Prashant Saini

Senior Security Researcher │ OSEP, OSCP, CRTE Certified │ WorldSkills 2024 Winner

A highly passionate and dynamic professional with three years of robust experience in Offensive Security within the field of Cyber Security. I hold industry-recognized certifications, including OSEP, OSCP, and CRTE, and I am proud to be a WorldSkills 2024 winner in Cyber Security. My expertise spans multiple cybersecurity domains, encompassing both Red Team (offensive) and Blue Team (defensive) operations, enabling me to tackle security challenges from various perspectives. I am currently seeking an ideal opportunity to further contribute to and grow within the cybersecurity field.

✉ prashant.saini345@gmail.com

🗔 0xprashant.in

⌨ github.com/0xprashant

📍 Roorkee , Uttarakhand, india

🔗 linkedin.com/in/0xprashant

💼 WORK EXPERIENCE

Senior Security Researcher
Firecompass

10/2021 - Present   *Bangalore , India*

Single Platform for Automated Pen Testing, Continuous Automated Red Teaming & NextGen Attack Surface Management

Task/Responsibility

- *Executing Red Team operations and penetration testing projects while leading teams for clients in diverse industries, including fintech, banking, automotive, and consulting at FireCompass.*
- Conducts comprehensive reconnaissance and OSINT for clients to enhance external attack surface understanding and management
- Creating an end to end automation algorithms and programs for automation of red team activities and FireCompass product improvement.
- Leading and conducting Ransomware Simulation and Cyber Drill assessments
- Conducting advanced phishing and post-phishing exercises for clients, aimed at facilitating initial access.
- As a senior member, I assist the team with various requirements, including penetration testing, Red Team projects, and research activities.
- Writing a comprehensive and detailed report for the assessment conducted for the client, focusing on low-level insights and findings.
- Conducts adversary emulation for various clients, including scenarios that simulate an assumed breach.

CrowdSource Researcher
Synack red team and Yogosha

Synack and Yogosha are crowdsourced bug bounty platforms that provide private access to various assessments related to penetration testing for researchers.

Tasks/Responsibilities

- Conducting web application and network penetration testing on host-based programs through Synack.
- Creating a comprehensive report of identified vulnerabilities, including descriptions, steps to reproduce, impact analysis, and recommended remediations.

🏆 HONOR AWARDS

World Skills 2024 Winner (Cybersecurity) ⬀
Medallion For Excellence

- I had the honor of receiving the Medallion for Excellence, a fourth-category medal, for my country, India, at the prestigious WorldSkills competition in the Cybersecurity skill. After four days of intense competition against 21 countries, I excelled in both Blue Team and Red Team challenges during a CTF-based event, which also involved tasks related to system and network hardening.

India Skills 2024 Champion (Cybersecurity)
Gold Medalist

- I won an all-India cybersecurity competition and was awarded the Gold Medal in a national event, representing my state, Uttarakhand, in a 3-day competition against 18 states of India. The event included system hardening, a Red Team CTF, and a Blue Team CTF on respective days. Following this achievement, I was selected to represent my country on the world stage as a face of cybersecurity at WorldSkills 2024.

📜 CERTIFICATES

OffSec Experienced Penetration Tester (OSEP) ⬀
I have successfully qualified in the exam conducted by OffSec for the PEN-300 course: Advanced Evasion Techniques and Breaching Defenses and obtained the respective OSEP certification.

Offsec Certified Professional (OSCP) ⬀
I have successfully qualified in the exam conducted by OffSec for the PEN-200 course: Penetration Testing with Kali Linux, and earned the OSCP certification.

Certified Red Team Expert (CRTE) ⬀
I have successfully qualified in the exam conducted by Altered Security for the Windows Red Team Lab and earned the Certified Red Team Expert (CRTE) certification.

HackTheBox Cybernetics [Red Team Operator 3] ⬀
I have achieved 100% completion of the Elite Red Team Lab "Cybernetics," which is on par with the Red Team Operator 3 level, and obtained the completion certificate.

HackThebox Rastalabs [Red Team Operator 2] ⬀
I have achieved 100% completion of the Elite Red Team Lab "Rastalabs," which is on par with the Red Team Operator 2 level, and obtained the completion certificate.

PUBLICATIONS

Blogs
Offensive Security Blogs ⬀
blog.0xprashant.in

I post write-ups for HackTheBox machines and challenges on my blog, along with detailed exam reviews.

EDUCATION

Bachelor of Technology in Computer Science Engineering
Quantum University Roorkee

08/2018 - 08/2022

Bachelor of Computer Science Engineering with a specialization in Cyber Security.

- Developed a web application for messaging, cloud storage, and secret storage from scratch using Java Servlets and Hibernate.

TECHNOLOGIES AND TOOLS

- MITRE ATT&CK TTPs, NIST, CVSS, OWASP (Not Limited to)
- Burp Suite Pro, Nessus Pro, Acunetix, Nuclei, Metasploit (Not Limited to)
- Cobalt Strike, BruteRatel C4, Bloodhound, Impacket Tools (Not Limited to)
- Python, Bash, C#, Powershell (Not Limited to)

FUTURE GOALS AND PROJECTS

OffSec Web Expert (OSWE)
WEB-300: Advanced Web Attacks and Exploitation

Cloud Security and Cloud Red Teaming
Enhancing my skills in Cloud Security and associated Red Team operations.

CERTIFICATES

HackThebox Offshore Red Team Operator 2] ⬀
I have achieved 100% completion of the Elite Red Team Lab "Offshore," which is on par with the Red Team Operator 2 level, and obtained the completion certificate.

ACHIEVEMENTS

HackTheBox - Bug Killer Badge (2020) ⬀
- Found and reported a security bug in the HackTheBox platform, awarded with bug killer badge as reward/appreciation.

Oracle - Critical Patch HOF (2021) ⬀
- Found and reported vulnerability in Oracle products and got Hall of Fame as appreciation/reward.

AREA OF EXPERTISE

Web Application Penetration Testing

Network Penetration Testing

Active Directory Penetration Testing

Attack Surface Reconnaissance

Security Automation (Python)

Adversary Emulation

Phishing Simulation

Source Code Review

Network Forensics

Linux System Hardening

Incident Response