# *Gecertificeerd Lead Ethical Hacker, PECB-certificering*

*Praktijkcursus van 4 dagen - 28u*
*Ref : CEY - Prijs 2024 : € 3 940 excl. BTW*

U verwerft de kennis en vaardigheden die nodig zijn om interne en externe pentests te plannen en uit te voeren, in overeenstemming met verschillende standaarden (PTES, OSSTMM), maar ook om rapporten te schrijven en tegenmaatregelen voor te stellen. De cursus is compatibel met de NICE Protect and Defend-rubriek.

## PEDAGOGISCHE DOELSTELLINGEN

Na afloop van de opleiding kan de cursist:

Het mechanisme van de belangrijkste aanvallen begrijpen

Zwakke plekken in systemen detecteren door de verschillende doelwitten van een hackaanval te kennen

Basismaatregelen en -regels toepassen om hacking tegen te gaan

Een pentest-rapport schrijven

## CERTIFICERING

Als u met deze cursus de nodige expertise hebt opgedaan, leg u het "PECB Certified Lead Ethical Hacker" examen af. Het examen, dat 6 uur duurt en op afstand wordt afgelegd, bestaat uit twee delen: het praktijkexamen en het rapport. Het praktijkexamen vereist dat de kandidaat ten minste twee doelmachines compromitteert met behulp van penetratietests. Het proces moet worden gedocumenteerd in een schriftelijk rapport. Het PECB Certified Lead Ethical Hacker examen is een open boek examen. Kandidaten mogen cursusmateriaal en persoonlijke aantekeningen gebruiken tijdens het examen. Het PECB-certificaat certificeert dat u de nodige vaardigheden hebt verworven voor penetratietesten volgens de beste standaarden.

## DEELNEMERS

Beveiligingsmanagers en -architecten. Systeem- en netwerktechnici en -beheerders.

## VOORAFGAANDE VEREISTEN

Goede kennis van netwerken en systemen (Microsoft en Linux).

## VAARDIGHEDEN VAN DE CURSUSLEIDER

De deskundigen die de cursus leiden zijn specialisten op het betreffende vakgebied. Zij werden geselecteerd door onze pedagogische teams zowel om hun vakkennis als hun pedagogische vaardigheden voor elke cursus die zij geven. Zij hebben minstens vijf tot tien jaar ervaring in hun vakgebied en oefenen of oefenden verantwoordelijke bedrijfsfuncties uit.

## BEOORDELINGSMODALITEITEN

De cursusleider beoordeelt de pedagogische vooruitgang van de deelnemer gedurende de gehele cursus aan de hand van meerkeuzevragen, praktijksituaties, praktische opdrachten, …
De deelnemer legt ook van tevoren en naderhand een test af ter bevestiging van de verworven kennis.

## PEDAGOGISCHE EN TECHNISCHE MIDDELEN

• De gebruikte pedagogische middelen en cursusmethoden zijn voornamelijk: audiovisuele hulpmiddelen, documentatie en cursusmateriaal, praktische oefeningen en correcties van de oefeningen voor praktijkstages, casestudies of reële voorbeelden voor de seminars.
• Na afloop van de stages of seminars verstrekt ORSYS de deelnemers een evaluatievragenlijst over de cursus die vervolgens door onze pedagogische teams wordt geanalyseerd.
• Na afloop van de cursus wordt een presentielijst per halve dag verstrekt, evenals een verklaring van de afronding van de cursus indien de stagiair alle sessies heeft bijgewoond.

## TOEGANGSMODALITEITEN EN -TERMIJNEN

De inschrijving dient 24 uur voor aanvang van de cursus plaatsgevonden te hebben.

## TOEGANKELIJKHEID VOOR MINDERVALIDEN

Is voor u speciale toegankelijkheid vereist? Neem contact op met mevr. FOSSE, contactpersoon voor mindervaliden, via het adres psh-accueil@ORSYS.fr om uw verzoek en de haalbaarheid daarvan zo goed mogelijk te bestuderen.

# HET PROGRAMMA

laatste update: 08/2023

### 1) Cyberbeveiliging en architectuur

- Een overzicht van cyberbeveiliging en hedendaagse architectuur.
- Het uitvoeren van een inbraaktest, een pentest, de verschillende soorten pentests.
- Architecturen, besturingssystemen en bekende kwetsbaarheden.

### 2) Actieve herkenning

- Actieve en passieve vormen van herkenning.
- Herkennen, scannen en opsommen.
- Verzamel informatie over kwetsbaarheden.
- Scannen van poorten.
- Misbruik maken van bekende beveiligingslekken in diensten die gekoppeld zijn aan poorten, enz.

*Overzicht van automatische kwetsbaarheden: Nessus, OpenVAS.*

### 3) Werking van systemen

- Operationele kaders.

- CVE's begrijpen: typen (op afstand, lokaal, web).
- Proces-exploits: Buffer Overflow, ROP, Dangling Pointers.
- Shellcodes en rootkits.
- Aanval op Microsoft-authenticaties, PassTheHash.
- Windows: Buffer Overflow met de hand, exploits.

*Misbruik maken van kwetsbaarheden in systemen (Microsoft en Linux).*

### 4) Operatie en postoperatie

- Het document voorbereiden en het rapport schrijven.
- Beschrijf de gevonden kwetsbaarheden.
- Doe veiligheidsaanbevelingen.

*Het rapport schrijven en opmaken.*

## DATA

Neem contact met ons op