ANALISIS METODE LIVE FORENSIK DAN STATISTIK LOG JARINGAN BERBASIS NEURAL DALAM MENDETEKSI SERANGAN DDoS PADA ROUTER

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Informatika

disusun oleh

HARDLY JOSHUA IMANUEL

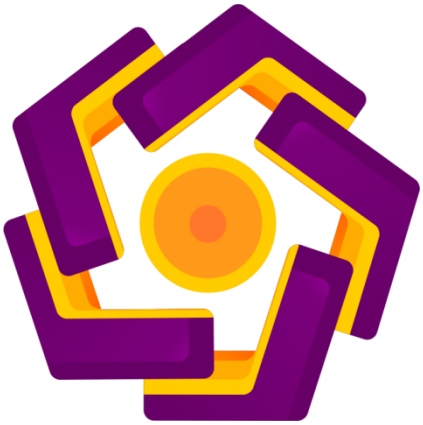
15.11.9258

PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2023

ANALISIS METODE LIVE FORENSIK DAN STATISTIK LOG JARINGAN BERBASIS NEURAL DALAM MENDETEKSI SERANGAN DDoS PADA ROUTER

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Informatika



disusun oleh

Hardly Joshua Imanuel

15.11.9258

PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2023

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS METODE LIVE FORENSIK DAN STATISTIK LOG JARINGAN BERBASIS NEURAL DALAM MENDETEKSI SERANGAN DDoS PADA ROUTER

yang disusun dan diajukan oleh

Hardly Joshua Imanuel

15.11.9258

telah disetujui oleh Dosen Pembimbing Skripsi

pada tanggal 14 Desember 2022

Dosen Pembimbing,

Andika Agus Slameto, M.Kom

NIK. 190302109

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS METODE LIVE FORENSIK DAN STATISTIK LOG JARINGAN BERBASIS NEURAL DALAM MENDETEKSI SERANGAN DDoS PADA ROUTER

yang disusun dan diajukan oleh

Hardly Joshua Imanuel

15.11.9258

Telah dipertahankan di depan Dewan Penguji
pada tanggal 30 Januari 2023

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Arifiyanto Hadinegoro, S.Kom., M.T. **NIK. 190302289**	
Subektiningsih, M.Kom **NIK. 190302413**	
Arif Akbarul Huda, S.Si., M.Eng. **NIK. 190302287**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 1 Febuari 2023

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta,S.Kom., M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Hardly Joshua Imanuel
NIM : 15.11.9258

Menyatakan bahwa Skripsi dengan judul berikut:

Analisi Metode Live Forensik Dan Statistik Log Jaringan Berbasis Neural Dalam Mendeteksi Serangan DDoS Pada Router

Dosen Pembimbing : Andika Agus Slameto, M.Kom

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 1 Februari 2023

Yang Menyatakan,

Hardly Joshua Imanuel

MOTTO

Segala hal yang diperjuangkan memang tidak ada yang mudah tetapi harus dijalani dengan hati yang lapang, karna "*Hati yang gembira adalah obat yang manjur, tetapi semangat yang patah mengeringkan tulang"*

Amsal 17:22

HALAMAN PERSEMBAHAN

Segala puji syukur atas berkat Rahmat dan karunia Tuhan Yang Maha Esa telah memberikan kelancaran bagi penulis dalam menyelesaikan skripsi ini dengan sebaik-baiknya. Skripsi ini penulis persembahkan untuk:

1. Kedua orang tua penulis yang tercinta, Bapak Moey Dayanashoba dan Ibu Vera Ardiana yang telah memberikan dukungan terbesar, menguatkan, dan menyemangati penulis dalam kondisi suka maupun duka.

2. Adik penulis, Gladys Natasha Evangeline yang selalu memberikan dukungan pada penulis.

3. Skripsi ini saya persembahkan kepada Almamaterku Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta.

KATA PENGANTAR

Puji dan syukur kehadiran Tuhan Yang Maha Esa atas berkat rahmat serta kasih-Nya sehingga penulis dapat menyelesaikan skripsi ini yang mengambil judul "Analisis Metode Live Forensik Dan Statistik Log Jaringan Berbasis Neural Dalam Mendeteksi Serangan DDoS Pada Router" guna memenuhi sebagian syarat memperoleh gelar Sarjana Komputer (S.Kom) bagi mahasiswa program S-1 di Program Studi Informatika pada Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta. Penulis menyadari bahwa skripsi ini masih jauh dari kesempurnaan, oleh sebab itu penulis mengharapkan kritik dan saran yang bersifat membangun dari semua pihak demi kesempurnaan skripsi ini.

Terselesaikannya skripsi ini tidak terlepas dari bantuan banyak pihak, sehingga pada kesempatan ini dengan segala kerendahan hati dan penuh rasa hormat penulis mengucapkan terima kasih yang sebesar-besarnya bagi semua pihak yang telah memberikan bantuan moril maupun materil baik langsung maupun tidak langsung dalam penyusunan skripsi ini hingga selesai, terutama kepada yang saya hormati:

1. Bapak M. Suyanto, Prof., Dr., M.M selaku Rektor Universitas AMIKOM Yogyakarta yang telah memberi kesempatan kepada penulis untuk menimba ilmu di Universitas AMIKOM Yogyakarta.
2. Bapak Hanif Al Fatta, S.Kom., M.Kom. selaku Dekan Fakultas Ilmu Komputer Univeristas AMIKOM Yogyakarta yang telah memberikan izin dalam penulisan skripsi ini.
3. Ibu Windha Mega Pradnya Dhuhita, M.Kom selaku Ketua Program Studi Informatika Universitas AMIKOM Yogyakarta yang senantiasa memberi motivasi selama perkuliahan dan memberikan semangat dalam penyelesaian penulisan skripsi ini.
4. Bapak Andika Agus Slameto, M.Kom. selaku Dosen Pembimbing yang telah senantiasa memberi saya motivasi dan arahan untuk penyusunan skripsi ini.
5. Ibu, Bapak, dan Adik penulis yang selalu memberi semangat, dan doa kepada penulis, sehingga skripsi ini dapat diselesaikan dengan baik.

6. Bapak /Ibu dosen dan staf Ilmu Komputer khususnya pada program studi infomatika Universitas AMIKOM Yogyakarta, yang telah memberikan pengetahuan yang telah membimbing, mendidik, dan mengajarkan tentang pengetahuan kepada penulis selama menempuh kuliah di Program Studi Informatika.

Akhirnya, Penulis mengucapkan banyak terima kasih kepada semua pihak dan apabila ada yang tidak tersebutkan penulis mohon maaf, besar harapan skripsi yang ditulis oleh penulis ini dapat bermanfaat khususnya bagi Penulis sendiri dan umumnya bagi pembaca. Bagi para pihak yang telah membantu dalam penulisan skripsi ini semoga segala amal dan kebaikannya mendapatkan balasan yang berlimpah dari Tuhan Yang Maha Esa.

Yogyakarta, 04 Februari 2023

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Latar Belakang Masalah serangan *Denial of Service* (DoS) pada suatu jaringan terus berkembangan dilingkungan masyarakat. Khususnya serangan DoS yang dilakukan oleh oknum tertentu dan ditujukkan pada jaringan *Router* orang lain untuk memperoleh hak akses dan tidak jarang serangan yang dilakukan menyebabkan jaringan *Router* yang ditargetkan menjadi *down* (lumpuh) karena tidak mampu melayani permintaan *user* yang memiliki hak akses secara sah, sehingga diperlukannya analisis serangan *DoS* pada *Router* dan mengali informasi, serta menarik data sebagai bukti digital adanya serangan *DoS* pada *Router* menggunakan *Wireshark*. Serangan *Denial of Service* (*DoS*) adalah serangan jaringan terstruktur yang berasal dari berbagai sumber dan berkumpul untuk membentuk arus paket besar. Serangan *DoS* bertujuan untuk mengganggu layanan yang tersedia pada jaringan target dengan membanjiri *bandwidth* atau sistem kapasitas pemrosesan yang membuat jaringan *server* target menjadi kelebihan beban. *Wireshark* merupakan salah satu dari sekian banyak *Tool Network Analyzer* yang banyak digunakan oleh *Network Administrator* untuk menganalisa kinerja jaringannya terrmasuk protokol didalamnya. *Tool Wireshark* dapat menganalisa transmisi paket data dalam jaringan, proses koneksi dan transmisi data antar komputer, mendeteksi serangan *DoS* pada jaringan *Router*, melakukan analisis lalu lintas jaringan yang memiliki fungsi untuk para profesional jaringan, administrator jaringan, peneliti, dan pengembangan perangkat lunak jaringan yang membutuhkan deteksi serangan *DoS* pada *Router* dan mengali informasi serta menarik data sebagai bukti digital adanya serangan DoS pada *Router* secara *Real Time Processing*. Metode *Real Time Processing* adalah mekanisme pengontrolan, perekaman data, pemrosesan yang sangat cepat sehinga output yang dihasilkan dapat diterima dalam waktu yang relatif sama. Perbedaan dengan sistem *online* adalah satuan waktu yang digunakan *real-time* biasanya seperseratus atau seperseribu detik sedangkan *online* masih dalam skala detik atau bahkan kadang beberapa menit. Perbedaan lainnya, *online* biasanya hanya berinteraksi dengan pemakai, sedangkan *real-time* berinteraksi langsung dengan pemakai dan lingkungan yang dipetakan. Manfaat dari pelaksanaan penelitian ini adalah menarik data informasi serangan DoS yang berisikan *data log activity* dan *IP address* pelaku penyerang terhadap *Router*.

Kata Kunci: Serangan (*Denial of Service*), Live Forensik, *Router*, *Wireshark*, Statistik Log Jaringan...

ABSTRACT

Background of The problem of Denial of Service (DoS) attacks on a network continues to grow in the community. In particular, DoS attacks carried out by certain individuals and aimed at other people's Router networks to gain access and not infrequently the attacks carried out cause the targeted Router network to be down (paralyzed) because it is unable to serve user requests that have legal access, so it is necessary analysis of DoS attacks on Routers and extracting information, as well as extracting data as digital evidence of DoS attacks on Routers using Wireshark. A Denial of Service (DoS) attack is a structured network attack that originates from multiple sources and aggregates to form a large stream of packets. DoS attacks aim to disrupt the services available on the target network by overwhelming the system bandwidth or processing capacity which overloads the target server network. Wireshark is one of the many Network Analyzer Tools that are widely used by Network Administrators to analyze network performance including the protocols in it. The Wireshark tool can analyze data packet transmission in a network, process connections and data transmission between computers, detect DoS attacks on router networks, perform network traffic analysis which has functions for network professionals, network administrators, researchers, and network software developers who need detection of DoS attacks on Routers and extracting information and extracting data as digital evidence of DoS attacks on Routers in Real Time Processing. The Real Time Processing method is a control mechanism, data recording, very fast processing so that the resulting output can be received in relatively the same time. The difference with the online system is that the units of time used in real-time are usually hundredths or thousandths of a second, while online is still on a scale of seconds or sometimes even minutes. Another difference, online usually only interacts with users, while real-time interacts directly with users and the mapped environment. The benefit of conducting this research is to collect DoS attack information data which contains activity log data and the attacker's IP address against the Router.

Keyword: *Attacks (Denial of Service), Live Forensic, Router, Wireshark, Network Log Statistic*