Article Side

Penetration Testing Jobs â€“ a Valuable Online Resource by Stephanie Barnes

Article published on July 11th 2012 | Career

Prestigious companies and organisations, precisely because of their relative success and high profiles, always need to be on the lookout for IT security threats. Furthermore, they are not being over-cautious â€“ far from it. During 2011, the UK government published a report stating that cybercrime was costing the economy some 27 billion pounds a year. Businesses took most of the hit, with losses to business standing around 21 billion pounds a year. Indeed, 2011 is sometimes reported as being the worst year in modern computing history for security breaches of high-profile companies. As a consequence, enterprises are increasingly taking preventative measures, including penetration testing. Indeed, there are often plenty of penetration testing jobs available if you happen to be in the market for one of these roles.

Penetration testing is the process of simulating a hacking attack or other security breakdown on a company server in order to expose vulnerabilities, which can then be addressed and hopefully fixed. The roots of penetration testing lie in ethical hacking. Ethical hacking is the approved, or fully authorised, intrusion into a computer network with the aim of exposing vulnerabilities. In the past, bona fide hackers with genuine experience of unauthorised hacking were hired ad hoc by concerned managers to break in to their networks on a â€œwhite hatâ€• basis. Today, ethical hacking is now much more formalised and penetration testing jobs no longer require a background in genuine â€œblack hatâ€• hacking.

There are a number of professional qualifications and certifications available for those in the market for any of the various penetration testing jobs. For example, the respected not-for-profit â€œTiger Schemeâ€• provides three formal certifications: Associate Security Tester (AST), Qualified Security Team Member (QSTM) and Senior Security Tester (SST). Furthermore, the Information Assurance Certification Review Board (IACRB) provides the Certified Penetration Tester (CPT) qualification. There are plenty of opportunities available today for penetration testers looking to raise their profile in the job market by adding some specific, professional qualifications to their CVs.

Penetration testing jobs break down in to a number of tasks, all linked together and designed ultimately to increase a clientâ€™s confidence in their systems. For instance, it is likely a test will go through a number of phases. These include:

Scoping â€“ deciding on and listing the appropriate targets for testing

Vulnerability scanning â€“ testing for known weaknesses

Target penetration â€“ if felt necessary, systems may, with full permissions, be compromised

Analysis â€“ a thorough analysis of the test results

Reporting â€“ reporting back to the client, often using less technical language than in the analysis stage, with the emphasis on what actions need to be taken

Acumin is a leading recruitment agency with years of experience behind them in the information security business. Penetration testing jobs are a common feature of their books and, what is more, they provide a personal, supportive and friendly service to their candidates and their clients who are striving to fill vacancies, sometimes at short notice. Their website is an invaluable first port-of-call for those in the market for penetration testing jobs.

Article Source:
http://www.articleside.com/career-articles/penetration-testing-jobs-a-valuable-online-resource.htm - Article Side

Stephanie Barnes - About Author:
Stephanie has being writing for Acumin for many years, and is an expert in the field of a penetration testing jobs and recruitment. Find out more at http://www.acumin.co.uk

Article Keywords:
Penetration Testing Jobs, Information Security Recruitment, Information Security Jobs, IRM Recruitment, Infosec jobs

You can find more free articles on Article Side. Sign up today and share your knowledge to the community! It is completely FREE!