JOMLAI: Journal of Machine Learning and Artificial Intelligence
Vol. 1, No. 2, Juni 2022, pp. 133~142
ISSN: 2828-9102 (Print) | 2828-9099 (Online)
DOI: 10.55123/jomlai.v1i2.816

Optimasi Sistem Keamanan Jaringan Komputer Terhadap Serangan Malware Menggunakan Filtering Firewall dengan Metode Port Blocking

Optimization of Computer Network Security System Against Malware Attacks Using Firewall Filtering with Port Blocking Method

Andri[1], Indra Gunawan[2], Ika Okta Kirana[3]
STIKOM Tunas Bangsa, Pematangsiantar, Indonesia

Article Info

Genesis Artikel:

Diterima, 14 Agustus 2022
Direvisi, 15 Agustus 2022
Disetujui, 16 Agustus 2022

Kata Kunci:

Sistem Keamanan
Jaringan Komputer
Malware
Firewall
Port Blocking

ABSTRAK

Jaringan komputer memiliki peranan penting dalam kegiatan belajar mengajar di sekolah, akan tetapi adapula dampak negatif yang ditimbulkan. Salah satunya rawan di serang oleh *malware* seperti virus dan lain sebagainya, begitu pula hal nya di SMK Swasta Satria Mandiri Bandar Huluan. Selama ini jaringan komputer di sekolah tersebut sangat mudah diserang oleh *malware*. Dampak negatif adanya *malware* dalam jaringan adalah overload traffic bandwidth, sehingga menyebabkan kendala bandwidth yang cepat habis atau lalu lintas transfer data menjadi lambat dari biasanya. Kehandalan suatu jaringan dapat ditentukan dari faktor keamanan jaringan itu sendiri. Beberapa router memiliki kemampuan pengaturan *Firewall* yang sudah cukup mumpuni namun perlu dikelola lebih spesifik berdasarkan kebutuhan skala jaringan 1500 Kbps dan bandwidth yang tersedia. Menciptakan rule-rule yang baik di dalam *Firewall* akan lebih mudah dalam melakukan *Filter*ing terhadap lalu lintas trafik jaringan dan bandwidth sehingga dapat menciptakan keamanan dan kenyamanan pengguna jaringan dan bandwidth. *Port Blocking* memungkinkan pengguna atau user dapat berinteraksi dengan server mikrotik pada jaringan lokal, dimana user yang terhubung sudah melalui verifikasi yang dapat melakukan *Filter* aktivitas *malware* dengan rule yang telah ditanamkan.

Keywords:

Security System
Computer Network
Malware
Firewall
Blocking Port

ABSTRACT

Computer networks have an important role in teaching and learning activities in schools, but there are also negative impacts. One of them is prone to attack by malware such as viruses and so on, as is the case at the Satria Mandiri Private Vocational School in Bandar Huluan. So far, the computer network at the school is very easy to attack by malware. The negative impact of malware on the network is bandwidth traffic overload, causing bandwidth constraints to run out quickly or data transfer traffic to be slower than usual. The reliability of a network can be determined from the security factor of the network itself. Some routers have Firewall settings that are quite capable but need to be managed more specifically based on the needs of the 1500 Kbps network scale and available bandwidth. Creating good Rules in the Firewall will make it easier to Filter network traffic and bandwidth so that it can create security and convenience for network and bandwidth users. Port Blocking allows users or users to interact with the proxy server on the local network, where the connected user has gone through verification that can Filter malware activity with embedded Rules.

Penulis Korespondensi:

Andri,
Program Studi Teknik Informatika,
STIKOM Tunas Bangsa, Pematangsiantar, Indonesia
Email: andristb34@gmail.com

1. PENDAHULUAN

Perkembangan teknologi saat ini membuat teknologi sangat berperan penting dalam kehidupan kita saat ini. seiring dengan perkembangan teknologi Informasi saat ini yang selalu berubah, menjadikan keamanan suatu informasi sangatlah penting Jaringan komputer terhadap saat ini amat berkembang dan menjadi kebutuhan [1]–[5]. Banyak serangan sering

dilakukan pada suatu port–port yang dalam keadaan terbuka, sehingga nantinya akan membuat orang–orang yang tidak mempunyai hak akses maupun yang tidak berkepentingan dapat dengan mudah mengendalikan port–port yang telah dimasuki [6]–[9]. Maka untuk melakukan keamanan pada jaringan komputer dalam mengatasi serangan pada port-port, salah satunya adalah dengan menggunakan metode *Port Blocking*.

Port Blocking merupakan suatu sistem keamanan yang dibuat secara khusus untuk sebuah jaringan. Pada dasarnya cara kerja dari *Port Blocking* adalah menutup semua port yang ada, dan hanya user tertentu saja yang dapat mengakses sebuah port yang telah ditentukan, yaitu dengan cara mengetuk terlebih dahulu [10]–[16]. Berbeda dengan cara kerja dari *Firewall*, cara kerja dari *Firewall* adalah menutup semua port tanpa memperdulikan apapun meskipun user tersebut memiliki hak untuk mengakses port tersebut. Sehingga user yang memiliki hak akses tersebut juga tidak bisa untuk mengaksesnya. Kelebihan dari *Port Blocking* dengan *Firewall* adalah meskipun semua port yang ada telah ditutup, tetapi pengguna yang memiliki hak akses dan mengetahui blocking untuk membuka suatu port maka user tersebut tetap dapat menggunakan port yang telah buka [17]. *Firewall* merupakan sebuah sistem pengaman jadi *Firewall* bisa berupa apapun baik hardware maupun software. *Firewall* dapat digunakan untuk melakukan *Filter* 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 *Filter*ing terhadap paket berdasarkan isi dari paket tersebut. *Firewall* merupakan sistem pertahanan yang paling depan untuk jaringan komputer [18].

Penyebaran *malware* komputer 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. Penggunaan jaringan komputer di SMK Swasta Satria Mandiri Bandar Huluan yang terlalu sering digunakan saat proses belajar baik itu offline atau online yang tidak dibatasi saat menggunakan komputer dapat menyebarkan sebuah masalah yang menyerang jaringan komputer. Sehingga diperlukan pengaturan *Filter*ing. *Firewall* yaitu sebuah sistem keamanan jaringan yang dapat memeriksa aktivitas sebuah jaringan komputer dan terhindar dari sebuah serangan yang menuju jaringan komputer yang digunakan, dan menggunakan *Port Blocking* merupakan suatu sistem keamanan yang dibuat secara khusus untuk sebuah jaringan.

Berdasarkan latar belakang permasalahan yang telah diuraikan, maka dilakukan penelitian ini untuk mengkaji lebih dalam permasalahan sebuah sistem keamanan jaringan komputer yang diharapkan dapat membantu pengamanan jaringan komputer yang sering diserang oleh *malware*, sehingga dapat terhindar dari serangan *malware* dan pengguna dapat dengan nyaman menggunakan komputer di SMK Swasta Satria Mandiri Bandar Huluan dalam pelaksanaan kegiatan proses belajar mengajar.

2. METODE PENELITIAN

2.1. Sumber Data dan Waktu Penelitian

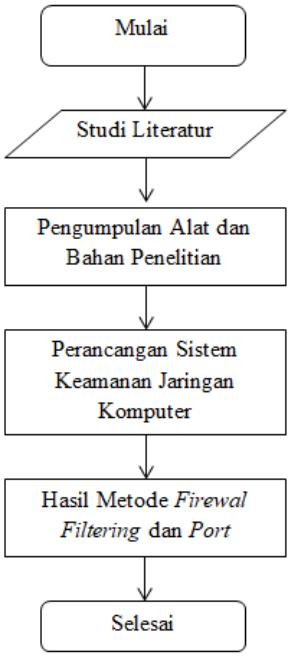
Lokasi penelitian dilakukan di SMK Swasta Satria Mandiri Bandar Huluan yang terletak di Kabupaten Simalungun. Adapun waktu pelaksanaannya dimulai pada bulan Mei sampai dengan Juli 2021. Sumber data yang digunakan pada penelitian ini diperoleh dari wawancara dan observasi terhadap infrastruktur jaringan komputer pada laboratorium sekolah, sehingga dapat melakukan pengembangan terhadap infrastruktur jaringan tersebut. Maka di dapat data sebuah jaringan komputer yang disajikan pada tabel 1 berikut.

Tabel 1. Data Jaringan Laboratorium Komputer

No	Data Jaringan	Kebutuhan Jaringan
1	Kecepatan *Bandwith*	1000 – 1500 Kbps
2	Jaringan Komunikasi	3G
3	Jumlah PC	15
4	IP *Server*	IP Address 192.168.1.2 Subnet Mask 255.255.255.0 Gateway 192.168.1.1
5	IP *Router*	IP Address 192.168.1.3 Subnet Mask 255.255.255.0 Gateway 192.168.1.1
6	IP PC	IP Address 192.168.1.3 - 192.168.1.23

2.2. Rancangan Penelitian

Software pemblokiran yang digunakan pada penelitian ini yaitu Router OS dan teknik pemblokiran menggunakan *Firewall* dan *Port Blocking*. Tahapan ini dimaksudkan agar perancangan lebih mudah dipahami berdasarkan urutan langkah dari awal hingga akhir proses. Perancangan sistem, Setelah itu akan merancang sistem dengan melakukan konfigurasi yang diperlukan agar sistem dapat bekerja sesuai dengan yang diharapkan.



Gambar 1. *Flowchart* Penelitian

Prosedur dan pengambilan data dilakukan dengan beberapa tahapan yaitu:

1. Observasi
   penulis melakukan pengamatan secara langsung ke SMK Swasta Satria Mandiri Bandar Huluan untuk memperoleh data yang akan diperlukan.
2. Studi pustaka
   Merupakan metode pengumpulan data yang diperoleh dari buku-buku atau jurnal dalam pencarian referensi terkait pengumpulan data maupun perancangan aplikasi yang akan dibangun, yaitu referensi mengenai Jaringan komputer, *Firewall Filter*ing dan *Port Blocking*.
3. Analisis kebutuhan
   Penulis akan melakukan analisis kebutuhan untuk menjadi solusi terhadap permasalahan, berupa perangkat yang digunakan, topologi baru yang akan diterapkan, software yang digunakan untuk melakukan pemblokiran yaitu Router OS v5.26 dan teknik pemblokiran menggunakan *Firewall* dan *Port Blocking*.
4. Wawancara Penelitian
   Melakukan wawancara dengan sekretaris yang ada di sekolah dan pengguna untuk mendapatkan data dan informasi yang berkaitan dengan penggunaan jaringan internet pada SMK Swasta Satria Mandiri Bandar Huluan.
5. Pengujian fungsionalitas sistem
   Pada tahap ini, sistem yang telah dikonfigurasi diuji coba fungsionalitasnya apakah sistem keamanan jaringan komputer yang dirancang bekerja dengan semestinya.
6. Pengujian validitas sistem
   Jika sistem keamanan jaringan komputer sudah bekerja sesuai dengan yang diharapkan, kemudian dilakukan uji validitas terhadap parameter yang digunakan untuk melakukan pemblokiran terhadap serangan yang terjadi.

3. HASIL DAN ANALISIS

3.1. Analisis Hardware dan Software

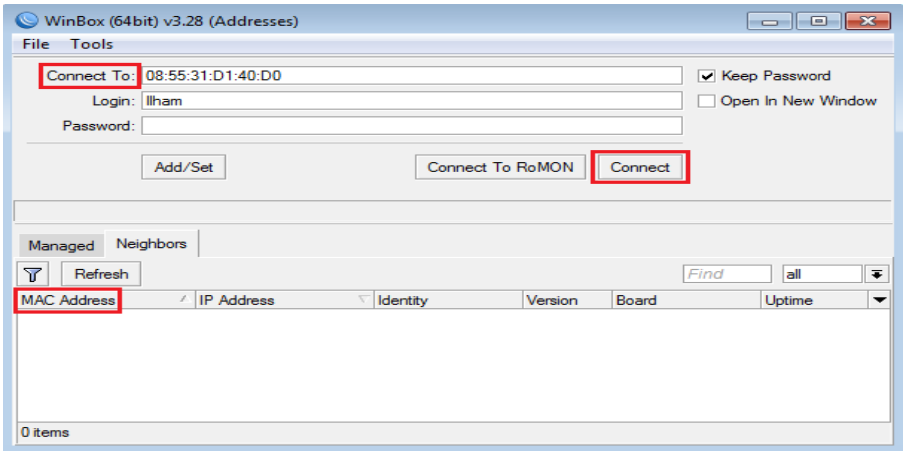
Perangkat keras (Hardware) yang dibutuhkan yaitu router board mikrotik, wireless Access Point, PC client, dan laptop. Router board merupakan device yang digunakan untuk me-routing jaringan dengan sistem operasi mikrotik. Tahap pertama yaitu mengganti router RB941-2nD-Tc yang diinstalasi dengan OS mikrotik, kemudian menghubungkan access point yang akan terhubung langsung dengan mikrotik. Sedangkan perangkat lunak (*Software*) yang dibutuhkan untuk kelancaran sistem adalah winbox v3.28.

3.2. *Filter*ing *Firewall* dan *Port Blocking*

Sistem keamanan jaringan komputer akan menggunakan mikrotik dengan metode *Firewall Filter*ing. Sistem ini akan melakukan pem-*Filter*-an terhadap serangan *malware* menggunakan New *Filter*ing *Firewall Rules* mikrotik, dan *Port Blocking* yang bertugas memblok semua port yang ada di komputer agar tidak ada virus yang dapat menyerang jaringan komputer.

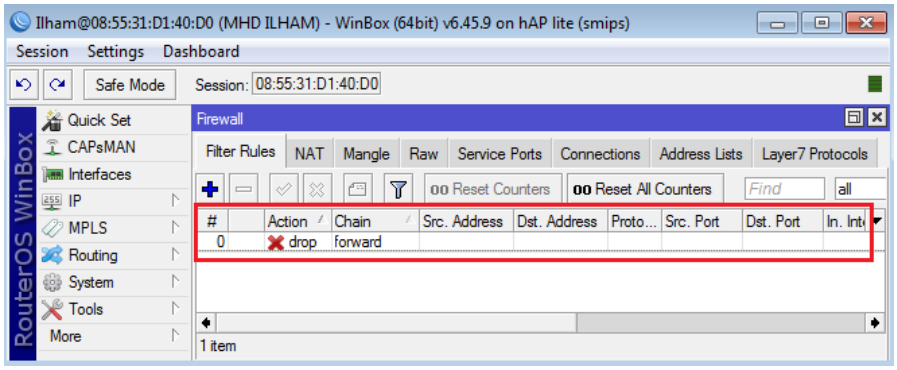
3.3. Hasil Percobaan

1. Login Mikrotik Router board RB941-2Nd-Tc
   Buka aplikasi winbox dan kolom connect to pilih Mac Address Mikrotik yang akan digunakan. Untuk login menggunakan user Ilham dan password default.



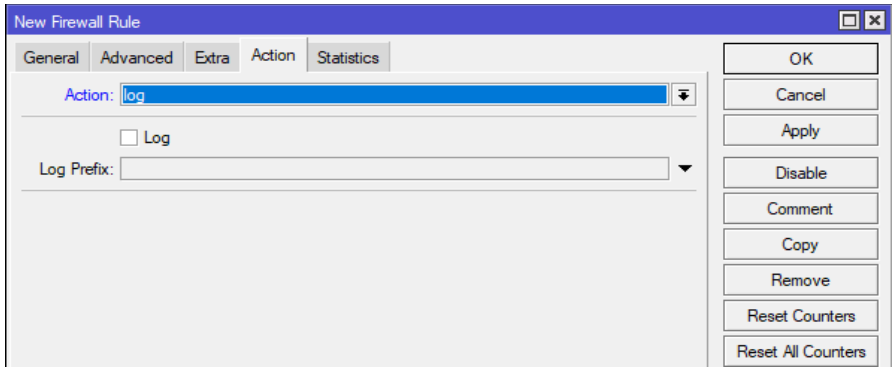
Gambar 2. Menjalankan aplikasi winbox

Setelah Login kedalam software winbox, tahap berikutnya yaitu membuat rule pada *Firewall Filter*. Masih di jendela *Firewall*, klik tab *Filter Rules* kemudian klik tombol add (+) berwarna biru, kemudian lakukan konfigurasi *Filter Rules* General dan *Filter Rules* Action, sehingga menghasilkan *Filter Rules* seperti gambar 3.



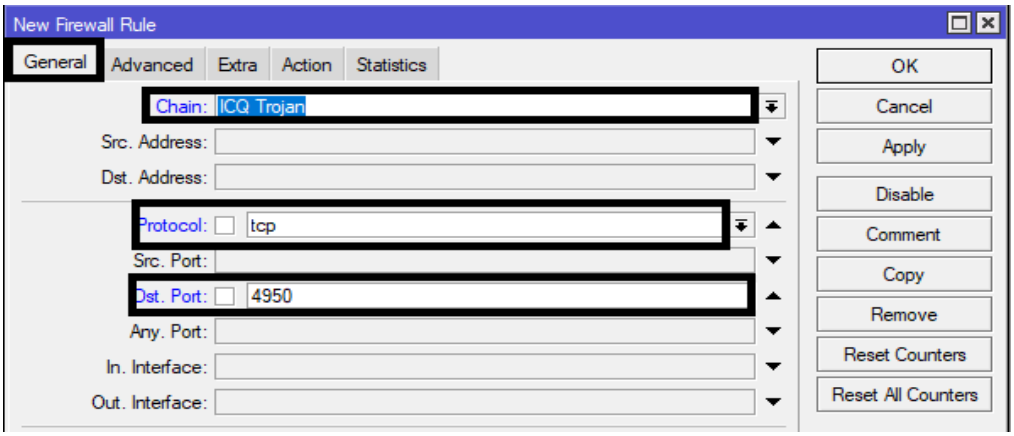
Gambar 3. Hasil *Filter Rules*

Untuk masuk kedalam penambahan rule pada pengaturan *Firewall* maka dibutuhkan akses sebagai admin utama pada router board kemudian menambahkan rule, seperti yang disajikan pada gambar 4.



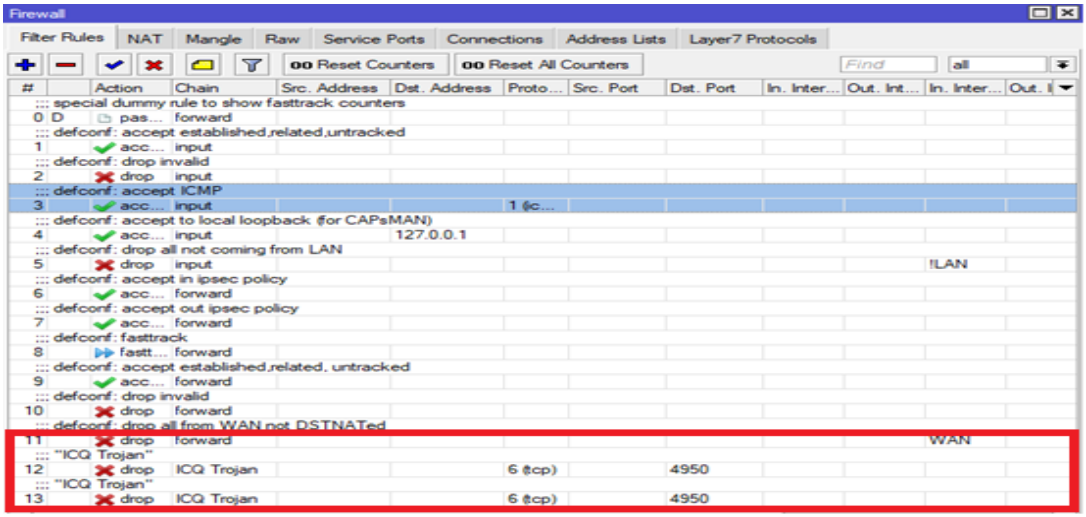
Gambar 4. *Firewall* Rule Mikrotik

2. Pengaturan *Firewall* Memblok ICQ Trojan
   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 5 berikut ini.



Gambar 5. *Firewall* Rule Blok ICQ Trojan

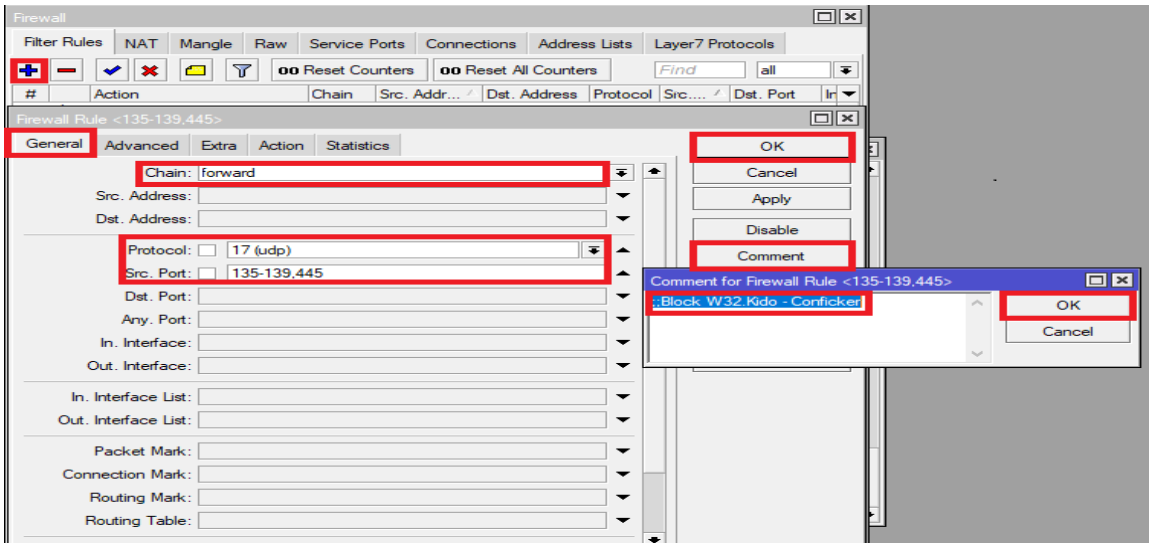
Berdasarkan hasil yang sudah dikaji dapat diartikan bahwa terdapat *malware* pada setiap user atau perangkat komputer yang di gunakan. Hasil nya dapat dilihat seperti pada gambar 6 berikut ini.



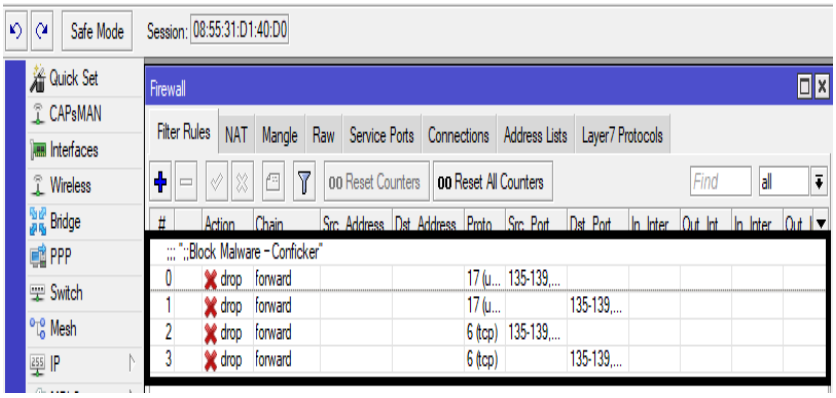
Gambar 6. Hasil *Firewall* Rule Blok ICQ Trojan

3. Pengaturan *Firewall* dan Bridge Blok *Malware*-Confikcer

Pilih *Filter Rules* , kemudian klik add (+) berwarna biru, akan muncul jendela baru seperti gambar dibawah ini. Lalu pilih General dengan mengganti Chain :forward,Protocol:17(udp),Src.port:135-139,445, Comment:;;Block W32*Conficker;; lalu ok kemudian digunakan Action:drop.

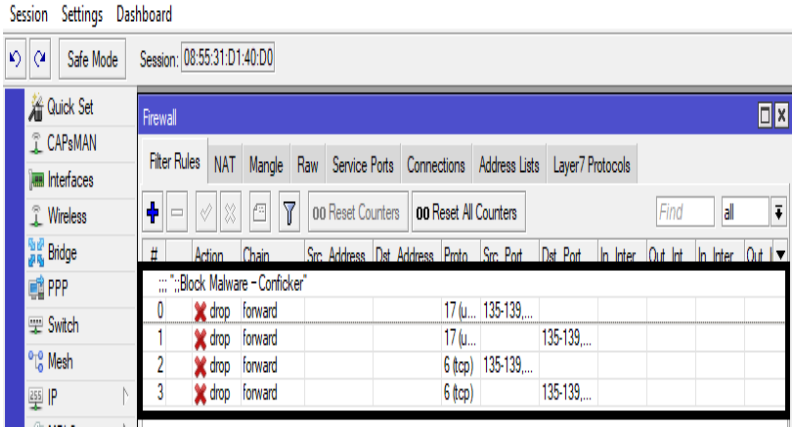


Gambar 7. *Firewall* Rule Blok W32-Conficker



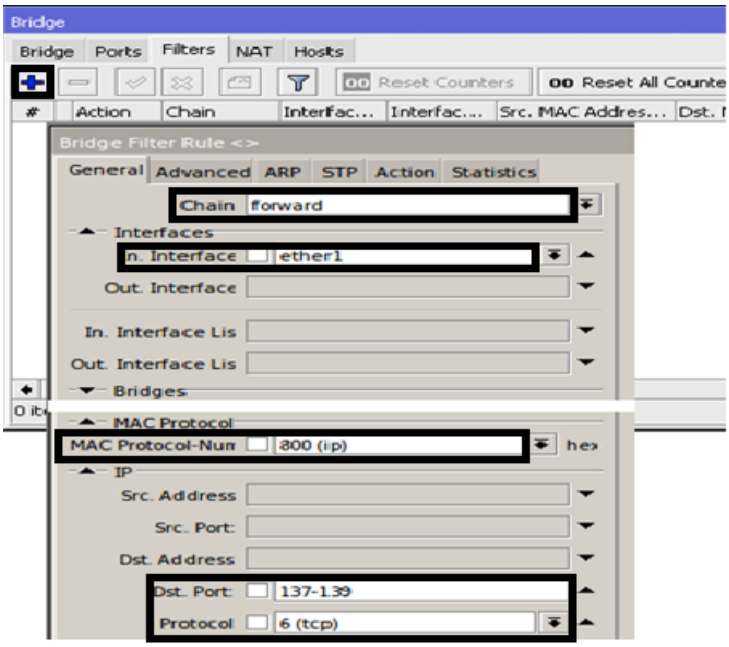
Gambar 8. *Firewall Rules* Action

Berdasarkan pemblokiran Blok Maleware W32-Conficker dari gambar 6, dapat diartikan terdapat *malware* pada setiap user atau perangkat komputer yang di gunakan. Sehingga mendapatkan hasil pemblokiran *malware* tersebut dan didapatkan hasil seperti pada gambar 8 berikut.

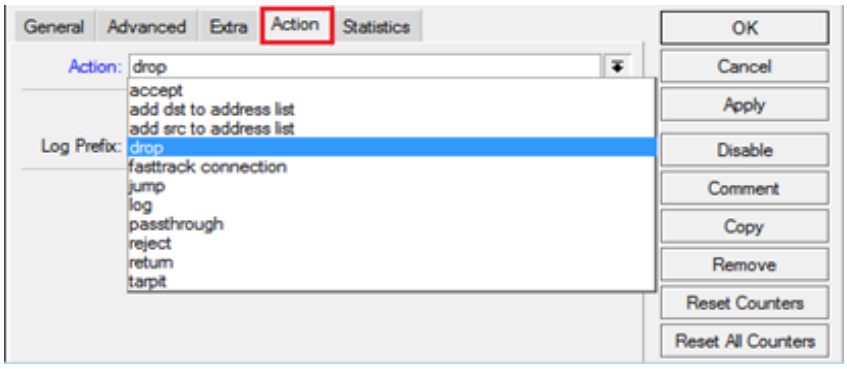


Gambar 9. *Firewall* Blok *Malware* Conficker

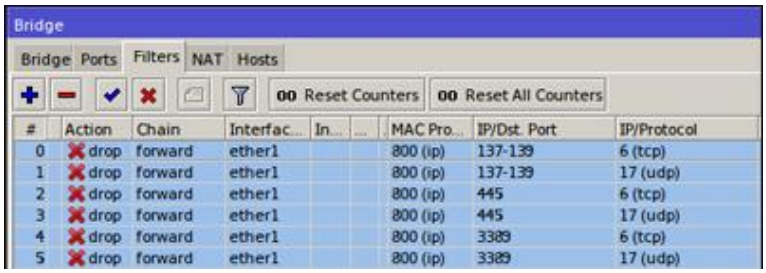
Teknik ini dapat diterapkan pada jaringan dimana semua host berada dalam subnet / segment ip yang sama dan dalam kondisi bridging. Langkahnya definisikan matcher kemudian gunakan action=drop.



Gambar 10. Bridge Rule Blok W32-Conficker



Gambar 11. Bridge *Rules* Action



Gambar 12. Hasil Bridge Rule Blok W32-Conficker

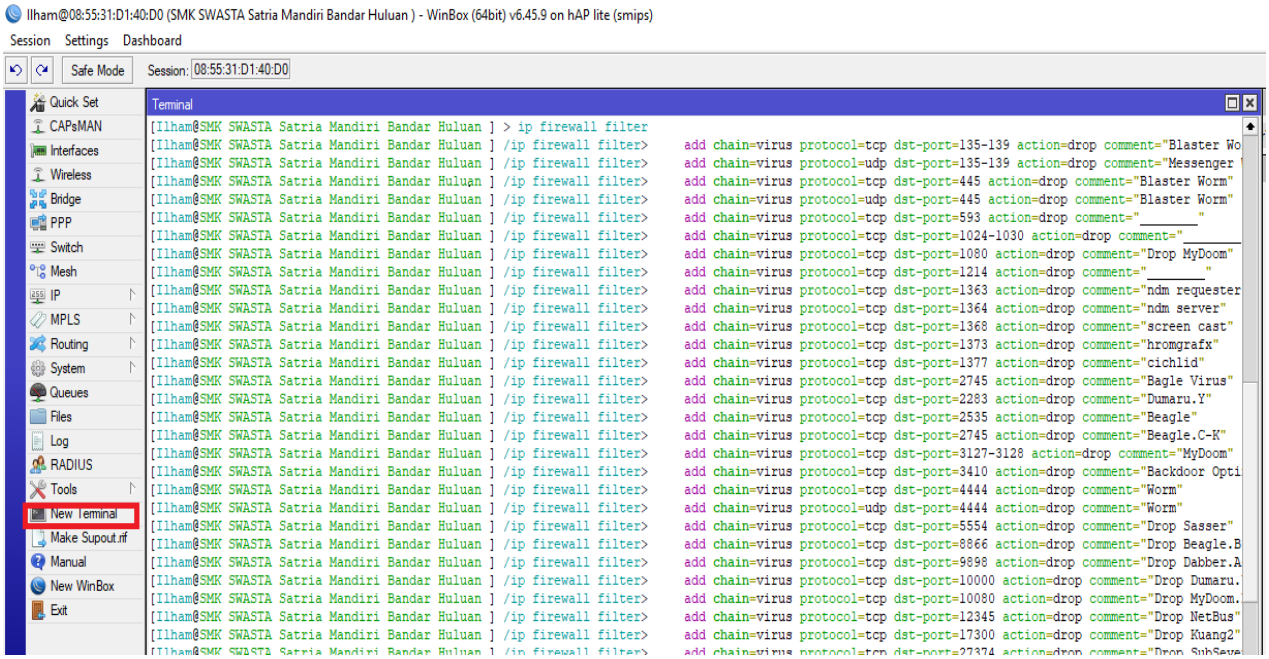
4. Pengaturan *Firewall* Blok Virus

   Sebelum melakukan pemblokiran terhadap virus yang dapat menyerang jaringan komputer, terlebih dahulu harus melakukan pencarian virus dan port mana saja yang dapat diserang oleh virus, sehingga menemukan virus serta port apa saja yang berpotensi diserang seperti yang ada di dalam tabel 2 berikut.

Tabel 2. Data Jaringan Laboratorium Komputer

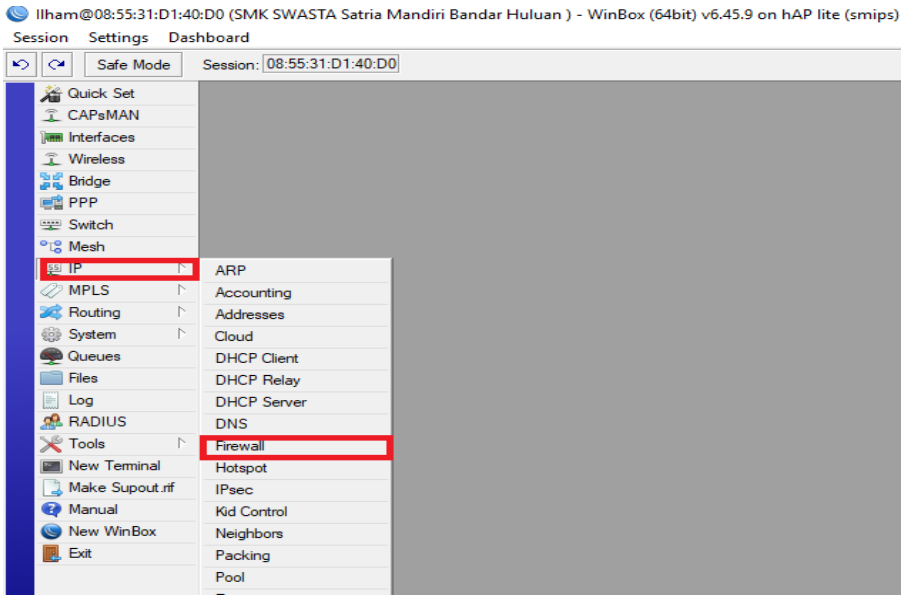
No	Port	Jenis Virus
1	port=135-139	“Blaster Worm"
2	port=135-139	“Massenger Worm"
3	port=445	“Blaster Worm"
4	port=1080	“Drop Mydom"
5	port=1363	"ndm requester"
6	port=1364	"ndm server"
7	port=1368	"screen cast"
8	port=1373	" hromgrafx "
9	port=1377	" cichlid "
10	port=2745	" Bagle Virus "
11	port=2283	" Dumaru.Y "
12	port=2745	" Beagle "
13	port=3127	" Beagle.C-K "
14	port= 3410	" MyDoom "
15	port=444	" Backdoor OptixPro "
16	port=445	" Worm "
17	port=444	" Worm "
18	port=5554	" Drop Sasser
19	port=8866	" Drop Beagle.B "
20	port=9898	" Drop Dabber.A-B"
21	port=10000	" Drop Dumaru.Y "
22	port=10080	" Drop MyDoom.B "
23	port=12345	" Drop NetBus "
24	port=17300	" Drop Kuang2"
25	port=27374	" Drop SubSeven "
26	port=65506	" Drop PhatBot,Agobot, Gaobot "
27	port=12667	" Trinoo "
28	port=27665	" Trinoo "
29	port=31335	" Trinoo "
30	port=2744	" Trinoo "
31	port=27665	" Trinoo "
32	port=31846	" Trinoo "
33	port=34555	" Trinoo "
34	port=35555	" Trinoo "
35	port= 17390	" Trinoo "

Untuk melakukan pemblokiran virus maka dapat dilakukan dengan cara membuka *tools* yang ada di winbox yaitu terminal kemudian ketik ip *Firewall/ add chain = virus protocol = tcp dst-port = 135-139 action = drop comment = "Blaster Worm"*
add chain = virus protocol = udp dst-port = 135-139 action = drop comment = "Messenger Worm"
add chain = virus protocol = tcp dst-port = 445 action = drop comment = "Blaster Worm"
add chain = virus protocol = udp dst-port = 445 action = drop comment = "Blaster Worm"
add chain = virus protocol = tcp dst-port = 1080 action = drop comment = "Drop MyDoom"
add chain = virus protocol = tcp dst-port = 1363 action = drop comment = "ndm requester"
add chain = virus protocol = tcp dst-port = 1364 action = drop comment = "ndm server"
add chain = virus protocol = tcp dst-port = 1368 action = drop comment = "screen cast"
dan seterus nya disesuaikan dengan jenis virus dan jenis port yang dapat diserang seperti gambar yang ada dibawah ini.



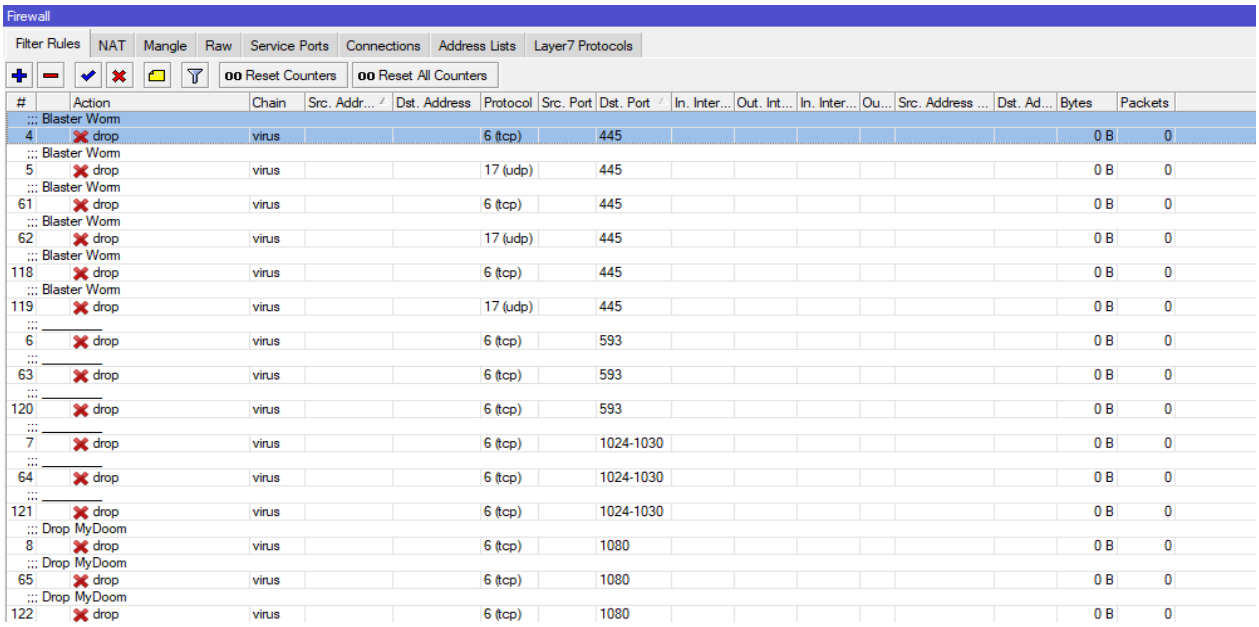
Gambar 13. Penulisan virus di Terminal

Setelah menuliskan jenis virus dan jenis port pada terminal maka selanjutnya dilakukan dengan cara membuka tools ip-*Firewall* seperti gambar 14 berikut ini.



Gambar 14. IP *Firewall*

Selesai melakukan IP-*Firewall* maka mendapatkan hasil pemblokiran virus seperti pada gambar 15 berikut ini.



Gambar 15. Hasil Pemblokiran Virus

4. KESIMPULAN

Pemblokiran *Malware* dan virus dalam port komputer serta membatasi penggunaan jaringan komputer menggunakan mikrotik dapat menghilangkan kekhawatiran bagi setiap user yang terhubung ke jaringan. Jaringan lebih aman, lebih cepat dan stabil. Administrator dapat mengetahui port yang harus dibuka atau ditutup, dan dapat menjadi lapis kedua untuk menutup akses *malware* pada jaringan.

REFERENSI

[1] W. F. Fatoni *et al.*, "Jurnal Mahasiswa Ilmu Komputer (JMIK) DENGAN METODE PORT KNOCKING PADA Jurnal Mahasiswa Ilmu Komputer (JMIK)," vol. 03, no. 01, 2022.

[2] Rahmat, R. Wiji Wahyuningrum, E. Haerullah, and Sodikin, "Analisis Monitoring Sistem Jaringan Komputer Menggunakan Aplikasi Spiceworks," *Jurnal PROSISKO*, vol. 9, no. 1, pp. 44–52, 2022.

[3] A. Wanto, J. T. Hardinata, H. F. Silaban, and W. Saputra, "Analisis Dan Pemodelan Posisi Access Point Pada Jaringan Wi-Fi Menggunakan Metode Simulate Annealing," *Jurnal Sains Komputer dan Informatika (JSAKTI)*, vol. 1, no. 1, pp. 134–143, 2017.

[4] A. Pariddudin and M. Syawaludin, "Penerapan Algoritma Rivest Shamir Adleman untuk Meningkatkan Keamanan Virtual Private Network," *Teknois : Jurnal Ilmiah Teknologi Informasi dan Sains*, vol. 11, no. 2, pp. 73–84, 2021.

[5] Allwine and A. O. D. Aritonang, "Keamanan Jaringan Terpusat Mengunakan Intrusion Detection System (IDS) di STMIK Methodist Binjai," *Jurnal Armada Informatika*, vol. 1, no. 2, pp. 1–11, 2020.

[6] P. Riska, P. Sugiartawan, and I. Wiratama, "Sistem Keamanan Jaringan Komputer Dan Data Dengan Menggunakan Metode Port Knocking," *Jurnal Sistem Informasi dan Komputer Terapan Indonesia (JSIKTI)*, vol. 1, no. 2, pp. 53–64, 2018.

[7] M. R. Lubis *et al.*, *Pengenalan Teknologi Informasi*, 1st ed. Medan: Yayasan Kita Menulis, 2020.

[8] M. Amin *et al.*, *Teknologi Jaringan Nirkabel*, 1st ed. Medan: Yayasan Kita Menulis, 2022.

[9] I. Y. Sari *et al.*, *Keamanan Data dan Informasi*, 1st ed. Medan: Yayasan Kita Menulis, 2020.

[10] Sartomo and W. Sulistyo, "Model Keamanan Jaringan Menggunakan Firewall Port Blocking," *Krea-TIF: Jurnal Teknik Informatika*, vol. 10, no. 1, pp. 10–18, 2022.

[11] R. Rizal, R. Ruuhwan, and K. A. Nugraha, "Implementasi Keamanan Jaringan Menggunakan Metode Port Blocking dan Port Knocking Pada Mikrotik RB-941," *Jurnal ICT : Information Communication & Technology*, vol. 19, no. 1, pp. 1–8, 2020.

[12] T. Brades and I. Irwansyah, "Pemanfaatan Metode Port Knocking dan Blocking Untuk Kamanan Jaringan BPKAD Provinsi Sumsel," *Prosiding Semhavok*, vol. 3, no. 2, pp. 99–107, 2022.

[13] K. Al Fikri and Djuniadi, "Keamanan Jaringan Menggunakan Switch Port Security," *InfoTekJar : Jurnal Nasional Informatika dan Teknologi Jaringan*, vol. 5, no. 2, pp. 302–307, 2021.

[14] D. A. Juhana, Soecipto, and A. Amaliyah, "Perancangan Sistem Keamanan Jaringan Menggunakan Mikrotik Router Pada Management Bandwidth di CV . Algi Pin Bandung," *Telematika*, vol. 3, no. 1, pp. 29–44, 2021.

[15] M. Ryansyah and M. S. Maulana, "*Malware* Security Menggunakan *Filter*ing Firewall Dengan Metode Port Blocking Pada Mikrotik RB 1100AHx2," *Jurnal Sistem dan Teknologi Informasi (JUSTIN)*, vol. 6, no. 3, pp. 116–120, 2018.
[16] P. Akbar, "Metode Block Access Serta Memanejemen Bandwith Pada MikroTik RB951Ui dan MikroTik RB 941-2nD di Caffe Ready Jombang Jawa Timur," *Jurnal Teknologi Dan Sistem Informasi Bisnis*, vol. 4, no. 1, pp. 398–406, 2022.
[17] I. Marzuki, "Perancangan dan Implementasi Sistem Keamanan Jaringan Komputer Menggunakan Metode Port Knocking Pada Sistem Operasi Linux," *Jurnal Teknologi Informasi Indonesia (JTII)*, vol. 2, no. 2, pp. 18–24, 2019.
[18] M. S. Maulana and M. Ryansyah, "*Malware* Security Menggunakan *Filter*ing Firewall Dengan Metode Port Blocking Pada Mikrotik RB 1100AHx2," *Jurnal Sistem dan Teknologi Informasi (JUSTIN)*, vol. 6, no. 3, p. 112, 2018.