[5] Benjamin Ampel, Sagar Samtani, Steven Ullman, and Benjamin Ampel. 2021. Linking Common vulnerabilities and exposures to the

MITRE ATT&CK framework: A self-distillation approach. CoRR abs/2108.01696 (2021). https://arxiv.org/abs/2108.01696.

[6] Yevonnael Andrew, Charles Lim, and Eka Budiarto. 2022. Mapping linux shell commands to MITRE ATT&CK using NLP-based approach.

In Proceedings of the International Conference on Electrical Engineering and Informatics (ICELTICs’22). 37–42. https://doi.org/10.1109/

ICELTICs56128.2022.9932097

[22] Aditya Kuppa, Lamine Aouad, and Nhien-An Le-Khac. 2021. Linking CVE’s to MITRE ATT&CK techniques. In Proceedings of the 16th

International Conference on Availability, Reliability and Security (ARES’21). Association for Computing Machinery, New York, NY, Article

21, 12 pages. https://doi.org/10.1145/3465481.3465758

[23] Valentine Legoy, Marco Caselli, Christin Seifert, and Andreas Peter. 2020. Automated retrieval of att&ck tactics and techniques for cyber

threat reports. arXiv:2004.14322. Retrieved from https://arxiv.org/abs/2004.14322.

[24] Swee Kiat Lim, Aldrian Obaja Muis, Wei Lu, and Chen Hui Ong. 2017. MalwareTextDB: A database for annotated malware articles.

In Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers). Association for

Computational Linguistics, 1557–1567. https://doi.org/10.18653/v1/P17-1143

[40] Zhaohui Zheng, Xiaoyun Wu, and Rohini Srihari. 2004. Feature selection for text categorization on imbalanced data. SIGKDD Explor.

Newsl. 6, 1 (Jun. 2004), 80–89. https://doi.org/10.1145/1007730.1007741