Priyanshu Singh

priyanshusecurity@gmail.com | Lucknow, India | GitHub

SUMMARY

Offensive Security Researcher with 3.5 years of hands-on experience in penetration testing, Active Directory security, and vulnerability assessment within lab and simulated enterprise environments. Skilled in attack-path analysis, security validation, technical reporting, and offensive security operations, with experience leveraging industry-standard tools and MITRE ATT&CK-based methodologies.

EXPERIENCE

Offensive Security Researcher

Self-Directed Research & Simulated Enterprise Lab Environments | 2023 – Present

- Conducted structured black-box penetration testing against web applications, Windows endpoints, and Active Directory environments within controlled lab simulations.
- Performed Active Directory security assessments covering domain enumeration, attack-path analysis, and privilege escalation research using BloodHound, Impacket, NetExec, and Responder.
- Identified and validated authentication weaknesses, access-control misconfigurations, and attack-surface exposures; mapped findings to MITRE ATT&CK techniques for risk prioritization.
- Authored structured technical reports documenting vulnerability impact, attack-chain reconstruction, proof-of-concept validation, and prioritized remediation guidance.

TECHNICAL SKILLS

Offensive Security

Black-Box Penetration Testing · Vulnerability Assessment · Attack Surface Analysis · MITRE ATT&CK

Active Directory

BloodHound · SharpHound · NetExec · Impacket · Responder

Web & API Security

Burp Suite · Caido · API Security Testing · REST APIs · ffuf · Gobuster

Network Analysis

Nmap · Wireshark · TCP/IP · HTTP/HTTPS · DNS

Reverse Engineering

Ghidra · x64dbg · PE Studio · Detect It Easy (DIE)

Operating Systems

Windows · Kali Linux · Ubuntu Linux

PROJECTS

HackerOne Research

- Conducted vulnerability research across 25+ organizations through responsible disclosure and structured security testing.

OPSCORE – Red Team Engagement Management Platform

- Developing a red team operations platform supporting engagement tracking, operational planning, evidence management, and structured reporting workflows.
- Applies offensive security methodology to organize multi-phase red team engagements with operational visibility, traceability, and documentation.

Active Directory Security Lab

- Designed and operated a simulated enterprise AD environment for domain enumeration, attack-path analysis, privilege escalation research, and security hardening validation.

CERTIFICATION

Deloitte Cybersecurity Virtual Experience Program | 2024