IKRAM CAFFOOR

+94 766720278
ikramcafoorikram@gmail.com
Linkedin Profile
GitHub Profile
Personal Portfolio

Executive Summary

Passionate cybersecurity enthusiast (born 2006) fluent in Linux systems with hands-on practice in penetration testing and CTF challenges. Proficient in Nmap, Burp Suite, Metasploit, Wireshark, Python, and Bash. Skilled in OSINT, vulnerability assessment, and web application security. Currently pursuing advanced cybersecurity studies and available for internships or entry-level roles.

Academic Creditiality

EDITH COWAN UNIVERSITY
Bachelor's of Science (Cyber Security) - In Progress (2025 - 2028)

CICRA CAMPUS
Degree Foundation In Cyber Security - Passed (2025)

ZAHIRA COLLEGE MATALE
G.C.E. Ordinary Level - Passed (2022) / G.C.E. Advanced Level - Candidate (2025)

Skills & Expertise

Tools: Nmap, Burp Suite, Wireshark, Metasploit, Hydra, Netcat, Gobuster, Nikto, HashCat, Etc...

Languages: Python, Bash, HTML, JavaScript , C++, C, Can Understand Others.

Platforms: Hack The Box, TryHackMe, PicoCTF, Kali Linux, Parrot OS, VirtualMechines, Port Swigger

Techniques: Enumeration, OSINT, Web Application Testing, Privilege Escalation, Password Cracking, Reverse Engineering, Etc..

Soft Skills: Critical Thinking, Attention to Detail, Team Collaboration, Fast Learner, Problem Solving, Time Management, Negotiation, Etc..

Hand-On Practice

Hack The Box | CTF Labs
Active Member | 2024 – Present
-Solved various retired and active machines, simulating real-world attack scenarios.
-Demonstrated exploitation techniques including misconfigured services, reverse shells, and kernel exploits.
-Created detailed writeups to document methodologies and post-exploitation steps

TryHackMe | Hands-On Training
Active Participant | 2024 – Present
-Completed multiple rooms focused on enumeration, web exploitation, privilege escalation, and OSINT
-Gained practical skills in Linux, Nmap scanning, password cracking, and LFI/RFI vulnerabilities.
-Applied real-world attack chains in guided and unguided rooms to simulate adversarial behavior.

PortSwigger Web Security Academy
Web Application Security Labs | 2024 – Present
-Completed hands-on labs covering OWASP Top 10 vulnerabilities, including XSS, SQLi, CSRF, IDOR, and more.
-Practiced real-world attack scenarios in a safe environment using Burp Suite.