Penerapan Metode *Port Knocking* Pada Sistem Keamanan Jaringan Berbasis Notifikasi Telegram

Muhammad Rizal Agustian
Universitas Buana Perjuangan
Karawang, Indonesia
if17.muhammadagustian@mhs.ubpkarawang.ac.id

Tatang Rohana
Universitas Buana Perjuangan
Karawang, Indonesia
tatang.rohana@ubpkarawang.ac.id

Tohirin Al Mudzakir
Universitas Buana Perjuangan
Karawang, Indonesia
tohirin@ubpkarawang.ac.id

***Abstract*—**
Dalam keamanan data dan informasi pada suatu teknologi informasi akan terus diperbaharui setiap waktu, dengan perkembangan teknologi informasi pada masa ini yang akan selalu berkembang, sehingga menyebabkan kemanan menjadi sebuah prioritas utama. Penggunaan prosedur penelitian metode *Network Development Life Cycle* (NDLC) dimulai dengan *Analysis, Deisgn, Prototype, Implementation, Monitoring,* dan *Management*. Oleh karena itu dengan semakin banyaknya serangan yang dilakukan oleh oknum yang tidak bertanggung jawab sehingga menyebabkan kerusakan terhadap *server*. Serangan tersebut seringkali dilakukan melalui suatu *port* yang tersedia pada *server* dan menyebabkan pengguna yang mempunya akses maupun tidak berkepentingan dapat masuk pada port yang tersedia. Salah satu metode keamanan jaringan yang digunakan pada *port* adalah metode *port knocking* bertujuan memberi lapisan keamanan pada *port* yang tersedia dan menyamarkan *port* yang akan di akses. Sehingga tidak terdeteksi *port* awal yang harus diakses terlebih dahulu agar perangkat masih tetap bisa diakses, dan pengguna yang tidak memiliki akses dapat diblokir pada perangkat. Hasil penelitian ini yaitu dapat mengamankan perangkat pada saat akan di akses dan setiap aktifitas akses perangkat tersebut akan dihubungkan pada aplikasi telegram yang terhubung secara *online* kepada *administrator* jaringan dan akan mendapatkan notifikasi melalui *bot* telegram.

Kata kunci — Keamanan jaringan, NDLC *(Network Depelopment life Cycle), Port Knocking,*

I. PENDAHULUAN

Perkembangan *internet* merupakan salah satu teknologi yang paling cepat dan memiliki dampak meningkatnya *cyber crime* dengan tingkat yang tinggi. Keamanan jaringan secara umum jika sebuah komputer yang terhubung ke sebuah jaringan maka akan lebih berpotensi terserang berbagai ancaman keamanan dibandingkan komputer yang tidak terkoneksi ke jaringan. Keamanan jaringan yang mampu untuk mengantisipasi ancaman di dalam jaringan komputer baik dari ancaman sistem maupun fisik. Ancaman sistem yang dimaksud adalah berupa penyusupan,pencurian data, maupun tindakan *hacking* pada sistem sedangkan ancaman fisik yaitu yang merusak fisik atau *hardware* perangkat.

Cimun Net merupakan sebuah *internet café* skala *mikro* yang beralamat di Jl. Kp. Lamaran No.6, Palumbonsari, Kec. Karawang Timur, Kabupaten Karawang, yang bergerak di bidang jasa, bidang jasa usaha ini berfokus pada jasa layanan *internet* yang bervariasi masa waktunya yaitu bisa berupa hitungan jam, hari, maupun bulanan. Setiap keamanan pasti mempunyai beberapa kelemahan, termasuk pada keamanan jaringan komputer. Keamanan jaringan komputer merupakan proses pencegahan dan identifikasi terhadap penggunaan hak akses pada jaringan yang bertujuan untuk mencegah pihak yang tidak memiliki otorisasi agar tidak bisa mengakses jaringan komputer. Kewaspadaan tersebut tentu harus diiringi dengan kemampuan pengelola jaringan komputer agar bisa meningkatkan keamanan jaringan komputer dari pihak yang akan melakukan *hacking*.

Bertujuan untuk memudahkan *administrator* jaringan agar bisa memantau perangkat jaringan yaitu *router* Mikrotik, dengan mengirimkan notifikasi berupa pesan melalui aplikasi Telegram apabila terjadi serangan pada *router* yang berupa tindakan mencoba *login* berulang kali. Berdasarkan uraian diatas maka dibuatlah penelitian dengan judul yang relevan menggunakan latar belakang penelitian ini adalah "Penerapan Metode *Port Knocking* Pada Sistem Keamanan Jaringan Berbasis Notifikasi Telegram".

II. DATA DAN METODE

A. Teknik Pengumpulan Data

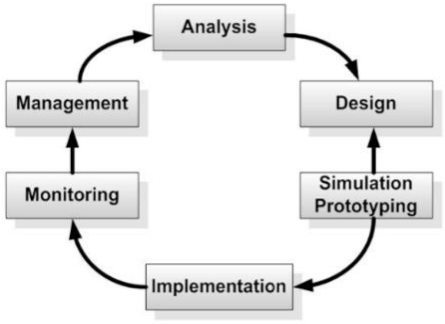
Teknik pengumpulan data penelitian adalah sebagai berikut:

1. Wawancara
   Melakukan wawancara dengan administrator jaringan dalam hal ini pemilik Cimun Net dengan maksud untuk mengetahui manajemen jaringan dan harapan yang diinginkan pemilik tentang keamanan jaringan.
2. Studi Pustaka
   Melakukan kegiatan mencari referensi yang bersumber baik dari buku, jurnal ilmiah yang disesuai dengan keperluan analisis data.

B. Prosedur Penelitian

Prosedur penelitian ini mengacu pada Metode yang digunakan yaitu NDLC dari tahapan sebagai berikut: Analisis, Perancangan, Pembuatan prototipe simulasi, Implementasi, Pemantauan dan Pengelolaan.

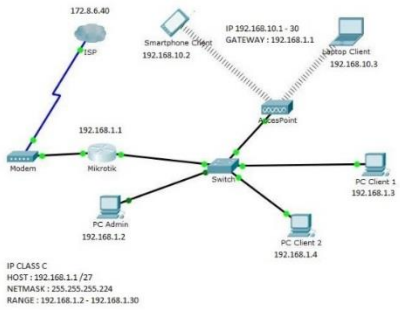
Tahapan-tahapan dalam *Network Development Life Cycle*, yaitu :



Gambar 1 Metode Pengembangan Sistem
(Sumber : library.binus.ac.id)

1. *Analysis*: Pada tahapan awal ini dilakukan analisa kebutuhan, terhadap permasalahan yang muncul, serta kekurangan sistem yang akan diteliti. Metode yang digunakan pada tahap ini antara lain: wawancara, dan studi pustaka.
2. *Design*: Berdasarkan data yang diperoleh, maka tahapan perancangan ini akan membuat *design* topologi jaringan yang sudah berjalan dan topologi jaringan usulan, maupun *design* sistem usulan, sehingga bisa memberikan gambaran yang jelas mengenai design keseluruhan yang akan dibangun.

   Berikut gambaran akan dipaparkan Topologi sistem usulan, tahapan desain topologi menggunakan aplikasi simulator Cisco Packet Tracer, jaringan yang dibuat berdasarkan data yang didapat pada proses analisa



Gambar 2 Topologi Sistem Berjalan

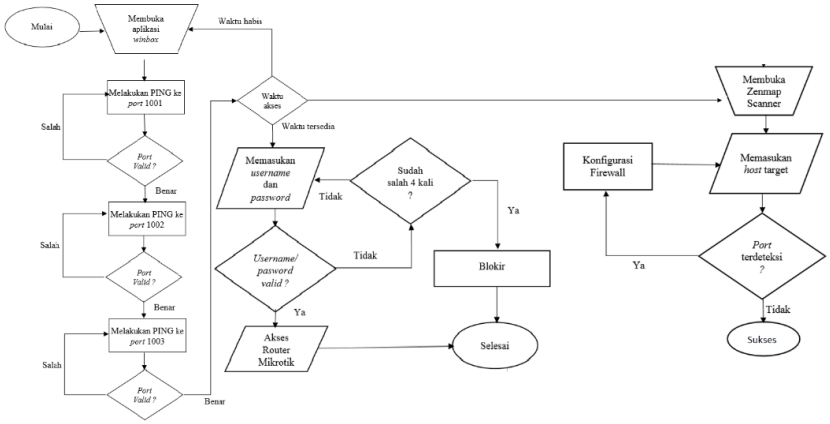
Berdasarkan topologi sistem berjalan ,dengan menggunakan IP *class* C dengan menggunakan *network* 192.168.1.0/27, dan 192.168.1.1 sebagai *host* yang tersambung dengan *modem* dengan akses *internet* dan IP 172.8.6.40 dari ISP untuk menyalurkan *internet* ke mikrotik untuk disebarkan melewati *switch*. Maka perlu ditambahkan sebuah *firewall* yang bertugas untuk mengamankan jaringan komputer, dengan menerapkan metode *port knocking* diharapkan dapat menambah keamanan *server* jaringan komputer

3. *Simulation prototype*: Pada tahap ini akan dilakukan simulasi *port knocking* pada perangkat mikrotik dimaksudkan untuk melihat fungsionalitas pada sistem kemanan jaringan.
4. *Implentation*: Pada tahap ini akan dilakukan penerapan sistem keamanan jaringan dengan berdasarkan hasil analisa dari tahap sebelumnya yang dilakukan pada sistem dengan metode *port knocking* yang mempunyai cara kerja menutup *port* yang ditentukan sehingga *user* hanya bisa mengakses *server* dengan cara mengetuk (*knock*) terlebih dahulu. Berdasarkan data pada Gambar 3.

No	*Port* di *knock*	Urutan Port Knocking			Waktu akses
		1	2	3	
1	1001				60 Detik
2	1002				60 Detik
3	1003				60 Menit

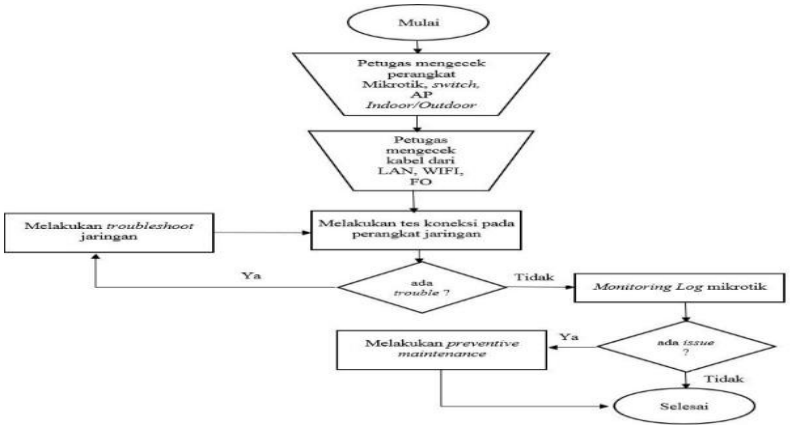
Gambar 3 Tabel *Port Knocking*

5. *Monitoring*: Pada tahap ini dilakukan *monitoring* terhadap hasil yang telah di implementasikan dengan melakukan *monitoring* pada l*og* mikrotik secara teratur dan juga dilakukan beberapa tahap pengujian. Berdasarkan alur pada Gambar 4.



Gambar 4 Alur Pengujian

6. *Management*: Tahap terakhir ini perlu dibuatkan kebijakan yang mengatur agar sistem yang telah dikembangkan dapat berjalan dengan baik serta dapat mengamankan sistem sehingga dapat bertahan lama, maka akan dibuatkan SOP (*Standard Operating Procedure*) yang akan diterapkan. Yang akan diterapkan berdasarkan Gambar 5.



Gambar 5 Alur SOP pengujian jaringan

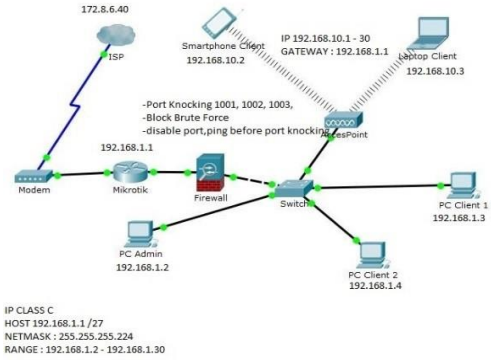
III. HASIL DAN PEMBAHASAN

A. *Analysis*

Pada tahap awal ini dilakukan beberapa tahapan analisis, antara lain: analisis kebutuhan, analisis masalah, analisis kebutuhan pengguna, dan analisis topologi atau jaringan yang sedang berjalan. Metode yang umum digunakan pada tahap ini antara lain wawancara dan studi pustaka.

B. *Design*

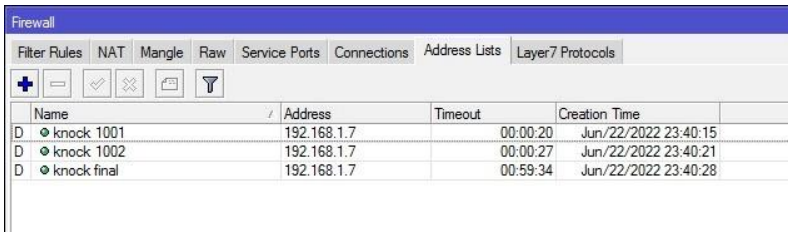
Fase ini digunakan untuk merancang topologi jaringan usulan yang akan dibangun dengan adanya citra ini diharapkan dapat memberikan gambaran tentang topologi yang akan diterapkan. Berdasarkan topologi sistem berjalan maka direkomendasikan topologi sistem usulan dengan menambahkan *firewall* pada perangkat *router* mikrotik yang bertugas untuk mengamankan jaringan komputer, dengan menerapkan metode *port knocking* diharapkan dapat menambah keamanan *server* jaringan komputer.



Gambar 6 Design Topologi Usulan

C. *Simulation Prototype*

Pada tahap ini akan dilakukan simulasi *port knocking* pada perangkat mikrotik berdasarkan Gambar 6 yang dimaksudkan untuk melihat fungsionalitas awal pada sistem kemanan jaringan mikrotik yang menghasilkan *log* pada *address lists* di *firewall* mikrotik seperti pada Gambar 7.



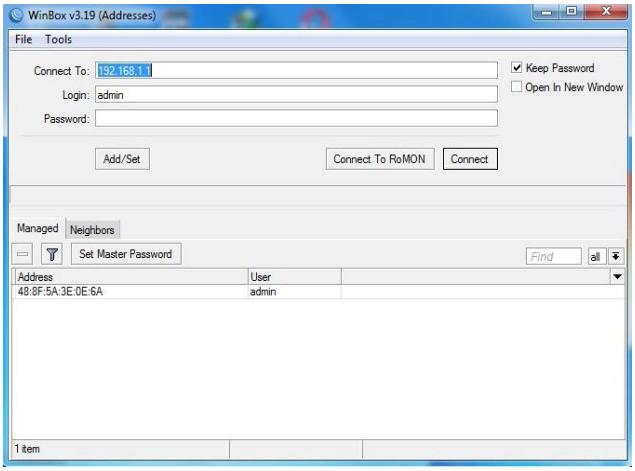
Gambar 7 Log address lists pada firewall

D. *Implementation*

Tahapan keempat ini digunakan untuk mengimplementasikan perencanaan pada rancangan yang telah dibuat sebelumnya sehingga akan sesuai dengan tujuan awal penelitian.

1. Tampilan *login w*inbox

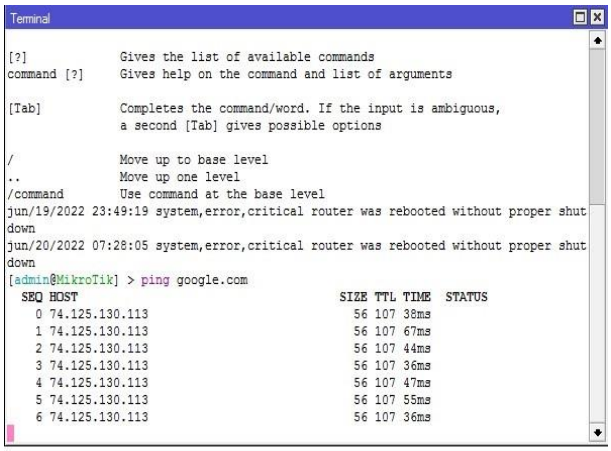
   Pada halaman berikut berfungsi sebagai halaman *login* kedalam Winbox dengan menggunakan akun yang telah dibuat.



Gambar 8 Halaman *Login* Winbox

2. Tampilan winbox yang telah terkoneksi dengan *Internet*

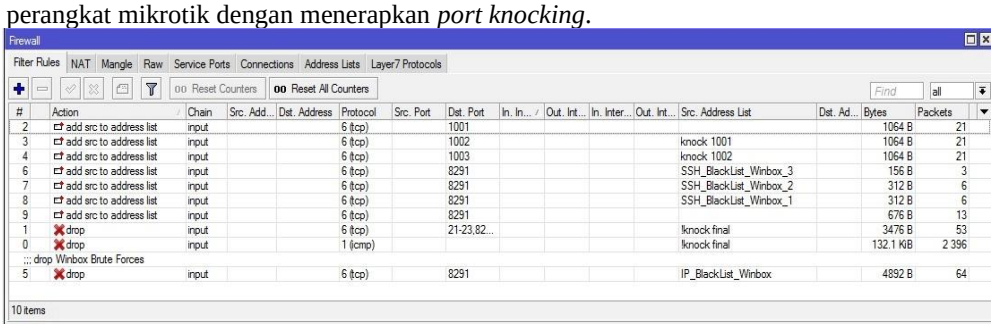
Pada halaman berikut telah diperlihatkan bahwa mikrotik telah terkoneksi dengan *internet* yang bertujuan untuk menghubungkan *router* agar terhubung dengan API Telegram.



Gambar 9 Halaman identity

3. Tampilan hasil konfigurasi pada menu f*irewall*

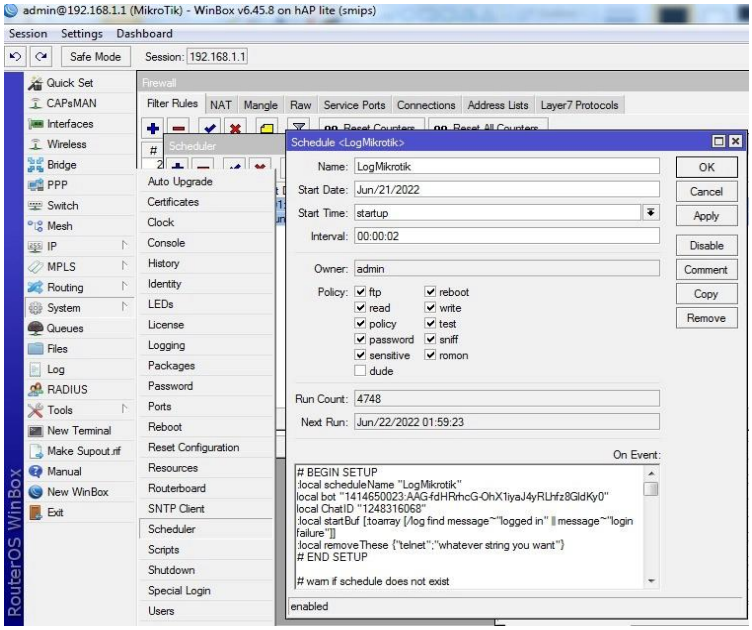
Pada halaman berikut telah diperlihatkan beberapa *filter rule* pada menu *firewall* yang berfungsi sebagai proteksi tambahan pada perangkat mikrotik dengan menerapkan *port knocking*.



Gambar 10 *Filter rule* pada menu *firewall*

4. Tampilan konfigurasi *System Scheduler*

Pada konfigurasi *System Scheduler* berfungsi untuk menghubungkan *log* mikrotik apabila ada percobaan l*ogin* pada perangkat mikrotik, dan akan dikirimkan notifikasi berupa *chat* pada *bot* pada aplikasi telegram yang telah diintegrasikan pada *fitur Scheduler* yang berisi *Script* yang dapat menghubungkan ke API Telegram,



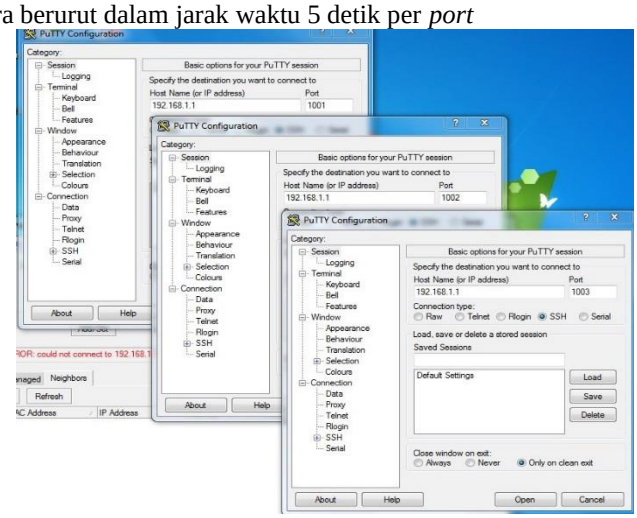
Gambar 11 Konfigurasi *System Scheduler*

E. *Monitoring*

Pada tahap ini dilakukan *monitoring* terhadap hasil yang telah di implementasikan dengan melakukan *monitoring* pada *log* mikrotik secara teratur dan juga dilakukan pengujian melalui aplikasi *open-source* yaitu, Winbox sebagai aplikasi *remote acces* perangkat mikrotik berbasis GUI, Putty sebagai aplikasi *remote acces* berbasis CLI, Zenmap *Scanner* dan *Wireshark* sebagai aplikasi scanning jaringan berbasis GUI.

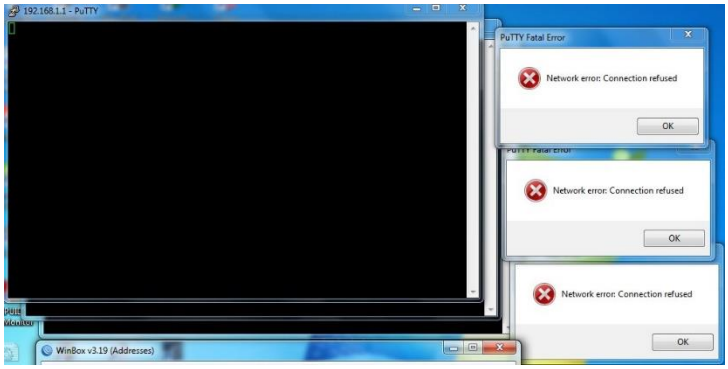
1. Pengujian *Port Knocking*

Pengujian *port knocking* yang dilakukan adalah mencoba *login* tanpa melakukan metode *port knocking* yang menyebabkan tidak dapat tersambung pada *router*. Pada Gambar 12 dilakukan percobaan knocking pada port 1001, 1002, 1003 yang dilakukan secara berurut dalam jarak waktu 5 detik per *port*



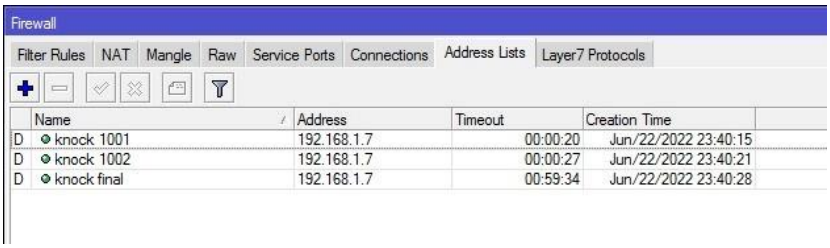
Gambar 12 Gambar percobaan *port knocking*

Hasil *knocking port* pada aplikasi putty akan mendapatkan notifikasi *refused* sebanyak 3 kali dalam waktu yang singkat, namun hal tersebut menjelaskan bahwa pada *host* 192.168.1.1 tidak terdapat *port* 1001, 1002, 1003.



Gambar 13 Notifikasi *Refused Putty*

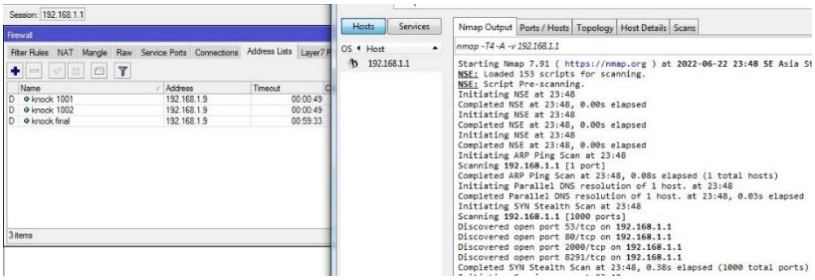
Metode *port knocking* yang dilakukan dicatat pada *Address Lists* dan pada bagian *Timeout* terdapat variasi waktu karena pada *port* 1001 diberi waktu 1 menit untuk dapat mengakses *port* 1002, dan pada *port* 1002 diberi waktu waktu 1 menit agar bisa mengakses *port* 1003, pada *port* 1003, adalah *port* terakhir yang harus dilewati dan diberi waktu 1 jam untuk mengakses *router*.



Gambar 14 Log *Activity Port Knocing*

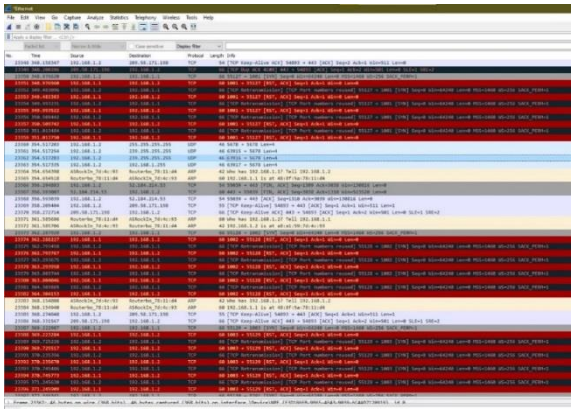
2. Pengujian *Port Scanning*

Pengujian *port scanning* menggunakan aplikasi Zenmap yang berfungsi memindai *port* yang tersedia pada suatu jaringan.



Gambar 15 Hasil proses *scan* Zenmap

Hasil yang didapat setelah proses scanning adalah ditampilkannya *port* 51, 80, 2000, 8291, namun tidak ditampilkannya *port* 1001, 1002, 1003 walaupun sudah dilakukan *port knocking* pada perangkat mikrotik.

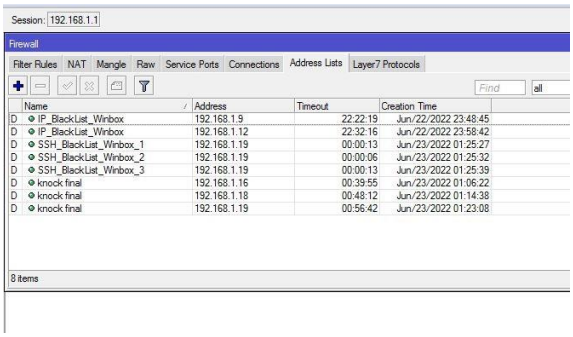


Gambar 16 Hasil proses *scan Wireeshark*

Namun hasil yang didapatkan saat melakukan proses *capture activity network* pada aplikasi *wireshark* dapat membaca *log port* yang digunakan untuk *port knocking*, jika melakukan *port knocking* saat proses *capture* berlangsung.

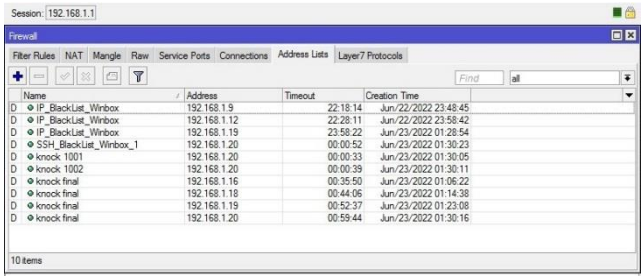
3. Pengujian *Brute Force*

Pengujian *brute force* dilakukan dengan mencoba *login* kedalam mikrotik melewati winbox secara terus menerus.



Gambar 17 Percobaan *Brute Force*

Pada percobaan yang ketiga kali maka *firewall* akan memblokir IP *user* yang telah melakukan percobaan *login* dengan proses salah *password* selama 4 kali berturut – turut, pada IP 192.168.1.19 walaupun sudah melakukan *port knocking*, jika melakukan percobaan *login* salah *password* maka akan masuk menjadi daftar *blacklist*.



Gambar 18 *List Filter Firewall*

Pada percobaan yang ketiga kali maka *status* SSH_BlackList_Winbox_1 sampai 3 akan berubah menjadi IP_BlackListWinbox berdasarkan IP yang di *block*.

Gambar 19 Notifikasi Mikrotik Ke Telegram

Notifikasi yang mengindikasi adanya aktivitas *login* akan terkirim ke akun *bot* telegram *administrator* jaringan.

F. *Management*

Tahap terakhir ini perlu dibuatkan kebijakan yang mengatur agar sistem yang telah dikembangkan dapat berjalan dengan baik serta dapat mengamankan sistem agar dapat bertahan lama, maka perlu dibuatkan SOP (*Standard Operating Procedure*)

Gambar 20 SOP *monitoring* jaringan

IV. KESIMPULAN DAN SARAN

A. Kesimpulan

Kesimpulan dari penelitian yang telah diperoleh adalah sebagai berikut:

1. Hasil penerapan metode *port knocking* pada *firewall* di perangkat mikrotik yang dilakukan pada Cimun Net diterapkan menjadi lebih baik karena belum menggunakan *firewall*, dengan menggunakan metode *port knocking* maka *user* biasa yang tidak memiliki otoritas tidak lagi bisa mengakses perangkat mikrotik dengan bebas, dengan menerapkan tambahan *port* 1001 sampai 1003, jika *user* yang berupaya melakukan *brute force* pada proses *login* maka *user* harus mengetahui langkah – langkah *knocking port* pada perangkat agar bisa masuk sebagai *admin*.
2. Hasil *log* yang muncul pada mikrotik dengan sebuah kata spesifik seperti akses *login succes, login failure*, maka *log* mikrotik tersebut akan langsung terkirimkan melewati aplikasi telegram kepada akun *bot* telegram yang telah dibuat sehingga akan muncul *notifikasi* pada pesan teks dengan kata yang sama pada *log* mikrotik.

B. Saran

Berdasarkan kesimpulan yang didapat, saran-saran sebagai bahan masukan untuk penelitian selanjutnya adalah:

1. Dapat mengembangkan penggunaan metode keamanan jaringan dengan memaksimalkan fungsi *firewall* pada mikrotik sehingga hasil yang diharapkan dapat lebih efektif dalam pengelolaan keamanan jaringan.
2. Dapat lebih mengantisipasi serangan dari luar sistem keamanan jaringan dengan mempelajari dan mengkaji lebih mendalam lagi mengenai ilmu *cyber attack* dan dapat mengamankan sistem.

PENGAKUAN

Naskah ilmiah ini adalah sebagian dari penelitian Tugas Akhir milik Muhammad Rizal Agustian dengan judul Penerapan Metode *Port Knocking* Pada Sistem Keamanan Jaringan Berbasis Notifikasi Telegram, yang dibimbing oleh Tatang Rohana dan Tohirin Al Mudzakir.

DAFTAR PUSTAKA

[1] A. "Analisis Dan Implementasi Keamanan jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking," *Seminar Nasional Sains Dan Teknologi*, pp. 1-7, 2018.

[2] M. Apriani and A. Harbani, "Pengembangan Notifikasi Email Untuk keamanan Port Menggunakan Metode Port Knocking," *Jurnal Ilmiah Teknologi - Informasi dan Sains (TeknoIS)*, pp. 25-36, 2018.

[3] P. Riska, P. Sugiartawan and I. Wiratama, "Sistem Keamanan Jaringan Komputer Dan Data Dengan Menggunakan Metode Port Knocking," *Jurnal Sistem Informasi dan Komputer Terapan Indonesia (JSIKTI)*, pp. 53-64, 2018.

[4] A. and F. Ulum, "Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking," *Jurnal*

TEKNOINFO, pp. 72-75, 2018.

[5] Y. Mulyanto, M. Julkarnain and A. J. Afahar, "Implementasi Port Knocking Untuk Keamanan Jaringan SMKN 1 Sumbawa Besar," *Jurnal Informatika Teknologi dan Sains*, pp. 326-335, 2021.