Penetration Tester / Ethical Hacker

Security | SMB | Enterprise

[Company Name] is seeking a Penetration Tester to proactively identify security vulnerabilities in our applications, infrastructure, and cloud environments. You will conduct authorized attack simulations, write detailed findings reports, and work with engineering teams to validate remediations. This role is ideal for a creative, methodical security professional who enjoys thinking like an adversary to protect our users and data.

Key Responsibilities

- Conduct web application, API, and network penetration tests against production and staging environments
- Perform cloud infrastructure security assessments across AWS, Azure, or GCP environments
- Write clear, actionable penetration test reports with risk ratings and remediation guidance
- Collaborate with development teams to validate that remediations effectively resolve identified vulnerabilities
- Research emerging attack techniques, CVEs, and exploit chains to keep testing methodologies current
- Participate in red team exercises and adversary simulation campaigns
- Contribute to the development of internal security testing tools and automation

Required Skills & Experience

- 3+ years of experience in penetration testing or offensive security roles
- Strong knowledge of web application vulnerabilities (OWASP Top 10) and exploitation techniques
- Proficiency with penetration testing tools such as Burp Suite, Metasploit, and Nmap
- Experience with scripting for custom exploits and automation (Python, Bash, or PowerShell)
- Understanding of networking protocols, common misconfigurations, and privilege escalation techniques
- Ability to write clear, professional penetration test reports for both technical and executive audiences
- Familiarity with cloud security assessment methodologies

Nice-to-Have

- Relevant certifications (OSCP, GPEN, GWAPT, or CRTO)
- Experience with mobile application penetration testing (iOS and Android)
- Knowledge of Active Directory attack paths and Kerberos exploitation
- Contributions to bug bounty programs or published CVEs
- Experience with container and Kubernetes security testing

Tech Stack

Burp Suite Professional | Metasploit | Nmap | Cobalt Strike | BloodHound | Kali Linux | Python | Wireshark | Nuclei

What We Offer

- Competitive salary and equity package
- Flexible remote or hybrid work arrangement
- Health, dental, and vision insurance
- Annual learning and development budget
- Generous PTO policy

Interview Process

1. Recruiter phone screen (30 min) — role fit and logistics
2. Technical phone screen (45 min) — security fundamentals and methodology discussion
3. Practical exercise — conduct a time-boxed penetration test on a deliberately vulnerable application
4. Report review — present findings and remediation recommendations to the security team
5. On-site or virtual final round (2 hours) — red team scenario discussion and team fit
6. Offer and reference checks