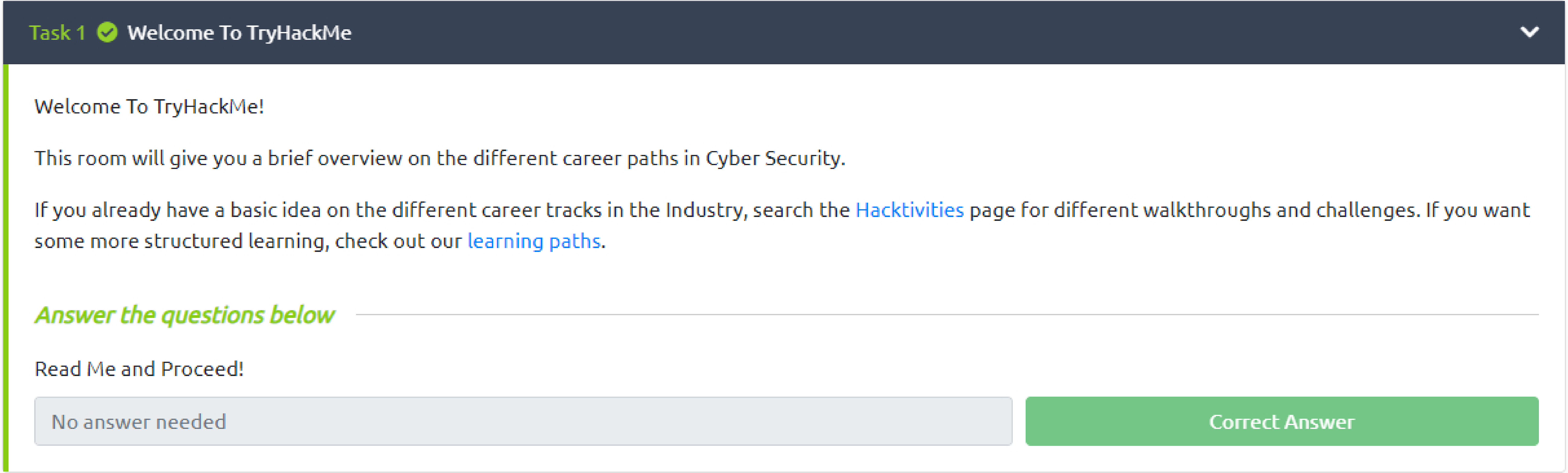


Task 1 ✓ Welcome To TryHackMe

Welcome To TryHackMe!

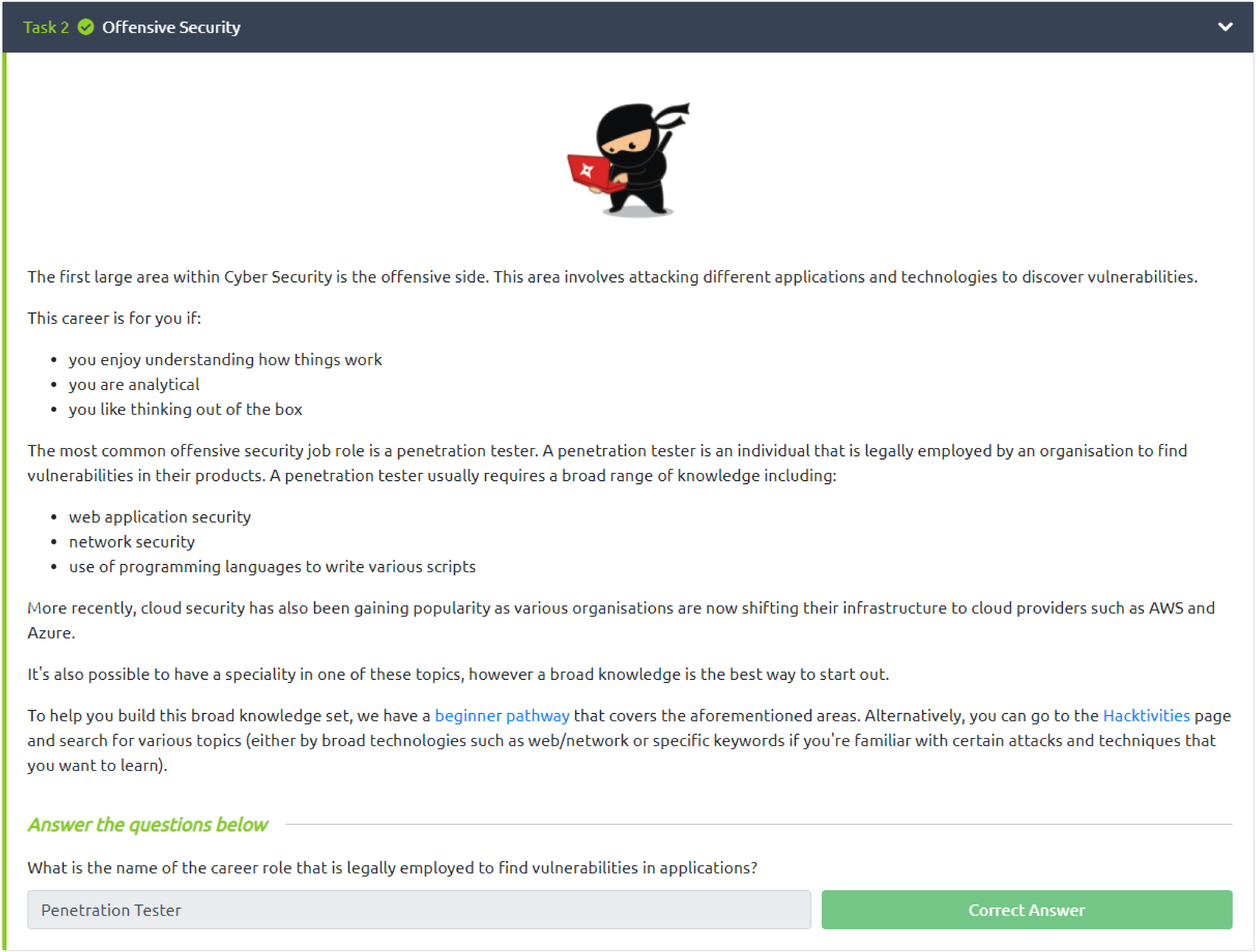
This room will give you a brief overview on the different career paths in Cyber Security.

If you already have a basic idea on the different career tracks in the Industry, search the Hacktivities page for different walkthroughs and challenges. If you want some more structured learning, check out our learning paths.

Answer the questions below

Read Me and Proceed!

No answer needed



Offensive Security

The first large area within Cyber Security is the offensive side. This area involves attacking different applications and technologies to discover vulnerabilities.

This career is for you if:

- you enjoy understanding how things work
- you are analytical
- you like thinking out of the box

The most common offensive security job role is a penetration tester. A penetration tester is an individual that is legally employed by an organisation to find vulnerabilities in their products. A penetration tester usually requires a broad range of knowledge including:

- web application security
- network security
- use of programming languages to write various scripts

More recently, cloud security has also been gaining popularity as various organisations are now shifting their infrastructure to cloud providers such as AWS and Azure.

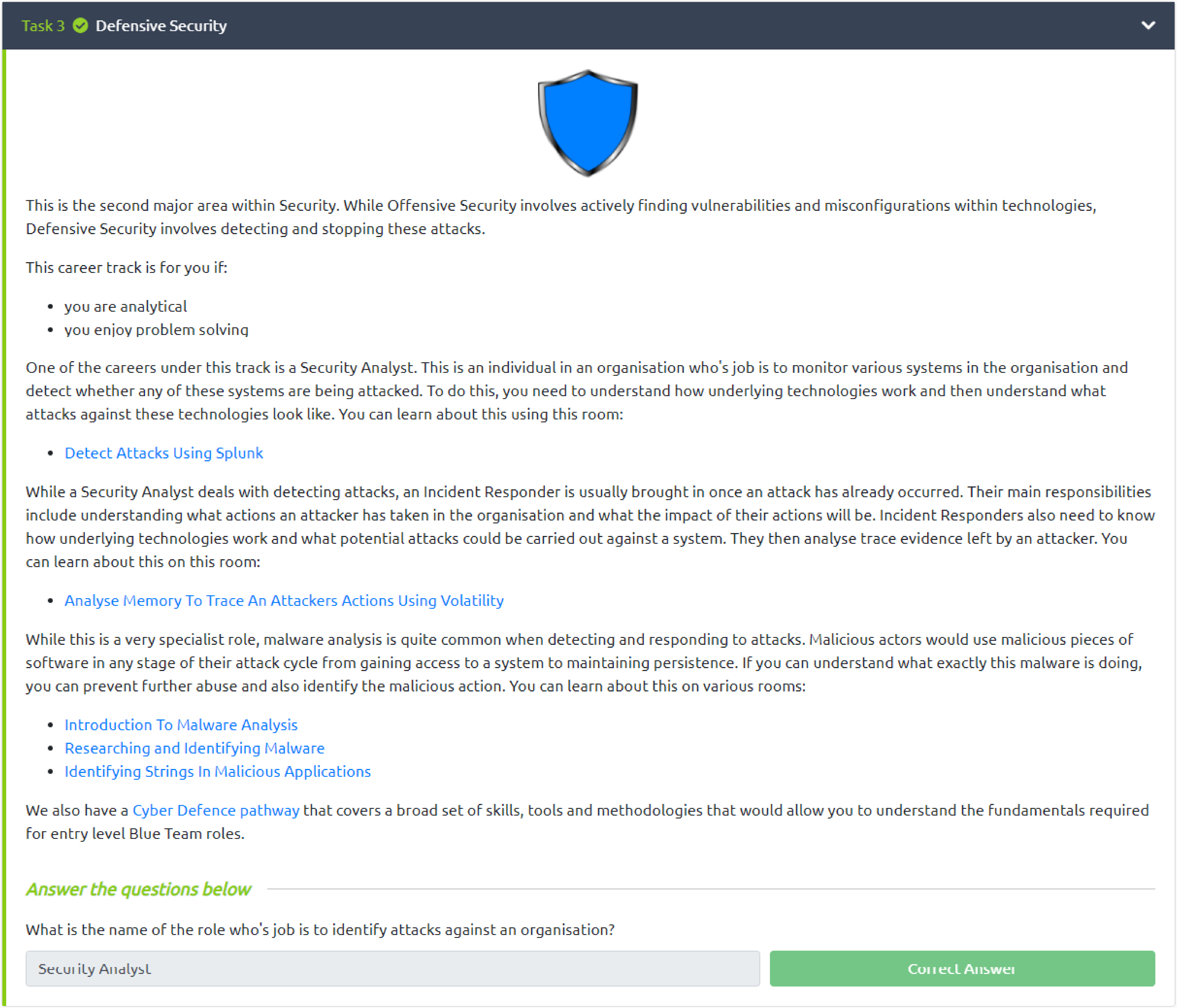
It's also possible to have a speciality in one of these topics, however a broad knowledge is the best way to start out.

To help you build this broad knowledge set, we have a beginner pathway that covers the aforementioned areas. Alternatively, you can go to the Hacktivities page and search for various topics (either by broad technologies such as web/network or specific keywords if you're familiar with certain attacks and techniques that you want to learn).

Answer the questions below

What is the name of the career role that is legally employed to find vulnerabilities in applications?

Penetration Tester



Task 3 ✓ Defensive Security

This is the second major area within Security. While Offensive Security involves actively finding vulnerabilities and misconfigurations within technologies, Defensive Security involves detecting and stopping these attacks.

This career track is for you if:

- you are analytical
- you enjoy problem solving

One of the careers under this track is a Security Analyst. This is an individual in an organisation who's job is to monitor various systems in the organisation and detect whether any of these systems are being attacked. To do this, you need to understand how underlying technologies work and then understand what attacks against these technologies look like. You can learn about this using this room:

- Detect Attacks Using Splunk

While a Security Analyst deals with detecting attacks, an Incident Responder is usually brought in once an attack has already occurred. Their main responsibilities include understanding what actions an attacker has taken in the organisation and what the impact of their actions will be. Incident Responders also need to know how underlying technologies work and what potential attacks could be carried out against a system. They then analyse trace evidence left by an attacker. You can learn about this on this room:

- Analyse Memory To Trace An Attackers Actions Using Volatility

While this is a very specialist role, malware analysis is quite common when detecting and responding to attacks. Malicious actors would use malicious pieces of software in any stage of their attack cycle from gaining access to a system to maintaining persistence. If you can understand what exactly this malware is doing, you can prevent further abuse and also identify the malicious action. You can learn about this on various rooms:

- Introduction To Malware Analysis
- Researching and Identifying Malware
- Identifying Strings In Malicious Applications

We also have a Cyber Defence pathway that covers a broad set of skills, tools and methodologies that would allow you to understand the fundamentals required for entry level Blue Team roles.

Answer the questions below

What is the name of the role who's job is to identify attacks against an organisation?

Security Analyst

Correct Answer