Shubham Ranpise

shubhamrnps@gmail.com 9370096139 Mumbai/Pune shubhamranpise.com shubham-ranpise

Profile

With OSCP and eJPT certifications. As a Cybersecurity Analyst at KPMG, I performed penetration testing, network security, and API/mobile application assessments, also managed firewall access reviews and implemented comprehensive security controls to safeguard critical systems.

Education

Savitribai Phule Pune University 2021 – 2024
Bachelor of Business Administration - Computer Application [BBA-CA]
GPA 8.55

Experience

KPMG 2024/09 – present
Cyber Security Analyst Mumbai (On-Site)

- Conducted **internal and external network penetration tests** for a BFSI client, targeting live infrastructure to identify exposed services, weak configurations, and privilege escalation paths across corporate environments.
- Performed **web application penetration testing**, identifying OWASP Top 10 vulnerabilities including IDOR, XSS, authentication flaws, and insecure session handling across high-value applications.
- Executed **API security testing** across RESTful and SOAP endpoints, uncovering broken object-level authorization, improper input validation, token misconfigurations, and access control issues.
- Delivered detailed **technical reports with business-aligned remediation**, working directly with developers and infra teams to implement secure configurations and retest resolved issues.

SecureLayer 7 2024/06 – 2024/08
Security Consultant Intern Pune(Remote)

- Performed security assessments on web applications, identifying and reporting vulnerabilities with actionable remediation steps.
- Provided detailed reports with remediation recommendations to improve the security posture of the applications.

Certifications

OSCP — (Offensive Security Certified Professional) | Credential ID 92620888 | January 2024

eJPT — (eLearnSecurity Junior Penetration Tester) | Credential ID 79634453 | October 2022

Skills

Penetration Testing Expertise
Deep experience in internal and external network assessments, leveraging TCP/IP and OSI knowledge to identify misconfigurations and vulnerable services. In Kali Linux, I use tools such as Nmap, ffuf, WPScan, DNSRecon, and Metasploit—following the Cyber Kill Chain—from reconnaissance through post-exploit validation with custom Python and Bash scripts.

Windows & Active Directory Exploitation
Proficient in Windows privilege escalation and AD attacks. I perform Pass-the-Hash, Kerberoasting, AS-REP Roasting, and credential dumping with Mimikatz, map domains with BloodHound/SharpHound, and leverage CrackMapExec, Empire, and Covenant for lateral movement and persistence.

Web Application & API Security
Skilled in uncovering OWASP Top 10 flaws such as IDOR, XSS, SQLi, auth bypass—and business-logic errors using tools such as Burp Suite, Gobuster, and Nessus. For API testing, I craft and fuzz requests in Postman and soapUI, detecting broken authorization, rate-limit bypasses, and improper input validation, then translate findings into precise remediation guidance.

Projects

Home Lab

- In my home lab, explored Large Language Models (LLMs) and agentic AI frameworks to automate tasks and prototype cybersecurity tools; also built educational projects using NodeMCU, such as Wi-Fi deauthers and jammers, for hands-on experimentation.
- Solved over 220+ CTF challenges across platforms such as TryHackMe, Hack The Box, VulnHub, PortSwigger, and Offensive Security Proving Grounds