Certified Ethical Hacker

Descrición

A formación CEH versión 11 (CEHv11) dedica máis da metade do curso a habilidades prácticas a través dos laboratorios de EC- Council e a súa certificación está considerada unha das máis avanzadas do mundo en materia de Hacking Ético e Auditoría de Seguridade de Sistemas Informáticos. Entre as novidades máis destacables da versión 11 inclúense as seguintes características:

- Conxunto das últimas ferramentas de hacking utilizadas por pentesters e profesionais da ciberseguridade
- Foco en importantes áreas de especialización baixo o framework NIST/ NICE Protect and Defend (PR)
- Desafíos de hacking ao final de cada módulo
- Actualización dos módulos de Cloud e IoT para incorporar CSPs, tecnoloxías de contedores como Docker e Kubernetes, ameazas de Cloud computing e ferramentas de hackeo de IoT como Shikra, Bus Pirate, Facedancer21, etc.
- Novos sistemas operativos como Windows Server 2019, Windows Server 2016 e Windows 10 configurados con controlador de dominio, firewalls e aplicacións web vulnerables para practicar e mellorar as habilidades de hacking
- Últimas tácticas de análises de malware para ransomware, malware bancario e financeiro, botnets de IoT, análise de malware OT e Android

As probas de selección realizaranse mediante plataforma online, sen necesidade de desprazamento presencial ao CNTG, a poderá realizar o alumnado inscrito ao curso dende o seu domicilio ou lugar de traballo, tendo en conta que a plataforma online abrirase automaticamente na data e hora indicada para iso.

O alumnado inscrito recibira un mail dende a entidade adxudicataria co acceso a esta proba uns 2 días antes da mesma.

A plataforma online de probas de selección é compatible coas versións estables máis recentes de todos a navegadores web e sistemas operativos máis populares (Windows, MacOS, Android ou calquera distribución Linux).

Por tanto, para acceder á plataforma simplemente necesitarase un equipo de sobremesa, portátil con acceso a unha conexión estable de Internet.

Recomendable ter coñecemento/nivel medio de comprensión lectora en inglés debido a que a proba de nivel pode incluír preguntas en inglés e o exame oficial de certificación ao que se opta neste curso xeralmente realízase en Inglés.

Para seguir o curso é necesario que o equipo conte con altofalantes ou auriculares.

O CNTG facilitará os correos electrónicos das persoas inscritas á empresa organizadora das probas para que esta poida crearlles e comunicarlles as ligazóns de acceso tanto á proba como ao curso.

A inscrición poderá pecharse antes da data indicada no caso de superarse o máximo de 200 personas inscritas.

Obxectivos

O obxectivo da formación é axudarlle a dominar a metodoloxía dun/dunha Hacker Ético/a, a cal poderá ser utilizada tanto nunha proba de intrusión como en calquera situación de hacking ético. Os asistentes, unha vez superado o exame correspondente, lograrán obter unha das certificacións de hacking ético de maior interese global: Certified Ethical Hacker – CEH.

Dirixido a

Este curso está dirixido particularmente a responsables de seguridade, auditores/as, profesionais de seguridade, administradores/as de sistemas e a quen estea interesado/a na seguridade dos sistemas de información.

Recomendable ter coñecemento nivel medio comprensión lectora de inglés.

Perfil do docente

Os nosos formadores e formadoras son persoas con máis de 5 anos de experiencia en áreas de alta especialización técnica nos ámbitos de aplicación. Dispoñen das certificacións oficiais de EC Council, para impartir estes cursos.

DURACIÓN	60 horas
PROGRAMA	Programación 2020/21
MATRÍCULA	Gratuíta
METODOLOXÍA	Virtual
TIPO	CURSO
CERTIFICACIÓN OFICIAL	Sí
EXAME CERTIFICACIÓN	EC-Council 312-50: Certified Ethical Hacker (CEH)
BENEFICIOS	
HORARIO	De luns a venres de 09:30 a 13:30 horas.
PERIODO INSCRICIÓN	19/01/2021 - 01/02/2021
PROBA DE SELECCIÓN	08/02/2021, 10:00
LUGAR DE DOCENCIA	
Nº PRAZAS	16 (Mínimo 10)

Temario

- Módulo 01: Introdución ao Hacking Ético
- Módulo 02: Técnicas de Recoñecemento
- Módulo 03: Escaneo de redes
- Módulo 04: Enumeración
- Módulo 05: Análise de vulnerabilidades
- Módulo 06: Hacking de Sistemas
- Módulo 07: Ameazas de Malware
- Módulo 08: Sniffing
- Módulo 09: Enxeñería Social
- Módulo 10: Denegación de Servizos (DoS)
- Módulo 11: Secuestro de Sesións
- Module 12: Evasión de IDS, Firewalls e Honeypots
- Módulo 13: Hacking de Servidores Web
- Módulo 14: Hacking de Aplicacións Web
- Módulo 15: Inxección de SQL
- Módulo 16: Hacking de Redes sen fíos
- Módulo 17: Hacking de Plataformas Móbiles
- Módulo 18: Hacking IoT
- Módulo 19: Cloud computing
- Módulo 20: Criptografía