

Dakshitha Navodya Perera

Email: d42kw01f@gmail.com

Website: d42kw01f.com

LinkedIn: [linkedin.com/in/dakshitha-navodya-170141198](https://www.linkedin.com/in/dakshitha-navodya-170141198)

GitHub: github.com/d42kw01f

Professional Summary

Cyber Security Engineer with experience in malware reverse engineering, penetration testing, web application development, and artificial intelligence projects. Passionate about learning and implementing new technologies to address complex challenges in the cybersecurity landscape. Committed to enhancing organizational security through innovative solutions and continuous professional development.

Education

Bachelor of Science in Cyber Security

Edith Cowan University, Perth, Australia | 2019 - 2022

- GPA: 3.84 | WAM: 84.38
- Awards: ECU Gold Medal for Cyber Security 2022
- **Relevant Coursework**
 - Ethical Hacking and Defence
 - Software Reverse Engineering
 - Network Security Fundamentals

Advanced Level – Science (Physics, Chemistry, Biology)

Nalanda College, Colombo, Sri Lanka

Ordinary Level

Nalanda College, Colombo, Sri Lanka

Experience

IT Operations and Security Specialist

The Software Practice Pte Ltd, Singapore (Remote) | October 2022 – Present

- Built and managed the company's IT infrastructure from the ground up, delivering secure, scalable systems.
- Performed penetration testing and security assessments on internal and client-facing applications.
- Developed internal IT operations and applications
 - Example: Internal Access Management: using C#, TypeScript, Python, Go, Nuxt.js, Tailwind CSS, and Firebase.
- Deployed and administered Microsoft Intune organization-wide to strengthen endpoint management and security.
- Designed and implemented secure VPN solutions to support reliable remote access.
- Managed and monitored self-hosted services
 - Including GitLab, YouTrack, Bitwarden, mail servers, and Pritunl VPN with centralized logging and monitoring.
- Automated operational workflows and integrated APIs with Git, YouTrack, SonarQube, and Pritunl to improve efficiency.
- Supported information security compliance initiatives (e.g., DPTM), contributed to security policies, and delivered cybersecurity awareness programs.
- Provided technical support and collaborated across teams to align IT operations with business objectives.

Skills

- **Programming Languages:** Python, Bash, PowerShell, C++, TypeScript
- **Version Control:** Git, GitHub, GitLab
- **Databases:** MySQL, PostgreSQL
- **Development Tools and Others:** HTML5, CSS3, Docker, Kubernetes

Technical Skills:

- **Operating Systems:** *Linux (Arch, Gentoo, Debian) with 9 years of experience, Windows OS*
- **Programming Concepts:** *Algorithms, Data Structures*
- **Networking:** *TCP/IP*
- **Cloud Computing:** *AWS, Azure, GCP*
- **Penetration Testing:**
 - **Information Gathering:** *OSINT, Google Hacking, DNS Enumeration, Port Scanning, SMB Enumeration, SMTP Enumeration, SNMP Enumeration*
 - **Web Application Attacks:** *XSS, LFI/RFI, SQL Injection*
 - **Exploits:** *Buffer Overflows (Windows/Linux), Client-Side Attacks (Macros), Antivirus Evasion*
- **Active Directory:**
 - *Enumeration, Attacks, Lateral Movements, Persistence*

Tools & Libraries:

- **Python Libraries:** *NumPy, Pandas, TensorFlow, PyTorch, Keras, Scikit-Learn*
- **Reverse Engineering Tools:** *IDA Pro, Ghidra, Radare2, OllyDBG*
- **Penetration Testing Tools:** *NetCat, Socat, Powercat, Burp Suite, Wireshark, Nmap, Impacket Tools, Gobuster, HashCat*
- **Security Platforms:** *ELK Stack (Elasticsearch), Splunk, QRadar*
- **Data Analysis Tools:** *R Studio (tidyverse, ggplot2)*
- **Virtualization:** *VMware, VirtualBox*
- **Penetration Testing Distributions:** *BlackArch, Kali Linux, Parrot OS*

Other Skills:

- Strong troubleshooting and analytical problem-solving abilities
- Detail-oriented and methodical approach
- Fast learner and hardworking
- Leadership and interpersonal skills
- Excellent report writing and communication skills
- Fluent in English

Personal Projects

Predict Election based on Social Media Content Analysis Using AI

- Built an automated web scraping system using Puppeteer and TypeScript to collect large-scale Facebook post data, handling multiple layout variations.
- Developed a Python-based machine learning model with NLP techniques to classify political and non-political content and analyze sentiment.
- Implemented a secondary data collection pipeline to extract engagement metrics (reactions, shares, comments) for political posts.
- Designed a weighted scoring algorithm to rank posts based on engagement and sentiment to assess influence.
- Architected and managed MongoDB schemas (Post, FullPost, PoliticalPost) for structured data processing.
- Developed an interactive web dashboard using Nuxt.js and Tailwind CSS for data visualization and exploration.
- Integrated a Flask-based backend using RESTful APIs to automate data processing, classification, and storage.

Technology Stack: Puppeteer, TypeScript, Python, MongoDB, Nuxt.js, Tailwind CSS, Flask, Natural Language Processing (NLP), Machine Learning, Data Visualization.

Source Code: <https://github.com/d42kw01f/s0m3m0>

Candidates Classification Model: https://huggingface.co/d42kw01f/the_candi

Political Classification Model: https://huggingface.co/d42kw01f/the_poli

Tools and Techniques to Combat Cyber Radicalization in Sri Lanka

- Developed a radicalization analysis system using NLP, deep learning, and traditional machine learning techniques with Python and PyTorch.
- Built and curated real-world datasets of radicalized and non-radicalized content by scraping blogs, deep websites, and social media platforms (Twitter, Reddit, YouTube).
- Implemented a deep learning-based image analysis component to detect radicalized images shared online.
- Created an interactive Streamlit dashboard to visualize analysis results and support informed decision-making.

Sinhala and Tamil *RoBERTa* Model

- Developed a pre-trained RoBERTa model for the Sinhalese language using Masked Language Modeling (MLM).
- Trained on the OSCAR Sinhala dataset to enhance NLP tasks in the Sinhala language.

Sinhala RoBERTa Model: <https://huggingface.co/d42kw01f/Sinhala-RoBERTa>

Tamil RoBERTa Model: <https://huggingface.co/d42kw01f/Tamil-RoBERTa>

Certifications and Licenses

- Offensive Security Certified Professional (OSCP) – Pursuing
 - Student ID: OS-55686
 - C/C++ Programming – Esoft Metro Campus (Colombo)
-

Professional Profiles

- **Kaggle:** kaggle.com/d42kw01f
- **Hugging Face:** huggingface.co/d42kw01f
- **Hack The Box:** hackthebox.com/profile/d42kw01f
- **TryHackMe:** tryhackme.com/p/d42kw01f

I confirm that the above information is true and correct to the best of my knowledge.