Jurnal Borneo Informatika & Teknik Komputer **p-ISSN:** 2808-8190
Vol. 3, No. 2, 2023. Hlm 23—33 **e-ISSN:** 2808-6600

Analisis Implementasi *Port Knocking* pada Keamanan Jaringan di SMK PGRI 1 Nganjuk

Yanto Setiayoko[1], Daniel Swanjaya[2], Intan Nur Farida[3]

[1,2,3] UNIVERSITAS NUSANTARA PGRI KEDIRI, Kediri, Jawa Timur, 64112, Indonesia

e-mail: [*1]yantoyoko065@gmail.com, [2]daniel@unpkediri.ac.id, [3]in.nfarida@gmail.com

Diterima	Direvisi	Disetujui
17-07-2023	13-09-2023	24-10-2023

Abstract**:** *SMK PGRI 1 Nganjuk is a private school that offers internet network to support learning. The MikroTik server is often attacked during the process. Such attacks include probes, DDoS, port scanning, and sniffing. This research aims to address the emerging issues and hopes that similar problems will not occur in the future. The method used in this research is port knocking to close access ports, and further development includes closing the Mac interface winbox and adding anti-DDoS functionality. The goal of this research is to enhance the security of the internet network at SMK PGRI 1 Nganjuk. By implementing the method of blocking DDoS, it is expected to strengthen the server firewall. After going through the research process based on NDLC feedback, a network security plan is created and functions as intended. By utilizing network security applications, port tapping, and DDoS prevention methods, it can minimize the misuse of router access by unauthorized parties. As for recommendations for further research, testing should be conducted using other hacking tools with advanced testing techniques. Additionally, there is a need to develop a gate knocking method that can be employed.*

Keywords: *Network; DDOS; Port Knocking; Firewall; Education.*

Abstrak: SMK Pgri 1 Nganjuk merupakan sekolah swasta yang menawarkan jaringan internet untuk mendukung pembelajaran. Server mikrotik sering diserang selama proses berlangsung. Serangan semacam itu termasuk probe, *DDOS*, kontrol *port*, dan *sniffing.* Penelitian ini bertujuan untuk menjawab isu-isu yang sedang berkembang. Berharap masalah serupa tidak akan muncul di masa depan. Metode yang digunakan dalam penelitian ini adalah *port knocking* untuk menutup akses *port* dan mengembangkan metode tersebut dengan menutup *mac interface winbox* dan menambahkan fungsi anti *DDOS*. Tujuannya penelitian ini untuk meningkatkan keamanan jaringan internet di SMK PGRI 1 Nganjuk. Dengan menambahkan metode pemblokiran *DDOS*, diharapkan dapat memperkuat *firewall server*. Setelah melalui proses penelitian berdasarkan umpan *NDLC*, rencana keamanan jaringan dibuat dan berfungsi seperti yang diharapkan. Dengan menggunakan aplikasi keamanan jaringan, *port tapping* dan metode pencegahan *DDOS* dapat meminimalisir penyalahgunaan akses *router* oleh pihak yang tidak bertanggung jawab. Adapun rekomendasi untuk penelitian lebih lanjut, pengujian harus dilakukan menggunakan alat peretasan lain dengan teknik pengujian yang lebih tinggi. Selain itu, ada kebutuhan untuk mengembangkan metode ketukan gerbang yang dapat digunakan.

Kata kunci: Jaringan; *DDOS*; *Port Knock*; Keamanan; Pendidikan.

I. PENDAHULUAN

SMK PGRI 1 Nganjuk yang bergerak dalam bidang pendidikan terdapat ruang-ruang yang mendukung proses belajar mengajar, yang membantu siswa mencari informasi dan menerapkan materi yang dipelajari di kelas. Salah satunya adalah akses *hotspot* yang memungkinkan siswa terhubung ke internet di area tertentu. SMK PGRI 1 Nganjuk menggunakan *server router* mikrotik dikarenakan selain fungsinya yang lengkap dan mudah digunakan, *router* juga sangat handal untuk

mengelola infrastruktur jaringan. Berdasarkan hasil wawancara dengan admin jaringan di tempat penelitian. Beberapa siswa atau pihak luar mencoba meretas manajemen *router* mikrotik tersebut. Salah satu contoh kejadian yang terjadi adalah serangan *DDOS* dan probe pada *server*.

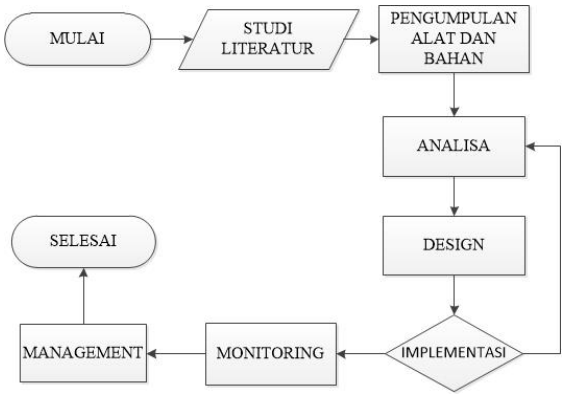
Adapun penelitian yang pernah dilakukan terkait dengan penelitian ini dengan judul "Implementasi keamanan jaringan pada *router* os menggunakan metode *port knocking* dengan protokol tcp dan *icmp*". Studi ini membahas implementasi *port knock* pada jalur *tcp* dan *icmp*. Dalam kasus yang dipelajari oleh Aldean, Aldean mengusulkan untuk mengamankan jaringan dengan metode *port-knocking*, karena tidak ada pengamanan khusus dalam pengelolaan jaringan yang ada (Alg Kawulusan,2019).Penelitian selanjutnya dengan judul "Desain keamanan jaringan pada mikrotik *router* os menggunakan metode *port knocking*". Penelitian ini menjelaskan tentang desain dan rangkaian percobaan rangkaian keamanan jaringan dengan gate knocker. Dalam studi yang dilakukan oleh kedua sahabat ini, mereka mensimulasikan pentingnya keamanan jaringan utama dengan memastikan gate knocking (Amarudin dan Faruk Ulum, 2018). Penelitian yang lain yaitu berjudul "Analisis dan implementasi *firewall* dengan metode *port address translation* pada mikrotik OS". Studi ini membahas analisis dan implementasi *port-address firewall* di Mikrotik OS. Untuk penelitian yang berfokus pada keamanan dilakukan pada penyortiran alamat IP yang diangkat oleh *proxy* untuk mencegah akses lebih lanjut oleh perangkat manajemen jaringan yang ada (Fitri dan Yahya 2018).

Berdasarkan temuan masalah diatas, maka tujuan penelitian ini adalah Dalam rangka meningkatkan keamanan jaringan komputer yang ada, digunakan metode *port knocking* dengan tujuan mengurangi jumlah serangan komputer. Selain itu, dibuatlah aturan yang dapat diikuti oleh administrator jaringan untuk menentukan siapa saja yang berhak mengakses dan memasuki *port* tertentu. Penggunaan metode penangkalan *DDOS* diharapkan mampu menangkal penyerangan DDOS pada pusat mikrotik. Dilakukan analisis efisiensi penggunaan metode *port knocking* dan metode anti-*DDOS* dalam menjaga keamanan jaringan. Metode *port knocking* dapat melindungi mikrotik dari serangan *hacker*, namun juga perlu menguji kelemahan metode tersebut dalam konteks keamanan jaringan. Selain itu, pengembangan metode *port knocking* juga dilakukan.

II. METODE PENELITIAN

Bagian metode berisi tentang rancangan penelitian, subjek penelitian, instrumen, prosedur pengumpulan data, dan analisis data yang dipaparkan penjelasannya dalam bentuk paragraf.

1. Rancangan penelitian



Gambar 1 Alur *Flowchart* Penelitian

Pada gambar 1 menunjukkan proses Alur *Flowchart* Penelitian dan prosedur penelitian dalam pengumpulan data serta penerapan dari sebuah metode yang diusulkan.

2. Subjek penelitian

Dalam penulisan penelitian ini yang menjadi objek penelitian adalah kemanan jaringan pada SMK PGRI 1 Nganjuk.

3. Instrument penelitian

Metode Literatur

Metode ini digunakan dengan cara membaca buku, jurnal, referensi internet dan artikel terkait untuk menemukan temuan penelitian yang dapat mendukung dan referensi saat menulis penelitian ini.

Wawancara (Interview)

Wawancara adalah teknik pengumpulan data dengan mengajukan pertanyaan langsung untuk memperoleh informasi yang diperlukan. Informasi yang diperoleh dari hasil wawancara diolah kembali dalam penelitian.

Pengamatan (Observasi)

Merupakan teknik pengumpulan data secara langsung di SMK PGRI 1 Nganjuk. Hasil pengamatan membantu menentukan alat ukur yang tepat untuk digunakan.

4. Prosedur Pengumpulan data

Berikut adalah instrumen penelitian yang digunakan guna pengumpulan data dalam penelitian:

Perencanaan

Merancang instrument penelitian, seperti daftar pertanyaan wawancara, panduan observasi.

Persiapan

Mencari surat izin dari pihak kampus untuk diberikan kepada tempat penelitian, guna untuk mendapatkan ijin mengakses data yang relevan.

Wawancara

Dilakukan dengan cara pengambilan data melaui tanya jawab secara langsung pada pihak yang berhubungan dengan penelitian ini. Pada penelitian ini melakukan wawancara denagan staff admin jaringan SMK PGRI 1 Nganjuk.

Observasi

Melaksanakan studi masalah dengan langsung ikut serta dalam pembenahan dan perbaikan jaringan internet ditempat lokasi. Guna mendapatkan data dan alat ukur apa saja yang akan digunakan.

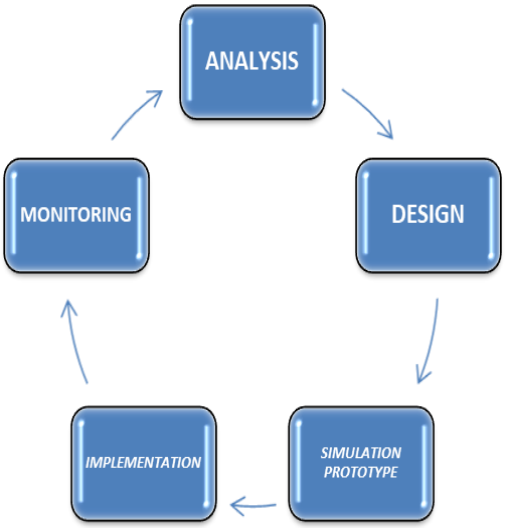
Pengumpulan data

Pada tahap ini didapatkan data dari prosedur perencanaan, persiapan, wawancara, dan tahap observasi.

5. Analisis data

Analisis data pada penelitian ini menerapkan Pengembangan sistem terkait pelaporan mengikuti metode NDLC (*Network Design Life Cycle*). Metode NDLC didasarkan pada fase pengembangan sebelumnya. Dengan demikian, proses penelitian dapat dilakukan secara terstruktur, terarah dan sistematis.

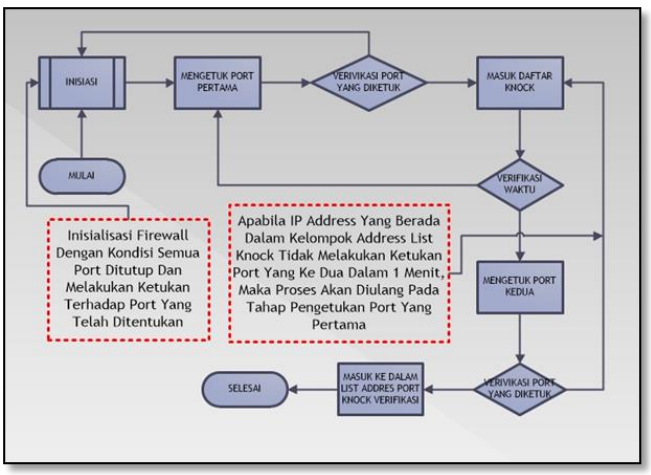
Proses NDLC memiliki beberapa alur proses yang akan dijalankan dan diterapkan dalam prosesnya yaitu analisis, *design*, simulasi, implementasi, monitoring. Analisa adalah proses untuk mendapatkan data-data penelitian. Setelah proses analisa selesai selanjutnya adalah proses desain yang tahap ini adalah merumuskan serta membuat desain dari permasalahan yang timbul. Setelelah di dapatkan hasil dari desain tahap selanjutnya adalah melakukan simulasi dari hasil desain apakah sudah sesuai ataukah belum sesuai. Setelah hasil simulasi langkah selanjutnya adalah implementasi hasil desain dan analisa kedalam permasalahan yang telah ada. Selanjutnya langkah terakhir adalah monitoring, dalam proses ini meninjau serta mengevaluasi apakah sudah berjalan sesuai dengan rancangan atau belum. Apabila dalam proses berjalannya masih ditemukan permasalahan maka akan dilanjutkan dari porses awal seperti terlihat pada gambar 2 :



Gambar 2 Proses tahapan penelitian NDLC

III. HASIL

Pembahasan kali ini mengenai hasil implementasi dari skema yang telah dibuat, dapat dilihat pada alur implementasi dari analisa permasalahan, tahap desain, tahap simulasi, tahap implementasi, tahap monitoring dan tahap manajemen.

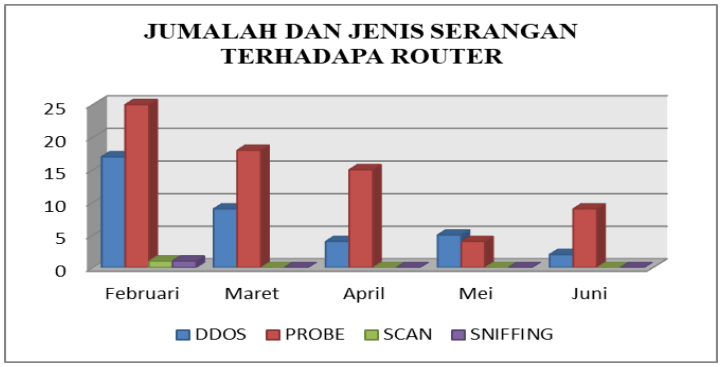


Gambar 3 Skema metode *port knocking*

Pada gambar 3 dijelaskan alur pengimplentasian *port knocking* pada *router* OS. Ada beberapa tahapan yang harus dijalankan agar seseorang dapat memasuki sebuah *router* yang telah diimplementasikan metode *port knocking*.

1. Analisa permasalahan

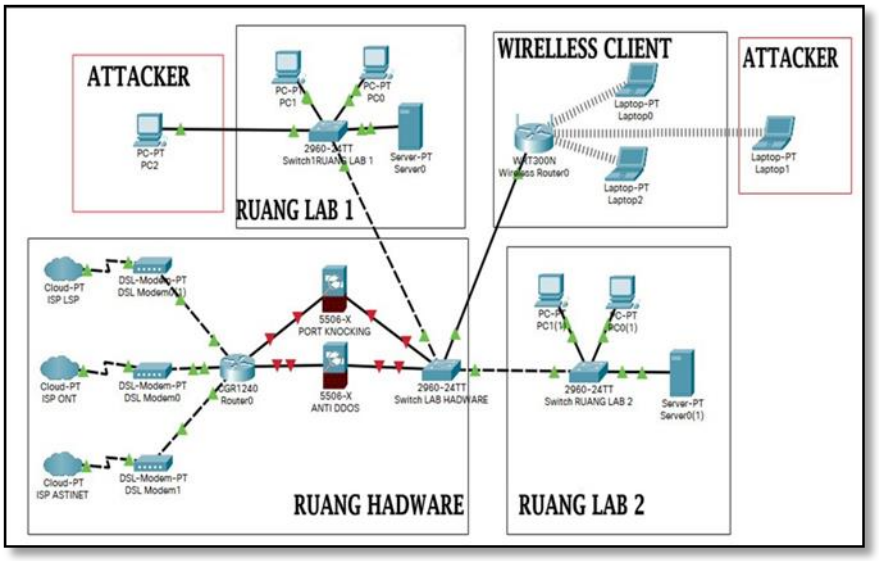
Setelah dilakukan analisis awal terhadap sistem yang beroperasi di mikrotik *router Rb 1100ahx4* yang menjadi pusat manajemen jaringan memiliki beberapa kelemahan. Ada beberapa serangan terhadap *router Rb 1100ahx4* yang dilakukan pihak yang tidak ber tanggung jawab agar dapat melakukan koneksi secara ilegal maupun merusak sistem yang berjalan seperti gambar 4.



Gambar 4 Grafik jumlah serangan terhadap mikrotik

2. Tahap Desain

Berikut ini topologi usulan guna untuk menunjang proses penerapan metode *port knocking* yang akan diterapkan kepada *router* pusak SMK PGRI 1 Nganjuk yaitu mikrotik *server RB 1100ahx4* yang ditunjukkan pada gambar 5.



Gambar 5. Topologi yang diusulkan

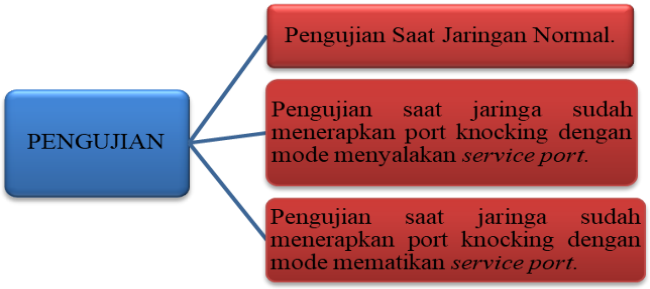
3. Tahap Simulasi

Tahapan ini adalah tahapan dimana simulasi atas desain jaringan yang telah dibuat dengan paket tracer dan implementasi konfigurasi pada *router* uji coba. Dalam tahap simulasi ini ada beberapa aturan yang telah di terapkan seperti berikut ini :

Konfigurasi sistem keamanan jaringan port knocking.
Konfigurasi sistem keamanan jaringan anti DDOS.
Penutupan dan pembukaan mac dari interface router.
Pengembangan sistem port knocking dan anti DDOS

Pada tahapan simulasi ini juga akan dijalankan simulasi pengujian sistem yang telah dibuat diatas dan pada tahapan pengujian dengan metode normal dan mematikan *service port* itu tidak jauh berbeda. Skenario uji coba dilakukan dalam tiga proses, yaitu :

Pengujian saat jaringan normal.
Pengujian saat jaringan sudah menerapkan port knocking dengan mode menyalakan service port.
Pengujian saat jaringan sudah menerapkan port knocking dengan mode mematikan service port.



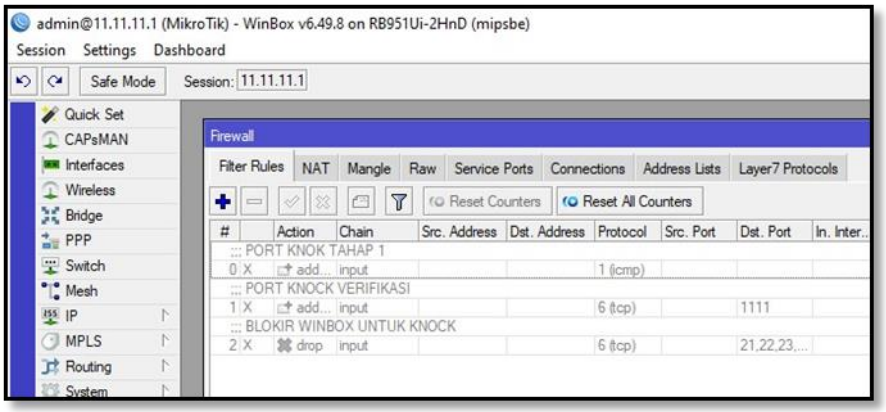
Gambar 6 Alur simulasi pengujian

4. Tahap Implemetasi

Tahapan ini menerapkan sistem keamanan jaringan yang telah di desain pada tahap sebelumnya. Pada tahapan implementasi ini nantinya akan dilakukan pengujian *hacking* terhadap *routerOS* yang telah dikonfigurasi sesuai tahapan sebelumnya.

Pengujian port knocking mode normal

Pengujian *port knocking* dilakukan pada *router* mikrotik dengan alamat (11.11.11.1/24). Dari hasil uji coba melakukan proses *login* kedalam mikrotik jalur *winbox* (8921) berjalan lancar tanpa ada halangan apapun. Begitupula ketika melakukan proses *login* mikrotik jalur *webpage* (80) dan jalur *telnet* (23) juga berjalan dengan baik dan tidak ada kendala yang timbul. Pada gambar 7 menjukkan proses tampilan saat melakukan proses *login* mikrotik menggunakan aplikasi *winbox*.



Gambar 7 Hasil *login winbox mode* normal

Pengujian port knocking mode enable

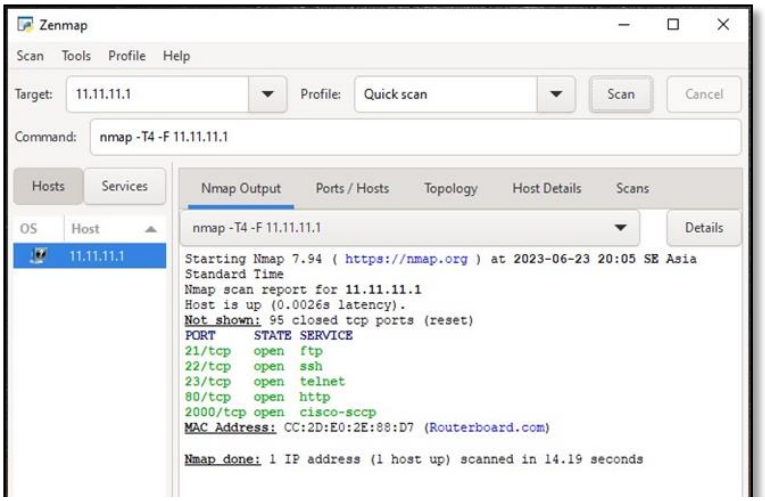
Pada bagian ini pengujian *port knocking* dilakukan pada *router* mikrotik dengan alamat (11.11.11.1/24). Dari hasil uji coba melakukan proses *login* kedalam mikrotik jalur *winbox* (8921) terdapat permasalahan dan tidak dapat berjalan. Begitupula ketika melakukan proses *login* mikrotik jalur *webpage* (80) dan jalur *telnet* (23) juga tidak dapat berjalan. Pada tahap ini menjelaskan bahwa *rule port knocking* sudah berjalan dengan baik. Berikut ini tampilan saat melakukan proses *login* mikrotik tanpa melakukan proses pengetukan *port* menggunakan aplikasi *winbox*.

Gambar 8 Gagal *login* mikrotik via *winbox*

Seperti yang terlihat pada gambar 8 ketika *mode enable port* dinyalakan, semua jalur masuk kedalam mikrotik telah ditutup. Agar dapat masuk kedalam mikrotik kembali diperlukannya proses *knock* untuk membuka *port* yang telah di tutup oleh metode *port knocking*.

Pengujian scan port mode normal

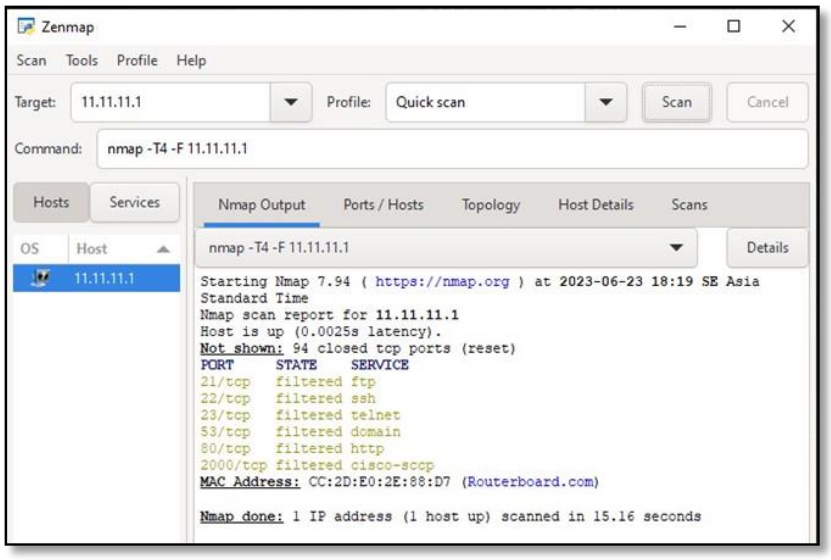
Berdasarkan hasi uji coba yang telah dilaksanakan, didapatkan hasil bahwa *port* yang ada pada jaringan mode normal masih bisa dilakukan *scan* dan terbaca. Adapun hasil dari *scanning* ditunjukkan oleh gmbar 9 :



Gambar 9 Hasil *Scan port router*

Pengujian scan port mode enable

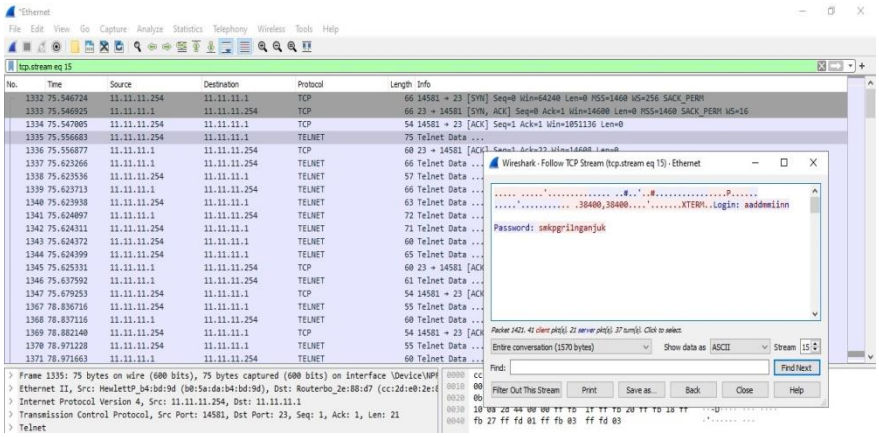
Berdasarkan hasi uji coba yang telah dilakasanakan, didapatkan hasil bahwa *port* yang ada pada jaringan mode *enable* sudah tidak bisa dilakukan *scan* dan tidak terbaca. Adapun hasil dari *scanning* seperti yang ditampilkan gambar 10 :



Gambar 10 Hasil *Scan port router mode disable*

Pengujian sniffing mode normal

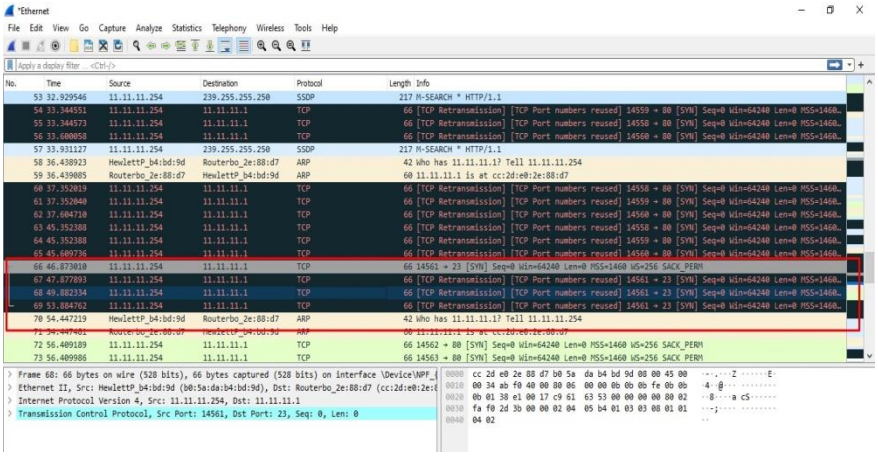
Dalam tahap pengujian proses *sniffing* kali ini proses pencurian data dapat dilaksanakan dengan baik. Akan tetapi hasil yang bisa di baca secara langsung oleh aplikasi *wireshark* hanya data pada *login telnet* sedangkan untuk data *login* dari *winbox* dan *webpage* masih *terenkripsi*. Seperti yang terlihat pada gambar 11.



Gambar 11 Hasil *Sniffing router* jalur telnet

Pengujian sniffing mode enable

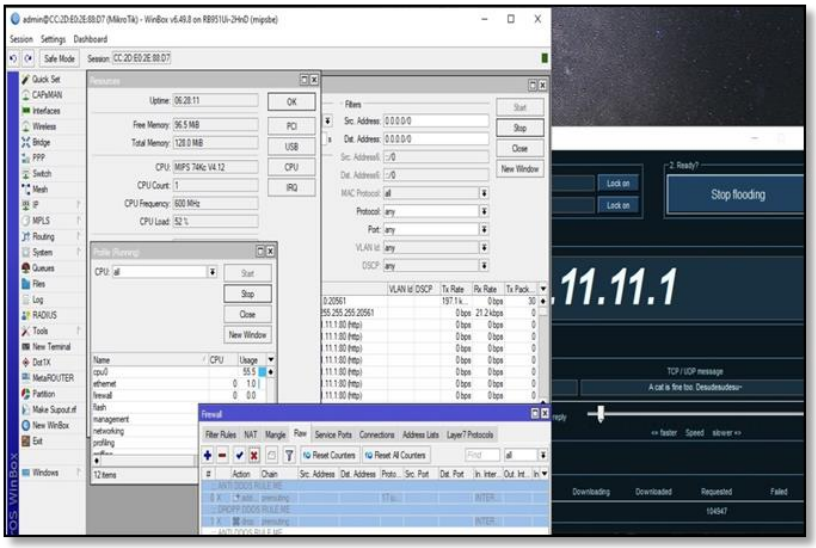
Dalam tahap pengujian proses *sniffing* kali ini proses pencurian data tidak dapat dilaksanakan dengan baik. Alasannya adalah terjadinya *error* dalam pembacaan *port* dan mengakibatkan kebuntuan sistem pencurian data terhadap *router* mikrotik. Seperti yang terlihat pada gambar 12.



Gambar 12 Hasil *Sniffing router* jalur *telnet*

Pengujian mode normal

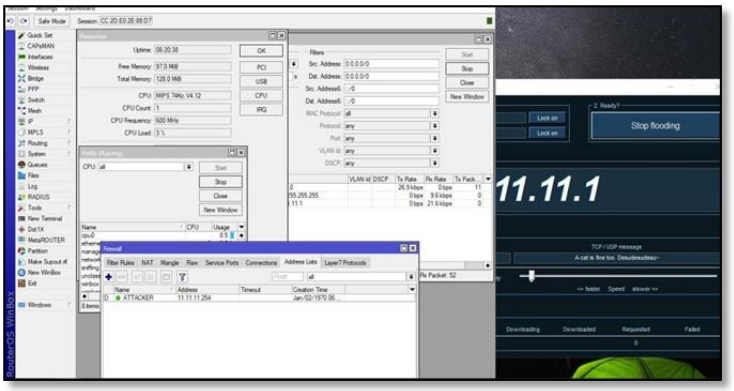
Setelah implementasi *port knocking* telah selesai, tahap selanjutnya adalah pengujian keamanan jaringan terhadap serangan *DDOS*. Pada tahap pengujian kali ini dengan cara menonaktifkan *rule raw* anti *DDOS* yang telah dibuat sebelumnya, sehingga didapatkan hasil seperti gambar 13 :



Gambar 13 Hasil *DDOS router mode* normal

Pengujian rule anti DDOS aktif

Setelah melihat betapa efektifnya serangan *DDOS* untuk melemahkan atau *mentakedown* mikrotik *router*. Oleh karena itu pada tahap pengujian selanjutnya dilakukan dengan cara mengaktifkan *rule raw* anti *DDOS* yang telah dibuat sebelumnya, sehingga didapatkan hasil pada gambar 14 :



Gambar 14 Implementasi anti *DDOS*

5. Tahap Monitoring

Setelah dilakukannya tahap pengujian, tahapan ini berfokus pada dilakukannya monitoring terhadap :

Topologi yang sudah dibuat.
Konfigurasi yang sudah di terapkan dan di uji coba.
Insfratruktur yang sudah dibuat

Dengan dilakukannya monitoring terhadap poin-point diatas diharapkan hasil dari implementasi *port knocking* dapat berjalan sesuai dengan fungsi dan harapan serta memenuhi kebutuhan.

6. Tahap Manajemen

Pada tahap manajemen merupakan tahapan terakhir, yang dimana perlu dibuatkan sebuah kebijakan management untuk mengawasi serta mengatur sistem yang sudah dikembangkan agar dapat berjalan dengan baik dan dapat dikembangkan lagi dikemudian hari.

IV. PEMBAHASAN

Berdasarkan hasil dari analisa dan pengujian sistem yang telah dilakukan diatas, diperoleh hasil bahwa konfigurasi *port knocking* dapat berfungsi dengan baik. Melihat hasil pengujian, pada saat jaringan berada pada mode normal *router* dapat dilakukannya *port scan*, *sniffing* dan berhasil *login*. Kemudian berkebalikan dari *mode* normal, pada saat *mode disable* akses, *router* tidak dapat dilakukannya *port scan*, *sniffing* maupun *login* juga tidak berhasil. Adapun hasil dari tahap pengujian bisa dilihat pada table 1.

Table 1 Hasil Pengujian

No	Mode Akses	Jenis Pengujian	Alat Uji	Hasil Pgengujian
1	Mode Normal	*Port Knocking*	*Port Knock Client*	Berhasil *login* dan normal
2	Mode Normal	*Scan Port*	*Nmap*	Semua *port service* terlihat dan terbuka.
3	Mode Normal	*Sniffing*	*Wireshark*	Terenkripsi keseluruhan data kecuali dari paket *telnet*.
4	Mode Normal	*DDOS*	*LOIC*	Kinerja cpu menjadi besar dan banyak paket yang masuk kedalam *routerbord*. Mengakiabtkan *router* menjadi panas dan tidak berfungsi.
5	*Mode Disable*	*Port Knocking*	*Port Knock Client*	Gagal *login*, diperlukan proses *knock.*
6	*Mode Disable*	*Scan Port*	*Nmap*	Semua *port service filtered*.
7	*Mode Disable*	*Sniffing*	*Wireshark*	Terenkripsi keseluruhan data tanpa

8	*Mode Disable*	*DDOS*	*LOIC*	terkecuali Kinerja cpu menjadi ringan dan berhasil mengamankan alamat *attacker* tersebut.

V. KESIMPULAN

Dengan adanya penerapan implementasi keamanan jaringan menggunakan metode *port knocking*, dapat meminimalisir terjadinya penyalahgunaan akses *router* dari pihak yang tidak bertanggung jawab.

Ucapan Terima Kasih

Ucapan terima kasih terutama ditujukan kepada pihak SMK PGRI 1 Nganjuk yang telah mengizinkan tempatnya digunakan untuk tempat penelitian, serta kepada kedua orang tua yang selalu memberikan dukungan serta doa. Tidak lupa dosen pembimbing penelitian saya yang telah mengevaluasi hasil kerja yang saya buat.

REFERENSI

Amarudin, & Atri. (2018). Analisis Penerapan Mikrotik Router Sebagai User Manager Untuk Menciptakan Internet Sehat Menggunakan Simulasi Virtual Machine. *Jurnal TAM (Technology Acceptance Model)*, 62-66.

Amarudin, & Ulum, F. (2018). Desain Keamanan Jaringan Pada Mikrotik Router Os. *Jurnal TEKNOINFO*, 72-75.

Dewi, N. K., & Putra, A. S. (2021). Pengembangan Sistem Jaringan Menggunakan Local Area Network Untuk Meningkatkan Pelayanan (Studi Kasus di PT. ARS Solusi Utama). *TEKINFO Vol. 22*, 66-79.

Indonesia, C. N. (2022, Agustus 2). Retrieved 1 10, 2023, from cni.net.id: https://cni.net.id/berita/detail/pengertian-mengenai-keamanan-jaringan#:~:text=Sistem%20keamanan%20jaringan%20merupakan%20sebuah,mengakses%20sistem%20jaringan%20komputer%20kita.

Kompirasi. (2022, September 22). Retrieved Januari 10, 2023, from Kompirasi Media: https://www.kompirasi.com/inilah-jenis-jenis-serangan-jaringan-pada-komputer/

Ramadhani, F., & Tadjuddin, A. M. (2018). Analisis Dan Implementasi Firewall Dengan Metode Port Address Translation Pada Mikrotik OS. *Universitas Muhammadiyah Makassar*.

Sanjaya, T., & Setiyadi, D. (2019). etwork Development Life Cycle (NDLC) Dalam Perancangan Jaringan Komputer Pada Rumah Shalom Mahanaim. *Jurnal Mahasiswa Bina Insani*, 1-10.

Saputro, A., Saputro, N., & Wijayanto, H. (2020). Metode Demilitarized Zone Dan Port Knocking Untuk Keamanan Jaringan Komputer. *CyberSecurity dan Forensik Digital*, 22-27.

SELAMATPAGI.ID. (2020, Mei 27). *Teknologi*. Retrieved Januari 10, 2023, from www.selamatpagi.id: https://www.selamatpagi.id/pengertian-wan-wide-area-network/#!

Syafrizal, M. (2020). *Pengantar Jaringan Komputer.* Yogyakarta: ANDI.

Teddy. (2020). Analisis Keamanan Jaringan Wireless Fidelity Sekolah Menengah Atas Negeri 10 Luwu. *Fakultas Teknik Komputer Universitas Cokroaminoto Palopo*.

Trimadani, P. (2020). IMPLEMENTASI KEAMANAN JARINGAN PADA MIKROTIK ROUTER OS MENGGUNAKAN METODE PORT KNOCKING DIASRAMA JAMBI SULTAN TAHA SYAEFUDDIN (. *Universitas AMIKOM Yogyakarta*.

trivus. (2022, September 18). Retrieved Januari 2023, 10, from trivus web ID: https://www.trivusi.web.id/2022/08/tcp-ip-model.html

Trivusi. (2022, September 17). Retrieved januari 10, 2022, from Trivusi Web ID: https://www.trivusi.web.id/2022/08/network-address-translation.html