



**ANALISIS DAN IMPLEMENTASI SISTEM KEAMANAN
JARINGAN MENGGUNAKAN METODE IDPS (INTRUSION
DETECTION DAN PREVENTION SYSTEM) BERBASIS
SNORT
(Studi Kasus : SMK Cengkareng 1 Jakarta)**

LAPORAN TUGAS AKHIR

MUHAMMAD DENNY SETIAWAN

41520010213

**UNIVERSITAS
MERCU BUANA**

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS MERCU BUANA

JAKARTA

2024



**ANALISIS DAN IMPLEMENTASI SISTEM KEAMANAN
JARINGAN MENGGUNAKAN METODE IDPS (INTRUSION
DETECTION DAN PREVENTION SYSTEM) BERBASIS
SNORT**

(Studi Kasus : SMK Cengkareng 1 Jakarta)

LAPORAN TUGAS AKHIR

MUHAMMAD DENNY SETIAWAN

41520010213

**UNIVERSITAS
MERCU BUANA**

Diajukan sebagai salah satu syarat untuk memperoleh gelar sarjana

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA**

2024

HALAMAN PERNYATAAN KARYA SENDIRI

Saya yang bertanda tangan di bawah ini:

Nama : Muhammad Denny Setiawan
NIM : 41520010213
Program Studi : Teknik Informatika
Judul Laporan Skripsi : ANALISIS DAN IMPLEMENTASI SISTEM KEAMANAN JARINGAN MENGGUNAKAN METODE IDPS (*INTRUSION DETECTION DAN PREVENTION SYSTEM*) BERBASIS SNORT (Studi Kasus : SMK Cengkareng 1 Jakarta).

Menyatakan bahwa Laporan Skripsi ini adalah hasil karya sendiri dan bukan plagiat, serta semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar. Apabila ternyata ditemukan di dalam Laporan Skripsi saya terdapat unsur plagiat, maka saya siap mendapatkan sanksi akademis yang berlaku di Universitas Mercu Buana.

UNIVERSITAS
MERCU BUANA

Jakarta, 14 Juli 2024



Muhammad Denny Setiawan

HALAMAN PENGESAHAN

Laporan Skripsi ini diajukan oleh :

Nama : Muhammad Denny Setiawan

NIM : 41520010213

Program Studi : Teknik Informatika

Judul Laporan Skripsi : Analisis dan Implementasi Sistem Keamanan Jaringan Menggunakan Metode IDPS (Intrusion Detection dan Prevention System) Berbasis Snort (Studi Kasus : SMK Cengkareng 1 Jakarta)

Telah berhasil dipertahankan pada sidang di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar sarjana Strata I pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Disahkan oleh:

Pembimbing : Dr. Harwikarya, M.T

NIDN : 014075805

Ketua Penguji : Prastika Indriyanti, S.Kom., M.Cs

NIDN : 0312089401

Penguji 1 : Muhammad Rifqi, S.Kom., M.Kom

NIDN : 0301067101

Penguji 2 : Dr. Misbahul Fajri, M.TI

NIDN : 0306077203

Jakarta, 19 Juli2024

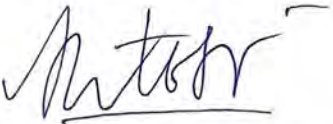
Mengetahui,

Dekan

Ketua Program Studi


Dr. Bambang Jokonowo, S.Si., M.T.I

NIDN : 0320037002


Dr. Hadi Santoso, S.Kom, M.Kom

NIDN : 0225067701

KATA PENGANTAR

Puji syukur saya panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat dan Rahmat-Nya, saya dapat menyelesaikan Proposal Penelitian ini. Penulisan Proposal Penelitian ini dilakukan dalam rangka memenuhi salah satu syarat untuk disidangkan pada seminar proposal. Saya menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan skripsi ini, sangatlah sulit bagi saya untuk menyelesaikan Laporan MPTI ini. Oleh karena itu, saya mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. Ir. Andi Adriansyah, M.Eng selaku Rektor Universitas Mercu Buana
2. Bapak Dr. Bambang Jokonowo, S.Si, MTI selaku Dekan Fakultas Ilmu Komputer
3. Bapak Dr. Hadi Santoso, S.Kom, M.Kom selaku Kepala Program Studi Teknik Informatika
4. Bapak Dr. Harwikarya., MT selaku Dosen Pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan saya dalam penyusunan MPTI ini.
5. Kepada orang tua saya yang telah memberikan dukungan serta motivasi agar saya bisa menjadi sarjana yang terbaik.
6. Kepada keluarga dan teman-teman serta semua pihak yang tidak dapat penulis sebutkan satu persatu.

Akhir kata, saya berharap Tuhan Yang Maha Esa berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga Proposal Penelitian ini membawa manfaat bagi pengembangan ilmu.

Jakarta, 14 Juli 2024



Muhammad Denny Setiawan

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Saya yang bertanda tangan di bawah ini:

Nama : Muhammad Denny Setiawan
NIM : 41520010213
Program Studi : Teknik Informatika
Judul Laporan Skripsi : ANALISIS DAN IMPLEMENTASI SISTEM KEAMANAN JARINGAN MENGGUNAKAN METODE IDPS (INTRUSION DETECTION DAN PREVENTION SYSTEM) BERBASIS SNORT (Studi Kasus : SMK Cengkareng 1 Jakarta).

Demi pengembangan ilmu pengetahuan, dengan ini memberikan izin dan menyetujui untuk memberikan kepada Universitas Mercu Buana Hak Bebas Royalti Non-Eksklusif (Non-exclusive Royalty-Free Right) atas karya ilmiah saya yang berjudul di atas beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksklusif ini Universitas Mercu Buana berhak menyimpan, mengalihmedia/format-kan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan Laporan Magang/Skripsi/Tesis/Disertasi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

UNIVERSITAS
MERCU BUANA

Jakarta, 14 Juli 2024

Yang menyatakan,



Muhammad Denny Setiawan

ABSTRAK

Nama : Muhammad Denny Setiawan
NIM : 41520010213
Program Studi : Teknik Informatika
Judul Proposal Penelitian : Analisis dan Implementasi Sistem Keamanan Jaringan Menggunakan Metode IDPS (Intrusion Detection dan Prevention System) Berbasis Snort (Studi Kasus : SMK Cengkareng 1 Jakarta)
Pembimbing : Dr. Harwikarya., MT

Teknologi informasi mengalami kemajuan pesat di era globalisasi, memberikan dampak positif pada peningkatan kinerja sistem dan pengelolaan yang lebih efisien. Namun, kemajuan ini juga membawa tantangan serius terutama terkait dengan serangan siber. Statistik BSSN Indonesia tahun 2022 mencatat penurunan anomali serangan siber sebesar 40%, namun risiko Network Scanning, DDoS, dan Brute Force masih meningkat. Server merupakan elemen kunci dalam sebuah jaringan, yang menjadi target utama serangan. Oleh karena itu, perlindungan server menjadi krusial, dan salah satu pendekatan yang efektif adalah dengan mengimplementasikan Intrusion Detection and Prevention System (IDPS). Intrusion Detection and Prevention System (IDPS) merupakan jenis metode untuk keamanan jaringan dengan memantau aktivitas yang tidak diinginkan sehingga dapat mengganggu konektivitas jaringan IDPS dapat mengambil tindakan segera untuk mencegah aktivitas tersebut. Snort merupakan sebuah perangkat lunak deteksi intrusi dan sistem pencegahan yang efektif digunakan dalam memantau data lalu lintas jaringan dan mencegah serangan yang berpotensi merugikan. Snort diintegrasikan dengan Splunk sebagai alat analisis log data serangan, agar dapat memudahkan administrator dalam membaca log. Implementasi ini menunjukkan bahwa Snort, iptables, dan Splunk bekerja dengan baik dalam memberikan perlindungan dan analisis terhadap serangan siber, memastikan keamanan jaringan yang lebih baik.

Kata Kunci : *Intrusion Detection and Prevention System (IDPS), Snort, Splunk, Keamanan Jaringan, Serangan Siber*

ABSTRACT

Nama : Muhammad Denny Setiawan
NIM : 41520010213
Study Program : Teknik Informatika
Title Research Proposal : Analisis dan Implementasi Sistem Keamanan Jaringan Menggunakan Metode IDPS (Intrusion Detection dan Prevention System) Berbasis Snort (Studi Kasus : SMK Cengkareng 1 Jakarta)
Pembimbing : Dr. Harwikarya., MT

Information technology has advanced rapidly in the era of globalization, positively impacting system performance and more efficient management. However, this progress also brings serious challenges, particularly concerning cyber attacks. BSSN Indonesia's statistics for 2022 recorded a 40% decrease in cyber attack anomalies, but the risks of Network Scanning, DDoS, and Brute Force attacks are still increasing. Servers are a key element in a network and the primary target of attacks. Therefore, server protection is crucial, and one effective approach is implementing an Intrusion Detection and Prevention System (IDPS). An IDPS is a method for network security that monitors unwanted activities that can disrupt network connectivity and takes immediate action to prevent such activities. Snort is an effective intrusion detection and prevention software used to monitor network traffic data and prevent potentially harmful attacks. Snort is integrated with Splunk as a log data analysis tool, making it easier for administrators to read logs. This implementation demonstrates that Snort, iptables, and Splunk work well in providing protection and analysis against cyber attacks, ensuring better network security.

Keywords: *Intrusion Detection and Prevention System (IDPS), Snort, Splunk, Network Security, Cyber Attacks*

DAFTAR ISI

HALAMAN PERNYATAAN KARYA SENDIRI	ii
HALAMAN PENGESAHAN	iii
KATA PENGANTAR	iv
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS	v
ABSTRAK	vi
ABSTRACT	vii
DAFTAR ISI	viii
DAFTAR TABEL	x
DAFTAR GAMBAR	xi
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Tujuan dan Manfaat	3
1.3.1 Tujuan	3
1.3.2 Manfaat	3
1.4 Batasan Penelitian	4
1.5 Sistematika Penulisan	4
BAB II TINJAUAN PUSTAKA	6
2.1 Teori Utama	6
2.1.1 Keamanan Jaringan	6
2.1.2 Jenis – Jenis Ancaman Keamanan Jaringan	6
2.1.3 Intrusion Prevention System (IPS)	8
2.1.4 Intrusion Detection System (IDS)	9
2.2 Teori Pendukung	11
2.2.1 Snort	11
2.2.2 Splunk	11
2.2.3 Virtual Box	12
2.2.4 Firewall	12
2.2.5 IPTables	12
2.3 Penelitian Terdahulu	13

BAB III METODE PENELITIAN	25
3.1 Jenis Penelitian	25
3.2 Tahapan Penelitian.....	28
3.2.1 Studi Literatur	29
3.2.2 Analisis Sistem.....	29
3.2.3 Analisa Kebutuhan	30
3.2.4 Perancangan Sistem	31
3.2.5 Instalasi	32
3.2.6 Simulasi Pengujian.....	33
3.2.7 Hasil Pengujian	34
3.2.8 Analisis Hasil Pengujian	34
3.2.9 Pembuatan Laporan Akhir	35
BAB IV HASIL DAN PEMBAHASAN	36
4.1 Konfigurasi	36
4.1.1 Topologi	36
4.1.2 Konfigurasi VMWare.....	37
4.1.3 Instalasi Ubuntu Server di VMware.....	38
4.1.4 Snort	43
4.1.5 Splunk	50
4.1.6 Konfigurasi IPTables	54
4.2 Hasil Pengujian Sistem.....	56
4.2.1 Pengujian Pertama.....	56
4.2.2 Pengujian Kedua	60
4.2.3 Pengujian Ketiga	64
4.2.4 Pengujian Keempat	68
4.2.5 Pengujian Kelima	72
4.2.6 Pengujian Keenam	76
4.3 Analisis Hasil Pengujian	79
BAB V KESIMPULAN DAN SARAN	82
5.1 Kesimpulan.....	82
5.2 Saran	82
DAFTAR PUSTAKA	84
LAMPIRAN.....	86

DAFTAR TABEL

Tabel 2. 1 Penelitian Terdahulu	13
Tabel 3. 1 Detai Perangkat Keras (Hardware)	30
Tabel 3. 2 Detail Perangkat Lunak (Software).....	31
Tabel 4. 1 Hasil Keseluruhan Pengujian Skenario 1 sampai 5.....	80
Tabel 4. 2 Hasil Pengujian Skenario 6	81



DAFTAR GAMBAR

Gambar 1. 1 Grafik Traffic Anomali	1
Gambar 1. 2 Topologi Jaringan SMK Cengkareng 1 Jakarta	3
Gambar 2. 1 Intrusion Prevention System	8
Gambar 2. 2 Intrusion Detection System.....	9
Gambar 3. 1 Metode NDLC	25
Gambar 3. 2 Tahapan Penelitian	29
Gambar 3. 3 Server IDPS	30
Gambar 4. 1 Topologi jaringan (Sebelum adanya IDPS)	36
Gambar 4. 2 Topologi jaringan (Setelah adanya IDPS)	37
Gambar 4. 3 Langkah instalasi Ubuntu Server	38
Gambar 4. 4 Website Ubuntu (Download)	39
Gambar 4. 5 File ISO Ubuntu Server	39
Gambar 4. 6 Penambahan File ISO Ubuntu Server	40
Gambar 4. 7 Disk Capacity.....	40
Gambar 4. 8 Spesifikasi VM Ubuntu Server	41
Gambar 4. 9 Hasil Ubuntu Server Setelah Ditambahkan	41
Gambar 4. 10 Proses instalasi Ubuntu Server	42
Gambar 4. 11 Tampilan Ubuntu Server	43
Gambar 4. 12 Hasil Snort Version Setelah Diinstal.....	47
Gambar 4. 13 Rules Snort.....	48
Gambar 4. 14 Konfigurasi Service Snort.....	50
Gambar 4. 15 Status Service Snort	50
Gambar 4. 16 Website Download Splunk.....	51
Gambar 4. 17 Proses Download Splunk	51
Gambar 4. 18 File Deb Splunk	52
Gambar 4. 19 Proses Instalasi Splunk	52
Gambar 4. 20 Tampilan Awal Web Splunk.....	53
Gambar 4. 21 Instalasi Snort JSON Alerts	53

Gambar 4. 22 Konfigurasi Service IPTables	56
Gambar 4. 23 Status Service IPTables.....	56
Gambar 4. 24 Resources CPU sebelum terjadi serangan DDoS (Pengujian Pertama).....	57
Gambar 4. 25 Pengujian Pertama DDoS	57
Gambar 4. 26 Hasil Resources CPU (Pengujian Pertama).....	58
Gambar 4. 27 Hasil Log Splunk DDoS (Pengujian Pertama)	58
Gambar 4. 28 Hasil Port Scanning (Pengujian Pertama).....	59
Gambar 4. 29 Hasil Log Splunk Port Scanning (Pengujian Pertama).....	59
Gambar 4. 30 Hasil Brute Force (Pengujian Pertama)	60
Gambar 4. 31 Hasil Log Splunk Brute Force (Pengujian Pertama)	60
Gambar 4. 32 Resources CPU sebelum terjadi serangan DDoS (Pengujian Kedua).....	61
Gambar 4. 33 Pengujian Kedua DDoS	61
Gambar 4. 34 Hasil Resources CPU (Pengujian Kedua).....	61
Gambar 4. 35 Hasil Log Splunk DDoS (Pengujian Kedua)	62
Gambar 4. 36 Hasil Port Scanning (Pengujian Kedua)	62
Gambar 4. 37 Hasil Log Splunk Port Scanning (Pengujian Kedua)	63
Gambar 4. 38 Hasil Brute Force (Pengujian Kedua).....	63
Gambar 4. 39 Hasil Log Splunk Brute Force (Pengujian Kedua).....	64
Gambar 4. 40 Resources CPU sebelum terjadi serangan DDoS (Pengujian Ketiga)	64
Gambar 4. 41 Pengujian Ketiga DDoS.....	65
Gambar 4. 42 Hasil Resources CPU (Pengujian Ketiga)	65
Gambar 4. 43 Hasil Log Splunk DDoS (Pengujian Ketiga).....	66
Gambar 4. 44 Hasil Port Scanning (Pengujian Ketiga)	66
Gambar 4. 45 Hasil Log Splunk Port Scanning (Pengujian Ketiga)	67
Gambar 4. 46 Hasil Brute Force (Pengujian Ketiga).....	67
Gambar 4. 47 Hasil Log Splunk Brute Force (Pengujian Ketiga).....	68
Gambar 4. 48 Resources CPU sebelum terjadi serangan DDoS (Pengujian Keempat).....	68

Gambar 4. 49 Pengujian Keempat DDoS	69
Gambar 4. 50 Hasil Resources CPU (Pengujian Keempat).....	69
Gambar 4. 51 Hasil Log Splunk DDoS (Pengujian Keempat)	70
Gambar 4. 52 Hasil Port Scanning (Pengujian Keempat)	70
Gambar 4. 53 Hasil Log Splunk Port Scanning (Pengujian Keempat)	71
Gambar 4. 54 Hasil Brute Force (Pengujian Keempat).....	71
Gambar 4. 55 Hasil Log Splunk Brute Force (Pengujian Keempat).....	72
Gambar 4. 56 Resources CPU sebelum terjadi serangan DDoS (Pengujian Kelima)	72
Gambar 4. 57 Pengujian Kelima DDoS.....	73
Gambar 4. 58 Hasil Resources CPU (Pengujian Kelima)	73
Gambar 4. 59 Hasil Log Splunk DDoS (Pengujian Kelima).....	74
Gambar 4. 60 Hasil Port Scanning (Pengujian Kelima).....	74
Gambar 4. 61 Hasil Log Splunk Port Scanning (Pengujian Kelima)	75
Gambar 4. 62 Hasil Brute Force (Pengujian Kelima)	75
Gambar 4. 63 Hasil Log Splunk Brute Force (Pengujian Kelima).....	76
Gambar 4. 64 Pengujian Keenam DDoS	77
Gambar 4. 65 Hasil Resources CPU (Pengujian Keenam).....	77
Gambar 4. 66 Hasil Port Scanning (Pengujian Keenam)	78
Gambar 4. 67 Hasil Brute Force (Pengujian Keenam).....	78