Liyander Rishwanth L

liyanderrishwanth18@gmail.com 8610164765

3,City Apartments,Thattanvillai Road - 629177,Nagercoil,Tamilnadu Liyander

Liyander Liyander CyberGhost05

ASPIRATION

Cyber Security Engineer with hands-on expertise in Red Teaming, Web Application Security, API pentesting, Malware Analysis, and Adversary Emulation. Proven success in CTF competitions, enterprise-grade security tooling, and responsible vulnerability disclosure across global organizations. Strong background in Linux security, DevSecOps, SOC operations, and AI exploitation.

Professional Experience

CyberSecurity Intern 12/2025

ISRO (Indian Space Research Organisation) Kavalkinaru , TamilNadu

- Conducted security assessments and internal audits
- Performed vulnerability discovery, reporting, and mitigation recommendations
- Worked on system hardening and secure configuration validation
- Contributed to security documentation and incident analysis

EDUCATION

B.Tech in Computer Science and Engineering (Cyber Security) 2023 - 2027

Sri Shakthi Institute of Engineering and Technology coimbatore

cgpa : 8.1

Senior Secondary kanyakumari

St.Joseph Calasanz CBSE School

percentage : 86

Higher Secondary kanyakumari

St.Joseph Calasanz CBSE School

percentage: 95

Awards

Exploit-X Winner - international Hacking Event (CTF)

KPR and EC-Council

HackQuest 2nd Runner-up - National Level Hacking Event (CTF)

JMC and CyberHeals

ACNCTF RunnerUp - National level Hacking Event

Amrita Vishwa Vidyapeetham Chennai

L3m0nCTF Winner - National Level Hacking Event (CTF)

Amrita Vishwa Vidyapeetham Coimbatore

Hard SKILLS

Python | OS | Red-Team Operations | OSINT | Malware Analysis | Security Hardening | Custom Scripts | Web Penetration Testing | Phishing | Security Operations | DevSecOps | Vulnerability Assessment | Javascript | Bash

Key Projects

Star Fighter 08/2025 - 11/2025

Star Fighter is an autonomous AI-powered pentesting agent that can perform complete web penetration tests, detect and fix vulnerabilities, analyze code, generate security reports, solve CTF challenges.

Tech Stack : javascript

Beneficiaries: Penetration Testing requiring manual Testing

Project Status: Deployed and actively improving

Automated CIS Benchmark Auditing Tool (Windows/Linux) 07/2024 - 01/2025

Autonomous auditing scripts developed for both Linux and Windows environments.

Tech Stack: Bash script, PowerShell scripting, PyQt6

Beneficiaries: Tech companies seeking systematized auditing for their internal networks

Project Status: Deployed

Malware Analysis Tool 02/2024 - 05/2024

This is an malware analysis tool engineered to perform a variety of analyses on a given file

Tech Stack: Python, VirusTotal API key

Beneficiaries: Those requiring autonomous static analysis

Project Status: Deployed

BLACKOPS Field Vulnerability Exploiter 06/2024 - 06/2024

A Comprehensive Field Vulnerability Exploiter for Ethical Hacking and CTF Operations

Tech Stack: Python

Beneficiaries: cybersecurity professionals and CTF enthusiasts.

Project Status: Deployed

CyberBytes 04/2025 - 05/2025

Blog Post Site

Tech Stack: MERN

Beneficiaries: CyberBytes is a full-stack blog web application developed for users to create, read, and share blog posts easily. It integrates modern technologies and cloud services for a seamless user experience.

Project Status: Deployed

Red-Vault 07/2025 - 07/2025

Red Vault is a knowledge hub and toolkit reference designed specifically for penetration testers and red teamers.

Tech Stack: HTML , CSS , JS and Markdown

Beneficiaries: Person looking for gaining knowledge about various red teaming tools and techniques.

Certificates

GitHub Advanced Security Certification - GitHub
Skills : Secure Deployment and version control

ODYSSEY - Mini PRO lab - HackTheBox
Skills : VoIP exploitation , source code review , Game Server Exploitation , Kubernetes exploitation

ZEPHYR - PRO Labs - HackTheBox
Skills : Relay attacks , pivoting , certificate attacks , crossing trust boundaries

Practical Web hacking
Skills : Ethical Hacking · Cybersecurity · web hacking · OWASP · Web Application Security Assessment

Web Application Pentesting - Tryhackme
Skills : Web Application Security · web exploitation · Bug Bounty

OSINT - TCM Security
Skills : open source intelligence and recon

Linux Privilege Escalation
Skills : Linux · Penetration Testing

Puppet - Mini PRO labs - HackTheBox
Skills : C2 operations , stealth movement , lateral movement , persistence , situational awareness

HADE - Mini PRO labs - HackTheBox
Skills : Network sniffing , AD attacks , pivoting , lateral movement , Disk backup forensics

Dante - PRO Labs - HackTheBox
Skills : Exploit development , lateral movement , Advanced Web Exploitation

Full house - Mini Pro labs - HackTheBox
Skills : Blockchain Exploitation , AI Exploitation /Bypass

API Penetration Testing - Api university
Skills : API vulnerability assessment

Certified Network Security Practitioner
Skills : Network Security

SOC 101 - TCM Security
Skills : Security Operations , Event Management ,Networking , Anti-phishing , Traffic Analysis , monitering , incident response

DevOps Fundamentals - QA Platform
Skills : DevOps · Amazon Web Services (AWS) · Cloud Computing

Active Directory Labs - HackSmarter
Red Team Operations , Initial Access , Enumeration , Privilege Escalation , Bloodhound Enumeration

XEN - Mini PRO labs - HackTheBox
Skills : Phishing techniques , situational awareness

P.O.O - Mini PRO lab - HackTheBox
Skills : local privilege escalation , web attacks

Cybernetics - PRO Labs - HackTheBox
Skills : DevOps security controls , Evading Enpoint protections , Advanced Exploitation

Junior Penetration Tester - Tryhackme
Skills : Cybersecurity · Web Application Security · Penetration Testing

Practical Windows Forensics - TCM Security
Skills : Windows · Forensic Analysis

Practical API hacking
Skills : Ethical Hacking · Web Application Security · OWASP · Penetration Testing · Web Application Security Assessment

DevOps Playbook - CI/CD Tools and Services - QA Platform
Skills : DevOps · Continuous Integration (CI) · Continuous Delivery (CD) with various tools

achievements

Reported critical security flaws across high-profile organizations including Oxford (SQL Injection), Harvard (XSS), and Princeton (Information Disclosure).

Found new CVE in October CMS (CVE-2025-59540)

Discovered and responsibly disclosed vulnerabilities in Microsoft WSL (RCE) and OctoberCMS (XSS), with CVE applications submitted.

Conducted advanced AI exploitation research, successfully jailbreaking Gemini and Grok, found data exfiltration through RCE via hidden prompt injection in gemini-cli and microsoft copilot and report to google and microsoft

Identified and documented exploits affecting NASA systems, showcasing strong penetration testing and vulnerability research skills.

Reported Critical vulnerabilities like SQLi (Oxford University subdomain) , XSS(Harvard University Main Site), Security misconfiguration(princeton University), XSS(Cambridge University) and LFI (Australian Government)

References

R . Karthiban, *Associate Professor,* Sri Shakthi Institute Of Engineering and Technology
rkarthiban@siet.ac.in

Tools

BurpSuite
Feroxbuster
Shodan
MetaSploit
BloodHound
NetExec
BloodyAD
Certipy-Ad
Empire C2
Covenant C2
Sliver C2
Ligolo-ng
Linpeas
Winpeas
Impacket-Suite
Responder
NTLM theft
Rebeus
MimiKatz
PowerView
Enum4linux
Evilwinrm
Notion
Nuclei
Gophish

Soft Skills

Critical Thinking & Analytical Reasoning
Problem Solving & Attack Surface Reasoning
Attention to Detail & Accuracy
Incident Response Decision-Making
Risk Awareness & Threat Mindset
Structured Documentation & Reporting
Ethical Responsibility & Integrity
Adaptability in High-Pressure Environments