|  |  |  |
| --- | --- | --- |
| `Topik Capstone | **Topik Capstone** | |
| Siklus / Tahun | **Gasal (Nov) atau Genap (Mei) / 2022** | |
| Judul Dokumen | **Capstone TA**  Judul Capstone Proyek kelompok | |
| Jenis Dokumen | **PENGUJIAN PRODUK**  Catatan: Penggunaan dan penyebaran dokumen ini dikendalikan oleh Departemen Teknik Komputer Universitas Diponegoro | |
| Nomor Dokumen | **C500.[NoRev]TA[tahun].[1/2].[KodeKelompok]** | |
| Nomor Revisi | **NoRev** | |
| Nama File | **KodeKelompok.doc** | |
| Tanggal Penerbitan | **Tanggal Penerbitan** | |
| Unit Penerbit | **Departemen Teknik Komputer Universitas Diponegoro** | |
| Jumlah Halaman | **Jumlah Halaman** | Tidak termasuk sampul |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Data Pengusul** | | | | |
| Pengusul | Nama |  | Jabatan | Anggota |
|  | NIM |  |  |  |
|  | Tanggal |  | Tanda Tangan |  |
|  | Nama |  | Jabatan | Anggota |
|  | NIM |  |  |  |
|  | Tanggal |  | Tanda Tangan |  |
|  | Nama |  | Jabatan | Anggota |
|  | NIM |  |  |  |
|  | Tanggal |  | Tanda Tangan |  |
| Pembimbing 1 (Utama) | Nama |  | Tanda Tangan |  |
|  | Tanggal | **NIP.** |  |  |
| Pembimbing 2 | Nama |  | Tanda Tangan |  |
|  | Tanggal | **NIP.** |  |  |

|  |  |
| --- | --- |
| Versi, Tanggal, Oleh | Perbaikan |
|  |  |

**Daftar Isi**

[1. Pendahuluan 4](#_Toc188032160)

[1.1. Ringkasan isi dokumen 4](#_Toc188032161)

[1.2. Aplikasi Dokumen 4](#_Toc188032162)

[1.3. Referensi 4](#_Toc188032163)

[1.4. Daftar Singkatan 4](#_Toc188032164)

[2. Pengujian 4](#_Toc188032165)

[2.1. Pengujian model 4](#_Toc188032166)

[2.2. Pengujian Aplikasi 5](#_Toc188032167)

# **Pendahuluan**

## **Ringkasan isi dokumen**

*Isi Ringkasan Dokumen*

## **Aplikasi Dokumen**

*Dokumen ini berlaku berfungsi untuk menjelaskan:*

1. *Tahap pengujian produk yang telah dibuat dalam dokumen C300 dan C400*
2. *Acuan keberhasilan produk sesuai spesifikasi yang telah dijabarkan dalam dokumen C200*
3. *Menjadi catatan pengerjaan dan proses pengujian produk yang dilakukan*
4. *Catatan proses pengerjaan dan revisi yang sedang berlangsung*

## **Referensi**

## **Daftar Singkatan**

# **Pengujian**

## **Pengujian model**

*Jelaskan hasil pengujian tentang bagaimana model yang digunakan diuji, rumus pengujian, dan perhitungan presisinya.*

**Contoh:**

Pengujian dilakukan hanya menggunakan dataset yang telah ada. Pengujian algoritma deteksi menggunakan dataset CIC-IDS-2017, CSE-CIC-IDS2018, dan CICDDoS2019. Dataset ini mencakup trafik normal dan serangan Slow DoS dan DRDoS.

Recall atau sensitivitas (juga disebut True Positive Rate) adalah metrik yang mengukur proporsi serangan yang diidentifikasi dengan benar relatif terhadap serangan yang sebenarnya dalam lalu lintas sampel. Hal ini dicapai melalui penerapan persamaan berikut:

𝑅𝑒𝑐𝑎𝑙𝑙 = 𝑇𝑃/𝑇𝑃 + 𝐹𝑁

Precision atau ketepatan adalah kemampuan sistem dalam memastikan bahwa apa yang diidentifikasi sebagai serangan benar-benar adalah serangan. Precision dihitung dengan menggunakan persamaan berikut:

𝑃𝑟𝑒𝑐𝑖𝑠𝑖𝑜𝑛 = 𝑇𝑁/𝑇𝑁 + 𝐹𝑃

F1 Score adalah ombinasi dari precision dan recall, memberikan gambaran keseluruhan tentang keseimbangan antara keduanya Precision dihitung dengan menggunakan persamaan berikut:

𝐹1 𝑆𝑐𝑜𝑟𝑒 = 2 \* 𝑃𝑟𝑒𝑐𝑖𝑠𝑖𝑜𝑛 + 𝑅𝑒𝑐𝑎𝑙𝑙/𝑃𝑟𝑒𝑐𝑖𝑠𝑖𝑜𝑛 \* 𝑅𝑒𝑐𝑎𝑙𝑙

Akurasi sistem deteksi didefinisikan sebagai persentase deteksi akurat yang dilakukan pada aliran lalu lintas sampel. Metrik ini dihitung dengan menggunakan persamaan berikut:

𝐴𝑐𝑐𝑢𝑟𝑎𝑐𝑦 = 𝑇𝑃 + 𝑇𝑁/𝑇𝑃 + 𝐹𝑁 + 𝐹𝑃 + 𝐹𝑁

Tabel 2.9 Hasil pengujian sistem deteksi DoS dengan Ensemble Stacking menggunakan Test Set

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Dataset** | **Recall** | **Precision** | **F1-Score** | **Akurasi** |
| CIC-IDS2017  CSE-CIC-IDS2018 | 99,98804% | 99,98801% | 99,988013% | 99,988041% |
| CIC-DDOS2019 | 99,97972948% | 99,97972952% | 99,97972948% | 99,97972946% |

Tabel 2.9 menunjukkan hasil dari pengetesan sistem deteksi DoS berdasarkan Test Set Performa ensemble stacking menunjukkan performa yang baik dengan akurasi sebesar 99,9880413%, presisi sebesar 99,9880193%, F1 score sebesar 99,9880139%, recall sebesar 99,9880413%.

Hasil dari pengetesan sistem deteksi reflection-based DDoS berdasarkan Test Set Performa ensemble stacking menunjukkan performa yang baik dengan akurasi sebesar 99,97972948% presisi sebesar 99,97972952%, F1 score sebesar 99,97972948%, recall sebesar 99,97972946%.

## **Pengujian Aplikasi**

*Jelaskan hasil pengujian aplikasi yang meliputi aspek fungsional, keamanan, waktu respon, dan portabilitas (jika memungkinkan) dengan skenario yang telah direncanakan.*

**Contoh:**

Melakukan pengujian aplikasi setelah melakukan implementasi dalam pengembangan perangkat lunak React Js, Html dan Javascript. Pada tahapan ini memiliki fungsi dan tujuan untuk memastikan bahwa aplikasi yang dikembangkan bisa berjalan sesuai dengan fungsinya dan tidak mengalami kegagalan selama sistem berjalan. Sehingga bisa dipastikan bahwa sistem berjalan sesuai dengan kebutuhan pengguna. Metode pengujian aplikasi yang digunakan adalah Black Box Testing.

1. **Pengujian Fungsional Sistem dengan *Black Box Testing***

Pengujian dengan metode Black Box testing adalah suatu pendekatan di mana pengujian dilakukan tanpa memerhatikan struktur internal atau logika implementasi dari suatu sistem atau perangkat lunak [3]. Fokus utama dari Black Box testing adalah pada input yang diberikan dan output yang dihasilkan, tanpa memperhatikan cara sistem mencapai hasil tersebut. Tujuannya adalah untuk mengevaluasi fungsionalitas dan respons sistem tanpa memerlukan pengetahuan detail tentang kode sumbernya. Black Box testing efektif dalam mengidentifikasi bug atau kesalahan yang mungkin terjadi pada tingkat fungsionalitas atau antarmuka pengguna.

1. **Pengujian Autentikasi**

Pada pengujian fitur autentikasi untuk Administrator menjelaskan tentang hasil pengujian pada halaman Sign In, dan Sign Out pada sistem. Penjelasan terkait hasil pengujian ini terdapat pada Tabel 2.1.

Tabel 2.1. Pengujian Fitur Autentikasi

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **SRS-id** | **Kode Pengujian** | **Nama Pengujian** | **Bentuk Pengujian** | **Hasil yang Diharapkan** | **Hasil Pengujian** |
| (dipetakan dengan SRS-id yang ada di C-300) | A101 | *Sign in* ke sistem. | Memasukkan nama pengguna dan kata sandi akun Administrator. | Sistem menampilkan halaman *dashboard* sistem. | Berhasil |
|  | A102 | Validasi data pada *form sign in.* | Memasukkan *username* dan *password* yang tidak terdaftar dalam sistem. | Sistem membatalkan proses *sign in* dan memberikan pesan peringatan/*invalid credentials* kepada pengguna. | Berhasil |
|  | A103 | *Sign out* dari sistem. | Melakukan *logout* dari menu *account* yang terdapat halaman *dashboard* | Sistem menampilkan halaman *login* | Berhasil |

Berdasarkan Tabel 2.1 yang memuat pengujian black box pada fitur Autentikasi untuk Administrator didapatkan hasil yang fungsional. Fungsi tersebut sudah berjalan dengan baik sesuai dengan hasil yang diharapkan.

1. **Pengujian Fitur**

Pada pengujian aplikasi untuk Administrator menjelaskan tentang hasil pengujian setiap halaman pada sistem. Penjelasan terkait hasil pengujian ini terdapat pada Tabel 2.8.

Tabel 2.8 Pengujian aplikasi

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **SRS-id** | **Kode**  **Pengujian** | **Nama**  **Pengujian** | **Bentuk Pengujian** | **Hasil yang Diharapkan** | **Hasil**  **Pengujian** |
| (dipetakan dengan SRS-id yang ada di C-300) | A201 | Melihat data grafik pada *Dashboard* | Administrator dapat melihat data grafik pada halaman *Dashboard* | Halaman *Dashboard* menampilkan data grafik sesuai yang diharapkan | Berhasil |
|  | A202 | Melihat *table summary* pada *Dashboard* | Administrator dapat melihat tabel *summary* dari serangan siber yang terdeteksi | Halaman *Dashboard* menampilkan tabel *summary* sesuai yang diharapkan | Berhasil |
|  | A203 | Melihat grafik serangan siber dalam satuan waktu pada *Dashboard* | Administrator dapat melihat grafik serangan siber dalam satuan waktu | Halaman *Dashboard* menampilkan data grafik serangan siber dalam satuan waktu sesuai yang diharapkan | Berhasil |
|  | A204 | Melihat *bar chart* pada *Dashboard* | Administrator dapat melihat *bar chart* dari IP yang terkena serangan siber | Halaman *Dashboard*  menampilkan data *bar chart* sesuai yang diharapkan | Berhasil |
|  | A205 | Melihat data *bar chart Top IP Attacker* pada menu *Distribution Attack* | Administrator dapat melihat *bar chart Top IP Attacker* | Halaman menu *Distribution Attack* menampilkan data *top ip attackers* sesuai dengan yang diharapkan | Berhasil |
|  | A206 | Melihat data *bar chart Top IP Targets* pada menu D*istribution Attack* | Administrator dapat melihat bar chart *Top IP Targets* | Halaman menu *Distribution 1 Attack* menampilkan data *top ip targets* sesuai dengan yang diharapkan | Berhasil |
|  | A207 | Melihat data *pie chart Top 2 Attack Detection p*ada menu *Distribution Attack* | Administrator dapat melihat pie chart *Top 2 Attack Detection* | Halaman menu *Distribution 1 Attack* menampilkan data *top 2 attack detection* sesuai dengan yang diharapkan | Berhasil |
|  | A208 | Melihat tabel *Alerts Summary p*ada menu *Distribution Attack* | Administrator dapat melihat tabel *Alerts Summary* | Halaman menu *Distribution 1 Attack* menampilkan data *top 2 attack detection* sesuai dengan yang diharapkan | Berhasil |
|  | A209 | Melihat data pada *chart bar Source IP Distribution* menu *IP* Distribution | Administrator dapat melihat *chart bar Source IP Distribution* | Halaman menu *Distribution Attack* menampilkan data *source ip distribution* sesuai dengan yang diharapkan | Berhasil |
|  | A210 | Melihat data *chart bar Destination IP*  *Distribution* pada menu *IP Distribution* | Administrator dapat melihat *chart bar Destination IP Distribution* | Halaman menu *destination ip distribution* menampilkan data *top ip targets* sesuai dengan yang diharapkan | Berhasil |
|  | A211 | Melihat data pada menu *Port Distribution* | Administrator dapat melihat *bar chart Most Attacker Port* | Halaman menu P*ort Distribution* menampilkan data *most attacker port.* sesuai dengan yang diharapkan | Berhasil |
|  | A212 | Melihat data *bar chart Most Attacked Port* pada menu *Port Distribution* | Administrator dapat melihat *bar chart Most Attacked Port* | Halaman menu *Port Distribution* menampilkan data *most attacked port* sesuai dengan yang diharapkan | Berhasil |
|  | A213 | Melihat data tabel *Summary Most Attacker Port* pada menu *Port* Distribution | Administrator dapat melihat tabel *Summary Most Attacker Port* | Halaman menu *Port Distribution* menampilkan data *summary most attacker ports* Sesuai dengan yang diharapkan | Berhasil |
|  | A214 | Melihatdata tabel *Summary Most Attacked Port* pada menu *Port* Distribution | Administrator dapat melihat tabel *Summary Most Attacked Port* | Halaman menu *Port Distribution* menampilkan data *summary most attacked port.* Sesuai dengan yang diharapkan | Berhasil |

Berdasarkan Tabel 2.8 yang memuat pengujian *black box* pada fitur Dashboard untuk Administrator didapatkan hasil yang fungsional. Fungsi tersebut sudah berjalan dengan baik sesuai dengan hasil yang diharapkan.

1. **Pengujian Non-Fungsional**
2. **Pengujian *Portability***

Pada proyek ini, dilakukan suatu pengujian Portablitias terhadap sistem Sistem Monitoring dan Deteksi Serangan DoS/DRDoS Berbasiskan Ensemble Learning menggunakan ELK Stack. Tujuannya adalah untuk memastikan bahwa aplikasi ini dapat berfungsi dengan baik di berbagai sistem operasi, khususnya Windows dan Ubuntu, serta diakses melalui web browser yang umum digunakan seperti Google Chrome, Mozilla Firefox, dan Microsoft Edge. Pengujian ini akan mengidentifikasi apakah ada kendala teknis atau perbedaan performa yang signifikan yang dapat mempengaruhi pengalaman pengguna saat mengoperasikan aplikasi di platform yang berbeda. Dengan demikian, pengujian ini tidak hanya bertujuan untuk menilai kompatibilitas teknis tetapi juga untuk memastikan bahwa aplikasi mampu memberikan pengalaman yang konsisten dan aman bagi pengguna di berbagai lingkungan.

A screenshot of a computer

Description automatically generated

Gambar 2.1 Hasil uji portabilitas pada Chrome Windows

A screenshot of a computer

Description automatically generated

Gambar 2.2 Hasil uji portabilitas pada Microsoft Edge Windows

A screenshot of a computer

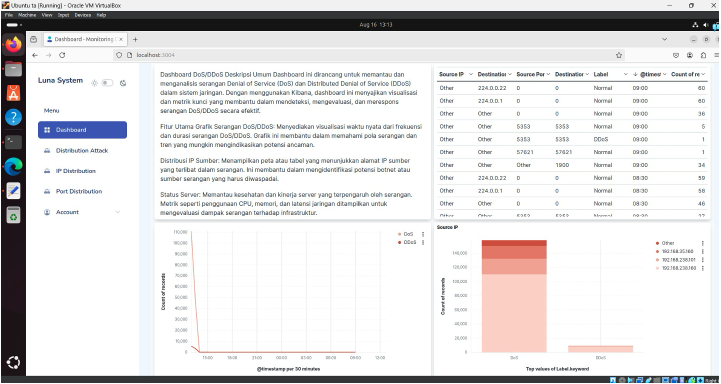
Description automatically generated

Gambar 2.3 Hasil uji portabilitas pada Mozilla Firefox Windows

Tabel 2.3 Pengujian Portabilitas pada Windows

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Komponen** | **Windows 10 – Chrome** | **Windows 10 – Firefox** | **Windows 10 – Edge** | **Windows 11 - Edge** |
| Tampilan UI | Konsisten | Konsisten | Konsisten | Konsisten |
| Fungsi *Monitoring* | Berfungsi | Berfungsi | Berfungsi | Berfungsi |
| Grafik Visualisasi | Ditampilkan dengan benar | Ditampilkan dengan benar | Ditampilkan dengan benar | Ditampilkan dengan benar |
| CORS | Tidak ada masalah | Tidak ada masalah | Tidak ada masalah | Tidak ada masalah |

Selanjutnya dilakukan uji portabilitas pada sistem operasi Ubuntu.



Gambar 2.4 Hasil uji portabilitas pada Mozilla Firefox Ubuntu

A screenshot of a computer

Description automatically generated

Gambar 2.5 Hasil uji portabilitas pada Edge Ubuntu

A screenshot of a computer

Description automatically generated

Gambar 2.6 Hasil uji portabilitas pada Chrome Ubuntu

Tabel 2.4 Pengujian portabilitas pada Ubuntu

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Komponen** | **Ubuntu 24.04 – Chrome** | **Ubuntu 24.04 – Firefox** | **Ubuntu 24.04 – Edge** | **Ubuntu 24.04 – Chrome** |
| Tampilan UI | Konsisten | Konsisten | Konsisten | Konsisten |
| Fungsi *Monitoring* | Berfungsi | Berfungsi | Berfungsi | Berfungsi |
| Grafik Visualisasi | Ditampilkan dengan benar | Ditampilkan dengan benar | Ditampilkan dengan benar | Ditampilkan dengan benar |
| CORS | Tidak ada masalah | Tidak ada masalah | Tidak ada masalah | Tidak ada masalah |

Pengujian yang dilakukan pada Sistem ini menunjukkan bahwa aplikasi memiliki tingkat portability yang baik ketika diakses melalui sistem operasi Windows dan Ubuntu, serta di berbagai web browser seperti Google Chrome, Mozilla Firefox, dan Microsoft Edge. Secara umum, tidak ada masalah signifikan yang menghambat fungsionalitas inti dari sistem, dan aplikasi berhasil berfungsi sesuai dengan harapan di semua kombinasi sistem operasi dan browser yang diuji.

1. **Pengujian Response Time**

Pada pengujian ini, fokus utama adalah untuk mengevaluasi kinerja Sistem dalam merespons berbagai interaksi pengguna. Pengujian dilakukan dengan mengukur waktu muat halaman, dan waktu render grafik pada berbagai kombinasi sistem operasi (Windows dan Ubuntu) dan web browser (Google Chrome, Mozilla Firefox, dan Microsoft Edge). Hasil pengujian ini akan memberikan wawasan tentang seberapa efisien aplikasi dalam menyajikan data dan memberikan pengalaman yang optimal kepada pengguna.

Tabel 2.5 Pengujian *Response Time*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Pengujian** | **Ubuntu 24.04 – Chrome** | **Ubuntu 24.04 – Firefox** | **Windows 10 - Chrome** | **Windows 10 – Edge** | **Windows 10 – Firefox** |
| Waktu muat halaman | 4 detik | 4,5 detik | 4 detik | 5 detik | 4 detik |
| Waktu *render* grafik | 1 detik | 900 milidetik | 1,3 detik | 1 detik | 960 milidetik |
| Waktu respon Kibana | 3 detik | 3 detik | 3,3 detik | 2,5 detik | 2,5 detik |

Berdasarkan pengujian yang dilakukan, sistem ini menunjukkan kinerja waktu respons yang memuaskan di berbagai platform yang diuji. Secara umum, waktu muat halaman berada dalam kisaran 3 hingga 4 detik, menunjukkan bahwa aplikasi mampu memuat konten dengan cepat di semua kombinasi sistem operasi dan browser.

1. **Pengujian *Safety***

Pengujian ini dirancang untuk mengidentifikasi dan mengatasi potensi kelemahan yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab. Selain itu, pengujian juga mengevaluasi bagaimana aplikasi menangani konfigurasi kritis seperti penggunaan CORS dan protokol HTTP di lingkungan pengembangan, serta bagaimana kesiapan aplikasi ini ketika dipindahkan ke lingkungan produksi. Langkah-langkah pengujian ini akan memberikan gambaran yang jelas tentang tingkat keamanan yang telah dicapai oleh aplikasi, serta rekomendasi untuk peningkatan lebih lanjut.

Tabel 2.6 Pengujian *safety*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Pengujian** | **Ubuntu 24.04 – Chrome** | **Ubuntu 24.04 – Firefox** | **Windows 10 – Chrome** | **Windows 10 - Firefox** |
| CORS *Configuration* | CORS dikonfigurasi dengan benar, akses hanya dari domain yang sah | CORS dikonfigurasi dengan benar, akses hanya dari domain yang sah | CORS dikonfigurasi dengan benar, akses hanya dari domain yang sah | CORS dikonfigurasi dengan benar, akses hanya dari domain yang sah |
| Proteksi Data (HTTP) | HTTP digunakan pada *localhost,* risiko rendah di pengembangan | HTTP digunakan pada *localhost,* risiko rendah di pengembangan | HTTP digunakan pada *localhost,* risiko rendah di pengembangan | HTTP digunakan pada *localhost,* risiko rendah di pengembangan |
| *Vulnerability Scanning* | Tidak ada kerentanan serius | Tidak ada kerentanan serius | Tidak ada kerentanan serius | Tidak ada kerentanan serius |
| *Incident Response* | Deteksi cepat, *logging* lengkap | Deteksi cepat, *logging* lengkap | Deteksi cepat, *logging* lengkap | Deteksi cepat, *logging* lengkap |

Berdasarkan hasil pengujian keamanan, aplikasi ini menunjukkan tingkat kesiapan yang baik dalam menghadapi ancaman keamanan. Meskipun aplikasi saat ini beroperasi di localhost dengan HTTP, pengujian menunjukkan bahwa konfigurasi CORS telah diatur dengan baik, membatasi akses hanya pada domain yang sah. Selain itu, hasil pengujian menunjukkan bahwa tidak ada kerentanan serius yang terdeteksi, dan aplikasi mampu menangani insiden keamanan dengan respons yang cepat dan efisien.

1. **Pengujian *Security***

Pengujian ini bertujuan untuk mengidentifikasi kerentanan potensial, memastikan konfigurasi keamanan yang tepat, dan menguji respons sistem terhadap berbagai serangan dan ancaman. Dengan hasil pengujian ini, kita dapat menilai efektivitas langkah-langkah keamanan yang diimplementasikan dan memberikan rekomendasi untuk perbaikan lebih lanjut.

Tabel 2.7 Pengujian *security*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Pengujian** | **Ubuntu 24.04 – Chrome** | **Ubuntu 24.04 – Firefox** | **Windows 10 – Chrome** | **Windows 10 - Firefox** |
| Autentikasi dan Otorisasi | Akses dan autentikasi terkontrol | Akses dan autentikasi terkontrol | Akses dan autentikasi terkontrol | Akses dan autentikasi terkontrol |
| Konfigurasi keamanan | Konfigurasi aman | Konfigurasi aman | Konfigurasi aman | Konfigurasi aman |
| *Vulnerability Scanning* | Tidak ada kerentanan serius | Tidak ada kerentanan serius | Tidak ada kerentanan serius | Tidak ada kerentanan serius |

Berdasarkan hasil pengujian keamanan, Sistem ini menunjukkan tingkat keamanan yang sangat baik di berbagai platform. Aplikasi ini bebas dari kerentanan serius, memiliki mekanisme autentikasi yang kuat, dan melindungi data sensitif dengan enkripsi yang memadai. Pengujian penetrasi mengonfirmasi bahwa aplikasi cukup tangguh terhadap serangan yang disimulasikan, dan konfigurasi keamanan telah diterapkan dengan benar untuk melindungi terhadap potensi ancaman.