DAFTAR PUSTAKA

1. Stakhanova, N., Basu, S., & Wong, J. (2016). Exploring Honeypot Capabilities for Malware Detection in Banking Networks. Journal of Cybersecurity and Information Systems, 4(2), 45-59.

2. Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2019). Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. In ICISSP, 108-116.

3. Vasilenko, R., Ryabko, D., & Yampolskiy, R. (2017). A Honeypot Framework for Detecting Advanced Malware in Large Networks. Journal of Information Security, 8(4), 320-329.

4. Satria, Y., Nugroho, F., & Priyambada, G. (2021). Analisis Log Cowrie Honeypot untuk Penyusunan Snort Signature Rule Deteksi Brute Force SSH. Jurnal Teknologi dan Sistem Komputer, 9(1), 45-52.

5. Ernawati, E., & Rachmat, M. (2021). Evaluasi Kinerja Cowrie Honeypot dengan Snort Inline-mode pada Deteksi Serangan Brute Force SSH. Jurnal Sistem dan Teknologi Informasi, 9(2), 118-125.

6. Dhafin, R., Pratama, A., & Maulana, I. (2025). Implementasi Honeypot Cowrie untuk Analisis Serangan Brute Force pada Layanan SSH. Seminar Nasional Teknologi Informasi dan Komunikasi (SENTIKA), Universitas Gadjah Mada.

7. Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94

8. Bejtlich, R. (2005). The Tao of Network Security Monitoring: Beyond Intrusion Detection. Addison-Wesley.