

Pulling Up Your Boot Camp Straps

del.icio.us

Discuss in Forums {mos_smf_discuss:/root}

By T. Martin Brown, CISSP

The CEH and similar certifications are hot in some circles. If you decide to attend an ethical hacker boot camp (or any boot camp for that matter), a bit of prep work can ensure you make the most of your investment. In brainstorm format, here are several items to consider before and during your training.

This list is in basic chronological order, but not stringent. So, here we go...

1. Search out your training options. Several vendors offer training on the various certifications. Don't always assume that the training offered by the company that issues the certification is the best. Especially regarding the CEH cert. I'd recommend almost any other vendor over the EC Council's own camp.
2. Carefully review the class outline of what will be covered. If this isn't available, look elsewhere.
3. Search for reviews by those who attended. For example, a member of CSP Mag, EH-Net's sister site, reviewed mile2's Certified Pen Testing Specialist (CPTS) training (check it out [here](#)). However, keep in mind that everyone has specific biases and perspectives.
4. Ask the vendor to send you name and resume/bio of the instructor. Often the vendor won't know who will teach the class until a few weeks before the class, but in that case, have them send you the resumes of all of the instructors that normally teach for them. This will also give you an idea of the caliber of talent retained by the training company. Check out their credentials. Regardless of their specialty - general computing, security, or ethical hacking - you'll be better off with a well-rounded instructor. If the instructor doesn't know Unix as well as Windows, you're in for a disappointment. The

more networks, firewalls, programming languages, databases, etc., with which the instructor has worked, the better. Some instructors can teach the class, but that's about it; they can't go any deeper than the prescribed script because they haven't spent time in the trenches.

5. Do an Internet search for the names of the instructors. What do others say about them? Can you even find them listed? On the more popular certs like CISSP, you should be able to find at least one hit on them. Often, this will lead you to other reviews by attendees. The more specific the cert, the less likely you find anything but try anyway. It's worth the effort.

6. Ask the vendor the following questions:

A. How many times has the boot camp been offered? If less than 5, be careful.

B. How many times has the instructor taught the boot camp? If less than 3, be wary.

C. What materials are provided in the classroom? Websites often don't provide this. (Once, I found out that a book I was just going to buy was included in the boot camp materials.)

D. How often is the curriculum updated? The more technical and dynamic the material, the more it should be updated. Less than twice a year is usually not frequent enough for hacking related training.

E. Is the training and the hotel in the same building? If not, how far away are they? Is transportation provided, or do you have to rent a car?

F. If the training and the hotel are in the same building, is it really one building? (Again, shavedlegs, member of CSP Mag, reports that she went to a camp at a resort that had 10 big, detached buildings. The training was in the center building and her room was all the way on the other end of the campus.)

G. Is broadband available in the room? Is wireless? Is it free? (Can you imagine a security or IT professional spending 7 days without fast Internet? It happens.)

H. What hours do the classes meet? Are there any night sessions? Are the night sessions mandatory?

I. What meals, snacks, and drinks are included? What restaurants are in the facility or nearby?

7. Review the class outline and do some preliminary reading on the topics to be discussed. There's usually several books, articles, Internet forums, etc., that focus on the subject at hand. Even if the material you find isn't exactly the same slant as the boot camp curriculum, your preliminary reading will help jumpstart your understanding of the subject. In addition, when you attend the camp, your brain will be able to better connect the new material with the tidbits you've already ingested. And your questions in class will be more focused, resulting in a deeper understanding.

8. Download and play with any software or tools the class will employ. For example, in mile2's CPTS camp, they use VMWare Workstation, which can be downloaded as trial software. Remember, when you attend a camp that uses loads of different tools like a CEH camp does, the instructor and the materials will only cover a fraction of the software or tool's capabilities, so the more you learn upfront, the better you can absorb what is being taught. In addition, you'll be more likely to ask better questions regarding the use of the tool that aren't a normal part of the curriculum.

9. Ask for an advance copy of the materials so you have more time to review it. Vendors seldom do this, even after you pay for the training, but it's worth a shot.

Once the camp starts, here are a few more tips:

1. Each night, review what you did during class. Read any material that you didn't cover in class. Catch up on any lab work.

2. Read the next day's material the night before. If you can't read the material, at least skim it. Avoid the TV, surfing, and alcohol - this is your technical vacation away from the family, bills, and relatives. Make the most of it.

3. Give the instructor feedback immediately so adjustments can be made if necessary. You only have a few days, and most instructors will tailor the class based on collective feedback and consensus. If the class has mostly noobs, ask to slow down and cover more basics. Or vice versa. If the class has too many noobs, talk to the instructor for advice; instructors have usually faced this many times before and have all kinds of ideas, based on the subject matter. The instructor might spend extra time with you outside of class (see the next tip).

4. Pump the instructor dry. Take him or her out to lunch, dinner, drinks, whatever (this is easier if you can put this on a company expense report, obviously). Swap stories. Ask for advice on specific issues. Get your money's worth! (Here's a secret: this is how you hear the inside stories, industry gossip, and advice the instructor cannot give publicly.)

5. Spend at least 10 minutes doing the evaluation. Offer praise for the good things and constructive criticism for the weaknesses. Suggest what to leave out and what to include in the future. Thoroughly review the instructor (step 3 immediately above suggests you do this verbally also). Too many attendees are too eager to get home, so they neglect this critical feedback that the company and the instructor need.

To some of you, many of these suggestions are just common sense; to others, these suggestions are another load of work to be added to an already busy agenda. However, if you're serious about learning the subject at hand, these tips can substantially enrich your experience, ensure you get the most out of the material, and avoid wasting a week wishing you were in someone else's boots.

T. Martin Brown is the security officer for a Fortune 500 company. You can contact him at [tmart500\(at\)hotmail.com](mailto:tmart500(at)hotmail.com).

Check out Martin's article, [Writing Passwords Down Right](#), at CSP Mag.