AKSHAY SOMIDI

Penetration Tester | VAPT Analyst | Red Team Operator

Hyderabad, Telangana | +91 98661 84293 | akshu4875@gmail.com

PROFESSIONAL SUMMARY

Penetration tester and red team operator with 2 years of hands-on Vulnerability Assessment and Penetration Testing (VAPT) experience across web, mobile (Android), network, and Active Directory environments. Certified CRTO, CRTP, CEH. Across 45+ client engagements, uncovered 232+ Critical vulnerabilities and cut high-risk exposure by around 60% by chaining manual exploitation with business-logic testing that automated scanners miss. Comfortable owning an assessment end to end, from scoping and exploitation through CVSS risk reporting and remediation retesting.

Portfolio: knowntonone.pages.dev | **LinkedIn:** linkedin.com/in/akshay-73b6bb254 | **GitHub:** github.com/Knowntonone | **TryHackMe:** tryhackme.com/p/unabletofinduser

PROFESSIONAL EXPERIENCE

Junior Security Analyst Vatins Systems, Hyderabad, India Sep 2025 - Present

- Delivered end-to-end VAPT engagements spanning web, mobile (Android), internal and external networks, malware reverse engineering and Active Directory domains, owning each from scoping through exploitation to remediation retest.
- Identified 232+ Critical vulnerabilities across client environments and reduced high-risk attack surface by roughly 60% through prioritized, risk-rated findings.
- Surfaced critical business-logic flaws, IDORs, RCEs and authentication bypasses that automated scanners missed, using manual exploitation and parameter manipulation.
- Mapped Active Directory attack paths with BloodHound and validated exposure through Kerberoasting, AS-REP Roasting, and Delegations.
- Tested mobile applications against the OWASP MASVS and Mobile Top 10, reporting insecure data storage, weak cryptography, and unprotected API communication.
- Wrote risk-rated reports with executive summaries, CVSS v3.1 scoring, and clear remediation steps, then re-validated fixes after client patching.

Cybersecurity Analyst TriArmour AI Pvt. Ltd., Hyderabad, India Mar 2024 - Mar 2025

- Ran web application penetration tests in Burp Suite Professional against the OWASP Top 10, finding IDOR, SQL injection, XSS, and broken access control.
- Monitored endpoint telemetry across Bitdefender GravityZone and Sophos MDR and isolated compromised hosts during incident response drills.
- Reviewed reported phishing emails by inspecting headers and attachments, which cut false-positive alerts by around 30%.

CERTIFICATIONS

- **Certified Red Team Operator (CRTO)**, Zero-Point Security
- **Certified Red Team Professional (CRTP)**, Altered Security
- **Certified Red Team Analyst (CRTA)**, Cyberwarfare Labs
- **Certified Ethical Hacker (CEH v12)**, EC-Council
- **Certified AppSec Practitioner (CAP)**, The SecOps Group
- **Certified in Cybersecurity (CC)**, ISC2

TECHNICAL SKILLS

Vulnerability Assessment & Penetration Testing: Web Application, Mobile (Android), Network (Internal/External), Active Directory, Business Logic Testing, Malware reverse engineering

Offensive Techniques: Manual Exploitation, Privilege Escalation, Kerberoasting, AS-REP Roasting, Pass-the-Hash, Lateral Movement, IDOR, SQL Injection, XSS, Authentication Bypass

Frameworks & Standards: OWASP Top 10, OWASP MASVS / MASTG, OWASP API Security Top 10, MITRE ATT&CK, Cyber Kill Chain

Tools: Burp Suite Professional, Nmap, Nessus, Metasploit, BloodHound, Mimikatz, MobSF, Wireshark, Postman

Platforms: Windows, Windows Server, Linux, Active Directory

OFFENSIVE SECURITY PROJECTS

Custom Remote Access Tool (RAT) & C2 Infrastructure

- Built a complete RAT and multi-session C2 platform from scratch in Rust with a Node.js operator dashboard: remote shell, keylogging, screen capture, Wi-Fi credential extraction, and registry persistence masquerading as a OneDrive sync helper.
- Achieved stable remote access on a fully updated Windows host running Microsoft Defender with zero alerts, using unique per-session authentication keys and plain HTTP task polling that blended with normal web traffic.
- Evaded Kaspersky Next EDR Optimum by adding randomized execution delays, and routing tasking through native Windows utilities so implant activity mirrored legitimate system processes.

In-Memory Shellcode Loader

- Developed a fully fileless loader that downloads an encrypted payload over HTTP, manually decodes it in memory with custom Base64 and rotating-key XOR routines, then executes it by chaining VirtualAlloc (RW), VirtualProtect (RX), and CreateThread.
- Bypassed fully patched Microsoft Defender by adding randomized sleep delays to outlast sandbox detonation windows, and disguising the binary with benign executable metadata.

Reflective PE Loader (IronPE Extension)

- Extended the open source IronPE manual PE loader (section mapping, base relocations, import resolution, x86/x64) with remote PE fetching to download and run payloads directly from memory, and replaced public framework shells with a custom Winsock reverse shell written in C.
- Demonstrated that minimal custom implementations evade signature-based detection that reliably flags public offensive tools, proving detection keys on behavior patterns rather than payload content.

All projects were built and tested strictly in isolated, authorized lab environments for security research and detection engineering purposes.

EDUCATION

B.Tech, Cyber Security, Sri Indu College of Engineering & Technology, Hyderabad
Intermediate (MPC), Sri Chaitanya Junior College, Hyderabad