KARTHIK P

Penetration Tester | *Cybersecurity Researcher*

+91 8594069844 | Malappuram, Kerala, India | karthikparambil.github.io | linkdin

SUMMARY

Cybersecurity enthusiast with hands-on expertise in network security, Active Directory exploitation, web application security, and vulnerability assessment. Skilled in red team techniques, CTF machine development, and building vulnerable lab environments for security research and training. Seeking an entry-level cybersecurity position to apply technical knowledge in real-world environments.

EXPERIENCE

Security Researcher & R&D Member | *Offenso Hackers Academy, Calicut* 2025 – Present

- Worked as part of cybersecurity research and development team
- Designed and developed custom CTF machines and vulnerable lab environments for hands-on offensive security training.
- Researched real-world CVEs and mapped them to practical exploitation exercises across web, network, and Active Directory.
- Built internal security tools and automation scripts to streamline penetration testing workflows.

PROJECTS

Mission-Escape - Vulnerable VM • CTF *github.com/karthikparambil/Mission-Escape*

Prison-break themed vulnerable linux VM with web exploitation and privilege escalation.

Mission-Space - Vulnerable VM • CTF *github.com/karthikparambil/Mission-Space*

Custom vulnerable linux VM for enumeration, exploitation, and privilege escalation training.

DarkPatch - Vulnerable VM • Pentest Lab

Custom vulnerable VM with real-world vulnerabilities and public exploits for penetration testing practice.

scanix - Bash *github.com/karthikparambil/scanix*

Automated reconnaissance suite covering host discovery, port scanning, service enumeration, and vulnerability fingerprinting.

lxd2root - Shell *github.com/karthikparambil/lxd2root*

Privilege escalation exploit targeting LXD group misconfiguration on Linux systems.

CERTIFICATIONS

- CompTIA Pentest+ (pursuing)
- Google Cybersecurity Professional Certificate
- Advanced Diploma in Information Security (ADIS)
- Certified Cybersecurity Educator Professional (CCEP)

TECHNICAL SKILLS

- **Web Pentesting**
  OWASP Top 10, SQL Injection, XSS, CSRF, SSRF, IDOR , JWT Attacks, LFI, SSTI, NoSQL Injection.

- **Active Directory**
  Kerberoasting, AS-REP Roasting, Pass-the-Hash, LDAP Enumeration, GPO Abuse, Ticket Attacks

- **Scripting**
  Python, Bash

TOOLS

Nmap, Metasploit, BurpSuite, Wireshark, Hashcat, Hydra, SQLmap, Nikto, Nuclei, Nessus, Impacket, NetExec, Kerbrute, Mimikatz, Rubeus, Feroxbuster, FFUF, LinPeas, WinPeas

EDUCATION

Advanced Diploma In Information Security | *Offenso Hackers Academy, Calicut* *2025 – 2026*

Higher Secondary - Computer Science | *IHRD Vazhakkad, Kerala* 2023 – 2025

ADDITIONAL INFORMATIONS

- Active CTF participant focusing on web exploitation and security concepts.
- Currently developing skills in bug bounty hunting and vulnerability discovery.
- CTF challenge creator for learning and skill development.