Keyur Parmar

keyurparmar182003@gmail.com — +91-9023979352 — LinkedIn — TryHackMe

Objective

Cybersecurity postgraduate with hands-on experience in SIEM (Splunk, Wazuh). Skilled in threat detection, incident response, and penetration testing, with practical exposure to real-world attack simulations. Strong background in network traffic analysis and vulnerability assessment using tools such as Wireshark, Metasploit, and Burp Suite for SOC operations and security automation.

Education

Indus University (IU), Ahmedabad — *2024 – Present*
Master of Science in Cyber Security, Aggregate: 10.00 CGPA
Sardar Patel University, V. V. Nagar, Anand — *2021 – 2024*
Bachelor of Computer Applications, Aggregate: 9.00 CGPA

Certifications

- **Certificate in Penetration Testing and Digital Forensics** — Cyber Security India
- **SOC Foundation Training** — Microsoft
- **Digital Forensics Essentials** — Indus University
- **Security Engineer** — Try Hack Me

Technical Skills

Cyber Security Domains: Network Security, Vulnerability Assessment, Penetration Testing, Incident Response, Malware Analysis, OSINT
Technical Tools: Nmap, Metasploit, Burp Suite, Splunk, Wazuh, Wireshark, FTK Imager, Autopsy, Nessus, Hashcat

Projects

SOC Setup

- Implemented a mini SOC environment using Wazuh SIEM, monitoring Windows and Linux endpoints.
- Analyzed and correlated logs to detect security incidents such as brute-force attacks and unauthorized access using MITRE ATTCK.
- Performed alert triage, incident analysis, and documentation of SOC workflows and detection use cases.

NetCrypt – Network Traffic Analyzer & Encrypted Communication Tool
Python, Flask, Scapy, React, Tailwind CSS, SSL/TLS

- Built a tool to simulate and monitor real-time network traffic in SOC-like environments, focusing on detecting insecure communication channels.
- Captured and analyzed over **5,000 network packets**, uncovering **20+ instances** of exposed passwords, API keys, and DNS leaks.

Experience

Cyber Security & Digital Forensics Intern - *CID, Gandhinagar, Gujarat*
Aug 2025 – Nov 2025

- Assisting in ongoing cybercrime investigations and digital evidence analysis.
- Supporting officers in OSINT, social media tracing, and case documentation.
- Learning advanced cyber forensics tools and investigative procedures.

SOC Threat Research Intern - *Hacker4Help*
Dec 2025 – Present

- Operating SOC setup and SIEM tool
- Threat research based on attack
- Managing and alerting AD attacks and their alerts

Extra curricular

Write-ups and blogs — Medium