DETEKSI AKTIVITAS MALWARE AKIBAT SOFTWARE PIRACY DENGAN MENGGUNAKAN SURICATA BERBASIS NETWORK BASED INTRUSION PREVENTION SYSTEM

'Azizil'an Sarina Putra[1], Bana Handaga[2]

[1,2]Program Studi Teknik Informatika, Fakultas Komunikasi dan Informatika, Universitas Muhammadiyah Surakarta, Jl. A. Yani, Pabelan, Kartasura, Sukoharjo, Jawa Tengah 57169 Indonesia

Email korespondensi: azizilansarinaputra@gmail.com

Abstrak. Perkembangan teknologi yang pesat telah meningkatkan ketergantungan pada sistem jaringan dan komputer, namun di balik manfaatnya, muncul ancaman keamanan seperti pembajakan perangkat lunak (*software piracy*). *Software piracy* adalah tindakan ilegal yang merugikan ekonomi global dan berpotensi menyebarkan *malware* melalui aktivator tidak tepercaya atau unduhan dari sumber yang tidak sah. Untuk mengatasi ini, *Network-based Intrusion Prevention System (NIPS)* menjadi solusi penting karena kemampuannya mendeteksi dan memblokir lalu lintas jaringan mencurigakan secara *real-time*. Penelitian ini bertujuan untuk mendeteksi aktivitas *software piracy* melalui analisis lalu lintas jaringan menggunakan Suricata sebagai NIPS. Metode yang digunakan adalah penelitian eksperimen dengan pendekatan kuantitatif. *Custom rules* Suricata dirumuskan berdasarkan analisis mendalam dari VirusTotal dan Wireshark untuk menargetkan *signature* komunikasi unik aktivator. Hasil penelitian menunjukkan bahwa NIPS berbasis Suricata efektif dalam mendeteksi dan memblokir lalu lintas mencurigakan dari aktivator *software piracy*. Deteksi ini meliputi identifikasi permintaan DNS ke *Command and Control (C&C) domain* untuk aktivator WinRAR dan IDM. Pemblokiran koneksi TCP ke alamat IP C&C terkait berhasil untuk aktivator WinRAR, namun tidak teramati untuk IDM meskipun permintaan DNS-nya terdeteksi. *Custom rules* Suricata menunjukkan presisi deteksi tinggi, dan pengujian dengan aplikasi resmi mengonfirmasi *false positive rate* yang rendah. Sistem ini juga mampu mendeteksi *query* DNS mencurigakan bahkan dalam kondisi *offline*.

Kata kunci: NIPS , Suricata, Software Piracy, Keamanan Jaringan, Malware

PENDAHULUAN

Perkembangan teknologi yang pesat meningkatkan kebutuhan akan sistem jaringan dan komputer dalam kehidupan sehari-hari. Kemajuan ini membawa manfaat besar, seperti komunikasi yang cepat dan akses informasi luas [1]. Namun, hal ini juga memicu munculnya berbagai ancaman keamanan, termasuk aktivitas ilegal seperti pembajakan perangkat lunak (*software piracy*).

Software piracy merupakan tindakan ilegal yang melibatkan penyalinan, distribusi, atau penggunaan perangkat lunak tanpa izin dari pemegang hak cipta. Perangkat lunak bajakan dapat dengan mudah diperoleh melalui pusat perbelanjaan, penjual komputer, internet, maupun pedagang kaki lima. Dalam beberapa kasus, versi bajakan dari perangkat lunak bahkan sudah beredar sebelum peluncuran resminya. Tingginya angka pembajakan menyebabkan kerugian ekonomi global yang signifikan dan berdampak besar terhadap industri teknologi serta iklim investasi [2]. Pembajakan perangkat lunak merupakan penggunaan perangkat lunak tanpa lisensi resmi, sering kali melibatkan aktivator ilegal, situs tidak resmi, dan unduhan dari sumber yang tidak terpercaya. Aktivitas ini tak hanya melanggar hukum, tetapi juga berisiko terhadap keamanan jaringan karena dapat menjadi jalur masuk malware. *Malicious software*, biasanya disebut sebagai malware, mencakup semua perangkat lunak yang menimbulkan risiko bagi pengguna, komputer, atau jaringan. Ada beberapa kategori malware, termasuk *trojan, worm, rootkit, scareware*, dan *spyware* [3].

Ada beberapa pendekatan dalam mendeteksi aktivitas malware di antaranya melalui Network-based Intrusion Prevention System (NIPS) yang menganalisis lalu lintas jaringan secara real-time untuk mendeteksi pola mencurigakan dan melalui Host-based Intrusion Detection System (HIDS), yang memanfaatkan pemantauan log aktivitas pada endpoint untuk mendeteksi anomali dari dalam sistem. HIDS berperan sebagai lini pertahanan terakhir terhadap serangan siber setelah pertahanan perimeter [4]. Salah satu solusi yang digunakan untuk mengatasi ancaman ini adalah *Intrusion Prevention System* (IPS), yang berfungsi mendeteksi dan menangani lalu lintas jaringan mencurigakan secara otomatis [5]. Salah satu jenis IPS adalah *Network-based Intrusion Prevention System* (NIPS), yang bekerja secara inline dan mampu menganalisis serta memblokir trafik berbahaya secara real-time [6].Suricata, sebagai sistem network-based intrusion detection and prevention system, mampu melakukan inspeksi paket jaringan secara mendalam dan mendukung pembuatan rules khusus untuk mengidentifikasi aktivitas semacam ini [7].

Deteksi ancaman siber, termasuk aktivitas *malware* akibat *software piracy*, umumnya mengandalkan dua pendekatan fundamental berbasis *signature* dan berbasis perilaku [8]. Deteksi berbasis *signature* mengidentifikasi ancaman menggunakan pola unik atau karakteristik digital yang telah dikenal dari *malware* atau aktivitas berbahaya.

Keunggulannya terletak pada akurasi tinggi untuk ancaman yang dikenal dan *false positive rate* yang rendah, namun kelemahannya adalah ketidakmampuannya mendeteksi ancaman baru (*zero-day attacks*) tanpa pembaruan *signature* berkelanjutan. [8], [9] menyediakan tinjauan komprehensif mengenai teknik-teknik deteksi *malware* dan intrusi jaringan ini, menyoroti efektivitas serta tantangan masing-masing pendekatan dalam lingkungan siber modern. Meskipun Suricata secara inheren lebih kuat dalam deteksi berbasis *signature [10]*, kemampuannya dalam analisis lalu lintas mendalam juga dapat dimanfaatkan untuk mengidentifikasi indikasi perilaku anomali, seperti pola koneksi tidak lazim yang terkait dengan *software piracy*, yang kemudian dapat dijadikan dasar untuk *custom rules* tambahan. Di sisi lain, deteksi berbasis perilaku mengidentifikasi ancaman dengan menganalisis penyimpangan dari pola aktivitas normal sistem atau jaringan.

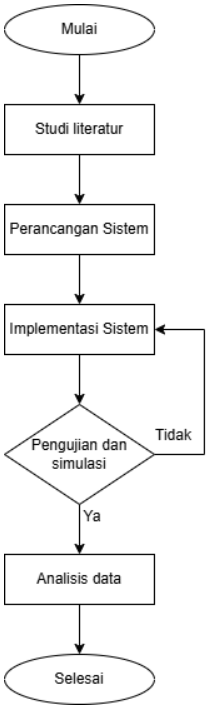
Operation sistem linux ubuntu sangat cocok diterapkan untuk menjalankan Suricata sebagai NIPS karena kompatibilitasnya yang sangat baik dengan sistem keamanan yang menggunakan Linux [11]. Dalam studi ini, efektivitas Suricata, yang berfungsi sebagai Network-based Intrusion Prevention System (NIPS), dievaluasi untuk deteksi *malware* terkait *software piracy* di lingkungan jaringan yang terkontrol [12], [13].

Beberapa alat yang dapat digunakan sebagai perumusan custom rules seperti *wireshark* merupakan alat memantau dan menganalisis lalu lintas jaringan secara mendalam, termasuk koneksi *DNS* dan *TCP*, guna mengidentifikasi alamat IP dan port tujuan yang mencurigakan [14]. VirusTotal merupakan alat menganalisis *file* aktivator guna mendapatkan informasi tambahan terkait *malware* dan pola komunikasi. Data hasil identifikasi ini akan menjadi dasar untuk perumusan *custom rules* Suricata [15]. Pendekatan pengujian dengan skenario simulasi serangan ini selaras dengan metodologi yang diterapkan dalam berbagai penelitian IPS/IDS sebelumnya [16]. Suricata, yang beroperasi sebagai IPS, akan mendeteksi setiap kecocokan paket dengan *signature rules* yang telah disesuaikan [15].

Penelitian ini bertujuan mendeteksi aktivitas *software piracy* melalui analisis lalu lintas jaringan dengan Suricata sebagai NIPS. Diharapkan sistem ini dapat memberikan solusi deteksi anomali yang efisien dan membantu administrator jaringan dalam mencegah ancaman keamanan.

METODE

Rangka penelitian berfungsi sebagai panduan saat menjalankan penelitian sehingga hasil yang dicapai tetap sesuai dengan sasaran. Proses kerja diatur dalam format diagram alir seperti yang terlihat pada Gambar 1.



Gambar 1. Diagram Alir Penelitian

2.1 Studi literatur

Dalam kajian ini mengkaji salah satu jurnal untuk dijadikan acuan dalam merancang system keamanan jaringan. Dalam penelitian [6] membahas mengenai Implementasi *Intrusion Prevention System* (IPS) *OSSEC* dan *Honeypot Cowrie.* Pada penelitian ini menggunakan OSSEC untuk melakukan pencegahan dengan metode NIPS.

2.2 Analisis Kebutuhan

Penelitian ini merupakan jenis penelitian eksperimen dengan pendekatan kuantitatif, yang bertujuan untuk menguji efektivitas sistem deteksi aktivitas *malware* akibat *software piracy*. Analisis kebutuhan dalam penelitian ini berfokus pada identifikasi persyaratan teknis untuk membangun sistem deteksi aktivitas *malware* akibat *software piracy*. Dalam penelitian ini, akan dibangun sistem deteksi malware berbasis Suricata yang difokuskan pada fungsi NIPS untuk mengidentifikasi indikasi aktivitas pembajakan perangkat lunak melalui analisis lalu lintas jaringan. Dalam penelitian ini, *custom rules* Suricata akan dibuat berdasarkan *signature* koneksi spesifik yang teridentifikasi dari *software piracy* atau *aktivator software piracy* melalui analisis wireshark dan VirusTotal.

Untuk membangun NIPS diperlukan hal-hal sebagai berikut:

2.2.1 Kebutuhan Perangkat Lunak

1. Sistem Operasi
    a. Linux ubuntu diterapkan untuk menjalankan Suricata sebagai NIPS
    b. Windows 10 digunakan sebagai *end-user* pengguna untuk menjalankan software piracy.
2. Suricata
    a. Suricata NIPS digunakan untuk memantau aktivitas lalu lintas jaringan yang masuk secara real-time
    b. Melakukan deteksi aktivitas malware berdasarkan signature (pola yang telah dikenal) dengan perilaku lalu lintas jaringan yang mencurigakan.
3. VMware
    a. Menyediakan lingkungan virtual untuk menjalankan VM Linux (Suricata NIPS).

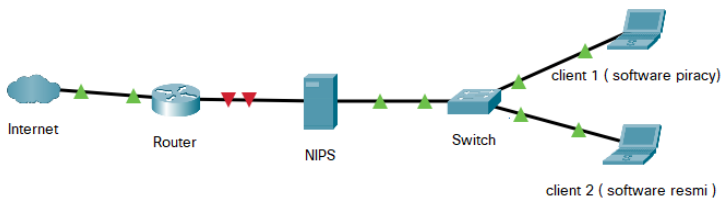
2.2.2 Kebutuhan Perangkat Keras

Kebutuhan perangkat keras yang akan digunakan dalam penelitian ini terdapat dalam tabel 1.

Tabel 1. Kebutuhan Perangkat Keras

NO	Perangkat	Unit	Deskripsi
1	Router	1	Menghubungkan jaringan lokal ke internet.
2	laptop	2	Satu laptop terpasang *software piracy*, yang lain bersih dari *software piracy*, mewakili client untuk LAN target.
3	NIPS	1	VM untuk Menjalankan NIPS.
4	Kabel Lan	4	Koneksi antar perangkat.
5	Switch	1	Penghubung antara NIPS dengan client

2.3 Perancangan Sistem



Gambar 2.1 Perancangan Sistem

Topologi jaringan yang dirancang untuk penelitian ini, seperti terlihat pada Gambar 2.1, bertujuan untuk mensimulasikan lingkungan jaringan yang terkontrol guna menguji efektivitas Network-based Intrusion Prevention System (NIPS) dalam mendeteksi aktivitas *malware* akibat *software piracy*. Pada topologi ini:

1. Internet: Menyalurkan akses internet
2. Router: Berfungsi sebagai gerbang utama, menghubungkan jaringan lokal dengan Internet dan mengarahkan lalu lintas data. Pada *router* ini, hanya digunakan konfigurasi standar dengan DHCP server untuk menyalurkan koneksi internet ke jaringan lokal.
3. NIPS (Network-based Intrusion Prevention System): Ini adalah komponen inti yang menjalankan Suricata. NIPS ditempatkan secara *inline* antara *router* dan *switch*, memastikan seluruh lalu lintas jaringan yang masuk dan keluar dari klien melewati NIPS untuk diinspeksi. Pada NIPS ini, konfigurasi Suricata dilakukan untuk fungsi deteksi dan pencegahan. Selain itu, penggunaan Wireshark juga dilakukan untuk melakukan pra pengujian.
4. Switch: Menghubungkan NIPS dengan perangkat klien, mendistribusikan lalu lintas jaringan ke klien yang terhubung.
5. Client 1 (Software Piracy): Merepresentasikan laptop yang digunakan untuk menginstal dan menjalankan perangkat lunak bajakan beserta aktivatornya. Klien ini digunakan untuk menghasilkan lalu lintas mencurigakan yang menjadi target deteksi.
6. Client 2 (Software Resmi): Merepresentasikan komputer pengguna yang menginstal dan menjalankan perangkat lunak resmi. Klien ini digunakan sebagai kontrol untuk menghasilkan lalu lintas jaringan normal, memastikan sistem tidak menghasilkan *false positive*.

Dengan topologi ini, seluruh lalu lintas jaringan dari Internet dialirkan melalui *router* menuju NIPS sebelum diteruskan ke *switch* dan perangkat klien.

2.4 Skenario Pengujian Sistem

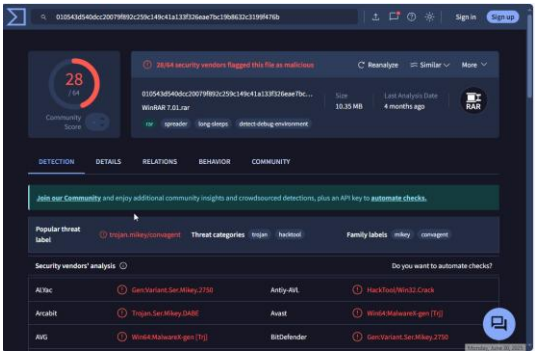
Pengujian sistem ini bertujuan untuk memvalidasi kemampuan Suricata sebagai Network-based Intrusion Prevention System (NIPS) dalam mendeteksi aktivitas *malware* akibat *software piracy* pada WinRAR dan IDM yang dijalankan di Client 1. Sebelum dijalankan pra pengujian suricata di install pada server nips dan dikonfigurasi dengan af-packet mode ips dan di install juga wireshark.

2.4.1 Analisis Pra-Pengujian

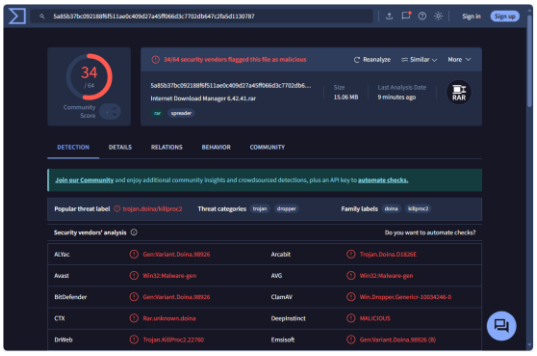
Pada tahap ini, analisis mendalam terhadap software dan aktivator software piracy yang satu paket dengan softwarenya, Tujuan utama adalah untuk mendapatkan karakteristik unik dari aktivator tersebut yang nantinya akan digunakan dalam perumusan *custom rules* Suricata.

2.4.1.1 Analisis File dengan VirusTotal

Tahapan ini diambil dari software piracy yang di unduh pada client 1 dan di unggah pada web VirusTotal, Hasil Analisis pada gambar 2.2, untuk WinRAR 7.01.rar merupakan paket instalasi bajakan. Hasil analisis VirusTotal menunjukkan bahwa *file* ini terdeteksi sebagai berbahaya oleh 28 dari 64 vendor keamanan, dengan label ancaman populer seperti trojan.mikey/convagent, kategori trojan dan hacktool. Ini mengindikasikan adanya komponen *malware* dalam paket instalasi bajakan. Sedangkan untuk Internet Download Manager 6.42.41.rar merupakan paket instalasi bajakan yang tercantum pada gambar 2.3, hasil dari *File* ini terdeteksi sebagai berbahaya oleh 34 dari 64 vendor keamanan. Label ancaman populer yang teridentifikasi mencakup trojan.doina/killproc2, dengan kategori trojan dan dropper, yang menunjukkan adanya komponen berbahaya dalam paket instalasi IDM bajakan ini.



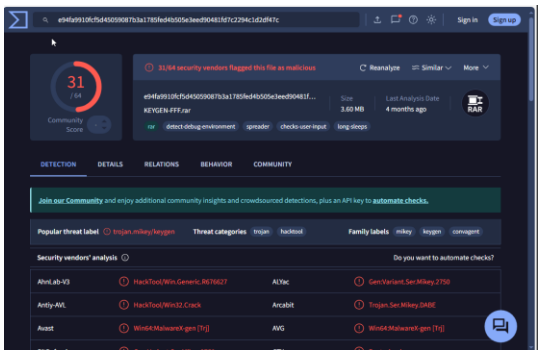
Gambar 2.2. Tangkapan Layar VirusTotal Hasil Deteksi *Malware* untuk *WinRAR* 7.01.rar



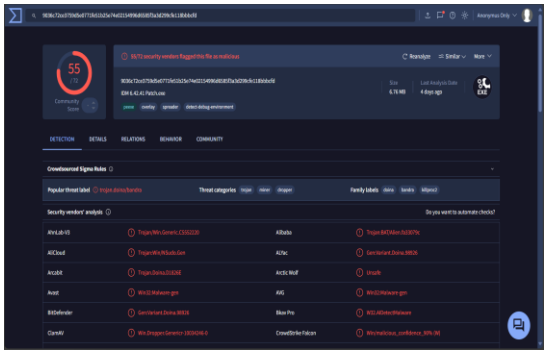
Gambar 2.3. Tangkapan Layar VirusTotal Hasil Deteksi Malware untuk IDM 6.42.41.rar

Selanjutnya Pada gambar 2.4 merupakan aktivator pada WinRaR yaitu *KEYGEN-FFF.rar*. Hasil dari *file* ini terdeteksi sebagai berbahaya oleh 31 dari 64 vendor keamanan. Label ancaman yang ditemukan mencakup trojan.mikey/keygen, dengan kategori trojan dan hacktool. Hal ini mengkonfirmasi sifat mencurigakan dari aktivator. Selain itu Untuk IDM.6.42.41.Patch.exe merupakan aktivator IDM yang tercantum pada gambar 2.5, hasil dari *file* ini terdeteksi sebagai berbahaya oleh 55 dari 72

vendor keamanan. Label ancaman populer yang teridentifikasi mencakup trojan.doina/bandra, dengan kategori trojan, miner, dan dropper, yang mengkonfirmasi sifat *malware* yang kuat pada aktivator IDM ini.



Gambar 2.4. Tangkapan Layar VirusTotal Hasil Deteksi Malware untuk KEYGEN-FFF.rar.

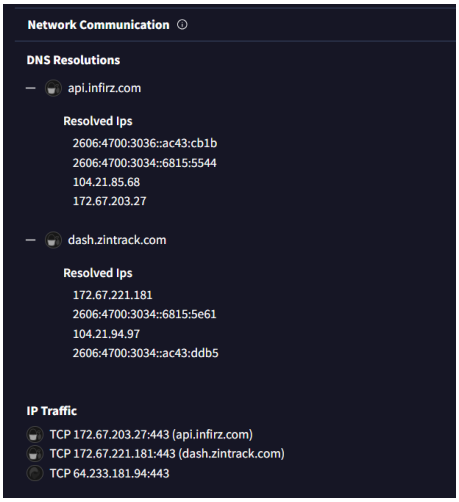


Gambar 2.5. Tangkapan Layar VirusTotal: Hasil Deteksi Malware untuk IDM.6.42.41.Patch.exe

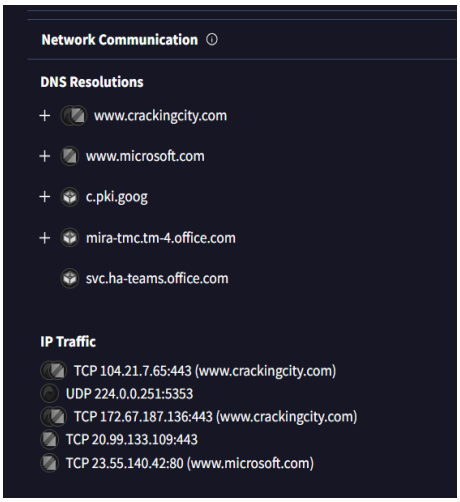
Selanjutnya Analisis laporan "Network Communication" pada VirusTotal untuk KEYGEN-FFF.rar (aktivator WinRaR) dan IDM.6.42.41.Patch.exe mengungkapkan adanya resolusi DNS dan IP yang tertera pada tabel 2 dan dibuktikan pada gambar 2.6 dan 2.7. Pola komunikasi ini jelas mengindikasikan aktivitas yang tidak normal bagi perangkat lunak resmi, yang menguatkan adanya aktivitas mencurigakan terkait pembajakan. Untuk secara spesifik mengindikasikan upaya komunikasi mencurigakan yang terkait dengan aktivasi ilegal.

Tabel 2. Ringkasan Analisis Komunikasi Jaringan Aktivator dari VirusTotal

no	Aktivator	Resolusi DNS	IP
1	KEYGEN-FFF.rar	api.infirz.com dash.zintrack.com	104.21.85.68 172.67.203.27 104.21.94.97 172.67.221.181
2	IDM.6.42.41.Patch.exe	www.crackingcity.com	104.21.7.65 172.67.187.136

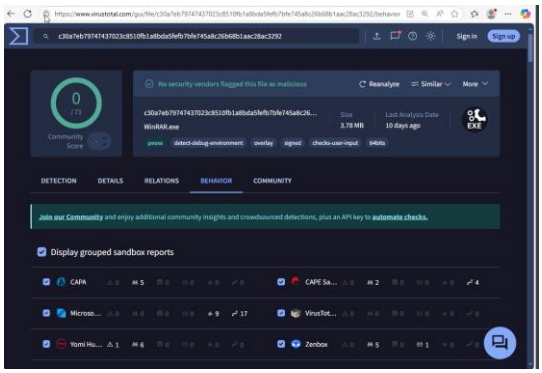


Gambar 2.6. tangkapan layar VirusTotal komunikasi jaringan terdeteksi dari *KEYGEN-FFF.rar*.

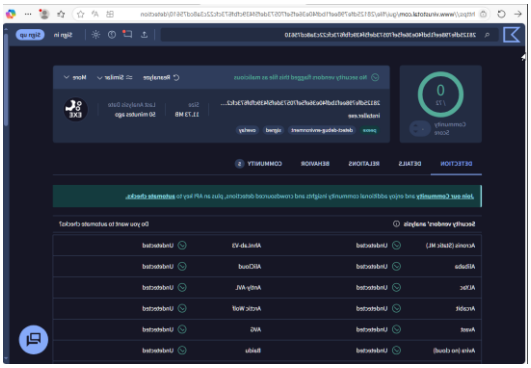


Gambar 2.7. tangkapan layar VirusTotal komunikasi jaringan terdeteksi dari IDM.6.42.41.Patch.exe

Selanjutnya pada analisis WinRAR.exe software inti dari paket WinRAR 7.01.rar yang tercantum pada gambar 2.8, dalam analisis VirusTotal menunjukkan hasil yang bersih, yaitu 0 dari 71 vendor keamanan tidak mendeteksi file ini sebagai berbahaya. Hal ini mengkonfirmasi bahwa *executable* utama dari software WinRAR, meskipun berasal dari paket bajakan, tidak mengandung *malware*. Ini menunjukkan bahwa ancaman lebih berpusat pada komponen aktivasi atau metode distribusi yang tidak sah. Sedangkan untuk installer.exe software inti dari paket Internet Download Manager 6.42.41.rar yang tercantum pada gambar 2.9, dari hasil Analisis VirusTotal menunjukkan hasil yang bersih, yaitu 0 dari 72 vendor keamanan tidak mendeteksi *file* ini sebagai berbahaya. Sama halnya dengan analisis pada WinRaR.



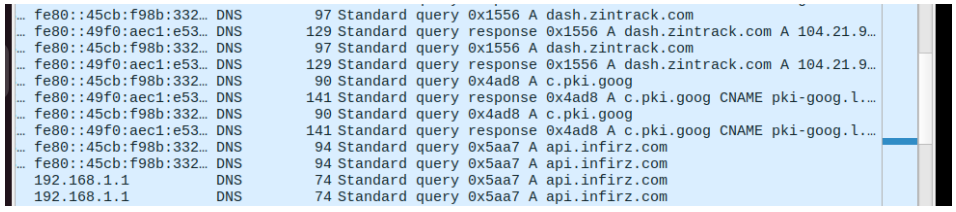
Gambar 2.8. Tangkapan Layar VirusTotal Hasil Deteksi untuk WinRAR.exe.



Gambar 2.9. Tangkapan Layar VirusTotal Hasil Deteksi untuk installer.exe (IDM).

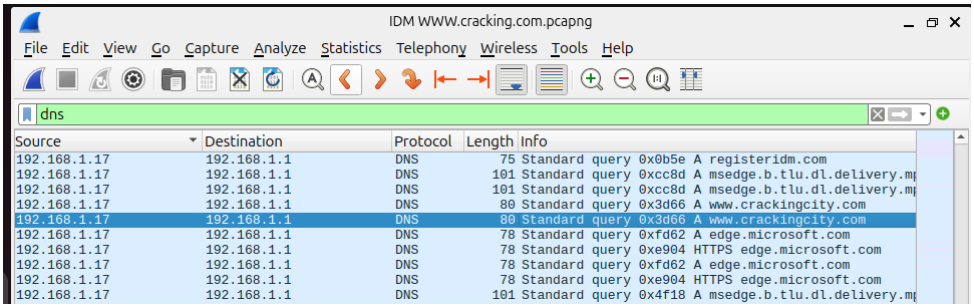
2.4.1.2 Analisis Lalu Lintas Jaringan dengan Wireshark

Selanjutnya tahapan ini mencakup analisis terhadap installasi software WinRAR dan IDM yang dilakukan secara terpisah, dengan pemantauan menggunakan Wireshark, dalam hal ini software di install pada client 1 kemudian di amati oleh Wireshark. Hasil dari Observasi WinRAR terhadap lalu lintas jaringan saat instalasi WinRAR dan pengaktifan aktivator menunjukkan adanya pola komunikasi yang anomali terlihat pada gambar 2.10. Teridentifikasi permintaan DNS ke domain yang sama pada analisis di VirusTotal yaitu dash.zintrack.com dan api.infirz.com. selanjutnya pada statistik percakapan aktivitas WinRaR yang ditangkap pada gambar 2.11, bahwa teridentifikasi 2 alamat ip yang sama pada analisis VirusTotal yaitu 104.21.94.97 dan 104.21.85.68. Sedangkan pada aktivator IDM, observasi Wireshark menunjukkan adanya permintaan DNS ke domain www.crackingcity.com. Selain itu, teramati juga koneksi TCP ke alamat IP 104.21.7.65 yang bisa diliat pada gambar 2.12 dan gambar 2.13.

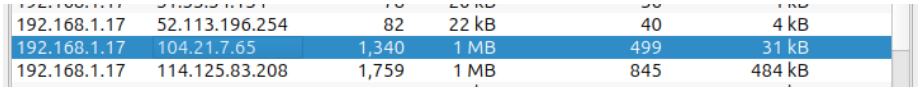


Gambar 2.10. Tangkapan Layar Wireshark: Analisis DNS Aktivitas WinRAR Crack

Gambar 2.11. Tangkapan Layar Wireshark Statistik Percakapan Aktivitas WinRAR Crack.



Gambar 2.12. Tangkapan Layar Wireshark: Analisis DNS Aktivitas WinRAR Crack



192.168.1.17	52.113.196.254	82	22 kB	40	4 kB
192.168.1.17	104.21.7.65	1,340	1 MB	499	31 kB
192.168.1.17	114.125.83.208	1,759	1 MB	845	484 kB

Gambar 2.13. Tangkapan Layar Wireshark Statistik Percakapan Aktivitas WinRAR Crack.

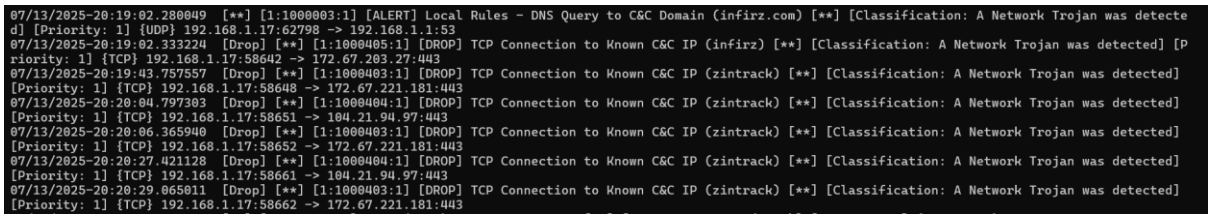
2.4.2 Pengujian Deteksi Sistem.

pengujian deteksi sistem yang telah diimplementasikan, memvalidasi efektivitas Suricata dalam mengidentifikasi aktivitas *malware* akibat *software piracy* berdasarkan *custom rules*.

1. Pengujian pada client 1 software piracy

   Pengujian dijalankan oleh client 1 dalam kondisi internet normal, setelah itu software di jalankan dengan aktivatornya, pada gambar 2.14 bisa dilihat bahwa Suricata berhasil mendeteksi aktivitas jaringan yang cocok dengan *custom rules*. Teridentifikasi adanya *alert* yang berkaitan dengan permintaan DNS ke domain api.infirz.com. Selanjutnya adanya koneksi TCP ke alamat IP C&C seperti 172.67.203.27, 172.67.221.181, dan 104.21.94.97 juga berhasil dideteksi dan diblokir oleh Suricata. Kegagalan aktivator untuk terhubung ke server C&C mengindikasikan keberhasilan pemblokiran.

   Selanjutnya pada gambar 2.15, IDM hanya berhasil mendeteksi permintaan DNS walaupun pada pra pengujian sudah teramati dengan baik dan tidak adanya aktifitas pemblokiran yang terjadi mengindikasikan bahwa aktivator IDM mungkin mengadopsi mekanisme komunikasi yang lebih sulit diblokir secara *inline* oleh *rules* TCP yang spesifik, namun deteksi DNS tetap memberikan indikasi awal adanya upaya komunikasi ilegal.



```
07/13/2025-20:19:02.280049  [**] [1:1000003:1] [ALERT] Local Rules - DNS Query to C&C Domain (infirz.com) [**] [Classification: A Network Trojan was detecte
d] [Priority: 1] {UDP} 192.168.1.17:62798 -> 192.168.1.1:53
07/13/2025-20:19:02.333224  [Drop] [**] [1:1000405:1] [DROP] TCP Connection to Known C&C IP (infirz) [**] [Classification: A Network Trojan was detected] [P
riority: 1] {TCP} 192.168.1.17:58642 -> 172.67.203.27:443
07/13/2025-20:19:43.757557  [Drop] [**] [1:1000403:1] [DROP] TCP Connection to Known C&C IP (zintrack) [**] [Classification: A Network Trojan was detected]
[Priority: 1] {TCP} 192.168.1.17:58648 -> 172.67.221.181:443
07/13/2025-20:20:04.797303  [Drop] [**] [1:1000404:1] [DROP] TCP Connection to Known C&C IP (zintrack) [**] [Classification: A Network Trojan was detected]
[Priority: 1] {TCP} 192.168.1.17:58651 -> 104.21.94.97:443
07/13/2025-20:20:06.365940  [Drop] [**] [1:1000403:1] [DROP] TCP Connection to Known C&C IP (zintrack) [**] [Classification: A Network Trojan was detected]
[Priority: 1] {TCP} 192.168.1.17:58652 -> 172.67.221.181:443
07/13/2025-20:20:27.421128  [Drop] [**] [1:1000404:1] [DROP] TCP Connection to Known C&C IP (zintrack) [**] [Classification: A Network Trojan was detected]
[Priority: 1] {TCP} 192.168.1.17:58661 -> 104.21.94.97:443
07/13/2025-20:20:29.065011  [Drop] [**] [1:1000403:1] [DROP] TCP Connection to Known C&C IP (zintrack) [**] [Classification: A Network Trojan was detected]
[Priority: 1] {TCP} 192.168.1.17:58662 -> 172.67.221.181:443
```

Gambar 2.14 *log alert* Suricata yang terpicu saat aktivator WinRAR dijalankan di Client 1.

```
07/14/2025-02:28:53.320535  [**] [1:1000005:1] [ALERT] Local Rules - DNS Que
ry to C&C Domain (crackingcity.com) [**] [Classification: A Network Trojan w
as detected] [Priority: 1] {UDP} 192.168.1.17:50796 -> 192.168.1.1:53
07/14/2025-02:28:57.814555  [**] [1:1000005:1] [ALERT] Local Rules - DNS Que
ry to C&C Domain (crackingcity.com) [**] [Classification: A Network Trojan w
as detected] [Priority: 1] {UDP} 192.168.1.17:55068 -> 192.168.1.1:53
```

Gambar 2.15 *log alert* Suricata yang terpicu saat aktivator IDM dijalankan di Client 1.

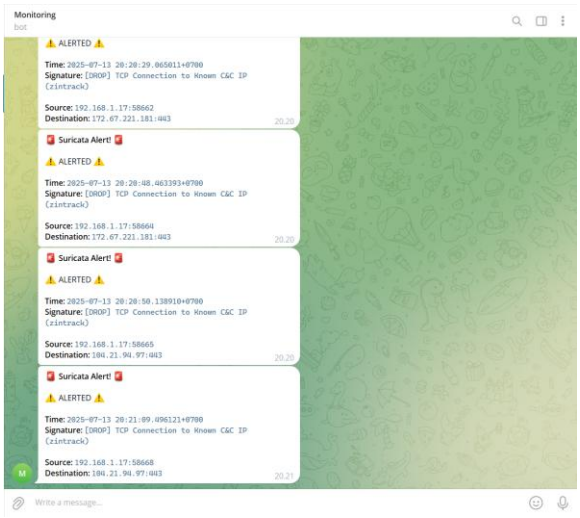
Selain kondisi internet normal, pengujian juga dilakukan saat server dalam keadaan *offline* atau tanpa koneksi internet, untuk menguji kemampuan deteksi pada fase awal komunikasi *malware*. Dalam skenario ini, Suricata tetap berhasil mendeteksi adanya permintaan DNS. Namun karena tidak ada koneksi internet, *rule* deteksi TCP yang seharusnya memblokir koneksi ke IP C&C tidak terpicu, mengindikasikan bahwa hanya fase resolusi nama domain yang berhasil diamati. Ketika koneksi internet diaktifkan kembali, tidak terjadi adanya koneksi mencurigakan yang terdeteksi oleh Suricata.

2. Pengujian pada client 2 software resmi

   Selanjutnya pengujian dijalankan oleh client 2 bahwa Suricata tidak menghasilkan *false positive* terhadap aktivitas jaringan yang sah. Hasil deteksi suricata Selama seluruh periode pengujian aktivitas normal pada client 2, Suricata tidak menghasilkan *alert* yang terkait dengan *custom rules* yang dirumuskan untuk mendeteksi *software piracy* atau *malware*. Ini mengindikasikan bahwa lalu lintas yang dihasilkan oleh aplikasi resmi tidak cocok dengan *signature* aktivitas mencurigakan yang telah didefinisikan.

3. Mekanisme Notifikasi Telegram.

   Sebelum diintegrasikan, bot Telegram dibuat menggunakan BotFather, dan API serta ID chat yang diperlukan telah diperoleh. Integrasi dilakukan dengan mengkonfigurasi Suricata untuk mengirimkan *alert* ke skrip yang kemudian akan memanggil API Telegram Bot. Skrip ini akan memformat informasi *alert* yang menjadi pesan mudah dibaca. Selanjutnya ketika apabila Suricata mendeteksi adanya aktivitas yang cocok dengan *custom rules* yang telah diterapkan, maka akan mengirimkan pesan melalui bot telegram yang sudah diintegerasikan. Hasil notifikasi yang diterima di Telegram seperti pada gambar 2.16.



Gambar 2.16 menampilkan notifikasi *alert* Suricata yang diterima melalui Telegram Bot.

HASIL

hasil analisis pra-pengujian menggunakan VirusTotal dan Wireshark yaitu perumusan *custom rules* Suricata, sebagai inti kemampuan deteksi sistem, didasarkan pada Pola komunikasi anomali serta indikator dari aktivator *software piracy* yang teridentifikasi, seperti domain dan alamat IP mencurigakan, menjadi dasar prinsip deteksi berbasis *signature*, digunakan untuk memicu *alert* pada Suricata.

Pada gambar 3.1 dan gambar 3.2 menunjukkan hasil custom rules yang kita buat berdasarkan analisis pada pra pengujian, custom rules yang sudah dibuat disimpan dalam file local.rules dan diaktifkan dalam konfigurasi utama suricata.yaml agar sistem dapat memuat dan memprosesnya selama pemantauan lalu lintas jaringan.

```
alert dns any any -> any any (msg:"[ALERT] Local Rules - DNS Query to C&C Domain (infirz.com)";
dns.query; content:"api.infirz.com"; nocase; classtype:trojan-activity; sid:1000003; rev:1;)
alert dns any any -> any any (msg:"[ALERT] Local Rules - DNS Query to C&C Domain (zintrack.com)";
dns.query; content:"dash.zintrack.com"; nocase; classtype:trojan-activity; sid:1000004; rev:1;)

alert dns any any -> any any (msg:"[ALERT] Local Rules - DNS Query to C&C Domain (crackingcity.com)";
dns.query; content:"crackingcity.com"; nocase; classtype:trojan-activity; sid:1000005; rev:1;)
```

Gambar 3.1 Tangkapan Layar rules untuk deteksi query DNS

ke domain C&C WinRAR dan IDM

```
drop tcp any any -> 172.67.221.181 any (msg:"[DROP] TCP Connection to Known C&C IP (zintrack)"; classtype:trojan-activity; sid:1000403; rev:1;)
drop tcp any any -> 104.21.94.97 any (msg:"[DROP] TCP Connection to Known C&C IP (zintrack)"; classtype:trojan-activity; sid:1000404; rev:1;)
drop tcp any any -> 172.67.203.27 any (msg:"[DROP] TCP Connection to Known C&C IP (infirz)"; classtype:trojan-activity; sid:1000405; rev:1;)
drop tcp any any -> 104.21.85.68 any (msg:"[DROP] TCP Connection to Known C&C IP (infirz)"; classtype:trojan-activity; sid:1000405; rev:1;)

drop tcp any any -> any 104.21.7.65 any (msg:"[DROP] TCP/SSL Connection to C&C IP (crackingcity.com)"; classtype:trojan-activity; sid:1000406; rev:1;)
drop tcp any any -> any 172.67.187.136 any (msg:"[DROP] TCP/SSL Connection to C&C IP (crackingcity.com)"; classtype:trojan-activity; sid:1000407; rev:1;)
```

Gambar 3.2 Tangkapan Layar rules untuk memblokir koneksi

TCP ke alamat IP C&C WinRAR dan IDM

PEMBAHASAN

Implementasi Network-based Intrusion Prevention System (NIPS) berbasis Suricata terbukti efektif dalam mendeteksi aktivitas *malware* yang terkait dengan *software piracy*. Hasil pengujian pada Client 1 menunjukkan bahwa Suricata berhasil mengidentifikasi dan memicu *alert* serta memblokir koneksi yang dihasilkan oleh aktivator WinRAR (KEYGEN-FFF.rar). Deteksi ini mencakup permintaan DNS ke domain api.infirz.com dan dash.zintrack.com serta koneksi TCP ke alamat IP *Command and Control* (C&C) yang teridentifikasi (172.67.203.27, 172.67.221.181, 104.21.94.97, 104.21.85.68). Senada dengan WinRAR dalam hal deteksi awal, Suricata juga berhasil mendeteksi aktivitas mencurigakan yang dihasilkan oleh aktivator IDM pada Client 1. Deteksi untuk IDM ini melibatkan identifikasi permintaan DNS ke domain crackingcity.com. Namun, perlu dicatat bahwa tidak ada aktivitas pemblokiran TCP yang teramati untuk aktivator IDM, berbeda dengan deteksi WinRAR. Hal ini mengindikasikan bahwa meskipun niat komunikasi ilegal teridentifikasi melalui DNS, mekanisme *blocking* pada level TCP mungkin tidak sepenuhnya efektif untuk pola komunikasi spesifik IDM, atau aktivitas tersebut tidak melibatkan koneksi TCP yang sesuai dengan *rules* drop. Keberhasilan deteksi baik DNS maupun pemblokiran TCP untuk WinRAR, dan DNS untuk IDM didasarkan pada *custom rules* Suricata yang dirumuskan secara spesifik, yang secara langsung menargetkan *signature* komunikasi anomali dari aktivator tersebut. Pendekatan ini selaras dengan prinsip deteksi berbasis *signature*, di mana pola atau karakteristik unik dari aktivitas berbahaya digunakan sebagai ciri khas untuk identifikasi.

Penelitian ini juga mengungkapkan kemampuan Suricata untuk mendeteksi *intent* komunikasi *malware* bahkan dalam kondisi server *offline* atau tanpa koneksi internet. Dalam skenario ini, permintaan DNS oleh aktivator tetap terdeteksi oleh Suricata, meskipun koneksi TCP ke IP C&C tidak terjadi karena ketiadaan konektivitas. Hal ini menunjukkan bahwa sistem mampu mengidentifikasi fase awal aktivitas berbahaya. Kemudian, ketika koneksi internet diaktifkan kembali, tidak terjadi adanya koneksi mencurigakan yang terdeteksi, mengindikasikan efektivitas pencegahan aktif. Temuan

ini menyoroti pentingnya deteksi berlapis dan responsif, sejalan dengan prinsip NIPS yang bekerja

KESIMPULAN

Penelitian ini berhasil mengimplementasikan dan menguji Network-based Intrusion Prevention System (NIPS) berbasis Suricata untuk mendeteksi aktivitas malware yang disebabkan oleh *software piracy*. Sistem ini, yang dilengkapi dengan aturan khusus (custom rules), terbukti sangat efektif dalam mengidentifikasi dan memblokir lalu lintas jaringan mencurigakan dari aktivator bajakan, seperti permintaan DNS ke domain Command and Control (C&C) dan koneksi TCP berbahaya. Meskipun demikian, ada perbedaan respons; untuk aktivator WinRAR, pemblokiran TCP teramati, sementara untuk aktivator IDM, hanya deteksi permintaan DNS yang terjadi tanpa pemblokiran TCP. Keberhasilan ini didukung oleh presisi tinggi custom rules yang dirancang berdasarkan analisis mendalam menggunakan VirusTotal dan Wireshark, memastikan tingkat *false positive* yang rendah saat diuji dengan aplikasi resmi.

Selain kemampuan deteksi dan pemblokiran yang kuat, Suricata juga menunjukkan keandalannya dalam mendeteksi aktivitas malware bahkan saat server *offline* atau tanpa koneksi internet, dengan berhasil mengidentifikasi *query* DNS mencurigakan sebagai fase awal komunikasi malware. Efektivitas sistem ini diperkuat oleh mekanisme notifikasi *real-time* melalui integrasi bot Telegram, yang segera memberikan peringatan kepada administrator jaringan mengenai insiden keamanan. Secara keseluruhan, penelitian ini tidak hanya membuktikan keampuhan deteksi berbasis *signature* dalam mengidentifikasi ancaman siber yang sudah dikenal, tetapi juga berhasil mengembangkannya untuk mendeteksi aktivitas malware spesifik akibat *software piracy* melalui penerapan *custom rules* dan NIPS secara aktif.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada semua pihak yang telah memberikan kontribusi teknis dalam penyusunan artikel ini, khususnya kepada dosen pembimbing atas bimbingan dan arahannya yang sangat berarti. Ucapan terima kasih tidak ditujukan kepada pihak-pihak yang telah tercantum sebagai penulis.

DAFTAR PUSTAKA

[1] B. S. Anggoro dan W. Sulistyo, “Implementasi Intrusion Prevention System Suricata dengan Anomaly-Based untuk Keamanan Jaringan PT. Grahamedia Informasi,” 2021.

[2] Deni dan Misnen, “Piracy as a Violation of the Ethics of the Informatics Engineering Profession,” *IMPROSCI*, vol. 1, no. 6, 2024, [Daring]. Tersedia pada: https://annpublisher.org/ojs/index.php/improsci

[3] Y. Rahayu dan N. Trianto, "Analisis Malware Menggunakan Metode Analisis Statis dan Dinamis untuk Pembuatan IOC Berdasarkan STIX Versi 2.1," *Jurnal Info Kripto*, vol. 15, hlm. 106–111, 2021.

[4] Z. T. Sworna, Z. Mousavi, dan M. A. Babar, "NLP methods in host-based intrusion detection systems: A systematic review and future directions," *Journal of Network and Computer Applications*, vol. 220, hlm. 103761, Nov 2023, doi: 10.1016/J.JNCA.2023.103761.

[5] A. Rahmat Aulia, E. I. Alwi, A. Widya, dan M. Gaffar, "Perancangan Sistem Keamanan Jaringan Intrusion Prevention System Menggunakan Suricata Dan IPTables," *Literatur Informatika & Komputer*, vol. 1, no. 3, hlm. 235–240, 2024, doi: 10.33096/linier.vxix.xxxx.

[6] R. E. Susanti, A. W. Muhammad, dan W. A. Prabowo, "Implementasi Intrusion Prevention System (IPS) OSSEC dan Honeypot Cowrie," *Jurnal Sisfokom (Sistem Informasi dan Komputer)*, vol. 11, no. 1, hlm. 73–78, Apr 2022, doi: 10.32736/sisfokom.v11i1.1246.

[7] M. Syani, "Implementasi Intrusion Detection System (IDS) Menggunakan Suricata Pada Linux Debian 9 Berbasis Cloud Virtual Private Servers (VPS)," *Jurnal Inkofar* , vol. 1, no. 1, hlm. 2581–2920, 2020.

[8] A. Ugbari dan S. O. Adebayo, "A Comprehensive Review of Network Intrusion Detection Systems," *International Journal of Research in Engineering and Science (IJRES) ISSN*, vol. 13, hlm. 190–198, 2025, [Daring]. Tersedia pada: www.ijres.org

[9] A. Bensaoud, J. Kalita, dan M. Bensaoud, "A survey of malware detection using deep learning," *Machine Learning with Applications*, vol. 16, hlm. 100546, Jun 2024, doi: 10.1016/j.mlwa.2024.100546.

[10] V. K. Ravindran, S. S. Ojha, dan A. Kamboj, "A Comparative Analysis of Signature-Based and Anomaly-Based Intrusion Detection Systems," *IJLTEMAS*, vol. XIV, no. V, hlm. 209–214, 2025, doi: 10.51583/IJLTEMAS.

[11] I. Cahyo Utomo dan S. Rokhmah, "Konfigurasi SSL Untuk Meningkatkan Keamanan Web server Pada Program Studi Teknik Informatika Universitas Muhammadiyah Surakarta," *JURTI*, vol. 6, no. 2, 2022.

[12] A. Kurniawan dan L. M. Silalahi, "Analisis Keamanan Jaringan Menggunakan Intrusion Prevention System (IPS) Dengan Metode Traffic Behavior," *Jurnal Rekayasa dan Teknologi Elektro*, vol. 17, no. 1, 2023.

[13] M. Suci dan Lukman, "Analisis Perbandingan Kinerja Snort Dan Suricata Sebagai Intrusion Detection System Dalam Mendeteksi Serangan Syn Flood Pada Web Server Apache," *Jurnal Teknologi Informasi*, vol. XV, hlm. 6–15, 2020.

[14] R. M. Farhan, G. Hendita, dan A. Kusuma, "Teknik Sniffing Jaringan Menggunakan Wireshark," *Journal of Informatics and Advanced Computing (JIAC)*, vol. 4, no. 1, 2023.

[15] F. T. Anugrah, S. Ikhwan, dan J. Gusti, "Implementasi Intrusion Prevention System (IPS) Menggunakan Suricata Untuk Serangan SQL Injection," *Techné Jurnal Ilmiah Elektroteknika*, vol. 21, hlm. 199–210, 2022.

[16] Y. Yuliana, H. Adnan Mooduto, dan R. Hadi, "Deteksi Ancaman Keamanan Pada Server dan Jaringan Menggunakan OSSEC," *Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 3, no. 1, hlm. 8–15, 2022, [Daring]. Tersedia pada: http://jurnal-itsi.org