

MITIGASI DHCP STARVATION ATTACK PADA ROUTER BOARD MIKROTIK DAN PENGARUHNYA TERHADAP PERFORMANSI

Dian Novianto¹⁾, Yohanes Setiawan Japriadi²⁾, Lukas Tommy³⁾, Sujono⁴⁾

^{1), 2), 3)} Program Studi Teknik Informatika, ISB Atma Luhur

⁴⁾ Program Studi Sistem Informasi, ISB Atma Luhur

Email : diannovianto@atmaluhur.ac.id¹⁾, ysetiawanj@atmaluhur.ac.id²⁾, lukastommy@atmaluhur.ac.id³⁾, sujono@atmaluhur.ac.id⁴⁾

ABSTRACT

As people become more dependent on information technology, the need for Internet availability increases. Various types of devices are connected to the network, increasing the convenience of using information technology. However, this convenience can often be disrupted by attacks on the network infrastructure, one of which is a DHCP Starvation attack. The Dynamic Host Configuration Protocol (DHCP) is a client-server-based protocol used to automatically assign or obtain IP addresses for client computers or other network devices. Mitigating DHCP Starvation attacks is one form of protection for users. The impact of this attack is that the attacker can become one of the hosts on the network and perform a man-in-the-middle attack, so the impact of information leakage can occur. In addition, it is necessary to know the impact on router resources when a DHCP Starvation attack occurs, so that network managers can calculate how much resources are needed. The author uses a Filtering method based on Mac address es, ARP, and alerts on the Mikrotik router. In addition, the PPDIOO method is also used to develop this system, which consists of preparation, planning, design, Implementation, operation, and optimization. The test results showed that the application of this Filtering method proved to be very effective in preventing DHCP Starvation attacks, and the router board resources were not significantly affected when this Filtering method was applied.

Keywords : DHCP Starvation, Mac address Filtering, Mikrotik.

ABSTRAK

Dengan meningkatnya ketergantungan manusia pada teknologi informasi, kebutuhan akan ketersediaan internet semakin meningkat. Berbagai jenis perangkat yang saling terhubung di jaringan, meningkatkan kenyamanan dalam penggunaan teknologi informasi. Akan tetapi, seringkali kenyamanan ini dapat terganggu akibat adanya serangan terhadap infrastruktur di jaringan, salah satunya adalah akibat DHCP Starvation attack. Protokol Konfigurasi Host Dinamis (DHCP) adalah protokol yang berbasis klien-server, digunakan untuk secara otomatis memberikan atau menerima alamat IP pada komputer klien atau perangkat jaringan lainnya. Melakukan mitigasi serangan DHCP Starvation merupakan salah satu bentuk perlindungan terhadap pengguna. Dampak dari serangan ini adalah penyerang dapat menjadi salah satu host di jaringan dan dapat melakukan serangan man in the middle, sehingga dampak kebocoran informasi dapat terjadi. Selain itu perlunya mengetahui dampak terhadap sumberdaya router saat serangan DHCP Starvation ini terjadi, sehingga pengelola jaringan dapat memperhitungkan seberapa besar kebutuhan sumberdaya yang ada. Penulis menggunakan metode Filtering berbasis mac address , arp, dan peringatan pada router mikrotik, selain itu metode PPDIOO juga digunakan untuk mengembangkan sistem ini, yang terdiri dari persiapan, perencanaan, desain, penerapan, operasional, dan optimalisasi. Adapun hasil dari pengujian didapatkan bahwa dengan menerapkan metode Filtering ini terbukti sangat efektif dalam mencegah serangan DHCP Starvation dan resource routerboard tidak terpengaruh secara signifikan saat metode Filtering ini diterapkan.

Kata Kunci : DHCP Starvation, Mac address Filtering, Mikrotik.

1. Pendahuluan

Berbagai jenis server maupun komputer yang saling terhubung satu sama lain dapat memberikan kemudahan bagi pengguna dalam perkembangan teknologi informasi saat ini. Namun, dengan perkembangan teknologi saat ini, diperlukan tingkat keamanan yang lebih tinggi, karena perkembangan ini diikuti dengan berkembangnya ancaman kejahatan cyber. Salah satu yang mungkin terjadi adalah serangan pada DHCP (Dynamic Host Configuration Protocol) Server. DHCP adalah server yang memungkinkan sistem penyebaran IP secara

otomatis ke perangkat satu dengan yang lainnya. Ini membuat pengalokasian alamat IP menjadi lebih mudah karena pengguna tidak perlu mengisi parameter IP secara manual. Selain itu, DHCP juga memiliki layanan untuk memperbarui alamat IP secara otomatis (D. Kurnia, 2020) (Riduwan, dkk, 2010). Pada tahap awal interaksi antara DHCP klien dan DHCP server untuk Implementasi protokol DHCP, akan dimulai dari pengiriman paket DHCP Discover, Offer, Request dan ACK.

Salah satu bentuk serangan pada DHCP server adalah DHCP Starvation attack, yaitu sebuah jenis serangan

dimana penyerang mencoba untuk menghabiskan semua alamat *IP* yang tersedia dalam jaringan yang diatur menggunakan DHCP (*Dynamic Host Configuration Protocol*). Serangan ini dapat menyebabkan kegagalan dalam penugasan alamat *IP* kepada perangkat yang sah, mengakibatkan gangguan atau bahkan kegagalan total pada jaringan. DHCP *Starvation attack* adalah jenis serangan dimana penyerang mencoba untuk menghabiskan semua alamat *IP* yang tersedia didalam *pool router* di jaringan yang diatur menggunakan DHCP (*Dynamic Host Configuration Protocol*). Serangan DHCP *Starvation* dilakukan dengan mengirimkan banyak paket DHCP *DISCOVER*. Ini menyebabkan DHCP server kehabisan persediaan alamat *IP*, sehingga klien yang sah tidak dapat melakukan konfigurasi alamat *IP* secara otomatis. (Umasuthan, V. 2016).

Pada dasarnya, DHCP berfungsi untuk memberikan alamat *IP* kepada setiap *host* dengan syarat menggunakan subnetting yang sama. Namun, teknik ini memiliki kelemahan karena serangan dapat membuat si penyerang menjadi DHCP *Server* yang palsu menggantikan DHCP *server* yang sebenarnya (Saputra, B. R, 2022).

Beberapa organisasi mungkin tidak menyadari potensi serangan DHCP *Starvation* atau mungkin tidak memprioritaskan keamanan jaringan dengan tepat. Hal ini dapat membuat mereka rentan terhadap serangan semacam itu jika tidak dihadapi dengan langkah-langkah yang tepat. Oleh karena itu diperlukan sebuah mitigasi sebagai tindakan pencegahan dari masalah yang ada. Salah satu teknik yang dapat digunakan adalah *Filtering mac address*, *arp Static* dengan mode *reply-only*, dan *alert*.

Mac address Filtering dalam DHCP *pool* adalah metode yang digunakan untuk mengendalikan akses ke jaringan berdasarkan alamat MAC (*Media Access Control*) dari perangkat yang terhubung. Ini berfungsi dengan cara memeriksa alamat MAC dari perangkat yang meminta alamat *IP* melalui protokol DHCP, dan kemudian memutuskan apakah perangkat tersebut diizinkan untuk menerima konfigurasi jaringan atau tidak. Adapun fungsi *Mac address Filtering* dalam DHCP *pool* antara lain : kontrol akses, keamanan, Pengendalian Sumber Daya Jaringan, Konfigurasi Jaringan yang Lebih Tepat, dan Manajemen Inventaris Perangkat.

ARP *Static* adalah metode di mana administrator jaringan secara manual mengkonfigurasi tabel ARP pada perangkat jaringan untuk menetapkan korespondensi antara alamat *IP* dan alamat MAC secara statis. Dengan kata lain, alamat MAC dari setiap perangkat dalam jaringan didefinisikan secara manual dalam tabel ARP. Manfaat dari ARP *Static* adalah mengurangi kemungkinan serangan spoofing ARP, di mana penyerang mencoba untuk mengirimkan lalu lintas jaringan palsu dengan menyatakan bahwa mereka adalah perangkat lain dalam jaringan. Selain itu memberikan kontrol lebih besar kepada administrator atas tabel ARP, memungkinkan mereka untuk dengan tepat menentukan korespondensi antara alamat *IP* dan alamat MAC tanpa harus bergantung pada proses ARP otomatis.

Mode *Reply-Only* pada ARP adalah konfigurasi di mana perangkat jaringan hanya merespons permintaan ARP yang diterimanya, tetapi tidak mengirimkan permintaan ARP sendiri. Dengan kata lain, perangkat hanya akan merespons permintaan ARP yang ditujukan kepadanya, tetapi tidak akan menginisiasi permintaan ARP ke perangkat lain dalam jaringan. Manfaat dari mode "Reply-Only" ARP adalah dapat mengurangi risiko serangan ARP poisoning, di mana perangkat jaringan disesatkan untuk mengaitkan alamat *IP* dengan alamat MAC palsu yang dikendalikan oleh penyerang. Selain itu juga dapat mengurangi lalu lintas ARP yang tidak perlu dalam jaringan, karena perangkat hanya merespons permintaan ARP yang langsung ditujukan kepadanya.

Router Mikrotik memiliki fitur DHCP *Alert*, yang dapat digunakan untuk mengidentifikasi beberapa dhcp server pada jaringan yang sama, yang dapat mengganggu distribusi alamat *IP*. Parameter pada rule *alert* termasuk *interface*, yang digunakan untuk menentukan *interface router* yang menjalankan DHCP *Server*. Kemudian ada parameter valid server, yang berisi *Mac address* dari DHCP *Server* yang asli, dan parameter *On Alert*, yang digunakan untuk mengidentifikasi DHCP *Server* yang tidak aktif. Selain itu, fitur DHCP *Alert* juga dapat digunakan untuk mengidentifikasi adanya DHCP *rogue*. Penelitian ini menggunakan model pengembangan jaringan PPDIIO (*Prepare, Plan, Design, Implement, Operate, and Optimize*). PPDIIO adalah metode perancangan dan pengembangan jaringan yang dikembangkan oleh Cisco (Imam Solikin, 2017), dan akan memberikan langkah-langkah penting untuk keberhasilan perancangan jaringan (Dian, 2020). Penerapan metode atau teknik diatas diharapkan dapat mengatasi overcoming DHCP *discover* yang diakibatkan oleh serangan DHCP *Starvation*, sehingga jaringan dapat bekerja dengan baik dan mampu membuat pengguna merasa aman dan nyaman. Metode ini juga diharapkan tidak berpengaruh secara signifikan terhadap *resource* dari *router* sehingga dapat digunakan pada jaringan yang menggunakan sumberdaya *router* yang terbatas.

A. Metode Penelitian

Penelitian ini menggunakan metode kualitatif, dengan peneliti berperan sebagai alat utama dalam pengumpulan data (Dian, 2022). Metode ini digunakan sebagai cara untuk mengumpulkan data dan menemukan solusi untuk masalah (Marinu, 2023). Peneliti mengumpulkan data dengan mencari referensi dari jurnal ilmiah dan buku. sehingga peneliti dapat memahami dan memahami cara metode atau teknik yang akan digunakan digunakan, sehingga diharapkan pengembangan sistem jaringan akan berjalan dengan baik dan lancar di masa mendatang. Mempersiapkan, merencanakan, membangun, menerapkan, mengoperasikan, dan mengoptimalkan adalah beberapa tahapan yang harus diikuti oleh peneliti saat mengembangkan sistem dengan model PPDIIO ini.

1. *Prepare* (Persiapan)

Pada tahap ini, penulis akan menyiapkan peralatan dan bahan-bahan atau studi literatur dengan mengumpulkan referensi jurnal dari lima tahun terakhir untuk membantu mereka menjalankan penelitian. Judul penelitian yang direferensikan antara lain:

- Penelitian pada tahun 2019 dengan judul Filter Paket Berdasarkan Differentiated Services Code Point untuk Pencegahan Serangan DHCP Starvation (Sarip, 2019).
- Penelitian pada tahun 2023 mengenai Analisis Serangan DHCP Starvation attack Pada Router OS Mikrotik (Tamsir dkk, 2023).
- Penelitian pada tahun 2020 dengan judul Analisis Serangan DHCP Starvation attack Pada Router OS Mikrotik (Kurnia, 2020).
- Penelitian pada tahun 2022 dengan judul Analisis Pengamanan Jaringan Menggunakan Router Mikrotik dari Serangan DoS dan Pengaruhnya Terhadap Performansi (Arief, 2022).
- Penelitian pada tahun 2020 dengan judul Mitigating Dhcp Starvation attack Using Snooping Technique (Abdulhafiz, 2022).

2. *Plan* (Perencanaan)

Tabel 1 dan 2 menunjukkan spesifikasi *hardware* dan *software* yang dibutuhkan peneliti untuk penelitian mitigasi selama pengembangan sistem:

Tabel 1. Kebutuhan *Hardware*

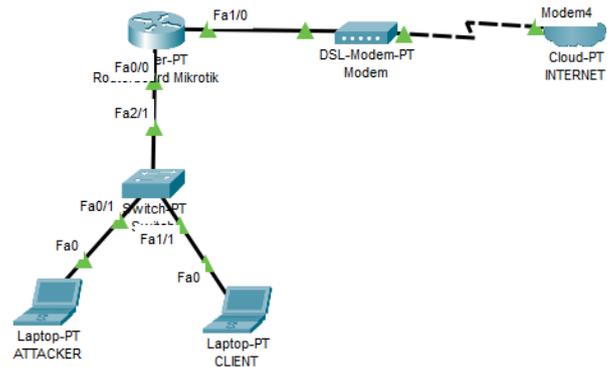
No	Perangkat Keras	Keterangan	Jumlah
1	Mikrotik RB 750	Routerboard yang digunakan	1
2	Kabel UTP siap pakai	Sebagai media penghubung	1
3	Laptop	Berperan sebagai klien dan penyerang	2

Tabel 2. Kebutuhan *Software*

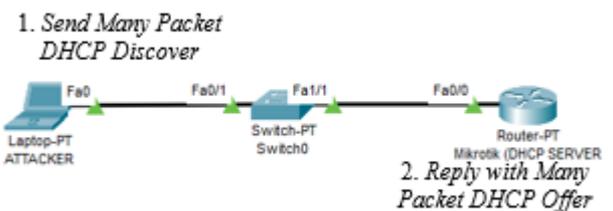
No	Perangkat Lunak	Keterangan	Jumlah
1	RouterOS misbe 6.48	Sistem operasi router	1
2	Windows 8.1	Sistem operasi klien	1
3	Kali linux	Sistem operasi penyerang	1
3	Cisco packet tracer 7.3.0	Digunakan untuk mendesain topologi	1
4	yersenia	Digunakan untuk serangan dhcp starvation	1

3. *Design* (Desain)

Setelah tahap perencanaan selesai, tahap selanjutnya adalah desain, yang dilakukan menggunakan model *ppdioo*. Peneliti menggunakan perangkat lunak *cisco packet tracer* versi 7.3.0 untuk membuat simulasi topologi jaringan, seperti yang ditunjukkan pada gambar 1 dan gambar 2.



Gambar 1. Topologi Jaringan Simulasi

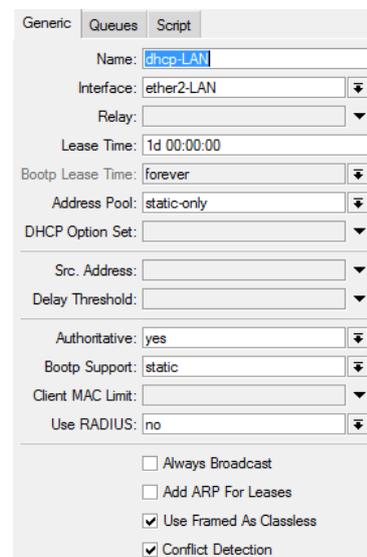


Gambar 2. DHCP Starvation attack

Dari gambar 2 proses yang terjadi adalah penyerang melakukan ddos berupa dhcp discover ke router yang menjadi dhcp server, kemudian dhcp server akan membalas semua paket discover dengan dhcp offer sampai semua alamat ip yang tersedia habis, sehingga user lain tidak mendapatkan ip address, dan penyerang dapat membuat dhcp server palsu untuk klien di jaringan tersebut.

4. *Implement* (Implementasi)

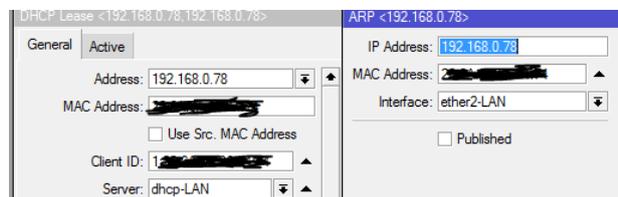
Dalam tahap ke empat ini, konfigurasi atas router diterapkan sesuai dengan desain pada tahapan sebelumnya, dengan cara menerapkan teknik keamanan *Filtering mac address*, yaitu mendaftarkan mac address pengguna pada router untuk mendapatkan alamat ip tertentu.



Gambar 3. Konfigurasi DHCP Server

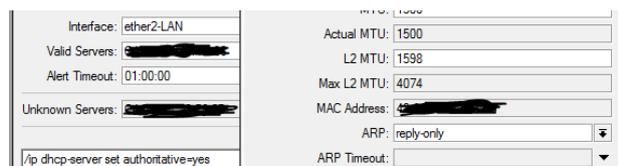
Parameter yang di ubah untuk *Filtering* ini antara lain *address pool: Static-only*, *authoritative yes*, dan *no checklist* untuk add ARP for *leases* seperti yang ditunjukkan pada gambar 3.

Tujuan dari parameter *address pool Static-only* adalah untuk memastikan bahwa klien hanya dapat mendapatkan alamat *IP* dari perangkat yang telah didaftarkan pada *router*. Di sisi lain, tujuan dari parameter *authoritative* adalah untuk mengetahui bagaimana *DHCP Server* menangani permintaan layanan *DHCP* mengirim *NACK (Negative Acknowledgment)*. Parameter yang dapat digunakan mengatasi *DHCP server* palsu atau *DHCP Rogue* yang terdapat dalam jaringan. Tujuan dari tidak menambah ARP untuk sewa adalah untuk mencegah *dhcp server* secara otomatis menambah data ke tabel ARP. Konfigurasi ini diikuti dengan konfigurasi *arp: reply-only* pada *interface* yang berfungsi sebagai *gateway* jaringan lokal seperti yang ditunjukkan pada gambar 4.



Gambar 4. DHCP Lease dan ARP

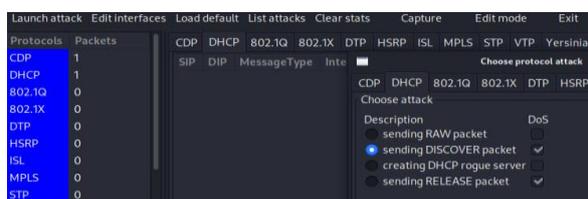
Tujuan dari *reply-only* pada *arp* di *interface gateway* seperti yang ditunjukkan pada gambar 5 adalah untuk memastikan bahwa *Router* hanya dapat berkomunikasi dengan klien yang menerima alamat *IP* dari proses *DHCP*, sehingga *DHCP server* mengabaikan penemuan penyerang *DHCP*. Karena *mac address* penyerang tidak terdaftar di *router*. Namun, *alert dhcp server* bertujuan untuk memberi tahu admin jaringan jika ada *dhcp server* palsu atau tandingan di jaringan.



Gambar 5. DHCP Alert dan arp reply only

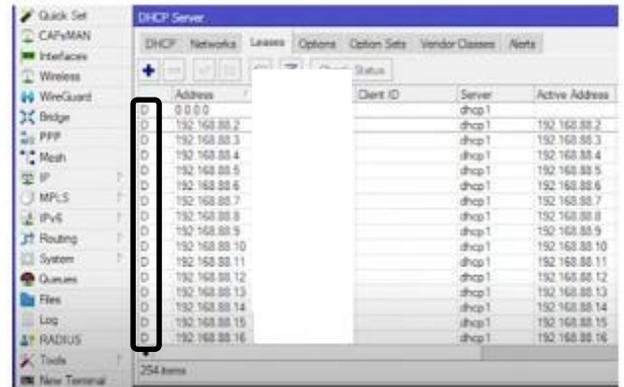
5. Operate (Operate)

Pada tahap *operate* dilakukan penulis dengan cara melakukan simulasi dan konfigurasi atas teknik pencegahan yang dipilih. Simulasi yang pertama dilakukan adalah menggunakan *yersenia* pada sistem operasi kali linux untuk mengirimkan beberapa paket *dhcp*, seperti pada gambar 6.



Gambar 6. Simulasi Starvation attack

Serangan yang dipilih menggunakan *yersenia* adalah mengirimkan paket *discover* dan paket *release* dengan tujuan membanjiri *dhcp server* dengan paket *discover* secara terus menerus, karena serangan ini termasuk kedalam serangan yang bertujuan untuk membuat *router* tidak bekerja sebagaimana mestinya.



Gambar 7. Dampak Starvation attack

Hasil serangan *dhcp Starvation* seperti pada gambar 7, membuat *dhcp server* melepaskan alamat *ip* yang berada pada *pool* untuk diberikan ke penyerang, sehingga alamat tersebut habis, dan pengguna yang sah tidak mendapatkan alamat tersebut, lalu dapat membuat *dhcp server* palsu yang bertujuan agar pengguna jaringan tersebut terhubung ke *dhcp server* palsu tersebut.

6. Optimize (Optimasi)

Fase Optimasi dilakukan setelah jaringan beroperasi. Tahapan ini akan dilakukan monitoring performa pada *resource router* sebelum dan setelah teknik keamanan di terapkan.

2. Hasil dan Pembahasan

Pada bagian ini akan ditampilkan hasil dari simulasi serangan *dhcp Starvation* yang dilakukan oleh laptop penyerang ke *dhcp server* pada *router* dan pengguna mencoba untuk mengakses *dhcp server* pada *router*.



Gambar 8. Hasil percobaan serangan

Dari gambar 8 terlihat bahwa *yersenia* pada perangkat penyerang tidak dapat terhubung ke *dhcp server* karena paket *discover* dari perangkat penyerang diabaikan, hal ini terjadi karena *mac address* dari penyerang tidak terdaftar pada *leases dhcp server* di *router* mikrotik, hal ini menyebabkan perangkat – perangkat yang tidak di kenal tidak akan mendapatkan alamat *ip* yang sesuai dengan jaringan tersebut, sehingga tidak mendapatkan

akses di jaringan tersebut. Selain itu apa bila penyerang mencoba langsung untuk memasang dhcp server palsu, maka akan langsung dikenali sebagai dhcp rogue, dan script peringatan akan di eksekusi, lalu tercatat didalam log router.



Gambar 9. Peringatan dhcp server rogue

Gambar 9 menunjukkan peringatan pada log didalam router yang sekaligus menjadi dhcp server, seorang administrator dapat mengambil tindakan keamanan lanjutan sesuai dengan sop yang berlaku.

DHCP Server				
DHCP Networks				
Address	MAC Address	Client ID	Server	
192.168.0.80			dhcp-LAN	
192.168.0.81			dhcp-LAN	
192.168.0.82			dhcp-LAN	
192.168.0.83			dhcp-LAN	
192.168.0.84			dhcp-LAN	
192.168.0.85			dhcp-LAN	
192.168.0.86			dhcp-LAN	
192.168.0.87			dhcp-LAN	
192.168.0.88			dhcp-LAN	
192.168.0.89			dhcp-LAN	
192.168.0.90			dhcp-LAN	

Gambar 10. Leases DHCP Server

Gambar 10 menunjukkan hasil dari konfigurasi membuat router tidak lagi dipenuhi oleh dhcp discover penyerang, dan dhcp server tidak mengeluarkan atau melepas alamat ip dari pool untuk ditawarkan kepada penyerang melalui leases. Hal ini terlihat perbedaan pada gambar 7 dan gambar 10, dimana pada gambar 7 terlihat tag D yang berarti dynamic, yang berarti alamat dapat berubah – ubah dan di request oleh siapapun, sedangkan pada gambar 10 tag D telah hilang, menandakan tidak semua perangkat dapat terhubung, hanya yang telah didaftarkan mac address yang mendapatkan alamat ip.

Kemudian terlihat pada gambar 11 pada bagian resource yang dimonitoring saat pengujian berlangsung terlihat saat serangan terjadi penggunaan CPU meningkat cukup tinggi, menjadi sebesar 35% persen.

Free Memory:	98.2 MiB
Total Memory:	128.0 MiB
CPU: MIPS 74Kc V4.12	
CPU Count:	1
CPU Frequency:	600 MHz
CPU Load:	35 %
Free HDD Space:	109.5 MiB
Total HDD Size:	128.0 MiB

Gambar 11. Penggunaan resource sebelum penerapan teknik

Saat tidak adanya serangan dhcp Starvation karena sudah diterapkan teknik keamanan, penggunaan CPU lebih rendah seperti yang ditunjukkan gambar 12.

Free Memory:	98.2 MiB
Total Memory:	128.0 MiB
CPU: MIPS 74Kc V4.12	
CPU Count:	1
CPU Frequency:	600 MHz
CPU Load:	15 %
Free HDD Space:	109.5 MiB
Total HDD Size:	128.0 MiB

Gambar 12. Penggunaan resource routerboard

Hal ini berarti resource pada router tidak terpengaruh saat teknik pencegahan ini diterapkan, terlihat dari load cpu yang masih rendah sekitar 5-25%, memory yang tersedia sebesar 98 MB, dan total HDD sebesar 109 MB, tentunya hal ini juga dipengaruhi aktivitas lain, tapi didalam skenario simulasi ini, router dapat berjalan dengan baik dan pengguna dapat menggunakan akses internet dengan lebih aman tanpa adanya gangguan dari DHCP Starvation.

3. Kesimpulan

Setelah dilakukan penelitian ini, penulis dapat mengambil beberapa kesimpulan dari penulisan penelitian ini, sebagai berikut :

1. Teknik Filtering mac address yang dikombinasikan dengan arp dan dhcp alert terbukti mampu mengamankan jaringan dari percobaan serangan dhcp Starvation.
2. Sumberdaya router tidak terpengaruh secara signifikan saat teknik keamanan yang dipilih diterapkan pada jaringan yang berjalan, hal ini ditunjukkan dari hasil monitoring pada bagian hasil.

Daftar Pustaka

Abdulhafiz A. Nuhu, Faith O. Echobu, Oyenike M. Olanrewaju. 2022. Mitigating Dhcp Starvation attack Using Snooping Technique. Vol. 4 No. 1: FUDMA Journal of Sciences.

Arief Indriarto Haris, dkk. 2022. Analisis Pengamanan Jaringan Menggunakan Router Mikrotik dari Serangan DoS dan Pengaruhnya Terhadap Performansi. Komputika: Jurnal Sistem Komputer Volume 11, Nomor 1, April 2022, hlm. 67 – 76.

Dian Novianto, Tri Sugihartono. 2020. Sistem Deteksi Kualitas Buah Jambu Air Berdasarkan Warna Kulit

- Menggunakan Algoritma Principal Component Analysis (Pca) dan K-Nearest Neighbor (K-NN). Jurnal Ilmiah Informatika Global Volume 11 No. 2 Desember 2020.
- Dian Novianto, dkk. 2022. *Implementasi Keamanan Akses Terhadap Website Menggunakan Wireguard VPN Di Routerboard Mikrotik*. Jurnal Ilmiah Informatika Global Volume 13 No. 2 Agustus 2022.
- D. Kurnia. (2020). Analisis serangan DHCP *Starvation attack* pada *router OS Mikrotik*". Jurnal Ilmiah Core IT Vol. 8, No. 5 [2] T. Ariyadi. (2018). Mitigasi Keamanan Dynamic Host Control Protocol (DHCP) Untuk Mengurangi Serangan Pada Local Area Network (LAN). Jurnal Inovtek Polbeng, Vol. 3.
- Imam Solikin. 2017. Penerapan Metode PPDIOO dalam Pengembangan LAN dan WLAN. Teknomatika, Vol.07, No.01, hal 65-73.
- Kurnia, Dian. 2020. Analisis Serangan DHCP *Starvation attack* Pada *Router OS Mikrotik*. JURNAL ILMIAH CORE IT Vol. 8 No. 5.
- Marinu Waruwu. 2023. Pendekatan Penelitian Pendidikan: Metode Penelitian Kualitatif, Metode Penelitian Kuantitatif dan Metode Penelitian Kombinasi (Mixed Method). Jurnal Pendidikan Tambusai: Volume 7 Nomor 1, halaman 2896-2910.
- Riduwan, A., I. Triyuwono, G. Irianto, dan U. Ludigdo . 2010. Semiotika Laba Akuntansi: Studi Kritis - Posmodernis Derridean . *Jurnal Akuntansi dan Keuangan Indonesia* 7(1): 38–60.
- Saputra, B. R dan Chandra, D. W. (2022). Simulasi Keamanan Jaringan Dengan Metode DHCP Snooping Dan VLAN Menggunakan CISCO. Jurnal Teknik Informatika dan Sistem Informasi. Vol 9 No 4.
- Sarip, Arief Setyanto. 2019. Filter Paket Berdasarkan Differentiated Services Code Point untuk Pencegahan Serangan DHCP *Starvation*. Jurnal Pekommas, Vol. 4 No. 2, Oktober 2019:137-146.
- Tamsir Ariyadi, dkk. 2023. Analisis Serangan DHCP *Starvation attack* Pada *Router OS Mikrotik*. Jurnal Ilmiah Informatika Volume 11 No. 01.
- Umasuthan, V. (2016). Protecting the Communications Network at Layer 2. In 2016 IEEE/PES Transmission and Distribution Conference and Exposition.