

**ANALISIS DAN IMPLEMENTASI SISTEM KEAMANAN JARINGAN
DENGAN METODE SIGNATURE-BASED MENGGUNAKAN SURICATA
PADA MIKROTIK RB951G-2HND**

SKRIPSI



disusun oleh

Herlambang Bayu Aji

16.11.0689

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2021**

**ANALISIS DAN IMPLEMENTASI SISTEM KEAMANAN JARINGAN
DENGAN METODE SIGNATURE-BASED MENGGUNAKAN SURICATA
PADA MIKROTIK RB951G-2HND**

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Informatika



disusun oleh

Herlambang Bayu Aji

16.11.0689

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

2021

PERSETUJUAN

SKRIPSI

ANALISIS DAN IMPLEMENTASI SISTEM KEAMANAN JARINGAN DENGAN METODE SIGNATURE-BASED MENGGUNAKAN SURICATA PADA MIKROTIK RB951G-2HND

yang dipersiapkan dan disusun oleh

Herlambang Bayu Aji

16.11.0689

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 24 Maret 2021

Dosen Pembimbing,

Joko Dwi Santoso, M.Kom

NIK. 190302181

PENGESAHAN

SKRIPSI

ANALISIS DAN IMPLEMENTASI SISTEM KEAMANAN JARINGAN DENGAN METODE SIGNATURE-BASED MENGGUNAKAN SURICATA PADA MIKROTIK RB951G-2HND

yang dipersiapkan dan disusun oleh

Herlambang Bayu Aji

16.11.0689

telah dipertahankan di depan Dewan Penguji
pada tanggal 20 April 2021

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Melwin Syafrizal, S.Kom., M.Eng.
NIK. 190302105

Erni Seniwati, S.Kom., M.Cs.
NIK. 190302231

Joko Dwi Santoso, M.Kom.
NIK. 190302181

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 3 Mei 2021

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta, S.Kom., M.Kom.
NIK. 190302096

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, 4 Mei 2021



Herlambang Bayu Aji

NIM. 16.11.0689

MOTTO

*“MUSUH YANG PALING BERBAHAYA DI ATAS DUNIA INI ADALAH
PENAKUT DAN BIMBANG. TEMAN YANG PALING SETIA, HANYALAH
KEBERANIAN DAN KEYAKINAN YANG TEGUH”*

(HAMKA)

*NIKMATI PROSESNYA, JALANI DAN IKUTI ARUSNYA. TERKAIT
HASIL, KITA SERAHKAN PADA YANG MAHA KUASA.*

*Allah tidak membebani seseorang itu melainkan sesuai dengan
kesanggupannya.*

(Al-Baqarah:286)

*APAPUN YANG TERJADI, TERUSLAH MELANGKAH DAN TETAP
SEMANGAT. PERCAYALAH, SEMUA AKAN BAIK-BAIK SAJA JIKA KAU
MAU MELIBATKAN TUHANMU DALAM URUSANMU.*

USAHA KERAS ITU TAK AKAN MENGKHIANATI.

(JKT48)

PERSEMBAHAN

Alhamdulillah, Puji syukur kehadiran Allah SWT yang senantiasa memberikan rahmat dan ridho kepada hamba-Nya. Shalawat serta salam kepada Nabi Muhammad SAW yang menuntun umat manusia kepada jalan yang diridhoi Allah SWT.

Dalam penulisan skripsi ini, penulis menyadari bahwa dalam proses pembuatannya tidak lepas dari peranan dan bantuan dari berbagai pihak.

Oleh karena itu, dalam kesempatan ini perkenankan penulis menyampaikan ucapan terima kasih kepada :

- 1) Kepada Ibu Supartini dan Bapak Danang Mujiantoro yang selalu memberikan doa, motivasi dan kepercayaannya kepada anaknya dalam menuntut ilmu.
- 2) Bapak Joko Dwi Santoso, M.Kom., selaku dosen pembimbing yang telah membimbing penulis dalam menyusun Skripsi ini sehingga dapat selesai dengan baik.
- 3) Teman – teman kontrakan yang sudah mensupport saya dalam menempuh pendidikan ini.
- 4) Teman – teman kelas 16 Informatika 11 atas kerjasama dan kebersamaannya.
- 5) Segenap dosen Amikom Yogyakarta yang telah memberikan ilmu yang bermanfaat.
- 6) Oshi saya Aninditha Rahma Cahyadi yang sudah memberikan semangat kepada saya dalam menyelesaikan skripsi.
- 7) Semua pihak yang tidak bias saya sebutkan satu persatu saya ucapkan terima kasih.

KATA PENGANTAR

Alhamdulillah, Segala Puji bagi Allah, Tuhan semesta alam. Syukur senantiasa Penulis ucapkan kepada Allah Yang Maha Penyayang atas petunjuk, rahmat, kasih sayang, karuniaNya penulis dapat menyelesaikan studi, penelitian dan penyusunan tesis ini, dengan judul “Analisis Dan Implementasi Sistem Keamanan Jaringan Dengan Metode Signature-Based Menggunakan Suricata Pada Mikrotik RB951G-2HND”.

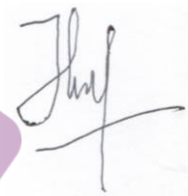
Penulis dapat menyelesaikan perkuliahan dan penulisan skripsi ini dengan usaha, bantuan bimbingan dan dorongan dari berbagai pihak. Oleh karena itu Penulis dengan segala kerendahan hati dan rasa hormat menyampaikan ucapan terima kasih yang sedalam-dalamnya kepada :

1. Bapak Prof. Dr. Mohammad Suyanto, M.M., selaku Rektor Universitas Amikom Yogyakarta
2. Bapak Hanif Al Fatta, S.Kom., M.Kom., selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta
3. Ibu Windha Mega Pradnya D, M.Kom., selaku Ketua Program Studi S1 Informatika Universitas Amikom Yogyakarta
4. Bapak Joko Dwi Santoso, M.Kom., Selaku Dosen Pembimbing yang telah memberikan bimbingan serta pengarahan dalam menyelesaikan penulisan Skripsi ini.
5. Bapak dan Ibu Dosen Universitas Amikom Yogyakarta yang telah membantu dalam proses belajar mengajar.
6. Teman-teman seperjuangan dan semua teman kelas 16 S1 Informatika 11 Universitas Amikom Yogyakarta
7. Serta semua pihak yang telah membantu dalam proses penyusunan Skripsi ini yang tidak bisa penulis sebutkan satu per satu.

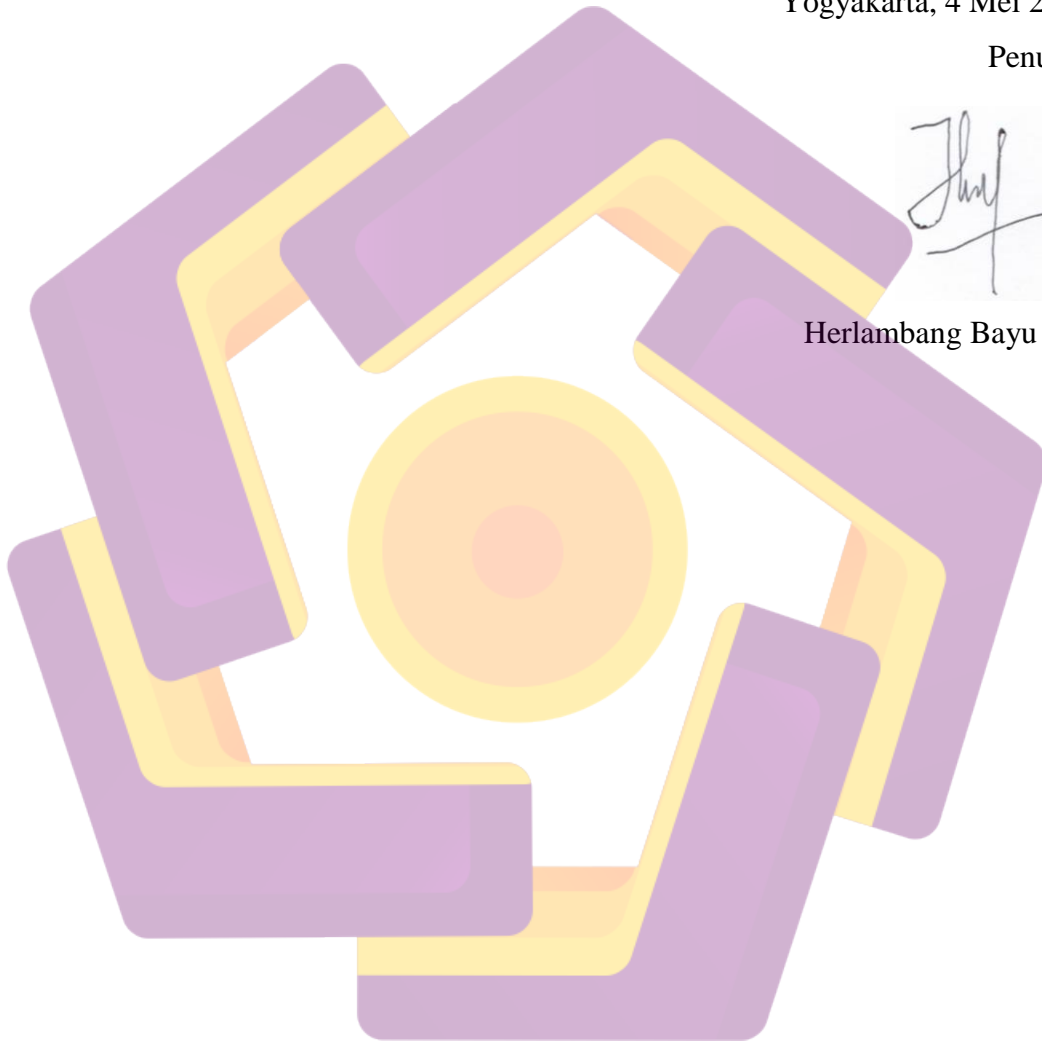
Penulis menyadari skripsi ini masih jauh dari sempurna, maka perlu masukan maupun kritikan yang membangun untuk penelitian skripsi ini. Semoga karya ini dapat bermanfaat bagi pembaca. Mohon maaf atas segala kesalahan dan kekurangan, Semoga rahmat Allah senantiasa tercurah kepada kita semua.

Yogyakarta, 4 Mei 2021

Penulis,



Herlambang Bayu Aji



DAFTAR ISI

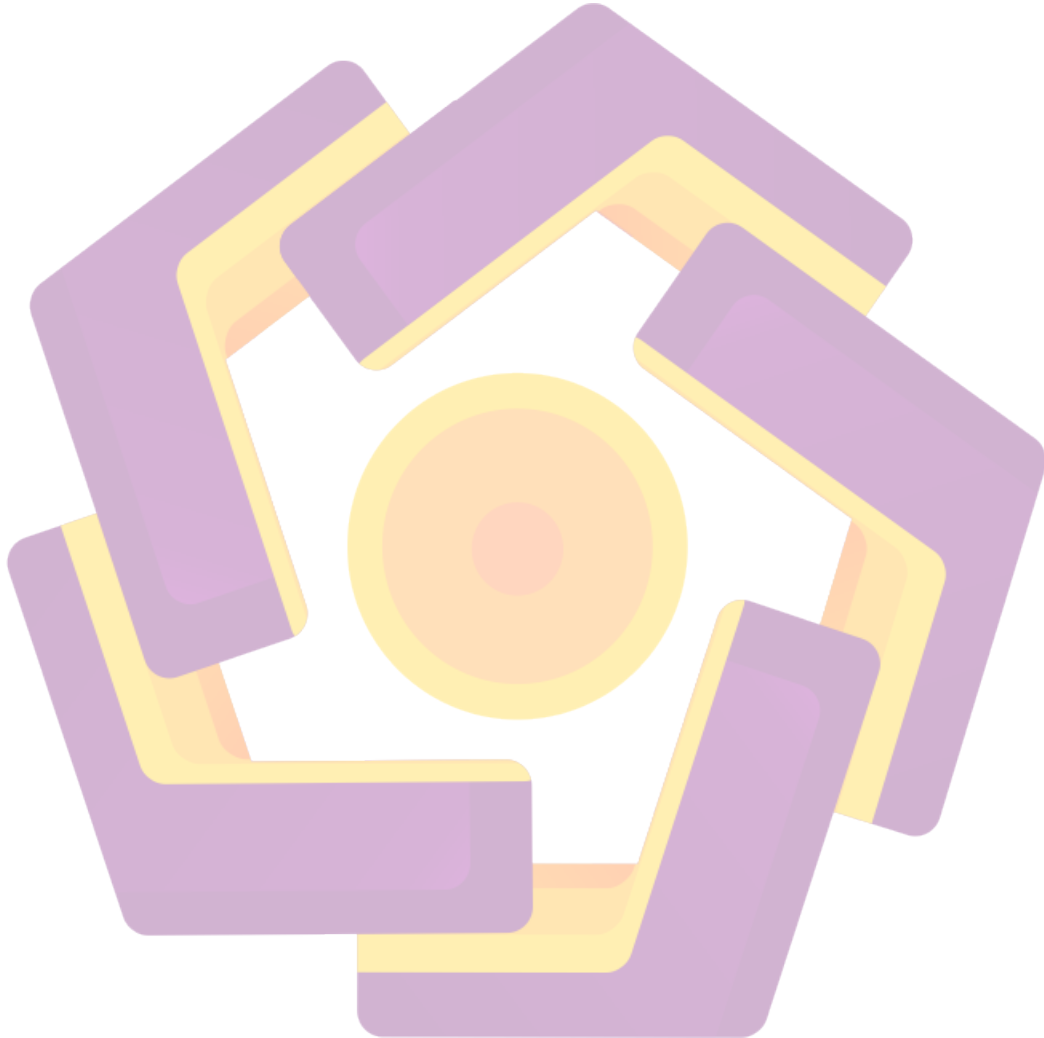
COVER	I
LEMBAR JUDUL.....	II
PERSETUJUAN.....	III
PENGESAHAN.....	IV
PERNYATAAN KEASLIAN.....	V
MOTTO	VI
PERSEMBAHAN.....	VII
KATA PENGANTAR.....	VIII
DAFTAR ISI.....	X
DAFTAR TABEL	XIII
DAFTAR GAMBAR.....	XIV
INTISARI	XVI
ABSTRACT	XVII
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah.....	3
1.4 Maksud Penelitian.....	3
1.5 Tujuan Penelitian	4
1.6 Manfaat Penelitian	4
1.7 Metode Penelitian.....	4
1.7.1 Studi Literatur	5
1.7.2 Metode Analisis	5
1.8 Sistematika Penulisan	6
BAB II LANDASAN TEORI	8
2.1 Tinjauan Pustaka	8
2.2 Definisi Jaringan Komputer	10
2.3 Topologi Jaringan.....	10
2.3.1 Topologi Bus.....	10
2.3.2 Topologi Token Ring	11
2.3.3 Topologi Ring	12
2.3.4 Topologi Star	12
2.3.5 Topologi Tree	13
2.3.6 Topologi Mesh	14
2.3.7 Topologi Peer To Peer (P2P)	14
2.4 Keamanan Jaringan	15
2.4.1 Aspek – Aspek Keamanan Komputer	15
2.4.2 Aspek – Aspek Ancaman Keamanan	16
2.5 Penyusunan Jaringan	16

2.6	Intrusion Detection System	18
2.7	Metode Analisis Event IDS	19
2.7.1	<i>Knowledge-based</i> atau <i>misuse detection (signature)</i>	19
2.7.2	<i>Behavior based (anomaly)</i>	20
2.7.3	<i>Passive Detection</i>	20
2.7.4	<i>Reactive Detection</i>	20
2.8	Tipe Intrusion Detection System (IDS)	21
2.8.1	<i>Network-based Intrusion Detection System (NIDS)</i>	21
2.8.2	<i>Host-based Intrusion Detection System (HIDS)</i>	21
2.9	Jenis Koneksi Antar Jaringan	21
2.9.1	<i>Peer To Peer</i>	21
2.9.2	<i>Client Server</i>	22
2.10	Protokol TCP/IP	22
2.11	Suricata	23
2.12	Mikrotik	23
2.12.1	<i>Routerboard</i> Mikrotik	23
2.12.2	Winbox Mikrotik	24
2.12.3	<i>Firewall</i>	24
2.12.4	Ports	25
2.13	Oracle VM VirtualBox	26
2.14	Elasticsearch	27
2.15	Kibana	27
2.16	Filebeat	28
2.17	Nmap	28
2.18	Denial of Service (DoS)	29
BAB III ANALISIS DAN PERANCANGAN		30
3.1	Identifikasi Masalah	30
3.2	Analisis Masalah	30
3.3	Hasil Analisis	32
3.4	Analisis Kebutuhan	33
3.4.1	Analisis Kebutuhan Fungsional	33
3.4.2	Analisis Kebutuhan Non-Fungsional	33
3.4.2.1	Kebutuhan Perangkat Keras	33
3.4.2.2	Kebutuhan Perangkat Lunak	36
3.4.2.3	Kebutuhan Sistem Operasi	37
3.5	Desain	38
3.5.1	Topologi Sistem	38
3.5.2	Arsitektur Sistem.....	40
3.6	Implementasi	41
3.6.1	Instalasi Sistem Operasi	41
3.6.2	Instalasi IDS Suricata	41
3.6.3	Instalasi Elasticsearch, Kibana dan Filebeat	42
3.6.4	Instalasi dan Konfigurasi Nginx	43
3.6.5	Konfigurasi <i>Outside Router</i>	45
3.6.6	Konfigurasi <i>Internal Router</i>	48
3.6.7	Konfigurasi PC Server	51

3.7	Audit Sistem Keamanan IDS Suricata	57
3.7.1	Rancangan Pengujian	55
3.7.2	Skenario Pengujian.....	58
3.7.3	Menjalankan IDS Suricata	59
3.7.2	Pengujian <i>Denial of Service</i> (DoS)	60
3.7.3	Pengujian <i>Ping Attack</i>	61
3.7.4	Pengujian <i>Port Scanning</i>	61
3.8	Evaluasi Sistem IDS Suricata	62
BAB IV HASIL DAN PEMBAHASAN		63
4.1	Hasil Penelitian dan Pembahasan	63
4.2	Hasil Pengujian <i>Firewall</i> IDS Suricata	63
4.2.1	Hasil Pengujian <i>DoS Attack</i>	63
4.2.2	Hasil Pengujian <i>Ping Attack</i>	64
4.2.3	Hasil Pengujian <i>Port Scanning</i>	65
4.3	Hasil Pengujian <i>Firewall Router</i> Mikrotik (<i>Internal Router</i>)	66
4.3.1	Hasil Pengujian Akses <i>Web Server</i>	68
4.4	Hak Akses <i>Web Server</i>	70
4.4.1	Halaman <i>Discover</i> Kibana	71
4.4.2	Halaman <i>Dashboard</i> Kibana	72
4.4.3	Halaman <i>Logs</i> Kibana	73
BAB V PENUTUP		75
5.1	Kesimpulan	75
5.2	Saran	76
DAFTAR PUSTAKA		77

DAFTAR TABEL

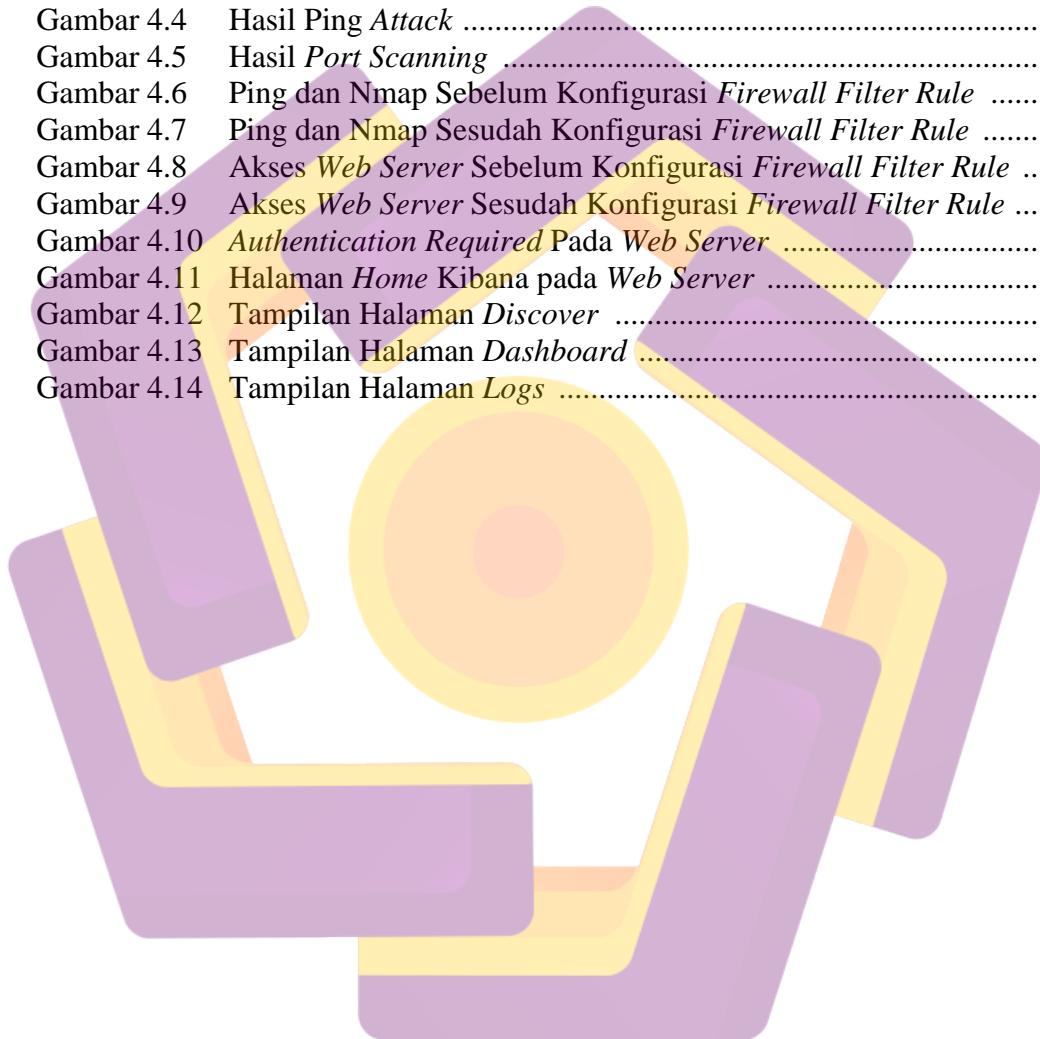
Tabel 3.1	Spesifikasi Laptop Yang Digunakan Dalam Penelitian	34
Tabel 3.2	Spesifikasi Mikrotik RB951G-2HND	35
Tabel 3.3	Desain <i>Interface</i> Skenario Jaringan	39
Tabel 3.4	Laporan Pengujian Sistem Keamanan IDS Suricata	62



DAFTAR GAMBAR

Gambar 2.1	Topologi Bus	11
Gambar 2.2	Topologi Token Ring	11
Gambar 2.3	Topologi Ring	12
Gambar 2.4	Topologi Star	13
Gambar 2.5	Topologi Tree	13
Gambar 2.6	Topologi Mesh	14
Gambar 2.7	Topologi Peer To Peer (P2P)	15
Gambar 2.8	Konsep <i>IDS</i>	19
Gambar 2.9	Logo Mikrotik	23
Gambar 2.10	Ilustrasi Firewall	24
Gambar 2.11	Logo Oracle VM VirtualBox	27
Gambar 2.12	<i>Prospector File</i>	28
Gambar 3.1	Pemantauan Trafik dan Deteksi Intrusi 2018.....	31
Gambar 3.2	Metode Security Policy Development Life Cycle (SPDLC)	33
Gambar 3.3	Mikrotik RB951G-2HND	35
Gambar 3.4	Desain Topologi Jaringan <i>IDS</i>	39
Gambar 3.5	Arsitektur Sistem <i>IDS</i>	40
Gambar 3.6	Konfigurasi <i>Interface</i> Outside Router	45
Gambar 3.7	Konfigurasi <i>IP Address</i> Outside Router	45
Gambar 3.8	Konfigurasi <i>DNS Server</i> Outside Router	46
Gambar 3.9	Konfigurasi <i>IP Route</i> Outside Router	47
Gambar 3.10	Konfigurasi <i>Firewall NAT Rule</i> Outside Router	48
Gambar 3.11	Konfigurasi <i>Interface</i> Internal Router	48
Gambar 3.12	Konfigurasi <i>IP Address</i> Internal Router	49
Gambar 3.13	Konfigurasi <i>DNS Server</i> Internal Router	50
Gambar 3.14	Konfigurasi <i>IP Route</i> Internal Router	50
Gambar 3.15	Konfigurasi <i>Firewall NAT Rule</i> Internal Router	51
Gambar 3.16	Konfigurasi <i>Firewall Filter Rules</i> Internal Router	52
Gambar 3.17	Konfigurasi <i>Web Server</i>	53
Gambar 3.18	Konfigurasi <i>SSH Server</i>	53
Gambar 3.19	Konfigurasi <i>Elasticsearch</i>	54
Gambar 3.20	Konfigurasi <i>Filebeat</i>	54
Gambar 3.21	Konfigurasi <i>Kibana</i>	55
Gambar 3.22	Konfigurasi <i>IDS Suricata</i>	55
Gambar 3.23	Konfigurasi <i>HOME_NET Suricata.yaml</i>	56
Gambar 3.24	Konfigurasi <i>Suricata Rules</i>	56
Gambar 3.25	Alur Pengujian Sistem	57
Gambar 3.26	Skenario Pengujian Serangan <i>Host</i>	58
Gambar 3.27	Skenario Pengujian Serangan <i>Client</i>	59
Gambar 3.28	Mengoperasikan <i>IDS Suricata</i>	59
Gambar 3.29	<i>TCP SYN Flood Attack</i>	60

Gambar 3.30	<i>UDP Flood Attack</i>	60
Gambar 3.31	<i>Ping Attack</i>	61
Gambar 3.32	<i>Port Scanning dengan Nmap</i>	61
Gambar 4.1	Melihat <i>log Suricata</i>	63
Gambar 4.2	Hasil <i>TCP SYN Flood Attack</i>	64
Gambar 4.3	Hasil <i>UDP Flood Attack</i>	64
Gambar 4.4	Hasil <i>Ping Attack</i>	65
Gambar 4.5	Hasil <i>Port Scanning</i>	65
Gambar 4.6	Ping dan Nmap Sebelum Konfigurasi <i>Firewall Filter Rule</i>	67
Gambar 4.7	Ping dan Nmap Sesudah Konfigurasi <i>Firewall Filter Rule</i>	68
Gambar 4.8	Akses <i>Web Server</i> Sebelum Konfigurasi <i>Firewall Filter Rule</i> ...	69
Gambar 4.9	Akses <i>Web Server</i> Sesudah Konfigurasi <i>Firewall Filter Rule</i>	69
Gambar 4.10	<i>Authentication Required</i> Pada <i>Web Server</i>	70
Gambar 4.11	Halaman <i>Home Kibana</i> pada <i>Web Server</i>	71
Gambar 4.12	Tampilan Halaman <i>Discover</i>	72
Gambar 4.13	Tampilan Halaman <i>Dashboard</i>	73
Gambar 4.14	Tampilan Halaman <i>Logs</i>	74



INTISARI

Intrusion Detection System (IDS) dapat didefinisikan sebagai kegiatan yang bersifat *anomaly, incorrect, inappropriate* yang terjadi di jaringan atau *host*. Dan IDS sendiri adalah sistem keamanan yang bekerja bersama *Firewall* untuk mengatasi *Intrusion*. IDS mampu mendeteksi penyusup dan memberikan respon secara *real time*. Terdapat dua teknik yang digunakan dalam IDS yaitu, NIDS (*Network Based Intrusion Detection System*) dan HIDS (*Host Based Intrusion Detection System*).

Pada penelitian ini IDS dibangun menggunakan perangkat lunak Suricata. Suricata merupakan *Open Source Intrusion Detection System (IDS)* yang digunakan untuk pemantauan dan pendeteksian gangguan pada jaringan komputer. Agar mempermudah administrator dalam melihat dan membaca hasil *log* dari setiap paket data yang masuk dan keluar maka menggunakan *Elasticsearch, Kibana, dan Filebeat*. Metode yang digunakan dalam penelitian ini adalah metode *Signature-based*. IDS dengan metode *Signature-based* merupakan metode dalam mendeteksi serangan pola atau paket data yang dibaca kemudian dibandingkan dengan data atau paket yang sudah tersimpan dalam *database* yang ada atau *rule* yang sudah ada. IDS berbasis *Signature-based* bekerja dengan menyadap paket yang melalui lalu lintas jaringan, kemudian membandingkan dengan pola serangan yang ada, jika paket data mempunyai pola yang sama dengan salah satu pola yang terdapat pada *rule database*, maka paket tersebut dianggap sebagai sebuah serangan.

Berdasarkan hasil pengujian IDS dengan *Router Mikrotik* sebagai *firewall* yang membantu memblock jaringan dari penyerang, diketahui bahwa metode *Signature-based* mempunyai kelebihan dalam mendeteksi jenis serangan seperti *port scanning, exploit* dan *denial of service*. Dimana hasil serangan yang disebabkan DoS dan *Port Scanning* dapat dikenali oleh Suricata IDS dan menampilkan *log* secara lengkap, baik dari waktu, tanggal kejadian dan sumber IP *Address* dari penyerang.

Kata Kunci: Keamanan Jaringan, IDS Suricata, Metode *Signature based*, Mikrotik

ABSTRACT

Intrusion Detection System (IDS) can be defined as anomalous, false, inappropriate activity that occurs on a network or host. And IDS itself is a security system that works with Firewall to overcome intrusion. IDS is able to spot intruders and respond in real time. There are two techniques used in IDS, namely, NIDS (Network Based Intrusion Detection System) and HIDS (Host Based Intrusion Detection System).

In this research, IDS was built using Suricata software. Suricata is an Open Source Intrusion Detection System (IDS) which is used for prevention and prevention of interference on computer networks. To make it easier for administrators to view and read log results from each incoming and outgoing data packet to use Elasticsearch, Kibana, and Filebeat. The method used in this research is a signature-based method. IDS with the signature-based method is a method in attack that reads patterns or data packets which are then compared with data or packets already stored in existing databases or existing rules. Signature-based IDS works by intercepting packets in network traffic, then comparing it with existing attack patterns, if the data packet has the same pattern as one of the patterns in the rules database, then the packet will be used as an attack.

Based on the results of IDS testing with the Mikrotik Router as a firewall that helps block the network from attackers, it is known that the Signature-based method has evidence of types of attacks such as port scanning, exploits and denial of service. Where the results of attacks caused by DoS and Port Scanning can be recognized by Suricata IDS and display a complete log, both from the time, date of the incident and the source IP Address of the attacker.

Keyword: Network Security, IDS Suricata, Signature based method, Mikrotik