



# ETHICAL HACKING FOUNDATION

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 Foundation 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.

## **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 Foundation Certificate, you demonstrate that you can use Wi-Fi hacking, web vulnerability scanning, SQL injection, password cracking and file inclusion techniques. You understand the way hackers think, and you are able to perform a basic black-box penetration test.

## **Exam format**

Computer-based with remote proctoring

- 40 multiple-choice questions
- Time allowed: 60 minutes
- Closed-book exam
- Pass mark: 60%

## Questions



### Question 1

You have found a live system on IP-address 192.168.11.54. Which Nmap command allows you to identify the target's operating system?

- A. nmap -oS 192.168.11.54
- B. nmap -sn 192.168.11.54
- C. nmap -O 192.168.11.54
- D. nmap -sL 192.168.11.54

### Question 2

Using Wireshark, you encounter the following text in a packet: "Authorization: Basic aHR0cHdhdGNoOmY=". What are you looking at?

- A. A form of authentication using a digest
- B. An HTTP protocol packet with basic authentication
- C. A TCP/IP packet to log in to an SSH server
- D. Authorization packet to log in to a WEP-encrypted Wi-Fi network

### Question 3

You find a live webserver. For what purpose would you use Dirb?

- A. To scan the webserver for folders and filenames that are not at glance obviously present on the webserver
- B. To test the website of application for known vulnerabilities
- C. To check for the presence of injection vulnerabilities on the login page
- D. To act as a MitM proxy and alter packets

### Question 4

What does the CONCAT function within SQL do?

- A. Concatenates two string values
- B. Splits the value of a string into two values
- C. Changes the table and merges two columns into one column
- D. Returns the values of two fields as one field

**Question 5**

If you click the login button on a webpage, what kind of request does the browser generally send to the server?

- A. An HTTP POST request
- B. An HTTP GET request
- C. An HTTP PUT request
- D. An HTTP OPTIONS request

## Answers



Question	Answer	Explanation
1	C	The correct Nmap option is -O. The other options change the output (-o), skip DNS resolution(-n) or list all hosts present (-L).
2	B	The correct answer is HTTP with basic authentication.
3	A	Scanning for folders and files on a webserver is the function of Dirb. For the others you should use other testing tools, such as Nikto.
4	A	Within SQL the CONCAT function concatenates two string values
5	A	With normal forms in HTML, the browser will send a HTTP POST request.



© 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.