

CompTIA Pentest+

Descrición

O curso CompTIA PenTest + valida a capacidade do alumnado para identificar, mitigar e notificar vulnerabilidades do sistema. Abarca todas as etapas das probas de penetración en superficies de ataque como a nube, as aplicacións web, as API e o IoT, e fai fincapé en habilidades prácticas como a xestión de vulnerabilidades e o movemento lateral.

Tanto o material formativo como o exame de certificación están en inglés.

Obxectivos

- Planificar e definir o alcance das probas de penetración, garantindo o cumprimento dos requisitos legais e éticos, e elaborar informes detallados con recomendacións de corrección para apoiar a xestión dos compromisos.
- Realizar recoñecementos activos e pasivos, recompilar información e enumerar sistemas para descubrir vulnerabilidades de forma eficaz.
- Realizar análise de vulnerabilidades, analizar os resultados e validar os achados para identificar e abordar as debilidades de seguridade.
- Executar ataques á rede, baseados en hosts, aplicacións web e baseados na nube utilizando as ferramentas e técnicas adecuadas para poñer a proba as defensas do sistema.
- Manter a persistencia, realizar movementos laterais e documentar os achados para apoiar os esforzos de corrección durante as actividades posteriores á explotación.

Dirixido a

Este curso é ideal para profesionais de TI e ciberseguridade que contan con coñecementos básicos sobre seguridade de redes e sistemas e desexan avanzar cara a postos relacionados coa seguridade ofensiva.

O alumnado adoita ser práctico, analítico e con ganas de desenvolver habilidades prácticas en probas de penetración, avaliación de vulnerabilidades e hacking ético para mellorar as súas perspectivas profesionais ou prepararse para certificacións máis avanzadas.

Postos de traballo relevantes:

- Penetration Tester
- Analista de vulnerabilidades
- Consultor/a de seguridade
- Membro do equipo vermello
- Analista SOC (especializado en seguridade ofensiva)
- Especialista en ciberseguridade
- Enxeñeiro/a de seguridade de redes
- Hacker ético

BENEFICIOS

Diploma de asistencia

Opción gratuita dun exame de certificación oficial

Perfil do docente

Consultor/a con máis de 20 anos de experiencia, especializado/a no sector IT e formador/a certificado/a en Microsoft e Comptia.

PROGRAMA Programación 2026/27

TIPO CURSO

MATRÍCULA Gratuíta

PERIODO INSCRICIÓN 01/02/2027 - 15/02/2027

PROBA DE SELECCIÓN 16/02/2027 (00:00)



CompTIA Pentest+

CRITERIOS DE SELECCIÓN	Proba técnica presencial no CNTG en Santiago de Compostela
Nº PRAZAS	20 (Mínimo 10)
METODOLOXÍA	Virtual
TIPO DE EDICIÓN	Edición única tarde (desempregados/as e ocupados/as)
DURACIÓN	35 horas
DATA INICIO	01/03/2027
DATA FIN	12/03/2027
HORARIO	De luns a venres de 16:30 a 20:00 horas.
CERTIFICACIÓN OFICIAL	Sí
EXAME CERTIFICACIÓN	PT0-003 - CompTIA Pentest+ Certification (en inglés)
MÓDULOS TRANSVERSAIS	Igualdade de 5 horas
TECNOLOXÍA	CompTIA Ciberseguridade/Ciberseguridad
PERIODO DOCENCIA	01/03/2027 - 12/03/2027

Temario

- Lección 1: Determinación do alcance dos requisitos da organización/cliente.
- Lección 2: Definición das regras de compromiso.
- Lección 3: Pegada dixital e recompilación de información.
- Lección 4: Avaliación de vulnerabilidades humanas e físicas.
- Lección 5: Preparación da análise de vulnerabilidades.

- Lección 6: Análise de vulnerabilidades lóxicas.
- Lección 7: Análise dos resultados da análise.
- Lección 8: Evitar a detección e borrar o rastro.
- Lección 9: Explotar a LAN e a nube.
- Lección 10: Probar redes sen fíos.
- Lección 11: Atacar dispositivos móbiles.
- Lección 12: Atacar sistemas especializados.
- Lección 13: Ataques baseados en aplicacións web.
- Lección 14: Hackear sistemas.
- Lección 15: Desenvolvemento de scripts e software.
- Lección 16: Aproveitamento do ataque: pivotar e penetrar
- Lección 17: Comunicación durante o proceso de probas de penetración
- Lección 18: Resumo dos compoñentes do informe
- Lección 19: Recomendación de medidas correctivas
- Lección 20: Realización de actividades posteriores á entrega do informe