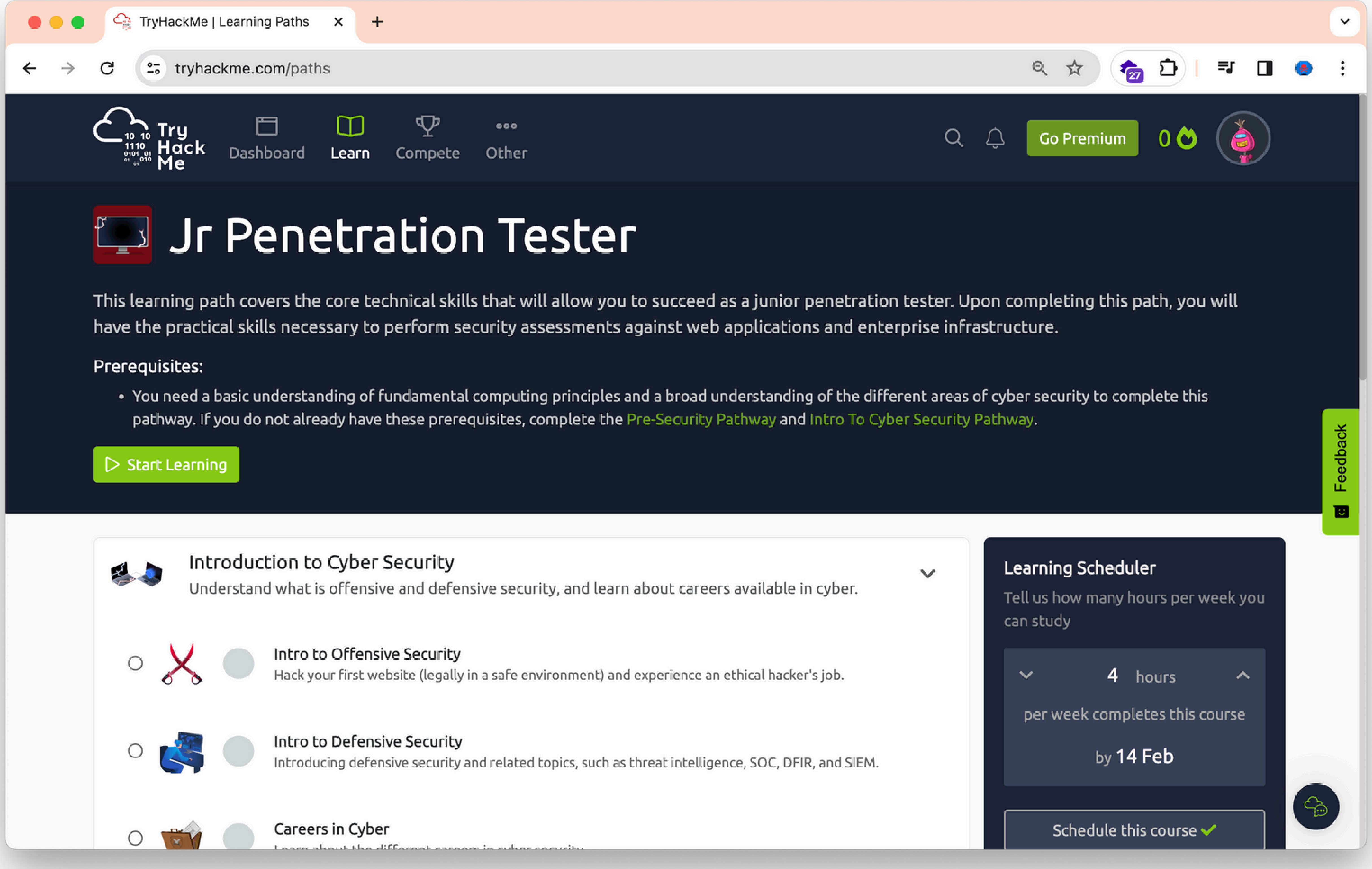
CYBER SECURITY



Jr Penetration Tester

This learning path covers the core technical skills that will allow you to succeed as a junior penetration tester. Upon completing this path, you will have the practical skills necessary to perform security assessments against web applications and enterprise infrastructure.

Prerequisites:

- You need a basic understanding of fundamental computing principles and a broad understanding of the different areas of cyber security to complete this pathway. If you do not already have these prerequisites, complete the Pre-Security Pathway and Intro To Cyber Security Pathway.

▷ Start Learning

Introduction to Cyber Security

Understand what is offensive and defensive security, and learn about careers available in cyber.

○ **Intro to Offensive Security**
Hack your first website (legally in a safe environment) and experience an ethical hacker's job.

○ **Intro to Defensive Security**
Introducing defensive security and related topics, such as threat intelligence, SOC, DFIR, and SIEM.

○ **Careers in Cyber**
Learn about the different careers in cyber security.

Learning Scheduler

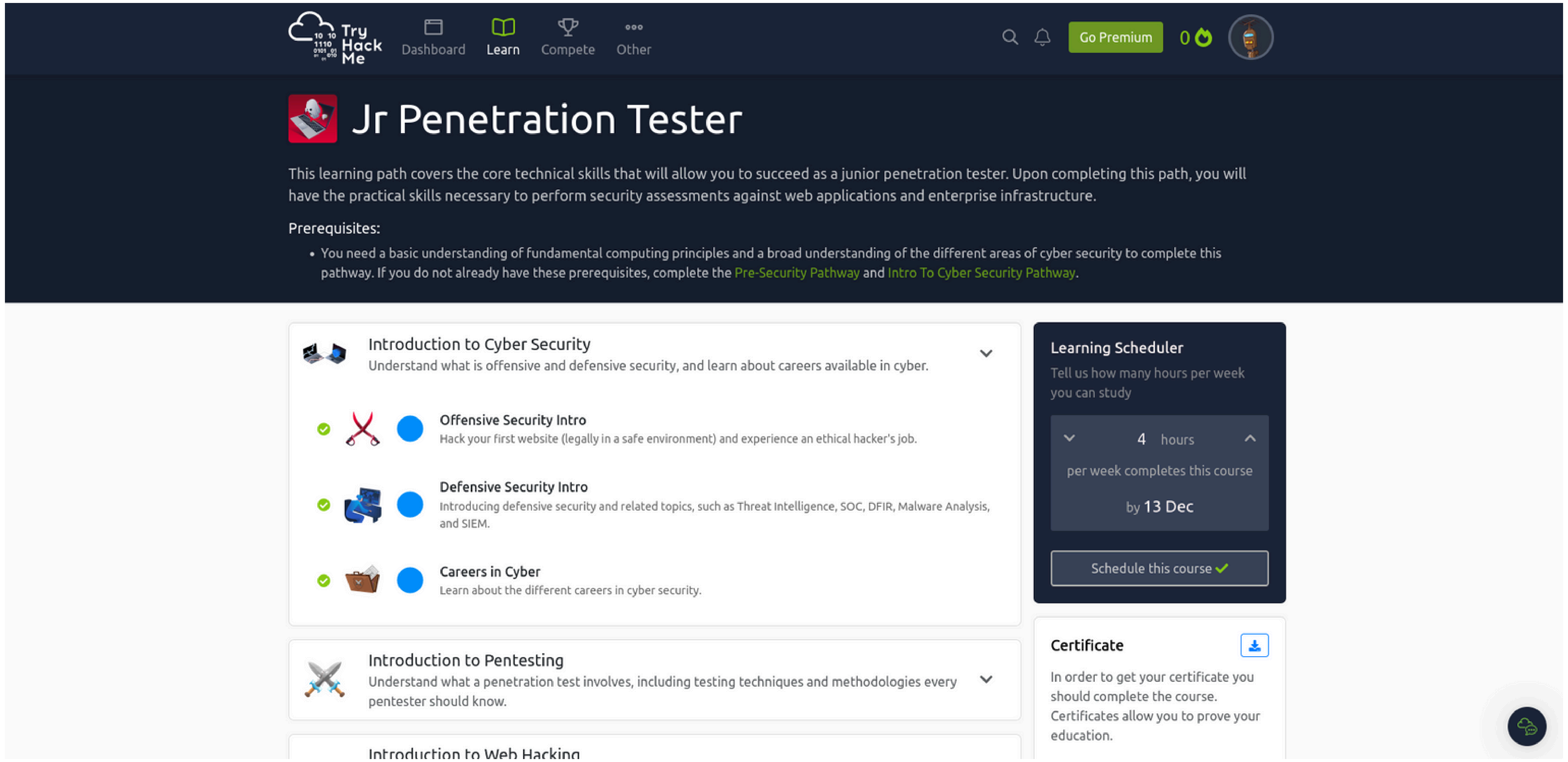
Tell us how many hours per week you can study

4 hours

per week completes this course

by 14 Feb

Schedule this course ✓



Jr Penetration Tester

This learning path covers the core technical skills that will allow you to succeed as a junior penetration tester. Upon completing this path, you will have the practical skills necessary to perform security assessments against web applications and enterprise infrastructure.

Prerequisites:

- You need a basic understanding of fundamental computing principles and a broad understanding of the different areas of cyber security to complete this pathway. If you do not already have these prerequisites, complete the Pre-Security Pathway and Intro To Cyber Security Pathway.

Introduction to Cyber Security

Understand what is offensive and defensive security, and learn about careers available in cyber.

✓ **Offensive Security Intro**
Hack your first website (legally in a safe environment) and experience an ethical hacker's job.

✓ **Defensive Security Intro**
Introducing defensive security and related topics, such as Threat Intelligence, SOC, DFIR, Malware Analysis, and SIEM.

✓ **Careers in Cyber**
Learn about the different careers in cyber security.

Introduction to Pentesting

Understand what a penetration test involves, including testing techniques and methodologies every pentester should know.

Introduction to Web Hacking

Learning Scheduler

Tell us how many hours per week you can study

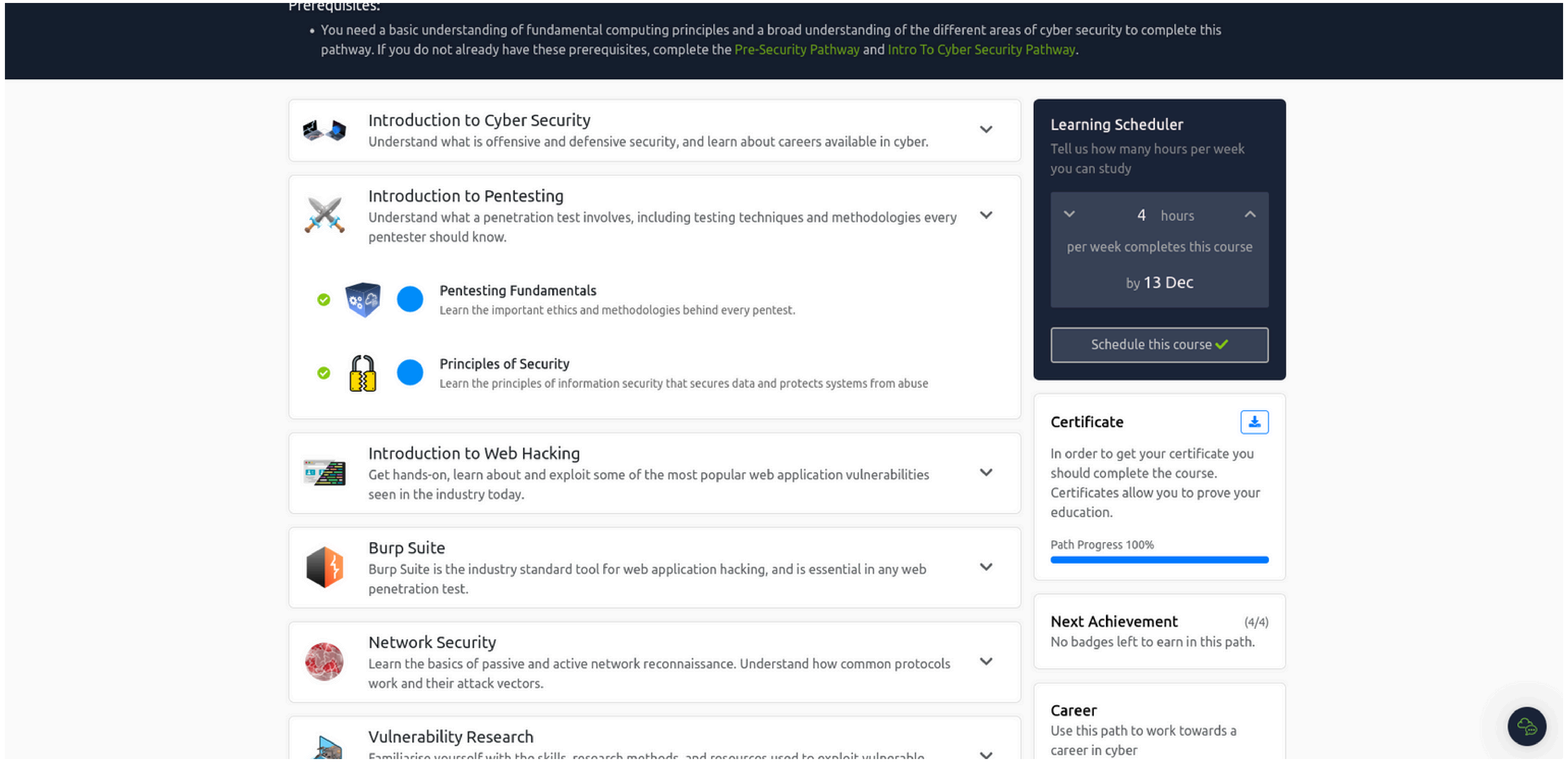
4 hours

per week completes this course

by 13 Dec

Certificate

In order to get your certificate you should complete the course. Certificates allow you to prove your education.



Prerequisites:

- You need a basic understanding of fundamental computing principles and a broad understanding of the different areas of cyber security to complete this pathway. If you do not already have these prerequisites, complete the Pre-Security Pathway and Intro To Cyber Security Pathway.

Introduction to Cyber Security

Understand what is offensive and defensive security, and learn about careers available in cyber.

Introduction to Pentesting

Understand what a penetration test involves, including testing techniques and methodologies every pentester should know.

- ✓ **Pentesting Fundamentals** — Learn the important ethics and methodologies behind every pentest.
- ✓ **Principles of Security** — Learn the principles of information security that secures data and protects systems from abuse

Introduction to Web Hacking

Get hands-on, learn about and exploit some of the most popular web application vulnerabilities seen in the industry today.

Burp Suite

Burp Suite is the industry standard tool for web application hacking, and is essential in any web penetration test.

Network Security

Learn the basics of passive and active network reconnaissance. Understand how common protocols work and their attack vectors.

Vulnerability Research

Familiarise yourself with the skills, research methods, and resources used to exploit vulnerable

Learning Scheduler

Tell us how many hours per week you can study

4 hours

per week completes this course

by 13 Dec

Schedule this course ✓

Certificate

In order to get your certificate you should complete the course. Certificates allow you to prove your education.

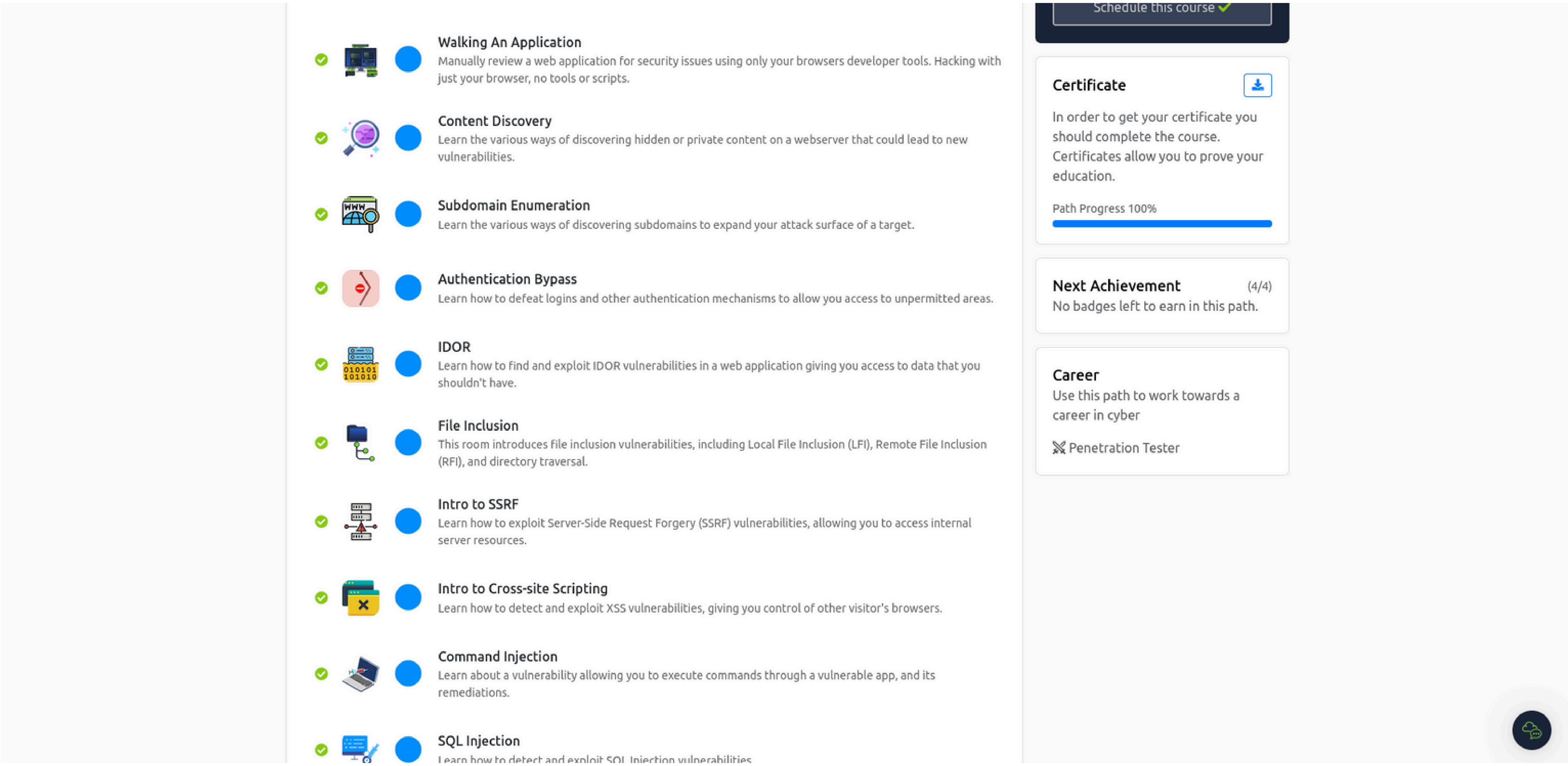
Path Progress 100%

Next Achievement (4/4)

No badges left to earn in this path.

Career

Use this path to work towards a career in cyber



Schedule this course ✓

✓ **Walking An Application**
Manually review a web application for security issues using only your browsers developer tools. Hacking with just your browser, no tools or scripts.

✓ **Content Discovery**
Learn the various ways of discovering hidden or private content on a webserver that could lead to new vulnerabilities.

✓ **Subdomain Enumeration**
Learn the various ways of discovering subdomains to expand your attack surface of a target.

✓ **Authentication Bypass**
Learn how to defeat logins and other authentication mechanisms to allow you access to unpermitted areas.

✓ **IDOR**
Learn how to find and exploit IDOR vulnerabilities in a web application giving you access to data that you shouldn't have.

✓ **File Inclusion**
This room introduces file inclusion vulnerabilities, including Local File Inclusion (LFI), Remote File Inclusion (RFI), and directory traversal.

✓ **Intro to SSRF**
Learn how to exploit Server-Side Request Forgery (SSRF) vulnerabilities, allowing you to access internal server resources.

✓ **Intro to Cross-site Scripting**
Learn how to detect and exploit XSS vulnerabilities, giving you control of other visitor's browsers.

✓ **Command Injection**
Learn about a vulnerability allowing you to execute commands through a vulnerable app, and its remediations.

✓ **SQL Injection**
Learn how to detect and exploit SQL Injection vulnerabilities

Certificate

In order to get your certificate you should complete the course. Certificates allow you to prove your education.

Path Progress 100%

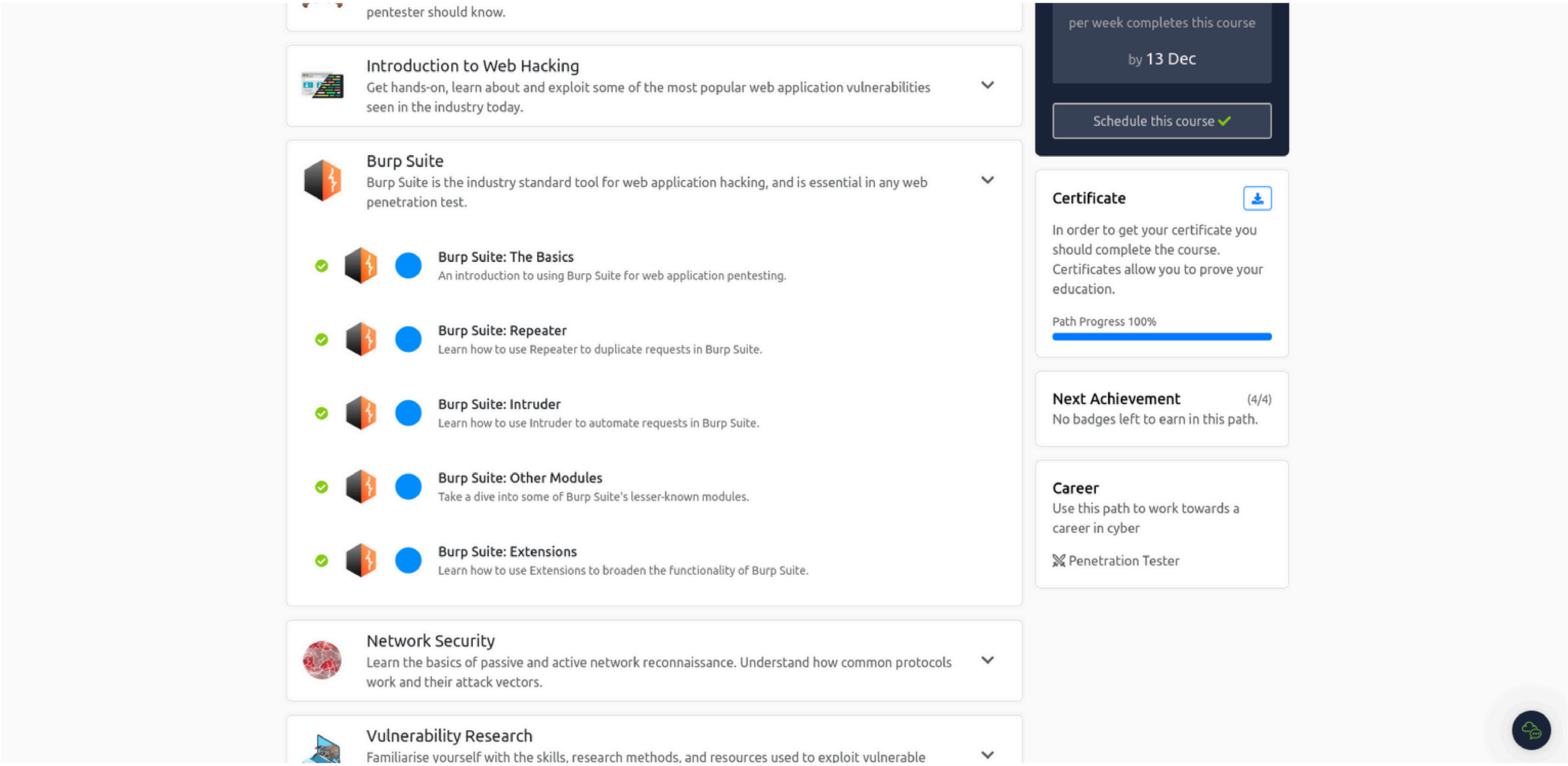
Next Achievement (4/4)

No badges left to earn in this path.

Career

Use this path to work towards a career in cyber

Penetration Tester



pentester should know.

Introduction to Web Hacking

Get hands-on, learn about and exploit some of the most popular web application vulnerabilities seen in the industry today.

Burp Suite

Burp Suite is the industry standard tool for web application hacking, and is essential in any web penetration test.

- ✓ **Burp Suite: The Basics**
  An introduction to using Burp Suite for web application pentesting.
- ✓ **Burp Suite: Repeater**
  Learn how to use Repeater to duplicate requests in Burp Suite.
- ✓ **Burp Suite: Intruder**
  Learn how to use Intruder to automate requests in Burp Suite.
- ✓ **Burp Suite: Other Modules**
  Take a dive into some of Burp Suite's lesser-known modules.
- ✓ **Burp Suite: Extensions**
  Learn how to use Extensions to broaden the functionality of Burp Suite.

Network Security

Learn the basics of passive and active network reconnaissance. Understand how common protocols work and their attack vectors.

Vulnerability Research

Familiarise yourself with the skills, research methods, and resources used to exploit vulnerable

per week completes this course

by 13 Dec

Certificate

In order to get your certificate you should complete the course. Certificates allow you to prove your education.

Path Progress 100%

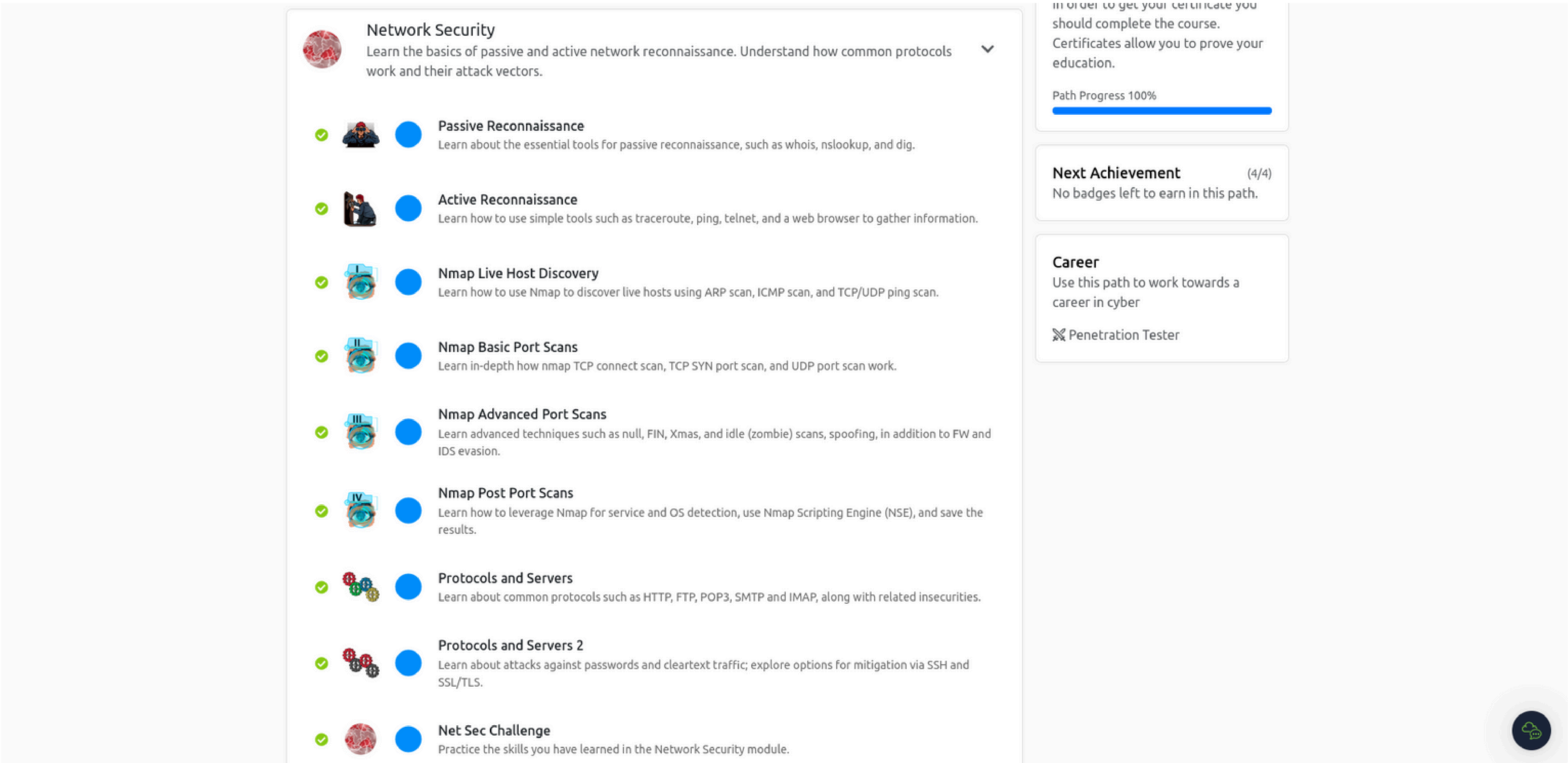
Next Achievement (4/4)

No badges left to earn in this path.

Career

Use this path to work towards a career in cyber

Penetration Tester



Network Security

Learn the basics of passive and active network reconnaissance. Understand how common protocols work and their attack vectors.

- ✓ **Passive Reconnaissance** — Learn about the essential tools for passive reconnaissance, such as whois, nslookup, and dig.
- ✓ **Active Reconnaissance** — Learn how to use simple tools such as traceroute, ping, telnet, and a web browser to gather information.
- ✓ **Nmap Live Host Discovery** — Learn how to use Nmap to discover live hosts using ARP scan, ICMP scan, and TCP/UDP ping scan.
- ✓ **Nmap Basic Port Scans** — Learn in-depth how nmap TCP connect scan, TCP SYN port scan, and UDP port scan work.
- ✓ **Nmap Advanced Port Scans** — Learn advanced techniques such as null, FIN, Xmas, and idle (zombie) scans, spoofing, in addition to FW and IDS evasion.
- ✓ **Nmap Post Port Scans** — Learn how to leverage Nmap for service and OS detection, use Nmap Scripting Engine (NSE), and save the results.
- ✓ **Protocols and Servers** — Learn about common protocols such as HTTP, FTP, POP3, SMTP and IMAP, along with related insecurities.
- ✓ **Protocols and Servers 2** — Learn about attacks against passwords and cleartext traffic; explore options for mitigation via SSH and SSL/TLS.
- ✓ **Net Sec Challenge** — Practice the skills you have learned in the Network Security module.

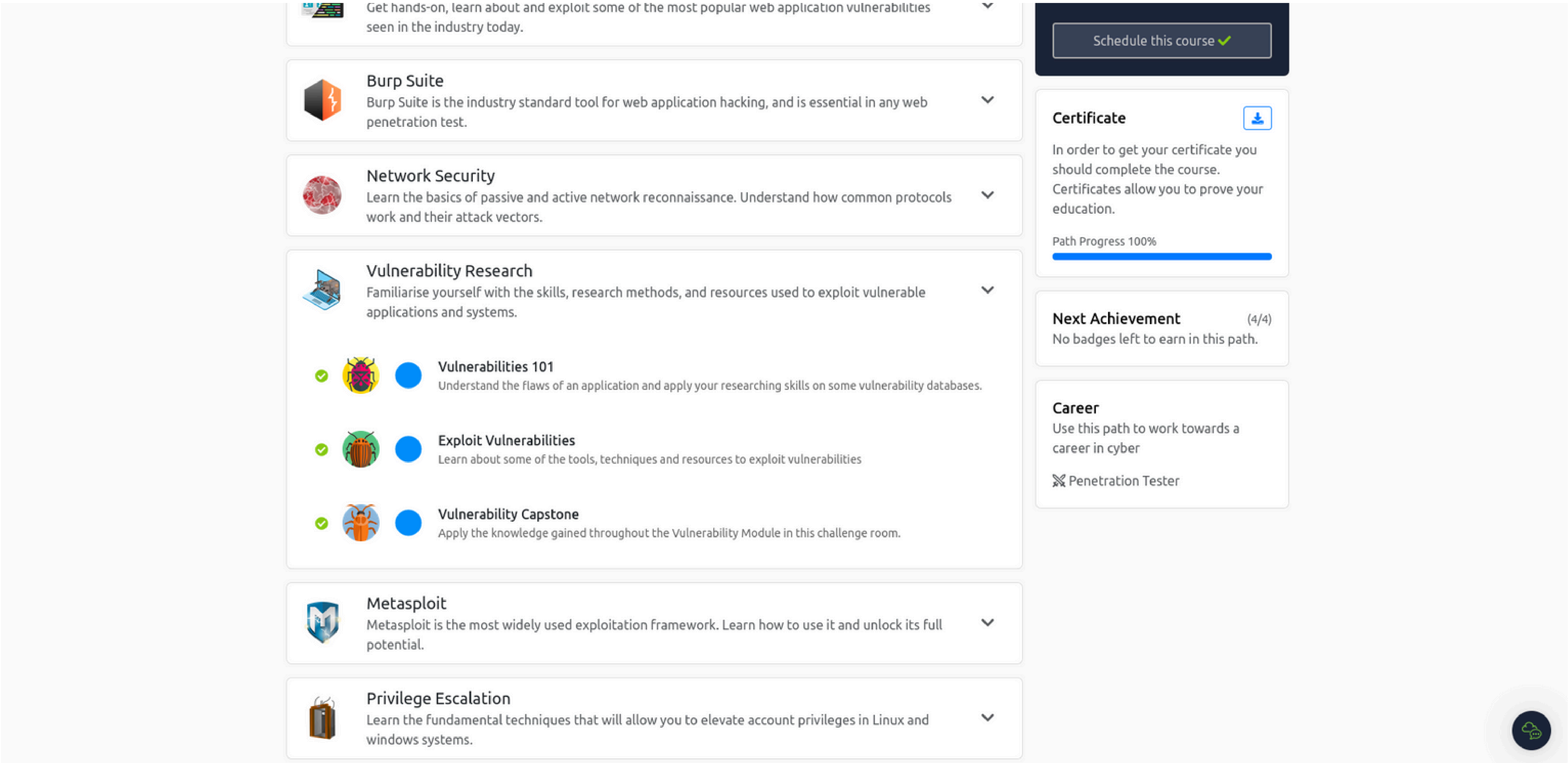
In order to get your certificate you should complete the course. Certificates allow you to prove your education.

Path Progress 100%

Next Achievement (4/4)
No badges left to earn in this path.

Career
Use this path to work towards a career in cyber

Penetration Tester



Get hands-on, learn about and exploit some of the most popular web application vulnerabilities seen in the industry today.

Burp Suite
Burp Suite is the industry standard tool for web application hacking, and is essential in any web penetration test.

Network Security
Learn the basics of passive and active network reconnaissance. Understand how common protocols work and their attack vectors.

Vulnerability Research
Familiarise yourself with the skills, research methods, and resources used to exploit vulnerable applications and systems.

- ✓ **Vulnerabilities 101** — Understand the flaws of an application and apply your researching skills on some vulnerability databases.
- ✓ **Exploit Vulnerabilities** — Learn about some of the tools, techniques and resources to exploit vulnerabilities
- ✓ **Vulnerability Capstone** — Apply the knowledge gained throughout the Vulnerability Module in this challenge room.

Metasploit
Metasploit is the most widely used exploitation framework. Learn how to use it and unlock its full potential.

Privilege Escalation
Learn the fundamental techniques that will allow you to elevate account privileges in Linux and windows systems.

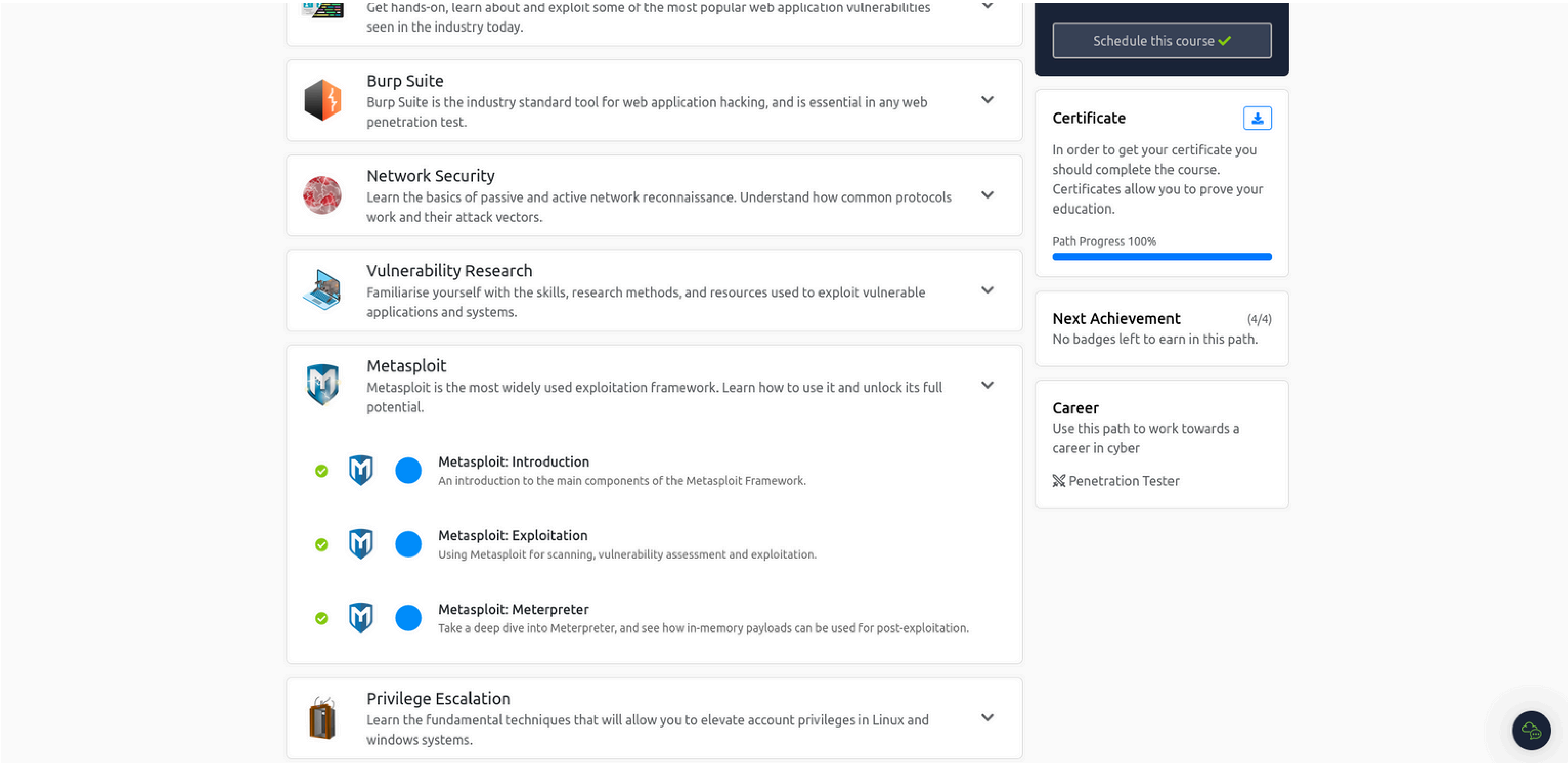
Certificate
In order to get your certificate you should complete the course. Certificates allow you to prove your education.

Path Progress 100%

Next Achievement (4/4)
No badges left to earn in this path.

Career
Use this path to work towards a career in cyber

Penetration Tester



Get hands-on, learn about and exploit some of the most popular web application vulnerabilities seen in the industry today.

Burp Suite

Burp Suite is the industry standard tool for web application hacking, and is essential in any web penetration test.

Network Security

Learn the basics of passive and active network reconnaissance. Understand how common protocols work and their attack vectors.

Vulnerability Research

Familiarise yourself with the skills, research methods, and resources used to exploit vulnerable applications and systems.

Metasploit

Metasploit is the most widely used exploitation framework. Learn how to use it and unlock its full potential.

- ✓ **Metasploit: Introduction**
  An introduction to the main components of the Metasploit Framework.
- ✓ **Metasploit: Exploitation**
  Using Metasploit for scanning, vulnerability assessment and exploitation.
- ✓ **Metasploit: Meterpreter**
  Take a deep dive into Meterpreter, and see how in-memory payloads can be used for post-exploitation.

Privilege Escalation

Learn the fundamental techniques that will allow you to elevate account privileges in Linux and windows systems.

Certificate

In order to get your certificate you should complete the course. Certificates allow you to prove your education.

Path Progress 100%

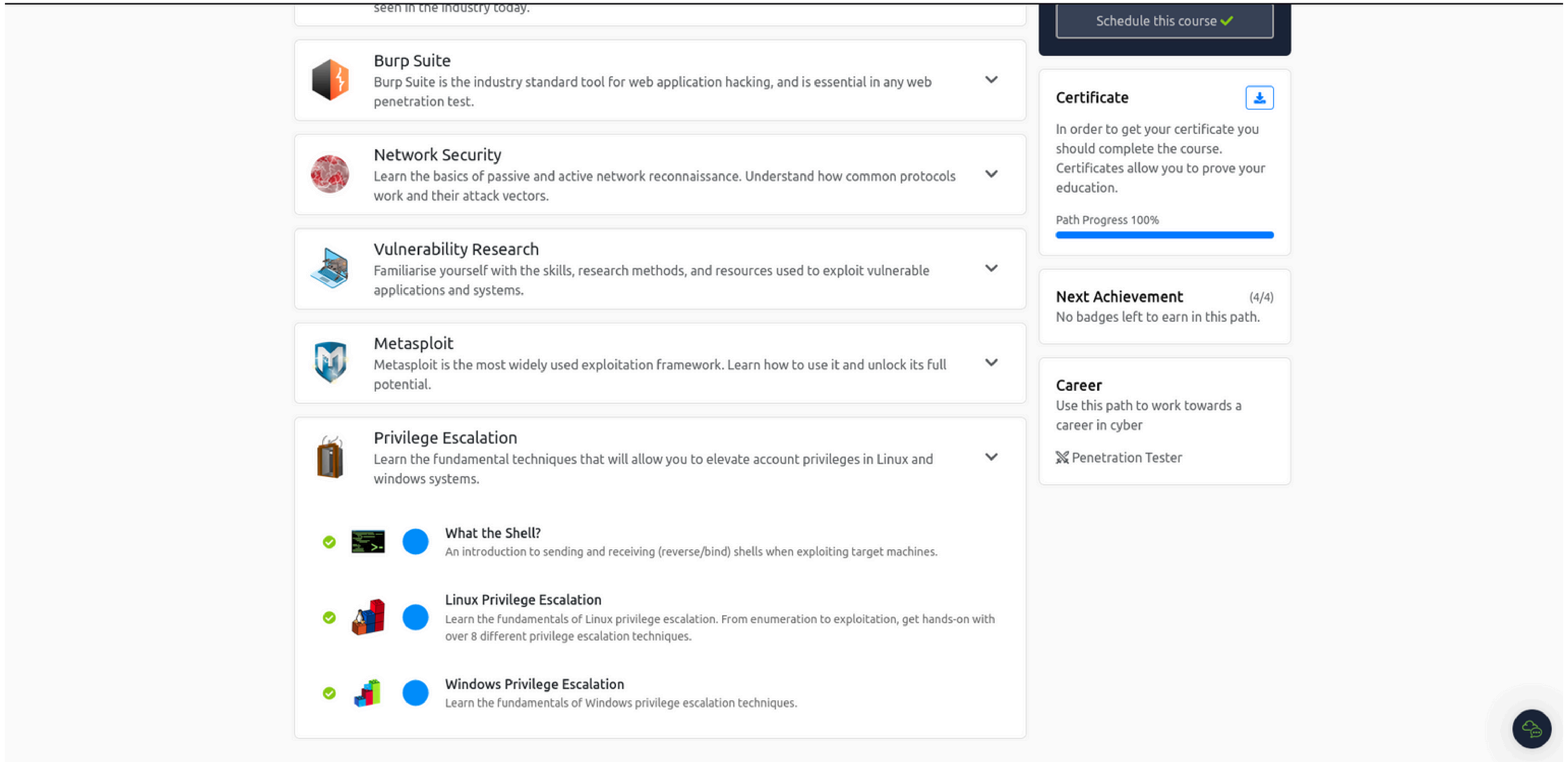
Next Achievement (4/4)

No badges left to earn in this path.

Career

Use this path to work towards a career in cyber

Penetration Tester



seen in the industry today.

Burp Suite
Burp Suite is the industry standard tool for web application hacking, and is essential in any web penetration test.

Network Security
Learn the basics of passive and active network reconnaissance. Understand how common protocols work and their attack vectors.

Vulnerability Research
Familiarise yourself with the skills, research methods, and resources used to exploit vulnerable applications and systems.

Metasploit
Metasploit is the most widely used exploitation framework. Learn how to use it and unlock its full potential.

Privilege Escalation
Learn the fundamental techniques that will allow you to elevate account privileges in Linux and windows systems.

✓ ● **What the Shell?**
An introduction to sending and receiving (reverse/bind) shells when exploiting target machines.

✓ ● **Linux Privilege Escalation**
Learn the fundamentals of Linux privilege escalation. From enumeration to exploitation, get hands-on with over 8 different privilege escalation techniques.

✓ ● **Windows Privilege Escalation**
Learn the fundamentals of Windows privilege escalation techniques.

Schedule this course ✓

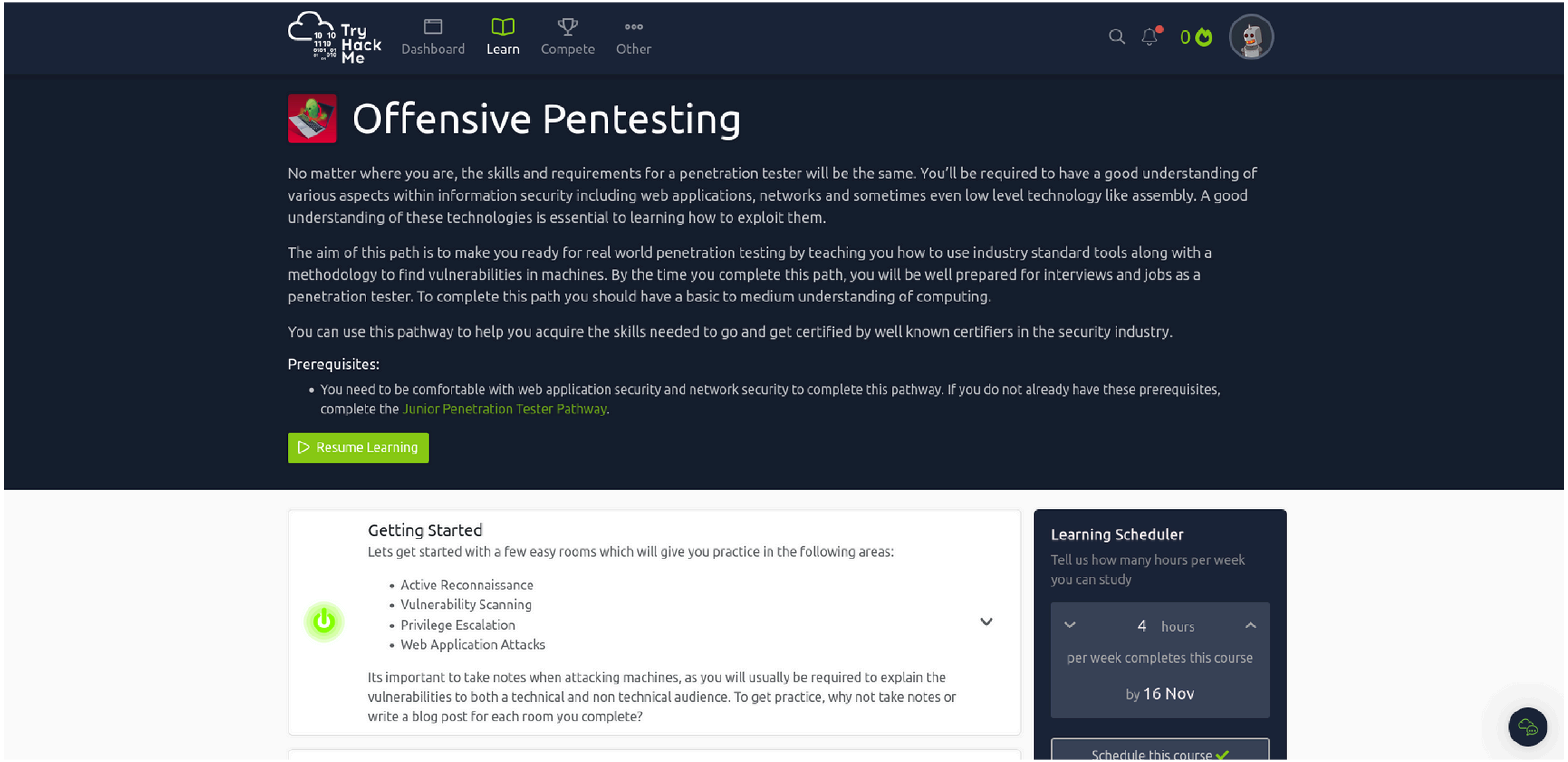
Certificate
In order to get your certificate you should complete the course. Certificates allow you to prove your education.

Path Progress 100%

Next Achievement (4/4)
No badges left to earn in this path.

Career
Use this path to work towards a career in cyber

Penetration Tester



Offensive Pentesting

No matter where you are, the skills and requirements for a penetration tester will be the same. You'll be required to have a good understanding of various aspects within information security including web applications, networks and sometimes even low level technology like assembly. A good understanding of these technologies is essential to learning how to exploit them.

The aim of this path is to make you ready for real world penetration testing by teaching you how to use industry standard tools along with a methodology to find vulnerabilities in machines. By the time you complete this path, you will be well prepared for interviews and jobs as a penetration tester. To complete this path you should have a basic to medium understanding of computing.

You can use this pathway to help you acquire the skills needed to go and get certified by well known certifiers in the security industry.

Prerequisites:

- You need to be comfortable with web application security and network security to complete this pathway. If you do not already have these prerequisites, complete the Junior Penetration Tester Pathway.

Getting Started

Lets get started with a few easy rooms which will give you practice in the following areas:

- Active Reconnaissance
- Vulnerability Scanning
- Privilege Escalation
- Web Application Attacks

Its important to take notes when attacking machines, as you will usually be required to explain the vulnerabilities to both a technical and non technical audience. To get practice, why not take notes or write a blog post for each room you complete?

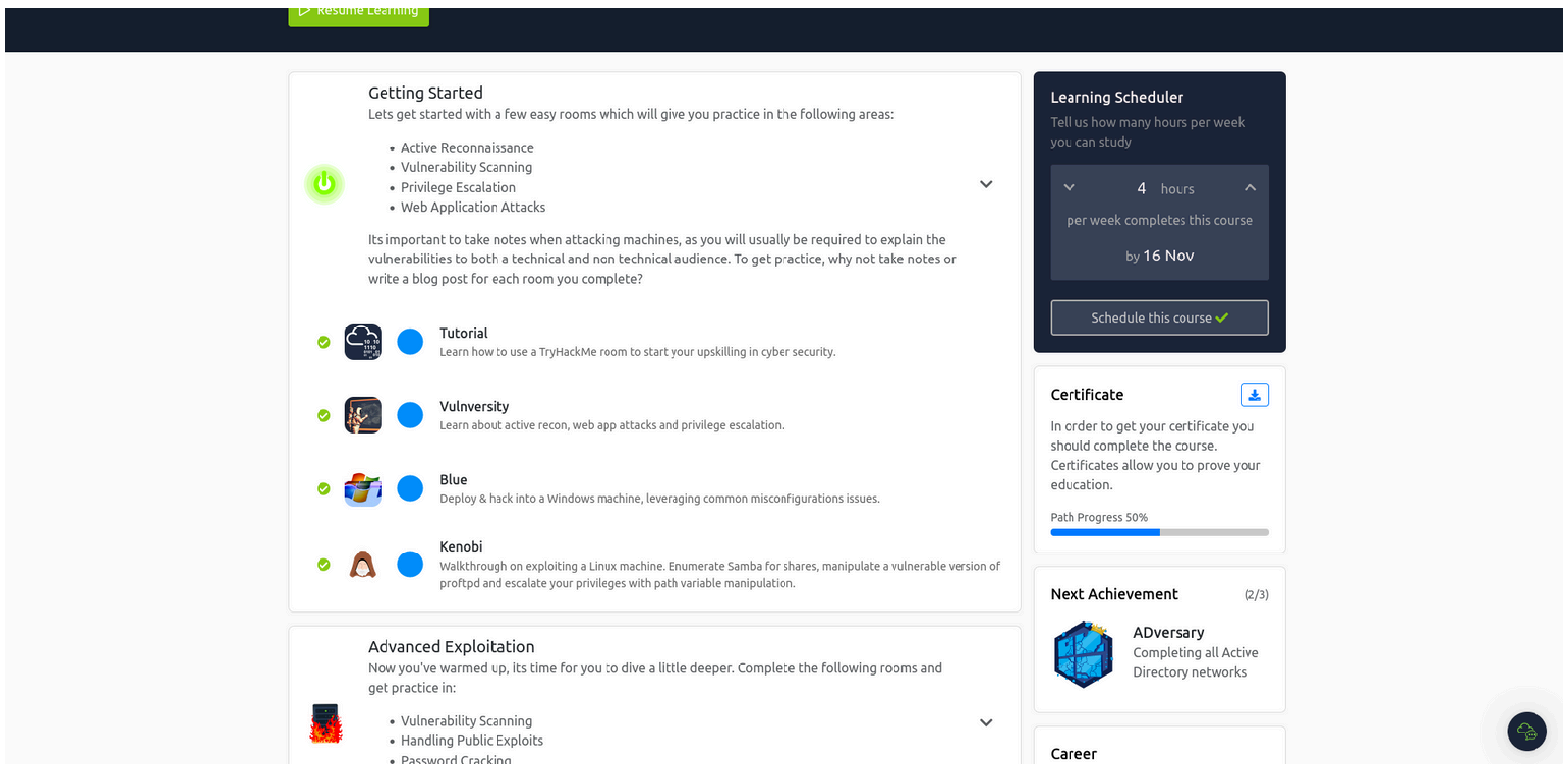
Learning Scheduler

Tell us how many hours per week you can study

4 hours

per week completes this course

by 16 Nov



Getting Started

Lets get started with a few easy rooms which will give you practice in the following areas:

- Active Reconnaissance
- Vulnerability Scanning
- Privilege Escalation
- Web Application Attacks

Its important to take notes when attacking machines, as you will usually be required to explain the vulnerabilities to both a technical and non technical audience. To get practice, why not take notes or write a blog post for each room you complete?

✓ Tutorial
Learn how to use a TryHackMe room to start your upskilling in cyber security.

✓ Vulnversity
Learn about active recon, web app attacks and privilege escalation.

✓ Blue
Deploy & hack into a Windows machine, leveraging common misconfigurations issues.

✓ Kenobi
Walkthrough on exploiting a Linux machine. Enumerate Samba for shares, manipulate a vulnerable version of proftpd and escalate your privileges with path variable manipulation.

Advanced Exploitation

Now you've warmed up, its time for you to dive a little deeper. Complete the following rooms and get practice in:

- Vulnerability Scanning
- Handling Public Exploits
- Password Cracking

Learning Scheduler

Tell us how many hours per week you can study

4 hours

per week completes this course

by 16 Nov

Certificate

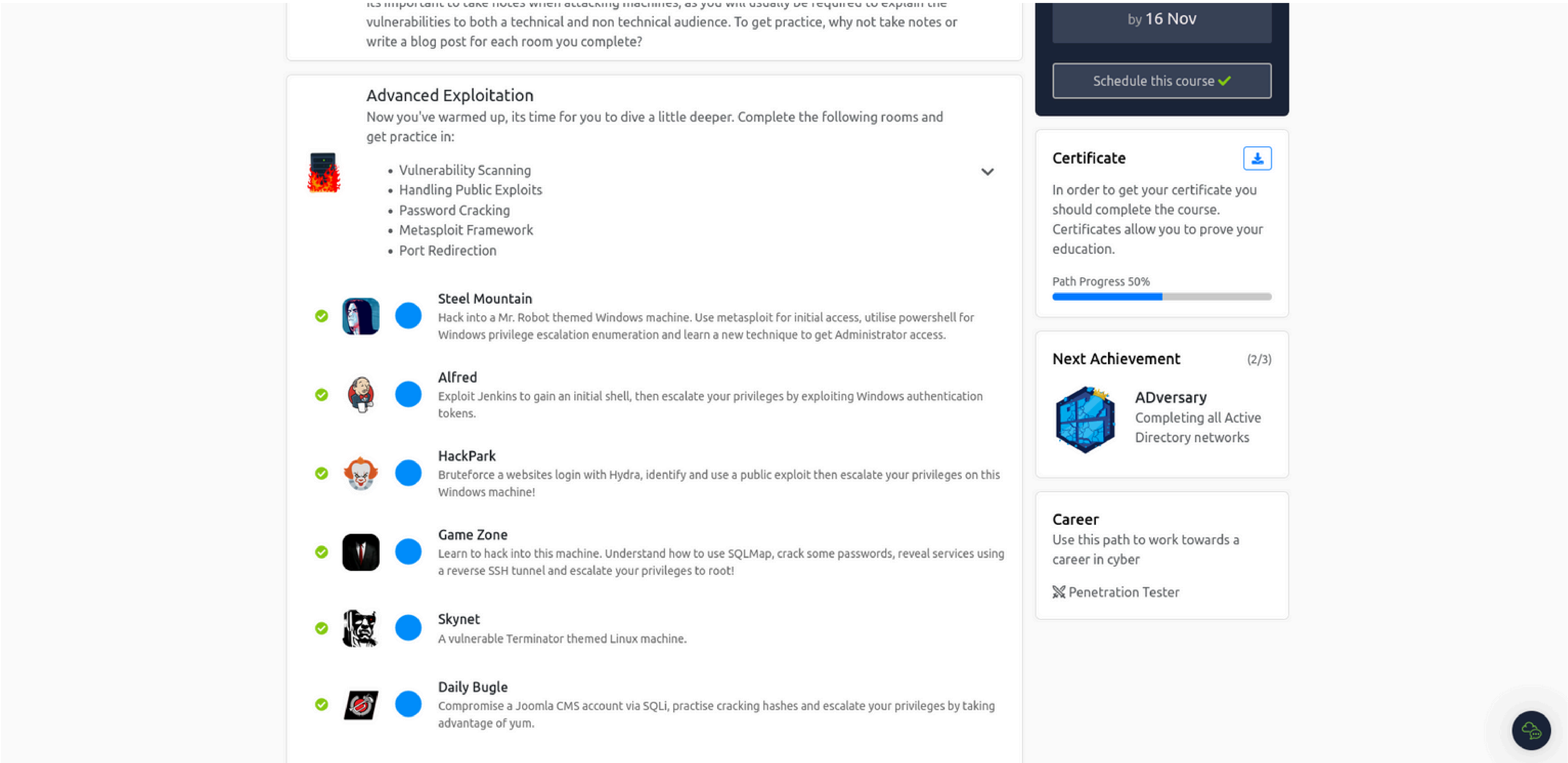
In order to get your certificate you should complete the course. Certificates allow you to prove your education.

Path Progress 50%

Next Achievement (2/3)

ADversary
Completing all Active Directory networks

Career



its important to take notes when attacking machines, as you will usually be required to explain the vulnerabilities to both a technical and non technical audience. To get practice, why not take notes or write a blog post for each room you complete?

Advanced Exploitation

Now you've warmed up, its time for you to dive a little deeper. Complete the following rooms and get practice in:

- Vulnerability Scanning
- Handling Public Exploits
- Password Cracking
- Metasploit Framework
- Port Redirection

✓ **Steel Mountain**
Hack into a Mr. Robot themed Windows machine. Use metasploit for initial access, utilise powershell for Windows privilege escalation enumeration and learn a new technique to get Administrator access.

✓ **Alfred**
Exploit Jenkins to gain an initial shell, then escalate your privileges by exploiting Windows authentication tokens.

✓ **HackPark**
Bruteforce a websites login with Hydra, identify and use a public exploit then escalate your privileges on this Windows machine!

✓ **Game Zone**
Learn to hack into this machine. Understand how to use SQLMap, crack some passwords, reveal services using a reverse SSH tunnel and escalate your privileges to root!

✓ **Skynet**
A vulnerable Terminator themed Linux machine.

✓ **Daily Bugle**
Compromise a Joomla CMS account via SQLi, practise cracking hashes and escalate your privileges by taking advantage of yum.

by 16 Nov

Schedule this course ✓

Certificate

In order to get your certificate you should complete the course. Certificates allow you to prove your education.

Path Progress 50%

Next Achievement

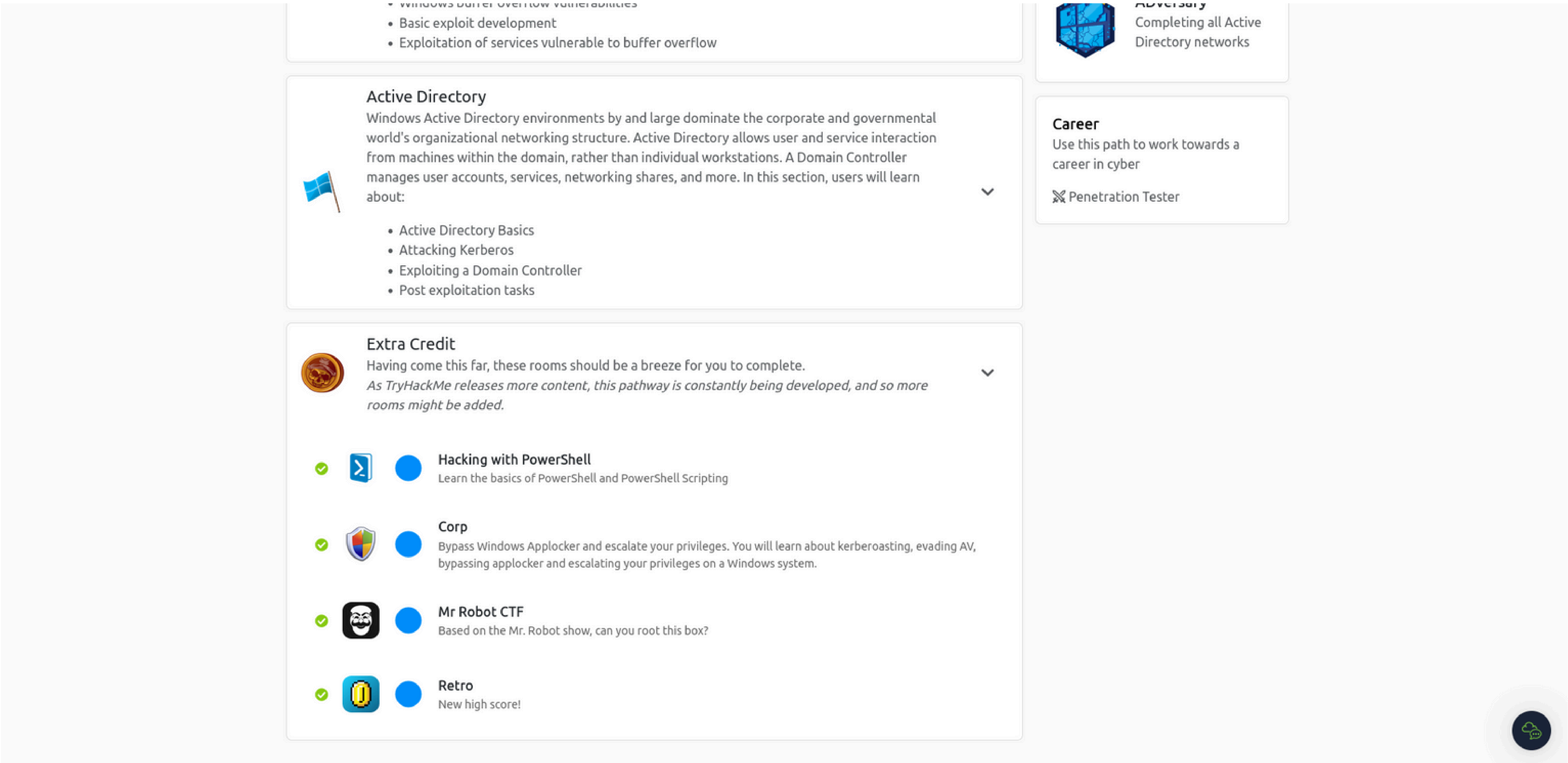
(2/3)

ADversary
Completing all Active Directory networks

Career

Use this path to work towards a career in cyber

Penetration Tester



- Windows buffer overflow vulnerabilities
- Basic exploit development
- Exploitation of services vulnerable to buffer overflow

Active Directory

Windows Active Directory environments by and large dominate the corporate and governmental world's organizational networking structure. Active Directory allows user and service interaction from machines within the domain, rather than individual workstations. A Domain Controller manages user accounts, services, networking shares, and more. In this section, users will learn about:

- Active Directory Basics
- Attacking Kerberos
- Exploiting a Domain Controller
- Post exploitation tasks

Extra Credit

Having come this far, these rooms should be a breeze for you to complete.

As TryHackMe releases more content, this pathway is constantly being developed, and so more rooms might be added.

✓ **Hacking with PowerShell**
Learn the basics of PowerShell and PowerShell Scripting

✓ **Corp**
Bypass Windows Applocker and escalate your privileges. You will learn about kerberoasting, evading AV, bypassing applocker and escalating your privileges on a Windows system.

✓ **Mr Robot CTF**
Based on the Mr. Robot show, can you root this box?

✓ **Retro**
New high score!

ADversary
Completing all Active Directory networks

Career
Use this path to work towards a career in cyber

Penetration Tester