ABUL KALAM AZAD

Penetration Tester | VAPT · Ethical Hacking · Web Application Security · Network Security

+91-6002567418 | abul.kalam.azad.cyber@gmail.com | Bhubaneswar, Odisha, India

abul-kalam-azad.pages.dev | github.com/Abulkalam1524 | linkedin.com/in/abul-kalam-azad-a7a41a260 | tryhackme.com/p/G00dM4nGr1t | medium.com/@azad93204

PROFESSIONAL SUMMARY

eJPTv2- and CRTA-certified junior penetration tester and final-year B.Tech (Electronics & Computer Science) student specializing in web application and network VAPT. Completed a full grey-box engagement end to end — 19 validated findings across Windows and web targets, scored with CVSS v3.1 and delivered as a 97-page report with a prioritized remediation roadmap and verified retest results. Hands-on with Burp Suite, Nmap, Metasploit, Nessus, and Python security tooling across TryHackMe (Top 2% global; All India Rank 12, October 2024) and Hack The Box, and author of open-source offensive-security tools. Internship experience in network VAPT, web application testing, and security reporting. Seeking a VAPT / penetration testing role.

TECHNICAL SKILLS

Web & Application Security: Burp Suite (Repeater, Intruder, Proxy), HTTP/S interception, OWASP Top 10, SQL Injection, Cross-Site Scripting (XSS), IDOR, authentication testing

Network Security: Nmap, Wireshark, Netcat, port scanning, service enumeration, packet analysis, network penetration testing

Exploitation & Assessment: Metasploit Framework, Nessus, Nikto, Nuclei, privilege escalation, vulnerability assessment, MITM / ARP spoofing

Red Team & Active Directory: MITRE ATT&CK TTPs, Kerberos-based attacks (patched AD), lateral movement, stealth network pivoting, adversary simulation, internal/external recon

Programming Languages: Python (Scapy), C, SQL, Bash

Tooling & Environments: Git/GitHub, Linux (Kali), Windows, VMware, security tool development

Reporting & Standards: Vulnerability Assessment and Penetration Testing (VAPT) reporting, CVSS v3.1 scoring, CWE mapping, OWASP WSTG v4.2, PTES, NIST SP 800-115, remediation guidance, technical documentation

Cloud Security: AWS, Azure and GCP red team techniques, IAM and RBAC, compute and storage security, cloud asset recon and enumeration, MITRE Cloud ATT&CK, cloud security fundamentals

SECURITY PROJECTS

Full-Scope VAPT Engagement — Web & Network Assessment *github.com/Abulkalam1524/vapt-lab-assessment*

- Executed an end-to-end grey-box VAPT against four in-scope assets (two Windows hosts, two web applications) following PTES and OWASP WSTG v4.2, identifying 19 validated vulnerabilities including 2 Critical and 7 High, each scored with CVSS v3.1 and mapped to CWE.
- Manually validated all 18 automated scanner findings and rejected 39% as non-actionable or unconfirmed; identified 8 additional vulnerabilities — 42% of the total, including 5 of 7 High-severity issues — that no scanner reported.
- Achieved SYSTEM-level compromise via MS17-010 (EternalBlue) and extracted the full local credential database, demonstrating real-world impact beyond automated scanner output.
- Delivered a 97-page report with executive summary, business impact analysis, and a prioritized remediation roadmap; retested all 19 findings, verifying 6 resolved and reporting 4 partially resolved and 9 unresolved.

ARP Spoofer — Python MITM Tool (Scapy) *github.com/Abulkalam1524/arp-spoofer*

- Built a Python ARP cache-poisoning tool that performs a man-in-the-middle attack between a target host and gateway by forging Layer-2 Ethernet/ARP frames with Scapy.
- Resolved MAC addresses once to prevent ARP cache flapping and automatically restored original ARP tables on exit for clean, non-disruptive teardown.
- Tested in an isolated VMware lab (Kali attacker, Windows 10 target) and documented detection and defenses — Dynamic ARP Inspection, static ARP entries, and arpwatch.

Network Scanner — ARP-Based Host Discovery (Python, Scapy) *github.com/Abulkalam1524/network-scanner*

- Developed a lightweight ARP-based scanner that discovers live hosts across a /24 subnet and maps their IP and MAC addresses using Scapy srp(), with no external scanning tools required.

MAC Address Changer — Linux Network Utility (Python) *github.com/Abulkalam1524/mac-address-changer*

- Wrote a Linux MAC-spoofing tool that changes and verifies a network interface's MAC address, including root-privilege checks and post-change validation.

PUBLICATIONS & WRITE-UPS

TryHackMe: Mr. Robot Walkthrough — Penetration Testing Write-up *medium.com/@azad93204*

- Published a detailed penetration-testing walkthrough covering enumeration, web exploitation, and privilege escalation, demonstrating end-to-end methodology and clear technical reporting.

EXPERIENCE

Cyber Security Mentor — IoT Lab (Cyber Security Society), KIIT *Aug 2024 – Present*

- Mentor and train 20–25 students in the college cyber security society, delivering hands-on sessions on network security, penetration testing, and CTF techniques.
- Design and host OSINT-based CTF challenges for lab events, building challenges across recon, research, and web exploitation.
- Lead collaborative vulnerability research and guided practice labs on TryHackMe and Hack The Box.

Cybersecurity Intern — The Red Users *Nov 2024 – Dec 2024*

- Conducted network penetration testing across assigned targets to identify vulnerabilities and assess overall security posture.
- Used Burp Suite to intercept, analyze, and modify HTTP/S requests, surfacing injection and authentication flaws in web applications.
- Documented findings with actionable remediation recommendations in structured security reports.

EDUCATION

B.Tech, Electronics & Computer Science Engineering *Jul 2023 – Jul 2027*

KIIT, Bhubaneswar

Relevant Coursework: Computer Networks, Operating Systems, Network Security, Cybersecurity Fundamentals, Cryptography

CERTIFICATIONS

- **CRTA — Certified Red Team Analyst** (CyberWarFare Labs), August 2026
- **MCRTA — Certified Multi-Cloud Red Team Analyst** (CyberWarFare Labs), August 2026
- **eJPTv2 — Junior Penetration Tester** (INE Security)
- **ICCA — INE Certified Cloud Associate** (INE)
- **Certified in Cybersecurity (CC)** — ISC2 / (ISC)²
- **Introduction to Azure Red Teaming** — Course Completion (Altered Security), August 2026
- **TryHackMe Paths:** Jr Penetration Tester, Cyber Security 101, Complete Beginner

ACHIEVEMENTS & CTF RECOGNITION

- **OS Bug Bounty Challenge 2026 — C-DAC / MeitY, Government of India** (National-level, C-DAC Kolkata, July 2026) — 36-hour security assessment of BOSS OS covering static and dynamic analysis, fuzzing, reverse engineering, proof-of-concept development, and CVSS-scored vulnerability reporting under a defined Rules of Engagement
- **3rd Place — Capture The Flag, D3 Fest 2025** (IIIT Bhubaneswar, November 2025) — competed as Team 7h3_UnKnw0n
- **Top 2% Global — TryHackMe** (All India Rank 12, October 2024 Wall of Fame) — penetration testing, web exploitation, privilege escalation, network security
- **CTF Competitor** — BSides, DEADFACE, Pentathon, H7CTF