

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: XXXXXXXXXXXXXXXX

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



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

Copyright © 2015 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 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 into 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 constantly 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

Module Number	Module Name	Page No.
00	Student Introduction	I
01	Introduction to Ethical Hacking	01
02	Footprinting and Reconnaissance	151
03	Scanning Networks	301
04	Enumeration	441
05	System Hacking	509
06	Malware Threats	756
07	Sniffing	995
08	Social Engineering	1112
09	Denial-of-Service	1197
10	Session Hijacking	1283
11	Hacking Webservers	1357
12	Hacking Web Applications	1446
13	SQL Injection	1632
14	Hacking Wireless Networks	1730
15	Hacking Mobile Platforms	1911
16	Evading IDS, Firewalls, and Honeypots	2058
17	Cloud Computing	2181
18	Cryptography	2265
	References	2360

This page is intentionally left blank.

Welcome to Certified Ethical Hacker Class!

Student Introduction

Unmask the Invisible Hacker.



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



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

Course Materials



Identity Card



Student Courseware



Lab Manual/
Workbook

Course Evaluation



Reference Materials



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

CEHv9 Course Outline		
01	Introduction to Ethical Hacking	07 Sniffing
02	Footprinting and Reconnaissance	08 Social Engineering
03	Scanning Networks	09 Denial-of-Service
04	Enumeration	10 Session Hijacking
05	System Hacking	11 Hacking Webservers
06	Malware Threats	12 Hacking Web Applications
		13 SQL Injection
		14 Hacking Wireless Networks
		15 Hacking Mobile Platforms
		16 Evading IDS, Firewalls, and Honeypots
		17 Cloud Computing
		18 Cryptography

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 Secure Programmer (ECSF)	
EC-Council Certified Security Specialist (ECSS)	EC-Council Certified Security Analyst (ECSA)	
EC-Council Network Security Administrator (ENSA)	Licensed Penetration Tester (LPT)	
Certified Ethical Hacker (CEH) <small>... You are here</small>	Certified Chief Information Security Officer (CCISO)	
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

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

CEH Certification Track

Complete the following steps:

- Attend the Ethical Hacking and Countermeasures Course
- Pass the CEH Exam 312-50 (ECC Exam Portal) / 312-50 (VUE)

CEH
Certified Ethical Hacker

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

CEHv9 Exam Information

- ✓ Exam Title: Certified Ethical Hacker
- ✓ Exam Code: 312-50 (ECC Exam Portal) / 312-50 (VUE)
- ✓ Number of Questions: 125
- ✓ Duration: 4 hours
- ✓ Availability: ECC Exam Portal / VUE
- ✓ Passing Score: 70%
- ✓ The training center / instructor will advise you about the exam schedule and voucher details
- ✓ 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

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?

Network Security

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

Ethical Hacking

Denial of Service, Trojans, Worms, Virus, Social Engineering, Password cracking, Session Hijacking, System failure, Spam, Phishing, Identity theft, Wadrviring, 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?

CEH class is NOT a *Network Security* training program

- Please attend EC-Council's **ENSA** class for that

CEH class is NOT a *Security Analysis* training program

- Please attend EC-Council's **ECSA** class for that

CEH class is NOT a *Security Testing* training program

- Please attend EC-Council's **LPT** Exam for that

CEH class is 100% *NETWORK OFFENSIVE* Training Program

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

C|EH
Certified Ethical Hacker

- 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



certifiedhacker.com

CEH Classroom Attack Lab Website

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

NDA Document

C|EH
Certified Ethical Hacker

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

C|EH
Certified Ethical Hacker

The diagram illustrates the Advanced Lab Environment. At the top, six icons represent different operating systems: Windows 8.1, Windows Server 2008, Windows 7, Kali Linux, Android, and Ubuntu. Below each icon is the system's name. A horizontal dashed line connects all these icons. Arrows point from this line down to two computer icons at the bottom: an 'Instructor Machine' (laptop) and 'Student Machines' (monitor and tower). The background is a gradient from orange to green.

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

C|EH
Certified Ethical Hacker

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

- Windows Server 2012 as host
- Windows Server 2008 as VM
- Windows 8.1 as VM
- Windows 7 as VM
- Kali Linux as VM
- Android as VM
- Ubuntu as VM

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

Student Computer Checklist

C|EH
Certified Ethical Hacker

- 1 Write down IP addresses of the host and all the Virtual Machines
- 2 Check if you can ping between the VM and the hosts
- 3 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
- 4 Check if you can launch command shell by right clicking on a folder
- 5 Check if you can access Internet and browse the web using IE, Chrome, Safari and Firefox
- 6 Check for Checkpoints of Virtual Machines
- 7 Check if you can access <http://www.certifiedhacker.com>
- 8 Make sure you can access MovieScope and GoodShopping websites at <http://www.moviescope.com> and <http://www.goodsshopping.com>

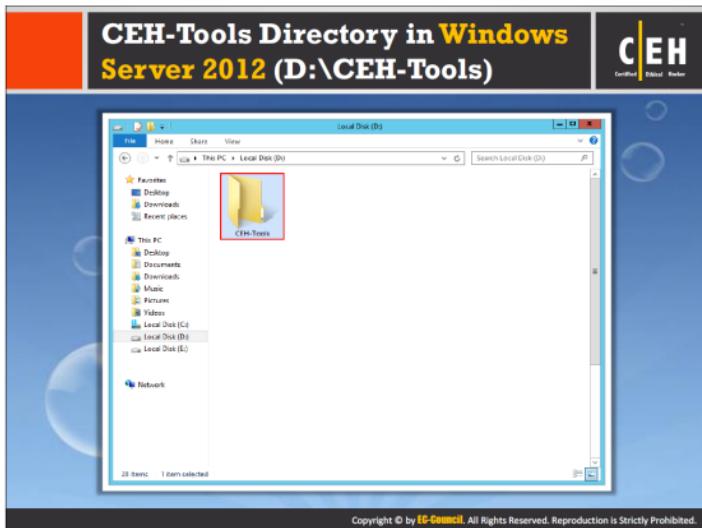
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ping Between Virtual Machines and Host

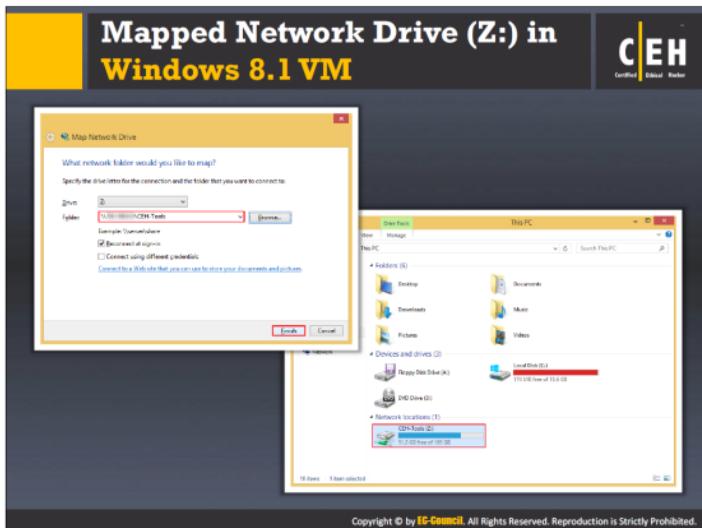
C|EH
Certified Ethical Hacker

```
Administrator: Command Prompt
C:\Windows\system32>ping 192.168.0.10
Pinging 192.168.0.10 with 32 bytes of data:
Bytes from 192.168.0.10: icmp_seq=1 ttl=128 time=0.1ms
Bytes from 192.168.0.10: icmp_seq=2 ttl=128 time=0.1ms
Bytes from 192.168.0.10: icmp_seq=3 ttl=128 time=0.1ms
Bytes from 192.168.0.10: icmp_seq=4 ttl=128 time=0.1ms
Ping statistics for 192.168.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in ms:
        Min = 0.1, Max = 0.1, Avg = 0.1
C:\Windows\system32>
Administrator: Command Prompt
C:\Windows\system32>ping 192.168.0.11
Pinging 192.168.0.11 with 32 bytes of data:
Bytes from 192.168.0.11: icmp_seq=1 ttl=128 time=0.1ms
Bytes from 192.168.0.11: icmp_seq=2 ttl=128 time=0.1ms
Bytes from 192.168.0.11: icmp_seq=3 ttl=128 time=0.1ms
Bytes from 192.168.0.11: icmp_seq=4 ttl=128 time=0.1ms
Ping statistics for 192.168.0.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in ms:
        Min = 0.1, Max = 0.1, Avg = 0.1
C:\Windows\system32>
Administrator: Command Prompt
C:\Windows\system32>ping 192.168.0.12
Pinging 192.168.0.12 with 32 bytes of data:
Bytes from 192.168.0.12: icmp_seq=1 ttl=128 time=0.1ms
Bytes from 192.168.0.12: icmp_seq=2 ttl=128 time=0.1ms
Bytes from 192.168.0.12: icmp_seq=3 ttl=128 time=0.1ms
Bytes from 192.168.0.12: icmp_seq=4 ttl=128 time=0.1ms
Ping statistics for 192.168.0.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in ms:
        Min = 0.1, Max = 0.1, Avg = 0.1
C:\Windows\system32>
```

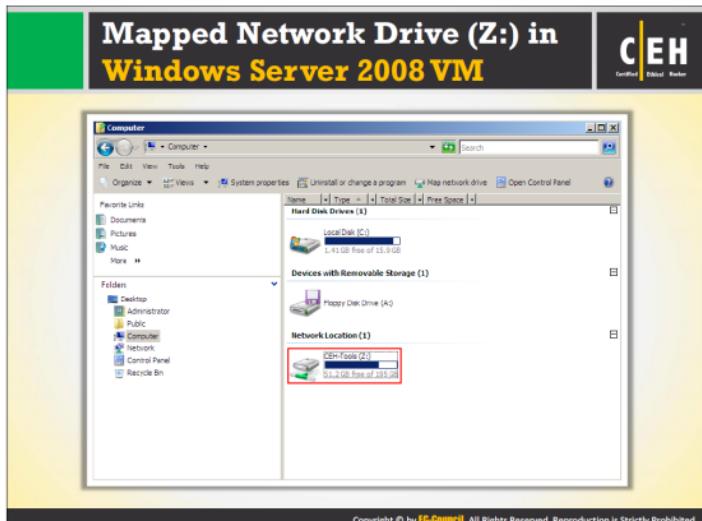
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



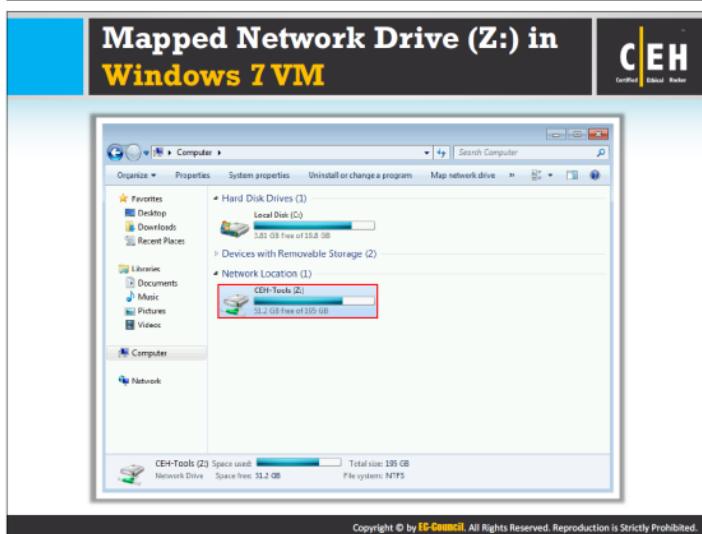
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



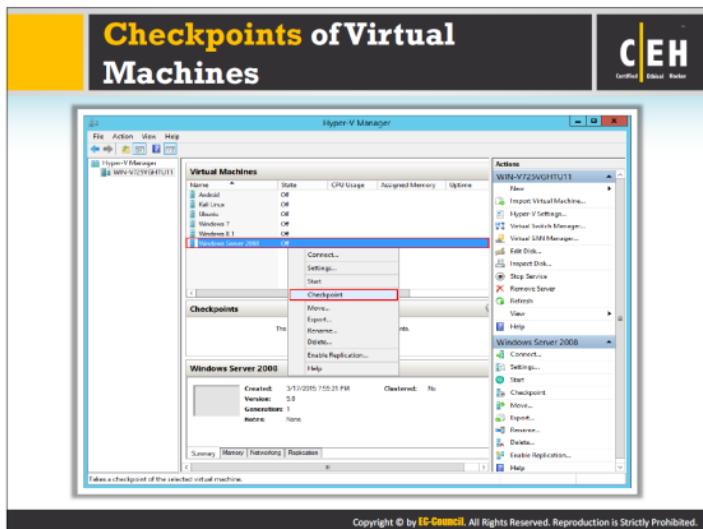
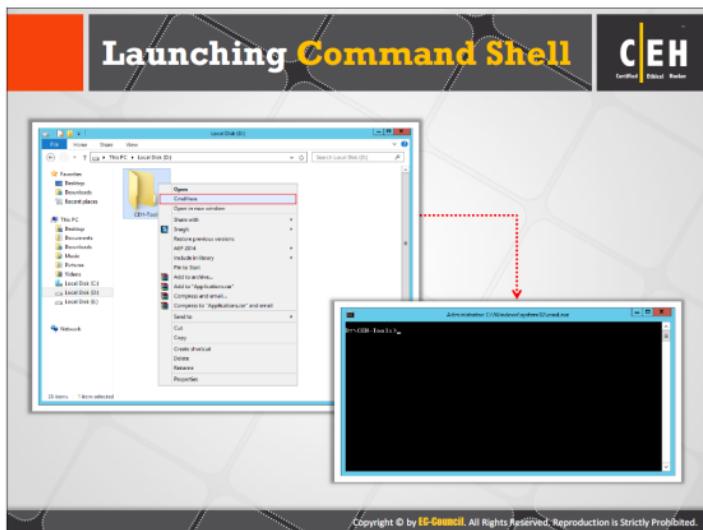
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



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



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



Moviescope and GoodShopping Websites

The image shows two separate browser windows. The left window displays the 'Moviescope' website, which features a dark background with a large image of a traditional building with a red-tiled roof. The right window displays the 'GoodShopping' website, which features a blue background with a large image of a person snowboarding. Both windows show navigation menus and login forms.

Moviescope: <http://www.moviescope.com>

GoodShopping: <http://www.goodshopping.com>

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

Live Hack Website

<http://www.certifiedhacker.com>

The image shows four separate browser windows, each displaying a different website that has been compromised or hacked. The websites include a corporate landing page, a beauty page, a fashion page, and another corporate page. Each window shows a different aspect of the hacked site, such as altered content or visual elements.

CEH Labs

CEH Labs

CEH Labs

CEH Labs

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



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

This page is intentionally left blank.