

A man with short, dark, curly hair, wearing a white long-sleeved shirt and a dark grey vest, is leaning over a desk. He is looking down at a smartphone in his hand. On the desk, there is a laptop, a white coffee cup on a saucer, and another smartphone. The background shows a window with a grid pattern, suggesting an office or business environment. The image is overlaid with blue geometric shapes: a large blue triangle in the top left and a large blue trapezoid in the bottom right.

Certified Ethical Hacker (CEH)

Contents

About the Programme

Key Features

Prerequisites

Who Should Enroll in this Programme

Key Learning Outcomes

Course Curriculum



About the Programme

CEH certification training course provides you with the hands-on training required to master the techniques hackers use to penetrate network systems, helping you fortify your system against it. This ethical hacking course is aligned with the latest version of CEH (v11) by the EC-Council and adequately prepares you to increase your blue team skills



Key Features



Covers 340 attack technologies



Access to CEH Virtual Labs



40 hours of instructor-led training



Prerequisites

There is no specific eligibility criteria for Certified Ethical Hacker (CEH) training and certification, but we recommend a basic knowledge of TCP/IP



Who Should Enroll in this Programme?

The CISSP course is ideal for professionals who are working in the roles of Chief Information Security Officer, Chief Information Officer, Network Architect, Security Systems Engineer, Security heads/directors and IT Director/Manager.

Certified Ethical Hacker

Key Learning Objectives

By the end of this online Certified Information Security Manager (CISM®) training course, you will have full, working knowledge of

- Grasp the step-by-step methodology and tactics that hackers use to penetrate network systems
- Understand the finer nuances of trojans, backdoors, and countermeasures
- Get a better understanding of IDS, firewalls, honeypots, and wireless hacking
- Master advanced hacking concepts, including mobile device and smartphone hacking, writing virus codes, exploit writing and reverse engineering, and corporate espionage
- Gain expertise on advanced concepts such as advanced network packet analysis, securing IIS and Apache web servers, Windows system administration using Powershell, and hacking SQL and Oracle databases
- Cover the latest developments in mobile and web technologies, including Android, iOS, BlackBerry, Windows Phone, and HTML 5
- Learn advanced log management for information assurance and manage information security with more clarity

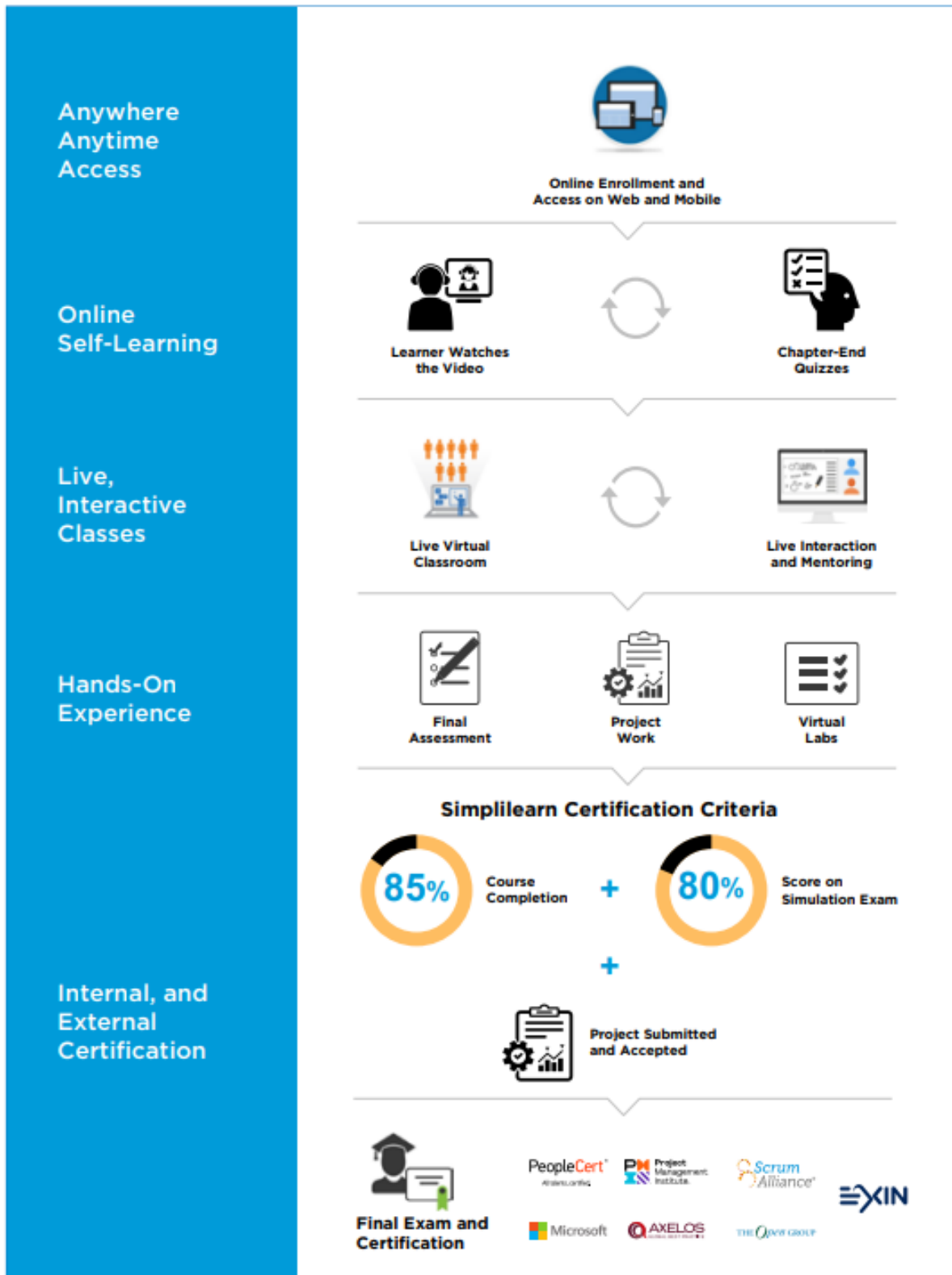
Course Curriculum

- Module 01 - Introduction to Ethical Hacking
- Lesson 02 - Footprinting and Reconnaissance
- Module 03 - Scanning Networks
- Module 04 - Enumeration
- Module 05 - Vulnerability Analysis
- Module 06 - System Hacking
- Module 07 - Malware Threats
- Module 08 - Sniffing
- Module 09- Social Engineering
- Module 10- Denial-of-Service
- Module 11- Session Hijacking
- Module 12 - Evading IDS, Firewalls, and Honeypots

Course Curriculum

- Module 13- Hacking Web Servers
- Module 14- Hacking Web Applications
- Module 15- SQL Injection
- Module 16- Hacking Wireless Networks
- Module 17- Hacking Mobile Platforms
- Module 18- IoT Hacking
- Module 19- Cloud Computing
- Module 20- Cryptography

Classroom-Level Immersion: Delivered Digitally



Features of Corporate Training:



Tailored learning solutions



Flexible pricing options



Enterprise-grade learning management system (LMS)



Enterprise dashboards for individuals and teams



24X7 learner assistance and support

About Us

Deviare is a leader in digital skills training, focused on the emerging technologies that are transforming Africa. Our blended learning approach drives learner engagement. Partnering with professionals and companies, we identify their unique needs and provide outcome-centric solutions to help them achieve their professional goals.

For more information, please visit our website: www.deviare.africa

