

**ANALISA DAN PERANCANGAN SISTEM PENGAMANAN AKSES
AUTHENTICATION MENGGUNAKAN METODE *PORT
KNOCKING* DAN *FIREWALL ACTION DROP*
PADA JARINGAN KANTOR WAROENG SS**

SKRIPSI



disusun oleh

Iip Shoifuddin

14.11.8204

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2018**

**ANALISA DAN PERANCANGAN SISTEM PENGAMANAN AKSES
AUTHENTICATION MENGGUNAKAN METODE *PORT
KNOCKING* DAN *FIREWALL ACTION DROP*
PADA JARINGAN KANTOR WAROENG SS**

SKRIPSI



disusun oleh

Iip Shoifuddin

14.11.8204

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2018**

PERSETUJUAN

SKRIPSI

**ANALISA DAN PERANCANGAN SISTEM PENGAMANAN AKSES
AUTHENTICATION MENGGUNAKAN METODE *PORT
KNOCKING* DAN *FIREWALL ACTION DROP*
PADA **JARINGAN KANTOR WAROENG SS****


yang dipersiapkan dan disusun oleh

Iip Shoifuddin

14.11.8204

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 31 Maret 2018

Dosen Pembimbing,


Sudarmawan, S.T., M.T.
NIK. 190302035

PENGESAHAN

SKRIPSI

**ANALISA DAN PERANCANGAN SISTEM PENGAMANAN AKSES
AUTHENTICATION MENGGUNAKAN METODE PORT
KNOCKING DAN FIREWALL ACTION DROP
PADA JARINGAN KANTOR WAROENG SS**

yang dipersiapkan dan disusun oleh

Iip Shoifuddin

14.11.8204

telah dipertahankan di depan Dewan Penguji
pada tanggal 20 April 2018

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Ferry Wahyu Wibowo, S.Si, M.Cs
NIK. 190302235

Bayu Setiaji, M.Kom
NIK. 190302216

Hastari Utama, M.Cs
NIK. 190302230




Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 20 April 2018

DEKAN FAKULTAS ILMU KOMPUTER


Krisnawati, S.Si, MT.
NIK. 190302038



PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 25 April 2018



IIP SHOIFUDDIN

NIM. 14.11.8204

MOTTO

”Teruslah mencari celah dari sebuah tembok penghalang atau melompatlah dari atas tebing ketika dikejar musuh. Dan teruslah mencari kebenaran, karena kebenaran tersebut dirahasiakan oleh sang maha benar(Al-Haq)”



PERSEMBAHAN

1. Terimakasih untuk keluarga, ibu, mas dan mbak ku yang selalu memberikan suport kepada saya.
2. Terimakasih kepada guru - guru saya, yang telah memberikan nasihat kepada saya.
3. Terimakasih kepada Dosen pembimbing, Dosen penguji, maupun Dosen Perkuliahan. Berkat Bapak/Ibu Dosen skripsi ini berjalan dengan lancar.
4. Terimakasih kepada Rekan Waroeng SS, dan terimakasih pada manajemen Waroeng SS yang telah mengizinkan saya melakukan penelitian di kantor Waroeng SS.
5. Terimakasih kepada pak Teguh atas nasihat yang diberikan kepadaku.
6. Untuk temen - temen kelas RPL 1 SMKN 1 PANDEGLANG
7. Untuk temen - temen kelas TI10 angkatan 2014.
8. Untuk temen - temen UKI Jashtis.
9. Untuk temen - temen Forum Asisten
10. Terimakasih untuk M Rudy Setyawan, S.Kom
11. Persembahan terakhir yang spesial untuk ayah saya AMAD SURACHMAN.

KATA PENGANTAR

Puji syukur kehadiran Allah yang telah melimpahkan rahmat dan karunianya, serta memberi kekuatan kepada penulis sehingga dapat menyelesaikan skripsi ini dengan judul “ANALISA DAN PERANCANGAN SISTEM PENGAMANAN AKSES *AUTHENTICATION* MENGGUNAKAN METODE *PORT KNOCKING* DAN *FIREWALL ACTION DROP* PADA JARINGAN KANTOR WAROENG SS”.

Adapun tujuan dari penelitian ini adalah untuk mengamankan konfigurasi *router*. Karena, jika konfigurasi *router* tersebut di akses oleh yang tidak berwenang maka akan menimbulkan kerugian. Salah satu dari kerugian tersebut adalah tidak dapat mengakses internet, karena perubahan konfigurasi *router* oleh pihak yang tidak berwenang atau masalah masalah yang terkait dengan konfigurasi *router* yang menjadi kacau.

Terimakasih kepada pihak yang telah membantu atau telah menjadi suport dalam pembuatan skripsi ini. Keterlibatannya membuat penulis bisa menyelesaikan skripsi ini. Dan ucapan terimakasih dari penulis atas keterlibatannya.

Yogyakarta, 25 April 2018

Penulis,

IIP SHOIFUDDIN

14.11.8204

DAFTAR ISI

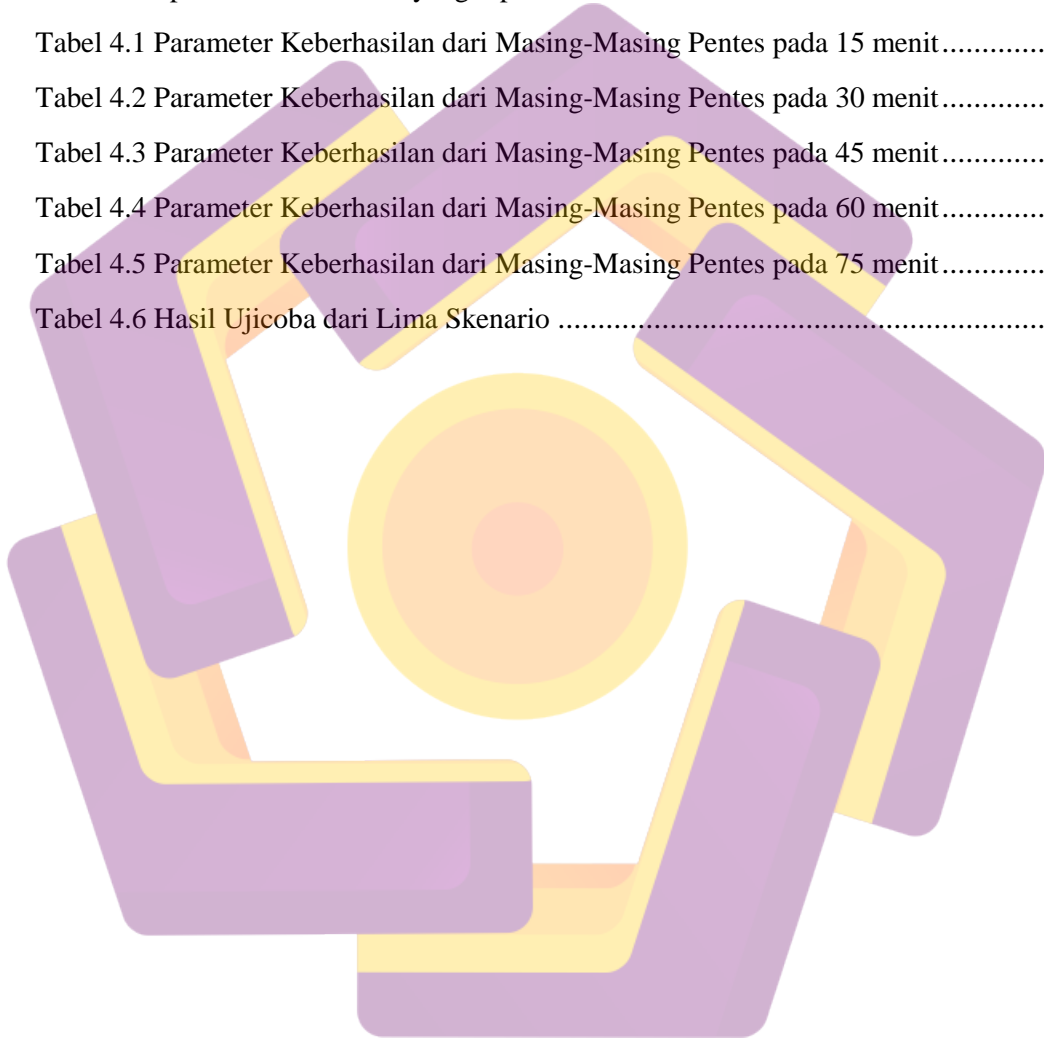
ANALISA DAN PERANCANGAN SISTEM PENGAMANAN AKSES <i>AUTHENTICATION</i> MENGGUNAKAN METODE <i>PORT</i>	I
<i>KNOCKING</i> DAN <i>FIREWALL ACTION DROP</i>	I
PADA JARINGAN KANTOR WAROENG SS	I
PERSETUJUAN	III
PENGESAHAN	IV
PERNYATAAN.....	V
MOTTO	VI
PERSEMBAHAN	VII
KATA PENGANTAR	VIII
DAFTAR ISI.....	IX
DAFTAR TABEL.....	XII
DAFTAR GAMBAR	XIII
INTISARI.....	XVI
<i>ABSTRACT</i>	XVII
BAB I PENDAHULUAN	1
1.1 LATAR BELAKANG MASALAH.....	1
1.2 RUMUSAN MASALAH	3
1.3 BATASAN MASALAH	3
1.4 MAKSUD DAN TUJUAN PENELITIAN.....	4
1.5 MANFAAT PENELITIAN.....	4
1.6 METODE PENELITIAN	4
1.6.1 <i>PPDIOO</i>	4
1.7 SISTEMATIKA PENULISAN.....	5

BAB II LANDASAN TEORI	6
2.1 KAJIAN PUSTAKA	6
2.2 DASAR TEORI	8
2.2.1 <i>Internet</i>	8
2.2.2 <i>TCP/IP</i>	8
2.2.3 <i>IP Address</i>	8
2.2.4 <i>Keamanan Jaringan</i>	9
2.2.5 <i>Jaringan Komputer</i>	10
2.2.6 <i>Port Knocking</i>	10
2.2.7 <i>Port</i>	11
2.2.8 <i>Firewall</i>	12
2.2.9 <i>Mikrotik</i>	13
2.2.10 <i>WinBox</i>	14
2.2.11 <i>PuTTY</i>	14
2.2.12 <i>Nmap</i>	15
2.2.13 <i>Google Chrome</i>	16
2.2.14 <i>VM VirtualBox</i>	16
2.2.15 <i>BackTrack</i>	16
2.2.16 <i>Wireshark</i>	17
2.2.17 <i>arpspoof</i>	18
2.2.18 <i>Hydra</i>	18
2.2.19 <i>router_flood6</i>	19
BAB III ANALISIS DAN PERANCANGAN	21
3.1 TINJAUAN UMUM	21
3.1.1 <i>Profile Kantor</i>	21
3.1.2 <i>Visi dan Misi Waroeng Spesial Sambal (SS)</i>	21
3.1.3 <i>Struktur Organisasi</i>	22
3.1.4 <i>Jaringan Komputer Waroeng Spesial Sambal (SS)</i>	23
3.1.5 <i>Topologi Jaringan Waroeng Spesial Sambal (SS)</i>	24
3.2 ANALISIS MASALAH	25

3.3 TAHAP PENELITIAN	26
3.4 TAHAP PREPARE.....	28
3.5 TAHAP PLAN (PERENCANAAN).....	29
3.5.1 <i>Kebutuhan Hardware (Perangkat Keras)</i>	29
3.5.2 <i>Kebutuhan Software (Perangkat Lunak)</i>	30
3.5.3 <i>Skenario Perancangan</i>	32
3.6 TAHAP DESIGN.....	35
3.6.1 <i>Konfigurasi Port Knocking Pada Router Mikrotik</i>	36
3.6.2 <i>KONFIGURASI IPV4 PADA CLIENT</i>	45
BAB IV IMPLEMENTASI DAN PEMBAHASAN	47
4.1 IMPLEMENTASI	47
4.1.1 <i>Implementasi Menejemen User</i>	47
4.1.2 <i>Implementasi Port Knocking</i>	47
4.2 PENGUJIAN	50
4.2.1 <i>Skenario 1</i>	50
4.2.3 <i>Skenario 3</i>	72
4.2.4 <i>Skenario 4</i>	79
4.2.5 <i>Skenario 5</i>	85
4.3 HASIL KESELURUHAN UJICoba	92
4.4 KELEMAHAN DAN KELEBIHAN SISTEM YANG DIRANCANG	93
BAB V PENUTUP	95
5.1 KESIMPULAN	95
5.2 SARAN	96
DAFTAR PUSTAKA	98
LAMPIRAN A (KONFIGURASI HOTSPOT DAN USERMANAGER)	1

DAFTAR TABEL

Tabel 2.1 Perbandingan penelitian yang dilakukan dengan penelitian sebelumnya.....	7
Tabel 3.1 Daftar IP Hardware Topologi Riil	24
Tabel 1.2 Tahap-Tahap Penelitian.....	27
Tabel 3.3 Spesifikasi Hardware yang dipakai.....	36
Tabel 4.1 Parameter Keberhasilan dari Masing-Masing Pentas pada 15 menit.....	65
Tabel 4.2 Parameter Keberhasilan dari Masing-Masing Pentas pada 30 menit.....	71
Tabel 4.3 Parameter Keberhasilan dari Masing-Masing Pentas pada 45 menit.....	78
Tabel 4.4 Parameter Keberhasilan dari Masing-Masing Pentas pada 60 menit.....	84
Tabel 4.5 Parameter Keberhasilan dari Masing-Masing Pentas pada 75 menit.....	91
Tabel 4.6 Hasil Ujicoba dari Lima Skenario	92

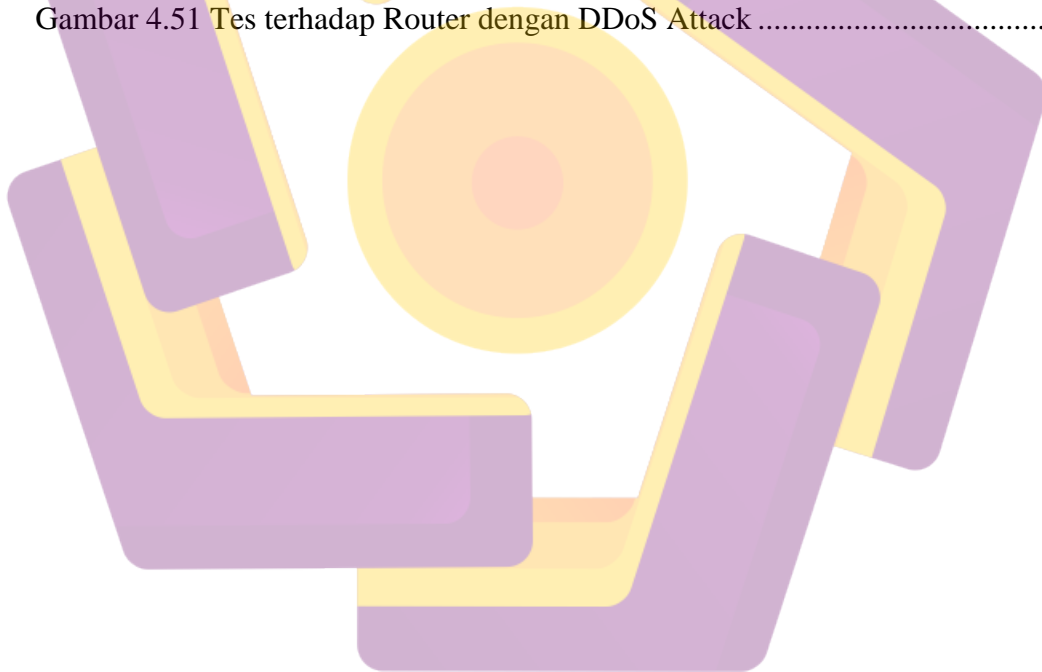


DAFTAR GAMBAR

Gambar 3.1 Logo Waroeng SS	21
Gambar 3.2 Struktur Organisasi Waroeng Spesial Sambal (SS).....	22
Gambar 3.3 Kecepatan Internet Waroeng Spesial Sambal (SS)	23
Gambar 3.4 Topologi Jaringan Kantor Waroeng SS	24
Gambar 3.5 Hasil Scan Port Mikrotik.....	25
Gambar 3.6 Desain jaringan <i>Port Knocking</i>	36
Gambar 3.7 Login menggunakan WinBox.....	37
Gambar 3.8 Konfigurasi DHCP Client	37
Gambar 3.9 Konfigurasi IPv4	38
Gambar 3.10 Konfigurasi internet.....	38
Gambar 3.11 Konfigurasi Internet.....	39
Gambar 3.12 Konfigurasi <i>Port Knocking</i>	39
Gambar 3.13 Konfigurasi <i>Port Knocking</i>	40
Gambar 3.14 Konfigurasi <i>Port Knocking</i>	41
Gambar 3.15 Konfigurasi <i>Port Knocking</i>	41
Gambar 3.16 Konfigurasi <i>DHCP</i> pada Wlan.....	42
Gambar 3.17 Konfigurasi <i>Network</i>	43
Gambar 3.18 Menentukan <i>Gateway</i>	43
Gambar 3.19 Menentukan <i>IP pool</i>	44
Gambar 3.20 Menentukan <i>IP DNS server</i>	44
Gambar 3.21 Menentukan <i>Lease Time</i>	45
Gambar 3.22 Konfigurasi DHCP Client.....	46
Gambar 4.1 Tes terhadap Router dengan Bruteforce Attack.....	50
Gambar 4.2 Tes terhadap Router dengan Dictionary Attack.....	51
Gambar 4.3 Tes terhadap Router dengan <i>DDoS Attack</i>	52
Gambar 4.4 Hasil Tes terhadap Router dengan Wireshark.....	52
Gambar 4.5 Hasil Tes terhadap Router dengan Wireshark.....	53
Gambar 4.6 Hasil Tes terhadap Router dengan Wireshark.....	53
Gambar 4.7 Hasil Tes terhadap Router dengan Wireshark.....	54

Gambar 4.8 Hasil Tes terhadap Router dengan Wireshark.....	54
Gambar 4.9 Hasil Tes terhadap Router dengan Wireshark	55
Gambar 4.10 Hasil Tes terhadap Router dengan Wireshark.....	55
Gambar 4.11 Hasil Tes terhadap Router dengan Wireshark.....	56
Gambar 4.12 Hasil Tes terhadap Router dengan Wireshark.....	56
Gambar 4.13 Hasil Tes terhadap Router dengan Wireshark.....	57
Gambar 4.14 Hasil Tes terhadap Router dengan Wireshark.....	57
Gambar 4.15 Hasil Tes terhadap Router dengan Wireshark.....	58
Gambar 4.16 Hasil Tes terhadap Router dengan Wireshark.....	58
Gambar 4.17 Hasil Tes terhadap Router dengan Wireshark.....	59
Gambar 4.18 Hasil Tes terhadap Router dengan Wireshark.....	59
Gambar 4.19 Hasil Tes terhadap Router dengan Wireshark.....	60
Gambar 4.20 Hasil Tes terhadap Router dengan Wireshark.....	60
Gambar 4.21 Hasil Tes terhadap Router dengan Wireshark.....	61
Gambar 4.22 Tes arpspoof pada vicitim	62
Gambar 4.23 Tes arpspoof pada vicitim	62
Gambar 4.24 Tes arpspoof pada vicitim	62
Gambar 4.25 Tes terhadap Router dengan Bruteforce Attack	63
Gambar 4.26 Tes terhadap Router dengan Dictionary Attack	63
Gambar 4.27 Tes terhadap Router dengan DDoS Attack	64
Gambar 4.28 Hasil Tes terhadap Router dengan Wireshark.....	66
Gambar 4.29 Tes terhadap Router dengan Dictionary Attack.....	67
Gambar 4.30 Tes terhadap Router dengan DDoS Attack	67
Gambar 4.31 Tes terhadap Router dengan Bruteforce Attack	69
Gambar 4.32 Tes terhadap Router dengan Dictionary Attack.....	69
Gambar 4.33 Tes terhadap Router dengan DDoS Attack	70
Gambar 4.34 Tes terhadap Router dengan Bruteforce Attack	72
Gambar 4.35 Tes terhadap Router dengan Dictionary Attack	73
Gambar 4.36 Tes terhadap Router dengan DDoS Attack	74
Gambar 4.37 Tes terhadap Router dengan Bruteforce Attack	75
Gambar 4.38 Tes terhadap Router dengan Dictionary Attack	76

Gambar 4.39 Tes terhadap Router dengan DDoS Attack	77
Gambar 4.40 Tes terhadap Router dengan Bruteforce Attack	79
Gambar 4.41 Tes terhadap Router dengan Dictionary Attack	80
Gambar 4.42 Tes terhadap Router dengan DDoS Attack	80
Gambar 4.43 Tes terhadap Router dengan Bruteforce Attack	82
Gambar 4.44 Tes terhadap Router dengan Dictionary Attack	82
Gambar 4.45 Tes terhadap Router dengan DDoS Attack	83
Gambar 4.46 Tes terhadap Router dengan Bruteforce Attack	85
Gambar 4.47 Tes terhadap Router dengan Dictionary Attack	86
Gambar 4.48 Tes terhadap Router dengan DDoS Attack	87
Gambar 4.49 Tes terhadap Router dengan Bruteforce Attack	88
Gambar 4.50 Tes terhadap Router dengan Dictionary Attack	89
Gambar 4.51 Tes terhadap Router dengan DDoS Attack	89



INTISARI

Jaringan (*network*) adalah sebuah sistem operasi yang terdiri atas sejumlah komputer dan perangkat jaringan lainnya yang bekerja bersama-sama untuk mencapai suatu tujuan yang sama atau suatu jaringan kerja yang terdiri dari titik-titik (*nodes*) yang terhubung satu sama lain, dengan atau tanpa kabel. Masing-masing *nodes* berfungsi sebagai stasiun kerja (*workstations*). Salah satu *nodes* sebagai media jasa atau server, yaitu yang mengatur fungsi tertentu dari *nodes* lainnya. Pada Waroeng SS, jaringan komputer yang ada belum diatur. Sehingga setiap orang dapat mengakses sebuah Router hanya dengan satu syarat terhubung dengan jaringan tersebut.

Metode analisis yang digunakan penulis salah satunya adalah metode observasi. Observasi yang dilakukan yaitu pada simulasi sebuah jaringan dengan menggunakan Router Mikrotik.

Hasil dari penelitian ini didapat manajemen Otentikasi berdasarkan MAC Address sehingga tidak setiap orang dapat mengakses Router. Dan yang dapat mengakses Router tersebut hanya komputer dengan MAC Address tertentu saja.

Kata Kunci: *Port Knocking, Port, Firewall, Authentication, Attacker, Sniffing*

ABSTRACT

Network (network) is an operating system which consists of a number of other network computers and devices that work together to achieve a similar or a tujuam network that consists of the points (nodes) that are connected each other, with or without wires. Each of these nodes serve as a work station (workstations). One of the nodes as a media service or server, i.e., regulating certain functions from other nodes. At Waroeng SS, the existing computer network has not been set. So that everyone can access a Router with only one condition is linked to the network.

Methods of analysis used the author of one of these is the method of observation. The observation is done in simulation of a network by using the Mikrotik Router.

The results of this research were obtained based on the MAC Address Authentication management so that not everyone is able to access the Router. And who can access the computer with just the Router MAC Address.

Keyword: *Port Knocking, Port, Firewall, Authentication, Attacker, Sniffing*

