IMPLEMENTASI PORT SCAN DETECTION DAN EMAIL SCHEDULER SEBAGAI PENCEGAHAN SERANGAN

Disusun leh : Panji Yudha Tama

KATA PENGANTAR

Puji dan syukur kehadirat Tuhan Yang Maha Esa yang telah memberikan karunia-Nya sehingga Karya Tulis Ilmiah ini dapat diselesaikan dengan baik dan tepat waktu. Karya Tulis ini saya buat untuk mengikuti Lomba Olimpiade Jaringan Mikrotik 2020 Antar SMK Tingkat Nasional.

Selama pembuatan Karya Tulis Ilmiah ini, penulis banyak mendapat bantuan dari berbagai pihak. Oleh karena itu, penulis ingin mengucapkan terima kasih kepada Teman-teman penulis yang selalu memberikan dukungan dan semangat.

Penulis berharap karya tulis ini dapat diapresiasi dan diaplikasikan guna meningkatkan kemanan dalam jaringan komputer terutama pada instansi pendidikan. Penulis menyadari masih banyak kekurangan dalam Karya Tulis Ilmiah ini, oleh karena itu saran dan kritik yang membangun akan sangat dibutuhkan untuk menyempurnakan Karya Tulis Ilmiah ini. Semoga Karya Tulis Ilmiah ini dapat bermanfaat dan berguna bagi para pembaca. Selamat membaca.

Yogyakarta, 14 Juli 2020

Penulis

Daftar Isi

A. Latar Belakang Masalah

Keamanan jaringan komputer sebagai salah satu bagian dari sebuah sistem merupakan hal yang perlu diperhatikan untuk menjaga validitas dan integritas data serta untuk menjamin ketersediaan layanan bagi penggunanya. Sebuah sistem dalam jaringan harus terlindungi dari segala macam serangan serta usaha untuk melakukan penyusupan dan pencurian data oleh pihak yang tidak bertanggung jawab.

Umumnya dalam sistem - sistem yang ada saat ini sudah dilengkapi dengan tools yang berfungsi untuk meningkatkan keamanan pada sistem tersebut. Namun tanpa kesadaran dari administrator atau pengelola jaringan untuk menganalisa dan memperbaiki sistem keamanan dalam jaringannya tools tools yang ada tidak dapat melakukan pencegahan ataupun pengamanan secara optimal, sehingga masih akan sangat memungkinkan bagi penyerang untuk dapat menyusup kedalam jaringan kita.

Masih sangat sering kita mendengar adanya kasus peretasan jaringan atau server yang banyak menargetkan instansi - instansi seperti sekolah. Oleh karena itu administrator atau pengelola jaringan tetap berkewajiban untuk mencegah dan mendeteksi serangan sedini mungkin untuk meminimalisir adanya kemungkinan penyusupan dijaringannya.

Sebagian administrator atau pengelola jaringan sudah berusaha mengamankan jaringan mereka dengan berbagai cara, seperti menutup service yang tidak digunakan, menggunakan password yang kuat, memblokir beberapa koneksi dari WAN, dan lain - lain. Namun cara - cara tersebut baru akan bekerja ketika penyerang sudah memasuki tahap penyerangan, sehingga cara tersebut kurang efektif untuk melakukan deteksi dan penanggulangan serangan sedini mungkin.

Selain itu administrator tidak mungkin juga untuk selalu memonitoring jaringan selama 24 jam penuh sehingga sangat sering administrator telat menyadari adanya potensi serangan yang masuk ke jaringan yang mereka kelola.

Berdasarkan permasalahan diatas, maka sangat diperlukan adanya teknik untuk mendeteksi serangan dan menanggulangi adanya kemungkinan serangan sedini mungkin sebelum penyerang memasuki tahap exploitation.

B. Tujuan dan Manfaat

Tujuan :

a) Untuk melindungi sistem jaringan komputer
b) Untuk mendeteksi kemungkinan serangan sejak dini
c) Untuk menanggulangi kemungkinan serangan sejak dini
d) Untuk meminimalir kemungkinan terjadinya serangan

Manfaat :

e) Wujud upaya pengamanan jaringan yang lebih baik
f) Terbentuknya sistem jaringan yang lebih aman
g) Terjaganya validitas dan integritas data dalam sebuah jaringan
h) Terciptanya rasa aman dan nyaman dalam pengguna jaringan

C. Gambaran Umum

Dalam sebuah sistem jaringan keamanan merupakan aspek yang wajib terpenuhi untuk mencegah penyalahgunaan sumberdaya dalam sebuah jaringan oleh pihak yang tidak sah atau tidak bertanggung jawab. Terdapat 5 point penting yang harus terjamin dalam sebuah jaringan, yaitu :

A) Confidentialy

Menjamin bahwa data hanya dapat diakses oleh pihak yang berwenang

B) Integrity

Menjamin bahwa data hanya dapat diubah oleh pihak yang berwenang

C) Availability

Menjamin ketersediaan data untuk pihak yang berwenang ketika data tersebut dibutuhkan

D) Authentication

Terjaminnya identitas pengirim atau sumber suatu informasi

E) Non-repudiation

Pengirim dan Penerima tidak dapat menyangkal adanya pengiriman dan penerimaan pesan

Sedangkan ancaman - ancaman yang terdapat pada sebuah sistem jaringan terbagi menjadi beberapa kategori, yaitu :

A) Interuption

Ancaman terhadap suatu sumber daya atau sistem dalam jaringan yang menyebabkannya tidak dapat digunakan atau tidak tersedia ketika dibutuhkan

B) Interception

Ancaman dimana suatu pihak yang tidak berwenang dapat mendapatkan akses terhadap suatu sistem atau sumber daya

C) Modification

Ancaman berupa perubahan sumber daya atau sistem oleh pihak yang tidak sah

D) Fabrication

Ancaman penyisipan suatu object palsu dalam sebuah sistem jaringan

Dalam melakukan serangan terhadap jaringan terdapat beberapa tahapan yang harus dilakukan oleh penyerang, yaitu :

A) Planning
B) Information Gathering
C) Vulnerability Assessment
D) Exploiting

Tugas dari suatu administrator atau pengelola jaringan adalah untuk dapat mencegah kemungkinan serangan yang dapat terjadi sedini mungkin sehingga akan memperkecil kemungkinan adanya penyusup dalam jaringan.

Berdasarkan paparan diatas, Port Scan Detection dan tools email dapat diimplementasikan dalam jaringan untuk mencegah serangan serta memperingatkan Administrator sedini mungkin, dimana Port Scan Detection akan berusaha melakukan pencegahan saat penyerang masih berada dalam tahap Information Gathering atau pengumpulan informasi yang ada dalam jaringan target sedangkan scheduler akan memicu tools email untuk dapat mengirimkan email peringatan kepada Administrator.

Kelebihan :

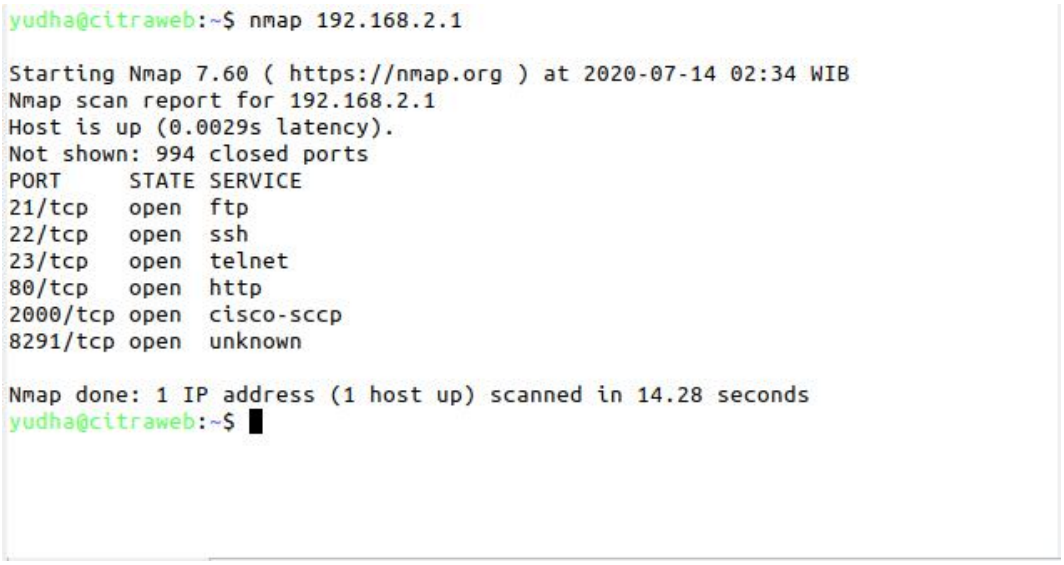
A) Port Scan Detection dapat melakukan pencegahan dan penanggulangan kemungkinan serangan sejak tahap Information Gathering
B) Tindakan yang dapat dilakukan kepada penyerang dapat lebih bervariasi dan fleksibel
C) Dapat dikombinasikan dengan teknik pencegahan lain seperti email notifikasi dan Honeypot

Kekurangan :

A) Tidak dapat mendeteksi ancaman serangan yang tahapannya tidak menggunakan port scanning
B) Perlu dikombinasikan dengan rule - rule lain agar rule Port Scan Detection lebih optimal.

D. Analisis dan Pemecahan Masalah

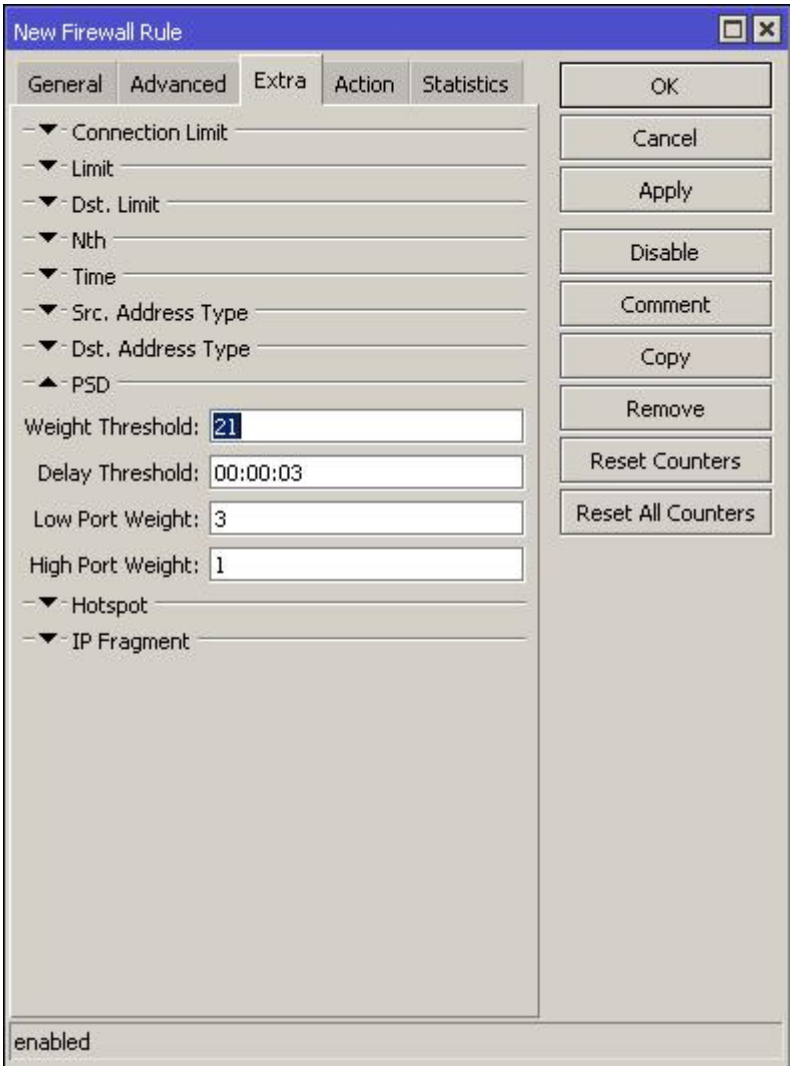
Saat berada dalam tahap information gathering Penyerang akan berusaha untuk mengumpulkan informasi yang berkaitan dengan target sebanyak - banyaknya sehingga akan membantunya dalam menjalankan tahapan - tahapan selanjutnya. Saat proses pengumpulan informasi inilah penyerang akan menggali informasi port dan service apa yang berjalan.



Jika penyerang berhasil mendapatkan informasi port yang terbuka serta service yang berjalan seperti gambar diatas maka hal tersebut akan mempermudah langkah penyerang dalam melakukan tahapan selanjutnya.

Oleh karena itu untuk memperkecil kemungkinan berhasilnya penyusup masuk ke Jaringan, Administrator perlu melindungi jaringannya dari Ancamana Port Scanning.

Dalam Mikrotik RouterOS terdapat built in firewall yang didalamnya terdapat matcher Port Scan Detection yang ditujukan untuk mengenali adanya ancaman port scanning dan melakukan penanggulangan terhadap ancaman tersebut



Port Scan Detection merupakan matcher yang terdapat dalam firewall Mikrotik RouterOS. Matcher Port Scan Detection ini dapat bekerja di beberapa chain. Dalam Firewall Filter Sendiri terdapat 3 chain utama yaitu :

A) Forward

Forward merupakan chain untuk menangkap koneksi yang melewati router

B) Input

Input merupakan chain untuk menangkap koneksi yang masuk kedalam router

C) Output

Output merupakan chain untuk menangkap koneksi yang keluar dari router

Setelah Chain ditentukan kita perlu menentukan protocol apa yang akan kita tangkap, Port Scan Detection sendiri dapat bekerja pada protocol TCP atau UDP.

Untuk mengaktifkan Port Scan Detection dapat dilakukan pada tab Extra dan membuka parameter PSD. Terdapat beberapa 4 Parameter yang harus ditentukan dalam PSD yaitu :

A) Weight Threshold

Weight Threshold merupakan parameter batas maksimal nilai, dimana action rule akan bekerja ketika nilai mencapai atau lebih dari nilai Weight Threshold tersebut.

B) Delay Threshold

Delay Threshold adalah rentang interval waktu tiap koneksi dari source address yang sama ke destination port yang berbeda. Jika rentang waktu tiap koneksi lebih kecil akan dihitung sebagai ancaman port scanning

C) Low Port Weight

Nilai setiap koneksi ke port - port rendah atau biasa disebut well-known port, yaitu port dibawah 1024

D) High Port Weight

Nilai setiap koneksi ke port port tinggi, yaitu port yang berada diatas 1024

Prinsip atau cara kerja dari port scan detection ini adalah sebagai berikut :

1. Router akan menangkap atau memonitor setiap traffic pada chain yang kita gunakan
2. Saat terdapat koneksi dari source address dan destination address yang sama dengan destination port yang berbeda dalam rentang waktu yang lebih rendah atau sama dengan delay threshold router akan menambahkan nilai sesuai kategori port yang diakses, apabila melakukan koneksi ke port rendah akan ditambahkan nilai yang ada di parameter low port weight dan apabila destination port pada port tinggi akan ditambahkan sesuai nilai yang ada pada parameter high port weight.
3. Saat Total nilai mencapai nilai Wight Threshold maka action pada rule tersebut akan dilakukan oleh router.

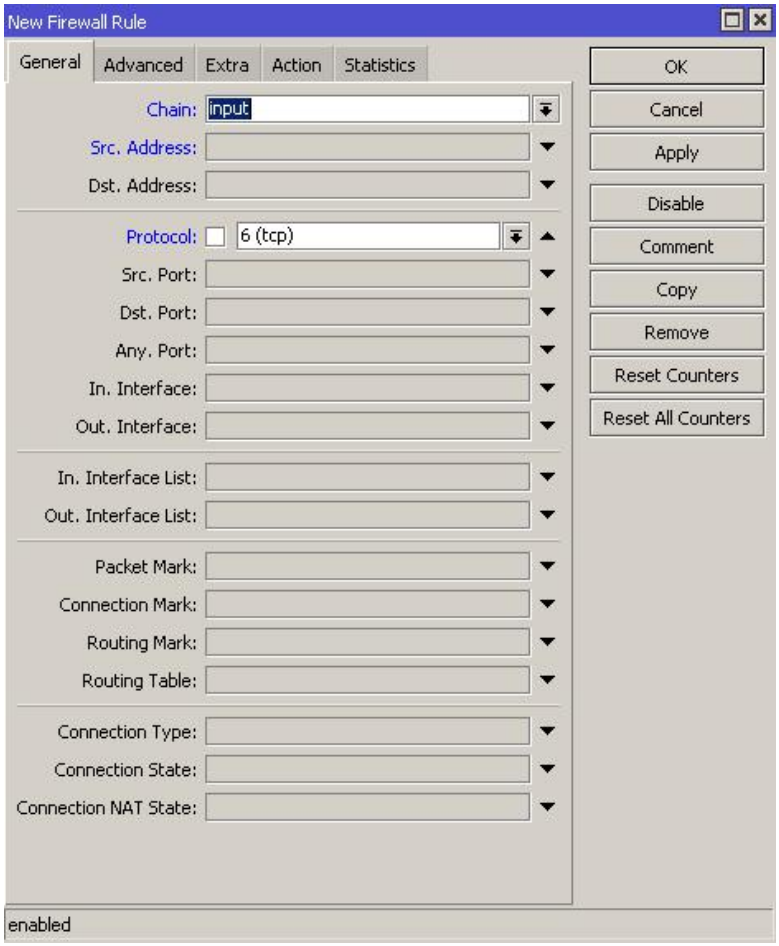
Pada Mirkotik RouterOS juga terdapat tools bernama scheduler dimana tools ini dapat digunakan untuk melakukan tindakan yang sama berulang kali dalam interval waktu tertentu secara otomatis. Oleh karena itu dengan memanfaatkan tools ini Router dapat mengirimkan notifikasi kepada administrator apabila terdapat ancaman serangan yang datang dengan melakukan checking terhadap Address List.

E. Contoh Implementasi

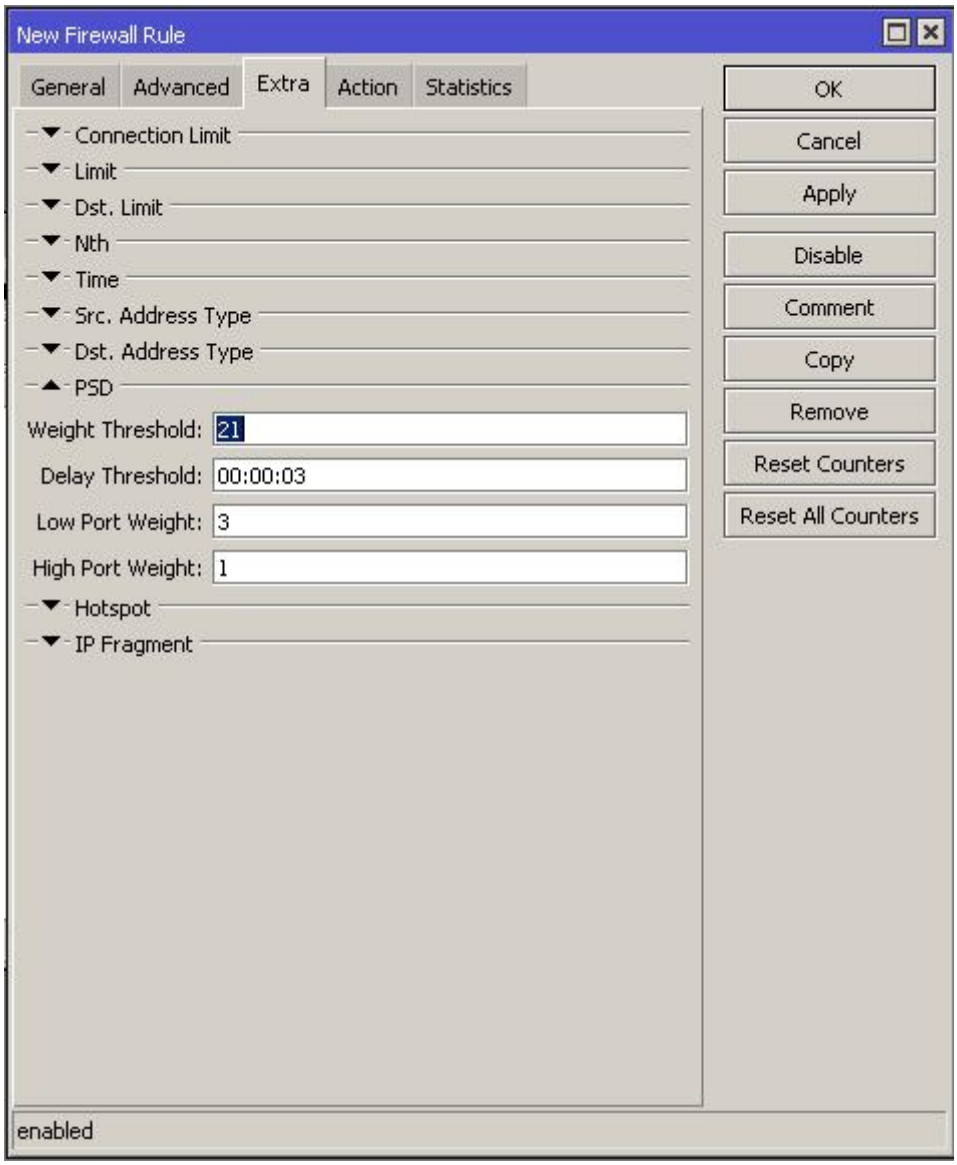
Pada topologi berikut terdapat satu router yang akan diimplementasikan Port Scan Detection didalamnya untuk melindungi router tersebut dari ancaman port scan detection dari dalam jaringan lokal atau dari luar jaringan atau WAN.

Untuk mengimplementasikan Port Scan Detection terdapat beberapa langkah yang perlu dilakukan, langkah - langkahnya sebagai berikut :

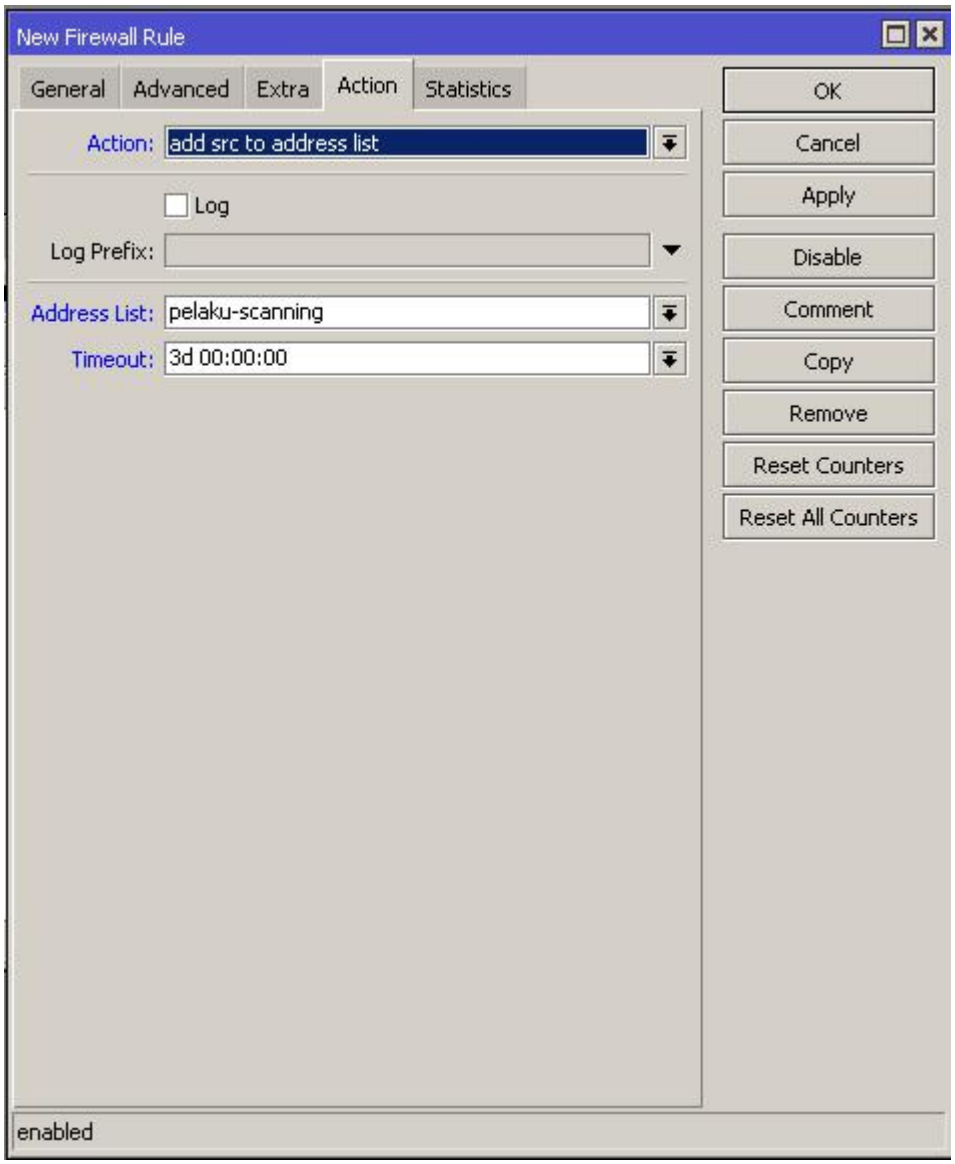
1. Masuk ke IP -> Firewall -> Add
2. Tentukan chain dan protocol pada tab general, pada kasus berikut chain yang digunakan adalah input dikarenakan yang akan dilindungi dari ancaman port scanning adalah router itu sendiri



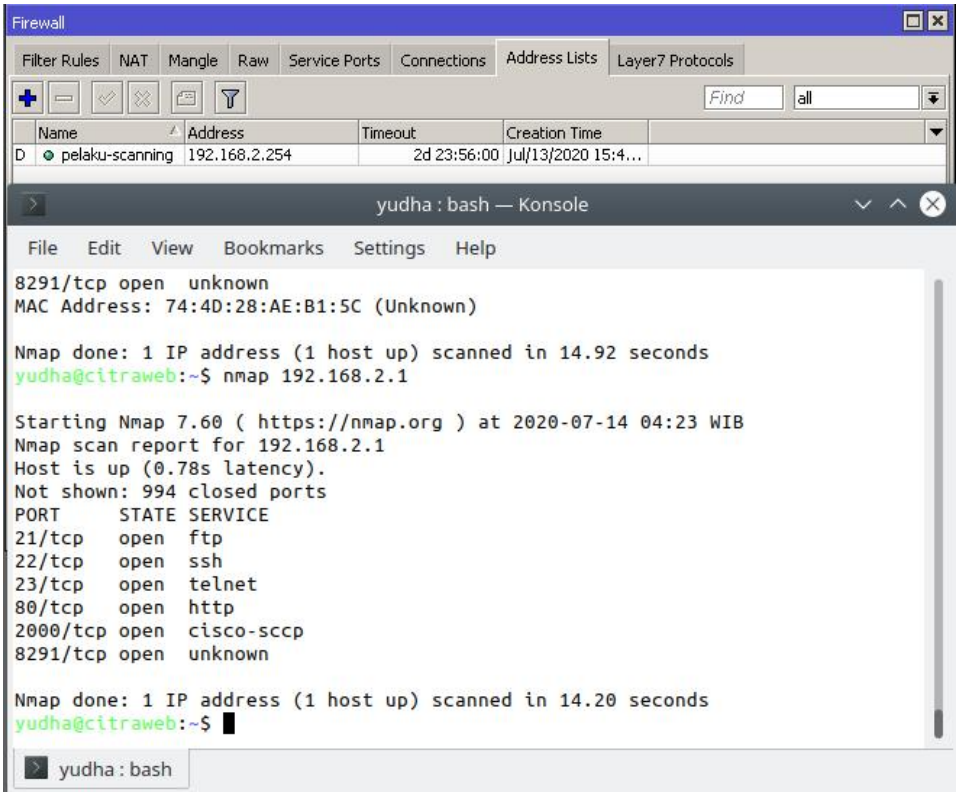
3. Masuk ke Tab Ekstra kemudian aktifkan PSD



4. Masuk Tab Action, isikan parameter Action dengan value ‘add src to address list’, isikan nama address list dan waktu berlakunya. Kemudia klik Ok.

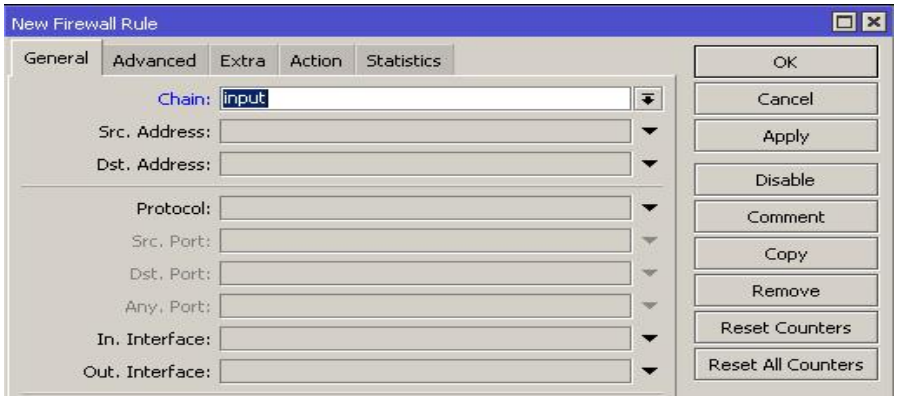


Sampai tahap ini saat dilakukan uji coba dengan melakukan scanning port maka IP Address host yang melakukan scanning akan masuk ke dalam address list dengan nama Pelaku Scanning seperti pada gambar berikut :

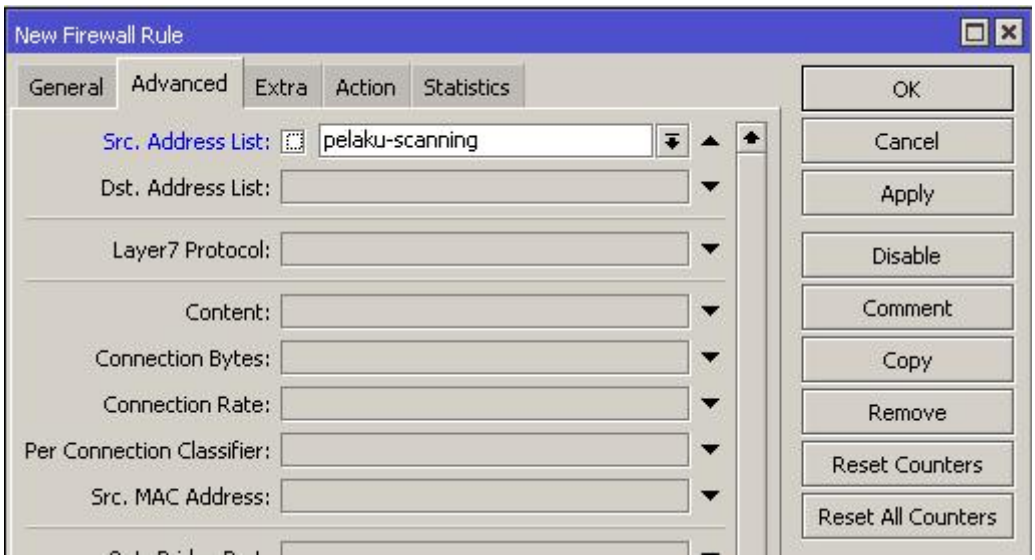


Setelah rule Port Scan Detection bekerja langkah selanjutnya adalah membuat rule tindakan bagi host yang melakukan port scanning

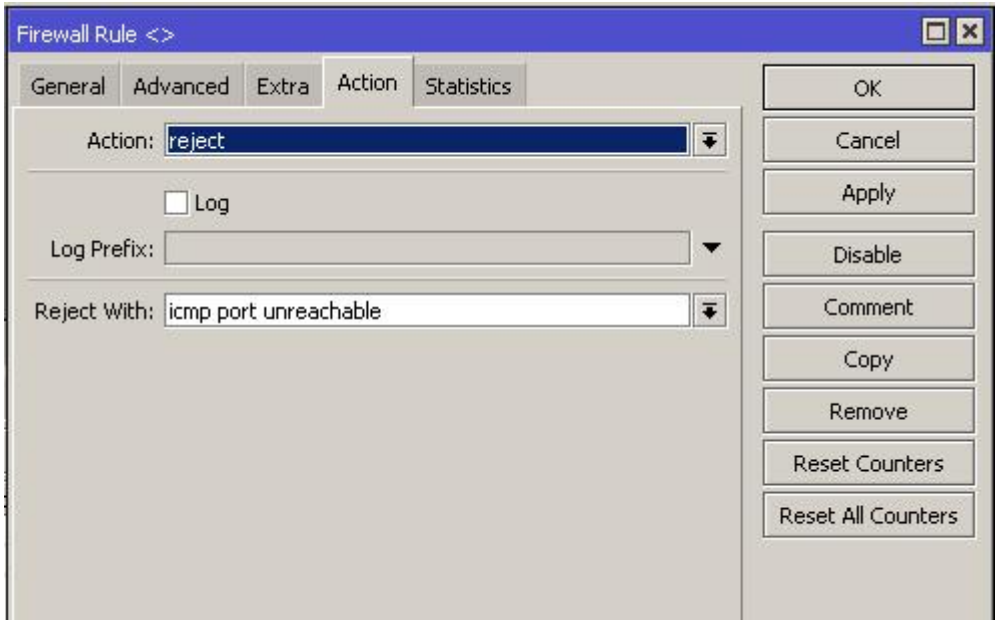
1. Masuk IP->Firewall->Add
2. Masukkan value input pada parameter Chain



3. Masuk Tab Advanced, Isikan parameter ‘Src. Address-list’ dengan pelaku-scanning



4. Masuk ke menu Action, masukkan value ‘reject’ pada parameter action dan value ‘icmp port unreachable’ pada parameter ‘Reject with’

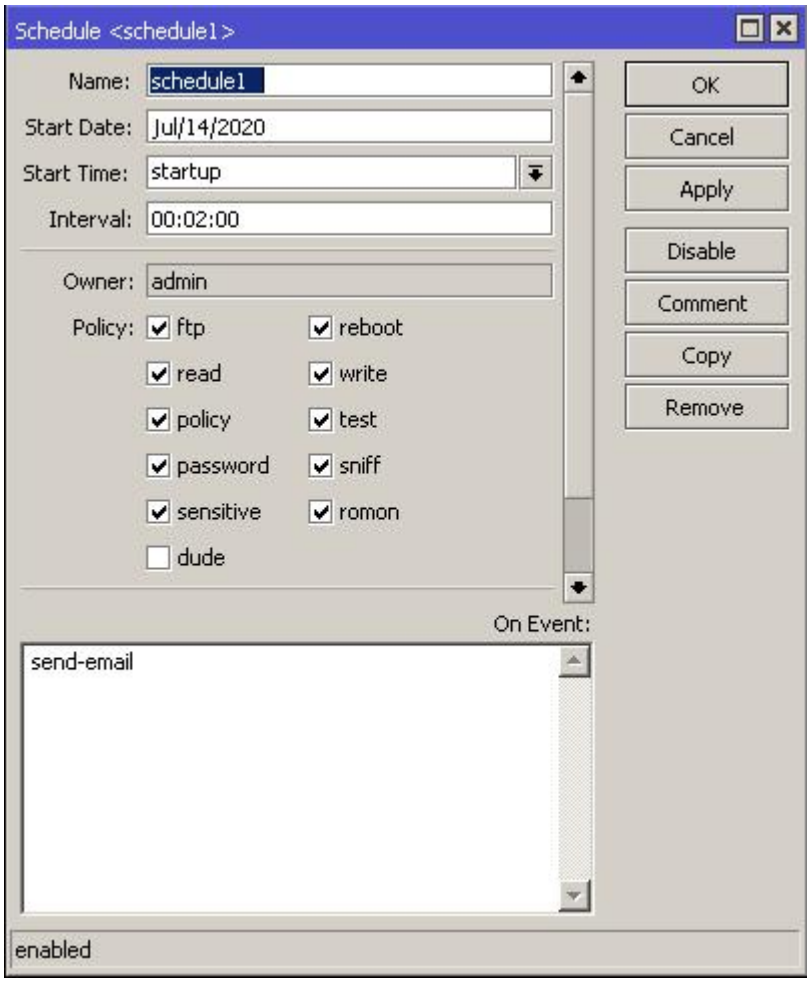


Setelah rule untuk tindakan selesai dibuat langkah selanjutnya adalah membuat script untuk mengirim email notifikasi dan scheduler untuk mentrigger script. Langkah pembuatannya sebagai berikut :

1. Membuat script di System -> Script dengan isi sebagai berikut :

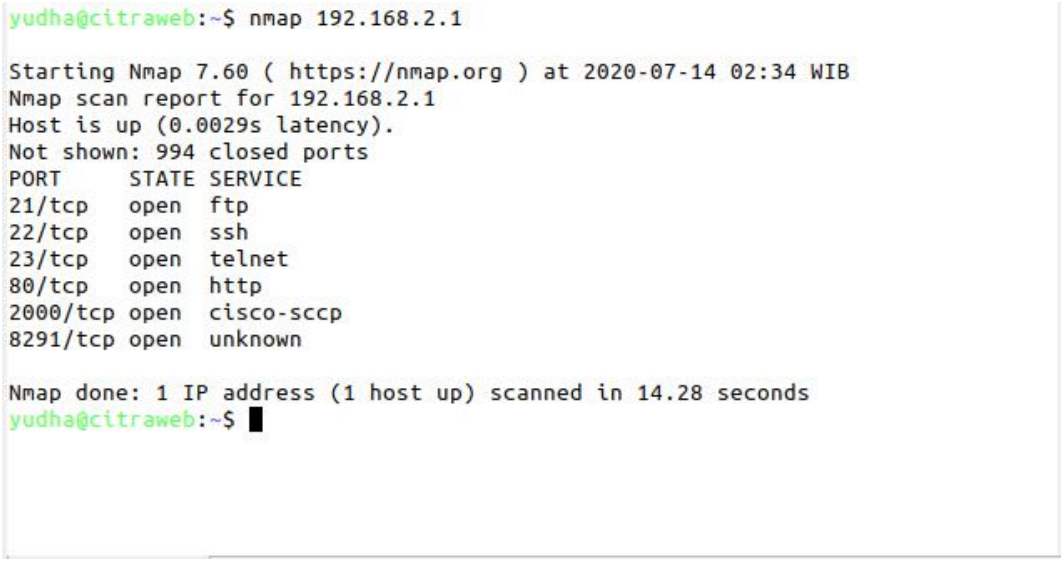
   “:foreach a in=[/ip firewall address-list find list=pelaku-scanning] do={:global ip [/ip firewall address-list get $a address];
   :log warning ("Scan Attacl From:" .$ip);
   :local sysname [/system identity get name];
   :local date [/system clock get date];
   :local time [/system clock get time];
   */tool e-mail send from="Router $sysname<yudha.mawon24@gmail.com>" to="yudha.mawon24@gmail.com" start-tls=yes server=smtp.gmail.com port=587 user=yudha.mawon24@gmail.com password=********** subject="Scan Attack@" body="Pada $date jam $time. Terjadi serangan pada $sysname dari IP $ip."}”*

2. Add scheduler baru di System -> Scheduler dengan interval 2 menit sesuai dengan interval address list Port Scan Detection, sebagai berikut :

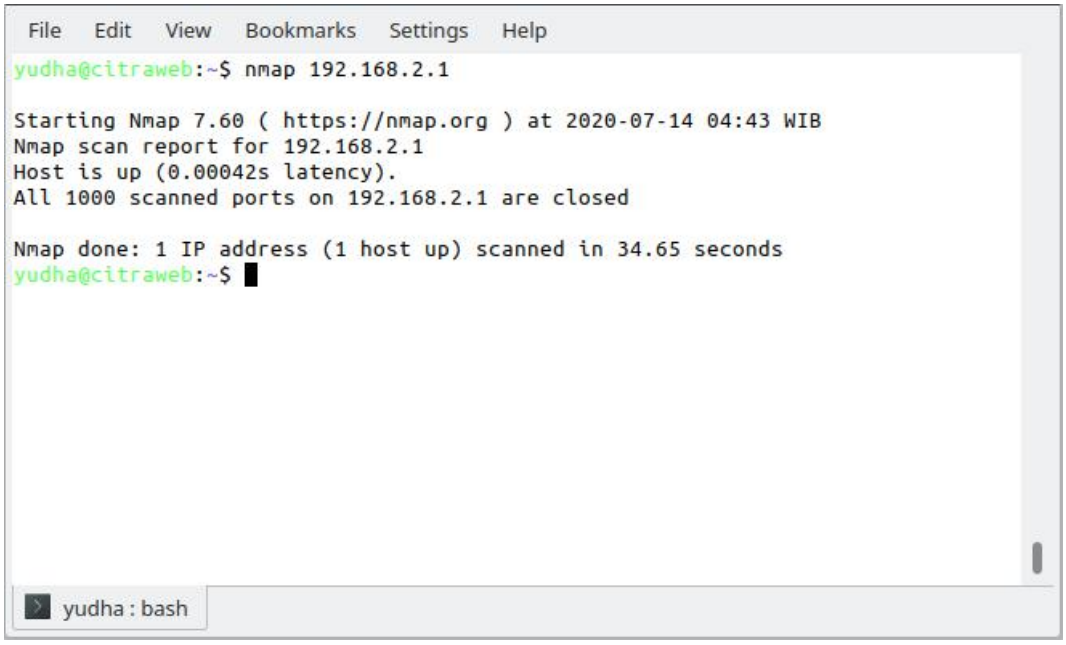


Untuk melakukan pengujian dapat dilakukan port scanning saat Port Scan Detection belum diimplementasikan dan setelah Port Scan Detection diimplementasikan. Hasilnya sebegai berikut :

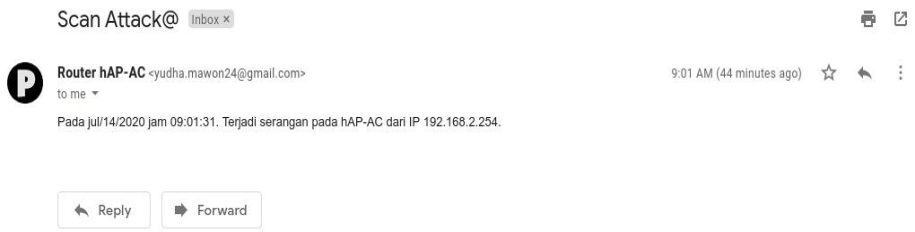
A) Sebelum Implementasi Port Scan Detection



B) Setelah Port Scan Detection Diimplementasikan



C) Email Notifikasi yang terkirim



F. Kesimpulan

Banyaknya ancaman - ancaman yang terdapat di Jaringan mengakibatkan perlunya Administrator untuk meningkatkan keamanan pada jaringannya agar dapat mendeteksi dan menanggulangi kemungkinan adanya serangan sedini mungkin. Namun rule yang biasa diterapkan pada suatu jaringan biasanya hanya mampu mendeteksi dan memblock saat terjadinya exploitation sedangkan untuk meminimalisir kemungkinan berhasilnya penyerang menyusup kedalam jaringan perlu dilakukan deteksi dan penanggulangan secara lebih dini.

Oleh karena itu perlu adanya implementasi Port Scan Detection dan Email Notification untuk melakukan deteksi ancaman port scanning sehingga diharapkan Router mampu untuk mendeteksi dan menanggulangi ancaman serangan sejak masih dalam tahap Information Gathering.

Daftar Pustaka

Tulisan Berjudul “Keamanan Jaringan” yang diterbitkan di Wikipedia.
https://id.wikipedia.org/wiki/Keamanan_jaringan

Artikel yang tayang di Mikrotik Indonesia dengan judul “Port Scan Detection (PSD)”.
http://www.mikrotik.co.id/artikel_lihat.php?id=284

Artikel yang tayang di Mikrotik Indonesia dengan judul “Mengirim File Backup Router Melalui Email Otomatis”.
http://www.mikrotik.co.id/artikel_lihat.php?id=119

Manual:Scripting pada Wiki Mikrotik
https://wiki.mikrotik.com/wiki/Manual:Scripting