IMPLEMENTASI SIMPLE PORT KNOCKING PADA DYNAMIC ROUTING (OSPF) MENGGUNAKAN SIMULASI GNS3

Aprianto Puji Adi Kusuma
Manajemen Informatika, Fakultas Teknik, Universitas Negeri Surabaya, apriantopujiadi@outlook.com

Asmunin
Jurusan Teknik Informatika, Fakultas Teknik, Universitas Negeri Surabaya, asmunin@yahoo.com

Abstrak

Keamanan sistem pada komputer adalah salah satu tugas dari sistem administrator. Hal ini berdasarkan pada karakteristik umum jaringan komputer yang pada dasarnya tidak aman untuk diakses secara bebas. Berbagai celah sisi server untuk membuat pihak tidak bertanggung jawab untuk mencoba masuk ke sistem dengan berbagai teknik. Membuka port untuk akses layanan yang umum merupakan hal yang pribadi, tetapi memiliki risiko tinggi untuk kemungkinan akan diserang oleh attacker.

Penelitian ini menekankan pelaksanaan dalam melakukan port knocking untuk melakukan autentifikasi ke port maupun server. Meskipun server-side firewall yang dipasang sudah cukup canggih, namun hingga sampai saat ini masih bisa diserang oleh attacker. Hal ini karena port terbuka dan dapat dilihat oleh pihak luar dengan melakukan scanning port. Dalam penelitian ini, penulis menjelaskan implementasi menggunakan metode simple port knocking untuk memberikan akses filter pada firewall, bertujuan memberikan keamanan untuk pengguna akses komputer sehingga tidak akan ada pencurian data atau informasi sehingga data tetap terjaga aman.

Hasil akhir penelitian menunjukkan bahwa autentifikasi untuk port sehingga membuat server aman, karena penutupan port untuk mencegah adanya serangan akses dari attacker yang tidak berhak untuk mengakses server. Dengan menggunakan metode port knocking akan membuat attacker akan berusaha lebih keras untuk menembus dinding system pada firewall.

Kata Kunci: Port Knocking, Port, Firewall, Autentifikasi, Attacker.

Abstract

The security system on your computer is one of the tasks of system administrators. It is based on the General characteristics of the network computers that are basically not safe to be accessed freely. A variety of server-side slits to make irresponsible parties to try to get into the system with a variety of techniques. Open the port for access to public services is a personal thing, but have a high risk for are likely to be attacked by the attacker.

This study emphasizes the implementation of port knocking in doing to do the authentication credentials to the port or the server. Although the server-side firewall installed already quite sophisticated, but up until now still can be attacked by the attacker. This is because the port is open and can be viewed by outside parties by carrying out port scanning. In this study, the authors describe a simple method using implementations of port knocking to grant access the filter on firewall, aims to provide security for user access to the computer so that there will be no theft of data or information so that the data is maintained securely.

Final results of the research indicate that the authentication credentials for the server so as to make port safely, due to the closure of the port to prevent the existence of the attacker access attacks are not entitled to access the server. Using port knocking would make the attacker will try harder to penetrate the walls of the system on the firewall.

Keywords: Port Knocking, Port, Firewall, Authentication, Attacker.

PENDAHULUAN

Keamanan sistem informasi saat ini menjadi peran yang penting bagi semua pengguna. Terlebih disaat ini kemajuan perkembangan sistem teknologi jaman modern kian semakin maju dan mengalami perubahan yang cukup amat pesat. Dengan semakin majunya teknologi informasi, maka akan memberikan adanya kemampuan untuk mengakses data serta menyediakan berbagai sumber informasi secara cepat, tepat, dan akurat. Sehingga menjadi sarana faktor yang sangat penting bagi suatu organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan, maupun individual (pribadi).

Namun walau memberikan dampak positif yang baik, tapi jika kita lihat seksama muncul sisi dari faktor

negatifnya pula. Dengan begitu maka semakin banyak pula ancaman serangan yang cukup meresahkan bagi pengguna. Maka kini keamanan sistem jaringan dan informasi menjadi suatu pertanyaan, apakah penyimpanan akses data dan informasi akan aman untuk kedepannya. Apabila kita ketahui saat ini akses jaringan internet yang dulunya sifatnya publik kini sudah bukan menjadi rahasia umum lagi, disamping adanya perkembangan teknologi yang semakin maju. Sehingga menyebabkan terjadinya ancaman berupa pencurian data, kerusakan data, system down.

Kini banyak upaya yang secara tidak langsung dapat dilakukan dalam mengamankan suatu data dan informasi yang salah satunya ialah dengan menggunakan Firewall. Akan tetapi penggunaan Firewall itu sendiri masih memiliki kelemahan yang masih bisa ditembus. Maka ditemukan suatu metode yang mampu untuk menghindari dan menutupi kelemahan dari suatu sistem informasi yaitu metode Simple Port Knocking.

Penerapan Simple Port Knocking diusulkan sebagai salah satu metode solusi yang dapat digunakan dalam membantu mengamankan router mikrotik serta monitoring jaringan melalui pembatasasan akses blocking pada port yang terdapat dalam jaringan tersebut. Simple Port Knocking diterapkan karena sistem ini tersebut mampu untuk medeteksi dan menghindari serangan berbahaya pada jaringan dan langsung memberikan peringatan kepada pengatur jaringan (administrator) tentang kondisi jaringannya saat kejadian berlangsung. Penerapan Simple Port Knocking sendiri menggunakan media router Mikrotik yang berfungsi untuk melakukan perubahan konfigurasi setting dan proteksi router sehingga tetap aman dari serangan hacker.

Berdasarkan latar belakang diatas maka dapat diambil rumusan masalahnya adalah bagaimana cara untuk mengimplementasikan akses open dan blocking port menggunakan metode Simple Port Knocking di dalam RouterOS Mikrotik.

Tujuan penelitian ini adalah bertujuan yaitu, untuk dapat mengimplementasikan Simple Port Knocking dengan simulasi cloud menggunakan Dynamic Routing OSPF. Manfaat Simple Port Knocking dalam Firewall diperlukan guna untuk mengamankan data dan informasi.

KAJIAN PUSTAKA

Pada bagian ini akan dijelaskan mengenai berbagai macam bahan referensi tambahan yang akan digunakan sebagai penunjang dalam penulisan tugas akhir ini. Referensi tersebut nantinya juga akan digunakan untuk memberikan tambahan pengetahuan dalam pengujian penelitian *Simple Port Knocking*.

Port Knocking

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. Sebuah sistem harus memiliki keseimbangan antara keamanan dan fleksibilitas. Salah satu cara untuk mencapai sistem seperti demikian yaitu dengan menggunakan akses firewall. Dengan menggunakan firewall, maka secara langsung kita dapat mendefinisikan user yang dapat dipercaya dan yang tidak dapat dipercaya dengan menggunakan alamat IP sebagai kriteria filter.

Kelemahan dari *firewall* ialah bahwa tidak mampu membedakan user yang dapat dipercaya. Karena firewall hanya mampu membedakan alamat IP yang diasumsikan digunakan oleh orang yang tidak dapat dipercaya. Untuk mendapatkan tingkat keamanan yang diperlukan dan kemampuan untuk mengizinkan user yang bisa dipercaya untuk mengakses sebuah server atau jaringan maka diperlukan suatu metoda yang memenuhi dua syarat kriteria tersebut. Salah satu metoda baru dianggap memiliki kemampuan untuk memenuhi dua kriteria tersebut adalah dengan metode *Port Knocking*. (Krzywinski, M., 2003.)

Firewall

Firewall adalah sebuah sistem atau perangkat lunak yang mengizinkan komunikasi aliran lalu lintas jaringan yang dianggap aman untuk dapat dilaluinya dan mencegah lalu lintas jaringan yang sekiranya dianggap tidak aman. Pada dasarnya sebuah Firewall dipasang pada sebuah router yang berjalan pada gateway antara jaringan local dengan jaringan internet.

Firewall dan paket pada mikrotik digunakan untuk memilih dan memilah paket yang akan diizinkan (accept) dan paket yang tidak diizinkan (drop). Ketentuan ini merupakan kebutuhan dari konfigurasi sebuah jaringan tersebut. (Towidjojo, Rendra:2016)

Mikrotik

Mikrotik adalah system operasi yang bisa dijalankan pada sebuah PC atau pada sistem mini Routerboard yang bisa berfungsi sebagai router, bridge, hotspot gateway, firewall, bandwith limiter, dll. Mikrotik dibuat oleh ***MikroTikls*** sebuah perusahaan di kota Riaga, Latvia yang merupakan “pecahan” dari negara Uni Soviet yang kini

dikenal sebagai Rusia. Mikrotik pada awalnya ditujukan untuk perusahaan jasa layanan Internet (*PJI*) atau *Internet Service Provider*(*ISP*) yang bertujuan melayani pengguna (end-user) dengan menggunakan teknologi nirkabel atau wireless. Mikrotik merupakan merk dagang dan juga sebagai sistem operasi berbasis linux kernel 2.6 yang dibuat khusus untuk komputer yang dirubah fungsinya sebagai router. Saat ini Mikrotikls memberikan layanan kepada banyak ISP nirkabel untuk menikmati suatu layanan akses Internet dibanyak negara di dunia dengan menyediakan hardware dan software. (Andi, 2008)

GNS3 (Graphic Network Simulator version 3)

Graphic Network Simulator (*GNS3*) adalah open source (*GNU GPL*) perangkat lunak yang dapat mensimulasikan jaringan dengan masalah yang kompleks dan mendekati dari cara jaringan nyata, semua ini tanpa didedikasikan perangkat keras jaringan seperti router dan switch (Joko Saputro, 2010:4). *GNS3* itu sendiri adalah sebuah program graphical network simulator yang dapat mensimulasikan topologi jaringan yang lebih kompleks dan sangat mudah diakses hanya "plug and play" dibandingkan dengan simulator lainnya. *GNS3* menyediakan antar muka penggunaaan grafis untuk merancang dan mengkonfigurasi di jaringan virtual, itu berjalan pada hardware PC dan dapat digunakan pada beberapa sistem platform operasi termasuk Windows, Linux, dan Mac OS X. Dalam memberikan simulasi yang lengkap dan akurat , *GNS3* adalah emulator untuk menjalankan sistem operasi yang sama seperti pada jaringan nyata.

OSPF (Open Shortest Path First)

Open Shortest Path First (*OSPF*) merupakan protocol routing link state dan digunakan untuk menghubungkan router-router yang yang berada dalam satu *Autonomus System* (*AS*), sehingga protocol routing ini termasuk juga dalam kategori *Interior Gateway Protocol* (*IGP*). *OSP*F dikembangkan untuk menutupi kekurangan-kekurangan yang dimiliki oleh *RIP*, terutama pengimplementasian di jaringan berskala besar, *RIP* mempunyai kekurangan dalam kecepatan mencapai kondisi konvergensi untuk jaringan berskala besar. Untuk dapat menangani jaringan yang berskala besar, maka *OSP*F menerapkan konsep area dalam implementasinya, yaitu single Area untuk jaringan berskala kecil dan Multi Area untuk jaringan berskala besar. Router yang menjalankan *OSPF* hanya akan bertukar informasi route (*routing update*) dengan router *OSPF* lainnya yang berada dalam satu *Autonomus System* (*AS*). Router OSPF akan mengirimkan beberapa paket *OSPF* lainnya yang ke semuanya digunakan membentuk table routing. Pada *OSPF* dikenal kondisi adjency antar router. Sebelum router-router tersebut bertukar informasi routing, maka sebuah router harus terlebih dahulu mencapai kondisi adjency (bertetangga dan bersepakat) dengan router tetangganya. Router-router tidak akan bertukar routing update jika kondisi adjency belum tercapai. (Anonim, 2016)

Port

Port adalah suatu mekanisme yang 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 dimana sebuah server dapat memberikan sebuah layan kepada klien atau bagaimana sebuah layanan kepada klien atau bagaimana sebuah layanan kepada klien dapat mengakses sebuah layanan yang ada dalam server. Port dapat dikenali dengan angka 16-Bit (dua byte) yang digunakan, ke dalam Port TCP dan Port UDP. Karena memiliki angka 16-bit, maka total maksimum yang digunakan adalah 65536 buah.

OSI (Open System Interconnection)

Open System Interconnection (OSI) dibuat pada tahun 1977 oleh suatu organisasi yang bernama International Organization for Standardization (ISO). Model Osi menjadi suatu acuan untuk network communication dan dikatakan bahwa sistem tersebut open system architecture. Bahwasannya di karenakan bahwa model OSI tersebut menghubungkan satu komputer dengan komputer lainnya menggunakan komunikasi terbuka atau saling berlawanan. Komputer yang terhubung tidak harus selalu pabrikan dan memiliki sistem yang sama.

OSI model terdiri dari tujuh layer. Masing-masing layer menggambarkan fungsi yang akan dilakukan ketika data ditransfer antara dua aplikasi yang saling berkomunikasi. OSI Model akan menjadi rujukan untuk pengembang aplikasi pada saat mengembangkan sebuah aplikasi yang akan digunakan pada jaringan. (Edison Siregar, 2010)

Router

Router adalah sebuah perangkat jaringan yang memiliki peran sebagai pengaturan aliran data WAN (Wide Area Network) yang berada di rute sekitar jaringan. Dengan memeriksa data yang diterima, router dapat menentukan alamat tujuan data dengan menggunakan routing table yang dapat menentukan cara terbaik untuk menlanjutkan perjalanan data. (Harwood, 2009)

Router menggunakan konfigurasi software *network address* keputusan terhadap data yang masuk dan keluar. Hal ini yang membuat router lebih kompleks karena harus bekerja lebih keras untuk menentukan informasi.

TCP/IP

Transmission Control Protocol / Internet Protocol atau yang biasa kita kenal dengan (*TCP/IP*) adalah standar komunikasi data yang digunakan oleh komunitas internet dalam proses tukar-menukar data dari satu komputer ke komputer lain di dalam jaringan Internet. Protokol ini tidaklah dapat berdiri sendiri, karena memang protokol ini berupa kumpulan protokol (protocol suite). Protokol ini juga merupakan protokol yang paling banyak digunakan saat ini.

Protokol ini bersifat routable yang berarti protokol ini cocok untuk menghubungkan sistem yang berbeda. Pengembangan ini dilakukan oleh beberapa badan, seperti halnya Internet Society (ISOC), Internet Architecture Board (IAB), dan Internet Engineering Task Force (IETF). Macam-macam protokol yang berjalan di atas TCP/IP, skema pengalamatan, dan konsep TCP/IP didefinisikan dalam dokumen yang disebut sebagai Request for Comments (RFC) yang dikeluarkan oleh IETF. (Joko,2010)

NAT (Network Address Translation)

NAT (Network Address Translation) merupakan suatu protocol, dimana metode ini adalah proses penulisan ulang (masquerade) pada alamat IP asal (source) dan atau alamat IP tujuan (destination) yang menghubungkan computer ke jaringan internet setelah melalui router dan firewall. NAT digunakan pada jaringan dengan workstation yang menggunakan IP private supaya dapat terkoneksi dengan internet menggunakan IP public atau ke dalam internal jaringan sehingga memiliki hak untuk melakukan akses data atau koneksi ke dalam sebuah jaringan. NAT biasanya digunakan untuk menghubungkan dua atau beberapa jaringan yang spesifikasinya berbeda sehingga jaringan tersebut saling terhubung koneksi satu sama lain. NAT memiliki dua tipe yang dimana kedua jenis tipe tersebut dapat digunakan secara terpisah.

Virtual Box

Oracle VM VirtualBox (Virtual Machine) atau yang biasa sering disebut dengan vbox atau virtualbox. Aplikasi virtualbox dikembangkan oleh Oracle. Awal mula aplikasi ini pertama kali dikembangkan oleh perusahaan Jerman, Innotek GmbH. Februari 2008, Innotek GmbH kemudian diakusisi oleh Sun Microsystems. Dan pada akhirnya Sun Microsystems juga diakuisisi oleh Oracle.

Virtualbox dapat digunakan untuk membuat virtualisasi jaringan computer secara sederhana. Penggunaan virtualbox ditargetkan untuk keperluan seperti server, desktop, dan penggunaan embedded. Berdasarkan jenis VM yang ada, virtualbox merupakan jenis hypervisor type 2.

Virtualbox merupakan suatu alat perangkat lunak secara virtualisasi, yang dapat digunakan untuk mengeksekusi suatu sistem operasi tambahan di dalam sistem operasi utama. Fungsi ini penting jika seseorang ingin melakukan uji coba dan melakukan simulasi instalasi suatu sistem tanpa harus kehilangan sistem yang ada. Aplikasi dengan fungsi sejenis VirtualBox lainnya adalah Vmware dan Microsoft Virtual PC

METODE

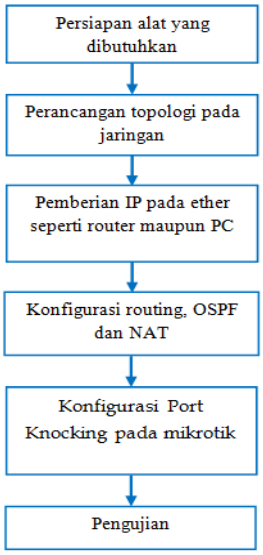
Pada bagian ini akan dijelaskan mengenai analisa sistem, tahapan penelitian, desain jaringan sistem, dan implementasi simulasi sistem yang akan dibuat. Hal ini diperlukan sebagai tahap awal dalam pengujian

Deskripsi Sistem

Metode *Simple Port Knocking* dengan menggunakan *Dynamic Routing OSPF* sebagai cloud atau internet dengan *CHR RouterOS Mikrotik* sebagai sistem operasi. Tujuan dari Port Knocking untuk akses memonitoring bagi administrator jaringan dan mencegah serangan *attacker* yang melakukan scanning port untuk mencuri suatu informasi mengenai data-data yang berada di port yang terbuka pada router atau server sehingga metode ini tidak hanya untuk mengamankan suatu data atau informasi saja melainkan juga antisipasi untuk mengamankan perangkat jaringan seperti router dan server. Dan pengujian akan dilakukan dengan menggunakan bantuan software *VirtualBox* sebagai virtualisasi platform operating system dan *GNS3* sebagai media penghubung virtualbox semacam "*plug and play*".

Tahapan Penelitian

Dalam metode penelitian ini menjelaskan pembahasan tentang langkah-langkah pengujian Implementasi *Simple Port Knocking* dengan menggunakan *Dynamic Routing* (*OSPF*) sebagai cloud (*internet*) dan *RouterOS Mikrotik Cloud Hosted Router (CHR*) menggunakan fasilitas free lisensi dan dengan akses hingga level 6. Tujuan dari implementasi ini berfungsi untuk melindungi user sebagaimana contoh jika perusahaan A maka di perusahaan B dipasangi metode *Port Knocking* sehingga fasilitas keamanan akan data aman dan benar-benar IP yang dapat dipercaya. Proses perancangan metode Implementasi *Simple Port Knocking* menggunakan protokol TCP/ICMP/UDP dengan router Mikrotik akan dijabarkan sebagai berikut.



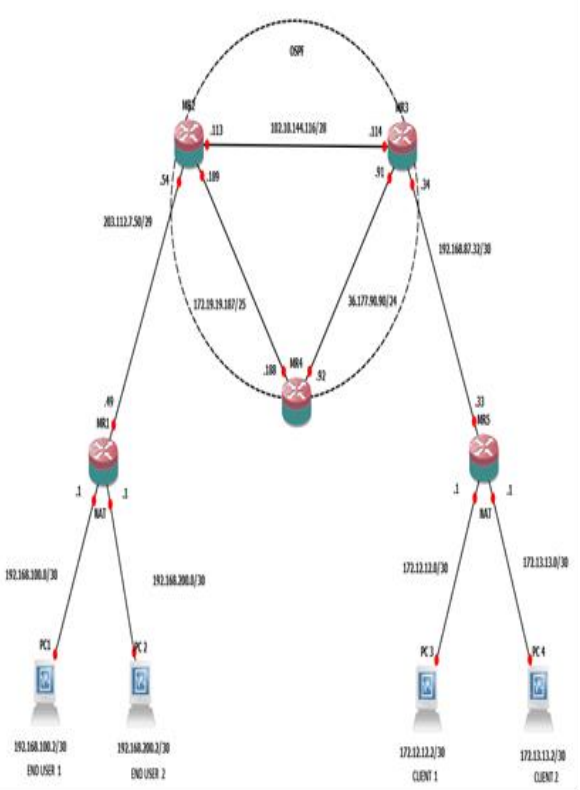
Gambar 1. Tahapan Penelitian Implementasi Simple Port Knocking

Sesuai dengan tahapan penelitian pada Gambar 1, akan dijelaskan secara detail sebagai berikut :

1. Persiapan alat yang dibutuhkan
   Yaitu disini antara lain saya mempersiapkan alat yang dibutuhkan antara lain adalah buku-buku mengenai tentang baik itu mikrotik dan firewall. Dan software yang akan digunakan dalam simulasi Simple Port Knocking seperti Mikrotik RouterOS, VirtualBox, dan GNS3.
2. Perancangan topologi pada jaringan
   Yaitu merupakan rancangan desain jaringan yang digunakan untuk simulasi Simple Port Knocking.
3. Pemberian IP pada ether seperti router dan PC.
   Merupakan pelengkap dari topologi jaringan, yaitu pemberian nama pada perangkat jaringan, kemudian IP address sebagai pengalamatan / pengalokasian alamat yang akan di akses.
4. Konfigurasi routing, OSPF dan NAT
   Dalam penjelasan no.4 ialah setelah selesai membuat desain rancangan topologi jaringan dan pemberian IP address, perlu digaris bawahi dalam topologi ada protocol jaringan. Disini saya menggunakan OSPF sebagai protocol atau pengganti internet, dan NAT sebagai jaringan lain yang diartikan fungsi dari NAT sebagai metode menghubungkan komputer dengan jaringan internet dengan menggunakan satu alamat IP, dimana IP tersebut adalah IP private, dan dirubah menjadi IP public.
5. Konfigurasi Port Knocking pada mikrotik
   Mengenai maksud dan tujuan ini sebagai maksud dari pengimplementasian yang dilakukan si penulis sebagai bentuk sarana ujian Tugas Akhir yang dimana penulis menjelaskan pembahasan mengenai implementasi dari Simple Port Knocking. Yaitu dengan mengkonfigurasi router yang akan diproses sebagai router block port knocking access.
6. Pengujian
   End User sebagai objek sarana untuk akses me-remote client, dimana si End User tersebut tidak dapat mengakses atau mengirimkan paket data kepada client yang terhubung ke mikrotik yang sudah di konfig port knocking. Sehingga dalam pengujian ini End User harus melakukan akses open port knocking, dan mengikuti rule yang telah disediakan oleh Administrator jaringan sebagaimana kunci akses rule untuk membuka mikrotik yang telah di konfigurasi port knocking, sehingga End User dapat mengirimkan paket data atau dapat terkoneksi ke PC Client.

Desain Jaringan

Dalam penelitian implementasi metode Simple Port Knocking dengan menggunakan sebuah jaringan antar sesama routing yang dikenal sebagai akses *Dynamic Routing* (*OSPF*) sebagai cloud. Dalam pengujian dari lima buah router yang akan saling koneksi terhubung router satu sama lainnya, dimana satu diantara lima router tersebut menjadi media uji penelitian Simple Port Knocking yang berfungsi membatasi End User (PC) agar akses koneksi ke client saat mengirimkan data maupun komunikasi yang akan dilewati host tidak mudah, sebelum melewati rule yang sudah diatur untuk bukti bahwa telah diakui sebagai user yang dipercaya.



Gambar 2. Perancangan desain jaringan Simple Port Knocking

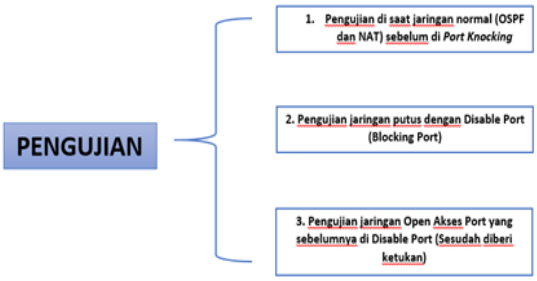
Berikut ini penjelasan detail mengenai Gambar 2 ;

1. *End User*
   End User merupakan pengguna yang menggunakan teknologi jaringan komputer. Salah satu fungsi peran dari End User ialah sebagai me-remote atau me-monitoring akses jaringan.
2. *Client*
   Client adalah pengguna yang menggunakan jaringan komputer yang bertujuan sebagai uji coba simulasi Simple Port Knocking. Dimana akses ke client ini telah di block akses port.
3. *Router*
   Router adalah sebuah alat jaringan komputer yang mengirimkan paket data melalui sebuah jaringan atau internet menuju tujuannya, melalui sebuah proses yang dikenal sebagai routing. Fungsi router ialah penghubung antar dua jaringan untuk meneruskan data dari satu jaringan ke jaringan yang lainnya.
4. *NAT (Network Address Translation)*
   NAT merupakan proses penulisan ulang pada alamat IP ke alamat IP tujuan. Digunakan untuk IP private supaya dapat terkoneksi ke internet dengan menggunakan satu atau lebih IP public.
5. *Dynamic Routing (OSPF)*
   Dynamic Routing merupakan fungsi dari routing protocol yang menghubungkan router yang satu dengan lainnya sebagai indikasi internet. Dan Dynamic Routing dapat menentukan sendiri route berdasarkan situasi kondisi setiap saat. Simulasi cloud dengan menggunakan OSPF.

Untuk pembagian network IP address pada masing-masing perangkat yang ada pada Gambar 2 akan dijelaskan secara detail, sebagai berikut ;

1. R1
   Ethernet 1 : 203.112.7.49/29
   Ethernet 2 : 192.168.100.1/30
   Ethernet 3 : 192.168.200.1/30
   End User 1 : 192.168.100.2/30
   End User 2 : 192.168.200.2/30
2. R2
   Ethernet 1 : 203.112.7.54/29
   Ethernet 2 : 102.10.144.113/28
   Ethernet 3 : 172.19.19.189/25
3. R3
   Ethernet 1 : 102.10.144.114/28
   Ethernet 2 : 36.177.90.91/24
   Ethernet 3 : 192.168.87.34/30
4. R4
   Ethernet 1 : 36.117.90.92/24
   Ethernet 2 : 172.19.19.188/25
5. R5
   Ethernet 1 : 192.168.87.33/30
   Ethernet 2 : 172.12.12.1/30
   Ethernet 3 : 172.13.13.1/30
   Client 1 : 172.12.12.2/30
   Client 2 : 172.13.13.2/30

Skenario Pengujian



Gambar 3. Skenario Pengujian

Berikut ini merupakan penjelasan detail mengenai tahapan dari skenario pengujian yang ada pada Gambar 3, maka penjelasan sebagai berikut :

1. Pengujian disaat jaringan normal *(OSPF dengan NAT)*

Pengujian disaat jaringan antara routing (komunikasi 2 arah) kemudian jaringan tersebut dipisahkan dimana menggunakan protocol OSPF dan NAT. Disaat jaringan normal koneksi akan melewati jalur utama yang ditentukan dengan menjadikan jalur alternatif sebagai jalan OSPF. Ketika Client dan Host yang ada pada jalur routing di konfigurasi sebagai jaringan NAT maka akan terputus. Tidak akan bisa berfungsi koneksi sebagaimana semestinya meskipun jalur sudah diberikan gateway sebagai jalur jalan yang harus lewati sebagai peralihan ke jalur utama. Dan setelah jalur utama yang mengalami kendala sudah mulai berangsur normal koneksi kembali seperti semula, ketika redistribusi-connected dibuka dari OSPF media jalur utama yang dilewati NAT sebagai jaringan yang bukan dari OSPF agar dikenali jaringan yang dipercaya.

2. Pengujian jaringan putus dengan disable port (Blocking Port)

Melakukan suatu rekayasa pemutusan pada jaringan dengan melakukan disable port pada router yang ingin diujikan. Dengan begitu koneksi akan melewati jalur alternatif sebagaimana semestinya dan ketika itu maka akan terputus dan menampilkan timeout saat melakukan PING dikarenakan port yang digunakan untuk akses dimatikan tersebut. Secara tidak langsung otomatis menggangu konektifitas jalur lainnya. Tetapi fungsi dari pengujian adalah untuk segi keamanan jaringan. Ini salah satu metode yang diperlukan untuk keamanan jaringan baik untuk data komunikasi maupun perangkat jaringan.

3. *Pengujian jaringan Open Akses Port yang sebelumnya Disable Port (Sesudah diberi ketukan)*

Melakukan pengujian open dan blocking pada port dengan menggunakan Port Knocking. Dengan melakukan konfigurasi Port Knocking pada router mikrotik dapat dianalisa masing-masing koneksi pada router tiap router yang diberikan system Port Knocking maka mengetahui bahwa ada IP yang masuk. Sehingga dapat diketahui bahwa apakah IP ini adalah orang yang tidak dipercaya atau yang dipercaya. Jika tidak dipercaya maka si End User tetap tidak dapat akses pada PC Client, ketika si End User mengikuti rule yang ada yang sudah diikuti maka akan muncul penanda bahwa yang akses PING adalah termasuk IP yang sudah di "white-list" yang artinya IP address tersebut adalah network pengguna yang dapat dipercaya. Dan pengujian ini dikatakan simple adalah end user hanya menggunakan browser sebagai media open akses port knocking.

HASIL DAN PEMBAHASAN

Pada bab ini akan dijelaskan hasil dari tugas akhir yang sudah dibuat. Berdasarkan pembahasan pada bab sebelumnya ada beberapa tujuan yang ingin dicapai, yaitu bagaimana mengimplementasikan akses open dan blocking port menggunakan metode Simple Port Knocking di dalam RouterOS Mikrotik guna untuk menutupi kelemahan firewall yang menjadi kekurangan dalam sistem keamanan dan mengamankan data dari hal yang tak diduga.

Hasil Penelitian

Hasil pada tugas akhir ini berupa akses yang memerlukan autentikasi validasi agar sehingga user dapat mengakses jaringan yang telah dikonfigurasi *Simple Port Knocking* pada *firewall* di "*filter*" yang ada pada Mikrotik. Sehingga untuk masuk dan menggunakan akses ke port tertentu yang telah dibatasi, maka user harus mengetuk terlebih dahulu dengan memasukkan rule secara berurutan dan cepat atau yang telah diatur oleh administrator jaringan tersebut. Itu berarti bahwa untuk melakukan konfigurasi kita konfigurasi pada firewall yang ada di router itu sendiri.

Untuk simulasi pada simple port knocking ini sesuai seperti pada Gambar 2 , bahwa pengujian yang akan di lakukan pada router Mikrotik 5. Maka dari itu, lakukan konfigurasi terlebih dahulu pada Router 5 (R5) dengan cara mengetik "*ip firewall filter*". Itu berarti bahwa melakukan sistem metode keamanan jaringan semuanya hanya ada di *firewall* karena cara dan fungsi *simple port knocking* ada di *firewall*. Kemudian menuliskan perintah script ;

a. Add chain=input action=add-src-to-address-list protocol=tcp address-list=sequence address-list-timeout=10 dst-port=60001
b. Add chain=input action=add-src-to-address-list protocol=tcp src-address-list=sequence address-list="white-list" address-list-timeout=1m dst-port=60002
c. Add chain=input action=accept src-address-list=white-list
d. Add chain=input action=drop

```
[admin@RS] /ip firewall filter> print
Flags: X - disabled, I - invalid, D - dynamic
 0   chain=input action=add-src-to-address-list protocol=tcp
     address-list=sequence address-list-timeout=10s dst-port=60001

 1   chain=input action=add-src-to-address-list protocol=tcp
     src-address-list=sequence address-list=white-list
     address-list-timeout=1m dst-port=60002

 2   chain=input action=accept src-address-list=white-list

 3   chain=input action=drop
[admin@RS] /ip firewall filter>
```

Gambar 4. Perintah scrypt *Simple Port Knocking* router 5 (*R5*)

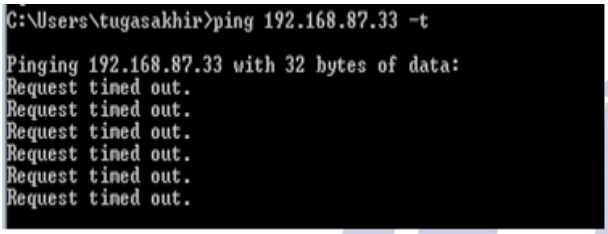
Gambar 4 adalah rule untuk melakukan simple port knocking block akses atau open akses tanpa buka dari firewall. Sehingga pada Gambar 4, akan saya jelaskan secara detail tahapan rulenya sebagai berikut;

a. Koneksi yang masuk dengan protocol TCP. Tambahkan ke addresslist berikut dengan nama listnya "*Sequence*". Dan pada rule 1 ini kita kasih waktu selama 10s. Ketika melebihi 10s , kita tidak memasukkan rule ke-2 maka kita harus mengetuk kembali. Karena harus sesuai dengan urutan rule, mana mungkin langsung loncat ke rule lain. Dengan memasukkan port 60001 untuk membukanya.
b. Koneksi kurang lebih sama penjelasan pada no.1 diatas, bahwa koneksi yang masuk ber-protocol TCP, dengan tambahkan isi yang ada di addresslist yang sudah didaftar dengan nama "*Sequence*", kemudian diberi nama listnya yang baru "*White-List*". *White-List* disini pengertiannya adalah daftar putih dimana bahwa IP yang masuk sudah dikategorikan aman karena melalui proses dari rule ke-1 ketika kita mengetuk rule-1. Dengan waktu 1 menit (1m) ketika, kita sudah mengetuk rule yang ke-2 ini, kita hanya punya waktu 1 menit untuk menggunakan akses tersebut. Dengan mengetuk port 60002.
c. Ketika kita sudah melakukan ketukan ke-1 dan ke-2 maka koneksi yang masuk sumber IPnya terdaftar di white-list.
d. Melakukan block pada akses semua port. Sehingga semua port tidak bisa di akses, bahwa pada rule ke-4 ini kita harus sudah memasukkan rule pada no.1 dan 2. Dan di proses pada rule no.3

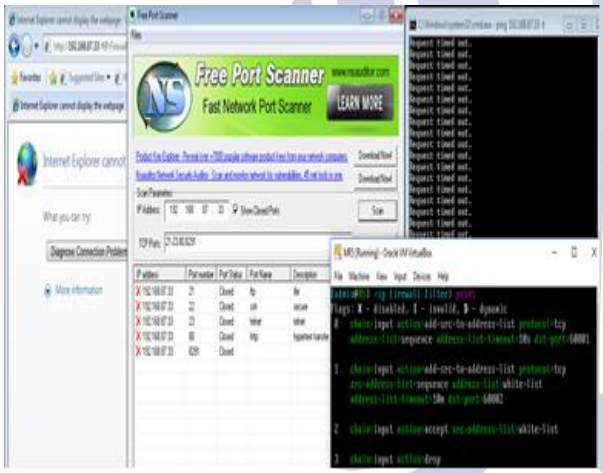
Sehingga saat kita melakukan uji coba test PING atau untuk melakukan akses port pada router 5 (R5) dengan IP

address 192.168.87.33 tidak bisa dilakukan. Dan hasilnya pada gambar sebagai berikut ;

Gambar 5. Ping R1 ke R5 timeout



Gambar 6. Ping PC1(end user) ke R5 timeout



Gambar 7. Melakukan port scanner pada R5 (Port yang tertutup)

Maka setelah dilakukan check port scanner pada R5 kita dapat mengetahui port yang mau kita akses masih tertutup.

Gambar 8. Melakukan telnet pada R1 untuk ke R5 port:60001

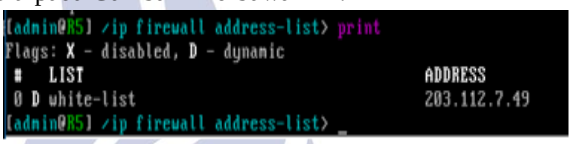
Maka setelah melakukan pada R1 pada Gambar 8 diatas, maka kita telah mendaftarkan list IP address sebagai "*Sequence*". Cara kita mengecheck "*sequence*" melalui router 5 (*R5*) . Yaitu dengan perintah "*ip firewall address-list print*", maka hasilnya seperti Gambar 9 dibawah ini.

Gambar 9. IP address R1 di R5 sebagai "Sequence"

Pada Gambar 9 kita telah terdaftar sebagai address list dengan nama "*Sequence*" dan hanya diberi waktu 10 detik (10s) untuk melanjutkan mengetuk ke rule ke-2. Jika kita lebih dari 10s maka hasilnya IP yang telah ditambahkan ke address list dengan nama "*Sequence*" akan hilang. Alhasil, harus mengetuk lagi.

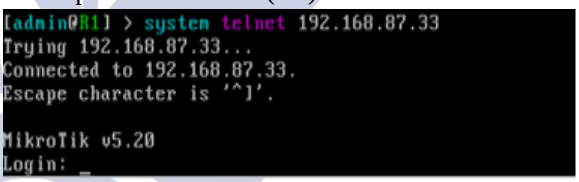
Gambar 10. Melakukan telnet pada R1 untuk ke R5 port:60002

Setelah melakukan rule ke-2 dengan mengisi port 60002, maka secara tidak langsung saat mengecheck router 5 (R5) di "*ip firewall address-list print*" hasilnya seperti pada Gambar 11 dibawah ini.



Gambar 11. IP address R1 di R5 sebagai "White-List"

Maka setelah rule ke-2 diisi, IP yang sudah masuk terdaftar di white list boleh akses router. Dan hasilnya kita bisa melakukan akses ke router 5 (R5) tersebut selama dalam tempo waktu 1 menit (1m).

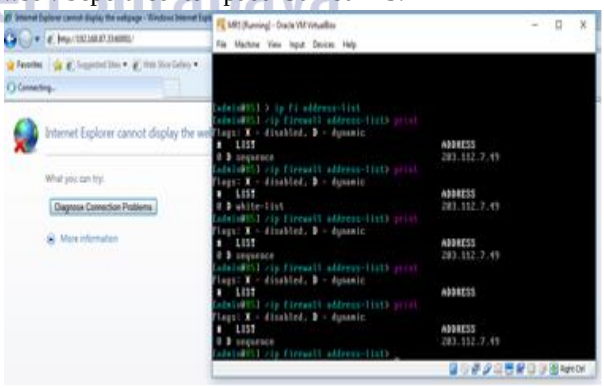


Gambar 12. R1 dapat akses ke R5"

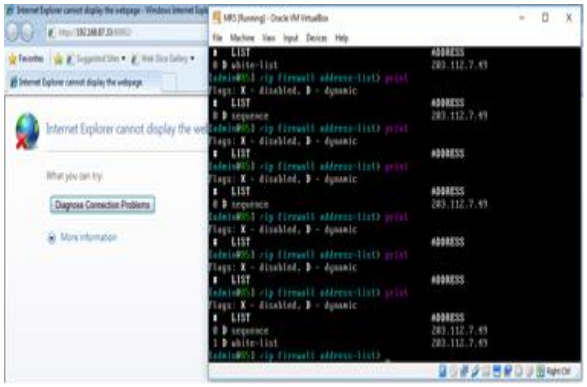
Maka setelah access port knocking dibuka R1 dapat terkoneksi R5, maka PC1 (client) yang terhubung ke R1 dapat akses ke R5.

Simulasi Open Port Knocking menggunakan Browser

Simulasi dilakukan dengan mengetuk ketukan lewat browser. Seperti contoh pada Gambar 13.

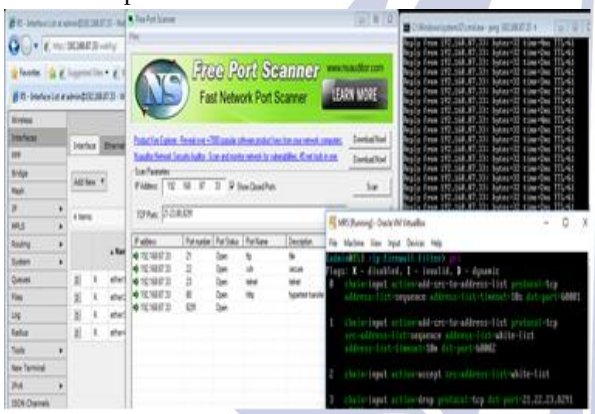


Gambar 13. Ketuk port:60001 lewat browser

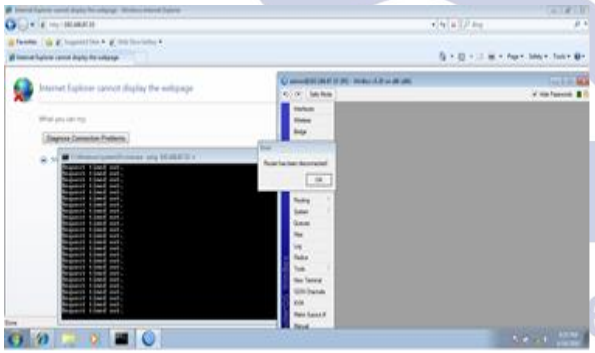


Gambar 14. ketuk port:60002 lewat browser

Setelah kita mengetuk port 60001 dan 60002 pada browser, kini kita dapat akses ke Router 5 (R5) baik itu PING, check port scanner terlihat, atau membuka webfig maupun membuka aplikasi winbox ke IP address 192.168.87.33 pada Gambar 15 ini secara detail.



Gambar 15. Check port scanner setelah diberi ketukan knocking



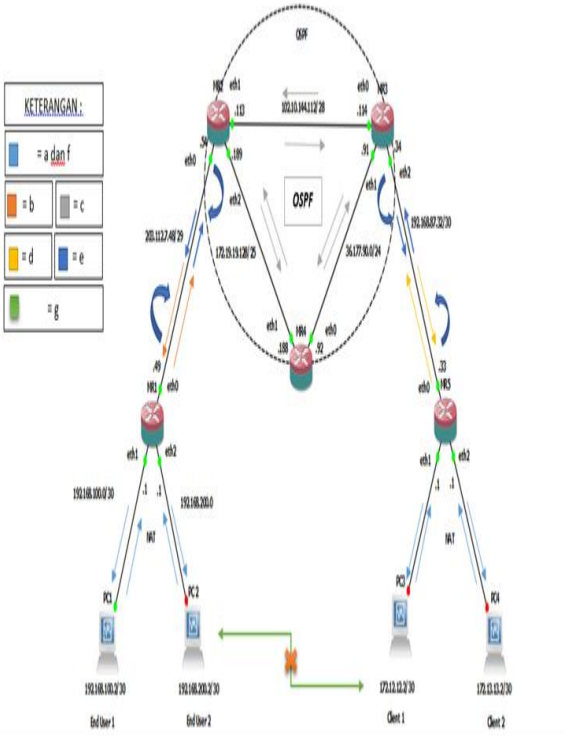
Gambar 16. Akses mengalami disconnect ke R5 lebih dari 1m

Tujuan dari diberikan akses *Time To Live* (***TTL***), ketika si *end user* lupa untuk menutup, maka diberi waktu agar tidak ada orang yang bisa akses selain si *end user* tersebut yang telah diberikan kunci atau rule sistem untuk membuka akses dari port tersebut.

Pembahasan

Pembahasan Jaringan Berjalan Normal (Umum)

Pengujian disaat jaringan berjalan normal dan tidak ada kendala sebagaimana user A mengakses user B sekaligus mengakses ke semua 5 router baik itu router R1, R2, R3, R4, dan R5 serta akses ke computer client sebagaimana koneksi terhubung dikarenakan akses 2 arah (basic routing).



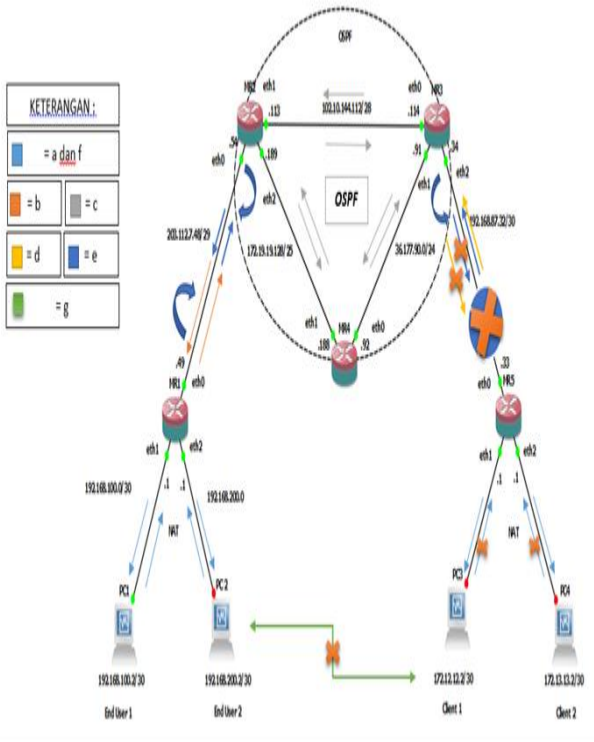
Gambar 17. Pengujian Berjalan Normal (Umum)

Penjelasan Gambar 17, sebagai berikut ;

a. PC End User1 dapat akses ke R1 dan PC End User2, begitu juga sebaliknya.
b. R1 koneksi ke R2 terhubung koneksi 2 arah.
c. R2, R3, R4 koneksi terhubung sebagai OSPF.
d. R5 dapat terkoneksi ke R3 terhubung koneksi 2 arah.
e. R1 dan R5 dapat saling terkoneksi, ketika jalur penghubung ke router (gate router) dimana R1 terhubung ke R2, begitu juga R5 terhubung ke R3 dimana R2 dan R3 tersebut telah diaktifkan "redistribution-connected" untuk mengadvertise R1 dan R5 yang bukan list OSPF menjadi jaringan yang di OSPF.
f. R5 dapat terhubung ke koneksi PC Client1 dan Client2, begitu juga sebaliknya PC Client1 dan Client2 saling terkoneksi dimana sama-sama terhubung ke R5.
g. Antara PC End User 1 dan 2, tidak bisa terhubung koneksi ke PC Client 1 dan 2 dikarenakan jaringan NAT.

Pembahasan Jaringan Setelah diberi Port Knocking (Disabled Port)

Pengujian disaat jaringan diberi akses port knocking pada Router 5 bahwa PC User A dan B maupun R1, R2, R3, R4 tidak dapat akses ke Router 5. Port Knocking yang bertujuan untuk membuat port tertutup dengan beberapa aksi dengan menutup aksesnya melalui firewall tersebut.



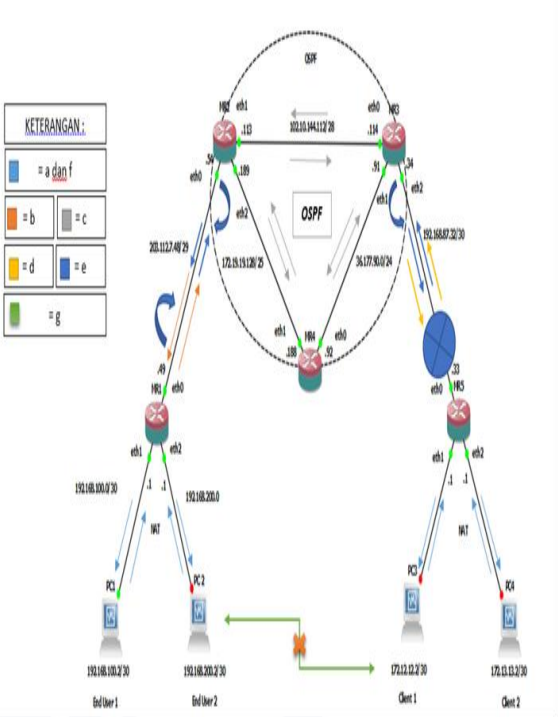
Gambar 18. Pengujian diberi gangguan (putus) pada Router 5 (R5) dengan diberi Port Knocking

Penjelasan Gambar 18, sebagai berikut ;

a. PC End User1 dapat akses ke R1 dan PC End User2, begitu juga sebaliknya.
b. R1 koneksi ke R2 terhubung koneksi 2 arah.
c. R2, R3, R4 koneksi terhubung sebagai OSPF.
d. R5 dapat terkoneksi ke R3 terhubung koneksi 2 arah.
e. R1 dan R5 tidak dapat terkoneksi, meski pun jalur penghubung ke router. Dimana R1 terhubung ke R2, begitu juga R5 terhubung ke R3, dimana R2 dan R3 tersebut diaktifkan "redistribution-connected" untuk mengadvertise R1 dan R5 yang bukan list OSPF menjadi jaringan yang di OSPF tetapi akses semua router untuk ke R5 dari PC End User dan R1,R2,R3,R4 tidak bisa terhubung dikarenakan telah di konfigurasi Port Knocking dikarenakan untuk masuk harus memasukkan autentikasi validasi agar dapat terkoneksi, sementara R5 masih bisa terkoneksi koneksi ke R1, R2, R3, dan R4.
f. R5 dapat terhubung ke koneksi PC Client1 dan Client2, tetapi sebaliknya PC Client1 dan Client2 tidak saling terkoneksi dan tidak bisa terhubung ke R5.
g. Antara PC End User 1 dan 2, tidak bisa terhubung koneksi ke PC Client 1 dan 2 dikarenakan jaringan NAT.

Pembahasan Jaringan Kembali Normal sesudah diberi Ketukan (Open Port Knocking)

Pengujian disaat jaringan berjalan normal ketika sudah mengikuti rule yang diatur konfigurasinya sebagai sistem simple port knocking. Sehingga R1 dapat akses ke R5 melalui R2, atau R3, dan langsung ke R5. Begitu juga dengan PC1 dan PC2 sebagai end user dapat akses ke Router 5 melalui jalur gateway dari R1 ke R2. Berikut penjelasan ping User A ke User B serta mengakses internet.



Gambar 19. Pengujian kembali normal setelah di beri ketukan Knocking

Penjelasan Gambar 19, sebagai berikut ;

a. PC End User1 dapat akses ke R1 dan PC End User2, begitu juga sebaliknya.
b. R1 koneksi ke R2 terhubung koneksi 2 arah.
c. R2, R3, R4 koneksi terhubung sebagai OSPF.
d. R5 dapat terkoneksi ke R3 terhubung koneksi 2 arah.
e. Setelah dibuka autentikasi memasukkan rule yang sudah diatur maka dari PC End User dapat koneksi R5, dan R1, R2, R3, R4 dapat koneksi ke R5. Serta PC Client 1 dapat koneksi ke PC Client 2, dan PC Client dapat koneksi terhubung ke R5
f. R5 dapat terhubung ke koneksi PC Client1 dan Client2, tetapi sebaliknya PC Client1 dan Client2 tidak saling terkoneksi dan tidak bisa terhubung ke R5.
g. Antara PC End User 1 dan 2, tidak bisa terhubung koneksi ke PC Client 1 dan 2 dikarenakan jaringan NAT.

KESIMPULAN DAN SARAN

Simpulan

Berdasarkan penelitian yang telah dilakukan, maka dapat diambil kesimpulan yaitu bagaimana cara

mengimplementasikan akses open dan block disable port dengan menggunakan metode Simple Port Knocking yang bertujuan agar menutup celah pada sisi server dengan membuat port pada router tidak terlihat oleh pihak lain yang tidak dipercaya meskipun sudah di scanning port, namun tetap akan terlihat terbuka dan dapat diakses oleh pihak yang sudah terautentifikasi sehingga untuk mencegah adanya serangan akses dari attacker.

Saran

Saran dalam mengimplementasi Simple Port Knocking menggunakan Dynamic Routing (OSPF) dengan routerOS mikrotik antara lain :

1. Untuk sebuah perusahaan atau perorangan yang memanfaatkan fitur dari Port Knocking pada mikrotik disarankan menggunakan protokol NAT karena pada protokol ini semua rule ditentukan secara manual oleh administrator jaringan.
2. Pada penelitian berikutnya diharapkan dapat di praktikkan secara nyata dan menggunakan scanning port yang dapat memonitoring dan memantau akses port yang diakses oleh siapapun.

DAFTAR PUSTAKA

Anonim.2007.Jaringan Komputer.Jurusan Teknik Elektro.Fakultas Teknik.Universitas Mataram

Towidjojo, Rendra. (2016). Buku:4 Mikrotik Kung Fu. Jakarta: Jasakom.

Christiano. 2014. Pengertian dan macam-macam jaringan Komputer. Diakses pada 5 Januari 2015

Edison Siregar, 2010. Langsung Praktik Mengelola Jaringan Lebih Efektif dan Efisien. Yogyakarta: Andi Offset. (20 Maret 2015)

ELCOM. 2012. Computer Networking. Yogyakarta: Andi. (20 Maret 2015)

Harwood, Mike. 2009. CompT1A Network + N10-004 Exam Prep (3rd Edition)

Moch. Linto Herlambang & Aziz Catur L, Panduan Lengkap Menguasai Router Masa Depan Menggunakan MikroTik RouterOS™, 2008. ANDI

Perlman, Radia (1985). "An Algorithm for Distributed Computation of a Spanning Tree in an Extended LAN". ACM SIGCOMM Computer Communication Review 15 (4): 44–53

Saputro, Joko.2010. Praktikum CCNA di Komputer Sendiri Menggunakan GNS3: Media Kita

Akrom Musajid, 2012. Panduan cara Mikrotik Fundamental and Medium study. Connected. Jakarta:Jasakom

Syafrizal, Melwin, 2008, Pengantar Jaringan Komputer: AndiOffset. (18 Mei 2015)

Towidjojo, Rendra. (2012). Konsep Konsep dan Implementasi Routing dengan Router Mikrotik, 100% Connected. Jakarta: Jasakom.

Muhammad Ibrahim. 2014. 1001 Cara Menggunakan Mikrotik. Connected. Jakarta: Jasakom

Moch. Linto Herlambang & Aziz Catur L, Panduan Lengkap Menguasai Router Masa Depan Menggunakan MikroTik RouterOS™, 2008. ANDI

Akrom Musajid, 2012. Panduan cara Mikrotik Fundamental and Medium study. Connected. Jakarta:Jasakom

Krzywinski, M., 2003. Port Knocking: Network Authentication Across Closed Ports

Ivan Haryadi, Bernadus. 2013. Definisi dan Implementasi dari Port Knocking