MALISHA RASIRU

Security + | (ISC)² - CC | Cyber Security

About Me

I am third year undergraduate pursuing a BSc (Hons) Degree in Information Technology Specializing in cyber security and eager to leverage my expertise in endpoint security, risk management, and ethical hacking to address real-world challenges. By proactively identifying and investigating security vulnerabilities, I aim to support enterprises in strengthening their defenses and safeguarding against potential threats.

☎ +94783407661 / +94714312730

✉ malisharasiru@gmail.com

⌂ Malabe, Colombo, SriLanka

in https://www.linkedin.com/in/malisha-rasiru

https://medium.com/@malishakali2002

https://github.com/Malisha-Kali

SKILLS

- Troubleshooting
- Incident Response
- Malware Analysis
- Penetration Testing
- Reverse Engineering
- Leardership
- Presenting
- Critical Thinking & Problem Solving

EXPERIENCE

Intern - Trainee Technical Support Engineer
Sanfer Technologies (Pvt) Ltd May 2024 - Present
Subsidiary of **South Asian Technologies** pvt ltd (**SAT**)

- Deployed and configured **CrowdStrike** Falcon Endpoint Protection across enterprise environments, including modules like NGAV, EDR, NG-SIEM, ITDR, and Data Protection.
- Integrated third-party data sources to NG-SIEM for improved threat detection and response.
- Troubleshoot issues and provided technical support to customers/partners.
- Created RFP technical proposals and performed health checks of the Falcon platform, to ensure customers had optimal protection.
- Implemented response actions from CrowdStrike Fusion SOAR Workflows to automate remediation and enhance incident handling.
- Collaborated with teams to align security solutions and provided tailored solutions for customer use cases.

- Manage **Forcepoint** DLP policies and settings to prevent data exfiltration, ensuring compliance with data protection standards, while providing support for Forcepoint Endpoint installations and configurations.

PROJETCTS (CYBER SECURITY RELATED)

- **MEDUSA 1.0 CTF Challenge Development- University of Kelaniya 2024**

Developed the 'Forgot That' Medusa 1.0 CTF challenge, incorporating port scanning, Local File Inclusion (LFI) exploitation, bypassing SSH with a knock sequence, and password cracking using the rockyou.txt wordlist. I have created a complete bash script to automate the challenge deployment on a fresh Ubuntu server.

Medium Writeup **Automated Script**

CYBER SECURITY TOOLS

- Burpsuit pro
- Nessus
- Wireshark
- Nmap
- Gobuster
- Nikto
- Metasploit Framework
- Python/C/bash/Java/Solidity

FRAMEWORKS AND STANDARDS

- Familiar with ISO 27001 framework
- HIPAA, PCI DSS, PDPA

EDUCATION

July 2022 - 2026
BSc (Hons) in Information Technology
Specialization in Cybersecurity
Sri Lanka Institute of Information Technology

2019 - 2021
GCE Advanced Level, Physical Science Stream)
Combined Maths - A
Physics - B
Chemistry - C
Richmond College

LANGUAGE

- English (**Intermidiate**)
- Sinhala (**Fluent**)

REFERENCES

Sanoj Fernando - Cheif Technical Officer
Email : sanoj@sanfer.biz
Phone : +94 71 7545 686

Dr. Lakmal Rupasinghe - (Phd, MBA, CISSP, CISA)
Email : lakmalr@gmail.com
Phone : 0777561061

- **The Hacker's Lair: Challenging Room**

  Developed "The Hacker's Lair: Challenging Room," a cybersecurity training scenario simulating real-world vulnerabilities such as SQL Injection, IDOR, XSS, and command injection in a web application. Participants navigated the fictional hacker group's operations, uncovering evidence and learning to identify and mitigate security threats.

  TryHackMe | CTF | Flask **View Project**

- **Polkit Privilege Escalation Challenge (TryHackMe Room)**

  Created '**Polkit Privilege Escalation Challenge**' on TryHackMe, teaching users about a real-world vulnerability in Polkit's pkexec utility. Demonstrates commitment to cybersecurity education and community engagement

  TryHackMe | Linux | pkexec **View Project**

- **SpamGuardian** (Spam Email Detect System)

  Designed and implemented a Spam Email Detection System utilizing Machine Learning algorithms, enhancing email security and efficiency.

  Python | Machine Learning | **View Project**

CERTIFICATION

FHT 100: Falcon Platform Architecture Overview

CrowdClass Sales Engineering

ITSEC 121: Vulnerability Management Fundamentals

FALCON 115: Create a Falcon Fusion Workflow

Dec 2024: **Google Cloud Certified Professional Cloud Security Engineer**

Apr 2024: **(ISC)² - CC - Certified in Cyber Security**

Apr 2024: **CompTIA Security +** (Reading)

Dec 2023: Cisco's Ethical Hacker course, covering Cloud Security, Penetration Testing, and Ethical Hacking skills.

Mar 2024: Cisco's Network Defense course, covering Cloud Security and Cryptography skills.

Mar 2024: Cisco's Cyber Threat Management course, focusing on Threat Intelligence skills.

Dec 2023: Cisco's Endpoint Security course, focusing on Network Security and Operating System and Endpoint Security skills.

Mar 2024: Cisco's Introduction to Cybersecurity course, emphasizing Incident Response, Risk Management, and Network Security skills.

Jan 2024: Cybrary's CIS Critical Security Control 3: Data Protection (v8) course.