ABHINAV THOMAS

Cybersecurity Researcher

Kannur, Kerala, India | +91 9496396882 | abhinavthomas15@gmail.com | LinkedIn

SUMMARY

Cybersecurity researcher with hands-on experience in ethical hacking, penetration testing, and vulnerability assessments. I am skilled in web application security, SOC monitoring, malware analysis, and incident response. Passionate about exploring advanced cybersecurity tools and techniques, with a strong academic foundation and practical training. Known for problem-solving ability and a continual drive to stay updated in the field.

EDUCATION

B.Sc. Digital & Cyber Forensic Science
Srinivas University, Mangalore
2023 – Present

Higher Secondary (Commerce)
Government Higher Secondary School, Kaniyanchal, Kannur
March 2020

SSLC
Government Higher Secondary School, Kaniyanchal, Kannur
March 2018

KEY COMPETENCIES

Security Tools: Burp Suite, Metasploit, Nmap, Wireshark, Wazuh, Splunk, Malware Analysis, Vulnerability Scanning, Web Server Management

Operating Systems & Platforms: Linux, Windows, Android, Active Directory

Security Concepts: Penetration Testing, SOC, Web Application Security, Ethical Hacking, Network Security, Incident Response, SIEM, Red Teaming

Other Skills: Problem Solving, Multilingual Communication, Microsoft Tools, Software Troubleshooting

CERTIFICATIONS

Certified Ethical Hacker v12 – EC-Council

Advanced Diploma in Cyber Defence – RedTeam Hacker Academy

Certified Penetration Tester – RedTeam Hacker Academy

Network Defense Essentials – Codered from EC-Council

ACHIEVEMENTS

HackTheBox – Hacker Rank

TryHackMe – Top 2% Global Rank

PROJECTS

- **Vulnerable Lab Setup & Network Scanning**
  Tools: Kali Linux, Metasploitable2 , Nmap, Wireshark
  - Built an isolated lab with attacker and victim VMs.
  - Conducted port scanning, service enumeration, and OS fingerprinting.
  - Captured and analyzed network traffic to identify suspicious patterns.

- **SOC Log Analysis with Splunk**
  Tools: Splunk, Windows Event Logs, Kali Linux
  - Configured a simulated Security Operations Center (SOC) environment using Splunk.
  - Ingested and analysed system and network logs to detect brute-force attacks, privilege escalation, and lateral movement.
  - Designed dashboards and real-time alerts for effective threat monitoring and response simulation.

- **Automated Ai powered Web Vulnerability Scanner**
  Tools: Python, Requests, BeautifulSoup
  - Developed a command-line scanner using AI assistance to detect XSS, SQL Injection, and CSRF vulnerabilities.
  - Implemented input fuzzing and payload injection.
  - Generated clean vulnerability reports with remediation suggestions.