DAFTAR PUSTAKA

Administrator. (2017, Desember 13). *SMB Share - SCF File Attack*. Diambil kembali dari Penetration Testing Lab: https://pentestlab.blog/2017/12/13/smb-share-scf-file-attacks/, diakses pada 6 Januari 2021

Alghofiqi, M. H. (2019). Analisis Struktur Basisdata Berorientasi Dokumen untuk Kebutuhan Sistem Keamanan Jaringan berbasis Honeypot Dionaea.

Ali. P, D. G. (2017). *Malware Capturing and Detection in Dionaea Honeypot*.

Anonim. (t.thn.). *Conficker.AE*. Diambil kembali dari Virus Radar: https://www.virusradar.com/en/Win32_Conficker.AE/description, diakses pada 26 Juli 2021

Anonim. (t.thn.). *Worm:W32/Downadup*. Diambil kembali dari F-Secure: https://www.f-secure.com/v-descs/worm_w32_downadup.shtml, diakses pada 26 Juli 2021

Arntz, P. (2018, Desember 14). *How threats actors are using SMB vulnerabilities*. Diambil kembali dari Malwarebytes LABS: https://blog.malwarebytes.com/101/2018/12/how-threat-actors-are-using-smb-vulnerabilities/, diakses pada 16 Maret 2021

Arridha, R. d. (2017). *Classification Extension based on IoT-Big Data Analytics for Smart Environment Monitoring and Analytics in Real-Time*, 82-92.

Asher-Dotan, L. (2016, September 12). *What is the Conficker worm*. Diambil kembali dari Cybereason: https://www.cybereason.com/blog/what-is-the-conficker-worm, diakses pada 26 Juli 2021

Baitha, A. K. (2018). Session Hijacking and Prevention Technique. *International Journal of Engineering & Technology*, 193-198.

Bhavsar, V. d. (2018). Study on Phishing Attacks. *International Journal of Computer Applications (0975 - 8887)*.

Do, E. H. (2019). An Entropy-based approach to Network Attack Classification with Deep Neural Network.

GoldSparrow. (t.thn.). *Kido*. Diambil kembali dari Enigma Software: https://www.enigmasoftware.com/kido-removal/, diakses pada 26 Juli 2021

Hendry. (2018). Implementasi SAMBA Server untuk Mendukung Sharing Printer di SD Swasta Al-Washliyah 6/39 Medan . *Jurnal Ilmiah Core IT*.

Hope, C. (2020, Agustus 31). *What is the Windows lsass.exe file and process?* Diambil kembali dari Computer Hope: https://www.computerhope.com/issues/ch000913.htm, diakses pada 20 April 2021

Imran, B. R. (2012). *Studi Klasifikasi Keamanan Data untuk Enterprise*.

Lailiyah, M. (2017). SENTIMENT ANALYSIS MENGGUNAKAN RULE BASED METHOD PADA DATA PENGADUAN PUBLIK BERBASIS LEXICAL RESOURCES.

Luo, Y. d. (2019). *Classification of TCP 445 Attacks and Global Snapshot with Honeypot Analysis*.

Lutfi, F. (2017, Januari 19). *Mengenal Node.js*. Diambil kembali dari Codepolitan: https://www.codepolitan.com/mengenal-nodejs-5880234fe9ae3, diakses pada 12 September 2020

Michel Cukier, R. B. (2006). A Statistical Analysis of Attack Data to Separate Attacks.

Naufal Arkaan, D. V. (2019). Implementasi Low Interaction Honeypot Untuk Peningkatan Keamanan Server dan Analisa Serangan Pada Protokol SSH . *Jurnal Nasional Teknologi dan Sistem Informasi*, 112-120.

Pilici, S. (2018, Juli 28). *How To Remove Csrss.exe Malware (Virus Removal Guide)*. Diambil kembali dari Malwaretips: https://malwaretips.com/blogs/remove-csrss-exe/, diakses pada 10 Juli 2021

Putra, S. N. (2020). Analisis Log Honeypot Dionaea untuk Mengklasifikasikan Jenis Serangan terhadap Basisdata SQL Menggunakan DionaeaSI.

Rash, W. (2018, November 21). *SMB Malware: What Are the Threats and Why Are They Getting Worse*. Diambil kembali dari PCMAG: https://www.pcmag.com/news/smb-malware-what-are-the-threats-and-why-are-they-getting-worse, diakses pada 20 Mei 2021

Salian, I. (2018, Agustus 2). *SuperVize Me: What's the Difference Between Supervised, Unsupervised, Semi-Supervised and Reinforcement Learning?* Diambil kembali dari NVIDIA: https://blogs.nvidia.com/blog/2018/08/02/supervised-unsupervised-learning/, diakses pada 18 April 2021

Shajit, B. A. (2016). Developing an In-kernel File Sharing Solution Based on Server Message Block Protocol.

Singh, L. J. (2018). A Survey on Phishing and Anti-Phishing Techniques. *International Journal of Computer Science Trends and Technology (IJCST)*.

Sochor, T. d. (2016). *Analysis of Attackers Against Windows Emulating Honeypots in Various Types of Networks and Regions*.

Sunardi, A. d. (2011). *Implementasi dan Evaluasi Honeypot Dionaea dan Glastopf di ID-SIRTII*.

Supriyono, A. R. (2018). *Metode Live Forensics Acquisition File Sharing Samba untuk Ekplorasi Bukti Digital pada Smart Router*.

Ullah, I. (2016). Detecting Lateral Movement Attacks through SMB using BRO.

Unterfingher, V. (2020, November 27). *What is an SMB Relay Attack*. Diambil kembali dari Heimdal Security: https://heimdalsecurity.com/blog/what-is-an-smb-relay-attack/, diakses pada 10 Februari 2021

Valente, d. (2020). REST vs GraphQL: A Controlled Experiment.

Vipul A M, P. S. (2016). *ReactJS by Example - Building Modern Web Application with React.* Birmingham: Packt.

Wagner, G. (2016). Introduction to Simulation using JavaScript.

Waseem, M. (2021, Juli 15). *How To Implement Classification In Machine Learning*. Diambil kembali dari Edureka: https://www.edureka.co/blog/classification-in-machine-learning/, diakses pada 20 April 2021

Zhu, L. d. (2017). *Express Supervision System Based on NodeJS and MongoDB*.