**CEH PRACTICAL**

[lwahch](https://letslearncybersecurity.wordpress.com/author/oussamabendiousscyber/)[24 Feb 2022](https://letslearncybersecurity.wordpress.com/2022/02/24/778/)[Unclassified](https://letslearncybersecurity.wordpress.com/category/non-classe/)

**Article browsing**

[Previous](https://letslearncybersecurity.wordpress.com/2022/02/19/steel-mountain/)

**What is CEH practical?**

It is an exam proposed by Ec-Council which lasts 6 hours and which aims to assess the essential skills of an Ethical Hacker. The exam contains 20 real scenarios, in the form of 20 questions, each question allows you to validate a required skill, and allows you to measure the candidate's reflection. It's true, you will find questions that do not require a lot of work, on the other hand others that require the application of all the steps followed by an Ethical hacker

|  |  |
| --- | --- |
| Exam title | Certified Ethical Hacker (Practical) |
| Number of challenge (Question) | 20 |
| The duration | 6 hours |
| The form | iLabs Cyber ​​Range |
| The pass mark | 70% (14/20) |
| Open Book | Yes, you can use any resources on the internet, as if you were doing a mission in real life |

Like any exam, there are two essential points to pass it, these have no relation to skills and knowledge:

* Self-confidence
* No stress

On the other hand here for the CEH (Pratical), there are two other important points, it is:

* Have a very good connection
* Know where to look for your need

Have a good connection, because you will need it to search the internet, stay connected to the meet with the invigilator, and connect to the exam LAB. And knowing where to look for information is only to save time. Indeed it is true that you have 6 hours which is more than enough, on the other hand it really depends on your level and your skills, so if you are not competent enough, you must know where to look and how to find your objective, moreover the CEH is an exam for 'script-kiddies', so the main objective is not to know the tools but to know how to find them.

**Preparation for the exam**

To prepare for the exam, it is absolutely necessary that you are very practical, and when I say practical I rather mean the challenges, to become familiar with the tools, the CTFs, the LABs…. For this I prefer to divide the possible resources into two main parts, paid and free. For paid resources are quite effective, for example the ilabs de eccoucil…. But they are quite expensive. Personally, I can't tell you about these tools, since I haven't used them. For me, I limited myself to free resources (if I don't count 'TryHackMe')

Personally, I started with a free account on Tryhackme, and frankly I quickly realized the usefulness of having a premium account. Frankly, it's the cheapest way, because a Tryhackme account your £90 (for a year, I preferred to pay for a year because tryhackme is useful beyond preparing for the CEH pratical, it's really a mine gold to learn).

To prepare, I did a lot of research and read a lot of people's feedback, postings on reddit, github, linkdine and others, here you will find the conclusion of it all.

First, on term of course and notion, I started by viewing a series on Youtube (120 videos from 7 min to 28 min, they are made by Mr Yasser Ramzy, here is the link [https://www.youtube .com/watch?v=gmOGkmn0jRk&list=PLCIJjtzQPZJ-gm80\_z7Svq4UlJSbOKdM4](https://www.youtube.com/watch?v=gmOGkmn0jRk&list=PLCIJjtzQPZJ-gm80_z7Svq4UlJSbOKdM4) ), and frankly these videos are useful to prepare not only for the practical CEH, but for the ANSI CEH, unfortunately these videos are in 'Arabic', so I understand very although they are not useful for everyone, that's why I tried on my blog to formalize and summarize all the courses that they were useful for me for the CEH (Pratical) in French, I just to start with articles on the different tools to master, just visit the 'Tools' part on my site to master them.

Note: just for information, you will find videos of ilabs on Youtube, frankly I find it not useful, on the one hand there is no explanation, on the other hand the main objective is not only to pass the exam but also to improve your skills, that's how you really have to practice.

1. **Tools:**

Here are the tools that I find essential to pass the CEH (Pratical):

* wpscan
* Nmap
* Burp Suite
* ZAP
* Exiftool
* Hydra
* John the ripper
* hashcat
* SQLMAP
* Enum4linux
* Metasploit
* Steghide
* Searchsploit
* Veracrypt
* dirb
* Gobuster
* Hashcalc
* Wireshark
* Nikto
* Rainbow crack
* Netdiscover
* Ophcrack
* Pwdump7
* Snow
* Hping3
* Aircrack
* Cryptool
* MD5 calculator

Frankly, I can confirm that if you master these tools, you will absolutely have your certificate (because at least you will have the min mark: 14).

But only for information, personally there were no tools that I discovered during the exam (especially Windows tools)

I tried to put a link on the courses and the summaries that I have already written for each tool and for the rest they will be added soon.

* **Practice**

As I already mentioned, the ilabs is very good to practice but it is expensive. For this, personally I realized the different LAB that I saw on the video series, I will try to formalize them also in an apart section in my site. On the other hand, it is really on tryhackme that I prepared myself well. My strategy was as follows:

* I do the challenges on the different tools in order to master them
* If no challenge exists for such a tool, I try to look for one on the internet and mount it locally, sometimes even on the cloud (since I have a lack of hardware resources)
* Afterwards, I moved on to CTF-type challenges, to improve the methodology with which I deal with challenges, without forgetting that it really helps me to improve my thinking.

If by chance you are starting from afar, do not hesitate to start on tryhackme with all that is of the 'info' type because it will really help you to master the different basic notions.

Here I tried to cite the challenges to be met for each tool:

To have the basics I suggest you start with the 'Path Complete Beginner'. After you can start the other rooms (for info the order does not mean anything here, because I forgot the order that I followed hhhh)

* Basic pentester tools in a nutshell: <https://tryhackme.com/room/ccpentesting>
* To learn Linux <https://tryhackme.com/room/zthlinux>
* To get familiar with the find command, which is essential <https://tryhackme.com/room/thefindcommand>
* Nmap:   <https://tryhackme.com/room/rpnmap>
* Hydra: <https://tryhackme.com/room/hydra>
* OWASP top 10 <https://tryhackme.com/room/owasptop10>
* Steganography tools in a summarized way: CC Steganography <https://tryhackme.com/room/ccstego>
* Hashcat <https://tryhackme.com/room/crackthehash>
* ZAP: <https://tryhackme.com/room/learnowaspzap>
* Escalation of privilege on linux: <https://tryhackme.com/room/commonlinuxprivesc>
* Burp suite: <https://tryhackme.com/module/learn-burp-suite>
* SQL Injection: <https://tryhackme.com/room/sqlilab>
* John the ripper: <https://tryhackme.com/room/johntheripper0>

After starting with all this, I moved on to different CTF type challenges to get used to the challenge and improve my thinking about the different challenges. For the CEH, I limited myself to 'beginner' level CTFs and frankly that's enough, because as I said CEH practical and only for 'script-kiddies'. But frankly before moving on to the challenges, I did the 'advent cyber 2023' from tryhackme, it's still available, and it allows us to learn a lot of things, certainly these are basic things but it's enough for our current goal.

To be a little exhaustive on the challenges I have done:

* <https://tryhackme.com/room/rrootme> : Escalation of Privilege
* <https://tryhackme.com/room/wgelctf>
* <https://tryhackme.com/room/brooklynninenine> : nmap, gobuster, steganography
* <https://tryhackme.com/room/blog>  : I did this just to get familiar with wpscan
* <https://tryhackme.com/room/owaspjuiceshop> : Burp, owasp top 10
* <https://tryhackme.com/room/lianyu> Elevation of privilege, steganography, gobuster

Note: you will find on my site writups for the different challenges, I have tried to explain well and give several methods to solve each challenge (if there is one), and this will help you to have a lot of ideas when you are facing a challenge.

**Exam day:**

As I said at the start, you have to be very sure of your connection, in addition to that you must have an identity document with you, and you must be in an empty room (you are the only one in room) because you are not allowed to talk to anyone during the exam.

On the day of the exam, try to connect 15 min before the departure time, you will start by installing the video call application requested, after the supervisor will explain to you all what you can do and what you cannot must not do. At one point, he will ask you to take control of your PC to enter his code in order to start your exam. In general, he will have a closed microphone, and he will communicate with you in writing (in the chat). The exam is in the form of iLabs, you have 3 machines:

* Kali
* windows server 2016
* windows server 2019

Unfortunately, it was very long for me and it's the first time I've seen a machine as long as that (in fact it was the case for me, I'm not sure if it's the case for everyone ), but if it does, don't worry.

As soon as the test begins, I suggest that you read all the questions to get an idea of ​​the different challenges to be dealt with. For the time, if you have prepared well, 6 hours is enough, we can even say that it is doable in 2 hours. To do this, start by reading all the questions and then try to start with the one that seems easiest to you, and be careful, some challenges are dependent.

Frankly, there are very simple challenges that require a ping, or a launch of nmap, it's good to start with these challenges so that your stress decreases.

For cryptography challenges, if you are faced with tools that you have never used, don't worry, it's normal because with a simple search on the internet you will solve your challenge. That's why I suggest you start with the cryptography challenges as soon as you get stuck. Indeed, these do not require reflection, but rather the use of the tool. That's why you just have to learn how to use the tools. And as I have already mentioned, you will find tutorials on all the tools on our site.

As soon as you have finished, mention this to your invigilator and he will ask you to confirm that you want to complete your exam. After, it will show you your grades as well as how to download the certification.

**Useful links**

Here is a github repository that I used too much during my preparation:

<https://github.com/Samsar4/Ethical-Hacking-Labs>

Here are CEH notes that are very practical: