Jurnal Transformasi Pendidikan Berkelanjutan
https://ejurnals.com/ojs/index.php/jtpb
Vol. 7, No. 2
Mei 2026

ANALISIS SERANGAN MALWARE DENGAN MENGGUNAKAN SNORT DAN HONEYPOT

Fridolin Marsianus Milo Ragha[1]
[1]Stikom Uyelindo Kupang NTT
fridolinmilo@gmail.com

ABSTRAK

Perkembangan pesat teknologi informasi kini membawa risiko serangan malware yang semakin rumit, mengancam kestabilan dan keamanan jaringan secara keseluruhan. Untuk mengatasi hal ini, dibutuhkan sistem deteksi yang presisi dalam mengenali pola aktivitas mencurigakan. Penelitian kami mengkaji ciri-ciri serangan malware melalui penggabungan Snort sebagai Intrusion Detection System (IDS) dengan honeypot sebagai perangkap bagi perilaku penyerang.Penelitian ini dilaksanakan dengan menyusun lingkungan virtual yang mencakup mesin penyerang, honeypot, serta IDS berbasis Snort. Honeypot difungsikan untuk menampung arus lalu lintas serangan, sementara Snort memeriksa paket-paket jaringan menggunakan tanda (signature) yang sesuai. Data yang diperoleh kemudian diurai untuk mengungkap pola serangan, jenis ancaman jahat, dan tingkat keberhasilan deteksi Snort diukur melalui indikator seperti latensi (delay), kehilangan paket (packet loss), throughput, serta notifikasi signature dari log Snort dan rekaman Wireshark.Hasil analisis diharapkan dapat mengonfirmasi bahwa perpaduan honeypot dan Snort dapat menghasilkan deteksi malware yang lebih unggul. Honeypot efektif menjerat upaya seperti pemindaian (scanning) dan serangan kecerobohan (brute force), sedangkan Snort memunculkan peringatan atas signature terkait malware. Temuan ini memperkuat argumen bahwa penerapan kedua alat secara terintegrasi tidak hanya menyempurnakan ketepatan analisis, tetapi juga memperkokoh pertahanan jaringan.

Kata Kunci: *Honeypot, IDS, Malware, Snort,* Keamanan Jaringan.

ABSTRACT

The rapid development of information technology now brings the risk of increasingly complex malware attacks, threatening the stability and security of the overall network. To overcome this, a precise detection system is needed to recognize suspicious activity patterns. Our research examines the characteristics of malware attacks by combining Snort as an Intrusion Detection System (IDS) with a honeypot as a trap for attacker behavior. This research was carried out by constructing a virtual environment that includes an attacker's machine, a honeypot, and a Snort-based IDS. The honeypot functions to accommodate the flow of attack traffic, while Snort examines network packets using appropriate signatures. The obtained data is then parsed to reveal attack patterns, types of malicious threats, and the success rate of Snort detection measured through indicators such as latency (delay), packet loss (packet loss), throughput, and signature

notifications from Snort logs and Wireshark recordings. The results of the analysis are expected to confirm that the combination of honeypot and Snort can produce superior malware detection. The honeypot is effective in trapping attempts such as scanning and brute-force attacks, while Snort generates alerts on malware-related signatures. These findings strengthen the argument that implementing both tools in an integrated manner not only improves analytical accuracy but also strengthens network defenses.

Keywords: *Social Emotional Learning, Students Empathy, Social Emotional Learning.*

A. PENDAHULUAN

Perkembangan teknologi jaringan komputer saat ini berkembang sangat pesat dan diikuti dengan meningkatnya ancaman keamanan siber. Serangan terhadap sistem jaringan dapat menyebabkan kerusakan data, pencurian informasi, hingga gangguan layanan jaringan. Salah satu jenis serangan yang sering terjadi adalah *brute force attack* pada layanan *Secure Shell* (SSH). Serangan *brute force* dilakukan dengan mencoba berbagai kombinasi *username* dan *password* secara otomatis hingga berhasil memperoleh akses ke sistem target.

Ancaman serangan *brute force* SSH menjadi perhatian penting karena layanan SSH banyak digunakan sebagai media *remote access server* pada lingkungan jaringan komputer. Apabila sistem keamanan jaringan tidak mampu mendeteksi aktivitas serangan secara cepat, maka penyerang dapat memperoleh akses ilegal terhadap sistem. Oleh karena itu diperlukan mekanisme keamanan jaringan yang mampu mendeteksi aktivitas serangan secara *real-time.*

Intrusion Detection System (IDS) merupakan sistem keamanan jaringan yang digunakan untuk mendeteksi aktivitas mencurigakan pada jaringan komputer. Salah satu IDS *open source* yang banyak digunakan adalah *Snort. Snort* mampu melakukan monitoring lalu lintas jaringan dan memberikan *alert* ketika ditemukan aktivitas yang sesuai dengan *rule* deteksi.

Selain IDS, teknologi *Honeypot* juga dapat digunakan untuk membantu mendeteksi dan menganalisis aktivitas penyerang. *Honeypot* merupakan sistem jebakan yang dirancang menyerupai layanan asli sehingga dapat menarik perhatian *attacker*. Pada penelitian ini digunakan *Honeypot Cowrie* yang mampu mensimulasikan layanan SSH serta merekam aktivitas *login attacker* secara detail.

Penelitian ini menggabungkan *Snort* dan *Honeypot Cowrie* pada lingkungan virtual untuk menganalisis kemampuan sistem dalam mendeteksi serangan *brute force* SSH menggunakan *tools Hydra.* Dengan adanya penelitian ini diharapkan sistem keamanan yang dibangun dapat membantu administrator jaringan dalam melakukan monitoring dan analisis serangan pada jaringan komputer.

Rumusan Masalah

Berdasarkan latar belakang diatas maka rumusan masalah dalam penelitian ini adalah:

1. Bagaimana implementasi Snort dan Honeypot Cowrie pada lingkungan virtual?
2. Bagaimana kemampuan Snort dalam mendeteksi serangan brute force SSH?
3. Bagaimana Honeypot Cowrie merekam aktivitas penyerang pada layanan SSH?

Tujuan Penelitian

Adapun tujuan penelitian adalah sebagai berikut:

1. Membangun sistem keamanan jaringan menggunakan *Snort* dan *Honeypot cowrie*
2. Menganalisis kemampuan *Snort* dalam mendeteksi serangan *brute force SSH.*
3. Mengidentifikasi aktivitas penyerang berdasarkan *log Honeypot Cowrie.*

Manfaat Penelitian

1. Manfaat bagi kampus Menambah referensi penelitian mengenai keamanan jaringan berbasis IDS dan *Honeypot.*
2. Manfaat bagi mahasiswa Menambah pengetahuan mengenai implementasi *Snort* dan *Honeypot Cowrie* pada lingkungan virtual.
3. Manfaat bagi administrator jaringan Membantu administrator jaringan dalam melakukan monitoring dan deteksi serangan *brute force SSH*.

Ruang Lingkup Penelitian

1. Penelitian menggunakan *Snort* sebagai *Intrusion Detection System.*
2. *Honeypot* yang digunakan adalah *Cowrie.*
3. Serangan yang diuji adalah *brute force SSH* menggunakan *Hydra.*
4. Penelitian dilakukan pada lingkungan virtual menggunakan *VirtualBox*

B. METODE PENELITIAN

1) Prosedur Penelitian

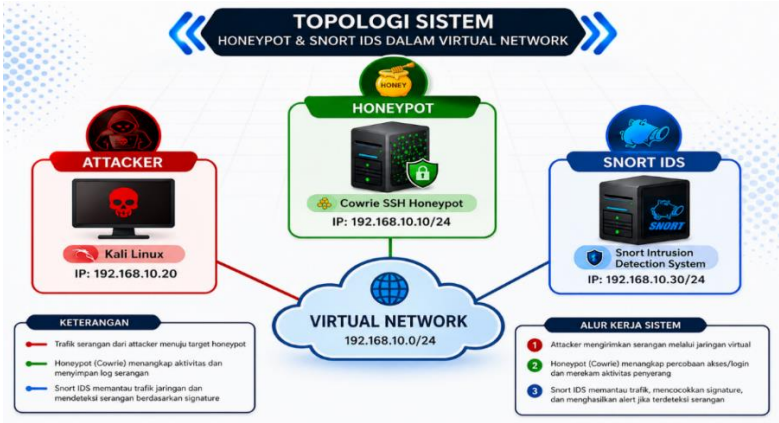
Penelitian dilakukan melalui beberapa tahapan mulai dari pengumpulan informasi, perancangan sistem, implementasi, pengujian sistem, hingga analisis hasil penelitian.

1. Pengumpulan Data Tahap ini dilakukan melalui studi literatur, observasi, dan pengumpulan referensi terkait IDS, *Honeypot, Snort, Cowrie*, dan *brute force SSH.*
2. Pengumpulan Alat dan Bahan Peneliti menyiapkan perangkat keras dan perangkat lunak yang digunakan dalam penelitian seperti *VirtualBox, Snort, Cowrie, Hydra,* dan *TShark.*
3. Perancangan Sistem Tahap ini meliputi perancangan topologi jaringan virtual dan konfigurasi sistem keamanan jaringan.
4. Implementasi Sistem Semua *tools* diinstal dan dikonfigurasi sesuai kebutuhan penelitian.
5. Pengujian Sistem Pengujian dilakukan dengan melakukan simulasi *brute force SSH* menggunakan *Hydra.*
6. Analisis Hasil Data hasil pengujian dianalisis berdasarkan *alert Snort* dan *log Cowrie.*
7. Penyusunan Laporan Seluruh hasil penelitian disusun dalam bentuk jurnal penelitian.

2) Perancangan Sistem

Pada penelitian ini sistem dibangun menggunakan lingkungan virtual yang terdiri dari mesin *attacker,* server *Honeypot Cowrie*, dan *Snort IDS.* Mesin *attacker* digunakan untuk melakukan simulasi *brute force* SSH menggunakan *Hydra. Snort* digunakan untuk memonitor lalu lintas jaringan dan mendeteksi aktivitas serangan. Sedangkan *Honeypot Cowrie* digunakan untuk merekam aktivitas *attacker.*

3) Diagram Blok



Dari topologi tersebut dapat dijelaskan bahwa attacker melakukan serangan *brute force* SSH menuju server *Honeypot Cowrie.* Seluruh lalu lintas jaringan dimonitor oleh *Snort IDS* untuk mendeteksi aktivitas mencurigakan dan menghasilkan *alert* ketika ditemukan serangan.

4) Tools Penelitian

No	***Software***	**Versi**	**Fungsi**
1	*Snort*	2.9.x	*Intrusion Detection*
2	*Cowrie*	Latest	*Honeypot*
3	*VirtualBox*	7.x	Virtualisasi
4	*Hydra Brute force attacking*	7.x	*Tools* Simulasi serangan
5	*Wireshark/Tshark*		Perhitungan tcp

5) Teknik Pengumpulan Data

Data penelitian diperoleh dari:

1. *Log Snort*
2. *Log Honeypot Cowrie*
3. Hasil monitoring trafik jaringan
4. *Screenshot* hasil pengujian

6) Teknik Analisis Data

Analisis dilakukan menggunakan parameter:

1) *Detection Rate*
2) *False Positive Rate*
3) *Attack Success Rate*
4) *Delay* jaringan

C. HASIL DAN PEMBAHASAN

Hasil

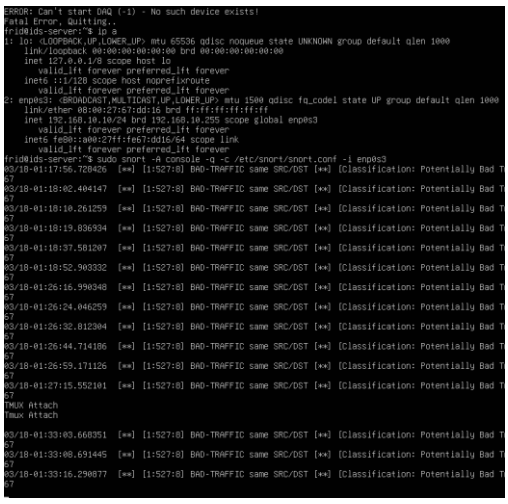
1. Implementasi Sistem

Implementasi sistem keamanan jaringan dilakukan dengan mengintegrasikan *Snort* dan *Honeypot Cowrie* pada lingkungan virtual. Sistem dibangun menggunakan beberapa virtual *machine* yang saling terhubung dalam satu jaringan virtual.

Pada implementasi ini *Snort* digunakan sebagai *Intrusion Detection System* yang berfungsi memonitor seluruh lalu lintas jaringan secara *real-time. Snort* dikonfigurasi menggunakan *rule* untuk mendeteksi aktivitas *brute force SSH.*

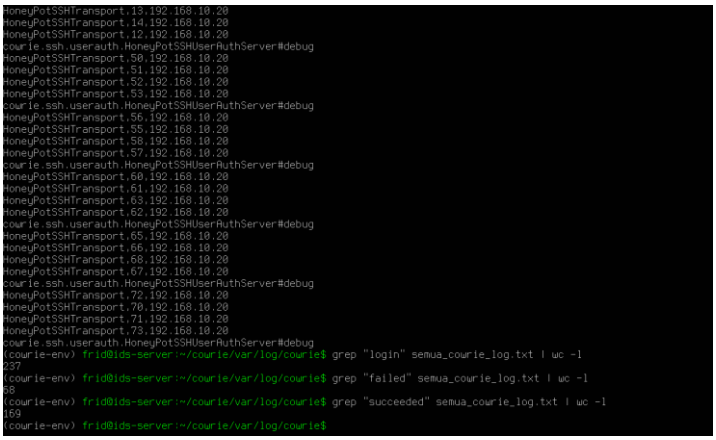
Sedangkan *Honeypot Cowrie* digunakan untuk mensimulasikan layanan SSH palsu sehingga attacker akan menganggap layanan tersebut sebagai server asli. Cowrie akan merekam seluruh aktivitas *login attacker* seperti *username, password, IP address,* dan *command* yang dijalankan.

2. Implementasi Snort



Gambar diatas menunjukkan bahwa Snort berhasil berjalan dalam mode IDS dan mampumelakukan monitoring lalu lintas jaringan secara *real-time.*

3. Implementasi Honeypot Cowrie



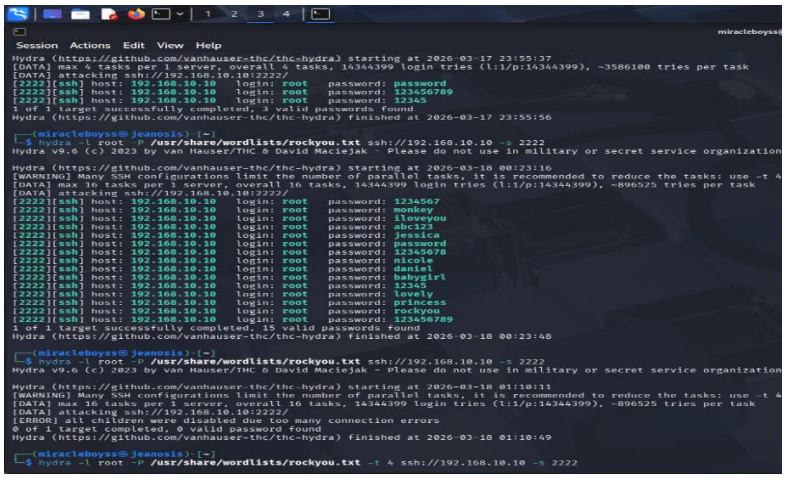
Gambar diatas menunjukkan aktivitas login attacker yang berhasil direkam oleh *Honeypot Cowrie*.

4. Pengujian Sistem

Pengujian sistem dilakukan untuk mengetahui kemampuan *Snort* dan *Honeypot Cowrie* dalam mendeteksi serangan *brute force SSH.*

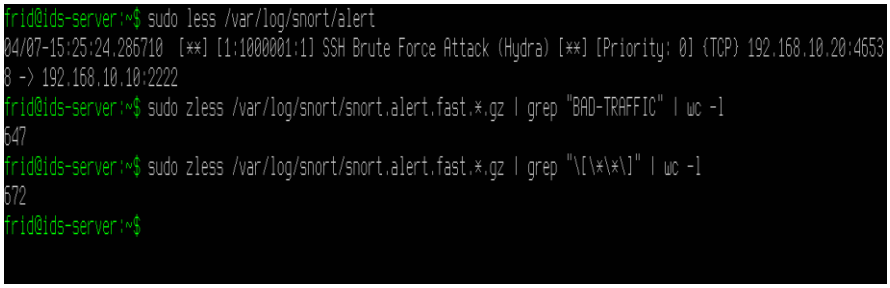
5. Simulasi Serangan *Hydra*

Pengujian dilakukan menggunakan Hydra untuk melakukan brute force SSH menuju *Honeypot Cowrie* pada port 2222. *Proses brute force* dilakukan menggunakan *wordlist username* dan *password.*



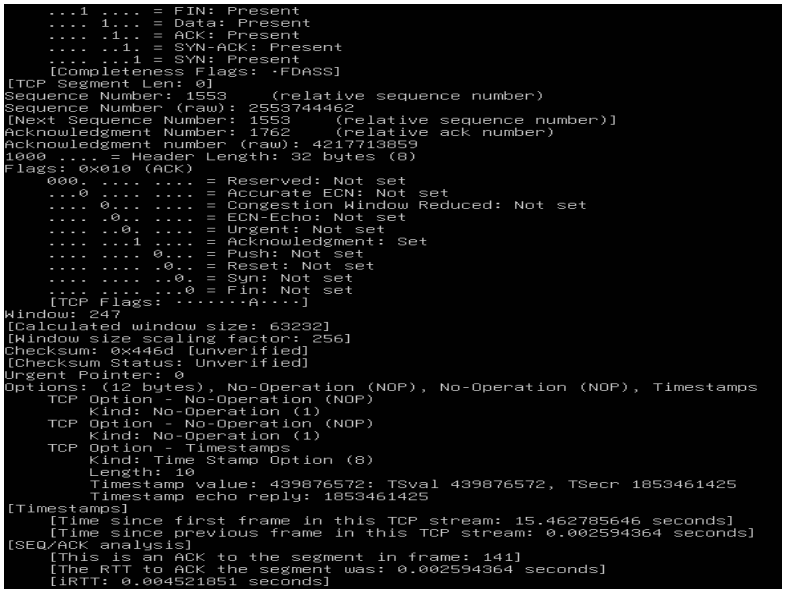
6. Deteksi Seangan Oleh *Snort*

Ketika serangan dilakukan, *Snort* berhasil mendeteksi aktivitas *brute force SSH* dan menghasilkan *alert* sesuai *rule* yang digunakan.



7. Monitoring Trafik Jaringan

Monitoring jaringan dilakukan dengan menggunakan *TShark* untuk menangkap lalu lintas data secara *real-time*. Hasil pengamatan menunjukkan adanya peningkatan jumlah paket TCP menuju port 2222 pada IP target 192.168.10.10. Paket yang terdeteksi didominasi oleh proses inisialisasi koneksi (SYN) dan balasan (ACK), yang menunjukkan adanya aktivitas *brute force*. Selain itu, interval waktu antar paket sangat cepat, menandakan serangan dilakukan secara otomatis menggunakan *tools Hydra*. Hal ini mengindikasikan adanya anomali trafik jaringan yang berhasil dimonitor oleh *TShark.*



Data hasil monitoring *TShark* dikorelasikan dengan log *honeypot Cowrie* dan *alert* dari *Snort*.

Pola Trafik Jaringan

Hasil analisis paket menunjukkan bahwa trafik didominasi oleh:

- Paket SYN (permintaan koneksi awal)
- Paket ACK (respon koneksi)
- Paket data (*payload login*)

Pola ini menunjukkan adanya proses komunikasi TCP yang berulang dalam waktu singkat, yang merupakan karakteristik utama dari serangan *brute force.*

Selain itu, interval waktu antar paket yang sangat cepat menunjukkan bahwa serangan dilakukan secara otomatis tanpa jeda signifikan.

8. Analisis Hasil Pengujian

Integrasi antara *Snort* dan *Cowrie* memungkinkan sistem mendeteksi serta merekam aktivitas serangan *brute force* SSH secara lebih efektif. *Snort* berfungsi mendeteksi pola lalu lintas mencurigakan berdasarkan *rule* IDS, sedangkan *Cowrie* merekam interaksi penyerang setelah koneksi berhasil dilakukan pada layanan SSH palsu. Kombinasi kedua sistem ini meningkatkan kemampuan monitoring keamanan jaringan dalam lingkungan virtual.

Parameter	Nilai
Jenis Serangan	SSH *Brute Force*
Bad Traffic	647
Alert Snort	672
True Positive	237
False Negative	0
Delay	0.0025 detik

9. Analisis *Detection Rate* IDS (*Snort)*

a. *Detection Rate*

$$Detection\ rate = \frac{TP}{TP+FN} \quad (14)$$

$$= \frac{237}{237+0} = (100\%)$$

Total alert yang dihasilkan *Snort* mencapai 672 alert, yang terdiri atas berbagai aktivitas jaringan dalam kategori *BAD-TRAFFIC*. Dari keseluruhan *alert* tersebut, sebanyak 237 *alert* dikategorikan sebagai *true positive* karena sesuai dengan pola serangan *brute force* SSH yang dilakukan menggunakan Hydra.

10. Honeypot Cowrie

Honeypot Cowrie berhasil merekam aktivitas *attacker* seperti alamat *IP, username, password*, dan waktu serangan. Informasi tersebut dapat digunakan administrator jaringan untuk melakukan analisis pola serangan.

Pembahasan

Hasil penelitian menunjukkan bahwa integrasi *Snort* dan *Honeypot Cowrie* mampu meningkatkan kemampuan monitoring keamanan jaringan pada lingkungan virtual. *Snort* berfungsi mendeteksi aktivitas serangan secara *real-time* sedangkan *Cowrie* merekam aktivitas *attacker* secara detail. Kombinasi kedua sistem ini dapat membantu administrator jaringan dalam melakukan identifikasi dan analisis serangan *brute force* SSH.

KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan hasil penelitian mengenai implementasi sistem deteksi serangan *malware* dengan menggunakan *Snort* dan *honeypot* pada lingkungan virtual, diperoleh kesimpulan, Sistem deteksi serangan yang dibangun dengan mengintegrasikan *Snort* sebagai *Intrusion Detection System* (IDS) dan *honeypot (Cowrie)* telah berhasil diimplementasikan dan dapat berjalan dengan baik pada lingkungan virtual. *Snort* mampu mendeteksi aktivitas serangan secara *real-time* dengan tingkat *detection rate* sebesar 100%, sedangkan *honeypot* mampu merekam aktivitas penyerang secara detail, baik percobaan *login* berhasil maupun gagal, sehingga mendukung proses analisis keamanan jaringan. Hasil analisis menunjukkan bahwa serangan yang terjadi merupakan serangan *brute force* yang dilakukan secara otomatis, dengan tingkat keberhasilan serangan sebesar 71,31% dan frekuensi serangan sebesar 7,41 serangan per detik.

Saran

Berdasarkan hasil penelitian yang telah dilakukan, terdapat beberapa saran untuk pengembangan sistem ke depan sebagai berikut:

1. Perlu dilakukan pembaruan (*update*) *rule* pada *Snort* secara berkala agar sistem mampu mendeteksi jenis serangan terbaru, termasuk serangan *zero-day*.
2. Sistem dapat dikembangkan lebih lanjut dengan menambahkan mekanisme pencegahan seperti *Intrusion Prevention System* (IPS),dengan menambahkan *Artificial Inteligent* (AI) sehingga pendeteksian dan pencegahan dapat dilakukan secara optimal.
3. Mengembangkan aplikasi untuk proses keamanan jaringan yang dapat dipantau menggunakan aplikasi *mobile.*
4. Penelitian selanjutnya dapat dilakukan pada lingkungan jaringan yang lebih luas atau pada kondisi jaringan nyata (*real network*) untuk memperoleh hasil yang lebih representatif.

DAFTAR PUSTAKA

Aminanto, A., Sulistyo, W. 2023. Simulasi sistem keamanan jaringan komputer berbasis IPS Snort dan honeypot Artillery. *Aiti: Jurnal Teknologi Informasi*,

20(1), 110. [internet]. [diakses 25 November 2025].Tersedia pada:https://ejournal.uksw.edu/aiti/article/view/3628

Badan Siber dan Sandi Negara (BSSN). 2024. *Laporan tahunan ancaman siber Indonesia*. [internet]. [diakses 25 November 2025].Tersedia pada: https://bssn.go.id

Behl, A., Behl, K. 2021. *Cyberwar and information warfare*. Oxford University Press.[internet]. [diakses 25 November 2025].Tersedia pada:https://scholar.google.com/scholar?q=Cyberwar+and+information+warfare+Behl

Bejtlich, R. 2020. *Network security monitoring: An analyst's handbook*. NSM Press.[internet]. [diakses 25 November 2025].Tersedia pada:https://scholar.google.com/scholar?q=Network+Security+Monitoring+Bejtlich

Creswell, J. W., Creswell, J. D. 2023. *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage Publications.
[internet]. [diakses 25 November 2025].Tersedia pada:https://scholar.google.com/scholar?q=Research+Design+Creswell

Easttom, C. 2022. *Computer security fundamentals*. Pearson Education.
[internet]. [diakses 25 November 2025].Tersedia pada:https://scholar.google.com/scholar?q=Computer+Security+Fundamentals+Easttom

ENISA. 2023. *ENISA threat landscape 2023*.
[internet]. [diakses 25 November 2025].Tersedia pada:https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Ernawati, T., Rachmat, F. F. 2025. Network security with Cowrie honeypot and Snort inline-mode as intrusion prevention system. *Jurnal RESTI*, 5(1), 62–70. [internet].[diakses 25 November 2025].Tersedia pada:https://doi.org/10.29207/resti.v5i1.2825

Gunawan, A. R., Sastra, N. P., Wiharta, D. M. 2021. Penerapan keamanan jaringan menggunakan sistem Snort dan honeypot sebagai pendeteksi dan pencegah malware. *Jurnal MITE*, 15(1), 1–10. [internet].[diakses 25 November 2025].Tersedia pada:https://ojs.unud.ac.id/index.php/mite/article/view/69655

Kurniawan, I., Sari, D. 2024. Analisis signature Snort untuk deteksi malware berbasis jaringan. *Jurnal Teknologi Keamanan*, 5(1), 77–86.

[internet]. [diakses 25 November 2025].Tersedia pada:https://doi.org/10.1234/jtk.v5i1.567

Mousa, M., Al-Hadhrami, T., Yousif, M. 2021. Enhanced Snort IDS using honeypot-captured traffic. *IEEE Access*, 9, 411–420.
[internet]. [diakses 25 November 2025].Tersedia pada:https://doi.org/10.1109/ACCESS.2021.3056789

National Institute of Standards and Technology (NIST). 2022. *Guide to intrusion detection and prevention systems (SP 800-94)*.
[internet]. [diakses 25 November 2025].Tersedia pada:https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

Panggabean, R., Hutagalung, M., Situmorang, A. 2024. Analisis lingkungan virtual untuk pengujian keamanan jaringan. *Jurnal Keamanan Siber*, 6(1), 45–55.
[internet]. [diakses 25 November 2025].Tersedia pada:https://scholar.google.com/scholar?q=Analisis+lingkungan+virtual+keamanan+jaringan

Prasetya, A., Nugroho, Y., Santoso, B. 2014. Analisis dan implementasi rule Snort untuk deteksi serangan jaringan. *Jurnal Informatika*, 8(2), 101–110. [internet]. [diakses 25 November 2025].Tersedia pada:https://scholar.google.com/scholar?q=Analisis+implementasi+rule+Snort

Pratama, R., Susanto, D., Raharjo, B. 2021. Implementasi honeypot low-interaction untuk monitoring aktivitas penyerang. *Jurnal Siber Indonesia*, 3(2), 90–98. [internet]. [diakses 25 November 2025].Tersedia pada:https://scholar.google.com/scholar?q=Implementasi+honeypot+low+interaction

Provos, N., Holz, T. 2020. *Virtual honeypots: From botnet tracking to intrusion research*. Addison-Wesley.
[internet]. [diakses 25 November 2025].Tersedia pada:https://scholar.google.com/scholar?q=Virtual+Honeypots+Provos

Ramadhan, A., Suryani, D. 2023. Simulasi serangan malware menggunakan honeypot virtual. *Jurnal Rekayasa Komputer*, 7(2), 144–155.
[internet]. [diakses 25 November 2025].Tersedia pada:https://scholar.google.com/scholar?q=Simulasi+serangan+malware+honeypot

Sanders, C. 2022. *Practical packet analysis*. No Starch Press.

[internet]. [diakses 25 November 2025].Tersedia pada:https://scholar.google.com/scholar?q=Practical+Packet+Analysis+Sanders

Scarfone, K., Mell, P. 2020. *Guide to intrusion detection and prevention systems (IDPS)*. NIST.

[internet]. [diakses 25 November 2025].Tersedia pada:https://csrc.nist.gov/publications/detail/sp/800-94/final

Singh, A., Kumar, V., Patel, R. 2021. Hybrid intrusion detection with honeypot-assisted Snort framework. *Journal of Information Security Applications*, 18(4), 221–230.

[internet]. [diakses 25 November 2025].Tersedia pada:https://doi.org/10.1016/j.jisa.2021.103012

Stallings, W. 2020. *Network security essentials*. Pearson Education.

[internet]. [diakses 25 November 2025].Tersedia pada:https://scholar.google.com/scholar?q=Network+Security+Essentials+Stallings

Verizon. 2023. *Data breach investigations report*.

[internet]. [diakses 25 November 2025].Tersedia pada:https://www.verizon.com/business/resources/reports/dbir

VMware. 2022. *Virtualization and security best practices*.

[internet]. [diakses 25 November 2025].Tersedia pada:https://www.vmware.com/security

Wongkar, S. 2020. Implementasi honeypot medium interaction pada keamanan server SSH. *Jurnal Sistem Informasi*, 7(1), 12–20.

[internet]. [diakses 25 November 2025].Tersedia pada:https://ejournal.unsrat.ac.id/index.php/informatika/article/view/30919

Zeltser, L. 2023. *Malware behavior analysis*. Cyber Institute Press.

[internet]. [diakses 25 November 2025].Tersedia pada:https://scholar.google.com/scholar?q=Malware+Behavior+Analysis+Zeltser

Zhang, Y., Yao, J. 2020. Snort-enhanced honeypot architecture for profiling attacks. *Computers & Security*, 92, 101734.

[internet]. [diakses 25 November 2025].Tersedia pada:https://doi.org/10.1016/j.cose.2020.101734.