Jurnal Ilmiah Universitas Batanghari Jambi
Volume 26, Issue 01, Februari 2026, 271-279
Webite: https://ji.unbari.ac.id, E-Mail: jiubj.unbari@gmail.com
e-ISSN: 2549-4236 (Online), p-ISSN: 1411-8939 (Print), DOI: 10.33087/jiubj.v26i1.6425

Penerapan Algoritma *Isolation Forest* dan Metode *Rule Based* untuk Deteksi Serangan *Brute Force*

Muhammad Rifky Dharmawan, Evasaria Magdalena Sipayung
Program Studi Informatika, Fakultas Teknologi dan Desain, Universitas Bunda Mulia
Correspondence: rifkydhar102@gmail.com, 1874@lecturer.ubm.ac.id

ABSTRAK
Serangan *brute force* merupakan salah satu bentuk serangan siber yang masih sering ditemukan pada layanan autentikasi jaringan, seperti *Secure Shell* (SSH), *File Transfer Protocol* (FTP), dan aplikasi berbasis web. Serangan ini dilakukan dengan cara mencoba kombinasi username dan password secara berulang hingga memperoleh akses yang valid. Aktivitas *brute force* sering kali sulit dibedakan dari lalu lintas jaringan normal karena memiliki pola komunikasi yang serupa, sehingga diperlukan metode deteksi yang mampu mengidentifikasi pola anomali secara otomatis dari data log jaringan. Penelitian ini mengimplementasikan sistem deteksi serangan *brute force* berbasis analisis log jaringan menggunakan algoritma *Isolation Forest* dan metode *Rule-Based*. Data yang digunakan berasal dari log hasil tangkapan paket jaringan menggunakan *Wireshark* yang diekspor dalam format CSV. Tahap preprocessing dilakukan untuk menyesuaikan struktur data, mengonversi timestamp ke bentuk numerik, serta mengekstraksi fitur tambahan berupa jumlah paket per alamat IP sumber. Algoritma *Isolation Forest* diterapkan untuk mendeteksi aktivitas anomali secara unsupervised tanpa memerlukan data berlabel. Data yang terdeteksi sebagai anomali kemudian diproses menggunakan metode *Rule-Based* untuk mengidentifikasi pola *brute force* berdasarkan kemunculan kata kunci tertentu pada log, jumlah percobaan login, dan jendela waktu yang telah ditentukan. Hasil pengujian menunjukkan bahwa *Isolation Forest* mampu mengidentifikasi aktivitas jaringan yang menyimpang dari pola normal, sementara penerapan metode *Rule-Based* berhasil menyaring anomali yang memiliki karakteristik serangan *brute force.* Kombinasi kedua metode menghasilkan deteksi yang lebih spesifik dan mudah diinterpretasikan, ditunjukkan oleh berkurangnya anomali yang tidak relevan serta teridentifikasinya aktivitas login gagal berulang dari alamat IP yang sama dalam rentang waktu singkat. Sistem juga menampilkan hasil deteksi dalam bentuk tabel dan visualisasi untuk mendukung proses analisis.

Kata kunci: *Brute Force; Isolation Forest; Rule-Based; Wireshark;* Deteksi Anomali; Keamanan Jaringan.

ABSTRACT
Brute force attacks remain one of the most common cyber threats targeting network authentication services such as Secure Shell (SSH), File Transfer Protocol (FTP), and web-based login systems. This type of attack is performed by repeatedly attempting various combinations of usernames and passwords until valid credentials are obtained. Brute force activities are often difficult to distinguish from legitimate network traffic because they exhibit communication patterns similar to normal user behavior. Therefore, an automated detection approach is required to identify abnormal patterns from network log data. This study implements a brute force attack detection system based on network log analysis using the Isolation Forest algorithm and a Rule-Based method. The dataset used in this research consists of network traffic logs captured using Wireshark and exported in CSV format. Data preprocessing was conducted to standardize log structure, convert timestamps into numerical values, and extract additional features, including packet count per source IP address. The Isolation Forest algorithm was applied as an unsupervised anomaly detection method, enabling the identification of abnormal network activities without requiring labeled data. Subsequently, a Rule-Based method was employed as a verification stage to classify detected anomalies as brute force attacks based on predefined rules, such as the presence of specific keywords in log information fields, repeated login attempts, and defined time windows. The experimental results indicate that the Isolation Forest algorithm effectively identifies anomalous network activities that deviate from normal traffic patterns. The application of the Rule-Based method further refines the detection results by filtering anomalies that exhibit brute force characteristics. The combination of both methods produces more specific and interpretable detection outcomes, as demonstrated by the identification of repeated failed login attempts originating from the same source IP within a short time interval. Detection results are presented through tabular outputs and visualizations to support further analysis.

Keywords: *Brute Force; Isolation Forest; Rule-Based; Wireshark; Anomaly Detection; Network Security.*

PENDAHULUAN

Serangan siber merupakan salah satu ancaman utama terhadap keamanan jaringan komputer yang terus mengalami peningkatan baik dari segi teknik maupun intensitas serangan (Stallings, 2020). Salah satu jenis serangan yang masih sering digunakan hingga saat ini adalah serangan *brute force*, yaitu metode serangan yang dilakukan dengan mencoba berbagai kombinasi username dan password secara berulang hingga berhasil memperoleh akses ke sistem target (Raza et al., 2021). Serangan *brute force* sering menargetkan layanan autentikasi seperti SSH, FTP, dan *web login*, terutama pada sistem yang tidak menerapkan mekanisme pengamanan tambahan seperti pembatasan percobaan login atau autentikasi multifaktor (Kurose & Ross, 2021). Meskipun tekniknya tergolong sederhana, *brute force* tetap berbahaya karena dapat dilakukan secara otomatis

menggunakan botnet dan berjalan dalam waktu lama tanpa terdeteksi (Bejtlich, 2014).

Aktivitas *brute force* sering kali sulit dibedakan dari lalu lintas jaringan normal karena memiliki pola komunikasi yang menyerupai aktivitas pengguna sah, sehingga memerlukan teknik analisis yang lebih mendalam untuk mengidentifikasinya (Buczak & Guven, 2021). Oleh karena itu, analisis forensik jaringan menjadi aspek penting dalam mendeteksi dan menginvestigasi serangan ini (Hidayat & Kurniawan, 2021). *Wireshark* merupakan salah satu alat forensik jaringan yang banyak digunakan karena kemampuannya dalam menangkap dan menganalisis paket jaringan secara detail (Wireshark Foundation, 2023). Namun, analisis manual menggunakan Wireshark membutuhkan waktu dan keahlian teknis yang tinggi, sehingga diperlukan pendekatan otomatis berbasis *machine learning* untuk meningkatkan efisiensi dan akurasi deteksi (Cndravathi et al., 2024).

Penelitian ini digunakan algoritma *Isolation Forest* sebagai metode deteksi anomali karena kemampuannya dalam mendeteksi pola tidak normal tanpa memerlukan data berlabel (Liu et al., 2008; Chua et al., 2024). Untuk meningkatkan ketepatan identifikasi serangan *brute force*, hasil deteksi anomali kemudian diverifikasi menggunakan *metode rule-based*, yang memanfaatkan karakteristik umum serangan seperti percobaan login gagal berulang dari satu alamat IP (Mubarok & Romli, 2025).

Kajian Pustaka

Jaringan Komputer

Jaringan komputer adalah sekumpulan perangkat yang saling terhubung dengan tujuan untuk bertukar data dan berbagi sumber daya, baik perangkat keras maupun perangkat lunak. Menurut Kurose & Ross (2021), *computer network* dapat didefinisikan sebagai "*a collection of interconnected devices that exchange data and share resources through communication links and protocols*." Definisi ini menegaskan bahwa komunikasi antarperangkat dalam jaringan bergantung pada media transmisi dan protokol yang disepakati bersama.

Keamanan Jaringan

Keamanan jaringan (*network security*) merupakan seperangkat kebijakan, praktik, dan teknologi yang dirancang untuk melindungi jaringan komputer dan data yang dikirim melalui jaringan tersebut dari akses tidak sah, penyalahgunaan, gangguan, serta serangan. Menurut Stallings (2020), *network security* adalah *"the process of preventing and detecting unauthorized use of your network and ensuring its confidentiality, integrity, and availability*." Tiga aspek utama yang harus dijaga dalam keamanan jaringan adalah kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) yang dikenal sebagai prinsip CIA Triad. Untuk mencapai tujuan tersebut, keamanan jaringan memanfaatkan berbagai mekanisme seperti *firewall* untuk memfilter lalu lintas berbahaya, *Intrusion Detection/Prevention System* (IDS/IPS) untuk mendeteksi dan menghentikan aktivitas mencurigakan, enkripsi untuk melindungi data selama transmisi, serta *Virtual Private Network* (VPN) untuk menyediakan komunikasi yang aman melalui jaringan publik (Khan et al., 2022).

Kejahatan Cyber (Cybercrime)

Kejahatan siber (*cybercrime*) adalah tindakan kriminal yang dilakukan dengan memanfaatkan komputer, perangkat digital, atau jaringan internet sebagai sarana maupun target serangan. Menurut Stallings (2020), *cybercrime* didefinisikan sebagai "*any criminal activity that involves a computer or network, either as the target or as a tool to perpetrate an offense*." Bentuk kejahatan ini meliputi *hacking, phishing*, penyebaran malware dan ransomware, pencurian data, hingga serangan *brute force* yang menargetkan sistem autentikasi.

Autentikasi dan Login

Autentikasi merupakan proses penting dalam sistem keamanan yang digunakan untuk memastikan identitas pengguna sebelum mengakses sumber daya atau layanan tertentu. Menurut Stallings (2020), autentikasi adalah "*the process of verifying the identity of a user or system to ensure that the entity is who it claims to be*." Proses autentikasi umumnya dilakukan melalui mekanisme login dengan menggunakan kombinasi *username* dan *password* sebagai kredensial dasar.

Serangan Brute force

Serangan *brute force* merupakan salah satu metode serangan siber yang dilakukan dengan mencoba seluruh kemungkinan kombinasi kata sandi hingga menemukan kombinasi yang benar. Menurut Schneier (2018), *brute force* attack termasuk dalam kategori serangan eksploratif (*exhaustive search*), di mana penyerang memanfaatkan kemampuan komputasi untuk menebak kredensial autentikasi tanpa memerlukan informasi awal mengenai target.

Machine Learning

Machine Learning merupakan cabang dari kecerdasan buatan yang memungkinkan sistem komputer untuk belajar dari data dan meningkatkan kinerjanya tanpa diprogram secara eksplisit. Menurut Alpaydin (2020), *machine learning* memungkinkan sistem mengidentifikasi pola dan membuat keputusan berdasarkan data historis. Dalam bidang keamanan jaringan, *machine learning* digunakan untuk mendeteksi intrusi, mengklasifikasikan lalu lintas jaringan, dan mengidentifikasi anomali yang berpotensi sebagai serangan (Buczak & Guven, 2021).

Algoritma Anomaly Detection

Anomaly detection merupakan teknik dalam *machine learning* yang bertujuan untuk mengidentifikasi data atau pola yang menyimpang dari perilaku normal

sistem. Menurut Chandola et al. (2021), *anomaly detection* digunakan untuk menemukan kejadian langka yang sering kali mengindikasikan kesalahan sistem atau serangan keamanan. Dalam keamanan jaringan, pendekatan ini sangat efektif untuk mendeteksi serangan yang belum memiliki pola serangan yang dikenal sebelumnya (*unknown attacks*).

Wireshark

Wireshark merupakan aplikasi *open-source* yang digunakan untuk menangkap (*packet capturing*) dan menganalisis paket data pada jaringan komputer. Menurut Wireshark Foundation (2023), Wireshark adalah salah satu *network protocol analyzer* yang paling banyak digunakan karena kemampuannya dalam menampilkan detail paket jaringan secara komprehensif serta mendukung berbagai protokol komunikasi modern.

Algoritma *Isolation Forest*

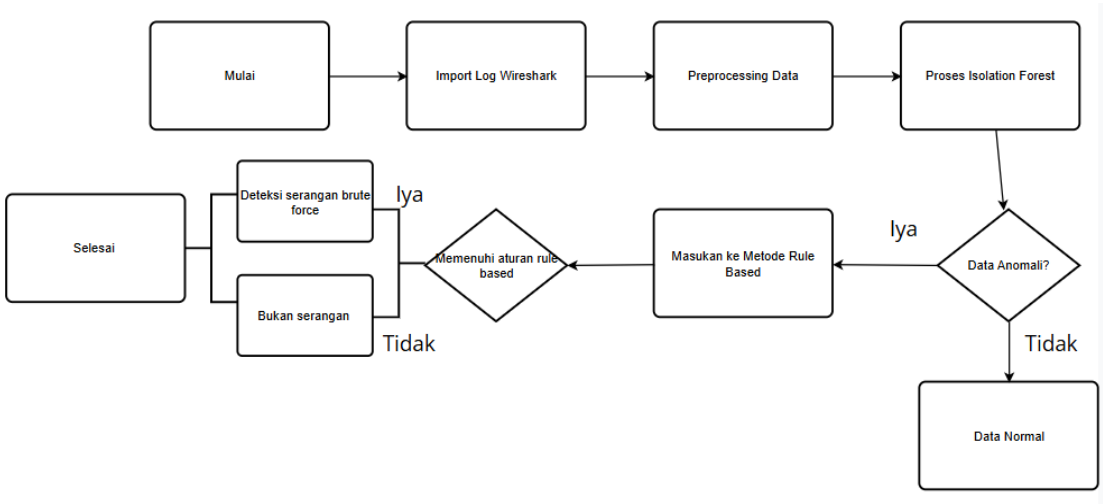
Isolation Forest merupakan algoritma *unsupervised learning* yang digunakan untuk mendeteksi anomali dengan cara mengidentifikasi data yang memiliki pola berbeda dari mayoritas data lainnya. Dalam pendekatan ini, data yang bersifat anomali akan lebih mudah dipisahkan dibandingkan data normal karena memiliki karakteristik yang menyimpang (Chua et al., 2024).

Metode Rule Based

Metode *Rule-Based* merupakan pendekatan deteksi yang menggunakan sekumpulan aturan logis berbentuk *if–then* untuk mengidentifikasi aktivitas mencurigakan berdasarkan pola tertentu dalam data. Pendekatan ini banyak digunakan dalam sistem keamanan jaringan karena bersifat transparan, mudah dipahami, dan dapat langsung diimplementasikan (Buczak & Guven, 2021).

METODE

Pemilihan metode dalam penelitian ini didasarkan pada kebutuhan untuk mendeteksi serangan *Brute force* pada data log jaringan Wireshark yang bersifat tidak berlabel, berukuran besar, dan berpola kompleks, sehingga digunakan pendekatan *anomaly detection* yang efisien dan mudah diinterpretasikan. Penelitian ini mengombinasikan algoritma *Isolation Forest* sebagai tahap deteksi awal anomali karena keunggulannya dalam *unsupervised learning*, skalabilitas tinggi, serta kemampuan menangani data berdimensi tinggi, dengan metode *Rule-Based* sebagai tahap verifikasi untuk memastikan bahwa anomali yang terdeteksi benar-benar merupakan serangan *Brute force* berdasarkan aturan logis yang spesifik dan transparan. Kombinasi dua tahap ini diharapkan mampu meningkatkan akurasi dan interpretabilitas hasil deteksi guna mendukung analisis forensik jaringan. Selain itu, pengembangan sistem menggunakan metode *Rapid Application Development* (RAD) agar proses perancangan, implementasi, dan pengujian dapat dilakukan secara cepat, iteratif, dan adaptif sesuai karakteristik penelitian eksperimental berbasis *machine learning*.



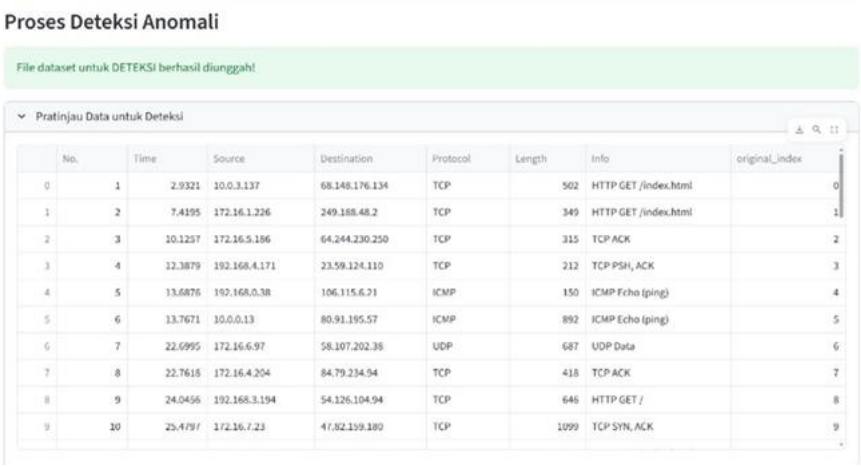
Sumber: data olahan

Gambar 1
***Flowchart* Alur Proses Deteksi**

HASIL

Pengujian Upload Dataset Deteksi.

Pengujian ini bertujuan untuk memastikan bahwa pengguna dapat mengunggah file berformat CSV yang digunakan sebagai dataset untuk proses *training* model *Isolation Forest*. Pada pengujian ini, pengguna melakukan pemilihan file CSV melalui menu unggah yang tersedia pada sidebar aplikasi. Setelah file dipilih, sistem melakukan validasi terhadap format file yang diunggah.

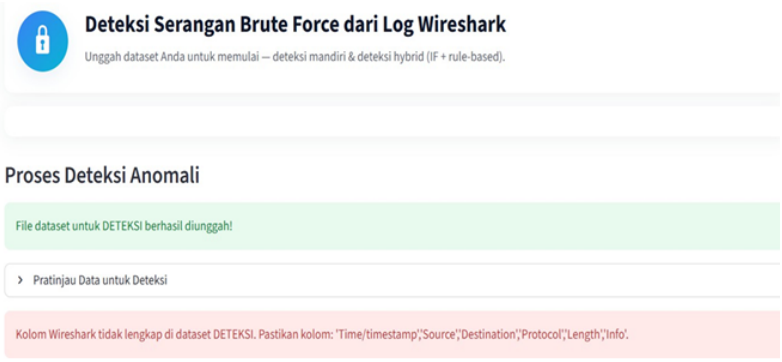


	No.	Time	Source	Destination	Protocol	Length	Info	original_index
0	1	2.9321	10.0.3.137	68.148.176.134	TCP	502	HTTP GET /index.html	0
1	2	7.4195	172.16.1.226	249.188.48.2	TCP	349	HTTP GET /index.html	1
2	3	10.1257	172.16.5.186	64.244.230.250	TCP	315	TCP ACK	2
3	4	12.3879	192.168.4.171	23.59.124.110	TCP	212	TCP PSH, ACK	3
4	5	13.6876	192.168.0.38	106.115.6.21	ICMP	150	ICMP Echo (ping)	4
5	6	13.7671	10.0.0.13	80.91.195.57	ICMP	892	ICMP Echo (ping)	5
6	7	22.6995	172.16.6.97	58.107.202.36	UDP	687	UDP Data	6
7	8	22.7615	172.16.4.204	84.79.234.94	TCP	418	TCP ACK	7
8	9	24.0456	192.168.3.194	54.126.104.94	TCP	646	HTTP GET /	8
9	10	25.4797	172.16.7.23	47.82.159.180	TCP	1099	TCP SYN, ACK	9

Sumber: data olahan

Gambar 2
Pengujian upload dataset valid *(log wireshark)*

Apabila format file sesuai, sistem akan menampilkan pesan keberhasilan serta menampilkan pratinjau data untuk memastikan bahwa dataset berhasil dibaca oleh sistem tanpa mengalami kesalahan seperti pada Gambar 2, apabila pada dataset yang di *upload* tidak terdapat kolom kolom yang dibutuhkan, maka sistem akan menampilkan pesan error seperti yang dapat dilihat pada Gambar 3. Hasil yang diharapkan dari pengujian ini adalah sistem mampu menerima file CSV dengan format yang sesuai, menampilkan pratinjau data, serta tidak menimbulkan pesan kesalahan selama proses unggah berlangsung.

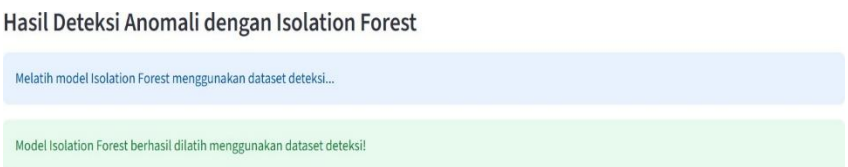


Sumber: data olahan

Gambar 3
Pengujian upload dataset tidak valid

Pengujian Training Model Isolation Forest

Pengujian ini bertujuan untuk memastikan bahwa sistem dapat melakukan proses pelatihan *model Isolation Forest* menggunakan *dataset* yang telah melalui tahap *preprocessing*. Setelah data dinyatakan valid, sistem secara otomatis melatih model menggunakan fitur numerik yang telah ditentukan. Proses training dilakukan tanpa label karena *Isolation Forest* merupakan algoritma *unsupervised learning*. Sistem juga menampilkan notifikasi untuk menunjukkan bahwa proses *training* telah berhasil dilakukan seperti pada Gambar 4. Hasil yang diharapkan dari pengujian ini adalah model *Isolation Forest* dapat dilatih dengan baik menggunakan dataset yang tersedia dan tidak terjadi kesalahan selama proses pelatihan berlangsung.

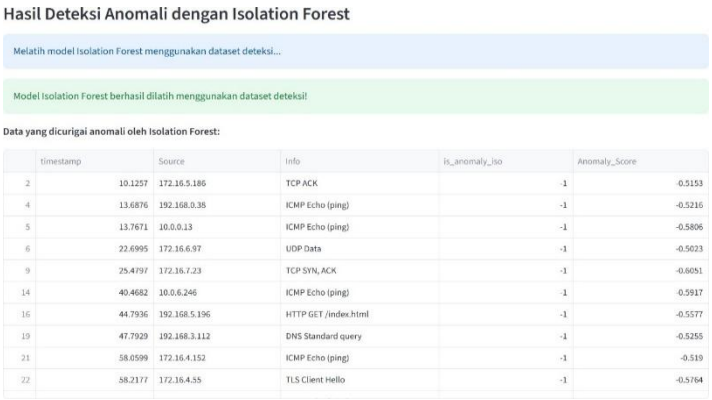


Sumber: data olahan

Gambar 4
Notifikasi berhasil melatih model *Isolation Forest*

Pengujian Deteksi Anomali Menggunakan Isolation Forest

Pengujian ini dilakukan untuk memastikan bahwa sistem mampu menjalankan proses deteksi anomali menggunakan model *Isolation Forest* yang telah dilatih. Sistem melakukan prediksi terhadap data log jaringan dan memberikan label anomali atau normal pada setiap data. Selain itu, sistem juga menghitung nilai *anomaly score* untuk menunjukkan tingkat keanehan suatu data. Hasil deteksi kemudian ditampilkan dalam bentuk Tabel dan ringkasan statistik seperti pada Gambar 5. Hasil yang diharapkan dari pengujian ini adalah sistem mampu mengklasifikasikan data sebagai normal atau anomali secara otomatis dan menampilkan hasil deteksi tanpa mengalami kegagalan proses.


Hasil Deteksi Anomali dengan Isolation Forest

Melatih model Isolation Forest menggunakan dataset deteksi...

Model Isolation Forest berhasil dilatih menggunakan dataset deteksi!

Data yang dicurigai anomali oleh Isolation Forest:

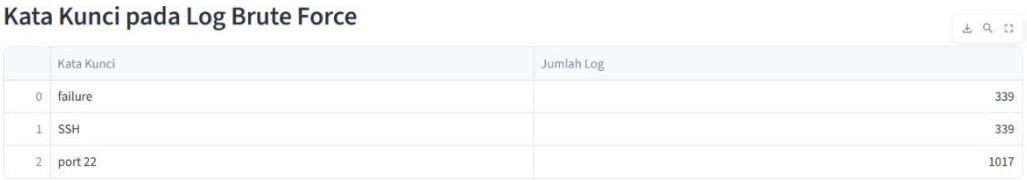
	timestamp	Source	Info	is_anomaly_iso	Anomaly_Score
2	10.1257	172.16.5.186	TCP ACK	-1	-0.5153
4	13.6876	192.168.0.38	ICMP Echo (ping)	-1	-0.5216
5	13.7671	10.0.0.13	ICMP Echo (ping)	-1	-0.5806
6	22.6995	172.16.6.97	UDP Data	-1	-0.5023
9	25.4797	172.16.7.23	TCP SYN, ACK	-1	-0.6051
14	40.4682	10.0.6.246	ICMP Echo (ping)	-1	-0.5917
16	44.7936	192.168.5.196	HTTP GET /index.html	-1	-0.5577
19	47.7929	192.168.3.112	DNS Standard query	-1	-0.5255
21	58.0599	172.16.4.152	ICMP Echo (ping)	-1	-0.519
22	58.2177	172.16.4.55	TLS Client Hello	-1	-0.5764

Sumber: data olahan

Gambar 5
Hasil Deteksi *Isolation Forest*

Pengujian Deteksi Brute force Berbasis Rule Based

Pengujian ini bertujuan untuk memastikan bahwa sistem mampu melakukan deteksi serangan *brute force* menggunakan pendekatan *rule-based* terhadap data yang sebelumnya terdeteksi sebagai anomali oleh *Isolation Forest.* Sistem memfilter data berdasarkan kemunculan kata kunci tertentu serta jumlah percobaan login dalam jendela waktu tertentu. Pengujian ini memastikan bahwa hanya aktivitas yang benar-benar mencurigakan yang dikategorikan sebagai serangan *brute force.*

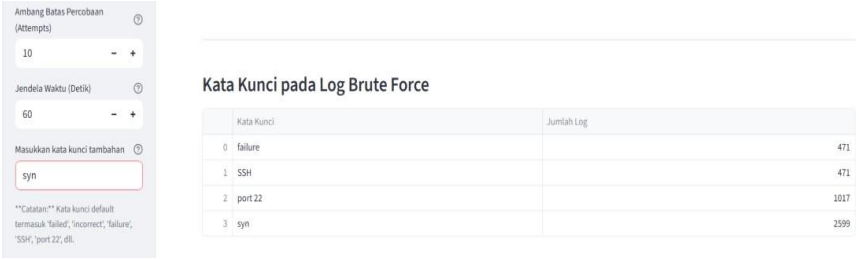

Kata Kunci pada Log Brute Force

	Kata Kunci	Jumlah Log
0	failure	339
1	SSH	339
2	port 22	1017

Sumber: data olahan

Gambar 6
Pengujian *Default Keyword*

Seperti pada Gambar 6 sistem berhasil melakukan filter terhadap data yang mengandung *default keywords* dan juga melebihi ambang *treshold attempt* dan *time window*. Gambar 7 sistem berhasil melakukan filter data yang dicurigai oleh *isolation forest* berdasarkan rule berupa *custom keyword* yang merupakan inputan dari user.


Ambang Batas Percobaan (Attempts)

10

Jendela Waktu (Detik)

60

Masukkan kata kunci tambahan

syn

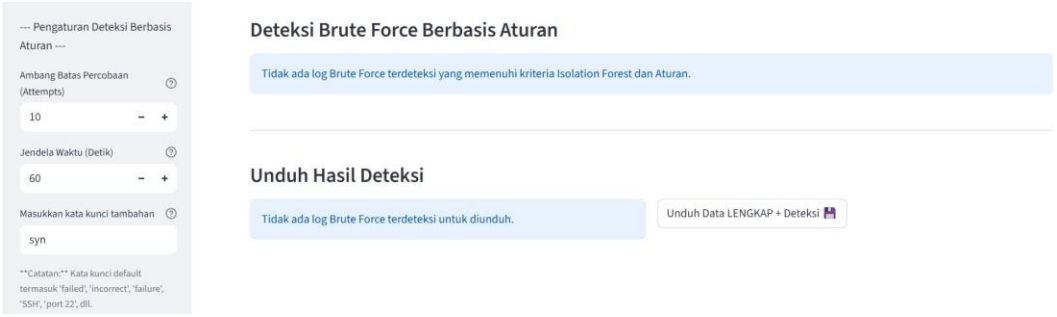
Catatan: Kata kunci default termasuk 'failed', 'incorrect', 'failure', 'SSH', 'port 22', dll.

Kata Kunci pada Log Brute Force

	Kata Kunci	Jumlah Log
0	failure	471
1	SSH	471
2	port 22	1017
3	syn	2599

Sumber: data olahan

Gambar 7
Pengujian *Custom Keyword* Inputan User



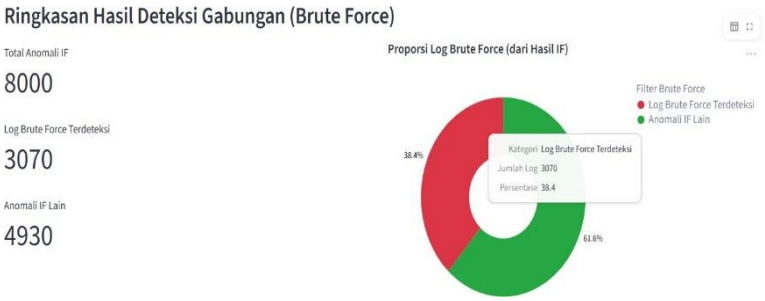
Sumber: data olahan

Gambar 8
Pengujian menggunakan dataset yang tidak terdapat keyword

Seperti yang dapat dilihat pada Gambar 8, apabila sistem tidak menemukan adanya *keyword* pada dataset anomali baik *default keywords* maupun *custom keywords*, maka sistem akan memunculkan informasi bahwa tidak terdapat log *brute force* yang memenuhi *rule based.* Pada bagian unduh hasil deteksi juga tidak akan terdapat tombol unduh untuk hasil deteksi yang dicurigai sebagai *brute force*

Pengujian Visualisasi Hasil Deteksi

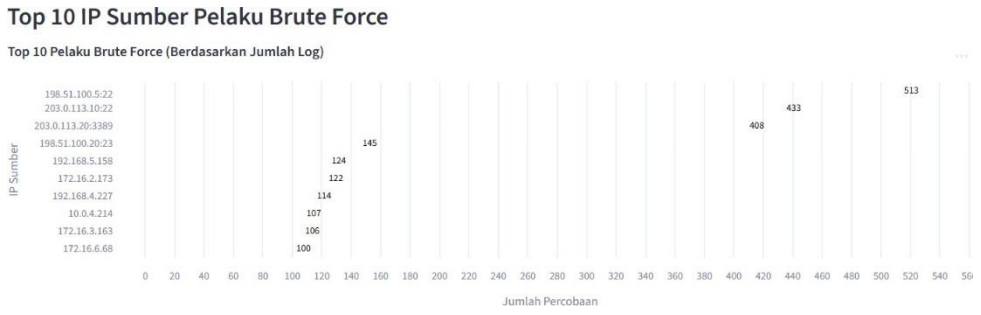
Pengujian ini dilakukan untuk memastikan bahwa sistem mampu menampilkan hasil deteksi dalam bentuk visualisasi yang informatif. Visualisasi meliputi tabel hasil deteksi, grafik pie proporsi data aman dan mencurigakan seperti yang dapat dilihat pada Gambar 9.



Sumber: data olahan

Gambar 9
***Pie chart* hasil deteksi**

Sistem juga menampilkan grafik batang untuk menampilkan IP sumber yang paling sering melakukan percobaan *brute force* seperti pada gambar 10.



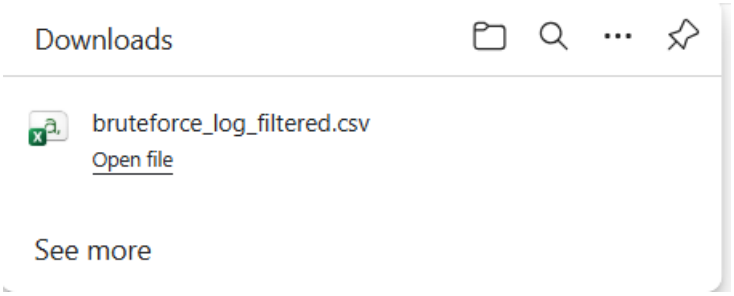
Sumber: data olahan

Gambar 10
Bar Graph* untuk *top ip

Pengujian ini bertujuan untuk memastikan bahwa seluruh visualisasi tampil dengan benar dan mudah dipahami oleh pengguna. Hasil yang diharapkan dari pengujian ini adalah seluruh grafik dan tabel dapat ditampilkan dengan benar sesuai dengan hasil deteksi yang diperoleh.

Pengujian Unduh Hasil Deteksi

Pengujian ini bertujuan untuk memastikan bahwa sistem menyediakan fitur unduh hasil deteksi dalam format CSV. Sistem menyediakan dua jenis unduhan, yaitu dataset lengkap yang telah ditambahkan hasil deteksi serta dataset yang hanya berisi log *brute force*. Pengujian ini memastikan bahwa file hasil deteksi dapat diunduh dan digunakan kembali untuk analisis lanjutan. Hasil yang diharapkan dari pengujian ini adalah sistem mampu menghasilkan file CSV hasil deteksi dan pengguna dapat mengunduh file tersebut tanpa mengalami kesalahan seperti yang dapat dilihat pada Gambar 11.



Sumber: data olahan

Gambar 11
Pengujian unduh hasil deteksi *brute force*

Setelah pengguna melakukan unduh hasil deteksi *brute force*, didalam file CSV terdapat informasi lengkap seperti pada log wireshark awal dan terdapat label anomali dan skor anomali seperti pada Gambar 11.

	No.,timestamp,Source,Destination,Protocol,Length,Info,is_anomaly_iso,Anomaly_Score
2	3131,10000.684654,198.51.100.5:22,172.16.2.112,TCP,126,SSH Authentication failure for user 'root',-1,-0.6299398756747849
3	3132,10000.703957,172.16.2.112,198.51.100.5:22,TCP,64,TCP SYN > to port 22,-1,-0.6238366794683682
4	3134,10000.79813,172.16.2.112,198.51.100.5:22,TCP,60,TCP SYN > to port 22,-1,-0.6246814095926495
5	3135,10000.810297,198.51.100.5:22,172.16.2.112,TCP,66,"TCP SYN, ACK",-1,-0.6412819397890839
6	3136,10000.818609,172.16.2.112,198.51.100.5:22,TCP,75,TCP SYN > to port 22,-1,-0.6246187149756354
7	3138,10000.853858,172.16.2.112,198.51.100.5:22,TCP,84,TCP SYN > to port 22,-1,-0.6240581567400287
8	3139,10000.955566,198.51.100.5:22,172.16.2.112,TCP,115,"TCP SYN, ACK",-1,-0.6356091657710746
9	3140,10000.975112,172.16.2.112,198.51.100.5:22,TCP,90,TCP SYN > to port 22,-1,-0.6227053703597365
10	3141,10001.046743,198.51.100.5:22,172.16.2.112,TCP,90,"TCP SYN, ACK",-1,-0.6401806668255082
11	3142,10001.057791,172.16.2.112,198.51.100.5:22,TCP,80,TCP SYN > to port 22,-1,-0.6241962494342629
12	3143,10001.161871,198.51.100.5:22,172.16.2.112,TCP,78,"TCP SYN, ACK",-1,-0.6412819397890839
13	3144,10001.172392,172.16.2.112,198.51.100.5:22,TCP,62,TCP SYN > to port 22,-1,-0.6246814095926495
14	3145,10001.185892,198.51.100.5:22,172.16.2.112,TCP,90,"TCP SYN, ACK",-1,-0.6401806668255082
15	3146,10001.197324,172.16.2.112,198.51.100.5:22,TCP,64,TCP SYN > to port 22,-1,-0.6238366794683682
16	3147,10001.206423,198.51.100.5:22,172.16.2.112,TCP,95,"TCP SYN, ACK",-1,-0.6397476758415652
17	3148,10001.214841,172.16.2.112,198.51.100.5:22,TCP,68,TCP SYN > to port 22,-1,-0.6210353212831464
18	3149,10001.320701,198.51.100.5:22,172.16.2.112,TCP,69,"TCP SYN, ACK",-1,-0.6425849094525966
19	3150,10001.324917,172.16.2.112,198.51.100.5:22,TCP,80,TCP SYN > to port 22,-1,-0.6241962494342629
20	3151,10001.365361,198.51.100.5:22,172.16.2.112,TCP,99,"TCP SYN, ACK",-1,-0.6401806668255082
21	3152,10001.376658,198.51.100.5:22,172.16.2.112,TCP,131,SSH Authentication failure for user 'root',-1,-0.630792870067359
22	3153,10001.387921,172.16.2.112,198.51.100.5:22,TCP,66,TCP SYN > to port 22,-1,-0.6210353212831464
23	3155,10001.435567,198.51.100.5:22,172.16.2.112,TCP,143,SSH Authentication failure for user 'root',-1,-0.6358318380265615
24	3156,10001.443995,172.16.2.112,198.51.100.5:22,TCP,74,TCP SYN > to port 22,-1,-0.6246187149756354
25	3157,10001.54616,198.51.100.5:22,172.16.2.112,TCP,118,"TCP SYN, ACK",-1,-0.6336616729992451
26	3158,10001.555063,172.16.2.112,198.51.100.5:22,TCP,80,TCP SYN > to port 22,-1,-0.6241962494342629
27	3159,10001.574632,198.51.100.5:22,172.16.2.112,TCP,120,"TCP SYN, ACK",-1,-0.6336616729992451
28	3160,10001.581761,172.16.2.112,198.51.100.5:22,TCP,82,TCP SYN > to port 22,-1,-0.6250414664481292

Sumber: data olahan

Gambar 12
Isi file unduh hasil deteksi

Rekapitulasi Hasil Pengujian Black Box

Sub bab ini menyajikan rekapitulasi hasil pengujian Black Box Testing yang telah dilakukan pada seluruh fitur utama sistem. Rekapitulasi ini bertujuan untuk memberikan gambaran ringkas mengenai keberhasilan setiap fungsi sistem berdasarkan skenario pengujian yang telah dilakukan sebelumnya.

Tabel 1
Rekapitulasi hasil *Black box testing*

No	Fitur yang Diuji	Tujuan Pengujian	Langkah Uji	Hasil yang Diharapkan	Hasil Pengujian	Keterangan
1	Upload Dataset	Memastikan sistem dapat menerima file CSV sebagai dataset deteksi	Pengguna mengunggah file CSV melalui menu upload pada sidebar	File berhasil diunggah dan pratinjau data ditampilkan tanpa error	Berhasil	Sistem menerima file CSV sesuai format

No	Fitur yang Diuji	Tujuan Pengujian	Langkah Uji	Hasil yang Diharapkan	Hasil Pengujian	Keterangan
2	Preprocess ing Data	Memastikan sistem dapat melakukan prapemrosesan data log *Wireshark*	Mengunggah dataset dengan kolom *Time, Source, Destination, Protocol, Length,* dan Info	Data berhasil diproses, timestamp dikonversi dan data kosong dihapus	Berhasil	*Preprocessing* berjalan sesuai rancangan
3	*Training* Model *Isolation Forest*	Memastikanmodel *Isolation Forest* dapat dilatih mengguna kan dataset deteksi	Sistem menjalankan pelatihan model secara otomatis setelah *preprocessing*	Model berhasil dilatih tanpa error	Berhasil	Model dilatih secara *unsupervised*
4	Deteksi Anomali (*Isolation Forest*)	Memastikan sistem dapat Mendeteksi anomali pada data log jaringan	Sistem menjalankan proses prediksi menggunaka *Isolation Forest*	Data diberi label normal (1) dan anomali (- 1)	Berhasil	Anomali terdeteksi dengan baik
5	Rule- Based Filtering	Memastikan sistem dapat memfilter anomali menjadi kandidat *brute force*	Sistem menerapkan keyword, threshold attempt, dan time window	Log *brute force* teridentifi kasi sesuai aturan	Berhasil	*Rule-Based* berjalan sesuai parameter
6	Visualisasi Hasil	Memastikan hasil deteksi ditampilkan dalam bentuk visual	Sistem menampilkan tabel, metrik, dan grafik pie	Visualisasi tampil sesuai rancangan	Berhasil	Informasi mudah dipahami pengguna
7	Unduh Hasil Deteksi	Memastikan sistem menyediakan fitur unduh hasil deteksi	Pengguna menekan tombol unduh hasil deteksi	File CSV berhasil diunduh	Berhasil	Output sesuai hasil analisis

Sumber: data olahan

SIMPULAN

Berdasarkan hasil perancangan, implementasi, dan pengujian sistem deteksi serangan *brute force* pada log jaringan *Wireshark,* dapat disimpulkan bahwa sistem yang dibangun mampu mendeteksi aktivitas jaringan mencurigakan secara otomatis dengan memanfaatkan algoritma *Isolation Forest* dan metode *rule-based*. Pendekatan *unsupervised learning* yang digunakan memungkinkan sistem melakukan deteksi anomali tanpa memerlukan data berlabel, sehingga lebih fleksibel dalam menghadapi pola serangan yang beragam. Hasil implementasi menunjukkan bahwa algoritma *Isolation Forest* dapat mengidentifikasi anomali pada lalu lintas jaringan berdasarkan karakteristik statistik data, seperti waktu, ukuran paket, dan frekuensi pengiriman dari suatu alamat IP. Selanjutnya, penerapan *rule-based filtering* berfungsi sebagai tahap verifikasi untuk mempersempit hasil deteksi dengan mengidentifikasi pola serangan *brute force* berdasarkan kemunculan kata kunci tertentu, jumlah percobaan login, serta rentang waktu yang ditentukan. Kombinasi kedua pendekatan ini terbukti mampu meningkatkan akurasi dalam mengidentifikasi serangan *brute force* dan mengurangi potensi *false positive.* Berdasarkan hasil pengujian menggunakan metode *blackbox testing*, seluruh fungsi utama sistem, mulai dari unggah dataset, p*reprocessing* data, pelatihan model, deteksi anomali, penerapan rule-based filtering, visualisasi hasil, hingga fitur unduh data, telah berjalan sesuai dengan kebutuhan yang telah ditentukan. Dengan demikian, sistem ini dapat digunakan sebagai alat bantu analisis keamanan jaringan dalam mendeteksi serangan *brute force* berbasis log jaringan.

DAFTAR PUSTAKA

Alpaydin, E., 2020. *Introduction to machine learning*. MIT Press.

Bejtlich, R., 2014. *The practice of network security monitoring: Understanding incident detection and response*. No Starch Press.

Buczak, A. L., Guven, E.. 2021. A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials, 18*(2), 1153–1176.

Chandola, V., Banerjee, A., Kumar, V., 2021. Anomaly detection: A survey. *ACM Computing Surveys, 41*(3), 1–58.

Chandravathi, B., Rao, K. S., Reddy, A. V., 2024. Network forensic analysis using Wireshark and machine learning techniques. *Journal of Network and Computer Applications, 224*, 103567.

Chua, Y., Lim, W., Wong, K., 2024. *Isolation Forest* based anomaly detection for network intrusion detection systems. *Computers & Security, 134*, 103455.

Hidayat, R., Kurniawan, F., 2021. Analisis forensik jaringan menggunakan Wireshark untuk mendeteksi serangan brute force. *Jurnal Keamanan Informasi, 7*(2), 85–94.

Khan, M. A., Karim, A., Kim, Y., 2022. A scalable machine learning based intrusion detection system for networks. *Future Generation Computer Systems, 128*, 83–95.

Kurose, J. F., Ross, K. W., 2021. *Computer networking: A top-down approach*. Pearson.

Liu, F. T., Ting, K. M., Zhou, Z. H. 2008. Isolation Forest. Proceedings of the IEEE International Conference on Data Mining, 413–422.

Mubarok, A., Romli, R., 2025. Rule-based and machine learning approaches for *brute force* attack detection. *Journal of Network Security, 14*(1), 22–35.

Raza, M., Rafiq, A., Iqbal, S., 2021. Detection of *brute force* attacks using machine learning techniques. *Journal of Information Security and Applications, 58*, 102713.

Schneier, B., 2018. *Click here to kill everybody: Security and survival in a hyper- connected world*. W. W. Norton & Company.

Stallings, W., 2020. *Network security essentials: Applications and standards*. Pearson.

Wireshark Foundation. 2023. *Wireshark user's guide*. https://www.wireshark.org