

# Certified Penetration Testing Professional (CPENT)

Código: CPENT-001

Propuesta de Valor: EC-COUNCIL

Duración: 40 Horas



El programa Certified Penetration Tester (CPENT) de EC-Council le enseña cómo realizar una prueba de penetración eficaz en un entorno de red empresarial que debe ser atacado, explotado, evadido y defendido. Si solo ha estado trabajando en redes planas, la gama de prácticas en vivo de CPENT le enseñará a llevar sus habilidades al siguiente nivel enseñándole cómo realizar pruebas de penetración en sistemas IoT, sistemas OT, cómo escribir sus propios exploits, construir sus propias herramientas, realizar explotación avanzada de binarios, doble pivote para acceder a redes ocultas y también personalizar scripts / exploits para ingresar a los segmentos más internos de la red.



## AUDIENCIA

- Hackers éticos.
- Probadores de penetración.
- Network server administrators.
- Administradores de firewall.
- Probadores de seguridad.
- Administradores de sistemas y profesionales de evaluación de riesgos.



## PRE REQUISITOS

- El programa CPENT es el siguiente paso después de la certificación Certified Ethical Hacker (CEH).



## OBJETIVOS

- Proporcionar una sólida guía para la redacción de informes.
- Brindar una experiencia del mundo real a través de un rango de prueba de penetración avanzado.
- Proporcionar a los candidatos una prueba de lápiz estándar para su uso en el campo.



## CERTIFICACIÓN DISPONIBLE

Características del examen:

- Certified Penetration Testing Professional.
- Duración del examen: 12 horas.
- Código de examen: CPENT.



## CONTENIDO

1. INTRODUCCIÓN A LAS PRUEBAS DE PENETRACIÓN
2. COMPROMISO Y ALCANCE DE LAS PRUEBAS DE PENETRACIÓN
3. INTELIGENCIA DE CÓDIGO ABIERTO (OSINT)
4. PRUEBAS DE PENETRACIÓN DE INGENIERÍA SOCIAL
5. PRUEBA DE PENETRACIÓN DE RED EXTERNA
6. PRUEBA DE PENETRACIÓN DE RED INTERNA
7. PRUEBA DE PENETRACIÓN DE LA RED DISPOSITIVOS PERIMETRALES
8. PRUEBA DE PENETRACIÓN DE APLICACIONES WEB
9. PRUEBA DE PENETRACIÓN INALÁMBRICA
10. PRUEBA DE PENETRACIÓN DE IOT
11. PRUEBA DE PENETRACIÓN OT / SCADA
12. PRUEBA DE PENETRACIÓN DE LA NUBE
13. ANÁLISIS BINARIO Y EXPLOTACIÓN
14. ESCRITURA DE INFORMES Y ACCIONES POSTERIORES A LA PRUEBA



## BENEFICIOS

- 100% mapeado con el marco NICE.
- Programa de pruebas de penetración 100% basado en metodología.
- Combina enfoques de pruebas de penetración manuales y automatizados.