



# ETHICAL HACKING PRACTITIONER

Sample Exam Questions

## Introduction

This document contains 4 questions (and answers) that help you familiarise yourself with the structure and topic areas of the SECO-Institute's Ethical Hacking Practitioner certification exam.

To download our Complete Sample Exam, create a free study account at <https://members.seco-institute.org>

We recommend you to take the Complete Sample Exam before registering for the certification exam.

The results of the Sample Exam do not count towards your examination score.

**Note: The Complete Sample Exam prepares you for the written part of the certification exam.**

- *The certification exam consists of a computer-based written exam and a lab exercise (Capture the Flag). You will complete the lab exercise on your last course day. The lab exercise makes up 30% of your final examination score.*
- *After completing the lab exercise in class, you will be asked to save your results as a text file. When taking the written exam, you will have to upload this text file to the online exam environment.*

## Certification exam

You can book your exam with an accredited training partner or directly with the SECO-Institute.

To book an exam with the SECO-Institute, go to: <https://www.seco-institute.org/how-to-book-your-exam-schedule-an-exam/>

By passing the certification exam and earning a SECO-Ethical Hacking Practitioner Certificate, you demonstrate that you have hands-on experience in each stage of the penetration testing process. You can scan network traffic, hack wireless networks, exploit vulnerabilities to penetrate computers and websites, and draft a final penetration test report for your management.

## Exam format

Part 1: Lab exercise completed in class (30%)

Part 2: Computer-based written exam with remote proctoring

- 10 multiple-choice questions
- 5 open-ended questions
- Time allowed: 120 minutes
- Closed-book exam
- Pass mark: 60% of the total marks

## Questions



### Question 1

What is a popular tool to keep track of penetration test results?

- A. KeepTrack
- B. KeepNote
- C. TrackTrace
- D. OpenVAS

### Question 2

Which CVSS score suits best for an SQL Injection that can be exploited remotely?

- A. CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N
- B. CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:U/C:H/I:L/A:N
- C. CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:C/C:N/I:L/A:N
- D. CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H

### Question 3

Robert wants to know the IPv6 address for [www.seco-institute.org](http://www.seco-institute.org). Which record is he looking for?

- A. CNAME
- B. PTR
- C. NS
- D. AAAA

### Question 4

Julia wants to scan all TCP/IP ports including a service scan on the open ports and determine which operating system the target is running. Which command would be best to achieve this?

- A. `nmap -vv -T5 -A -p 1-65545 <target>`
- B. `nmap -vv -T4 -A -p - <target>`
- C. `nmap -vv -p all -sV -O <target>`
- D. `nmap -vv -p 0-65535 --scripts=os_detect,service_ident <target>`

**Question 5**

What elements does a proper penetration test report contain?

## Answers



1. **B**  
KeepNote is used to keep track of notes during penetration testing. It is a free and open-source tool, which is included in Kali Linux by default.
2. **A**  
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N
3. **D**  
AAAA
4. **B**  
`nmap -vv -T4 -A -p - <target>`
5. An introductory text, definition of scope, management summary, findings described properly and in a reproduceable manner, often providing information towards a solution, and a conclusion. During the training, a sample penetration test report was discussed.



© SECO Institute

All rights reserved. No part of this document or its contents may be adapted, translated, stored, reproduced and/or made public in any form or by any means, either electronically through print, (photo)copy, recording, in digital form or in any other way, without the prior written permission of the SECO Institute. Making this document public also explicitly includes its use within courses, lessons, trainings, seminars and other forms of instruction or demonstration.

This document is granted to those who are participating or have participated in a training, course, seminar, or similar event developed or authorised by the SECO Institute. The contents of this document, or parts thereof, may not be submitted or made available to third parties under whatever title without the prior explicit permission of the SECO Institute.

Although the SECO Institute has done everything to prevent irregularities in this document, errors may still occur. Therefore, any person who acts on the basis of the content of this document does so at his/her own risk and is aware of the fact that the SECO Institute cannot be held accountable for any possible damage ensuing from his/her actions.

The authors of this document have done their utmost to identify all possible rightful parties other than the SECO Institute. Should you be a rightful party, or represent one, or know one, and be of the opinion that this document unjustly contains copyrighted material, please do not hesitate to contact the SECO Institute.