Dakshitha Navodya Perera

Email: dakshitha@d42kw01f.com
Phone: +94 766 326 903
Website: d42kw01f.github.io
LinkedIn: 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: 3.875 | WAM: 84.75
- Awards: ECU Gold Medal for Cyber Security 2022
- Relevant Coursework
  - Data Analysis and Visualization
  - Ethical Hacking and Defense
  - Software Reverse Engineering
  - Cryptographic Concepts
  - Cyber Security Incident Detection and Response
  - Network Security Fundamentals
  - Information Security
  - Enterprise Security and Governance

Transcript | Certificate | AHEGS

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

- IT Infrastructure Development:
  - Established the company's IT infrastructure from the ground up, collaborating with seasoned professionals to ensure robust and scalable systems.
  - Developed IT operations software and applications, including laptop management apps and Identity and Access Management (IAM) solutions.
  - Utilized technologies such as C#, TypeScript, Python, Go, Nuxt.js, Tailwind CSS, and Firebase to create efficient and user-friendly applications.
  - Deployed Microsoft Intune organization-wide, enhancing device management and security across the company.
  - VPN Setup Project:
    - Served as a key member of the VPN setup project team, ensuring secure and reliable remote access for all employees.
    - Collaborated with cross-functional teams to design and implement VPN solutions that meet organizational security standards.
- Special Security Tasks:
  - Assisted in performing penetration tests on applications and features developed by other project teams for the organization's clients, ensuring comprehensive security assessments and enhancing overall application security.
- Server Management and Monitoring:
  - Managed and monitored self-hosted servers like GitLab, YouTrack, VaultWarden, Mail Servers, and Pritunl VPN.
  - Implemented real-time monitoring systems to track server performance and security metrics.
  - Monitored and maintained the security of data, VPN, network logs, and server logs to ensure compliance and protect against threats.
- Automation and Deployment:

    - Automated various operational tasks and deployed them on the cloud, improving efficiency and reducing manual workload.
    - Developed and integrated APIs with tools such as Git, YouTrack, SonarQube, and Pritunl to streamline processes and enhance functionality.
- Security and Compliance:
    - Facilitated the company's journey to attain esteemed information security certifications like DPTM, strengthening its credibility.
    - Assisted in creating security and data protection policies, asset identification and protection strategies, and conducted cybersecurity awareness programs for employees.
- Technical Support and Collaboration:
    - Provided desk support to employees, resolving both software and hardware-related issues promptly.
    - Collaborated with cross-functional teams to align IT operations with business objectives and enhance overall productivity.

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 – Source Code

- Automated Data Scraping:
    - Developed a web scraper using Puppeteer and TypeScript to automatically collect bulk posts and data from Facebook user profiles and pages.
    - Implemented custom scraping strategies to handle different Facebook layouts and content structures, ensuring data consistency and accuracy.
- Political Content Detection:
    - Designed a machine learning model using Python to classify posts as political or non-political based on the content.
    - Leveraged natural language processing (NLP) techniques to analyze post text and detect keywords and sentiment indicative of political or radical content.
- Advanced Data Scraping for Detailed Analysis:

    - If a post was identified as political, a secondary scraping phase was initiated to gather detailed post information such as reactions, shares, comments, and additional content.
    - Extracted and parsed user comments, reactions, and other engagement metrics to enrich the dataset.
- Weight Score Calculation:
    - Developed a weight scoring algorithm to rank political posts based on engagement metrics like reactions, shares, and comment sentiment.
    - Used the calculated weight scores to assess the potential influence of each political post.
- Database Design and Management:
    - Built a MongoDB database schema to store and organize scraped data, processed results, and weight scores.
    - Designed three main schemas: Post, FullPost, and PoliticalPost to handle different stages of the data processing pipeline.
- Data Visualization:
    - Created a web application using Nuxt.js, TypeScript, and Tailwind CSS to visualize the results and provide insights into political trends and social media activity.
    - Enabled interactive data exploration and filtering, allowing users to view political content rankings and engagement statistics.
- Backend Integration:
    - Connected the backend API (built with Flask and Python) to the web scraper and machine learning model for seamless data flow and automation.
    - Used RESTful APIs to send scraped data to the backend for processing, classification, and storage.
- Technology Stack: `Puppeteer, TypeScript, Python, MongoDB, Nuxt.js, Tailwind CSS, Flask, Natural Language Processing (NLP), Machine Learning, Data Visualization.`

Tools and Techniques to Combat Cyber Radicalization in Sri Lanka

- Radicalization Analyzer:
    - Developed a sentiment analysis tool using Natural Language Processing (NLP) techniques, deep learning, and conventional machine learning.
    - Utilized Python and PyTorch to analyze text data for signs of radicalization.
- Data Scraping and Mining:

    - Created a real-world dataset comprising radicalized and non-radicalized posts and comments.
    - Scraped data from normal blogging sites, deep websites, and social media platforms like Twitter, Reddit, and YouTube.
- Radicalized Image Detection Tool:
    - Employed image processing techniques with deep learning to detect radicalized images being shared online.
- Data Visualization:
    - Built an interactive website using Streamlit to visualize data and analysis results, aiding in better understanding and decision-making.

Sinhala and Tamil `RoBERTa` Model - 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.

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.