IMPLEMENTASI KEAMANAN JARINGAN TERHADAP SERANGAN *SYN FLOOD* DENGAN MENGGUNAKAN *FIREWALL RAW* BERBASIS *ROUTERBOARD* MIKROTIK

SKRIPSI

Teuku Reynaldi

1811500096

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INFORMASI

INSTITUT SAINS DAN BISNIS

ATMA LUHUR

PANGKALPINANG

2022

IMPLEMENTASI KEAMANAN JARINGAN TERHADAP SERANGAN *SYN FLOOD* DENGAN MENGGUNAKAN *FIREWALL RAW* BERBASIS *ROUTERBOARD* MIKROTIK

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :
Teuku Reynaldi
1811500096

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI
INSTITUT SAINS DAN BISNIS
ATMA LUHUR
PANGKALPINANG

2022

LEMBAR PERNYATAAN

Yang bertanda tangan di bawah ini :

NIM : 1811500096

Nama : Teuku Reyanldi

Judul Skripsi : IMPLEMENTASI KEAMANAN JARINGAN TERHADAP SERANGAN *SYN FLOOD* DENGAN MENGGUNAKAN *FIREWALL RAW* BERBASIS *ROUTERBOARD* MIKROTIK

Menyatakan bahwa Laporan Skripsi saya adalah hasil karya sendiri dan bukan plagiat. Apabila ternyata ditemukan didalam laporan Skripsi saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Pangkalpinang, 12 Juli 2022

Teuku Reynaldi

LEMBAR PENGESAHAN SKRIPSI

IMPLEMENTASI KEAMANAN JARINGAN TERHADAP SERANGAN *SYN FLOOD* DENGAN MENGGUNAKAN *FIREWALL RAW* BERBASIS *ROUTERBOARD* MIKROTIK

Yang dipersiapkan dan disusun oleh

Teuku Reynaldi

1811500096

Telah dipertahankan di depan Dewan Penguji

Pada tanggal 12 Juli 2022

Susunan Dewan Penguji

Anggota	Dosen Pembimbing
Benny Wijaya, S.T, M.Kom	Dian Novianto, M.Kom
NIDN. 0202097902	NIDN. 0209119001
Kaprodi Teknik informatika	Ketua Penguji
Chandra Kirana. M.Kom	Yohanes Setiawan Japriadi, M.Kom
NIDN. 0228108501	NIDN. 0219068501

Skripsi ini telah diterima dan sebagai salah satu persyaratan

untuk memperoleh gelar Sarjana Komputer

Tanggal 19 Juli 2022

DEKAN FAKULTAS TEKNOLOGI INFORMASI

ISB ATMA LUHUR

Ellya Helmud, M.Kom

NIDN. 0201027901

KATA PENGANTAR

Puji syukur Alhamdulillah kehadirat Allah SWT yang telah melimpahkan segala rahmat dan karuniaNya, sehingga penulis dapat menyelesaikan laporan skripsi yang merupakan salah satu persyaratan untuk menyelesaikan jenjang strata satu (S1) pada Program Studi Teknik Informatika Institut Sains dan Bisnis (ISB) Atma Luhur. Penulis menyadari bahwa laporan skripsi ini masih jauh dari sempurna. Karena itu, kritik dan saran akan senantiasa penulis terima dengan senang hati.

Dengan segala keterbatasan, penulis menyadari pula bahwa laporan skripsi ini takan terwujud tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada:

1. Allah Subhanahu Wata'ala yang telah menciptakan dan memberikan kehidupan di dunia.
2. Ayah dan mamak tercinta yang telah mendukung penulis baik spirit maupun materi.
3. Bapak Drs. Djaetun Hs yang telah mendirikan Atma Luhur .
4. Bapak Dr. Husni Teja Sukmana, S.T., M.Sc, selaku Rektor ISB Atma Luhur.
5. Bapak Chandra Kirana, M. Kom Selaku Kaprodi Teknik Informatika.
6. Bapak Dian Novianto, M. Kom selaku dosen pembimbing.
7. Isteri dan anakku tercinta yang selalu memberikan spirit maupun materi untuk terus meyelesaikan laporan skripsi ini.
8. Saudara dan sahabat-sahabatku terutama kawan-kawan angkatan 2018 yang telah memberikan dukungan moral untuk terus meyelesaikan skripsi ini.

Semoga Tuhan Yang Maha Esa membalas kebaikan dan selalu mencurahkan hidayah serta taufikNya, Aamiin.

Pangkalpinang, 12 Juli 2022

Penulis

ABSTRACT

The development of technology in the field of information has grown so rapidly. It can be seen from the widespread use of the internet in all fields, both personal and office. An open network system allows for abuse or cyber attack. Therefore, this study aims to provide an understanding and application when an attack occurs against a routerboard especially against DoS/DDoS attacks, namely SYN-Flood. attack by increasing network security using features on the proxy routerboard , namely firewall raw. In this study, the author uses the PPDIOO (Prepare Plan Design Implement Operate Optimize) method as a research methodology that is considered appropriate to the topic of discussion taken. From the test results of the launched SYN-Flood , it can be concluded that the firewall able to drop attacks that are considered SYN directly after configuring the firewall RAW rule by applying prerouting to the chain and using action drop settings RAW so that attacks known as SYN Floods can be dropped and configure protocol into rules with flags SYN is then switched with action jump to SYN-Protect by commenting Syn Flood Protect. This happens to stop incoming SYN packets before connection tracking.

Keywords: Technology, Security, firewall, Router Mikrotik, SYN-Flood

ABSTRAK

Perkembangan teknologi di bidang informasi sudah berkembang sedemikian pesat. dapat terlihat dari maraknya pemakaian internet di segala bidang baik pribadi ataupun perkantoran. Sistem jaringan yang terbuka memungkinkan terjadinya penyalahgunaan atau kejahatan *cyber*. Oleh karena itu penelitian ini bertujuan untuk memberikan pemahaman serta penerapan saat terjadi serangan terhadap perangkat *routerboard* mikrotik terutama terhadap serangan DoS/DdoS yaitu *SYN-Flood attack* dengan melakukan penigkatan keamanan jaringan menggunakan fitur pada *routerboard* mikrotik yaitu *firewall raw*. Dalam penelitian ini penulis menggunakan metode PPDIOO (*Prepare Plan Design Implement Operate Optimize*) sebagai metodologi penelitian yang dianggap sesuai dengan topik pembahasan yang diambil. Dari hasil pengujian terhadap serangan *SYN-Flood* yang diluncurkan dapat ditarik hasil bahwa *firewall* mampu men-*drop* serangan yang dianggap sebagai serangan *SYN* secara langsung setelah dilakukan konfigurasi terhadap *firewall RAW rule* dengan menerapkan *prerouting* pada *chain* dan menggunkan *action drop* pada pengaturan *RAW* agar serangan yang dikenal sebagai *SYN Flood* dapat di-*drop* dan mengkonfigurasi pengaturan *protocol* TCP ke dalam *rule* dengan *flag SYN* lalu di alihkan dengan *action jump* ke *SYN-Protect* dengan komen *Syn Flood Protect*. Hal tersebut terjadi untuk menghentikan paket SYN yang masuk sebelum terjadinya *connection tracking*.

Kata Kunci : Teknologi, Keamanan, firewall, *Router* Mikrotik , *SYN-Flood*

DAFTAR ISI

Halaman

LEMBAR PERNYATAAN i
LEMBAR PENGESAHAN SKRIPSI iii
KATA PENGANTAR iv
ABSTRACT v
ABSTRAK vi
DAFTAR ISI vii
DAFTAR GAMBAR x
DAFTAR TABEL xii
DAFTAR SIMBOL xiii
BAB I 1
PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 3
1.3 Batasan Masalah 3
1.4 Tujuan dan Manfaat Penelitian 3
1.4.1 Tujuan 3
1.4.2 Manfaat 4
1.5 Sistematika Penulisan 4
BAB II 6
LANDASAN TEORI 6
2.1 Model Pengembangan Jaringan Komputer 6
2.1.1 Metode PPDIOO 6
2.2. Tools Pengembangan Jaringan 7
2.2.1 *Unified Modelling Language* (UML) 7
2.2.1.1 *Activity* Diagram 7
2.2.1.2 *Deployment* Diagram 8
2.3. Teori Pendukung 9
2.3.1 Jaringan Komputer 9

2.3.2 Topologi Jaringan 9
2.3.3 Keamanan Jaringan Komputer 10
2.3.4 Tujuan Keamanan Jaringan Komputer 10
2.3.5 Klasifikasi Jenis Serangan Jaringan Komputer 11
2.3.6 *SYN Flood Attack* 11
2.3.7 *Firewall* 14
2.3.8 *Firewall Raw* 14
2.3.9 *Router* 15
2.3.10 OSI 15
2.3.11 NAT 16
2.3.12 TCP/IP 17
2.3.13 Kali Linux 18
2.4 Penelitian Terdahulu 18
BAB III 22
METODOLOGI PENELITIAN 22
3.1 Model pengembangan jaringan 22
3.2 Metode pengumpulan data 24
3.3 Tool Pengembangan Sistem 24
BAB IV 25
PEMBAHASAN 25
4.1. Analisa Masalah 25
4.2.2 Pemecahan Masalah 25
4.2.3 Analisa Kebutuhan Sistem 26
4.3 Rancangan Sistem 26
4.3.1 *Activity* Diagram Sebelum Konfigurasi 26
4.3.2 *Activity* Diagram Sesudah Konfigurasi 27
4.3.3 *Deployment* Diagram 28
4.3.4 Rancangan Aplikasi 29
4.3.5 Manajemen Jaringan Usulan 30
4.3.5 Topologi Jaringan Pengujian 30
4.4 Implementasi 31
4.4.1 Konfigurasi *Routerboard* Mikrotik 31

4.4.2 Konfigurasi *Firewall* 38
4.4.3 Konfigurasi Serangan *SYN Flood* 42
4.5 Pengujian 43
4.5.1 Analisa Jaringan Normal 43
4.5.2 Analisa Serangan *SYN Flood* Pada *Router* 44
4.5.3 Hasil 47
PENUTUP 48
5.1 Kesimpulan 48
5.2 Saran 48
DAFTAR PUSTAKA 49
LAMPIRAN 51

DAFTAR GAMBAR

Halaman

Gambar 2.1 Bentuk TCP Normal.....11
Gambar 2.2 Bentuk Serangan *SYN Flood*.....12
Gambar 2.3 TCP *Header*.....12
Gambar 2.4 Diagram status TCP.....13
Gambar 2.5 Contoh jaringan komputer LAN yang dihubungkan dengan *gateway* dan terkoneksi ke jaringan internet.....17
Gambar 3.1 Metode PPDIOO.....22
Gambar 4.1 *Activity* diagram sebelum dikonfigurasi.....27
Gambar 4.2 *Activity* diagram setelah dikonfigurasi.....28
Gambar 4.3 *Diployment* diagram.....29
Gambar 4.4 Topologi Pengujian.....30
Gambar 4.5 Penempatan jalur kabel pada *router* mikrotik.....31
Gambar 4.6 Tampilan awal Winbox.....32
Gambar 4.7 Pengaturan nama *interface* pada *port*.....32
Gambar 4.8 Pengaturan pengalamatan Ip *Address*.....33
Gambar 4.9 Pengaturan *Route* di Mikrotik.....33
Gambar 4.10 Pengaturan DNS *Server*.....34
Gambar 4.11 Pengaturan DHCP *Server*.....34
Gambar 4.12 Pengaturan *Firewall*.....35
Gambar 4.13 Pengaturan *action* pada *firewall*.....35
Gambar 4.14 Pengujian Jaringan Internet.....36
Gambar 4.15 Pengujian Alamat *gateway*.....36
Gambar 4.16 Pengujian alamat di *Port* 1.....37
Gambar 4.17 Pengujian Alamat di *Port* 2.....37
Gambar 4.18 Pengujian Jaringan internet di jaringan yang masuk ke PC.....37
Gambar 4.19 Tampilan menu pengaturan *Firewall*.....38
Gambar 4.20 Proses pembuatan *raw rule*.....39

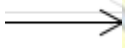
Gambar 4.21 Proses pengaktifan *action* di *raw rule*.....39
Gambar 4.22 Tampilan *firewall raw* setelah dimasukkan perintah.....40
Gambar 4.23 tampilan *firewall filter* setelah dimasukkan perintah.....41
Gambar 4.24 Perintah untuk menginstal hping3.....42
Gambar 4.25 Tampilan nmap pada ip target.....42
Gambar 4.26 Tampilan grafik dan resource *router* saat normal.....43
Gambar 4.27 *Port* yang terbuka pada ip target dan perintah menjalankan *SYN Flood* kepada ip target.....45
Gambar 4.28 Pemantauan *resource router*.....45
Gambar 4.29 Tampilan *router* "sibuk" dan tidak bisa diakses.....46
Gambar 4.30 Tampilan grafik dan *log* yang terpantau saat dilakukan serangan terhadap *router*.....46

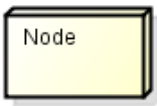
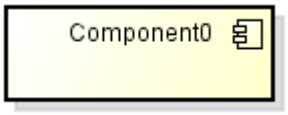
DAFTAR TABEL

Halaman

Tabel 2.1 Simbol *Activity* Diagram.....8
Tabel 2.2 Simbol *Deployment* Diagram.....8
Tabel 2.3 Tabel Pemodelan *Layer* OSI.....15
Tabel 2.4 Penelitian Terdahulu.....18
Tabel 3.1 Hardware yang digunakan.....23
Tabel 3.2 *Software* yang digunakan.....23
Tabel 4.1 Kebutuhan *hardware*.....26
Tabel 4.2 Kebutuhan *software*.....26
Tabel 4.3 *Hardware* yang digunakan.....29
Tabel 4.4 *Software* yang digunakan.....29

DAFTAR SIMBOL

Simbol Activity Diagram		
Simbol	**Nama**	**Keterangan**
	*Start point*	Poin awal dari aktivitas
	*End point*	Poin akhir dari aktivitas
	*Action*	Menggambarkan suatu proses atau kegiatan bisnis
	*Decision*	Mengambarkan pilihan atau keputusan dari sebuah aktivitas
	*State transition*	Menggambarkan aliran perpindahan suatu aktivitas atau *state*

Simbol Deployment Diagram		
Simbol	**Nama**	**Keterangan**
	*Node*	Node menggambarkan bagian-bagian hardware dalam sebuah sistem.
	Association	Association digambarkan sebagai sebuah garis yang menghubungkan dua buah node yang mengisyaratkan jalur kominukasi antara elemen-elemen hardware
	Komponen	Komponen sistem

Simbol Jaringan		
Simbol	**Nama**	**Keterangan**
	*Computer*	Sebagai end device

	Wire-Straight	Simbol untuk menghubungkan perangkan menggunkaan kabel *straight*
	Wire-Cross	Simbol untuk menghubungkan perangkan menggunkaan kabel *cross*
	*Home Gateway*	Sebagai penghubung antara smartphone dengan perangkat atau peralatan yang dikendalikan
	*Router-Wireless*	Simbol yang menggambrkan sebagai peralatan pengatur lalu lintas data alam suatu jaringan kpmputer yang mampu digunakan sebagai alat pemancar/pemberi sinyal wireless
	*Cloud*	Menggambarkan ISP atau penyedia jasa layanan internet
	*Modem Cable*	Simbol yang menggambarkan sebagai alat yang berfungsi untuk mengubah sinyal analog menjadi sinyal digital