Charitha Jayasinghe

+94 71 536 6314 charithnuwan054@gmail.com charith-jayasinghe Nuwan-droid charithanuwan.me

Education

Bachelor of Science (Honors) in Computer Science and Technology **2022 – Present**
Uva Wellassa University of Sri Lanka *CGPA: 3.36 / 4.0*

Research

GANs-Based Data Augmentation for Multiclass Intrusion Detection in AG-IoT **Nov 2025 – Present**

- Developing a lightweight Generative Adversarial Network framework to generate high-quality synthetic attack data for agricultural IoT environments.
- Implementing data augmentation pipeline to mitigate class imbalance in intrusion detection datasets and evaluate IDS performance metrics.

Projects

Building a Honeypot | *Python, Docker, Ubuntu Server, Networking* **Sep 2025**

- Deployed an SSH honeypot using Docker containers to capture and log unauthorized access attempts in isolated environment.
- Configured network monitoring and logging systems to analyze attacker behavior patterns and common exploitation techniques.
- Documented attack vectors, IP addresses, and payloads for threat intelligence gathering and security research.

File Integrity Monitor | *Python, Hashlib, SQLite, Linux, Logging* **Jul 2025**

- Developed a Python file-integrity monitoring tool using SHA-256 hashing to detect unauthorized file modifications.
- Implemented baseline creation, automated change detection, and continuous file monitoring with SQLite database backend.
- Added logging and real-time alerting for suspicious modifications, validated on Linux systems for accuracy and performance.

Active Directory Automation | *PowerShell, Active Directory, Windows Server* **May 2025**

- Automated user and group management in Active Directory using PowerShell scripts to reduce manual administrative overhead.
- Implemented bulk user provisioning, password resets, and organizational unit structuring workflows.
- Streamlined AD administrative tasks on Windows Server, improving efficiency and reducing configuration errors.

Malware Analysis Lab | *VirtualBox, Wireshark, Process Monitor, Cuckoo* **Mar 2025**

- Built an isolated malware analysis environment with Windows and Linux VMs using VirtualBox and REMnux distribution.
- Analyzed malware behavior, network communications, and system interactions using Wireshark, Process Monitor, and Cuckoo Sandbox.
- Documented indicators of compromise (IoCs), attack patterns, and malware signatures while maintaining secure handling procedures.

Technical Skills

Programming Languages: Python, JavaScript, Bash, PowerShell
Security Tools: Wireshark, Nmap, Metasploit, Burp Suite, Cuckoo Sandbox
Operating Systems: Kali Linux, Ubuntu Server, Windows Server, Windows
Networking: TCP/IP, DNS, Firewalls, VPNs, Network Security
Cloud Platforms: Microsoft Azure
Version Control: Git, GitHub
Web Technologies: React, Node.js, Express.js, MongoDB
Cybersecurity: Intrusion Detection, Malware Analysis, SOAR/EDR, Active Directory

Certifications

- Junior Cybersecurity Analyst | Cisco Networking Academy | In Progress
- Cybersecurity Essentials | Cisco Networking Academy | 2025
- TryHackMe Cyber Security Pathway | In Progress
- Python Essentials 1 & 2 | Cisco Networking Academy | 2025
- JavaScript Essentials 1 | Cisco Networking Academy | 2025