{B(W)} CYBER SERVICES

Penetration Tester

Overview

Emulate adversary tactics, techniques, and procedures (TTPs) to validate security controls effectiveness; develop rules of engagement, brief clients on findings and mitigation techniques

Key Responsibilities

- Perform technical security assessments of client environments which include (non-exclusive):
  - Infrastructure Penetration Tests
  - Vulnerability Assessments
  - Web Application Tests
  - Wireless Security Tests
  - Social Engineering Campaigns (phishing, spearphishing, and pretexting)
  - Public Cloud Hygiene Reviews
- Develop rules of engagement, and configure, tune, and operate industry standard assessment tools
- Coordinate, schedule, and support security testing requests
- Evaluate findings to determine applicability, saturation, and potential impact
- Analyze results and produce reports for clients
  - Detailed technical reports for IT staff
  - High-level summary presentations for executives
- Advise client stakeholders of findings and provide remediation guidance
- As appropriate, monitor remediation efforts of findings and communicate progress to stakeholders
- As appropriate, work with client stakeholders to develop Plan of Action & Milestones (POA&M) tracker to ensure identified weaknesses are addressed in a timely and cost-effective manner
- As needed, assist in cyber incident response for clients

Desired Skills

- Expertise creating exploits for vulnerabilities or demonstrated expertise using a scripting language such as PowerShell, Python, Ruby, or Perl for penetration testing or incident response
- Expert in common vulnerability scanners, e.g. Nessus, OpenVAS, Qualys
- Expert in common penetration testing tools, e.g. Metasploit, Burp, ZAP

Experience Required

- Bachelor's degree or higher
- 3-5 years of experience in penetration testing or incident response
- One of the following active certifications: Exploit Researcher and Advanced Penetration Tester (GXPN), Offensive Security Certified Expert (OSCE), Offensive Security Certified Professional (OSCP), Offensive Security Exploitation Expert (OSEE) or one or more years' experience responding to Advanced Persistent Threat (APT) type incidents

Desired Location: Raleigh, NC

Interested in joining our team? Please send your resume and cover letter to info@bwcyberservices.com.