

DAFTAR PUSTAKA

- Ahmadi, a., akbar, t., & putra, h. M. (t.t.). *Perbandingan hasil tool forensik pada file image smartphone android menggunakan metode nist*. <https://doi.org/10.33387/jiko>
- Amin, a. S., & arnesia, d. (2023). *Pengembangan sistem keamanan jaringan menggunakan network forensics* (vol. 20, nomor 1).
- Aulianita, r., musyaffa, man, & martiwi, r. (t.t.). Penggunaan metode ids dalam implementasi *firewall* pada jaringan untuk deteksi serangan distributed denial of service (*ddos*). Dalam *jusikom : jurnal sistem komputer musirawas rizki aulianita, dkk* (vol. 6, nomor 2).
- Bahri, s. (t.t.). Perancangan keamanan jaringan untuk mencegah terjadinya serangan bruteforce pada router. *Indotech indonesian journal of education and computer science*, 1(3), 2023.
- Cunong, d. N., saputra, m., & puspitasari, w. (2020). *Analysis of oros modeler data reporting process to sap hana in activity based costing for indonesia telecommunication industry*. 7(1).
- Firman, a., suryawan, d., graha, f., putra, d., lovely, v. A., setiawan teknologi, a., komputer, r., vokasi, s., & pertanian bogor, i. (2024). Keamanan iot dan sistem terdistribusi. *Journal of internet and software engineering*, 1(3), 1–10. <https://doi.org/10.47134/pjise.v1i3.2619>
- Mikola, a., nurcahyo, a. C., informasi, t., & bhuana, s. (2022). Analisis load balancing berbasis mikrotik dalam meningkatkan kemampuan server di institut shanti bhuana. *Jifotech (journal of information technology)*, 2(2).
- Pendidikan, j. D., pembelajaran, d., nafysah, m., & laksana, e. A. (2023). *Rancang bangun teknologi edukasi berbasis moodle dan private cloud di sman 26 bandung*. <http://journal.umpo.ac.id/index.php/dimensi/index>
- Penelitian, m., khaliq, a., & sari, n. (2022). Lisensi lisensi internasional creative commons attribution-sharealike 4.0. 150. *Jurnal nasional teknologi komputer*, 2(3).
- Prathama, g. H., andaresta, d., & darmaastawan, k. (2021). Instalasi framework iot berbasis platform thingsboard di ubuntu server. *Tiers information technology journal*, 2(2), 1–9. <https://doi.org/10.38043/tiers.v2i2.3329>
- Purnama, t., muhyidin, y., singasatia, d., studi, p., informatika, t., teknologi, s. T., & purwakarta, w. (2023). *Implementasi intrusion detection system (ids) snort sebagai sistem keamanan menggunakan whatsapp dan telegram sebagai*

- Putra, s. P., & ramdhani, y. (2021). *Memfaatkan fitur firewall rules pada mikrotik untuk keamanan jaringan di hotel lenora bandung* (vol. 2, nomor 1). [Https://eprosiding.ars.ac.id/index.php/pti](https://eprosiding.ars.ac.id/index.php/pti)
- Ridho, m. A., & arman, m. (2020). Analisis serangan *ddos* menggunakan metode jaringan saraf tiruan. *Jurnal sisfokom (sistem informasi dan komputer)*, 9(3), 373–379. [Https://doi.org/10.32736/sisfokom.v9i3.945](https://doi.org/10.32736/sisfokom.v9i3.945)
- Santoso, n. A., ainurohman, m., & kurniawan, r. D. (2022). Penerapan metode penetration testing pada keamanan jaringan nirkabel. *Jurnal responsif*, 4(2), 162–167. [Https://ejurnal.ars.ac.id/index.php/jti](https://ejurnal.ars.ac.id/index.php/jti)
- Suhaidi, m., & nurhadi, n. (2023). Implementasi dan analisis keamanan jaringan pada stia lancang kuning dumai menggunakan port scanning dan *firewall tarpit*. *Arcitech: journal of computer science and artificial intelligence*, 3(2), 110. [Https://doi.org/10.29240/arcitech.v3i2.8181](https://doi.org/10.29240/arcitech.v3i2.8181)
- Suharti, s., yudhana, a., & riadi, i. (2022). Forensik jaringan *ddos* menggunakan metode addie dan hids pada sistem operasi proprietary. *Matrik: jurnal manajemen, teknik informatika dan rekayasa komputer*, 21(3), 567–582. [Https://doi.org/10.30812/matrik.v21i3.1732](https://doi.org/10.30812/matrik.v21i3.1732)
- Surya kusuma, r. (2023). Forensik serangan ransomware ryuk pada jaringan cloud. Dalam *forensik serangan ransomware ryuk pada jaringan cloud jurnal multinetics* (vol. 9, nomor 2).
- Yasin, f., abdul fadlil, & rusydi umar. (2021a). Identifikasi bukti forensik jaringan virtual router menggunakan metode nist. *Jurnal resti (rekayasa sistem dan teknologi informasi)*, 5(1), 91–98. [Https://doi.org/10.29207/resti.v5i1.2784](https://doi.org/10.29207/resti.v5i1.2784)