Vishakhan Pillai V P

Kozhikode, Kerala, India | linkedin.com/in/vishakhanpillai | github.com/vishakhanpillai
hackerrank.com/vishakhanpillai

Objective

Aspiring cybersecurity professional with a growing interest in red teaming and offensive security. Currently building hands-on experience in ethical hacking, scripting (Python), and cybersecurity tools. Eager to contribute to real-world security projects and learn from industry professionals.

Hands-On Experience

CTF Player, TryHackMe.com — June 2024 – Present

- Playing Capture the Flag (CTF) challenges to enhance my cybersecurity skills.
- Developing proficiency in network exploitation, web application hacking, cryptography, and system reconnaissance.
- Applying problem-solving and analytical thinking to tackle real-world security scenarios.

Education

Master of Computer Applications (MCA) — Expected: March 2026
Rajagiri College of Social Sciences (Autonomous)

- **Current CGPA - 8.8**

Bachelor of Computer Applications (BCA) — April 2024
St. Joseph's College (Autonomous), Devagiri

- **Graduated with a CGPA of 8.6**

Projects

Red Teaming and Offensive Security Chatbot

- An AI-powered chatbot designed to answer questions related to cybersecurity, red teaming, penetration testing, and offensive security.
- Used **Gradio** for the frontend, **Groq API** for blazing fast LLM responses and **Meta LLaMA 3 (8B)** as the language model behind the chatbot

OpenRecon – Passive Website Reconnaissance Tool

- Developed a Python tool to automate domain information gathering (WHOIS, DNS records, IP resolution, HTTP headers, robots.txt).
- Applied libraries (**requests, dnspython, socket, whois, tldextract**) to implement modular, scalable functions.
- Showcased practical knowledge of passive reconnaissance techniques in cybersecurity.

Keylogger Using Python

- Captured keystrokes using the **pynput** library and logged them with timestamps into daily rotating files to simulate post-compromise monitoring
- Automated email exfiltration of logs every 10 minutes using **smtplib** over SSL and scheduled background tasks with **schedule** and **threading**.
- Designed for stealth and low resource usage, with graceful shutdown handling and empty-log filtering.

Skills

Programming: Python, C, C++, Bash
Cybersecurity: Red Teaming, Nmap, Burp Suite, Metasploit, Gobuster, Dirb, Hydra

Tools/OS: Kali Linux, Ubuntu, Git, Wireshark, VirtualBox, VMWare Workstation

Certifications

Mastercard Cybersecurity Virtual Experience (Forage)

- Designed a phishing email simulation and interpreted results.

Certified Ethical Hacking Associate (Red Team Hacker Academy)

- Gained foundational knowledge in penetration testing, network security, and ethical hacking principles.

Achievements

- **Achieved highest academic distinction as First Semester Topper in the class**
- **Subject Topper in Data Structures Using C**

Workshops

Red Team Hacker Academy - Vulnerable Kochi

- Attended hands-on security workshop on real-world physical access vulnerabilities
- Learned and practiced lock picking techniques on common lock types
- Worked with the Flipper Zero device to emulate RFID/NFC, read/write signals, and analyze wireless protocols

TechySpot - Advanced AI Program

- Participated in hands-on training on applied artificial intelligence and computer vision and Gen AI
- Built custom chatbots using Groq for fast inference and Gradio for interactive UI deployment
- Worked on real-time motion tracking projects using OpenCV and Python

Inspire Software Development - Database Administration Workshop

- Participated in a workshop focused on core concepts of database administration
- Learned about different types of database backups (full, incremental, differential)
- Explored database recovery, user access control, and performance optimization basics