SANS GSEC Exam Preparation & Tips
Author: Leo Ni

Being a Security and Compliance professional for over a decade, I recently just undertook the SANS GSEC exam, and got some feelings and tips to share with everyone who is about to attend that exam.

Take my background for example: I am a bachelor degree holder majoring in computer science, with more than 14 years of combined working experience on the Information Security Risk Management field. I passed my CISA and ISO27001 Lead Auditor exams back to year 2005 and passed CISSP exam in year 2009. Prior to year 2002, I was focusing on more technical related topics and attained relevant technical certifications: MCSE + Internet, MCSD, MCDBA, etc.

SANS is famous for its in-depth technical research on Information Security and it is becoming more and more popular. For the CISSP designation holder like me, I would like to say, it is not as easy as people think to pass this exam. Some people may think CISSP is the ultimate certification in the Information Security field, and why bother taking SANS GSEC, and G-S-E-C is referring to GIAC Security Essential and it looks like an entry-level designation.

As a person who owns both CISSP and GSEC, I would like to say the answer is: Yes, GSEC is a SANS's entry-level designation, but it is harder and more practical than CISSP.

CISSP is ten miles wide and one-inch depth but SANS GSEC is to further most of CISSP concepts by introducing its real world and practical operation. It is commonly to see those people who passed CISSP are not able to do actual information security technical work, but you can rest assured that people who are SANS certified can do them effectively. Imaging you are the Information Security consultant of a company, how are you able to effectively give the your client (normally: technical staff) practical suggestions they are highly likely to buy-in and unlike using an "aliens' language"? For example: during the Information Security Assessment Phase, when you are walking through with your clients in discussing how to harden Linux TCP/IP rule settings. When you are being asked how to do that and whether or not there are any tools can do this in Linux? Your first reaction is using IPTABLE command, which is built-in in Linux. You can imagine the scenario that you wrongly told your clients to use other tools and later on clients figured it out by themselves. That is like a slap on the face of the professionalism of Information Security professionals.

I undertook SANS GSEC exam on Oct 18, 2013 and I used about 4 out of 5 hours in completing the exam at the score of 81 (Passing mark is 73) at the first attempt. Below are the tips in preparing for that exam:

1) Familiarizing the six books is the most important thing. Like most people mentioned, preparing an index file as much detailed as possible. However, I want to add: Please do more tests and experiments, and memorize as much topics as possible in your brain otherwise time is not allowable for you to do everything through searching for index;

2) Making the index file to be intuitive is the key. For the key world just like IPSEC, please put "IPSEC (Internet Protocol Security)" in your key column of index, instead of using "Internet Protocol Security (IPSEC)". Via this way, it can boost your searching speed during the exam;

3) Treating the two mock tests as real exams to know your skill level. Just regarding the mock test to be exactly the same like the real exam, since its difficulties and exam layout are extremely similar to the real exam. The score that you got from mock test is a good leading indicator which tells you how much score you are likely going to get in the real exam. According to the statistics, the real exam is 5% - 10% harder than the mock test. Thus, targeting at mock test score of 90, and people can normally look forward to getting about 86 in the real exam;

4) Creating Mind Map to get a clear structure of six thick books. SANS GSEC intentionally does not make a TOC (Table of contents) for us. To compensate this, we can build it on our own. For me, I am using Free Mind

software (It can be downloaded from http://freemind.sourceforge.net/) to create a mind map of SANS GSEC books. When that mind map is fully built, you will find it is very rewarding: You will have to appreciate the thought of author why they arrange the topics and sequence like that way. Although it looks it is a mass initially, you will find its structure more and more clear and logical to you, which also helps you understand the content of books better

5) Attending SANS GSEC official training workshop / courses. Although it is possible that people can get SANS GSEC by attending the challenging test by paying $999 USD, it is still recommended to attend the SANS GSEC official training workshop, especially your employer is willing to pay for the training fee. The tutors from SANS very experienced professionals and they carefully selected by SANS. They can effectively answer your questions / clear your confusions during the learning process. (Take myself for example, I had the opportunity to attend a very impressive Toronto SANS GSEC course from April 2013 to June 2013, and the tutor is Erich Samuel)

Passing SANS GSEC is just a starting point in your Information Security career, and there are much more things to update in the future. People may complain it is a little bit hard to maintain SANS GSEC in the long run but I tend to believe an ounce of gain is worth an ounce of pain, as long as if people has passion on Information Security and continuously updating it, people will find SANS courses are full of fun.

Above-mentioned are just some of my thoughts on SANS GSEC. Any of your comments and feedback is highly welcomed. We can discuss more later on. Cheers!