DAFTAR PUSTAKA

[1] J. M. Ceron, C. Scholten, A. Pras, and J. Santanna, "MikroTik Devices Landscape, Realistic Honeypots, and Automated Attack Classification," in *Proceedings of IEEE/IFIP Network Operations and Management Symposium 2020: Management in the Age of Softwarization and Artificial Intelligence, NOMS 2020*, Institute of Electrical and Electronics Engineers Inc., Apr. 2020. doi: 10.1109/NOMS47738.2020.9110336.

[2] H. L. J. Bijmans, T. M. Booij, and C. Doerr, "Just the tip of the iceberg: Internet-scale exploitation of routers for cryptojacking," in *Proceedings of the ACM Conference on Computer and Communications Security*, Association for Computing Machinery, Nov. 2019, pp. 449-464. doi: 10.1145/3319535.3354230.

[3] J. Ao, M. Ceron, C. Scholten, A. Pras, E. Lastdrager, and J. Santanna, "Characterising attacks targeting low-cost routers: a MikroTik case study (Extended)," 2020.

[4] A. Mangino, M. S. Pour, and E. Bou-Harb, "Internet-scale Insecurity of Consumer Internet of Things," *ACM Trans. Manag. Inf. Syst.*, vol. 11, no. 4, Dec. 2020, doi: 10.1145/3394504.

[5] G. Chalhoub and A. Martin, "But is it exploitable? Exploring how Router Vendors Manage and Patch Security Vulnerabilities in Consumer-Grade Routers," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Oct. 2023, pp. 277-295. doi: 10.1145/3617072.3617110.

[6] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions," Mar. 01, 2023, *MDPI*. doi: 10.3390/electronics12061333.

[7] A. Kusuma and I. H. Agus Sulistyono Reksoprodjo, "Forecasting Cyber Threat Landscapes in Indonesia (2025-2026): A Predictive Analysis Using the MITRE ATT&CK Framework," 2026.

[8] A. Azzam Ajhari, M. Agustian Manaon, D. Febriyan Priambodo, D. Bidang Keamanan Siber dan Sandi Perekonomian, and B. Siber dan Sandi Negara, "Security Awareness Framework untuk Usaha Mikro, Kecil dan Menengah di Indonesia."

[9] J. Ye, X. de Carné de Carnavalet, L. Zhao, M. Zhang, L. Wu, and W. Zhang, "Exposed by Default: A Security Analysis of Home Router Default Settings," in *ACM AsiaCCS 2024 - Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*, Association for Computing Machinery, Inc, Jul. 2024, pp. 63-79. doi: 10.1145/3634737.3637671.

[10] A. Anwar, Y. H. Chen, R. Hodgman, T. Sellers, E. Kirda, and A. Oprea, "A Recent Year On the Internet: Measuring and Understanding the Threats to Everyday Internet Devices," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Dec. 2022, pp. 251-266. doi: 10.1145/3564625.3564649.

[11] Dasril, M. Muhallim, S. Paembonan, and Syawal, "Rancang Bangun Sistem Keamanan Jaringan Menggunakan Metode Port Knocking Dan Port Blocking Dengan Notifikasi Email Pada SMK Kartika XX-2 Palopo," 2024. [Online]. Available: https://ojs.unanda.ac.id/index.php/jutinda

[12] Ardiansyah, A. Asvin Mahersatillah Suradi, and W. Saputra, "Strategi Keamanan Router MikroTik: Deteksi dan Mitigasi Serangan Brute Force Berbasis Scripting," *JUKI : Jurnal Komputer dan Informatika*, vol. 7, 2025.

[13] H. Husain, I. P. Hariyadi, K. A. Latif, and G. T. Aditya, "Implementation of Port Knocking with Telegram Notifications to Protect Against Scanner Vulnerabilities," *MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 23, no. 1, pp. 215-228, Nov. 2023, doi: 10.30812/matrik.v23i1.3459.

[14] E. Hutabri, "RANCANG BANGUN SISTEM KEAMANAN JARINGAN MIKROTIK MENGGUNAKAN FIREWALL FILTERING DAN PORT KNOCKING DENGAN NOTIFIKASI TELEGRAM PADA EVENT VIRTUAL," *JURNAL COMASIE*, 2023.

[15] J. vom Brocke, A. Hevner, and A. Maedche, "Introduction to Design Science Research," 2020, pp. 1-13. doi: 10.1007/978-3-030-46781-4_1.

[16] K. A. Scarfone, M. P. Souppaya, A. Cody, and A. D. Orebaugh, "NIST SP 800-115: Technical Guide to Information Security Testing and Assessment.," Gaithersburg, MD, 2008. doi: 10.6028/NIST.SP.800-115.

[17] A. Shandilya, "ABSOLUTELY ROUTED!! WHY ROUTERS ARE THE NEW BULLSEYE IN CYBER ATTACKS," 2019.

[18] R. Albar and R. O. Putra, “ANALISIS KEAMANAN JARINGAN MENGGUNAKAN METODE SNIFFING DAN IMPLEMENTASI KEAMANAN JARINGAN PADA MIKROTIK ROUTER OS V6.48.3 MENGGUNAKAN METODE PORT KNOCKING,” *Journal of Informatics and Computer Science*, vol. 8, no. 1, 2022.

[19] Z. Amanda Indira Azmi, “IMPLEMENTATION OF A NETWORK SECURITY SYSTEM USING THE PORT KNOCKING METHOD AT TARUNA SATRIA VOCATIONAL SCHOOL PEKANBARU PENERAPAN SISTEM KEAMANAN JARINGAN MENGGUNAKAN METODE PORT KNOCKING PADA SMK TARUNA SATRIA PEKANBARU,” vol. 9, no. 2, p. 2024, 2024.

[20] V. T. Aditya, “MANAJEMEN ANCAMAN DAN KEAMANAN JARINGAN MELALUI PENGGUNAAN FIREWALL DENGAN MIKROTIK PADA PT DINAMIKA MEDIAKOM,” 2023.

[21] A. Kurniawan and L. M. Silalahi, “Analisis Keamanan Jaringan Menggunakan Intrusion Prevention System (IPS) Dengan Metode Traffic Behavior,” 2023.

[22] A. Syaputera, Riska, and Yessi Mardiana, “Sistem Keamanan Jaringan Hotspot Dari Serangan Brute Force Menggunakan Firewall Eksternal Pfsense (Studi Kasus Hotspot Wifi-Ku.Net),” *JURNAL KOMITEK*, vol. 3, no. 1, pp. 205-218, 2023, doi: 10.53697/jkomitek.v3i1.

[23] M. A. Kinenda, R. B. Huwae, and A. H. Jatmika, “IMPLEMENTASI INTRUSION PREVENTION SYSTEM SNORT PADA ROUTER MIKROTIK RB-941-2nd TERHADAP SERANGAN BRUTEFORCE (IMPLEMENTATION OF THE SNORT INTRUSION PREVENTION SYSTEM ON THE RB-941-2nd MIKROTIC ROUTERBRUTEFORCE ATTACK),” 2024.

[24] Y. Setiayoko, D. Swanjaya, I. N. Farida, and D. D. Disetujui, “Analisis Implementasi Port Knocking pada Keamanan Jaringan di SMK PGRI 1 Nganjuk,” 2023.

[25] M. A. Rozan and M. Tahir, “Implementation and Security Testing of Mikrotik Router Againts Cyber Attacks Using Firewall and Penetration Testing,” 2025. [Online]. Available: https://ioinformatic.org/

[26] F. W. Christanto, P. Cholillah, and A. M. Hirzan, “Optimizing Mikrotik-Based Network Security using Address List, Firewall Filter Rules, and Raw Firewall,”

Revista de Informatica Teorica e Aplicada, vol. 32, no. 3, pp. 66-76, Aug. 2025, doi: 10.22456/2175-2745.142954.

[27] T. Maluku Utara Indonesia Yasir Muin, "MikroTik Router Vulnerability Testing for Network Vulnerability Evaluation using Penetration Testing Method," 2022.

[28] Seprianus Kenat, "Analisis Keamanan Jaringan Menggunakan Mikrotik Pada Lab Komputer STMIK Widuri," *Neptunus: Jurnal Ilmu Komputer Dan Teknologi Informasi*, vol. 2, no. 3, pp. 16-24, Jun. 2024, doi: 10.61132/neptunus.v2i3.177.

[29] Forum of Incident Response and Security Teams (FIRST), "Common Vulnerability Scoring System version 3.1 Specification Document Revision 1," 2019. [Online]. Available: https://www.first.org/cvss/

[30] M. Hasan, M. Raihan, and R. Rahman, "Pengujian Keamanan Jaringan Wireless terhadap Serangan Rogue Access Point."

[31] C. Maathuis and S. Chockalingam, "Responsible Digital Security Behaviour: Definition and Assessment Model," 2022.

[32] X. Liang and Y. Xu, "A novel framework to identify cybersecurity challenges and opportunities for organizational digital transformation in the cloud," Apr. 01, 2025, *Elsevier Ltd*. doi: 10.1016/j.cose.2025.104339.

[33] Y. Mulyanto, Herfandi, and R. C. Kirana, "ANALISIS KEAMANAN WIRELESS LOCAL AREA NETWORK (WLAN) TERHADAP SERANGAN BRUTE FORCE DENGAN METODE PENETRATION TESTING (Studi kasus: RS H.LMANAMBAI ABDULKADIR)".

[34] J. S. Komputer, K. Buatan, M. A. Adiguna, and B. W. Widagdo, "Analisis Keamanan Jaringan Wpa2-Psk Menggunakan Metode Penetration Testing (Studi Kasus : Router Tp-Link Mercusys Mw302r)," Mar. 2022.

[35] A. Rahman, "OPTIMALISASI KINERJA JARINGAN WIRELESS MENGGUNAKAN METODE QOS DAN KEAMANAN JARINGAN PORT KNOCKING BERBASIS MIKROTIK," 2024.

[36] B. Collier and R. Clayton, "Peer(ing) pressure: a cybersecurity intervention at global scale in the internet infrastructure," *J. Cybersecur.*, vol. 11, no. 1, 2025, doi: 10.1093/cybsec/tyaf014.

[37] X. Wang *et al.*, “Secure Inter-domain Routing and Forwarding via Verifiable Forwarding Commitments,” Nov. 2023, [Online]. Available: http://arxiv.org/abs/2309.13271

[38] R. Yazdani *et al.*, “Mirrors in the Sky: On the Potential of Clouds in DNS Reflection-based Denial-of-Service Attacks,” in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Oct. 2022, pp. 263-275. doi: 10.1145/3545948.3545959.

[39] T. Dai and H. Shulman, “SMap: Internet-wide Scanning for Spoofing,” in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Dec. 2021, pp. 1039-1050. doi: 10.1145/3485832.3485917.

[40] D. Novianto, Y. S. Japriadi, and L. Tommy, “Implementasi Keamanan Akses Terhadap Website Menggunakan Wireguard VPN Di Routerboard Mikrotik,” *Jurnal Ilmiah Informatika Global*, vol. 13, no. 2, Aug. 2022, doi: 10.36982/jiig.v13i2.2308.