Analisis Kinerja Mikrotik Terhadap Serangan Brute Force Dan DDoS

Analysis of Mikrotik Performance Against Brute Force and DDoS Attacks

Bongga Arifwidodo[1], Yusup Syuhada[2], Syariful Ikhwan[3]
[1,2,3] S1 Teknik Telekomunikasi, Institut Teknologi Telkom Purwokerto
E-mail: [1]bongga@ittelkom-pwt.ac.id

Abstrak

Serangan cyber yang semakin meningkat menjadikan persoalan bagi penyedia layanan jasa internet. Contoh jenis serangan cyber yang digunakan adalah dengan teknik serangan DDoS dan Brute Force. Perangkat jaringan seperti Mikrotik pun bisa menjadi target dari serangan. Upaya mencegah serangan diperlukan dengan suatu sistem keamanan. Penelitian ini menggunakan metode kuantitatif dengan menganalisis performasi dan kinerja dari Mikrotik apabila terjadi serangan. Hasil Pengujian, serangan DDos sebanyak 171847 serangan ke port 80 terpantau CPU Mikrotik sebesar 96,81% dan pada webserver sebesar 16,61%. Perangkat Mikrotik yang telah terkena serangan DDoS sudah tidak dapat lagi beroperasi secara normal. Namun saat skenario serangan *Brute Force*, terpantu normal 4,76% pada CPU Mikrotik karena *port forwarding* telah meneruskan paket serangan ke server Honeypot. Kesimpulan dari penelitian ini serangan *DDoS* dan *Brute Force* mengakibatkan peningkatan beban kinerja CPU baik pada Mikrotik maupun pada *server Honeypot.*

Kata kunci: *3-5 Honeypot, Brute Force, DDos, Server,* Mikrotik

Abstract

Increasing cyber attacks have become a problem for internet service providers. Examples of types of cyber attacks used are DDoS and Brute Force attack techniques. Network devices such as Mikrotik can also become targets of attacks. Efforts to prevent attacks are needed with a security system. This research uses quantitative methods by analyzing the performance and performance of Mikrotik in the event of an attack. Test results, DDos attacks as many as 171847 attacks on port 80 monitored by CPU Mikrotik by 96.81% and on the webserver by 16.61%. Mikrotik devices that have been hit by a DDoS attack can no longer operate normally. However, during the Brute Force attack scenario, normal 4.76% supports the Mikrotik CPU because port forwarding has forwarded the attack packet to the Honeypot server. The conclusion of this study DDoS and Brute Force attacks resulted in an increase in the CPU performance load both on Mikrotik and on the Honeypot server.

Keywords: 3-5 Honeypot, Brute Force, DDos, Server, Mikrotik

1. PENDAHULUAN

Jumlah ancaman dan serangan keamanan siber selalu meningkat setiap saat [1] dan seringkali standar keamanan seperti IDS (Intrusion Detection Systems), access control system dan firewall tidak cukup untuk mengamankan server dari penyerang [2]. Salah satu perangkat yang paling penting pada suatu jaringan dengan cakupan yang luas adalah router. Pesatnya kemajuan teknologi router membuktikan bahwa router adalah perangkat yang paling dibutuhkan khususnya pada penyedia jasa internet dalam membangun sebuah jaringan maupun keamanannya khususnya perangkat router Miktorik. Target utama attacker sebelum masuk pada sistem utama atau pusat data adalah dengan mematikan kinerja router [3]. Ancaman serangan siber seperti serangan Brute Force dan DDoS dapat dengan mudah menyerang server maupun

router. DDoS merupakan serangan yang bertujuan untuk mematikan target dengan cara memadati jalur data dengan paket yang illegal, secara serempak [4][5]. Brute force merupakan ancaman dari penyerang yang mencoba untuk login dengan menggunakan protocol SSH dan telnet untuk mengungkap password login [6]. Penyelesaian dalam menebak password menggunakan algoritma Brute Force dapat dengan mudah mencari password dengan mengkombinasikan karakter dan panjang password [7].

Pada penelitian [8] menjelaskan peningkatan keamanan pada router Mikrotik menggunakan Firewall Filter dan Firewall Raw terbukti efektif dalam mencegah terjadinya serangan DoS pada router mikrotik. Masalah akan muncul apabila kita terkoneksi ke internet melalui sebuah router. Hasil penelitian [9] menjelaskan bahwa perlu perubahan settingan pada router yaitu fungsi Port Forwarding pada Firewall yang harus diaktifkan karena pada umumnya fungsi Port Forwarding telah dimatikan secara default.

Pada penelitian [10] menyarankan sejumlah teknik optimasi keamanan jaringan yang akan berfungsi untuk meningkatkan kualitas pengalaman bagi pengguna internet, keamanan jaringan dan bagaimana menerapkan Firewall dan Intrusion Detection System. Sejalan dengan optimasi keamanan jaringan, hasil penelitian [11] untuk mengatasi serangan pada perangkat jaringan, diperlukan sebuah sistem layanan tiruan untuk menjebak penyerang yaitu menggunakan honeypot. Menggunakan honeypot sangatlah tepat untuk menangani serangan, karena kemampuannya dalam mendeteksi, mencegah hingga mempelajari bagaimana penyerang menembus ke dalam informasi sistem keamanan kemudian memberikan hasil serangan berupa data log[12][13][14].

Berdasarkan penelitian [15] dampak serangan DDoS dan DoS cukup membebani dan sangat menggangu kinerja sistem dan aktifitas pengguna. firewall atau router sebagai penghubung internet atau jaringan luar ke jaringan internal yang menuju sumber daya server harus melakukan filterisasi dan tindakan pencegahan agar serangan-serangan tersebut tidak berdampak besar pada sistem yang berjalan. Penelitian ini membuat sistem integrasi port forwarding pada router Mikrotik dan server Honeypot Cowrie, dimana Honeypot ini difungsingkan sebagai monitoring dan analisis saat terjadinya serangan ke server utama. Honeypot Cowrie dilengkapi dengan instalasi MySql dan Kippo Graph. Server utama dilengkapi oleh Apache2. Perangkat Mikrotik terpasang untuk menghubungkan kedua server. Selanjutnya, untuk pengambilan data dilakukan dengan cara memonitoring Mikrotik, webserver dan server honeypot saat terjadinya serangan.

2. METODE PENELITIAN

Penelitian ini metode penelitian yang ditempuh dimulai dengan melakukan analisa kebutuhan, alur dan topologi, dan uji skenario.

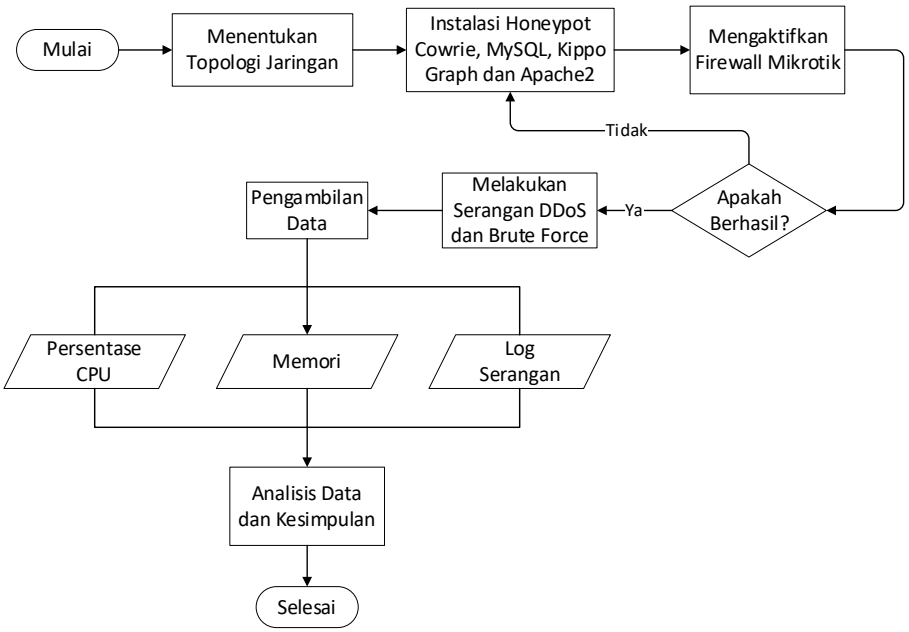
2.1 Analisa Kebutuhan

Pada tahapan ini, penulis melakukan identifikasi analisa terhadap kebutuhan sistem. Data yang dikumpulkan dalam tahap ini diperoleh dari penelitian, percobaan, konsultasi dengan pakar dan studi literatur. Berdasarkan studi literatur yang berhubungan dengan DDoS dapat dijelaskan bahwa Honeypot merupakan salah satu alternatif yang dapat diimplementasikan sebagai proteksi server dari serangan karena efisien dan ekonomis tanpa mengorbankan kualitas pengamanan yang ditawarkan pada jaringan yang memakainya. Tool yang digunakan untuk membantu implementasi honeypot pada penelitian ini menggunakan aplikasi *cowrie*. Selanjutnya hasil dari serangan tersebut masuk ke dalam log honeypot cowrie dan dapat dilihat pada kippo graph menggunakan browser.

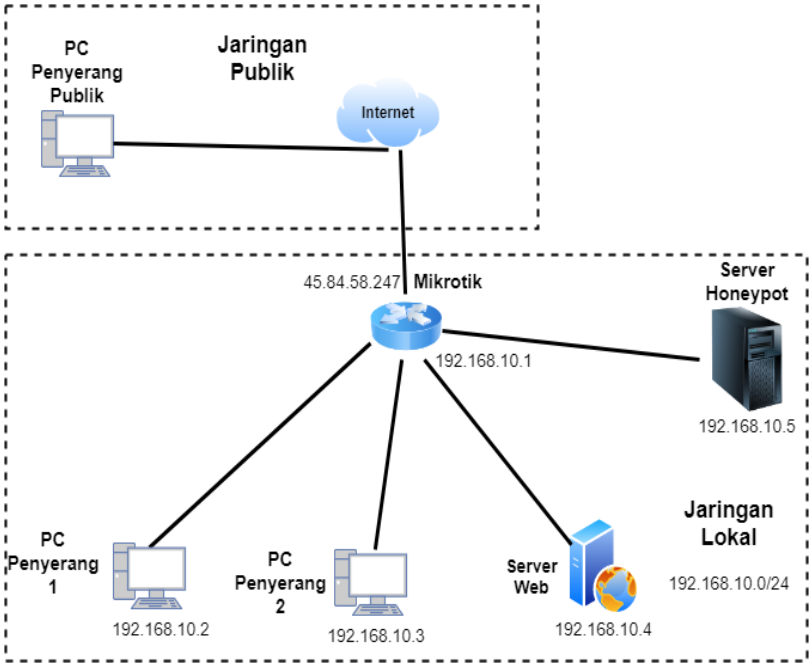
2.2 Alur dan Topologi

Tahapan ini merupakan perancangan sistem terhadap solusi dari permasalahan yang ada dengan menentukan topologi terlebih dahulu, selanjutnya melakukan instalasi honeypot cowrie, MySQL, kippo graph pada server honeypot dan menginstall apache2 pada webserver.

Selanjutnya mengaktifkan firewall Mikrotik yang berupa port forwarding dimana untuk mengalihkan serangan ke server tiruan yaitu webserver dan server honeypot cowrie. Kemudian melakukan serangan DDoS dan Brute Force ke Mikrotik yang nantinya serangan tersebut dialihkan ke server tiruan. pengambilan data dilakukan dengan cara memonitoring Mikrotik, webserver dan server honeypot saat terjadinya serangan. Hasil monitoring tersebut berupa penggunaan beban CPU dan memori.



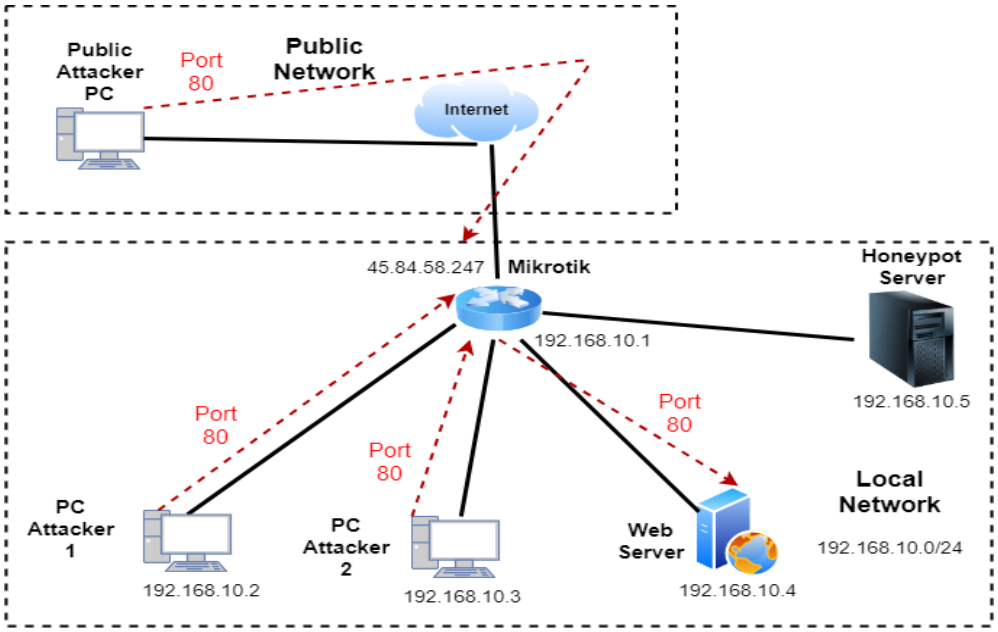
Gambar 1 Alur penelitian



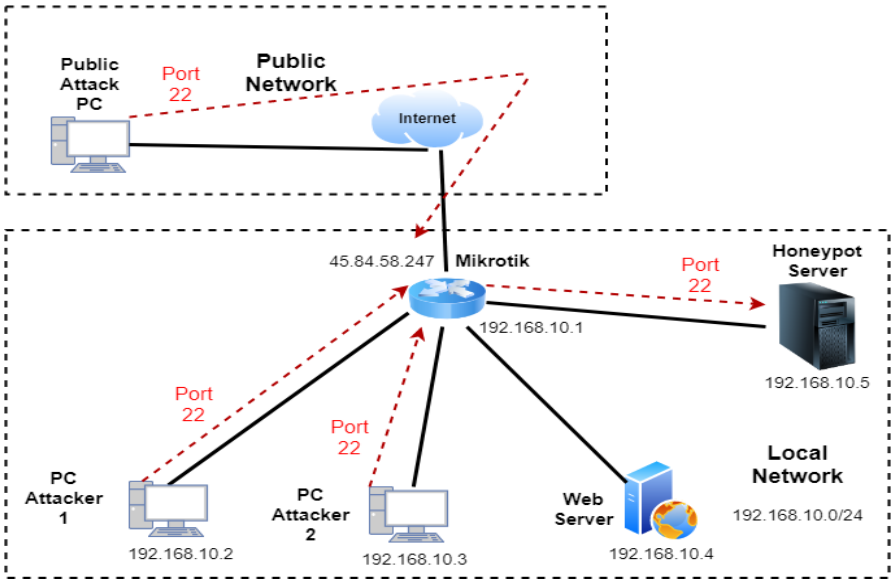
Gambar 1 Topologi penelitian

2.3 Uji skenario

Bagian ini memberikan informasi lanjut bagaimana topologi diuji dengan 2 pola uji skenario. Beberapa PC dikonfigursaikan sebagai penyerang yang bertugas sebagai penyerang, yaitu PC penyerang 1 dan PC penyerang 2 yang terletak pada jaringan lokal sedangkan PC penyerang publik terletak pada jaringan publik. Fungsi Miktorik sebagai gateway antar jaringan serta difungsikan sebagai target penyerang.



Gambar 2 Pola serangan pertama



Gambar 3 Pola serangan kedua

3. HASIL DAN PEMBAHASAN

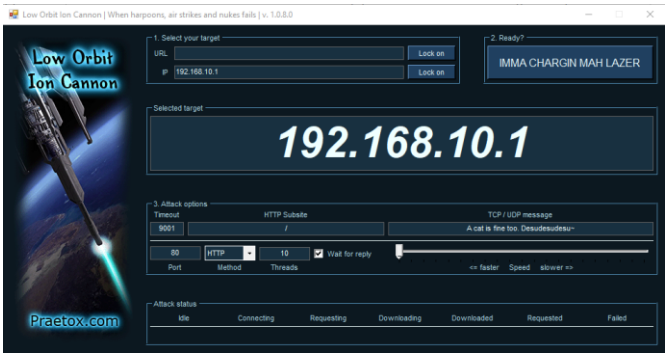
Berdasarkan rancangan pengujian sistem dan skenario yang telah diuraikan, menyebabkan kondisi perangkat mikrotik mengalami kenaikan resource tinggi saat terjadi serangan. Sehingga diperlukan port forwarding pada firewall NAT di Mikrotik. Penulis menggabungkan server tiruan dengan firewall NAT agar serangan yang terjadi tidak memberikan log serangan pada Mikrotik melainkan ke server tiruan dan juga meringankan kinerja dari Mikrotik saat terjadinya serangan.

3.1 Hasil Pengujian Skenario Pertama

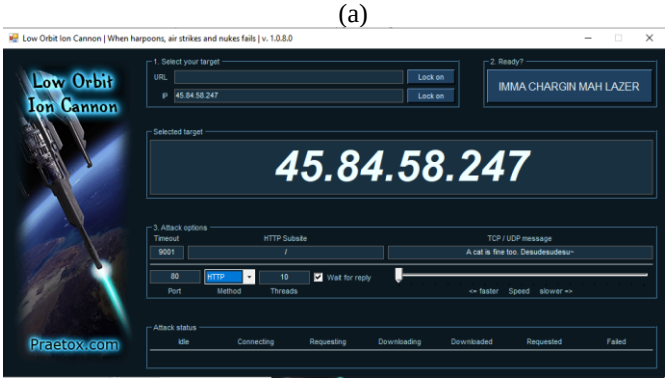
Penyerang menggunakan serangan DDoS dengan metode HTTP flood untuk menyerang mikrotik port 80. Proses penyerangan menggunakan aplikasi LOIC. Serangan HTTP flood merupakan jenis serangan dari DDoS (Distributed Denial of Service) yang dirancang untuk membanjiri target yaitu server dengan permintaan HTTP. Pada Tabel 1 penyerang menggunakan aplikasi LOIC untuk menyerang mikrotik dengan IP 192.168.10.1 dan 45.84.58.247 dengan port 80.

Tabel 1 Hasil uji serangan DDoS

Penyerang	**IP Target**	***Port***	**Aplikasi Penyerang**	**Waktu Penyerangan**
PC 1	192.168.10.1	80	LOIC	7 Menit
PC 2	192.168.10.1	80	LOIC	7 Menit
PC Publik	45.84.58.247	80	LOIC	7 Menit



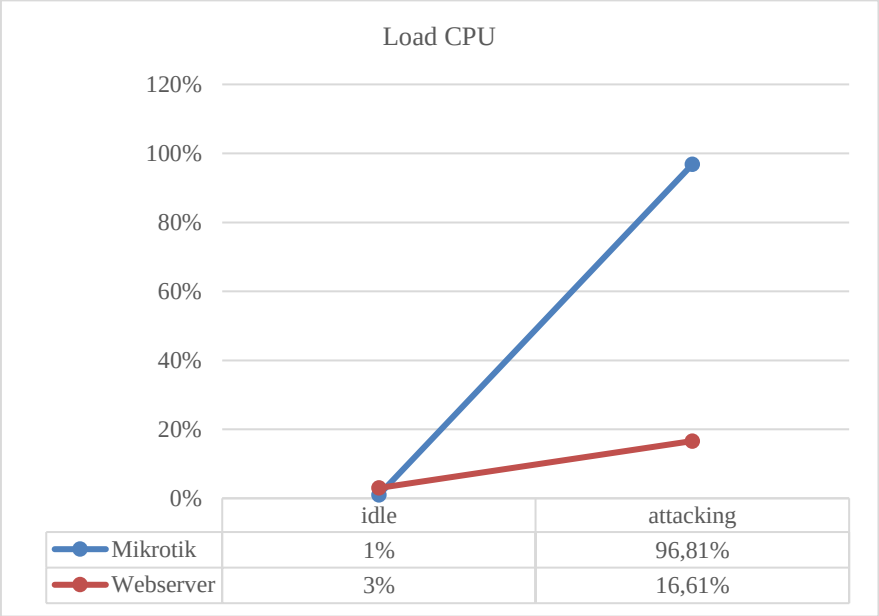
(a)



(b)

Gambar 4 Aplikasi LOIC
(a) Uji Penyerangan PC 1 dan PC 2
(b) Uji Penyerangan PC Publik

Total serangan yang tercatat pada webserver sebanyak 515542 serangan DDoS sehingga menyebabkan beban kerja CPU mengalami kenaikan. Terpantau beban kerja CPU saat kondisi attacking pada Gambar 5 sebesar 96,81% pada Mikrotik dan 16,61% pada webserver. CPU bekerja sangat keras karena menerima banyak permintaan dari client. Permintaan tersebut merupakan bentuk serangan DDoS yang dijalankan dari ketiga PC penyerang. Semakin banyaknya jumlah sernagan mengakibatkan beban CPU meningkat. Perangkat Miktorik yang telah terkena serangan ini sudah tidak dapat lagi beroperasi secara normal, akibatnya proses pengiriman data menjadi tidak maksimal. Faktor spesifikasi minimal Mikrotik Tipe: RB941-2nD-TC (hAP-Lite2) membuat kehandalannya kurang maksimal saat terjadi serangan.



Gambar 5 Beban CPU scenario I (%)

3.2 Hasil Pengujian Skenario Kedua

Pada skenario kedua, penyerang baik dari jaringan lokal dan publik menggunakan teknik serangan brute force untuk menyerang Mikrotik melalui port 22 menggunakan aplikasi Nmap untuk menemukan *username* dan *password* yang sesuai. Firewall pada Mikrotik RouterOS berupa port forwarding diaktifkan untuk mengalihkan serangan tersebut ke server honeypot. Proses penyerangan menggunakan aplikasi Nmap, dengan target mikrotik dengan teks perintah terminal:

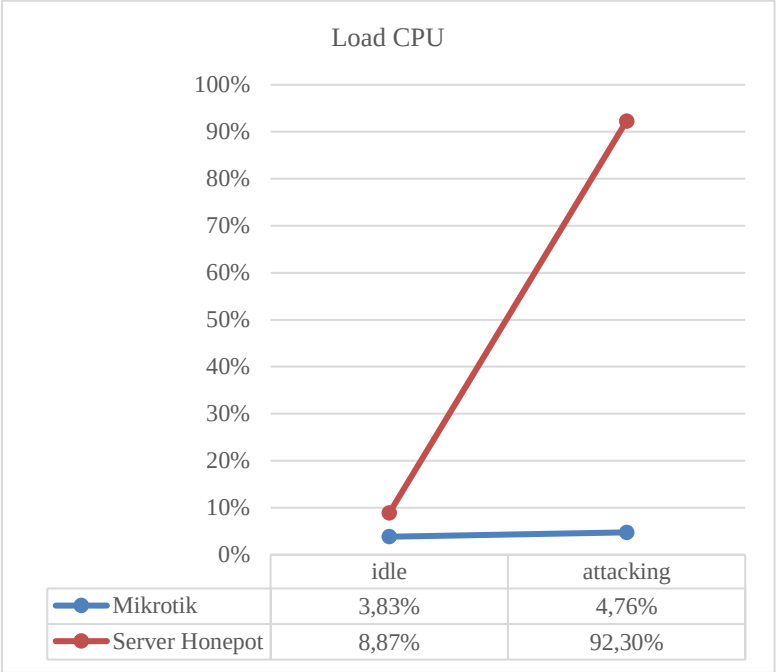
Nmap -sS -sU -T4 -v -n –script ssh-brute 192.168.10.1
Nmap -T4 -A -v -––script ssh-brute 45.84.58.247

Hasil log pada Tabel 2 menemukan serangan yang berhasil masuk dari PC 1, PC 2 dan PC publik dengan username “root” dengan password acak yang tercatat pada server Honeypot Cowrie.

Tabel 2 Hasil uji serangan Brute Force

Penyerang	**Berhasil**	***Username***	***Password***	**Berhasil *login***
PC 1	Ya	*root*	*root*	5
PC 2	Ya	*root*	12345	6
PC Publik	Ya	*root*	123	6

Total serangan yang tercatat pada server Honeypot sebanyak 7268 serangan Brute Force sehingga menyebabkan beban kerja CPU mengalami peningkatan. Kondisi CPU pada server honeypot mengalami peningkatan sebesar 92,30 % dan sebesar 4,76% untuk Mikrotik. Pada saat terjadi serangan, server Honeypot menerima serangan Brute Force yang merupakan paket *forwarding* dari perangkat mikrotik. Adanya fitur port forwarding menjadikan load CPU pada Mikrotik tidak mengalami peningkatan pada saat serangan.



	idle	attacking
Mikrotik	3,83%	4,76%
Server Honepot	8,87%	92,30%

Gambar 6 Beban Memori scenario II (%)

4. KESIMPULAN DAN SARAN

Kesimpulan dari penelitian ini serangan DDoS dan Brute Force mengakibatkan peningkatan beban kinerja CPU baik pada Mikrotik maupun pada server Honeypot. Adanya port forwarding yang telah diaktifkan pada Mikrotik memberikan solusi untuk mengalihkan paket serangan ke perangkat server Honeypot untuk mengurangi kinerja CPU mikrotik sehingga miktorik dapat berjalan secara normal. Saran penelitian kedepannya menambahkan keamanan ke dalam setiap port pada perangkat jaringan, khususnya perangkat infrastuktur komputasi awan.

DAFTAR PUSTAKA

[1] G. K. Sadasivam, C. Hota, and B. Anand, "Honeynet Data Analysis and Distributed SSH Brute-Force Attacks," *Towar. Extensible Adapt. Methods Comput.*, no. October, pp. 107–118, 2018, doi: 10.1007/978-981-13-2348-5_9.

[2] C. Wang and Z. Lu, "Cyber Deception: Overview and the Road Ahead," *IEEE Secur. Priv.*, vol. 16, no. 2, pp. 80–85, 2018, doi: 10.1109/MSP.2018.1870866.

[3] A. Yudhana, I. Riadi, and F. Ridho, "DDoS classification using neural network and naïve bayes methods for network forensics," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 11, pp. 177–183, 2018, doi: 10.14569/ijacsa.2018.091125.

[4] R. Adrian and N. Isnianto, "Pada Performa Router," no. October, pp. 1257–1259, 2016.

[5] - Syaifuddin, D. Risqiwati, and E. A. Irawan, "Realtime Pencegahan Serangan Brute Force dan DDOS Pada Ubuntu Server," *Techno.Com*, vol. 17, no. 4, pp. 347–354, 2018,

doi: 10.33633/tc.v17i4.1766.

[6] S. Sandra, D. Stiawan, and A. Heryanto, "Visualisasi Serangan Brute Force Menggunakan Metode K-Means dan Naïve Bayes," *Proceeding - Annu. Res. Semin. Proceeding*, vol. 2, no. 1, pp. 315–320, 2016.

[7] J. Kaur, R. Singh, and P. Kaur, "Prevention of DDoS and Brute Force Attacks on Web Log Files using Combination of Genetic Algorithm and Feed forward Back Propagation Neural Network," *Int. J. Comput. Appl.*, vol. 120, no. 23, pp. 10–13, 2015, doi: 10.5120/21399-4406.

[8] B. Jaya, Y. Yunus, and S. Sumijan, "Peningkatan Keamanan Router Mikrotik Terhadap Serangan Denial of Service (DoS)," *J. Sistim Inf. dan Teknol.*, vol. 2, pp. 5–9, 2020, doi: 10.37034/jsisfotek.v2i4.81.

[9] F. Adhi Purwaningrum, A. Purwanto, E. Agus Darmadi, P. Tri Mitra Karya Mandiri Blok Semper Jomin Baru, and C. -Karawang, "Optimalisasi Jaringan Menggunakan Firewall," vol. 2, no. 3, pp. 17–23, 2018.

[10] D. Kumar and M. Gupta, "Implementation of Firewall & Intrusion Detection System Using pfSense To Enhance Network Security," *Int. J. Electr. Electron. Comput. Sci. Eng.*, pp. 131–137, 2018, [Online]. Available: www.ijeecse.com.

[11] N. Arkaan and D. V. S. Y. Sakti, "Implementasi Low Interaction Honeypot Untuk Analisa Serangan Pada Protokol SSH," *J. Nas. Teknol. dan Sist. Inf.*, vol. 5, no. 2, pp. 112–120, 2019, doi: 10.25077/teknosi.v5i2.2019.112-120.

[12] P. Sokol, J. Míšek, and M. Husák, "Honeypots and honeynets: issues of privacy," *Eurasip J. Inf. Secur.*, vol. 2017, no. 1, pp. 1–9, 2017, doi: 10.1186/s13635-017-0057-4.

[13] W. Cabral, C. Valli, L. Sikos, and S. Wakeling, "Review and analysis of cowrie artefacts and their potential to be used deceptively," *Proc. - 6th Annu. Conf. Comput. Sci. Comput. Intell. CSCI 2019*, pp. 166–171, 2019, doi: 10.1109/CSCI49370.2019.00035.

[14] D. S. Hermawan, S. Syaifuddin, and D. Risqiwati, "Analisa Real-Time Data log honeypot menggunakan Algoritma K-Means pada serangan Distributed Denial of Service," *J. Repos.*, vol. 2, no. 5, p. 541, 2020, doi: 10.22219/repositor.v2i5.440.

[15] M. Arman and N. Rachmat, "Implementasi Sistem Keamanan Web Server Menggunakan Pfsense," *Jusikom J. Sist. Komput. Musirawas*, vol. 5, no. 1, pp. 13–23, 2020, doi: 10.32767/jusikom.v5i1.752.