

## Mile2's Version of the CEH: A Review

del.icio.us

Discuss in Forums {mos\_smf\_discuss:Opinions}

By shavedlegs (Expanded version of a member post in CSP Mag Community Forums)

The Mile2 version of CEH is called CPTS, Certified Pen Testing Specialist, which consists of 5 days of instruction and labs. Overall, it was a good class. I learned a ton of stuff and enjoyed it.

Here's what I received when I arrived:

- A huge binder (larger than any Microsoft binder I have) of lecture notes, instruction, and lab exercises. (more on this later)
- Shon Harris' Gray Hat Hacking book (this wasn't part of the class per se; it was a freebie). This book gives basic instructions for writing Windows exploits among other stuff. If you haven't read a Harris book, this isn't a bad place to start.
- A DVD with tools galore, tutorials, tips, etc.
- A couple other DVDs with Linux distros and other stuff on it.
- A nice DVD case to protect the DVDs and a cool pen.
- A small ring binder for notes taken during the class.

Here are the issues that I had with the class:

- The instructor was not a \*nix expert. He was able to explain the \*nix material, work us through the labs and solve basic issues, He wasn't too far above me in his \*nix skills, and that is not saying much. It didn't hurt the class per se, but he was unable to answer some of my questions about general \*nix stuff. I don't think I'm being unreasonable because you can't be a security expert unless you know \*nix. Therefore, I expected a more skilled person.
- Too many noobs in the class in terms of \*nix, networking, and security basics. My classmates knew Windows admin, but that was it. This slowed the class down, and, as a result, we skipped some of the more advanced material and labs. At the same time, this class is geared toward those folks, so I can't complain too much. Also, the instructor helped me

with the more advanced stuff and stayed after the class ended to answer my questions.

I'm not against noobs, don't get me wrong; I'm still a noob in some areas; I was just hoping for a higher level of participation. For example, I had read about or used about 75% of the tools and methods the class focused on. The others in the class had not even heard of 90% of the tools or methods before this class. Even worse, some didn't even know that there were such things as bootable Linux distros.

Some of the tools and software were preloaded and preconfigured, which was great, but too much of it was not. We spent way too much time in class loading and configuring some software. I didn't go to the class to learn how to load Foundstone's Hacmebank and IIS; I came to hack it. I blasted mile2 for this in the evaluation.

I would still recommend this class over the regular EC-Council CEH. Some of my friends went to the official CEH training, and they said it was terrible. According to the vendor and Mile2's website, Mile2 helped the EC Council develop the original CEH material and training. But as time passed and the EC Council didn't keep their material up-to-date, Mile2 veered off on its own and created its own version of the class.

Back to the CPTS binder I received in the Mile2 class:

- The Linux Fundamentals section was useless. If you didn't know anything about Linux, it meant nothing. If you know Linux a little bit like me (or a lot more), it was not helpful. Most of the section was a listing of files that could be configured in Linux, like `stab` and `http`. Big Whoop.
- Several sections dealt with the ethics of ethical hacking, guidance on what approvals you need to pen test, ROI of pen testing, etc.
- Each section has a Q&A, but we didn't go over them, which was fine.
- Each technical section has lab exercises. I'd say we did about 50% of the labs. The instructor provided some of his own and others we just skipped. Most of them you can do at home.
- One lab was running the Foundstone Hacmebank app. However, we didn't get a printed copy of the pdf instructions needed to exploit the bank, so we were trying to switch back and forth between the pdf and the application. A real disaster. The instructor didn't want to ask the training center, where the class was held, to print the 32+ page book for everyone in the class. I'm going to have to finish this one later. I highly recommend this exercise, you can download it for free from Foundstone, but you have to install IIS on a 2000 or XP workstation to get it to run.
- Most of the lab exercises worked pretty well and were fun and educational.
- Overall, there were too many typos and goofs in the materials written by mile2, but not more than in the usual Microsoft training manuals. For example, in the "running Nessus," they had you adding Nessus users and updating the plugins before you even start Nessus.

What I benefited the most from:

- Learning VMWare Workstation 5 which is used to run the various OSs that you use in the class. This is incredible software that allows you to run multiple Windows and Linux (and other) OSs inside Windows. I loaded VMWare on my work laptop and purchased the software (\$200). If you take mile2's training, make sure you play with VMWare before you go to class.
- Learning Cain & Abel. This was always on my list of things to learn, I just never found the time. This runs on Windows

and is a one-stop shop for hacking period. WOW! I finally learned how to create and use Rainbow tables for cracking passwords. Also, ARP poisoning is SO EASY with this tool. Cain also sniffs all kinds of passwords on the network, and best of all, it's free. Not the easiest tool to figure out and use, though, but a free tutorial is available. The SW is also free.

- Learning Metasploit, another free tool. Using this, running exploits is click, click, click. Scary. This has a good tutorial, too, and is easy to use. While this tool works mainly on unpatched systems, there are still plenty of those out there.
- The exercise at the end of the class where the instructor set up a couple servers in a domain and gave us 3 hours to exploit them which is not a normal part of the curriculum. I was able to exploit one of them; the other two were fairly well patched. Only one other person in the class was able to exploit any of the servers.

My main takeaways from this class:

- I learned some new tools, learned to use tools I currently have even better and learned how little I really know about security and hacking. Mainly, the class helped connect some loose ends and create many others to tie off later.
- How EASY it is to exploit servers with some tools. I'm more paranoid than ever.
- I switched all my Windows network passwords to 15+characters. While I already knew that LAN MAN passwords are stored as two 7-character hashes, which makes them easy to crack, I never realized that creating passwords longer than 14 characters prevents Windows from storing the password in LAN MAN hashes. Fifteen-character+ passwords are stored in the more secured NTLM hash format. Cracking a 15-character password is a heck of a lot more work and takes longer.
- I'm much more confident in moving forward in studying security.
- It will be a little easier to convince management to increase security as I can show them how simple hacking systems can be.

Just realize that an ethical hacking course does not REALLY teach you to hack. They teach you basic concepts and tools that can be used on systems that aren't well secured.