Cybersecurity Pentester

Job: Consulting
Job Title: Cybersecurity Pentest Engineer
Primary Location: California
Schedule: Part-time
Travel: 25-50% of the Time

A successful Pentest Engineer consultant at Novesh should possess a deep understanding of both information security and computer science. They should understand basic concepts such as networking, applications, and operating system functionality and be able to learn advanced concepts such as application manipulation, exploit development, and stealthy operations. This is not a “press the ‘pwn’ button” type of job; this career is technical and challenging with opportunities to work in some of the most exciting areas of security consulting on extremely technical and challenging work. A typical job could be breaking into a segmented secure zone, reverse engineering an application and encryption method in order to gain access to sensitive data, all without being detected. If you can exploit at scale while remaining stealthy, identify and exploit misconfigurations in network infrastructure, parse various types of output data, present relevant data in a digestible manner, think well outside the box, or are astute enough to quickly learn these skills, then you’re the type of consultant we’re looking for.

About Novesh Ltd.

Novesh provides innovative and state-of-the-art cybersecurity solutions and products to help businesses and organizations in securing their networks and protect their data from cybersecurity breaches. The core mission behind our work is to help companies thrive with a strong IT and OT cybersecurity infrastructure. We offer a thorough assessment of companies’ IT and OT/ICS/SCADA/IIoT networks and facilitate their regulatory compliance process via automation. Novesh serves companies and organizations in different industry sectors and verticals.

Responsibilities:

In this role, you’ll be faced with complex problem solving opportunities and hands-on testing opportunities on a daily basis. We help our clients protect their most sensitive and valuable data through comprehensive and real world scenario testing. If you are a part of the red team, the objective doesn’t end at gaining “domain admin” or “root”; this is expected and is only a starting point. This is expected to quickly assimilate new information as you will face new client environments on a weekly or monthly basis. You will be expected to understand all the threat vectors to each environment and properly assess them. You will get to work with some of the best red teamers in the industry, causing you to develop new skills as you progress through your career.

To qualify for the role you must have

- A bachelor's degree in a related field and approximately 3 years of related work experience; or a graduate degree and approximately 2 years of related work experience

- Perform network penetration, web and mobile application testing, source code reviews, threat analysis, wireless network assessments, and social-engineering assessments
- Demonstrating experience with common pentesting tools;
- Demonstrating proficiency with a programing or scripting language (C/C++, C#, Python, Go, PowerShell);
- Demonstrating knowledge of Active Directory concepts;
- Demonstrating knowledge of Azure, Google Cloud and Amazon Web Services;
- Demonstrating knowledge of the MITRE ATT&CK Framework;
- Demonstrating high level understanding of the principles of information security engineering, architecture, and application security; and,
- Demonstrating prior system administration, incident response, Security Operations Center (SOC) or network engineering experience.
- A strong background of the security frameworks and standards such as ISO 27001/2, PCI DSS, NIST 800-53 and the cybersecurity laws and regulations such as HIPAA, FISMA and GLBA
- A willingness to travel to meet client needs; travel estimated at 30%; a valid driver's license in the US
- Develop comprehensive and accurate reports and presentations for both technical and executive audiences
- Effectively communicate findings and strategy to client stakeholders including technical staff, executive leadership, and legal counsel
- Recognize and safely utilize attacker tools, tactics, and procedures
- Develop scripts, tools, or methodologies to enhance pentesting processes

Ideally, you'll also have

- Strong presentation and communication skills
- CISSP, CISM, CISA, CIPT, CIPM, CRISC or other relevant certification desired

What We Look For

We're interested in intellectually curious people with a genuine passion for cybersecurity. With your broad exposure across Cybersecurity, we will rely on you to speak up with innovative ideas that could make a lasting difference not only to us – but also to the industry as a whole. If you have the confidence in both your presentation and technical abilities to grow into a leading expert here, this is the role for you.

If you can demonstrate that you meet the criteria above, please apply via Novesh website, www.novesh.om from the career section or email us your resume and letter of application to jobs@novesh.com.

Equal Employment Opportunity
Novesh is an equal opportunity, affirmative action employer providing equal employment opportunities to applicants and employees without regard to race, color, religion, age, sex, sexual orientation, gender identity/expression, national origin, protected veteran status, disability status, or any other legally protected basis, including arrest and conviction records, in accordance with applicable law. Novesh is committed to providing reasonable accommodation to individuals with disabilities. If you are a qualified individual with a disability and either need assistance applying online or need to request an accommodation during the interview process, please email jobs@novesh.com