RASHID

Cybersecurity Analyst

CONTACT

Phone:
+971-55 213 8984

Email Address:
rahsidok.csec@gmail.com

Github
https://github.com/rashid-csec

Linkedin
www.linkedin.com/in/rashid-ok-csec

Website
https://rashid7csec.vercel.app/

Address:
Abu Dhabi, UAE

SOFT SKILLS

- Time management
- Documentation (report writing, analysis)
- Critical thinking during incidents
- Team collaboration
- strong analatycal
- problem solving

TECH SKILLS

- Splunk / ELK / WaZuh
- Snort IDS / Fail2ban
- Nmap / SQLMap / WPScan / Metasploit / Nessus
- Burpsuit / Nessus / OpenVass
- Ubuntu / Kali / Windows

LANGUAGES

- English (Fluent)
- Hindi (Basic)
- Malayalam (Fluent)

PROFILE

Cybersecurity enthusiast with hands-on experience in penetration testing, threat detection, and log analysis. CPT and CSA certified. Built a full IDS/IPS lab using Snort, ELK, and Splunk. Passionate about SOC operations and real-world attack simulation.

EDUCATION

Bachelor of Commerce - in progress 2022 - 2025
IGNOU University | India

National Institute of open school 2021 - 2022
High School Diploma

PROFESSIONAL EXPERIENCE

Cybersecurity Analyst Intern MAY 2025 - JUNE 2025
RedTeam Hacker Academy | Dubai

- Conducted black-box penetration testing and VAPT
- assessments
- Created professional VAPT reports with CVE and MITRE
- ATT&CK mapping
- Implemented Snort IDS and Fail2Ban IPS on Ubuntu servers
- Wrote Snort rules for detecting SSH brute force, SQLi, XSS, and
- WordPress abuse
- Built centralized logging pipelines with Filebeat, Logstash,
- Elasticsearch, Kibana
- Integrated Splunk for log visualization and alerting
- Simulated attacks using curl, WPScan, and SQLMap

PROJECTS

WordPress Server with IDS/IPS, SIEM, and Attack Simulation

- Set up a secure WordPress environment on Ubuntu with Apache and MySQL
- Developed 15+ Snort detection rules based on OWASP Top 10 attack categories
- Configured Fail2Ban jails to detect and block suspicious activity on SSH, MySQL, and
  WordPress login portals
- Forwarded logs using Filebeat into the
  ELK Stack and Splunk SIEM for log correlation and threat visualization
- Created real-time dashboards in
  Kibana and Splunk to monitor active attack patterns
- Executed simulated cyberattacks to validate detection rules and system resilience.

CERTIFICATIONS

- **Certified Penetration Tester (CPT)** – RedTeam Hacker Academy
- **Certified Security Analyst (CSA)** – EC-Council
- **TryHackMe: Cyber Security 101** · Pre-Security
- **Jr Penetration tester** - TryHackme Learning Path