# DAFTAR PUSTAKA


[1] International Telecommunication Union Radiocommunication. Detailed Specifications of the Terrestrial Radio Interfaces of International Mobile Telecommunications-2020 (2020)

[2] Ijaz Ahmad, Shariar Shahabuddin, Tanesh Kumar, Jude Okwuibe, Andrei Gurtov, Mika Ylianttila. Security for 5G and Beyond. Centre for Wireless Communications, University of Oulu, VTT Technical Research Centre, Nokia, Department of Computer and Information Science, Linkoping University, (2019).

[3] A. N. Bikos and N. Sklavos, "LTE/SAE Security Issues on 4G Wireless Networks," IEEE Security Privacy, vol. 11, no. 2, pp. 55–62, March (2013)

[4] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J. Seifert, "Practical attacks against privacy and availability in 4g/lte mobile communication systems," CoRR, vol. abs/1510.07563, (2015)

[5] Hussain, Syed Rafiul, Mitziu Echeverria, Omar Chowdhury, Ninghui Li, Elisa Bertino. "Privacy attacks to the 4G and 5G cellular paging protocols using side channel information." Network and Distributed Systems Security (NDSS) Symposium 2019 (2019)

[6] Damayanti dkk. (2022). Desain and Build 4G Open Radio Access Network at SmartLab Politeknik Negeri Jakarta. Doi: 10.31289/jite.v6i2.7537

[7] github.com. (2022, 13 Januari). Aligungr/UERANSIM. Diakses pada 22 Juli 2023, dari https://github.com/aligungr/UERANSIM

[8] tif.uad.ac.id. (2023, 27 Maret). WireShark: Perangkat Lunak Analisis Jaringan. Diakses pada 22 Juli 2023, dari https://tif.uad.ac.id/wireshark-perangkat-lunak-analisis-jaringan/

[9] 5gtechnologyworld.com. (2022,15 Maret). Private 5G: What is it? How does it work?. Diakses pada 22 juli 2023, dari https://www.5gtechnologyworld.com/private-5g-what-is-it-how-does-it-work/.

[10] Aladren, Domingo., Carmen, Del Maria. (2022). A Degree Thesis: Log-based monitoring, detection and automated correction of anomalies in the 5G core.

[11] Open5Gs, "Quick start Open 5GS," 2023 [Online] https://open5gs.org/open5gs/docs/

[12] Lee lin dkk. (2021). "Realizing 5G Network Slicing Provisioning with Open Source Software". Proceedings, APSIPA Annual Summit and Conference 2021*, Page 8*.

[13] Pande, S., Khamparia, A., Gupta, D., and Thanh, D.N. DDOS Detection using Machine Learning Technique. In Recent Studies on Computational Intelligence, pp. 59-68, 2021.

[14] wikipedia.org, (last edited 2023,7 agustus). Fuzzing. Diakses pada 2 Agustus 2023, dari https://en.wikipedia.org/wiki/Fuzzing.

[15] Salazar dkk, (2021) "5Greplay: a 5G Network Traffic Fuzzer - Application to Attack Injection," ARES 2021, August 17–20, 2021, Vienna, Austria arXiv:2304.05719v1 [cs.NI] page 12.

[16] PANGESTU, Teguh; LIZA, Risko. Analisis Keamanan Jaringan pada Jaringan Wireless dari Serangan Man In The Middle Attack DNS Spoofing. JiTEKH, 2022, 10.2: 60-67.

[17] V, C, Ginting, D. P. Kartikasari "Deteksi Serangan ARP Spoofing Berdasarkan Analisis Lalu Lintas Paket Protokol ARP". Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer. Vol. 3, No. 5. Hlm. 5049-5057. E-ISSN: 2548-964X, 2019.

[18] A. R. Taqwa, D. H. Sulaksono, "Implementasi Kriptografi Dengan Metode Elliptic Curve Cryptography (ECC) Untuk Aplikasi Chatting Berbasis Android", Jurnal Riset Inovasi Bidang Informatika dan Pendidikan Informatika (KERNEL). Vol. 1. No. 1, 2020

[19] Nainggolan dkk, (2022) “Monitoring Keamanan Jaringan Pada Server Ubuntu Dari Serangan DDoS Menggunakan Snort IDS,” e-ISSN :2776-5792 Vol. 2, No. 2, Oktober 2022, pp. 1-10 page 10.

[20] Zongjian Wang and Xiaobo Li, (2013) “Intrusion Prevention System Design,” Engineering 218, DOI: 10.1007/978-1-4471-4847-0_47, Springer-Verlag London 2013 page 8.

[21] Tan J (2003) With firewall intrusion detection system design and implementation, vol 07. Sichuan University, Chengdu, pp 32–36

[22] Mengatasi Serangan DNS Spoofing. (2023). Diakses pada 15 Agustus 2023, dari https://www.initialboard.com/mengatasi-serangan-dns-spoofing#gsc.tab=0.

[23] Rianda. (2022). “Ketahui Pengertian DNS Spoofing dan Cara Pencegahannya”. Diakses pada 15 Agustus 2023, dari https://dewabiz.com/pengertian-dns-spoofing/