

**IMPLEMENTASI *PORT KNOCKING* UNTUK KEAMANAN LAYANAN
JARINGAN PADA *ROUTER* MIKROTIK**

PROJEK

Sebagai salah satu syarat untuk menyelesaikan studi di
Program Studi Teknik Komputer DIII



Oleh

FIKRI SYAPUTRA

NIM 09040581822030

PROGRAM STUDI TEKNIK KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

MARET 2022

HALAMAN PENGESAHAN

**IMPLEMENTASI *PORT KNOCKING* UNTUK KEAMANAN LAYANAN
JARINGAN PADA *ROUTER* MIKROTIK**

PROJEK

Sebagai salah satu syarat untuk menyelesaikan studi di Program Studi
Teknik Komputer DIII

Oleh:

Fikri Syaputra 09040581822030

Palembang, 21 Februari 2022

Pembimbing I,



**Ahmad Heryanto, M.T.
NIP 197801222015041002**

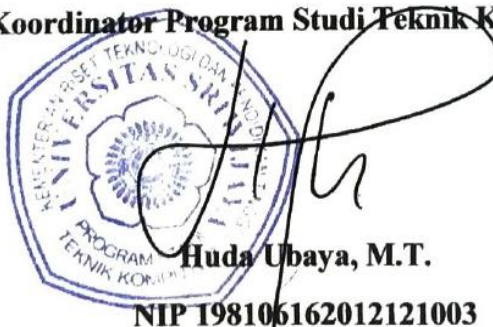
Pembimbing II,



**Adi Hermansyah, M.T.
NIK 1613033004890001**

Mengetahui

Koordinator Program Studi Teknik Komputer,



**Huda Ubaya, M.T.
NIP 198106162012121003**

HALAMAN PERSETUJUAN

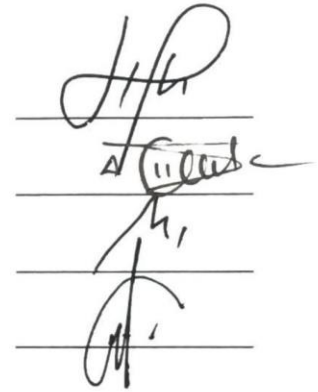
Telah diuji dan lulus pada:

Hari : Jumat

Tanggal : 28 Januari 2022

Tim Penguji:

- | | |
|------------------|------------------------|
| 1. Ketua | : Huda Ubaya, M.T. |
| 2. Pembimbing I | : Ahmad Heryanto, M.T. |
| 3. Pembimbing II | : Adi Hermansyah, M.T. |
| 4. Penguji | : Ahmad Zarkasi, M.T. |



Mengetahui

Koordinator Program Studi Teknik Komputer,



Huda Ubaya, M.T.

NIP 198106162012121003

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : Fikri Syaputra

NIM : 09040581822030

Program Studi : Teknik Komputer

Peminatan : Teknik Komputer Jaringan

Judul : Implementasi *Port Knocking* Untuk Keamanan Layanan Jaringan
Pada Router MikroTik

Hasil Pengecekan *Software iThenticate/Turnitin* : 3 %

Menyatakan bahwa laporan proyek saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya.

Demikian pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.



Palembang, 21 Februari 2022



Fikri Syaputra

NIM 09040581822030

HALAMAN PERSEMBAHAN

وَمَنْ يَتَوَكَّلْ عَلَى اللَّهِ فَهُوَ حَسْبُهُ

*Barangsiapa bertawakkal kepada Allah, niscaya Allah akan mencukupkan
keperluannya. – (QS. At-Thalaq: 3)*

*“Sebaik-baik manusia adalah yang paling bermanfaat bagi manusia”
(HR. Ahmad)*

*Alhamdulillah bersyukur kepada Allah Subhanahu Wata'alaatas nikmat dan
kesempatan, sehingga dapat terselesaikan sedikit karya yang akan
kupersembahkan untuk...*

Kedua Orang Tua

(Alm. Hasan Basri dan Almh. Maskunah)

Teman-teman seperjuangan

(Teknik Komputer Jaringan 2018)

Almamater perjuangan

(Universitas Sriwijaya)

Februari 2022

KATA PENGANTAR

Puji dan Syukur kepada Allah Subhanahu wata'ala yang telah memberikan rahmat dan nikmat islam serta karunia-Nyalah penulis dapat menyelesaikan penulisan projek akhir yang berjudul **“IMPLEMENTASI *PORT KNOCKING* UNTUK KEAMANAN LAYANAN JARINGAN PADA *ROUTER MIKROTIK*”**. Penulisan projek akhir ini dibuat dalam rangka memenuhi persyaratan untuk menyelesaikan pendidikan di Program Studi Teknik Komputer Fakultas Ilmu Komputer Universitas Sriwijaya untuk memperoleh gelar Ahli Madya Komputer.

Pada kesempatan ini, penulis mengucapkan terima kasih kepada seluruh pihak yang telah membantu, membimbing, dan mendukung penulis dalam menyelesaikan laporan projek akhir ini dengan baik. Penulis ucapkan terima kasih kepada:

1. Allah Subhanahu Wata'ala, atas rahmat dan nikmat-Nya yang rencana dan jalan terbaik, mempermudah segala urusan, memberikan kesehatan, ilmu dan rezeki yang tak dapat dihitung jumlahnya.
2. Kedua Orang tua, Kakak-kakak, serta keluarga tercinta, yang senantiasa untuk menasehati, mendidik serta memberikan dukungan moril maupun materil kepada penulis dalam menyelesaikan projek akhir.
3. Bapak Ahmad Heryanto, S.KOM., M.T. selaku Dosen Pembimbing I Projek Akhir, yang telah memberikan bimbingan dan semangat kepada penulis dalam menyelesaikan laporan projek akhir.

4. Bapak Adi Hermansyah, S.KOM., M.T. selaku Dosen Pembimbing II Projek Akhir, yang telah memberikan support dan bimbingan kepada penulis dalam menyelesaikan laporan projek akhir.
5. Bapak Huda Ubaya, S.T., M.T. selaku Koordinator Program Studi Teknik Komputer Fakultas Ilmu Komputer Universitas Sriwijaya serta sebagai Dosen Pembimbing Akademik penulis.
6. Dan juga seluruh Dosen Program Studi Teknik Komputer, Fakultas Ilmu Komputer Universitas Sriwijaya.
7. Staf Dosen Program Studi Teknik Komputer, khususnya Mbak Faula yang selalu membantu dalam proses administrasi.
8. Keluarga Besar Fakultas Ilmu Komputer, bagian akademik, kemahasiswaan, tata usaha, perlengkapan, dan keuangan.
9. Seluruh Pimpinan yang ada di lingkungan Fakultas Ilmu Komputer Universitas Sriwijaya.
10. Seluruh Teman-teman satu angkatan, Teknik Komputer Jaringan 2018, Balada, Rifki, Salsa, Fiero, Angga, Fahrie, Faris, Agung, Dippo, Dirga, Dios, Alfina, Dwi, dan semuanya. Semoga sukses untuk kita semua.
11. Keluarga Besar DPM (Dewan Perwakilan Mahasiswa) Fakultas Ilmu Komputer terima kasih atas kesempatannya, serta ilmu yang bermanfaat.
12. Serta semua pihak yang telah membantu baik moril maupun material yang tidak dapat disebutkan satu persatu dalam menyelesaikan projek akhir ini. Terima kasih semuanya.

Semoga dengan terselesainya proyek akhir ini dapat bermanfaat untuk menambah wawasan dan pengetahuan bagi kita semua dalam mempelajari implementasi *port knocking* untuk keamanan layanan jaringan *router* MikroTik.

Dalam penulisan laporan ini, penulis menyadari bahwa masih banyak terdapat kekurangan dan ketidaksempurnaan, oleh karena itu penulis mohon saran dan kritik yang membangun untuk perbaikan laporan proyek ini, agar menjadi lebih baik dimasa yang akan datang.

Palembang, 21 Februari 2022

Penulis

Fikri Syaputra

NIM.09040581822030

IMPLEMENTASI *PORT KNOCKING* UNTUK KEAMANAN LAYANAN JARINGAN PADA *ROUTER* MIKROTIK

Oleh

Fikri Syaputra

NIM 09040581822030

Abstrak

Fokus pada penelitian ini adalah metode *port knocking*, yang diterapkan pada router MikroTik. Sering terjadinya serangan-serangan yang dilakukan melalui layanan *port* dalam keadaan terbuka secara bebas, hal ini menjadi ancaman bagi keamanan data dalam sistem jaringan komputer. Untuk meminimalisir serangan pada server, salah satu metode keamanan jaringan komputer yaitu metode *port knocking*. Pada penelitian ini implementasi metode *port knocking* untuk mengamankan *port* yang mudah *remote access* pada server router MikroTik seperti *port* 22 (ssh), 23 (telnet), 80 (www), dan 8291 (winbox). Berdasarkan hasil pengujian yang telah dilakukan untuk terhubung pada server MikroTik *user/client* harus melakukan autentikasi *knocking* 1-2-3 pada *port* pemicu, pada setiap autentikasi *knocking* memiliki waktu timeout 10 detik, dan waktu akses pada server MikroTik yaitu dengan timeout 30 menit.

Kata kunci: *Port Knocking*, Keamanan Jaringan, *Firewall*, *Port*, MikroTik.

**IMPLEMENTASI *PORT KNOCKING* UNTUK KEAMANAN LAYANAN
JARINGAN PADA *ROUTER MIKROTIK***

Oleh

Fikri Syaputra

NIM 09040581822030

Abstrak

The focus of this research is the port knocking method, which is applied to MikroTik routers. Frequent attacks are carried out through the service port in a freely open state, this is a threat to data security in computer network systems. To minimize attacks on servers, one of the computer network security methods is the port knocking method. In this study the implementation of the port knocking method to secure ports that are easy to remote access on MikroTik router servers such as ports 22 (ssh), 23 (telnet), 80 (www), and 8291 (winbox). Based on the results of the tests that have been carried out to connect to the MikroTik server, the user/client must authenticate knocking 1-2-3 on the trigger port, each knocking authentication has a timeout of 10 seconds, and the access time on the MikroTik server is 30 minutes.

Keywords: Port Knocking, Network Security, Firewall, Port, MikroTik.

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN	ii
HALAMAN PERSETUJUAN	iii
HALAMAN PERNYATAAN	iv
HALAMAN PERSEMBAHAN	v
KATA PENGANTAR	vi
ABSTRAK	ix
DAFTAR ISI	xi
DAFTAR SIMBOL	xiv
DAFTAR TABEL	xvi
DAFTAR GAMBAR	xvii
DAFTAR LAMPIRAN	xx
BAB I PENDAHULUAN	xx
1.1 Latar Belakang	1
1.2 Tujuan.....	3
1.3 Manfaat.....	3
1.4 Rumusan Masalah	3
1.5 Batasan Masalah.....	4
1.6 Metodologi Penelitian	4
1.7 Sistematika Penelitian	5
BAB II LANDASAN TEORI	7
2.1 Keamanan Komputer.....	7
2.1.1 Fungsi Keamanan Komputer	7
2.2 Model Referensi OSI.....	7
2.2.1 Karakteristik Lapisan OSI	8
2.2.2 OSI Layer.....	9
2.3 TCP/IP (Transmisi Control Protocol) / (Internet Protocol).....	12
2.4 Firewall.....	12
2.4.1 Fungsi Firewall	13
2.5 Port knocking	13
2.5.1 Karakteristik Port Knocking	14
2.5.2 Cara Kerja Port Knocking.....	15

2.6 Router	16
2.7 Mikrotik.....	16
2.7.1 Sejarah Mikrotik	16
2.7.2 Macam-macam Mikrotik	17
2.7.3 Mikrotik RB941-2nD.....	18
2.8 Access Point	19
2.8.1 Access Point TL-WR1043ND	19
2.9 Winbox	20
2.10 Putty.....	21
BAB III METODOLOGI PENELITIAN	22
3.1 Kerangka Kerja Penelitian.....	22
3.2 Perancangan Sistem.....	23
3.2.1 Perancangan Topologi	23
3.2.2 Pengalamatan IP Topologi Penelitian.....	24
3.2.3 Komponen Perangkat Keras	25
3.2.4 Komponen Perangkat Lunak	26
3.2.5 Setting MikroTik ISP (<i>Internet Service Provider</i>)	26
3.2.6 Data Implementasi <i>Port Knocking</i>	33
3.2.7 Konfigurasi Port Knocking SSH (22).....	34
3.2.8 Konfigurasi Port Knocking Telnet (23).....	39
3.2.9 Konfigurasi Port Knocking WWW (80).....	44
3.2.10 Konfigurasi Port Knocking Winbox (8291)	49
3.2.11 Setting DHCP <i>server</i> MikroTik.....	54
3.2.12 Setting Access Point	55
3.3 Skenario Pengujian Implementasi <i>Port Knocking</i> MikroTik.....	58
3.3.1 Skenario Pengujian <i>Scanning Port</i> MikroTik.....	60
3.3.2 Skenario Pengujian <i>filter rules</i> dan Akses <i>Port</i> Tanpa <i>Knocking</i>	60
3.3.3 Skenario Pengujian Akses <i>Port</i> Menggunakan <i>Knocking</i>	61
3.3.4 Skenario Pengambilan Data.....	62
3.4 Hasil dan Pembahasan.....	63
BAB IV HASIL DAN PEMBAHASAN	64
4.1 Pendahuluan	64
4.2 Tahapan pengujian <i>Scanning Port</i> MikroTik.....	64
4.2.1 <i>Scanning</i> Konfigurasi <i>Disable</i>	64

4.2.2 Scanning Konfigurasi <i>Enable</i>	66
4.3 Tahapan pengujian Akses tanpa melakukan <i>knocking</i>	67
4.3.1 Pengujian Akses port MikroTik (<i>Disable</i>).....	68
4.3.2 Pengujian Akses <i>port</i> MikroTik (<i>Enable</i>) Tanpa <i>Knocking</i>	71
4.4 Tahapan Pengujian Akses Menggunakan <i>Knocking</i>	75
4.4.1 Mengakses <i>Port</i> 22 MikroTik Menggunakan <i>Knocking</i>	75
4.4.2 Mengakses <i>Port</i> 23 MikroTik Menggunakan <i>Knocking</i>	77
4.4.3 Mengakses <i>Port</i> 80 MikroTik Menggunakan <i>Knocking</i>	79
4.4.4 Mengakses <i>Port</i> 8291 MikroTik Menggunakan <i>Knocking</i>	80
4.5 Hasil Perbandingan Implementasi <i>Port Knocking</i>	82
BAB V KESIMPULAN DAN SARAN	84
5.1 Kesimpulan.....	84
5.2 Saran	84
DAFTAR PUSTAKA	86

DAFTAR SIMBOL

SSH	=	<i>Secure Shell</i>
Telnet	=	<i>Telecommunication Network</i>
TCP	=	<i>Transmission Control Protocol</i>
UDP	=	<i>User Data Protocol</i>
ICMP	=	<i>Internet Control Message Protocol</i>
OSI	=	<i>Open System Interconnection</i>
BIT	=	<i>Binary Digit</i>
HTTP	=	<i>Hypertext Transfer Protocol</i>
SMTP	=	<i>Simple Mail Transfer Protocol</i>
FTP	=	<i>File Transfer Protocol</i>
IP	=	<i>Internet Protocol</i>
LAN	=	<i>Local Area Network</i>
ISP	=	<i>Internet Service Provider</i>
WLAN	=	<i>Wireless Local Area Network</i>
DHCP	=	<i>Dynamic Host Configuration Protocol</i>
DNS	=	<i>Domain Name Server</i>
CPU	=	<i>Central Processing Unit</i>
RAM	=	<i>Random Access Memory</i>
WIFI	=	<i>Wireless Fidelity</i>
AP	=	<i>Access Point</i>
MAC	=	<i>Media Access Control</i>
GUI	=	<i>Graphical User Interface</i>
NMAP	=	<i>Network Mapper</i>
WPA-PSK	=	<i>Wi-Fi Protected Access – Pre-Shared Key</i>
WPA2-PSK	=	<i>Wi-Fi Protected Access 2 – Pre-Shared Key</i>
SSID	=	<i>Service Set Identifier</i>
GHZ	=	<i>Gigahertz</i>
NTP	=	<i>Network Time Protocol</i>
NAT	=	<i>Network Address Translation</i>

WWW = *World Wide Web*

WPS = *Wi-Fi Protected Setup*

DAFTAR TABEL

Tabel 3.1 <i>IP Address</i> Topologi.....	24
Tabel 3 2 Komponen perangkat keras	25
Tabel 3 3 Komponen perangkat lunak	26
Tabel 3 4 Data Implementasi <i>Port Knocking</i>	33
Tabel 4. 1 Hasil Perbandingan Implementasi Port Knocking	82

DAFTAR GAMBAR

Gambar 2. 1 Karakteristik Lapisan OSI	8
Gambar 2. 2 Lapisan OSI layer	9
Gambar 2. 3 TCP/IP (Transmission Control protocol/Internet Protocol)	12
Gambar 2. 4 Konsep Cara Kerja Port Knocking	15
Gambar 2. 5 Mikrotik RB941-2ND-TC	18
Gambar 2. 6 Access Point TL-WR1043ND	19
Gambar 2. 7 Aplikasi Winbox	20
Gambar 2. 8 Aplikasi Putty	21
Gambar 3. 1 Flowchart Kerangka Kerja Penelitian.....	22
Gambar 3. 2 Desain Topologi Penelitian	23
Gambar 3. 3 konfigurasi wlan ISP	27
Gambar 3. 4 Setting Security Profile.....	28
Gambar 3. 5 Setting DHCP client	28
Gambar 3. 6 Setting DNS Router	29
Gambar 3. 7 Pengujian Koneksi Internet.....	30
Gambar 3. 8 Setting IP Router MikroTik.....	30
Gambar 3. 9 Setting firewall NAT	31
Gambar 3. 10 Setting firewall NAT	31
Gambar 3. 11 Setting IP laptop	32
Gambar 3. 12 Pengujian Melalui Command Prompt	33
Gambar 3. 13 Konfigurasi rule pertama 1212	35
Gambar 3. 14 Action rule pertama 1212	35
Gambar 3. 15 Konfigurasi rule kedua 2323	36
Gambar 3. 16 Advanced rule kedua 2323	36
Gambar 3. 17 Action rule kedua 2323.....	36
Gambar 3. 18 konfigurasi rule ketiga 3434	37
Gambar 3. 19 Advanced rule ketiga 3434	37
Gambar 3. 20 Action rule ketiga 3434	37
Gambar 3. 21 Konfigurasi Port 22 (SSH).....	38
Gambar 3. 22 Advanced port 22 (SSH).....	38
Gambar 3. 23 Action port 22 (SSH)	38
Gambar 3. 24 Konfigurasi Drop port 22 (SSH).....	39
Gambar 3. 25 Advanced Drop port 22 (SSH)	39
Gambar 3. 26 Action Drop port 22 (SSH).....	39
Gambar 3. 27 Konfigurasi rule pertama 9999	40
Gambar 3. 28 Action rule pertama 9999	40
Gambar 3. 29 Konfigurasi rule kedua 8888	41
Gambar 3. 30 Advanced rule kedua 8888	41
Gambar 3. 31 Action rule kedua 8888.....	41
Gambar 3. 32 Konfigurasi rule ketiga 7777	42
Gambar 3. 33 Advanced rule ketiga 7777	42
Gambar 3. 34 Action rule ketiga 7777	42

Gambar 3. 35 Konfigurasi Port 23 (telnet)	43
Gambar 3. 36 Advanced Port 23 (telnet)	43
Gambar 3. 37 Action Port 23 (telnet)	43
Gambar 3. 38 Konfigurasi Drop port 23 (telnet)	44
Gambar 3. 39 Advanced Drop port 23 (telnet)	44
Gambar 3. 40 Action Drop port 23 (telnet)	44
Gambar 3. 41 Konfigurasi rule pertama 1020	45
Gambar 3. 42 Action rule pertama 1020	45
Gambar 3. 43 Konfigurasi rule kedua 2030	46
Gambar 3. 44 Advanced rule kedua 2030	46
Gambar 3. 45 Action rule kedua 2030.....	46
Gambar 3. 46 Konfigurasi rule ketiga 3040	47
Gambar 3. 47 Advanced rule ketiga 3040	47
Gambar 3. 48 Action rule ketiga 3040	47
Gambar 3. 49 Konfigurasi Port 80 (www)	48
Gambar 3. 50 Advanced Port 80 (www)	48
Gambar 3. 51 Action Port 80 (www)	48
Gambar 3. 52 Konfigurasi Drop port 80 (www)	49
Gambar 3. 53 Advanced Drop port 80 (www)	49
Gambar 3. 54 Action Drop port 80 (www)	49
Gambar 3. 55 Konfigurasi rule pertama 1234	50
Gambar 3. 56 Action rule pertama 1234	50
Gambar 3. 57 Konfigurasi rule kedua 2345	51
Gambar 3. 58 Advanced rule kedua 2345	51
Gambar 3. 59 Action rule kedua 2345.....	51
Gambar 3. 60 Konfigurasi rule ketiga 3456	52
Gambar 3. 61 Advanced rule ketiga 3456	52
Gambar 3. 62 Action rule ketiga 3456	52
Gambar 3. 63 Konfigurasi Port 8291 (winbox).....	53
Gambar 3. 64 Advanced Port 8291 (winbox).....	53
Gambar 3. 65 Action Port 8291 (winbox)	53
Gambar 3. 66 Konfigurasi Drop port 8291 (winbox).....	54
Gambar 3. 67 Advanced Drop port 8291 (winbox).....	54
Gambar 3. 68 Action Drop port 8291 (winbox)	54
Gambar 3. 69 Konfigurasi DHCP Server MikroTik.....	55
Gambar 3. 70 Wireless Settings AP	56
Gambar 3. 71 Disable WPS Access point	56
Gambar 3. 72 Disable Wireless Security.....	57
Gambar 3. 73 Setting IP address Access Point.....	58
Gambar 3. 74 Proses Pengujian Metode Port Knocking pada Router MikroTik	59
Gambar 3. 75 Flowchart Skenario Pengujian Pertama.....	60
Gambar 3. 76 Flowchart Skenario Pengujian Kedua	61
Gambar 3. 77 Flowchart Skenario Pengujian Ketiga.	62
Gambar 4. 1 Ipconfig Client	65
Gambar 4. 2 Konfigurasi Filter Rules Disable	65

Gambar 4. 3 Scanning Port MikroTik Disable	66
Gambar 4. 4 Konfigurasi Filter Rules Enable	66
Gambar 4. 5 Scanning Port MikroTik Enable.	67
Gambar 4. 6 Konfigurasi Filter Rules Disable	68
Gambar 4. 7 Akses Port 22 Mode Disable	69
Gambar 4. 8 Akses Port 23 Mode Disable	69
Gambar 4. 9 Akses Port 80 Mode Disable	70
Gambar 4. 10 Akses Port 8291 Mode Disable	71
Gambar 4. 11 Konfigurasi Firewall Rules Enable.....	71
Gambar 4. 12 Proses Akses port 22 Putty	72
Gambar 4. 13 User/client gagal mengakses port 22 putty	73
Gambar 4. 14 User/client gagal mengakses port 23 CMD	73
Gambar 4. 15 User/client gagal mengakses port 80 browser	74
Gambar 4. 16 User/client gagal mengakses port 8291 winbox	75
Gambar 4. 17 Proses Rule Knocking	76
Gambar 4. 18 Akses Port 22.....	76
Gambar 4. 19 Address list Port Knocking.....	77
Gambar 4. 20 Proses Rule Knocking	78
Gambar 4. 21 Akses Port 23	78
Gambar 4. 22 Address list Port Knocking.....	79
Gambar 4. 23 Proses Rule Knocking	79
Gambar 4. 24 Akses Port 80.....	80
Gambar 4. 25 Address list Port Knocking.....	80
Gambar 4. 26 Proses Rule Knocking	81
Gambar 4. 27 Akses Port 8291	81
Gambar 4. 28 Address list Port Knocking.....	82

DAFTAR LAMPIRAN

Lampiran 1 SKTA	A
Lampiran 2 Surat Rekomendasi Ujian Projek pembimbing 1	B
Lampiran 3 Surat Rekomendasi Ujian Projek Pembimbing 2.....	C
Lampiran 4 Verifikasi Suliat	D
Lampiran 5 TURNITIN	E
Lampiran 6 From Revisi Pembimbing 1.....	F
Lampiran 7 From Revisi Pembimbing 2.....	G
Lampiran 8 From Revisi Penguji	H

BAB I PENDAHULUAN

1.1 Latar Belakang

Sering terjadinya serangan-serangan yang dilakukan melalui layanan *port* yang dalam keadaan terbuka secara bebas, hal ini menjadi ancaman bagi keamanan data dalam sistem jaringan komputer. Untuk memberikan perlindungan bagi keamanan komputer, *firewall* sangat dibutuhkan dalam sebuah jaringan komputer tersebut. Akan tetapi *firewall* memiliki beberapa kelemahan, sistem kerja dari *firewall* menutup semua *port* dan tidak mengizinkan *user* mengaksesnya meskipun *user* tersebut memiliki wewenang untuk mengaksesnya [1].

Maka dari itu untuk mendapatkan keamanan yang diperlukan dan mengurangi serangan pada *server*, memungkinkan pengguna yang terpercaya dapat mengakses server, meskipun *port-port* terlihat tertutup diperlukannya metode yang memenuhi kondisi ini. Salah satu metode keamanan yang dapat memenuhi standar tersebut adalah metode *Port Knocking*.

Pembahasan keamanan jaringan menurut penelitian [2], membahas mengenai penerapan *firewall* pada perangkat *router* MikroTik, dengan menggunakan fitur dari *firewall* untuk mendeteksi, memfilter, dan membatasi akses yang akan masuk maupun keluar dengan meminimalisirkan *port* komunikasi. Penelitian sejenis sebelumnya [3], [4], menjelaskan mengenai keamanan *port* komunikasi dengan metode *port knocking*. Penelitian ini, menggunakan *port knocking* dalam upaya mengakses *port* pada MikroTik yang telah dibatasi oleh *firewall*, dengan cara mengirim suatu paket atau koneksi khusus untuk mengakses *port* tertentu pada MikroTik. Namun, masih terdapat

port-port yang penting pada MikroTik seperti *port* ssh, telnet, webfig, dan winbox yang mudah *remote* pada *server* MikroTik.

Port knocking merupakan suatu metode untuk keamanan jaringan dengan memanfaatkan sistem *firewall* dengan menggunakan sistem kerja seperti membuka atau menutup akses *port* tertentu pada perangkat jaringan [5]. Manfaat dari metode *port knocking* yaitu memberikan autentikasi bagi pengguna sebelum dapat mengakses ke suatu *server* pada perangkat jaringan. Metode ini juga dapat dijalankan pada protokol TCP, UDP maupun ICMP.

Berdasarkan pembahasan latar belakang penulis bermaksud untuk membuat penelitian sebagai laporan akhir yang berjudul Implementasi *Port Knocking* Untuk Keamanan Layanan Jaringan Pada *Router* MikroTik. Tujuan dari penelitian ini guna meningkatkan keamanan dengan membangun sebuah *rules firewall* pada MikroTik dan membatasi hak akses *user*, sehingga hanya *user* tertentu yang dapat mengakses *server* secara penuh.

1.2 Tujuan

Tujuan dari penulisan dan pembuatan projek ini adalah:

1. Membangun *rules Knocking* untuk mengakses layanan *port* pada *routerboard* MikroTik.
2. Membatasi *port* yang mudah mengakses *remote routerboard* MikroTik.
3. Mengetahui langkah-langkah dari metode *port knocking*.

1.3 Manfaat

Manfaat dari penulisan dan pembuatan projek ini adalah:

1. Meningkatkan keamanan layanan jaringan pada *routerboard* mikrotik agar terhindar dari penyalahgunaan data.
2. Mengurangi penyalahgunaan akses layanan *port* pada *routerboard* MikroTik.
3. Memberikan manfaat bagi penulis dari metode *port knocking*.

1.4 Rumusan Masalah

Rumusan masalah dari projek ini adalah:

1. Bagaimana membuat sebuah *rules* pada *routerboard* MikroTik dengan menggunakan metode *port knocking*.
2. Bagaimana cara mengamankan layanan jaringan pada *routerboard* MikroTik.

1.5 Batasan Masalah

Penulis telah membatasi masalah dari proyek ini adalah:

1. Membuat *rules* keamanan, hanya *user* yang telah ditentukan yang dapat memiliki akses masuk pada *router* MikroTik.
2. Menutup *port-port* yang penting pada *router* MikroTik dan hanya *user/client* yang telah mengetahui langkah-langkahnya yang dapat memasuki layanan jaringan tersebut.

1.6 Metodologi Penelitian

Dari proyek ini diselesaikan dengan menggunakan urutan metodologi sebagai berikut:

1. Tahapan *Literature*

Menggunakan metode pengumpulan data atau informasi dari berbagai sumber seperti jurnal, buku, web, dan dari informasi lainnya yang berhubungan dari penelitian proyek ini yang berjudul implementasi *port knocking* untuk keamanan layanan jaringan pada router.

2. Tahapan Konsultasi

Tahap ini merupakan tanya jawab dengan dosen pembimbing atau dengan dosen yang bersangkutan dengan tujuan untuk membatasi kesalahan yang ada pada laporan proyek.

3. Tahapan Perancangan

Menjalankan simulasi dengan menerapkan secara langsung menggunakan alat yang dibutuhkan seperti *routerboard* Mikrotik dan alat lainnya, serta menguji coba dari penelitian proyek ini.

4. Tahapan Hasil dan Kesimpulan

Pada tahap ini menjelaskan mengenai hasil dari perancangan penelitian dan dapat mengambil kesimpulan dari pembuatan proyek akhir yang telah dibuat.

1.7 Sistematika Penelitian

Untuk pembuatan proyek adanya langkah-langkah penjelasan mengenai proses yang akan dilakukan pada setiap BAB yang ada, sebagai berikut:

BAB I PENDAHULUAN

Pada bagian awal dari proyek ini merupakan bagian yang bersumber dari penelitian yang akan akan dibahas mengenai apa yang akan dikerjakan oleh seorang penulis.

BAB II TINJAUAN PUSTAKA

Pada bab ini merupakan dasar teori yang bersangkutan dengan proyek yang dibahas yang berdasarkan sejarah dan pengertian yang dapat di buku, jurnal ataupun sumber yang berhubungan dari proyek ini.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan tentang perancangan dari penelitian yang akan dilakukan dari *flowchart*, topologi, struktur serta metodologi yang digunakan.

BAB IV HASIL DAN PEMBAHASAN

pada bab ini merupakan hasil dari pembahasan yang telah dilakukan dan sistem yang diterapkan pada implementasi pada alat yang telah dipakai. Hasil berupa data yang telah dilakukan pada bagian sebelumnya.

BAB V KESIMPULAN DAN SARAN

Bab ini merupakan kesimpulan dan saran dari projek atau penelitian yang telah dilakukan mengenai pembahasan dari awal bab I pendahuluan hingga bab IV hasil implementasi dan uji coba.

DAFTAR PUSTAKA

- [1] A. P. A. Kusuma and Asmunin, "Implementasi Simple Port Knocking Pada Dynamic Routing (OSPF) Menggunakan Simulasi GNS3," *J. Manaj. Inform.*, vol. 5, no. 2, pp. 7–17, 2016.
- [2] I. G. K. O. Mardiyana, "Keamanan Jaringan Dengan Firewall Filter Berbasis Mikrotik Pada Laboratorium Komputer STIKOM Bali," *Stmik Stikom*, no. 86, pp. 804–807, 2015.
- [3] A. Amarudin, "Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking," *J. Teknoinfo*, vol. 12, no. 2, p. 72, 2018, doi: 10.33365/jti.v12i2.121.
- [4] M. Julkarnain and A. J. Afahar, "Implementasi Port Knocking Untuk Keamanan Jaringan Smkn 1 Sumbawa Besar," *J. Inform. Teknol. dan Sains*, vol. 3, no. 2, pp. 326–335, 2021, [Online]. Available: <http://www.jurnal.uts.ac.id/index.php/JINTEKS/article/view/1016>.
- [5] A. Prihanto and P. Knocking, "Implementasi Port-Knocking di Mikrotik dengan Menggunakan Komponen Delphi TcpClient," no. Ste, pp. 533–538, 2013.
- [6] A. Widodo, "Implementasi Metode Discovery Pada Game Edukasi Keamanan Jaringan Komputer," *IJNS – Indones. J. Netw.*, vol. 4345, no. 2, pp. 0–412, 2015.
- [7] K. Anugrah, "Pengenalan Osi Layer Kata Kunci : Pengenalan Osi Layer," pp. 1–5, 2016.
- [8] A. Amarudin and A. Yuliansyah, "Analisis penerapan mikrotik router sebagai user manager untuk menciptakan internet sehat," *Tam*, vol. 9, no. 1, pp. 62–66, 2018.
- [9] T. D. Purwanto and W. Cholil, "Analisis Kinerja Wireless Radius Server Pada Perangkat Access Point 802 . 11g (Studi Kasus di Universitas Bina Darma)," *Semin. Nas. Teknol. Inf. Komun. Terap. 2013 (Semantik 2013)*, vol. 2013, no. November, pp. 371–376, 2013.

- [10] F. Ardianto, T. Akbar, "Perancangan Sistem *Monitoring* Keamanan Jaringan Jarak Jauh Menggunakan MikroTik *Operational System* Melalui *Virtual Private Network*", Vol. 2, No. 1, September 2017.
- [11] F. Wahyudi and L. T. Utomo, "Perancangan Security Network Intrusion Prevention System Pada PDTI Universitas Islam Raden Rahmat Malang," *Edumatic J. Pendidik. Inform.*, vol. 5, no. 1, pp. 60–69, 2021, doi: 10.29408/edumatic.v5i1.3278.