Way of Thinking

The field of information security is massive. It would be impossible for any one person to learn everything. Let us take the following example:

> Imagine you want to become a programmer, and you know that there are more than 200 different programming languages that can be used to create applications that can be cracked by debugging or reverse engineering. If we learned every programming language within 100 hours, we would spend 20,000 hours or 2,500 days (8 hours per day) or, in other words, almost seven years to learn all of these programming languages. As a result, we spent seven years learning all these languages and never tried to debug or reverse engineer the program we created. Great! Let us spend another seven years learning to debug and reverse engineering.

We have got the idea. No one wants to spend so much time on just one area. Furthermore, this is not necessary. We will need some time to learn different technical principles, structures, and processes, but we will not need to spend seven years. Every programming language has its own strengths and weaknesses. Also, if we can obtain a deep understanding of a single programming language, we will learn others much faster. We do not need to learn every programming language to understand how to read their code. All of them follow the same principles which R. D. Tennent initially defined:

1. `The Principle of Abstraction`
2. `The Principle of Correspondence`
3. `The Principle of Data Type Completeness`

In information security, we have to learn and understand these principles, structures, and processes quickly. Additionally, we have to adapt our knowledge to the various environments we encounter. We will have many situations where we will not understand how "it" works. That is good. At this point, we have to find out what we do not know. More about that later.

There are many learning-focused information security communities available to us. Many of these communities provide free reviews of tested applications, vulnerable machines, and guides to help each other and improve their members' skills. When we speak with the other members, we will notice there are generally two types of people.

- `Those that do not know anything.`
- `Those who think they do not know anything.`

This can be very frustrating, and this is a normal part of the learning process. Communication within these communities should be respectful, always keeping in mind that we all started with zero knowledge of this field. This is a critical point of success for the community and everyone learning and working in this field. Within Hack The Box, we can use the Forum and Discord server to interact with the community.

- Forum: https://forum.hackthebox.eu

- Discord: https://discord.gg/hackthebox

Another important point is our knowledge level. Many people do not know their actual skill and knowledge level. This is a complicated topic because penetration testers must have a deep understanding of a wide variety of technologies. As previously mentioned, the problem in this field is the sheer volume of information available to us. We can learn about every topic and still not master any one area, or we can learn about just one topic and become an expert in it.

Another option is developing our research methodology, the learning process, and how to use this to improve our knowledge. We will be successful if we know how to search for the required information on the internet, and we know how to learn fast and adapt it to the environment we are working in. However, before we can do this, we have to learn and practice how to do it.

We will become a good penetration tester only through considerable practice. There is no other way to improve our practical skills. For example, we can read 50 books about programming, and we will understand how to read the code. This is the process of passive learning. This can be useful. However, if we need to write our own program, we have to practice active learning, which means we have to write code and test it on our own.

One of the most common questions is:

> When is a penetration tester good enough?

We know that one person cannot know everything. In this case, we have to learn how to `find`, `choose`, and `adapt` the information we need.

Right now, we are considering these three key terms. There is one key term missing.

Which key term is missing from the above list?

The crucial missing term is: `LEARN`

The process of "learning how to `learn`" is not easy. Most people have never truly learned how to learn effectively. For example, in school, our teachers discussed some topics with our class. First, teachers show us just one way to solve a problem. They explained one way to solve the problem, and after that, they gave us exercises to practice further.

Let us take a closer look at the problem. Look at this simple math equation and try to solve it:

> 20 * ________+ ________ = 65535

This equation is easy to solve, but did we think about how many different ways are there to solve it?

Optional Exercise:
Ask yourself why you didn't solve the problem in a different way. Write it down and try to think about the reasons for choosing the method that you chose. Take as much time as you need for it before you continue.

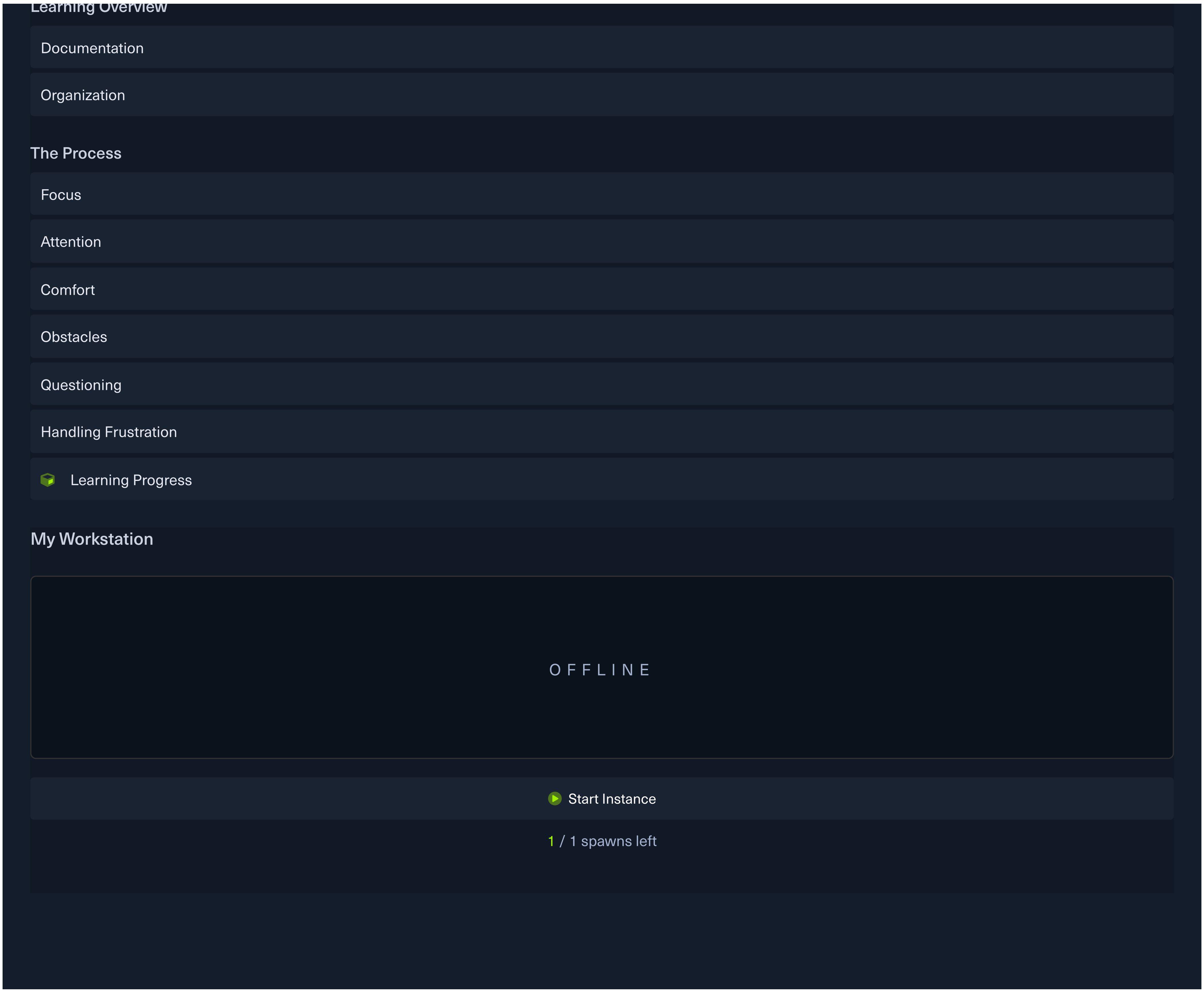
Next →

Mark Complete & Next

Table of Contents

Mindset

Learning Dependencies



Learning Overview

Documentation

Organization

The Process

Focus

Attention

Comfort

Obstacles

Questioning

Handling Frustration

Learning Progress

My Workstation

OFFLINE

Start Instance

1 / 1 spawns left