DETEKSI EXPLOIT REVERSE TCP DARI APK TROJAN PADA NETWORK TRAFFIC DENGAN METODE RANDOM FOREST

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH:

MUHAMMAD ARYA DANUARTA

09011282025035

SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

TAHUN 2024

LEMBAR PENGESAHAN

DETEKSI EXPLOIT REVERSE TCP DARI APK TROJAN PADA NETWORK TRAFFIC DENGAN METODE RANDOM FOREST

SKRIPSI

Program Studi Sistem Komputer

Jenjang S1

OLEH:

MUHAMMAD ARYA DANUARTA

09011282025035

Indralaya, 11 Juni 2024

Mengetahui,

Ketua Jurusan Sistem Komputer	Pembimbing Tugas Akhir
Dr. Ir. H. Sukemi, M.T.	Prof. Deris Stiawan, M.T., Ph.D.
NIP. 196612032006041001	NIP. 197806172006041002

AUTHENTICATION PAGE

DETECTION OF REVERSE TCP EXPLOIT FROM TROJAN APK IN NETWORK TRAFFIC USING RANDOM FOREST METHOD

THESIS

Dept. of Computer System

Bachelor's Degree

By:

MUHAMMAD ARYA DANUARTA

09011282025035

Indralaya, 11 June 2024

Acknowledge,

Head of Computer System Department	Final Project Advisor
Dr. Ir. H. Sukemi, M.T.	Prof. Deris Stiawan, M.T., Ph.D.
NIP. 196612032006041001	NIP. 197806172006041002

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Rabu

Tanggal : 22 Mei 2024

Tim Penguji :

1. **Ketua** : **Kemahyanto Exaudi, M.T.** (.....)
2. **Sekretaris** : **Iman Saladin B. Azhar, M.M.S.I.** (.....)
3. **Pembimbing** : **Prof. Deris Stiawan, M.T., Ph.D.** (.....)
4. **Penguji** : **Ahmad Heryanto, M.T.** (.....)

Mengetahui 11/6/24
Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.
NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama : Muhammad Arya Danuarta

NIM : 09011282025035

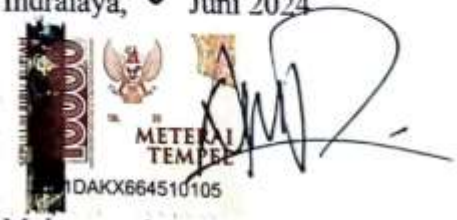
Judul TA : Deteksi *Exploit Reverse* TCP dari APK Trojan pada *Network Traffic* dengan Metode *Random Forest*

Hasil Pengecekan Software (*Thenticate/Turnitin*) : 1%

Menyatakan bahwa tugas akhir/skripsi ini merupakan hasil karya sendiri dan bukan merupakan plagiasi/duplikasi dari penelitian orang lain. Adapun jika ditemukan unsur plagiasi/duplikasi dari penelitian orang lain, maka saya bersedia menerima sanksi akademik dari pihak Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian pernyataan ini saya buat dengan sebenar-benarnya dengan tanpa adanya paksaan.

Indralaya, 6 Juni 2024



Muhammad Arya Danuarta

NIM. 09011282025035

KATA PENGANTAR

Segala puji dan syukur penulis ucapkan atas kehadiran Allah SWT, karena atas izin-Nya penulis dapat menyusun dan menyelesaikan skripsi dengan judul **"Deteksi Exploit Reverse TCP dari APK Trojan pada Network Traffic dengan Metode Random Forest".**

Proses dalam penyusunan skripsi ini tidak terlepas dari bantuan, dukungan dan semangat dari banyak pihak. Oleh karena itu, penulis ingin menyampaikan ucapan terimakasih dan penghargaan setinggi-tingginya kepada:

1. Kedua orang tua penulis yang telah merawat, mengajari, mendanai serta menyertai doa kepada anak pertamanya dalam menjalankan penyusunan skripsi.
2. Bapak Ir. Sukemi, M.T., selaku Ketua jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Bapak Prof. Deris Stiawan, M.T., Ph.D. sebagai Dosen Pembimbing Skripsi penulis yang telah berkenan membagi ilmu, saran, serta waktu untuk penulis dalam menyusun skripsi.
4. Bapak Huda Ubaya, M.T. selaku Dosen Pembimbing Akademik penulis pada jurusan Sistem Komputer.
5. Para staff jurusan Sistem Komputer Universitas Sriwijaya.
6. Bapak Drs. Sholihin beserta keluarga yang telah membantu penulis dalam penyediaan tempat tinggal serta bantuan finansial selama kuliah.
7. Grup Research COMNETS yang telah memberikan kesempatan kepada penulis untuk ikut berkontribusi dan menyediakan sarana fasilitas yang dapat membantu penulis dalam menyusun penelitian skripsi.
8. Teman-teman OBE, SK20 yang telah membantu penulis selama berkuliah di jurusan Sistem Komputer Universitas Sriwijaya dan Saudara seperjuangan Xenon yang telah dan masih membantu penulis untuk mencapai tahap ini.

9. Annisa Sabrina Giri yang telah datang dan memilih penulis pada waktu yang tepat dalam memberikan variasi warna dan semangat yang baru kepada penulis untuk menjalani kehidupan. *If the stars could sing, the songs would be yours*.
10. Developer Game, para Musisi, dan Content Creator yang telah menciptakan karya-karyanya sehingga dapat menemani penulis dalam mengisi rasa sepi selama berkuliah.

Penulis menyadari secara betul bahwa skripsi ini masih jauh dari kata sempurna dan punya banyak ruang untuk dapat ditingkatkan kualitasnya. Oleh karena itu, penulis dengan terbuka mendengarkan saran dan kritik yang membangun untuk pembelajaran penulis dan membuat skripsi ini menjadi lebih baik. Penulis berharap, skripsi ini dapat berguna dan menjadi inspirasi bagi pembaca dan pihak yang terlibat.

Penulis,

Muhammad Arya Danuarta

NIM. 09011282025035

DETEKSI EXPLOIT REVERSE TCP DARI APK TROJAN PADA NETWORK TRAFFIC DENGAN METODE RANDOM FOREST

MUHAMMAD ARYA DANUARTA (09011282025035)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer

Universitas Sriwijaya

Email: danurta97@gmail.com

ABSTRAK

Android menjadi OS paling populer pada perangkat mobile membuatnya menjadi target utama *threat actor* dalam membuat *malware*. Beberapa penelitian menunjukkan bahwa deteksi malware pada perangkat mobile dapat dilakukan dengan bantuan *Machine Learning*. Penelitian yang dilakukan penulis memiliki tujuan dalam mendeteksi eksploit *reverse* TCP pada *network traffic* dengan metode *Random Forest*. Deteksi yang dilakukan menggunakan *Random Forest* pada penelitian ini mencapai akurasi tertinggi yaitu 99.94% dengan 64 Decision Trees dan jumlah rasio data uji dan latih sebesar 80:20. Model *Random Forest* dengan akurasi terbaik juga diimplementasikan sebagai NIDS untuk menunjukkan *traffic* yang diduga kegiatan eksploit *reverse* TCP.

Kata Kunci: Deteksi, *Network Traffic*, Android, *Random Forest*, Trojan APK, *Machine Learning*, Metasploit, NIDS.

Mengetahui,

Ketua Jurusan Sistem Komputer	**Pembimbing Tugas Akhir**
Dr. Ir. H. Sukemi, M.T.	**Prof. Deris Stiawan, M.T., Ph.D.**
NIP. 196612032006041001	**NIP. 197806172006041002**

DETECTION OF REVERSE TCP EXPLOIT FROM TROJAN APK IN NETWORK TRAFFIC USING RANDOM FOREST METHOD

MUHAMMAD ARYA DANUARTA (09011282025035)

Dept. of Computer System, Faculty of Computer Science, Sriwijaya University

Email: danurta97@gmail.com

ABSTRACT

Android for being the most popular OS on mobile devices makes it the main target for threat actors in creating malware. Several studies show that malware detection on mobile devices can be done with the help of Machine Learning. The research carried out by the author aims to detect reverse TCP exploits in network traffic using the Random Forest method. Detection carried out using Random Forest in this study achieved the highest accuracy, namely 99.94% with 64 Decision Trees and a total ratio of test and training data of 80:20. The Random Forest model with the best accuracy is also implemented as NIDS to show traffic that is suspected of reverse TCP exploit activity.

***Keywords*: *Detection*, *Network Traffic*, Android, *Random Forest*, Trojan APK, *Machine Learning*, Metasploit, NIDS.**

Acknowledge,

Head of Computer System Department	**Final Project Advisor**
Dr. Ir. H. Sukemi, M.T.	**Prof. Deris Stiawan, M.T., Ph.D.**
NIP. 196612032006041001	**NIP. 197806172006041002**

DAFTAR ISI

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB I
PENDAHULUAN

1.1 Latar Belakang

Jumlah perangkat *mobile* dari tahun ke tahun semakin meningkat, hal ini karena pekerjaan, hiburan serta komunikasi sudah dapat dilakukan melalui perangkat *mobile* [1]. Pada tahun 2022 tercatat sebanyak 7.2 miliar pengguna perangkat *mobile* aktif dan diperkirakan akan terus meningkat menyentuh 7.4 miliar pengguna perangkat *mobile* pada tahun 2025 [2], dengan mayoritas perangkat *mobile* menggunakan sistem operasi Android [3], [4].

Android sebagai OS yang populer dalam perangkat *mobile* bukan tanpa sebuah alasan, hal ini dikarenakan Android bersifat *open source* yaitu gratis dan dapat dikembangkan oleh semua pihak sehingga lebih digemari oleh para vendor perangkat *mobile* [1], [5]. Namun dibalik semua itu, hal ini juga menarik perhatian para pelaku kejahatan siber untuk menjadikan perangkat mobile Android sebagai target korban *malware* [4].

Malware yang merupakan singkatan dari *malicious software* adalah semua program yang dapat merusak, merugikan, dan memasuki sistem sebuah perangkat tanpa izin [6], [7]. Pada semester pertama 2020, terdapat 1 juta *sample mobile malware* dengan rata-rata 6 ribu *sample malware* baru per hari [4]. Data yang diberikan oleh [8] pada bulan Agustus 2023 menunjukkan bahwa mayoritas aktivitas serangan siber yang terjadi ke Indonesia merupakan aktivitas *malware* trojan. Trojan merupakan salah satu jenis dari *malware* yang terlihat seperti aplikasi/program yang berjalan dan berfungsi dengan normal untuk mengelabui *user*. Trojan dapat memberikan akses tanpa izin kepada *threat actor* untuk mencuri data dan merusak sistem ke perangkat yang terinfeksi [1], [9]. Penelitian yang dilakukan oleh [10] dan [11] menunjukkan bahwa perangkat Android dapat di eksploitasi dengan membuat *user* menginstal APK trojan yang telah dibuat dengan tools Metasploit. Oleh karena itu, deteksi dan pencegahan terhadap malware dengan

salah satunya trojan sangatlah penting untuk menjaga privasi dan keamanan data pada semua perangkat.

Upaya deteksi terhadap *malware* dapat dilakukan dengan 3 metode yaitu metode statis, dinamis atau *hybrid* [3], [12]. Metode yang ada memiliki kelebihan dan kekurangan masing-masing. Ketika penggunaan algoritma AI menjadi popular, AI juga digunakan untuk mendeteksi *malware* [13]. Penelitian yang dilakukan oleh [9] menggunakan metode statis dengan langsung menganalisa file APK menggunakan CNN dapat mendeteksi *malware* perangkat *mobile* dengan akurasi 84.9%. Penelitian [14] menggunakan metode hybrid dengan mengekstrak API dan perizinan dari APK untuk dijadikan *signature* dalam deteksi malware menggunakan Random Forest berhasil mencapai akurasi sebesar 95%. Sedangkan, pendapat dari [6] mengatakan bahwa deteksi pada jaringan lalu lintas lebih cocok untuk mendeteksi *mobile malware* karena kebanyakan *mobile malware* akan melakukan komunikasi melalui jaringan. Sehingga penelitian yang dilakukan oleh [6] menggunakan metode statis dengan menganalisa *network traffic* yang dihasilkan *malware* pada perangkat mobile menggunakan *deep learning* mencapai akurasi sebesar 98.9%. Penelitian yang dilakukan [15] untuk mendeteksi *malware* pada *network traffic* dengan metode XGBoost mencapai akurasi 95.7%. Namun penelitian-penelitian tersebut menggunakan dataset lama atau tidak terlalu fokus pada lingkungan perangkat *mobile* sehingga penulis terinspirasi untuk melakukan penelitian deteksi *mobile malware trojan* dari penelitian sebelumnya [15], [10], [11] menggunakan dataset yang lebih baru, kombinasi algoritma AI Random Forest dan berfokus pada ruang lingkup perangkat *mobile.* Diharapkan dari percobaan ini dapat menghasilkan model AI Random Forest dengan akurasi tinggi dalam mendeteksi aktivitas malware trojan pada lalu lintas jaringan oleh perangkat *mobile* yang terinfeksi.

1.2 Rumusan Masalah

Berdasarkan penjelasan latar belakang diatas, dapat diuraikan perumusan masalah sebagai berikut:

1. Bagaimana membangun NIDS dengan model AI Random Forest untuk mendeteksi aktivitas malware trojan pada lalu lintas jaringan yang dihasilkan oleh perangkat *mobile* yang terinfeksi?
2. Apa saja fitur yang dapat digunakan untuk melatih model AI Random Forest dalam mendeteksi trojan metasploit pada lalu lintas jaringan *mobile*?
3. Bagaimana meningkatkan akurasi model Random Forest untuk mendeteksi *traffic* trojan Metasploit *Reverse* TCP pada Android?

1.3 Batasan Masalah

Batasan-batasan masalah yang dibahas di dalam penelitian ini adalah:

1. Melakukan deteksi khusus pada *malware* trojan *reverse tcp* yang dihasilkan dengan menggunakan tools Metasploit.
2. Dataset yang digunakan oleh penulis dibuat di Laboratorium COMNETS Indralaya Universitas Sriwijaya.
3. NIDS yang dihasilkan hanya mendeteksi eksploit *reverse* TCP dari APK trojan pada *network traffic*.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut:

1. Membuat dataset *network traffic* yang berisi komunikasi *malware* trojan *reverse* TCP dari APK yang dibuat dengan Metasploit.
2. Mendeteksi aktivitas APK Trojan dengan klasifikasi Random Forest dan sebagai pengenalan pola serangan pada jaringan.
3. Mengukur akurasi deteksi aktivitas trojan Metasploit *reverse* TCP pada jaringan.
4. Membuat NIDS yang dapat mendeteksi serangan reverse TCP dari APK trojan pada jaringan.

1.5 Manfaat Penelitian

Manfaat yang bisa dihasilkan dari penelitian ini adalah sebagai berikut:

1. Menghasilkan dataset yang memuat *traffic* serangan *reverse* TCP dari Android.
2 Memahami *feature* yang dapat digunakan secara efektif untuk mengenali serangan reverse TCP Android.
3 Menghasilkan program NIDS untuk mendeteksi *reverse* TCP Android.

1.6 Metodologi Penelitian

Penelitian akan dilakukan dengan tahapan-tahapan berikut:

1. Tahap Pertama (Studi Literatur)
   Pada tahap ini, penulis melakukan studi terhadap topik penelitian yang terkait melalui jurnal artikel, paper konferensi dan dokumen ilmiah lainya.
2. Tahap Kedua (Pembuatan Topologi dan Dataset)
   Penulis melakukan rancangan topologi untuk membuat dataset *network traffic* malware trojan pada perangkat *mobile* yang nanti digunakan sebagai data *learning* model *random forest.*
3. Tahap Ketiga (Pengolahan Data)
   Pada tahap ini, data dari tahap kedua diambil, diolah dan diekstrak untuk mendapatkan *feature* yang nanti digunakan untuk *learning* model.
4. Tahap Keempat (Perancangan Model Deteksi)
   Pada tahap ini, penulis akan membuat model-model RF (*random forest*) yang akan dilatih dengan dataset *traffic* malware trojan Metasploit untuk dapat mendeteksi malware tersebut.
5. Tahap Kelima (Pengujian Model Deteksi)
   Model yang telah dibangun pada tahap sebelumnya diuji dengan *test* dataset untuk mengetahui performa dan kemampuan dari tiap model serta dilakukan validasi. Model dengan performa terbaik akan diimplementasikan menjadi program yang bertindak sebagai NIDS.
6. Tahap Keenam (Hasil dan Analisa)
   Pengujian yang telah dilakukan di evaluasi dan dianalisa untuk mencari akurasi, kelemahan dan kelebihan yang dapat mempengaruhi kinerja model yang dibuat.
7. Tahap Ketujuh (Kesimpulan dan Saran)

Tahap terakhir penulis melakukan penarikan kesimpulan berdasarkan perumusan masalah, studi literatur, hasil perancangan model dan analisa dari pengujian model. Penulis juga akan menyantumkan saran jika penelitian ini dijadikan referensi untuk penelitian selanjutnya.

1.7 Sistematika Penulisan

Sistematika dalam penulisan skripsi ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab pertama akan menyampaikan tentang latar belakang, rumusan masalah, batasan masalah, tujuan dari penelitian ini, dan sistematika penulisan yang dipakai.

BAB II TINJAUAN PUSTAKA

Bab kedua akan menjelaskan mengenai dasar-dasar teori dan istilah-istilah penting yang menjadi landasan penelitian.

BAB III METODOLOGI PENELITIAN

Bab ketiga akan menjelaskan tahapan dan urutan kegiatan yang dilakukan pada penelitian ini. Dimulai dari studi literatur, perancangan topologi dan tahapan pembuatan dataset, pengumpulan dan pengolahan data, ekstraksi fitur, pembuatan model, uji coba model, hingga analisa dan pengujian model.

BAB IV HASIL DAN ANALISIS

Bab keempat akan menjelaskan hasil dari pengujian serta analisis terhadap hasil yang diperoleh serta proses validasi terhadap model. Model terbaik akan diterapkan menjadi NIDS.

BAB V KESIMPULAN DAN SARAN

Bab terakhir akan berisi kesimpulan dan saran penulis dari hasil dan analisa dari penelitian yang telah dilakukan.

DAFTAR PUSTAKA

[1] I. Riadi, D. Aprilliansyah, and S. Sunardi, “Mobile Device Security Evaluation using Reverse TCP Method,” *Kinet. Game Technol. Inf. Syst. Comput. Netw. Comput. Electron. Control*, Sep. 2022, doi: 10.22219/kinetik.v7i3.1433.

[2] “Mobile Statistic 2021-2025,” The Radicati Group, Inc, Jan. 2021. Accessed: Oct. 23, 2023. [Online]. Available: https://www.radicati.com/?p=17218

[3] Y. S. I. Hamed, S. N. A. AbdulKader, and M.-S. M. Mostafa, “Mobile Malware Detection: A Survey,” vol. 17, no. 1, 2019.

[4] J. Zhou, W. Niu, X. Zhang, Y. Peng, H. Wu, and T. Hu, “Android Malware Classification Approach Based on Host-Level Encrypted Traffic Shaping,” in *2020 17th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*, Chengdu, China: IEEE, Dec. 2020, pp. 246–249. doi: 10.1109/ICCWAMTIP51612.2020.9317429.

[5] M. F. A. H. Kamal, I. R. A. Hamid, N. Abdullah, Z. Abdullah, M. Ahmad, and W. M. Shah, “Android Botnet Detection Based on Network Analysis Using Machine Learning Algorithm,” in *Recent Advances in Soft Computing and Data Mining*, vol. 457, R. Ghazali, N. Mohd Nawi, M. M. Deris, J. H. Abawajy, and N. Arbaiy, Eds., in Lecture Notes in Networks and Systems, vol. 457. , Cham: Springer International Publishing, 2022, pp. 282–291. doi: 10.1007/978-3-031-00828-3_28.

[6] M. Gohari, S. Hashemi, and L. Abdi, “Android Malware Detection and Classification Based on Network Traffic Using Deep Learning,” in *2021 7th International Conference on Web Research (ICWR)*, Tehran, Iran: IEEE, May 2021, pp. 71–77. doi: 10.1109/ICWR51868.2021.9443025.

[7] S. D. Azmi, S. Deris, and S. Tata, “Implementasi Sistem Deteksi Ransomware Menggunakan Deep Packet Inspection pada Layanan SMK Negeri 1 Palembang,” vol. 1, no. 2, 2023.

[8] “Laporan Bulanan Publik Agustus 2023,” Badan Siber dan Sandi Negara, Agustus 2023. [Online]. Available: https://cloud.bssn.go.id/s/GgpKGGGSDzLE5go

[9] A. Lekssays, B. Falah, and S. Abufardeh, “A Novel Approach for Android Malware Detection and Classification using Convolutional Neural Networks:,” in *Proceedings of the 15th International Conference on Software Technologies*, Lieusaint - Paris, France: SCITEPRESS - Science and Technology Publications, 2020, pp. 606–614. doi: 10.5220/0009822906060614.

[10] R. Satrio Hadikusuma, L. Lukas, and E. M. Rizaludin, “Methods of Stealing Personal Data on Android using a Remote Administration Tool with Social Engineering Techniques,” *Ultim. J. Tek. Inform.*, pp. 44–49, Jun. 2023, doi: 10.31937/ti.v15i1.3122.

[11] R. D. Putra and I. Mardianto, “Exploitation with Reverse_tcp Method on Android Device using Metasploit,” *J. Edukasi Dan Penelit. Inform. JEPIN*, vol. 5, no. 1, p. 106, Apr. 2019, doi: 10.26418/jp.v5i1.26893.

[12] W. Waheed and H. Alyasiri, “Evolving trees for detecting android malware using evolutionary learning,” *Int. J. Nonlinear Anal. Appl.*, no. Online First, Sep. 2022, doi: 10.22075/ijnaa.2022.6874.

[13] C. Liu, Z. Gu, and J. Wang, “A Hybrid Intrusion Detection System Based on Scalable K-Means+ Random Forest and Deep Learning,” *IEEE Access*, vol. 9, pp. 75729–75740, 2021, doi: 10.1109/ACCESS.2021.3082147.

[14] L. Taheri, A. F. A. Kadir, and A. H. Lashkari, “Extensible Android Malware Detection and Family Classification Using Network-Flows and API-Calls,” in *2019 International Carnahan Conference on Security Technology (ICCST)*, CHENNAI, India: IEEE, Oct. 2019, pp. 1–8. doi: 10.1109/CCST.2019.8888430.

[15] S. Rahmat, Q. Niyaz, A. Mathur, W. Sun, and A. Y. Javaid, “Network Traffic-Based Hybrid Malware Detection for Smartphone and Traditional Networked Systems,” in *2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, New York City,

NY, USA: IEEE, Oct. 2019, pp. 0322–0328. doi: 10.1109/UEMCON47517.2019.8992934.

[16] V. S. Devi, S. Roopak, T. Thomas, and Md. M. Uddin, "Multi-Pattern Matching Based Dynamic Malware Detection in Smart Phones," in *Energy Efficient Computing & Electronics*, 1st ed., K. Iniewski, S. K. Kurinec, and S. Walia, Eds., Boca Raton : CRC/Taylor & Francis, [2019] | Series: Devices, circuits, & systems: CRC Press, 2019, pp. 421–441. doi: 10.1201/9781315200705-15.

[17] "What Is a Trojan Horse? Trojan Virus and Malware Explained," Fortinet. Accessed: Nov. 07, 2023. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/trojan-horse-virus

[18] A. Krishna, A. Lal M.A., A. J. Mathewkutty, D. S. Jacob, and M. Hari, "Intrusion Detection and Prevention System Using Deep Learning," in *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)*, Coimbatore, India: IEEE, Jul. 2020, pp. 273–278. doi: 10.1109/ICESC48915.2020.9155711.

[19] U. S. Musa, M. Chhabra, A. Ali, and M. Kaur, "Intrusion Detection System using Machine Learning Techniques: A Review," in *2020 International Conference on Smart Electronics and Communication (ICOSEC)*, Trichy, India: IEEE, Sep. 2020, pp. 149–155. doi: 10.1109/ICOSEC49089.2020.9215333.

[20] L. Ashiku and C. Dagli, "Network Intrusion Detection System using Deep Learning," *Procedia Comput. Sci.*, vol. 185, pp. 239–247, 2021, doi: 10.1016/j.procs.2021.05.025.

[21] Z. Kanmai, "TCP/IP Protocol Security Problems and Defenses," in *2020 International Conference on Intelligent Computing and Human-Computer Interaction (ICHCI)*, Sanya, China: IEEE, Dec. 2020, pp. 117–120. doi: 10.1109/ICHCI51889.2020.00033.

[22] K. H. Rahouma, M. S. Abdul-Karim, and K. S. Nasr, "TCP/IP Network Layers and Their Protocols (A Survey)," in *Internet of Things—Applications and Future*, vol. 114, A. Z. Ghalwash, N. El Khameesy, D. A. Magdi, and A. Joshi,

Eds., in Lecture Notes in Networks and Systems, vol. 114. , Singapore: Springer Singapore, 2020, pp. 287–323. doi: 10.1007/978-981-15-3075-3_21.

[23] “An Inside Look at TCP Headers and UDP Headers,” Lifewire. Accessed: Nov. 12, 2023. [Online]. Available: https://www.lifewire.com/tcp-headers-and-udp-headers-explained-817970

[24] Y. Liu, R. Cai, X. Yin, and S. Liu, “An Exploit Traffic Detection Method Based on Reverse Shell,” *Appl. Sci.*, vol. 13, no. 12, p. 7161, Jun. 2023, doi: 10.3390/app13127161.

[25] Y. Kolli, T. K. Mohd, and A. Y. Javaid, “Remote Desktop Backdoor Implementation with Reverse TCP Payload using Open Source Tools for Instructional Use”.

[26] T. Yu, F. Zou, L. Li, and P. Yi, “An Encrypted Malicious Traffic Detection System Based on Neural Network,” in *2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, Guilin, China: IEEE, Oct. 2019, pp. 62–70. doi: 10.1109/CyberC.2019.00020.

[27] N. K. Zuin, Eugene, and V. Selvarajah, “A Case Study: SYN Flood Attack Launched Through Metasploit:,” presented at the 3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021), Bangalore, India, 2021. doi: 10.2991/ahis.k.210913.065.

[28] A. Banik and J. P. Singh, “Android Malware Detection by Correlated Real Permission Couples Using FP Growth Algorithm and Neural Networks,” *IEEE Access*, vol. 11, pp. 124996–125010, 2023, doi: 10.1109/ACCESS.2023.3323845.

[29] “FAQ | Apktool.” Accessed: Jan. 10, 2024. [Online]. Available: https://apktool.org/docs/faq

[30] J. L. J. Pandari and W. Sulistyo, “IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) UNTUK MENDETEKSI SERANGAN METASPLOIT EXPLOIT MENGGUNAKAN SNORT DAN WIRESHARK”.

[31] Z. Zhou and T. Huang, “Open VPN Application Under Campus Network,” *J. Phys. Conf. Ser.*, vol. 1865, no. 4, p. 042014, Apr. 2021, doi: 10.1088/1742-6596/1865/4/042014.

[32] “What Is A VPN? | VPN Definition,” OpenVPN. Accessed: Jan. 11, 2024. [Online]. Available: https://openvpn.net/what-is-a-vpn/

[33] M. Y. Sediqy, M. Hakimollahi, and M. M. Tehrani, “Preventing DoS, Brute Force and winbox exploit attack against Mikrotik Router,” vol. 12, no. 1, 2023.

[34] “Termux.” Accessed: Jan. 11, 2024. [Online]. Available: https://github.com/termux

[35] W. A. Ningrum and I. Mubarok, “PENGUJIAN KEAMANAN BASIS DATA SISTEM INFORMASI BERBASIS WEB,” 2021.

[36] E. Faranda, “emanuele-f/PCAPdroid.” Jan. 10, 2024. Accessed: Jan. 12, 2024. [Online]. Available: https://github.com/emanuele-f/PCAPdroid

[37] N. A. L. Mabsali, H. Jassim, and J. Mani, “Effectiveness of Wireshark Tool for Detecting Attacks and Vulnerabilities in Network Traffic,” in *Proceedings of the 1st International Conference on Innovation in Information Technology and Business (ICIITB 2022)*, N. Bacanin and H. Shaker, Eds., Dordrecht: Atlantis Press International BV, 2023, pp. 114–135. doi: 10.2991/978-94-6463-110-4_10.

[38] “Applications | Research | Canadian Institute for Cybersecurity | UNB.” Accessed: Nov. 30, 2023. [Online]. Available: https://www.unb.ca/cic/research/applications.html

[39] G. Lv, R. Yang, Y. Wang, and Z. Tang, “Network Encrypted Traffic Classification Based on Secondary Voting Enhanced Random Forest,” in *2020 IEEE 3rd International Conference on Computer and Communication Engineering Technology (CCET)*, Beijing, China: IEEE, Aug. 2020, pp. 60–66. doi: 10.1109/CCET50901.2020.9213165.

[40] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi, and R. Ahmad, “Machine Learning and Deep Learning Approaches for CyberSecurity: A Review,” *IEEE Access*, vol. 10, pp. 19572–19585, 2022, doi: 10.1109/ACCESS.2022.3151248.

[41] H. Liu and B. Lang, “Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey,” *Appl. Sci.*, vol. 9, no. 20, p. 4396, Oct. 2019, doi: 10.3390/app9204396.

[42] M. A. Kazi, S. Woodhead, and D. Gan, “An Investigation to Detect Banking Malware Network Communication Traffic Using Machine Learning Techniques,” *J. Cybersecurity Priv.*, vol. 3, no. 1, pp. 1–23, Dec. 2022, doi: 10.3390/jcp3010001.

[43] M. Haddouchi and A. Berrado, “A survey of methods and tools used for interpreting Random Forest,” in *2019 1st International Conference on Smart Systems and Data Science (ICSSD)*, Rabat, Morocco: IEEE, Oct. 2019, pp. 1–6. doi: 10.1109/ICSSD47982.2019.9002770.

[44] A. Parmar, R. Katariya, and V. Patel, “A Review on Random Forest: An Ensemble Classifier,” in *International Conference on Intelligent Data Communication Technologies and Internet of Things (ICICI) 2018*, vol. 26, J. Hemanth, X. Fernando, P. Lafata, and Z. Baig, Eds., in Lecture Notes on Data Engineering and Communications Technologies, vol. 26. , Cham: Springer International Publishing, 2019, pp. 758–763. doi: 10.1007/978-3-030-03146-6_86.

[45] B. A. Pratomo, P. Burnap, and G. Theodorakopoulos, “BLATTA: Early Exploit Detection on Network Traffic with Recurrent Neural Networks,” *Secur. Commun. Netw.*, vol. 2020, pp. 1–15, Aug. 2020, doi: 10.1155/2020/8826038.

[46] D. S. Deris Stiawan, D. W. Deris Stiawan, T. W. S. Dimas Wahyudi, M. Y. I. Tri Wanda Septian, and R. B. Mohd Yazid Idris, “The Development of an Internet of Things (IoT) Network Traffic Dataset with Simulated Attack Data,” 網際網路技術學刊, vol. 24, no. 2, pp. 345–356, Mar. 2023, doi: 10.53106/160792642023032402013.

[47] A. Rhohim, V. Suryani, and M. A. Nugroho, “Denial of Service Traffic Validation Using K-Fold Cross Validation on Software Defined Network”.

[48] T. Emmanuel, T. Maupong, D. Mpoeleng, T. Semong, B. Mphago, and O. Tabona, “A survey on missing data in machine learning,” *J. Big Data*, vol. 8, no. 1, p. 140, Oct. 2021, doi: 10.1186/s40537-021-00516-9.

[49] T. Wongvorachan, S. He, and O. Bulut, “A Comparison of Undersampling, Oversampling, and SMOTE Methods for Dealing with Imbalanced Classification in Educational Data Mining,” *Information*, vol. 14, no. 1, p. 54, Jan. 2023, doi: 10.3390/info14010054.

[50] A. Muzaffar, H. Ragab Hassen, M. A. Lones, and H. Zantout, “An in-depth review of machine learning based Android malware detection,” *Comput. Secur.*, vol. 121, p. 102833, Oct. 2022, doi: 10.1016/j.cose.2022.102833.