

Course Review: CPT by InfoSec Institute

Review by Michael R. Heinzl

Thanks to The Ethical Hacker Network (EH-Net) I received the November 2010 Giveaway of a free seat in InfoSec Institute's Ethical Hacking Course. I had read and heard positive feedback about InfoSec Institute and their courses, so I was already interested to see if their reputation holds up. The course teaches the fundamentals of penetration testing and prepares students for both EC-Council's Certified Ethical Hacker (CEH) and IACRB's Certified Penetration Tester (CPT) certifications. Besides their basic ethical hacking course, InfoSec Institute also offers two more courses focused on penetration testing, targeting a more experienced audience, as well as two courses towards reverse code engineering (all with regards to their pentesting track).

InfoSec Institute describes their Ethical Hacking Course as follow: "Our most popular information security and hacking training goes in-depth into the techniques used by malicious, black hat hackers with attention getting lectures and hands-on lab exercises. While these hacking skills can be used for malicious purposes, this class teaches you how to use the same hacking techniques to perform a white-hat, ethical hack, on your organization. You leave with the ability to quantitatively assess and measure threats to information assets; and discover where your organization is most vulnerable to hacking in this network security training course."

If you are in the same situation as me, and wouldn't be able to sit for the live training in person, InfoSec Institute offer some of their courses in an online format, which is basically a recorded class from the live version, split into a couple of modules.

So let's take a closer look at the online version of InfoSec Institute's Ethical Hacking Course and IACRB's Certified Penetration Tester certification.

del.icio.us

Discuss in Forums {mos_smf_discuss:/root}

Once you are registered you'll get a package with the following contents:

- A student textbook with about +600 pages and three DVDs (Ethical Hacking Toolkit, Linux and Windows VMs for the hands-on part)
- A lab manual with about +250 pages
- A Certified Ethical Hacker V6 Review Guide
- An installation guide for the lab setup
- Credentials for their online portal
- IACRB CPT voucher
- CEH voucher (they were nice enough to exchange this with an ECSA voucher, since I already hold a CEH)

Through their online portal you get access to prerecorded lectures (instructor was Keatron Evans), which consist basically of modules that cover the theoretical aspects and labs for the hands-on. In total there are 28 modules and 22 labs ranging from the very basics (methodologies, passive intelligence gathering, abusing protocols, network reconnaissance, service identification, password cracking, etc.) to some more advanced topics (covert channels and basic exploitation). Keatron first explains the theoretical aspects of a topic and then walks you through the labs. Finally you do it by yourself. From time to time Keatron throws in some of his personal experience and anecdotes, which is always something I appreciate in such courses and bootcamps, especially if it's from a person who knows his stuff. The course covered most of the well-known and standard tools a pentester uses but also a couple of lesser-known ones, which is again something that I highly appreciated. The tools were a little outdated, however, since the concepts remain the same and this wasn't an advanced course, which might have covered specific features from recent versions, I don't see it as a real drawback.

The student textbook consists of all the slides and also some more detailed (or simply additional) explanations and side-notes. Also enough space is reserved for personal notes for later reference and studying. The recordings are clear to understand and also include the questions asked from the students while the class was recorded, which is a good thing in my opinion. Although you can't directly ask the instructor in person if you have a question yourself, you can always forward an email to the guys at InfoSec Institute, who answered any question in a timely manner (at least that's what I experienced).

The first modules covered the very basics and fundamentals of penetration testing, such as what penetration testing is and the common approaches of it, available methodologies in the field and so on. A short introduction into VMware and Linux (particularly the CLI) followed, before it went on with passive intelligence gathering (included topics were ARIN, APNIC, RIPE, NCC, LACNIC, EDGAR, whois, Google hacking, document grinding etc.).

The next module was titled "Abusing DNS" and explained DNS itself, record types, zone transfers and how to utilize tools such as nslookup, dig and DNSBruteforce.

Next was a module focused solely on how SNMP can be abused and was also the last module covered on the first day of the live version of this course (being an online version, I could continue past the first day at my own pace). The day would normally be finalized with a Capture the Flag (CTF) event, which obviously isn't the case with the online version (in the live version students would have four CTFs in this 5-day course).

The next topics explained were TCP, UDP and ICMP from a "hacker's perspective" and prepared the students for later modules ((stealthy) scanning techniques, service interrogation, system fingerprinting, etc.). Some of the tools covered in the supplementing labs included nmap, hping, netcat, xprobe2 and a couple of others. It was nice to see that also some stealthier scanning techniques, such as decoy and idle scans, were covered, too. Another good part of some of these exercises was that the students were instructed to view the logs of the machine being scanned, so that they can see both sides of the coin. By analyzing the traffic and reviewing the logs, this really helps students to understand what's going on.

The next few modules were all about password security and how to break them, covering both Windows and Unix systems. The lectures explained password storage mechanisms, various cracking techniques (brute force attacks, dictionary attacks, hybrid-type attacks, rainbow tables, etc.) and explained in some more detail the specifics of how passwords are stored in Windows and Unix systems. In the labs students would then actually try to crack various passwords by utilizing John the Ripper, Cain and Abel, and pwdump2.

It continued with the fundamentals of exploitation, including such topics as vulnerability scanning, buffer overflows, privilege escalation, SUID root attacks, and the like, and went on with keyloggers, trojans, rootkits and anti-forensics, again covering both Windows and Unix systems. In the labs you played around with Nessus for vulnerability scanning, launched exploits through Metasploit, and tried out malicious tools such as Nuclear RAT and the Hacker Defender rootkit. For example one of the scenarios in the labs was where students must first scan a machine for vulnerabilities, compromise it with Metasploit and dump the password hashes from the machine, and finally crack them on the student's local machine. These modules are probably the most interesting and fun ones for newcomers in the field.

One of the last modules was about wireless security. Unfortunately this module was mainly about WEP and mentioned WPA and WPA2 only incidental. The supplemental lab consisted of only cracking an (already supplied) 40- and 128-bit WEP key, which was somewhat disappointing. Fortunately this was the only skin-deep module I encountered.

The last module was about web application security and explained some of the OWASP Top 10 vulnerabilities, mainly SQL Injections. The lab went through some of the modules of the WebGoat Framework and introduced the Burp Suite. Again, this module was not as in-depth as previous ones, but it supplied enough information for further research by oneself and gave a brief introduction into web security.

The complete syllabus can be seen [here](#).

CPT Exam

One of the great things about the CPT exam is that it consists of two parts: A theoretical multiple choice exam (50 questions, 70% passing score, 90 minutes time for completion) and a practical exam, where supplied virtual machines must be rooted, one way or another, and specific tokens retrieved. Lastly a report must be created, which includes the tokens and a description of the steps taken to retrieve them. Your report will then be reviewed by an exam proctor, who notifies you about win or fail (I got my results back within a few days). The exam isn't too hard and if you understood and practiced the material taught in the course, it shouldn't be a problem to pass both parts of the exam, while still not giving away the key to the kingdom too easily. For the practical exam the candidate has 60 days from the completion of the multiple choice exam to hand in the report (again students pass with a score of at least 70%). The 60 days given are also more than enough to solve the tasks. Unfortunately there are way too few such certificates with practical, hands-on portions. Other ones would be the courses/ certifications offered by Offensive Security.

Regarding the theoretical part of the exam, it's also worth to mention that the questions were realistic and plausible, and not kind of awkward in the sense of confusing or inappropriate.

The CPT certification is valid for four years. Then certified individuals must complete the same exam that current certification candidates must take in order to keep the certification valid. Luckily there are no fees associated with the re-certification process.

Conclusion

The material was presented very well and contained only very few errors and typos. Throughout each module I felt that there was a leitmotif and the modules were not just thrown together. The instructor did a great job and explained each module very well and kept things throughout interesting.

Obviously most of the presented topics could be covered in much more depth; however, as this was a course developed for five days and focuses on the basics of penetration testing, I think the guys at InfoSec Institute did a great job in introducing the students to many of the basic skills a Penetration Tester / Ethical Hacker / Security Consultant needs to know.

Although I enjoyed the online version, I still would recommend going for the live version if travel budgets make it possible. Both formats have their own pros and cons, but in this case the advantages of a live training would exceed the ones from an online training in my opinion (such as live interaction with the instructor, nightly CTFs, networking etc.) If you are not that new to security - or even better to pentesting, you shouldn't need to watch the videos over and over again to understand a certain topic (and even if – you still would have the courseware), which would be one of the advantages of the online format.

The CPT certification was fun and mirrored the topics covered in the course very well, which is an important part when deciding for a bootcamp. Although the CPT certification is hardly known here in Central Europe, I'm still happy to have obtained it, since it was not just another memorize-type exam to add to the list.

I'd recommend this great, hands-on class to everyone who wants to enter into the field of penetration testing (the core skills should be already known, though such as Operating Systems, Networking, Shell, etc.) without hesitation. It's one of the best entry-level courses in the field I've taken so far. In fact, I enjoyed it so much, that I'm already enrolled in their Advanced Ethical Hacking course. This advanced course deals with exploit development and reverse engineering (and it's again available in an online format as well), which is also more towards my field of expertise. Keep listening for another review.

More from Mr. Heinzl: <http://www.awesec.com/>