 4 ditampilkan menu *General Firewall Rule*. Pada tahap ini, konfigurasi *firewall* dilakukan untuk mem*block* IP penyerang. Caranya adalah dengan memilih *Chain* "*input*". Setelah itu, lanjutkan ke tab *action* seperti yang ditunjukkan pada Gambar 5.



Gambar 5. *Firewall Block Action*.

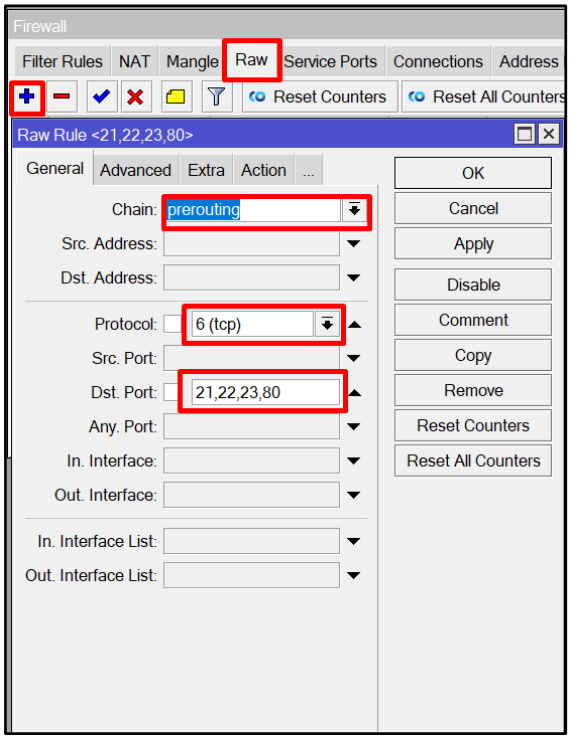
Pada Gambar 5 ditampilkan menu *action* pada aturan *firewall*. Pada tahap ini, digunakan *action* "*drop*". *Action* ini berfungsi untuk memblokir lalu lintas jaringan yang sesuai dengan aturan *firewall* yang telah ditetapkan. Dengan kata lain, setiap paket data yang memenuhi kriteria dalam aturan tersebut akan dibuang dan tidak akan diteruskan ke tujuan, sehingga membantu mencegah akses yang tidak diinginkan ke jaringan.



Gambar 6. Hasil Konfigurasi *Firewall Rule*.

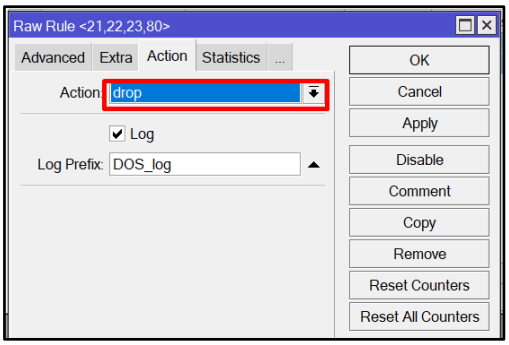
Panthera : Jurnal Ilmiah Pendidikan Sains dan Terapan
E-ISSN 2808-246X; P-ISSN 2808-3636
Volume 5, Issue 3, July 2025; Page, 570-592
Email: pantherajurnal@gmail.com

Pada Gambar 6 ditampilkan hasil konfigurasi *firewall rule* yang telah dilakukan. Selanjutnya akan dilakukan konfigurasi pada tab *raw* seperti pada Gambar 7.



Gambar 7. Konfigurasi *Firewall Raw General*.

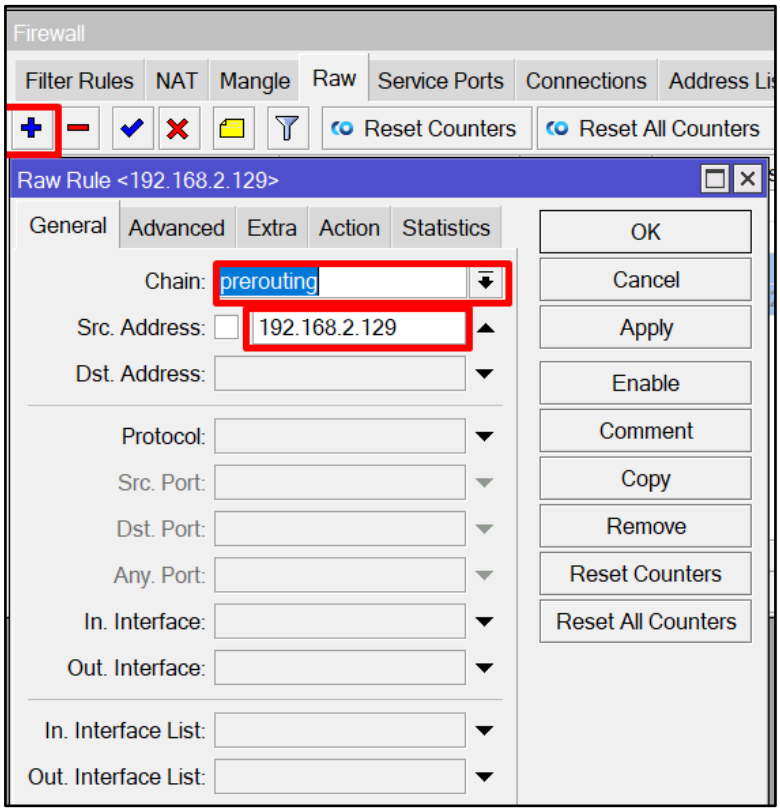
Pada Gambar 7 ditampilkan tampilan *raw* pada tab *general* yang menunjukkan aturan *firewall* dengan penggunaan *chain prerouting* untuk memproses paket sebelum mencapai tujuan akhir. Protokol yang digunakan adalah TCP, dan aturan ini diterapkan pada beberapa *port* tujuan penting, yaitu port 21 untuk FTP (*transfer file*), *port* 22 untuk SSH (koneksi aman jarak jauh), port 23 untuk TELNET (komunikasi jarak jauh), serta port 80 untuk HTTP (akses *web*). Aturan ini berfungsi untuk mengelola lalu lintas jaringan yang berkaitan dengan layanan-layanan tersebut. Selanjutnya, konfigurasi akan dilanjutkan pada tab *action* sebagaimana ditampilkan pada Gambar 8.



Gambar 8. Konfigurasi *Firewall Raw Action*.

Panthera : Jurnal Ilmiah Pendidikan Sains dan Terapan
E-ISSN 2808-246X; P-ISSN 2808-3636
Volume 5, Issue 3, July 2025; Page, 570-592
Email: pantherajurnal@gmail.com

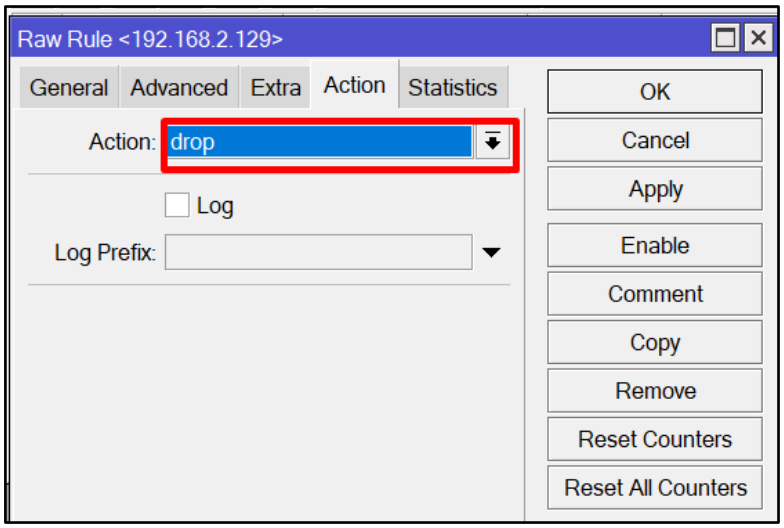
Pada Gambar 8, tampilan menu *action* di *firewall raw* menunjukkan penggunaan *action* "*drop*", yang berarti paket data yang memenuhi aturan tertentu akan dibuang tanpa diproses lebih lanjut. *Action* "*drop*" ini digunakan untuk memblokir lalu lintas jaringan yang dianggap tidak diinginkan atau berpotensi berbahaya sebelum mencapai tujuan, sehingga meningkatkan keamanan jaringan dengan mencegah akses atau aktivitas yang tidak diotorisasi. Selanjutnya dilakukan konfigurasi untuk *blocking* alamat IP yang mencurigakan, seperti pada Gambar 9.



Gambar 9. Konfigurasi *Firewall Raw Block General.*

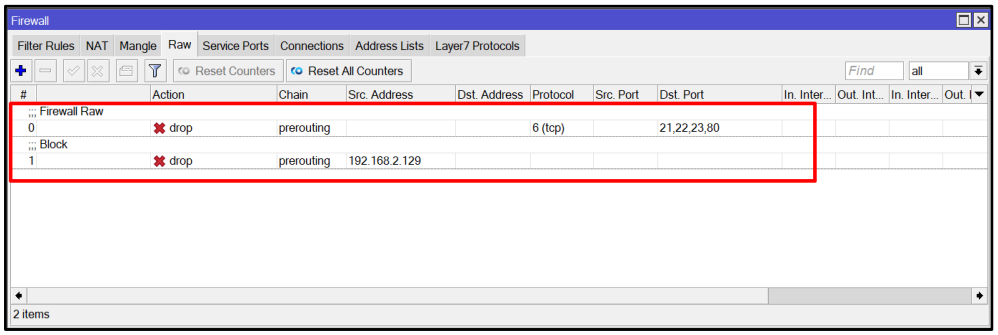
Pada Gambar 9, tampilan menu *general* di *firewall raw* menunjukkan penggunaan *chain prerouting*, dimana aturan diterapkan pada paket sebelum mencapai tujuan akhirnya. Selain itu, *src address* (alamat sumber) yang digunakan adalah "192.168.2.129" yang berarti aturan ini berlaku khusus untuk lalu lintas yang berasal dari alamat IP tersebut. Dengan demikian, *firewall* akan memproses atau memfilter paket data yang datang dari alamat IP 192.168.2.129 sesuai dengan aturan yang telah ditetapkan. Aturan ini dapat mencakup tindakan seperti menerima (*accept*), menolak (*drop*), atau meneruskan (*redirect*) paket tersebut, tergantung pada konfigurasi spesifik yang ditetapkan dalam *rule firewall*. Dengan menggunakan *chain prerouting*, pemrosesan dilakukan sebelum *routing decision* dibuat, sehingga sangat efektif untuk mengarahkan atau memanipulasi paket sejak awal, misalnya dalam implementasi NAT. Konfigurasi ini berguna untuk mengontrol akses awal ke jaringan dan meningkatkan keamanan. Selanjutnya dilakukan konfigurasi pada tab *action* seperti pada Gambar 10.

Panthera : Jurnal Ilmiah Pendidikan Sains dan Terapan
E-ISSN 2808-246X; P-ISSN 2808-3636
Volume 5, Issue 3, July 2025; Page, 570-592
Email: pantherajurnal@gmail.com



Gambar 10. Konfigurasi *Firewall Raw Block Action*.

Pada Gambar 10 ditampilkan tampilan menu *action* pada *firewall raw* yang menunjukkan penggunaan opsi *action* "*drop*". Opsi ini berarti bahwa paket data yang memenuhi kriteria aturan tertentu akan dibuang tanpa diproses lebih lanjut. Penggunaan *action* "*drop*" bertujuan untuk memblokir lalu lintas jaringan yang tidak diinginkan atau berbahaya sebelum mencapai tujuan akhirnya. Dengan demikian, aturan ini berperan penting dalam meningkatkan keamanan jaringan, karena dapat mencegah akses dari sumber yang tidak sah atau tidak terotorisasi.



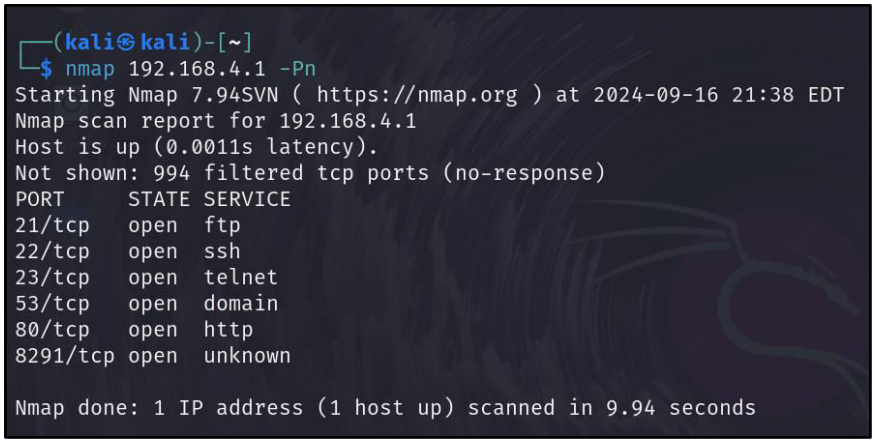
Gambar 11. Hasil Konfigurasi *Firewall Raw*.

Pada Gambar 11, tampilan menunjukkan hasil konfigurasi *firewall raw* yang dirancang untuk memfilter paket yang masuk dan memblokir alamat IP yang mencurigakan. Konfigurasi ini membantu dalam mengelola lalu lintas jaringan dengan mengidentifikasi dan menolak paket dari sumber yang dianggap berpotensi berbahaya atau tidak diinginkan, sehingga meningkatkan keamanan jaringan secara keseluruhan dengan mencegah akses dari IP yang mencurigakan.

2) Hasil Pengujian Serangan

Pada tahap ini dilakukan pengujian terhadap serangan yang terdiri atas *port scanning* dan *Denial of Service* (DoS). Pengujian pertama adalah serangan *port scanning*, dimana serangan dilakukan terhadap alamat IP target 192.168.4.1 menggunakan aplikasi NMAP. Hasil serangan dapat dilihat pada Gambar 12.

Panthera : Jurnal Ilmiah Pendidikan Sains dan Terapan
E-ISSN 2808-246X; P-ISSN 2808-3636
Volume 5, Issue 3, July 2025; Page, 570-592
Email: pantherajurnal@gmail.com

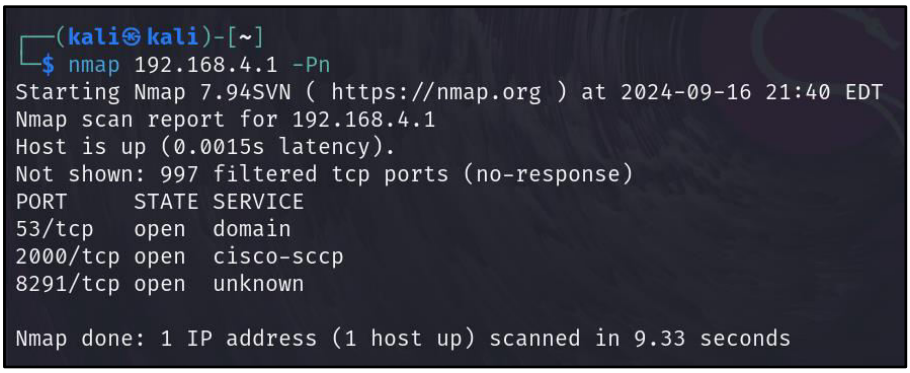


Gambar 12. *Port Scanning* Sebelum Diterapkan Keamanan.

Tabel 2. *Port Scanning* Sebelum Diterapkan Keamanan.

No.	IP	*Port*	*State*	*Service*
1	192.168.4.1	21/tcp	*open*	*ftp*
2	192.168.4.1	22/tcp	*open*	*ssh*
3	192.168.4.1	23/tcp	*open*	*telnet*
4	192.168.4.1	53/tcp	*open*	*domain*
5	192.168.4.1	80/tcp	*open*	*http*
6	192.168.4.1	8291/tcp	*open*	*unknown*

Hasil uji coba serangan *port scanning* sebelum penerapan tindakan keamanan ditunjukkan pada Gambar 12 yang memperlihatkan banyak *port* dalam kondisi terbuka, antara lain *port* 21 (FTP), *port* 22 (SSH), *port* 23 (Telnet), *port* 53 (DNS), *port* 80 (HTTP), dan *port* 8291 (*Winbox*). *Port* 22 memberikan akses *remote* yang aman, sementara *port* 80 digunakan untuk layanan *web*. Selanjutnya yang kedua, setelah konfigurasi keamanan diterapkan, dilakukan kembali serangan *port scanning* terhadap IP target 192.168.4.1 menggunakan NMAP. Hasil pemindaian tersebut ditunjukkan pada Gambar 13.



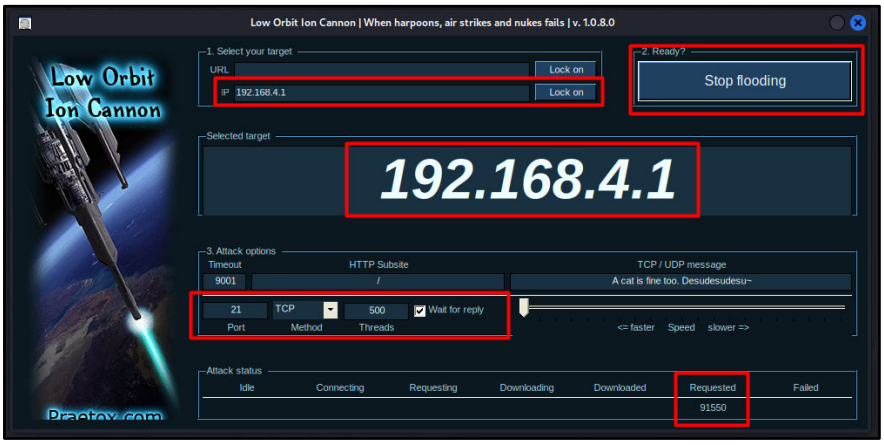
Gambar 13. *Port Scanning* Setelah Diterapkan Keamanan.

Tabel 3. *Port Scanning* Setelah Diterapkan Keamanan.

No.	IP	*Port*	*State*	*Service*
1	192.168.4.1	53/tcp	*open*	*Domain*
2	192.168.4.1	2000/tcp	*open*	*cisco-sccp*
3	192.168.4.1	8291/tcp	*open*	*unknown*

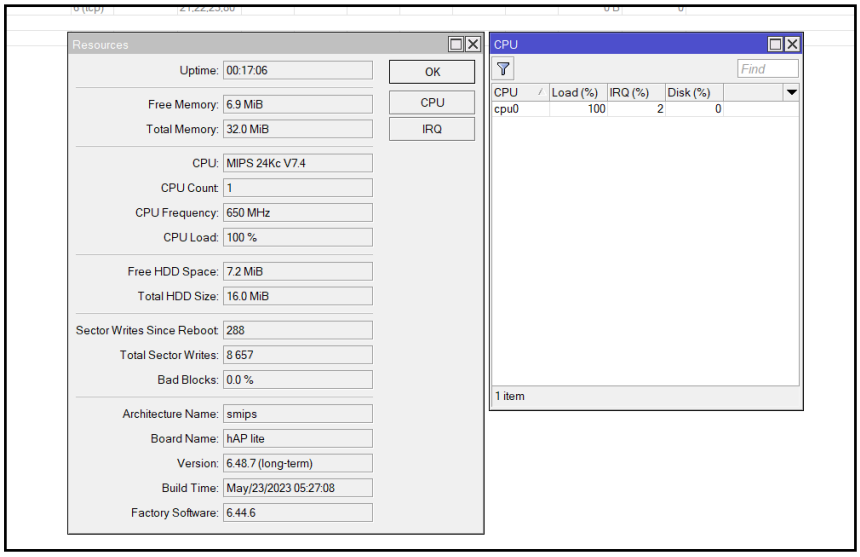
Panthera : Jurnal Ilmiah Pendidikan Sains dan Terapan
E-ISSN 2808-246X; P-ISSN 2808-3636
Volume 5, Issue 3, July 2025; Page, 570-592
Email: pantherajurnal@gmail.com

Setelah prosedur keamanan diterapkan, hanya *port* 53 (DNS), *port* 2000 (*Cisco* SCCP), dan *port* 8291 (*Winbox*) yang tetap terbuka, sebagaimana ditunjukkan pada Gambar 13. Hal ini menunjukkan adanya penurunan jumlah *port* terbuka yang signifikan dibandingkan sebelumnya. Untuk mengurangi risiko eksploitasi dari luar, *port* 21, 22, 23, dan 80 telah ditutup. Selanjutnya, tahap ketiga adalah serangan *Denial of Service* (DoS), dimana dilakukan serangan terhadap IP target 192.168.4.1 pada *port* 21, 22, 23, dan 80 menggunakan aplikasi LOIC.



Gambar 14. Serangan DoS pada *Port* 21.

Pada Gambar 14, aplikasi LOIC memasukkan IP target 192.168.4.1. Kemudian, pada bagian *port*, ditambahkan 21, metode TCP, dan jumlah *threads* atau permintaan yang akan dikirimkan diatur menjadi 500. Selanjutnya, buka aplikasi *Winbox* dan cari tab *Resources*.

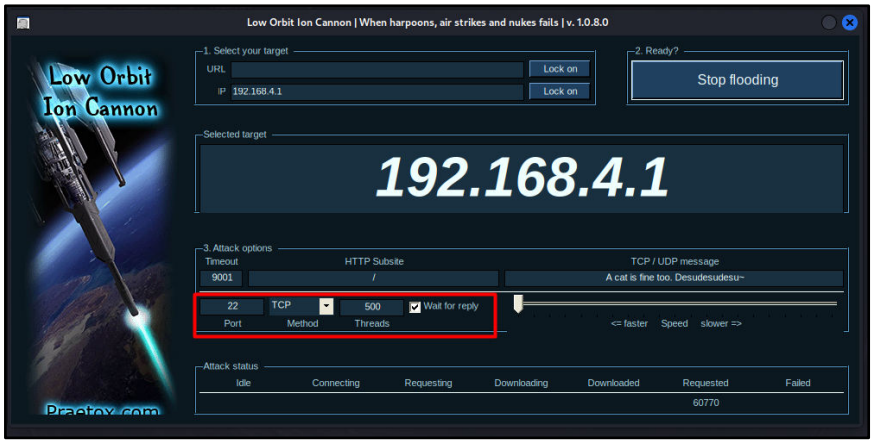


Gambar 15. Hasil Serangan DoS.

Sebelum langkah-langkah keamanan diambil, Gambar 15 menunjukkan bahwa sistem sangat rentan terhadap serangan *Denial of service* (DoS). Dalam situasi ini, penyerang berusaha membuat *server* kewalahan dengan mengirimkan

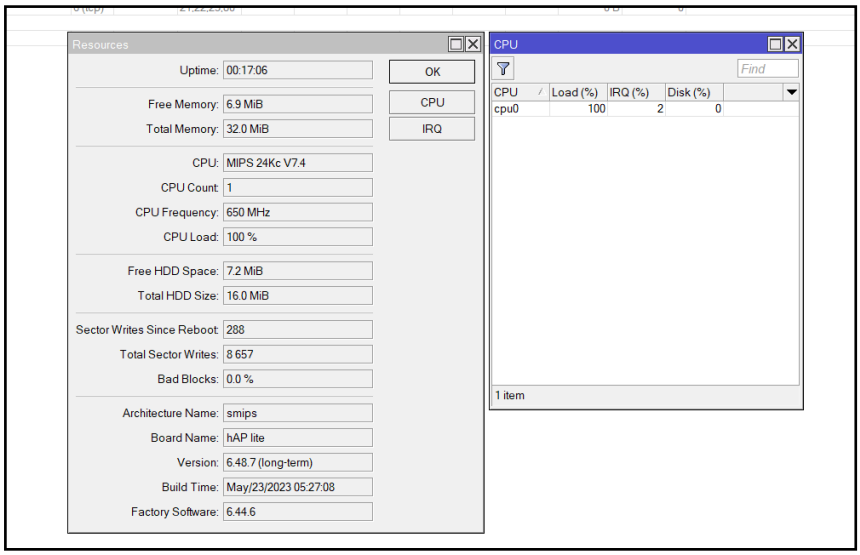
Panthera : Jurnal Ilmiah Pendidikan Sains dan Terapan
E-ISSN 2808-246X; P-ISSN 2808-3636
Volume 5, Issue 3, July 2025; Page, 570-592
Email: pantherajurnal@gmail.com

banyak permintaan secara bersamaan. Hasil uji coba serangan DoS menunjukkan peningkatan penggunaan CPU hingga 100% yang menyebabkan layanan tidak responsif atau *downtime*.



Gambar 16. Serangan DoS pada *Port* 22.

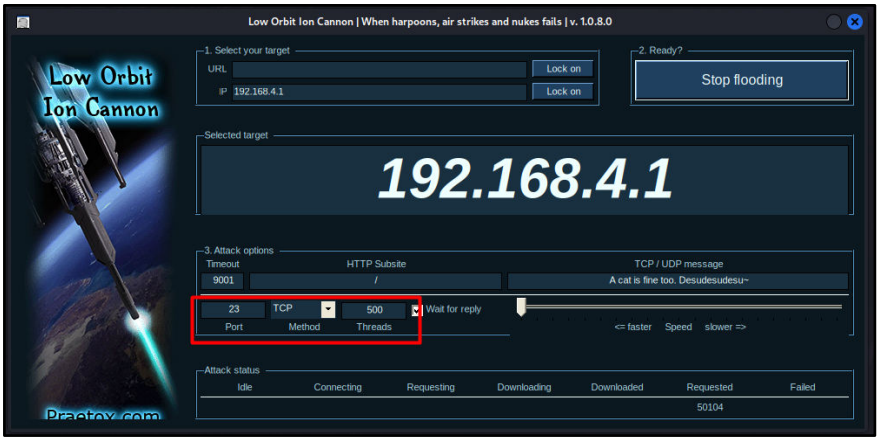
Pada Gambar 16, aplikasi LOIC memasukkan IP target 192.168.4.1. Kemudian, pada bagian *port*, ditambahkan 22, metode TCP, dan jumlah *threads* atau permintaan yang akan dikirimkan diatur menjadi 500. Selanjutnya, buka aplikasi *Winbox* dan cari tab *Resources*.



Gambar 17. Hasil Serangan DoS.

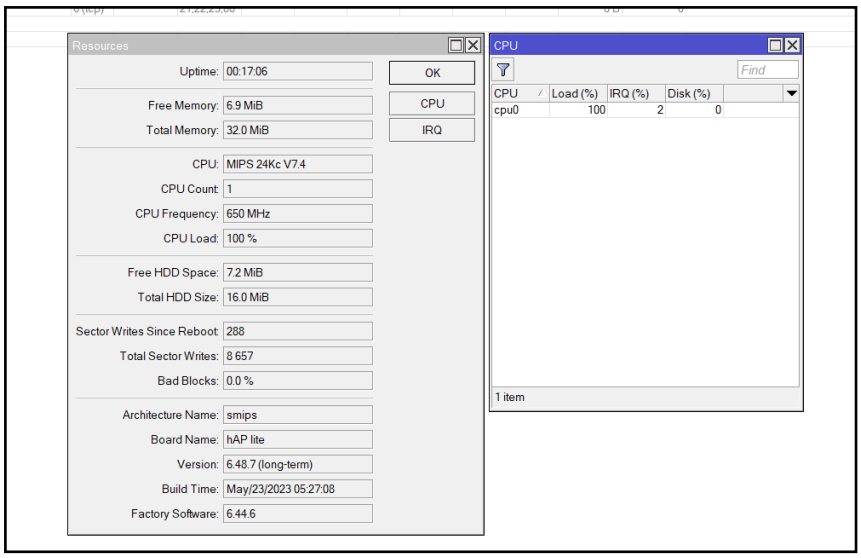
Sebelum langkah-langkah keamanan diambil, Gambar 17 menunjukkan bahwa sistem sangat rentan terhadap serangan *Denial of service* (DoS). Dalam situasi ini, penyerang berusaha membuat *server* kewalahan dengan mengirimkan banyak permintaan secara bersamaan. Hasil uji coba serangan DoS menunjukkan peningkatan penggunaan CPU hingga 100%, yang menyebabkan layanan tidak responsif atau *downtime*. Setelah penerapan keamanan, ketahanan sistem meningkat, penggunaan CPU menurun, dan layanan tetap responsif.

Panthera : Jurnal Ilmiah Pendidikan Sains dan Terapan
E-ISSN 2808-246X; P-ISSN 2808-3636
Volume 5, Issue 3, July 2025; Page, 570-592
Email: pantherajurnal@gmail.com



Gambar 18. Serangan DoS pada *Port* 23.

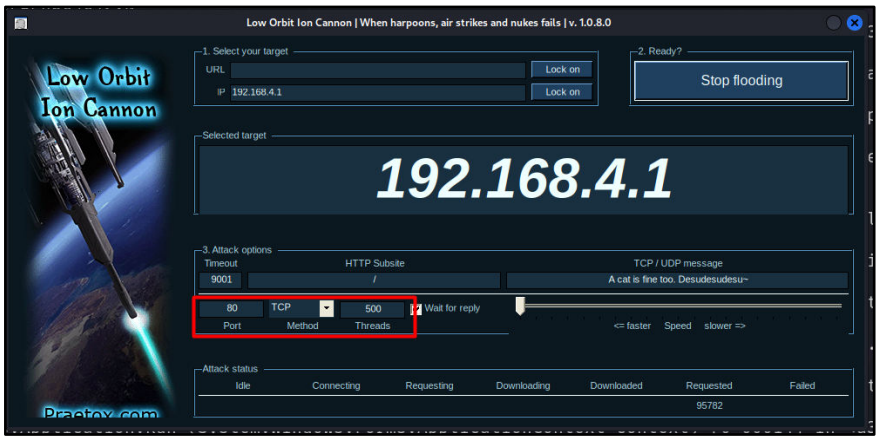
Pada gambar 18, aplikasi LOIC memasukkan IP target 192.168.4.1. Kemudian, pada bagian *port* ditambahkan 23, metode TCP, dan jumlah *threads* atau permintaan yang akan dikirimkan diatur menjadi 500. Selanjutnya, buka aplikasi *Winbox* dan cari tab *Resources*.



Gambar 19. Hasil Serangan DoS.

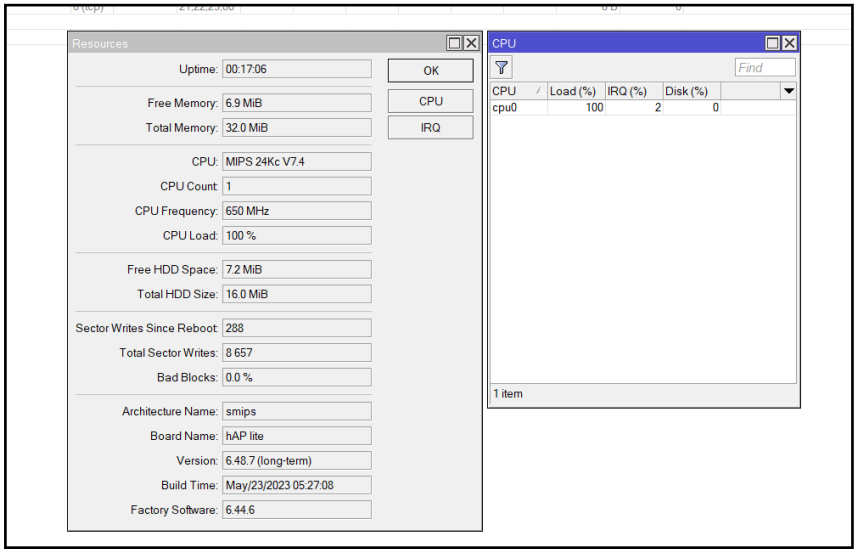
Sebelum langkah-langkah keamanan diambil, Gambar 19 menunjukkan bahwa sistem sangat rentan terhadap serangan *Denial of service* (DoS). Dalam situasi ini, penyerang berusaha membuat *server* kewalahan dengan mengirimkan banyak permintaan secara bersamaan. Hasil uji coba serangan DoS menunjukkan peningkatan penggunaan CPU hingga 100%, yang menyebabkan layanan tidak responsif atau *downtime*. Kondisi ini menunjukkan bahwa server tidak memiliki mekanisme proteksi yang memadai untuk menangani lonjakan lalu lintas yang tidak wajar, seperti pembatasan laju (*rate limiting*), *Firewall* Aplikasi Web (WAF), atau sistem deteksi dan pencegahan intrusi (IDS/IPS). Tanpa mitigasi yang tepat, serangan ini dapat mengganggu layanan, merusak reputasi, dan menimbulkan kerugian besar.

Panthera : Jurnal Ilmiah Pendidikan Sains dan Terapan
E-ISSN 2808-246X; P-ISSN 2808-3636
Volume 5, Issue 3, July 2025; Page, 570-592
Email: pantherajurnal@gmail.com



Gambar 20. Serangan DoS pada *Port* 80.

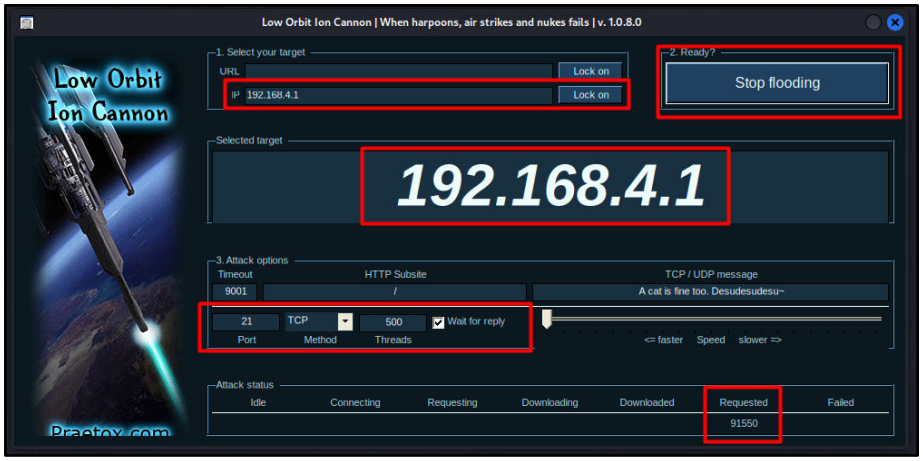
Pada Gambar 20, aplikasi LOIC memasukkan IP target 192.168.4.1. Kemudian, pada bagian *port* ditambahkan 80, metode TCP, dan jumlah *threads* atau permintaan yang akan dikirimkan diatur menjadi 500. Selanjutnya, buka aplikasi *Winbox* dan cari tab *Resources*.



Gambar 21. Hasil Serangan DoS.

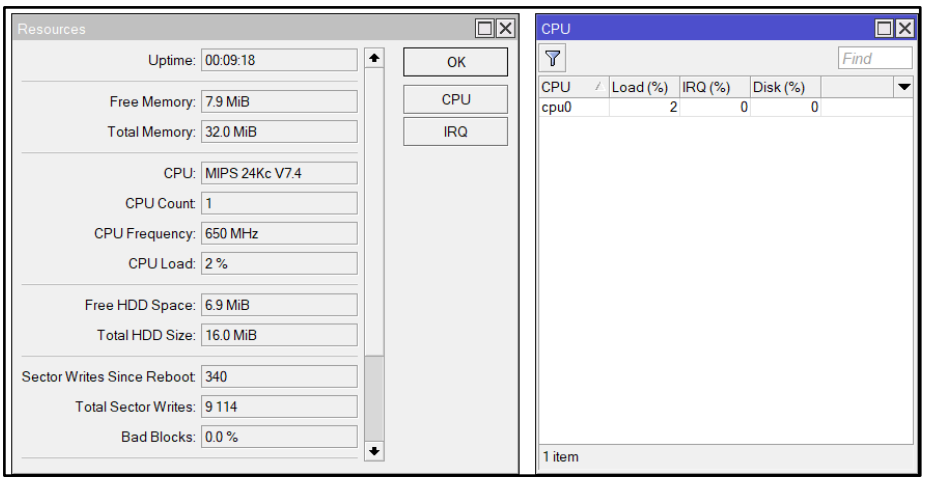
Sebelum langkah-langkah keamanan diambil, Gambar 21 menunjukkan bahwa sistem sangat rentan terhadap serangan *Denial of service* (DoS). Dalam situasi ini, penyerang berusaha membuat *server* kewalahan dengan mengirimkan banyak permintaan secara bersamaan. Hasil uji coba serangan DoS menunjukkan peningkatan penggunaan CPU hingga 100%, yang menyebabkan layanan tidak responsif atau *downtime*. Setelah penerapan keamanan, sistem tahan serangan DoS dengan CPU stabil di bawah 70% dan layanan tetap responsif. Selanjutnya tahap keempat, yaitu *Denial of Service* (DoS) setelah diterapkan keamanan, pada tahap ini, dilakukan serangan DoS setelah diterapkan keamanan dengan IP target 192.168.4.1 pada port 21, 22, 23, dan 80 menggunakan LOIC, seperti berikut ini.

Panthera : Jurnal Ilmiah Pendidikan Sains dan Terapan
E-ISSN 2808-246X; P-ISSN 2808-3636
Volume 5, Issue 3, July 2025; Page, 570-592
Email: pantherajurnal@gmail.com



Gambar 22. Serangan DoS pada *Port* 21.

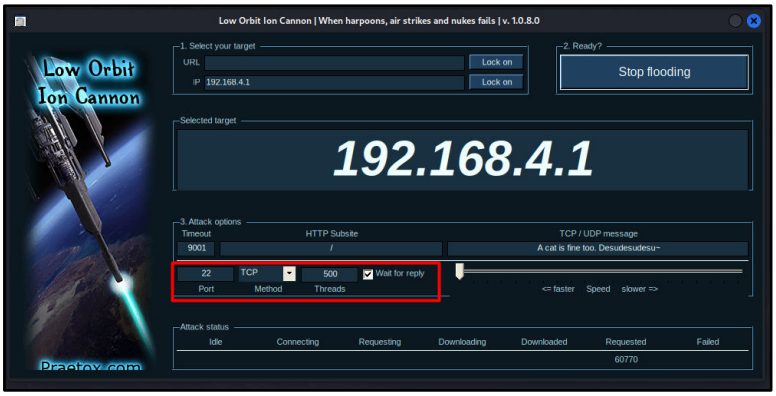
Pada Gambar 22, aplikasi LOIC memasukkan IP target 192.168.4.1. Kemudian, pada bagian *port* ditambahkan 21, metode TCP, dan jumlah *threads* atau permintaan yang akan dikirimkan diatur menjadi 500. Selanjutnya, buka aplikasi *Winbox* dan cari tab *Resources*.



Gambar 23. Hasil Serangan DoS.

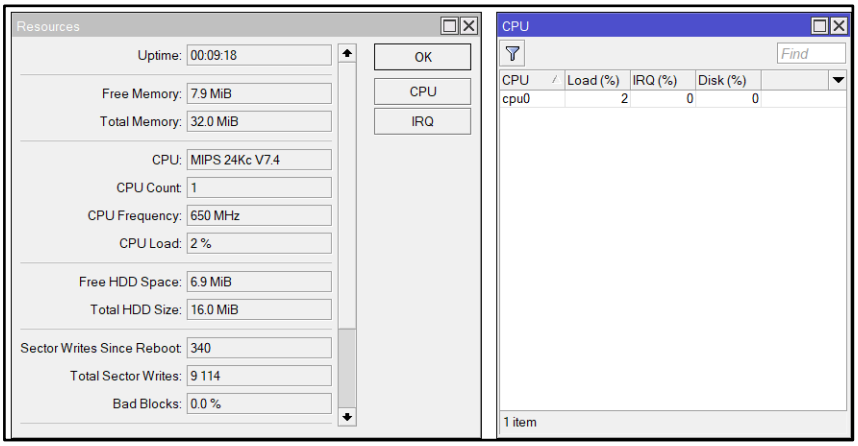
Setelah langkah-langkah keamanan diterapkan, sistem menunjukkan peningkatan yang signifikan dalam menahan serangan *Denial of service* (DoS). Akibatnya, penggunaan CPU tetap stabil pada 2% meskipun terjadi serangan DoS. Hal ini menunjukkan efektivitas mekanisme proteksi yang diterapkan, sehingga mampu menjaga ketersediaan layanan tanpa mengorbankan performa sistem secara keseluruhan. Dengan stabilnya penggunaan CPU, sistem dapat tetap responsif dan melayani pengguna secara optimal meskipun dalam kondisi serangan. Penurunan beban pada sumber daya sistem juga mengurangi risiko terjadinya *downtime* dan memperpanjang umur perangkat keras. Keberhasilan ini membuka peluang untuk mengimplementasikan langkah-langkah keamanan tambahan yang lebih canggih guna menghadapi ancaman siber di masa mendatang.

Panthera : Jurnal Ilmiah Pendidikan Sains dan Terapan
E-ISSN 2808-246X; P-ISSN 2808-3636
Volume 5, Issue 3, July 2025; Page, 570-592
Email: pantherajurnal@gmail.com



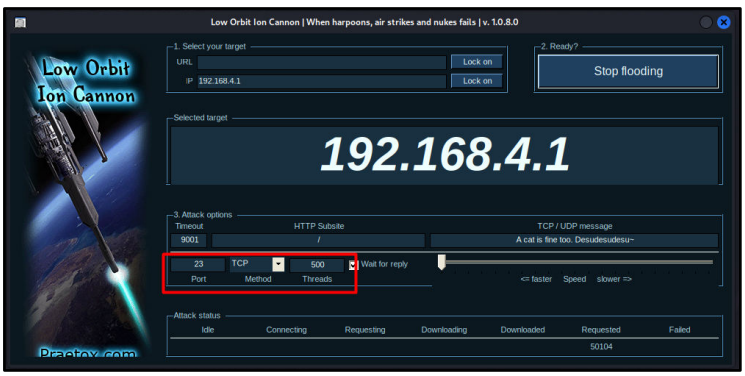
Gambar 24. Serangan DoS pada *Port* 22.

Pada Gambar 24, aplikasi LOIC memasukkan IP target 192.168.4.1. Kemudian, pada bagian *port* ditambahkan 22, metode TCP, dan jumlah *threads* atau permintaan yang akan dikirimkan diatur menjadi 500. Selanjutnya, buka aplikasi *Winbox* dan cari tab *Resources*.



Gambar 25. Hasil Serangan DoS.

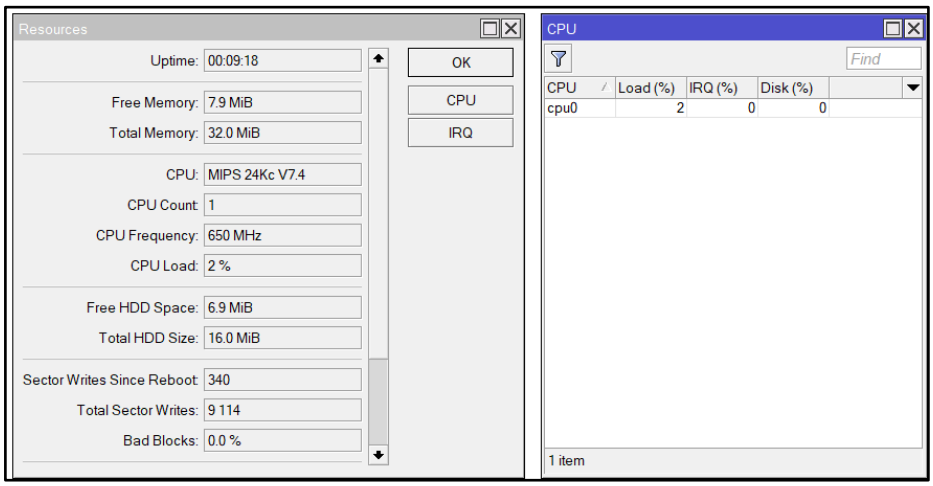
Setelah langkah-langkah keamanan diterapkan, sistem menunjukkan peningkatan yang signifikan dalam menahan serangan *Denial of service* (DoS). Akibatnya, penggunaan CPU tetap stabil pada 2% meskipun terjadi serangan DoS.



Gambar 26. Serangan DoS pada *Port* 23.

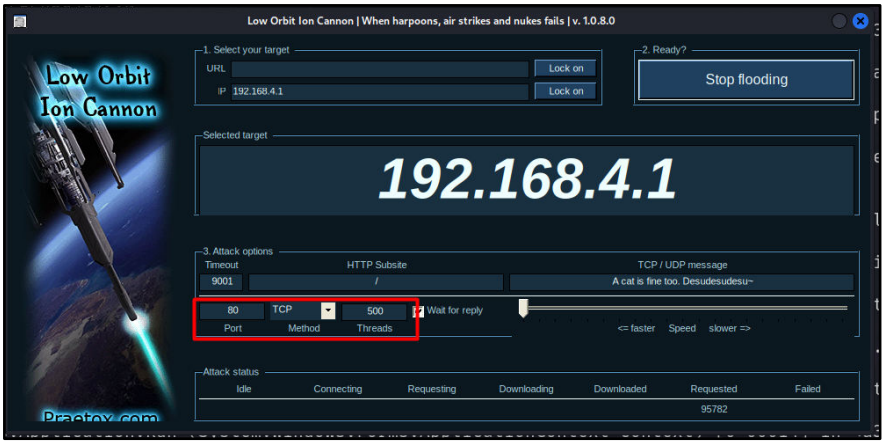
Panthera : Jurnal Ilmiah Pendidikan Sains dan Terapan
E-ISSN 2808-246X; P-ISSN 2808-3636
Volume 5, Issue 3, July 2025; Page, 570-592
Email: pantherajurnal@gmail.com

Pada Gambar 26, aplikasi LOIC memasukkan IP target 192.168.4.1. Kemudian, pada bagian *port* ditambahkan 23, metode TCP, dan jumlah *threads* atau permintaan yang akan dikirimkan diatur menjadi 500. Selanjutnya, buka aplikasi *Winbox* dan cari tab *Resources*.



Gambar 27. Hasil Serangan DoS.

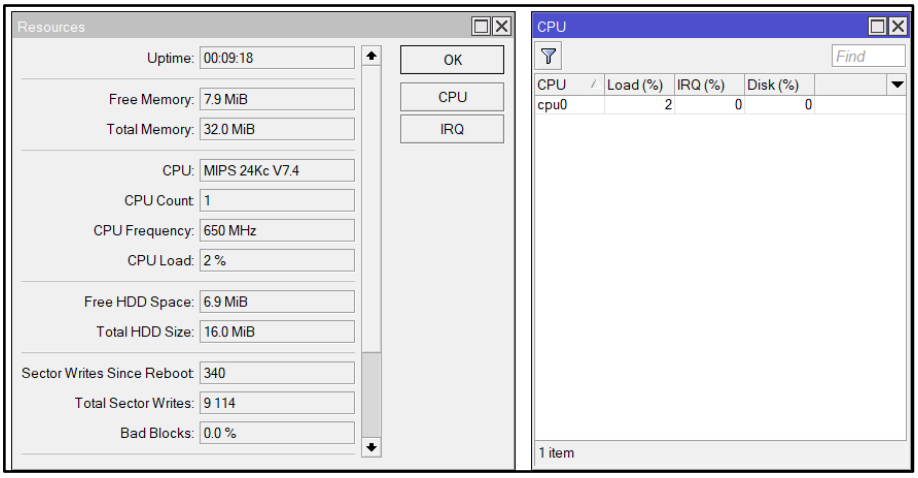
Setelah langkah-langkah keamanan diterapkan, sistem menunjukkan peningkatan yang signifikan dalam menahan serangan *Denial of service* (DoS). Akibatnya, penggunaan CPU tetap stabil pada 2% meskipun terjadi serangan DoS.



Gambar 28. Serangan DoS pada *Port* 80.

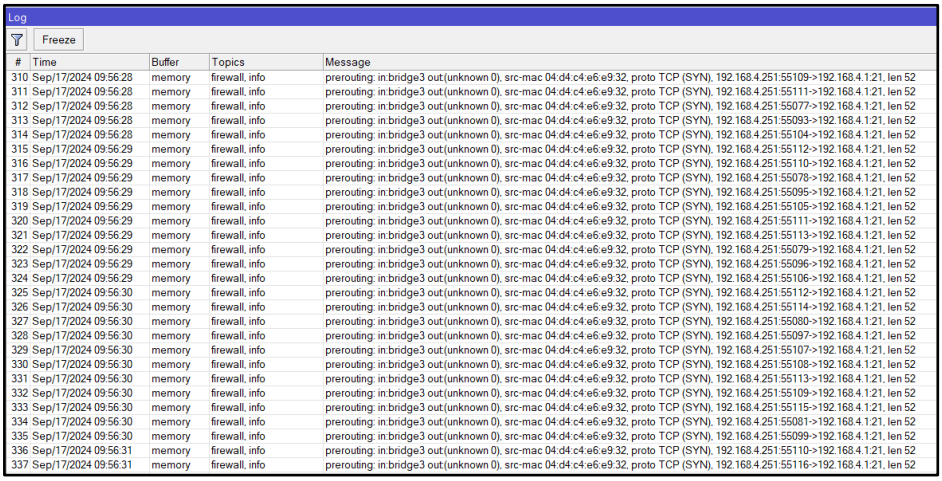
Pada Gambar 28, aplikasi LOIC memasukkan IP target 192.168.4.1. Kemudian, pada bagian *port* ditambahkan 80, metode TCP, dan jumlah *threads* atau permintaan yang akan dikirimkan diatur menjadi 500. Selanjutnya, buka aplikasi *Winbox* dan cari tab *Resources* untuk memantau penggunaan sumber daya pada perangkat Mikrotik, seperti *CPU usage*, *memory usage*, dan *traffic load*. Jika serangan LOIC berhasil mengirimkan sejumlah besar permintaan TCP ke *port* 80 dari IP target 192.168.4.1, maka pada tab *Resources* akan terlihat lonjakan signifikan pada penggunaan CPU dan *bandwidth*, yang menunjukkan bahwa perangkat sedang mengalami tekanan akibat serangan tersebut.

Panthera : Jurnal Ilmiah Pendidikan Sains dan Terapan
E-ISSN 2808-246X; P-ISSN 2808-3636
Volume 5, Issue 3, July 2025; Page, 570-592
Email: pantherajurnal@gmail.com



Gambar 29. Hasil Serangan DoS.

Setelah langkah-langkah keamanan diterapkan, sistem menunjukkan peningkatan yang signifikan dalam menahan serangan *Denial of service* (DoS). Akibatnya, penggunaan CPU tetap stabil pada 2% meskipun terjadi serangan DoS.



Gambar 30. *Log* Serangan pada *Winbox*.

Pada Gambar 30 ditampilkan *log* aplikasi *Winbox* yang menunjukkan adanya percobaan serangan DoS (*Denial of service*). *Log* tersebut memperlihatkan bahwa *firewall* berhasil mendeteksi dan memblokir (*drop*) paket-paket yang mencurigakan, menandakan bahwa mekanisme keamanan *firewall* berfungsi dengan baik.

HASIL DAN PEMBAHASAN

Hasil Pengujian *Port Scanning*

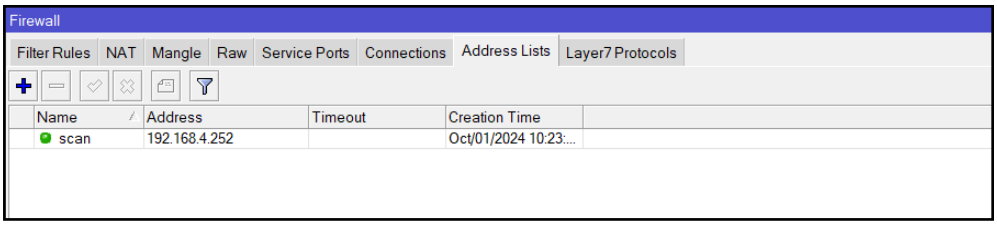
Pengujian ini dilakukan menggunakan NMAP untuk mengevaluasi efektivitas konfigurasi *firewall* dalam menutup *port-port* yang rentan pada tiga *router*, dengan tujuan untuk mengidentifikasi celah keamanan yang masih terbuka serta menilai sejauh mana konfigurasi saat ini mampu mencegah akses tidak sah atau potensi serangan dari luar jaringan. Hasil pengujian dirangkum pada Tabel 4.

Panthera : Jurnal Ilmiah Pendidikan Sains dan Terapan
E-ISSN 2808-246X; P-ISSN 2808-3636
Volume 5, Issue 3, July 2025; Page, 570-592
Email: pantherajurnal@gmail.com

Tabel 4. Hasil Rata-rata Pengujian *Port Scanning* Sebelum dan Sesudah Penerapan Keamanan.

No.	Tujuan	*Port*	*Service*	Status Penerapan Keamanan		Durasi Waktu Rata-rata	
				Sebelum	Sesudah	Sebelum	Sesudah
1	*Router* 1	21	FTP	*Open*	*Closed*	9.95s	9.32s
		22	SSH	*Open*	*Closed*		
		23	Telnet	*Open*	*Closed*		
		53	DNS	*Open*	*Open*		
		80	HTTP	*Open*	*Closed*		
		2000	UDP	*Open*	*Open*		
		8291	*Winbox*	*Open*	*Open*		
2	*Router* 2	21	FTP	*Open*	*Closed*	9.89s	9.23s
		22	SSH	*Open*	*Closed*		
		23	Telnet	*Open*	*Closed*		
		53	DNS	*Open*	*Open*		
		80	HTTP	*Open*	*Closed*		
		2000	UDP	*Open*	*Open*		
		8291	*Winbox*	*Open*	*Open*		
3	*Router* 3	21	FTP	*Open*	*Closed*	9.94s	9.33s
		22	SSH	*Open*	*Closed*		
		23	Telnet	*Open*	*Closed*		
		53	DNS	*Open*	*Open*		
		80	HTTP	*Open*	*Closed*		
		2000	UDP	*Open*	*Open*		
		8291	*Winbox*	*Open*	*Open*		

Hasil menunjukkan bahwa sebelum konfigurasi keamanan diterapkan, *port* penting seperti FTP (21), SSH (22), Telnet (23), dan HTTP (80) berada dalam keadaan terbuka, mengindikasikan kerentanan jaringan terhadap potensi eksploitasi. Namun, setelah konfigurasi *firewall* dilakukan, *port-port* tersebut berhasil ditutup, menyisakan hanya *port* DNS (53), UDP (2000), dan *Winbox* (8291) yang tetap terbuka untuk keperluan operasional. Temuan ini sejalan dengan hasil studi Putra *et al.* (2023) dan Syahputra *et al.* (2024) yang menyatakan bahwa konfigurasi *port filtering* pada *firewall* Mikrotik efektif dalam mencegah eksploitasi terhadap layanan terbuka. Keberadaan *address list* sebagai hasil dari aturan *firewall* juga menunjukkan bahwa sistem mampu mengidentifikasi IP penyerang (Gambar 31), sehingga meningkatkan kontrol terhadap sumber lalu lintas mencurigakan. Penutupan *port* ini tidak hanya mengurangi risiko serangan *brute force* dan eksploitasi terhadap kelemahan perangkat lunak, tetapi juga secara umum menurunkan potensi serangan, sehingga menjadikan jaringan lebih sulit diakses oleh pihak yang tidak berwenang. Langkah ini menegaskan pentingnya manajemen *port* yang baik dalam strategi keamanan jaringan.



Gambar 31. Tampilan *Address List*.

Panthera : Jurnal Ilmiah Pendidikan Sains dan Terapan
E-ISSN 2808-246X; P-ISSN 2808-3636
Volume 5, Issue 3, July 2025; Page, 570-592
Email: pantherajurnal@gmail.com

Pada Gambar 31, ditampilkan menu *address list* pada *firewall*. Pada bagian ini, IP penyerang yang melakukan pemindaian (*scanning*) *port* terhadap alamat IP *router* akan terlihat.

Hasil Pengujian DoS (*Denial of Service*)

Pengujian dilakukan dengan menggunakan *Low Orbit Ion Cannon* (LOIC) terhadap empat *port* utama pada masing-masing *router*. Efektivitas pengamanan diukur melalui indikator beban CPU. Hasilnya disajikan dalam Tabel 5.

Tabel 5. Perbandingan Beban CPU Sebelum dan Sesudah Penerapan Keamanan.

No.	Tujuan	*Port*	*Method*	Status Penerapan Keamanan	
				Sebelum	Sesudah
1	*Router* 1	21 (FTP)	TCP	CPU *Load* 100%	CPU *Load* 2%
		22 (SSH)	TCP	CPU *Load* 100%	CPU *Load* 8%
		23 (Telnet)	TCP	CPU *Load* 100%	CPU *Load* 5%
		80 (HTTP)	TCP	CPU *Load* 100%	CPU *Load* 4%
2	*Router* 2	21 (FTP)	TCP	CPU *Load* 100%	CPU *Load* 2%
		22 (SSH)	TCP	CPU *Load* 100%	CPU *Load* 3%
		23 (Telnet)	TCP	CPU *Load* 100%	CPU *Load* 5%
		80 (HTTP)	TCP	CPU *Load* 100%	CPU *Load* 6%
3	*Router* 3	21 (FTP)	TCP	CPU *Load* 100%	CPU *Load* 5%
		22 (SSH)	TCP	CPU *Load* 100%	CPU *Load* 4%
		23 (Telnet)	TCP	CPU *Load* 100%	CPU *Load* 2%
		80 (HTTP)	TCP	CPU *Load* 100%	CPU *Load* 2%

Berdasarkan Tabel 5, hasil pengujian menggunakan LOIC sebagai alat serangan menunjukkan bahwa penerapan langkah-langkah keamanan pada *Router* 1, *Router* 2, dan *Router* 3 sangat efektif dalam menangkal serangan *Denial of Service* (DoS) pada berbagai *port* menggunakan protokol TCP. Sebelum konfigurasi keamanan diterapkan, beban CPU pada ketiga *router* mencapai 100% untuk setiap *port* yang diserang. Namun, setelah langkah-langkah keamanan diterapkan, terjadi penurunan signifikan. Pada *Router* 1 (AP Master), beban CPU pada *port* 21 (FTP) turun dari 100% menjadi 2%, *port* 22 (SSH) menjadi 8%, *port* 23 (Telnet) menjadi 5%, dan *port* 80 (HTTP) menjadi 4%. Pada *Router* 2 (*Repeater* 1), beban CPU pada *port* 21 turun menjadi 2%, *port* 22 menjadi 3%, *port* 23 menjadi 5%, dan *port* 80 menjadi 6%. Sementara itu, pada *Router* 3 (*Repeater* 2), beban CPU pada *port* 21 turun menjadi 5%, *port* 22 menjadi 4%, *port* 23 menjadi 2%, dan *port* 80 menjadi 2%. Penurunan ini membuktikan bahwa konfigurasi *firewall* yang diterapkan mampu mereduksi beban sistem secara drastis dan melindungi jaringan dari serangan DoS yang berpotensi merusak.

Data menunjukkan bahwa sebelum penerapan *firewall*, seluruh *port* yang diserang mengalami penggunaan CPU maksimal sebesar 100%, yang mengindikasikan bahwa serangan DoS berhasil membebani sistem hingga berpotensi menyebabkan *downtime*. Namun, setelah penerapan aturan *firewall*, terjadi penurunan signifikan pada beban CPU di semua *router*, dengan rata-rata penurunan mencapai 90–98%. Temuan ini menunjukkan bahwa mekanisme *filter*, *drop*, dan *address list* yang diterapkan berhasil menyaring serta memblokir paket mencurigakan sebelum mencapai sistem inti (*pre-routing*), sejalan dengan prinsip *connection tracking* dalam pendekatan NDLC dan implementasi *firewall raw* (Jaya *et al.*, 2020).

Panthera : Jurnal Ilmiah Pendidikan Sains dan Terapan
E-ISSN 2808-246X; P-ISSN 2808-3636
Volume 5, Issue 3, July 2025; Page, 570-592
Email: pantherajurnal@gmail.com

SIMPULAN

Penelitian ini menyimpulkan bahwa penerapan fitur *firewall* pada perangkat *router* Mikrotik secara signifikan meningkatkan keamanan jaringan terhadap serangan *Denial of Service* (DoS) dan aktivitas pemindaian *port* (*port scanning*). Berdasarkan hasil pengujian menggunakan NMAP dan *Low Orbit Ion Cannon* (LOIC), konfigurasi *firewall* yang diterapkan pada *Router* 1, *Router* 2, dan *Router* 3 terbukti efektif dalam menutup sejumlah *port* yang rentan, seperti FTP, SSH, Telnet, dan HTTP, sementara *port* DNS dan *Winbox* tetap dibuka untuk keperluan operasional.

Efektivitas perlindungan jaringan juga tercermin dari penurunan drastis beban CPU setelah penerapan *firewall*. Sebelum konfigurasi keamanan diterapkan, serangan DoS menyebabkan beban CPU mencapai 100% pada ketiga *router*. Namun, setelah konfigurasi *firewall* diberlakukan, beban CPU menurun secara signifikan, yaitu menjadi 4% pada *Router* 1 dan *Router* 2, serta 3% pada *Router* 3. Temuan ini menunjukkan bahwa konfigurasi *firewall* yang tepat, mampu menghentikan paket serangan secara efektif dan menurunkan lalu lintas jaringan yang mencurigakan.

SARAN

Berdasarkan hasil penelitian ini, disarankan agar implementasi *firewall* dilakukan secara menyeluruh pada seluruh perangkat jaringan yang memiliki potensi kerentanan terhadap serangan siber, khususnya pada *port-port* yang umum menjadi sasaran dalam serangan *Denial of Service* (DoS) dan *port scanning*. Pemantauan jaringan secara berkala perlu diterapkan untuk memastikan bahwa konfigurasi *firewall* tetap efektif dan adaptif terhadap pola serangan baru yang mungkin muncul. Selain itu, penggunaan fitur tambahan seperti *port knocking*, sistem deteksi, dan pencegahan intrusi (*IDS/IPS*), serta pembaruan *firmware* Mikrotik secara rutin perlu dipertimbangkan sebagai lapisan keamanan tambahan, guna meningkatkan ketahanan jaringan.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada semua pihak yang telah berkontribusi dalam penyusunan studi literatur ini, khususnya kepada para peneliti, akademisi, dan praktisi yang telah menghasilkan berbagai artikel ilmiah, buku, serta laporan penelitian yang relevan terkait serangan *Denial of Service* (DoS), fitur-fitur *firewall* pada perangkat Mikrotik, dan metode pertahanan jaringan. Karya-karya tersebut menjadi sumber informasi yang sangat berharga dalam memperkaya pemahaman, serta memperkuat landasan teoretis dalam penelitian ini.

DAFTAR RUJUKAN

BSSN. (2020). Retrieved June 17, 2025, from BSSN. Interactwebsite: https://www.bssn.go.id/rekap-serangan-siber-januari-april-2020/

Jaya, B., Yuhandri, Y., & Sumijan, S. (2020). Peningkatan Keamanan *Router* Mikrotik terhadap Serangan *Denial of Service* (DoS). *Jurnal Sistem Informasi dan Teknologi, 2*(4), 115-123. https://doi.org/10.37034/jsisfotek.v2i4.32

Marta, I. K. K. A., Hartawan, I. N. B., & Satwika, I. K. S. (2020). Analisis Sistem Monitoring Keamanan *Server* dengan SMS *Alert* Berbasis *Snort*. *Insert : Information System and Emerging Technology Journal, 1*(1), 25-40. https://doi.org/10.23887/insert.v1i1.25874

Nurilahi, D. K., Munial, R., Syahrial, S., & Bahri, A. (2022). Penerapan Metode *Naïve Bayes* pada *Honeypot Dionaea* dalam Mendeteksi Serangan *Port Scanning*. *Elkomika : Jurnal Teknik Energi Elektrik, Teknik Telekomunikasi, & Teknik Elektronika, 10*(2), 309-321. https://doi.org/10.26760/elkomika.v10i2.309

Putra, F. P. E., Hamzah, A., Agel, W., & Kusuma, R. O. F. (2023). Implementasi Sistem Keamanan Jaringan Mikrotik Menggunakan *Firewall Filtering* dan *Port Knocking*. *Jurnal Sistim Informasi dan Teknologi, 5*(4), 82-87. https://doi.org/10.60083/jsisfotek.v5i4.329

Romadhan, I. A., Syaifudin, S., & Akbi, D. R. (2020). Implementasi *Multiple Honeypot* pada *Raspberry Pi* dan Visualisasi *Log Honeypot* Menggunakan ELK *Stack*. *Jurnal Repositor, 2*(4), 475-484. https://doi.org/10.22219/repositor.v2i4.30525

Syaftahan, P. (2024). Retrieved June 17, 2025, from CyberHub. Interactwebsite: https://cyberhub.id/berita/gcore-ungkap-lonjakan-serangan-ddos

Syahputra, A., Nurcahyo, Y., & Arlis, S. (2024). Penerapan Metode *Live* Forensik untuk Analisis Serangan DoS pada *Router* Mikrotik. *Variable Research Journal, 1*(2), 721-731. https://doi.org/10.35134/komtekinfo.v11i4.555

Tambunan, M. R. H., & Neyman, S. N. (2024). Implementasi *Firewall* pada *Linux* untuk Pencegahan dari Serangan DoS. *Journal of Technology and System Information, 1*(4), 10-17. https://doi.org/10.47134/jtsi.v1i4.2648

Wicaksono, D., & Widiasari, I. R. (2022). Sistem Keamanan Jaringan Menggunakan *Firewall* dengan Metode *Port Blocking* dan *Firewall Filtering*. *Jurnal Ilmiah Sistem Informasi, 9*(2), 1380-1392.

Zukhruf, A., Fatkhurrozi, B., & Kurniawan, A. A. (2023). Comparative Study of Distributed Denial of Service (DDoS) Attack Detection in Computer Networks. *Jurnal Teknik Informatika (JUTIF), 4*(5), 1033-1039. https://doi.org/10.52436/1.jutif.2023.4.5.756