

**IMPLEMENTASI SISTEM KEAMANAN JARINGAN PADA  
SERVER DENGAN METODE PORT KNOCKING BERBASIS  
MIKROTIK ROUTER OS**

**SKRIPSI**



Oleh :

**MUHAMMAD ARIEF UBAIDILLAH**

**NPM. 1534010019**

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN"**

**JAWA TIMUR**

**2019**



# LEMBAR PENGESAHAN

## SKRIPSI

Judul : IMPLEMENTASI SISTEM KEAMANAN JARINGAN PADA  
SERVER DENGAN METODE PORT KNOCKING BERBASIS  
MIKROTIK ROUTER OS

Oleh : MUHAMMAD ARIEF UBAIDILLAH  
NPM : 1534010019

Telah Diseminarkan Dalam Ujian Skripsi Pada :  
Hari Rabu, Tanggal 24 Juli 2019


Mengetahui


Dosen Pembimbing:

Dosen Penguji 1:

1.

1.

  
Henni Endah W., ST., M.Kom.  
NPT. 3 7809 13 0348 1

  
Budi Nugroho, S.Kom, M.Kom.  
NPT. 3 8009 05 0205 1

2.

2.

  
Mohammad Idhom, SP., S.Kom., MT.  
NPT. 3 8303 10 0285 1

  
Fawwaz Ali Akbar, S.Kom., M.Kom.  
NIP. 19920317 201803 1 002

3.

  
Eka Prakarsa Mandyartha, ST., M.Kom.  
NIP. 19880525 201803 1 001

Menyetujui

Dekan

Koordinator Program Studi  
Teknik Informatika,

Fakultas Ilmu Komputer,

  
Dr. Ir. Ni Ketut Sari, MT  
NIP. 19650731 199203 2 001

  
Budi Nugroho, S.Kom, M.Kom  
NPT. 3 8009 05 0205 1



## SURAT PERNYATAAN ANTI PLAGIAT

Saya, mahasiswa Teknik Informatika UPN "Veteran" Jawa Timur, yang bertandatangan dibawah ini:

Nama : MUHAMMAD ARIEF UBAIDILLAH

NPM : 1534010019

Menyatakan bahwa Judul Skripsi / Tugas Akhir yang Saya ajukan dan akan dikerjakan, yang berjudul:

**"IMPLEMENTASI SISTEM KEAMANAN JARINGAN PADA SERVER  
DENGAN METODE PORT KNOCKING BERBASIS MIKROTIK  
ROUTER OS"**

Bukan merupakan plagiat dari Skripsi / Tugas Akhir / Penelitian orang lain dan juga bukan merupakan produk dan atau software yang saya beli dari pihak lain. Saya juga menyatakan bahwa Skripsi / Tugas Akhir ini adalah pekerjaan Saya sendiri, kecuali yang dinyatakan dalam Daftar Pustaka dan tidak pernah diajukan untuk syarat memperoleh gelar di UPN "Veteran" Jawa Timur maupun di institusi pendidikan lain.

Jika ternyata di kemudian hari pernyataan ini terbukti tidak benar, maka Saya siap menerima segala konsekuensinya.

Surabaya, Juli 2019

Hormat Sd



MUHAMMAD ARIEF UBAIDILLAH

NPM. 1534010019

# IMPLEMENTASI SISTEM KEAMANAN JARINGAN PADA SERVER DENGAN METODE PORT KNOCKING BERBASIS MIKROTIK ROUTER OS

Nama Mahasiswa : Muhammad Arief Ubaidillah  
NPM : 1534010019  
Program Studi : Teknik Informatika  
Dosen Pembimbing : Henni Endah Wahanani, S.T., M.Kom.  
Mohammad Idhom, S.P., S.Kom., M.T.

## ABSTRAK

Perkembangan teknologi sampai saat ini terus berkembang. Perkembangan tersebut berdampak pada keamanan sistem yang ada di dalamnya. Sehingga bagi pengguna aplikasi yang terhubung pada jaringan internet perlu lebih waspada terhadap penetrasi yang dilakukan oleh pihak lain yang tidak bertanggung jawab. Tidak sedikit pengguna jaringan (internet) yang telah menjadi korban penetrasi. Kewaspadaan ini tentunya tidak cukup hanya dilakukan oleh pengguna jaringan internet saja melainkan juga perlu dilakukan bagi pengelola jaringan. Untuk meningkatkan keamanan jaringan dari penetrasi yang dilakukan oleh para *hacker*, maka perlu adanya penelitian yang dapat memberikan solusi terhadap permasalahan tersebut. Sebagai salah satu solusi dari permasalahan tersebut, maka dalam penelitian ini dibangun sebuah *protocol* pada *firewall* yang disebut dengan *port knocking*. Diuji pada sebuah *server* dimana fungsi *port knocking* ini adalah untuk menjaga hak akses perangkat *server* dari pengguna yang tidak berwenang untuk mengaksesnya. Metode *port knocking* diterapkan pada Mikrotik Router OS dengan cara kerja yaitu dapat membuka atau menutup akses *port* tertentu melalui *firewall* pada *server* sesuai dengan pola yang dibangun. Adapun *port* yang dibangun pada *firewall* dalam penelitian ini memanfaatkan tiga port yaitu 22 (SSH), 23 (Telnet), dan 80 (Webfix/HTTP). Pada penelitian diuji pada jaringan publik dan lokal. Dimana mengakses server pada jaringan publik lebih lama beberapa detik daripada mengakses server via jaringan lokal. Pada protokol SSH mempunyai selisih 2,42 detik, untuk protokol Telnet 2,14 detik, sedangkan untuk pengaksesan via Web mempunyai selisih 2.19 detik. Hal ini juga dipengaruhi oleh kecepatan internet masing-masing.

**Kata kunci:** *port knocking, server, ssh, telnet, web.*

## KATA PENGANTAR

Puji syukur kehadirat Allah SWT yang telah memberikan iman, kekuatan, serta semangat kepada penulis. Karena dengan izin dan ridho-Nya lah penulis mampu untuk berfikir dan menyelesaikan skripsi dengan judul **“Implementasi Sistem Keamanan Jaringan Pada Server Dengan Metode Port Knocking Berbasis Mikrotik Router OS”**.

Banyak dukungan dan bantuan yang didapatkan selama melakukan penelitian hingga akhirnya mampu menyelesaikan penulisan laporan skripsi ini. Dengan rasa hormat, ucapan terima kasih penulis haturkan kepada seluruh pihak terkait yang turut membantu dan terlibat dalam penyusunan laporan ini dari awal hingga akhir.

Penulis menyadari bahwa masih banyak kekurangan mengingat keterbatasan pengetahuan dan kemampuan penulis. Oleh karena itu, penulis menerima segala bentuk kritik dan saran dari semua pihak dalam penyempurnaan laporan ini.

Surabaya, Juli 2019

Penulis

## UCAPAN TERIMA KASIH

1. Allah SWT, karena berkat rahmat dan berkahnya dapat menyusun dan menyelesaikan laporan skripsi ini hingga selesai.
2. Dr. Ir. Akhmad Fauzi, MMT., selaku Rektor Universitas Pembangunan Nasional “Veteran” Jawa Timur.
3. Dr. Ir. Ni Ketut Sari, M.T., selaku Dekan Fakultas Ilmu Komputer Universitas Pembangunan Nasional “Veteran” Jawa Timur.
4. Budi Nugroho, S.Kom., M.Kom., selaku Koordinator Program Studi Teknik Informatika Universitas Pembangunan Nasional “Veteran” Jawa Timur.
5. Kedua Orang Tua dan Keluarga yang telah memberikan doa, kasih sayang, serta semangat pada saat pengerjaan dan juga dalam penulisan laporan ini.
6. Henni Endah W., S.T., M.Kom., selaku Dosen Pembimbing 1 yang dengan sabar membimbing, mengarahkan serta memberikan masukan sejak awal penelitian ini berlangsung hingga akhir.
7. Mohammad Idhom, S.P., S.Kom., M.T., selaku Dosen Pembimbing 2 yang dengan sabar membimbing, mengarahkan serta memberikan masukan sejak awal penelitian ini berlangsung hingga akhir.
8. Nur Aini Ersanti yang selalu memberikan dukungan serta doa yang tiada henti-hentinya dalam proses penyelesaian penelitian ini.
9. Kawan-kawan pengurus Himpunan Mahasiswa Teknik Informatika yang telah menyediakan tempat untuk proses pengerjaan laporan penelitian ini.

10. Keluarga besar Unit Kegiatan Pers Mahasiswa Giri Taruna Universitas Pembangunan Nasional “Veteran” Jawa Timur yang telah menyediakan tempat untuk proses pengerjaan laporan penelitian ini.
11. Kawan-kawan jurusan Teknik Informatika angkatan 2014, 2015, 2016, dan 2017 yang telah membantu dalam penyelesaian penelitian ini beserta laporannya.

## DAFTAR ISI

LEMBAR PENGESAHAN.....	ii
SURAT PERNYATAAN ANTI PLAGIAT .....	iii
ABSTRAK .....	iv
KATA PENGANTAR .....	v
UCAPAN TERIMA KASIH .....	vi
DAFTAR ISI .....	viii
DAFTAR GAMBAR .....	xii
DAFTAR TABEL .....	xv
BAB I PENDAHULUAN .....	1
1.1    Latar Belakang .....	1
1.2    Rumusan Masalah .....	4
1.3    Batasan Masalah.....	5
1.4    Tujuan .....	5
1.5    Manfaat .....	5
BAB II TINJAUAN PUSTAKA .....	7
2.1    Penelitian Terdahulu.....	7
2.2    Sistem.....	9
2.3    Keamanan Jaringan.....	10



2.4	Server .....	11
2.4.1	Ubuntu .....	13
2.5	Port.....	15
2.5.1	Port Secure Shell (22).....	17
2.5.2	Port Telnet (23) .....	17
2.5.3	Port Hypertext Transfer Protocol (80).....	17
2.6	Port Knocking .....	17
2.7	Mikrotik .....	20
BAB III METODOLOGI.....		25
3.1	Waktu Penelitian .....	25
3.2	Tempat Penelitian.....	25
3.3	Rancangan Penelitian.....	25
3.3.1	Studi Literatur dan Pengumpulan Data.....	27
3.3.2	Analisis Kebutuhan.....	27
3.3.3	Topologi Jaringan.....	29
3.3.4	Desain dan Perancangan .....	30
3.3.5	Konfigurasi Port Knocking .....	32
3.3.6	Uji Coba.....	34
3.3.7	Analisis Hasil .....	36
BAB IV HASIL DAN PEMBAHASAN .....		38
4.1	Konfigurasi.....	38

4.1.1	Konfigurasi Router .....	38
4.1.1.1	IP Address Router.....	38
4.1.1.2	Konfigurasi Firewall Router .....	40
4.1.2	Konfigurasi Server.....	46
4.1.2.1	Instalasi SSH .....	47
4.1.2.2	Instalasi Telnet .....	48
4.1.2.3	Instalasi Apache2.....	48
4.1.3	Konfigurasi Client .....	49
4.2	Uji Coba dan Implementasi.....	50
4.2.1	Skenario Tanpa Metode .....	50
4.2.1.1	Client Linux .....	51
4.2.1.2	Client Windows .....	54
4.2.2	Skenario Dengan Metode.....	57
4.2.2.1	Client Linux .....	57
4.2.2.2	Client Windows .....	60
4.3	Analisis Hasil .....	67
BAB V KESIMPULAN DAN SARAN.....		76
5.1	Kesimpulan .....	76
5.2	Saran .....	77

DAFTAR PUSTAKA.....	78
---------------------	----

## DAFTAR GAMBAR

Gambar 3. 1 Rancangan Penelitian.....	25
Gambar 3. 2 Topologi Jaringan .....	29
Gambar 3. 3 Desain dan Rancangan IP Address .....	30
Gambar 3. 4 Flowchart Port Knocking .....	31
Gambar 3. 5 Rancangan Firewall Port Knocking.....	33
Gambar 4. 1 Konfigurasi IP Address Ether2.....	39
Gambar 4. 2 Konfigurasi IP Address Wlan1/Ether1 .....	39
Gambar 4. 3 Rule Firewall Pertama Tab General .....	40
Gambar 4. 4 Rules Firewall Pertama Tab Action.....	40
Gambar 4. 5 Rule Firewall Kedua Tab General .....	41
Gambar 4. 6 Rule Firewall Kedua Tab Action.....	42
Gambar 4. 7 Rule Firewall Ketiga Tab General.....	42
Gambar 4. 8 Rule Firewall Ketiga Tab Advanced .....	42
Gambar 4. 9 Rule Firewall Ketiga Tab Action.....	43
Gambar 4. 10 Rule Firewall Keempat Tab General .....	43
Gambar 4. 11 Rule Firewall Keempat Tab Advanced.....	44
Gambar 4. 12 Rule Firewall Keempat Tab Action .....	44
Gambar 4. 13 Rule Firewall Kelima Tab General.....	45
Gambar 4. 14 Rule Firewall Kelima Tab Advanced .....	46
Gambar 4. 15 Rule Firewall Kelima Tab Action.....	46
Gambar 4. 16 Konfigurasi IP Address Server .....	47
Gambar 4. 17 Status SSH.....	47

- ii. Menurut Mahmud (Mahmud, 2018) yang berjudul *Implementasi Authentication System Pada Port Knocking Ubuntu Server Menggunakan Knockd Dan Python* yang membahas tentang penggunaan metode *port knocking* untuk mengatasi serangan yang dilakukan pada *server* yang kebanyakan dari layanan *port* yang terbuka, teknik yang sering dilakukan oleh penyerang yaitu *Scanning* dan *bruteforce*. Penggunaan metode ini dilakukan pada sistem operasi *Linux* dan menggunakan *knockd* sebagai perangkat *port knocking*. *Knockd* berperan mendengarkan ketukan semua lalu lintas pada *Ethernet*, mendengarkan urutan ketukan khusus sampai sesuai. Penelitian ini mengusulkan metode menggunakan *authentication* untuk meningkatkan keamanan, *client* harus mempunyai *file* yang digunakan *authentication* pada *server* sehingga memperoleh hak untuk mengakses layanan yang diperlukan dari *server*. *Port knocking* memiliki potensi pengembangan yang cukup luas terutama dibagian pengamanan *sequence* dan *timeout* serta otentikasi yang terjadi setelah *sequence* terpenuhi, dalam penelitian ini metode *Authentication port knocking* digunakan guna otentikasi dari *server* ke *client* dan sebaliknya, Hasil yang diharapkan dari penelitian ini adalah tercapainya implementasi *port knocking* yang mampu mengatasi permasalahan otentikasi dan serangan *bruteforce*. Dapat juga menyederhanakan metode *port knocking* itu sendiri, namun perlu juga menambah keamanan dengan waktu yang relatif lebih sedikit.
- iii. Menurut Wilman (Wilman, 2018) yang berjudul *Port Knocking Dan Honeypot Sebagai Keamanan Jaringan Pada Server Ubuntu Virtual* yang



Gambar 4. 18 Status Telnet .....	48
Gambar 4. 19 Status Apache2 .....	49
Gambar 4. 20 IP Address Client Linux .....	49
Gambar 4. 21 IP Address Client Windows .....	50
Gambar 4. 22 Disable Firewall.....	51
Gambar 4. 23 Scanning Port Linux Skenario Pertama .....	51
Gambar 4. 24 Linux Akses SSH Skenario Pertama .....	52
Gambar 4. 25 Linux Akses Telnet Skenario Pertama.....	52
Gambar 4. 26 Linux Akses Web Skenario Pertama .....	53
Gambar 4. 27 Proses Brute Force Berhasil .....	53
Gambar 4. 28 Scanning Port Windows Skenario Pertama.....	54
Gambar 4. 29 Tampilan Windows Akses SSH Sukses .....	55
Gambar 4. 30 Tampilan Windows Akses Telnet Sukses .....	56
Gambar 4. 31 Windows Akses Web Skenario Pertama.....	56
Gambar 4. 32 Enable Firewall.....	57
Gambar 4. 33 Scanning Port Linux Skenario Kedua.....	57
Gambar 4. 34 Tampilan Linux Akses SSH Gagal.....	58
Gambar 4. 35 Tampilan Linux Akses Telnet Gagal .....	59
Gambar 4. 36 Tampilan Linux Akses Web Gagal.....	59
Gambar 4. 37 Proses Brute Force Gagal.....	60
Gambar 4. 38 Scanning Port Windows Skenario Kedua .....	60
Gambar 4. 39 Tampilan Windows Akses SSH Gagal .....	61
Gambar 4. 40 Tampilan Windows Akses Telnet Gagal.....	61
Gambar 4. 41 Tampilan Windows Akses Web Gagal .....	62

Gambar 4. 42 Knocking Pertama.....	63
Gambar 4. 43 Knocking Address List Pertama .....	63
Gambar 4. 44 Knocking Kedua .....	63
Gambar 4. 45 Knocking Address List Kedua.....	64
Gambar 4. 46 Knocking Ketiga.....	64
Gambar 4. 47 Knocking Address List Ketiga .....	65
Gambar 4. 48 SSH Login Berhasil Setelah Knocking .....	66
Gambar 4. 49 Telnet Login Berhasil Setelah Knocking .....	66
Gambar 4. 50 Web Server Berhasil Setelah Knocking.....	67
Gambar 4. 51 Capture SSH Pada Wireshark.....	71
Gambar 4. 52 Capture Telnet Pada Wireshark .....	71
Gambar 4. 53 Log Server .....	73
Gambar 4. 54 Grafik Perbandingan Delay Jaringan Lokal dan Publik .....	74

## DAFTAR TABEL

Tabel 3. 1 Kebutuhan Perangkat Keras.....	28
Tabel 3. 2 Kebutuhan Perangkat Lunak.....	28
Tabel 3. 3 Batasan Uji Coba.....	35
Tabel 3. 4 Kondisi Port .....	36
Tabel 3. 5 Urutan Knock.....	37
Tabel 4. 1 IP Address Router .....	38
Tabel 4. 2 IP Address Server.....	47
Tabel 4. 3 IP Address Client .....	49
Tabel 4. 4 Analisis Kondisi Port.....	68
Tabel 4. 5 Waktu Scanning Port.....	69
Tabel 4. 6 Analisis Remote Server .....	69
Tabel 4. 7 Hasil Pengujian .....	72
Tabel 4. 8 Delay Remote Server.....	74