

Review: CEH Via Self Study

[del.icio.us](#)

Discuss in Forums {mos_smf_discuss:Hoffman}

By Daniel V. Hoffman, CISSP, CWNA, CEH

I remember the first time I heard about the Certified Ethical Hacker certification. It was around the time that I was studying for my CISSP, and I was quite intrigued simply by the name of the certification. Upon first visiting the EC-Council website to find out more about the certification, I must admit that my initial impression was that of being rather unimpressed. This was mainly due to the fact that the EC-Council website looks rather unprofessional, and I almost dismissed the CEH certification as really being rather hokey. That notwithstanding, there is a buzz around CEH, and, in looking at the actual topics that were covered, I began getting quite interested in achieving this certification. Personally, I couldn't find very much worthwhile, objective or first-hand information regarding the CEH and its Self Study program when looking online. I hope that this article is helpful to those seeking to achieve the CEH via self study. I also hope this information is useful for anyone considering the CEH vs. other security certifications.

Thoughts on the Validity of CEH after Passing the Exam

Every time my new Certified Ethical Hacker certification comes up in conversation, I am met with a look of wonder and confusion. This is easily cleared-up by explaining that possessing the knowledge of a hacker helps protect against them. Still, there are those that can't help but think that something is wrong with teaching someone how to hack, and

they never quite look at you the same knowing that you can really mess them up if you wanted to. I suppose that's not all bad. ;)

Overall, I feel as though I learned some very good information going through this process. I have been unofficially "ethically hacking" for years and read the usual hacking books, so it was nice to go through a formal process to learn about things that I never considered. I was aware of SQL injection, for example, but never really had an inclination to learn about it. Upon doing so, it was pretty interesting. Likewise, it was very useful to learn how to modify existing Trojans and Viruses, so that they could pass undetected by Anti-Virus programs. The CEH's choice of modules does a very good job in covering the areas where hackers would use their skills. If nothing else, it is a guide to the areas of technology that are vulnerable to hackers/crackers and areas that SysAdmins need to address.

The thing I liked most about the CEH is that it is very hands-on; you actually use the tools just like a hacker would. While the CISSP is the Gold Standard of security certifications, it is more conceptual than tactical. I am in no ways suggesting that the CEH is better and more worthwhile than the CISSP, though I will say that it is an excellent supplement. CISSP gives you the framework and CEH shows you how the attacks are actually done. I find that to be a pretty darned good combination, and I highly recommend it for any security professional.

An important item to realize, I believe, is that you don't have to be a genius to use most of the tools that are available to hack/crack. The intelligence in hacking/cracking is in the process itself and with those that have the deep level of understanding to create the tools that script kiddies use. Anyone can learn to use nmap, but not everyone could create the concept and code for the nmap program. Consequently, every CEH, and cracker/hacker for that matter, owes quite a bit to those that really understand the technology and developed the tools. That notwithstanding, having knowledge of these tools, how hackers/crackers actually utilize them and how to protect against them, certainly does have value in and of itself. For that reason, I am proud to have achieved the Certified Ethical Hacker certification and found the process to be very worthwhile. In the end, I was glad to find it wasn't as hokey as I had originally thought.

The Order Process and Materials Received

Initially, my intention was to achieve the CEH via a week long, boot camp style training session. I had done this for my CISSP and thought highly of the class that was offered by the (ISC)² instructors. Plus, my intention was actually to learn as much as I could, not just get the cert itself. Because there wasn't a training session that meshed with my schedule, I opted to go for self-study, which was the same manner I took to achieve my CWNA (Certified Wireless Network Administrator) certification. I find this worth noting, as I will be comparing the CEH courseware to that of the CWNA.

I ordered the Ethical Hacking and Countermeasures v4.1 (2005 Release) self study material via the link offered on the EC-Council website. It arrived within a reasonable amount of time and was delivered in red box, sealed with the obligatory "Only use these materials for ethical purposes; opening this box will serve as acceptance of this agreement, etc." disclaimer. Inside, there were 4 thick books, 4 CDs, a mouse pad, a notepad and pen. 3 of the 4 books were the course material and 1 book was for the Labs. 2 of the CDs related to the Labs and the other two contained bootable CDs of Knoppix and Auditor. The Lab Courseware CDs weren't bad and contained a pretty good set of tools, though they didn't necessarily align with the lab book. It also included actual Trojans and Viruses, which can be helpful in learning to use the various tools. As for the Knoppix and Auditor CDs, I thought this was a good thing to include, especially if a student doesn't have a Linux box. Personally, I'm a big fan of Auditor as you can probably tell from some of my previous articles.

Study Guide Content

Each of the books was quite thick, containing literally hundreds of pages. I was quite surprised at the amount of text I was to begin studying. It didn't take me long to realize that these books were written extremely poorly. The CEH's choice of actual modules was quite good, though I have issue with how the actual content of the modules was presented. The courseware books really came across as being more of a Teacher's Guide than a self-study course. I say this because there would commonly be a PowerPoint slide on the top of a page, then an explanation written beneath each slide. I don't so much have issue with that, though it also wasn't uncommon for the explanation written beneath to be the exact text that just appeared in the above PowerPoint with nothing extra added. That didn't seem to make much sense.

I found a number of core issues with the courseware books:

- Proofread: The books are in dire, dire need of being proofread.

- No Clear Flow: Technical information can be dry, but there is still a need to make the content readable in an attempt to at least be in somewhat of a story format. The content of the modules often didn't have any logical flow, and often an area would be covered to what you believe to be completion, then an item relating to that area would appear seemingly out-of-turn later in the module.

- Overwhelmed with Tools: Without question, it is important to be familiar with the various hacking tools that are available; that is pretty much the point of this course. That notwithstanding, tool after tool is literally dumped on the reader, without context of why you would want to use one tool over another. The tools were not logically grouped within each module, either, so it was difficult to have comprehension of the purpose of the tools after reading the module. Also, there's more to hacking than just knowing the tools. The tool's use needs to be put into context with an example of when the tool should be utilized. This was not adequately done in the courseware material. I actually went back to count the various tools that were discussed, and unofficially the count was over 250. I didn't have the heart to actually go back and count each and every one for an exact number. Personally, I think that number could have been drastically reduced with more emphasis on select tools, their use and the situations in which you would want to use that tool. Instead, the reader is just literally dumped with brief explanations of hundreds of tools.

- Choppy: Reading the material felt like reading thousands of individual pages - not thought-out and modules had no flow to them. I actually told my boss that in reading this material, that I truly felt the authors had Attention Deficit Disorder with poor grammar skills.

- Quantity Does Not Equal Quality – More organization and less pages would be an improvement.

I cannot say that the books were completely bad. The information that I needed was actually contained in the modules; it just seemed to be hidden. The data needs to be organized in a more logical manner, and that's exactly what I did after I read the books. I took each module and organized the important parts into my own study guide. The problem is that my study guide was over 72 pages long, and I was a little disturbed that I felt I had to go to that much trouble to decipher something for which I paid over \$400.

To the contrary, I felt the CWNA self study guide from Planet3 Wireless was much more organized, professionally done and contained only 600 pages. This is the guide I used to achieve my CWNA, and, while reading that guide, I felt I comprehended the material in each of the chapters after it was completed. The information was also presented in a professional manner with few grammatical mistakes and typos. With the CEH study guide, I felt I needed to backtrack to try to make sense of what I had just read.

Prepared for the Exam?

Upon completing the self-study material, writing my own study guide and memorizing the material, I felt quite prepared for the exam. With a few days left before I was to take the exam, I decided to download a practice test, just to make sure I was covered. I chose PrepLogic's CEH Practice Exam. It contained two actual exams and cost \$99. I took the first test and frankly did not do very well. This obviously made me quite nervous, as I was to take the real exam in just a few days. The PrepLogic Practice Exam seemed to have a very heavy emphasis on detailed areas of the CEH that I didn't feel required that much detailed knowledge. I also felt it had way too many errors.

In any event, I had no way of knowing what would actually be on the exam, so I used the PrepLogic Practice Exam as my guide. I restudied my own notes and downloaded the CEH Mega Guide from PrepLogic (A 101 Page Study Guide). The guide wasn't bad, though didn't really give me any information that I didn't already know and didn't cover the portions of the PrepLogic Practice Exam where I did not perform well. Perhaps, it was a little fluffy, but it didn't hurt. I also made a detailed list and grouping of the tools covered in the CEH modules and studied them intently. I then took the second PrepLogic test and still did not do well. At this point, I came to the conclusion that the PrepLogic Practice Exams were simply not in line with what needed to be known for the CEH. After taking the actual exam and comparing it to this practice test, I was correct. I would HIGHLY advise that the PrepLogic Practice Exam NOT be utilized to prepare for the CEH exam. It not only made me question if I was prepared for the exam by covering in dramatic detail material that didn't need to be known, it cost \$99 and was full of errors.

The Exam

As anyone who ever took a technical certification knows, you can't reveal the contents of the exam. I will say; however, that the exam questions were more straightforward and less technical than I originally thought they would be. Perhaps, I was mistakenly influenced by the PrepLogic Practice Exam. If you want to know what the CEH exam is like, think the opposite of the PrepLogic Practice Exam.

Something else that is important to remember is that you need to fill out and submit a CEH Exam Application Form before taking the CEH exam via Self Study. You fill out the form, submit it to EC-Council, then they provide you with a code to be used to register for the exam. This process is not instantaneous, and I recommend filling it out and getting the required code well in advance of taking the exam. Do so weeks, not days, before your exam.

CEH Room for Improvement

As I stated, I do think the CEH is worthwhile and do recommend it, especially as a supplement to the CISSP. With anything, there are areas that could use improvement:

- Wireless Hacking Module – This module was out-of-date and never covered Denial of Service attacks, AP Phishing, etc. I believe this module requires the most work of all as it was very poorly covered.

- Penetration Testing Module - This was one of the longest modules, and I think I know why. The CPTS certification tries

to discount CEH by saying that it doesn't equip its members with the knowledge to actually perform penetration tests. Though this module was long in the study guide, it still requires quite a bit of work. Too much emphasis was on the plethora of tools and not enough on penetration testing methodology.

- Linux Hacking – This seemed to focus mostly on rootkits and program compilation. I imagined it being much more detailed on actually breaking into Linux, but it was not.

- Background Check – For the CISSP, you actually need to prove that you have experience in the various security domains and a form needs to be signed by either another CISSP or an officer in the company for which you work, in order to actually get the certification. I believe EC-Council should also implement a more formal means to verify the integrity of the individuals seeking the CEH.

Conclusion and Tips

Again, I do think the CEH is worthwhile and that a lot can be learned from the process. Plus, the title of the cert is definitely pretty cool.

I offer the following tips for self-study:

- Read the Hacking Exposed books.

- Seriously consider getting the official EC-Council Study Guide. Even though it is poorly written, it does seem to give you everything you need to know.

- Make your own list and logical grouping of the tools covered in the study guide and include a brief description. There are a ton of tools covered and that is the only way to keep track of them.

- Get hands-on experience by actually using the various tools. It will not only help you pass the exam, it will help give you the actual knowledge you are seeking.

- Steer clear from the PrepLogic Practice Exams.

I hope you found this information helpful. If you have any questions, please post your questions in the CEH Forum, so that others may benefit from your inquiry.

[Home](#) [Columns](#) [Hoffman](#)