

LAPORAN AKHIR
KEAMANAN JARINGAN KOMPUTER MENGGUNAKAN FIREWALL
MIKROTIK DARI SERANGAN MEDIA MAC-CLONE DI JURUSAN
TEKNIK KOMPUTER



Laporan Akhir ini disusun sebagai salah satu syarat
Menyelesaikan Pendidikan Diploma III
Pada Jurusan Teknik Komputer Program Studi Teknik Komputer

Disusun Oleh :

ENDANG RAHMI PUSPASARI

061730701191

POLITEKNIK NEGERI SRIWIJAYA
PALEMBANG
2020

LEMBAR PERSETUJUAN LAPORAN AKHIR
KEAMANAN JARINGAN KOMPUTER MENGGUNAKAN FIREWALL
MIKROTIK DARI SERANGAN MEDIA MAC-CLONE DI JURUSAN
TEKNIK KOMPUTER



Oleh :
ENDANG RAHMI PUSPASARI
061730701191

Palembang, September 2020

Pembimbing I

Pembimbing II

Ir. A. Bahri Joni Malvan, M. Kom.
NIP. 196007101991031001

Adi Sutrisman, S.Kom., M.Kom.
NIP.197503052001121005

Mengetahui,
Ketua Jurusan Teknik Komputer

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

Keamanan Jaringan Komputer Menggunakan Firewall Mikrotik Dari Serangan Media MAC-Clone Di Jurusan Teknik Komputer



Telah diuji dan dipertahankan di depan Dewan Penguji pada sidang Laporan Akhir pada Senin, 24 Agustus 2020

Ketua Dewan Penguji

Izzahy Azro, S.Kom., M.Kom.
NIP. 197310012002122007

Anggota Dewan Penguji


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

Ema Laila, S.Kom., M.Kom.
NIP. 197703292001122002

Adi Sutrisman, S.Kom., M.Kom.
NIP. 197503052001121005

Mustaziri, S.T., M.Kom.
NIP. 196909282005011002

Tanda Tangan











Mengetahui,

Ketua Jurusan Teknik Komputer



Alwardi, S.T., M.T.

NIP. 197005232005011004



KEMENTERIAN RISET, TEKNOLOGI, DAN PENDIDIKAN TINGGI
POLITEKNIK NEGERI SRIWIJAYA
Jalan Sriwijaya Negara, Palembang 30139
Telp. 0711-353414 Fax. 0711-355918
Website : www.polisriwijaya.ac.id E-mail : info@polisri.ac.id



SURAT PERNYATAAN BEBAS PLAGIARISME

Yang bertanda tangan di bawah ini :

Nama : Endang Rahmi Puspasari
NIM : 0617 3070 1191
Jurusan/Program Studi : Teknik Komputer
Judul Laporan Akhir : Keamanan Jaringan Komputer Menggunakan Firewall Mikrotik Dari Serangan Media MAC-Clone Di Jurusan Teknik Komputer

Dengan ini menyatakan :

1. Laporan akhir yang saya buat dengan judul sebagaimana tersebut di atas beserta isinya merupakan hasil penelitian saya sendiri.
2. Laporan akhir tersebut bukan plagiat atau menyalin laporan akhir milik orang lain.
3. Apabila laporan akhir ini dikemudian hari dinyatakan plagiat atau menyalin laporan akhir milik orang lain, maka saya bersedia menanggung konsekuensinya.

Demikian surat pernyataan ini saya buat dengan sebenarnya untuk diketahui oleh pihak-pihak yang berkepentingan.

Palembang, September 2020

Yang membuat pernyataan,

Endang Rahmi Puspasari

NIM 061730701191

MOTTO

*“Siapa yang menempuh jalan untuk mencari ilmu, maka Allah akan memudahkan baginya jalan menuju surga.”
(HR. Muslim, No. 2699)*

*“Hargai orang lain seperti menghargai dirimu sendiri.”
(Anonim)*

*“Give thanks for Allah blessings.”
(Penulis)*

Kupersembahkan Untuk :

- ♥ *Kedua Orang Tuaku Tersayang, Bapak Ansori dan Ibu Fitri Jami'ah, S.Ag.*
- ♥ *Adikku Shofwan Wiraguna*
- ♥ *Teman-teman yang selalu memotivasi*
- ♥ *Teman Seperjuanganku CE 2017*
- ♥ *Almamaterku*

ABSTRAK

Keamanan Jaringan Komputer Menggunakan Firewall Mikrotik Dari Serangan Media MAC-Clone Di Jurusan Teknik Komputer

Endang Rahmi Puspasari, 2020 (xiv + 43 halaman)

Email: endang.rahmi9@gmail.com

Jurusan Teknik Komputer Politeknik Negeri Sriwijaya

Fasilitas jaringan *internet* sangat dibutuhkan untuk mencari referensi sekaligus menambah wawasan. Jaringan *internet* yang digunakan salah satunya adalah jaringan *wireless* berupa teknologi *hotspot*. Saat ini sudah banyak *hotspot* yang diterapkan di Perguruan Tinggi. Sering terjadi serangan yang mengganggu jaringan *internet* seperti *Wireless Hacking*. Laporan Akhir ini membahas tentang keamanan jaringan komputer menggunakan *firewall* mikrotik dari serangan media *mac-clone* di jurusan teknik komputer. Oleh karena itu, untuk mengatasi masalah tersebut dibangun keamanan jaringan dengan pengaturan *firewall* yaitu *filter rule* dan NAT. Berdasarkan masalah tersebut, pembahasan yang akan diulas yaitu mengenai pembuatan *hotspot* pada mikrotik, melakukan *monitoring* lewat *hotspot* dan melakukan pengujian terhadap jaringan *hotspot* yang dirancang. Berdasarkan hasil pengujian dapat disimpulkan bahwa pada *firewall*, dapat mengatasi serangan *Mac Clone* yang ada pada *hotspot* mikrotik. Dengan terbangunnya keamanan *internet* menggunakan *firewall* yaitu melakukan *setting* pada *filter rules* dan NAT membantu pengguna untuk meminimalisir terjadinya serangan dari luar. *Firewall* mampu melakukan penyaringan akses ke dalam sebuah komputer menggunakan daftar perijinan (*permissions list*) yang dibuatkan berdasarkan *MAC address*. *MAC-Clone* merupakan suatu tindakan pembobolan, duplikasi (*cloning*) pada alamat sebuah *hardware* atau alamat fisik pada komputer agar memiliki *MAC address* yang sama tujuannya agar dapat dengan mudah masuk ke dalam jaringan tanpa melakukan perijinan dari administrator terlebih dahulu. Dengan dilakukannya pemblokiran lewat *firewall* pada *MAC-Address Cloning*, user *illegal* tidak dapat dengan mudah untuk mengambil alih hak akses pemilik user asli.

Kata Kunci : *Firewall, Hotspot, Mac-Clone, Mikrotik.*

ABSTRACT

Computer Network Security Using Mikrotik Firewall From MAC-Clone Media Attack In Computer Engineering Department

Endang Rahmi Puspasari, 2020 (xiv + 43 pages)

Email: endang.rahmi9@gmail.com

Computer Engineering Department State Polytechnic of Sriwijaya

Internet network facilities are needed to find references as well as add insight. One of the internet networks used is a wireless network in the form of hotspot technology. Currently, many hotspots have been implemented in Higher Education. Attacks that disrupt the internet, such as Wireless Hacking, often occur. This final report discusses about Computer Network Security Using Mikrotik Firewall From MAC-Clone Media Attack In Computer Engineering Department. Therefore, to overcome this problem, network security is built with firewall settings, namely filter rules and NAT. Based on these problems, the discussion that will be reviewed is about making hotspots on mikrotik, monitoring via hotspots and testing the designed hotspot networks. Based on the test results, it can be concluded that the firewall can overcome Mac Clone attacks that are on the proxy hotspot. With the development of internet security using a firewall, namely setting the filter rules and NAT helps users to minimize attacks from outside. Firewalls are able to filter access to a computer using a permissions list that is created based on the MAC address. MAC-Clone is an act of breaking, duplicating (cloning) the address of a hardware or physical address on a computer so that it has the same MAC address so that it can easily enter the network without prior permission from the administrator. By blocking through the firewall on MAC-Address Cloning, illegal users cannot easily take over the access rights of the original user owner.

Keywords : Firewall, Hotspot, Mac-Clone, Mikrotik.

KATA PENGANTAR

Dengan memanjatkan puji dan syukur kehadiran Allah subhanahu wa ta'ala, karena atas rahmat dan karunia-Nya penulis dapat menyelesaikan Laporan Akhir ini dengan judul, “**Keamanan Jaringan Komputer Menggunakan Firewall Mikrotik Dari Serangan MAC-Clone Di Jurusan Teknik Komputer**”. Tujuan dari penulisan laporan ini adalah untuk memenuhi persyaratan menyelesaikan Diploma III Politeknik Negeri Sriwijaya. Selanjutnya penulis mengucapkan terima kasih kepada seluruh pihak yang telah membantu dalam penulisan laporan ini, antara lain:

1. Allah SWT dan Nabi Muhammad Saw atas berkah dan karunia-Nya lah penulis bisa menyelesaikan laporan ini.
2. Orangtua dan saudara tercinta, yang telah memberikan doa dan restu serta dukungan yang sangat besar selama ini.
3. Bapak Dr. Ing. Ahmad Taqwa, M.T. selaku Direktur Politeknik Negeri Sriwijaya.
4. Bapak Azwardi, S.T., M.T. 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 Ir. A. Bahri Joni Malyan, M. Kom. selaku Dosen Pembimbing I Jurusan Teknik Politeknik Negeri Sriwijaya yang telah berkenan meluangkan waktunya untuk membimbing serta memberikan masukan kepada penulis sehingga laporan akhir ini dapat diselesaikan sesuai dengan kriteria yang diharapkan.
7. Bapak Adi Sutrisman, S.Kom.,M.Kom. selaku Dosen Pembimbing II Jurusan Teknik Politeknik Negeri Sriwijaya yang telah berkenan meluangkan waktunya untuk membimbing serta memberikan masukan kepada penulis sehingga laporan akhir ini dapat diselesaikan sesuai dengan kriteria yang diharapkan.

8. Seluruh Bapak/Ibu Dosen Jurusan Teknik Komputer Politeknik Negeri Sriwijaya.
9. Staff administrasi Jurusan Teknik Komputer yang telah membantu segala kepentingan perihal administrasi dan akademik selama proses penyusunan laporan akhir ini hingga selesai.
10. Segenap teman-teman dan para sahabatku Anggi, Yuyun, Nisrina, Shafa dan Azzam yang telah memberikan motivasi dan dukungan dalam penyusunan laporan kerja akhir ini.
11. Teman-teman kelas 6 CE yang tidak bisa disebutkan satu-persatu atas bantuannya.

Semoga laporan ini dapat bermanfaat khususnya bagi penulis umumnya bagi para pembaca. Mengingat pengetahuan dan pengalaman penulis yang masih sedikit. Oleh karena itu penulis memohon kritik dan saran yang membangun demi perbaikan di masa depan. Terima kasih.

Palembang, September 2020

Penulis

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN	ii
HALAMAN PENGUJIAN	iii
SURAT PERNYATAAN BEBAS PLAGIARISME	iv
MOTTO	v
ABSTRAK	vi
ABSTRACT	vii
KATA PENGANTAR	viii
DAFTAR ISI	x
DAFTAR GAMBAR	xii
DAFTAR TABEL	xiv
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	2
1.4 Tujuan	3
1.5 Manfaat	3
BAB II TINJAUAN PUSTAKA	4
2.1 Penelitian Terdahulu	4
2.2 Jaringan Komputer	6
2.3 <i>MAC-Clone (MAC Address Clone)</i>	7
2.4 <i>Hotspot</i>	8
2.5 <i>Firewall</i>	9
2.5.1 Fungsi <i>Firewall</i>	9
2.6 Mikrotik	10
2.7 <i>Router</i>	10
2.8 <i>Access Point</i>	12

BAB III RANCANG BANGUN	14
3.1 Perancangan Sistem.....	14
3.2 Analisis Masalah.....	15
3.2.1 Analisis Permasalahan.....	15
3.3 Solusi Masalah	17
3.4 Rancang Bangun Jaringan.....	17
3.5 Perancangan <i>Hotspot</i> pada Mikrotik Router RB941-2ND	18
3.6 Perancangan Sistem Keamanan Menggunakan <i>Firewall</i>	20
3.7 Detail Alur Penyelesaian Masalah.....	22
 BAB IV HASIL DAN PEMBAHASAN.....	23
4.1 Konfigurasi Penanganan <i>Mac Clone</i> dengan Menggunakan <i>Firewall</i>	23
4.1.1 <i>Cloning MAC Address PC Client1</i>	23
4.1.2 Konfigurasi <i>Interface</i> Jaringan	24
4.1.3 Konfigurasi <i>IP Address</i>	25
4.1.4 Mengkoneksikan Mikrotik Ke <i>Internet</i>	26
4.1.5 Konfigurasi <i>Hotspot</i>	29
4.1.6 Konfigurasi <i>Firewall</i>	37
4.2 Monitoring <i>User Hotspot</i> Melalui Panel <i>Hotspot Winbox</i>	39
4.3 Hasil Pengujian.....	39
 BAB V KESIMPULAN DAN SARAN.....	42
5.1 Kesimpulan	42
5.2 Saran	42

DAFTAR PUSTAKA

LAMPIRAN

DAFTAR GAMBAR

Gambar 2. 1 Mikrotik <i>Router</i> RB941-2ND.....	12
Gambar 2. 2 Mikrotik <i>Access Point</i> RB951UI-2ND	12
Gambar 3. 1 Diagram Blok.....	14
Gambar 3. 2 Proses <i>Login PC Client1</i>	15
Gambar 3. 3 Proses <i>Login PC Client1 Clone</i>	16
Gambar 3. 4 Rancangan Jaringan	17
Gambar 3. 5 Konfigurasi <i>IP Address</i>	18
Gambar 3. 6 Perancangan <i>Hotspot</i> pada Mikrotik <i>Router</i> RB941-2ND	19
Gambar 3. 7 Block <i>MAC Address</i>	20
Gambar 3. 8 Hasil <i>Login</i> Setelah dilakukan <i>setting</i> pada <i>firewall</i>	21
Gambar 3. 9 Detail Alur Penyelesaian Masalah	22
Gambar 4. 1 Aplikasi <i>Change MAC Address</i>	23
Gambar 4. 2 <i>Login Winbox</i>	24
Gambar 4. 3 <i>Interface List</i>	25
Gambar 4. 4 Konfigurasi <i>IP Address</i>	25
Gambar 4. 5 <i>Wireless Tables</i>	26
Gambar 4. 6 <i>Interface wlan1</i>	27
Gambar 4. 7 Konfigurasi <i>DHCP Client</i>	27
Gambar 4. 8 <i>Status Interface DHCP Client</i>	28
Gambar 4. 9 Konfigurasi <i>NAT rule</i>	28
Gambar 4. 10 Konfigurasi <i>Action NAT Rule</i>	29
Gambar 4. 11 <i>Test Koneksi Internet</i>	29
Gambar 4. 12 <i>Hotspot Interface</i>	30
Gambar 4. 13 <i>Local Address of Network</i>	30
Gambar 4. 14 <i>Address Pool of Network</i>	30
Gambar 4. 15 <i>Select Certificate</i>	31
Gambar 4. 16 <i>IP Address of SMTP</i>	31
Gambar 4. 17 <i>DNS Server</i>	31
Gambar 4. 18 <i>DNS Name</i>	32

Gambar 4. 19 Hasil Konfigurasi <i>Hotspot</i>	32
Gambar 4. 20 <i>User Admin</i>	33
Gambar 4. 21 <i>User Endang</i>	33
Gambar 4. 22 <i>User Profile Admin</i>	34
Gambar 4. 23 <i>User Profile Endang</i>	34
Gambar 4. 24 Nonaktif <i>Cookies</i>	35
Gambar 4. 25 Tes Hasil Konfigurasi <i>Hotspot</i>	35
Gambar 4. 26 <i>PC Client1 Berhasil Login</i>	36
Gambar 4. 27 <i>PC Client1 Clone Login</i>	36
Gambar 4. 28 <i>NAT Chain</i>	37
Gambar 4. 29 <i>NAT Action Masquerade</i>	37
Gambar 4. 30 <i>Chain Firewall Rule</i>	37
Gambar 4. 31 <i>Src.MAC Address</i>	38
Gambar 4. 32 <i>Firewall Rule Action</i>	38
Gambar 4. 33 <i>Monitoring User Hotspot Melalui Panel Hotspot Winbox</i>	39
Gambar 4. 34 <i>Login PC Client1</i>	40
Gambar 4. 35 <i>PC Client1 Clone Gagal Login</i>	40
Gambar 4. 36 Keamanan pada <i>NAT</i>	42
Gambar 4. 37 Keamanan pada <i>Filter Rule</i>	42

DAFTAR TABEL

Gambar 4. 1 Hasil Pengujian	41
--	-----------

