IMPLEMENTASI IDENTIFIKASI SERANGAN *DENIAL OF SERVICE* (DOS) BERBASIS *BRUTE FORCE* MENGGUNAKAN WIRESHARK

LAPORAN TUGAS AKHIR

SALSHA FEBRIANINDA

NIM: 21021040

PROGRAM STUDI D-III TEKNOLOGI INFORMASI

POLITEKNIK 'AISYIYAH PONTIANAK

2024

IMPLEMENTASI IDENTIFIKASI SERANGAN *DENIAL OF SERVICE* (DOS) BERBASIS *BRUTE FORCE* MENGGUNAKAN WIRESHARK

LAPORAN TUGAS AKHIR

Diajukan Untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Ahli Madya Komputer

SALSHA FEBRIANINDA
NIM: 21021040

PROGRAM STUDI D-III TEKNOLOGI INFORMASI
POLITEKNIK 'AISYIYAH PONTIANAK
2024

LEMBAR PERSETUJUAN

IMPLEMENTASI IDENTIFIKASI SERANGAN *DENIAL OF SERVICE* (DOS) BERBASIS *BRUTE FORCE* MENGGUNAKAN WIRESHARK

LAPORAN TUGAS AKHIR

SALSHA FEBRIANINDA

NIM: 21021040

Telah Memenuhi Persyaratan Dan Disetujui Untuk Mengikuti Sidang
Laporan Tugas Akhir Di Politeknik Aisyiyah Pontianak
Pada Tanggal 10 Juli 2024

Menyetujui:

Pembimbing

Muhammad Faqih Dzulqarnain, S.T., M.Cs

NIDN : 11-2808-9301

LEMBAR PENGESAHAN

IMPLEMENTASI IDENTIFIKASI SERANGAN *DENIAL OF SERVICE* (DOS) *BERBASIS BRUTE FORCE* MENGGUNAKAN WIRESHARK

dipersiapkan dan disusun oleh

Salsha Febrianinda
21021040

Telah dipertahankan di depan Dewan Penguji
Pada tanggal 10 Juli 2024

Susunan Dewan Penguji:

Penguji Utama	Penguji Anggota
Irwan Adhi Prasetya, S.T., M.T	**M.Faqih Dzulqarnain, S.T., M.Cs**
NIDN : 11-2107-9302	**NIDN : 11-2808-9301**

Laporan Tugas Akhir ini telah diterima sebagai salah satu persyaratan
Untuk memperoleh gelar Ahli Madya Komputer

Pontianak, 10 Juli 2024
Ketua Program Studi D-III Teknologi Informasi

Irwan Adhi Prasetya, S.T., M.T
NIDN : 11-2107-9302

PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertanda tangan dibawah ini, saya :

Nama : **Salsha Febrianinda**
NIM : **21021040**
Program Studi : **D-III Teknologi Informasi**

Menyatakan bahwa saya tidak melakukan kegiatan plagiat dalam penulisan Laporan Tugas Akhir saya yang berjudul:

" IMPLEMENTASI IDENTIFIKASI SERANGAN *DENIAL OF SERVICE* (DOS) BERBASIS *BRUTE FORCE* MENGGUNAKAN WIRESHARK"

1. Karya Tulis ini benar-benar Karya ASLI dan diajukan untuk mendapatkan gelar akademik, di Politeknik Aisyiyah Pontianak.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Karya Ilmiah ini TIDAK menggunakan bantuan *Artificial Intelligence* (AI) dari program atau aplikasi manapun.
4. 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.
5. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Politeknik Aisyiyah Pontianak.

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.

Pontianak, 10 Juli 2024

(Salsha Febrianinda)
NIM: 21021040

IMPLEMENTASI IDENTIFIKASI SERANGAN *DENIAL OF SERVICE* (DOS) BERBASIS *BRUTE FORCE* MENGGUNAKAN WIRESHARK

Salsha Febrianinda[1], Muhammad Faqih Dzulqarnain[2], Irwan Adhi Prasetya[3]

INTISARI

Latar Belakang: Kejahatan siber menjadi ancaman dalam kehidupan manusia, sehingga menyulitkanm organisasi dan pemerintah untuk mengatasi kejahatan yang dilakukan dalam teknologi komputer. Kejahatan ini berdampak buruk pada masyarakat, perusahaan, perbankan, dan lainnya. Salah satu *cybercrime* yang sering terjadi pada suatu jaringan dan sistem yaitu *Denial of Service (DOS) Attack* dan *Brute force Attack*. Untuk mengurangi dan mencegah dampak serangan kejahatan *cyber* pada dunia digital, maka dibutuhkanlah *cyber security* atau kemananan siber yang bertugas untuk mencegah dan melindungi sistem komputer maupun data. Metode: *Anomaly-based:* Melakukan monitoring lalu lintas paket dan membandingkannya dengan pola lalu lintas normal sistem *(baseline)* terhadap intrusi. Jika ada lalu lintas yang mencurigakan dan tidak sesuai *baseline* maka akan diidentifikasi dan memberikan peringatan kepada administrator serta melakukan pencegahan. Karena adanya *baseline*, metode deteksi ini dapat mendeteksi serangan jenis baru yang masuk kedalam sistem. Hasil dan Kesimpulan: Implementasi penindakan serangan *Denial of Service* (DoS) berbasis *brute force* menggunakan Wireshark efektif dalam mendeteksi lalu lintas jaringan yang mencurigakan. Wireshark dapat menganalisa mendalam terhadap paket data yang melewati jaringan, sehingga serangan dapat diidentifikasi secara cepat dan akurat.

Kata Kunci **:** *Brute force*, serangan *Denial of Service*, kejahatan siber
Kepustakaan **:** 16 Jurnal (Tahun 2019-2024)
Jumlah Halaman **:** xi; 60 Halaman; Tabel 2.1 s.d Tabel 3.2; Gambar 3.1 s.d Gambar 4.19

[1.] Mahasiswa Prodi D-III Teknologi Informasi Politeknik 'Aisyiyah Pontianak

[2.] Dosen Politeknik 'Aisyiyah Pontianak

IMPLEMENTATION OF DENIAL OF SERVICE (DOS) ATTACK IDENTIFICATION BASED ON BRUTE FORCE USING WIRESHARK

Salsha Febrianinda [1], Muhammad Faqih Dzulqarnain[2], Irwan Adhi Prasetya[3]

ABSTRACT

Introduction: Cybercrime poses a significant threat to human life, making it challenging for organizations and governments to tackle crimes committed through computer technology. These crimes have adverse effects on society, businesses, banks, and other sectors. Two common types of cybercrime that often occur within networks and systems are Denial of Service (DOS) Attacks and Brute Force Attacks. To mitigate and prevent the impact of cyber attacks in the digital world, cybersecurity is essential. Cybersecurity aims to prevent and protect computer systems and data. Method: Anomaly-based Detection: This method involves monitoring packet traffic and comparing it to the system's normal traffic patterns (baseline) to detect intrusions. If suspicious traffic that deviates from the baseline is detected, it will be identified, and an alert will be sent to the administrator, along with preventive actions. Due to the presence of a baseline, this detection method can identify new types of attacks entering the system. Result and Conclusion: The implementation of mitigation measures against Denial of Service (DoS) attacks based on brute force using Wireshark is effective in detecting suspicious network traffic. Wireshark can deeply analyze the data packets passing through the network, allowing for quick and accurate identification of attacks.

Keywords **:** Brute force, Denial of Service attack, cyber crime.
Literature **:** 16 Journals (2019-2024)
Pages **:** xi; 60 Pages; Table 2.1 to Table 3.2; Picture 3.1 to Picture 4.19

[1.] Mahasiswa Prodi D-III Teknologi Informasi Politeknik ‘Aisyiyah Pontianak

[2.] Dosen Politeknik ‘Aisyiyah Pontianak

KATA PENGANTAR

Segala puji bagi Allah SWT yang telah memberikan segala pertolongan dan ampunan. Shalawat dan salam juga semoga tercurahkan dan dilimpahkan kepada Nabi Muhammad SAW sehingga peneliti dapat menyelesaikan Laporan Tugas Akhir yang berjudul **"IMPELEMENTASI IDENTIFIKASI SERANGAN *DENIAL OF SERVICE* (DOS) BERBASIS *BRUTE FORCE* MENGGUNAKAN WIRESHARK"**.

Peneliti menyadari bahwa keberhasilan penyusunan Laporan Tugas Akhir ini tidak lepas dari bimbingan dan dukungan pihak-pihak yang telah membantu peneliti. Oleh karena itu, peneliti ingin menyampaikan ucapan terima kasih kepada semua pihak yang telah membantu terlaksana dan terselesaikannya Laporan Tugas Akhir ini kepada:

1. Ibu Tilawaty Aprina, S.ST., M.Kes., selaku Direktur Politeknik 'Aisyiyah Pontianak.
2. Kedua Orang Tua dan keluarga peneliti yang telah memberikan dukungan materi dan non-materi kepada peneliti.
3. Bapak Irwan Adhi Prasetya, S.T., M.T, selaku Ketua Program Studi D-III Teknologi Informasi.
4. Bapak Muhammad Faqih Dzulqarnain, S.T., M.Cs, selaku Pembimbing dan Penguji 2 yang telah memberikan bimbingan dan masukan pada penyusunan Laporan Tugas Akhir ini.
5. Bapak/Ibu Irwan Adhi Prasetya, S.T., M.T, selaku Ketua Penguji yang telah memberikan masukan pada penyusunan Laporan Tugas Akhir ini.
6. Pihak lain yang telah membantu penyusunan Laporan Tugas Akhir ini.

Penyusunan Laporan Tugas Akhir ini diharapkan dapat memberikan pengetahuan dan penerapan ilmu yang telah diperoleh di lingkungan pendidikan peneliti kepada masyarakat untuk dipraktikkan lebih lanjut. Peneliti juga menyadari bahwa penyusunan laporan ini masih terdapat ketidaksempurnaan, oleh karena itu peneliti mengharapkan kritik dan saran sebagai perbaikan kedepannya dari laporan ini.

Pontianak, 10 Juli 2024

Peneliti

Salsha Febrianinda

DAFTAR ISI

LEMBAR PERSETUJUAN ..... **ii**

LEMBAR PENGESAHAN ..... **iii**

PERNYATAAN KEASLIAN TUGAS AKHIR ..... **iv**

INTISARI ..... **v**

ABSTRACT ..... **vi**

KATA PENGANTAR ..... **vii**

DAFTAR ISI ..... **viii**

DAFTAR GAMBAR ..... **x**

DAFTAR TABEL **11**

BAB I PENDAHULUAN ..... Error! Bookmark not defined.

1.1 Latar Belakang ..... **Error! Bookmark not defined.**

1.2 Rumusan Masalah ..... **Error! Bookmark not defined.**

1.3 Tujuan Penelitian ..... **Error! Bookmark not defined.**

1.4 Ruang Lingkup ..... **Error! Bookmark not defined.**

BAB II TINJAUAN PUSTAKA ..... Error! Bookmark not defined.

2.1 Landasan Teori ..... **Error! Bookmark not defined.**

2.1.1 *Cyber Security* ..... **Error! Bookmark not defined.**

2.1.3 *Brute force* ..... **Error! Bookmark not defined.**

2.1.4 *Denial of Service* (DOS) *Attack* ..... **Error! Bookmark not defined.**

2.1.5 Wireshark ..... **Error! Bookmark not defined.**

2.2. *Literature Review* ..... **Error! Bookmark not defined.**

BAB III METODOLOGI PENELITIAN ..... Error! Bookmark not defined.

3.1 Metode Pembangunan/Perancangan ..... **Error! Bookmark not defined.**

3.1.1 Spesifikasi Perangkat Keras ..... **Error! Bookmark not defined.**

3.2 Diagram Rancangan Penelitian ..... **Error! Bookmark not defined.**

3.3 Perancangan *Unified Modeling Language* (UML) **Error! Bookmark not defined.**

3.3.1 *Use Case Diagram* ..... **Error! Bookmark not defined.**
3.3.2 *Sequence Diagram* ..... **Error! Bookmark not defined.**
3.4 Rancangan Antar muka ..... **Error! Bookmark not defined.**
3.5 Rancangan Pengujian ..... **Error! Bookmark not defined.**
3.5.1 Matriks Evaluasi ..... **Error! Bookmark not defined.**
3.5.2 *Anomaly-Based Intrusion Detection System* (IDS) ..... **Error! Bookmark not defined.**
BAB IV HASIL DAN PEMBAHASAN ..... Error! Bookmark not defined.
4.1 Hasil Penelitian ..... **Error! Bookmark not defined.**
4.1.1 *Filter Packet* ..... **Error! Bookmark not defined.**
4.1.2 Pencarian ..... **Error! Bookmark not defined.**
4.1.3 Hasil Pencarian ..... **Error! Bookmark not defined.**
4.2 Pembahasan Penelitian ..... **Error! Bookmark not defined.**
4.2.1 *Filter Packet* ..... **Error! Bookmark not defined.**
4.2.1 Pencarian ..... **Error! Bookmark not defined.**
4.3 Hasil Pengujian ..... **Error! Bookmark not defined.**
BAB V PENUTUP ..... Error! Bookmark not defined.
5.1 Kesimpulan ..... **Error! Bookmark not defined.**
5.2 Saran ..... **Error! Bookmark not defined.**
DAFTAR PUSTAKA ..... Error! Bookmark not defined.

DAFTAR GAMBAR

Gambar 3.1 Diagram *Flowchart* .....**Error! Bookmark not defined.**
Gambar 3.2 *Use Case Diagram* .....**Error! Bookmark not defined.**
Gambar 3.3 *Sequence Diagram* .....**Error! Bookmark not defined.**
Gambar 3.4 Struktur Analisa .....**Error! Bookmark not defined.**
Gambar 4.1 *Filter port* 443 .....**Error! Bookmark not defined.**
Gambar 4.2 *Filter port* 49696 .....**Error! Bookmark not defined.**
Gambar 4.3 *Filter port* 1443 .....**Error! Bookmark not defined.**
Gambar 4.4 *Filter port* 138 .....**Error! Bookmark not defined.**
Gambar 4.5 *Filter port* 137 .....**Error! Bookmark not defined.**
Gambar 4.6 *Filter port* 53 .....**Error! Bookmark not defined.**
Gambar 4.7 *Filter port* 445 .....**Error! Bookmark not defined.**
Gambar 4.8 *Filter port* 80 .....**Error! Bookmark not defined.**
Gambar 4.9 Aktivitas paket SMB .....**Error! Bookmark not defined.**
Gambar 4.10 Aksi dari *attacker* .....**Error! Bookmark not defined.**
Gambar 4.11 Perpindahan *host* .....**Error! Bookmark not defined.**
Gambar 4.12 VMWare *attacker*.....**Error! Bookmark not defined.**
Gambar 4.13 *Lateral movement*.....**Error! Bookmark not defined.**
Gambar 4.14 *Log out* dari sesi "ssales" .....**Error! Bookmark not defined.**
Gambar 4.15 *Attacker* berpindah ke user "IEUser"**Error! Bookmark not defined.**
Gambar 4.16 *Attacker* menjalankan NetBIOS**Error! Bookmark not defined.**
Gambar 4.17 *Log off* dari sesi "IEUser" .....**Error! Bookmark not defined.**
Gambar 4.18 *Attacker* mencoba untuk *login* ke *user* "kosong"..... **Error! Bookmark not defined.**
Gambar 4.19 *Log off session*.....**Error! Bookmark not defined.**

DAFTAR TABEL

Tabel 2.1 Perbandingan Penelitian.....**Error! Bookmark not defined.**

Tabel 3.1 Spesifikasi Perangkat Keras……..**Error! Bookmark not defined.**

Tabel 3.2 Tabel *Matrix* Evaluasi Deteksi Sistem..**Error! Bookmark not defined.**