The term “hacker” has been in mainstream use for over a decade now. However, who really is a “hacker”? “Should we fear hackers? Intention is at the heart of this discussion,” wrote Kevin Mitnick, commenting on the “hacker hysteria” seen in the media (2000). For hackers, there are two primary intents: (1) to explore vulnerabilities and find new exploits so they can be fixed by developers, without hurting the organization, or (2) finding vulnerabilities and using those vulnerabilities to deface, steal, or other malicious and illegal acts. The former is known as an “ethical hacker” or “white hat” while the latter is known as a “cracker” or a “black hat”. In the field of cybersecurity, ethical hackers a.k.a. “penetration testers” (“pen tester” for short) are one of the many jobs where demand is steadily growing (“Penetration Tester”). In this paper I will explore the job of a penetration tester and what is needed to have a successful career.

Pen testers can work on a wide range of attack vectors, from websites to application servers and get paid to try and penetrate into these systems, hence the job title. Many of the available jobs are for private IT consulting firms, giving risk assessments to other companies or the government. One such job description is from TASC, a defense contractor who writes in the listing:

“TASC is searching for a Penetration Tester for upcoming work located in Chantilly. Candidates will work on a dynamic team responsible for providing support to customer’s enterprise cyber security program with Certification and Accreditation (C&A) of their IT systems, large and small. The team will provide C&A testing, engineering support, penetration testing, and media sanitization services to ensure compliance of Government IT systems with ICD 503, DCID 6/3, FISMA, and other Information Assurance laws, directives, policies and regulations. The candidate will:
• Provide support to all organizational Information Technology (IT) projects with obtaining Certification and Accreditation (C&A) approval
• Develop and document security test plans and procedures
• Assist in research and evaluation of INFOSEC policies
• Hands-on security testing, analysis of results, document risks and recommend countermeasures
• Assess/calculate risk based on threats and vulnerabilities
• Perform network security analysis and risk management
• Perform compliance check for unauthorized wireless networks during customer events
• Conduct assessments of authorized wireless technologies”

("Penetration Tester Job Details")

This job description shows that penetration testing is not just for the sake of patching holes, but because if those holes are left unpatched the organization in question will not be compliant with various IT standards. This is especially important in healthcare IT, where a security breach could lead to confidential patient data being leaked. Penetration testing is critical in fields which deal with financial data (credit card numbers, bank account info, etc.) as businesses could suffer major losses, more than the cost of hiring a penetration tester, if criminals exploit the vulnerabilities first. One example of this is the recent Target data breach, in which 40 million customers’ credit/debit card information was stolen (not counting additional personal information stolen). The breach cost at least $17 million to Target, far greater than the cost of an independent security audit (The Associated Press, 2014).

As a penetration tester, one’s responsibilities are to conduct formal tests on computer systems, whether it be a website, desktop application, network, server, etc. These tests are conducted on a regular basis so that security can be assured regularly. Pen testers may also be responsible for developing information security policies and training employees (usually other IT staff) on how to follow those policies and procedures. When carrying out a penetration test, they must document steps taken to exploit systems so those responsible for ensuring security can
perform the appropriate action to patch the holes, or if unable to patch the holes, mitigate risk as much as possible ("Penetration Tester").

In order to gain the skills necessary for becoming a pen tester, there are many ITM courses one can take. Pen tester job requirements include experience in vulnerability research and reverse engineering, so one can take ITMS 443, Vulnerability Analysis and Control, to get the necessary skill set. Second, any pen tester should have knowledge of the various tools available for cracking into a system, so ITMS 448, Cyber Security Technologies, can be used to gain that knowledge. When pen testers go about trying to exploit a program, they can either go with a black-box approach or a white-box approach. In a white-box approach, the source code is available to the tester, so they must have knowledge of how the code works (Wilhelm, 2010). Therefore, courses such as ITMD 415, Advanced Software Development, and ITMD 463, Intermediate Web Application Development will be useful. A pen tester may not always deal with applications though, so having networking skills from ITMO 441, Network Administration and Operations, is also important. Other relevant security courses include ITMS 428, Database Security, and ITMS 458, Operating System Security as being able to know what to do and what not to do is a desired skill. Finally, ITMM 485, Legal and Ethical Issues In Information Technology is a good course to take as pen testers often run into ethical issues when trying to exploit systems, so knowing how to deal with these issues is part of a job security plan ("Course Descriptions").

Not only are there many courses one can take to properly prepare for the job, but there are also lots of certifications one can get in order to gain access to special open positions or with certain employers. The most common certifications listed in job descriptions are “Certified Ethical Hacker” (CEH), “Certified Penetration Tester” (CPT), “Certified Reverse Engineering
Penetration testers are essentially hackers that get paid for what they do. Unlike the hackers portrayed in the media, pen testers break into systems and then turn back towards the organization to help patch the holes so they can no longer exploit those systems. I find this job to be a fun one. As I have always enjoyed puzzles, especially ones involving computers, I would like to have this job. Having participated in a cybersecurity competition recently, which was primarily penetration testing, the job is something I believe I could do well in. However, if I continue with web development, I would like to also perform the same tests that pen testers perform, so that the code I write is even more secure. Regardless, as more enterprises join the technology revolution and develop their own software, penetration testers are going to be in high demand (Woodford, 2005).
References


