

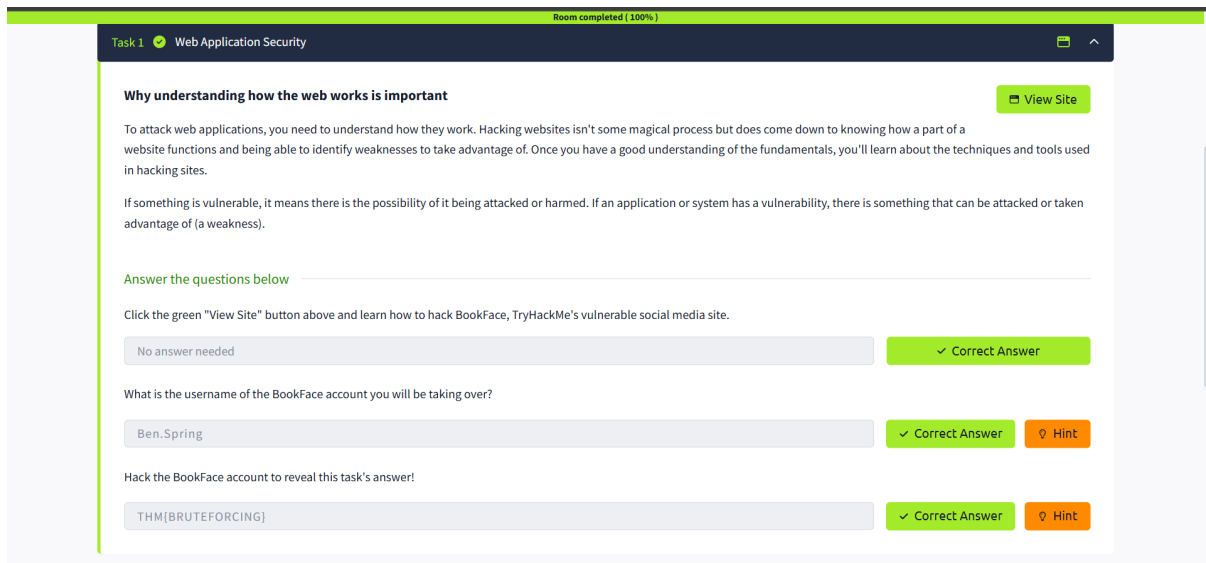
Learning Cyber Security: Writeup

AIM

Get a short introduction of a few of the security topics.

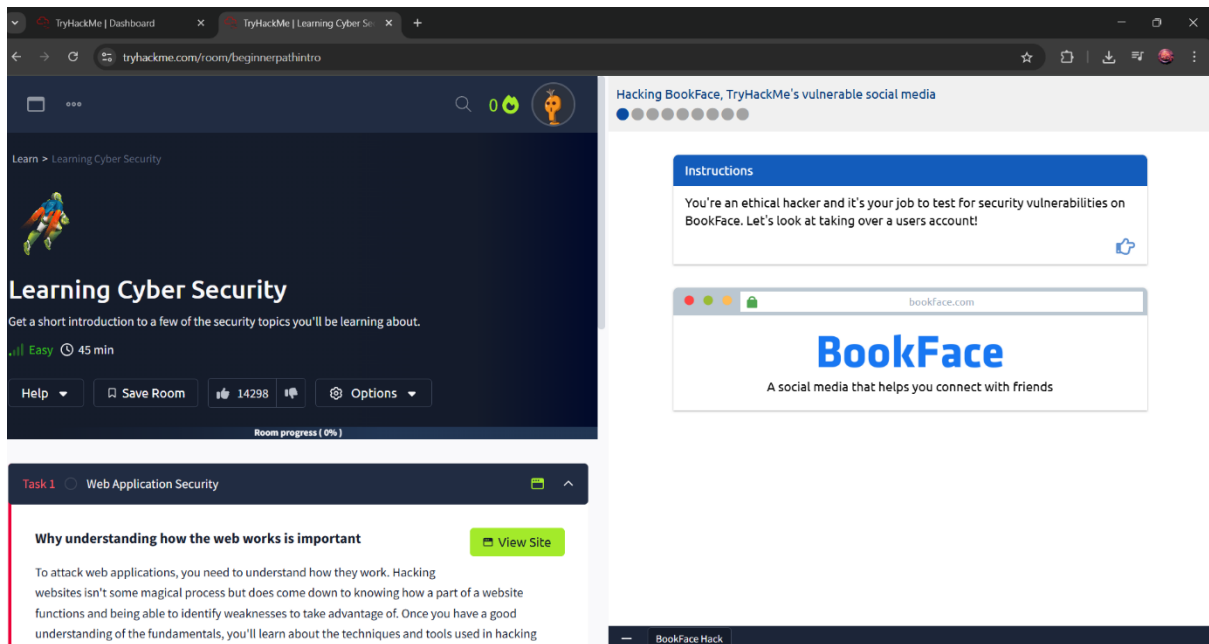
STEP BY STEP EXPLANATION

TASK 1: WEB APPLICATION SECURITY

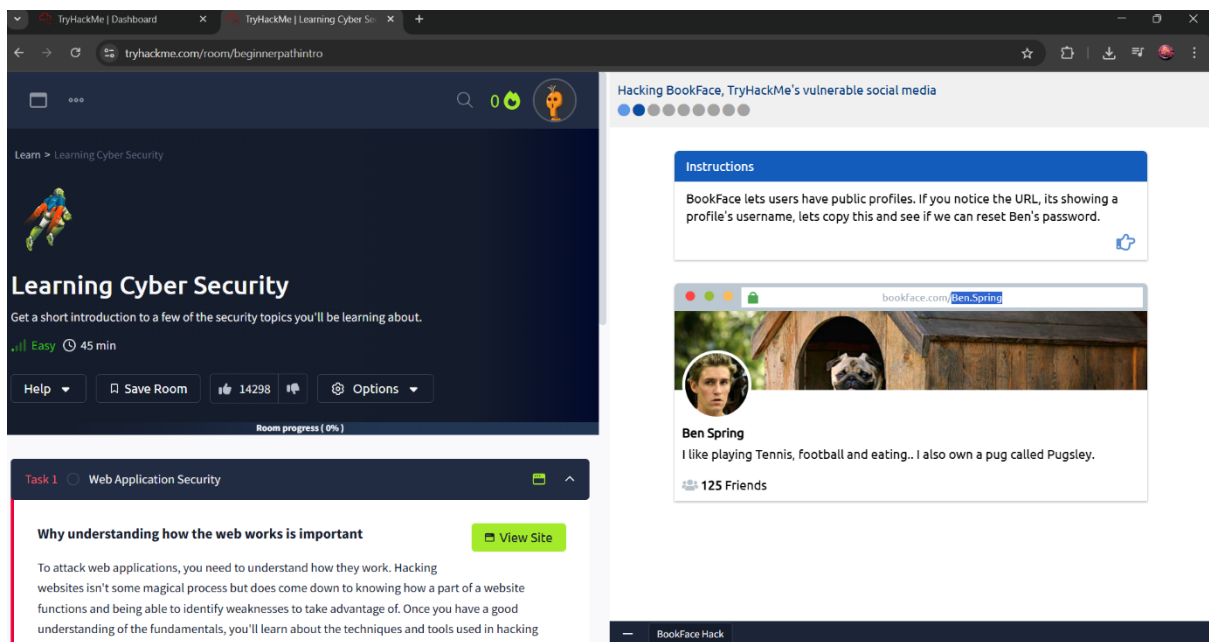


The screenshot shows a web application security task interface. At the top, a green bar indicates "Room completed (100%)". Below this, a dark blue header bar displays "Task 1" with a green checkmark and "Web Application Security". The main content area has a light gray background. It starts with the heading "Why understanding how the web works is important" and a green "View Site" button. The text explains that hacking websites isn't magical but requires understanding how they work and identifying weaknesses. It then states that if something is vulnerable, it can be attacked or harmed. Below this, a green bar says "Answer the questions below". The first question is "Click the green 'View Site' button above and learn how to hack BookFace, TryHackMe's vulnerable social media site." The answer is "No answer needed", and a green "Correct Answer" button is shown. The second question is "What is the username of the BookFace account you will be taking over?" The answer is "Ben.Spring", and a green "Correct Answer" button and an orange "Hint" button are shown. The third question is "Hack the BookFace account to reveal this task's answer!" The answer is "THM[BRUTEFORCING]", and a green "Correct Answer" button and an orange "Hint" button are shown.

In this task it mainly focuses on how to hack a website by knowing the basics. By clicking view site it shows a website room for studying this. By the end of this attend some questions to complete the task.

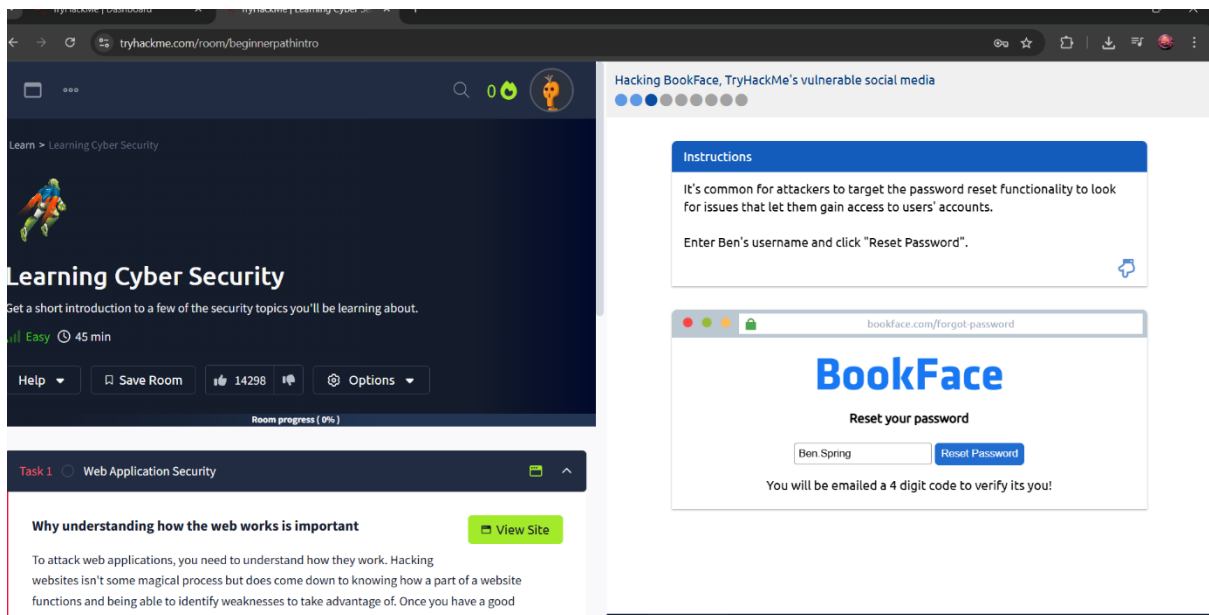


Here by clicking view site it shows book face website a social media platform which helps people to connect with friends. Our task is to find the security vulnerability and use this weakness to hack the website.

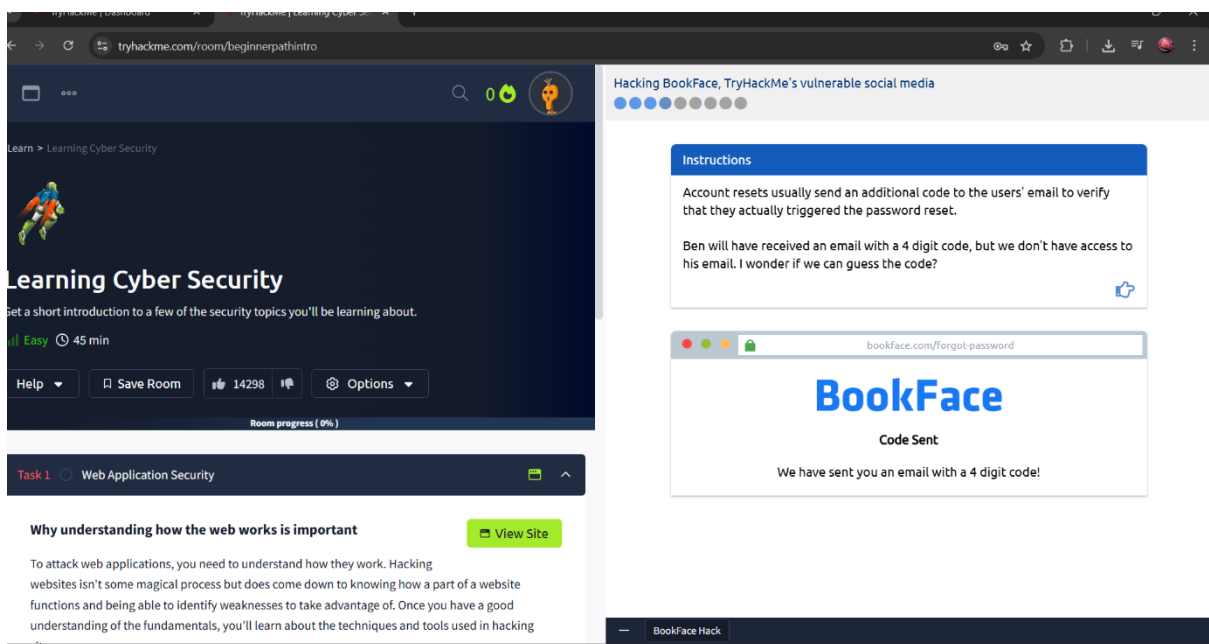


Ben Spring is a profile in BookFace. it shows the page URL as bookface.com/Ben.Spring.

Ben.Spring is the profile username and this is a weakness that we found. We could try to change the password using this username.

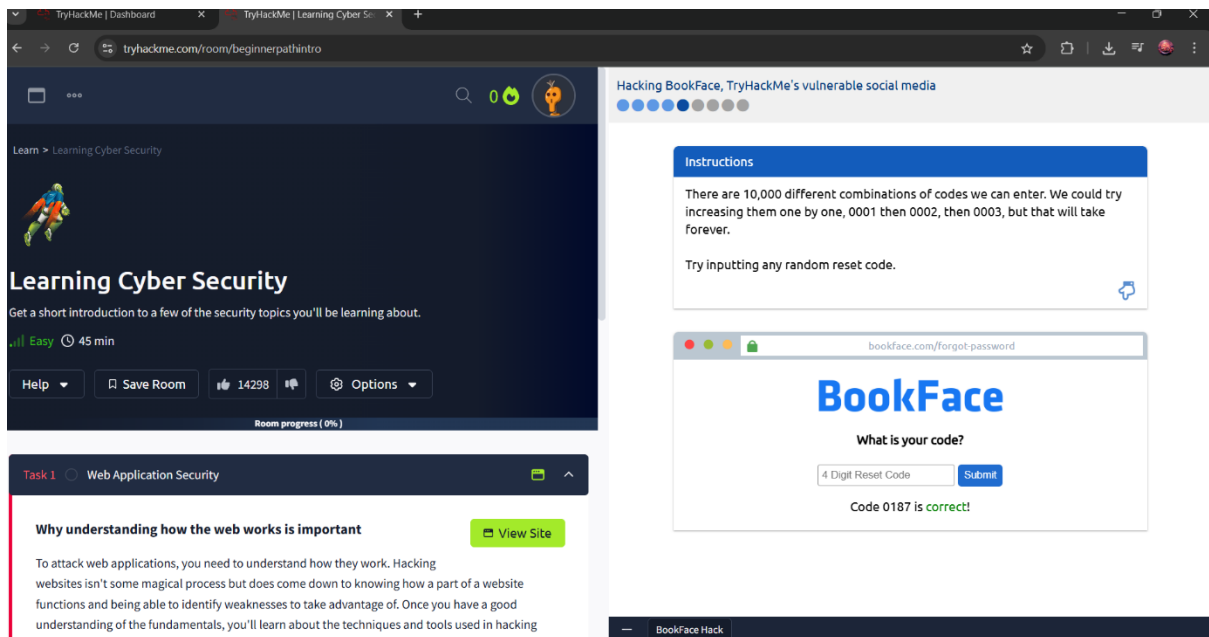


We mainly make use of the password reset functionality to look for issues to gain the account access. Enter the username that we found and click reset.

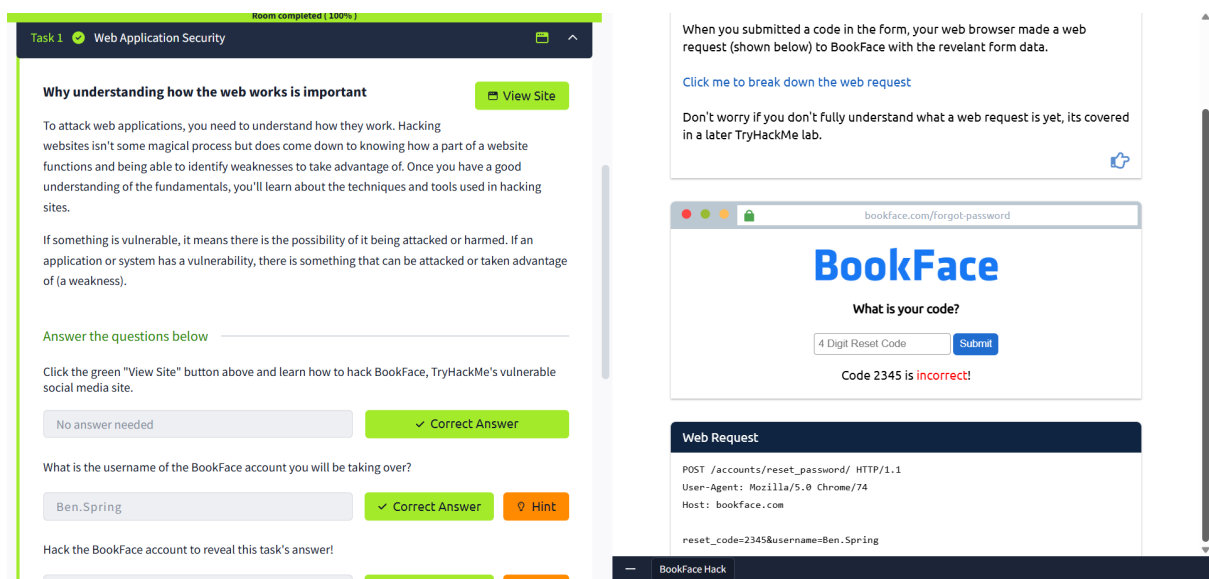


Account resets mostly send code to the users email to verify the account.

Ben would also receive a 4-digit code but as we do not have access to his email, we might have to guess the code



There are 10000 different combinations of codes we can enter. We could try to increase each number but that Methode would be a lot time consuming. Input a random reset code.



After submitting a random code, the web browser would make a web request to BookFace with the relevant data as shown below.

TryHackMe | Dashboard TryHackMe | Learning Cyber Security

tryhackme.com/room/beginnerpathintro

Learn > Learning Cyber Security

Get a short introduction to a few of the security topics you'll be learning about.

Easy 45 min

Help Save Room 14298 Options

Room progress (0%)

Task 1 Web Application Security

Why understanding how the web works is important View Site

To attack web applications, you need to understand how they work. Hacking websites isn't some magical process but does come down to knowing how a part of a website functions and being able to identify weaknesses to take advantage of. Once you have a good understanding of the fundamentals, you'll learn about the techniques and tools used in hacking

It's not going to be possible to manually guess every code, so lets repeat the code web request we sent earlier and each time increase the code value, automating the process using the "Request Repeater" below.

This process of trying different combinations until one is correct is called brute forcing, a common attack in cyber security.

Use the BruteForce tool with a code min (1) and max (10,000) value.

bookface.com/forgot-password

BookFace

What is your code?

4 Digit Reset Code Submit

Code 0187 is incorrect!

Web Request Repeater

Min Code Value
Max Code Value
BruteForce

POST /accounts/reset_password/ HTTP/1.1
User-Agent: Mozilla/5.0 Chrome/74
Host: bookface.com
reset_code=0187&username=Ben.Spring

BookFace Hack

Its not possible to manually guess the code so we would go for "Request Repeater" below. This process of trying different combination until one is correct is called brute forcing commonly used in cyber-attack. Use brute Force tool with a code min(1) and max(10000).

TryHackMe | Dashboard

TryHackMe | Learning Cyber Security

tryhackme.com/room/beginnerpathintro

Learning Cyber Security

Get a short introduction to a few of the security topics you'll be learning about.

Easy 45 min

Help Save Room 14298 Options

Room progress (0%)

Task 1 Web Application Security

Why understanding how the web works is important

View Site

To attack web applications, you need to understand how they work. Hacking websites isn't some magical process but does come down to knowing how a part of a website functions and being able to identify weaknesses to take advantage of. Once you have a good understanding of the fundamentals, you'll learn about the techniques and tools used in hacking

Hacking BookFace, TryHackMe's vulnerable social media

Instructions

This was a real-world attack, that (before it was patched) let you take over anyone's Instagram account. The hacker that found it reported it to Instagram and recieved \$10,000 as a reward.

It's important you understand how web applications work. Once you have a good understanding of the web, TryHackMe will teach you about new cyber attacks and the tools used in the industry by penetration testers and security analysts.

bookface.com

BookFace

Password has been reset

The answer to the TryHackMe task is: THM{BRUTEFORCING}

BookFace Hack

Room completed (100%)

Why understanding how the web works is important

View Site

To attack web applications, you need to understand how they work. Hacking websites isn't some magical process but does come down to knowing how a part of a website functions and being able to identify weaknesses to take advantage of. Once you have a good understanding of the fundamentals, you'll learn about the techniques and tools used in hacking sites.

If something is vulnerable, it means there is the possibility of it being attacked or harmed. If an application or system has a vulnerability, there is something that can be attacked or taken advantage of (a weakness).

Answer the questions below

Click the green "View Site" button above and learn how to hack BookFace, TryHackMe's vulnerable social media site.

No answer needed

Correct Answer

What is the username of the BookFace account you will be taking over?

Ben.Spring

Correct Answer

Hint

Hack the BookFace account to reveal this task's answer!

THM{BRUTEFORCING}

Correct Answer

Hint

After completing this hands-on experience, go for attending the questions below to complete this room.

TASK 2: NETWORK SECURITY

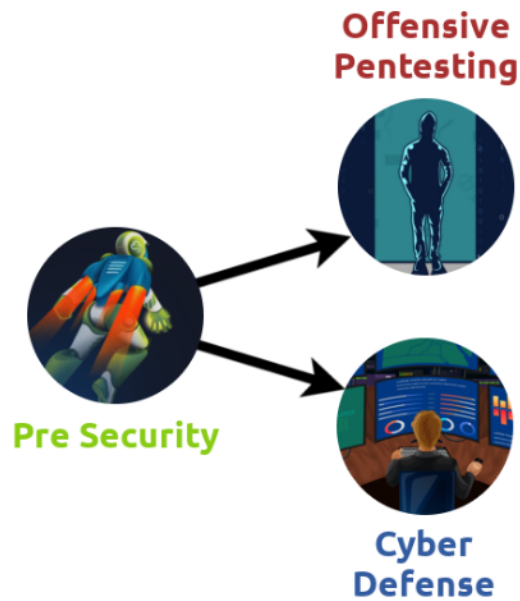
It mainly focuses on why networking is important.

The screenshot displays a cybersecurity training interface. On the left, a sidebar shows 'Room progress (83%)' and two tasks: 'Task 1 Web Application Security' and 'Task 2 Network Security'. Task 2 is active, showing a section titled 'Why networking is important' with a 'View Site' button. Below this, it asks 'How much did the data breach cost Target?' with a correct answer of '\$300 million'. On the right, a large panel titled 'All on the same network' explains the Target hack. It states that air conditioning units, which could be controlled remotely, were also connected to Target's main store network. A diagram shows an 'Attacker' connected to 'Air Conditioning' units, which are then connected to 'Tills' and 'Other Machines' within the store network. Text explains that this allowed an attacker to compromise the smart air conditioning unit and access other machines to steal credit card information.

This task mainly focuses on understanding basic concept of networking. Here it explains a real-world incident that is a retail company was hacked and the attackers stole credit cards from 110 customers and this was only due to air conditioning unit. The attack occurred as Targets air conditioning units could be controlled remotely but were also connected to targets main store network. Being in the same network as the others machine, led to an attacker scanning the network finding machines with vulnerability and exploiting them. The air conditioning units were not directly owned by target. In fact, they were owned by another third-party company who helped to monitor the stores temperature. This shows a basic segmentation flaw. Even more the target was even using a 1.6-million-dollar malware detection tool but attackers managed to fool the detection by pretending to be legitimate computer traffic.

This is a real incident which shows the importance on basic understanding on networking how it works between machines and it's used for hacking.

TASK 3: LEARNING ROADMAP



Above is a learning path roadmap. The Pre Security path will teach you the technical knowledge you need to get started in cyber security. Once you understand the basics, enroll in either the Offensive Pentesting (ethically hacking systems) or the Cyber Defense (investigating attacks and defending systems) path.

The skills you acquire from the learning paths will prepare you for a career as an ethical hacker, penetration tester or cyber security analyst.

Answer the questions below