

AKSHAY SOMIDI

PENETRATION TESTER · RED TEAM OPERATOR

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

Portfolio: knowntonone.pages.dev · LinkedIn: linkedin.com/in/akshay-73b6bb254

GitHub: github.com/Knowntonone · TryHackMe: tryhackme.com/p/unabletofinduser

Penetration tester with 2 years of hands-on Vulnerability Assessment and Penetration Testing (VAPT) delivery for consulting clients. Across 45+ client engagements covering web applications, Android apps, internal/external networks, and Active Directory, the findings that mattered came from manual exploitation and business logic testing that automated scanners do not reach, helping clients cut high-risk exposure by roughly 60%. Every reported fix is re-validated, and every assessment is owned end to end: scoping, exploitation, CVSS v3.1 reporting, and the post-remediation retest.

PROFESSIONAL EXPERIENCE

Junior Security Analyst

Sep 2025 - Present

Vatins Systems, Hyderabad, India

- Reported risk-rated, CVSS v3.1 scored findings that showed clients which attack chains mattered, so patching effort went to what attackers would actually use first.
- Conduct end-to-end VAPT engagements for consulting clients, from the scoping call through exploitation and reporting to the post-remediation retest. Scope spans manual and automated security testing of web applications, Android apps, internal/external networks, and Active Directory security assessments.
- Surface business logic flaws, IDORs, RCEs, authentication bypasses, and AD misconfigurations that scanners pass clean, and develop proof-of-concept exploits to confirm impact. Manual testing does most of that work.
- Ran an assumed-breach Active Directory red team assessment: mapped attack paths with BloodHound from a simulated compromised endpoint, validated exposure through Kerberoasting, AS-REP Roasting, and delegation abuse, and delivered the prioritized fixes that closed the shortest route to domain control first.
- Test Android applications against OWASP MASVS and the OWASP Mobile Top 10, covering insecure data storage, weak cryptography, unprotected API communication.
- Prepare detailed reports with executive summaries, CVSS-scored findings, and remediation guidance specific enough for a developer to apply directly. Every engagement closes with a post-remediation retest.

Cybersecurity Analyst

Mar 2024 - Mar 2025

TriArmour AI Pvt. Ltd., Hyderabad, India

- Performed web application penetration tests in Burp Suite Professional against the OWASP Top 10. Findings included IDOR, SQL injection, XSS, and broken access control flaws.
- Analysed endpoint telemetry across Bitdefender GravityZone and Sophos MDR during incident response drills, tracing suspicious activity and supporting compromised-host isolation.
- Analysed reported phishing emails through header and attachment inspection to identify spoofed senders and malicious attachments.

CERTIFICATIONS

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

OFFENSIVE SECURITY PROJECTS

Console Named-Pipe Injection Loader

- Built a process injection loader from scratch in C and x64 assembly that executes a payload inside a signed Windows process like nslookup.exe through its own standard input, so WriteProcessMemory, VirtualAllocEx, and CreateRemoteThread never appear in the injection path.
- Made all cross-process memory changes through hand-built direct syscalls with syscall numbers resolved from the clean KnownDlls copy of ntdll, invisible to the userland API hooks that security products install.
- Achieved clean runs against Microsoft Defender, Bitdefender Total Security, and Sophos XDR, with the payload executing inside the signed host process, zero alerts, and the process tree confirming it ran there.

SimpleAF C2

- Built SimpleAF, a custom implant and C2 server written from scratch in Rust and Node.js: remote shell, interactive remote control, keylogging with window-title tracking, screen capture, Wi-Fi credential extraction, and registry persistence disguised as a OneDrive sync helper.
- Bypassed Microsoft Defender on a fully updated Windows host, holding stable remote access with zero alerts through real-time protection and full scans across the assessment window.
- Per-session authentication keys and plain HTTP task polling keep the traffic looking ordinary. Against Kaspersky Next EDR Optimum, randomized execution delays and native-Windows tasking kept implant activity indistinguishable from legitimate system processes.

Rust Shellcode Loader

- Developed a fully fileless shellcode loader in Rust that pulls an encrypted payload over HTTP, 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 using randomized sleep delays that outlast sandbox detonation windows, plus benign executable metadata on the binary.

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

TECHNICAL SKILLS

TESTING SCOPE

Web application VAPT, mobile application security testing (Android), internal/external network penetration testing, Active Directory security assessments, business logic testing, malware reverse engineering

STANDARDS

OWASP Top 10, OWASP MASVS / MASTG, MITRE ATT&CK, Cyber Kill Chain, CVSS v3.1

ANALYSIS & RESPONSE

Endpoint telemetry analysis (Bitdefender GravityZone, Sophos MDR), phishing email header and attachment analysis, host isolation during incident response drills

OFFENSIVE TECHNIQUES

Manual exploitation, privilege escalation, Kerberoasting, AS-REP Roasting, Pass-the-Hash, lateral movement, IDOR, SQL injection, XSS, RCE, authentication bypass

TOOLING

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

PLATFORMS

Windows, Windows Server, Linux, Active Directory

EDUCATION

B.Tech, Cyber Security

Sri Indu College of Engineering & Technology, Hyderabad

Intermediate (MPC)

Sri Chaitanya Junior College, Hyderabad