Certified Lead Ethical Hacker, certificación PECB

Curso práctico de 4 días - 28h
Ref.: CEY - Precio 2024: 2 750€ sin IVA

Adquirirá los conocimientos y habilidades necesarios para planificar y llevar a cabo pentests internos y externos, de conformidad con diversas normas (PTES, OSSTMM), así como para redactar informes y proponer contramedidas. El curso es compatible con la rúbrica NICE Protect and Defend.

OBJETIVOS PEDAGÓGICOS

Al término de la formación, el alumno podrá:

Comprender el mecanismo de los principales ataques

Detectar los puntos débiles del sistema conociendo los diferentes objetivos de un ataque informático

Aplicación de medidas y normas básicas para combatir la piratería informática

Redactar un informe de pentest

CERTIFICACIÓN

Una vez que haya adquirido los conocimientos necesarios con este curso, se presentará al examen "PECB Certified Lead Ethical Hacker". El examen, que dura 6 horas y se realiza a distancia, consta de dos partes: el examen práctico y el informe. El examen práctico requiere que el candidato comprometa al menos dos máquinas objetivo utilizando pruebas de penetración. El proceso debe documentarse en un informe escrito. El examen PECB Certified Lead Ethical Hacker es un examen a libro abierto. Los candidatos pueden utilizar los materiales del curso y sus notas personales durante el examen. El certificado PECB acredita que se han adquirido los conocimientos necesarios para realizar pruebas de penetración de acuerdo con los mejores estándares.

PARTICIPANTES

Directores y arquitectos de seguridad. Técnicos y administradores de sistemas y redes.

REQUISITOS PREVIOS

Buenos conocimientos de redes y sistemas (Microsoft y Linux).

COMPETENCIAS DEL FORMADOR

Los expertos que imparten la formación son especialistas en las materias tratadas. Han sido validados por nuestros equipos pedagógicos, tanto en el plano de los conocimientos profesionales como en el de la pedagogía, para cada curso que imparten. Cuentan al menos con entre cinco y diez años de experiencia en su área y ocupan o han ocupado puestos de responsabilidad en empresas.

MODALIDADES DE EVALUACIÓN

El formador evalúa los progresos pedagógicos del participante a lo largo de toda la formación mediante preguntas de opción múltiple, escenificaciones de situaciones, trabajos prácticos, etc.
El participante también completará una prueba de posicionamiento previo y posterior para validar las competencias adquiridas.

MEDIOS PEDAGÓGICOS Y TÉCNICOS

• Los medios pedagógicos y los métodos de enseñanza utilizados son principalmente: ayudas audiovisuales, documentación y soporte de cursos, ejercicios prácticos de aplicación y ejercicios corregidos para los cursillos prácticos, estudios de casos o presentación de casos reales para los seminarios de formación.
• Al final de cada cursillo o seminario, ORSYS facilita a los participantes un cuestionario de evaluación del curso que analizarán luego nuestros equipos pedagógicos.
• Al final de la formación se entrega una hoja de presencia por cada media jornada de presencia, así como un certificado de fin de formación si el alumno ha asistido a la totalidad de la sesión.

MODALIDADES Y PLAZOS DE ACCESO

La inscripción debe estar finalizada 24 horas antes del inicio de la formación.

ACCESIBILIDAD DE LAS PERSONAS CON DISCAPACIDAD

¿Tiene alguna necesidad específica de accesibilidad? Póngase en contacto con la Sra. FOSSE, interlocutora sobre discapacidad, en la siguiente dirección psh-accueil@orsys.fr para estudiar de la mejor forma posible su solicitud y su viabilidad.

PROGRAMA

última actualización: 02/2024

1) Ciberseguridad y arquitectura

- Una visión general de la ciberseguridad y la arquitectura contemporánea.
- Realización de un test de intrusión, un pentest, los diferentes tipos de pentest.
- Arquitecturas, sistemas operativos y vulnerabilidades conocidas.

2) Reconocimiento activo

- Formas activas y pasivas de reconocimiento.
- Reconocimiento, escaneado y enumeración.
- Recopilar información sobre vulnerabilidades.
- Exploración de puertos.
- Explotar fallos de seguridad conocidos en servicios vinculados a puertos, etc.

Trabajo práctico : Revisión de vulnerabilidades automáticas: Nessus, OpenVAS.

3) Funcionamiento de los sistemas

- Marcos operativos.
- Comprensión de los CVE: tipos (Remoto, Local, Web).

- Explotaciones de procesos: desbordamiento del búfer, ROP, punteros colgantes.
- Shellcodes y rootkits.
- Ataque a las autenticaciones de Microsoft, PassTheHash.
- Windows: Desbordamiento de búfer a mano, exploits.

Trabajo práctico : Explotación de vulnerabilidades del sistema (Microsoft y Linux).

4) Operación y postoperatorio

- Preparación del documento y redacción del informe.
- Describa las vulnerabilidades encontradas.
- Hacer recomendaciones de seguridad.

Trabajo práctico : Redacción y formato del informe.

FECHAS

Contacto