WarCollar industries

Clearance Level Needed: None - TS/SCI

Category: Commercial and Government

Location: Virtual/Washington DC Metro Area

Penetration Tester

A penetration tester shall be capable of performing complex assessments while maintaining a focus on meeting client requirements. This position will work both independently and as part of a team to perform Security Assessments including vulnerability assessments and penetration tests. A Penetration tester also contributes to the development and continuous improvement of the Security Assessment practice through various team and industry contributions.

Job responsibilities include:

1. Assess an organization's network security posture through the use of automated tools and manual techniques to identify and verify common security vulnerabilities
2. Use creative approaches to identify vulnerabilities that are commonly missed in security assessments
3. Exploit vulnerabilities and identify specific, meaningful risks to clients based on industry and business focus
4. Perform complex wireless attacks both against wireless clients and access points
5. Use social engineering techniques to obtain sensitive information, network access and physical access to client sites
6. Execute opportunistic, blended and chained attack scenarios that combine multiple weaknesses to compromise client environments
7. Create comprehensive assessment reports that clearly identify root cause and remediation strategies
8. Interface with client personnel to gather information, clarify scope and investigate security controls.
9. Execute projects using established methodology, tools and documentation
10. Collaborate with other team members and practices to complete client projects and practice contributions
11. Maintain industry credentials/certifications
12. Participate in industry conferences to include delivering presentations
13. Provide support in the ongoing development of security assessment offerings through tool creation and process improvement
14. Perform other duties as assigned

Desired Qualifications:

1. Experience performing Vulnerability Assessments, Penetration Tests, Wireless Security Assessments and and/or Social Engineering including:
    a. Network Vulnerability Assessments
    b. Penetration Tests
    c. Wireless Network Security Assessments
    d. Social Engineering (Telephony, onsite and remote pre-texting, spear phishing, etc.)
    e. Product/Hardware Security Assessments
    f. Web application Vulnerability Assessments (SQLi, XSS, Session management issues, etc.)
2. Experience in a consulting services role, or related information security positions
3. Bachelor's Degree from a four-year college or university; or equivalent combination of education and experience
4. OSCP, OSCE, GIAC, CISSP certifications preferred
5. Ability to combine multiple separate findings to identify complex blended vulnerabilities
6. Ability to identify, describe and report of overall information system risk to clients through post-exploitation activities required.
7. Mastery of commercial and open source security tools required (e.g. Nessus, Nexpose, SAINT, Qualys, Burp, Nmap, Kali, Metasploit, Meterpreter, Wireshark, Kismet, Aircrack-ng etc.)
8. Familiarity with many different network architectures, network services, system types, network devices, development platforms and software suites required (e.g. Linux, Windows, Cisco, Oracle, Active Directory, JBoss, .NET, etc.) required.
9. Demonstrated ability to create comprehensive assessment reports required.
10. Must be able to work well with customers and self-manage through difficult situations, focusing on client satisfaction.
11. Ability to convey complex technical security concepts to technical and non-technical audiences including executives required.
12. Ability to work both independently as well as on teams required.
13. Ability to lead and mentor others.
14. Willingness to collaborate and share knowledge with team members.
15. Proven ability to review and revise reports written by peers.
16. Demonstrated effective time management skills, ability to balance multiple projects simultaneously and the ability to take on large and complex projects with little or no supervision required.
17. Motivation to constantly improve processes and methodologies required.
18. Passion for creating tools and automation to make common tasks more efficient required.
19. Project management experience preferred.
20. Strong programming skills preferred (Python, Ruby, Node.js, C/C++, Assembly, etc.)
21. Reverse engineering/Binary analysis experience (firmware, x86 applications, etc.) preferred.