(2024), 2 (11): 229-244 Scientica 3021-8209
Jurnal Ilmiah Sain dan Teknologi

IMPLEMENTASI PENCEGAHAN SERANGAN *DDOS* PADA *ROUTER* MIKROTIK MENGGUNAKAN METODE *ETHICAL HACKING*

Fajri Adietya Kushaeiri [1], Yusuf Muhyidin [2], Dayan Singasatia [3]
Program Studi Teknik Informatika S1, Fakultas Teknik,
Sekolah Tinggi Teknologi Wastukancana
Jl. Cikopak No.53, Sadang, Purwakarta, Jawa Barat, Indonesia

Abstrak (Indonesia)
Pada jaringan komputer perangkat yang memiliki kerentanan adalah *router*. *Router* merupakan perangkat paling luar yang menghubungkan *Local Area Network* (LAN) dengan internet sehingga dapat dengan mudah diserang oleh pihak yang tidak bertanggung jawab. Serangan yang umum dilakukan adalah *Distributed Denial-of-Service* yaitu serangan *cyber* yang dapat dengan mudah menyerang server maupun *router* pada mikrotik, dan bertujuan untuk mematikan target dengan cara memadati jalur data dengan paket yang illegal, secara serempak. Kemudian metode yang akan dipakai pada masalah kerentatan dari serangan *cyber* akan menggunakan metode *Ethical Hacker*, yaitu suatu aktifitas melakukan penetrasi ke suatu sistem, jaringan, dan aplikasi dengan cara mengkesploitasi kelemahan dengan maksud untuk mendapatkan hak akses atas data dan sistem, tujuanya adalah membantu perusahaan menguji keamanan system dan jaringan yang mereka miliki. Penelitian ini bertujuan untuk memberikan solusi atau alternatif pencegahan terjadinya serangan terhadap perangkat *router* mikrotik terutama terhadap serangan *DDoS* melalui peningkatan keamanan perangkat *router* dari segi *software* dan *hardware*. Penelitian kali ini menyimpulkan bahwa router mikrotik pada Perusahaan Zilenial.id belum ada system keamanan yang dapat mencegah serangan khususnya serangan DDoS. Beberapa port yang terbuka pada mikrotik diduga menjadi salah satu alasan perangkat mikrotik bisa diserang oleh DDoS. Langkah-langkah pada *exploitation* dan *maintaining acces* membantu dalam meningkatkan keamanan *firewall* perangkat mikrotik pada Perusahaan zilenial.id.

Sejarah Artikel
Submitted: 16 Juli 2024
Accepted: 19 Juli 2024
Published: 26 Juli 2024

Kata Kunci
Jaringan Komputer, *DDoS*, *Ethical Hacking*, *Router* Mikrotik

Abstract (English)
In computer networks, routers are highly vulnerable devices due to their strategic position connecting the Local Area Network (LAN) to the internet. This vulnerability makes routers easy targets for cyberattacks, one of which is Distributed Denial-of-Service (DDoS) attacks. A DDoS attack aims to incapacitate the target by flooding the data path with illegal packets simultaneously, which can cause disruptions to both servers and routers. The method employed to address this vulnerability to cyberattacks is Ethical Hacking, an activity that involves penetrating systems, networks, and applications by exploiting weaknesses to gain access to data and systems. The objective is to help companies test the security of their systems and networks. This research aims to provide solutions or alternatives to prevent attacks on Mikrotik routers, especially DDoS attacks, by enhancing the security of the routers both in terms of software and hardware. This research concludes that the Mikrotik routers at Zilenial.id have no security systems in place to prevent attacks, particularly DDoS attacks. Several open ports on the Mikrotik routers are suspected to be one of the reasons these devices are susceptible to DDoS attacks. Steps taken in exploitation and maintaining access help improve the firewall security of the Mikrotik routers at Zilenial.id.

Article History
Submitted: 16 Juli 2024
Accepted: 19 Juli 2024
Published: 26 Juli 2024

Key Words
Computer Networks, DDoS, Ethical Hacking, Mikrotik Route

1. Latar Belakang

Media internet sudah menjadi bagian kehidupan manusia untuk keperluan komunikasi dengan skala besar dalam kemajuan teknologi. Layanan internet untuk perusahaan, instansi pemerintahan, perkantoran, universitas dll, lebih dominan menggunakan jaringan komputer berbasis *Local Area Network* dan *Wireless Local Area Network* untuk penunjang komunikasi

antar komputer. Topologi yang sering diterapkan pada LAN dan WLAN adalah topologi start dengan satu titik terpusat device, lebih seringnya menggunakan *device router*. (Jaya et al., 2020)

Pada jaringan komputer perangkat yang memiliki kerentanan adalah *router*. *Router* merupakan perangkat paling luar yang menghubungkan *Local Area Network* (LAN) dengan internet sehingga dapat dengan mudah diserang oleh pihak yang tidak bertanggung jawab. (Haeruddin, 2021). Ukuran kinerja router sangat diperlukan untuk memadai kapasitas pengguna dengan pengiriman data yang begitu banyak, dan apabila terlalu banyak permintaan data dari user, akan terjadi Flood data atau kebanjiran data baik melalui transmisi Internet Protocol (IP) address atau mac address. (Hendrawan et al., 2016)

Serangan yang umum dilakukan adalah *Distributed Denial-of-Service* yaitu serangan *cyber* yang dapat dengan mudah menyerang server maupun router pada mikrotik, dan bertujuan untuk mematikan target dengan cara memadati jalur data dengan paket yang illegal, secara serempak. Dampak serangan *DDoS* cukup membebani dan sangat menggangu kinerja sistem dan aktifitas pengguna. 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 kinerja sebuah sistem.

Dan metode yang akan dipakai pada masalah kerentatan dari serangan *cyber* akan menggunakan metode *Ethical Hacker*, yaitu suatu aktifitas melakukan penetrasi ke suatu sistem, jaringan, dan aplikasi dengan cara mengkesploitasi kelemahan dengan maksud untuk mendapatkan hak akses atas data dan sistem, tujuanya adalah membantu perusahaan menguji keamanan system dan jaringan yang mereka miliki.(Muhyidin et al., 2020). Kemudian didapatkan karakteristik dari berbagai macam serangan pada Mikrotik berupa *Common Vulnerabilities and Exposures (CVE), DNS redirection, Brute-Force Attacks, Point-to-Point Tunneling Protocol, Distributed Denial-of-Service*. (Jaya et al., 2020).

Penelitian ini bertujuan untuk memberikan solusi atau alternatif pencegahan terjadinya serangan terhadap perangkat *router* mikrotik terutama terhadap serangan *DDoS* melalui peningkatan keamanan perangkat *router* dari segi *software* dan *hardware*. Sehingga instansi yang menggunakan perangkat *router* mikrotik dalam aktivitas operasionalnya dapat terhindar dari kerugian material dan nonmaterial akibat kondisi jaringan router yang *down* karena serangan dari orang yang tidak bertanggung jawab.

2. Kajian Pustaka

2.1 Jaringan Komputer

Jaringan komputer adalah jaringan yang memungkinkan antar komputer untuk saling berkomunikasi dengan bertukar data, perangkat lunak komputer sampai dengan aplikasi. Dengan adanya jaringan komputer ini menjadikan penggunaanya bisa berinteraksi atau berkomunikasi dengan pengguna lain. Dalam jaringan komputer tentu ada pihak-pihak yang terkait. Pihak penerima layanan disebut dengan klien (*client*) dan pemberi layanan disebut peladen (*server*). Pada desain yang satu ini biasanya dikenal dengan sistem *client-server*. Menurut Kamus Besar Bahasa Indonesia (KBBI), jaringan komputer adalah sekelompok komputer dan perangkat terkait yang dihubungkan dengan fasilitas komunikasi. [1].

2.2 Keamanan Jaringan

Keamanan jaringan adalah salah satu proses untuk mencegah dan memonitoring penggunaan jaringan yang tidak sah dari jaringan komputer. Tujuannya yaitu untuk mengantisipasi resiko jaringan komputer berupa bentuk ancaman fisik maupun *logic* baik

[1] putri Kurniawati, *No Title□□□□□□□□ □□□□□□□□□□. □□□□□ □□□□□ □□□ □□□□ «□□□□□□□□ □□*, *Universitas Nusantara PGRI Kediri*, 2017, 01.

langsung ataupun tidak langsung mengganggu aktivitas yang sedang berlangsung dalam jaringan komputer. Sistem keamanan *firewall* tidaklah cukup untuk meminimalkan terjadinya serangan terhadap suatu jaringan komputer. Banyak serangan yang terjadi pada jaringan komputer dapat diketahui setelah adanya kejadian-kejadian yang aneh pada jaringan. Para *administrator* jaringan tidak bisa mengetahui dengan pasti apa yang sedang terjadi, sehingga dibutuhkan waktu yang cukup lama untuk diatasi. [2].

2.3 *Routerboard* Mikrotik

Router mikrotik adalah sistem operasi berbasis *Linux* yang digunakan untuk menjadikan PC berbasis *Intel* atau *AMD* (*personal computer*) mampu melakukan beberapa fungsi di dalamnya yaitu *router*, *bridge*, *firewall*, pengaturan *bandwidth*, *wireless Access Point* atau *Client* & fungsi *networking* serta beberapa fungsi *server* .Mikrotik berfungsi sebagai pengatur aliran data yang terdapat pada jaringan local area, selain itu MikroTik dapat juga berfungsi sebagai *firewall*. [3].

2.4 *Winbox*

Winbox adalah sebuah *utility* yang digunakan untuk melakukan *remote* ke *server* mikrotik kita dalam mode GUI. Jika untuk mengkonfigurasi mikrotik dalam *text mode* melalui PC itu sendiri, maka untuk mode GUI yang menggunakan winbox ini kita mengkonfigurasi mikrotik melalui komputer client. [4]

2.5 *Kalilinux*

Kalilinux adalah satu sistem operasi yang sering digunakan dalam melakukan *penetration testing* serta untuk audit keamanan jaringan computer dari keluarga *Linux* sistem lanjut yang kembangkan oleh *offensive Security*. (Yusnanto et al., 2022)

2.6 DDoS Attack

Serangan *Distributed Denial of Services (DDoS)* terus menjadi salah satu ancaman paling menantang ke *Internet*. Intensitas dan frekuensi erangan ini meningkat dengan kecepatan yang mengkhawatirkan. Peningkatan level serangan *DoS* dengan melakukan pengubahan pada data *size* yang dikirimkan ke target *DoS* menyebabkan *router* yang dilewatinya mengalami peningkatan konsumsi daya listrik dan beban kerja *CPU* . (Jaya et al., 2020)

2.7 *Tools DDos*

1.*LOIC* (*Low Orbit Ion Canon*) merupakan sebuah tool atau aplikasi yang berfungsi untuk melumpuhkan server sebuah situs website dengan mengirimkan packet sebanyak mungkin sesuai dengan kemauan si penyerang ke komputer server yang ditujuh melalui domain atau ip server komputer target. [5]. Bentuk penyerangan tujuan dimana *Loic* sebagai *tools attacking* adalah sebelum penyerangan model sistem penyerangan yang bersifat sistem *Open Source* yang dijalankan dengan membuka domain IP yang dituju sehingga keluarlah *port-port* yang terbuka yang akan diserang dengan menggunakan *DDoS* pada *tools* sebagai *attakcing* untuk *meflooding* dengan jumlah paket yang akan diserang pada

[2] Asep Fauzi Mutaqin, 'Rancang Bangun Sistem Monitoring Keamanan Jaringan Prodi Teknik Informatika Melalui SMS Alert Dengan Snort', *Jurnal Sistem Dan Teknologi Informasi*, 1.1 (2016), pp. 1–6 <https://jurnal.untan.ac.id/index.php/justin/article/view/12537/11376>.

[3] Ummu Radiyah, 'Optimalisasi Keamanan Wide Area Network (WAN) Menggunakan Raw Firewall Berbasis Mikrotik Pada PT. Permata Graha Nusantara', *INTI Nusa Mandiri*, 17.1 (2022), pp. 16–23, doi:10.33480/inti.v17i1.3401.

[4] Didi Susianto, 'Implementasi Queue Tree Untuk Manajemen Bandwidth Menggunakan Router Board Mikrotik', *Jurnal Cendikia Vol 12No. 1Cendikia 2016 ISSN: 0216-9436 Bandar Lampung, April 2016*, 12.1 (2019), pp. 1–8.

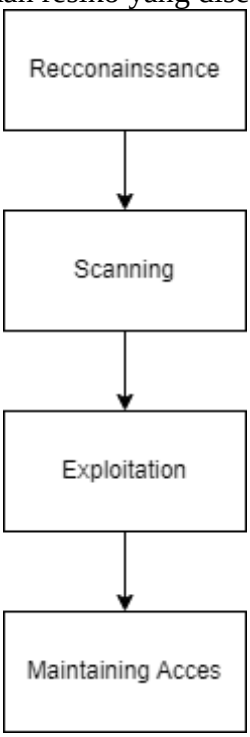
[5] Rusydi Umar and Agus Prasetyo Marsaid, 'Analisis Keamanan Jaringan LAN Terhadap Kerentanan Jaringan Ancaman DDoS Menggunakan Metode Penetration Testing', *Jurnal Riset Komputer)*, 10.1 (2023), pp. 2407–389, doi:10.30865/jurikom.v10i1.5835.

target. Bentuk penyerangan tujuan dimana *Loic* sebagai *tools attacking* adalah sebelum penyerangan model sistem penyerangan yang bersifat sistem *Open Source* yang dijalankan dengan membuka domain IP yang dituju sehingga keluarlah *port-port* yang terbuka yang akan diserang dengan menggunakan *DDoS* pada *tools* sebagai *attakcing* untuk *meflooding* dengan jumlah paket yang akan diserang pada target. [6].

2. *Slowloris* merupakan serangan DDoS dengan bandwith rendah sehingga pada filtering tidak terlalu kelihatan dalam volume jumlah paket dan bekerja pada protokol HTTP sehingga serangan Slowloris dari sebuah komputer diduga sangat dapat melumpuhkan web server. Slowloris membuka koneksi secara pada berulang melalui header HTTP. Slowloris bekerja pada protokol HTTP dan PoD bekerja pada protokol ICMP yang terakurasi pada jaringan berbasis lokal dan luas. [7].

2.8 *Ethical Hacking*

Ethical Hacking merupakan suatu aktifitas melakukan penetrasi ke suatu sistem, jaringan, dan aplikasi dengan cara mengkesploitasi kelemahan dengan maksud untuk mendapatkan hak akses atas data dan *system*. *Ethical Hacker* sangat diperlukan oleh perusahaan yang ingin menguji sistem yang dimiliki untuk diekploitasi dan dicari *vulnerability* nya sehingga ditemukan resiko yang disebabkan dari *vulnerability* tersebut.



Gambar 1 Alur Ethical Hacking

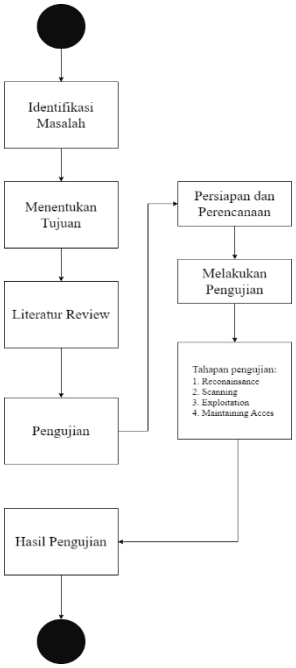
[6] Sri Suharti, Anton Yudhana, and Imam Riadi, 'Forensik Jaringan DDoS Menggunakan Metode ADDIE Dan HIDS Pada Sistem Operasi Proprietary', *MATRIK : Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer*, 21.3 (2022), pp. 567–82, doi:10.30812/matrik.v21i3.1732.

[7] Suharti, Yudhana, and Riadi.

3. Metode

3.1 Kerangka Penelitian

Adapun kerangka penelitian yang akan dilaksanakan terdapat di gambar 2 sebagai berikut:



Gambar 2 Kerangka Penelitian

3.4 Identifikasi Masalah

Identifikasi masalah merupakan proses mengidentifikasi permasalahan yang akan dijadikan fokus pada penelitian. Masalah yang menjadi fokus pada penelitian ini adalah penanganan celah keamanan pada Mikrotik.

3.5 Menentukan Tujuan

Menentukan tujuan adalah langkah yang sangat penting dalam proses penelitian. Tujuan penelitian ini adalah menentukan target yang akan menjadi objek keamanan, menganalisis celah keamanan pada mikrotik

3.6 Literatur *Review*

Literatur *Review* adalah sebuah proses mencari, mengevaluasi dan menyatukan sumber-sumber informasi yang relevan dengan topik penelitian. Studi literatur dapat mengarahkan penelitian dalam menyusun kerangka penelitian yang jelas dan terarah sehingga penelitian memiliki referensi yang jelas dalam pemecahan masalahnya.

3.7 Pengujian

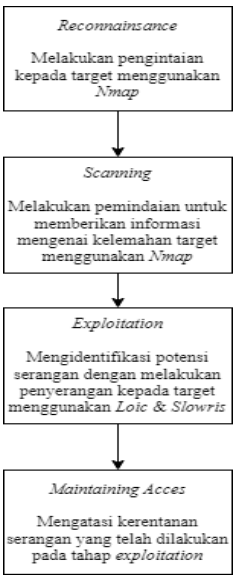
Pada fase ini akan melakukan pengujian pada mikrotik dengan 2 fase yang akan dilakukan uji coba antara lain :

3.7.1 Persiapan dan Perencanaan

Pada tahap ini yaitu mempersiapkan sistem keamanan yang akan menjadi sasaran penelitian ini. Setelah mempersiapkan sistem keamanan serta alat yang akan digunakan, maka dilakukan penyusunan rencana untuk pengujian dari sistem keamanan tersebut.

3.7.2 Melakukan Pengujian

Sebelum melakukan pengujian peneliti membuat alur pengujian dan terdapat beberapa fase yang akan digunakan sebagaimana gambar berikut:



Gambar 3 Alur Penyerangan

1. *Recconaissance*

   Tahapan ini menggunakan *tools nmap* untuk melakukan pengintaiann dan mendapatkan informasi mengenai jaringan internet yang akan diserang.

2. *Scanning*

   Pada scanning menggunakan *tools nmap* untuk mengidentifikasi *port* apa saja yang terbuka di target, yang dapat mengindikasikan layanan atau aplikasi yang berjalan.

3. *Exploitation*

   Pada tahapan ini menggunakan *tools LOIC* dan *Slowloris* untuk mengekploitasi kelemahan pada jaringan internet atau sistem.

4. *Maintaining Access*

   Pada tahapan ini akan mengatasi kerentanan serangan *DDOS* dan menjaga *router* mikrotik agar tidak dapat di ekploitasi kembali oleh serangan *DDOS*.

3.9 Hasil Pengujian

Setelah semua tahapan selesai, selanjutnya akan dilakukan pengujian kembali pada router mikrotik untuk mencegah terjadinya serangan DDoS pada masa mendatang.

4. Hasil dan Pembahasan

4.1 Hasil Pengumpulan Data

Dalam penelitian kali ini , peneliti melakukan pengumpulan data dengan metode kualitatif dengan cara identifikasi masalah, menentukan tujuan, dan studi literatur. Dan pengujian menggunakan metode *ethical hacking*. Berikut ini adalah hasilnya:

4.2 Identifikasi Masalah

Identifikasi masalah mengenai serangan *DDoS (Distributed Denial of Service)* terhadap perangkat MikroTik melibatkan analisis terhadap berbagai aspek yang berkaitan dengan mencari kerentanan, serta mitigasi serangan. Dari identifikasi masalah yang telah diteliti, ditemukan masalah utamanya yaitu pencegahan serangan *DDoS* pada zilenial.id menggunakan metode *ethical hacking*.

4.3 Menentukan Tujuan

Menentukan tujuan objek yang akan menjadi penelitian, pada tahap ini terdapat tujuan yang akan menjadi objek penelitian yaitu mikrotik rb750r yang berada di Zilenial.id sebagai sasaran yang akan dilakukan *exploitation*.

4.4 Literatur *Review*

Hasil dari literatur *Review* yang peneliti lakukan untuk memperkuat penelitian ini adalah dengan mencari referensi mengenai konsep dan teknik dari buku, jurnal, maupun tugas akhir mengenai penyerangan *DDoS* menggunakan metode *ethical hacking*.

4.5 Pengujian

Pada tahap pengujian ini menggunakan metode *ethical hacking* untuk melakukan pengujian dan pencegahan keamanan pada mikrotik. Berikut merupakan hasil dari pengujian:

4.5.1 *Recconainssance*

Berikut merupakan kebutuhan yang diperlukan dalam melakukan penelitian:

1). Lokasi Penelitian

Pada penelitian kali ini berlokasi di Zilenial ID, yaitu sebuah Perusahaan yang bergerak di bidang digital marketing, dan bertempat di Kabupaten Purwakarta Kecamatan Jatiluhur.

2). Identitas Perangkat yang di Uji

Mikrotik *rb750r*

Mikrotik rb750r ini dilengkapi dengan jumlah 1 CPU dan berkapasitas 64 MB serta memiliki 5 *port fast ethernet* 10/100 Mbps. Dengan lima *port Fast Ethernet*, router ini mampu menghubungkan berbagai perangkat sekaligus dan mendistribusikan *bandwidth* dengan efektif. Dengan ukurannya yang kecil dan ringan, RB750r2 mudah dipasang dan tidak memakan banyak ruang. Ini sangat cocok untuk instalasi di tempat dengan ruang terbatas. Kemudian ada beberapa spesifikasi lainnya yaitu:

a. Ip addreess: 192.168.100.22
b. Layanan yang berjalan dan port yang terbuka

Tabel 1

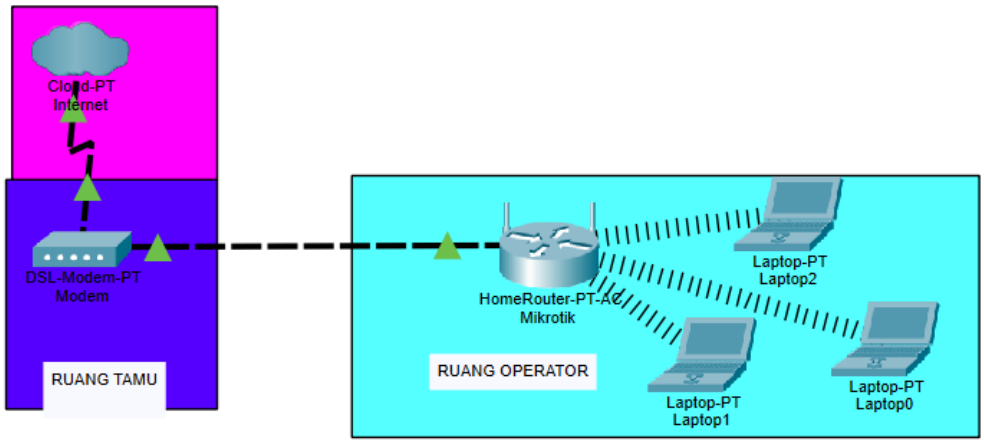
Port	*Status*	*service*
21	*Open*	*ftp*
22	*Open*	*Ssh*
23	*Open*	*telnet*
53	*Open*	*Domain*
80	*Open*	*http*
2000	*Open*	*Cisco-sccp*
8291	*Open*	*unknowm*

3). Topologi Penelitian

Pada topologi yang ada pada tempat yang sedang dilakukan penelitian terdapat beberapa perangkat, diantaranya yaitu ada:

a. Modem wifi
b. Router mikrotik
c. Laptop

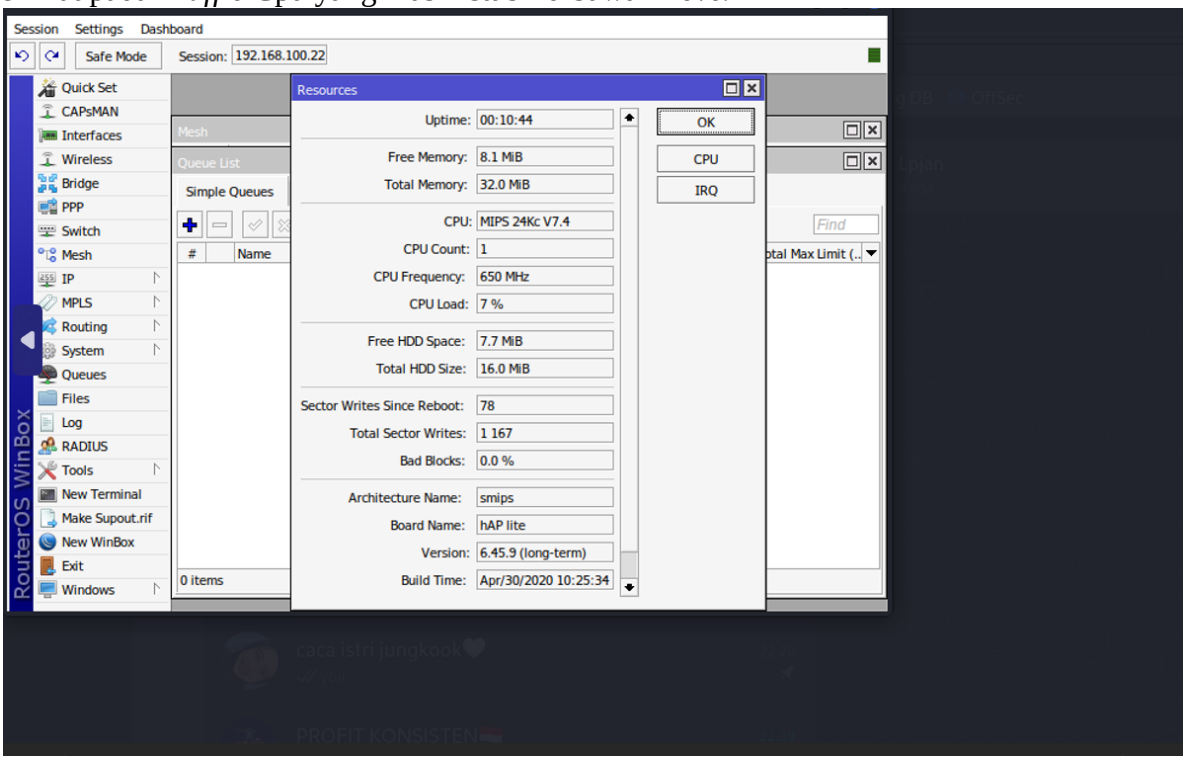
(2024), 2 (11): 229-244 Scientica 3021-8209
Jurnal Ilmiah Sain dan Teknologi



Gambar 4 Topologi

4.5.2 *Scanning*

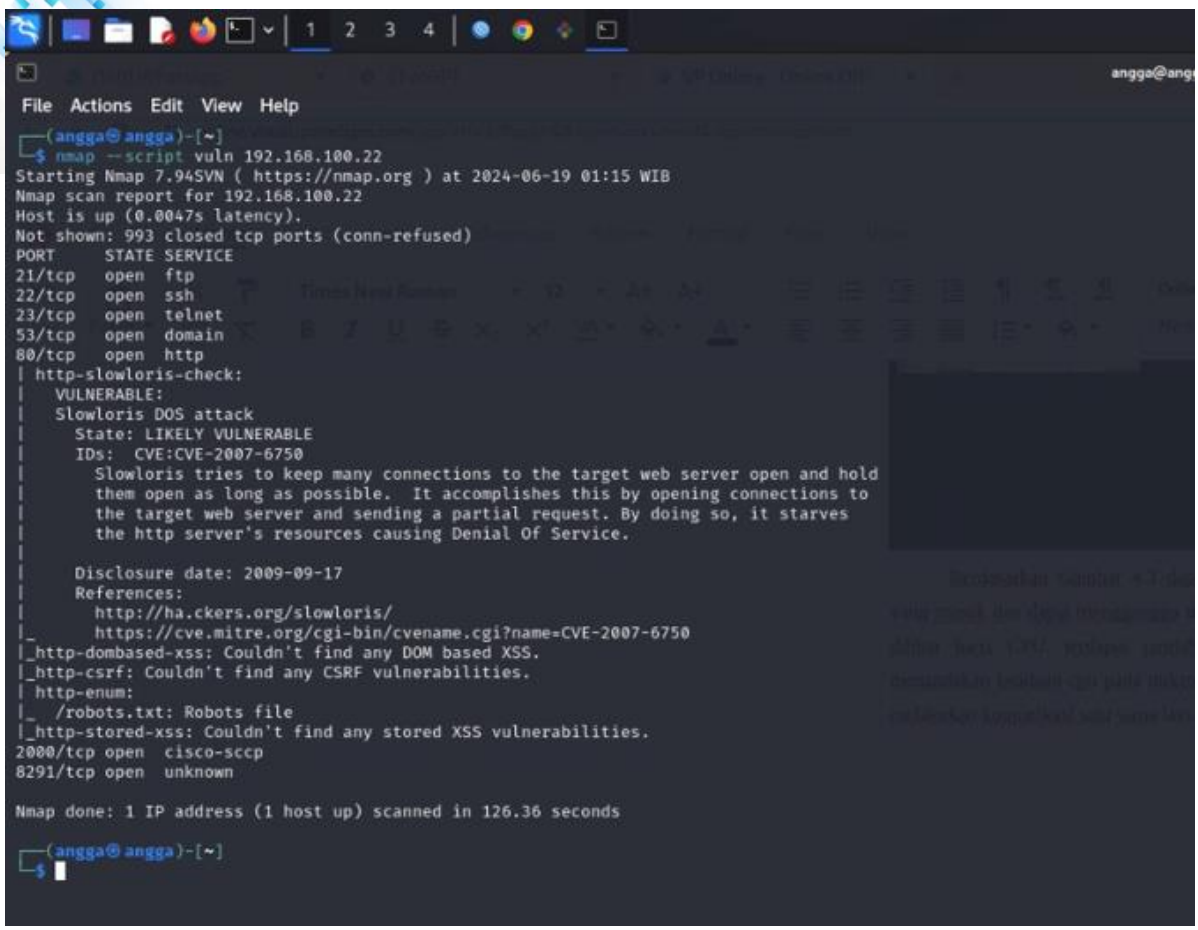
Proses pertama untuk mengetahui apakah *router* masih dalam keadaan normal atau ada serangan DDoS, dapat dilakukan melalui pengecekan pada menu *WinBox* yaitu melalui menu *Resources*. Setelah dilakukan pengecekan, diketahui belum ada serangan masuk DDoS, hal ini terlihat pada *Traffic* Cpu yang masih stabil dibawah 10%.



Gambar 5 Cek Kondisi CPU

Berdasarkan Gambar 5 dapat disimpulkan belum terjadinya serangan yang masuk dan dapat mengganggu *traffic* jaringan. Hal ini terlihat Hal ini dapat dilihat baris CPU, terdapat jumlah CPU load yang masih dibawah 10% menandakan keadaan cpu pada mikrotik masih dalam keadaan normal dan dapat melakukan komunikasi satu sama lain.

Langkah lain untuk mengetahui apakah router dalah keadaan normal atau sudah diserang dapat dilakukan dengan pengecekan menggunakan perintah nmap –script vuln 192.168.100.22



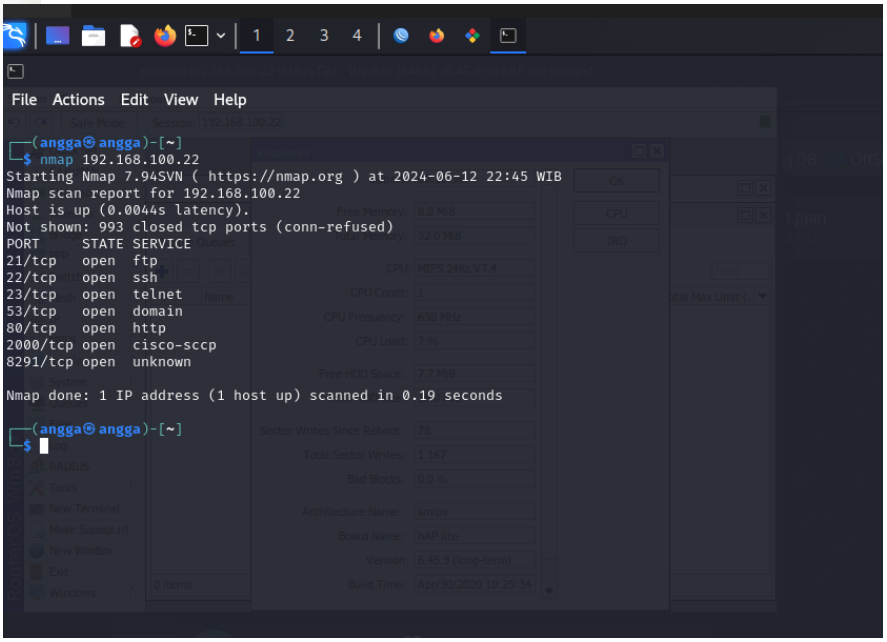
Gambar 6 Scanninng Port vuln

Dapat dlihat bahwa keadaan mikrotik belum terdapat serangan, namun pada port http diduga terdapat kerentanan terhadap serangan slowloris. Berikut adalah tahapan scaning pada mikrotik:

1). Melihat *Port Open* Pada Mikrotik

Nmap (*Network Mapper*) adalah alat *open-source* yang digunakan untuk eksplorasi jaringan dan audit keamanan. Salah satu fitur utamanya adalah kemampuan untuk melakukan port scanning, yaitu proses untuk mendeteksi *port* yang terbuka, tertutup, atau terfilter pada sistem target. Informasi ini sangat berguna untuk memahami layanan yang berjalan pada suatu sistem dan potensi kerentanannya.

Pada proses kali ini, melakukan scanning pada ip mikrotik dengan ip 192.168.100.22 dengan perintah nmap <ip target>. Dapat dilihat dari gambar berikut.

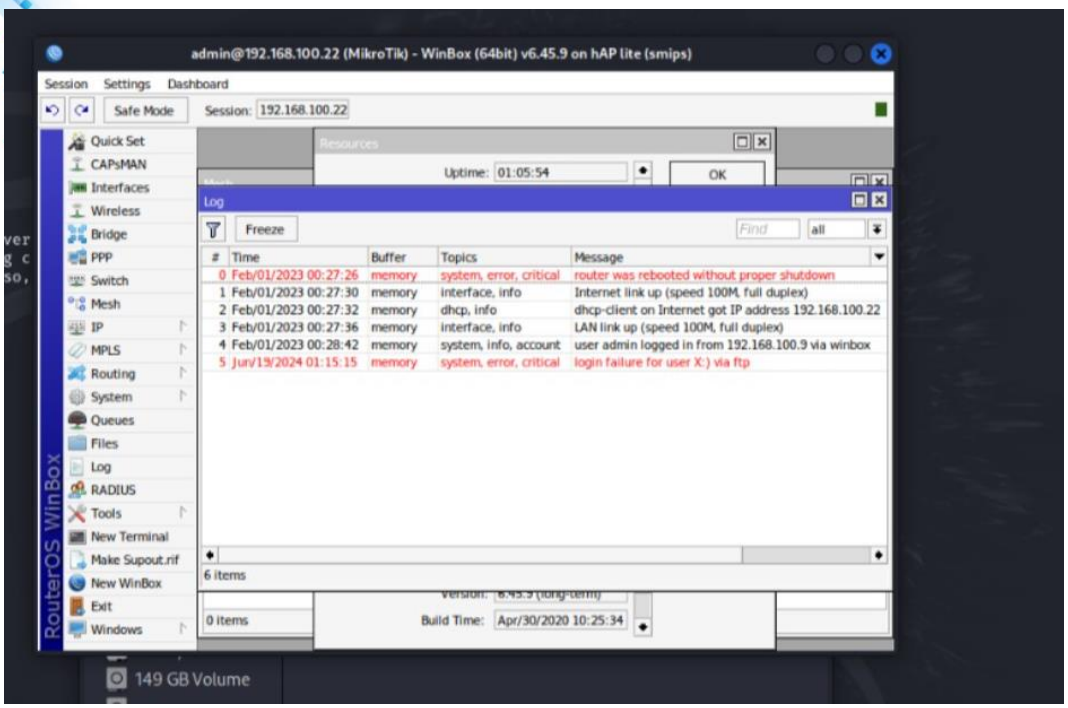


Gambar 7 Scanning Nmap port

Hasil dari perintah Nmap memberikan informasi rinci mengenai target yang dipindai. Dapat dilihat bahwa perintah nmap dapat mengetahui *port* yang terbuka di mikrotik.

2). *Log_Activity*

Log aktivitas adalah catatan atau rekaman yang berisi informasi detail tentang berbagai kejadian atau aktivitas yang terjadi dalam sistem komputer, jaringan, atau aplikasi. Log ini mencatat berbagai jenis aktivitas seperti *login* pengguna, akses file, permintaan jaringan, perubahan konfigurasi, dan kesalahan system, dan mempunyai fungsi untuk Melacak aktivitas pengguna untuk memastikan tidak ada tindakan mencurigakan atau pelanggaran kebijakan keamanan.

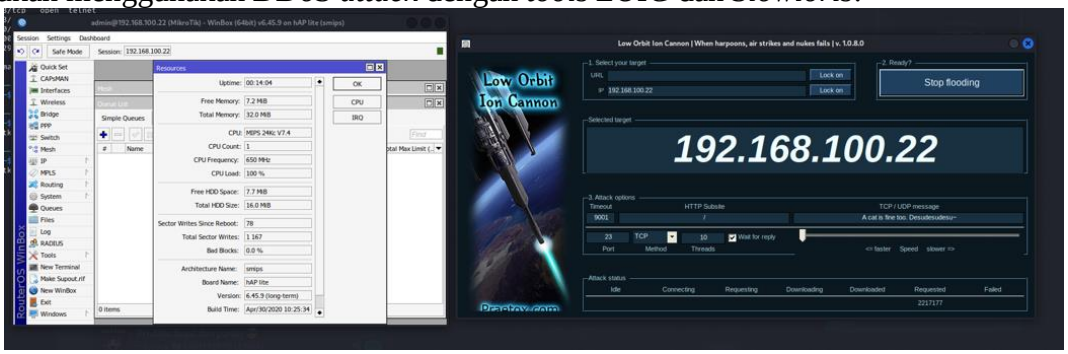


Gambar 8 Log Activity

Pada gambar 8. terlihat bahwa terdapat kegiatan yang mencurigakan sehingga membuat *router reboot* dengan sendirinya dan pengguna kesulitan dalam melakukan *login*. Hal ini disebabkan sudah ada orang yang melakukan penyerangan kepada mikrotik.

4.5.3 *Exploitation*

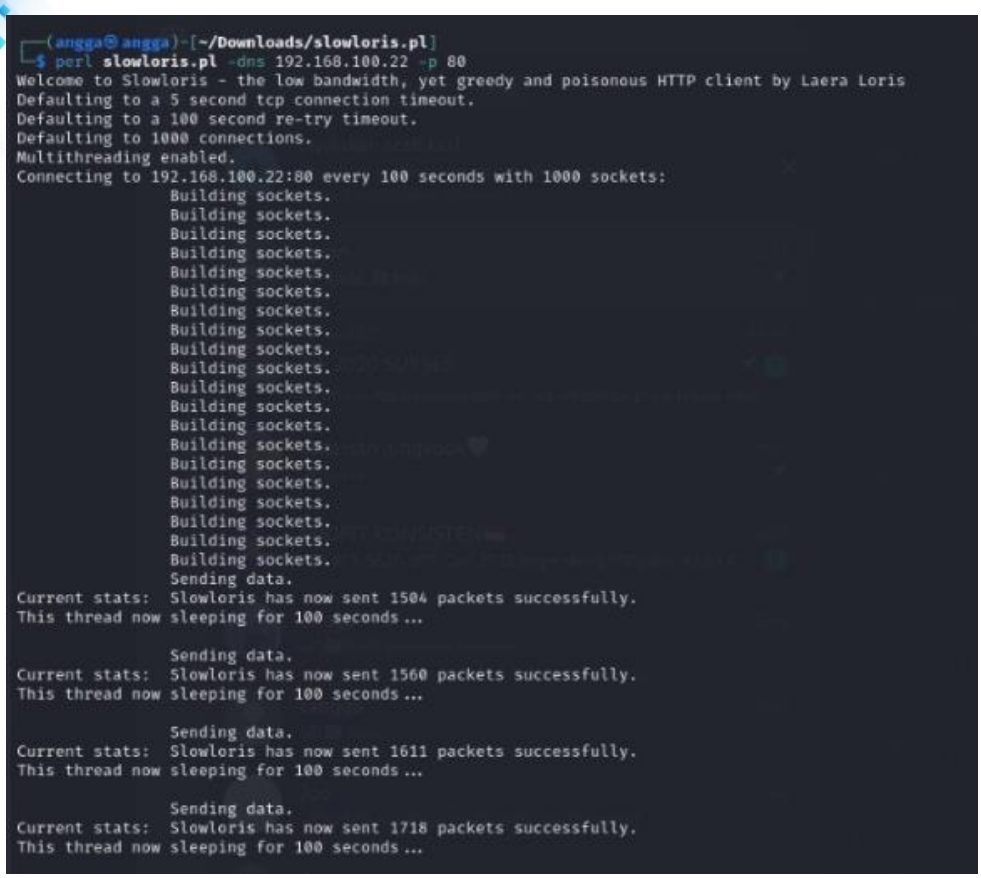
Eksploitasi DDoS (*Distributed Denial of Service*) adalah serangan siber di mana penyerang berusaha untuk membuat suatu layanan, situs web, atau jaringan tidak dapat diakses oleh pengguna yang sah. Hal ini dilakukan dengan cara membanjiri target dengan lalu lintas internet yang sangat besar dari berbagai sumber. Berikut merupakan contoh exploitation yang dilakukan menggunakan *DDoS attack* dengan *tools LOIC* dan *Slowloris*:



Gambar 9 Serangan Loic

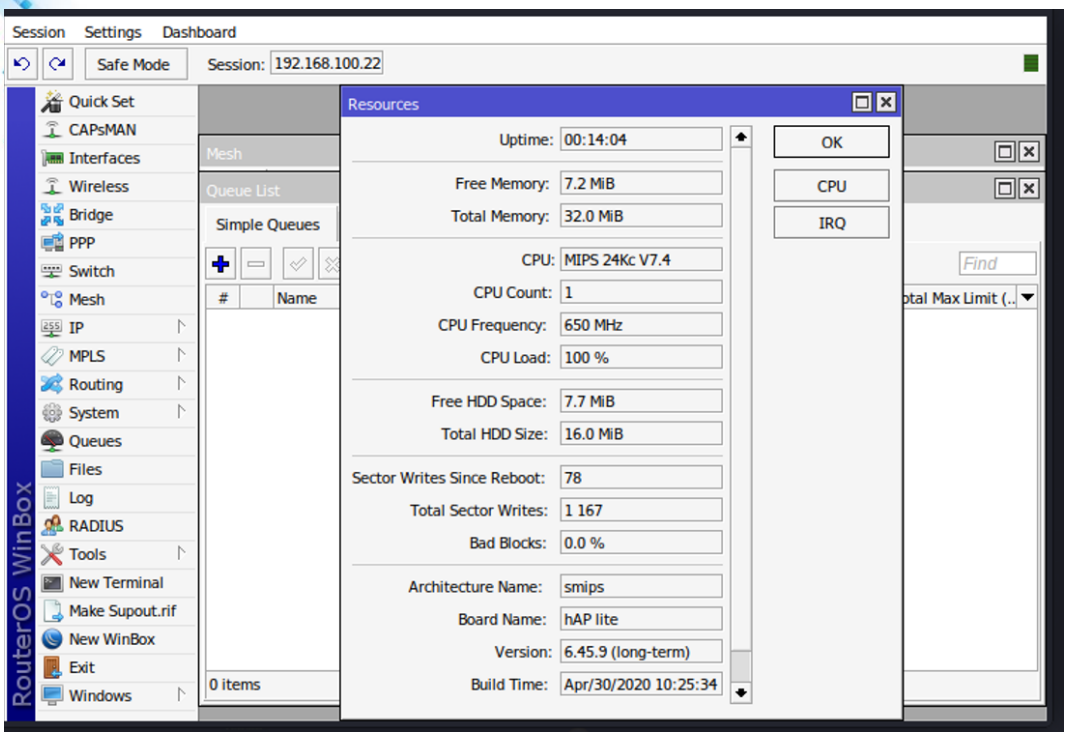
Dengan Menggunakan port 23/tcp dalam penyerangan dan ip *address* 192.168.100.22, hasil dari penyerangan dapat dilihat bahwa kinerja mikrotik mengalami kenaikan secara drastis yang semula dibawah 10% kini menjadi 100%, maka serangan menggunakan *tools LOIC* sudah berhasil dijalankan.

Selanjutnya akan dilakukan tahap pengujian menggunakan *tools SLOWLORIS* yang bertujuan untuk menguji keamanan serangan DDos pada mikrotik.



Gambar 10 Serangan Slowloris

Slowloris bertujuan untuk menonaktifkan server web tanpa memerlukan banyak bandwidth. Serangan ini bekerja dengan membuka banyak koneksi ke server target dan menahan koneksi tersebut terbuka selama mungkin dengan mengirimkan permintaan HTTP yang tidak lengkap. Penyerang mengirimkan header HTTP parsial secara berkala untuk menjaga koneksi tetap terbuka, namun tidak pernah mengirimkan permintaan HTTP lengkap dan akan menghabiskan sumber daya memori menjadi penuh.

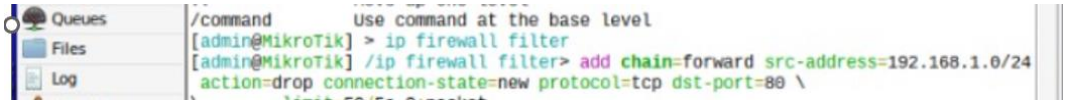


Gambar 11 Kondisi setelah di serang Slowloris

Dapat dilihat pada gambar diatas serangan Slowloris menghabiskan sumber daya (seperti memori dan CPU) untuk mempertahankan banyak koneksi yang belum selesai dan untuk pengguna yang sah mungkin mengalami penurunan kinerja, seperti lambatnya waktu respons atau ketidakmampuan mengakses layanan. Maka untuk penyerangan slowloris sudah berjalan dan dapat melakukan penyerangan terhadap mikrotik.

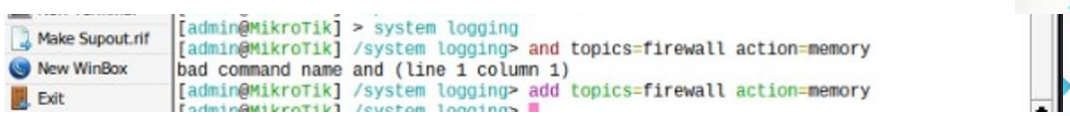
4.5.4 *Mintaining Access*

Pada tahap *maintaining Acces* akan dilakukan konfigurasi *firewall* untuk memblokir lalu lintas yang mencurigakan atau tidak diinginkan, contohnya seperti serangan yang dilakukan oleh tools *LOIC* dan *Slowloris*. Pada tahap ini serangan DDoS akan di blokir sehingga tidak dapat menembus keamanan yang ada pada mikrotik. Konfigurasi *firewall* akan dilakukan di dalam aplikasi winbox menggunakan terminal.



Aturan ini membatasi jumlah koneksi baru yang dapat dibuat dari satu IP untuk mencegah satu IP membanjiri server dengan permintaan baru.

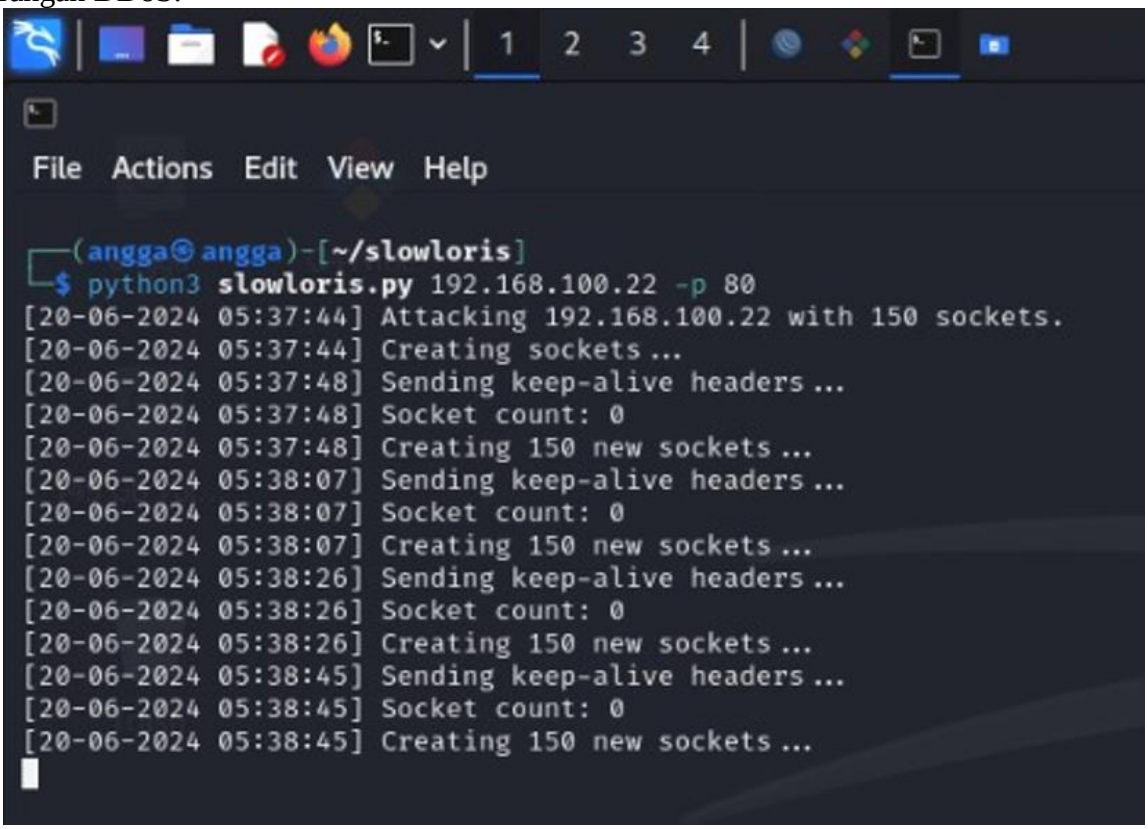
Membatasi *syn protect* dan aturan ini hanya berlaku untuk *port* tcp dan http.



Sistem *logging firewall* pada perangkat MikroTik digunakan untuk mencatat dan memantau aktivitas lalu lintas jaringan serta aturan *firewall* yang diterapkan. *Logging* sangat penting untuk keamanan jaringan karena membantu dalam deteksi keamanan dari serangan DDoS. Pada tahap ini sangat penting untuk keamanan jaringan dan manajemen lalu lintas. Dengan mengaktifkan *logging*, Anda dapat memantau aktivitas jaringan, mendeteksi serangan, dan memecahkan masalah dengan lebih efisien.

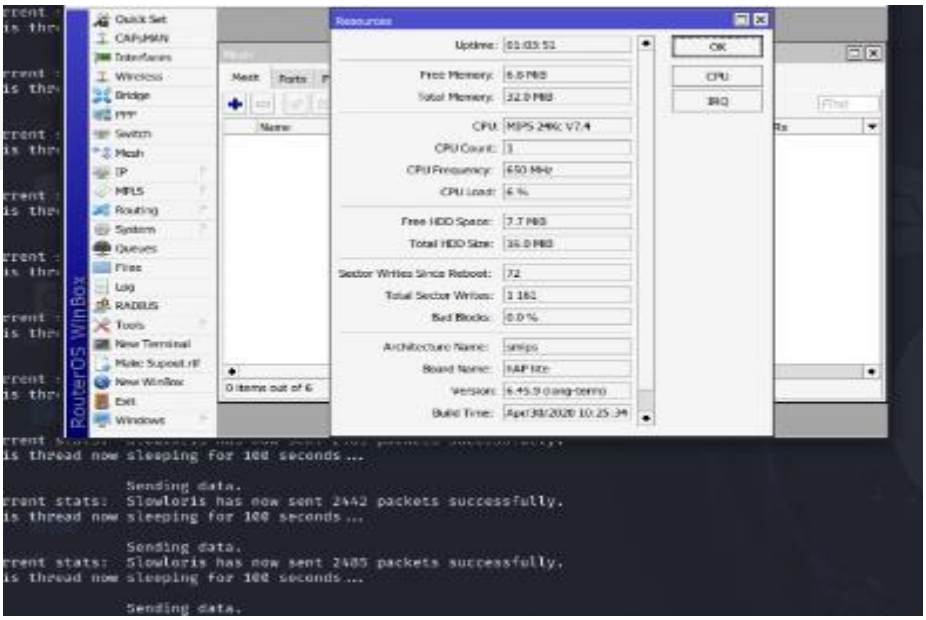
4.6 Hasil Pengujian

Pada tahap ini dilakukan pengujian Kembali serangan DDoS yang telah dikonfigurasi *firewall* untuk mengetahui apakah mikrotik masih bisa diserang atau sudah memblokir serangan DDoS.



Gambar 12 Pengujian Setelah di Firewall

Pada pengujian ini menggunakan tools Slowloris dan memakai port 80 untuk port yang akan diserang.



Gambar 13 Hasil Pengujian setelah di konfigurasi Firewall

Penyerangan yang dilakukan menggunakan *slowloris* kali ini terhenti di paket ke 2405 dan cpu pada mikrotik tidak mengalami kenaikan hal ini menandakan *slowris* tidak dapet menembus keamanan pada mikrotik, karna mikrotik sudah dilapisi oleh system keamanan *firewall*.

Berikut merupakan table hasil pengujian sebelum dan sesudah dilakukan pengujian pada mikrotik rb750r:

Tabel 2 Hasil Pengujian

sebelum	sesudah
Kondisi cpu pada mikrotik sebelum dilakukan pengujian dapat meningkat secara drastis apabila ada serangan DDoS, hal ini mengakibatkan kinerja pada mikrotik akan mengalami penurunan dikarnakan perangkat mikrotik mengalami *down*.	Kondisi cpu pada mikrotik masih normal walaupun diserang oleh *DDoS*, hal ini menandakan *firewall* yang telah dikonfigurasi pada mikrotik telah berhasil dijalankan, sehingga dapat mencegah serangan DDoS.

5. Kesimpulan

Pada kesempatan kali ini peneliti berhasil menyimpulkan bahwa *router* mikrotik terdapat *port* yang diduga terdapat kerentanan terhadap serangan DDos dan belum dilindungi oleh *firewall*, sehingga dapat di ekploitasi oleh orang yang tidak bertanggung jawab untuk mengirim paket secara berlebih dan mengakibatkan kinerja cpu menjadi naik drastis. Maka pada mikrotik dilakukan konfigurasikan *firewall* untuk mencegah serangan *DDoS*. Setelah dilakukan konfigurasi *firewall* serangan DDoS tidak dapat menembus router mikrotik.

6. Daftar Pustaka

Asep Fauzi Mutaqin, 'Rancang Bangun Sistem Monitoring Keamanan Jaringan Prodi Teknik Informatika Melalui SMS Alert Dengan Snort', *Jurnal Sistem Dan Teknologi Informasi*, 1.1 (2016), pp. 1–6 <https://jurnal.untan.ac.id/index.php/justin/article/view/12537/11376>

Didi Susianto, 'Implementasi Queue Tree Untuk Manajemen Bandwidth Menggunakan Router Board Mikrotik', *Jurnal Cendikia Vol 12No. 1Cendikia 2016 ISSN: 0216-9436 Bandar Lampung, April 2016*, 12.1 (2019), pp. 1–8

Radiyah, Ummu, 'Optimalisasi Keamanan Wide Area Network (WAN) Menggunakan Raw Firewall Berbasis Mikrotik Pada PT. Permata Graha Nusantara', *INTI Nusa Mandiri*, 17.1 (2022), pp. 16–23, doi:10.33480/inti.v17i1.3401

Suharti, Sri, Anton Yudhana, and Imam Riadi, 'Forensik Jaringan DDoS Menggunakan Metode ADDIE Dan HIDS Pada Sistem Operasi Proprietary', *MATRIK : Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer*, 21.3 (2022), pp. 567–82, doi:10.30812/matrik.v21i3.1732

Umar, Rusydi, and Agus Prasetyo Marsaid, 'Analisis Keamanan Jaringan LAN Terhadap Kerentanan Jaringan Ancaman DDoS Menggunakan Metode Penetration Testing', *Jurnal Riset Komputer)*, 10.1 (2023), pp. 2407–389, doi:10.30865/jurikom.v10i1.5835