ADHITH P B

THRISSUR | adhith.pb3@gmail.com | 9961075771 | LinkedIn

Professional Summary

Offensive cybersecurity enthusiast with hands-on experience in vulnerability assessment, web application testing, and network exploitation. Skilled in conducting reconnaissance, enumeration, and post-exploitation using tools like Nmap, Burp Suite, Metasploit, and Wireshark. Experienced in exploiting web vulnerabilities such as SQLi, XSS, and LFI, and performing privilege escalation on Linux and Windows environments. Strong understanding of TCP/IP, OSI layers, VPNs, and common network protocols used in attack and defence scenarios. Continuously learning exploit development, privilege escalation techniques, and adversarial tactics to strengthen offensive security capabilities.

Skills

Cybersecurity Tools: Burp Suite, Wireshark, Nmap, Metasploit, sqlmap, Nikto, Hydra, John the Ripper, Nessus, OpenVAS, Responder.

Offensive Security Operations: Reconnaissance, Enumeration, Vulnerability Assessment, Exploitation, Post-Exploitation, Privilege Escalation, MITRE ATT&CK Mapping, Reporting.

Networking & Security Fundamentals: TCP/IP, OSI Layer, ARP, ICMP, HTTP/S, DNS, VPNs, Routing, Switching, Packet Analysis, Network Devices.

Operating Systems: Linux (Ubuntu, Kali), Windows.

Leadership & Collaboration : Collaborated in CTF and TryHackMe/HTB challenges to identify vulnerabilities and report findings, including a verified disclosure to NPCI.

Projects and Achievements

Home Lab Project: Built a personal offensive security lab simulating real-world environments using Kali Linux, Metasploit, and vulnerable machines. Practiced end-to-end attack workflows — reconnaissance, exploitation, privilege escalation, and post-exploitation

Recon Workflow Automation: Developed a Python-based automation script for reconnaissance tasks, integrating tools like Nmap, Sublist3r, and dirsearch to streamline target discovery and enumeration. Enhanced efficiency in data collection and reporting during vulnerability assessment workflows.

Web Exploitation Project: Identified and responsibly reported web vulnerabilities including SQLi, OTP bypass, and misconfigurations using Burp Suite, sqlmap, and manual testing, documenting findings with proof-of-concept and remediation steps.

NCIIPC Acknowledgement: Acknowledged by NCIIPC for reporting a critical SQLi in a government website.

Certificates

- **Jr Penetration Tester -** TryHackMe (Pursuing)
- **Certified Ethical Hacker (CEH V13) -** EC-Council
- **Advanced Diploma in Cyber Defence (ADCD)** – Red Team Hacker Academy
- **Leveraging AI for Pentesting** – LinkedIn Learning

Education

Advanced Diploma in Cyber Defence ADCD
Red Team Hacker Academy, Kochi

Bachelor of Computer Science
University of Calicut, College of applied science IHRD, Vattamkulam

Professional Development

Actively learning through TryHackMe, Hack The Box, and PortSwigger Academy, with regular participation in bug-bounty programs to practice real-world disclosure workflows. Attend hands-on workshops and labs to sharpen skills in web exploitation, reconnaissance automation, privilege escalation, and incident analysis.