

**ANALISIS SISTEM KEAMANAN JARINGAN VLAN
MENGUNAKAN FIREWALL SECURITY PORT**

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Informatika



disusun oleh

MUHAMMAD ATTALLA NOVAL BIJAKSA

20.11.3693

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2024

**ANALISIS SISTEM KEAMANAN JARINGAN VLAN
MENGUNAKAN FIREWALL SECURITY PORT**

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Informatika



disusun oleh

MUHAMMAD ATTALLA NOVAL BIJAKSA

20.11.3693

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA**

YOGYAKARTA

2024

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS SISTEM KEAMANAN JARINGAN VLAN
MENGUNAKAN FIREWALL SECURITY PORT

yang disusun dan diajukan oleh

MUHAMMAD APTALI & NOVAL RIKAZA
18.11.2003

sebagai syarat untuk memperoleh gelar Sarjana
pada tanggal 3 Desember 2023

Dosen Pembimbing,



Setiawan, M.Kom
NID. 190302013

HALAMAN PENGESAHAN
SKRIPSI
ANALISIS SISTEM KEAMANAN JARINGAN VLAN
MENGGUNAKAN FIREWALL SECURITY PORT

yang dibuat dan dibikin oleh

MUHAMMAD AYTALLA SOVAL BIJAKNA

20.01.2009

Terima dipertanyakan di depan Dewan Pengaji
pada tanggal 19 February 2024

Sesungguhnya Dewan Pengaji

Nama Pengaji

Tanda Tangan

Jehi Kurnawati, M.Kom.
NIK. 190301456

Haryoko, S.Kom., M.Cs.
NIK. 190302290

Sulichilingsih, M.Kom.
NIK. 190302413

Skrripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 19 February 2024

DEKAN FAKULTAS ILMU KOMPUTER



Hendri Al Fatah S.Kom., M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : MUHAMMAD ATTALLA NOVAL BIJAKSA
NIM : 26.11.2693

Mengatakan bahwa Skripsi dengan judul berikut:

**ANALISIS SISTEM KEAMANAN JARINGAN VLAN MENGGUNAKAN
FIREWALL SECURITY PORT**

Dasar Pendidikan : Sastra Kletegab, M.Kom

1. Karya tulis ini adalah benar-benar ASLI dan BUKAN PUNJAI/ dijiplak untuk mendapatkan gelar akademis, baik di Universitas ASHCCOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, tulisan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan dibubuhi nama pengarang dan diterbitkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 19 February 2024.

Yang Menandatangani,

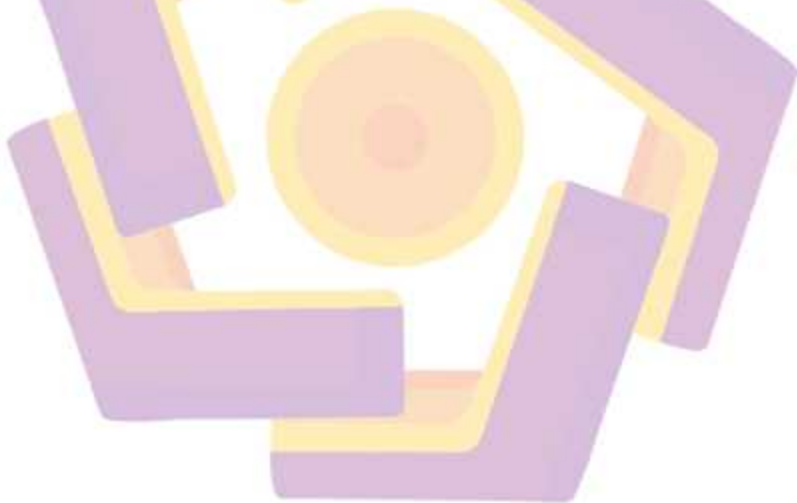


MUHAMMAD ATTALLA NOVAL BIJAKSA

HALAMAN PERSEMBAHAN

Puji syukur kepada Allah SWT atas rahmat serta hidayah nya sehingga skripsi ini dapat selesai dengan lancar serta diberikan kemudahan untuk mengerjakannya. Skripsi ini saya persembahkan untuk:

1. Keluarga saya, papa dan mama (Almh) yang telah memberikan dukungan moril maupun materi serta doa yang tiada henti untuk kesuksesan saya, serta kakak saya yang selalu mensupport saya.
2. Semua teman saya yang telah mensupport serta membantu ketika saya kesusahan dalam hal apapun terimakasih.
3. Squad NasyaM terimakasih dan sukses selalu.
4. "innamal a'malu binniyat"



KATA PENGANTAR

Puji syukur kehadiran Allah SWT atas limpahan rahmatnya sehingga penulis dapat menyelesaikan skripsi yang berjudul “Analisis Sistem Keamanan Jaringan VLAN Menggunakan Firewall Security Port” Sholawat serta salam senantiasa tercurah kepada junjungan kita Nabi Muhammad SAW.

Dalam penyusunan skripsi penulis menyadari banyak pihak yang memberikan dukungan dan bantuan selama menyelesaikan skripsi ini. Oleh karena itu, penulis mengucapkan terimakasih kepada:

1. Hanif Al Fatta, S.Kom, M.Kom selaku Dekan Fakultas Ilmu Komputer.
2. Windha Mega Pradnya D, M.Kom selaku Ketua Program Studi Prodi Informatika.
3. Subektiningsih, M.Kom selaku pembimbing dalam penyusunan skripsi ini dan telah meluangkan waktu untuk memberikan bimbingan, arahan, dan masukan sehingga skripsi ini dapat terselesaikan dengan baik.

Yogyakarta, 14 February 2024

Penulis

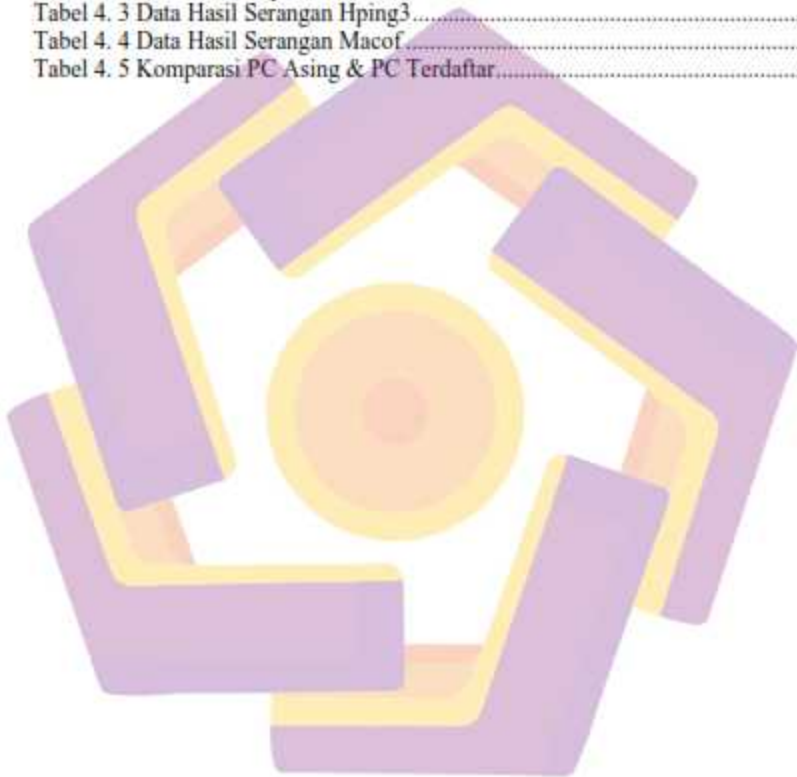
DAFTAR ISI

HALAMAN JUDUL	1
HALAMAN PERSETUJUAN	2
HALAMAN PENGESAHAN.....	3
HALAMAN PERNYATAAN KEASLIAN SKRIPSI.....	4
HALAMAN PERSEMBAHAN	5
KATA PENGANTAR.....	6
DAFTAR ISI.....	7
DAFTAR TABEL	9
DAFTAR GAMBAR.....	10
INTISARI	12
<i>ABSTRACT</i>	13
BAB I PENDAHULUAN.....	1
1.1 LATAR BELAKANG.....	1
1.2 RUMUSAN MASALAH.....	2
1.3 BATASAN MASALAH.....	2
1.4 TUJUAN PENELITIAN	2
1.5 MANFAAT PENELITIAN	2
1.6 METODE PENELITIAN	2
1.7 SISTEMATIKA PENULISAN	3
BAB II LANDASAN TEORI	4
2.1 STUDI LITERATUR.....	4
2.2 DASAR TEORI.....	13
2.2.1 <i>Firewall Security Port</i>	13

2.2.2	<i>Port Security</i>	14
2.2.3	<i>Keamanan Jaringan</i>	15
2.2.4	<i>VLAN</i>	15
BAB III METODE PENELITIAN		16
3.1	OBJEK PENELITIAN	16
3.2	ALUR PENELITIAN	17
3.3.1	<i>Analisis</i>	20
3.3.2	<i>Design</i>	21
BAB IV HASIL DAN PEMBAHASAN		22
4.1	TAHAPAN SIMULASI	22
4.2	HASIL SIMULASI	29
4.3	TAHAPAN IMPLEMENTASI	34
4.4	HASIL AKHIR IMPLEMENTASI	41
4.5	HASIL PENGUJIAN IMPLEMENTASI DAN PEMBAHASAN	42
4.6	PENGUJIAN IMPLEMENTASI MENGGUNAKAN MACOF DAN HPING3	47
4.7	TAHAPAN MONITORING	56
4.8	TAHAPAN MANAGEMENT	69
BAB V PENUTUP		72
5.1	KESIMPULAN	72
5.2	SARAN	72
REFERENSI		73

DAFTAR TABEL

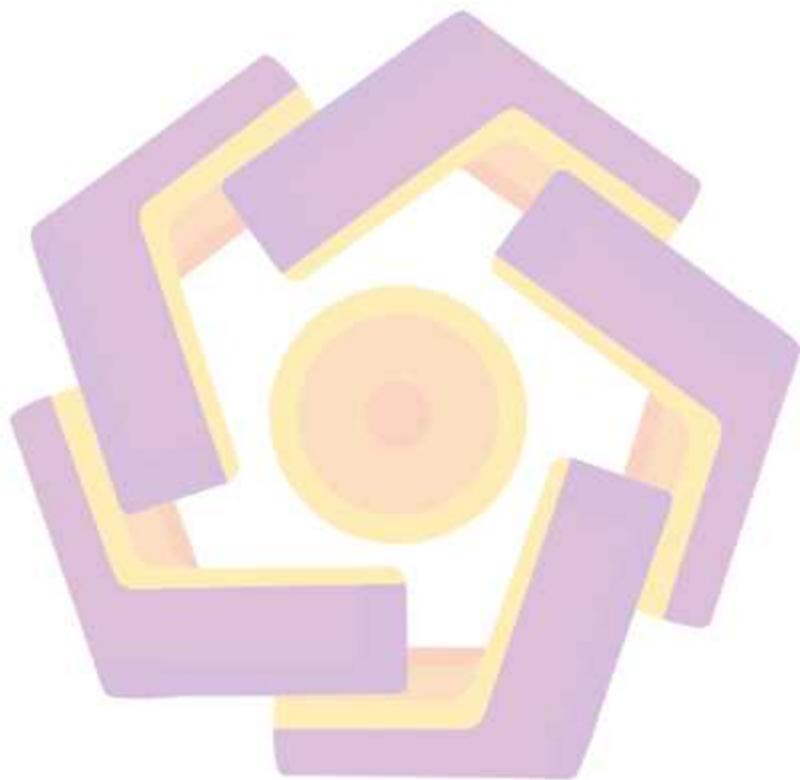
Tabel 3. 1 Analisis kebutuhan.....	20
Tabel 3. 2 Analisis Permasalahan	20
Tabel 3. 3 Tabel IP Address	21
Tabel 4. 1 Data Hasil simulasi	33
Tabel 4. 2 Data Hasil Implementasi.....	46
Tabel 4. 3 Data Hasil Serangan Hping3.....	50
Tabel 4. 4 Data Hasil Serangan Macof.....	54
Tabel 4. 5 Komparasi PC Asing & PC Terdaftar.....	57



DAFTAR GAMBAR

Gambar 3. 1 Alur Penelitian	18
Gambar 3. 2 Topologi Jaringan.....	21
Gambar 4. 1 Alur Pembuatan Simulasi.....	23
Gambar 4. 2 Topologi Jaringan Simulasi	28
Gambar 4. 3 Hasil Berhasil dan Saling Terkoneksi.....	29
Gambar 4. 4 Hasil Berhasil dan Saling Terkoneksi.....	30
Gambar 4. 5 Hasil Berhasil dan Saling Terkoneksi.....	30
Gambar 4. 6 Hasil Berhasil dan Saling Terkoneksi.....	31
Gambar 4. 7 Hasil Ketika Ada Device Asing Mencoba Masuk	31
Gambar 4. 8 Hasil Terblokir karena mac address dan ip tidak sesuai	32
Gambar 4. 9 Hasil Ketika Ada Device Asing Mencoba Masuk	32
Gambar 4. 10 Alur Pembuatan Implementasi.....	35
Gambar 4. 11 Topologi Jaringan Implementasi.....	41
Gambar 4. 12 Hasil Pengujian Berhasil dan Saling Terkoneksi.....	42
Gambar 4. 13 Hasil Pengujian Berhasil dan Saling Terkoneksi.....	42
Gambar 4. 14 Hasil Pengujian Berhasil dan Saling Terkoneksi.....	43
Gambar 4. 15 Hasil Pengujian Berhasil dan Saling Terkoneksi.....	43
Gambar 4. 16 Hasil Pengujian Berhasil dan Saling Terkoneksi.....	44
Gambar 4. 17 Hasil Pengujian Ketika Ada Device Asing Mencoba Masuk	44
Gambar 4. 18 Hasil Pengujian Terblokir dan Tidak Terkoneksi	45
Gambar 4. 19 Hasil Pengujian Terblokir dan Tidak Terkoneksi.....	45
Gambar 4. 20 Alur Serangan.....	47
Gambar 4. 21 Serangan Hping3 TCP.....	49
Gambar 4. 22 Serangan Hping3 ICMP	49
Gambar 4. 23 Serangan Macof	51
Gambar 4. 24 Serangan Macof	52
Gambar 4. 25 Serangan Macof	53
Gambar 4. 26 Hasil Pengujian Macof.....	53
Gambar 4. 27 Hasil Pengujian Macof.....	53
Gambar 4. 28 Topologi Pengujian Serangan	55
Gambar 4. 29 Hasil Monitoring Sticky Port Security Terdaftar.....	56
Gambar 4. 30 Hasil Monitoring Sticky Port Security Asing	56
Gambar 4. 31 Hasil Monitoring Hping3 TCP	60
Gambar 4. 32 Hasil Monitoring Hping3 TCP.....	60
Gambar 4. 33 Hasil Monitoring Hping3 TCP.....	61
Gambar 4. 34 Hasil Monitoring Hping3 TCP.....	61
Gambar 4. 35 Hasil Monitoring Hping3 TCP.....	62
Gambar 4. 36 Hasil Monitoring Hping3 ICMP	63
Gambar 4. 37 Hasil Monitoring Hping3 ICMP.....	63
Gambar 4. 38 Hasil Monitoring Hping3 ICMP	64
Gambar 4. 39 Hasil Monitoring Hping3 ICMP	64
Gambar 4. 40 Hasil Monitoring Hping3 ICMP	65
Gambar 4. 41 Hasil Monitoring Macof.....	66

Gambar 4. 42 Hasil Monitoring Macof.....	66
Gambar 4. 43 Hasil Monitoring Macof.....	67
Gambar 4. 44 Hasil Monitoring Macof.....	67
Gambar 4. 45 Hasil Monitoring Macof.....	68
Gambar 4. 46 Hasil Monitoring Macof.....	68



INTISARI

Dalam perkembangan teknologi jaringan komputer yang terus berlangsung dengan cepat, seiring dengan peningkatan permintaan akan akses jaringan yang efisien, stabil, dan cepat, serta tingkat keamanan yang memadai, keamanan jaringan memainkan peran yang sangat penting. Keamanan jaringan melibatkan berbagai teknik yang bertujuan untuk meningkatkan keamanan jaringan. Salah satu teknik ini melibatkan pembangunan sistem firewall menggunakan metode port security. port security digunakan untuk mengelola penggunaan port jaringan dengan tujuan mengendalikan akses ke jaringan. Selain itu, menggunakan security port berguna untuk memblokir akses jaringan, memantau dan mencegah terjadinya pencurian data oleh pihak yang tidak bertanggung jawab. dengan menerapkan metode firewall security port setidaknya dapat mengantisipasi suatu permasalahan dalam sistem jaringan komputer dan lebih meningkatkan kualitas keamanan jaringan itu sendiri. Penulis akan menganalisis keandalan dalam penggunaan firewall security port

Kata kunci: Firewall, Keamanan Jaringan, Port Security.

ABSTRACT

In the rapid development of computer network technology, along with the increasing demand for efficient, stable and fast network access, as well as adequate levels of security, network security plays a very important role. Network security involves various techniques aimed at improving network security. One of these techniques involves building a firewall system using port security methods. port security is used to manage the use of network ports with the aim of controlling access to the network. Apart from that, using security ports is useful for blocking network access, unifying and preventing data theft by irresponsible parties. By implementing the port security firewall method, you can at least anticipate problems in the computer network system and further improve the quality of network security itself. The author will analyze the use of firewall security ports.

Keyword: Firewall, Network Security, Port Security.