



**ANALISA *INTRUSION DETECTION SYSTEM* DENGAN
METODE *ANOMALY BASED* TERHADAP SERANGAN *SIBER***

SKRIPSI

Muammar Fadhlurrohman

1710511038

PROGRAM STUDI INFORMATIKA, PROGRAM SARJANA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

2021



**ANALISA *INTRUSION DETECTION SYSTEM* DENGAN
METODE *ANOMALY BASED* TERHADAP SERANGAN *SIBER***

SKRIPSI

Muammar Fadhlurrohman

1710511038

PROGRAM STUDI INFORMATIKA, PROGRAM SARJANA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

2021

PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri, dan semua sumber yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama : Muammar Fadhlurrohman

NIM 1710511038

Tanggal : 27 Juni 2021

Bilamana di kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Tangerang, 27 Juni 2021
Yang Menyatakan,



(Muammar Fadhlurrohman)

**PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK
KEPENTINGAN AKADEMIS**

Sebagai civitas akademik Universitas Pembangunan Nasional Veteran Jakarta, saya yang bertanda tangan dibawah ini:

Nama : Muammar Fadhlurrohman
NIM 1710511038
Fakultas : Ilmu Komputer
Program Studi : Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti NonEklusif (Non-Exclusive Royalty Free Right) atas karya ilmiah saya yang berjudul:

***ANALISA INTRUSION DETECTION SYSTEM DENGAN METODE
ANOMALY BASED TERHADAP SERANGAN SIBER***

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan Skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di :Tangerang
Pada Tanggal : 27 Juni 2021
Yang Menyatakan,



(Muammar Fadhlurrohman)

LEMBAR PERSETUJUAN

Dengan ini menyatakan bahwa proposal berikut:

Nama : Muammar Fadhlurrohman

NIM 1710511038

Program Studi : Informatika

Judul : Analisa Intrusion Detection System dengan Metode Anomaly Based terhadap Serangan Siber

Sebagai bagian persyaratan yang diperlukan untuk mengikuti ujian Skripsi pada Program Studi Informatika Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.

Menyetujui,

Dosen Pembimbing 1

Anita Muliawati, S.Kom., MTI.

Dosen Pembimbing 2

Bayu Hananto, S.Kom., M.Kom.

Mengetahui,

Ketua Program Studi

Yuni Widiastiwi, S.Kom., Msi

Ditetapkan : Jakarta

Tanggal Persetujuan : 1 Juli 2021

PENGESAHAN

Dengan ini dinyatakan bahwa Tugas Akhir berikut :

Nama : Muammar Fadhlurrohman

NIM 1710511038

Program Studi : Informatika


Judul Tugas Akhir : Analisa Intrusion Detection System dengan Metode Anomaly Based terhadap Serangan Siber

Telah berhasil dipertahankan di hadapan Tim Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi Informatika Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.

Henki Bayu Seta, S.Kom., MTI
Ketua Penguji

I Wayan Widi P, S.Kom., MTI
Anggota Penguji

Anita Muliawati, S.Kom., MTI
Pembimbing 1



Batu Hananto, S.Kom., M.Kom.
Pembimbing 2



Dr. Ermatita, M.Kom.
Dekan

Yuni Widiastiwi, S.Kom., Msi.
Ketua Program Studi

Ditetapkan di : Jakarta
Tanggal Pengesahan : 10 Agustus 2021



ANALISA INTRUSION DETECTION SYSTEM DENGAN METODE ANOMALY BASED TERHADAP SERANGAN SIBER

Muammar Fadhlurrohman

ABSTRAK

Intrusion Detection System merupakan sebuah sistem yang melakukan pengawasan terhadap traffic jaringan dan terhadap kegiatan-kegiatan yang mencurigakan atau yang membahayakan didalam sistem jaringan. Untuk mengetahui efektivitas penggunaan *Intrusion Detection System* terhadap serangan siber, perlu diketahui bagaimana cara IDS tersebut dapat mendeteksi adanya sebuah serangan. Salah satu teknik pendeteksian IDS adalah pendeteksian anomaly. Teknik ini melibatkan pola lalu lintas sebuah serangan yang sedang dilakukan oleh penyerang dengan membandingkan kegiatan yang sedang dipantau dengan kegiatan normal untuk mendeteksi adanya sebuah kejanggalan. Berdasarkan hasil penelitian *Intrusion detection system* dapat mendeteksi 72 dari 175 serangan. Hal itu dikarenakan, pendeteksian anomaly memerlukan perubahan traffic yang sangat signifikan pada saat aktivitas normal dengan aktivitas saat terjadinya serangan, sehingga *Intrusion Detection System* menganggap adanya sebuah anomaly pada jaringan tersebut dan dapat mendeteksi adanya sebuah percobaan serangan

Kata Kunci : *Intrusion detection system, anomaly*

ANALYSIS OF INTRUSION DETECTION SYSTEM WITH ANOMALY BASED AGAINST CYBER ATTACKS

Muammar Fadhlurrohman

ABSTRACT

Intrusion Detection System is a system that conducts surveillance of network traffic and against suspicious or harmful activities in the network system. To know the effectiveness of using the Intrusion Detection System against cyberattacks, it is necessary to know how the IDS can detect the presence of an attack. One of IDS detection techniques is anomaly detection. This technique involves the traffic pattern of an attack being carried out by an attacker by comparing the activities being monitored with normal activities to detect any irregularities. Based on the results of the study Intrusion detection system can detect 72 out of 175 attacks. That's because anomaly detection requires a very significant change in traffic during normal activity with activity at the time of an attack, so the Intrusion Detection System considers an anomaly on the network and can detect an attempted attack.

Keywords : *Intrusion detection system, anomaly*

KATA PENGANTAR

Penulis ucapkan puji syukur atas kehadiran Allah S.W.T karena atas nikmat dan rezeki-Nya, penulis dapat menyelesaikan skripsi di pertengahan masa Covid-19 ini. Adapun judul skripsi ini adalah:

ANALISA INTRUSION DETECTION SYSTEM DENGAN METODE ANOMALY BASED TERHADAP SERANGAN SIBER

Selanjutnya ucapan terima kasih yang sebesar-besarnya juga ingin penulis berikan kepada pihak-pihak yang selalu sabar untuk menemani, membimbing, serta memberi saran terbaik yang mana tanpa kehadiran mereka, penulisan naskah skripsi ini tidak akan pernah selesai seperti sekarang ini. Adapun pihak terkait antara lain:

1. Kedua orang tua yang telah memberi dukungan dan semangat serta mendoakan penulis agar dapat menyelesaikan naskah skripsi ini tanpa kendala.
2. Ibu Anita Muliawati, S.Kom., MTI selaku dosen pembimbing satu yang membimbing penulis dalam menyusun naskah skripsi ini.
3. Bapak Bayu Hananto, S.Kom., M.Kom selaku dosen pembimbing dua yang juga telah membimbing dalam penulisan naskah skripsi ini.
4. Henki Bayu Seta, S.Kom., MTI selaku dosen penguji yang telah memberi arahan dan saran komprehensif.
5. Bapak I Wayan Widi P., S.Kom., MTI selaku dosen penguji yang telah memberi arahan dan saran komprehensif.
6. Bapak/Ibu dosen Informatika Universitas Pembangunan Nasional Veteran Jakarta yang telah memberi ilmu yang banyak dan bermanfaat.
7. Teman-teman semua yang sudah memberikan motivasi serta membantu dalam diskusi tentang tugas akhir.

Kemudian penulis juga menyadari bahwa penyusunan skripsi ini masih jauh dari kata sempurna, namun penulis berharap agar pihak yang membaca naskah ini mendapatkan ilmu yang dapat digunakan kelak. Dan penulis juga berharap atas kritik dan saran yang konstruktif dari pembaca.

Akhir kata, semoga Allah S.W.T memberi balasan yang berlipat ganda atas kebaikan dan jasa kepada semua pihak yang turut membantu penyelesaian naskah skripsi ini. Semoga tujuan daripada penulisan skripsi ini dapat tercapai sesuai dengan harapan.

DAFTAR ISI

PERNYATAAN ORISINALITAS	ii
PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS	iii
LEMBAR PERSETUJUAN	iv
PENGESAHAN	v
ABSTRAK	vi
ABSTRACT	vii
KATA PENGANTAR	viii
DAFTAR ISI	x
DAFTAR GAMBAR	xiii
DAFTAR TABEL	xvi
BAB I	1
PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	2
1.3 Tujuan Penelitian.....	2
1.4 Manfaat.....	3
1.5 Ruang Lingkup.....	3
1.6 Luaran yang diharapkan.....	3
1.7 Sistematika Penulisan.....	3
BAB 2	5
LANDASAN TEORI	5
2.1 Perangkat Lunak.....	5
2.2 Firewall.....	5
2.3 Intrusion Detection System.....	6
2.4 Port Scanner.....	7
2.5 Eksploit.....	8
2.6 IP Address.....	8
2.7 Virtualisasi.....	9
2.8 Suricata.....	9
2.9 Metasploit.....	9
2.10.1 Ping Flood.....	10
2.10.2 SYN Flood.....	11

2.10.3	FTP Brute Force	11
2.10.4	Malware	11
2.10.5	HeavyTraffic	11
BAB 3	13
METODOLOGI PENELITIAN	13
3.1.	Kerangka Pikir	13
3.1.1	Studi Literatur	14
3.1.2	Perancangan Perangkat Lunak.....	14
3.1.3	Melakukan Pengujian.....	15
3.1.4	Hasil dan Pembahasan	17
3.1.5	Laporan	17
3.2.	Alat Bantu Penelitian	17
3.3.	Jadwal Penelitian	18
BAB 4 PEMBAHASAN	19
4.1	PERANCANGAN PERANGKAT	19
4.1.2	Instalasi Ubuntu	20
4.1.3	Instalasi Kali linux.....	21
4.1.4	Instalasi dan konfigurasi suricata	22
4.2	PROSES PENGUJIAN	23
4.2.1	Ping Flood.....	23
4.2.2	SYN Flood	24
4.2.3	FTP Brute Force.....	25
4.2.4	Sending Malware	26
4.2.5	Sending traffic	27
4.3	HASIL DAN PEMBAHASAN.....	28
4.3.1	Ping Flood.....	28
4.3.2	SYN Flood	31
4.3.3	FTP Brute Force.....	33
4.3.4	Malware	36
4.3.5	Heavy Traffic	38
4.4	Analisa anomaly Intrusion Detection System	41
4.4.1	Ping Flood.....	45
4.4.2	SYN Flood	48
4.4.3	FTP Brute force.....	51
4.4.4	Sending Malware	57
4.4.5	Sending traffic	64

BAB 5	70
5.1 Kesimpulan.....	70
5.2 Saran	70
DAFTAR PUSTAKA	71
RIWAYAT HIDUP	74
LAMPIRAN	75

DAFTAR GAMBAR

Gambar 1 Cara kerja Metasploit	10
Gambar 2 Tahapan Penelitian.....	13
Gambar 3 Tahapan Perancangan Perangkat Lunak.....	14
Gambar 4 Implementasi Suricata terhadap serangan.....	15
Gambar 5 Cara Kerja Anomaly Based.....	16
Gambar 6 Topologi Jaringan.....	19
Gambar 7 Setting firewall pada ubuntu.....	20
Gambar 8 Faremowk-metasploit.....	21
Gambar 10 Pengujian Ping Flood	23
Gambar 11 Pengujian SynFlood.....	24
Gambar 12 File user Gambar 13 File pass	25
Gambar 14 Pengujian FTP brute force	25
Gambar 15 File malware.....	26
Gambar 16 Pengujian malware	26
Gambar 17 Hasil pengujian FTP Brute Force	35
Gambar 18 Proses decision tree.....	41
Gambar 19 Hasil pembagian data	43
Gambar 20 Akurasi	43
Gambar 21 Visualisasi decision tree.....	44
Gambar 22 Normal Network	45
Gambar 23 Paket Normal	45
Gambar 24 Grafik Paket Normal.....	45
Gambar 25 Network setelah serangan	46
Gambar 26 Paket Setelah serangan	46
Gambar 27 Grafik paket setelah serangan	47
Gambar 28 Normal Network	48
Gambar 29 Paket Normal	48
Gambar 30 Grafik Normal.....	49
Gambar 31 Network setelah serangan	49
Gambar 32 Paket setelah serangan	50
Gambar 33 Grafik network setelah serangan	50

Gambar 34 Network normal.....	51
Gambar 35 Paket normal.....	51
Gambar 36 Grafik network normal	52
Gambar 37 Network setelah serangan 1	52
Gambar 38 Paket setelah serangan 1	53
Gambar 39 Grafik network setelah serangan 1	53
Gambar 40 Normal network.....	54
Gambar 41 Paket normal.....	54
Gambar 42 Grafik network normal	55
Gambar 43 Network setelah serangan 2	55
Gambar 44 Paket setelah serangan 2	56
Gambar 45 Grafik network setelah serangan 2	56
Gambar 46 Normal network.....	57
Gambar 47 Paket normal.....	58
Gambar 48 Grafik network normal	58
Gambar 49 Network File malware ke 1	59
Gambar 50 Paket File malware ke 1	59
Gambar 51 Grafik File malware ke 1	59
Gambar 52 Network normal.....	60
Gambar 53 Paket normal.....	60
Gambar 54 Grafik normal network	60
Gambar 55 Network File malware ke 2	61
Gambar 56 Paket File malware ke 2	61
Gambar 57 Grafik network file malware ke 2	62
Gambar 58 Network File malware ke 9	62
Gambar 59 Paket File malware ke 9	63
Gambar 60 Grafik network file malware ke 9	63
Gambar 61 Normal network.....	64
Gambar 62 Paket normal	64
Gambar 63 Grafik network normal	65
Gambar 64 Network Serangan	65
Gambar 65 Paket Serangan	66
Gambar 66 Grafik network serangan.....	66

Gambar 67 Network normal Pengujian tambahan	67
Gambar 68 Paket normal pengujian tambahan.....	67
Gambar 69 Grafik normal network pengujian tambahan.....	68
Gambar 70 Network pengujian tambahan.....	68
Gambar 71 Paket pengujian tambahan.....	69
Gambar 72 Grafik pengujian tambahan	69

DAFTAR TABEL

Tabel 1 Penelitian yang terkait	12
Tabel 2 Jadwal kegiatan penelitian	18
Table 3 Jenis serangan.....	23
Table 4 Hasil pengujian.....	28
Table 5 Hasil pengujian Ping Flood	28
Table 6 Hasil pengujian SYN Flood	31
Table 7 Hasil Pengujian FTP Brute Force.....	33
Table 8 Hasil pengujian Malware.....	36
Table 9 Hasil pengujian Heavy traffic	38
Table 10 Sampel data.....	42