

ABHAY GUPTA

OSCP & OSCP+ CERTIFIED | PENETRATION TESTER | VAPT | WEB & ACTIVE DIRECTORY

+91 9205253438 • abhaygupta.sec@gmail.com • New Delhi, India
linkedin.com/in/abhay-gupta-sec • github.com/abhaygupta-sec • https://abhayguptasec.online/

PROFILE

OSCP and OSCP+ certified penetration tester focused on web application, network, and Active Directory security testing. Completed 104 Hack The Box machines, documented 46 technical writeups, and achieved Hack The Box global rank #982. Hands-on work covers reconnaissance, manual enumeration, exploitation, credential attacks, privilege escalation, pivoting, and Active Directory attack paths. Built a Python-based Nmap reconnaissance framework for repeatable discovery, service enumeration, NSE scanning, and structured reporting.

CERTIFICATIONS & SECURITY MILESTONE

- OSCP – OffSec Certified Professional | August 2026 | Credential ID: 192501787
- OSCP+ – OffSec Certified Professional Plus | August 2026–August 2029 | Credential ID: 192501996
- HTB – Hack The Box Global Rank #982 | 104 machines completed | 46 detailed writeups

PRACTICAL SECURITY EXPERIENCE

Hands-on Penetration Testing | Hack The Box & Independent Security Projects

- Applied penetration-testing methodology across Linux and Windows targets, including reconnaissance, enumeration, exploitation, privilege escalation, pivoting, and Active Directory attack paths.
- Produced reproducible technical documentation with commands, attack chains, findings, and validation steps.
- Built and maintained security tooling and methodology resources in Python, Bash, and PowerShell.

TECHNICAL SKILLS

Penetration Testing: Reconnaissance, Enumeration, Exploitation, Vulnerability Assessment, Privilege Escalation, Post-Exploitation, Reporting

Web Application Security: SQL Injection, XSS, LFI, Command Injection, Authentication Testing, HTTP Testing, Burp Suite, FFUF

Active Directory: LDAP, SMB, Kerberos, BloodHound, ACL Abuse, AD CS, RBCD, Kerberoasting, AS-REP Roasting

Network Security: Nmap, TCP/UDP Scanning, Service Enumeration, NSE, Network Discovery, Pivoting

Platforms: Kali Linux, Linux, Windows, Windows Server

Tools & Scripting: Python, Bash, PowerShell, Impacket, Evil-WinRM, Hashcat, John the Ripper

SELECTED SECURITY PROJECTS

HACK THE BOX SECURITY LABS

104 MACHINES | 46 DETAILED WRITEUPS | GLOBAL RANK #982

- Completed 104 authorized Hack The Box machines across Linux and Windows environments.
- Practiced reconnaissance, manual enumeration, web application testing, exploitation, credential attacks, privilege escalation, pivoting, and Active Directory attack paths.
- Documented 46 technical writeups covering attack chains, commands, findings, validation steps, and methodology.
- Technical portfolio: github.com/abhaygupta-sec/HTB-Writeups

NMAPTOOL-AUTOMATED-RECON

PYTHON | NMAP | NETWORK RECONNAISSANCE

- Developed a six-phase reconnaissance framework for TCP/UDP discovery, service enumeration, and Nmap NSE-based scanning.
- Implemented XML result parsing, HTML/JSON/XML/raw outputs, logging, caching, timeouts, and multi-target support.
- Built repeatable workflows that preserve raw scan evidence for manual analysis during authorized security assessments.
- GitHub: github.com/abhaygupta-sec/NmapTool-Automated-Recon

OFFENSIVE SECURITY METHODOLOGY

SECURITY METHODOLOGY | PENETRATION TESTING

- Maintained structured workflows covering reconnaissance, Active Directory, web application security, privilege escalation, pivoting, exploitation, and penetration-testing reporting.
- Organized practical techniques and tooling into reusable workflows for authorized lab and assessment environments.
- GitHub: github.com/abhaygupta-sec/Offensive-Security-Methodology

EDUCATION

- Bachelor of Computer Applications (BCA) | Delhi Skill and Entrepreneurship University, New Delhi
- School of Excellence | 2021–2024

Target roles: Penetration Tester • VAPT • Application Security • Offensive Security