CPENT: Certified Penetration Testing Professional

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

El corazón del programa CPENT es tratar de ayudarle a dominar sus habilidades de pentesting mediante su utilización en nuestros cyber range en vivo.

Los rangos CPENT fueron diseñados para ser dinámicos, con el fin de darle un programa de entrenamiento en un mundo real, por lo que así como los objetivos y la tecnología continúan cambiando en las redes en vivo, tanto la práctica CPENT como los rangos de exámenes, imitarán esta realidad a medida que nuestro equipo de ingenieros continúe añadiendo objetivos y defensas a lo largo de la vida útil del curso CPENT.

1.1 Resultados Clave

- 100% alineado con el framework NICE.
- Programa de pruebas de penetración 100% basado en metodología.
- Combina enfoques manuales y automatizados de pruebas de penetración.
- Diseñado con las prácticas de pruebas de penetración más comunes ofrecidas por los mejores proveedores de servicios.
- Mapas a todos los portales de trabajo principales. Título del rol: Penetration Tester & Security Analyst.
- Proporciona una guía sólida de escritura de informes.
- Ofrece una experiencia en el mundo real a través de un rango de pruebas de penetración avanzada.
- Proporciona a los candidatos una prueba de pluma estándar para su uso en el campo.

1.2 Temario

- Módulo 01: Introducción a las pruebas de penetración
- Módulo 02: Pruebas de penetración de alcance y participación
- Módulo 03: Inteligencia de código abierto (OSINT)
- Módulo 04: Pruebas de penetración de ingeniería social
- Módulo 05: Pruebas de penetración de red – Externa
- Módulo 06: Pruebas de penetración de red– Interno
- Módulo 07: Pruebas de penetración de red – Dispositivos perimetrales
- Módulo 08: Pruebas de penetración de aplicaciones web
- Módulo 09: Pruebas de penetración inalámbrica
- Módulo 10: Pruebas de penetración de IoT
- Módulo 11: Pruebas de penetración OT/SCADA
- Módulo 12: Pruebas de penetración en la nube
- Módulo 13: Análisis binario y explotación
- Módulo 14: Informar sobre las acciones de escritura y post-pruebas

1.3 Información del Examen

Características del examen:

- ¡Elige tu desafío! ¡Dos sesiones de 12 horas o un solo examen de 24 horas!
- Especialistas de EC-Council monitorean durante todo el examen; hacer trampa no es una opción.

- Logra un score de al menos un 70% y conviértete en un CPENT.
- ¡Consigue al menos el score de 90% y gana la muy respetada designación LPT (Master) adicional!
- Puntuación: Consulte https://cert.eccouncil.org/faq.html