



TAKEDOWNCON
www.takedowncon.com

TAKEDOWNCON is a hacking conference that was conceived by our members!
EC-Council has been flooded with requests to take our world-class courses on the road!
We have answered the call and created TakeDownCon!
This conference will be focused on the learner and will feature
several Certification & Certificate Training courses for Advanced Practitioners!

TAKEDOWNCON will host EC-Council's sought after Hacking, Forensics and Pen Test courses,
Certified Wireless Security Professional, and several highly technical and advanced workshops
which will cover current and important security topics such as advanced penetration testing,
cryptography, network defense, application security and mobile forensics.

At **TAKEDOWNCON** the learning doesn't stop when the training ends!
We have lined up a list of sought after industry practitioners and
subject matter experts that will present relevant and implementable topics!

*For more information, about **TAKEDOWNCON** please visit www.takedowncon.com*



Hacker | Halted
www.hackerhalted.com

Since 2004 EC-Council has hosted 20 Hacker Halted events across four continents and
in cities such as Myrtle Beach, Miami, Dubai, Singapore, Hong Kong, Mexico City,
Tokyo, Kuala Lumpur, Guangzhou, Taipei and Cairo.

Hacker Halted North America will be held in Miami for the 3rd year in a row and
based on past history is sure to boast an amazing turnout of Information Security Professionals!

Hacker Halted is more than just a conference event; practitioners travel from all over the world
to attend our world-class training, gain practical knowledge from our expert presenters and
get a preview of the latest technologies and Information Security tools
which will be showcased by our exhibitors and partners.

*For more information, about **Hacker Halted** please visit www.hackerhalted.com*

VAMPIRESCAN

www.vampiretech.com



Is your website vulnerably to an attack? Could hackers exploit a small weakness in your website and obtain access to sensitive company information?

VampireScan allows users to test their own Cloud and Web applications against advanced attacks and receive actionable results all within their own Web portal. Our easy to use online portal will simply ask you for the URL of your web application, from there, our Services do the rest.

For a limited time, VampireTech is offering its Baseline Scan free of charge to qualified customers. This entitles you to one Free Health Check for one domain utilizing our Baseline Scan. This Scan will test for Cross-site Scripting Vulnerabilities, Non-SSL Passwords, and Password Autocomplete.

Go to <http://www.vampiretech.com/freehealthcheck.aspx> to get a Free Health Check.

For More Information About VAMPIRESCAN Please Visit: www.vampiretech.com



Global CISO Executive Summit

Be on the forefront of a new global initiative where today's world-class leaders in information security will gather to navigate through international waters. Join these leaders as they follow the wind of change that is sweeping through the IS community motivating today's information guardians to develop a new way of thinking to ensure success in protecting their respective organizations.

The goal of EC-Council's Global CISO Forum is to create an open platform for top information security executives to discuss their successes, failures, obstacles, and challenges. The open conversation will lead to the creation of actionable items that can be discussed and applied to the organization.

For More Information About CISO Executive Summit Please Visit: www.eccouncil.org/resources/ciso-executive-summit.aspx

How to Download My CEHv8 E-Courseware and Additional Lab Manuals?

Please follow the steps below to download your CEHv8 e-courseware and additional lab manual.

Step 1:

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

Step 2:

Click Register and fill out the registration form.

Step 3:

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

Step 4:

Login using your Username and Password.

Step 5:

Once successfully logged in, expand the **About Academia** navigation menu and select **Access Code**.

Step 6:

Enter the access code provided to you to redeem access to the CEH V8 e-Courseware and Lab Manuals.

Access Code: XXXXXXXXXXXXXXXX

Step 8:

Once redeemed, expand the **Courses** menu and select **iLearn – PDF Courseware** – The resulting page will list your CEH v8 e-Courseware and Lab Manuals.

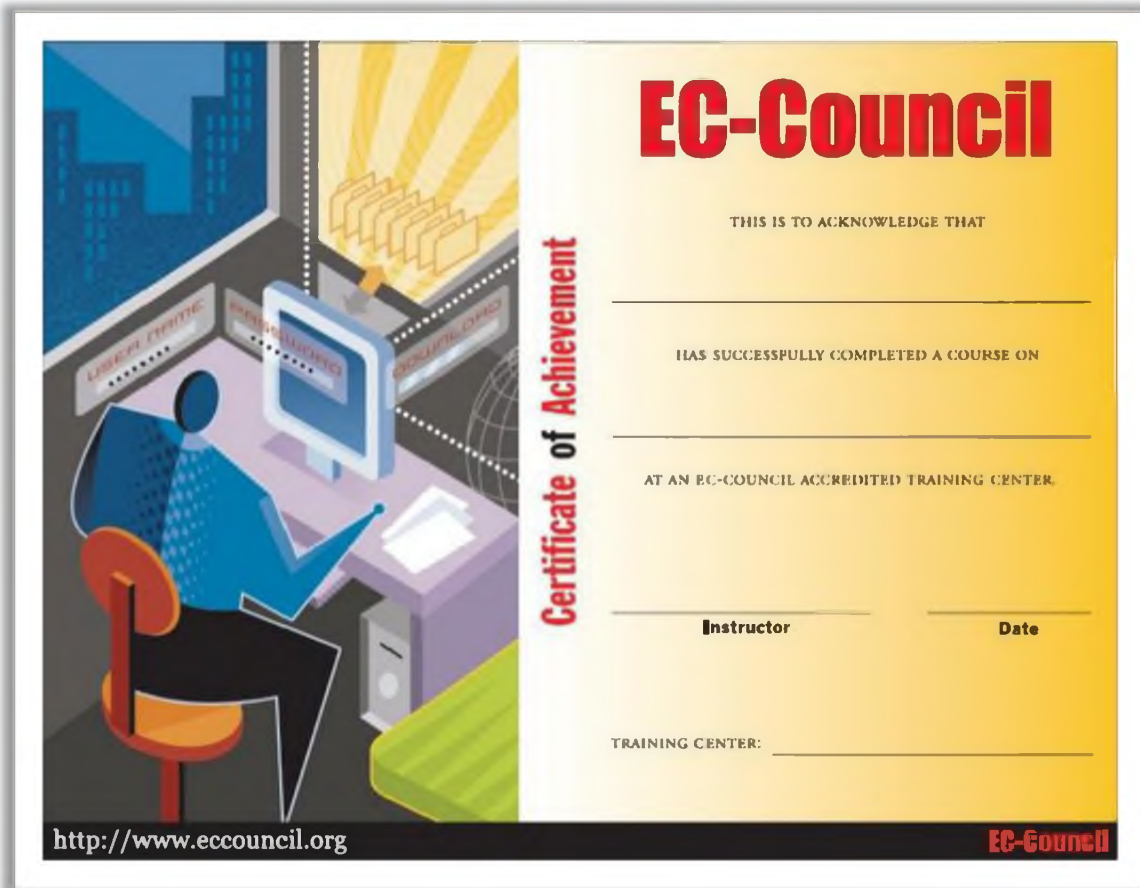
Support:

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

System Requirements:

Visit <https://academia.eccouncil.org/AboutAcademia/WhatisiLearn.aspx> to view the system requirements.

Download Class Certificate of Attendance



Please follow the below stated steps to download digital copy (PDF format) of your class certificate of attendance.

Step 1: Wait until the class is over (the last of the class).

Step 2: Visit <http://www.eccouncil.org/eval>.

Step 3: Complete the course evaluation form (please complete all the fields in the form – correct e-mail address is required).

Step 4: Evaluation code is required to submit the form. See the attached code.

Step 5: Submit the form.

Step 6: A web link will be sent to you to download your PDF copy of the certificate.

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

Ethical Hacking and Countermeasures

Version 8

EC-Council

Copyright © 2013 by EC-Council. All rights reserved. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

Information has been obtained by EC-Council from sources believed to be reliable. EC-Council uses reasonable endeavors to ensure that the content is current and accurate, however, because of the possibility of human or mechanical error we do not guarantee the accuracy, adequacy, or completeness of any information and are not responsible for any errors or omissions or the accuracy of the results obtained from use of such information.

The courseware is a result of extensive research and contributions from subject matter experts from the field from all over the world. Due credits for all such contributions and references are given in the courseware in the research endnotes. We are committed towards protecting intellectual property. If you are a copyright owner (an exclusive licensee or their agent), and if you believe that any part of the courseware constitutes an infringement of copyright, or a breach of an agreed licence or contract, you may notify us at **legal@eccouncil.org**. In the event of a justified complaint, EC-Council will remove the material in question and make necessary rectifications.

The courseware may contain references to other information resources and security solutions, but such references should not be considered as an endorsement of or recommendation by EC-Council.

Readers are encouraged to report errors, omissions and inaccuracies to EC-Council at **legal@eccouncil.org**.

If you have any issues, please contact **support@eccouncil.org**.

Foreword

Since you are reading this CEHv8 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.

This page is intentionally left blank.

Table of Contents

Module Number	Module Name	Page No.
00	Student Introduction	I
01	Introduction to Ethical Hacking	01
02	Footprinting and Reconnaissance	91
03	Scanning Networks	262
04	Enumeration	434
05	System Hacking	517
06	Trojans and Backdoors	827
07	Viruses and Worms	1006
08	Sniffing	1112
09	Social Engineering	1292
10	Denial of Service	1402
11	Session Hijacking	1503
12	Hacking Webservers	1600
13	Hacking Web Applications	1723
14	SQL Injection	1986
15	Hacking Wireless Networks	2134
16	Hacking Mobile Platforms	2392
17	Evading IDS, Firewalls, and Honeypots	2549
18	Buffer Overflow	2691
19	Cryptography	2782
20	Penetration Testing	2872
	References	2976

This page is intentionally left blank.



Ethical Hacking and Countermeasures

Module 00: Welcome to Certified Ethical Hacker Class

Exam 312-50

Introduction




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



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Course Materials



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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

CEHv8 Course Outline

1 Introduction to Ethical Hacking

2 Footprinting and Reconnaissance

3 Scanning Networks

4 Enumeration

5 System Hacking

Trojans and Backdoors

Viruses and Worms

Sniffing

Social Engineering

Denial-of-Service

6

7

8

9

10

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

CEHv8 Course Outline

11 Session Hijacking

12 Hacking Webservers

13 Hacking Web Applications

14 SQL Injection

15 Hacking Wireless Networks

Hacking Mobile Platforms

Evading IDS, Firewalls and Honeypots

Buffer Overflows

Cryptography

Penetration Testing

16

17

18

19

20

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council Certification Program

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

Certified Secure Computer User (CSCU)	→	EC-Council Disaster Recovery Professional (EDRP)
Certified e-Business Professional	→	EC-Council Certified Security Analyst (ECSA)
EC-Council Certified Security Specialist (ECSS)	→	EC-Council Certified Secure Programmer (ECSP)
EC-Council Network Security Administrator (ENSA)	→	Certified Secure Application Developer (CSAD)
Certified Ethical Hacker (CEH)	←	Licensed Penetration Tester (LPT)
Computer Hacking Forensic Investigator (CHFI)	→	Master of Security Science (MSS)

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Ethical Hacker Track

CEH Certification Track

Complete the following steps:

Attend the Ethical Hacking and Countermeasures Course


Pass the CEH Exam
Exam Code: **312-50-ANSI (IBT)**,
312-50v8 (VUE), or **350CEHv8 (APTC)**

```

graph TD
    Start([Start]) --> Attend[Attend Training]
    Attend --> Prepare[Prepare for 312-50 Exam]
    Prepare --> Take{Take Exam}
    Take -- Pass --> Achieved[Certification Achieved]
    Take -- Fail --> Start
    
```

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

CEHv8 Exam Information



- ✓ Exam Title: **Certified Ethical Hacker v8 (ANSI)**
- ✓ Exam Code: **312-50-ANSI (IBT), 312-50v8 (VUE), or 350CEHv8 (APTC)**
- ✓ Number of Questions: **125**
- ✓ Duration: **4 hours**
- ✓ Availability: **Prometric Prime/ Prometric APTC/ VUE**
- ✓ Passing Score: **70%**
- ✓ The instructor will tell you about the exam schedule/exam voucher details for your training
- ✓ This is a **difficult** exam and requires extensive knowledge of CEH Core Modules

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.


Student Facilities






Class Hours		Building Hours		Phones	
	Parking		Messages		Restrooms
Smoking		Meals		Recycling	

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Sessions

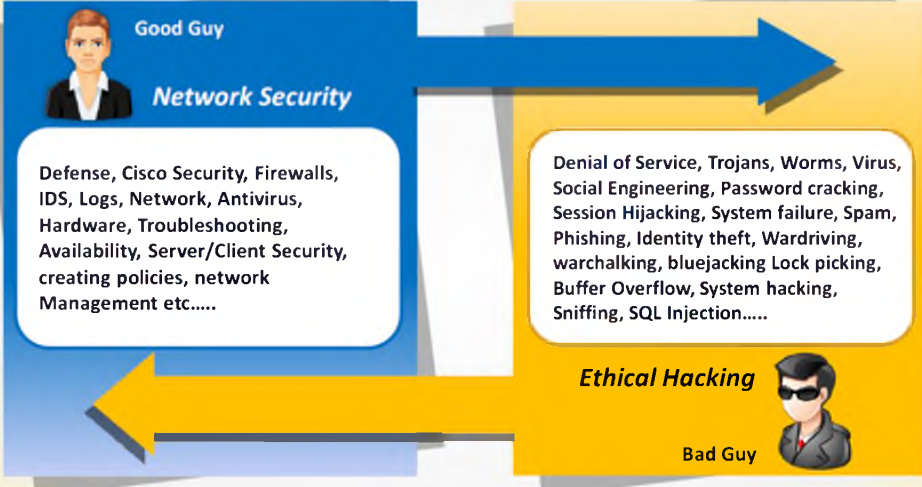



- Lab Sessions are designed to **reinforce** the classroom sessions
- The sessions are intended to give a **hands on experience** only and does not guarantee proficiency
- There are tons of labs in the lab manual. Please practice these labs back at home.



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

What Does **CEH** Teach You?



Good Guy
Network Security

Defense, Cisco Security, Firewalls, IDS, Logs, Network, Antivirus, Hardware, Troubleshooting, Availability, Server/Client Security, creating policies, network Management etc.....


Bad Guy
Ethical Hacking





Denial of Service, Trojans, Worms, Virus, Social Engineering, Password cracking, Session Hijacking, System failure, Spam, Phishing, Identity theft, Wardriving, warchalking, bluejacking Lock picking, Buffer Overflow, System hacking, Sniffing, SQL Injection.....

This is What CEH Teaches You!


Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

What CEH is **NOT**?



 <p>CEH class is NOT a Network Security training program</p> <ul style="list-style-type: none">➤ Please attend EC-Council's ENSA class for that	 <p>CEH class is NOT a Security Analysis training program</p> <ul style="list-style-type: none">➤ Please attend EC-Council's ECSA class for that
 <p>CEH class is NOT a Security Testing training program</p> <ul style="list-style-type: none">➤ Please attend EC-Council's LPT class for that	 <p>CEH class is 100% NETWORK OFFENSIVE Training Program</p>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.





Remember This!


The CEH Program Teaches you 100% Network Offensive Training and not Defensive


Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.


CEH Class Speed





 The CEH class is **extremely fast paced**

 The class “**speed**” can be compared to the climax scene from the movie Mission Impossible (Bullet train sequence)

 There are tons of hacking **tools** and hacking **technologies** covered in the curriculum

 The instructor **WILL NOT** be able to demonstrate **ALL** the tools in this class

 He will showcase only **selected tools**

 The students are required to **practice with the tools** not demonstrated in the class on their own

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

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



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Advanced Lab Environment



Windows 8

Windows Server 2008 (64 Bit)

Windows 7

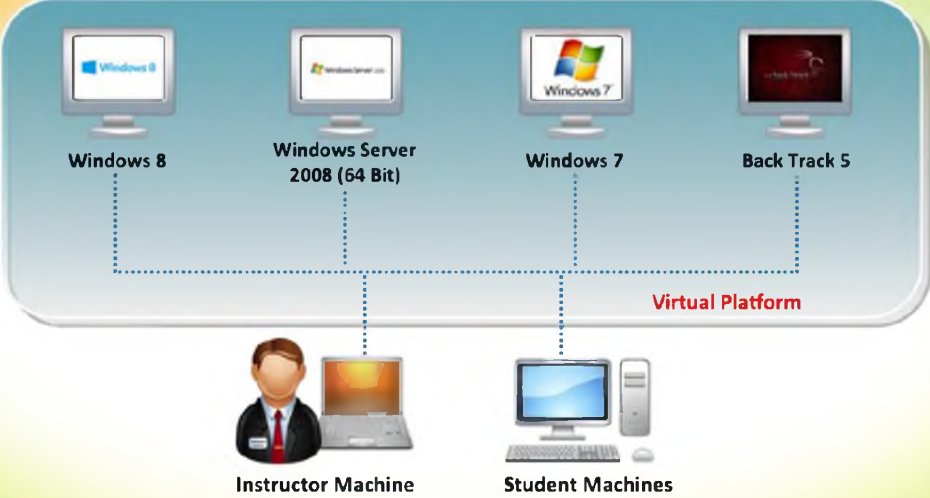
Back Track 5

Virtual Platform

Instructor Machine


Student Machines

Instructor and Student Machine Operating System: Windows Server 2012 (Fully Patched)








Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Student Computer Checklist







Check if your machine has the following Oses installed (Fully Patched)

-  Windows Server 2012 as host
-  Windows Server 2008 as VM
-  Windows 8 as VM
-  Windows 7 as VM
-  BackTrack 5 R3 as VM

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

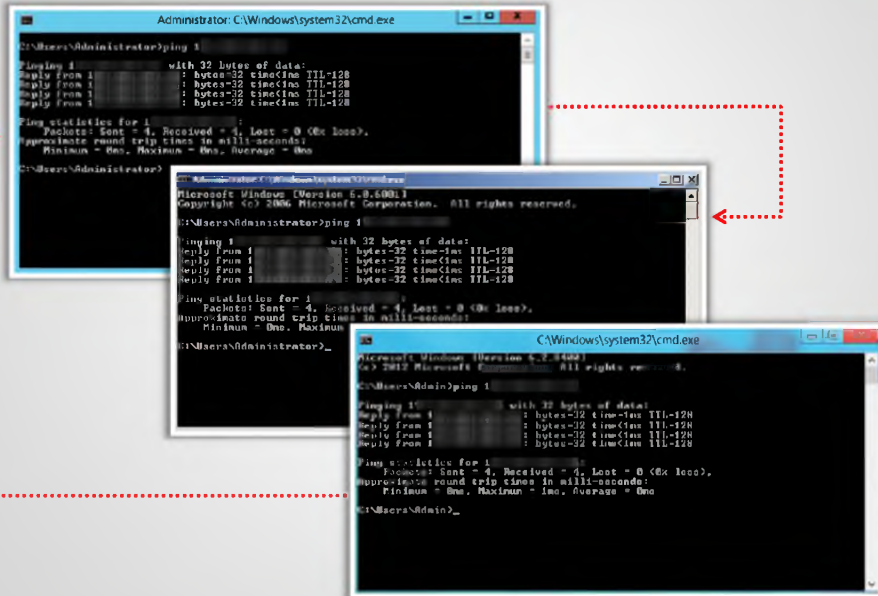
Student Computer Checklist



-  Write down IP addresses of the host and all the Virtual Machines
- Check if you can ping between the VM and the hosts
- Make sure that you can access D:\CEH-Tools directory in Windows Server 2012 and Z:\CEH-Tools from all the VM's; Z: is mapped Network Drive containing CEH tools
-  Check if you can launch command shell by right clicking on a folder
- Check if you can access Internet and browse the web using IE, Chrome, Safari and Firefox
- Check for snapshots of Virtual Machines
-  For Wireless Hacking module you will need AirPcap adapter
- Make sure you can access RealHome and Powergym websites at <http://localhost/realhome> and <http://localhost/powergym>
- Check if you can access <http://www.certifiedhacker.com>

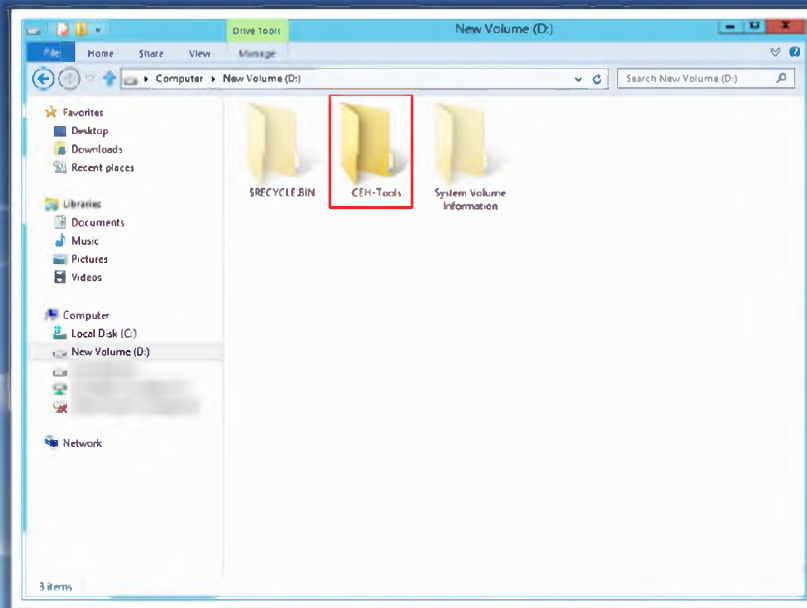
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ping Between Virtual Machines and Host



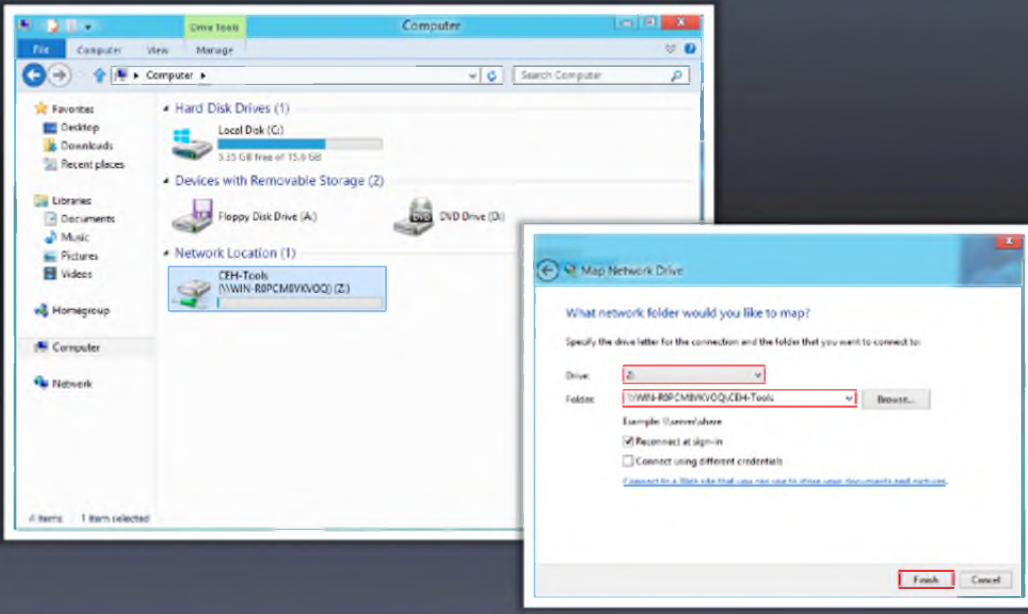
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

CEH-Tools Directory in Windows Server 2012 (D:\CEH-Tools)



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

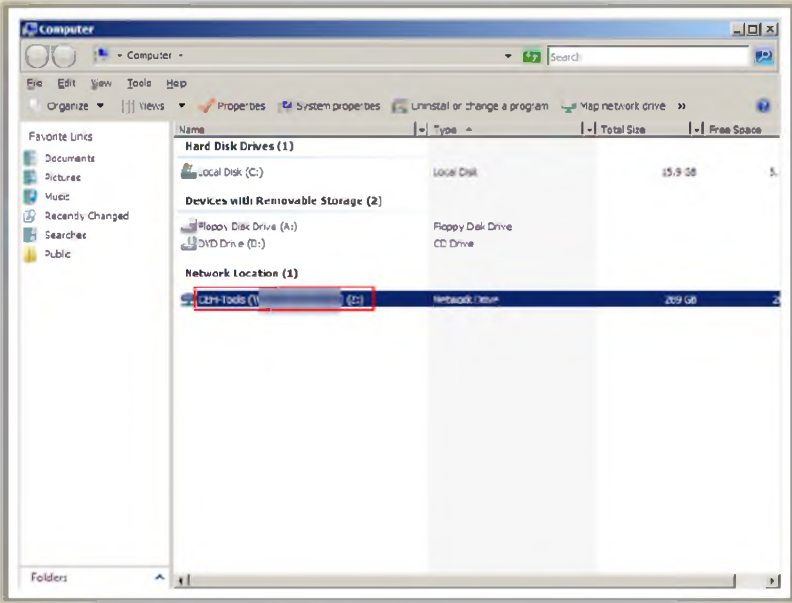
Mapped Network Drive (Z:) in Windows 8 VM



The screenshot shows a Windows 8 VM desktop. The 'Computer' window is open, displaying the 'Computer' ribbon tab. Under the 'Network Location (1)' section, a network drive is listed as 'CEH-Tools (\\WIN-RBPCMBVQOQ) (Z:)'. A 'Map Network Drive' dialog box is overlaid on the right, with the 'Drive' dropdown set to 'Z:' and the 'Folder' dropdown set to '\\WIN-RBPCMBVQOQ\CEH-Tools'. The 'Reconnect at sign-in' checkbox is checked. The 'Finish' button is highlighted.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

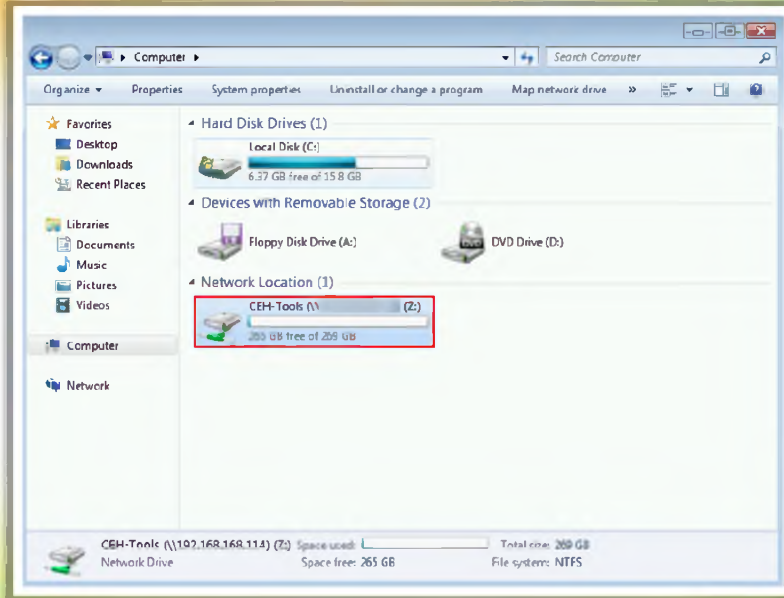


The screenshot shows a Windows Server 2008 VM desktop. The 'Computer' window is open, displaying the 'Computer' ribbon tab. The 'Network Location (1)' section is expanded, showing a table of network locations. The entry for 'CEH-Tools (\\) (Z:)' is highlighted with a red box.

Name	Type	Total Size	Free Space
Hard Disk Drives (1)			
Local Disk (C:)	Local Disk	15.9 GB	5.1 GB
Devices with Removable Storage (2)			
Floppy Disk Drive (A:)	Floppy Disk Drive		
DVD Drive (D:)	CD Drive		
Network Location (1)			
CEH-Tools (\\) (Z:)	Network (Net)	209 GB	209 GB

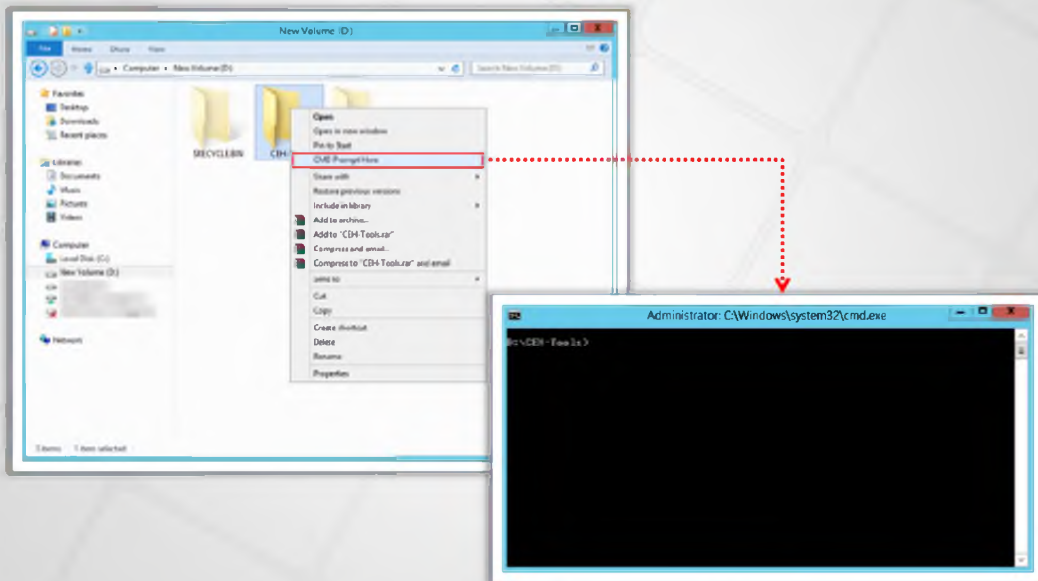
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mapped Network Drive (Z:) in Windows 7 VM



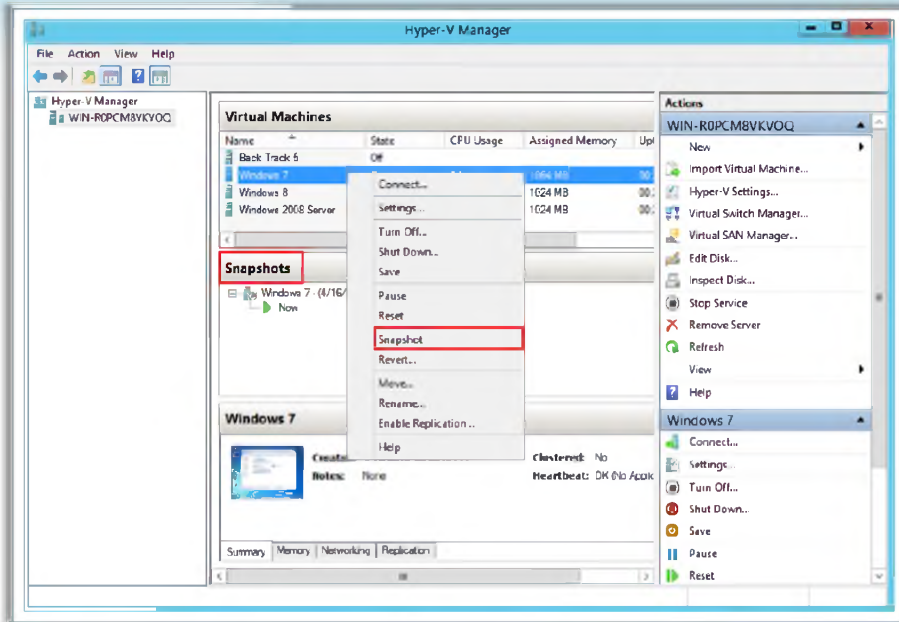
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Launching Command Shell



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Snapshots of Virtual Machines



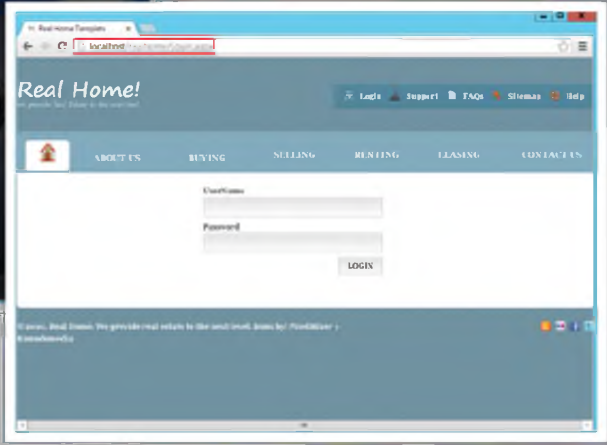
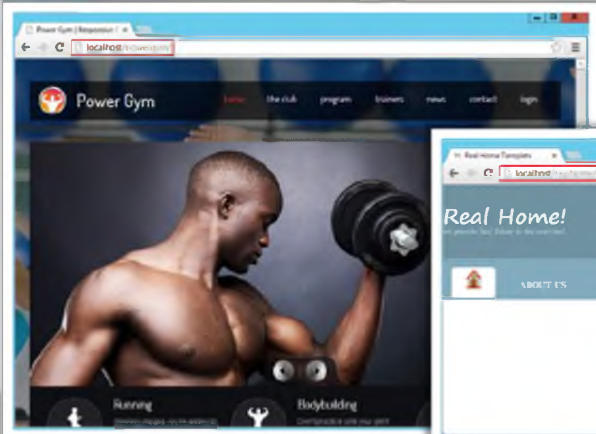

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

AirPcap



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Powergym and RealHome Websites



Powergym: <http://localhost/powergym>

RealHome: <http://localhost/realhome>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Live Hack Website

<http://www.certifiedhacker.com>



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The slide features a dark header bar at the top. On the left side of the header is a yellow square. On the right side is the CEH logo, which consists of the letters 'C' and 'E' in white, with a vertical yellow line between them, and 'H' in white to the right. Below the letters, the text 'Certified Ethical Hacker' is written in a smaller font. The main body of the slide is a light gray gradient. In the center, there is a black rounded rectangle with a yellow border. Inside this rectangle, the text 'Let's Start Hacking!' is written in a bold, white, sans-serif font. At the bottom of the slide, there is a dark gray footer bar containing the text 'Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.'