DAFTAR PUSTAKA

Ahmed. (2024, October 15). *Wireshark 101: Finding Passwords & Credentials in Plain Text Traffic*. Medium.

Bazzell, M. (2023). *Open source intelligence techniques: resources for searching and analyzing online information 8th edition* (8th ed.). CreateSpace Independent Publishing Platform.

Bhattacharjee, S. (2018). *Practical Industrial Internet of Things security: A practitioner's guide to securing connected industries*. Packt Publishing Ltd.

Block, L. (2023). The long history of OSINT. *Journal of Intelligence History*, *23*(2), 95–109. https://doi.org/10.1080/16161262.2023.2224091

Franco, M. F., Mullick, R., & Jha, S. (n.d.). *QBER: Quantifying Cyber Risks for Strategic Decisions*. https://zeron.one/

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). *Design Science in Information Systems Research* 1. In *Design Science in IS Research MIS Quarterly* (Vol. 28, Issue 1).

Hopkin, P. (2018). *Fundamentals of risk management: understanding, evaluating and implementing effective risk management*. Kogan Page Publishers.

Jay Jani. (2019, January 8). *S3 Bucket Misconfiguration: From Basics to Pawn*. Medium.

Keysight Application and Threat Intelligence (ATI) Research Center. (2020, November 11). *Deconstructing Apache Tomcat JSP Upload Remote Code Execution (CVE-2017-12615)*. Keysight Blogs.

Landoll, D. (2021). *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments*. CRC Press. https://books.google.co.id/books?id=P2g7EAAAQBAJ

Mining, W. I. D. (2006*). Data mining: Concepts and techniques*. Morgan Kaufinann, *10*(559–569), 4.

MITRE Corporation. (2013). *CVE-2013-2220*. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2220

MITRE Corporation. (2014). *CVE-2014-0160*. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160

MITRE Corporation. (2016). *CVE-2015-9251*. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-9251

MITRE Corporation. (2017a). *CVE-2016-10735*. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10735

MITRE Corporation. (2017b). *CVE-2017-12615*. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12615

MITRE Corporation. (2020). *CVE-2020-11022*. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11022

Morana, M. M., & Vélez, T. U. (2015). *Risk centric threat modeling: process for attack simulation and threat analysis*. John Wiley & Sons, Incorporated.

National Institute of Standards and Technology. (2012). *Guide for conducting risk assessments*. https://doi.org/10.6028/NIST.SP.800-30r1

National Institute of Standards and Technology. (2019). *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*. https://csrc.nist.gov/publications/detail/sp/800-131a/rev-2/final

National Institute of Standards and Technology. (2020). *Security and Privacy Controls for Information Systems and Organizations*. https://doi.org/10.6028/NIST.SP.800-53r5

OSINT Foundations. (2022). *OSINT Definitions*.

Pastor-Galindo, J., Nespoli, P., Gomez Marmol, F., & Martinez Perez, G. (2020). The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. *IEEE Access*, *8*, 10282–10304. https://doi.org/10.1109/ACCESS.2020.2965257

Rajamäki, J., & Tiitta, K. (2024). *Implementation of OSINT for Improving an International Finance Sector Organization's Cybersecurity*.

Rastogi, N., Dutta, S., Gittens, A., Zaki, M. J., & Aggarwal, C. (n.d.). *TINKER: A framework for Open source Cyberthreat Intelligence*.

Rescorla, E., Ray, M., Dispensa, S., & Oskov, N. (2010). *Transport Layer Security (TLS) Renegotiation Indication Extension*. https://www.rfc-editor.org/rfc/rfc5746

Roth, R. M., Dennis, A., & Wixom, B. H. (2012). *System analysis and design*.

Schneier, B. (2000). *Secrets and Lies: Digital Security in a Networked World. Indianapolis*. Wiley Publishing, Inc.

Shimonski, R. (2014). *Cyber reconnaissance, surveillance and defense*. Syngress.

Shostack, A. (2014). *Threat modeling: Designing for security*. John wiley & sons.

Singh, G. D. . (2023). *Reconnaissance for ethical hackers: focus on the starting point of data breaches and explore essential steps for successful pentesting*. Packt Publishing.

Verizon Business. (2024). *2024 Data Breach Investigations Report*.

Yazar, Z. (2000). *Global Information Assurance Certification Paper A qualitative risk analysis and management Tool-CRAMM*. http://www.giac.org/registration/gsec

Zhang, Y., Frank, R., Warkentin, N., & Zakimi, N. (2022). *Accessible from the open web: a qualitative analysis of the available open-source information involving cyber security and critical infrastructure.* Journal of Cybersecurity, *8*(1). https://doi.org/10.1093/cybsec/tyac003