Jurnal Teknologi Informatika (J-TIFA) V.6 .No.1 Maret 2023 ISSN: 2654-2617 (Cetak)
DOI: https://doi.org/10.52046/j-tifa.v6i2.1678 ISSN: 2654-2633(Online)

Website : jurnal.ummu.ac.id/index.php/J-TIFA

J-TIFA

(Jurnal Teknologi Informatika)

|Teknologi Informasi | Jaringan Komputer | Data Mining |

Penerapan Metode Signature Base Berbasis IDS Snort dan IDS Suricata Pada Keamaan Jaringan Laboratorium Komputer.

Viviyanti Iksan Sangadji[a], *Abdul Haris Muhammad[b], Erwin Gunawan[c]
[abcd] *Program Studi Teknik Informatika, Universitas Muhammadiyah Maluku Utara,,Indonesia*
Email: vivyantiiksansangadi@gmail.com, agry.arisandi@gmail.com[b], , ewyn@outlook.com[c],

Abstrak

Keamanan komputer dapat diartikan sebagai perlindungan sistem komputer dari bahaya yang datang melalui akses jaringan yang menyimpang dari prosedur keamanan. Seperti halnya komputer yang terhubung dengan Internet, berpotensi sangat rentan terhadap pencurian data oleh oknum yang tidak bertanggung jawab. Universitas Muhammadiyah Maluku Utara (UMMU) contohnya, salah satu perguruan tinggi di maluku utara yang mempunyai sistem jaringan dan server di Laboratorium IT Infrastructure program studi Teknik Informatika yg digunakan dalam pengelolaan jaringan dan internet yang rentan akan pencurian data dan informasi. Permasalahan yg diangkat pada penelitian ini adalah bagaimana upaya untuk meningkatkan keamanan sistem jaringan komputer pada Laboratorium IT Infrastructure program studi Teknik Informatika. Metode signature based berbasis IDS adalah metode pendeteksian serangan melalui pola atau paket data yang dibaca kemudian dibandingkan dengan database yang ada atau aturan yang ada dengan menggunakan data atau paket yang disimpan. Tujuan dari penelitian ini adalah menghasilkan suatu sistem yang dapat mendeteksi lalu lintas jaringan dan hal-hal mencurigakan dalam suatu sistem jaringan. Dari hasil analisis yang dilakukan, Snort mendeteksi serangan dengan pemakaian CPU hingga mencapai 50% serta penggunaan memory mencapai 470 Mega. Sedangkan Suricata mendeteksi serangan dengan pemakaian CPU hampir mencapai 100% dengan penggunaan memory mencapai 430 Mega. Jadi kesimpulannya jumlah pemakaian CPU snort lebih kecil dibandingkan dengan Suricata. Pemakaian CPU snort hanya sebatas 50%. Sedangkan suricata hampir mencapai 100%. Untuk pemakaian memory snort dan suricata sama-sama hemat dalam pemakaian memory. Untuk snort pemakaian memory mencapai hingga 470 Mega, sedangkan suricata mencapai hingga 430 Mega.

Kata kunci : Signature Base, IDS Snort, IDS Suricata, Keamanan Jaringan

Abstract

Computer security can be interpreted as the protection of computer systems from dangers that come through network access that deviates from security procedures. Like any computer connected to the Internet, it has the potential to be very vulnerable to data theft by irresponsible persons. Muhammadiyah University of North Maluku (UMMU), for example, is one of the tertiary institutions in North Maluku which has a network and server system in the IT Infrastructure Laboratory of the Informatics Engineering study program which is used in network and internet management which is vulnerable to data and information theft. The problem raised in this research is how to increase the security of computer network systems in the IT Infrastructure Laboratory of the Informatics Engineering study program. The IDS-based signature based method is an attack detection method through patterns or data packets that are read and then compared with existing databases or existing rules using stored data or packets. The purpose of this research is to produce a system that can detect network traffic and suspicious things in

Riwayat Artikel: Menerima(14 Januari 2023), Revisi (10 Februari 2023), Diterima (4 Maret 2023), Online (30 Maret 2023)

Jurnal Teknologi Informatika (J-TIFA) V.6 .No.1 Maret 2023
DOI: https://doi.org/10.52046/j-tifa.v6i2.1678
ISSN: 2654-2617 (Cetak)
ISSN: 2654-2633(Online)

a network system. From the results of the analysis carried out, Snort detects attacks with CPU usage up to 50% and memory usage reaching 470 Mega. Meanwhile, Suricata detects attacks with CPU usage reaching almost 100% with memory usage reaching 430 Mega. So in conclusion, the amount of snort's CPU usage is smaller compared to Suricata. Snort CPU usage is only limited to 50%. While suricata almost reached 100%. For memory usage, snort and Suricata are equally efficient in memory usage. For snort, memory usage reaches up to 470 Mega, while Suricata reaches up to 430 Mega.

Keywords: Signature Base, IDS Snort, IDS Suricata, Network Security

1. Pendahuluan

Keamanan komputer dapat diartikan sebagai perlindungan sistem komputer dari bahaya yang datang melalui akses jaringan yang menyimpang dari prosedur keamanan. Seperti halnya komputer yang terhubung dengan Internet, ia berpotensi sangat rentan terhadap pencurian data oleh oknum yang tidak bertanggung jawab. Hal ini akan sangat merugikan jika mereka yang tidak bertanggung jawab mengintai perusahaan atau instansi, misalnya kampus karena banyak sekali informasi-informasi mahasiswa yang bisa diperoleh dengan mudah. Universitas Muhammadiyah Maluku Utara (UMMU) contohnya, merupakan perguruan tinggi di maluku utara yang mempunyai sistem jaringan dan server di Laboratorium IT Infrastructure program studi Teknik Informatika yg digunakan dalam pengelolaan jaringan dan internet yang rentan akan pencurian data dan informasi. (Setiawan, Herri. dan Munandar, M. A. dan Astuti, L. W., 2021)

Oleh karena itu perlu dilakukan upaya untuk meningkatkan keamanan sistem jaringan salah satunya adalah firewall, namun jika hanya menggunakan firewall saja tidak dapat menjamin keamanannya. Oleh karena itu, diperlukan sebuah teknologi atau sistem keamanan yang dapat memantau lalu lintas jaringan, yang disebut dengan Intrusion Detection System (IDS) dengan menggunakan metode signature based. Jika hal-hal ini ditemukan, maka Intrusion Detection System (IDS) memberikan peringatan kepada administrator sistem atau jaringan.

2. Keamanan Jaringan, Signature Base dan Intrusion Detection System

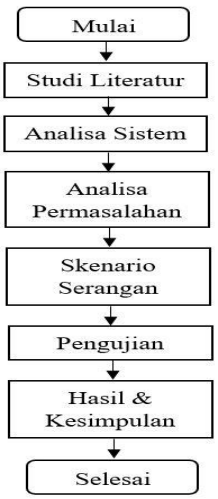
Dalam bukunya "An Analysis of security incidents on the internet", menurut John D. Howard, dia menyatakan bahwa (sistem) keamanan komputer merupakan suatu tindakan pencegahan perangkat dari agresi pengguna personal komputer atau pengakses jaringan yang bukan atau tidak bertanggung jawab.

IDS dengan metode signature based merupakan metode dalam mendeteksi serangan melalui pola atau paket data yang dibaca kemudian dibandingkan dengan data atau paket yang sudah tersimpan dalam database yang ada atau rule yang sudah ada. (Alviana, Sopian. dan Sumitra, I. D, 2018).

Selanjutnya Intrusion Detection System (IDS) adalah sebuah sistem yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. Jika ditemukan kegiatan-kegiatan yang mencurigakan berhubungan dengan traffic jaringan, maka IDS akan memberikan peringatan kepada sistem atau administrator jaringan (Akhmad, 2013: 2).

3. Metodologi Penelitian

Berikut tahapan penelitian yg dilaksanakan oleh peneliti



Gambar 1. Alur Proses Penelitian

Riwayat Artikel: Menerima(14 Januari 2023), Revisi (10 Februari 2023), Diterima (4 Maret 2023), Online (30 Maret 2023)

Jurnal Teknologi Informatika (J-TIFA) V.6 .No.1 Maret 2023 ISSN: 2654-2617 (Cetak)
DOI: https://doi.org/10.52046/j-tifa.v6i2.1678 ISSN: 2654-2633(Online)

Adapun penjelasan tahapan penelitian adalah sebagai berikut:

a) Studi Literatur

Langkah awal dalam penelitian ini adalah mengumpulkan dan mempelajari literatur terkait *Intrusion Detection System*, baik dari buku elektronik, jurnal, artikel serta referensi lainnya.

b) Analisa Sistem

Sistem yang sedang berjalan pada lab IT *Infrasturcture* saat ini masih mengandalkan implementasi berbasis *firewall*.

c) Analisa Permasalahan

Masalah keamanan sistem jaringan dan *server* pada laboratorium IT Infrastructure masih rentan terhadap serangan yang dilakukan sehinngga mengakibatkan *server* terkendala.

d) Skenario Serangan

Skenario serangan akan dilakukan penyerangan terhadap *server* IDS menggunakan metode penyerangan DDoS dan Malware. Dimana saat terjadinya serangan, IDS akan memberikan peringatan kepada administrator.

e) Pengujian

Tahapan pengujian dilakukan dengan pemasangan server pendeteksi serangan menggunakan aplikasi pendukung yaitu Snort dan Suricata pada sebuah *web server* yang akan digunakan. Pengujian dilakukan dengan dua tahap yaitu : Tahapan Pertama akan dilakukan pengujian Snort yang dilakukan menggunakan metode penyerangan DDoS dan Malware. Dan tahapan kedua akan dilakukan pengujian Suricata dengan metode penyerangan yang sama.

f) Hasil & Kesimpulan

Berdasarkan alur penelitian diatas, hasil dan kesimpulan merupakan bagian terpenting dalam kegiatan penelitian serta bertujuan untuk mengetahui hasil perbandingan performa IDS Snort dan IDS Suricata menggunakan metode *Signature Based*.

4. Hasil dan Pembahasan

Perancangan sistem pada penelitian ini, antara lain sebagai berikut:

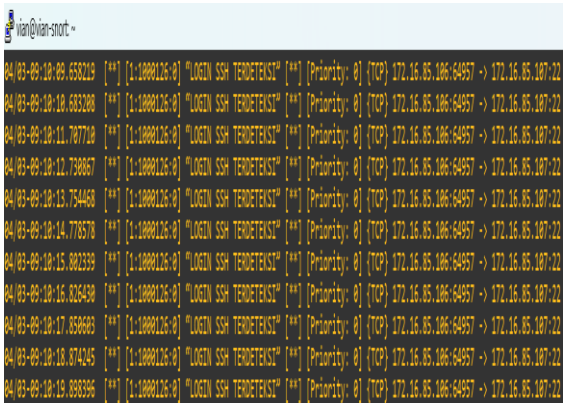
4.1 Skenario dan Pengujian Snort

Pada scenario dan pengujian snort dilakukan dengan beberapa rule antara lain sebagai berikut:

Skenario Pertama yaitu dengan mendeteksi koneksi SSH, dengan perintah

```
alert tcp any any -> $HOME_NET 22 (msg:
"LOGIN SSH TERDETEKSI"; sid:1000126;)
```

Hasil pengujian berdasarkan skenario mendeteksi koneksi SSH dapat dilihat pada gambar dibawah gambar 2. Dari hasil scenario ini dapat dilihat bahwa serangan koneksi SSH terdeteksi menggunakan protocol TCP yang berasal dari IP Address penyerang 172.16.85.106 ke IP server 172.16.85.107 melalui port 22.



Gambar 2. Hasil Pengujian Snort Mendeteksi Koneksi SSH

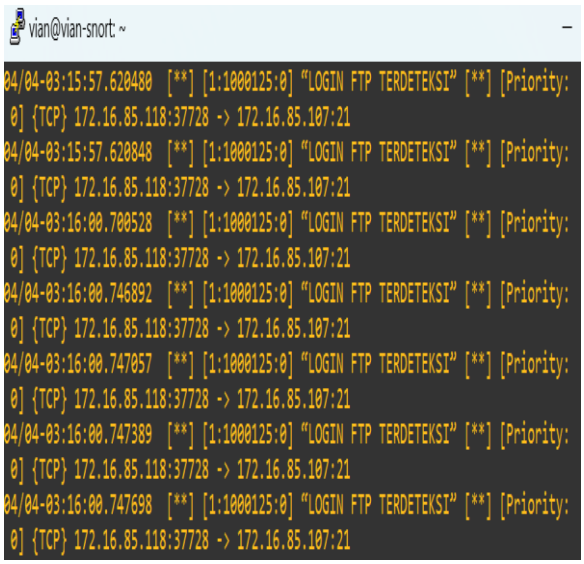
Selanjutnya pada **Skenario Kedua**, adalah dengan mendeteksi koneksi FTP dengan perintah :

```
alert tcp any any -> $HOME_NET 21
(msg:"LOGIN FTP TERDETEKSI";
sid:1000125;)
```

Riwayat Artikel: Menerima(14 Januari 2023), Revisi (10 Februari 2023), Diterima (4 Maret 2023), Online (30 Maret 2023)

Jurnal Teknologi Informatika (J-TIFA) V.6 .No.1 Maret 2023
DOI: https://doi.org/10.52046/j-tifa.v6i2.1678
ISSN: 2654-2617 (Cetak)
ISSN: 2654-2633(Online)

Hasil pengujian berdasarkan skenario mendeteksi koneksi FTP dapat dilihat pada gambar 3. Dimana dapat dilihat bahwa serangan koneksi FTP terdeteksi menggunakan protocol TCP yang berasal dari IP Address penyerang 172.16.85.118 ke IP server 172.16.85.107 melalui port 21.

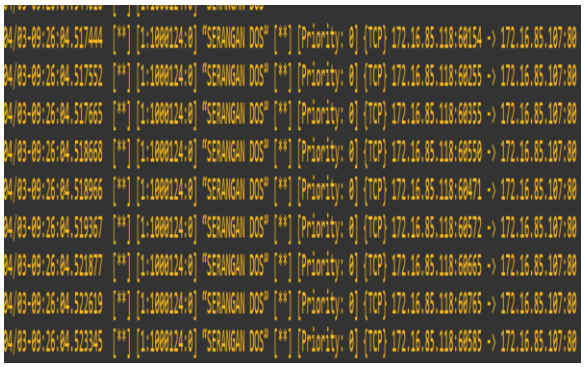


Gambar 3. Hasil Pengujian Snort Mendeteksi Koneksi FTP

Selanjutnya pada **Skenario Ketiga,** adalah mendeteksi Koneksi DOS. Rules untuk melakukan pendeteksian terhadap koneksi DOS dengan perintah :

```
alert tcp any any -> $HOME_NET 80 (msg:“SERANGAN DOS”;threshold:type threshold,track by_src,count 100,seconds 5;sid:1000124;)
```

Hasil pengujian berdasarkan skenario mendeteksi koneksi DOS dapat dilihat pada gambar dibawah ini dimana dapat dilihat bahwa serangan DOS terdeteksi menggunakan protocol TCP yang berasal dari IP Address penyerang 172.16.85.118 ke IP server 172.16.85.107 melalui port 80.



Gambar 4. Hasil Pengujian Snort Mendeteksi Koneksi DOS

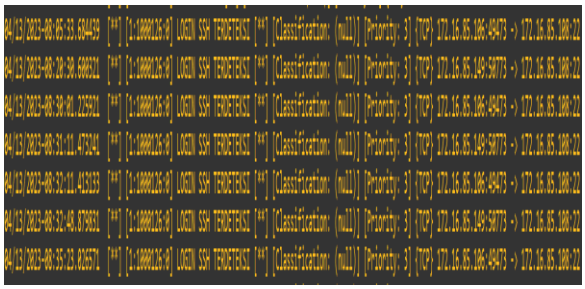
4.2 Skenario dan Pengujian Suricata

Pada scenario dan pengujian snort dilakukan dengan beberapa rule antara lain sebagai berikut:

Skenario Pertama yaitu dengan mendeteksi koneksi SSH, dengan perintah

```
alert tcp any any -> $HOME_NET 22 (msg: "LOGIN SSH TERDETEKSI"; sid:1000126;)
```

Hasil pengujian berdasarkan skenario mendeteksi koneksi SSH dapat dilihat pada gambar gambar 5. Dari gambar tersebut dapat dilihat bahwa serangan koneksi SSH terdeteksi menggunakan protocol TCP yang berasal dari IP Address penyerang 172.16.85.106 ke IP server 172.16.85.107 melalui port 22



Gambar 5. Hasil Pengujian Suricata Mendeteksi Koneksi SSH

Riwayat Artikel: Menerima(14 Januari 2023), Revisi (10 Februari 2023), Diterima (4 Maret 2023), Online (30 Maret 2023)

Jurnal Teknologi Informatika (J-TIFA) V.6 .No.1 Maret 2023
DOI: https://doi.org/10.52046/j-tifa.v6i2.1678
ISSN: 2654-2617 (Cetak)
ISSN: 2654-2633(Online)

Selanjutnya pada **Skenario Kedua**, adalah dengan mendeteksi koneksi FTP dengan metode suricata dengan perintah:

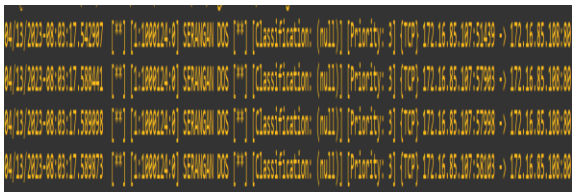
```
alert tcp any any -> $HOME_NET 21 (msg:“LOGIN FTP TERDETEKSI”; sid:1000125;)
```

Hasil pengujian berdasarkan skenario mendeteksi koneksi SSH dapat dilihat pada gambar 6, dapat dapat dilihat bahwa serangan koneksi FTP terdeteksi menggunakan protocol TCP yang berasal dari IP Address penyerang 172.16.85.118 ke IP server 172.16.85.107 melalui port 21.

Berikutnya pada skenario terakhir yaitu melakukan pendeteksian terhadap koneksi DOS dengan perintah beriku:

```
alert tcp any any -> $HOME_NET 80 (msg:“SERANGAN DOS”;threshold:type threshold,track by_src,count 100,seconds 5;sid:1000124;)
```

Hasil pengujian berdasarkan skenario mendeteksi koneksi SSH dapat dilihat pada gambar dibawah ini. dapat dilihat bahwa serangan DOS terdeteksi menggunakan protocol TCP yang berasal dari IP Address penyerang 172.16.85.118 ke IP server 172.16.85.107 melalui port 80.



Gambar 7. Hasil Pengujian Suricata Mendeteksi Koneksi DOS

4.3 Hasil Analisis

Pada bagian ini akan dipaparkan hasil analisis pengujian melalui hasil yang di dapat. Berikut dibawah ini adalah hasil analisis Snort dan Suricata. Pada tabel 1 merupakan hasil analisis snort sebelum melakukan penyerangan dan tabel 2 merupakan hasil analisi snort sesudah melakukan penyerangan.

Hasil analisis snort berdasarkan kedua tabel tersebut diperoleh bahwa Snort dalam mendeteksi serangan dengan pemakaian CPU hingga mencapai 50%, dan penggunaan memory mencapai 470 Mega. Kemampuan mendeteksi serangan koneksi SSH, koneksi FTP maupun DOS, snort mampu mendeteksi dengan cepat dan memiliki hasil yang baik

Tabel 1. Hasil Analisis Snort Sebelum Melakukan Serangan

Item Analisis	**Hasil Analisi**
CPU	0.0 %
Memori	407 M/ 7.58 G
SWAP	OK/OK

Tabel 2. Hasil Analisis Snort Setelah Melakukan Serangan

Item Analisis	**Hasil Analisi**
CPU	54.8 %
Memori	471 M/ 7.58 G
SWAP	OK/OK

Selanjutnya pada tabel 3 dan 4 merupakan hasil analisis Suricata sebelum melakukan serangan dan setelah melakukan serangan. Analisis berdasarkan pada tabel 3 dan 4 dibawah ini dapat dilihat bahwa Suricata dalam mendeteksi serangan dengan pemakaian CPU hampir mencapai 100%, dan penggunaan memory mencapai 430 Mega. Kemampuan mendeteksi serangan koneksi SSH, koneksi FTP maupun DOS, snort mampu mendeteksi dengan cepat dan memiliki hasil yang baik.

Tabel 1. Hasil Analisis Suricata Sebelum Melakukan Serangan

Item Analisis	**Hasil Analisi**
CPU	0.0 %
Memori	293 M/ 7.58 G
SWAP	OK/OK

Tabel 2. Hasil Analisis Suricata Setelah Melakukan Serangan

Item Analisis	**Hasil Analisi**
CPU	91.1 %
Memori	425 M/ 7.58 G
SWAP	OK/OK

Riwayat Artikel: Menerima(14 Januari 2023), Revisi (10 Februari 2023), Diterima (4 Maret 2023), Online (30 Maret 2023)

Jurnal Teknologi Informatika (J-TIFA) V.6 .No.1 Maret 2023
DOI: https://doi.org/10.52046/j-tifa.v6i2.1678
ISSN: 2654-2617 (Cetak)
ISSN: 2654-2633(Online)

5. Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan hasil implementasi menggunakan Signature berbasis IDS Snort dan IDS Suricata yang telah penulis jelaskan pada bab sebelumnya. Penulis menarik kesimpulan sebagai berikut:

1) Metode signature based berbasis IDS ini dapat membantu dalam mendeteksi serangan serta meminimalisir serangan yang masuk pada sistem jaringan komputer.
2) Snort dan Suricata keduanya mampu mendeteksi serangan dengan cepat.
3) Jumlah pemakaian CPU snort lebih kecil dibandingkan dengan Suricata. Pemakaian CPU snort hanya sebatas 50%. Sedangkan suricata hampir mencapai 100%. Untuk pemakaian memory snort dan suricata sama-sama hemat dalam pemakaian memory. Untuk snort pemakaian memory mencapai hingga 470 Mega, sedangkan suricata mencapai hingga 430 Mega.

5.2 Saran

Untuk penelitian selanjutnya yaitu dapat membangun sistem IDS dalam mendeteksi lebih banyak serangan, serta lebih menghemat dalam penggunaan jumlah CPU maupun memory.

Referensi

Alviana, Sopian. dan Sumitra, I. D. (2018). Analisis Pengukuran Penggunaan Sumber Daya Komputer Pada Intrusion Detection System Dalam Meminimalkan Serangan Jaringan, 7, 29.

Dantris sri, Junaidi Noh, Mustamin Hamid. (2020). Simulasi Protokol Autjentifikasi 802. 1x pada Jaringan Nirkabel di UMMU. JTIFA Vol 3 No 2 September 2020. Doi: https://doi.org/10.52046/j-tifa.v3i2.1044

.

DosenIT.com. 2015. 12 Pengertian Jaringan Komputer Menurut Para Ahli. https://dosenit.com/jaringan-komputer/pengertian-jaringan-komputer-menurut-para-ahli (diakses pada tanggal 31 maret 2022).

Efrando, Asril. dan Herwin. Dan Haryono, Dwi. (2019). Monitoring pada Server STMIK Amik Riau dengan Menggunakan Suricata Melalui Notifikasi Bot Telegram, 5, 38.

Fadhlulloh, M. F. dan Rahmat, Basuki. dan Irawan, A. I. (2020). ANALISIS Keamanan Jaringan Pada Smart Kwh Meter Berbasis Internet Of Things (Iot), 7, 3187.

Fadhlillah, A. S. dan Bogi, Nyoman. Dan Irawan, A. I. (2019). Analisis Performansi Ids Menggunakan Metode Deteksi Anomalybased Terhadap Serangan Dos, 6, 3400.

Hakim, L. N. dan Murtiyasa, Budi. dan Handaga, Bana. (2015). Analisis Perbandingan Intrustion Detection System Snort dan Suricata, 19.

Husen Irma, Adelina Ibrahim, Abdul Haris Muhammad. (2022). Implementasi PPPoE pada Jaringan Laboratorium Insrastruktur Teknologi Informasi UMMU. JTIFA Vol 5 No 1 Maret 2022. DOI: https://doi.org/10.52046/j-tifa.v5i1.1353

Jejaring. 2019. Pengertian dan Jenis Intrusion detection System (IDS). https://www.jejaring.web.id/pengertian-dan-jenis-intrusion-detection-system-ids/ (diakses pada tanggal 28 maret 2022).

Lukman. Suci, Melati. (2020). Analisis Perbandingan Kinerja Snort dan Suricata Sebagai Intrusion Detection System Dalam Mendeteksi Serangan Syn Flood Pada Web Server, 15.

Purba, W. W. dan Efendi, Rissal. (2020). Perancangan Dan Analisis Sistem Keamanan Jaringan Komputer Menggunakan Snort, 17, 154.

Ralianto, A. D. dan Cahyono, Setiyo. (2021). Perbandingan Nilai Akurasi Snort dan Suricata Dalam Mendeteksi Intrusi Lalu Lintas Di Jaringan, 15, 17.

Setiawan, Herri. dan Munandar, M. A. dan Astuti, L. W. (2021). Penggunaan Metode Signatured Based Dalam Pengenalan Pola Serangan Di Jaringan Komputer, 8, 518-522.

Sutarti. dan Pancaro, A. P. dan Saputra, F. I. (2018). Implementasi Ids (Intrusion Detectio System) Pada Sistem Keamanan Jaringan Sman 1 Cikeusal, 5, 2-3.

Syah Irjaman, Abdul Haris Muhammad, Erwin Gunawan. (2020) Simulasi Network Automation Menggunakan Ansible di GNS3. JTIFA Vol 3 No 2 September 2020. Doi : https://doi.org/10.52046/j-tifa.v3i2.1065

Udrus Karina. Sahriar Hamza, Gamaria Mandar. (2021). Optimalisasi Bandwidth Menggunakan Traffic Shapping di Lab. Networking Universitas Muhammadiyah Maluku Utara. JTIFA Vol 4 No 1 Marer 2021. Doi; https://doi.org/10.52046/j-tifa.v4i1.1162

Riwayat Artikel: Menerima(14 Januari 2023), Revisi (10 Februari 2023), Diterima (4 Maret 2023), Online (30 Maret 2023)