JINTEKS (Jurnal Informatika Teknologi dan Sains) ISSN 2686-3359 (Online)
Vol. 3 No. 2, Mei 2021, hlm. 326 – 335

IMPLEMENTASI *PORT KNOCKING* UNTUK KEAMANAN JARINGANSMKN 1 SUMBAWA BESAR

Yudi Mulyanto[1], M. Julkarnain[2*], Aldela Jabi Afahar[3]
[1), 2), 3)] Teknik Informatika, Universitas Teknologi Sumbawa
email: yudi.mulyanto@uts.ac.id

Abstrak: Penelitian dilakukan untuk menganalisa dan mengimplementasikan metode *port knocking* dalam keamanan jaringan dan agar dapat mencegah serangan pada *port-port* jaringan komputer SMKN 1 Sumbawa Besar. Peneliti melakukan peningkatan keamanan jaringan menggunakan metode *PortKnoking* yang dapat membantu meningkatkan keamanan jaringan dan membantu *administrator* dalam mengamankan *Mikrotik Routerboard* pada sistem jaringan komputer SMKN 1 Sumbawa Besar. Adapun metode yang digunakan dalam pengembangan jaringan yaitu menggunakan metode *Network Development Life Cycle* (NDLC) yang terdiri dari enam tahapan yaitu analisis, perancangan, simulasi, *prototype*, penerapan,dan monitoring.

Kata kunci: NDLC, *Port Knoking, Mikrotik Routerboard, jaringan komputer.*

Abstract: *Research is done to analyze and implement the port knocking method in tissue security and in order to prevent attacks on port-port computer networks SMKN 1 Sumbawa Besar. Researchers are increasing network security using a Port Knoking method that can help enhance network security and assist administrators in keeping a Mikrotik Routerboard system of SMKN 1 SumbawaBesar. As for the methods used in the development of the Network Development Life Cycle (NDLC), which consist of the six stages analysis, design, simulation, prototype, application, and monitoring.*

Keywords: *NDLC, Port Knoking, Microtic Routerboard, computer networking.*

PENDAHULUAN

Keamanan jaringan komputer atau *Computer Network Security* sangat berhubungan dengan keamanan data, oleh karena itu keamanan jaringan sangat penting untuk melindungi data dari berbagai serangan pihak - pihak yang tidak bertanggung jawab. Serangan tersebut dapat ditujukan terhadap instansi, perusahaan atau lembaga tertentu, tidak terkecuali Sekolah Menengah Kejuruan Negeri 1 Sumbawa Besar yang dapat mengalami hal tersebut.

Serangan dilakukan melalui celah-celah yang ada pada jaringan komputer, dan salah satunya melalui *port* - *port* yang dalam keadaan terbuka, sehingga nantinya akan membuat orang
- orang yang tidak mempunyai hak akses maupunyang tidak berkepentingan dapat dengan mudah mengendalikan *port* – *port* yang telah ia akses. Hal ini peneliti buktikan dengan memasukan IP Address *router* melalui Browser atau HTTP (port 80), SSH (22), atau *Telnet* (23) maka langsung menampilkan *interface login* ke *router*.

Untuk mengatasi serangan terhadap *port* - *port* pada sistem jaringan komputer peneliti menggunakan metode *Port Knoking* yang merupakan suatu sistem keamanan yang dibuat secara khusus untuk sebuah jaringan. Pada dasarnya cara kerja dari *port knocking* adalah menutup semua *port* yang ada, dan hanya *user* tertentu saja yang dapat mengakses sebuah *port* yang telah ditentukan, yaitu dengan cara mengetuk terlebih dahulu.

TINJAUAN PUSTAKA

Penelitian ini memiliki beberapa referensi terkait judul yaitu jurnal penelitian Fajri dkk yang berjudul "Analisa Port Knocking Pada Sistem Operasi Linux Ubuntu Server 12.04 LTS" menjelaskan bahwa metode *Port Knocking* digunakan sebagai metode autentikasi, artinya seorang administrator dapat meningkatkan sistem keamanan komputer dari serangan Brute Force yang ditujukan untuk berbagai layangan seperti SSH Server, FTPServer, dan MySQL Server. Jurnal penelitian Danie Yoga Krintianto dalam Nugraha yang berjudul "Keamanan Jaringan Menggunkan Firewall Dengan Metode Random *Port Knocking* Untuk Koneksi SSH" menjelaskan bahwa intergritas keamanan dewasa sangatlah penting untuk ditingkatkan, celah-celah keamanan yang terdapat pada jaringan dapat dilihat oleh orang yang tidak bertanggung jawab dan dapat menjadi ancaman yang patut diperhatikan. Salah satu bentuk keamanan jaringan yang sering digunakan oleh seorang *administrator* jaringan dalam pengelolaan *server* yaitu melalui *remote login* seperti *Secure Shell* (SSH) [1]. Penelitian selanjutnya memiliki kesamaan dengan penelitian yang dilakukan oleh penulis, kesamaan tersebut ada pada metode penelitian yang digunakan yaitu metode *Network Development Life Cycle* (NDLC). Sedangkan perbedaan dari penelitian ini adalah pada objek yang diteliti dan fokus penelitian yang dilakukan Mulyanto, dkk adalah berorientasi pada pembenahan infrastruktur [2].

Jaringan komputer menurut ahli yaitu Kriston (2003) dapat diartikan sebagai kumpulan sejumlah terminal komunikasi yang terdiri dari dua komputer atau lebih yang saling terhubung. Tujuan dibangunnya jaringan komputer adalah agar informasi/ data yang dibawa pengirim (*transmitter*) dapat sampai kepada penerima (*receiver*) dengan tepat dan akurat. Jaringan komputer memungkinkan penggunanya dapat melakukan komunikasi satu sama lain dengan mudah. Selain itu, peran jaringan komputer sangat diperlukan untuk mengintegrasi data antar komputer-komputer *client* sehingga diperolehlah suatu data yang relevan.

Dalam sebuah sistem jaringan computer terdapat beberapa bentuk ancaman jaringan komputer baik itu dari segi fisik maupun logika. Adapun ancaman dari sistem jaringan komputer yaitu :

A. *Sniffer*, ancaman terhadap peralatan yang dapat memonitor proses yang sedang berlangsung,
B. *Spoofing*, Penggunaan komputer untuk meniru (dengan cara menimpa identitas atau alamat IP),
C. *Phreaking*, ancaman perilaku menjadikansistem pengamanan telepon melemah
D. *Remote Attack*, segala bentuk serangan terhadap suatu mesin dimana penyerangnya tidak memiliki kendali terhadap mesin tersebut karena dilakukan dari jarak jaruh di luar sistem jaringan atau media transmisi
E. *Hole*, kondisi dari software atau hardware yang bisa diakses oleh pemakai yang tidak memiliki

otoritas atau meningkatnya tingkat pengaksesan tanpa melalui proses autorisasi

F. *Hacker*, ialah orang yang secara diam-diam mempelajari sistem yang biasanya sukar dimengerti untuk kemudian mengelolanya dan *men-share* hasil ujicoba yang dilakukannya, hacker tidak merusak sistem

G. *Craker*, ialah orang yang secara diam-diam mempelajari sistem dengam maksud jahat, muncul karena sifat dasar manusia yang selalu ingin membangun (salah satunya merusak).

Untuk mengurangi ancaman dari jaringan maka dibangun keamanan jaringan, Keamanan jaringan ialah proses pencegahan yang dilakukan terhadap penyerangan yang terhubung ke dalam jaringan komputer melalui akses yang tidak sah, atau penggunaan secara ilegal dari komputer dan jaringan (John D. Howard, 1989-1995).

Firewall didefinisikan sebagai suatu cara atau mekanisme yang diterapkan baik terhadap *hardware*, *software* ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya, sehingga dapat mencegah bahaya/ancaman yang datang dari jaringan publik.

Sebuah *port* dalam protokol jaringan *TCP/IP* merupakan suatu mekanisme yang memberikan atau mengizinkan sebuah komputer untuk mendukung beberapa sesi koneksi dengan komputer lainnya dan program di dalam jaringan. *Port* dapat mengidentifikasikan aplikasi dan layanan yang menggunakan koneksi di dalam jaringan *TCP/IP*. Sehingga, *port* juga mengidentifikasikan sebuah proses tertentu di mana sebuah *server* dapat memberikan sebuah layanan kepada klien atau bagaimana sebuah *clien* dapat mengakses sebuah layanan yang ada dalam server

Port Knocking merupakan metode sistem autentikasi yang secara khusus dibuat untuk jaringan. Ide dasar dari sistem autentikasi ini telah lama digunakan namun baru pada tahun 2003. Pada dasarnya *port knocking* dapat didefinisikan sebagai suatu metode komunikasi antara dua komputer,dimana informasi yang dikirimkan di-*encode* dalam bentuk usaha koneksi ke *port–port* dalam urutan tertentu. Usaha membangun koneksi ini bisa disebut juga ketukan. Mekanisme *port knocking* akan menggunakan file log yang dibuat oleh *firewall* untuk mengetahui apakah suatu usaha koneksi telah dibuat oleh suatu *host* atau tidak.

NDLC adalah daur hidup perancangan dan pengembangan jaringan komputer yang melalui tahapan atau fase sehingga menghasilkan *output* yang diproses secara spesifik. Adapun tahap NDLC adalah sebagai berikut:

Analysis

Tahap awal ini dilakukan analisis kebutuhan, analisis permasalahan yang muncul, analisis keinginan pengguna, dan analisis topologi jaringan yang sudah ada saat ini. Metode yang biasa digunakan pada tahap ini diantaranya: Wawancara, Survei langsung kelapangan, Membaca manual atau blueprint dokumentasi, proyek jaringan, dokumentasi menjadi syarat mutlak setelah sistem selesai dibangun.

Simulation Prototype

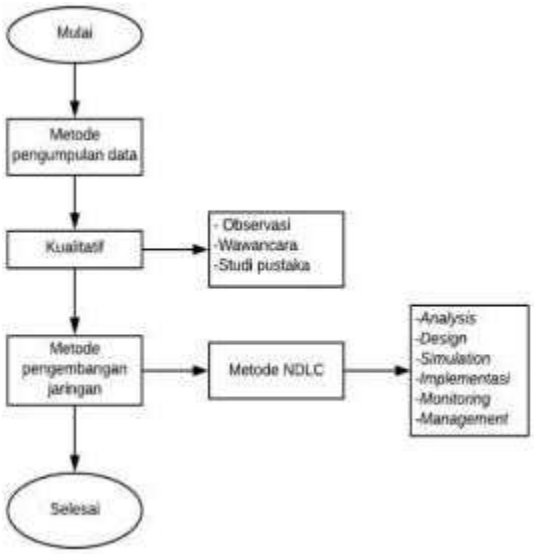
Pada tahap ini rancangan jaringan akan dimbuat dalam bentuk simulasi dengan bantuan *tools* khusus di bidang network seperti Boson, Packet Tracert, Netsim, dan sebagainya. Hal ini dimaksudkan untuk melihat kinerja awal dari jaringan yang akan dibangun dan sebagai bahan presentasi dan *sharing* dengan *team work* lainnya.

Monitoring

Tahapan *monitoring* merupakan tahapan yang penting, agar jaringan komputer dan komunikasi dapat berjalan sesuai dengan keinginan dan tujuan awal dari user pada tahap awal analisis, maka perlu dilakukan kegiatan *monitoring*.

METODE PENELITIAN

Peneliti menggunakan analisa penelitian kualitatif yang bersifat deskriptif. Hal ini dikarenakan sifat permasalahan yang menggambarkan atau mendeskripsikan keadaan subjek atau objek yang diteliti. Adapun pada tahapan analisis dan perancangan jaringan yaitu sebagai berikut :



Gambar 1.Tahapan Metode Penelitian

Metode yang dilakukan dalam penelitian ini ada dua yaitu menggunakan pendekatan observasi dan wawancara, dikarenakan peneliti terjun kelapangan menganalisis situasi secara nyata, memahami permasalahan yang terjadi secara alami dan mengambil kesimpulan dari proses tersebut.

Observasi

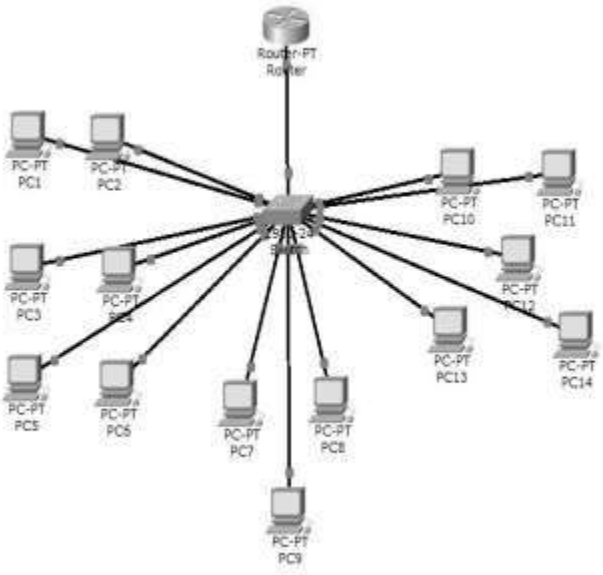
Pada metode ini peneliti melakukan survei lokasi untuk mengumpulkan data-data SMK Negeri 1 Sumbawa. Survei ini dilakukan untuk mencari data jaringan dan data pengguna jaringan.

Wawancara

Pada tahap ini peniliti melakukan wawancara terhadap kepala LAB komputer SMKN 1 Sumbawa. Untuk mendapatkan informasi terkait perkembangan dan fungsi keberadaan jaringan komuputer.

HASIL DAN PEMBAHASAN

Berdasarkan hasil observasi dan wawancara peneliti mendapati bahwa keamanan jaringan pada SMKN 1 Sumbawa Besar menggunakan *firewall* bawaan dari *mikrotik routerboard* yang menggamankan *mikrotik* pada jaringan komputer SMKN 1 Sumbawa Besar.



Gambar 2.Infrasruktur Jaringan

Perancangan

Adapun gambaran penggunaan metode *Port Knocking* pada *Mikrotik Routerboard* 1100 AH sebagai berikut:

1. *User* melakukan *Ping* ke *port* 1000 Dan *Mikrotik* RB1100AH akan menyimpan *user* yang ingin mengakses

Gambar 3. *User* Melalukan Ping

2. *User* mencoba akses *Mikrotik* dengan cara ping port 1000 router akan mengecek apakah *user* tersebut aman atau aman atau tidak.

Gambar 4. *User* Akses *Port* 1000

 ISSN 2686-3359 (Online)

3. Jika *user* masuk dalam *monitoring* pada *Mikrotik* RB1100AH maka *user* tersebut dapat mengakses jaringan pada *mikrotik* RB1100AH.

Gambar 5.*User* Berhasil Membuka Akses

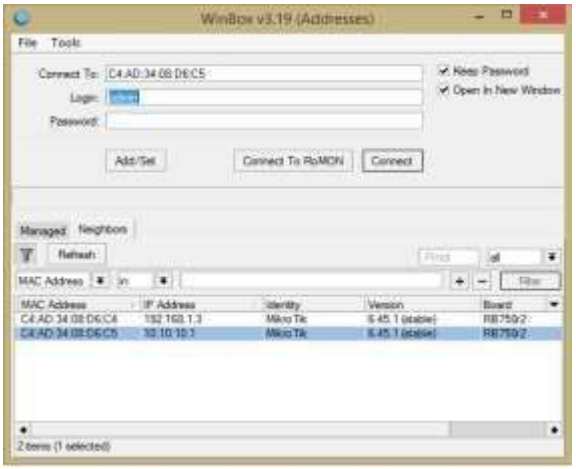
Simulasi dan *Prototype*

Pada tahap simulasi peneliti memilih simulator yang akan digunakan dalam penelitian yaitu *WinBox* Versi *3.19.* peneliti memilih simulator tersebut karena terdapat fitur-fitur yang memudahkan dalam merancang dan mengkonfigurasi keamanan jaringan *port knoking*.

Gambar 6. *WinBox*

Gambar 6 merupakan tampilan awal simulator yang akan digunakan dalam perancangan keamanan jaringan.

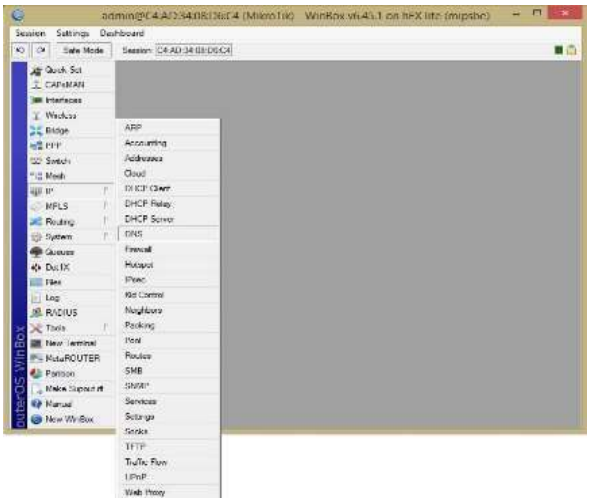
A. Login mikrotik



Gambar 7. Login *WinBox*

Gambar 7 merupakan tampilan utama *WinBox*, yang berisikan kolom login dan password. Pada gambar tersebut peneliti mengisi kolom login dan password untuk masuk ke *mikrotik.*

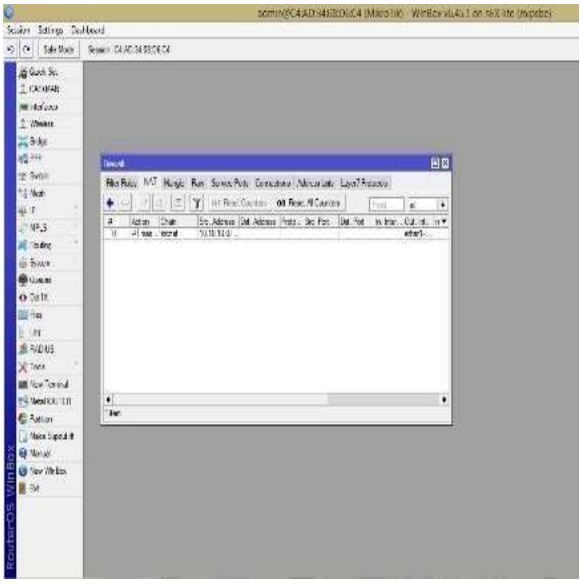
B. Konfigurasi Knock 1000



Gambar 8. Konfigurasi *Knock* 1000

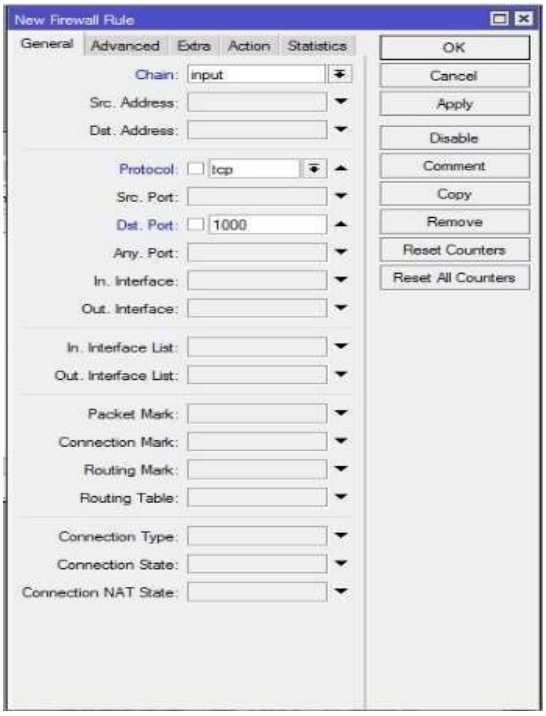
Gambar 8 merupakan tampilan setelah login *WinBox*, untuk melakukan konfigurasi peneliti meng-klik pada menu *IP* dan menuju pada menu *FIREWALL*.

 ISSN 2686-3359 (Online)



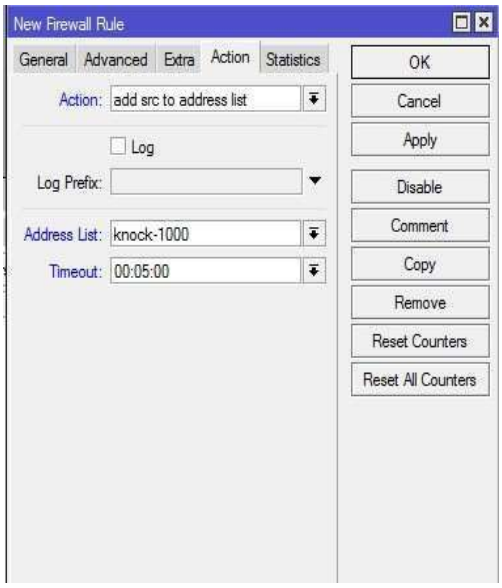
Gambar 9. Menu *Firewall*

Pada gambar 9 menampilkan menu *FIREWALL*, selanjutnya penilti memilih simbol tambah berwarna biru pojok kiri atas pada tab *FILTER RULES.*



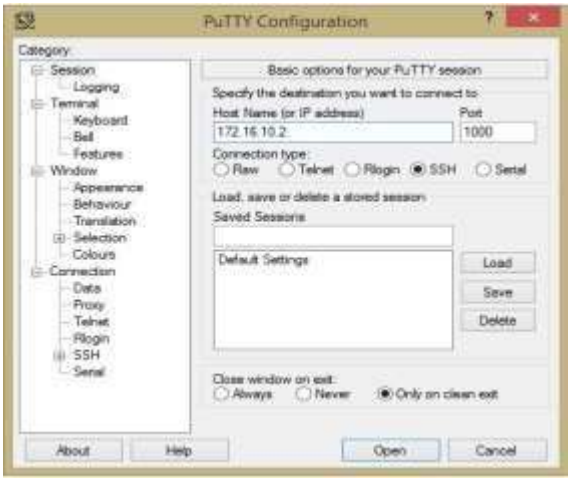
Gambar 10. Konfigurasi *Filter Rules*

Pada gambar 10 peneliti membuat gerbang atau *knock* 1000, dengan memilih tab *GENERAL* kemudian pada kolom *CHAIN* diisi *INPUT*, pada kolom protokol diisi TCP dan pada kolom *DST. PORT* diisi 1000 selalnjutnya memilih tab *ACTION.*



Gambar 11. Konfigurasi *Filter Rules*

Pada gambar 11 peneliti merubah kolom *ACTION* menjadi *ADD SRC TO ADDRESS LIST*, pada *ADDRESS LIST* diisi dengan *knock*1000 dan *TIMEOUT* diisi 5 menit untuk menghindari penumpukuan pada *address list.*

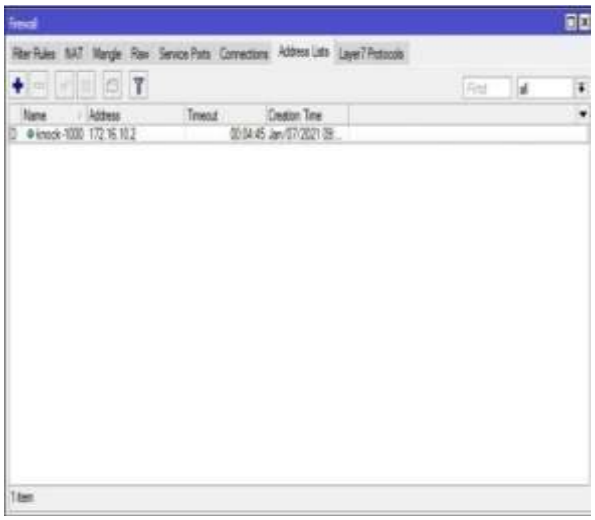


Gambar 12. Aplikasi *PuTTY*

Gambar 12 merupakan aplikasi yang digunakan untuk mencoba apakah konfigurasi *knok* 1000 berhasil dijalankan atau tidak. Langkah pertama untuk mencobanya yaitu memasukkan *ip address* dan *port*

 ISSN 2686-3359 (Online)

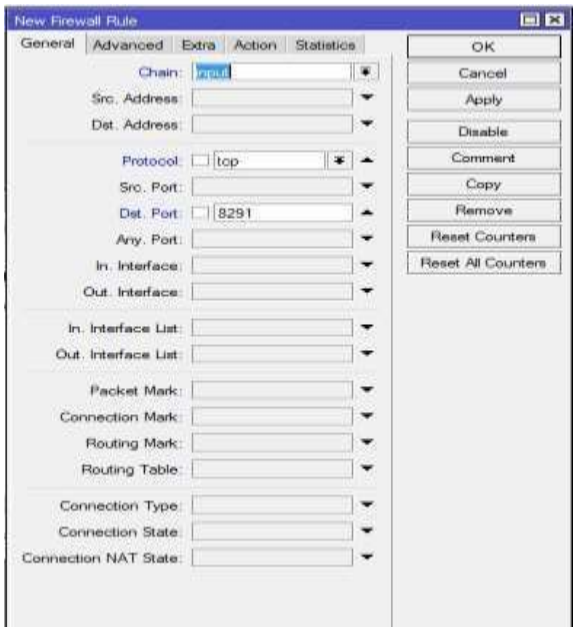
1000 kemudian klik *OPEN*. Selanjutnya tampilan dapat dilihat pada gambar 13.



Gambar 13. Hasil konfigurasi *knok* 1000

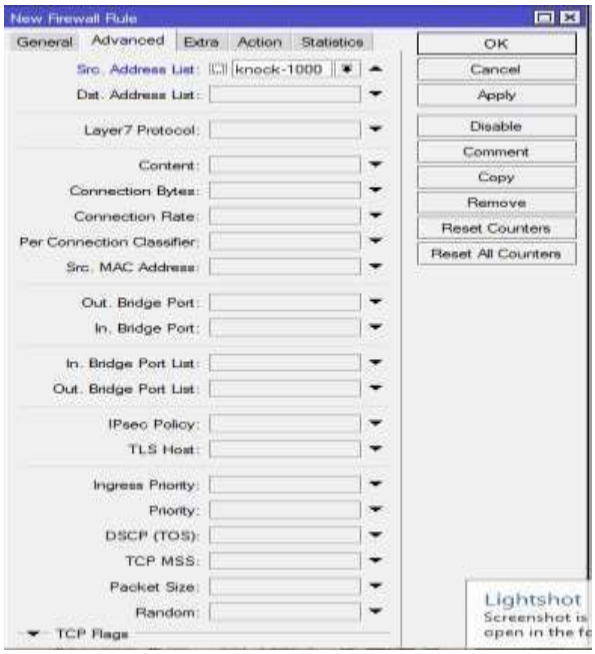
Pada gambar 13 dapat dilihat bahwa *ip address* sudah masuk dalam *knock* 1000 dengan estimasi waktu 5 menit.

C. Konfigurasi SAFE IP



Gambar 14. Safe IP

Pada gambar 14, sama halnya dengan mensetting *knock* 1000 hanya saja, perbedaannya terletak pada *port* yang digunakan merupakan *port* dari *mikrotik* yaitu 8291, kemudian beralih pada tab *ADVANCED*.



Gambar 15. Konfigurasi Safe IP

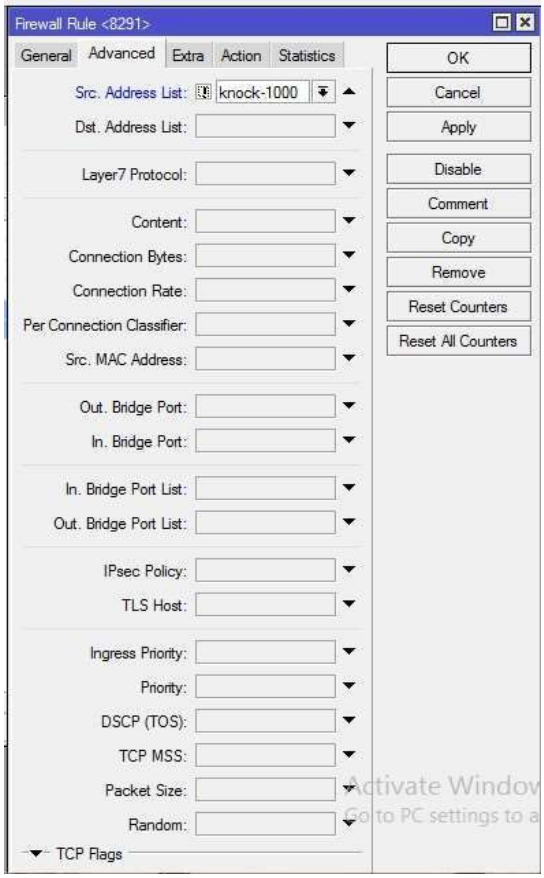
Pada gambar 15 merupakan tampilan dari tab *ADVANCED*, kemudian pada *SRC.ADDRESS LIST* pilih *KNOCK*-1000 yang telah disetting pada awal konfigurasi, karena ketika ip address atau user yang telah masuk pada *knock* 1000 akan masuk dalam kelompok *SAFE IP* atau *ip address* yang aman.

Gambar 16. Konfigurasi Safe IP

Pada gambar 16 merupakan tampilan dari tab *ACTION* langkah selanjutnya ACTION pada tab ACTION diisi dengan ADD ARC TO ADDRESS LIST agar dapat dimonitoring dimikrotik, kemudian selanjutnya pada ADDRESS LIST diisi dengan nama SAFE-IP.

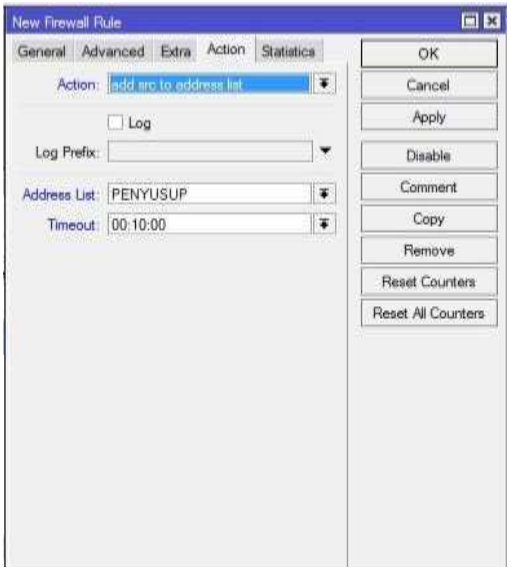
D. Konfigurasu IP Penyusup

Pada konfigurasi *IP* PENYUSUP sama halnya dengan setting dengan *knock* 1000 dan *SAFE IP* hanya saya pada bagian setiingan pada tab *ADVANCED* di kecualikan yang telah masuk di *knock* 1000 agar yang masuk pada mikrotik tanpa melalui *kcock* 1000 tidak dapat mengakses *mikrotik* tersebut.



Gambar 17. Konfigurasi IP Penyusup

Pada gambar 17 merupakan tampilan tab ADVANCED, pada settingan dapat dilihat SRC.ADDRESS LIST memilih knock-1000 dan ada tanda seru(!) di samping kiri yang artinya siapapun yang tidak masuk pada *knock* 1000 dinyatakan sebagai *IP* PENYUSUP terkecuali telah akses pada *port* 1000 atau *knock*-1000. Langkah berikutnya sama dengan *SAFE IP* dan *knock* 1000, hanya saja yang berbeda pada nama pada *ADDRESS LIST*.



Gambar 18. Konfigurasi IP Penyusup

Pada gambar 18 merupakan tampilan tab ACTION, sama dengan settingan SAFE-IP dan knock 1000 hanya saja pada ADDRESS LIST diubah atau diisi penyusup dengan estimasi waktu 10 menit

E. Konfiguras DROP IP

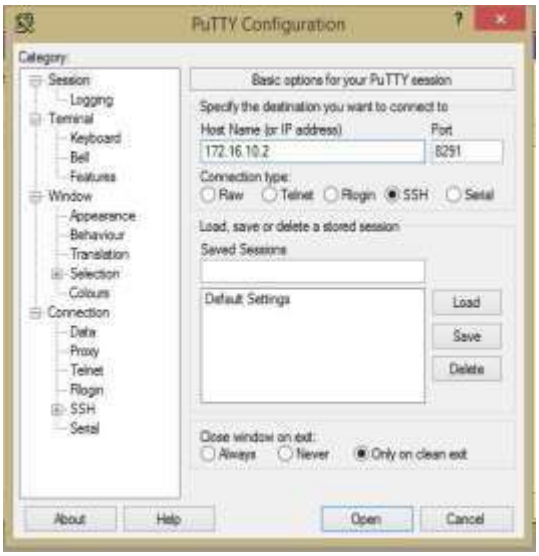
Konfigurasi DROP IP sama dengan tahap dari konfigurasi sebelumnya hanya saja yang berbeda pada tab ADVANCED dan tab ACTION.

Gambar 19. Konfigurasi Drop IP

Pada gambar diatas dapat dilihat pada *ADVANCED setting* yang berbeda dari settingan yang sebelumnya adalah pada *SRC. ADDRESS LIST* memilih *SAFE-IP* tapi dengan tanda seru (!) sehingga siapapun yang masuk ke *mikrotik* akan di *DROP* atau di BLOK terkecuali yang terdaftar di dalam *SAFE-IP*.

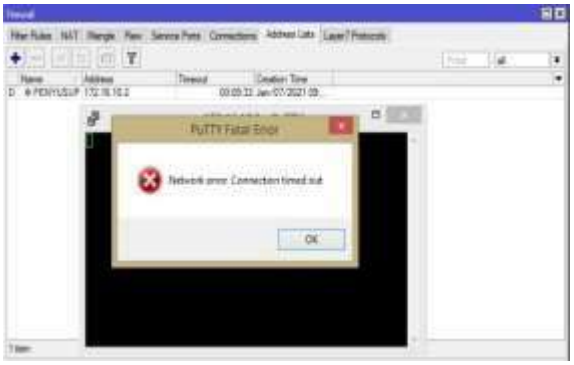
Gambar 20. Konfigurasi Drop IP

Pada gambar 20 merupakan tampilan dari tab ACTION, dapat dilihat pada ACTION memilih DROP, sehingga siapapun yang masuk tanpa masuk terlebih dahulu di *knock*-1000 atau tidak terdaftar didalam *SAFE-IP* maka akan di *DROP* atau di *BLOK*. Untuk mengetahui konfigurasi berhasil atau tidak nya peneliti mencoba menggunakan aplikasi *puTTY*untuk membantu dalam mecoba hasil konfigurasi.



Gambar 21. Percobaan dengan aplikasi *puTTY*

Pada gambar 21 peneliti mecoba untuk masuk kedalam *mikrotik* dengan menggunakan *port* 8291 dangan alamat *ip address* tanpa masuk terlebih dahulu ke *port* 1000.



Gambar 22. Percobaan dengan aplikasi puTTY

Pada gambar 22, dapat dilihat bahwa tanpa masuk terlebih dahulu ke *port* 1000 atau langsung ke *port mikrotik* maka *mikrotik* akan mendrop hak akses dari *user* tersebut.

Monitoring

Dalam tahap *monitoring* peniliti mengetahui tingkat keberhasilan dan kesalahan dari jaringan yang dibangun.

Gambar 23. Pengujian Konfigurasi *Port Knoking*

Pada gambar 14 menunjukkan bahwa pengujian dari berbagai konfigurasi *port knoking* menggunakan *mikrotik*, dan semua konfigurasi dari *knock* 1000.

KESIMPULAN

Dari hasil analisis dan perancangan kemanan jaringan yang telah dilakukan dengan menggunakan metode Network Development Life Cycle (NDLC)

maka penulis dapat mengambil kesimpulan bahwa implementasi Port Knocking untuk keamanan jaringan SMKN 1 Sumbawa Besar telah selesai dilakukan menggunakan perangkat *Routerboard Mikrotik* RB750r2 dan aplikasi pendukung lainnya.

Penerapan metode *Port Knocking* untuk keamanan jaringan SMKN 1 Sumbawa dapat membantu dalam meningkatkan keamanan jaringan dan membantu administrator dalam mengamankan Mikrotik Routerboard pada system jaringan komputer SMKN 1 Sumbawa Besar. Dengan demikian penelitian ini dapat memberikan kontribusi untuk keamanan jaringan komputer SMKN 1 Sumbawa Besar.

DAFTAR PUSTAKA

[1] D. Kristianto, "Keamanan Jaringan Menggunakan Firewall Dengan Metode Random Port Knocking Untuk Koneksi Ssh," *Keamanan Jar. Menggunakan Firewall Dengan Metod. Random Port Knocking Untuk Koneksi Ssh Kompetensi*, pp. 1–14, 2015.

[2] K. Yudi Mulyanto, "Analisis dan pengembangan infrastruktur jaringan komputer dalam mendukung implementasi sekolah digital," *J. JINTEKS*, vol. 1, no. 1, pp. 58–67, 2019.