PENDETEKSI DAN PENCEGAHAN SERANGAN JARINGAN MENGGUNAKAN *INSTRUSION DETECTION SYSTEM* (IDS) SURICATA

SKRIPSI

Diajukan untuk memenuhi sebagian persyaratan mencapai gelar SarjanaKomputer

DISUSUN OLEH :

KHAERUNNISA MARDA TILLAH

1911102441070

PROGRAM STUDI S1 TEKNIK INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS MUHAMMADIYAH KALIMANTAN TIMUR

SAMARINDA

2023

Pendeteksi dan Pencegahan Serangan Jaringan Menggunakan *Instrusion Detection System* (IDS) Suricata

Skripsi

Diajukan untuk memenuhi sebagian persyaratan mencapai gelar SarjanaKomputer

Disusun Oleh :

Khaerunnisa Marda Tillah

1911102441070

PROGRAM STUDI S1 TEKNIK INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS MUHAMMADIYAH KALIMANTAN TIMUR

SAMARINDA

2023

HALAMAN PENGESAHAN

PENDETEKSI DAN PENCEGAHAN SERANGAN JARINGAN MENGGUNAKAN *INSTRUSION DETECTION SYSTEM* (IDS) SURICATA

DISUSUN OLEH :

KHAERUNNISA MARDA TILLAH

1911102441070

Telah melaksanakan ujian skripsi dan dinyatakan lulus,

Pada tanggal 4 Juli 2023

Dosen Pembimbing	Penguji
Faldi, S.Kom.,M,Ti	Muhammad Taufiq Sumadi, S.Tr.Kom., M.Tr.Kom
NIDN. 1121079101	NIDN. 1111089501

Dekan	Ketua Program Studi
Prof. Ir.Sarjito, MT., Ph.D	Asslia Johar Latipah, M.Cs
NIDN. 0610116204	NIDN. 1124098902

PERNYATAAN KEASLIAN SKRIPSI

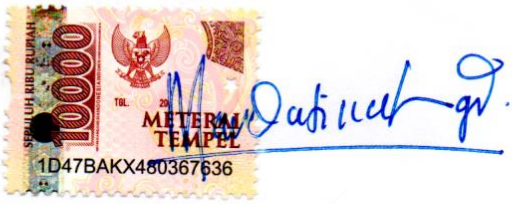
Saya yang bertanda tangan di bawah ini :

Nama	:	Khaerunnisa Marda Tillah
NIM	:	1911102441070
Program Studi	:	S1 Teknik Informatika
Judul Penelitian	:	PENDETEKSI DAN PENCEGAHAN SERANGAN JARINGAN MENGGUNAKAN *INSTRUSION DETECTION SYSTEM* (IDS) SURICATA.

Menyatakan bahwa penelitian yang saya tulis ini benar-benar hasil karya saya sendiri, bukan merupakan pengambil alihan tulisan atau pikiran orang lain yang saya akui sebagai tulisan atau pikiran saya sendiri.

Apabila dikemudian hari dapat dibuktikan bahwa terdapat plagiat dalam penelitian ini, maka saya bersedia menerima sanksi sesuai ketentuan perundang-undangan (Permendiknas No.17, tahun 2010).

Samarinda, 23 Juni 2023



Khaerunnisa Marda Tillah

1911102441070

PRAKATA

Alhamdulillah dengan memanjatkan puji syukur kehadirat Allah SWT yang telah memberikan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan penelitian dan penulisan Skripsi ini dengan tepat waktu. Dengan judul "Pendeteksi dan Pencegahan Serangan Jaringan Menggunakan *Instrusion Detection System* (IDS) Suricata " penulis bertujuan untuk memenuhi salah satu persyaratan bagi mahasiswa untuk bisa menyelesaikan pendidikan pada Program Studi Teknik Informatika Fakultas Sains dan Teknologi Universitas Muhammadiyah Kalimantan Timur.

Penulis menyampaikan terima kasih kepada beberapa pihak yang ikut mendukung serta membimbing dalam proses penelitian dan penulisan Skripsi ini hingga selesai. Yaitu :

1. Andriani dan Sadaruddin sebagai orang tua tercinta yang selalu mendoakan, memberi motivasi, dan bekerja keras untuk menyelesaikan Pendidikan penulis.
2. Suami tercinta penulis, Deny Amnur yang memotivasi penulis untuk selalu semangat dan pantang menyerah dalam menyelesaikan penelitian dan penulisan Skripsi.
3. Faldi, S.Kom., M.TI, selaku Dosen Pembimbing yang telah secara profesional dan kooperatif memberikan arahan dan petunjuk kepada penulis.
4. Muhammad Taufiq Sumadi, S.Tr.Kom., M.Tr.Kom yang telah menjadi penguji dalam seminar proposal penelitian dan sidang skripsi penulis.
5. Asslia Johar Latipah, M.Cs., selaku Ketua Program Studi S1 Teknik Informatika Universitas Muhammadiyah Kalimantan Timur.
6. Prof. Ir. Sarjito, M.T., Ph.D., selaku Dekan Fakultas Sains & Teknologi Universitas Muhammadiyah Kalimantan Timur.
7. Prof. Dr. H. Bambang Setiaji, selaku Rektor Universitas Muhammadiyah Kalimantan Timur.

8. Suci Mawaddah, Trisha NurHalisha, dan Dinamita Romadoni selaku sahabat dari penulis yang selalu supportif dan menemani penulis dalam keadaan apapun.
9. Serta semua pihak yang tidak dapat disebutkan satu persatu telah membantu penulis dalam menyelesaikan penelitian dan penyusunan Skripsi ini.

Semoga semua dukungan yang diberikan mendapat balasan dari Allah SWT. Penulis berharap penulisan Skripsi ini dapat memberikan kesan yang bagus dan bermanfaat kepada pembaca.

Samarinda, 23 Juni 2023

Penulis

ABSTRAK

Serangan jaringan merupakan ancaman yang serius dalam lingkungan akademik. Untuk melindungi jaringan dari serangan, diperlukan sistem yang mampu mendeteksi dan mencegah serangan tersebut. Penelitian ini bertujuan mengembangkan dan mengimplementasikan *Intrusion Detection System* (IDS) Suricata untuk mendeteksi dan mencegah serangan jaringan. Penelitian ini menggunakan metode *Security Policy Development Life Cycle* (SPDLC) dengan tahapan analisis kebutuhan, perancangan sistem IDS, implementasi IDS pada jaringan, serta pengujian dan evaluasi sistem IDS yang dikembangkan. Hasil analisis dari penelitian ini menunjukkan bahwa IDS Suricata mampu mendeteksi serangan *Slowloris, Nmap Scan, Denial of Service* (D0S), dan *PingFlood*. Waktu yang diperlukan untuk mendeteksi serangan *Slowloris* adalah 3 menit, sedangkan untuk serangan *Nmap Scan,* DoS, dan *PingFlood* terdeteksi *real-time.* IDS Suricata bekerja dengan baik dalam mendeteksi paket-paket ancaman, perbedaan waktu dalam deteksi serangan bervariasi dikarenakan setiap serangan memiliki karakteristik yang berbeda.

Kata kunci : *Instrusion Detection System* (IDS) Suricata, *Security Policy Development Life Cycle* (SPDLC), *SLowloris, Nmap Scan, Denial of Service* (DoS), *PingFlood.*

ABSTRACT

Network attacks pose a serious threat in academic environments. To protect the network from such attacks, a system capable of detecting and preventing them is needed. This research aims to develop and implement Suricata Intrusion Detection System (IDS) to detect and prevent network attacks. The research utilizes the Security Policy Development Life Cycle (SPDLC) method, involving stages such as requirement analysis, IDS system design, IDS implementation on the network, and testing and evaluation of the developed IDS system. The analysis results of this research show that Suricata IDS is capable of detecting Slowloris, Nmap Scan, Denial of Service (DoS), and PingFlood attacks. The detection time for Slowloris attack is 3 minutes, while real-time detection is achieved for Nmap Scan, DoS, and PingFlood attacks. Suricata IDS performs well in detecting threat packets, and the variation in detection time for different attacks is due to their distinct characteristics.

Keywords: Intrusion Detection System (IDS) Suricata, Security Policy Development Life Cycle (SPDLC), Slowloris, Nmap Scan, Denial of Service (DoS), PingFlood.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN