IMPLEMENTASI KEAMANAN MIKROTIK MENGUNAKAN METODE SIMPLE PORT KNOCKING PADA SMAN 1 NGANTANG

Nasrul Firdaus[1)], Angga Fitriawan[2)]
[1]Program Studi Sistem Informasi, STMIK PPKIA Pradnya Paramita
email: nasrul@stimata.ac.id
[2]Program Studi Teknologi Informasi, STMIK PPKIA Pradnya Paramita
email: angga.fitriawan@yahoo.com

Abstract

A computer network is a group of computers or more that are connected to each other electronically.Network security is currently one of the most important and growing issues.Microtic security at SMAN 1 NGANTANG is still not fully considered, it makes the network administrator nervous about the Brute Force attack.SMAN 1 NGANTANG is a high school located in the poor district of Malang, SMAN 1 NGANTANG has services for students and teachers, namely wifi based on mikrotik.At present the security of mikrotik there has not been prioritized, even the microticists there are still vulnerable to attacks from those who do not have authorization.Because security has not been prioritized, mikrotik there is vulnerable to attacks from outside and inside.Therefore, researchers are interested in implementing the Simple Port Knocking method on the mikrotik server of SMAN 1 NGANTANG.Testing in this study using a router that uses a mikrotik operating system, this study will compare mikrotik without using Simple Port Knocking with mikrotik that use Simple Port Knocking and will be attacked by Brute Force. The results of this study are the comparison table of security mikrotik without using Simple Port Knocking and using Simple Port Knocking.

Keywords: *Mikrotik Security, Firewall, Simple Port Knocking, Brute Force Method, SMAN 1 NGANTANG*

1. PENDAHULUAN

Mikrotik merupakan sebuah sistem operasi yang dipasang pada suatu komputer sehingga komputer tersebut dapat berperan sebagai pengendali dan pengatur lalu-lintas data antar jaringan, komputer jenis ini dikenal dengan nama router. Mikrotik merupakan salah satu server jaringan yang digunakan di Indonesia, Hal tersebut membuat penyerang gencar mencari kelemahan pada mikrotik untuk diserang, beberapa serangan yang digunakan antara lain brute force.

Menurut Indra Gunawan (2016:52) brute force adalah sebuah teknik serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci yang mungkin. Seringkali penyerang memasuki port di server dahulu dan penyerang melakukan brute force untuk mengetahui username dan password admin, penyerang memasuki port seringkali memanfaatkan kelemahan dari firewall server mikrotik.

Firewall merupakan sebuah sistem atau perangkat yang memberi otorisasi pada lalu lintas jaringan komputer yang dianggapnya aman untuk melaluinya dan melakukan pencegahan terhadapa jaringan yang dianggap tidak aman. Firewall berada diantara kedua jaringan seperti internet dan komputer. Didalam router mikrotik terdapat fitur firewall yang berfungsi untuk melindungi dengan cara memutus atau menerima sebuah paket yang akan masuk, melewati, atau keluar router. Firewall yang bisa diterapkan untuk melindungi serangan brute force adalah Simple Port Knocking.

Simple Port Knocking merupakan metode yang digunakan untuk membuka akses ke port tertentu yang telah ditolak oleh firewall pada perangkat jaringan dengan cara mengirimkan paket atau koneksi tertentu. Koneksi bisa berupa protocol TCP, UDP maupuan ICMP. Jika koneksi yang dikirimkan oleh host tersebut sudah sesuai dengan rule knocking yang diterapkan, maka secara dinamis firewall akan memberikan akses ke port yang sudah ditolak.

Penelitian ini menerapkan simple port knocking untuk meningkatkan keamanan dari serangan brute force mikrotik, hasil dari penelitian ini yaitu tabel perbandingan keamanan mikrotik dengan menggunakan simple port knocking dan tanpa menggunakannya

Mikrotik

Menurut Setya Wijaya. (2013) Mikrotik adalah Mikrotik Router OS adalah sistem operasi berbasis Linux yang memberikan kemudahan bagi penggunanya untuk menjadikan komputer menjadi router network yang handal[6]. Mikrotik Router OS selain dapat berfungsi sebagai router

juga dilengkapi dengan fungsi-fungsi firewall, tunneling, bridging dan IP security.

Brute Force

Menurut Syakur, M.S. (2015) Algoritma brute force adalah alur penyelesaian suatu permasalahan dengan cara berpikir yang sederhana dan tidak membutuhkan suatu permikiran yang lama. Algoritma ini merupakan algoritma yang muncul karena pada dasarnya alur pikir manusia adalah brute force (langsung/to the point). Algoritma brute force memecahkan masalah dengan sangat sederhana, langsung dan dengan cara yang jelas langsung ke pusat permasalahan. Algoritma ini biasanya tidak memerlukan teori khusus untuk mengimplementasikannya..

Menurut Indra Gunawan (2016) Brute-force attack adalah sebuah teknik serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci yang mungkin untuk memecahkan password, kunci, kode, atau sebuah kombinasi.

Hydra

Menurut Krisnaldi Eka Pramudita, (2010). Hydra adalah sebuah proyek software yang dikembangkan oleh sebuah organisasi bernama "The Hacker's Choice" (THC) yang menggunakan brute force dan dictionary attack untuk menguji untuk password yang lemah atau password sederhana pada satu atau banyak host remote menjalankan berbagai layanan yang berbeda.Hydra dirancang sebagai bukti untuk menunjukkan kemudahan cracking password karena password yang dipilih buruk. Proyek ini mendukung berbagai layanan dan protokol: AFP, TELNET, FTP, Firebird, HTTP, HTTPS, HTTP-PROXY, SMB, SMBNT, MS-SQL, MySQL, REXEC, RSH, rlogin, CVS, Subversion, SNMP, SMTP - AUTH, SOCKS5, VNC, POP3, IMAP, NNTP, NCP, PCNFS, ICQ, SAP/R3, LDAP, PostgreSQL, TeamSpeak, Cisco auth, Cisco memungkinkan, dan Cisco AAA.

Firewall

Menurut Arie Iswadi (2012) firewall yaitu sebuah sistem atau perangkat keamanan khususnya pada jaringan komputer yang bertugas untuk menjaga lalu lintas data di dalam jaringan komputer berjalan dengan aman, dan dalam waktu bersamaan juga mencegah lalu lintas data yang tidak aman untuk masuk di dalam jaringan komputer.

Menurut Sweetania, D. (2012)Firewall adalah istilah yang biasa digunakan untuk menunjuk pada suatu komponen atau sekumpulan komponen jaringan, yang berfungsi membatasi akses antara dua jaringan, lebih khusus lagi, antara jaringan internal dengan jaringan global Internet.

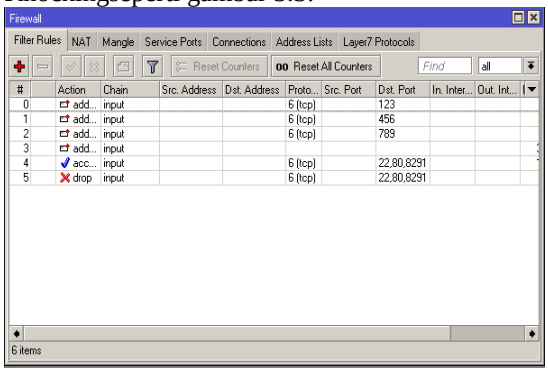
Port Knocking

Port Knocking merupakan metode yang dilakukan untuk membuka akses ke port tertentu yang telah diblock oleh Firewall pada perangkat jaringan dengan cara mengirimkan paket atau koneksi tertentu. Koneksi bisa berupa protocol TCP, UDP maupuan ICMP. Jika koneksi yang dikirimkan oleh host tersebut sudah sesuai dengan rule knocking yang diterapkan, maka secara dinamis firewall akan memberikan akses ke port yang sudah diblock http://mikrotik.co.id/artikel_lihat.php?id=105.

Menurut (Krzywinski, M., 2003.) Port Knocking merupakan suatu sistem keamanan yang bertujuan untuk membuka atau menutup akses block ke port tertentu dengan menggunakan Firewall pada perangkat jaringan dengan cara mengirimkan paket atau koneksi tertentu. Koneksi bisa berupa protocol TCP, UDP, maupun ICMP. Sehingga untuk masuk dan menggunakan akses ke port tertentu yang telah dibatasi, maka user harus mengetuk terlebih dahulu dengan memasukkan rule yang harus dilakukan terlebih dahulu. Rule yang dimana hanya diketahui oleh pihak administrator jaringan

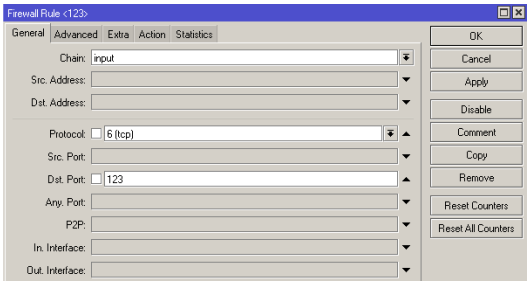
Metode Penelitian

Konfigurasi Simple Port Knocking pertama yang dilakukan yaitu dengan menambahkan konfigurasi Simple Port Knocking pada *Firewal*, Yaitu dengan klik menu IP lalu pilih *Firewall.* Setelah masuk *Firewall* lalu ke *tab filter rules* maka konfigurasi Simple Port Knockingseperti gambar 3.3:



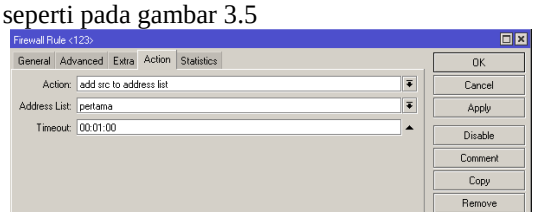
Gambar 3.3 Konfigurasi *Simple Port Knocking.*

Pada konfigurasi ini akan dilakukan membuat rule pertama yaitu *chain input* yaitu membuat rule admin yang mengakses / memasuki mikrotik. Admin yang ingin mengakses mikrotik harus melalui port 123:tcp seperti pada gambar 3.4:



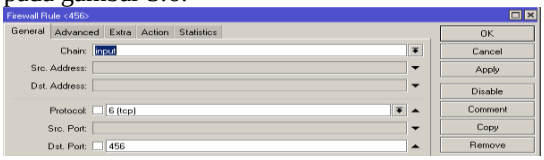
Gambar 3.4 *Setting rule* pertama.

Setelah memasuki mikrotik lewat port 123:tcp akan dimasukan ke *address list* "pertama" seperti pada gambar 3.5



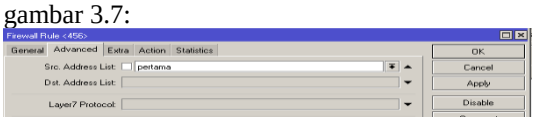
Gambar 3.5 *Setting rule* pertama.

Setelah masuk ke port 123:tcp dan dimasukan addres list "pertama" maka Admin harus masuk lagi melalui port 456:tcp seperti pada gambar 3.6:



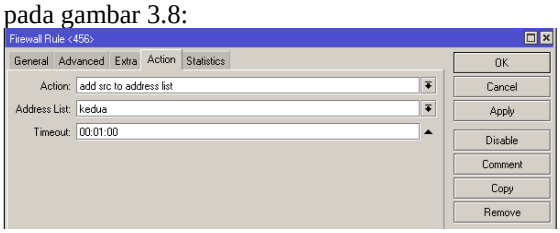
Gambar 3.6 rule kedua

Syarat untuk masuk ke port 456:tcp harus dari *addres list* "pertama" seperti pada gambar 3.7:



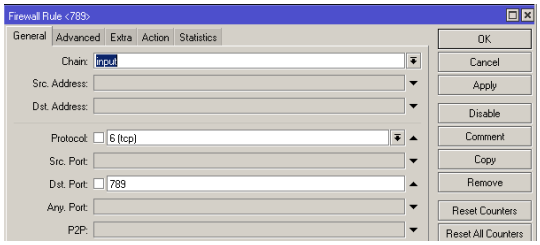
Gambar 3.7 rule kedua

Setelah memasuki port 456:tcp dan berasal dari *addres list* "pertama" selanjutnya akan dimasukan ke *address list* "kedua" seperti pada gambar 3.8:



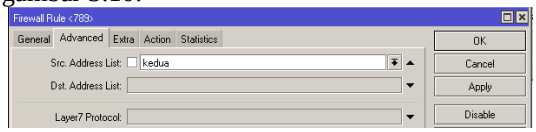
Gambar 3.8 rule kedua.

Setelah masuk ke port 456:tcp dan dimasukan addres list "kedua" maka Admin harus masuk lagi melalui port 789:tcp seperti pada gambar 3.9:



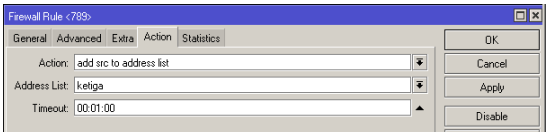
Gambar 3.9 rule ketiga

Syarat untuk masuk ke port 789:tcp harus dari *addres list* "kedua" seperti pada gambar 3.10:



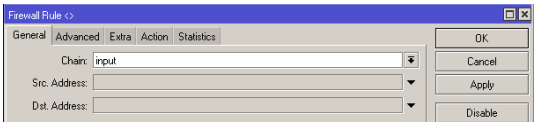
Gambar 3.10 rule ketiga

Setelah memasuki port 789:tcp dan berasal dari *addres list* "kedua" selanjutnya akan dimasukan ke *address list* "ketiga" seperti pada gambar 3.11:



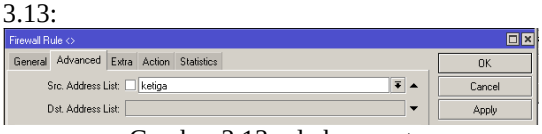
Gambar 3.11 rule ketiga

Setelah masuk ke port 789:tcp dan dimasukan addres list "ketiga" maka selanjutnya membuat rule *chain input* seperti pada gambar 3.12:



Gambar 3.12 rule keempat

Syarat untuk masuk ke mikrotik harus dari *addres list* "ketiga" seperti pada gambar 3.13:

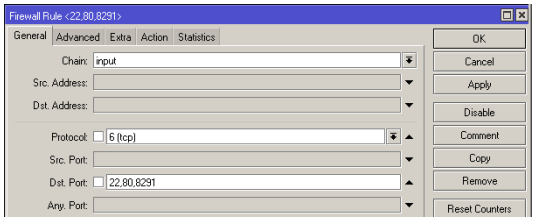


Gambar 3.13 rule keempat

Syarat untuk masuk harus berasal dari *addres list* "ketiga" selanjutnya akan dimasukan ke *address list* "boleh" seperti pada gambar 3.14:

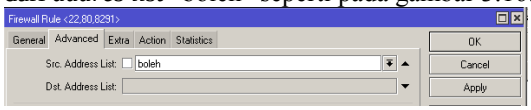
Gambar 3.14 rule keempat

Setelah membuat rule keempat maka selanjutnya harus membuat rule yang memperbolehkan masuk hanya lewat port 22 (ssh), 80 (web), dan 8291 (winbox) seperti pada gambar 3.15:



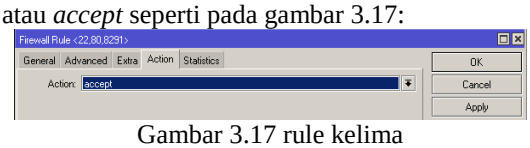
Gambar 3.15 rule kelima

Syarat untuk masuk ke mikrotik harus dari *addres list* "boleh" seperti pada gambar 3.16:



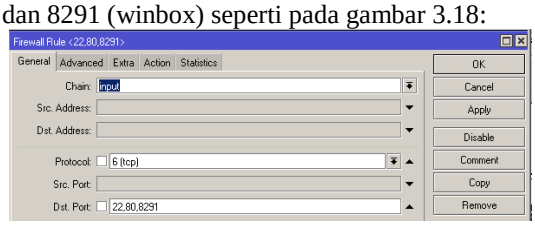
Gambar 3.16 rule kelima

Selanjutnya *address list* "boleh" bisa memasuki mikrotik maka hasilnya diperbolehkan atau *accept* seperti pada gambar 3.17:



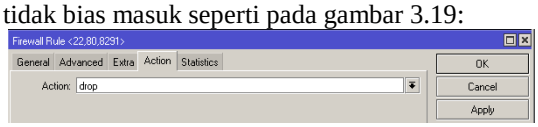
Gambar 3.17 rule kelima

Setelah membuat rule kelima selanjutnya membuat rule yang mencegah user yang ingin masuk ke mikrotik lewat port 22 (ssh), 80 (web), dan 8291 (winbox) seperti pada gambar 3.18:



Gambar 3.18 *rule* keenam

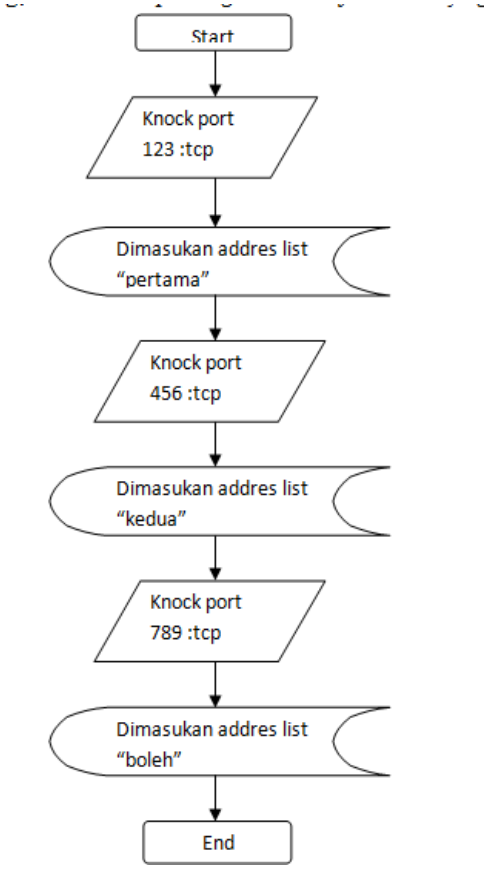
Lalu akan di arahkan ke *action drop* agar tidak bias masuk seperti pada gambar 3.19:



Gambar 3.19 *rule* keenam

Arsitektur Mesin Sistem

Arsitektur sistem keamanan mikrotik dengan menggunakan metode Simple Port Knocking terdapat 3 flowchart Berikut merupakan flowchart Simple Port Knocking Gambar 3.20 :



Gambar 3.21: *flowchart* login mikrotik tanpa konfigurasi *Simple Port Knocking*

Flowchart selanjutnya mengambarkan proses login mikrotik dengan konfigurasi *Simple Port Knocking*,

4. HASIL DAN PEMBAHASAN

implementasi metode Simple Port Knocking yang telah dirancang pada bab sebelumnya dan pengujian terhadap sistem kemanan mikrotik dengan tanpa menggunakan metode Simple Port Knocking. Pengujian pada bab ini bertujuan untuk mengetahui kekurangan sistem dan melengkapi kebutuhan admin jaringan.

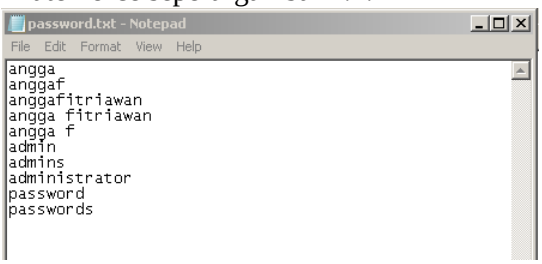
Pada tahap ini dilakukan pengujian terhadap sistem yang belum dikonfigurasi untuk mengetahui hasil yang diharapkan. Pengujian yang akan dilakukan yaitu menggunakan satu komputer dan virtual mikrotik. Pengujian ini dilakukan mulai dari uji coba login mikrotik dengan menyerang dengan brute force untuk mendapatkan login dan password.

Uji coba ini dilakukan untuk mendapatkan login dan password dari mikrotik, proses penyerangan ini dilakukan

dengan cara Brute Force melalui Hydra. Hydra merupakan sebuah tools yang digunakan untuk brute force guna menyerang password yang lemah, Hydra dapat menyerang protocol telnet, HTTP, dan sebagainya. Hydra seperti gambar 4.1:

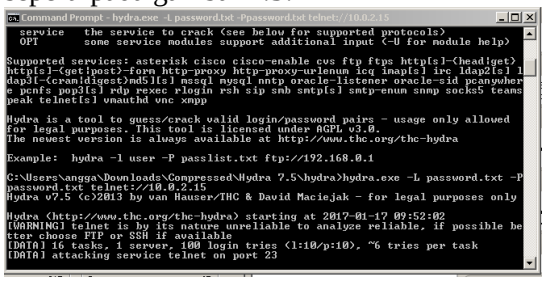
Gambar 4.1 interface Hydra

Hydra memiliki parameter –L, -P dan sebagainya, dan peneliti hanya menggunakan –L dan –P. terdapat perbedaan –L dan –l yaitu jika –L maka harus memasukan file txt yang berisi kamus kata untuk melakukan Brute Force seperti gambar 4.2.



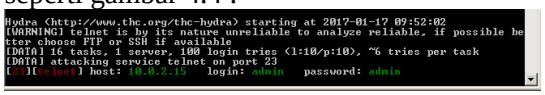
Gambar 4.2 file txt yang berisi kamus kata

Langkah selanjutnya melakukan proses penyerangan Brute Force ke ip mikrotik seperti pada gambar 4.3:



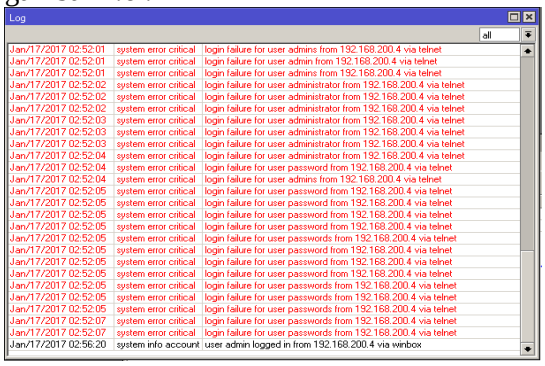
Gambar 4.3 proses Brute Force

Setelah proses brute force selesai maka akan keluar hasil login dan password yaitu login : “admin” dan password : “admin” seperti gambar 4.4 :



Gambar 4.4 hasil penyerangan Brute Force

Dapat disimpulkan bahwa serangan Brute Force berhasil dan dapat login ke mikrotik tanpa kofigurasi Simple Port Knocking. Setelah masuk dapat diketahui bahwa banyak jejak percobaan login ke mikrotik seperti gambar 4.6 :

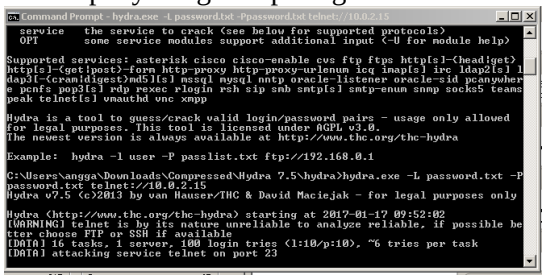


Gambar 4.6 jejak login mikrotik

Pembahasan Hasil Pengujian dan Pengukuran Sistem

Pada tahap ini dilakukan pengujian terhadap sistem yang telah dikonfigurasi metode Simple Port Knocking untuk mengetahui hasil yang diharapkan. Pengujian yang akan dilakukan yaitu menggunakan satu komputer dan virtual box. Pengujian ini dilakukan mulai dari login mikrotik dengan menggunakan login dan password yang telah diperoleh melalui penyerangan Brute Force.

Uji coba login mikrotik dengan menggunakan login dan password melalui penyerangan Brute Force, dan mikrotik yang telah dikonfigurasi Simple Port Knocking. Proses penyerangan seperti gambar 4.7:

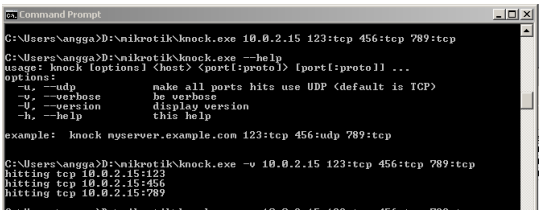


Gambar 4.7 serangan Brute Force

Setelah beberapa saat maka akan mendapatkan login dan password untuk bisa masuk ke mikrotik seperti gambar 4.8:

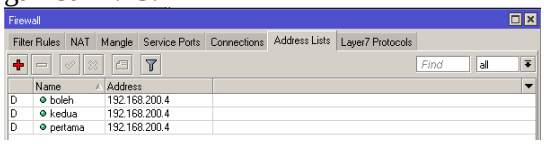
4.8 hasil Brute Force

Setelah menyerang dengan Brute Force dan mendapatkan hasil login dan password.Langkah selanjutnya untuk bisa masuk ke mikrotik maka terlebih dahulu memberikan rule ke mikrotik dengan mengknock port yang sudah ditentukan dan knock ke ip mikrotik seperti gambar 4.12 :



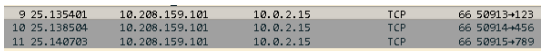
Gambar 4.12 knock port tertentu

Setelah knock port tertentu dan tidak muncul keterangan error maka knock tersebut berhasil dan dapat login ke mikrotik. Dapat diketahui bahwa ip admin yang knock masuk kedalam addreslist whitelist seperti gambar 4.13:



Gambar 4.13 address list

Setelah login dan knock ke mikrotik maka jejak knocking dapat diketahui dengan melihat Log seperti gambar 4.14:



Gambar 4.14 Log Knocking

5. KESIMPULAN

Kesimpulan yang dapat diambil dari hasil penelitian ini yaitu dengan adanya keamanan mikrotik dengan menggunakan metode Simple Port Knocking dapat meningkatkan keamanan mikrotik dalam serangan Brute Force. Hal tersebut membuat admin tidak lagi merasa khawatir akan user yang tidak memiliki otorisasi login kedalam mikrotik yang mana mengetahui login dan password yang didapat dari serangan Brute Force maupun menebak.

Keamanan mikrotik dengan menggunakan metode Simple Port Knocking dapat meminimalisir serangan Brute Force dikarenakan ketika login kedalam mikrotik terlebih dahulu harus mengetahui port yang harus di knock. Kesimpulan dari hasil penelitian ini menghasilkan tabel hasil penelitian : 5.1:

Tabel 5.1: Tabel Hasil Penelitian

Sebelum Dikonfigurasi *Simple Port Knocking*	**SetelahDikonfigurasi *Simple Port Knocking***
Rawan akan serangan user yang tidak memiliki otorisasi melalui *Brute Force* dikarenakan belum dikonfigurasi keamanan mikrotik dengan metode *Simple Port Knocking*	Dengan terkonfigurasi keamanan mikrotik dengan metode *Simple Port Knocking* dapat mencegah user yang tidak memiliki otorisasi melalui *Brute Force* karena ketika *login* harus mengetahui *port* berapa yang harus di *knock* terlebih dahulu

6. REFERENSI

Anonim. 2005. *Simple Port Knocking*.(http://mikrotik.co.id/artikel_lihat.php?id=105, 12 November 2016 14.24 WIB).

Anonim. 2011. *WINBOX* (http://www.trainingmikrotik.co.id/artikel/winbox-22.html, 12 November 2016 15.24 WIB).

Aprianto, Asmunin. 2016.*Implementasi simple port knocking pada dynamic routing (ospf) menggunakan simulasi gns3*.Manajemen Informatika, 5(2): 7 – 17.

Asyikin, Noor Arifin. 2013. *Arsitektur Jaringan Komputer Di Perpustakaan Madrasah Aliyah Negeri 1 Yogyakarta*.Poros Teknik, 5(1): 33 – 50.

Gunawan, I. 2016.*Penggunaan Brute Force Attack Dalam Penerapannya Pada Crypt8 Dan Csa-Rainbow Tool Untuk Mencari Biss*.InfoTekJar, 1(1): 52 – 55.

Harwood, Mike. (2009). *CompTIA Network+*. N10-004 Exam Prep (3rd Edition)

Haryanto, E., Widyawan., Adhipta, D. 2016. *Meningkatkan Mekanisme Keamanan Otorisasi Port Dengan Metode Simple Port KnockingTunneling*. SRITI, issn: 2502-6526 : 187 – 194.

Ikhwan. S., Elfitri, I. *Analisa delay yang terjadi pada penerapandemilitarized zone (dmz) terhadap server universitas andalas*. Jurnal Nasional Teknik Elektro, 3 (2): 118-124.

Irawan, Budhi. 2005. *Jaringan Komputer*. Graha Ilmu, Yogyakarta: 69-70.

Irawan, Dedi. 2015. *Keamanan Jaringan Komputer Dengan Metode Blocking*

Port Pada Laboratorium Komputer Program Diploma-Iii Sistem Informasi Universitas Muhammadiyah Metro. Jurnal Manajemen Informatika Program Diploma III UM Metro, 2 (5): 1-9 .

Iswadi, Arie. 2012. *Optimalisasi Jaringan Wireless Dengan Router Mikrotik Studi Kasus Kampus Bsi Tangerang.* BSI Purwokerto, ISSN: 2338 - 8161 2(1): 37 – 45.

Krzywinski, M. 2003. *Network Authentication Across Closed Ports*. Sys Admin, 12 (6): 9-12.

Pamungkas, Ajika Canggih. 2016. *Manajemen Bandwith Menggunakan Mikrotik Routerboard Di Politeknik Indonusa Surakarta.* Politeknik Indonusa Surakarta, ISSN : 2442-7942

Permadi, A. F., Raharjo. D.S., Christyowidiasmoro.2013. *Keamanan Jaringan pada IPTV*. POMITS, 1 (1): 1-6.

Pratama, I.P.A.E. 2014.*Smart City Beserta Cloud Computing dan Teknologi – Teknologi Pendukung Lainnya*. Bandung: Informatika Bandung.

Sumardi, Triyono, R.A. 2013. *Rancang bangun sistem keamanan jaringan dengan metode blocking port pada sekolahmenengah kejuruan karya nugraha boyolali*.IJNS.issn: 2302-5700. 2 (1):16 - 21.

Sweetania, D. (2012). *Uji Coba Teknologi Security Firewall Pada System Networking Dengan Menggunakan Microsoft Forefront Threat Management Gateway.* UG Jurnal. 6(2): 1 – 8.

Syakur, M. S., Wijanarto. 2015. *Generator Teka-Teki Silang Menggunakan Algoritma Backtracking dan Brute Force.* Journal of Applied Intelligent System, 1(1): 25-34.

Tamutama, Luka, Tamutama, H. 1993 .*Mengenal Local Area Network (LAN).* Jakarta: PT Elex Media Komputindo

Wijayanta, S., Muslihudin.2013. *Pembangunan Web Proxy Dengan Mikrotik Untuk Mendukung Internet Sehat Di Smk Muhammadiyah 1 Patuk Gunungkidul.* Universitas Ahmad Dahlan. 1 (1) : 259 – 267.

Yuwono, Tjahyadi. 1994. *Base III + Fox Base + Multi User (Local Area Network).* Jakarta: PT Elex Media Komputindo.