ADITYA SHARMA

Chandigarh, India | +91 7650024943 | iadityakamalsharma@gmail.com

LinkedIn | GitHub | Portfolio & Blog | OSCP+ Credential

PROFESSIONAL SUMMARY

OSCP+-certified penetration tester with hands-on experience compromising 300+ machines across HackTheBox, Offensive Security Proving Grounds, and VulnLab. Achieved global Platinum Tier ranking (Top 1,000) in HackTheBox Spring 2026 Seasonal Campaign. Specializes in manual exploitation, Active Directory attack chains, and web application security using Assumed Breach methodology. Augments offensive workflows with AI-driven CLI tooling (Gemini CLI, Claude CLI) for automated reconnaissance and payload prototyping. Published 9 technical security research articles and maintains 37+ repositories on GitHub spanning offensive tooling, exploitation scripts, and AI Red Teaming research.

TECHNICAL SKILLS

Security Domains: Web Application Penetration Testing, Active Directory Exploitation, Privilege Escalation, API Security, AI Red Teaming

Languages: Python, Bash, Rust

Tools & Infrastructure: Kali Linux, Burp Suite, BloodHound, Metasploit, Nessus, Nmap, Impacket, CrackMapExec, Hashcat, Git

AI & Automation: Gemini CLI, Claude CLI, LLM-Assisted Payload Prototyping, Automated Reconnaissance Pipelines

CERTIFICATIONS & EDUCATION

Offensive Security Certified Professional (OSCP+) *April 2026*

OffSec · Credential: https://credentials.offsec.com/027235bd-a4ce-48c9-90ba-632d924fbb7e#acc.lm0gR7ES

B.Tech – Computer Science and Engineering *2025*

Atal Bihari Vajpayee Government Institute of Engineering & Technology, Shimla

TECHNICAL PROJECTS

HackTheBox Seasonal Campaign *Spring 2026*

Global Platinum Tier · Top 1,000 Worldwide

- Placed in the top 1,000 competitors globally across the Spring 2026 HackTheBox Seasonal Campaign, earning Platinum Tier rank.
- Exploited hardened, enterprise-grade targets requiring full manual exploitation with no guided walkthroughs — network, application, and AD-layer attacks.
- Consistently identified non-obvious attack vectors through deep enumeration and creative chaining of misconfigurations.

Enterprise Active Directory Attack Lab *2025 – 2026*

- Designed and deployed a multi-domain Windows lab to simulate realistic enterprise Active Directory infrastructure.
- Executed cross-forest trust exploitation, Kerberoasting, AS-REP Roasting, and delegation abuse to escalate from standard domain user to Domain Admin.
- Automated lateral movement with custom Python and Bash scripts; mapped full attack paths using BloodHound to identify and exploit shortest privilege escalation routes.

Penetration Testing & AI Exploit Development *2024 – 2026*

- Compromised 300+ machines across Offensive Security Proving Grounds Practice, VulnLab, and HackTheBox — covering Windows, Linux, and Active Directory environments.
- Built AI-assisted terminal workflows integrating Gemini CLI and Claude CLI for OSINT automation, service fingerprinting, and vulnerability triage.
- Prototyped and deployed custom Python and Bash payloads targeting privilege escalation, SUID abuse, token impersonation, and credential harvesting.

TECHNICAL WRITING & KNOWLEDGE SHARING

Security Research Blog **https://aditya-kamal-sharma.pages.dev/**

- Published 9 long-form technical security articles covering offensive techniques across AI Red Teaming, Web Application Security, Active Directory exploitation, and OSCP methodology.

- Flagship resources: OSCP Enumeration Checklist (5,500+ words, 28-min read) and Active Directory Exploitation Cheatsheet (5,200+ words, 26-min read) — referenced pentesting community resources.
- Additional coverage: GraphQL API hacking methodology, XSS exploitation cheatsheet (3,000+ words), SQL injection tradecraft, Windows and Linux privilege escalation, and file transfer techniques for constrained environments.
- Launched an ongoing AI Red Teaming series exploring offensive applications of large language models — a rapidly growing niche in the security field.

OPEN SOURCE & GITHUB

Offensive Security Tooling *https://github.com/adityakamalsharma*

- Maintains 37+ repositories covering penetration testing automation, offensive scripting, and security research utilities.
- OSCP-Scripts: Custom Python automation suite streamlining OSCP exam workflows — automated enumeration, file transfer, privilege escalation checks, and post-exploitation helpers.

CTF COMPETITIONS

Participated in CTF events https://ctftime.org/user/253236

- Hackअस्त्र 2026 – Team0Skills – 75 Nationally
- K!nd4SUS CTF 2026 – Team0Skills – 50 Globally
- pingCTF 2026 – Team0Skills – 110 Globally, and many more.