P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i1

Pencegahan Dan Konsep IDS (Intrusion Detection System) Dalam Mendeteksi Serangan Siber Pada Sistem Keamanana Di Universitas Persada Indonesia Y.A.i

[1]Louis Saroha, [2]Rendy Octavianto, [3]Essy Malays Sari Sakti

[1,2,3]Prodi Informatika Fakultas Teknik Universitas Persada Indonesia Y.A.I, Jakarta

E-mail: [1]rendy.octavianto.2144190004@upi-yai.ac.id
[2]louis.saroha.2144190021@upi-yai.ac.id, [3]essy.malays@upi-yai.ac.id

ABSTRAK

Internet telah menjadi bagian tak terpisahkan dari kehidupan masyarakat, membuka akses informasi dan komunikasi tanpa batas.Namun di balik kemudahannya, Internet juga mengandung ancaman keamanan yang perlu diwaspadai. Serangan hacker terus meningkat, merugikan individu, organisasi, dan bahkan seluruh negara. Pencegahan merupakan pertahanan utama terhadap serangan hacker untuk melindungi data-data penting agar tidak mudah diserang oleh hacker. IDS (Intrusion Detection System) ibarat benteng di era digital, memantau dan melindungi jaringan komputer dari serangan cyber yang semakin canggih. Pencegahan sangat penting dan IDS berperan penting dalam mendeteksi dan merespons berbagai ancaman. IDS dapat memantau dan membandingkan pola aktivitas jaringan menggunakan database. Metode penelitian ini menggunakan desain studi kasus kualitatif. Data yang dikumpulkan diperiksa keasliannya, pemahamannya, dan keandalannya melalui pencarian dan analisis.Setiap kasus kemudian diselesaikan dan dibandingkan dengan data lain untuk menarik kesimpulan. Upaya agar tidak terkena serangan siber dalam sistem keamanan universitas banyak cara untuk mencegah terjadinya serangan siber pada sistem di universitas, sebagai contoh salah satu caranya dengan menggunakan honeypot yang dirancang menyerupai sistem atau layanan yang berguna untuk mengelabui hacker bisa menyusup ke sistem jaringan universitas dan untuk memonitoring jaringan bisa menggunakan IDS.

Kata Kunci : *Internet, Hacker, IDS, Pencegahan*

ABSTRACT

The Internet has become an inseparable part of people's lives, opening up unlimited access to information and communication. However, behind its convenience, the Internet also contains security threats that need to be watched out for. Hacker attacks continue to increase, harming individuals, organizations, and even entire countries. Prevention is the main defense against hacker attacks to protect important data from being easily attacked by hackers. IDS (Intrusion Detection System) is like a fortress in the digital era, monitoring and protecting computer networks from increasingly sophisticated cyber attacks. Prevention is critical and IDS plays a vital role in detecting and responding to various threats. IDS can monitor and compare network activity patterns using a database. This research method uses a qualitative case study design. The data collected is checked for authenticity, understanding and reliability through search and analysis. Each case is then resolved and compared with other data to draw conclusions. There are many ways to prevent cyber attacks on university systems, for example one way is to use a honeypot which is designed to resemble a system or service that is useful for tricking hackers into infiltrating university network systems and to monitor the network you can use IDS.

***Keyword** : Internet, Hacker, IDS, prevention*

https://doi.org/10.37817/tekinfo.v25i1
P-ISSN: 1411-3635
E-ISSN: 2962-5645

1. PENDAHULUAN

Internet telah menjadi bagian tak terpisahkan dari kehidupan masyarakat, membuka akses informasi dan komunikasi tanpa batas. Dengan adanya internet ,memungkinkan kepada semua orang melakukan kontak atau hubungan secara tidak langsung dengan adanya komunitas dunia maya lainnya. Teknologi komunikasi merupakan perkembangan yang sangat maju di era modern ini.Berbagai jenis teknologi diusulkan dengan tujuan memfasilitasi aktivitas manusia(Bukit & Rahmi Ayunda, 2022).

Namun dibalik kemudahannya, Internet juga mengandung ancaman keamanan yang perlu diwaspadai. Serangan hacker terus meningkat, merugikan individu,organisasi, dan bahkan seluruh negara.

Informasi yang diperoleh dari Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas) Badan Nasional Keamanan Siber dan Kriptografi (BSSN) menunjukkan bahwa telah terjadi sekitar 88.414.296 serangan sejak 1 Januari hingga 12 April 2020.(Iqbal et al., 2022)

Kejahatan yang berkaitan dengan komputer atau jaringan dikategorikan ke dalam cybercrime yang dapat berskala kecil dimana pelaku atau korbannya adalah individu atau kelompok kecil, atau berskala besar yang jaringan kriminalnya tersebar seperti pada contoh, Secara internasional. Teknologi Informasi dan Elektronika Seiring dengan berkembangnya tren penggunaan platform dan perangkat, tren dan jenis kejahatan dunia maya pun ikut berubah. Ponsel pintar kini telah menggantikan komputer dan laptop sebagai perangkat utama yang digunakan kebanyakan orang untuk mengakses Internet, dan layanan berbasis cloud juga semakin banyak tersedia. (Purwani, 2023)

Pencegahan merupakan pertahanan utama terhadap serangan hacker untuk melindungi data-data penting agar tidak mudah diserang oleh hacker. Untuk mencegah potensi serangan, sistem atau metode yang dikenal sebagai sistem deteksi intrusi “IDS”;. ,IDS (Intrusion Detection System) ibarat benteng diera digital, memantau dan melindungi jaringan komputer dari serangan cyber yang semakin canggih. Pencegahan sangat penting dan IDS berperan penting dalam mendeteksi dan merespons berbagai ancaman. IDS dapat memantau dan membandingkan pola aktivitas jaringan menggunakan database. IDS menggunakan algoritma pembelajaran mesin untuk mendeteksi anomali dalam aktivitas jaringan.

Misalnya, upaya administrator jaringan untuk mengamankan sistem jaringan komputer yang dikelola dari penjahat dunia maya bergantung pada penggunaan teknologi deteksi intrusi yang disebut sistem deteksi intrusi "IDS".Juga dikenal sebagai Sistem deteksi intrusi (IDS) adalah suatu sistem yang memiliki kemampuan untuk melacak lalu lintas jaringan dan menemukan aktivitas mencurigakan, sehingga dapat

P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i1

mencegah serangan atau aktivitas yang mungkin membahayakan sistem jaringan komputer yang dibangun di atasnya.

Click or tap here to enter text.Karena alasan ini, sistem keamanan Teknologi Informasi tradisional seperti firewall atau Intrusion Detection System/ Intrusion Prevention System (IDS/IPS) diperlukan adanya tambahan pengamanan guna memberikan perlindungan yang komprehensif(*321-Article Text-805-2-10-20220319,* n.d.).

Dengan adanya penerapan di universitas semoga dapat membangkitkan minat siswa dan meningkatkan keterlibatan dalam pembelajaran(Ekowati et al., n.d.).

2. LANDASAN TEORI

Perguruan tinggi sebagai pusat pendidikan tinggi dan penelitian menyimpan data dan informasi sensitif seperti data mahasiswa, guru, dan peneliti.Aset digital ini merupakan sasaran empuk serangan siber.Konsekuensi dari serangan semacam itu bisa sangat buruk, seperti yang dikemukakan oleh banyak pakar keamanan siber (misalnya, [Organisasi 1], [Organisasi 2]). Kerugian yang dapat terjadi meliputi:

- **Kebocoran data**:

Tersebarnya data yang sensitif bisa merusak nama baik universitas dan berakibat hukum.

- **Gangguan operasional**:

Terjadinya serangan dapat mengganggu operasional universitas, seperti sistem pembelajaran online, layanan administrasi, dan penelitian.

- **Kehilangan finansial**:

Tejadinya berakibat menibulkan kerugian finansial bagi universitas, seperti pencurian data keuangan dan kerusakan infrastruktur.

2.1 Pengertian Serangan Siber

Tujuannya adalah untuk mencuri, memodifikasi, merusak, dan bahkan menghancurkan target tertentu melalui peretasan. Serangan siber adalah serangan yang mengancam yang dilakukan oleh individu, kelompok, organisasi, atau negara. Pihak-pihak ini menargetkan sumber anonim, seperti sistem informasi perangkat komputer, jaringan, infrastruktur, atau perangkat pribadi. Tujuannya adalah mencuri, mengubah, merusak, dan bahkan menghancurkan target melalui peretasan.

2.2 Jenis-jenis serangan siber

malware yang dirancang untuk merusak atau mengambil kendali sistem komputer yang rentan. Serangan ini biasanya dilakukan melalui tautan atau lampiran yang tidak aman dalam email atau media sosial. Saat pengguna mengeklik tautan atau membuka lampiran, malware dapat memasuki sistem dan merusaknya, mencuri data, atau mengambil kendali dengan cara yang tidak diinginkan. (https://nordvpn.com/id/blog/serangan-siber/, n.d.)

Selain itu, serangan DDoS (Distributed Denial of Service) merupakan jenis kejahatan dunia maya yang sering terjadi. Dalam serangan DDoS, pelaku mencoba mengejutkan sistem dengan

https://doi.org/10.37817/tekinfo.v25i1
P-ISSN: 1411-3635
E-ISSN: 2962-5645

mengirimkan lalu lintas Internet dalam jumlah besar ke target yang dituju.
Artinya sistem tidak lagi berfungsi dengan baik atau tidak dapat diakses sama sekali. Serangan DDoS dapat menghabiskan banyak waktu, uang, dan sumber daya bagi perusahaan.

Gambar1. Jenis_Serangan_Siber
Sumber : (https://course-net.com/blog/5-tren-cyber-security-yang-perlu-diketahui-di-tahun-2023/, n.d.)

2.3 Pencegahan Serangan Siber

Pencegahan adalah langkah utama yang penting untuk melindungi sistem dari serangan dunia maya. Beberapa metode pencegahan yang dapat diterapkan di lingkungan universitas antara lain:

- **Edukasi dan Kesadaran:** Melatih untuk kesadaran sivitas akademika tentang keamanan siber melalui pelatihan, seminar, dan sosialisasi.
- **Kebijakan Keamanan:** Memberikan kebijakan keamanan yang kuat, termasuk menerapkan kata sandi, kontrol akses, dan penggunaan perangkat lunak yang aman.
- **Perlindungan Jaringan:** Memasang firewall, antivirus, dan sistem deteksi intrusi untuk menjaga jaringan dari serangan eksternal.
- **Pemeliharaan Sistem:** Melakukan update dan patch sistem operasi dan perangkat lunak secara berkala untuk menutup celah keamanan.
- **Pencadangan Data:** Melakukan backup data secara rutin untuk pemulihan bila terjadi serangan.
- **Manajemen Risiko:** Mengidentifikasi, menganalisis, dan mengelola risiko keamanan siber secara berkelanjutan.

2.4. pengertian IDS (Intrusion Detection System)

Tentang IDS Sistem deteksi intrusi (IDS) adalah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas mencurigakan pada sistem atau jaringan.

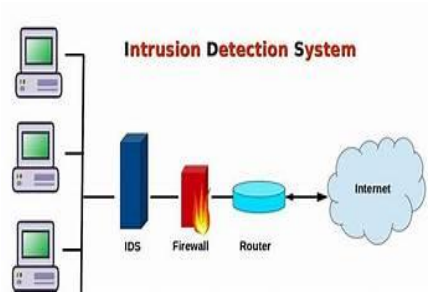
IDS digunakan untuk mendeteksi aktivitas mencurigakan pada suatu sistem atau jaringan. Intrusi adalah aktivitas apa pun yang tidak sah atau tidak diinginkan yang merusak kerahasiaan, integritas, dan/atau ketersediaan informasi yang terkandung dalam suatu sistem.

IDS memonitor lalu lintas di jaringan Anda dan mengambil data dari file log.

IDS menggunakan algoritma khusus untuk menganalisis dan memutuskan apakah akan mengeluarkan peringatan kepada administrator jaringan.

IDS (Intrusion Detection System) sendiri mempunyai beberapa arti : a.Sistem untuk mendeteksi penyusup jaringan. Pada awal serangan, penyusup biasanya hanya memeriksa data. Namun, pada tingkat yang lebih serius, penyusup berupaya mendapatkan akses ke sistem dengan membaca data sensitif, memodifikasi data tanpa izin, mengurangi akses ke sistem, atau bahkan mematikan sistem.(Gondohanindijo, 2019), (Laksana & Mulyani, 2024)

P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i1



Gambar2. IDS (Intrusion Detection System)

Sumber : (https://edukasiteki.blogspot.com/2018/01/cara-kerja-sistem-pendeteksi-dan.html, n.d.)

2.5. Konsep IDS (Intrusion Detection System)

IDS (Intrusion Detection System) adalah sistem yang berperan aktif dalam mengamankan jaringan dan sistem komputer dengan cara memantau aktivitas jaringan dan sistem untuk mendeteksi aktivitas mencurigakan yang mengindikasikan adanya serangan siber

Cara kerja IDS secara umum

a) Pemantauan jaringan: IDS bertindak sebagai pengamat yang waspada, memantau lalu lintas data yang melewati jaringan anda. Ini menganalisis setiap paket data, mencari pola atau aktivitas yang tidak biasa.Ini mungkin termasuk: Lonjakan volume lalu lintas, Beberapa upaya login gagal, Lalu lintas dari lokasi tidak sah, Upaya mengakses sumber daya yang dibatasi.(Indra Prasetya et al., 2014)

b) Deteksi Berdasarkan tanda Signature: Bayangkan sebuah IDS dengan perpustakaan sidik jari penjahat dunia maya (analog dengan keamanan dunia maya).Ia memelihara database tanda tangan, yang merupakan pola unik yang terkait dengan serangan cyber tertentu.Ketika IDS mendeteksi aktivitas jaringan yang cocok dengan tanda tangan di database-nya, IDS mengeluarkan peringatan, yang menunjukkan potensi serangan berdasarkan metode yang diketahui. Jika serangan terjadi dan pola serangan ditemukan di database, sistem deteksi intrusi dapat mengambil tindakan terhadap serangan yang terdeteksi.

c) Deteksi Anomali: Keadaan yang dimana terjadi pada network traffic yang menyebabkan kondisi menjadi tidak normal(Imam et al., n.d.). IDS tidak terbatas pada ancaman yang diketahui.Ia juga dapat bertindak sebagai analis perilaku. Dengan menggunakan algoritma tingkat lanjut, IDS dapat mempelajari pola aktivitas jaringan yang khas.Setiap penyimpangan yang signifikan dari perilaku dasar ini, seperti peningkatan lalu lintas secara tiba-tiba dari perangkat tertentu, dapat ditandai sebagai perilaku yang tidak wajar dan berpotensi rentan terhadap serangan.Hal ini membantu mendeteksi serangan baru atau serangan "zero-day" yang tidak tercatat.

d) Peringatan dan Respon: IDS akan dilengkapi dengan aturan untuk mendeteksi pemindaian jaringan dan serangan DOS. IDS akan menganalisis aktivitas jaringan berdasarkan aturan yang diberikan dan mengeluarkan peringatan "**peringatan**"; kepada pengelola apabila terjadi kegiatan yang melanggar peraturan(Widodo & Sekti Aji, 2022). Ketika IDS

https://doi.org/10.37817/tekinfo.v25i1
P-ISSN: 1411-3635
E-ISSN: 2962-5645

mendeteksi sesuatu yang mencurigakan, IDS tidak akan tinggal diam.Ini memicu alarm, memperingatkan personel keamanan akan potensi ancaman. Peringatan ini biasanya mencakup rincian seperti sifat aktivitas mencurigakan, sumber serangan, dan potensi dampaknya. Hal ini memungkinkan tim keamanan untuk menyelidiki lebih lanjut dan mengambil tindakan yang tepat untuk mengurangi serangan tersebut.

2.6. Honeypot

Layanan yang dirancang menyerupai sistem, dan layanan serta fitur dalam jaringan, dimaksudkan untuk menguping penyerang dan mempersulit hidup mereka.

Honeypot dapat diartikan sebagai penyesatan yang dilakukan oleh penyerang yang berasumsi bahwa mereka telah menyusup ke sistem dan memperoleh data di jaringan .

Peristiwa yang terjadi pada honeypots sangat berguna bagi administrator jaringan sebagai bentuk notifikasi untuk melakukan tindakan preventif sebelum terjadi serangan nyata pada server yang sebenarnya.(Purwoko et al., 2023)

3. METODOLOGI

Metode penelitian ini menggunakan desain studi kasus kualitatif. Data dikumpulkan peneliti berdasarkan hasil search dan analisis khususnya observasi partisipan dan dokumentasi. metode kualitatif dengan mencari referensi-referensi dari beberapa jurnal dengan meringkas ide pokok yang sesuai dengan judul dan diketik ulang dengan beberapa kalimat yang peneliti ubah.

Data yang dikumpulkan diperiksa keasliannya, pemahamannya, dan keandalannya melalui pencarian dan analisis.Setiap kasus kemudian diselesaikan dan dibandingkan dengan data lain untuk menarik kesimpulan. (Nasruji, 2019)

Gambar3. Process_diagram_pembuatan

Dalam proses pembuatan jurnal ini, saya mencari beberapa referensi jurnal yang berhubungan dengan judul jurnal saya. Setelah nya peneliti mencari ide pokok atau kesimpulan pada referensi untuk dijadikan isi jurnal peneliti khususnya di Bab 2 yang merupakan tinjauan pustaka.

4. HASIL DAN PEMBAHASAN

4.1. Memahami Jenis-Jenis Serangan Kejahatan Dunia Maya

Di era digital, kejahatan dunia maya telah menjadi ancaman yang semakin nyata dan serius bagi individu dan organisasi.

Serangan kejahatan dunia maya dapat berdampak signifikan terhadap keamanan dan privasi data, keandalan, dan stabilitas sistem secara keseluruhan (Azzahra, Furnamasari, dan Dewi 2021).

Oleh karena itu, penting untuk memahami jenis serangan

P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i1

kejahatan dunia maya () yang paling umum agar dapat mengambil tindakan pencegahan yang efektif.

Salah satu jenis serangan kejahatan dunia maya yang paling umum adalah serangan phishing (Taufik Ramadhan 2023). Serangan ini menipu korbannya agar mengungkapkan informasi pribadi atau rahasia, seperti kata sandi atau nomor kartu kredit, melalui situs web palsu atau email palsu. Pelaku serangan phishing ini seringkali menggunakan teknik rekayasa sosial yang canggih untuk menyamarkan keaslian website dan email sehingga korban dapat membedakan website palsu dan asli (Edy Haryanto 2016), (Laksana & Mulyani, 2024)

4.2. Pencegahan terhadap kejahatan siber dalam universitas

Kejahatan dunia maya yang umum mencakup pencurian identitas, penindasan, penipuan online, perampokan, dan banyak lagi. Sejauh ini, banyak pengguna yang menyatakan identitasnya di media sosial, bahkan banyak pula yang memposting tentang tempat-tempat yang pernah mereka kunjungi.

Dan banyak pelajar yang ingin menggunakan Wi-Fi gratis. Jika pengguna waspada dan berhati-hati, kejahatan dunia maya tidak akan terjadi. Mahasiswa perlu mewaspadai dampak negatif dunia maya. Untuk itu perlu dilakukan analisis popularitas pengguna media sosial. (Soni et al., 2019)

Memahami mekanisme, teknik, dan pelaku kejahatan dunia maya merupakan langkah awal yang penting dalam mengembangkan strategi untuk memerangi kejahatan dunia maya dan bisa menggunakan honeypot sebagai contoh untuk menghindari serangan siber.

4.3. Penggunaan IDS dalam memonitoring sistem jaringan di universitas

Keamanan komputer adalah perlindungan sistem komputer dari ancaman yang ditimbulkan oleh akses jaringan yang menyimpang dari prosedur keamanan. Seperti halnya komputer apa pun yang terhubung ke jaringan Internet, komputer ini sangat rentan terhadap pencurian data oleh pihak yang tidak bertanggungjawab. untuk mengembangkan suatu sistem yang dapat mendeteksi lalu lintas jaringan dan objek mencurigakan dalam suatu sistem jaringan. (Sangadji et al., 2023)

5. KESIMPULAN

Upaya agar tidak terkena serangan siber dalam sistem keamanan universitas Banyak cara untuk mencegah terjadinya serangan siber pada sistem di universitas, sebagai contoh salah satu caranya dengan menggunakan honeypot yang dirancang menyerupai sistem atau layanan yang berguna untuk mengelabui hacker bisa menyusup ke sistem jaringan universitas dan untuk memonitoring jaringan bisa menggunakan IDS. Namun masih banyak mahasiswa yang kurang kesadaran terhadap kejahatan siber dan cara menggunakan layanan honeypot tersebut,serta menganggap remeh/kecil resiko yang diterima.

P-ISSN: 1411-3635
E-ISSN: 2962-5645

DAFTAR PUSTAKA

321-Article Text-805-2-10-20220319. (n.d.).

Bukit, A. N., & Rahmi Ayunda. (2022). Urgensi Pengesahan RUU Perlindungan Data Pribadi Terhadap Perlindungan Kebocoran Data Penerimaan SMS Dana Cepat. *Reformasi Hukum*, *26*(1), 1–20. https://doi.org/10.46257/jrh.v26i1.376

Ekowati, S. P., Malays Sari Sakti, E., Valiant, V., & Gassing, S. S. (n.d.). *Pengenalan Komunikasi Digital Untuk Meningkatkan Minat Belajar Siswa*. https://doi.org/10.37817/10.37817/mediaabdimas.v3i2

Gondohanindijo, J. (2011). Sistem Untuk Mendeteksi Adanya Penyusup (IDS : Intrusion Detection System). *Semarang*, *2*.

https://course-net.com/blog/5-tren-cyber-security-yang-perlu-diketahui-di-tahun-2023/. (n.d.). *5-tren-cyber-security*.

https://edukasiteki.blogspot.com/2018/01/cara-kerja-sistem-pendeteksi-dan.html. (n.d.). *https://edukasiteki.blogspot.com/2018/01/cara-kerja-sistem-pendeteksi-dan.html*.

https://nordvpn.com/id/blog/serangan-siber/. (n.d.). *https://nordvpn.com/id/blog/serangan-siber/*.

Imam, R. M., Sukarno, P., & Nugroho, M. A. (n.d.). *Deteksi Anomali Jaringan Menggunakan Hybrid Algorithm*.

Indra Prasetya, N., Djanali, S., & Husni, M. (2014). VERIFIKASI SIGNATURE PADA KOLABORASI SISTEM DETEKSI INTRUSI JARINGAN TERSEBAR DENGAN HONEYPOT. In *JUTI: Jurnal Ilmiah Teknologi Informasi* (Vol. 12, Issue 2).

Iqbal, M., Rohmat Saedudin, Rd., & Fathinuddin, M. (2022). ANALISIS PERBANDINGAN AKURASI K-NEAREST NEIGHBOR DAN NAÏVE BAYES UNTUK KLASIFIKASI DATA SERANGAN JARINGAN KOMPUTER. *EDUSAINTEK: Jurnal Pendidikan, Sains Dan Teknologi*, *9*(3), 920–929. https://doi.org/10.47668/edusaintek.v9i3.611

Laksana, T. G., & Mulyani, S. (2024). PENGETAHUAN DASAR IDENTIFIKASI DINI DETEKSI SERANGAN KEJAHATAN SIBER UNTUK MENCEGAH PEMBOBOLAN DATA PERUSAHAAN. *Jurnal Ilmiah Multidisiplin*, *3*(01). https://doi.org/10.56127/jukim.v3i01.1143

Nasruji, N. (2019). MANAJEMEN PENDIDIKAN (Studi Kasus Sekolah Menengah Atas Islam Terpadu Ulil Albab di Batam). *HISTORIA: Jurnal Program Studi Pendidikan Sejarah*, *2*(2). https://doi.org/10.33373/j-his.v2i2.1670

Purwani, M. S. F. (2023). Analisis Peran dan Penanggulangan Kejahatan Siber: Studi Kasus Spearphishing. *Restorative : Journal of Indonesian Probation and Parole System*, *1*(1). https://doi.org/10.61682/restorative.v1i1.5

Purwoko, R., Priambodo, D. F., Permana, G. A., Saptomo, W. L. Y., Siswanti, S., & Hasbi, M. (2023). Honeypot-as-a-Service dengan Kubernetes Cluster. *Jurnal Edukasi Dan*

Penelitian Informatika (JEPIN), *9*(2). https://doi.org/10.26418/jp.v9i2.62076

Sangadji, V. I., Muhammad, A. H., & Gunawan, E. (2023). Penerapan Metode Signature Base Berbasis IDS Snort dan IDS Suricata Pada Keamaan Jaringan Laboratorium Komputer. *Jurnal Teknik Informatika (J-Tifa)*, *6*(1). https://doi.org/10.52046/j-tifa.v6i2.1678

Soni, S., Afdhil Hafid, & Didik Sudyana. (2019). ANALISIS KESADARAN MAHASISWA UMRI TERKAIT PENGGUNAAN TEKNOLOGI & MEDIA SOSIAL TERHADAP BAHAYA CYBERCRIME. *JURNAL FASILKOM*, *9*(3). https://doi.org/10.37859/jf.v9i3.1664

Widodo, T., & Sekti Aji, A. (2022). Pemanfaatan Network Forensic Investigation Framework untuk Mengidentifikasi Serangan Jaringan Melalui Intrusion Detection System (IDS). In *Jurnal Informatika Sunan Kalijaga)* (Vol. 7, Issue 1).