Penetration Tester

Employment Type
Full-time

Hiring organization
CrowdStrike

Job Location
USA
Remote work possible

Base Salary
$ 110,000 - $ 160,000

Description

?? Why This Job Isn't Just "Red Teaming"

CrowdStrike doesn't just find vulnerabilities — they hunt adversaries. As a **Penetration Tester**, you'll get paid to think like the bad guys and break into some of the most high-profile environments on the planet. Except here, instead of going to jail, you'll be building reports, helping defenders harden systems, and flexing your skills against real-world enterprise defenses.

If you love the adrenaline rush of finding that one overlooked misconfig and turning it into domain admin, welcome home.

?? At a Glance

Detail
Info

Estimated Salary Range
$110,000 – $160,000/year (varies by experience & location)

Location
Remote (U.S. preferred) with some travel for client engagements

What You'll Tackle
Web app pentests, network assessments, cloud environment exploitation, social engineering campaigns

Tech You'll Use
Kali Linux, Burp Suite, Cobalt Strike, Metasploit, custom scripts (Python/Go/PowerShell)

Certs That Help
OSCP, OSWE, OSEP, GPEN, GXPN

??? What You'll Do

- Perform penetration tests across apps, networks, endpoints, and cloud.
- Emulate adversary techniques (yes, red team fun included).
- Chain vulnerabilities into impactful attack paths (because one CVE isn't enough).
- Deliver clear reports: what you found, why it matters, and how to fix it.
- Collaborate with blue teams to help them detect + respond better.
- Stay sharp by researching new exploits, tools, and attack surfaces.

?? What You Bring

- 3–5+ years of hands-on pentesting or red team ops.
- Proficiency with common tools **and** custom exploit development.
- Strong understanding of attack methodologies (OWASP Top 10, MITRE ATT&CK).
- Solid reporting + communication skills (you'll brief execs, not just engineers).
- Bonus: experience in cloud pentesting (AWS, GCP, Azure) and mobile apps.

?? Why CrowdStrike?

- Work with one of the **most recognized names in cybersecurity**.
- Engage with a wide range of clients — no two projects are the same.
- Collaborate with elite red + blue teams who live and breathe threat intel.
- Competitive pay, remote flexibility, and a research-driven culture.
- Your work directly impacts how enterprises defend against advanced threats.

? Ready to Hack (Legally)?

- Bring a resume that shows where you've broken stuff (ethically).
- Be ready to walk through an engagement you crushed and how.
- Apply via CrowdStrike's career site or DamnJobs — but don't wait too long.
- Check out related roles like **Red Team Operator** or **Adversary Emulation Specialist**.