ANALISIS SERANGAN *DDOS* PADA *RESOURCE SERVER* MENGGUNAKAN *WIRESHARK*

SKRIPSI

Disusun Oleh

Ahmad Fauzi Irwan

15.11.9302

PROGAM SARJANA

PROGAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2021

ANALISIS SERANGAN *DDOS* PADA *RESOURCE SERVER* MENGGUNAKAN *WIRESHARK*

SKRIPSI

untuk memenuhi spersyaratan
mencapai gelar Sarjana
pada Program Studi Informatika

disusun oleh

Ahmad Fauzi Irwan

15.11.9302

PROGRAM SARJANA

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2021

PERSETUJUAN

SKRIPSI

ANALISIS SERANGAN *DDOS* PADA *RESOURCE SERVER* MENGGUNAKAN *WIRESHARK*

yang dipersiapkan dan disusun oleh

Ahmad Fauzi Irwan

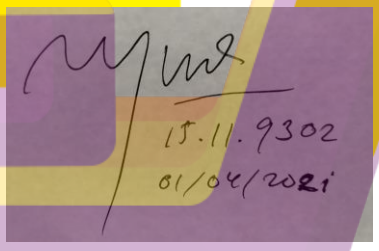
15.11.9302

telah disetujuai oleh Dosen Pembimbing Skripsi

pada tanggal

1 April 2021

Dosen Pembimbing



Yudi Sutanto, S.Kom, M.Kom.

NIK. 190302039

PENGESAHAN

SKRIPSI

ANALISIS SERANGAN *DDOS* PADA *RESOURCE SERVER* MENGGUNAKAN *WIRESHARK*

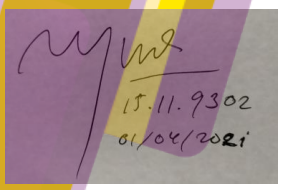
yang dipersiapkan dan disusun oleh

Ahmad Fauzi irwan

15.11.9302

telah dipertahankan di depan Dewan Penguji

pada tanggal

Nama Penguji	**Tanda Tangan**
Andika Agus Slameto, M.Kom **NIK. 190302109**	
Mulia Sulistyono, M.Kom **NIK. 190302248**	
Yudi Sutanto, M.Kom **NIK. 190302039**	

Skripsi ini telah diterima sebagai salah satu persyaratan

untuk memperoleh gelar Sarjana Komputer

Tanggal 1 April 2021

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta, M.Kom

NIK. 190302096

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 21 April 2021

Ahmad Fauzi Irwan

NIM. 15.11.9302

v

MOTTO

"A lesson without pain is meaningless. For you cannot gain something without sacrificing something else in return. But once you have recovered it and made it your own. You will gain an irreplaceable heart."

- Edward Elric -

"Tidak ada pengalaman sia-sia, yang terpenting adalah kau bisa memanfaatkannya atau tidak."

- World Trigger -

"Jika kau tau banyak pilihan namun tak mengambil pilihan itu maka hidupmu akan membosankan."

- Haikyuu -

PERSEMBAHAN

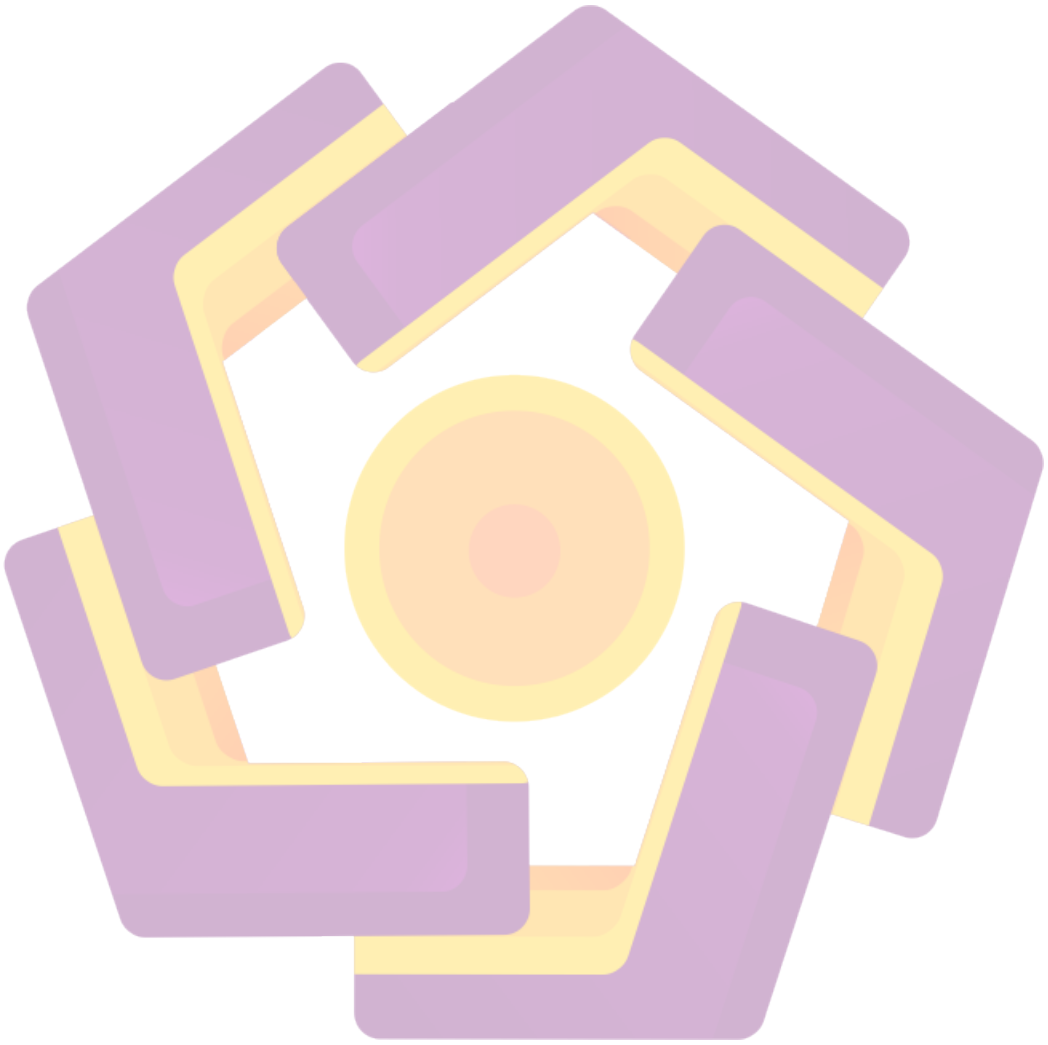
Alhamudlillah segala puji syukur atas kehadirat Allah SWT yang telah memberikan limpahan rahmat dan karunia-Nya sehingga penelitian ini dapat dilakukan dan diselesaikan dengan sebaik-baiknya. Penulis juga ucapkan terimakasih untuk dukungan dan bantuan semua pihak yang membantu selesainya penelitan ini. Ucapan terimakasih saya persembahkan kepada :

1. Kedua orang tua dan semua keluarga yang senantiasa memberikan dukungan dan do'a kepada saya.
2. Bapak Yudi Susanto, S.Kom, M.Kom selaku dosen pembimbing yang telah banyak memberikan bimbingan, pelajaran, serta ilmu yang sangat bermanfaat.
3. Teman-teman kelas 15-S1IF-12 yang menjadi teman seperjuangan dari awal perkuliahan hingga saat ini.
4. Sahabat-sahabat rantau, yang banyak memberikan dukungan dan kritik menulisan skripsi ini.
5. Yesi Rahmawati, S.S, yang telah membatu dalam proses penulisan skripsi dari awal sampai selesai.
6. Sohabat nongki kelas 12 yang sudah menemani, memberikan dorongan dan bersenang-senang bersama selama berkuliah

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR



INTISARI

Masalah serangan Distributed Denial of Service (DDoS) pada suatu jaringan web/*server* terus meningkat di lingkungan masyarakat, khususnya serangan DDoS yang dilakukan oleh oknum tertentu dan ditujukan pada jaringan *Server* orang lain untuk memperoleh hak akses. Tidak jarang, serangan yang dilakukan menyebabkan jaringan *server* yang ditargetkan menjadi down (lumpuh) karena tidak mampu melayani permintaan user yang memiliki hak akses secara sah, sehingga diperlukan analisis serangan DDoS pada *Server*.

Serangan Distributed Denial of Service (DDoS) adalah serangan jaringan terstruktur yang berasal dari berbagai sumber dan berkumpul untuk membentuk arus paket besar. Serangan DDoS bertujuan untuk menghabiskan sumber daya *server* dan mengganggu layanan yang tersedia pada jaringan target dengan membanjiri bandwidth atau sistem kapasitas pemrosesan yang membuat jaringan *server* target menjadi kelebihan beban.

Wireshark adalah alat yang dapat digunakan untuk mendeteksi serangan DDoS pada jaringan *Server* dan melakukan analisis lalu lintas jaringan yang memiliki fungsi Filtering Logical untuk mendeteksi serangan DDoS pada *Server* dan menggali informasi serta menarik data forensik sebagai bukti digital serangan DDoS pada *server* melalui metode live forensics. Output yang dihasilkan penelitian ini berhasil menarik data informasi serangan DDoS terkait data Log Activity, IP Address List, IO graph dan Flow graph.

Kata Kunci: Serangan *DDoS* (*Distributed Denial of Service*), *Resource Server*, *Live Forensic*, *Filtering Logical*.

ABSTRACT

The problem of Distributed Denial of Service (DDoS) attacks on a web network/server continues to increase in the community, especially DDoS attacks carried out by certain persons and aimed at other people's Server networks to gain access rights. Not infrequently, attacks are carried out causing the targeted server network to be down (paralyzed) because it is unable to serve user requests that have legitimate permissions, so it is necessary to analyze DDoS attacks on the Server.

Distributed Denial of Service (DDoS) attacks are structured network attacks that come from a variety of sources and come together to form a large package stream. DDoS attacks aim to consume server resources and disrupt services available on the target network by flooding bandwidth or processing capacity systems that make the target server network overloaded.

Wireshark is a tool that can be used to detect DDoS attacks on server networks and perform network traffic analysis that has a Logical Filtering function to detect DDoS attacks on servers and dig up information and pull forensic data as digital evidence of DDoS attacks on servers through live forensics methods. The output produced by this study successfully pulled DDoS attack information data related to Log Activity data, IP Address List, IO graph and Flow graph.

Keywords: Distributed Denial of Service (DDoS), Resource Server, Live Forensic, Filtering Logical.