CONTACT

EMAIL
dhakshan0819@gmail.com

GITHUB
github.com/dhakshan0819

LINKEDIN
linkedin.com/in/dhakshan0819

LOCATION
Tamil Nadu, India

DOMINANT SKILLS

- Pentesting (Web/AD)
- Malware Analysis
- Binary Exploitation
- API Security Auditing
- Wireless Vulnerabilities
- Python / Bash / C / x86

METHODOLOGIES

- OWASP Top 10 / ASVS
- MITRE ATT&CK
- NIST Framework
- PTES Standard
- Zero Trust Architecture

SECURITY STACK

- Burp Suite Professional
- Metasploit Framework
- Ghidra / IDA Pro
- BloodHound / Sharphound
- Nmap / Wireshark
- Hashcat / Aircrack-ng

LANGUAGES

- English (Professional)
- Tamil (Native)

AWARDS

- SIH 2025 Finalist
- Yukthi CTF 2025 Finalist

DHAKSHAN A

PENETRATION TESTER

PROFESSIONAL SUMMARY

Offensive security specialist with over 6 years of experience in pentesting and vulnerability research. Proven track record of discovering critical IDOR and logic flaws in enterprise environments. Expert in Active Directory attack paths and binary reverse engineering.

CORE EXPERIENCE

Independent Security Researcher & Bug Hunter 2022 – Present
HackerOne / Bugcrowd / Private

- Discovered Critical IDOR leading to full account takeover (CVSS 9.8).
- Chained Kerberoasting and NTLM Relay with BloodHound for AD compromise.
- Performed 60+ assessments on global platforms focusing on API & logic.

CTF Competitor & Security Researcher 2019 – Present
HackTheBox / TryHackMe / PsychCTF

- Specialized in Pwn/Rev; bypassed ASLR/Canary mitigations in ELF targets.
- Automated flag extraction on PsychCTF leveraging deep reverse-engineering and API exploitation.
- Built a distributed lab for malware analysis using Proxmox and Docker.

TECHNICAL PROJECTS

Titan-SIEM Framework 2023 – Present
Python / ELK Stack / Automated Detection

- Engineered SIEM for real-time log ingestion and correlation of security events.
- Integrated custom Sigma rules to identify APT indicators; secured automated agent deployments.

Custom Binary Fuzzer (Z-Fuzz) 2024
Python / Radare2 / Mutation Engine

- Built coverage-guided fuzzer to identify memory corruption in IoT binaries.

NOTABLE FINDINGS

Vuln-01: Zero-Interaction Account Takeover (CVSS 9.8)

- Exploited IDOR via parameter pollution to modify administrative sessions.

Vuln-02: AD Certificate Template Escalation (CVSS 8.8)

- Leveraged misconfigured templates (AD CS) for full Domain Administrator access.

EDUCATION

B.Sc. Computer Science with Cyber Security 2025 – Present
Sri Ramakrishna College of Arts & Science (SRCAS)