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 kehadirat 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".

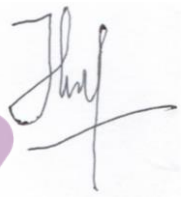
Penulis dapat menyelesaikan perkuliahan dan penulisan skripsi ini dengan usaha, bantuan bimbingan dan dorongan dari berbagai pihak. Oleh karena itu Penulis dengan segala kerendahan hati dan rasa hormat menyampaikan ucapan terima kasih yang sedalam-dalamnya kepada :

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

DAFTAR TABEL

DAFTAR GAMBAR

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 mem*block* 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*