KEAMANAN JARINGAN KOMPUTER DENGAN METODE BLOCKING PORT PADA LABORATORIUM KOMPUTER PROGRAM DIPLOMA-III SISTEM INFORMASI UNIVERSITAS MUHAMMADIYAH METRO

Dedi Irawan , S.Kom., M.T.I[1]
[1]Program Diploma-III Sistem Informasi – Universitas Muhammadiyah Metro
[1]Alamat: Jl. KI Hajar Dewantara No.116, Metro Timur, Kota Metro, Lampung 34124, Indonesia
[1]Email: dedi.mti@gmail.com

Abstrack - *Computer network basically has a weakness in security, connect a computer with other computers can allow one or the other party through the network and can access data can even change the content of the data. Mikrotik Router OS is one of the operating systems and software that can be used to make computer into a router network, has a variety of features that can perform bandwidth management and secure network. Diploma-III program Information Systems is one of the majors at the University of Muhammadiyah Metro were precisely located in the City Metro Lampung Province. This study aims to establish a computer network security system with port blocking method in Diploma-III Program Information Systems, University of Muhammadiyah Metro by using research methods of observation, library research and analysis.*

Keywords: *Computer Network, Port Blocking, Mikrotik Router, Router Network, UM Metro*

Abstrak - Jaringan komputer pada dasarnya memiliki kelemahan dalam keamanan, menghubungkan suatu komputer dengan komputer lainnya dapat memungkinkan seseorang atau pihak lain melalui jaringan tersebut dan dapat mengakses data bahkan dapat mengubah isi data tersebut. Router OS Mikrotik merupakan salah satu sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer menjadi router network, memiliki berbagai fitur yang dapat melakukan manajemen bandwith serta mengamankan jaringan. Program Diploma-III Sistem Informasi adalah salah satu jurusan di Universitas Muhammadiyah Metro yang tepatnya berada di Kota Metro Provinsi Lampung. Penelitian ini bertujuan untuk membangun sistem keamanan jaringan komputer dengan metode blocking port di Program Diploma-III Sistem Informasi Universitas Muhammadiyah Metro dengan menggunakan metode penelitian observasi, studi pustaka dan analisis.

Kata Kunci: Jaringan Komputer, Blocking Port, Mikrotik Router, Router Network, UM Metro

1. PENDAHULUAN

1.1 Latar Belakang Masalah

Menurut Kamus Besar dan Pakar, Pengertian Jaringan komputer merupakan sekelompok dari dua atau lebih sistem komputer yang dihubungkan bersama-sama. Dosen dan mahasiswa khususnya di Program Diploma D-III Sistem Informasi menggunakan akses internet sebagai sarana untuk pencarian informasi dan komunikasi. Local Area Network (LAN) bahwa setiap sistem jaringan komputer yang terhubung tidak ada jaminan sebuah keamanan. Di dalam mengimplementasikan komponen dari sistem keamanan jaringan seperti firewall yang berfungsi untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak semua hubungan/kegiatan suatu segemen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya. Dari beragam manfaat internet yang luas, menimbulkan beberapa dampak negatif yang diantaranya masuknya malware dan serangan dari luar yang dapat membahayakan sistem komputer dan menurunkan performa jaringan. Malware dan serangan dari luar dapat masuk melalui port-port terbuka yang tidak digunakan dalam sistem jaringan. Terdapat firewall didalam suatu jaringan komputer yang memiliki fungsi sebagai pencegah gangguan tersebut kemanan dengan kemampuan yang terbatas.

1.2 Rumusan Maasalah

Berdasarkan latar belakang masalah di atas maka dapat dirumuskan permasalahan, yaitu:

1. Bagaimana cara memperkuat kinerja firewall agar sistem keamanan dan data komputer di Laboratorium Program Diploma D-III Sistem Informasi menjadi lebih baik?
2. Bagaimana mengatasi celah keamanan yang memungkinkan malware dan serangan dari luar?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah di atas maka tujuan dari penelitian ini yaitu:

1. Memaksimalkan kinerjan ataupun kemampuan perangkat PC router untuk blocking port pada jaringan laboratorium Program Diploma D-III Sistem Informasi.
2. Meminimalkan resiko masuknya malware dan serangan dari luar yang bertujuan memperlambat jaringan melalui internet ke jaringan laboratorium Program Diploma D-III Sistem Informasi.
3. Menjadikan jaringan komputer laboratorium Program Diploma D-III Sistem Informasi menjadi stabil dan lancar.

1.4 Manfaat Penelitian

Adapun manfaat yang diharapkan dari penelitian ini adalah:

1. Dengan meningkatkatnya kinerja ataupun kemampuan perangkat PC router untuk blocking port diharapkan mahasiswa merasakan kenyamanan pada saat melakukan kegiatan praktium.
2. Dengan tidak adanya penyebaran malware dan serangan dari luar diharapkan jaringan komputer menjadi lancar.

3. Jaringan komputer yang stabil dan lancar membuat transfer atau pertukaran data menjadi aman dan lancar.

2. METODOLOGI PENELITIAN

2.1 Bahan dan Metode

Penelitian ini dilakukan di Laboratorium Komputer Program Diploma-III Sistem Informasi Universitas Muhammadiyah Metro menggunakan metode Research and Development. Menurut Sukmadinata (2006:164) Penelitian dan Pengembangan atau Research and Development (R&D) adalah suatu proses atau langkah-langkah untuk mengembangkan suatu produk baru atau menyempurnakan produk yang telah ada yang dapat dipertanggungjawabkan.

2.2 Perancangan Software (perangkat lunak)

Penyebaran virus dan malware pada jaringan komputer dapat terjadi jika tidak selektif dalam mengaktifkan port apa saja yang digunakan. Untuk mengamankan jaringan dari penyebaran virus dan malware, dapat menutup port komunikasi yang tidak digunakan dan rentan dimanfaatkan oleh virus. Caranya dengan menggunakan rule firewall Mikrotik untuk men-drop paket yang masuk ke port yang tidak digunakan. Beberapa fitur-fitur yang terdapat pada Mikrotik, seperti pada tabel 2.1 di bawah ini:

Tabel 2.1 Fitur Mikrotik

No	Nama Fitur	Keterangan
1.	Address List	Pengelompokan IP Address berdasarkan nama
2.	Asynchronous	Mendukung serial PPP dial-in / dial-out, dengan otentikasi CHAP, PAP, MSCHAPv1 dan MSCHAPv2, Radius, dial on demand, modem pool hingga 128 ports.
3.	Bonding	Mendukung dalam pengkombinasian beberapa antarmuka ethernet kedalam 1 pipa pada koneksi cepat.
4.	Bridge	Mendukung fungsi bridge spinning tree, multiple bridge interface, bridging firewalling.
5.	Data Rate Management	QoS berbasis HTB dengan penggunaan burst, PCQ, RED, SFQ, FIFO queue, CIR, MIR, limit antar peer to peer.
6.	DHCP	Mendukung DHCP tiap antarmuka; DHCP Relay; DHCP Client, multiple network DHCP; static and dynamic DHCP leases.
7.	Firewall dan NAT	Mendukung pemfilteran koneksi peer to peer, source NAT dan destination NAT. Mampu memfilter berdasarkan MAC, IP address, range port, protokol IP, pemilihan opsi protokol seperti ICMP, TCP Flags dan MSS.
8.	Hotspot	Hotspot gateway dengan otentikasi RADIUS. Mendukung limit data rate, SSL ,HTTPS.
9.	IPSec	Protokol AH dan ESP untuk IPSec; MODP Diffie-Hellmann groups 1, 2, 5; MD5 dan algoritma SHA1 hashing; algoritma enkirpsi menggunakan DES, 3DES, AES-128, AES-192, AES-256; Perfect Forwarding Secresy (PFS) MODP groups 1, 2,5.
10.	ISDN	Mendukung ISDN dial-in/dial-out. Dengan otentikasi PAP, CHAP, MSCHAPv1 dan MSCHAPv2, Radius. Mendukung 128K bundle, Cisco

		HDLC, x751, x75ui, x75bui line protokol.
11.	Routing	Routing statik dan dinamik; RIP v1/v2, OSPF v2, BGP v4.
12.	Simple Tunnel	Tunnel IPIP dan EoIP (Ethernet over IP).

2.3 Perancangan Hardware (perangkat keras)

Hardware (perangkat keras) yang digunakan untuk membuat PC Router ini adalah sebagai berikut, seperti pada tabel 2.2 di bawah ini:

Tabel 2.2 Rancangan Hardware (perangkat keras)

No	Nama Komponen	Detail
1.	1 Unit Komputer	Komputer dengan intel pentium dualcore.
2.	2 Unit Lancard (kartu jaringan)	D-Link
3.	Hub	D-Link

2.4 **Rancangan Port yang akan diblokir**

Adapun Port yang akan diblokir dalam penelitian ini adalah sebagai berikut, seperti pada tabel 2.3 di bawah ini.

Tabel 2.3 Rancangan Port yang akan diblokir

No	Nomor Port	Jenis Port	Keterangan
1	135-139	TCP	Drop Blaster Worm
2	135-139	UDP	Drop Messenger Worm
3	445	TCP	Blaster Worm
4	445	UDP	Blaster Worm
5	593	TCP	Trojan
6	1024-1030	TCP	Worm
7	1080	TCP	Drop MyDoom
8	1214	TCP	Worm
9	1363	TCP	ndm requester
10	1364	TCP	ndm server
11	1368	TCP	screen cast
12	1373	TCP	hromgrafx
13	1377	TCP	cichlid
14	1433-1434	TCP	Worm
15	2745	TCP	Bagle Virus
16	2283	TCP	Drop Dumaru.Y
17	2535	TCP	Drop Beagle
18	2745	TCP	Drop Beagle.C-K"
19	3127-3128	TCP	Drop MyDoom
20	3410	TCP	Drop Backdoor OptixPro
21	4444	TCP	Worm
22	4444	UDP	Worm
23	5554	TCP	Drop Sasser
24	8866	TCP	Drop Beagle.B
25	9898	TCP	Drop Dabber.A-B
26	10000	TCP	Drop Dumaru.Y

27	10080	TCP	Drop MyDoom.B
28	12345	TCP	Drop NetBus
29	17300	TCP	Drop Kuang2
30	27374	TCP	Drop SubSeven

3. HASIL DAN PEMBAHASAN

3.1 Proses Input Rule Firewall

Untuk mengamankan jaringan dari penyebaran virus dan malware, dapat menutup port komunikasi yang tidak digunakan dan rentan dimanfaatkan oleh virus. Caranya dengan menggunakan rule firewall Mikrotik untuk men-drop paket yang masuk ke port yang tidak digunakan. Caranya isikan command berikut ini ke terminal Mikrotik:

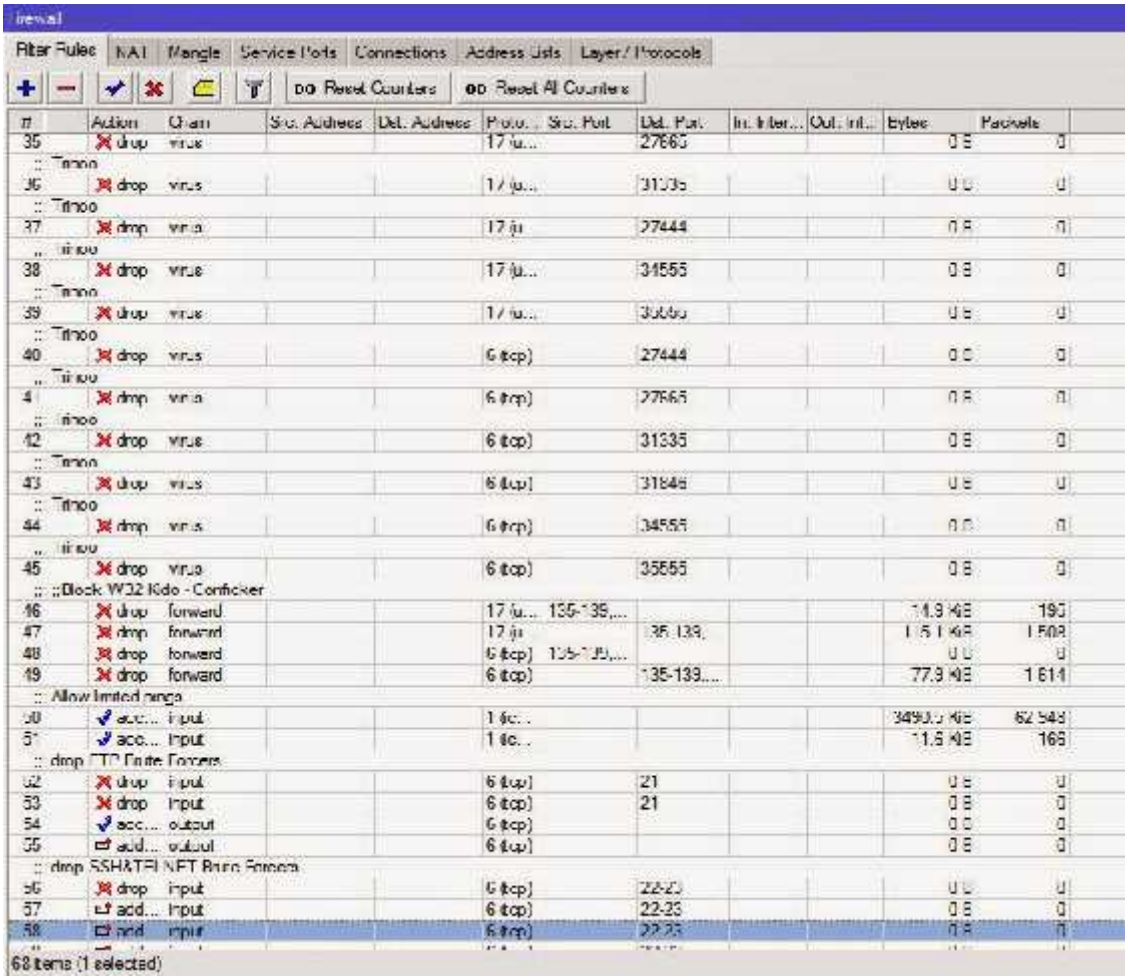
```
/ ip firewall filter
add chain=virus protocol=tcp dst-port=135-139 action=drop comment="Blaster Worm"
add chain=virus protocol=udp dst-port=135-139 action=drop comment="Messenger Worm"
add chain=virus protocol=tcp dst-port=445 action=drop comment="Blaster Worm"
add chain=virus protocol=udp dst-port=445 action=drop comment="Blaster Worm"
add chain=virus protocol=tcp dst-port=593 action=drop comment="_____"
add chain=virus protocol=tcp dst-port=1024-1030 action=drop comment="_____"
add chain=virus protocol=tcp dst-port=1080 action=drop comment="Drop MyDoom"
add chain=virus protocol=tcp dst-port=1214 action=drop comment="_____"
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"
add chain=virus protocol=tcp dst-port=1373 action=drop comment="hromgrafx"
add chain=virus protocol=tcp dst-port=1377 action=drop comment="cichlid"

add chain=virus protocol=tcp dst-port=2745 action=drop comment="Bagle Virus"
add chain=virus protocol=tcp dst-port=2283 action=drop comment="Dumaru.Y"
add chain=virus protocol=tcp dst-port=2535 action=drop comment="Beagle"
add chain=virus protocol=tcp dst-port=2745 action=drop comment="Beagle.C-K"
add chain=virus protocol=tcp dst-port=3127-3128 action=drop comment="MyDoom"
add chain=virus protocol=tcp dst-port=3410 action=drop comment="Backdoor OptixPro"
add chain=virus protocol=tcp dst-port=4444 action=drop comment="Worm"
add chain=virus protocol=udp dst-port=4444 action=drop comment="Worm"
add chain=virus protocol=tcp dst-port=5554 action=drop comment="Drop Sasser"
add chain=virus protocol=tcp dst-port=8866 action=drop comment="Drop Beagle.B"
add chain=virus protocol=tcp dst-port=9898 action=drop comment="Drop Dabber.A-B"
add chain=virus protocol=tcp dst-port=10000 action=drop comment="Drop Dumaru.Y"
add chain=virus protocol=tcp dst-port=10080 action=drop comment="Drop MyDoom.B"
add chain=virus protocol=tcp dst-port=12345 action=drop comment="Drop NetBus"
add chain=virus protocol=tcp dst-port=17300 action=drop comment="Drop Kuang2"
add chain=virus protocol=tcp dst-port=27374 action=drop comment="Drop SubSeven"
add chain=virus protocol=tcp dst-port=65506 action=drop comment="Drop PhatBot,Agobot,
Gaobot"
add chain=virus protocol=udp dst-port=12667 action=drop comment="Trinoo" disabled=no
add chain=virus protocol=udp dst-port=27665 action=drop comment="Trinoo" disabled=no
add chain=virus protocol=udp dst-port=31335 action=drop comment="Trinoo" disabled=no
add chain=virus protocol=udp dst-port=27444 action=drop comment="Trinoo" disabled=no
```

```
add chain=virus protocol=udp dst-port=34555 action=drop comment="Trinoo" disabled=no
add chain=virus protocol=udp dst-port=35555 action=drop comment="Trinoo" disabled=no
add chain=virus protocol=tcp dst-port=27444 action=drop comment="Trinoo" disabled=no
add chain=virus protocol=tcp dst-port=27665 action=drop comment="Trinoo" disabled=no
add chain=virus protocol=tcp dst-port=31335 action=drop comment="Trinoo" disabled=no
add chain=virus protocol=tcp dst-port=31846 action=drop comment="Trinoo" disabled=no
add chain=virus protocol=tcp dst-port=34555 action=drop comment="Trinoo" disabled=no
add chain=virus protocol=tcp dst-port=35555 action=drop comment="Trinoo" disabled=no
add action=drop chain=forward comment=";;Block W32.Kido - Conficker" disabled=no protocol=udp src-port=135-139,445
add action=drop chain=forward comment="" disabled=no dst-port=135-139,445 protocol=udp
add action=drop chain=forward comment="" disabled=no protocol=tcp src-port=135-139,445,593
add action=drop chain=forward comment="" disabled=no dst-port=135-139,445,593 protocol=tcp
add action=accept chain=input comment="Allow limited pings" disabled=no limit=50/5s,2 protocol=icmp
add action=accept chain=input comment="" disabled=no limit=50/5s,2 protocol=icmp
add action=drop chain=input comment="drop FTP Brute Forcers" disabled=no dst-port=21 protocol=tcp src-address-list=FTP_BlackList
add action=drop chain=input comment="" disabled=no dst-port=21 protocol=tcp src-address-list=FTP_BlackList
add action=accept chain=output comment="" content="530 Login incorrect" disabled=no dst-limit=1/1m,9,dst-address/1m protocol=tcp
add action=add-dst-to-address-list address-list=FTP_BlackList address-list-timeout=1d chain=output comment="" content="530 Login incorrect" disabled=no protocol=tcp
add action=drop chain=input comment="drop SSH&TELNET Brute Forcers" disabled=no dst-port=22-23 protocol=tcp src-address-list=IP_BlackList
add action=add-src-to-address-list address-list=IP_BlackList address-list-timeout=1d chain=input comment="" connection-state=new disabled=no dst-port=22-23 protocol=tcp src-address-list=SSH_BlackList_3
add action=add-src-to-address-list address-list=SSH_BlackList_3 address-list-timeout=1m chain=input comment="" connection-state=new disabled=no dst-port=22-23 protocol=tcp src-address-list=SSH_BlackList_2
add action=add-src-to-address-list address-list=SSH_BlackList_2 address-list-timeout=1m chain=input comment="" connection-state=new disabled=no dst-port=22-23 protocol=tcp src-address-list=SSH_BlackList_1
add action=add-src-to-address-list address-list=SSH_BlackList_1 address-list-timeout=1m chain=input comment="" connection-state=new disabled=no dst-port=22-23 protocol=tcp
add action=drop chain=input comment="drop port scanners" disabled=no src-address-list=port_scanners
add action=add-src-to-address-list address-list=port_scanners address-list-timeout=2w chain=input comment="" disabled=no protocol=tcp tcp-flags=fin,!syn,!rst,!psh,!ack,!urg
add action=add-src-to-address-list address-list=port_scanners address-list-timeout=2w chain=input comment="" disabled=no protocol=tcp tcp-flags=fin,syn
add action=add-src-to-address-list address-list=port_scanners address-list-timeout=2w chain=input comment="" disabled=no protocol=tcp tcp-flags=syn,rst
add action=add-src-to-address-list address-list=port_scanners address-list-timeout=2w chain=input comment="" disabled=no protocol=tcp tcp-flags=fin,psh,urg,!syn,!rst,!ack
add action=add-src-to-address-list address-list=port_scanners address-list-timeout=2w
```

```
chain=input comment="" disabled=no protocol=tcp tcp-flags=fin,syn,rst,psh,ack,urg
add action=add-src-to-address-list address-list=port_scanners address-list-timeout=2w
chain=input comment="" disabled=no protocol=tcp tcp-flags=!fin,!syn,!rst,!psh,!ack,!urg
```

Kode atau script di atas menghasilkan seperti pada gambar 3.1 di bawah ini:



Pada gambar 3.1 di atas bisa dilihat dengan jelas paket data melalui port apa saja yang sedang berjalan atau digunakan sehingga administrator pada laboratorium Program Diploma-III Sistem Informasi dengan mudah mendeteksi virus.

3.2 Perbandingan Sebelum dan Sesudah Penerapan Sistem Keamanan Jaringan Dengan Metode Blocking Port

Adapun hasil perbandingan sebelum dan sesudah penerapan system keamanan jaringan dengan metode Blocking Port dapat dilihat pada tabel 3.1 dibawah ini.

Tabel 3.1 perbandingan sebelum dan sesudah penerapan system keamanan jaringan

No	Sebelum Penerapan	Sesudah Penerapan
1	Banyak terdapat virus yang masuk memalui internet dan jaringan local pada laboratorium	Virus yang masuk memalui internet dan jaringan local pada laboratorium menjadi berkurang
2	Jaringan kurang stabil	Jaringan menjadi lebih stabil
3	Koneksi internet sering down	Koneksi internet lebih stabil

4. KESIMPULAN

Beberapa hal yang dapat disimpulkan dari penelitian ini adalah:

1. Dosen dan mahasiswa merasakan bahwa jaringan internet di Program Diploma-III Sistem Informasi menjadi lebih stabil dan aman.
2. Penerapan metode ini jaringan pada laboratorium sering down, namun setelah penerapan metode ini jaringan lokal menjadi lebih stabil.
3. PC Router Mikrotik dapat digunakan untuk memblokir port yang tidak digunakan pada jaringan komputer.
4. Metode ini dapat meminimalkan risiko masuknya malware dan serangan dari luar yang dapat memicu terjadinya kelumpuhan jaringan lokal.

5. REFERENSI

[1] Purbo, O. W. (2000), Linux Untuk Warung Internet, Jakarta: Elex Media Komputindo.

[2] Kurniawan, Wiharsono, Jaringan Komputer, Penerbit Andi, Semarang, 2007

[3] Rafiudin, R. (2006), Membangun Firewalll dan Traffic Filtering Berbasis Cisco, Yogyakarta: Penerbit Andi.

[4] Taringan, A. (2009), Bikin Gateway Murah Pakai Mikrotik, Yogyakarta: Penerbit Ilmu Komputer.

[5] Towidjojo, Rendra 2012, Konsep & Implementasi Routing dengan Router MIKROTIK 100% Connected, Jasakom, Jakarta

[6] MADCOMS 2009, Membangun Sistem Jaringan Komputer, ANDI, Yogyakarta.