

**ANALISIS DETEKSI SERANGAN PADA *VIRTUAL PRIVATE SERVER*  
(VPS)**

**SKRIPSI**



disusun oleh

**Muhammad Fikri Najib**

**15.11.8490**

**PROGRAM SARJANA  
PROGRAM STUDI INFORMATIKA  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA  
2019**

**ANALISIS DETEKSI SERANGAN PADA *VIRTUAL PRIVATE SERVER*  
(VPS)**

**SKRIPSI**

untuk memenuhi sebagian persyaratan  
mencapai gelar Sarjana  
pada Program Studi Informatika



disusun oleh

**Muhammad Fikri Najib**

**15.11.8490**

**PROGRAM SARJANA  
PROGRAM STUDI INFORMATIKA  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA  
2019**

**PERSETUJUAN**

**SKRIPSI**

**ANALISIS DETEKSI SERANGAN PADA *VIRTUAL PRIVATE SERVER*  
(VPS)**

yang dipersiapkan dan disusun oleh

**Muhammad Fikri Najib**

**15.11.8490**

telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal 8 Juli 2019

**Dosen Pembimbing,**



**Nila Feby Puspitasari, S.Kom., M.Cs**  
**NIK. 190302161**

**PENGESAHAN**

**SKRIPSI**

**ANALISIS DETEKSI SERANGAN PADA *VIRTUAL PRIVATE SERVER*  
(VPS)**

yang dipersiapkan dan disusun oleh

**Muhammad Fikri Najib**

**15.11.8490**

telah dipertahankan di depan Dewan Penguji  
pada tanggal 29 Juli 2019

**Susunan Dewan Penguji**

**Nama Penguji**

Hartatik, S.T., M.Cs.  
NIK. 190302232

Joko Dwi Santoso, M.Kom  
NIK. 190302181

Nila Feby Puspitasari, S.Kom, M.Cs  
NIK. 190302161

**Tanda Tangan**



Skripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
Tanggal 29 Juli 2019

**DEKAN FAKULTAS ILMU KOMPUTER**



Krisnawati, S.Si, M.T.  
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, 18 Juli 2019



Muhammad Fikri Najib

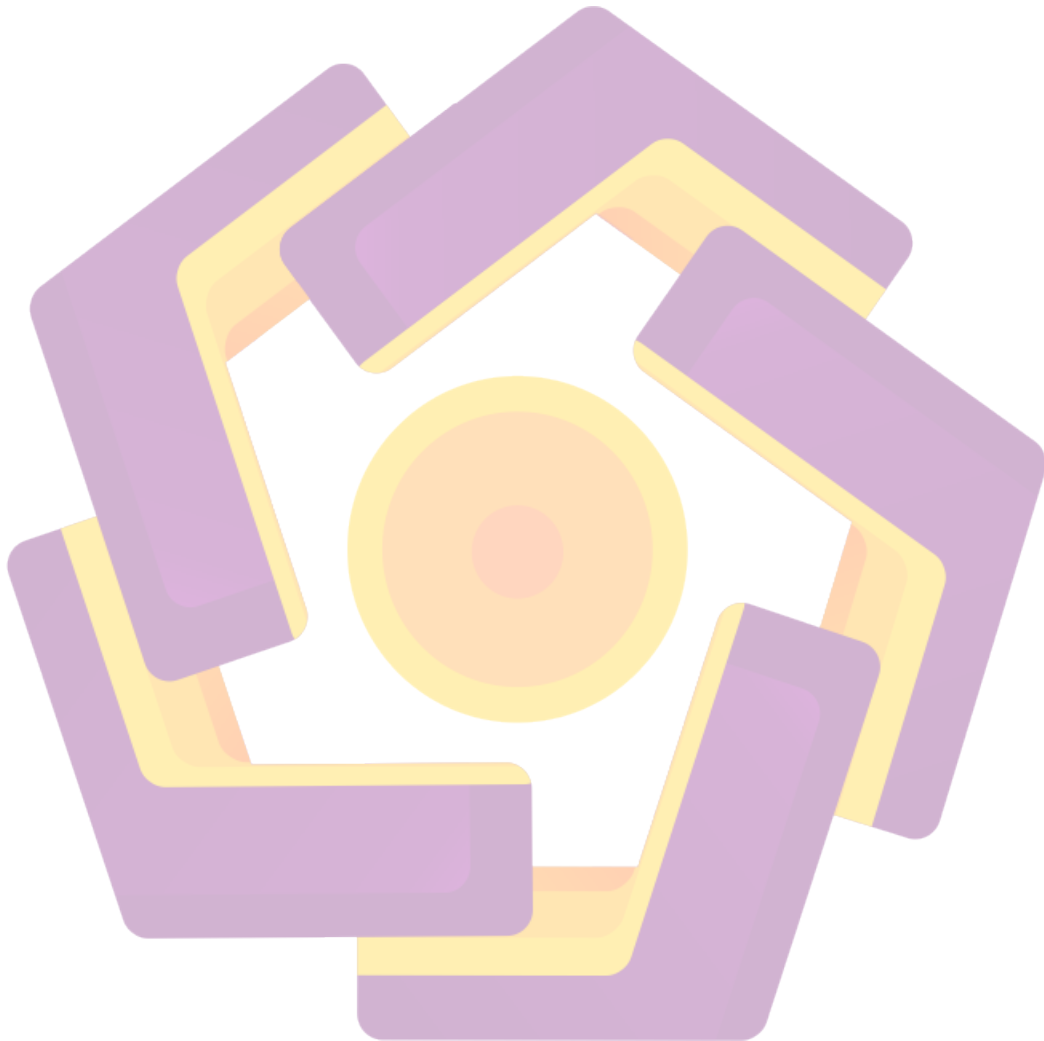
NIM. 15.11.8490

## MOTTO

Jangan pernah menunda pekerjaan karena akan berdampak di ujung waktu

You Will Never Walk Alone

Never Give Up



## PERSEMBAHAN

Alhamdulillah rabbil'alamin puji syukur atas kehadiran Allah SWT berkat rahmat dan karunia-Nya lah penulis dapat menyelesaikan skripsi ini sebagai salah satu persyaratan untuk mencapai gelar Sarjana Komputer. Skripsi ini saya persembahkan kepada :

1. Kedua Orang Tua, Bapak Nurdin dan Ibu Eni serta seluruh keluarga besar yang senantiasa memberikan semangat, doa, serta motivasi yang tiada henti.
2. Ibu Nila Feby Puspitasari, S.Kom., M.Cs selaku dosen pembimbing yang selalu mengarahkan dan memberikan masukan dalam proses penyusunan skripsi ini.
3. Teman – teman kelas 15-S1TI-01 atas kebersamaan selama kuliah di Universitas Amikom Yogyakarta.
4. Teman – teman AVBC (Amikom Volley Ball Club) atas kebersamaan dalam bidang olahraga voli.
5. Teman – teman kontrakan dan teman – teman alumni SMK Telekomunikasi Tunas Harapan atas kebersamaan dalam kegiatan sehari-hari serta bantuan yang telah diberikan dalam penyusunan skripsi ini.

## KATA PENGANTAR

Puji dan syukur penulis panjatkan kehadiran Allah SWT yang telah melimpahkan kasih sayang dan sayang-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul “Analisis Deteksi Serangan Pada *Virtual Private Server (VPS)*”.

Maksud dari penyusunan skripsi ini adalah untuk memenuhi salah satu syarat untuk mendapatkan gelar sarjana pada Program Studi Informatika di Universitas Amikom Yogyakarta.

Dalam penyusunan skripsi ini, banyak pihak yang membantu dalam berbagai hal. Oleh karena itu, penulis menyampaikan rasa terima kasih kepada :

1. Ibu Nila Feby Puspitasari, S.Kom., M.Cs. selaku pembimbing.
2. Seluruh dosen dan staff Universitas Amikom Yogyakarta.
3. Orang tua dan keluarga yang telah memberikan dukungan baik secara moril maupun materiil.
4. Teman-teman seperjuangan yang selalu membantu dalam penyusunan skripsi ini.

Yogyakarta, 17 Juli 2019



Penulis

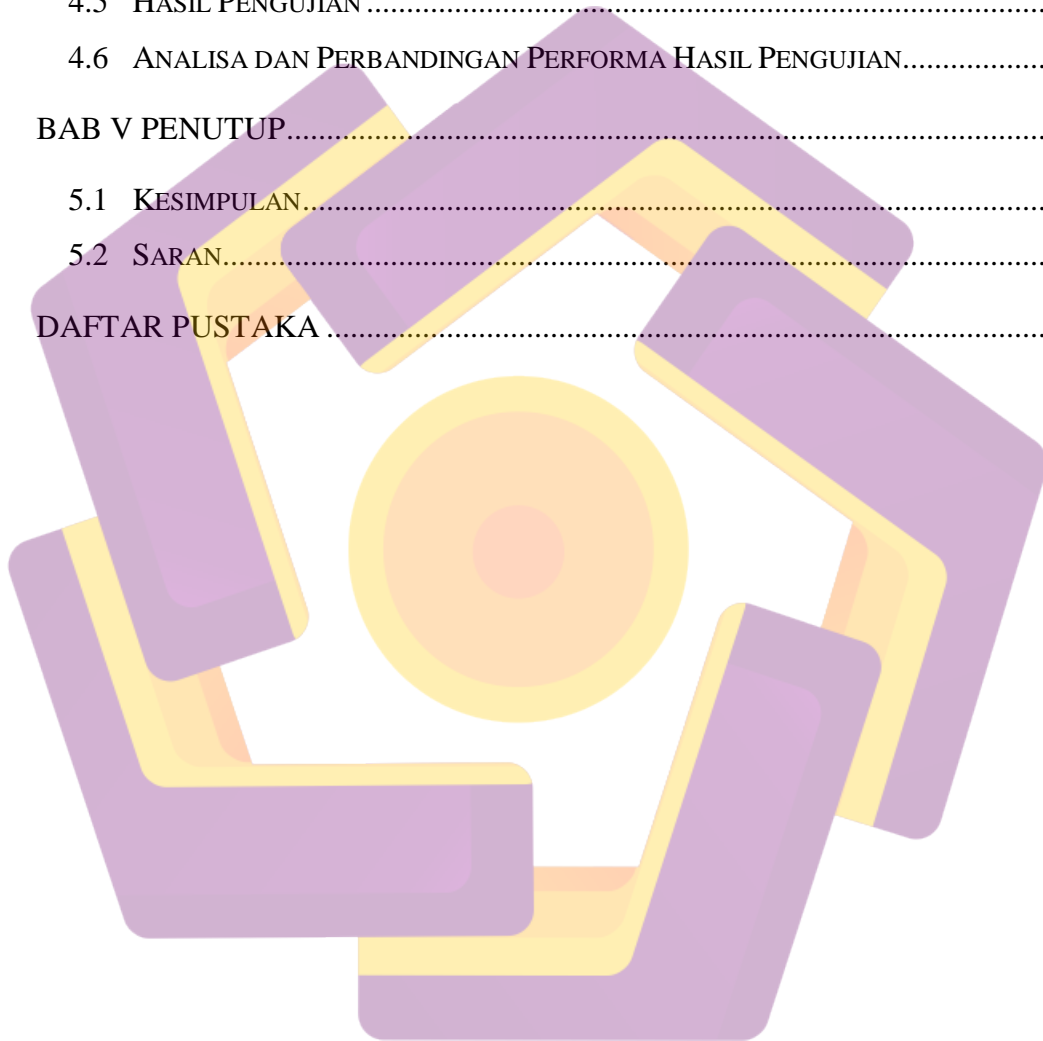


## DAFTAR ISI

JUDUL.....	I
PERSETUJUAN .....	II
PENGESAHAN .....	III
PERNYATAAN.....	V
MOTTO.....	VI
PERSEMBAHAN .....	VII
KATA PENGANTAR .....	VIII
DAFTAR ISI.....	IX
DAFTAR TABEL.....	XII
DAFTAR GAMBAR .....	XIII
ABSTRACT .....	XV
BAB I PENDAHULUAN.....	1
1.1 LATAR BELAKANG.....	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 .....	5
1.7 SISTEMATIKA PENULISAN .....	7
BAB II LANDASAN TEORI .....	9
2.1 KAJIAN PUSTAKA.....	9
2.2 LANDASAN TEORI .....	11
2.2.1 Keamanan Jaringan .....	11
2.2.2 Aspek-Aspek Keamanan Jaringan Komputer .....	11

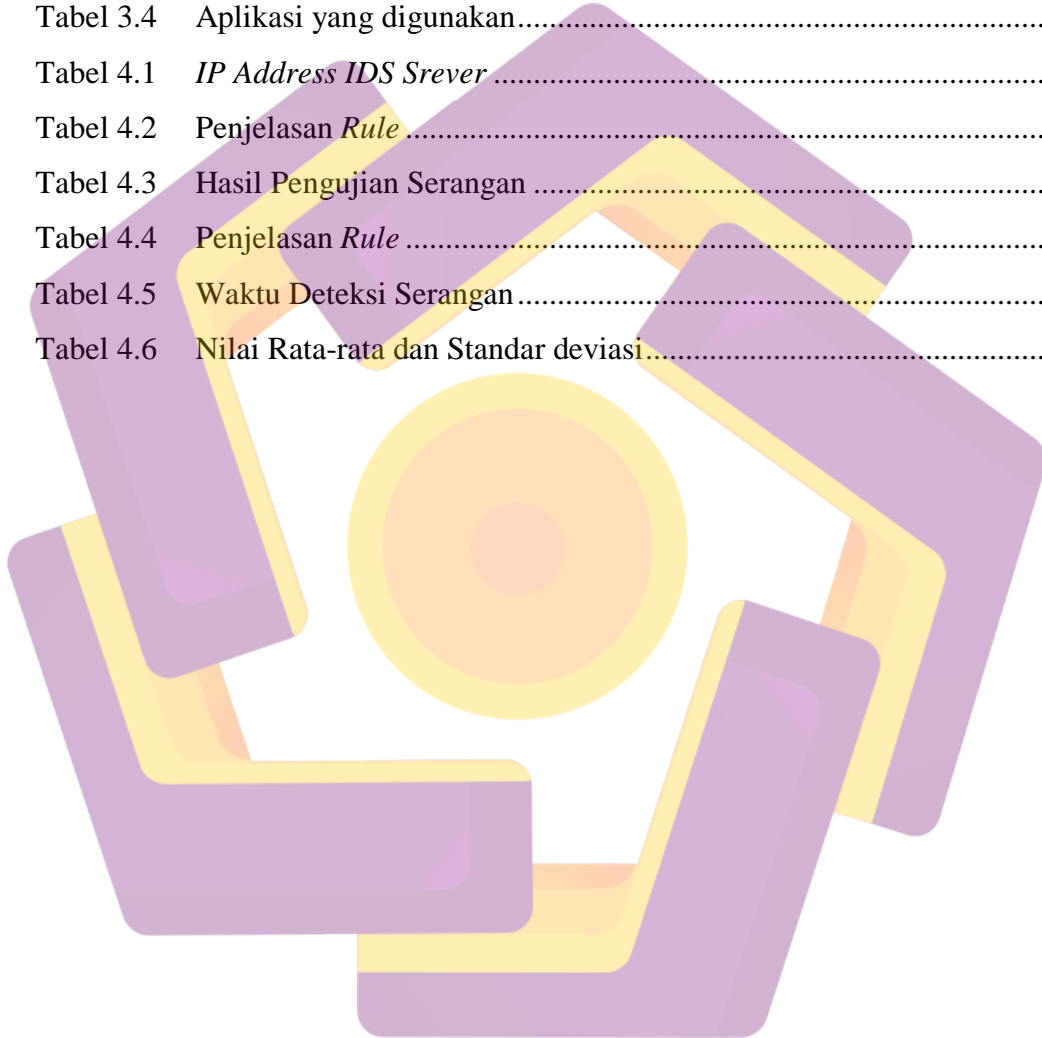
2.2.3	Aspek-Aspek Ancaman Keamanan.....	12
2.2.4	Ancaman dan Serangan Sistem Jaringan .....	13
2.2.5	Port Scannig .....	14
2.2.6	VPS (Virtual Private Server).....	15
2.2.7	Intrusion Detection System .....	16
2.2.8	Klasisfikasi IDS .....	17
2.2.9	Metode Deteksi .....	18
2.2.10	Snort .....	20
2.2.11	Mode Snort.....	21
2.2.12	Komponen Snort .....	23
2.2.13	Debian 7 ( Wheezy ) .....	27
2.2.14	Windows 8 .....	27
2.2.15	Zenmap.....	28
2.2.16	Nmap .....	28
2.2.17	PuTTY.....	29
2.2.18	Standar Deviasi .....	30
<b>BAB III ANALISIS DAN PERANCANGAN SISTEM .....</b>		<b>32</b>
3.1	ANALISIS (ANALYSIS).....	32
3.1.1	Analisis Kebutuhan Fungsional .....	32
3.1.2	Analisis Kebutuhan Perangkat Keras.....	32
3.1.3	Analisis Kebutuhan Perangkat Lunak.....	33
3.2	PERANCANGAN (DESIGN) .....	34
3.2.1	Alur Penelitian .....	34
3.2.2	Perancangan Jaringan dan IDS.....	35
3.3	SKENARIO PENGUJIAN.....	36
3.4	METODE PERHITUNGAN HASIL PENGUJIAN.....	37
<b>BAB IV IMPLEMENTASI DAN PEMBAHASAN .....</b>		<b>38</b>
4.1	IMPLEMENTASI ARSITEKTUR JARINGAN.....	38
4.1.1	IP Address VPS.....	38
4.2	IMPLEMENTASI PERANGKAT LUNAK .....	38

4.2.1	Install Paket Pendukung Snort .....	38
4.2.2	Konfigurasi Snort dalam Mode NIDS.....	40
4.2.3	Membuat Rule Snort .....	42
4.3	PENGUJIAN IDS DENGAN ZENMAP .....	43
4.4	PENGUJIAN IDS DENGAN NMAP .....	44
4.5	HASIL PENGUJIAN .....	45
4.6	ANALISA DAN PERBANDINGAN PERFORMA HASIL PENGUJIAN.....	47
BAB V PENUTUP.....		50
5.1	KESIMPULAN.....	50
5.2	SARAN.....	50
DAFTAR PUSTAKA .....		52



## DAFTAR TABEL

Tabel 3.1	Spesifikasi Laptop.....	32
Tabel 3.2	Spesifikasi VPS .....	33
Tabel 3.3	Spesifikasi Virtual Machine .....	33
Tabel 3.4	Aplikasi yang digunakan.....	34
Tabel 4.1	<i>IP Address IDS Srever</i> .....	38
Tabel 4.2	Penjelasan <i>Rule</i> .....	42
Tabel 4.3	Hasil Pengujian Serangan .....	45
Tabel 4.4	Penjelasan <i>Rule</i> .....	42
Tabel 4.5	Waktu Deteksi Serangan.....	47
Tabel 4.6	Nilai Rata-rata dan Standar deviasi.....	48



## DAFTAR GAMBAR

Gambar 2.1	Arsitektur IDS .....	20
Gambar 2.2	Komponen Snort .....	26
Gambar 3.1	Diagram alur penelitian.....	35
Gambar 3.2	Implementasi IDS.....	36
Gambar 4.1	Perintah instalasi aplikasi pendukung Snort .....	39
Gambar 4.2	Membuat direktori snort_src .....	39
Gambar 4.3	<i>Download</i> DAQ .....	39
Gambar 4.4	<i>Download</i> Snort .....	39
Gambar 4.5	<i>Update shared libraries</i> .....	40
Gambar 4.6	Konfigurasi NIDS .....	40
Gambar 4.7	Membuat direktori dan hak akses .....	40
Gambar 4.8	Merubah kepemilikan file .....	41
Gambar 4.9	Menyalin file .....	41
Gambar 4.10	Merubah isi <i>file</i> snort.conf .....	41
Gambar 4.11	<i>Rule Port Scanning</i> .....	42
Gambar 4.12	Tampilan Zenmap .....	43
Gambar 4.13	Tampilan Deteksi Serangan Zenmap .....	44
Gambar 4.14	Tampilan Nmap pada <i>Debian</i> .....	44
Gambar 4.15	Tampilan Deteksi Serangan Nmap.....	45

## INTISARI

*Virtual Private Server* (VPS) merupakan sebuah tipe *server* yang menggunakan teknologi virtualisasi untuk membagi *hardware server* fisik menjadi beberapa *server virtual* yang di *hosting* di infrastruktur yang sama. Dalam penggunaannya, VPS ini rentan terhadap berbagai macam serangan salah satunya *Port Scanning*.

*Port Scanning* merupakan suatu kegiatan atau aktifitas untuk mencari dan melihat serta meneliti *Port* pada suatu Komputer atau *Server*. *Port Scanning* adalah langkah pertama seorang penyerang untuk mencari informasi beberapa *port* yang digunakan dalam sebuah *Server*. Dengan mengetahui informasi *port* yang dapat terbuka, maka penyerang akan memanfaatkannya untuk melakukan eksploitasi dari *port* tersebut sehingga terdapat celah bagi penyerang untuk melakukan *hacking* terhadap VPS. Salah satu solusi untuk menangani masalah tersebut yaitu menggunakan *Snort* sebagai *Intrusion Detection System* (IDS).

IDS merupakan kombinasi perangkat lunak atau perangkat keras yang dapat melakukan deteksi penyusupan pada sebuah jaringan. IDS dapat mendeteksi adanya upaya yang menyangkut kerahasiaan, keaslian, dan ketersediaan data pada sebuah jaringan komputer.. Tujuan penelitian ini untuk mendeteksi serangan *Port Scanning* pada VPS menggunakan *Snort*. *Snort* akan dipasang pada VPS dengan OS Ubuntu 16.04. Sehingga mampu meningkatkan kinerja VPS dari serangan *Port Scanning*.

**Kata Kunci:** VPS (*Virtual Private Server*) , *Port Scanning*, *Snort*, IDS (*Intrusion Detectioin System*)

## **ABSTRACT**

*A Virtual Private Server (VPS) is a type of server that uses virtualization technology to divide physical server hardware into several virtual servers hosted on the same infrastructure. In its use, this VPS is vulnerable to various types of attacks, one of them is Port Scanning.*

*Port Scanning is an activity or activity to search and view and examine ports on a computer or server. Port Scanning is the first step for a writer to find information on several ports used in a server. By knowing the port information that can be opened, the attacker will use it to exploit the port so that there is a gap for the attacker to hack VPS. One solution to deal with this problem is to use Snort as an Intrusion Detection System (IDS).*

*IDS is a combination of software or hardware that can detect intrusion on a network. IDS can detect any efforts regarding confidentiality, authenticity, and availability of data on a computer network. The purpose of this study is to detect Port Scanning attacks on VPS using Snort. Snort will be installed on VPS with Ubuntu OS 16.04. So that it can improve the performance of VPS from Port Scanning attacks.*

**Keyword:** VPS (Virtual Private Server) , Port Scanning, Snort, IDS (Intrusion Detection System)