

LAPORAN AKHIR

**MALWARE SECURITY MENGGUNAKAN FILTERING FIREWAL
PADA ROUTER MIKROTIK DI JURUSAN TEKNIK KOMPUTER
POLITEKNIK NEGERI SRIWIJAYA**



**Laporan ini disusun untuk memenuhi syarat menyelesaikan
Pendidikan Diploma III Jurusan Teknik Komputer
Politeknik Negeri Sriwijaya**

Oleh :

Oki Winanda (0617 3070 0545)

**JURUSAN TEKNIK KOMPUTER
POLITEKNIK NEGERI SRIWIJAYA
PALEMBANG**

2020

MALWARE SECURITY MENGGUNAKAN FILTERING FIREWALL
PADA ROUTER MIKROTIK DI JURUSAN TEKNIK KOMPUTER
POLITEKNIK NEGERI SRIWIJAYA



Telah Diuji dan dipertahankan di depan dewan penguji pada sidang
Laporan Akhir pada Selasa, 18 Agustus 2020

Ketua Dewan penguji

Yulian Mirza, S.T., M.Kom.
NIP. 196607121990031003

Anggota Dewan penguji

Meiyi Darlies, S.Kom., M.Kom.
NIP. 197805152006041003

Alan Novi Tompang, S.T., M.T.
NIP. 197611082000031002

Hartati Deviana, S.T., M.Kom.
NIP. 197405262008122001

Tanda Tangan

Palembang, September 2020
Mengetahui,
Ketua Jurusan Teknik Komputer

Azwardi, S.T., M.T.
NIP. 197005232006011004

LEMBAR PENGESAHAN LAPORAN AKHIR
MALWARE SECURITY MENGGUNAKAN FILTERING FIREWALL
PADA ROUTER MIKROTIK DI JURUSAN TEKNIK KOMPUTER
POLITEKNIK NEGERI SURABAYA



OKI WINANDA
0617 3070 0545

Palembang, September 2020
Menyetujui,
Pembimbing II

Pembimbing I

Slamet Widodo, S.Kom., M.Kom.
NIP. 197305162002121001

Ali Firdaus, S.Kom., M.Kom.
NIP. 197010112001121001

Mengetahui,
Ketua Jurusan Teknik Komputer

Azwardi, S.T., M.T.
NIP. 197005232005011004

KATA PENGANTAR

Puji syukur kita panjatkan kehadirat Tuhan Yang Maha Esa karena berkat rahmat dan hidayah serta pertolongan-Nya sehingga kami dapat menyelesaikan Laporan Akhir ini dengan Judul Malware security menggunakan filtering firewall pada router mikrotik di jurusan Teknik Komputer Politeknik Negeri Sriwijaya.

Adapun maksud dan tujuan dari penyusunan Laporan Akhir ini adalah sebagai persyaratan untuk menyelesaikan Pendidikan Diploma III pada Jurusan Teknik Komputer Politeknik Negeri Sriwijaya.

Dalam penulisan laporan ini, penulis banyak mendapatkan pengarahan dan bimbingan serta bantuan dari berbagai pihak. Oleh karena itu penulis mengucapkan terima kasih kepada:

1. Yth. Bapak Dr. Ing. Ahmad Taqwa, MT. Direktur Politeknik Negeri Sriwijaya.
2. Yth. Bapak Azwardi, S.T., M.T. Ketua Jurusan Teknik Komputer.
3. Yth. Bapak Slamet Widodo, S.Kom., M.Kom. Dosen Pembimbing I, yang telah memberikan bimbingan dan pengarahan.
4. Yth. Bapak Ali Firdaus, S.Kom., M.Kom. Dosen Pembimbing II, yang telah memberikan bimbingan dan pengarahan.
5. Kedua orang tua yang telah memberikan semangat serta mendoakan hingga tersusunnya laporan ini.
6. Semua rekan seperjuangan yang selalu memberi motivasi dan kerja samanya dalam proses penyelesaian Laporan Akhir ini.

Serta pihak yang namanya tidak bisa kami sebutkan satu persatu, tanpa mengurangi rasa hormat dan terima kasih kami kepada mereka, Semoga Laporan Akhir ini dapat bermanfaat bagi kita semua.

Palembang, Agustus 2020

Penulis

ABSTRAK

Malware merupakan salah satu bentuk dari kejahatan komputer yang terjadi pada sebuah sistem jaringan komputer, malware NjRAT adalah salah satu dari malware yang sangat berbahaya karena besarnya dampak kerugian yang ditimbulkan, mulai dari pencurian data penting sampai mengubah hak akses pada computer korban. Aktivitas malware berkaitan erat dengan memory computer, performance computer dan juga aktifitas network pada system computer. Penelitian ini bertujuan untuk mengetahui cara kerja malware NjRAT dan melakukan investigasi terhadap performance pada system computer. Metodologi yang digunakan dynamic analysis dengan melakukan analisa malware pada suatu sistem dan melihat aktivitas atau proses yang diaktifkan oleh malware tersebut. Dampak perubahan yang terjadi pada PC Korban terlihat pada performance masing-masing PC yang telah disisipkan malware.

Kata kunci: Malware, NjRAT, System computer

ABSTRAK

Malware is a form of computer crime that occurs on a computer network system, NjRAT malware is one of the most dangerous malware because of the large impact of the loss, ranging from theft of important data to changing access rights on the victim's computer. Malware activity is closely related to computer memory, computer performance and network activity on computer systems. This study aims to determine how the NjRAT malware works and to investigate the performance of the computer system. The methodology used is dynamic analysis by analyzing malware on a system and seeing the activities or processes that are activated by the malware. The impact of changes that occur on the victim's PC can be seen in the performance of each PC where malware has been inserted.

Keywords: Malware, NjRAT, computer system

MOTTO

“Allah tidak membebani seseorang melainkan sesuai kesanggupannya”
(QS al-baqarah 286)

Kupersembahkan untuk kedua orang tuaku, dan adikku

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN.....	ii
MOTTO DAN PERSEMBAHAN.....	iii
ABSTRAK	iv
KATA PENGANTAR.....	vi
DAFTAR ISI.....	vii
DAFTAR GAMBAR.....	x
BAB I PENDAHULUAN	
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah	3
1.4 Tujuan dan Manfaat	3
1.4.1 Tujuan	3
1.4.2 Manfaat	3
1.5 Sistematika Penulisan	3
BAB II TINJAUAN PUSTAKA	
2.1 Penelitian Terdahulu	5
2.2 Mikrotik	6
2.2.1 Mikrotik OS.....	7
2.2.2 Akses Mikrotik.....	7
2.3 Jaringan Komputer.....	8
2.3.1 Jenis - Jenis Jaringan	8
2.3.2 Topologi Jaringan	11
2.3.3 Jenis - Jenis Topologi Jaringan	11
2.4 TCP	16

2.5	<i>Malware</i>	17
2.5.1	Jenis-Jenis <i>Malware</i>	19
2.6	<i>Port</i>	21
2.7	<i>Firewall</i>	22
2.8	Router.....	22
2.9	<i>Packet Filtering</i>	22
2.10	Aplikasi Winbox	25
2.10.1	Fungsi Winbox.....	25

BAB III RANCANG BANGUN

3.1	Perancangan Sistem.....	27
3.1.1	Diagram Alir Rancang Bangun Sistem	27
3.1.2	Metode Pengumpulan Data	29
3.2	Spesifikasi Kebutuhan Perangkat	29
3.2.1	Perangkat Keras	29
3.2.2	Perangkat Lunak	29
3.3	Perancangan Topologi Keamanan Jaringan	30
3.4	Perancangan Alat	31
3.4.1	Penyiapan Perangkat	31
3.4.2	Konfigurasi dan Instalasi Akses Internet Mikrotik	31
3.4.3	Instalasi Mikrotik untuk Kabel LAN	35
3.4.4	Instalasi Mikrotik untuk <i>wifi</i>	37
3.4.5	Instalasi <i>Access Point</i>	39

BAB IV IMPLEMENTASI DAN PEMBAHASAN

4.1	<i>Login Winbox</i>	42
4.2	Konfigurasi <i>firewall rule</i>	43
4.2.1	Hasil Konfigurasi <i>firewall rule</i>	49

BAB V PENUTUP

5.1 Kesimpulan50
5.2 Saran.....50

DAFTAR PUSTAKA

LAMPIRAN

DAFTAR GAMBAR

Gambar 2.1	Jaringan Komputer	8
Gambar 2.2	PAN (<i>Personal Area Network</i>).....	9
Gambar 2.3	LAN (<i>Local Area Network</i>).....	9
Gambar 2.4	MAN (<i>Metropolitan Area Network</i>)	10
Gambar 2.5	WAN (<i>Wide Area Network</i>)	10
Gambar 2.6	Topologi <i>Bus</i>	12
Gambar 2.7	Topologi <i>Star</i>	13
Gambar 2.8	Topologi <i>Ring</i>	14
Gambar 2.9	Topologi <i>Mesh</i>	15
Gambar 2.10	<i>Winbox</i>	26
Gambar 3.1	Blok Diagram.....	27
Gambar 3.2	Diagram Alir	28
Gambar 3.3	Topologi system keamanan Jaringan	30
Gambar 3.4	Login Mikrotik	31
Gambar 3.5	Membuat IP ISP	32
Gambar 3.6	Mengganti Nama Interfaces	32
Gambar 3.7	Membuat ISP Route	33
Gambar 3.8	Membuat Pengaturan Firewall NAT General	33
Gambar 3.9	Membuat Pengaturan Firewall NAT Action	34
Gambar 3.10	Membuat Pengaturan DNS	34
Gambar 3.11	Melakukan Test PING	35
Gambar 3.12	Login Mikrotik	35
Gambar 3.13	Membuat IP LAN.....	36
Gambar 3.14	Mengganti nama interfaces	36
Gambar 3.15	Melakukan pengaturan DHCP Server	37
Gambar 3.16	Login Mikrotik	37
Gambar 3.17	Membuat IP hotspot	38
Gambar 3.18	Mengganti nama Interfaces	38

Gambar 3.19 Melakukan pengaturan DHCP Server	39
Gambar 3.20 Pengaturan <i>Interface</i> APBridge	39
Gambar 3.21 Pengaturan Ports Bridge	40
Gambar 3.22 Aktifkan Wlan1	40
Gambar 3.23 Pengaturan SSID	41
Gambar 4.1 Tampilan <i>Winbox</i>	42
Gambar 4.2 <i>Login Mikrotik Via Winbox</i>	43
Gambar 4.3 <i>Tap Firewall</i>	44
Gambar 4.4 Menambahkan Filter Rules baru	44
Gambar 4.5 Penambahan Comment	45
Gambar 4.6 Pemilihan Chain.....	46
Gambar 4.7 Pemilihan <i>Protocol</i>	47
Gambar 4.8 Penginputan <i>Destination Port</i>	47
Gambar 4.9 Penginputan <i>Action</i>	48
Gambar 4.10 <i>Command</i> penambahan blok malware	48
Gambar 4.11 Hasil Pengaturan Firewall Di Mikrotik	49