



**ANALISA MALWARE PADA TRAFFIC JARINGAN
BERBASIS POLA LALU LINTAS DATA MENGGUNAKAN
METODE ANOMALY**

SKRIPSI

Diajukan Sebagai Syarat untuk Menyelesaikan

Pendidikan Program Strata-1

Pada Program Studi Teknik Informatika

Oleh:

Jian Malik Hidayat

2022110039P

PROGRAM TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS INDO GLOBAL MANDIRI

2024

**ANALISA MALWARE PADA TRAFFIC JARINGAN
BERBASIS POLA LALU LINTAS DATA MENGGUNAKAN
METODE ANOMALY**

SKRIPSI



Oleh :

NIM : 2022110039P
NAMA : JIAN MALIK HIDAYAT
JENJANG STUDI : STRATA SATU (S1)
PROGRAM STUDI : TEKNIK INFORMATIKA

**PROGRAM TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS INDO GLOBAL MANDIRI**

2024

LEMBAR PENGESAHAN SKRIPSI

**Analisa Malware pada Traffic Jaringan Berbasis Pola Lalu Lintas
Data Menggunakan Metode Anomaly**

Oleh

Jian Malik Hidayat

NPM : 2022110039P

Palembang , 23 Agustus 2024

Pembimbing I



Dr Herri Setiawan, M.Kom
NIK: 2003010060

Pembimbing II



Tasmi, S.Si., M.Kom
NIK: 2017010230

Mengetahui,

Dekan Fakultas Ilmu Komputer dan Sains

FAKULTAS TEKNIK DAN SAINS



Rudi Heriansyah, ST., M.Eng. Ph.D.
NIK: 2022010315

LEMBAR PERSETUJUAN DEWAN PENGUJI

Pada hari Kamis tanggal 22 Agustus 2024 telah dilaksanakan ujian sidang skripsi :

Nama : Jian Malik Hidayat

NPM : 2022110039P

Judul : Analisa Malware pada Traffic Jaringan Berbasis Pola Lalu Lintas Data Menggunakan Metode Anomaly

Oleh Prodi Teknik Informatika Fakultas Ilmu Komputer dan Sains Universitas Indo Global Mandiri Palembang

Palembang, 23 Agustus 2024

Penguji 1,

Ir. Nazori Suhandi, M.M

NIK: 1999010008

Penguji 2,

Dr. Shinta Puspasari, S.Si., M.Kom

NIK: 2015010132

Penguji 3,

Tasmi, S.St., M.Kom

NIK: 2017010230

Menyetujui,
Ka. Prodi Teknik Informatika

Zaid Rotnegar Mair, S.T., M.Cs

NIK: 2021010307



SURAT KETERANGAN REVISI SKRIPSI
PROGRAM STUDI TEKNIK INFORMATIKA (SI)
FASILKOM DAN SAINS UNIVERSITAS INDO GLOBAL MANDIRI

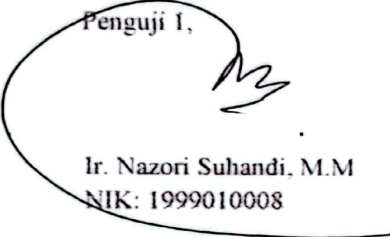
Kami yang bertanda tangan dibawah ini, menerangkan bahwa :

Nama : Jian Malik Hidayat
NPM : 2022110039P
Judul : Analisa Malware pada Traffic Jaringan Berbasis Pola Lalu Lintas
Data Menggunakan Metode Anomaly

Mahasiswa yang namanya tercantum diatas, telah selesai merevisi penulisan SKRIPSI


Palembang, 23 Agustus 2024

Penguji 1,




Ir. Nazori Suhandi, M.M
NIK: 1999010008

Penguji 2,



Dr. Shinta Puspasari, S.Si., M.Kom
NIK: 2015010132

Penguji 3,



Tasmi, S.Si., M.Kom
NIK: 2017010230

Menyetujui,
Ka. Prodi Teknik Informatika



Zaid Romegar Maar, S.T., M.Cs
NIK: 2021010307

MOTTO DAN PERSEMBAHAN

"Dunia ini adalah kejam, tetapi kita tidak boleh menyerah. Seperti Eren Yeager pada anime attack on titan yang menghadapi rintangan dengan tekad yang bulat, marilah kita terus maju untuk mewujudkan impian dan mengubah nasib kita sendiri."

Semoga motto ini menginspirasi semangat dan keteguhan hati dalam perjalanan hidup penulis. Dan selalu mengingat tetaplah fokus pada tujuanmu dan jangan pernah menyerah. Serta selalu ingat kata motivasi mu gas tipis-tipis, Ganbatte, Tatakae !

(Penulis)

Kupersembahkan untuk:

- Istriku Tercinta Noviyani, S.H
- Kedua Orang tuaku dan adik-adikku
- Dosen Jurusan Teknik Informatika Dan Fasilkom
- Alamaterku

ANALISA MALWARE PADA TRAFFIC JARINGAN BERBASIS POLA LALU LINTAS DATA MENGUNAKAN METODE ANOMALY

ABSTRAK

Di era digitalisasi yang semakin meningkat, keamanan jaringan telah menjadi aspek penting dalam melindungi informasi sensitif dari serangan malware. Penelitian ini berfokus pada analisis malware pada lalu lintas jaringan dengan menggunakan pendekatan berbasis pola lalu lintas menggunakan perangkat lunak Wireshark. Wireshark digunakan untuk merekam dan menganalisis paket data yang mengalir melalui jaringan.

Metode ini mengidentifikasi pola lalu lintas umum yang mungkin merupakan tanda malware.

Penelitian ini mengusulkan pendekatan baru terhadap deteksi dan analisis malware dengan memanfaatkan informasi yang terkandung dalam pola lalu lintas. Analisis dilakukan dengan mengidentifikasi perilaku mencurigakan atau karakteristik spesifik yang mungkin terkait dengan aktivitas malware.

Teknik ini diimplementasikan menggunakan Wireshark untuk memantau dan mencatat data lalu lintas secara *real time*. Penelitian menunjukkan bahwa analisis berdasarkan pola lalu lintas dapat meningkatkan deteksi malware tingkat jaringan. Informasi ini membantu bisnis melindungi jaringan mereka dengan lebih efektif dan memberikan respons ancaman keamanan dengan cepat.

Kata kunci: Analisis Malware, Traffic Jaringan, Wireshark, Pola Lalu Lintas Data, Keamanan Jaringan.

MALWARE ANALYSIS ON NETWORK TRAFFIC BASED ON DATA TRAFFIC PATTERNS USING ANOMALY METHOD

ABSTRACT

In the era of increasing digitalization, network security has become an important aspect in protecting sensitive information from malware attacks. This research focuses on analyzing malware in network traffic using a traffic pattern-based approach using Wireshark software. Wireshark is used to record and analyze data packets flowing through a network.

This method identifies common traffic patterns that may be signs of malware. This research proposes a new approach to malware detection and analysis by utilizing the information contained in traffic patterns. The analysis is performed by identifying suspicious behavior or specific characteristics that may be associated with malware activity.

This technique is implemented using Wireshark to monitor and log traffic data in real time. Research shows that analysis based on traffic patterns can improve network-level malware detection. This information helps businesses protect their networks more effectively and provide rapid security threat response.

Keywords: Malware Analysis, Network Traffic, Wireshark, Data Traffic Patterns, Network Security.

KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Puji dan syukur penulis panjatkan kehadiran Allah SWT, atas segala karunia dan rahmat-Nya sehingga penulis dapat menyelesaikan Skripsi ini dengan judul **“ANALISA MALWARE PADA TRAFFIC JARINGAN BERBASIS POLA LALU LINTAS DATA MENGGUNAKAN METODE ANOMALY”**.

Laporan ini disusun berdasarkan dari hasil penelitian penulis.

Dalam pelaksanaan skripsi dan penyusunan laporan, penulis banyak mendapatkan bantuan, bimbingan, dan petunjuk dari berbagai pihak hingga terselesainya laporan ini. Mulai dari pengumpulan data sampai proses penyusunan laporan. Untuk itu, penulis mengucapkan terima kasih kepada :

1. Bapak Dr. H. Marzuki Alie, S.E., M.M. Selaku Rektor Universitas Indo Global Mandiri
2. Noviyani, S.H sebagai wanita hebat sebagai *support system*. Kedua Orang tua dan adik-adikku yang selalu memberikan support dan doa.
3. Bapak Dr Herri Setiawan, M.Kom, selaku dosen pembimbing I dan Bapak Tasmi, S.Si., M.Kom selaku dosen pembimbing II

Penulis menyadari bahwa masih terdapat banyak kekurangan dalam penulisan laporan ini, baik dari segi materi maupun teknik penyajiannya. Untuk itu, penulis mengharapkan kritik dan saran dari pembaca yang bersifat membangun agar kedepannya penulis bisa lebih baik lagi.

Akhir kata semoga laporan skripsi ini bermanfaat bagi semua pihak yang membutuhkan khususnya Mahasiswa/i Jurusan Teknik Informatika Universitas Indo Global Mandiri Palembang.

Jakarta, 14 November 2023



Penulis

DAFTAR ISI

HALAMAN JUDUL LUAR	i
HALAMAN JUDUL DALAM	ii
LEMBAR PENGESAHAN SKRIPSI	iii
LEMBAR PERSETUJUAN DEWAN PENGUJI	iv
SURAT KETERANGAN REVISI SKRIPSI	v
MOTTO DAN PERSEMBAHAN	vi
ABSTRAK	vii
ABSTRACT	viii
KATA PENGANTAR	ix
DAFTAR ISI	x
DAFTAR GAMBAR	xiii
DAFTAR TABEL	xiv
DAFTAR LAMPIRAN	xv
BAB I PENDAHULUAN	
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Tujuan Penelitian	3
1.4 Batasan Penelitian	3
1.5 Manfaat Penelitian	4
1.6 Sistematika Penulisan	4
BAB II LANDASAN TEORI	
2.1 Pengertian Malware	5
2.1.1 Jenis-Jenis Malware	5

2.2	Serangan Keamanan Jaringan	7
2.2.1	Jenis Serangan pada jaringan	7
2.3	File Signature	9
2.3.1	File Magic Number	10
2.3.2	File Checksum	11
2.4	Malware Analisis	11
2.5	Analisis Pola Lalu Lintas Data dalam Jaringan	12
2.6	Rekayasa Perangkat Lunak	14
2.6.1	Wireshark	15
2.7	TCP	16
2.8	Metode Anomaly	18
2.9	Dataset Malware	18

BAB III METODOLOGI PENELITIAN

3.1	Sistematika Pemecahan Masalah	20
3.1.1	Tahap Awal	21
3.1.2	Tahap Eksperimen Pada Objek Malware.....	22
3.1.3	Tahap Analisis	24
3.1.4	Skema Analisa Malware	27
3.1.5	Tahap Akhir	28
3.2	Komponen Pengujian	29

BAB IV HASIL DAN PEMBAHASAN

4.1	Hasil Penelitian	30
4.1.1	Deteksi Malware dalam Lalu lintas Jaringan	30

4.1.2 Analisis Tingkah Laku Malware	32
4.1.2.1 TCP Scan	33
4.1.3 Dampak terhadap Traffic Jaringan	34
4.1.3.1 Network Scanner	34
4.1.3.2 ARP Scan	35
4.1.3.3 Kategorisasi Dampak pada jaringan	36
4.2 Pembahasan	37
4.2.1 Pengujian menggunakan Wireshark	37
4.2.2 Downloading Executable File Sample PCAP	38
4.2.3 C&C IRC	40
4.2.4 Relevansi Dampak Terhadap Keamanan Jaringan	40
4.2.5 Analisis Port	45
4.2.6 Analisa Port Menggunakan Metode Anomaly	50

BAB V KESIMPULAN

5.1 Kesimpulan	52
5.2 Saran	53

DAFTAR PUSTAKA

LAMPIRAN

DAFTAR GAMBAR

Gambar 3.1 Sistematika Pemecahan Masalah	20
Gambar 3.2 Flowchart Tahap Awal	21
Gambar 3.3 Flowchart Untuk Melakukan Analisis Malware	27
Gambar 4.1 Hasil Aktivitas <i>Anomaly</i> C&C IRC Malware neris Port 65500 ...	31
Gambar 4.2 Hasil Analisis <i>Graph</i> Malware Neris pada port 65500	32
Gambar 4.3 <i>scanning</i> menggunakan protokol TCP	33
Gambar 4.4 Hasil aktifitas <i>scanning</i>	34
Gambar 4.5 Hasil Aktivitas TCP Scanning Malware bot	35
Gambar 4.6 Aktifitas downloading executable file pcap malware neris	38
Gambar 4.7 Malware neris export CSV	39
Gambar 4.8 Aktifitas Malware neris export CSV	39
Gambar 4.9 Total Aktifitas Port 80	46
Gambar 4.10 Total Aktifitas Port 81	46
Gambar 4.11 Total Aktifitas Port 82	46
Gambar 4.12 Total Aktifitas Port 88	47
Gambar 4.13 Total Aktifitas Port 139	47
Gambar 4.14 Total Aktifitas Port 443	47
Gambar 4.15 Total Aktifitas Port 1398	47
Gambar 4.16 Total Aktifitas Port 2076	47
Gambar 4.17 Total Aktifitas Port 2343	47
Gambar 4.18 Total Aktifitas Port 5231	48
Gambar 4.19 Total Aktifitas Port 5296	48
Gambar 4.20 Total Aktifitas Port 6251	48
Gambar 4.21 Total Aktifitas Port 6667	48
Gambar 4.22 Total Aktifitas Port 9541	48
Gambar 4.23 Total Aktifitas Port 65500	49
Gambar 4.24 <i>Graph</i> port activity pada Virus Neris	51

DAFTAR TABEL

Tabel 2.10 Dataset <i>malware</i>	19
Tabel 4.1 Hasil Analisis Impact atau Resiko	37
Tabel 4.2 Analisis dampak <i>malware</i>	40
Tabel 4.3 Aktivitas Port Malware neris.exe	49

DAFTAR LAMPIRAN

Lampiran 1 Daftar Riwayat Hidup

Lampiran 2 Kartu Bimbingan

Lampiran 3 Surat Pernyataan Tidak Plagiat

Lampiran 4 Surat Keterangan Revisi Proposal Skripsi