

**IMPLEMENTASI SISTEM KEAMANAN JARINGAN KOMPUTER
MENGUNAKAN BLOCKING PORT PADA LABORATORIUM
JURUSAN TEKNIK KOMPUTER**



**Laporan Akhir Ini Disusun Untuk Memenuhi Syarat Menyelesaikan
Pendidikan Diploma III Jurusan Teknik Komputer
Politeknik Negeri Sriwijaya Palembang**

OLEH:

JUMADIL AZWAR

061730700563

POLITEKNIK NEGERI SRIWIJAYA

PALEMBANG

2020

HALAMAN PENGESAHAN LAPORAN AKHIR
IMPLEMENTASI SISTEM KEAMANAN JARINGAN KOMPUTER
MENGGUNAKAN BLOCKING PORT PADA LABORATORIUM
JURUSAN TEKNIK KOMPUTER



Oleh :

Jumadil Azwar

061730700563

Palembang, Agustus 2020

Pembimbing I

Pembimbing II

Adi Sutrisman, S.Kom., M.Kom

NIP. 197503052001121005

Mustaziri, S.T., M.Kom

NIP. 196909282005011002

Mengetahui,

Ketua Jurusan Teknik Komputer

Azwardi, S.T., M.T

NIP. 197005232005011004

MOTTO DAN PERSEMBAHAN

***Menuntut Ilmu merupakan Taqwa, Mengantarkan Ilmu merupakan Ibadah,
Mengulang Ilmu merupakan Dzikir, Mencari Ilmu merupakan Jihad.***

***Intelligence is not the determinant of success, but hard work is the real
determinant of your success***
***(Kecerdasan bukan penentu kesuksesan, tapi kerja keraslah yang merupakan
penentu kesuksesanmu yang sebenarnya)***

***It's Better to feel how hard education is at this time rather than fell the
bitterness of stupidity, later.***
***(Lebih baik merasakan sulitnya pendidikan saat ini daripada merasakan rasa
pahitnya kebodohan kelak)***

Do your best at any moment that you have.
(Lakukan yang terbaik dalam setiap momen yang anda miliki)

Kupersembahkan Untuk :

- ❖ Allah SWT**
- ❖ Bapak dan Mama**
- ❖ Adik – Adikku**
- ❖ Keluarga dan kerabat dekatku**
- ❖ Sahabat – Sahabatku**
- ❖ Teman Seperjuangan Kelas CC 2017**
- ❖ Mahasiswa Teknik Komputer
Angkatan 2017**
- ❖ Almamaterku**

ABSTRAK

“ IMPLEMENTASI SISTEM KEAMANAN JARINGAN KOMPUTER MENGUNAKAN BLOCKING PORT PADA LABORATORIUM JURUSAN TEKNIK KOMPUTER ”

(**Jumadil Azwar**) : (**2020 : 50 Halaman**)

Laporan akhir ini menjelaskan tentang bagaimana membangun dan mengimplementasikan sistem keamanan jaringan komputer dengan menggunakan metode *blocking port*. Sistem ini menggunakan *router* mikrotik sebagai media keamanan dan menggunakan *rule firewall* dalam pengimplementasiannya. Dalam pendeskripsian *port* yang akan diblokir karena rancangan *port* yang akan diblokir cukup banyak, *rule firewall* yang dibuat yaitu dengan menggunakan *script* untuk mengefektifkan waktu dalam penginputan *port*. Adapun cara kerja sistemnya yaitu *rule blocking port* akan aktif apabila ada *malware* atau serangan yang masuk melalui *port-port* yang aktif (terbuka). Sehingga dengan adanya sistem keamanan ini jaringan lokal yang ada pada laboratorium jurusan komputer menjadi stabil dan lancar.

Kata Kunci : Jaringan Komputer, *Blocking Port*, *Firewall*, *Malware*, *Router*

ABSTRACT

“ IMPLEMENTATION OF COMPUTER NETWORK SECURITY SYSTEM USING BLOCKING PORT IN COMPUTER ENGINEERING LABORATORY ”

(Jumadil Azwar): (2020: 50 Pages)

This final report describes how to build and implement a computer network security system using port blocking . This system uses a proxy router as a security medium and uses a firewall rule in its implementation. In describing the port to be blocked because there are quite a lot of port designs to be blocked, firewall rules are made by using a script to streamline port input time. The way the system works is that the port blocking rule will be active if there is malware or attacks that enter through the ports active (open). So that with this security system the local network in the computer department laboratory becomes stable and smooth.

Keyword: Computer Network, Port Blocking, Firewall, Malware, Router

KATA PENGANTAR

Puji dan syukur penulis haturkan kehadiran Allah SWT yang telah memberikan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan proposal laporan akhir yang berjudul “**Implementasi Sistem Keamanan Jaringan Komputer Menggunakan *Blocking Port* Pada Laboratorium Jurusan Teknik Komputer**”.

Laporan Akhir ini disusun untuk memenuhi syarat menyelesaikan Pendidikan Diploma III Teknik Komputer di Politeknik Negeri Sriwijaya.

Dalam mengerjakan laporan akhir dari persiapan hingga proses penyusunan laporan, penulis banyak mendapat bantuan dari berbagai pihak, berupa bimbingan, petunjuk, informasi maupun pelayanan. Oleh karena itu pada kesempatan ini penulis ingin menyampaikan terima kasih yang sebesar-besarnya kepada :

1. Allah SWT yang telah memberikan kesehatan, kesempatan, petunjuk dan karunia-Nya.
2. Kedua Orang Tua dan Keluarga yang selalu memberikan semangat, senantiasa mencurahkan segala kasih sayang dan doa restu dalam menyelesaikan Laporan Akhir ini.
3. Bapak Dr. Ing. Ahmad Taqwa, M.T., selaku Direktur Politeknik Negeri Sriwijaya.
4. Bapak Azwardi, ST., MT., selaku Ketua Jurusan Teknik Komputer Politeknik Negeri Sriwijaya.
5. Bapak Yulian Mirza, S.T., M.Kom., selaku Sekretaris Jurusan Teknik Komputer Politeknik Negeri Sriwijaya.
6. Bapak Adi Sutrisman, S.Kom., M.Kom., selaku Dosen pembimbing I Jurusan Teknik Komputer Politeknik Negeri Sriwijaya.
7. Bapak Mustaziri, S.T., M.Kom., selaku Dosen pembimbing II Jurusan Teknik Komputer Politeknik Negeri Sriwijaya.
8. Bapak/Ibu Dosen Jurusan Teknik Komputer yang telah mendidik dan memberikan ilmunya.

9. Teman-teman seperjuangan Jurusan Teknik Komputer, khususnya kelas CC tahun ajar 2017 yaitu Ditha, Salman, Imam, Dwiky, Akbar, Saldi, Ade, Yesi, Okky, Echa, Syifa, Cheria, Fikri, Adhan, Reyhan, Diah, Seh Nur, Bima, Torik, Ju dan Laila, yang selalu memberikan dorongan dan dukungan serta telah membantu dalam penyusunan laporan ini.
10. Teman-Teman ku dari SD, SMP, SMA (kelas 10,11,12) terkhusus Fathiyah, Mona, Mitak, Tasya, Kiki, Dina, Dianita, Feby Ayuk, Feby Adek, Ardi, Dian, Yuk Muti, Aam, Eva, Eyik dan teman teman lain yang telah memberikan dorongan dan semangat serta Doa demi kelancaran dalam penyusunan laporan ini.
11. Semua pihak yang telah membantu dalam menyelesaikan Laporan Akhir ini. Special Thanks untuk Laptop Dian , Printer dan Headset Ditha, Kabel LAN Ade, Flashdisk Saldi dan Yesi serta Printer Salman karena barang-barang kalian telah membantu saya dalam penyusunan laporan ini.

Penulis menyadari sepenuhnya bahwa masih terdapat kesalahan dan kekurangan dalam penyusunan laporan ini. Oleh karena itu, penulis mengharapkan saran dan kritik yang bersifat membangun demi kesempurnaan penulisan yang akan datang. Penulis berharap agar laporan akhir ini dapat dipahami, berguna dan bermanfaat bagi rekan-rekan pembaca, khususnya mahasiswa-mahasiswi Jurusan Teknik Komputer Politeknik Negeri Sriwijaya sehingga tujuan yang diharapkan dapat tercapai, Aamiin.

Palembang, September 2020

Penulis

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN	ii
HALAMAN PENGESAHAN PENGUJI	iii
MOTTO DAN PERSEMBAHAN	iv
ABSTRAK	v
ABSTRACT	vi
KATA PENGANTAR	vii
DAFTAR ISI	ix
DAFTAR GAMBAR	xii
DAFTAR TABEL	xiv

BAB I PENDAHULUAN

1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	3
1.4 Tujuan dan Manfaat	3
1.4.1 Tujuan	3
1.4.2 Manfaat	3

BAB II TINJAUAN PUSTAKA

2.1 Jaringan	4
2.1.1 Pengertian Jaringan Komputer	4
2.1.2 Klasifikasi Jaringan	4
2.1.3 IP Address.....	6
2.2 <i>Network Security</i> (Keamanan Jaringan).....	11
2.2.1 Pengertian Keamanan Jaringan	11
2.2.2 Sistem Keamanan Jaringan Komputer	12
2.2.3 Aspek Dasar Keamanan Jaringan Komputer.....	12
2.3 <i>Blocking Port</i>	14

2.4	<i>Firewall</i>	14
2.4.1	Pengertian <i>Firewall</i>	14
2.4.2	Fungsi <i>Firewall</i>	14
2.5	<i>Router</i>	15
2.5.1	Pengertian <i>Router</i>	15
2.6	Mikrotik <i>Router</i>	16
2.6.1	Pengertian Mikrotik	16
2.6.2	Jenis – Jenis Mikrotik	16
2.7	<i>Malware</i>	17
2.7.1	Pengertian <i>Malware</i>	17
2.7.2	Macam – Macam <i>Malware</i>	17
2.8	<i>Port</i>	18
2.8.1	Pengertian <i>Port</i>	18
2.9	<i>Port Scanning</i>	19
2.9.1	Pengertian <i>Port Scanning</i>	19
2.10	<i>Network Mapper</i> (NMAP)	19
2.10.1	Pengertian <i>NMAP</i>	19

BAB III RANCANG BANGUN

3.1	Tujuan Perancangan	21
3.2	Topologi Jaringan	21
3.3	<i>Flowchart</i> Sistem	22
3.4	Perangkat Keras Yang Digunakan	23
3.5	Perangkat Lunak Yang Digunakan	23
3.6	Perancangan <i>Port</i> Yang Akan Diblokir	23
3.7	Cara Kerja Sistem	25

BAB IV HASIL DAN PEMBAHASAN

4.1	Hasil	26
4.2	Pembahasan	26
4.2.1	Konfigurasi <i>Router</i> Mikrotik Sebagai <i>Gateway</i> Internet.	26
4.2.2	Konfigurasi <i>Blocking Port</i>	30

4.2.3	Konfigurasi <i>Client</i> ke <i>Router</i>	35
4.2.4	Pengujian Sistem	37
4.3	Analisa	49

BAB V KESIMPULAN DAN SARAN

5.1	Kesimpulan	50
5.2	Saran	50

DAFTAR PUSTAKA

LAMPIRAN

DAFTAR GAMBAR

	Halaman
Gambar 2.1 Model LAN.....	5
Gambar 2.2 Model MAN	5
Gambar 2.3 Model WAN	6
Gambar 2.4 Model WLAN	6
Gambar 2.5 <i>Format Penulisan IP Address</i> versi 4 (IPv4)	7
Gambar 2.6 <i>Macam Kelas IP Address</i>	7
Gambar 2.7 <i>Format Kelas IP Address</i>	10
Gambar 2.8 <i>Format IP Address</i>	10
Gambar 2.9 Mikrotik <i>Routerboard</i>	17
Gambar 3.1 Perancangan Topologi Jaringan	21
Gambar 3.2 <i>Flowchart</i> Sistem	22
Gambar 4.1 Tampilan <i>IP Address</i> pada Winbox	26
Gambar 4.2 Menambahkan <i>IP Gateway</i>	27
Gambar 4.3 Tampilan pada menu <i>Route</i>	27
Gambar 4.4 Setting DNS	28
Gambar 4.5 Ping Google	28
Gambar 4.6 Setting NAT.....	29
Gambar 4.7 Tampilan pada menu NAT	29
Gambar 4.8 Memasukkan <i>script</i> koneksi <i>firewall</i>	30
Gambar 4.9 Tampilan <i>script</i> untuk koneksi pada Winbox	31
Gambar 4.10 Memasukkan <i>script</i> <i>blocking port</i>	33
Gambar 4.11 Tampilan <i>rule</i> <i>blocking port</i> pada Winbox	33
Gambar 4.12 Memasukkan <i>script</i> ke <i>chain forward</i>	34
Gambar 4.13 Tampilan <i>rule</i> <i>script</i> <i>chain forward</i> pada Winbox	34
Gambar 4.14 <i>Setting IP Client 1</i>	35
Gambar 4.15 <i>Setting IP Client 2</i>	36
Gambar 4.16 <i>Monitoring Malware</i> yang Masuk	36
Gambar 4.17 Tampilan awal NMAP	37

Gambar 4.18 Setting Aplikasi <i>Scanning Port</i> NMAP	38
Gambar 4.19 Hasil <i>Port Scanning</i> Awal	39
Gambar 4.20 Tampilan <i>Rule Firewall</i> setelah ditambahkan <i>script</i>	40
Gambar 4.21 Hasil <i>Port Scanning</i> ketika <i>Rule Firewall Enable</i>	41
Gambar 4.22 Tampilan LOIC	42
Gambar 4.23 Tampilan LOIC setelah ditambahkan IP target	42
Gambar 4.24 Tampilan LOIC setelah ditambahkan <i>port</i> target	43
Gambar 4.25 Tampilan LOIC pada saat menyerang target	43
Gambar 4.26 Tampilan <i>monitoring byte</i> dan <i>packet data</i> yang masuk	44
Gambar 4.27 Tes ping untuk mengecek koneksi jaringan	45
Gambar 4.28 Tampilan <i>Rule Blocking Port</i> dalam kondisi <i>disable</i>	45
Gambar 4.29 Tampilan Aplikasi NMAP dalam kondisi <i>disable</i>	46
Gambar 4.30 Tampilan LOIC pada saat <i>rule blocking port</i> dimatikan	46
Gambar 4.31 Tes Ping dalam kondisi <i>rule blocking port</i> dimatikan	47
Gambar 4.32 Tampilan <i>Rule Blocking Port</i> dalam kondisi <i>enable</i>	48
Gambar 4.33 Pengetesan jaringan dengan melalui terminal	48

DAFTAR TABEL

	Halaman
Tabel 3.1 Rancangan <i>Port</i> yang akan diblokir	23
Tabel 4.1 Hasil <i>Port Scanning</i> sebelum dilakukan pemblokiran	39