Seven Super Security Certifications

In today's IT Security world, maintaining a competitive advantage in the marketplace is an absolute must. Although having real world experience does speak volumes for itself, having extra credentials behind it will add even more credibility to your name. Apart from that, having a major Security certification will not only separate you from the thousands of other applicants, but one can command a higher income as well.

The world of IT Security is very broad, so choosing the right certification for your career path is very important. For instance, there are fields opening up every day in Cyber Security, Network Security, Physical Access Security, Logical Access Security, Computer Security, etc. Some of the Security certifications are very broad in nature, whereas some are very specific.

Therefore, the goal of this article is to review the Top 7 Security Certifications which are available on the marketplace today, in an effort to help you select what is not only best for you, but will fuel and propel your career to brand new heights.

The Certifications

1) The Certified Penetration Testing Consultant (CPTC):

   Are you in the Network Security field, and the core of your work is in Penetration Testing? This field involves the testing and scanning of Security Vulnerabilities in a business or organization's Networking Infrastructure. The CPTC is more of a general type of certification, and is geared towards the professional whom is involved more in the business end of Penetration Testing. For example, this would involve developing and formulating the plan as to how an actual Penetration Test would operate, as well as setting up and establishing objectives and Key Performance Indicators (KPIs).

2) The Certified Penetration Testing Engineer (CPTE):

   The Penetration Testing Engineer is the actual person who follows the plans set forth as described above, and conducts the actual test, simulating Security breaches and threats against a businesses' or an organization's Servers, Firewalls, Routers, etc.

   You can take one or the other of these exams, or even both. Obviously taking both will greatly enhance your career, because it shows not only that you can plan a Penetration Test, but you can conduct one also. Both of these certification exams are offered by Mile2. Both of these exams consist of 100 multiple choice questions, and must be completed within 120 minutes. You must have a score of at least 75% in order to pass these exams.

3) The CompTIA – Security+:

   The Security+ Certification has been around for a very long time, thus giving strong credence to its coveted market value which it possesses. The organization which offers this Certification – CompTIA has also been in business for a very long time as well. It also continues to be a Security Vendor free testing organization. The Security based topics which are covered in this exam include the following knowledge domains:

   - Threat Mitigation;

- Cryptography;
- Authentication Systems;
- Messaging Security;
- User/Role Based Security;
- Public Key Infrastructure (PKI);
- Access Security;
- Network Ports and Protocols;
- Network Security;
- Wireless Security;
- Remote Access Security;
- Auditing/Logging/Monitoring;
- Penetration/Vulnerability Testing;
- Business/Organizational Security;
- Business/Organizational Continuity.

It is required that any Security Professional taking this exam must have at least a minimum of two years of real world work experience. This Certification Exam is regarded in the IT Security industry as one of the toughest ones to pass. But if you do make, the monetary accolades of it are phenomenal. To learn more about this exam, click here.

4) The Certified Security Testing Associate (CSTA):

This Security Certification Exam is currently maintained and operated by a testing organization in the United Kingdom known as '7Safe'. This is a relatively newer Certification Exam, but it too is also requires very comprehensive and detailed knowledge on part of the test taker. For example, this Certification Exam consists of a rigorous four day lecture based course, but is also designed to be both practical and very much hands on oriented.

In order to successfully pass this Security Certification Exam, one has to think and act very much like a Cyber based attacker. Therefore, coursework is geared primarily towards the IT Security personnel, Chief Information Security Officers (CISOs), Network System Administrators, and Penetration Testers as well.

5) The OPEN – GIAC Certified Penetration Tester:

Unlike the first two Network Penetration Certification Exams reviewed, this one is considered to be the most comprehensive available in the IT Security industry today. For example, its focus geared on solving actual Network Penetration problems and scenarios. The coursework that is involved includes the following topics:

- Detecting weak and extremely vulnerable Network Security Systems;
- Critically examining unpatched Network Infrastructures;
- What do if you, as the System Administrator inherit a terribly flawed Network Security System;
- How to plan and carry out meticulous Network Port Security scanning and reconnaissance;

- Learning how to formulate and compile Network Security Audit Reports, both from a business and technical perspective.

Probably what separates the preparation and training for Certification Exam is that the test taker is given various tools to work with conducting real world Network Security Exploitation exercises.

6) The Certified Ethical Hacker (CEH):

This Certification Exam is designed to give the IT Security professional the credibility they need in order to conduct legitimate Cyber based attacks and threats from the 'Ethical' standpoint. For example, the premise behind this is that in order to fully understand on how to defeat a hacker, you need to think and behave like a real one. In other words, in order to do good by protecting the IT Assets of a business or and organization, one needs to think first in 'bad terms', like an actual hacker. Therefore, the course work that is involved in preparing the test taker includes the following topics:

- How to successfully breach a Network Perimeter Defense Infrastructure;
- How to scan for and attack vulnerable Network Ports;
- Learning how to maliciously escalate and exploit end user rights and privileges;
- Learning how successfully launch Social Engineering and Distributed Denial of Service (DDoS) attacks;
- How to create and launch a major pieces of Malware, Spyware, and Adware.

This Certification Exam is currently operated and managed by the EC Council. The actual exam consists of 150 multiple choice questions, which must be completed in a 4 hour timespan. In order to pass the exam, a minimum score of at least 70% must be attained.

7) The ECSA – EC Council Certified Security Analyst (CSA):

This Certification Exam is also offered as well by the EC Council. The focus of this coursework of this learning how to communicate effectively with a client the end results of any Security Test which may have been conducted and executed. For example, the IT Security Professional is tested on how present both effective and accurate Security Testing Data and Recommendations to an actual, real world client. This gives an extra, added advantage to the test taker after they have successfully passed the exam.