

# **Certified Network Defender**

## Instructions for Downloading your CND 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 the **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 **eBooks** icon under the **Learning Resources** section. It will open the Academia page.

### Step 6:

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

**Access Code: XXXXXXXXXXXXXXXXX**

### 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 at [academia@eccouncil.org](mailto: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 the **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 the **Class Eval** icon in the **Student Services** section.

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

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

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

**Evaluation Code: \*\*\*CND-\*\*\*\*\***



## EC-Council

Copyright © 2016 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

The computer network has become more and more complex over the past few years and so has the threats to its security. The Certified Network Defender (CND) course has focused on helping the administrator to understand how to effectively deal with such issues that challenge the security of a network.

This course presents a defensive stand to network security. It enhances the skills of a network administrator so as to analyze the internal and external network security threats, how to proactively minimize their effect by developing necessary security policies, designing a defense strategy, implementing the security mechanisms, and by responding to security incidents in a timely manner.

The course covers all major domains in such a manner that the reader will be able to appreciate the way network security mechanisms have 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 and obtain a hands-on experience. The emphasis is on understanding various network security elements, updating the already deployed security mechanisms, spotting any known or possible vulnerabilities, and hardening security implementations using various tools. You will read about the defense mechanisms that are most widely used such as the firewalls, IDS, digital signatures, the secure configuration of various every-day applications, and a comprehensive set of policies that are to be enforced in the network to secure it from network breaches.

This courseware is a resource material. Any network administrator can tell you that there is no one straight methodology or sequence of steps that you can follow while securing a network. There is no one template that can meet all your needs. Your network defense strategy varies with the type of network, the security mechanisms you chose to deploy, and the resources at your disposal. However, for each stage you choose, be it training your staff on security awareness, identifying network threats, implementing packet filtering, deploying a honeypot, troubleshooting the network, configuring a digital signature, securing wireless networks, you will find something in this courseware that you can definitely use.

Finally, this is not the end. This courseware is to be considered as a 'work-in-progress', as it is updated by adding value to it over time. You may find some aspects detailed, while others may be in brief. The yardstick that is used in this respect is simple- "does the content explain the point at hand?" It would be great to hear the views of the reader with respect to viewpoints and suggestions. You can send your feedback so that this courseware can be a more useful one.



# Table of Contents

Module Number	Module Name	Page No.
00	Student Introduction	I
01	Computer Network and Defense Fundamentals	01
02	Network Security Threats, Vulnerabilities, and Attacks	102
03	Network Security Controls, Protocols, and Devices	152
04	Network Security Policy Design and Implementation	253
05	Physical Security	348
06	Host Security	418
07	Secure Firewall Configuration and Management	565
08	Secure IDS Configuration and Management	647
09	Secure VPN Configuration and Management	757
10	Wireless Network Defense	823
11	Network Traffic Monitoring and Analysis	908
12	Network Risk and Vulnerability Management	976
13	Data Backup and Recovery	1051
14	Network Incident Response and Management	1134
	References	1207

# Welcome to Certified Network Defender Class!

## Student Introduction



## Certified Network Defender

### Module 00: Welcome to Certified Network Defender Class!


#### Exam 312-38

# Introduction




- Name
- Company Affiliation
- Title / Function
- Job Responsibility
- Networking 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.



# CND Course Outline

CND

Certified Network Defender

1

Computer Network and Defense Fundamentals

2

Network Security Threats, Vulnerabilities, and Attacks

3

Network Security Controls, Protocols, and Devices

4

Network Security Policy Design and Implementation

5

Physical Security

6

Host Security

7

Secure Firewall Configuration and Management

8

Secure IDS Configuration and Management

9

Secure VPN Configuration and Management

10

Wireless Network Defense

11

Network Traffic Monitoring and Analysis

12

Network Risk and Vulnerability Management

13

Data Backup and Recovery

14

Network Incident Response and Management

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

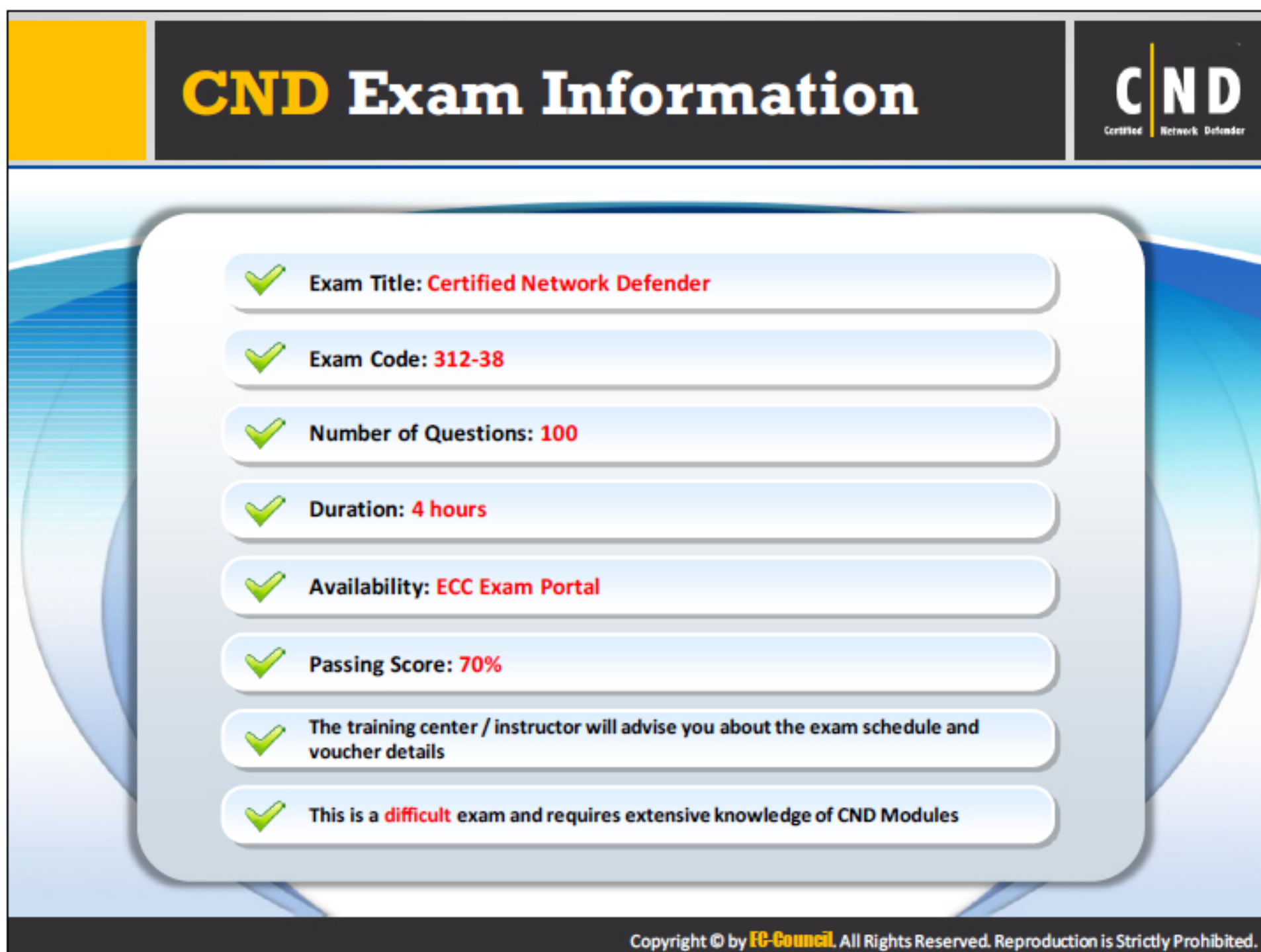
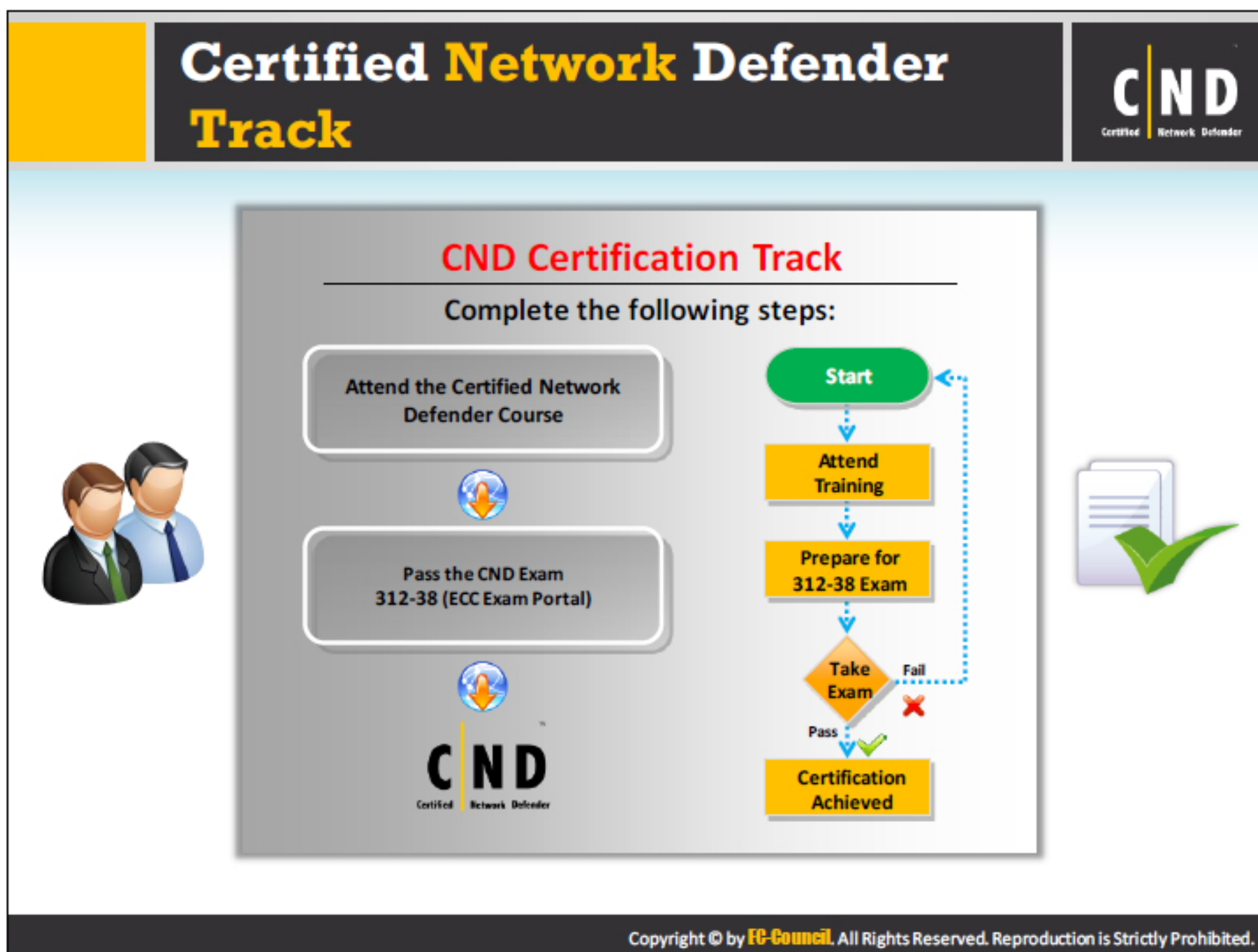
# EC-Council Certification Program

**CND**  
Certified Network Defender

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 (ECSP)
 EC-Council Certified Security Specialist (ECSS)	 EC-Council Certified Security Analyst (ECSA)
 Certified Network Defender(CND) ←... You are here	 Licensed Penetration Tester (LPT)
 Certified Ethical Hacker (CEH)	 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.






# Student Facilities



Class Hours		Building Hours		Phones	
	Parking		Messages		Restrooms
Smoking		Meals		Recycling	

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

# NDA Document






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

We will NOT start the class unless you sign this document


Sign this document and hand it over to the instructor

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



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

# What Does CND Teach You?




## Network Security Technologies

Physical security	Access control mechanism
Firewalls /IDS implementation	Proxy servers
OS hardening/patching	Packet/content filtering
Antivirus protection	Product evaluation based on common criteria
Encryption mechanism	Passwords security
Authentication mechanism	DMZ (demilitarized zones)
Configuration management	Network logs audit

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

# What Does CND Teach You?




## Network Security Operations


- Creating and enforcing **security policies**
- Creating and enforcing standard **network operating procedures**
- Planning **business continuity**
- Configuration **control management**
- Creating and implementing **incident response** processes
- Planning **data backup and recovery**
- Conducting **forensics activities** on incidents
- Providing security awareness and **training**
- Enforcing **security** as culture

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




# CND Lab







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



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




They 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.

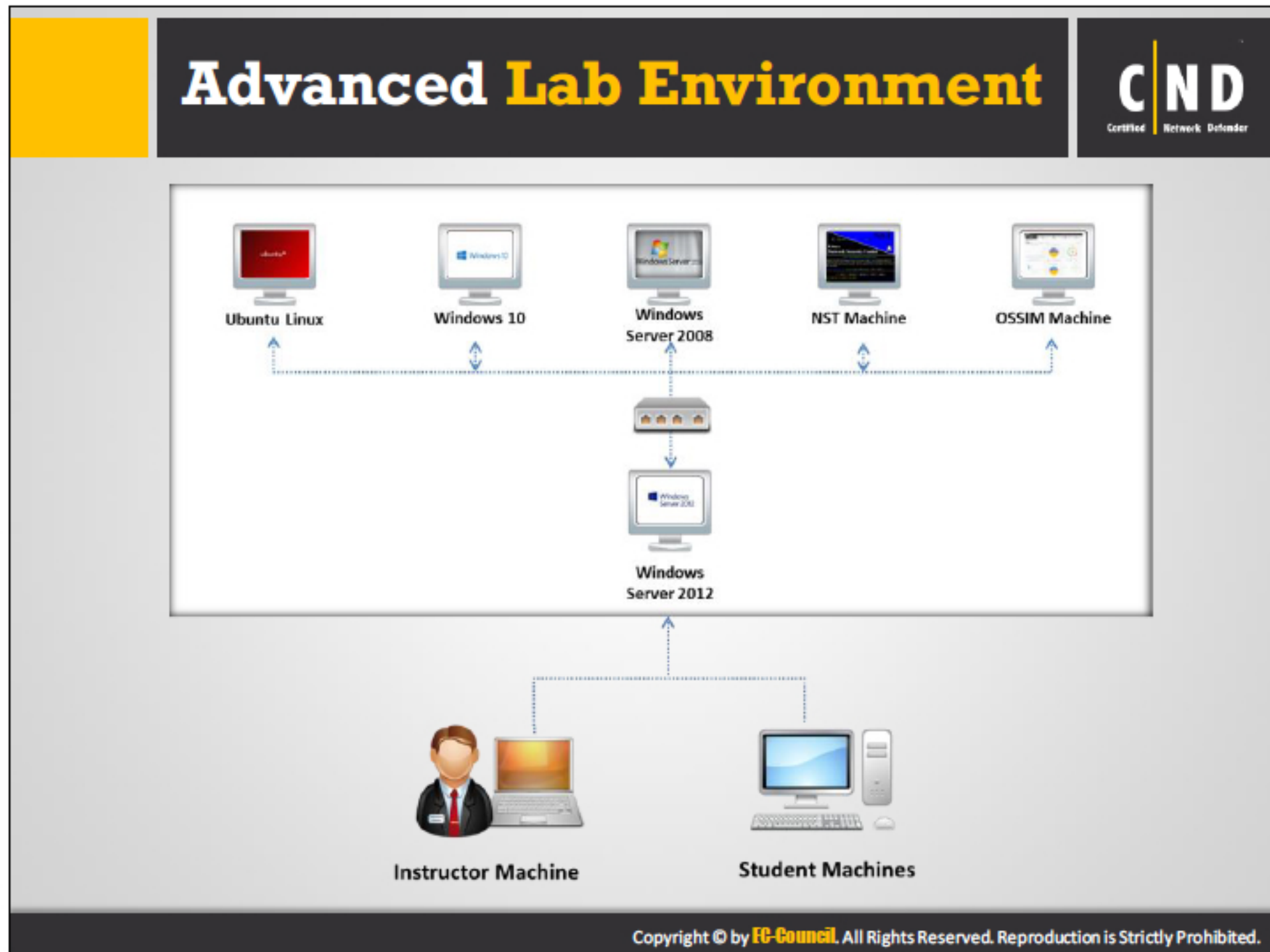
# Lab Sessions



- 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



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)


- Host Machine preferably installed with Windows server 2012 or Windows 10
- Windows Server 2012 as VM
- Windows Server 2008 as VM
- Windows 10 as VM
- Ubuntu as VM
- OSSIM as VM
- NST as VM

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





# Student Computer Checklist



I

Write down IP addresses of the **host** and all the **Virtual Machines**

II

Make sure that you can access **D:\CND-Tools** directory in **your host machine** and **Z:\CND-Tools** from all the VM's; Z: is mapped **Network Drive** containing **CND tools**


III

Check if you can access **Internet** and browse the web using **IE, Chrome,** and **Firefox**

IV

Check for **Checkpoints** of **Virtual Machines**

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



## Welcome to CND Class!

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