NETWORK FORENSICS UNTUK MENDETEKSI SERANGAN FLOODING PADA PERANGKAT INTERNET OF THINGS (IoT)

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Informatika

disusun oleh

MUHAMMAD AFFAN RIDHA

20.11.3392

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2024

NETWORK FORENSICS UNTUK MENDETEKSI SERANGAN FLOODING PADA PERANGKAT INTERNET OF THINGS (IoT)

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Informatika

disusun oleh

MUHAMMAD AFFAN RIDHA

20.11.3392

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2024

HALAMAN PERSETUJUAN

SKRIPSI

NETWORK FORENSICS UNTUK MENDETEKSI SERANGAN FLOODING PADA PERANGKAT INTERNET OF THINGS (IoT)

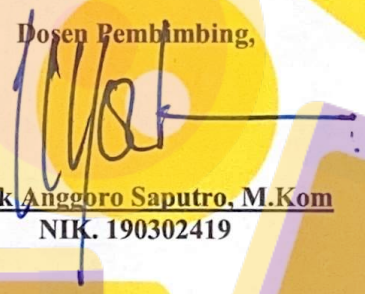
yang disusun dan diajukan oleh

Muhammad Affan Ridha

20.11.3392

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 19 Februari 2024

Dosen Pembimbing,



Uyock Anggoro Saputro, M.Kom
NIK. 190302419

HALAMAN PENGESAHAN

SKRIPSI

NETWORK FORENSICS UNTUK MENDETEKSI SERANGAN FLOODING PADA PERANGKAT INTERNET OF THINGS (IoT)

yang disusun dan diajukan oleh

Muhammad Affan Ridha

20.11.3392

Telah dipertahankan di depan Dewan Penguji
pada tanggal 19 Februari 2024

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Andika Agus Slameto, M.Kom **NIK. 190302109**	
Ali Mustopa, M.Kom **NIK. 190302192**	
Uyock Anggoro Saputro, M.Kom **NIK. 190302419**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 19 Februari 2024

DEKAN FAKULTAS ILMU KOMPUTER

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

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Muhammad Affan Ridha
NIM : 20.11.3392

Menyatakan bahwa Skripsi dengan judul berikut:

NETWORK FORENSICS UNTUK MENDETEKSI SERANGAN FLOODING PADA PERANGKAT INTERNET OF THINGS (IoT)

Dosen Pembimbing : Uyock Anggoro Saputro, 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, 19 Februari 2024

Yang Menyatakan,

Muhammad Affan Ridha

HALAMAN PERSEMBAHAN

Seiring rasa syukur kepada Tuhan Yang Maha Esa, Penelitian ini dipersembahkan kepada :

1. Tuhan Yang Maha Esa Allah SWT
2. Kedua Orang Tua
3. Dosen Pembimbing
4. Seluruh Dosen Teknik Komputer
5. Uyock Anggoro Saputro, M.Kom
6. Basecamp Moeslem
7. Seluruh Mahasiswa Jurusan Teknik Komputer Angkatan 2020
8. Teman – teman yang tidak bisa saya sebutkan satu per satu
9. Almamater, Universitas Amikom Yogyakarta

KATA PENGANTAR

Puji syukur saya panjatkan kepada Allah SWT atas Rahmat, Ridho, limpahan berkat, dan karunia-Nya, sehingga saya dapat menyelesaikan Proposal Skripsi yang berjudul "**NETWORK FORENSICS UNTUK MENDETEKSI SERANGAN FLOODING PADA PERANGKAT INTERNET OF THINGS (IoT)** " Penulisan Proposal Skripsi ini dilakukan dalam rangka memenuhi syarat untuk mencapai gelar Sarjana Komputer pada Program Studi Teknik Komputer Universitas Amikom Yogyakarta. Proposal Skripsi ini terwujud atas bimbingan, pengarahan, dan bantuan dari berbagai pihak yang tidak bisa saya sebutkan satu persatu dan pada kesempatan ini saya menyampaikan ucapan terima kasih kepada :

1. Bapak Prof. Dr. M. Suyanto, MM. selaku Rektor Universitas Amikom Yogyakarta.
2. Bapak Hanif Al Fatta,S.Kom., M.Kom, Ph. D. selaku Ketua Prodi Teknik Komputer.
3. Bapak Banu Santoso, S.T., M.Eng. selaku Sekretaris Prodi Sarjana Teknik Komputer Universitas Amikom Yogyakarta.
4. Bapak Uyock Anggoro Saputro, M.Kom selaku Dosen Pembimbing yang telah memberikan bimbingan dan arahan dalam penyusunan skripsi.
5. Semua dosen dan staff Prodi Teknik Komputer Universitas Amikom Yogyakarta.

Akhir kata penulis ingin meminta maaf atas segala kekurangan yang terdapat pada penulisan skripsi ini. Penulis berharap semoga skripsi ini dapat menjadi bacaan yang bermanfaat serta menambah wawasan bagi pembaca.

Yogyakarta, 19 Februari 2024

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Serangan banjir merupakan ancaman serius terhadap keamanan jaringan, terutama pada perangkat IoT yang mengakibatkan pemutusan koneksi, dan dibanjiri oleh penyerang dengan lalu lintas data tidak berguna yang ditujukan ke jaringan sehingga menghabiskan sumber daya. Langkah pertama yang harus dilakukan adalah merancang dan membangun sistem pendeteksi serangan yaitu Intrusion Detection System (IDS). Penggunaan wireshark berguna untuk merekam serangan Distributed Danial of Services (DDoS) serta data lalu lintas yang disimpan dalam log. Wireshark tidak hanya dapat digunakan sebagai logger tetapi juga dapat digunakan sebagai tahapan forensik jaringan untuk memperkuat bukti serangan sebagai proses pengumpulan data untuk keperluan uji coba. Hasil penelitian yang telah dilakukan mampu mendeteksi serangan banjir dengan menggunakan bantuan alat aplikasi penganalisa jaringan Wireshark untuk menangkap log lalu lintas pada sistem jaringan dan dapat digunakan sebagai dasar bukti adanya serangan.

Kata Kunci : Forensik Jaringan, Pemrograman, Internet Of Things, LOIC

ABSTRACT

Flooding attacks are a serious threat to network security, especially on IoT devices resulting in connection termination, and being flooded by the attacker with useless data traffic destined for the network exhausting resources. The first step that must be taken is to design and build an attack detection system, namely the Intrusion Detection System (IDS). The use of wireshark is useful for recording Distributed Danial of Services (DDoS) attacks as well as traffic data stored in logs. Wireshark can not only be used as a logger but can also be used as a network forensic stage to strengthen evidence of attacks as a process of collecting data for trial purposes. The results of research that have been carried out are able to detect flooding attacks using the help of the Wireshark network analyzer application tool to capture traffic logs in the network system and can be used as a basis for evidence of an attack.

Keyword: *Network Forensics, Programing, Internet Of Things, LOIC*