JUSTIN
Jurnal Sistem dan Teknologi Informasi
p-ISSN : 2460-3562 / e-ISSN : 2620-8989
Vol. 6, No.3, Juli 2018

Malware Security Menggunakan Filtering Firewall dengan Metode Port Blocking pada Mikrotik RB 1100AHx2

Muhamad Ryansyah[#1], Muhammad Sony Maulana[*2]
[#]*Program Studi Sistem Informasi STMIK Nusa Mandiri Jakarta*
Jl. Damai No.8, Warung Jati Barat, Jakarta Selatan, Indonesia
[1]muhamadryansyah@gmail.com
[*]*Program Studi Manajemen Informatika AMIK BSI Pontianak*
Jl. Abdurahman Saleh No.18A, Kota Pontianak, Indonesia
[2]muhammad.sony.mom@bsi.ac.id

Abstrak— **Penelitian ini bertujuan untuk mengatasi permasalahan-permasalahan terkait lambatnya suat jaringan yang disebabkan oleh penyebaran malware yang terdapat dalam jaringan kampus. Salah satu dampak adanya malware dalam jaringan kampus adalah overload traffic bandwidth, sehingga menyebabkan kendala bandwidth yang cepat habis atau lalu lintas transfer data baik yang masuk maupun yang keluar menjadi lambat dari biasanya. Umumnya sebuah kampus atau universitas memiliki struktur jaringan yang didalamnya dikelola oleh satu atau lebih router di dalam mengelola jaringan dan bandwidth. Beberapa router memiliki kemampuan pengaturan firewall yang sudah cukum mumpuni namun perlu dikelola lebih spsesifik berdasarkan kebutuhan skala jaringan dan bandwidth yang tersedia. Dengan menciptakan rule-rule yang baik di dalam firewall akan lebih mudah dalam melakukan filtering terhadap lalu lintas trafik jaringan dan bandwidth sehingga dapat menciptakan keamanan dan kenyamanan pengguna jaringan dan bandwidth. Hasil penelitian ini menunjukkan kinerja dari mikrotik router board RB 1100 AHx2 yang dapat memfilter aktivitas malware dengan rule yang telah ditanamkan.**

Kata kunci— **malware, jaringan, filtering, firewall, bandwidth, mikrotik**

I. PENDAHULUAN

Saat ini pengembangan teknologi yang berhubungan proses penyebaran berita telah banyak dilaksanakan. terhadap teknologi penyebaran berita dilaksanakan dengan dua metode yakni melalui media online serta media offline, namun perkembangan banyak dilaksanakan terhadap media online. Media offline tidak banyak merasakan pernyebaran disebabkan penggunaan media offline dinilai terbatas terhadap ruang lingkup tertentu Walaupun dinilai terbatas terhadap ruang lingkup terdefinisi jelas seperti perkantoran, media offline dinilai amat efisien buat media penyebaran berita dilingkungan tersebut. Namun penyampaian berita secara offline tak secepat media online, disebabkan media online didukung oleh teknologi yang paling efisien yakni jaringan komputer. terhadap ruang lingkup perkantoran lazimnya telah banyak menggunakan jaringan komputer sebagai teknologi pendukung pekerjaan dan sebagai media penyampaian informasi. Jaringan komputer terhadap saat ini amat berkembang dan menjadi kebutuhan.[1]

Penyebaran malware komputer pada jaman sekarang lebih cepat dan mudah dikarenakan juga oleh kemajuan-kemajuan teknologi komputer dan spesifikasi komputer tersebut. Salah satu kerja dari malware komputer ini adalah dengan menginfeksi salah satu file di komputer kemudian malware tersebut menyebar ke semua file yang ada di komputer, tidak hanya dalam komputer tersebut yang terkena malware. Jika dalam satu jaringan yang besar malware tersebut akan menyebar melalui jaringan internal atau yang terhubung internet dan akan dapat dicuri file yang ada dalam satu jaringan karena komputer saling terhubung satu sama lain sehingga pastinya setiap komputer akan saling berbagi file. Sebuah malware diciptakan untuk merusak atau membobol system operasi dengan melalui script yang dirahasiakan,artinya disisipkan oleh penyerang.[2]

Penyebaran trojan ini dilaksanakan dengan cara social engineering, yaitu metoda yang memakaikan kekurangan manusia, sehingga user dengan tidak curiga langsung mengeksekusi sesuatu program yang tak dikenal. kegiatan malware berhubungan erat dengan performa PC serta juga aktifitas network terhadap sistem komputer. Malware yang

Submitted 18-07-2018; Revised 21-07-2018; Accepted 30-07-2018

ikut berkembang di dalamnya, yang memungkinkan attacker masuk ke dalam sistem tanpa diketahui oleh pemilik.[3]

Windows menggunakan port libpcap yang dikenal sebagai WinPcap. Perangkat lunak pemantauan dapat menggunakan libpcap dan atau WinPcap untuk menangkap paket yang transmisi melalui jaringan dan, dalam versi yang lebih baru, untuk mengirim paket pada jaringan di link layer, serta mendapatkan daftar antarmuka jaringan untuk kemungkinan penggunaan dengan libpcap, dukungan ALO menyimpan paket yang diambil ke file, dan membaca file yang berisi paket-paket yang disimpan; aplikasi bisa ditulis, menggunakan libpcap untuk dapat menangkap lalu lintas jaringan dan menganalisisnya, atau membaca rekaman yang disimpan dan menganalisisnya, menggunakan kode analisis yang sama. File diambil disimpan dalam format yang libpcap dan gunakan dapat dibaca oleh aplikasi itu yang mengerti format itu.[4]

Ada beberapa jenis malware yang paling popular di tahun 2015 yaitu Trojan Ransomware, Exploit kits, Banking Trojans, worms, PoS (Point-of-Sale) Malware, Social Engineering Attacks, Fake Tech Support Services, Rogue Antivirus Software, Potentially Unwanted Programs, dan Adware.[5].

II. TINJAUAN PUSTAKA

A. Virus

Virus komputer adalah sebuah program komputer biasa yang memiliki prosedur untuk menggandakan sebagian atau bahkan keseluruhan bagian programnya ke dalam program lain, sehingga program yang di serang berjalan tidak sebagai mestinya dan program akan berjalan melambat tidak sebagaimana mestinya.[6]

B. Malware

Malware (malicious software) adalah perangkat lunak yang dapat mengganggu proses atau kinerja dalam sistem operasi komputer seperti mencuri informasi data sensitif dan melakukan remote pada Komputer targer tanpa seizin pemilik. Malware ada dalam berbagai bentuk seperti script, code, active content, dan perangkat lunak.[7]

C. Port

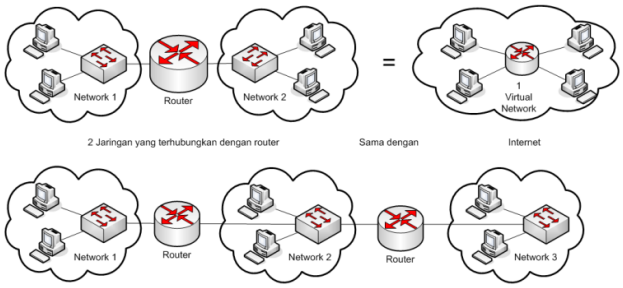
Port adalah tempat di mana informasi masuk dan keluar dari komputer, port scanning mengidentifikasi pintu terbuka ke komputer. Port memiliki penggunaan yang sah dalam mengelola jaringan, tetapi scanning port juga bisa berbahaya jika seseorang sedang mencari titik akses yang lemah untuk masuk ke komputer anda.[8]

D. Firewall

Firewall adalah sebuah sistem pengaman, jadi firewall bisa berupa apapun baik hardware maupun software. Firewall dapat digunakan untuk memfilter paket-paket dari luar dan dalam jaringan di mana ia berada. Jika pada kondisi normal semua orang dari luar jaringan anda dapat bermain-main ke komputer anda, dengan firewall semua itu dapat diatasi dengan mudah. Firewall yang sederhana biasanya tidak memiliki kemampuan melakukan filtering terhadap paket berdasarkan isi dari paket tersebut. Sebagai contoh, firewall tidak memiliki kemampuan melakukan filtering terhadap e-mail bervirus yang Anda download atau terhadap halaman web yang tidak pantas untuk dibuka. Yang bisa dilakukan firewall adalah melakukan blokir terhadap alamat IP dari mail server yang mengirimkan virus atau alamat halaman web yang dilarang untuk dibuka. Dengan kata lain, firewall merupakan sistem pertahanan yang paling depan untuk jaringan Anda.[9]

E. Internetworking

Tujuan dari TCP/IP adalah untuk membangun suatu koneksi antar jaringan (network), dimana biasa disebut internetwork, atau intenet, yang menyediakan pelayanan komunikasi antar jaringan yang memiliki bentuk fisik yang beragam. Tujuan yang jelas adalah menghubungkan empunya (hosts) pada jaringan yang berbeda, atau mungkin terpisahkan secara geografis pada area yang luas. [10]



Gambar 1. Contoh Internet

.

III. METODOLOGI PENELITIAN

Penelitian ini menggunakan metode studi pustaka dan kajian-kajian secara langsung memperhatikan cara kerja dari system malware sebagai pedoman dalam pembuatan penelitian ini. Untuk mendapatkan contoh suatu malware harus dideteksi dengan menggunakan banyak perangkat yang terhubung ke jaringan karena kita juga tidak tau jika perangkat tersebut terjangkit malware atau tidak. Setelah dikaji kita dapat mengevaluasi hasil dari lalu lintas jaringan pada router mikrotik tersebut.

Untuk mendapatkan informasi dari default port malware tersebut kita bisa cari dari berbagai media di internet. Berikut beberapa default port dan protocol pada malware [11]:

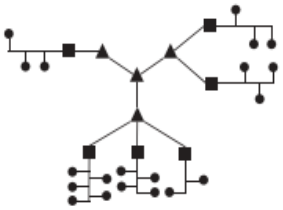
31/tcp	Agent 31, Hackers Paradise, Masters Paradise
1170/tcp	Psyber Stream
1234/tcp	Ultors Trojan
1243/tcp	SubSeven server (default for V1.0-2.0)
1981/tcp	ShockRave
2001/tcp	Trojan Cow
2023/tcp	Ripper Pro
2140/udp	Deep Throat, Invasor
2989/tcp	Rat backdoor

3024/tcp	WinCrash
3150/tcp	Deep Throat, Invasor
3700/tcp	Portal of Doom
4950/tcp	ICQ Trojan
6346/tcp	Gnutella
6400/tcp	The Thing
6667/tcp	Trinity intruder-to-master and master-To-daemon SubSeven server (default for V2.1 Icqfix and beyond)
6670/tcp	Deep Throat
12345/tcp	NetBus 1.x, GabanBus, Pie Bill Gates, X-Bill
12346/tcp	NetBus 1.x
16660/tcp	Stacheldraht intruder-to-master
18753/udp	Shaft master-to-daemon
20034/tcp	NetBus 2 Pro
20432/tcp	Shaft intruder-to-master
20433/udp	Shaft daemon-to-master
27374/tcp	SubSeven server (default for V2.1-Defcon)
27444/udp	Trinoo master-to-daemon
27665/tcp	Trinoo intruder-to-master
30100/tcp	NetSphere
31335/udp	Trinoo daemon-to-master
31337/tcp	Back Orifice, Baron Night, Bo Facil
33270/tcp	Trinity master-to-daemon
33567/tcp	Backdoor rootshell via inetd (from Lion worm)
33568/tcp	Trojaned version of SSH (from Lion worm)
40421/tcp	Masters Paradise Trojan horse
60008/tcp	Backdoor rootshel via inetd (from Lion worm)
65000/tcp	Stacheldraht master-to-daemon
1080	MyDoom.B,MyDoom.F, MyDoom.G, MyDoom.H
2283	Dumaru.Y
2535	Beagle.W, Beagle.X, other Beagle/Bagle variants
2745	Beagle.C through Beagle.K
3127	MyDoom.A
3128	MyDoom.B
3410	Backdoor.OptixPro.13 and variants
5554	Sasser through Sasser.C, Sasser.F
8866	Beagle.B
9898	Dabber.A and Dabber.B
10000	Dumaru.Y
10080	MyDoom.B
12345	NetBus
17300	Kuang2
27374	SubSeven
65506	various names: PhatBot, Agobot, Gaobot

IV. HASIL DAN PEMBAHASAN

A. Gambaran Umum

Setiap organisasi mengadopsi komputansi heterogen yang melibatkan berbedanya teknologi jaringan, yang paling popular adalah jaringan local area network (LAN). Jaringan ini menggunakan teknologi yang berbeda. Tiga yang paling umum topologi adalah bintang, cincin, dan bus. Ethernet dengan topologi bus mendominasi LAN teknologi. Jaringan contoh pada universitas memiliki tipikal topologi bus untuk jaringan area lokalnya yang kemudian dihubungkan ke jaringan inti membentuk topologi pohon. Menggambarkan jaringan teknologi yang dihasilkan, diwakili oleh grafik yang tidak diarahkan. [12]



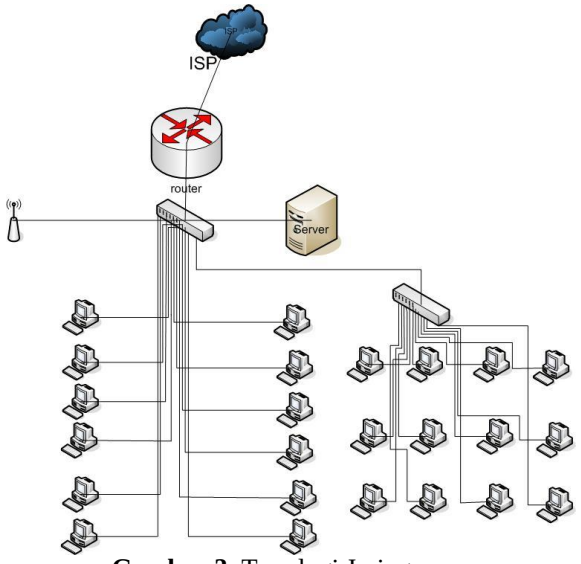
Gambar 2. Technological Network

Setiap paket berpindah dari sumber ke tujuan dengan dua protokol berbeda yang menggunakan port TCP dan UDP dan kedua protokol tersebut memiliki hingga 65.536 port yang berbeda. Penyusup sering memindai komputer korban untuk melihat port mana yang aktif dan port mana saja yang non aktif. Setelah penyerang atau penyusup mengidentifikasi open port (ort yang terbuka), penyusup mempersempit serangan ke jenis port tertentu di masa mendatang. Di lain kesempatan serangan port terjadi ketika penyerang mengirim paket ke mesin, memvariasikan port tujuan dan penyerang dapat mengetahui layanan apa yang kami jalankan dan untuk mendapatkan ide yang cukup bagus untuk melihat sistem operasi yang kami miliki. Di hari-hari ini kebanyakan situs internet mendapatkan selusin atau lebih pemindaian port per hari atau jam. Firewall harus memperhatikan kegiatan ini karena itu tidak biasa untuk komputer jarak jauh untuk terhubung ke lebih dari beberapa port sekaligus.[13]

B. Rancangan Topologi Jaringan

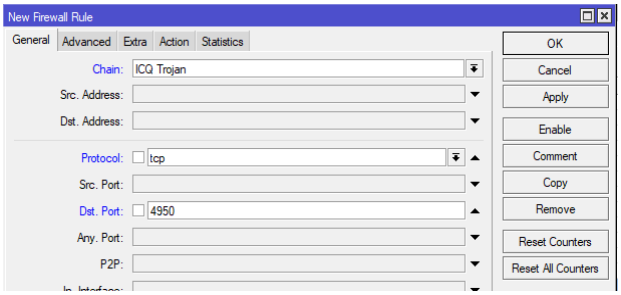
Adapun topologi jaringan yang dibuat dalam penelitan ini yaitu sebuah jaringan yang didalamnya terdapat router board mikrotik, ISP (Internet Service Provider) dan beberapa klien, baik local server, WLAN (Wireless Local Area Network) dan LAN (Local Area Network). Internet akan masuk langsung ke dalam jaringan router yang kemudian akan terpecah menjadi beberapa segmen jaringan yang terhubung melalui switch-switch berdasarkan lokal ruangan dan lantai gedung.

Selain menggunakan switch jaringan juga memiliki beberapa akses poin yang diletakkan di setiap lantai dengan segmen IP Address yang berbeda tergantung ruang. Secara keseluruhan topologi jaringan yang dibangun seperti pada gambar 3.



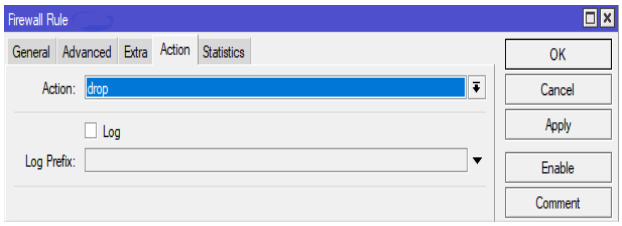
Gambar 3. Topologi Jaringan

Penulis menggunakan router mikrotik tipe RB1100AHx2 dalam penelitian ini dikarenakan spesifikasinya dengan CPU dual core, dapat mencapai hingga satu juta paket per detik dan mendukung enkripsi hardware. Memiliki tiga belas port Ethernet gigabit , dua kelompok switch 5-port, dan termasuk kemampuan bypass Ethernet. RAM 2GB SODIMM disertakan, ada satu slot kartu microSD. Menggunakan spesifikasi yang bagus dikarenakan dapat untuk pengembangan jaringan.



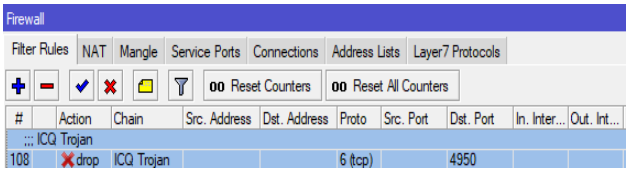
Gambar 4. New Firewall Rule Mikrotik

Untuk masuk kedalam penambahan rule pada pengaturan firelwall maka dibutuhkan akses sebagai admin utama pada router board kemudian menambahkan rule seperti gambar diatas.



Gambar 5. Firewall Rule Mikrotik

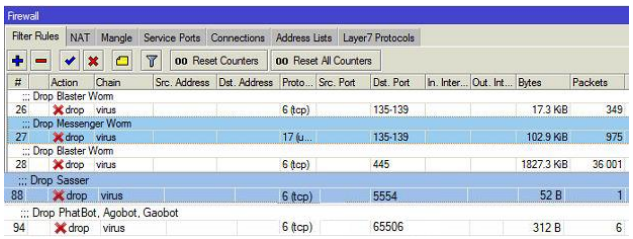
Ini merupakan metode untuk membuat peraturan firewall sesuai dengan nama virus, protocol dan port. Bisa juga dengan menggunakan perintah / ip firewall filter add chain= ICQ Trojan protocol=tcp dst-port=4950 action=drop comment="ICQ Trojan", maka akan didapatkan hasil seperti gambar dibawah ini.



Gambar 6. Hasil Pengaturan Firewall Di Mikrotik
Sumber : Penelitian 2018

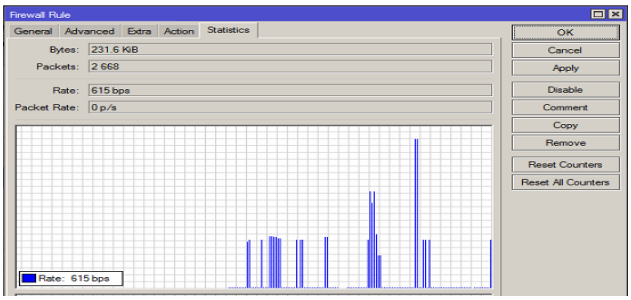
Metode ini telah tersedia pada router mikrotik, dan hasil pengaturannya akan terlihat pada gambar diatas. Sedangkan untuk penambahan rule malware dengan port-portnya dan berbagai jenis malware lainnya bisa dikaji dan didapatkan dari berbagai sumber lainnya dikarenakan jumlah malware dan port yang terus bertambah.

Dari hasil analisa terdapat lalu lintas malware pada jaringan dengan melihat bytes dan packets maupun statistik. Dengan hasil yang sudah dikaji dapat diartikan terdapat malware pada setiap user atau perangkat komputer yang di gunakan. Sebelum malware tersebut menyebar melalui jaringan router dapat menutup akses malware tersebut sehingga perangkat atau user lain tidak terserang oleh malware tersebut.



Gambar 7 .Hasil Pengaturan Firewall Di Mikrotik

Untuk melihat statistik malware yang ada atau melintas didalam jaringan dapat dilihat pada tab menu statistics yang ada pada menu firewall di mikrotik.



Gambar 8. Firewall Rule Mikrotik