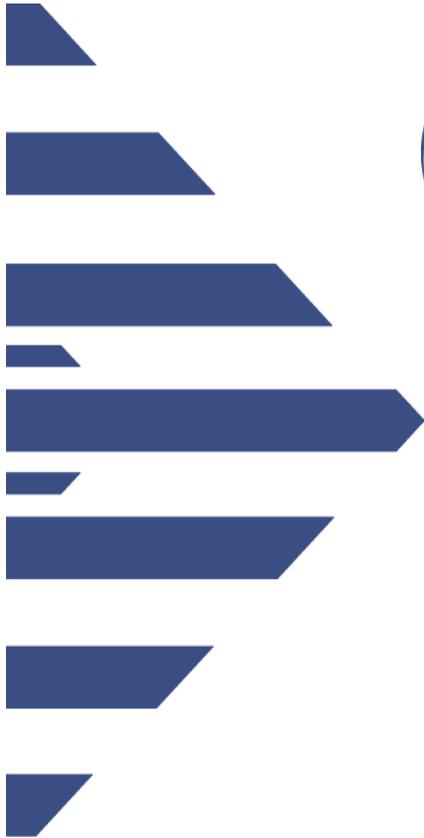


# Certified Ethical Hacker v7 Overview

## Table of Contents

Certified Ethical Hacker v7 .....	2
Notices .....	3
Overview .....	4
Course Objectives .....	5
Gap Area .....	6
About the Exam -1 .....	7
About the Exam -2 .....	9
Summary .....	10
Notices .....	11

## Certified Ethical Hacker v7



# Certified Ethical Hacker v7



Software Engineering Institute | Carnegie Mellon

© 2012 Carnegie Mellon University

\*\*001 Chris Evans: Well this is the certified ethical hacker version 7 review class. This is a fairly lengthy class.

## Notices

# Notices

---

© 2012 Carnegie Mellon University

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

This material was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The U.S. government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. government purposes, the SEI recommends attendance to ensure proper understanding.

THE MATERIAL IS PROVIDED ON AN "AS IS" BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

CERT® is a registered mark owned by Carnegie Mellon University.

\*\*002 There are nineteen blocks that we will be talking about over the course of this review class. The entire purpose of this is to kind of give you a background into basic network defense from an attacker perspective.

# Overview

---

Course Objectives

About the Exam

\*\*003 In this particular module we just have a little bit on the objectives of the class, the objectives of certified ethical hacker and a little bit of information on the exam itself so for those of you who are thinking about taking the exam and actually getting certified, kind of what's involved in that and what you'll need to do to pass that exam.

# Course Objectives

---

## Intent

- Provides a review of the 19 CEHv7 functional areas
- Supplement preparation for the CEHv7 certification exam

## Functional areas

Introduction to Ethical Hacking	Trojans & Backdoors	Session Hijacking	Evading IDS, Firewalls, & Honeypots
Footprinting & Reconnaissance	Viruses & Worms	Hacking Webservers	Buffer Overflows
Scanning Networks	Sniffers	Hacking Web Applications	Cryptography
Enumeration	Social Engineering	SQL Injection	Penetration Testing
System Hacking	Denial of Service	Hacking Wireless Networks	



\*\*004 The course itself, we will cover 19 blocks as we go through this, you can see them up here on the screen. We cover everything from what is a certified ethical hacker. We go into reconnaissance and enumeration, hacking into systems, what do you do once you get into the system, how do you pull information out, and then how do you maintain your access on those systems. So once you've broken into the system what do you do, how do you stay there, and how do you go about doing your job as a certified ethical hacker?

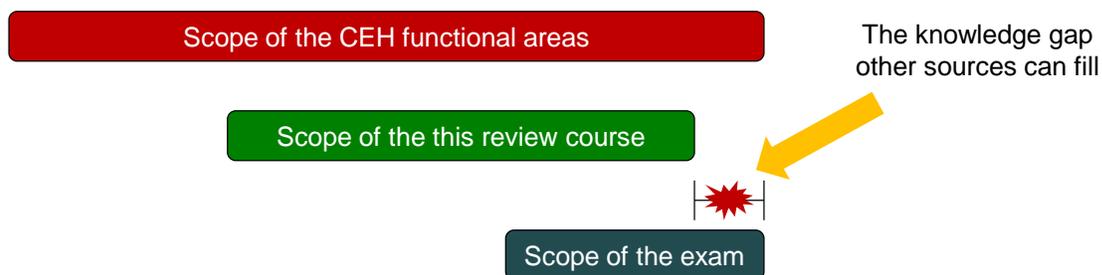
This actually is designed to be a supplement for your own preparation for the exam. I would caution you if you are

going to sit for the exam don't rely solely on any one source of information because you'll find that there is a certain gap in anything right over here.

## Gap Area

# Gap Area

You should consider and use other sources in preparation for the CEHv7 exam!



\*\*005 So if the red area up there is everything that could be covered on the CEH exam, the green bar there is what we'll actually talk about. What you'll see on the test may or may not be what we actually cover in the class. There might be a little portion of it that we don't talk about here but is still covered by CEH so you might see questions on that. My point being that as you're going through this, don't rely solely on this class. Pick up a CEH study guide. Take practice test questions. Look at

other sources of material as you prepare for this. You don't want to put all your eggs in one basket but this is going to give you a complete 100 percent review. We'll get close. We're probably somewhere between 80 and 90 percent of what you need for the exam, and certainly for those of you that aren't sitting for the exam, this will be a great way to understand what hacking is kind of all about at a very introductory level.

## About the Exam -1

# About the Exam -1

---

4 hours

150 questions, all multiple choice

Must score 70% correctly to pass

DoD-8570 compliant - CNDSP

- Computer Network Defense Service Provider (CNDSP)
- Analyst, infrastructure support, incident reporter, auditor



\*\*006 So if you are going to take the exam, it is a four-hour exam. You will not need all four hours on it. There are 150 questions, they're all multiple choice, four or five-answer questions. It's pick the best answer that you can on there, nothing

insanely difficult or nothing too obvious either so the questions are about right. They really make sure that you understand what the material is.

The CEH is designed for people who have two years of experience kind of doing not doing penetration tests, but having been exposed to that. So if you go right from this review class into the exam, you'll probably find the exam to be a little bit more difficult than if you had gone through this review class, gone home, done some self-study, actually applied some of the labs and some of the concepts that you see through this class, applied them and learned with them for six months or so. Then go take the exam you'll be a lot better prepared for that.

You've got to have a 70 percent on the exam to pass. Again that's not overly difficult to achieve, and for those of you who are concerned about DoD 8570 compliance this certification in this exam will actually meet that requirement for being either a CNDSP, a Computer Network Defense Service Provider in one of those roles. So if you're interested in DoD 8570, this certification will actually do it for you.

# About the Exam -2

## The CEHv7 exam guide

- Key areas of knowledge
  - It will NOT help you pass the exam
  - BUT – it can help you focus
- Exam information

[http://www.eccouncil.org/courses/exam\\_information/ceh\\_exam\\_312-50.aspx](http://www.eccouncil.org/courses/exam_information/ceh_exam_312-50.aspx)

Ethical Hacking and Countermeasures (312-50) Exam

CEH v7 Exam (312-50)

Credit towards Certification

- Certified Ethical Hacker 7

Exam Details

- Number of Questions: 150
- Passing Score: 70%
- Test Duration: 4 hours
- Test Format: Multiple choice
- Test Delivery:
  - Web based via Prometric Prime (Available from March 14th, 2011)
  - Authorized Prometric Testing Centers (Available from May 1st, 2011)
  - Vue Testing Center (Available from May 1st, 2011)

**IMPORTANT UPDATE as of May 1, 2011**

EC-Council has delayed the publishing of the CEH V7 exam on Prometric APTC and Pearson VUE channels. Any inconvenience is greatly regretted.

Exam Code

The exam code varies when taken at different testing centers.

- Exam 312-50v7: Web based 'Prometric Prime' at Accredited Training Centers (ATC).
- Exam EC0-350: Proctored test at Authorized Prometric Testing Centers (APTC) globally.
- Exam 312-50v7: VUE Testing centers

Skills Measured

The exam 312-50 tests CEH candidates on the following 19 domains.

1. Introduction to Ethical Hacking
2. Footprinting and Reconnaissance
3. Scanning Networks
4. Enumeration
5. System Hacking
6. Trojans and Backdoors



\*\*007 There is an exam guide available for you to download. You can go to this address right here and it gives you a 19-page PDF document of all the objectives and all the topics and things that could be on the exam. I will be honest with you. This will not help you pass the exam. All it does is tell you what will be on the exam, so from the standpoint of helping you focus on what to study and what to review, this is a good resource. But otherwise it's pretty general so it will tell you things like you have to know footprinting and reconnaissance and it will tell you a little bit about that, kind of the topics that you need to know in there, But as a study guide in and of itself it's not going to help you any. And it also has the information

on the exam kind of what we talked about with regard to the questions and pass rates and that sort of thing. So if you're going to sit for the exam I highly recommend you get a copy of this and take a look at it before you go.

## Summary

# Summary

---

Course Objectives

About the Exam



\*\*008 And so that is kind of the CEH background as far as certification goes. Any questions on that? Ok.

## Notices

# Notices

---

Copyright 2013 Carnegie Mellon University

This material has been approved for public release and unlimited distribution except as restricted below.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study. Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The U.S. Government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

NO WARRANTY. THE MATERIAL IS PROVIDED ON AN "AS IS" BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

CERT® is a registered mark of Carnegie Mellon University.