Paper

Analisis Pemanfaatan Teknik Serangan DDOS pada Mikrotik Cloud dan Melakukan upaya penangannya

Author : Syahendra Surya, Tengku Mohd Diansyah, Risko Liza

SNASTIKOM 10
Seminar Nasional Teknologi Informasi dan Komunikasi
UNIVERSITAS HARAPAN MEDAN 2012-2023
Program Studi Teknik Informatika
TEMA : DUNIA AKADEMIK DI ERA SOCIETY 5.0 : TANTANGAN DAN PELUANG
ISSN : 2964-1950

ISSN: 2964-1950

Analisis Pemanfaatan Teknik Serangan DDOS pada Mikrotik Cloud dan Melakukan upaya penangannya

Syahendra Surya[1*], Tengku Mohd Diansyah[2], Risko Liza[3]
[1*]Program Studi Teknik Infromatika, Fakultas Teknik dan Komputer, Universitas Harapan Medan, Medan, Indonesia
[1*]suryasyahendra@gmail.com, [2]dian.10.22@gmail.com, [3]risko.liza@gmail.com
[*)] suryasyahendra@gmail.com

Abstrak

Layanan internet memiliki manfaat yang banyak dan digunakan secara luas, namun juga memiliki kekurangan yang dapat dimanfaatkan oleh *hacker* untuk melakukan serangan seperti DDoS. Salah satu solusi untuk mengelola dan mengontrol jaringan internet adalah dengan menggunakan MikroTik CHR (*Cloud Hosted Router*), yaitu solusi router virtual yang disediakan oleh MikroTik. CHR dirancang untuk dapat dijalankan pada berbagai platform virtualisasi seperti VMware, VirtualBox, Hyper-V, dan Cloud seperti Amazon Web Services, Google Cloud Platform, dan Microsoft Azure.Penelitian ini bertujuan untuk menganalisis Teknik serangan DDoS digunakan dan di terapkan pada platform Mikrotik CHR dan strategi upaya pengamananya yang dapat digunakan untuk melindungi MikroTik CHR dari serangan DDoS yang dapat menyebabkan gangguan layanan dan kerugian finansial dan penangananya. Penelitian ini hanya berfokus pada serangan DDoS pada MikroTik CHR dan strataegi keamanan yang dapat melindunginya dari serangan. Hasil penelitian menunjukkan bahwa beberapa strategi keamanan yang efektif termasuk mengkonfigurasi *firewall*, mengaktifkan fitur *protection*, serta melakukan pemantauan dan pembaruan perangkat lunak secara teratur. Kesimpulannya, MikroTik CHR dapat dilindungi dari serangan DDoS dengan strategi keamanan yang tepat, dan perlu memperhatikan pemantauan keamanan yang ketat, pembaruan perangkat lunak, dan strategi keamanan yang terintegrasi dan komprehensif untuk melindungi MikroTik CHR dari serangan DDoS.

Kata Kunci: Mikrotik, DDoS, CHR, Firewall

Abstract

Internet services have many benefits and are widely used, but also have disadvantages that can be utilized by hackers to carry out attacks such as DDoS. One solution to manage and control internet networks is to use MikroTik CHR (Cloud Hosted Router), a virtual router solution provided by MikroTik. CHR is designed to run on various virtualization platforms such as VMware, VirtualBox, Hyper-V, and Clouds such as Amazon Web Services, Google Cloud Platform, and Microsoft Azure.This research aims to analyze DDoS attack techniques used and implemented on the MikroTik CHR platform and the security effort strategies that can be used to protect MikroTik CHR from DDoS attacks that can cause service disruptions and financial losses and their handling. This research only focuses on DDoS attacks on MikroTik CHR and security strategies that can protect it from attacks. The results show that some effective security strategies include configuring firewalls, enabling protection features, and performing regular monitoring and software updates. In conclusion, the MikroTik CHR can be protected from DDoS attacks with proper security strategies, and it is necessary to pay attention to strict security monitoring, software updates, and an integrated and comprehensive security strategy to protect the MikroTik CHR from DDoS attacks.

Keywords: Mikrotik, DDoS, CHR, Firewall

ISSN: 2964-1950

1. PENDAHULUAN

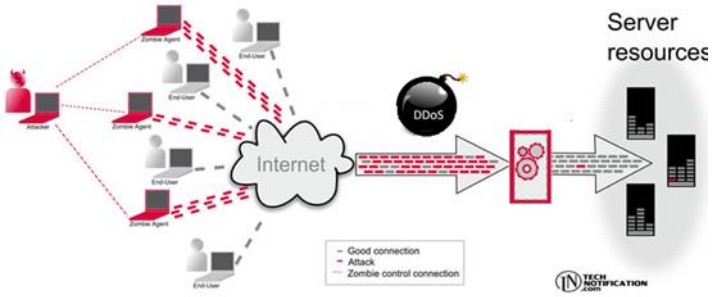
Penelitian ini secara khusus menganalisis pemanfaatan teknik serangan DDoS pada MikroTik CHR. dan upaya penanganannya masih terbatas[1]. Oleh karena itu, penelitian ini bertujuan untuk mengisi kekurangan tersebut dan memberikan wawasan yang lebih mendalam tentang pemanfaatan teknik serangan DDoS pada platform MikroTik CHR serta upaya yang dapat dilakukan untuk mengatasi serangan tersebut. Penelitian ini meliputi dua aspek utama. Pertama, analisis pemanfaatan teknik serangan DDoS pada MikroTik CHR. Dalam analisis ini, penelitian akan melibatkan penjelasan tentang berbagai teknik serangan DDoS yang umum digunakan[2], seperti serangan dengan membanjiri lalu lintas jaringan atau memanfaatkan celah keamanan pada MikroTik CHR[3].Tentang teknik-teknik ini akan memberikan tentang cara serangan dilakukan dan bagaimana MikroTik CHR dapat menjadi target[4].Serangan DDoS adalah jenis serangan yang paling sering terjadi pada jaringan saat ini. Serangan DDoS dapat menyebabkan banyak kerugian bagi perusahaan, termasuk kerusakan pada perangkat keras dan perangkat lunak, *down time* yang memengaruhi pengalaman pengguna, hilangnya data, dan kehilangan kepercayaan pelanggan [5].

Peneliti ini akan menerapkan Teknik dalam upaya penanganan yang dapat dilakukan untuk melindungi MikroTik CHR dari serangan DDoS[6]. Upaya ini mungkin termasuk penggunaan perangkat lunak pengamanan yang tepat, konfigurasi pengaturan lalu lintas yang cermat, serta metode deteksi dan mitigasi serangan yang efektif. Melalui analisis ini, diharapkan dapat diidentifikasi strategi dan taktik yang tepat untuk mengatasi serangan DDoS pada MikroTik CHR[7]. Dengan memahami pemanfaatan teknik serangan DDoS pada MikroTik CHR dan upaya penanganannya, organisasi dan profesional keamanan jaringan dapat meningkatkan ketahanan dan keamanan MikroTik CHR mereka. Penelitian ini diharapkan dapat memberikan sumbangan penting bagi pengembangan strategi keamanan yang efektif dalam melindungi MikroTik CHR dari serangan DDoS dan mempertahankan ketersediaan serta integritas jaringan.

2. METODE PENELITIAN

2.1 DDoS (Distributed Denial of Service)

Serangan DDoS adalah serangan mengganggu atau menghentikan aktivitas yang terkait dengan internet dengan cara membebani sumber daya target[8]. Ini dapat dilakukan dengan cara membuat perangkat keras mengalami *crash*, *reboot*, atau hang, atau dengan menggunakan sebagian besar *bandwidth* yang diperlukan oleh target untuk berkomunikasi dengan klien lain[9]. Serangan DDoS adalah upaya untuk menonaktifkan atau meganggu target dengan membanjiri jalur data dengan paket yang melanggar hukum, secara bersamaan. [10]. ICMP Flood adalah salah satu jenis serangan DDoS yang menggunakan protokol ICMP (*Internet Control Message Protocol*). Dalam serangan ini, penyerang akan mengirimkan banyak paket ICMP ke alamat IP target dengan intensitas tinggi dan berulang-ulang. Hal ini bisa menghabiskan sumber daya jaringan dan membuat jaringan menjadi tidak responsif atau bahkan *crash*. [5]. Skema serangan DDoS secara umum dapat dilihat pada gambar dibawah ini.[11]



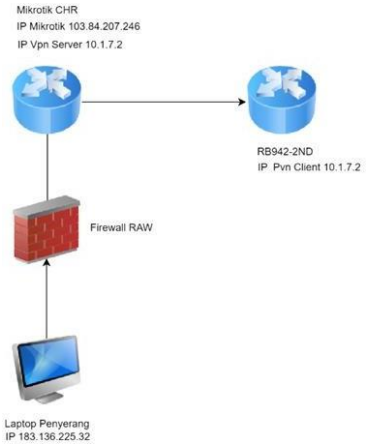
Gambar 1. DDoS Attack

Serangan *Distributed Denial of Service* (DDos) mengacu pada upaya untuk membuat layanan *online* mengalami kelebihan lalu lintas akibat *request* dari berbagai sumber. Serangan DDoS biasanya menargetkan situs-situs berita, bank, dan masih banyak lagi.[11]

2.2 Perancangan Skema Jaringan

ISSN: 2964-1950

Rancangan skema jaringan yang telah penulis kaji dalam penelitian atau riset ini, dengan menggunakan 1 unit Laptop sebagai penyerang yang menggunakan *software* LOIC dengan IP 183.136.255.32, 1 alamat IP target Mikrotik CHR yang berfungsi sebagai target serangan dan juga berfungsi sebagai server VPN duntuk *remote* dengan ip 10.1.7.2, serta 1unit RB941 yang terhubung sebagai *client* dengan ip 10.1.7.2. Berikut ini merupakan rancangan topologi yang akan digunakan dalam penelitian ini.

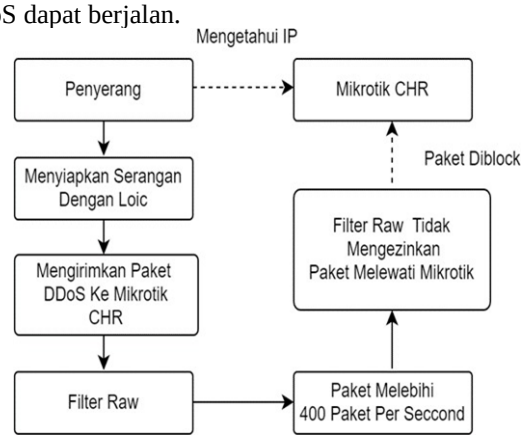


Gambar 2. Perancangan Skema Jaringan

Pada gambar 2 merupakan topologi jaringan atau scenario arsitektur jaringan yang akan penulis implementasikan pada uji coba penelitian ini. Bagian ini memberikan informasi lanjut bagaimana topologi di uji dengan 1 skenario. 1 laptop dengan *software* LOIC dikonfigurasi sebagai penyerang yang bertugas sebagai penyerang *public* terletak pada jaringan *public* dengan IP 183.136.255.32 serta target serangan menggunakan IP 103.84.207.246 pada port 80. Dan akan melakukan pemantauan lalulintas jaringan Ketika keadaan normal, dalam serangan dan Ketika penangan serangan dengan menggunakan *software* wireshark, lalu akan di hitung parameter *throughput* dan *delay* untuk *Quality of Service.*

2.3 Perancangan Skema Penyerangan

Perancangan serangan membutuhkan *tools* yang mendukung dalam melancarkan serangan agar dapat mengoptimalkan serangan DDoS dapat berjalan.



Gambar 3. Skema Penyerangan

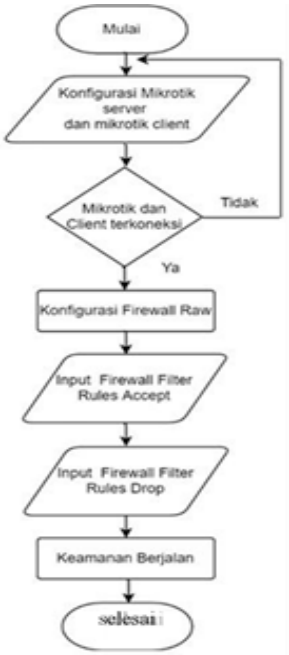
Pada Gambar 3 terlihat sebuah skema rancangan yang akan digunakan dalam pelaksanaan serangan. Skema ini menjadi dapat berjalan ketika seorang penyerang memperoleh informasi mengenai alamat IP dari perangkat MikroTik CHR yang menjadi sasaran, atau ketika mereka berhasil melakukan koneksi ke perangkat tersebut. Ketika fase ini tercapai, terutama setelah terjalinnya koneksi dengan jaringan yang sama atau dengan memperoleh alamat IP target, pelaksanaan berbagai teknik serangan DDoS dapat dilaksanakan. Dalam penelitian ini, penulis menggunakan perangkat MikroTik CHR yang diinstal pada sebuah VPS. Perangkat MikroTik CHR berperan sebagai target serangan yang ditujukan. Sementara itu, untuk menginisiasi serangan tersebut, penelitian ini

ISSN: 2964-1950

melibatkan penggunaan perangkat lunak LOIC (*Low Orbit Ion Cannon*), yang telah diinstal pada sebuah laptop. Dengan menyatukan perangkat ini, penelitian ini memiliki tujuan untuk melibatkan serangan yang mengincar MikroTik CHR yang menjadi subjek eksperimen.

2.4 Perancangan Skema Penanganan

Pada tahap ini, dilakukan perancangan sistem sebagai solusi untuk mengatasi permasalahan yang ada. Langkah pertama adalah menentukan topologi secara rinci. Selanjutnya, dilakukan instalasi Mikrotik CHR pada *virtual server* (pvs). Setelah itu, *filter raw* Mikrotik diaktifkan dan di konfigurasi untuk memantau setiap paket yang melewati perangkat, dan paket yang tidak memenuhi kriteria akan dihapus (*drop*). Kemudian, dilakukan serangan DDoS ke Mikrotik CHR, namun serangan tersebut akan dipantau dan dihadapi dengan *filter raw* yang telah diatur sesuai kriteria sebelumnya. Untuk memperoleh data yang akurat, dilakukan pemantauan Mikrotik CHR dan jaringan menggunakan *software Wireshark* sebelum dan setelah terjadinya serangan DDoS. Hasil dari pemantauan tersebut berupa informasi tentang penggunaan beban CPU, penggunaan memori, dan performa *Quality of Service* (QoS).

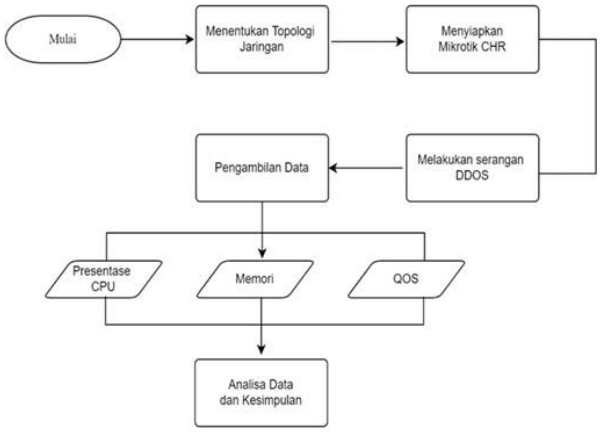


Gambar 4. Skema Penanganan

2.5 Perancangan Skema Pengambilan Data

Penelitian ini menggunakan metode pengumpulan data, yaitu uji coba dengan mengirimkan paket serangan untuk mencatat parameter CPU, *Memory*, *throughput*, dan *delay* untuk QoS, serta menganalisis data menggunakan perangkat lunak analisis jaringan Wireshark. serta studi kepustakaan untuk mengumpulkan informasi dari jurnal, dan internet yang relevan dengan penelitian sebelumnya dan parameter yang akan diteliti, pengamatan dilakukan dengan mengukur kinerja mikrotik yang mengalami serangan DDoS.

ISSN: 2964-1950



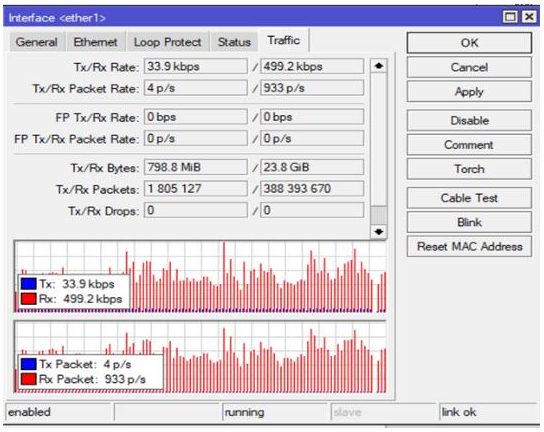
Gambar 5. Skema Pengambilan Data

3. HASIL DAN PEMBAHASAN

Pengujian pada jaringan dilakukan dengan beberapa tahap yakni tahap pertama pada kondisi normal,kondisi saat pada penyerangan dan kondisi setelah penanganan.

3.1 Serangan DDoS pada mikrotik CHR

Proses awal untuk analisis apakah mikrotik *cloud* masih dalam keadaan normal atau belum ada serangan DDoS, dapat dilakukan pemantauan menggunakan menu yang tersedia pada WinBox, yaitu seperti menu *Traffic*, *Torch*, dan *Resources*. menu *Traffic* adalah alat untuk memonitor berbagai parameter Router dari waktu ke waktu dan menempatkan data yang dikumpulkan kedalam bentuk grafik. Hal ini dapat dilihat pada grafik yang dikategorikan menjadi Tx (*Transmitted Rate*) dan Rx (*Received Rate*). *Transmitted Rate* ini diartikan sebagai jumlah data yang keluar dari Router melalui *interface*. Sedangkan *Received Rate* adalah data yang diterima masuk ke Router melalui interface. *Menu Torch* merupakan *tools Realtime Traffic Monitor* yang digunakan untuk pemantauan lalu lintas yang akan melalui sebuah *interface*. Pada penelitian ini, perhitungan QoS dilakukan pada jaringan *client* yang dimana Mikrotik RB941 sebagai client dan mikrotik CHR sebagai VPN server untuk *remote*. *Analisa Quality of service* dilakukan dengan menghitung nilai parameter Througput dan delay pada protokol tcp dengan menggunakan *wireshark*, aflikasi *wireshark* akan meng-capture paket data protokol tcp dalam 3 keadaan, pertama saat belum terjdi serangan, kedua saat terjadi serangan dan ketiga saat telah dilakukan penanganan. Analisa penulis membagi dalam 3 keadaan apakah ada perbedaan yang terjadi pada hasil perhitungan QoS.

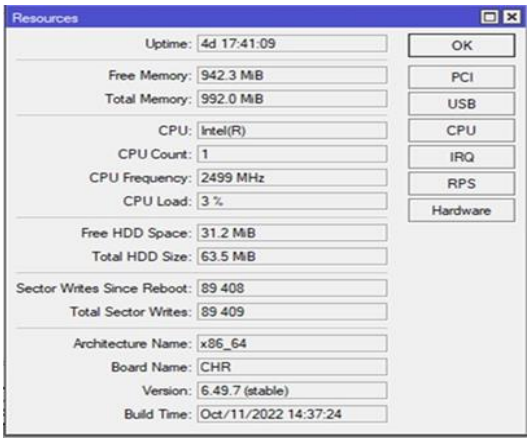


Gambar 6. Tampila Trafic Sebelum Terjadi Serangan

Dari gambar 6, dapat dilihat pada menu Trafic bahwa kodisi grafik data yang masuk ke Mikrotik dalam keadaan normal dan belum ada serangan yang masuk dan mengganggu lalu lintas jaringan pada Mikrotik. Seperti terlihat

ISSN: 2964-1950

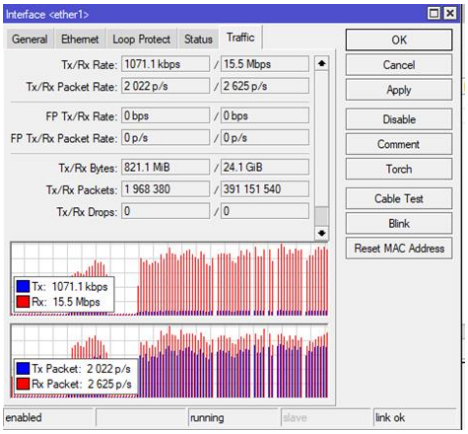
pada grafik yang tampak normal dimana nilai Tx/Rx Rate yaitu 33.9 kbps 499.2 kbps dan nilai Tx/Rx Packet yaitu 4 p/s / 933 p/s. Ini menunjukkan adanya komunikasi antara *client* dengan Router yang berjalan normal. Sedangkan pada menu *Torch* yang digunakan untuk memantau arus lalu lintas terlihat normal. Dan pada menu *resource* terlihat persentase *Cpu Load* adalah 3 % dan *Free Memory* 942.3.



Gambar 7. Tampila *Resources* Sebelum Terjadi Serangan

4.1 Serangan DDoS menggunakan Low Orbit Ion Cannon

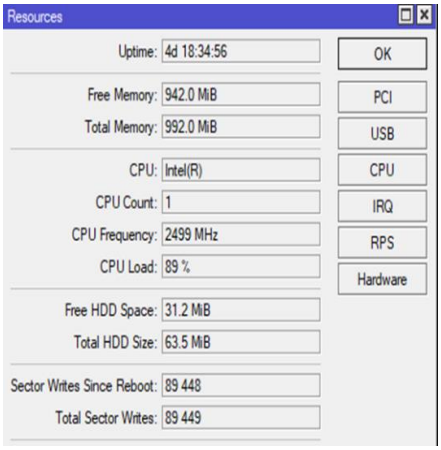
Proses pengujian dilakukan menggunakan *Low Orbit Ion Cannon* pada sistem operasi Windows. Pada proses ini *Low Orbit Ion Cannon* akan melancarkan serangan langsung ke target jaringan Router yang diserang. Adapun langkah-langkah yang dilakukan untuk melakukan serangan adalah sebagai berikut. Setelah melakukan penyerangan selanjutnya adalah melihat keadaan trafic seperti pada gambar 4.7, terlihat bahwa Trafic yang terlihat tidak normal dimana nilai Tx/Rx Rate yaitu 1071.1 kbps/15.5 Mbps dan nilai Tx/Rx Packet yaitu 2 022 p/s / 2 625 p/s. Hal ini dapat diartikan bahwa perangkat Mikortik CHR dari segi *interfaces* maksimal hanya mampu melewatkan data yang di *request* oleh *user* sebesar 1000 Mbps pada *interface* Mikrotik tersebut. Sedangkan dampak serangan DDoS ini menyebabkan *interface* sudah melewatkan data sebesar 821.1 Mbps. Ini menandakan bahwa traff
ic sudah tidak bisa lagi melewatkan permintaan akses *user* terhadap *server* yang melalui router tersebut.



Gambar 8. Tampilan Traffic saat dilakukan penyerangan

Ketika terjadi serangan DDoS yang masuk pada jaringan perangkat, *Load* CPU dan *memory* meningkat. meningkat. Berdasarkan hasil *Traffic Monitor System* setelah terjadi serangan DDoS diketahui *Traffic System Monitor Packet* data *CPU Load* meningkat menjadi 89% dan *Memory* 942.0 MiB. Hal ini yang menyebabkan *down* pada *Network Traffic* akibat serangan DDoS pada router. Dapat dilihat pada gambar berikut.

ISSN: 2964-1950

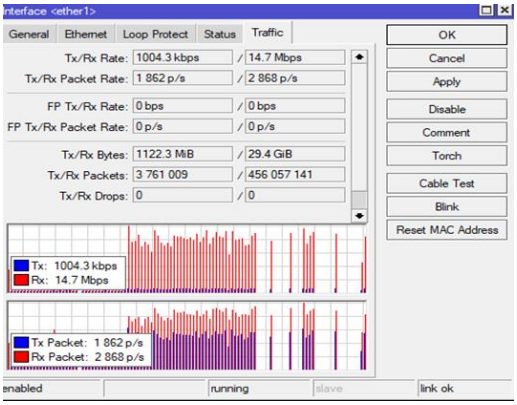


Gambar 9. Tampilan Menu Resources Saat Penyerangan

5.1 Proses Penanganan

Dari permasalahan diatas penulis mengambil tindakan untuk melakukan peningkatan keamanan terhadap Router yaitu dengan menggunakan fitur *Firewall Raw* pada Router MikroTik. RAW merupakan tabel *firewall* yang mirip dengan tabel filter yakni menangani filtering paket. Namun Raw memiliki keunggulan yaitu tidak memakan *resource* cpu sebanyak pada *firewall* filter. *Firewall Raw* sangat efektif dalam melakukan pengamanan pada serangan yang terjadi pada Router MikroTik.

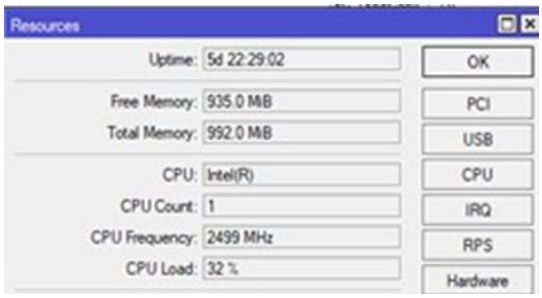
Selanjutnya pada gambar 10 dilakukan pengujian setelah menggunakan *Firewall Raw* pada gambar berikut dapat dilihat bahwa pada *menu Traffic* yang memang terlihat tidak normal dimana nilai Tx/Rx Rate yaitu 1004.3 kbps / 14.7 Mbps dan nilai Tx/Rx Packet yaitu 1862p/s / 2868p/s. Hal ini disebabkan karena serangan yang dilakukan tetap tercatat masuk kedalam grafik tetapi request yang dilakukan tidak diterima oleh Router karena protokol yang masuk yaitu protokol tcp yang sudah di-drop oleh *Firewall Raw* tersebut merupakan data yang ditolak untuk masuk ke jaringan Router.



Gambar 10. Tampilan *Traffic* Setelah Dilakukan Penanganan

Hal ini membuktikan bahwa Firewall Raw mampu memblok data-data yang dicurigai dikirim oleh penyerang pada perangkat. Sehingga perangkat tidak mengalami *down* seperti sebelum menggunakan *Firewall Raw*. Perubahan yang terjadi pada perangkat ketika menggunakan *Firewall Raw* dapat dilihat pada gambar berikut.

ISSN: 2964-1950



Gambar 11. Tampilan Resources Setelah Dilakukan Penanganan

Pada gambar 11, terlihat *CPU Load* dari 89% turun menjadi 32% setelah menggunakan *Firewall Raw.* Dapat disimpulkan bahwa *Firewall Raw* dapat mencegah serangan DDoS sehingga tidak terjadi *Router down.*

4. KESIMPULAN

Berdasarkan hasil pelaksanaan rancangan dan pengujian yang telah diterapkan pada Mikrotik CHR, simpulan yang dapat diambil adalah sebagai berikut:

1. Situasi rata-rata pemanfaatan CPU dan memori perangkat, ketika semuanya berjalan dengan normal, menunjukkan bahwa beban CPU hanya sekitar 3%, dan penggunaan memori mencapai 50 MiB. Namun, ketika perangkat menghadapi serangan, terjadi peningkatan besar pada penggunaan CPU hingga mencapai 89%, dengan penggunaan memori tetap menjadi 50 MiB. Setelah langkah-langkah penanganan diambil, pemanfaatan CPU berhasil dikurangi menjadi sekitar 32%, sementara penggunaan memori mengalami kenaikan menjadi 57 MiB.
2. Ditemukan bahwa dalam kondisi normal, *throughput* rata-rata adalah 198,62 kbps dengan *delay* 90,23 ms Saat terjadi serangan, *throughput* menjadi 134,71 kbps dengan *delay* 354,12 ms. Namun, dalam kondisi penanganan, *throughput* meningkat menjadi 238,14 dan delay berkurang menjadi 98,55. Ada situasi di mana server VPS secara otomatis memblokir akses IP saat serangan terjadi, terutama pada *port* 80. Serangan pada *port* 22 memerlukan tindakan seperti menutup *port* atau mengatur akses hanya untuk alamat IP tertentu karna tidak dapat di tangani Ketika serangan. Namun, serangan pada *port* 23 dapat diatasi dengan sukses.
3. Dampak serangan berpengaruh terhadap *speed download* maupun *upload*,ping juga mengalami menjadi tinggi yang bisa berakibat lambat nya pengiriman data,dan Ketika melakukan penganan dengan *firewall* maka *upload* dan *download* dapat pulih walau tidak seperti normal.
4. Dampak dari serangan DDoS adalah kenaikan beban kinerja CPU. Penggunaan *firewall* raw yang diaktifkan pada Mikrotik membuktikan efektivitasnya dalam membatasi paket serangan, mengurangi beban CPU Mikrotik, dan menjaga kinerja perangkat dalam kondisi normal.

DAFTAR PUSTAKA

[1] M. Aguk and N. Anggraini, "Uji Fitur Intrusion Prevention Pada Firewall Untangle Dengan Pengujian Dos Dan Ssh Brute Force," *J. Manaj. Inform.*, vol. 9, pp. 18–25, 2018.

[2] A. Saputra, "UNES Journal of Information System," *UNES J. Inf. Syst. Vol.*, vol. 3, no. 1, pp. 36–47, 2018.

[3] W. Syahputra, T. . Diansyah, and R. Liza, "Pemanfaatan Mikrotik Router Board Sebagai Pengaman Serangan DDOS Menggunakan Metode IDS," *Snastikom*, vol. 1, no. 1, pp. 492–499, 2020.

[4] E. S. R. O. B. Langobelen, Y. Rachmawati, and C. Iswahyudi, "Analisis Dan Optimasi Dari Simulasi Keamanan Jaringan Menggunakan Firewall Mikrotik Studi Kasus Di Taman Pintar Yogyakarta," *J. JARKOM*, vol. 7, no. 2, pp. 95–102, 2019.

[5] L. F. Nainggolan, N. F. Saragih, and F. G. N. Larosa, "Monitoring Keamanan Jaringan Pada Server Ubuntu Dari Serangan DDoS Menggunakan Snort IDS," *J. Ilm. Tek. Inform.* , vol. 2, no. 2, pp. 1–10, 2022, [Online]. Available: http://ojs.fikom-methodist.net/index.php/METHOTIKA

[6] R. Adrian and N. Isnianto, "Pada Performa Router," no. October, pp. 2–5, 2017.

[7] Y. H. Tung, H. C. Wei, Y. W. Ti, Y. T. Tsou, N. Saxena, and C. M. Yu, "Counteracting UDP flooding attacks in SDN," *Electron.*, vol. 9, no. 8, pp. 1–28, 2020, doi: 10.3390/electronics9081239.

[8] Y. Mulyanto, H. Herfandi, and R. Candra Kirana, "ANALISIS KEAMANAN WIRELESS LOCAL AREA NETWORK (WLAN) TERHADAP SERANGAN BRUTE FORCE DENGAN METODE PENETRATION TESTING (Studi kasus:RS H.LMANAMBAI ABDULKADIR)," *J. Inform. Teknol. dan Sains*, vol. 4, no. 1, pp. 26–35, 2022, doi: 10.51401/jinteks.v4i1.1528.

[9] S. Dwiyatno, A. P. Sari, A. Irawan, and S. Safig, "PENDETEKSI SERANGAN DDoS (DISTRIBUTED DENIAL OF SERVICE) MENGGUNAKAN HONEYPOT DI PT. TORINI JAYA ABADI," *J. Sist. Inf. dan Inform.*, vol. 2, no. 2, pp. 64–80, 2019, doi: 10.47080/simika.v2i2.606.

[10] B. Arifwidodo, Y. Syuhada, and S. Ikhwan, "Analisis Kinerja Mikrotik Terhadap Serangan Brute Force Dan DDoS," *Techno.Com*, vol. 20, no. 3, pp. 392–399, 2021, doi: 10.33633/tc.v20i3.4615.

[11] Fadhli, "Apa Itu Serangan DDoS? - MerahPutih." https://merahputih.com/post/read/apa-itu-serangan-ddos