

Anjula Meegalla

Cybersecurity UG

Enthusiastic Cybersecurity undergraduate with a focus on practical security domains including Security Operations (SecOps), Active Directory, Linux Administration, and OSINT.

✉ anjulameegalla@gmail.com

☎ +94 77 994 6869

🌐 www.anjula.live

🌐 [Anjula Meegalla](#)

📄 [Anjula M.](#)

Education

SLTMobitel Nebula Institute Of Technology

BTEC HND in Digital Technologies (Cyber Security)

📍 Welisara, Sri Lanka 2024 - Present

Nalanda College

G.C.E Advanced Level (Physical Science)

📍 Colombo, Sri Lanka 2024

Technical Skills

Security Operations & Tooling

SIEM (Wazuh/ Microsoft Sentinel)

EDR & Threat Mgmt Log Analysis (KQL)

Wireshark BurpSuite Nmap Nessus

Docker Git OWASP Top10

SysAdmin & Networking

Windows Active Directory Azure Entra ID

Linux Server Administration Windows Svr

Virtualization (VMWare) Cisco

Scripting & Automation

Python Powershell Bash Ansible

Professional Skills

Security Documentation Incident Ticketing

IT Help Desk Analytical Thinking

Certifications

RedHat Certified System Administrator (RHCSA) - Reading

CWL Certified Red Team Analyst (CRTA)

Microsoft Certified: Azure Fundamentals (AZ-900)

Microsoft Certified: Azure AI Fundamentals (AI-900)

Hobbies

Gaming

Chess

Songwriting

Badminton

Professional Experience

Sri Lanka Telecom

Internship Trainee

📍 Colombo, Sri Lanka

Aug 2024 - Oct 2024

Customer Support Data Entry Corporate Environment

- Gained professional exposure in a corporate environment, handling data entry, customer interactions, and sales support functions.
- Demonstrated strong communication and teamwork skills through direct engagement with customers and collaboration with internal teams.

Personal Projects

Wazuh Threat Detection Lab

🔗 [GitHub repo](#)

Wazuh SIEM TDR Windows Ubuntu

- Implemented a Wazuh SIEM solution to monitor endpoint security across Windows and Ubuntu agents, ensuring multi-channel alerting for critical events.
- Simulated intrusion attempts to validate detection rules, investigating findings through real-time log analysis and incident triage.

Windows Active Directory Lab

🔗 [GitHub repo](#)

Active Directory Azure AD DS AD CS Security Hardening

- Established a comprehensive Azure-based Windows AD lab (AD DS, AD CS) to replicate an enterprise environment and configure domain service accounts.
- Utilized the environment to test security policies and hardening techniques against common Active Directory vulnerabilities and simulated attack vectors.

Security Automation Lab

🔗 [GitHub repo](#)

SOAR EDR Incident Response Windows Server Endpoint Isolation

- Developed an automated SOAR workflow to detect credential dumping on Windows Server, utilizing real-time alerting to trigger immediate endpoint isolation.
- Successfully demonstrated automated incident escalation and analysis, effectively minimizing response times and mirroring core security team workflows.

Azure Honeypot & Log Analysis Lab

🔗 [GitHub repo](#)

Azure Microsoft Sentinel KQL Powershell Threat Intel

- Deployed an Azure honeypot to capture malicious RDP traffic, utilizing custom PowerShell scripts to automate threat intelligence gathering and attacker geolocation.
- Leveraged Microsoft Sentinel and KQL to analyze network logs, identify global attack patterns, and visualize threat data for documentation.

IT Help Desk & Documentation Lab

🔗 [GitHub repo](#)

Ticketing System Documentation ITIL Incident Management MySQL

- Implemented a Spiceworks-based ticketing system to manage the full lifecycle of IT support requests, from initial logging to resolution.
- Documented technical findings and escalation procedures for simulated incidents, mirroring standard ITIL-based service desk operations.

Activites & Societies

- Treasurer – Student Committee, BTEC DT 24/26, SLTM Nebula Institute of Technology (2024/26)
- Secretary – Scrabble Club, Nalanda College (2020/21)