CEH or OSCP ?

written by Mert SARICA | 15 December 2009

In the early 2000s, I had decided to take the CEH training from EC-Council at an educational institution in Altunizade, and I had high expectations for this course. Normally, this training, which is given in 5 days abroad, was turned into a 3-month course, if I remember correctly. I thought that by taking this course, I would be able to strengthen my knowledge of how to find and exploit vulnerabilities in software, and how to develop exploitation techniques. However, when one day the instructor showed us how to use the winnuke program, and told me that my expectations should be lowered, I realized that this course would not contribute much to me. In fact, although the training materials had interesting modules such as exploit writing and reverse engineering, these modules were not covered in the course. The reason for this was that EC-Council had decided that the modules between 22 and 26 should be self-study. If I remember correctly, the CEH version at that time was v4 (2003), and when the course began, v5 (2005) was released, so our training materials were updated. To get the certificate, you had to pass a multiple-choice exam (I think it still is).

Over the years, because of the weak training content, the availability of exam questions and answers that can be downloaded from the internet, and a exam system based on theoretical knowledge, I had negative opinions about this training and certification. Setting aside the exam system, the training content was not useful for people who had no knowledge of ethical hacking, and perhaps my expectations from the training were too high, so it disappointed me.

Years have passed and last year, I think it was around the beginning of June, version 6 was released. When looking at its content, while there were 26 modules in v5, v5'te 26 modül varken v6 consists of 67 modules and its content is quite satisfactory compared to 2005, but as in v5, the most enjoyable and informative modules are not shown to participants as part of the course (modules 1-21 are mandatory, the rest are self-study).

Due to my job, the first question most people ask me is whether I have a CEH certification. For years, I explained why I did not have a CEH certification due to the reasons mentioned above and this year, at the beginning of the year, through my research on ethical hacking training and certification, I

came across a training that I found very satisfying in terms of content and exam system, Offensive Security 101, also known as Penetration Testing with Backtrack. As its name suggests, it is a training prepared by the creators of Backtrack, and it can be taken either abroad or online. If you take the training online, you can read the training materials in pdf format, watch the modules in video format, and connect to their servers through VPN to apply what you have learned. It offers advanced knowledge, from discovering security vulnerabilities with Fuzzing, preparing exploitation applications with python, to finding return addresses with ollydbg, compared to CEH. The exam system is incomparable to CEH, as it is entirely based on practice, on the day of the exam, VPN definitions are made to give you access to the exam environment, and if I remember correctly, you were given 4 questions. One question asked you to research a buffer overflow vulnerability in an application and write an exploitation application that allows for remote code execution, while another question asked you to take over a Linux server in the lab and send them a line from a text file located in the root folder, and while doing this, using automated scanning tools (nessus, core impact) is prohibited, in short, the training is very successful from content to the exam.

In conclusion, If you are just starting out, your knowledge level in ethical hacking is low, the instructor is qualified (being a pentester should definitely be a preference), and occasionally, will be able to go beyond the course schedule, even if some modules are self-study (I don’t know if EC-Council allows this), I would recommend the CEH training and certification (you can also make do with the training because of the mediocre exam system). However, if you have some knowledge in ethical hacking and want to certify this with practice, I strongly recommend the OSCP training and certification.