Methotika : Jurnal Ilmiah Teknik Informatika
ISSN :2776-5792
Vol. 2, No. 1, April 2022, pp. 29-37
http://ojs.fikom-methodist.net/index.php/METHOTIKA

Pengamanan Mikrotik Routerboard Dari Serangan Keamanan Dengan Notifikasi BotTelegram

Arif Gunawan Simanjuntak[1], Naikson Fandier Saragih[2], Mufria J Purba[3]
[1,2,3]Fakultas Ilmu Komputer, Universitas Methodist Indonesia

Info Artikel

Histori Artikel:

Received, Sep 9 , 2022
Revised, May, 2020
Accepted, Jun 11, 2020

Keywords:

Mikrotik, IDS,
DDOS, Telegram
Bot, Script
Scheduler

ABSTRACT

Sebuah Jaringan dapat mengalami gangguan(down) bila terjadi serangan pada router, salah satunya adalah serangan ddos. Penelitian ini dilakukan menggunakan jaringan BPTD, dimana pada jaringan belum terdapat pengamanan terhadap router. Pengamanan mikrotik routerbouard dari serangan ddos menggunakan snort sebagai Intrusion Detection System (IDS) terhadap serangan : Ping Flood, Syn Flood dan Udp Flood. Penilitian diawali dengan : mengetahui alur sistem keamanan jaringan dan konsep pengamanan router mikrotik dari serangan ddos pada topologi jaringan BPTD, dilanjutkan dengan merancang topologi jaringan dengan menggunakan mikrotik, perancangan flowchart konfigurasi sistem keamanan Jaringan meliputi: Ping Flood, Syn Flood, Udp Flood. Perancangan dilanjutkan merancang Flowchart skema penyerangan meliputi: Ping Flood, Syn Flood, Udp Flood. proses dilanjutkan dengan implementasi diawali proses konfigurasi router. Ujicoba keamanan menggunakan tools cmd untuk ping flood,Nmap untuk syn flood, UDP Flood. Pengujian IDS terhadap semua jenis telah berhasil dideteksi dengan pemberian notifikasi melalui bot telegram.

Penulis Koresponden:

Naikson Fandier Saragih,
Faculty of Computer Science,
Universitas Methodist Indonesia, Medan,
Jl. Hang Tua No.8, Medan - Sumatera Utara.
Email: naikson@naikson.com

1. PENDAHULUAN

Router merupakan suatu alat yang digunakan untuk mengirimkan paket data melalui sebuah jaringan. Akan tetapi tidak semua perusahaan yang memiliki sebuah jaringan diaturmenggunakan mikrotik router. Salah satunya adalah Balai Pengelola Transportasi Darat (BPTD) kota Medan. Pada Balai Pengelola Transportasi Darat (BPTD) koneksi internet pada client masih disalurkan langsung dari modem internet melalui switch antar ruangan. Pada penggunaan internet dengan akses client yang cukup banyak, tentu dengan hanya mengandalkan modem bukan pilihan yang tepat. Oleh sebab itu dibutuhkanya penambahan router pada manajemen jaringan serta untukmenambah keamanan jaringan.

Router yang dapat digunakan untuk mengelola jaringan adalah mikrotik router. Pengelolaan mikrotik router tersebut tentu dilakukan oleh seorang administrator jaringan. Tugas administrator jaringan juga tidak dapat dikatakan mudah, hal ini dikarenakan seorang admin harus mengamankan jaringanya dari suatu serangan yang dapat mengakibatkan router jaringan down hingga rusak. Masalah keamanan jaringan komputer merupakan faktor yang sangat penting diperhatikan dan dikelola oleh seorang admin jaringan.

Sistem keamanan jaringan komputer bisa jadi secara fisik maupun secara non fisik. Secara fisik adalah sistem keamanan server beserta perangkat pendukungnya dari pencurian, bencana alam dan kerusakan akibat kesalahan manusia. Sedangkan secara non fisik adalah berupa kerusakan sistem operasi server, kerusakan pada program aplikasi ataupun terhadap gangguan dari luar sistem seperti serangan hacker, virus, trojan dan lain sebagainya (Sutarti, Pancaro, & Saputra, 2018). Banyak sekali cara yang ditempuh untuk menghalangi seseorang/perusahaan untuk dapat memberikan layanan yang optimal.

Namun seringnya jaringan server mengalami gangguan karena diserang yang disebabkan oleh serangan jenis DDoS, gangguan tersebut bisa berupa kegagalan sistem, halt, error request bahkan kerusakan hardware server. Serangan Distributed denial-of-service (DDoS) merupakan jenis serangan yang telah ada. sejak tahun 1990, dimana volume dan intensitas DDoS terus meningkat. Pada akhir tahun 2014, dilaporkan bahwa serangan DDoS merupakan teknik serangan yang paling populer. Dengan demikian, DDoS merupakan salah satu ancaman utama dunia maya dan menjadi masalah utama keamanan cyber (Gong et al., 2019).

Dalam penelitian menyatakan bahwa DDoS berhasil menyerang jaringan dengan tingkat 90%, sehingga dibutuhkanya sebuah sistem pendeteksi terhadap router ketika terjadinya sebuah serangan DDoS. Pendeteksi serangan tersebut bertujuan untuk mengamankan router dari pihak yang tidak bertanggung jawab. Oleh sebab itu dibutuhkanya sebuah keamanan jaringan dengan metode Intrusion Detection System (IDS) (Ginting, Napitupulu, & Jamaluddin, 2015). Intrusion Detection System (IDS) adalah metode yang digunakan untuk mendeteksi sebuah aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. Metode ini memberikan peringatan kepada admin bahwasanya terjadi suatu serangan dan menutup serangan tersebut. Sehingga serangan DDoS tidak sempat masuk kedalam sebuah router yang dapat menyebabkan router down.

Untuk menambah keamanan, maka digunakan fitur notifikasi untuk memberikan peringatan kepada admin jaringan ketika adanya serangan DDoS. Peringatan notifikasi serangan DDoS dapat dilakukan dengan konfigurasi alert bot telegram pada jaringan mikrotik. Penggunaan notifikasi bot telegram sangat berguna bagi seorang administrator jaringan dalam rangkan memberikan peringatan ketika adanya serangan DDoS, hal ini dikarenakan bot telegram mampu memberikan informasi berupa data penyerangan pada jaringan mikrotik. Sehingga monitoring jaringan dari tindakan yang dapat merugikan pengguna yang dilakukan secara realtime oleh notifikasi bot telegram.

Beradasarkan pada latar belakang masalah di atas dan kesimpulan dari penelitian sebelumnya, maka pada penelitian ini akan menambahkan sebuah router serta mengamankan router jaringan mikrotik dari sebuah serangan DDoS dengan IDS dan notifikasi bot telegram dengan riset jaringan pada Balai Pengelola Transportasi Darat (BPTD).

2. METODE PENELITIAN

2.1 Spoofing

Spoofing adalah teknik yang digunakan untuk memperoleh akses yang tidak sah ke suatu komputer atau informasi, dimana penyerang berhubungan dengan pengguna dengan berpura- pura memalsukan bahwa mereka adalah host yang dapat dipercaya (Ketaren, 2016).

2.2. DDOS

Serangan DOS (Denial-Of-Service attacks) adalah jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber (resource) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut (Pradipta, 2017).untuk kebutuhan sharing data melalui jaringan atau Network Attached Storage (NAS).

FreeNAS ini juga merupakan distro Linux yang khusus digunakan sebagai system operasi NAS (Network Attached Storage) berbasis FreeBAS[5]. sistem operasi FreeNAS secara umum menunjukkan kinerja yang lebih baik dibandingkan dengan NAS4Free[1]. FreeNAS juga mempunyai fitur unggulan yaitu ZFS/Z File System yang digunakan untuk protect, backup dan store data yang aman.

2.3 Sniffer

Sniffer paket atau penganalisa paket yang juga dikenal sebagai Network Analyzers atau Ethernet Sniffer ialah sebuah aplikasi yang dapat melihat lalu lintas data pada jaringan komputer (Pradipta, 2017).

2.4 DNS Poisioning

DNS poisoning merupakan sebuah cara untuk menembus pertahanan dengan cara menyampaikan informasi ip address yang salah mengenai sebuah host, dengan tujuan untuk mengalihkan lalu lintas paket data tujuan sebenarnya.

2.5. Ping Of Death

Penyerang mengirimkan serangkaian paket data ke target yang tidak sesuai ketentuan aturan jaringan. Jika secara terus menerus bisa mengakibatkan jalur koneksi penuh dan berakibat dropnya server karena tidak bisa menampung kebutuhan tersebut (Sada, 2019).

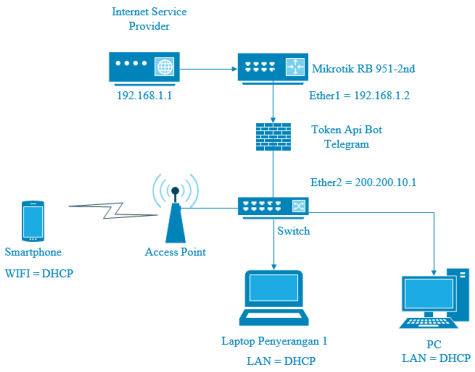
2.6 Quality of Service

Serangan brutal (bahasa Inggris: Brute-force attack) adalah sebuah teknik serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci yang mungkin (Purba & Efendi, 2021).

3. Hasil dan Pembahasan

3.1 Rancangan Topologi dan Konfigurasi Jaringan

1. Topologi Jaringan Uji Coba.



Gambar 1. Topologi Jaringan Uji Coba

2. Konfigurasi Jaringan

Topologi jaringan dengan mikrotik membutuhkan penomoran *ip address* secara detail sehingga akan mempermudah membangun dan mensetting sistem mikrotik untuk menjadi internet *gateway* dan *firewall* dari serangan DDoS. Penomoran *ip address* secara detail dapat dilihat pada tabel berikut:

Tabel 1. Konfigurasi *IP Address* Pada Jaringan Dirancangan

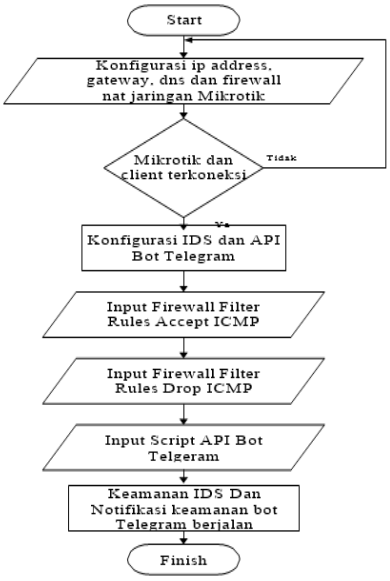
No	*Hardware*/*Software* Network	Port Ethernet	IP
1	ISP	1	Address 192.168.1.1
2	Mikrotik RB 951-2nd	Ether 1	Address 192.168.1.67/24 Gateway 192.168.1.1 Dns-server 192.168.1.1

		Ether 2	Address 192.168.100.1/24
4	Client Terhubung Jaringan Lokal	Port switch	Address 192.168.100.2 - 192.168.100.254 Netmask 255.255.255.0 Gateway 192.168.100.1 DNS *Server* 192.168.100.1

3.2 Rancangan Flowchart Keamanan IDS untuk Ping Flood, Syn Flood, UDP Flood

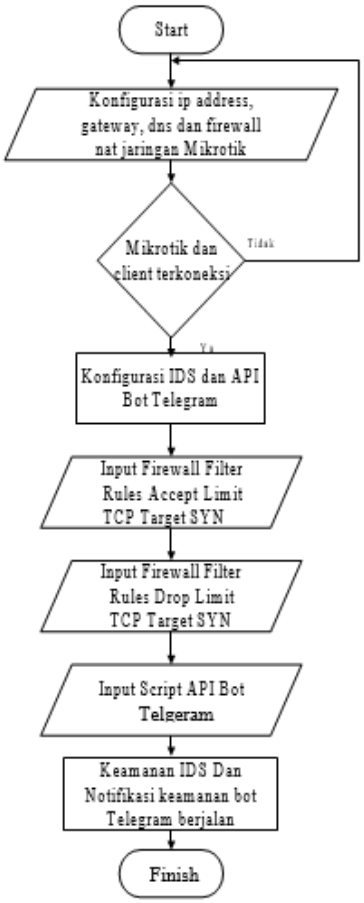
3.2.1 Flowchart Keamanan IDS Untuk Ping Flood

Pada bagian ini akan menggambarkan rancangan sistem kemananan jaringan menggunakan IDS untuk keamanan dari serangan DDoS *volumetric attack* dengan jenis serangan *ping flood* pada mikrotik. Berdasarkan pada gambar dibawah dapat dijelaskan bahwa untuk melakukan pengamanan jaringan, terlebih dahulu melakukan konfigurasi jaringan pada mikrotik, kemudian dilanjutkan dengan konfigurasi IDS dengan *Firewall Filter Rules Accept* protokol ICMP dan *Firewall* Filter *Rules Drop* protokol ICMP serta konfigirasi API bot telegram sehingga kemananan IDS dan notifikasi bot telegram dapat berjalan dapat dilihat gambar dibawah.



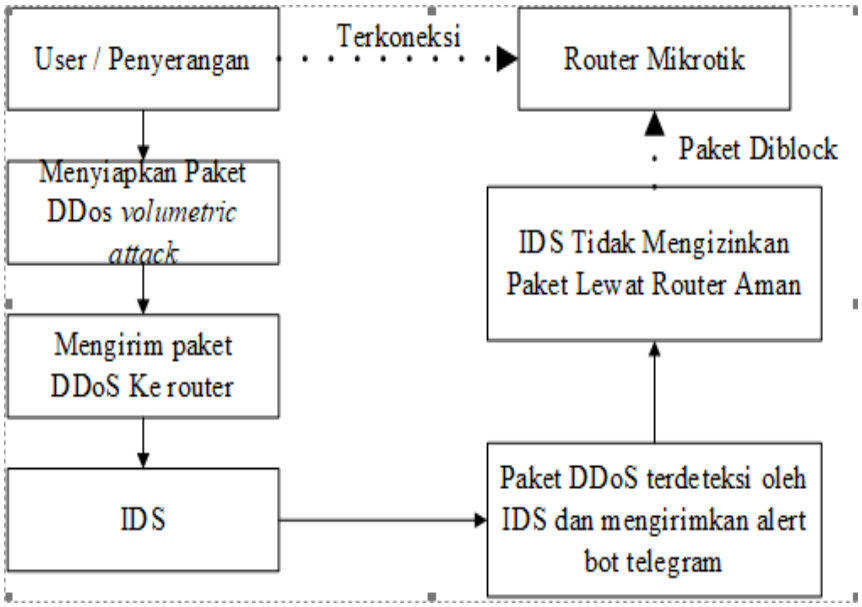
Gambar 2. *Flowchart* Rancangan IDS *Ping Flood*

3.2.2 Flowchart Keamanan IDS Untuk SYN Flood



Gambar 3. Flowchart Keamanan IDS Untuk SYN Flood

3.3 Perancangan Flowchart Skema Penyerangan Meliputi : Ping Flood , SYN Flood , UDP Flood.

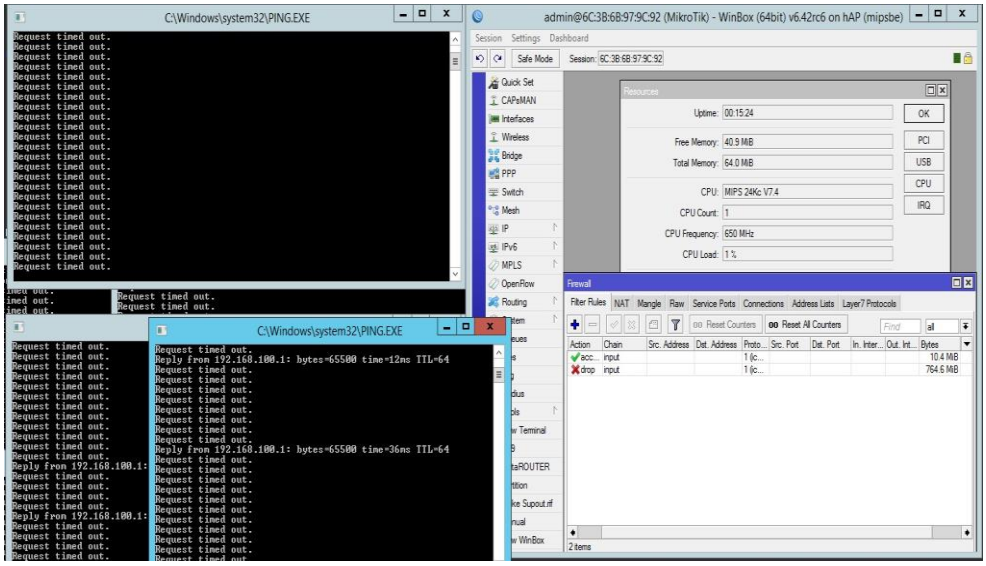


Gambar 4. Skema Penyerangan

Berdasarkan pada gambar 5.Proses serangan dapat terjadi apabila suatu *user* telah terhubung dengan jaringan router, baik melalui media kabel atau nirkabel. Kemudian *user* menyediakan sebuah *tools* penyerangan DDoS *volumetric attack* yang dapat dikonfigurasi untuk mengirimkan paket serangan DDoS *volumetric attack* dengan jenis *ping flood, SYN flood*dan *UDP flood* mengarah ke IP router, router yang memiliki keamanan IDS akan mendeteksi permintaan *user* yang dianggap berlebihan, sehingga IDS tidak akan mengizinkan paketserangan lewat untuk mengenai router, kemudian router mengirimkan pesan peringatan melaluibot telegram kepada *admin* jaringan.

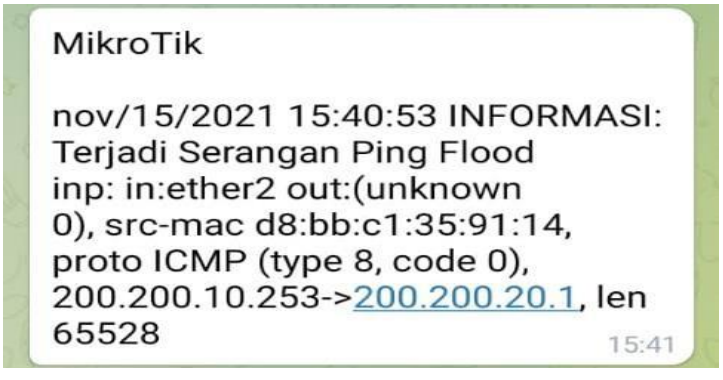
3.4 Pengujian Ping Flood, SYN Flood , UDP Flood Dan Notifikasinya :

3.4.1 Pengujian Ping Flood Dan Notifikasinya



Gambar 5. Pengujian Serangan DDoS *Ping flood*

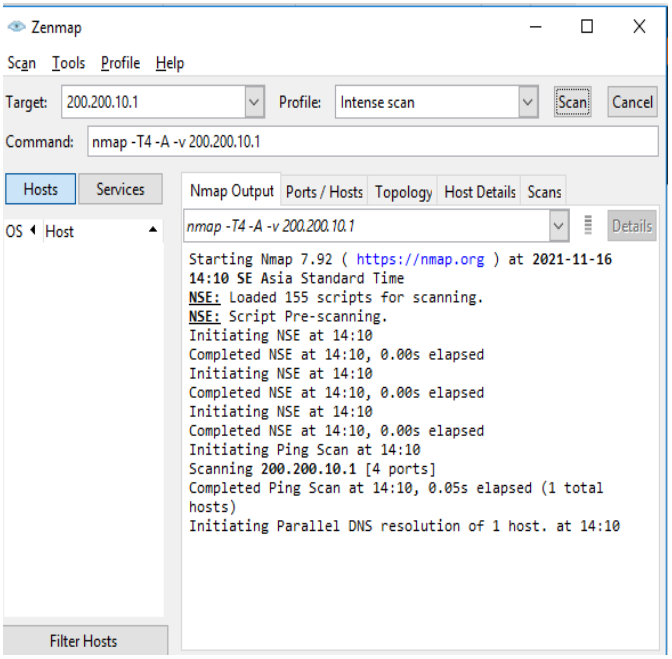
Berdasarkan pada gambar di atas, dapat diterangkan bahwa *firewall* IDS mendeteksi serangan DDoS *pingflood* yang berlebihan sehingga *firewall* IDS melalakukan *blocking* yang dapat dilihat pada tab *Bytesfirewallrules*.



Gambar 6. Notifikasi Serangan DDoS *Ping Flood pada Telegram*

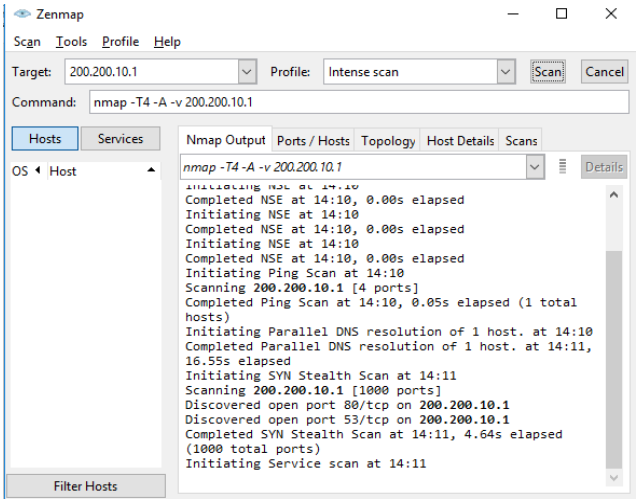
Berdasarkan pada gambar 6 di atas, mikrotik akan mengirimkan pesan informasi kepada Bot @Keamanan-IDS bahwa telah terjadi serangan DDoS *Ping Flood* yangtelah dilakukan oleh *Ip address client* =200.200.10.1. Sehingga proses pengujian notifikasi serangan DDoS *Ping Flood* menggunakan *bot* berhasil dilakukan.

3.4.2 Pengujian SYN Flood Dan Notifikasinya

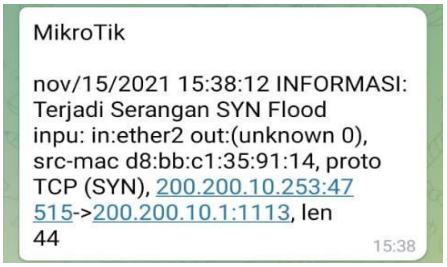


Gambar 7 Masukan IP *Target*

Setelah *Target* telah terisi oleh *IP address*, nmap akan melakukan *scan port* pada Wlan1 mikrotik untuk mendapat kan *port SYN Flood* yang terbuka pada ether2. Berikut adalah tampilan Zenmap yang berusaha melakuan *Port Scanning* ke *Ip addres* ether2 namun akan terjadi delay karena *firewall* yang telah di buat sebelum nya pada *filter rule SYN Flood.*



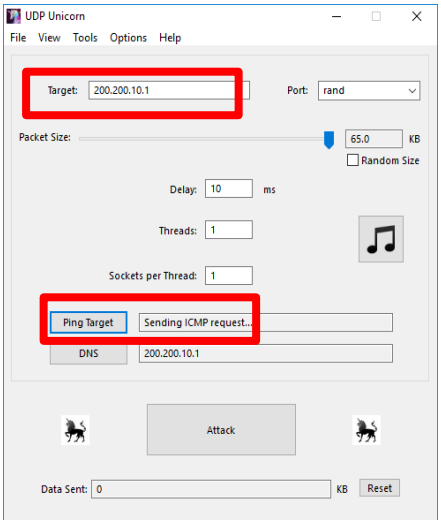
Gambar 8. Pengujian SYN Flood



Gambar 9. Notifikasi Serangan DDoS *SYN Flood*

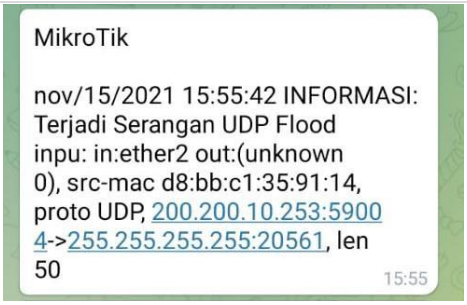
Berdasarkan pada gambar di atas, mikrotik akan mengirimkan pesan informasi kepada Bot @NotifMKRTK bahwa telah terjadi serangan DDoS *SYN Flood* yang telahdilakukan oleh *Ip address client* =200.200.10. 253. Sehingga proses pengujian notifikasi serangan DDoS *SYN Flood* menggunakan *bot* berhasil dilakukan.

3.4.3 Pengujian UDP Flood Dan Notifikasinya



Gambar 10. Pengujian UDP Flood

Untuk melakukan pengujian *UDP Flood* pada penelitian ini, menggunakan aplikasi yang bernama *UDP Unicorn*. Pertama buka aplikasi *UDP Unicorn* yang telah diinstall sebelumnya, selanjutnya isi IP *Target* yang akan dijadikan *Target*, IP DNS dari Google akan menjadi target yang akan di serang menggunakan UDP, lalu atur *Packet size* sampai dengan maksimum, Klik "*Ping Target*" dan "DNS" dan terakhir klik "*Attack*" lalu *UDP Unicorn* akan langsung melakukan *UDP Flooding* pada Target melalui jaringan Mikrotik.



Gambar 12. Notifikasi Serangan DDoS UDP Flood

Setelah dilakukan serangan *UDP Flood*, maka pada sistem mikrotik diketahui bahwa *ip address* yang melakukan *flood UDP* adalah 200.200.10.253 yang menyebabkan lonjakan *upload* yang sangat besar. Selanjutnya ketika terjadi serangan *UDP Flood* pada mikrotik, *script scheduler* yang ada dimikrotik akan mengirimkan notifikasi informasi berupa pemberitahuan telah terjadi yang dilihat pada gambar diatas.

4. KESIMPULAN

Setelah dilakukannya pengujian jaringan serangan DDoS, maka penulis dapat menarik kesimpulan sebagai berikut:

1. Optimalisasi keamanan mikrotik *routerboard* berhasil dilakukan dengan metode IDS dapat melakukan blocking terhadap serangan DDOS.
2. Adanya IDS tersebut memberi dampak antara lain, mampu mendeteksi serangan DDOS dan memberikan notifikasi kepada administrator berupa bot telegram.

REFERENSI ()

[1] Ginting, A. L. T., Napitupulu, J., & Jamaluddin. (2015). Sistem Monitoring Pendeteksian Penyusup Menggunakan Snort pada Jaringan Komputer Fakultas Ekonomi Universitas Methodist Indonesia. *Seminar Nasional Teknologi Informasi & Komunikasi (SNASTIKOM) 2015*, 83–87.Universitas Harapan Medan.

[2] Gong, D., Tran, M., Shinde, S., Jin, H., Sekar,V., Saxena, P., & Kang, M. S. (2019). Practical verifiable in-network filtering for DDoS defense. *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, 1161–1174. https://doi.org/10.1109/ICDCS.2019.00118

[3] Sutarti, Pancaro, A. P., & Saputra, F. I. (2018).Implementasi IDS (Intrusion Detection System) pada Sistem Keamanan Jaringan Sman 1 Cikeusal. *PROSISKO: Jurnal Pengembangan Riset Dan Observasi Sistem Komputer*, *5*(1), 1–8.

[4] Sada, A. (2019). *Notifikasi Keamanan Layanan SSH pada Mikrotik Menggunakan SMS*. Universitas Mercu Buana.

[5] Purba, W. W., & Efendi, R. (2021). Perancangan dan analisis sistem keamanan jaringan Komputer menggunakan SNORT. *AITI*, *17*(2), 143–1https://doi.org/10.24246/aiti.v17i2.143-158

[6] Pradipta, Y. W. (2017). Implementasi Intrusion Prevention System(IPS) Menggunakan Snort Dan IP Tables Berbasis Linux. *Jurnal Manajemen Informatika*, *7*(1).

[7] Ketaren, E. (2016). Cybercrime, Cyber Space, dan Cyber Law. *Jurnal Times*, *5*(2), 35– 42.

[8] Hendarsyah, D. (2012). Keamanan Layanan Internet Banking Dalam Transaksi Perbankan. *IQTISHADUNA: Jurnal* Hendarsyah, D. (2012). Keamanan Layanan Internet Banking Dalam Transaksi Perbankan. *IQTISHADUNA: Jurnal Ilmiah Ekonomi Kita*, *1*(1), 12–33. https://doi.org/10.46367/iqtishaduna.v1i1. 2