MUNAVVAR FAIROOS P

CYBERSECURITY ANALYST|SOC ANALYST|ETHICAL HACKER
+919027397801|munavvarfairoos001@gmail.com | Kerala,India|
linkedin.com/in/mnavvar-fairoos-39b0b631a | github.com/munavvarfairoos-p

PROFESSIONAL SUMMARY

Cybersecurity professional trained in ethical hacking, digital forensics, SIEM operations, and network defense. Experienced in VAPT, endpoint security, and threat hunting, with hands-on expertise in detecting and analyzing security threats. Possess foundational knowledge of malware analysis and adapt quickly to new technologies to build secure and resilient systems.

SKILLS

- **Operating Systems:** Kali Linux, Windows,
- **Tools:** Nmap, Nessus, Metasploit, Wireshark, Burp Suite,DNS Lookup, Nikto, John The Ripper, SQLmap,Aircrack ng, Splunk
- **Specializations:** VAPT, SOC Monitoring,Threat Detection, Log Analysis,
- Incident Response
- **Soft Skills:** Teamwork, Curiosity
- **Languages:** English, Malayalam

CERTIFICATIONS

- Certified Ethical Hacker (CEH V13) from EC-Council - 2026-2027
- Certified SOC Analyst (CSA) from EC-Council - 2026-2027
- Certified Security Tester (CST) from Techbyheart - 2026
- Advanced Computer Forensic (ACF) form Techbyheart - 2026

PROJECTS

Vulnerability Assessment & Penetration Testing (VAPT)

- Conducted end-to-end **Vulnerability Assessment & Penetration Testing (VAPT**) on a simulated enterprise network using industry-standard tools (Nmap, Nessus, Metasploit).
- Successfully exploited **BlueKeep (CVE-2019-0708)** to gain remote access, followed by privilege escalation, persistence setup, and post-exploitation activities.
- Simulated **real-world attack impact** by performing controlled data exfiltration, showcasing risks of outdated and unpatched systems.

GitHub: github.com/munavvarfairoos-p/BlueKeep-VAPT-Lab

SIEM Integration with Splunk

- **Implemented Splunk SIEM** within a simulated enterprise environment to enable centralized log management, monitoring, and incident detection.
- **Configured UFW** to automate the detection and blocking of brute-force login attempts, strengthening system security posture.

- **Developed and customized Splunk dashboards and alerts** to provide real-time visibility, threat analysis, and proactive incident response capabilities.

GitHub: github.com/munavvarfairoos-p/Enterprise-SIEM-Integration-with-Splunk

---

EDUCATION

- Bachelor of Computer Applications (BCA) - MANGALAYATAN UNIVERSITY
  Distance/Online Mode - 2026-Present
- Diploma in Cyber Security & Ethical Hacking – Tech By Heart | 2025
- Plus Two Computer Commerce - GVHSS omanoor | 2024