SISTEM DETEKSI SERANGAN OUTSIDER PADA GERAKAN LATERAL SSH MENGGUNAKAN METODE RULE BASED

PROJEK AKHIR

Sebagai salah satu syarat untuk menyelesaikan
Studi di Program Studi Teknik Komputer DIII

Oleh

Zinniarethie Andari Kostiene

09030582226007

PROGRAM STUDI TEKNIK KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

JULI 2025

HALAMAN PENGESAHAN

PROJEK AKHIR

Sistem Deteksi Serangan Outsider pada Gerakan Lateral SSH Menggunakan Metode Rule Based

Sebagai salah satu syarat untuk penyelesaian studi di

Program Studi D3 Teknik Komputer

Oleh:

ZINNIARETHIE ANDARI KOSTIENE
09030582226007

Pembimbing 1	**:**	**Aditya Putra Perdana P., M.T.**
		NIP. 198810202023211018
Pembimbing 2	**:**	**Nurul Afifah, M.Kom.**
		NIP. 199211102023212049

Mengetahui
Koordinator Program Studi Teknik Komputer

Dr. Ir. Ahmad Heryanto, M.T.
198701222015041002

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : **Kamis**

Tanggal : **26 Juni 2025**

Tim Penguji :

1. Ketua : Kemahyanto Exaudi, M.T.
2. Penguji : Ricy Fimando, M.Kom.
3. Pembimbing I : Aditya Putra Perdana P., S.Kom., M.T.
4. Pembimbing II : Nurul Afifah, S.Kom, M.Kom.

Mengetahui
Koordinator Program Studi Teknik Komputer,

Dr. Ir. Ahmad Heryanto., M.T.
NIP 198701222015041002 .

iii

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama	: Zinniarethie Andari Kostiene
NIM	: 0903058226007
Program Studi	: Teknik Komputer
Judul Projek	: Sistem Deteksi Serangan Outsider pada Gerakan Lateral SSH Menggunakan Metode Rule Based.

Hasil Pengecekan IThenticate/Turnitin : 13%

Menyatakan Bahwa Laporan Projek saya merupakan hasil karya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari universitas sriwijaya.

Demikian pernyataan ini saya buat tanpa dalam keadaan sadar dan tanpa paksaan dari siapapun.

Palembang, 30 Juni 2025

Zinniarethie Andari Kostiene
NIM 09030582226007

iv

MOTTO DAN PERSEMBAHAN

Motto:

“Hidup tidak akan berakhir hanya dengan satu kesalahan yang tidak disengaja, jadi tenanglah”

Zinniarethie Andari Kostiene

"Whatever you are, be a good one."

Abraham Lincoln

"I have not failed. I've just found 10,000 ways that won't work."

Thomas A. Edison

Persembahan:

Dengan segala kerendahan hati dan rasa syukur yang mendalam, karya ini kupersembahkan pertama dan terutama kepada **Allah Subhanahu Wa Ta’ala**, Dzat Yang Maha Kuasa, atas segala rahmat, hidayah, dan kekuatan yang diberikan. Kepada **kedua orang tuaku tercinta dan saudara**, yang dengan kasih sayang, doa, dan pengorbanan tiada henti menjadi cahaya dalam setiap langkahku. Untuk **keluarga besarku**, yang selalu memberikan dukungan moril dan semangat tanpa lelah. Juga kepada **dosen-dosenku**, yang telah membimbing, menginspirasi, dan menanamkan ilmu serta nilai kehidupan yang tak ternilai. Kupersembahkan pula kepada **almamater tercinta**, tempatku tumbuh, belajar, dan menempa diri menjadi pribadi yang lebih baik. Dan secara khusus, untuk o**rang-orang terdekat yang tidak bisa disebutkan satu per satu**, terima kasih atas segala bentuk dukungan, semangat, serta kebersamaan yang tulus—hadir kalian menjadi bagian penting dalam perjalananku hingga saat ini.

KATA PENGANTAR

Puji syukur kehadirat Allah Subhanahu wa Ta'ala atas limpahan rahmat, karunia, dan hidayah-Nya, penulis dapat menyelesaikan projek akhir dengan lancar dan tepat waktu. Projek akhir ini disusun sebagai bentuk memenuhi salah satu syarat untuk mengambil mata kuliah Projek di Program Studi Teknik Komputer Universitas Sriwijaya. Projek akhir ini berjudul "**Sistem Deteksi Serangan Outsider pada Gerakan Lateral SSH Menggunakan Metode Rule-based**" Dalam kesempatan ini penulis mengucapkan terima kasih kepada pihak yang telah memberikan bantuan serta motivasi sehingga penulis dapat menyelesaikan proses penulisan projek akhir ini, yaitu kepada:

1. Allah SWT, yang telah memberikan kekuatan, kesehatan, dan kemudahan sehingga penulis mampu menyelesaikan setiap tugas yang diemban.
2. Orang tua dan saudara, atas doa, dukungan, serta kasih sayang yang senantiasa mengiringi setiap langkah penulis.
3. Bapak Prof. Dr. Erwin, S.Si., M.Si. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. Ahmad Heryanto., M.T. selaku Koordinator Program Studi Teknik Komputer Universitas Sriwijaya.
5. Bapak Prof. Ir. Deris Stiawan, Ph.D., IPU., ASEAN Eng., yang telah membantu dan memfasilitasi penulis dalam membuat Projek Akhir ini.
6. Bapak Aditya Putra Perdana Prasetyo, S.Kom., M.T. selaku Dosen Pembimbing Akademik dan juga Dosen Pembimbing I dalam pembuatan Projek Akhir ini.
7. Ibu Nurul Afifah, S.Kom., M.Kom. selaku Dosen Pebimbing II penulis dalam pembuatan Projek Akhir ini.
8. Pak Ahmad Fali Oklilas, S.T., M.T. selaku Dosen Pembimbing Akademik.
9. Kak M. Rafie Al Hamas selaku kakak pebimbing dan pengarah penulis dalam pembuatan Proposal Projek ini.
10. Kak Dr. (C). Dendi Renaldo Permana, S.Kom., selaku kakak pebimbing dan pengarah penulis dalam pembuatan Proposal Projek ini.
11. Kak Septiani Kusuma Ningrum, S.Kom., selaku kakak pebimbing dan

pengarah penulis dalam pembuatan Proposal Projek ini.

12. Kak Habib Al Assyari selaku kakak asisten ruangan COMNETS.
13. Seluruh Dosen serta Staff Program Studi Teknik Komputer.
14. Sahabat penulis selama perkuliahan yaitu Sachio, Dinda, Aidil, Faisal, Pio, Desta, Devi, Fahri, Diaz, Tony, dan Habib yang telah menemani dan memberi semangat penulis semasa kuliah.
15. Farhan Ahmad Gusfi selaku penyemangat dan pendukung yang senantiasa setia menemani selama proses Proposal Projek ini.
16. Rekan-rekan Teknik Komputer angkatan 2022, atas kerja sama, dukungan, dan semangat kebersamaan yang telah terjalin selama ini.
17. Sahabat-sahabat SMA penulis yang tergabung dalam grup C.O yaitu Azzahra, Bella, Bulan, Hesti, Jihan, Nadya, Nisa, Pipit, Sasak, dan Tiara.

Penulis menyadari bahwa projek akhir ini masih jauh dari sempurna. Oleh karena itu, kritik dan saran yang membangun sangat penulis harapkan guna penyempurnaan projek akhir ini di masa mendatang. Semoga projek akhir ini dapat memberikan manfaat bagi pembaca dan pihak-pihak yang berkepentingan. Akhir kata, penulis ucapkan terima kasih kepada semua pihak yang telah membantu dalam penyusunan projek akhir ini. Semoga Tuhan Yang Maha Esa selalu memberikan rahmat dan hidayah-Nya kepada kita semua.

Palembang, 30 Juni 2025
Penulis,

Zinniarethie Andari Kostiene
NIM 09030582226007

SISTEM DETEKSI SERANGAN OUTSIDER PADA GERAKAN LATERAL SSH MENGGUNAKAN METODE RULE BASED

Oleh

Zinniarethie Andari Kostiene

09030582226007

ABSTRAK

Perkembangan teknologi jaringan komputer telah membawa dampak positif dalam hal pertukaran data dan komunikasi, namun juga memunculkan risiko serangan siber, salah satunya adalah *lateral movement*. Serangan ini terjadi ketika penyerang berhasil memperoleh akses awal ke suatu sistem dan kemudian berpindah secara horizontal ke sistem lain dalam jaringan internal untuk mendapatkan informasi yang lebih bernilai. Penelitian ini bertujuan untuk mensimulasikan dan mendeteksi serangan *brute force* terhadap layanan SSH sebagai salah satu metode yang dapat digunakan dalam serangan *lateral movement*. Simulasi dilakukan dengan mengarahkan serangan *brute force* ke *port* SSH non-standar (port 2222) menggunakan skrip Python dan *wordlist* sebagai kredensial *login*. Hasil menunjukkan bahwa serangan dari penyerang eksternal berhasil memperoleh akses ke sistem korban, dan aktivitas tersebut dapat dideteksi menggunakan *tools* analisis jaringan seperti Wireshark, Snort, dan NetworkMiner. Ketiganya menunjukkan efektivitas dalam mengidentifikasi pola-pola serangan berdasarkan paket data, *alert rules*, dan artefak jaringan. Selain itu, langkah mitigasi seperti perubahan *port* SSH, penonaktifan metode *login* konvensional, serta penggunaan otentikasi SSH *key* terbukti berhasil mencegah serangan serupa pada pengujian ulang. Dengan demikian, pendekatan *rule-based detection* dan konfigurasi keamanan yang tepat dapat meningkatkan ketahanan sistem terhadap ancaman *lateral movement* berbasis SSH.

Kata kunci: *Lateral Movement*, SSH, *Brute Force*, *Intrusion Detection System*, Snort, Wireshark, NetworkMiner, *Rule-Based Detection.*

OUTSIDER ATTACK DETECTION SYSTEM ON SSH LATERAL MOVEMENT USING RULE-BASED METHOD

By

Zinniarethie Andari Kostiene

09030582226007

ABSTRACT

The advancement of computer network technology has brought significant benefits in data exchange and communication, but it also introduces cybersecurity risks, one of which is *lateral movement*. This type of attack occurs when an attacker gains initial access to a system and then moves laterally across the internal network to obtain more valuable information. This study aims to simulate and detect brute force attacks on the SSH service, which can be exploited in *lateral movement* scenarios. The simulation involves targeting a non-standard SSH port (port 2222) using a Python script and a wordlist to guess login credentials. The results show that an external attacker was able to gain access to the victim's system, and this activity was successfully detected using network analysis tools such as Wireshark, Snort, and NetworkMiner. These tools demonstrated effectiveness in identifying attack patterns through data packets, alert rules, and network artifacts. Additionally, mitigation measures such as changing the SSH port, disabling conventional login methods, and implementing SSH key-based authentication proved effective in preventing similar attacks during repeated testing. Therefore, a rule-based detection approach combined with proper security configurations can significantly enhance a system’s resilience against SSH-based *lateral movement* attacks.

Keywords: Lateral Movement, SSH, Brute Force, Intrusion Detection System, Snort, Wireshark, NetworkMiner, Rule-Based Detection

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

1.1 Latar Belakang

Serangan siber (*Cyber Attack*) merupakan dampak negatif dari perkembangan teknologi jaringan komputer. Perkembangan teknologi jaringan komputer telah membawa kemajuan besar dalam pertukaran data dan komunikasi, namun juga membuka celah bagi pihak-pihak yang tidak bertanggung jawab untuk melakukan tindakan berbahaya melalui jaringan seperti serangan siber. Bentuk dari serangan siber itu bermacam-macam. *Lateral movement* merupakan salah satu bentuk serangan yang berakibat fatal dalam dunia jaringan komputer yang telah berkembang dan semakin maju ini.

Teknik yang diimplementasikan oleh seorang penyerang untuk bebas bergerak di dalam jaringan *internal* setelah mendapatkan akses awal adalah pengertian dari *Lateral movement*. Sebagai contoh, jika pada suatu kantor perusahaan terdapat seorang karyawan yang komputernya telah diserang oleh peretas. Namun, sang karyawan tidak memiliki informasi atau rahasia dalam bentuk data yang diinginkan oleh sang peretas, biasanya sang peretas akan berpindah ke komputer karyawan lain untuk mengakses data dan mendapatkan rahasia atau informasi yang ia inginkan.[1] *Lateral movement* bisa diimplementasikan dengan protokol SSH (*Secure Shell*) karena dapat digunakan pada akses yang jauh dan aman ke dalam sistem. Peretas yang mengimplementasikan *lateral movement via* SSH bisa merupakan *outsider* (penyerang *eksternal*) maupun *insider* (penyerang *internal*).

Pada umumnya, serangan *insider* atau serangan dari orang dalam lebih berbahaya daripada serangan dari orang luar atau biasa disebut dengan *outsider*.[2] Peretas ini telah berhasil menembus sistem jaringan komputer sehingga dapat bebas bergerak di jaringan *internal* sehingga memiliki akses untuk masuk ke sistem lain. Perilaku peretas siber ini sungguh berbahaya sehingga dibutuhkan sebuah sistem pendeteksi yang dapat mengenali pola-pola perilaku maupun gerakan tertentu yang bisa diketahui dari sebuah aturan atau

biasanya disebut dengan metode *rule-based*. Konsep dari metode *rule-based* yang akan digunakan oleh penelitian ini juga terbukti menghasilkan akurasi yang baik di penelitian lain. [3]

Serangan *lateral movement* melalui protokol SSH sangat sulit dideteksi karena aktivitasnya menyerupai aktivitas normal pengguna jaringan. [4] Penyerang yang sudah berhasil mendapatkan akses awal biasanya akan melakukan eksplorasi sistem dan mencari celah lebih lanjut untuk mendapatkan hak akses yang lebih tinggi. Proses ini sering kali dilakukan dengan menggunakan kredensial yang sah, sehingga sistem keamanan tradisional seperti *firewall* atau antivirus tidak mampu mendeteksi adanya anomali. Oleh karena itu, dibutuhkan pendekatan keamanan tambahan yang dapat mengenali pola perilaku pengguna dan mendeteksi aktivitas yang tidak biasa.

Metode rule-based merupakan salah satu pendekatan yang efektif dalam mendeteksi serangan siber, terutama jika aturan yang digunakan disusun berdasarkan pola-pola serangan yang sudah diketahui. Sistem deteksi berbasis *rule* ini bekerja dengan cara mencocokkan lalu lintas jaringan atau *log* aktivitas dengan aturan yang telah ditentukan sebelumnya. Jika ditemukan kecocokan, maka sistem akan memberikan peringatan bahwa kemungkinan besar sedang terjadi aktivitas mencurigakan. Dengan pendekatan ini, aktivitas *lateral movement* yang menggunakan SSH dan dilakukan oleh *outsider* dapat dideteksi lebih awal sebelum mencapai tahap yang lebih merusak.

Penggunaan *rule-based* juga dinilai lebih efisien dalam hal penggunaan sumber daya komputasi dibandingkan dengan metode deteksi berbasis *machine learning* yang membutuhkan pelatihan model dan pengolahan data dalam jumlah besar. Metode ini lebih mudah diterapkan dalam lingkungan jaringan perusahaan berskala kecil hingga menengah. Meskipun begitu, kekuatan metode ini sangat bergantung pada kelengkapan dan keakuratan aturan yang digunakan. Oleh karena itu, pembuatan aturan yang spesifik terhadap serangan *lateral* SSH oleh *outsider* menjadi aspek penting dalam implementasi sistem ini. Namun, sistem NIDS (*Network Intrusion Detection System*) berbasis aturan hanya bisa mendeteksi serangan yang pola atau aturannya sudah diketahui. Hal ini menjadi salah satu keterbatasan penting karena serangan baru yang lebih

canggih sering kali tidak terdeteksi, disebabkan belum adanya aturan yang sesuai untuk mengidentifikasi serangan tersebut. Penyerang pun dapat dengan mudah mencari dan mengeksploitasi celah (*loophole*) agar bisa melewati sistem keamanan yang telah disiapkan tanpa terdeteksi. Oleh karena itu, meskipun metode *rule-based* memiliki keunggulan dalam efisiensi dan implementasi, tetap dibutuhkan pengembangan aturan yang terus diperbarui agar mampu mendeteksi variasi serangan terkini secara akurat.[5]

Implementasi sistem deteksi ini dapat dibangun menggunakan *tool* seperti Snort, yang merupakan platform analisis jaringan *open-source* dan sangat mendukung pendekatan *rule-based*. Snort dapat memantau lalu lintas jaringan secara *real-time* dan menghasilkan log yang bisa dianalisis lebih lanjut untuk mendeteksi pola-pola serangan. Dengan mengonfigurasi Snort menggunakan set aturan tertentu, maka sistem mampu mengenali aktivitas yang menyimpang dari kebiasaan pengguna normal, seperti *login* SSH ke banyak host dalam waktu singkat atau upaya otentikasi berulang dari satu sumber.

Berdasarkan latar belakang yang telah dielaskan diatas, maka penulis mengusulkan projek dengan judul ”**Sistem Deteksi Serangan *Outsider* pada Gerakan Lateral SSH Menggunakan Metode *Rule-based***”. Sebuah penelitian yang yang berisi tentang implementasi dan rancangan dari sebuah sistem deteksi serangan khususnya *outsider* pada gerakan lateral SSH menggunakan metode *rule-based* yang dapat mengenali aktivitas tidak wajar yang mencerminkan upaya penyusupan atau eksploitasi jaringan adalah hasil yang diharapkan dari penelitian ini atau bisa disebut sebagai tujuan akhir dari penelitian ini.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah disusun, berikut beberapa rumusan masalah yang terbentuk, yaitu:

1. Bagaimana cara mendeteksi serangan *outsider* pada gerakan *lateral* SSH dengan metode *rule-based*?
2. Bagaimana melakukan proses mitigasi setelah terjadi serangan *outsider* pada gerakan *lateral* SSH?

1.3 Tujuan

Adapun tujuan dari Projek Tugas Akhir ini yakni:

1. Merancang sistem deteksi berbasis aturan (*rule-based*) untuk mendeteksi serangan *outsider* pada gerakan *lateral* SSH.
2. Menguji sistem deteksi serangan menggunakan data simulasi dalam lingkungan *virtual*.

1.4 Manfaat

Adapun manfaat dari penelitian ini yaitu:

1. Memberikan solusi praktis untuk mendeteksi serangan *lateral movement via* SSH dari penyerang *eksternal* menggunakan metode *rule-based*.
2. Menjadi referensi dan sumber pengetahuan tambahan terkait implementasi sistem deteksi berbasis aturan dalam keamanan jaringan.

1.5 Batasan Masalah

Pengerjaan projek ini dibatasi dalam ruang lingkup, sebagai berikut:

1. Fokus pada deteksi serangan *lateral movement via* SSH yang dilakukan oleh *outsider* (bukan *insider*).
2. Protokol yang diamati hanya SSH (*Secure Shell*).
3. Metode yang digunakan hanya *rule-based detection*.
4. Pengujian dilakukan pada jaringan simulasi atau lingkungan terbatas.

1.6 Metode Penelitian

Metode yang digunakan dalam penelitian ini sebagai berikut:

1.6.1 Studi Literatur

Studi literatur adalah sebuah metode dengan mendapatkan data maupun informasi yang berkaitan dengan topik yang diteliti dari banyak sumber yang dijadikan referensi. *Website*, buku, internet dan jurnal dapat dijadikan sumber-sumber dapat digunakan sebagai referensi dalam pembuatan projek akhir yaitu "**Sistem Deteksi Serangan *Outsider* pada Gerakan Lateral SSH Menggunakan Metode *Rule-based***"

1.6.2 Metode Observasi

Dalam penelitian ini, metode observasi di mana melihat dan mempelajari secara langsung bagaimana cara kerja sebuah sistem yang mendeteksi serangan yang yang menggunakan metode tertentu dilakukan.

1.6.3 Metode Konsultasi

Interaksi dengan dosen dan kakak pembimbing dilakukan dengan cara berdiskusi dan melakukan percakapan tanya jawab atau biasa disebut dengan metode konsultasi dilakukan pada penelitian projek ini. Metode ini dilakukan pada saat penelitian berlangsung maupun pada saat laporan dibuat dan disempurnakan.

1.6.4 Metode Implementasi dan Pengujian

a. Metode Implementasi

Metode implementasi digunakan pada penelitian projek ini, di mana proses penerapan rancangan sistem ke dalam sistem yang dijalankan diimplementasikan. Seperti instalasi dan konfigurasi Nmap pada jaringan simulasi maupun pembuatan *rule-based* berdasarkan serangan SSH *lateral movement.*

b. Metode Pengujian

Memastikan sistem deteksi yang telah diimplementasikan sehingga dapat berfungsi sesuai dengan tujuan merupakan arti dari metode pengujian yang digunakan pada penelitian ini. Salah satu bentuk metode pengujian ini adalah di mana dilakukannya simulasi serangan oleh *outsider* menggunakan *tools*.

DAFTAR PUSTAKA

[1] G. Ho *et al.*, "Hopper: Modeling and detecting lateral movement," *Proceedings of the 30th USENIX Security Symposium*, pp. 3093–3110, 2021.

[2] L. Lyu *et al.*, "Privacy and Robustness in Federated Learning: Attacks and Defenses," *IEEE Trans Neural Netw Learn Syst*, vol. 35, no. 7, pp. 8726–8746, 2024, doi: 10.1109/TNNLS.2022.3216981.

[3] P. Ray and A. Chakrabarti, "A Mixed approach of Deep Learning method and Rule-Based method to improve Aspect Level Sentiment Analysis," *Applied Computing and Informatics*, vol. 18, no. 1–2, pp. 163–178, 2022, doi: 10.1016/j.aci.2019.02.002.

[4] C. Larroche, "Designing a reliable lateral movement detector using a graph foundation model," 2025, [Online]. Available: http://arxiv.org/abs/2504.13527

[5] A. F. Diallo and P. Patras, "Adaptive clustering-based malicious traffic classification at the network edge," *Proceedings - IEEE INFOCOM*, vol. 2021-May, 2021, doi: 10.1109/INFOCOM42981.2021.9488690.

[6] L. Huang and Q. Zhu, "Farsighted Risk Mitigation of Lateral Movement Using Dynamic Cognitive Honeypots," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 12513 LNCS, pp. 125–146, 2020, doi: 10.1007/978-3-030-64793-3_7.

[7] A. Aloseel, S. Al-Rubaye, A. Zolotas, and C. Shaw, "Attack-Detection Architectural Framework Based on Anomalous Patterns of System Performance and Resource Utilization - Part II," *IEEE Access*, vol. 9, pp. 87611–87629, 2021, doi: 10.1109/ACCESS.2021.3088411.

[8] A. Z. Agghey, L. J. Mwinuka, S. M. Pandhare, M. A. Dida, and J. D. Ndibwile, "Detection of username enumeration attack on ssh protocol: Machine learning approach," *Symmetry (Basel)*, vol. 13, no. 11, 2021, doi: 10.3390/sym13112192.

[9] S. K. Wanjau, G. M. Wambugu, and G. N. Kamau, "SSH-Brute Force Attack Detection Model based on Deep Learning," *International Journal of Computer Applications Technology and Research*, vol. 10, no. 01, pp. 42–50, 2021, doi: 10.7753/ijcatr1001.1008.

[10] A. Mailewa and K. Rozendaal, "A Novel Method for Moving Laterally and Discovering Malicious Lateral Movements in Windows Operating Systems: A Case Study," *Advances in Technology*, vol. 2, no. 3, pp. 291–321, 2022, doi: 10.31357/ait.v2i3.5584.

[11] B. A. Powell, "Role-based lateral movement detection with unsupervised learning," *Intelligent Systems with Applications*, vol. 16, 2022, doi: 10.1016/j.iswa.2022.200106.

[12] D. Kushwaha *et al.*, "Lateral Movement Detection Using User Behavioral Analysis," no. Lm, pp. 1–16, 2022, [Online]. Available: http://arxiv.org/abs/2208.13524

[13] N. S. K. Bashah, T. S. Simbas, N. Janom, and S. R. S. Aris, "Proactive DDoS attack detection in software-defined networks with Snort rule-based

algorithms," *International Journal of Advanced Technology and Engineering Exploration*, vol. 10, no. 105, pp. 962–989, 2023, doi: 10.19101/IJATEE.2023.10101411.

[14] N. Alsharabi, M. Alqunun, and B. A. H. Murshed, "Detecting Unusual Activities in Local Network Using Snort and Wireshark Tools," *Journal of Advances in Information Technology*, vol. 14, no. 4, pp. 616–624, 2023, doi: 10.12720/jait.14.4.616-624.

[15] H. R. Chavoshi, A. H. Salasi, O. Payam, and H. Khaloozadeh, "Man-in-the-Middle Attack Against a Network Control System: Practical Implementation and Detection," *2023 IEEE 64th International Scientific Conference on Information Technology and Management Science of Riga Technical University, ITMS 2023 - Proceedings*, 2023, doi: 10.1109/ITMS59786.2023.10317671.

[16] T. Ariyadi, M. Rizky, M. K. Hadi, and A. A. Widodo, "Implementasi Firewall Pada Protokol SSH Linux Ubuntu Menggunakan Iptables," *Seminar Riset Mahasiswa-Computer & Electrical (SERIMA-CE*, vol. 1, no. 1, pp. 170–175, 2023.

[17] D. R. Az Zahra, F. P. Ilham, H. N. Ramdhani, and A. Setiawan, "Penerapan dan Pengujian Keamanan SSH Pada Server Linux menggunakan Hydra," *Journal of Internet and Software Engineering*, vol. 1, no. 3, p. 10, 2024, doi: 10.47134/pjise.v1i3.2627.

[18] I. J. King and H. H. Huang, "EULER: Detecting Network Lateral Movement via Scalable Temporal Link Prediction," *29th Annual Network and Distributed System Security Symposium, NDSS 2022*, no. April, 2022, doi: 10.14722/ndss.2022.24107.

[19] D. D. Mahendra and F. S. Mukti, "Sistem Deteksi dan Pengendalian Serangan Denial of Service pada Server Berbasis Snort dan Telegram-API," *Techno.Com*, vol. 21, no. 3, pp. 511–522, 2022, doi: 10.33633/tc.v21i3.6466.

[20] Y. MZ and H. Indrianta, "Penerapan Sistem Pakar Untuk Identifikasi Anak Berkebutuhan Khusus Menggunakan Metode Rule Based System," *Jurnal Informatika Dan Teknologi Informasi*, vol. 7, no. 1, pp. 1–78, 2022.