

**ANALISIS PERBANDINGAN KINERJA SNORT DAN SURICATA
SEBAGAI INTRUSION DETECTION SYSTEM DALAM
MENDETEKSI SERANGAN SYN FLOOD PADA
WEB SERVER APACHE**

SKRIPSI



disusun oleh

Melati Suci

16.11.0525

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2020**

**ANALISIS PERBANDINGAN KINERJA SNORT DAN SURICATA
SEBAGAI INTRUSION DETECTION SYSTEM DALAM
MENDETEKSI SERANGAN SYN FLOOD PADA
WEB SERVER APACHE**

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Informatika



disusun oleh

Melati Suci

16.11.0525

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2020**

PERSETUJUAN

SKRIPSI


**ANALISIS PERBANDINGAN KINERJA SNORT DAN SURICATA
SEBAGAI INTRUSION DETECTION SYSTEM DALAM MENDETEKSI
SERANGAN SYN FLOOD PADA WEB SERVER APACHE**

yang dipersiapkan dan disusun oleh

**Melati Suci
16.11.0525**

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 27 September 2019

Dosen Pembimbing,


**Lukman, M. Kom
NIK. 190302151**

PENGESAHAN

SKRIPSI

**ANALISIS PERBANDINGAN KINERJA SNORT DAN SURICATA
SEBAGAI INTRUSION DETECTION SYSTEM DALAM MENDETEKSI
SERANGAN SYN FLOOD PADA WEB SERVER APACHE**

yang dipersiapkan dan disusun oleh
Melati Suci

16.11.0525

telah dipertahankan di depan Dewan Penguji
pada tanggal 17 Januari 2020

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Lukman, M.Kom
NIK. 190302151

Agung Pambudi, S.T, M.A
NIK. 190302012

Ike Verawati, M.Kom
NIK. 190302237



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 17 Januari 2020



DEKAN FAKULTAS ILMU KOMPUTER

Krisnawati, S.Si, M.T.
NIK. 190302038

PERNYATAAN

Saya yang bertanda tangan di bawah ini menyatakan, skripsi ini merupakan karya saya sendiri (ASLI) dan isi didalam skripsi tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu Instansi Pendidikan dan sepanjang pengetahuan saya tidak terdapat karya atau pendapat yang pernah ditulis / 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 tanggung jawab saya pribadi.

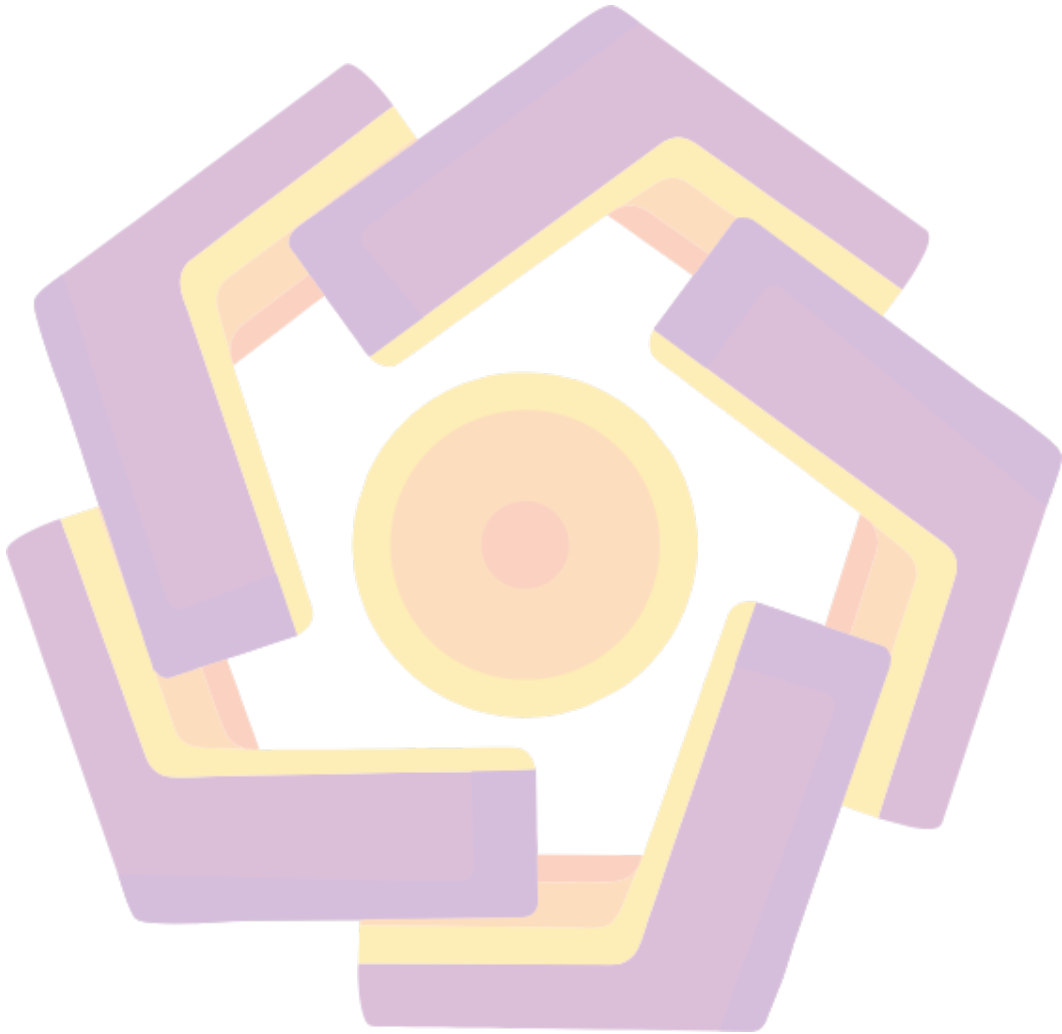
Yogyakarta, 21 Januari 2020



Melati Suci
NIM 16.11.0525

MOTTO

“Every journey begins with a single step. And you’ll never finish if you don’t start.”



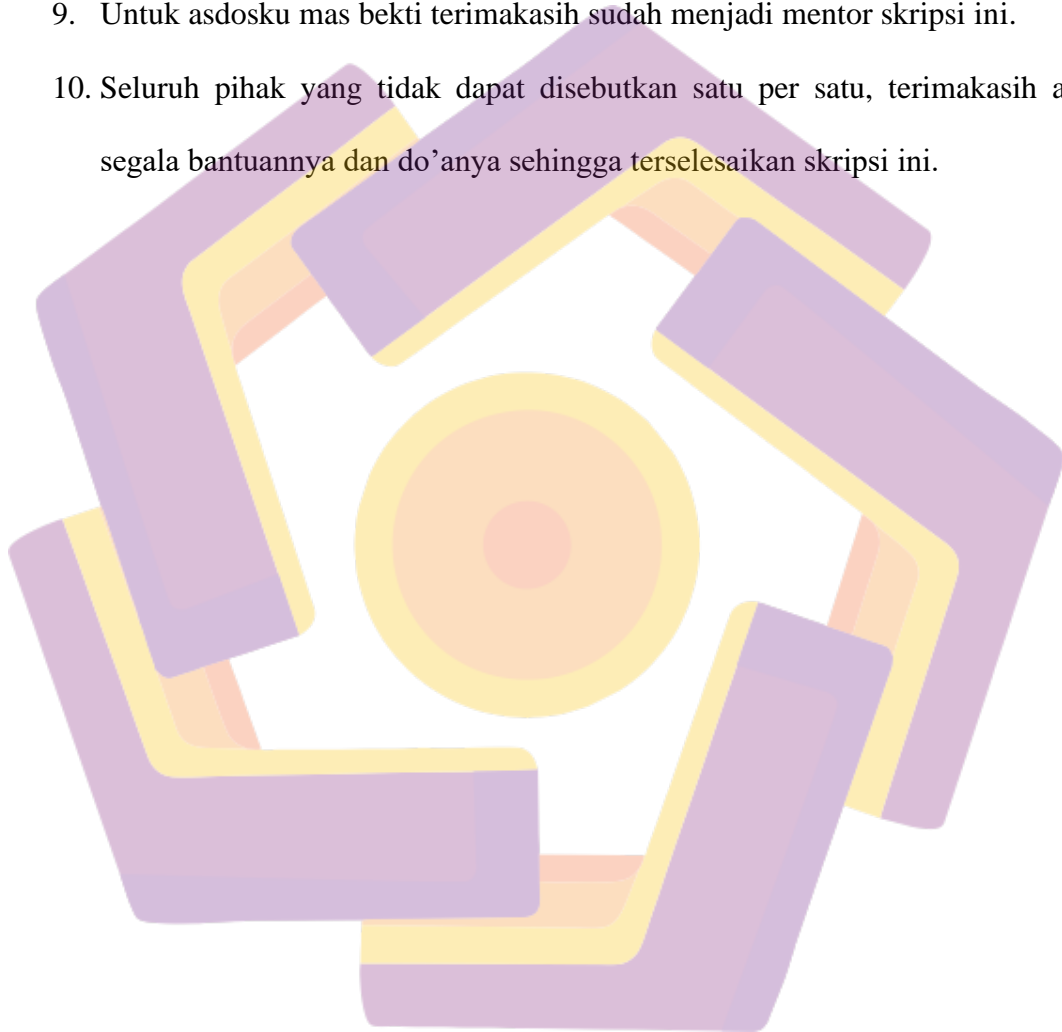
HALAMAN PERSEMBAHAN

Tak henti – hentinya saya mengucapkan syukur kepada Allah SWT yang telah memberikan saya kenikmatan, kesehatan, kesempurnaan, serta dapat menyelesaikan skripsi ini, dan skripsi ini saya persembahkan untuk:

1. Allah SWT yang telah mengabulkan semua do'a - do'a saya termasuk doa dalam menyelesaikan skripsi ini dengan lancar.
2. Untuk kedua orangtua saya yaitu Papa dan Mama yang selalu memberikan dorongan baik itu moril maupun materil, terimakasih selalu mendoakan yang terbaik dan mengasihiku sepenuh hati.
3. Untuk Kakak saya dan Adik saya, A Galih dan Dek Agung yang selalu memberikan dukungan dan semangatnya.
4. Untuk Bapak Lukman, M.Kom selaku dosen pembimbing sekaligus dosen wali, terimakasih banyak atas bimbingannya sehingga skripsi ini dapat terselesaikan.
5. Untuk Dian Lesmana sebagai support system yang selalu ada dan membantu dalam proses skripsi ini sehingga mendapatkan hasil yang terbaik. Terimakasih selalu sabar dan selalu mendoakanku.
6. Terimakasih untuk sister by heart a.k.a geng sobat ngegas yaitu Alifa, Anggita, Hesty,Dw,Ozka,Revi, telah bersamaku selama satu dekade, yang selalu memberikan semangat dan menghiburku sehingga memperlancar skripsiku.
7. Terimakasih untuk geng Kecehbong yaitu, Mayang yang selalu menjadi teman sepernasiban mungkin nasib kita memang berjodoh, Winda yang siap sedia

dalam bidang revisi penulisan, Fafa yang menjadi mentor jaringanku, Anes yang selalu menyemangatiku.

8. Untuk keluarga besar Informatika-08 terimakasih sudah hadir di pendadaranku meskipun hanya sebagian.
9. Untuk asdosku mas bekti terimakasih sudah menjadi mentor skripsi ini.
10. Seluruh pihak yang tidak dapat disebutkan satu per satu, terimakasih atas segala bantuannya dan do'anya sehingga terselesaikan skripsi ini.



KATA PENGANTAR

Puji dan syukur senantiasa peneliti panjatkan kepada ALLAH SWT, karena berkat pertolongan-Nya Alhamdulillah peneliti dapat menyelesaikan laporan skripsi ini dengan baik. Laporan skripsi yang dibuat untuk memenuhi syarat memperoleh gelar kesarjanaan Strata-1 (S1) jurusan Informatika Universitas AMIKOM Yogyakarta diharapkan bisa menjadi salah satu referensi pembuatan skripsi di Universitas AMIKOM Yogyakarta serta dapat memberikan penambahan ide yang dapat dikembangkan dimasa depan.

Skripsi ini disusun sebagai salah satu syarat kelulusan perguruan tinggi Program Studi Strata-1 Informatika di Universitas AMIKOM Yogyakarta. Selain itu skripsi ini bertujuan agar pembaca dapat menambah ilmu pengetahuan dan wawasannya.

Pada kesempatan ini dengan segala ketulusan, keikhlasan serta kerendahan hati penulis ingin mengucapkan banyak berterima kasih yang sebesar-besarnya dan penghargaan setinggi-tingginya kepada semua pihak yang telah membantu penulis dalam menyelesaikan skripsi ini. Dalam penulisan laporan skripsi ini, peneliti banyak mendapatkan bantuan serta semangat dari berbagai pihak. Untuk itu peneliti menyampaikan rasa hormat, dan terimakasih kepada:

1. Papa saya Edia Herdis, S.Pd, Ibu saya tercinta Hernaningsih, S.Pd, Kakak saya Galih CS, dan Adik saya Agung Gumilang.
2. Bapak M. Suyanto, Prof. Dr, M.M., selaku rektor Universitas AMIKOM Yogyakarta.

3. Bapak Sudarmawan, M.T selaku ketua program studi Informatika
4. Bapak Lukman, M.Kom selaku dosen pembimbing.
5. Tim penguji, segenap dosen dan karyawan Universitas AMIKOM Yogyakarta yang telah memberikan ilmu pengetahuan dan dukungan moral.
6. Keluarga sobat ngegas.
7. Keluarga besar kecehbong.
8. Keluarga besar Informatika-08

Peneliti juga memohon maaf kepada semua pihak jika dalam pelaksanaan dan penulisan laporan skripsi ini terdapat kesalahan atau hal yang kurang berkenan, semua tidak lepas karena keterbatasan peneliti.

Akhirnya, hanya dengan berdoa kepada ALLAH SWT, peneliti berharap semoga laporan skripsi ini dapat bermanfaat bagi kita semua. Amin.

Yogyakarta, 21 Januari 2020



Melati Suci

DAFTAR ISI

JUDUL	i
PERSETUJUAN.....	ii
PENGESAHAN.....	iii
PERNYATAAN	iv
MOTTO.....	v
HALAMAN PERSEMBAHAN.....	vi
KATA PENGANTAR	viii
DAFTAR ISI.....	x
DAFTAR TABEL	xiii
DAFTAR GAMBAR.....	xiv
INTISARI.....	xvi
<i>ABSTRACT</i>	xvii
BAB I.....	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.....	5
1.6. Metode Penelitian.....	6
1.7. Sistematika Penulisan.....	8
BAB II.....	10
2.1. Tinjauan Pustaka.....	10
2.2. Dasar Teori.....	14
2.2.1. Jaringan Komputer.....	14
2.2.2. Jenis jenis jaringan.....	14
2.2.3. Topologi jaringan Komputer.....	15
2.2.4. Keamanan Jaringan Komputer.....	18
2.2.5. Web Server.....	18
2.2.6. <i>Firewall</i>	20
2.2.7. Protokol TCP/IP.....	21
2.2.8. Jaringan Client-server.....	22

2.2.9.	<i>Intrusion Detection System (IDS)</i>	22
2.2.10.	Snort.....	25
2.2.11.	Suricata	25
2.2.12.	SYN Flood	26
2.2.13.	Ubuntu Linux	27
2.2.14.	HPing3	28
2.2.15.	Oracle VM Virtual box	29
2.2.16.	PuTTY.....	30
2.2.17.	Standar Deviasi.....	31
2.2.18.	Menentukan rasio performasi IDS Snort dan Suricata	32
BAB III.....		33
3.1.	Tinjauan Umum.....	33
3.2.	Identifikasi Masalah.....	34
3.3.	Analisis Masalah.....	35
3.4.	Hasil Analisis	35
3.5.	Analisis Kebutuhan.....	37
3.5.1.	Kebutuhan Fungsional	37
3.5.2.	Kebutuhan Non Fungsional.....	38
3.6.	Perancangan Sistem (Desain).....	40
3.6.1.	Rancangan Topologi Jaringan.....	40
3.6.2.	Skenario Pengujian	41
3.6.3.	Rancangan Skema Pengujian Serangan	42
BAB IV		44
4.1.	Fase <i>Implement</i> (Implementasi)	44
4.1.1.	Instalasi dan Konfigurasi Sistem.....	44
4.1.2.	Instalasi Virtual Machine VirtualBox.....	45
4.1.3.	Konfigurasi VirtualBox	46
4.1.4.	Konfigurasi Nama dan Sistem Operasi.....	47
4.1.5.	Instalasi VM Server	48
4.1.6.	Instalasi Sistem Operasi Ubuntu pada VM <i>Attacker</i>	48
4.1.7.	Instalasi dan Konfigurasi Putty	49
4.1.8.	Instalasi dan Konfigurasi Sistem Operasi Ubuntu Server.....	49

4.1.9.	Instalasi dan Konfigurasi <i>Web Server</i> pada OS Ubuntu	50
4.1.10.	Konfigurasi Snort	52
4.1.11.	Konfigurasi Suricata	56
4.1.12.	Konfigurasi Hping3	58
4.2.	Parameter Pengujian Sistem.....	59
4.3.	Pengujian IDS Snort	60
4.3.1.	Pengujian Koneksi VM <i>Attacker</i> dengan VM <i>web server</i>	60
4.3.2.	Mengaktifkan Service Snort.....	61
4.3.3.	Konfigurasi Hping3 Untuk Melakukan Serangan SYN Flood.....	61
4.4.	Pengujian IDS Suricata	62
4.4.1.	Pengujian Koneksi VM <i>Attacker</i> dengan VM <i>web server</i>	63
4.4.2.	Mengaktifkan Service Suricata	63
4.4.3.	Konfigurasi Hping3 Untuk Melakukan Serangan SYN Flood.....	64
4.5.	Hasil Pengujian Sistem IDS Snort dan Suricata.....	65
4.6.	Analisa Hasil Pengujian Sistem IDS Snort dan Suricata	73
4.7.	Metode Perhitungan Hasil Pengujian	74
4.7.1.	Perhitungan Rasio Performa Sistem IDS Snort dan Suricata.....	74
4.7.2.	Perhitungan Rasio Penggunaan Resource IDS Snort dan Suricata .	76
BAB V	79
8.1.	Kesimpulan.....	79
8.2.	Saran	80
Daftar Pustaka	81

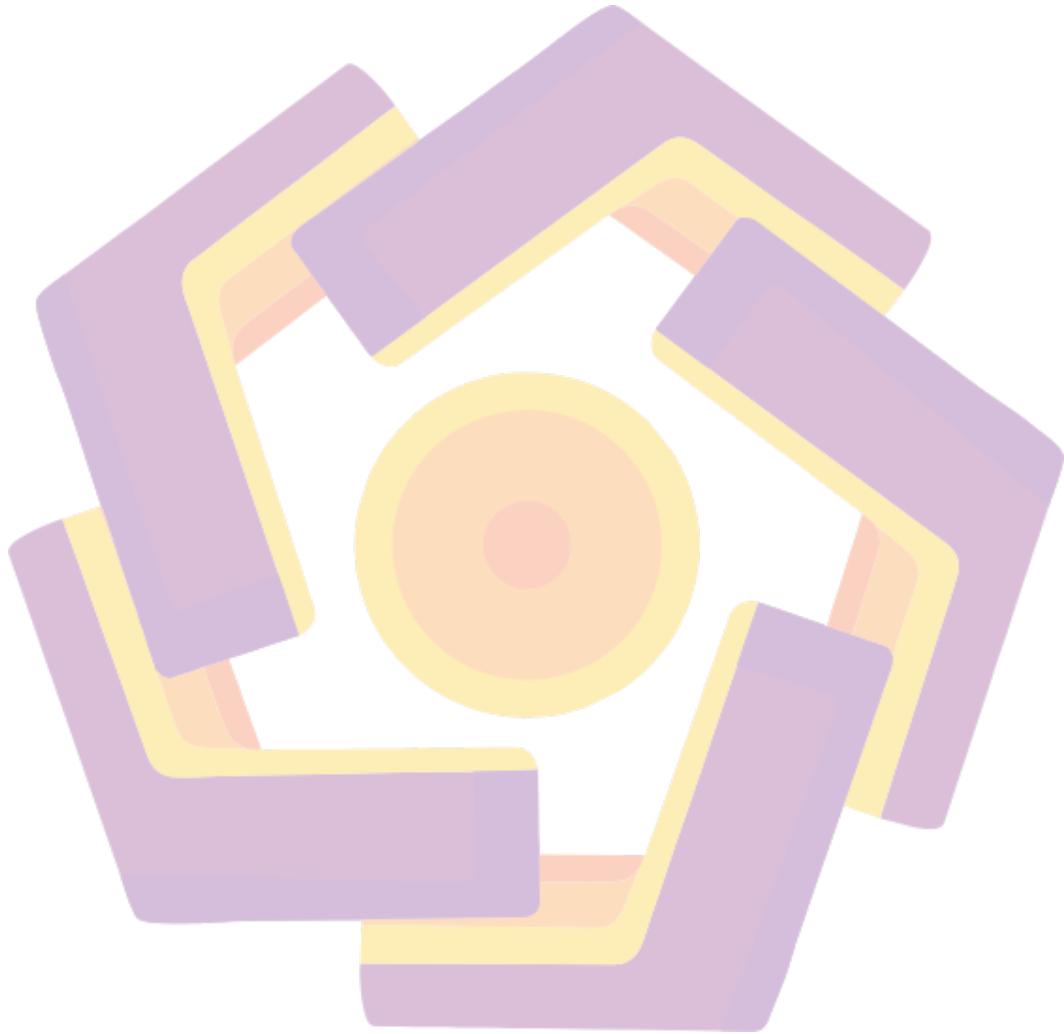
DAFTAR TABEL

Tabel 2.1 Perbandingan Jurnal Terkait	12
Tabel 2.1 Perbandingan Jurnal Terkait (Lanjutan 1)	13
Tabel 3.1 Kebutuhan Perangkat Keras	40
Tabel 3.2 Kebutuhan Perangkat Lunak	40
Tabel 4.1 Keterangan	56
Tabel 4.1 Analisa Jumlah Serangan Terdeteksi	67
Tabel 4.2 Data Penggunaan Resource	71
Tabel 4.3 Data Pengujian Efektifitas Serangan	72
Tabel 4.4 Rekapitulasi Hasil Pengujian Performa IDS Snort dan Suricata	73
Tabel 4.5 Rekapitulasi Hasil Pengujian CPU	73
Tabel 4.6 Rekapitulasi Hasil Pengujian RAM	73
Tabel 4.7 Rekapitulasi Hasil Pengujian Efektifitas Serangan	73
Tabel 4.8 Analisa Rasio Performa Serangan Terdeteksi IDS Snort dan Suricata	76
Table 4.9 Resume Hasil Rekapitulasi Data Serangan	77
Tabel 4.10 Analisa Rasio Efektifitas CPU IDS Snort dan Suricata	78
Tabel 4.11 Analisa Rasio Efektifitas RAM IDS Snort dan Suricata	79
Tabel 4.11 Analisa Rasio Efektifitas Paket dari <i>Uncaptured Paket (Dropped Paket)</i> IDS Snort dan Suricata	79

DAFTAR GAMBAR

Gambar 2.1 Contoh Skema Topologi Ring	16
Gambar 2.2 Contoh Skema Topologi Star	17
Gambar 2.3 Contoh Skema Topologi Bus	18
Gambar 2.4 Firewall yang melindungi jaringan local	21
Gambar 2.5 skema serangan SYN Flood	27
Gambar 2.6 Tool HPING3	29
Gambar 2.7 Logo Virtualbox	30
Gambar 3.1 Metode Security Policy Development Life Cycle	37
Gambar 3.2 Topologi Jaringan	41
Gambar 3.3 Skema Pengujian	43
Gambar 4.1 Instalasi VirtualBox	46
Gambar 4.2 konfigurasi jaringan internet virtualbox	47
Gambar 4.3 konfigurasi nama dan sistem operasi	49
Gambar 4.4 Tampilan Pemilihan Jumlah Memori	49
Gambar 4.5 konfigurasi Putty	50
Gambar 4.6 Tampilan Konfigurasi IP Address Server	51
Gambar 4.7 Test Ping	52
Gambar 4.8 Tampilan Web Server	52
Gambar 4.9 Pengeditan konfigurasi Snort pada File Snort.conf	55
Gambar 4.10 IDS Snort Menampilkan Rules	56
Gambar 4.11 Rules Suricata	58
Gambar 4.12 Konfigurasi suricat.yaml	59
Gambar 4.13 Test ping attacker ke web server	61
Gambar 4.14 Pengaktifan service snort	62
Gambar 4.15 IDS Snort mendeteksi serangan terhadap web server	63
Gambar 4.16 Test ping attacker ke web server Suricata	64
Gambar 4.17 Pengaktifan service IDS Suricata	65

Gambar 4.18 IDS suricata mendeteksi adanya serangan 66
Gambar 4.19 Nilai CPU dan RAM Sebelum Dilakukan Penyerangan 68
Gambar 4.20 Nilai CPU dan RAM Snort Setelah Dilakukan Penyerangan 69
Gambar 4.21 Nilai CPU dan RAM Suricata Sebelum Dilakukan Penyerangan ...70
Gambar 4.22 Nilai CPU dan RAM Suricata Setelah Dilakukan Penyerangan 70



INTISARI

Keamanan jaringan pada *web server* merupakan bagian yang paling penting untuk menjamin integritas dan layanan bagi pengguna. *Web server* sering kali menjadi target serangan yang mengakibatkan kerusakan data. Salah satunya serangan *SYN Flood* merupakan jenis serangan *Denial of Service (DOS)* yang memberikan permintaan *SYN* secara besar-besaran kepada *web server*.

Untuk memperkuat keamanan jaringan *web server* penerapan *Intrusion Detection System (IDS)* digunakan untuk mendeteksi serangan, memantau dan menganalisa serangan pada *web server*. *Software IDS* yang sering digunakan yaitu *IDS Snort* dan *IDS Suricata* yang memiliki kelebihan dan kekurangannya masing-masing.

Tujuan penelitian kali ini untuk membandingkan kedua *IDS* menggunakan sistem operasi *linux* dengan pengujian serangan menggunakan *SYN Flood* yang akan menyerang *web server* kemudian *IDS Snort* dan *Suricata* yang telah terpasang pada *web server* akan memberikan peringatan jika terjadi serangan. Dalam menentukan hasil perbandingan, digunakan parameter-parameter yang akan menjadi acuan yaitu jumlah serangan yang terdeteksi dan efektivitas deteksi serangan dari kedua *IDS* tersebut.

Kata kunci : *Intrusion Detection System*, keamanan jaringan, *Web Server*, *Snort*, *Suricata*

ABSTRACT

Network security on the web server is the most important part to guarantee the integrity and service for users. Web servers are often the target of attacks that result in data damage. One of them is the SYN Flood attack which is a type of Denial of Service (DOS) attack that gives a massive SYN request to the web server.

To strengthen the web server network security the application of Intrusion Detection System (IDS) is used to detect attacks, monitor and analyze attacks on web servers. IDS applications that are often used are IDS Snort and Suricata IDS which have their respective advantages and disadvantages.

The purpose of this study is to compare the two IDS using the Linux operating system with testing the attack using SYN Flood which will attack the web server then IDS Snort and Suricata that have been installed on the web server will give a warning if an attack occurs. In determining the results of the comparison, the parameters used will be the reference, namely the number of attacks detected and the effectiveness of attack detection from the two IDS.

KeyWords : *Intrusion Detection System, Network Security, Web Server, Snort, Suricata*