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,	**Pembimbing II,**
Ahmad Heryanto, M.T.	**Adi Hermansyah, M.T.**
NIP 197801222015041002	**NIK 1613033004890001**

Mengetahui

Koordinator Program Studi Teknik Komputer,

Huda Ubaya, M.T.

NIP 198106162012121003

HALAMAN PERSETUJUAN

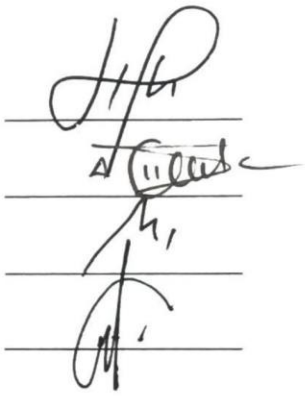
Telah diuji dan lulus pada:

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

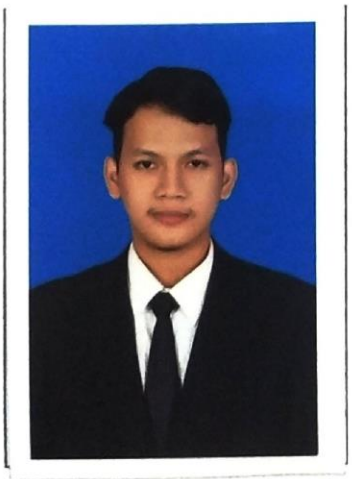
Peminatan : Teknik Komputer Jaringan

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

Hasil Pengecekan *Software iThenticate/Turnitin* : 3 %

Menyatakan bahwa laporan projek 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

وَمَن 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 seta 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 projek 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 projek 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

DAFTAR SIMBOL

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

WWW	=	*World Wide Web*
WPS	=	*Wi-Fi Protected Setup*

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

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 berjudulkan 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 projek 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 projek 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 projek 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 projek.

3. Tahapan Perancangan

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

4. Tahapan Hasil dan Kesimpulan

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

1.7 Sistematika Penelitian

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

BAB I PENDAHULUAN

Pada bagian awal dari projek 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 projek yang dibahas yang berdasarkan sejarah dan pengertian yang dapat di buku, jurnal ataupun sumber yang berhubungan dari projek 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.