YUPRO PLACEMENT
PART OF YEAR UP UNITED

This is a skills-based job posting example for a Penetration Tester. It puts skills and capabilities front and center and does not include any unnecessary obstacles that could discourage excellent candidates from applying. Moreover, it is presented in an inclusive and welcoming way to all potential candidates. You can use this as a template: Select "File" and "Make a copy" and then edit the document to meet your needs.

SKILLS-BASED JOB POSTING: PENETRATION TESTER (JUNIOR LEVEL)

Job Title: Penetration Tester (Junior Level)

Company Overview: *(Describe what makes your company unique and the importance of offensive security in your organization.)*

Junior Penetration Tester Job Description: *(Please describe why the role is being filled and how it fits into the organization and the team.)*

We are hiring a **Junior Penetration Tester** to help strengthen our security posture by identifying and mitigating vulnerabilities across our digital infrastructure. This role is ideal for individuals passionate about ethical hacking, security assessments, and continuous learning.

Junior Penetration Tester Job Responsibilities:

- Conduct penetration testing on networks, web applications, and cloud environments.
- Identify, document, and report security vulnerabilities with risk-based recommendations.
- Assist in security research to identify emerging threats and testing methodologies.
- Work with security engineers and developers to remediate vulnerabilities effectively.
- Maintain and refine automated security testing tools and methodologies.
- Participate in red teaming exercises and security audits.

YUPRO PLACEMENT
PART OF YEAR UP UNITED

Preferred Skills:

- Hands-on experience with penetration testing tools such as Metasploit, Burp Suite, Nmap, and Wireshark.
- Understanding of OWASP Top 10 vulnerabilities and exploitation techniques.
- Familiarity with scripting and automation (Python, PowerShell, Bash).
- Knowledge of cloud security fundamentals (AWS, Azure, Google Cloud).
- Analytical skills to assess security risks and recommend mitigation strategies.
- Documentation and communication skills for reporting findings to stakeholders.

Preferred Certifications *(Certifications are highly regarded but not mandatory. Candidates with equivalent experience or a strong willingness to obtain certifications are encouraged to apply.)***:**

- Offensive Security Certified Professional (OSCP)
- eLearnSecurity Junior Penetration Tester (eJPT)
- Certified Ethical Hacker (CEH)
- GIAC Penetration Tester (GPEN)

Valuing Transferable and Diverse Skillsets: We recognize that valuable skills can be developed through a variety of experiences. We encourage applicants with transferable skills from diverse backgrounds, including those transitioning from non-traditional careers, to apply.