Ethical Hacking and Countermeasures

Version 9

This page is intentionally left blank.

Instructions for Downloading your CEHv9 Electronic Courseware, Lab Manuals, and Tools.

Step 1:

Visit: https://aspen.eccouncil.org. If you have an account already, skip to Step 4.

Step 2:

Click **Register** and fill out the registration form. Click **Register** button.

Step 3:

Using the email you provided in step 2, follow the instructions in the auto-generated email to activate your EC-Council Aspen Portal account.

Step 4:

Login using your Username and Password.

Step 5:

Once successfully logged in, click **Academia** icon under the **Learning Resources** section. It will open Academia page.

Step 6:

Enter the access code below in the **Access Code** field and click **Submit** button.

Access Code: XXXXXXXXXXXXXXX

Step 7:

If your Access Code is valid, scroll down and you will be able to view instructions on how to access the Electronic Courseware, Lab Manuals, and Tools.

Support:

E-mail support is available from academia@eccouncil.org.

System Requirements:

The Academia page contains details about system requirements and how to download the e-courseware.

Instructions to Download Digital Copy of your Class Certificate of Attendance


EC-Council

Certificate of Attendance

THIS IS TO ACKNOWLEDGE THAT

HAS SUCCESSFULLY COMPLETED A COURSE ON

AT AN EC-COUNCIL ACCREDITED TRAINING CENTER

INSTRUCTOR NAME

CERTIFICATE NUMBER

DATE

Sanjay Bavisi, President

You can verify authenticity of this certificate by visiting https://aspen.eccouncil.org/VerifyEval.aspx

Step 1: Complete the official training.

Step 2: Visit: https://aspen.eccouncil.org. If you have an account already, skip to Step 5.

Step 3: Click **Register** and fill out the registration form. Click **Register** button.

Step 4: Using the email you provided in step 3, follow the instructions in the auto-generated email to activate your EC-Council Aspen Portal account.

Step 5: Login using your Username and Password.

Step 6: Click **Class Eval** icon in the **Student Services** section.

Step 7: Enter the **Evaluation Code** (see the attached code below) in the **Evaluation Code** field and click **Submit**.

Step 8: Fill the **Course Evaluation Form**. **Note:** All fields on this form are mandatory. Click **Submit Classroom Evaluation** button.

Step 9: In **Course Evaluation Submission** page, click the **Download Certificate of Attendance** button to download your certificate of attendance.

Evaluation Code: ***CEH-*********

EC-Council

Foreword

Since you are reading this CEHv9 courseware, you most likely realize the importance of information systems security. However, we would like to put forth our motive behind compiling a resource such as this one and what you can gain from this course.

You might find yourself asking what sets this course apart from the others out there. The truth is that no single courseware can address all the issues of information security in a detailed manner. Moreover, the rate at which exploits, tools, and methods are being discovered by the security community makes it difficult for one program to cover all the necessary facets of information security. This doesn't mean that this course is inadequate in any way as we have worked to cover all major domains in such a manner that the reader will be able to appreciate the way security has evolved over time as well as gain insight in to the fundamental workings relevant to each domain. It is a blend of academic and practical wisdom supplemented with tools that the reader can readily access in order to obtain a hands-on experience.

The emphasis throughout the courseware is on gaining practical know-how, which explains the stress on free and accessible tools. You will read about some of the most widespread attacks seen, the popular tools used by attackers, and how attacks have been carried out using ordinary resources.

You may also want to know what to expect once you have completed the course. This courseware is a resource material. Any penetration tester can tell you that there is no one straight methodology or sequence of steps that you can follow while auditing a client site. There is no one template that will meet all your needs. Your testing strategy will vary with the client, the basic information about the system or situation, and the resources at your disposal. However, for each stage you choose – be it enumeration, firewall, penetration of other domains - you will find something in this courseware that you can definitely use.

Finally this is not the end! This courseware is to be considered a constant work-in-progress because we will be adding value to this courseware over time. You may find some aspects extremely detailed, while others may have less detail. We are constantly asking ourselves if the content helps explain the core point of the lesson, and we constant calibrate our material with that in mind. We would love to hear your viewpoints and suggestions so please send us your feedback to help in our quest to constantly improve our courseware.

Table of Contents

This page is intentionally left blank.

Ethical Hacking and Countermeasures v9

Module 00: Welcome to Certified Ethical Hacker Class!

Exam 312-50

Introduction

- Name
- Company Affiliation
- Title / Function
- Job Responsibility
- System security related experience
- Expectations

Course Materials

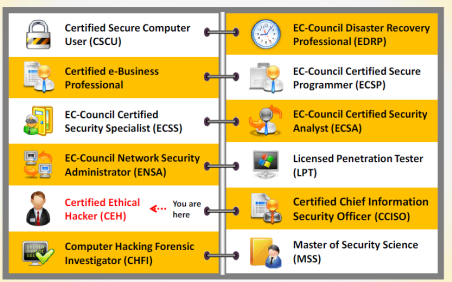
- Identity Card
- Student Courseware
- Lab Manual/ Workbook
- Course Evaluation
- Reference Materials

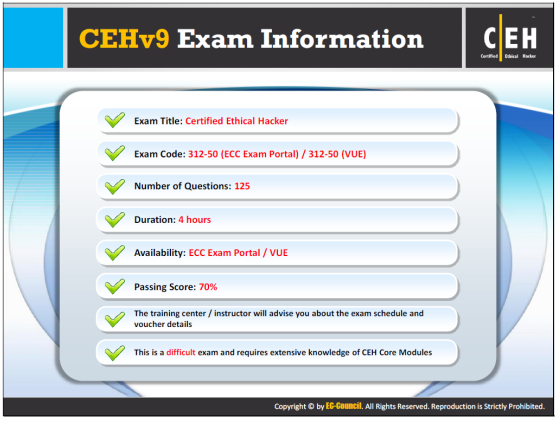
CEHv9 Course Outline

01	Introduction to Ethical Hacking	07	Sniffing	13	SQL Injection
02	Footprinting and Reconnaissance	08	Social Engineering	14	Hacking Wireless Networks
03	Scanning Networks	09	Denial-of-Service	15	Hacking Mobile Platforms
04	Enumeration	10	Session Hijacking	16	Evading IDS, Firewalls, and Honeypots
05	System Hacking	11	Hacking Webservers	17	Cloud Computing
06	Malware Threats	12	Hacking Web Applications	18	Cryptography

EC-Council Certification Program

There are several levels of certification tracks under the EC-Council Accreditation body:



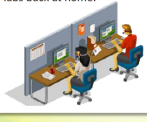


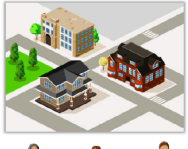
Student Facilities

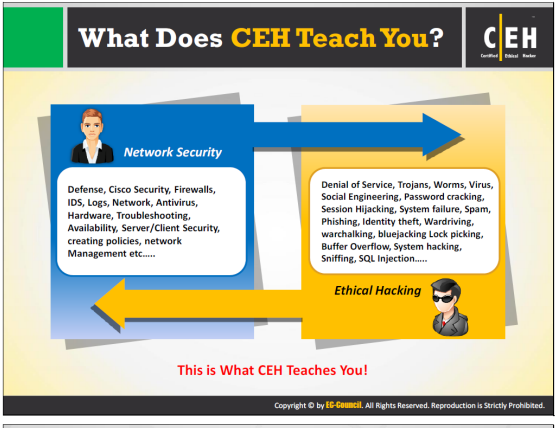
Class Hours		Building Hours		Phones	
	Parking		Messages		Restrooms
Smoking		Meals		Recycling	

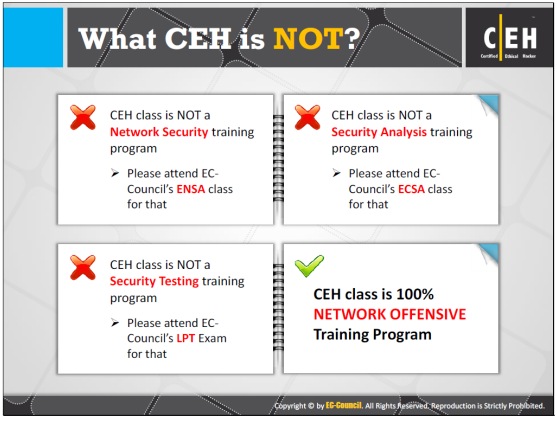
Lab Sessions

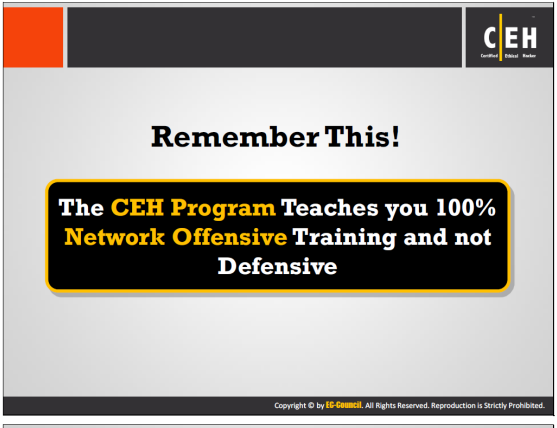
- Lab Sessions are designed to **reinforce** the classroom sessions
- The sessions are intended to give a **hands on experience** only and does not guarantee proficiency
- There are tons of labs in the lab manual. Please practice these labs back at home.

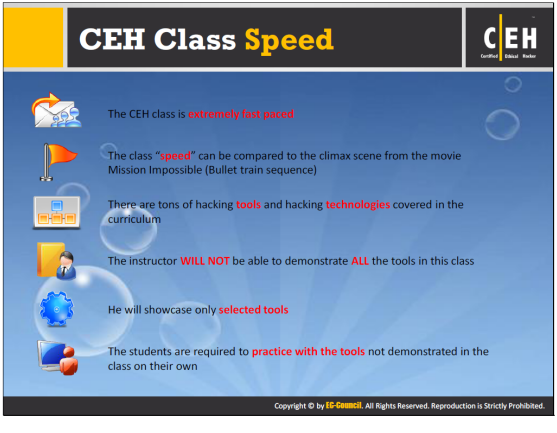












Live Hacking Website

- Please target your exercises for "Live Hacking" to www.certifiedhacker.com
- This website is meant for the students to try the tools on live target
- Please refrain from using the exploits on any other domains on the Internet

CEH Classroom Attack Lab Website

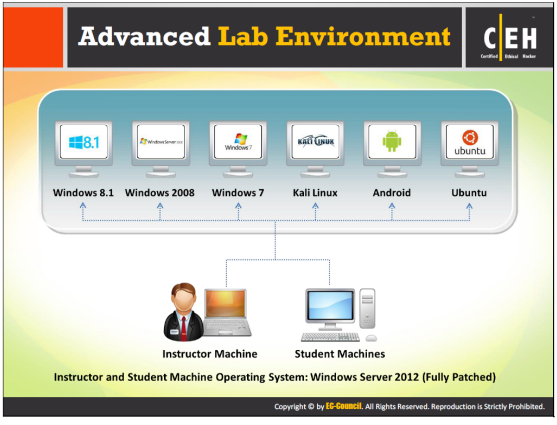
NDA Document

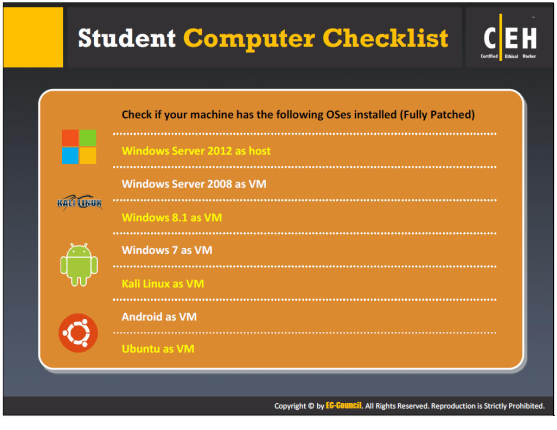
Please read the contents of the provided EC-Council's CEH NDA document

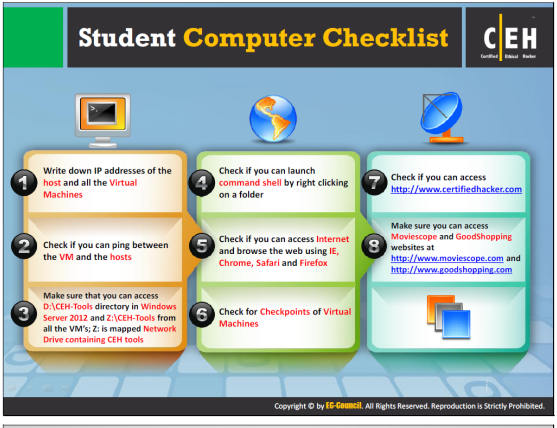
Sign this document and hand it over to the instructor

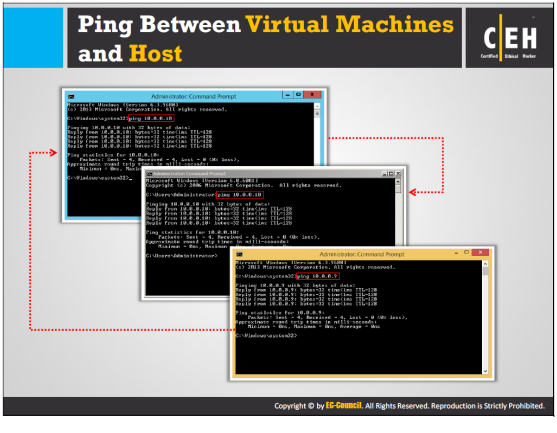
We will NOT start the class unless you sign this document

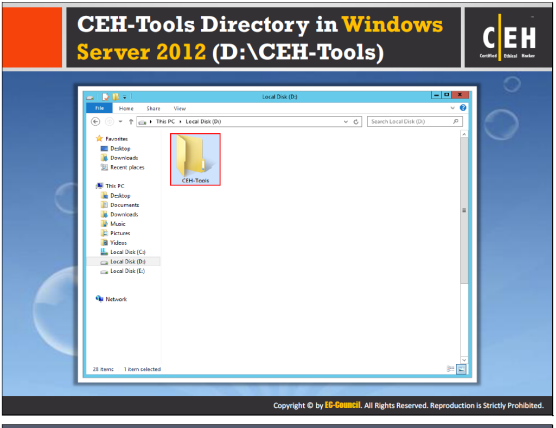
Please approach the instructor if you are not presented with this document

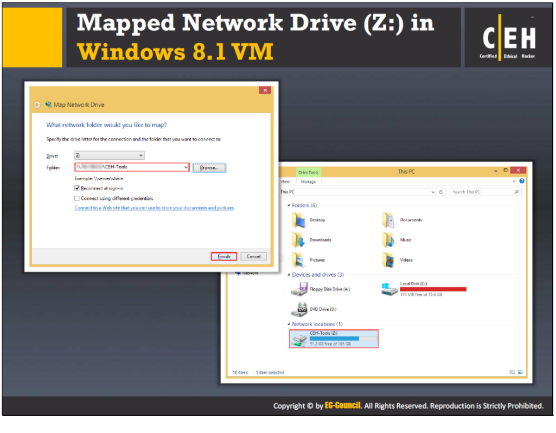




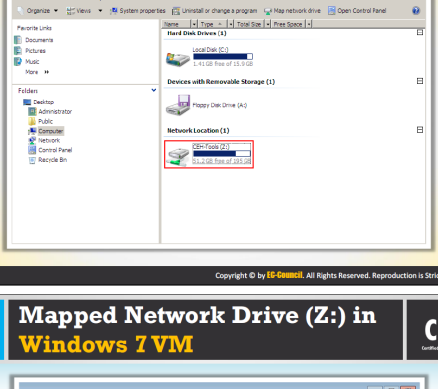




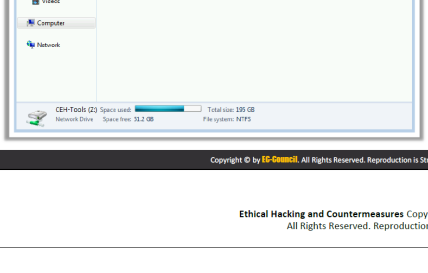


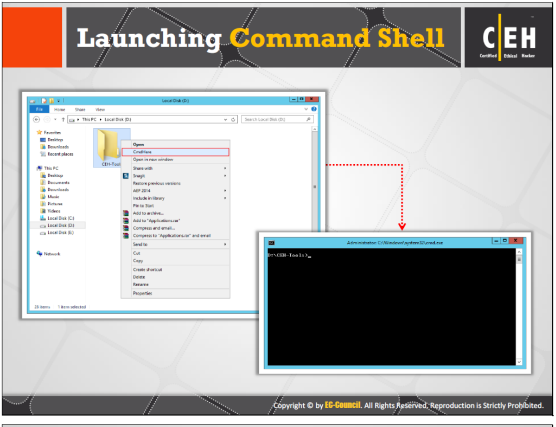


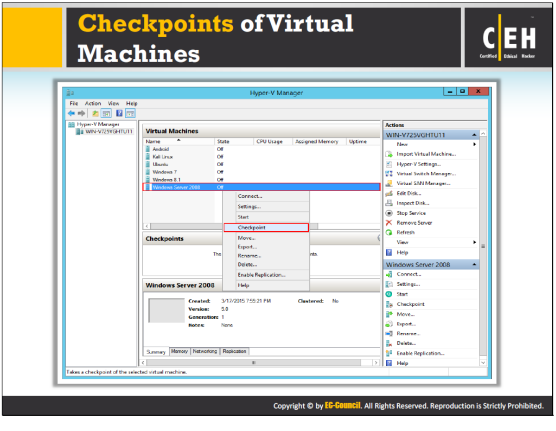
Mapped Network Drive (Z:) in Windows Server 2008 VM



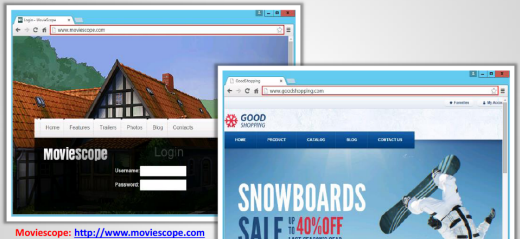
Mapped Network Drive (Z:) in Windows 7 VM







Moviescope and GoodShopping Websites

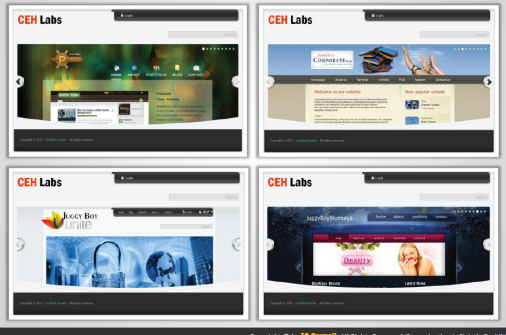


Moviescope: http://www.moviescope.com

GoodShopping: http://www.goodshopping.com

Live Hack Website

http://www.certifiedhacker.com



This page is intentionally left blank.