v4

Penetration Testing Student

Next Steps

Section03 |Module 07

Table of Contents

MODULE 07 | Next Steps

7.1 What to do Next

7.2 Penetration Testing Approach

7.3 Career Paths

7.4 Beyond PTS

Learning Objectives

By the end of this module, you should have a better understanding of:

- ✓ How to continue your penetration testing career
- ✓ What types of security-oriented jobs are available on the market

7.1

Preparing for the Exam

7.1.1 Preparing for the Exam

Congratulations! You completed the eLearnSecurity *Penetration Testing Student* course! This course gave you the skills required to start your career in information security and penetration testing.

7.1.1 Preparing for the Exam

In preparation for the Penetration Testing Student exam (eJPT), we have put together 3 extensive Black-box Penetration Testing labs. You will be able to take the knowledge and skills you acquired from the course and actively apply them to these Blind Penetration Tests.

**Please note, that these challenges are available for those with the Elite Edition. If you are interested in upgrading your account, please visit the following* *link*.

7.1.1 Preparing for the Exam

Each of these Black-box Penetration Testing labs contains 2-4 machines that should be exploited. There will be no hints on how approach them, so any technique you learned throughout the course may be applicable.

7.1.1 Preparing for the Exam

There is a flag file on every machine. If you are able to read it, this means that the machine was successfully compromised. But be aware, that this might not be the end! There could be more valuable information on the machine that could help you compromise additional hosts.

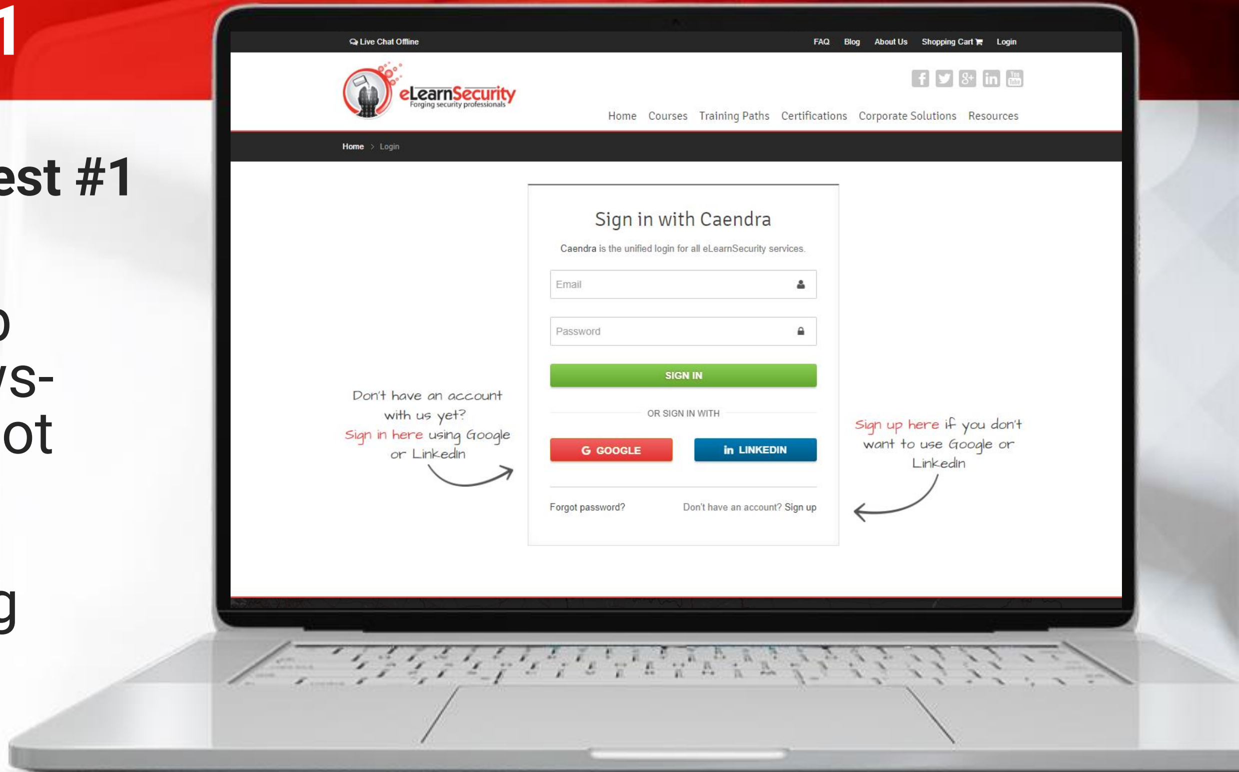
7.1.1 Preparing for the Exam

Furthermore, these Black-box Penetration Testing labs will be a great experience for your next steps outside of the course, as well as a great preparation tool for our PTP course.

7.1.1.1 Black-box Penetration Test #1

Black-box Penetration Test #1

The first Black-box Penetration Testing lab contains some windows-based machines (but not only!). Make sure you refresh your Windows command line scripting skills.



Sign in with Caendra

Caendra is the unified login for all eLearnSecurity services.

Don't have an account with us yet? Sign in here using Google or LinkedIn

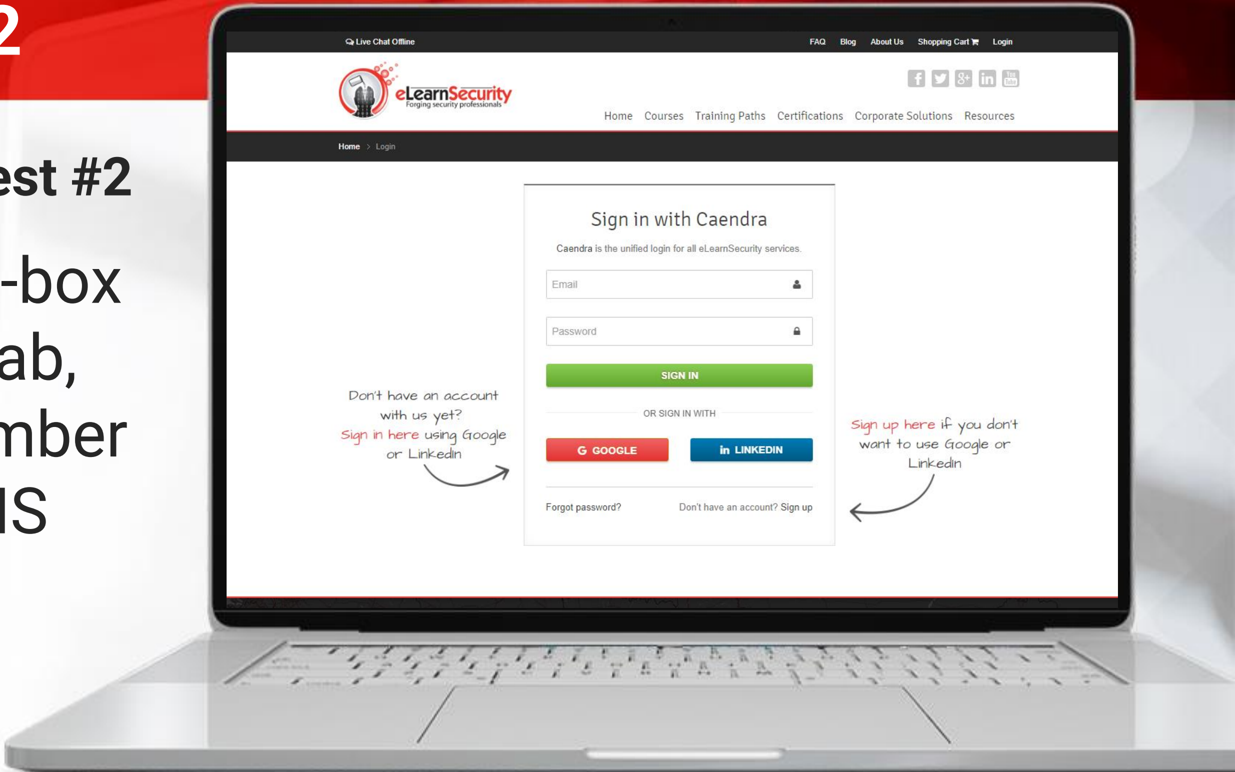
Sign up here if you don't want to use Google or LinkedIn

******The Lab Challenges are only available in the Elite Edition of this course. To upgrade, click HERE. To access, go to the course in your members area and click the labs drop-down in the appropriate module line or to the virtual labs tabs on the left navigation.*

7.1.1.2 Black-box Penetration Test #2

Black-box Penetration Test #2

For the second Black-box Penetration Testing lab, make sure you remember the basics of how DNS works.



Sign in with Caendra

Caendra is the unified login for all eLearnSecurity services.

Don't have an account with us yet? Sign in here using Google or LinkedIn

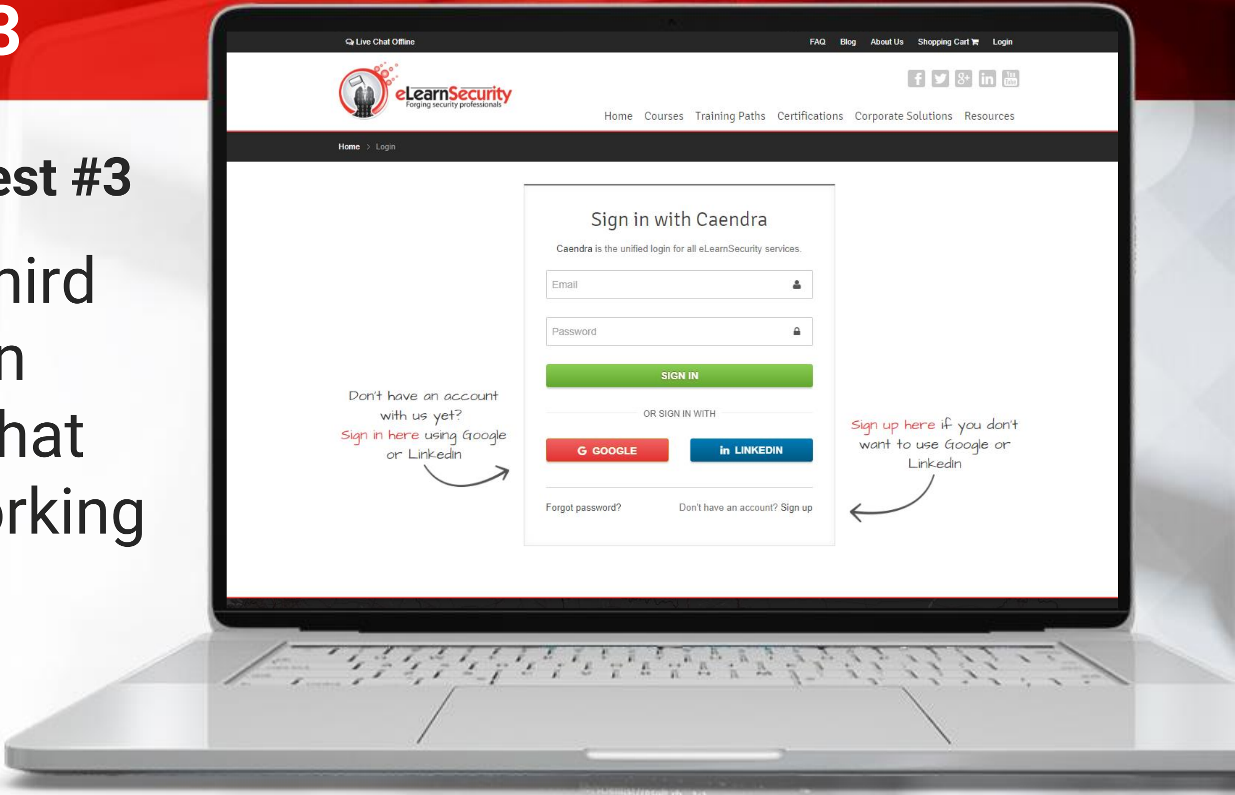
Sign up here if you don't want to use Google or LinkedIn

***The Lab Challenges are only available in the Elite Edition of this course. To upgrade, click HERE. To access, go to the course in your members area and click the labs drop-down in the appropriate module line or to the virtual labs tabs on the left navigation.**

7.1.1.3 Black-box Penetration Test #3

Black-box Penetration Test #3

When attacking the third Black-box Penetration Testing lab, be sure that you remember networking basics.



Sign in with Caendra

Caendra is the unified login for all eLearnSecurity services.

Don't have an account with us yet? Sign in here using Google or LinkedIn

Sign up here if you don't want to use Google or LinkedIn

*The Lab Challenges are only available in the Elite Edition of this course. To upgrade, click HERE. To access, go to the course in your members area and click the labs drop-down in the appropriate module line or to the virtual labs tabs on the left navigation.

7.1.2 Taking the eJPT

If you have the Full or Elite Edition, you can now test your practical pentesting skills with the ***eLearnSecurity Junior Penetration Tester* (eJPT) certification exam**!

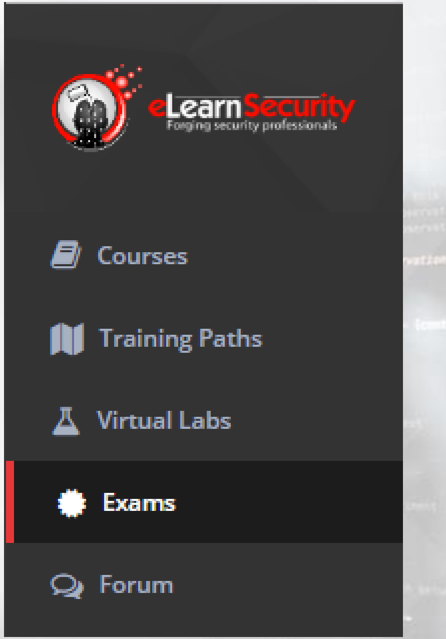
You got basic skills in penetration testing and you are able to exploit systems, networks and applications.

7.1.2 Taking the eJPT

If you feel ready to take the exam, make sure you have a sufficient amount of spare time to dedicate for solving all the exam's tasks.

7.1.2 Taking the eJPT

In order to start the exam, log into the member's area and click on the **Exams** tab on your left.



7.1.2 Taking the eJPT

There you will find detailed instructions on how to start the exam.

After you start the certification process, you will be able to access the **letter of engagement** – a document that includes the tasks to be performed in order to pass the exam. Read it carefully before you start.

7.1.3 Staying Connected

You should be aware, that a penetration tester never stops learning. If you stop, you will soon be behind, as the market is rapidly growing.

New (and updated) technologies and applications constantly appear and new exploitation techniques are being discovered daily.

7.1.3 Staying Connected

It is extremely important to be up-to-date. You are encouraged to follow your favourite researchers on social media, such as Twitter, in order to catch the latest discoveries from the field of IT Security. It's up to you who you will choose to follow.

7.1.3 Staying Connected

Many security researchers also maintain active blogs, that oftentimes include some interesting vulnerability writeups.

Remember to bookmark them and read from time to time!

7.2

Penetration Testing Approach

7.2 Penetration Testing Approach

In every penetration test you participate in, you should do your best.

Also, never be ashamed to learn things you do not understand.

7.2 Penetration Testing Approach

Curiosity can be a penetration tester’s greatest weapon; on every test you take, you should aim to understand every single detail of the tested assets.

You should be prepared to try numerous methods until you are sure something is really safe.

7.2 Penetration Testing Approach

On almost every test you conduct, you will need to use a search engine.

It is not possible to remember all the syntax, every function name and every exploit.

7.2 Penetration Testing Approach

In order to work more systematically, you can adopt one of the existing penetration testing methodologies. For example, **OWASP** published a “Testing Checklist” which you might want to use in order not to miss something during an engagement.

https://www.owasp.org/index.php/Testing_Checklist

https://www.owasp.org/index.php/Testing_Checklist

7.2 Penetration Testing Approach

Using a certain methodology (e.g. **OWASP**) also has another advantage – you can show your client what tests will be conducted exactly. The whole checklist can be used as an attachment to the penetration test contract or letter of engagement.

7.3

Career Paths

7.3 Career Paths

IT Security is a large branch of the market, with a wide range of career paths and specializations.

Let’s check out some possible options.

7.3 Career Paths

There are a few possible paths for an ethical hacker to choose from, for example:

- Web application / network penetration tester
- Red teamer / Social engineer
- Reverse engineer
- Security researcher
- Mobile application penetration tester

7.3 Career Paths

Depending on your interests, you may also want to engage more in the defense side as a/an:

- Incident Response team member
- CCERT analyst
- Malware analyst
- Threat Hunter
- Secure software developer
- Network and systems defender

7.3 Career Paths

We at **eLearnSecurity** also have some suggested training paths already prepared. Be sure to check them out if you are looking for that next career step:

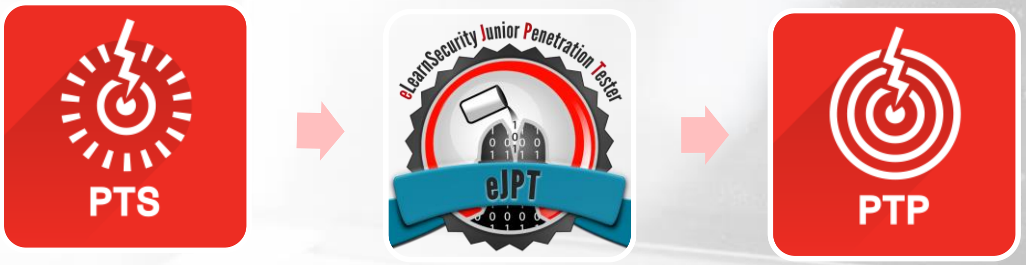
https://www.elearnsecurity.com/training_paths/

7.4

Beyond PTS

7.4 Beyond PTS

By obtaining the ***eJPT* certification** not only you can prove your skills during a job interview, but you also have the proof that you have all the pre-requisites to enroll in our advanced Penetration testing course: *Penetration Testing Professional* course.



https://www.elearnsecurity.com/course/penetration_testing/

7.4 Beyond PTS

Taking the *Penetration Testing Professional (PTP)* course is the next best step if you want to further develop your skills on:

- Professional pentesting
- System attacks
- Network attacks
- Web application attacks

- WiFi Attacks
- Exploit development
- Writing custom *Metasploit* modules

7.4 Beyond PTS

Moreover, the PTP course will offer you the opportunity to earn a **highly respected certification:** the **eCPPTv2**!

https://www.elearnsecurity.com/certification/ecpptv2/

7.4 Beyond PTS

We at eLearnSecurity hope that you enjoyed studying this course, and hope to see you in our other courses.

We wish you a long and successful career in Information Security.

7.4 Beyond PTS

Thank you very much for choosing the *Penetration Testing Student* course!

Yours truly,

The eLearnSecurity Training Team

References

References

Penetration Testing Student Course

https://www.elearnsecurity.com/course/penetration_testing_student/

Penetration Testing Professional Course

https://www.elearnsecurity.com/course/penetration_testing/

eLearnSecurity Training Paths

https://www.elearnsecurity.com/training_paths/

eCPPT

https://www.elearnsecurity.com/certification/ecppt

Labs

Blind Penetration Test 1

First lab contains some windows-based machines (but not only!). Do you remember windows command line scripting?

Blind Penetration Test 2

For this lab, be sure you remember basics of how DNS works.

*The Lab Challenges are only available in the Elite Edition of this course. To upgrade, click HERE. To access, go to the course in your members area and click the labs drop-down in the appropriate module line or to the virtual labs tabs on the left navigation.

Labs

Blind Penetration Test 3

When attacking this lab, be sure that you remember networking basics.

***The Lab Challenges are only available in the Elite Edition of this course. To upgrade, click HERE. To access, go to the course in your members area and click the labs drop-down in the appropriate module line or to the virtual labs tabs on the left navigation.**