Reju Kole

Cybersecurity Engineer | Red Team Specialist | Exploit Developer

rejukole@protonmail.com | linkedin.com/in/reju-kole | tryhackme.com/p/W40X | medium.com/@RejuKole.com

Summary

Cybersecurity engineer and ethical hacker with 6+ years of experience in red team operations, penetration testing, and exploit development. NASA Hall of Fame recipient and top 1% TryHackMe performer, specializing in advanced persistent threat simulation, malware research, and vulnerability discovery. Proven track record of identifying critical vulnerabilities in major organizations including NASA, SpaceX, Binance, Starlink, Telstra, and Lenovo.

Professional Experience

Cybersecurity Researcher & Bug Bounty Hunter 2018 – Present

Independent *Remote*

- Discovered critical vulnerabilities in major organizations including NASA, SpaceX, and Binance
- Developed advanced red team tools and techniques for penetration testing
- Achieved top 1% ranking on TryHackMe among over 3 million users globally
- Completed multiple Hack The Box Pro Labs demonstrating advanced exploitation skills

Penetration Testing Specialist 2020 – Present

Freelance *Global*

- Conducted comprehensive security assessments for enterprise clients
- Specialized in web application and infrastructure penetration testing
- Developed custom exploits and proof-of-concept demonstrations
- Provided detailed remediation guidance and security recommendations

Hall of Fame & Security Recognition

NASA – Official Letter of Recognition Hall of Fame

- Discovered critical vulnerabilities in NASA's infrastructure, enhancing space mission security

SpaceX – Security Vulnerability Disclosure Hall of Fame

- Identified critical security vulnerabilities in SpaceX systems, contributing to the security of space exploration missions

Binance – Cryptocurrency Exchange Security Hall of Fame

- Discovered critical vulnerabilities in the world's largest cryptocurrency exchange, protecting millions of users' assets

Starlink – Satellite Internet Security Hall of Fame

- Enhanced the security of global satellite internet infrastructure through responsible vulnerability disclosure

Telstra – Telecommunications Security Hall of Fame

- Improved the security posture of Australia's leading telecommunications infrastructure through vulnerability research

Lenovo – Enterprise Computing Security Hall of Fame

- Contributed to the security of enterprise computing solutions used by millions of businesses worldwide

Projects & Research

Advanced C2 Malware Framework | *C++, Assembly, Windows API, Cryptography, Evasion Techniques*

- Developed sophisticated command and control malware that successfully bypassed Windows Defender
- Implemented advanced evasion techniques including process hollowing and DLL injection
- Built encrypted communication channels for command and control operations
- Demonstrated during red team engagements with 95% success rate
- Featured in cybersecurity conferences as a case study for modern APT simulation

Automated Recon Toolkit | *Python, Bash, OSINT, Nmap, Custom APIs*

- Built comprehensive reconnaissance automation framework integrating multiple OSINT tools and techniques
- Streamlined vulnerability discovery process with custom reporting and threat intelligence correlation

Red Team Simulation Platform | *Python, PowerShell, Metasploit, Cobalt Strike, MITRE ATT&CK*

- Designed end-to-end red team engagement platform for simulating advanced persistent threats
- Includes payload generation, lateral movement automation, and comprehensive attack chain documentation

Vulnerability Research & Writeups | *Research, Exploit Development, Technical Writing, CVE Analysis*

- Published in-depth vulnerability research, exploit development tutorials, and cybersecurity writeups
- Covering topics from web application security to advanced persistent threats

Certifications

Certified Red Team Analyst (CRTA) – CyberWarfare Labs 2025
Burp Suite Certified Practitioner (BSCP) – PortSwigger 2025
Postman API Fundamentals Student Expert – Postman May 2025
eLearnSecurity Junior Penetration Tester (eJPT) – INE Security 2024
INE Certified Cloud Associate (ICCA) – INE Security July 2024

Hack The Box Achievements

Cyber Apocalypse CTF 2025 – Hack The Box Mar 2025
University CTF 2024 – Binary Badlands – Hack The Box Dec 2024
Pro Labs: P.O.O. – Hack The Box Nov 2024
Pro Labs: RPG – Hack The Box Nov 2024
Pro Labs: Dante – Hack The Box Nov 2024
Pro Labs: Hades – Hack The Box Nov 2024
Pro Labs: FullHouse – Hack The Box Nov 2024
Pro Labs: Solar – Hack The Box Oct 2024
Hack The Boo 2024 – CTF Competition – Hack The Box Oct 2024

TryHackMe

Top 1% Global Ranking – Among 3+ Million Users

- Completed 500+ rooms across multiple cybersecurity domains
- Specialized in advanced penetration testing and digital forensics challenges
- Active contributor to the cybersecurity learning community
- Profile: tryhackme.com/p/W40X

Technical Skills

Red Team & Pentesting: Red Team Operations, Exploit Development, Malware Development, APT Simulation, Binary Exploitation, Privilege Escalation
Programming: Python, PowerShell, Bash Scripting, Go, PHP, SQL, C++, Assembly
Security Tools: Metasploit, Cobalt Strike, Burp Suite, Nmap, Wireshark, SQLMap
Cloud & Infrastructure: AWS Security, Azure Security, Kubernetes, Docker
Specializations: Advanced Persistent Threat (APT) Simulation, Custom Exploit Development, Cloud Security Assessment, Malware Analysis & Research, Vulnerability Research & Disclosure

Upcoming Goals

OSCP – Offensive Security Certified Professional Target: 2025

CRTP – Certified Red Team Professional Target: 2025

CTF Team Leadership – Building and leading a competitive CTF team for international competitions

Advanced Research – AI-driven threat simulation and automated exploit generation

Consulting Services

• Red Team Operations & APT Simulation • Custom Malware & Exploit Development • Vulnerability Research & Security Assessments