# ETHICAL HACKING
# FOUNDATION

## Exam Syllabus

SECO
INSTITUTE

# Table of contents

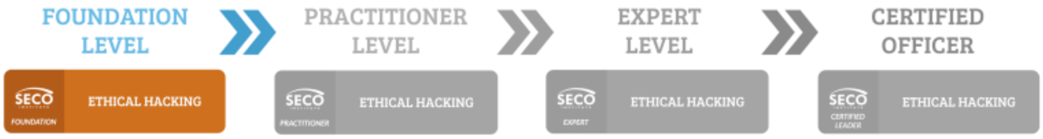
## Exam Syllabus: Ethical Hacking Foundation

Today's fast-developing technologies are changing the way we do business. Companies digitise all information by default, store their data in the cloud and use open source software. This practice raises serious information security concerns relating to network and system infrastructure. The Ethical Hacking Foundation course covers the basic steps of ethical hacking: intelligence gathering, scanning computer network/systems, and penetrating systems.

Candidates are expected to be very aware of the difference between legal and illegal hacking and the consequences of misuse.

## Context

The EHF (Ethical Hacking Foundation) certificate constitutes the first level of the SECO-Institute's Ethical Hacking certification track within the Cyber Security & Governance Certification Program. The successful completion of an Ethical Hacking Foundation course provides candidates with sufficient knowledge to be able to advance their careers by continuing with Ethical Hacking Practitioner.



## Course objectives

The candidate must demonstrate knowledge and understanding of the following topics:

- Network sniffing (gathering information from network traffic)
- Cracking a WEP and WPA(2) key from a wireless network
- Network vulnerability scanning
- Basic penetration of computer systems
- Password cracking
- Web-based hacking, containing SQL Injections (SQLi), Cross-Site Scripting (XSS), and remote File Inclusions (RFI)

## Target audience

Everyone who expects to be involved in implementing or monitoring information security.

And especially:

- security officers
- network architects
- network and system administrators
- security auditors
- security professionals
- computer programmers
- staff working in the field of ethical hacking
- ethical hackers (starting and experienced) who wish to get certified and verify their knowledge and understanding.

## Prerequisites

None. However, a working knowledge of Linux is highly recommended.

## Exam information

SECO-Institute provides the official Cyber Security & Governance courseware to accredited training centres where candidates are trained by accredited instructors. Candidates can take their exams at an accredited exam centre or directly with the SECO-Institute.

### Examination details

- Computer-based
- Multiple choice with 40 questions
- Time allotted: 60 minutes
- Pass mark: 60% (out of 100)
- Open book/notes: no
- Electronic equipment permitted: no

The Rules and Regulations for SECO-Institute examinations apply to this exam.

## Exam requirements

The following tables list the exam requirements and exam specifications.

| Ethical Hacking Foundation | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Requirements | 1. Introduction to Ethical Hacking<br>2. Network sniffing<br>3. Hacking wireless networks<br>4. System Penetration<br>5. Web-based Hacking | | | | | | | | | |
| **Required prior knowledge** | None | | | | | | | | | |
| **Learning-levels** | x | Know | x | Understand | | Apply | | Analyse, Synthesise | | Create |

# Exam specifications

| | Requirements, specifications, testing levels | | | Bloom level |
|---|---|---|---|---|
| **1.** | **Introduction to Ethical Hacking** | | | |
| | 1.1 | *The candidate can explain Hacking Ethics* | | |
| | | The candidate is able to: | | |
| | | 1.1.1 | *explain the legal implications of hacking* | 2 |
| | | 1.1.2 | *recall the different types of hackers* | 1 |
| | 1.2 | *The candidate can describe Basic Hacking Principles* | | |
| | | The candidate is able to: | | |
| | | 1.2.1 | *explain the difference between white and black box testing* | 2 |
| | | 1.2.2 | *describe the different phases in a hacking attempt* | 2 |

| | Requirements, specifications, testing levels | | | Bloom level |
|---|---|---|---|---|
| **2.** | **Network sniffing** | | | |
| | 2.1 | *The candidate can describe how to use hacking tools* | | |
| | | The candidate is able to: | | |
| | | 2.1.1 | *describe the differences between tools for Network sniffing* | 1 |
| | | 2.1.2 | *use the most common tools for network sniffing* | 3 |
| | 2.2 | *The candidate can extract information* | | |
| | | The candidate is able to: | | |
| | | 2.2.1 | *recall the function of HTTP headers* | 1 |
| | | 2.2.2 | *explain the meaning of information from HTTP headers* | 2 |

| | Requirements, specifications, testing levels | | | Bloom level |
|---|---|---|---|---|
| **3.** | **Hacking wireless networks** | | | |
| | 3.1 | *The candidate can prepare for…* | | |
| | | The candidate is able to: | | |
| | | 3.1.1 | *recall what information can be found about a network adaptor* | 1 |
| | 3.2 | *The candidate can explain the use of Aircrack-NG* | | |
| | | The candidate is able to: | | |
| | | 3.2.1 | *explain the purpose of Airodump-NG* | 2 |
| | | 3.2.2 | *reproduce the function of the different tools within Aircrack* | 1 |
| | | 3.2.3 | *recall the difference between ESSID en BSSID* | 1 |

| | Requirements, specifications, testing levels | | | Bloom level |
|---|---|---|---|---|
| **4.** | **System penetration** | | | |
| | 4.1 | *The candidate can perform Intel gathering* | | |
| | | The candidate is able to: | | |
| | | 4.1.1 | find information on a target online | 1 |
| | | 4.1.2 | find information on a target within a network | 1 |
| | 4.2 | *The candidate understands the workings of tools in Kali Linux and Metasploit* | | |
| | | The candidate is able to: | | |
| | | 4.2.1 | Explain how a target can be scanned | 2 |

| | | | | |
|---|---|---|---|---|
| | | 4.2.2 | Describe how tools can be combined | 2 |
| | 4.3 | *The candidate understands fingerprinting and vulnerabilities* | | |
| | | The candidate is able to: | | |
| | | 4.3.1 | Describe how vulnerabilities can be found based on scanning results | 2 |
| | | 4.3.2 | Explain how to perform manual fingerprinting | 2 |
| | 4.4 | *The candidate can describe the (post) Exploitation phase* | | |
| | | The candidate is able to: | | |
| | | 4.4.1 | Describe how to exploit a vulnerability with Metasploit | 2 |
| | | 4.4.2 | Describe how to extract system information after exploitation | 2 |

| | **Requirements, specifications, testing levels** | | | **Bloom level** |
|---|---|---|---|---|
| **5.** | **Web-based Hacking** | | | |
| | 5.1 | *The candidate can explain how Database attacks work* | | |
| | | The candidate is able to: | | |
| | | 5.1.1 | reproduce the steps to test for SQLi vulnerabilities | 1 |
| | | 5.1.2 | recall how to extract data with SQLi | 1 |
| | | 5.1.3 | explain how to use the functions: CONCAT, LOAD_FILE, UNION, SELECT, @@version, ORDER BY, LIMIT | 2 |
| | 5.2 | *The candidate can explain how Client-side attacks work* | | |
| | | The candidate is able to: | | |
| | | 5.2.1 | create use an XSS PoC (Proof of Concept) | 3 |
| | | 5.2.2 | Explain the basics of session hijacking i/c/w XSS | 2 |
| | | 5.2.3 | Explain how to bypass basic XSS filters | 2 |
| | 5.3 | *The candidate can explain how* Server-side attacks work | | |
| | | The candidate is able to: | | |
| | | 5.3.1 | explain how RFI is performed | 2 |
| | | 5.3.2 | explain basic functionalities of php shells such as r57 and c99 | 2 |
| | | 5.3.3 | explain the difference between Bind & Back connect shells and what they do | 2 |

## Literature

| | |
|---|---|
| **A** | Georgia Weidman - Penetration testing, A Hands-On Introduction to Hacking San Francisco, ISBN:978-1-59327-564-8 |
| **B** | Article EXIN Ethical Hacking Foundation. Free download at www.exin.com |
| **Optional** | |
| **C** | Stuart McClure, Joel Scambray, George Kurtz – Hacking Exposed 7: Network Security Secrets & Solutions, ISBN: 978-0071780285 |
| **D** | Prosecuting Computer Crimes Manual (2010) Chapter 1 |
| **E** | Documents and reports – Manuals/Guides |

## Exam-literature matrix

| Exam requirement | Exam specification | Literature (A, B, C) | Chapter reference(s) |
|---|---|---|---|
| **1** | 1.1 | B | Chapter 1, 2 |
| | 1.2 | B | Chapter 3 |
| **2** | 2.1 | A | Chapter 7 |
| | 2.2 | A | Chapter 7 |
| **3** | 3.1 | A | Chapter 15 |
| | 3.2 | A | Chapter 15 |
| **4** | 4.1 | A | Chapter 5, 7 |
| | 4.2 | A | Chapter 5 |
| | 4.3 | A | Chapter 6, 10 |
| | 4.4 | A | Chapter 4 |
| **5** | 5.1 | A | Chapter 14 |
| | 5.2 | A | Chapter 14 |
| | 5.3 | A | Chapter 14 |

## How to book your exam

All our exams are delivered through an online examination system called ProcterU. To enrol for an exam, go to: https://go.proctoru.com/
Make sure you are fully prepared. Use the ProctorU Preparation checklist to assess whether you are ready to take the exam.

If you are a new user, select Test Taker. Select "SECO-Institute" as the institution and fill in all the necessary information. See the instructions for more information. Once you have scheduled your exam, you will be asked to pay the exam fee. If you have an exam voucher, please fill in the access code.

Our online examination system allows you to book your exam and take it at any place convenient to you. Do you prefer your kitchen table, your home desk or your office? Would you rather take a test in the day or at night? It is all up to you!

## System requirements

To ensure the quality and security of the examination, you will have to meet specific requirements regarding your computer configuration, your exam environment and your behaviour during the exam. Click here to see the requirements.

The exam will be taken with special proctor software. To enable webcam and audio recording during the exam, you have to install software that monitors your activities.

Your exam will be recorded through your webcam and microphone. The recordings will be reviewed by multiple proctors after you have completed the exam. The proctors will check if you comply with all the requirements for the examination.

## Results

If no non-conformities are detected by the proctors, you will receive the final result by email one month after you complete the test. The email will also contain information on how to claim your certificate and digital badge as well as how to use your title.

# Digital badges

SECO-Institute and digital badge provider Acclaim have collaborated to provide certification holders with a digital badge of their SECO-Institute certification. Digital badges can be used in email signatures as well as on personal websites, social media sites such as LinkedIn and Twitter, and electronic copies of resumes. Digital badges help certification holders convey employers, potential employers and interested parties the skills they have acquired to earn and maintain a specialised certification.

**Claim your title at:** **https://www.seco-institute.org/claim-your-title**

EHF-EN-2018-01a

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.