EC-Council

TGK
DIGITAL BUSINESS

PENETRATION TEST

C|PENT
Certified Penetration Testing Professional

Domine las habilidades de pruebas de penetración de clase mundial para proteger a las empresas contra ataques cibernéticos avanzados.

PROFESIONAL CERTIFICADO EN PRUEBAS DE PENETRACIÓN

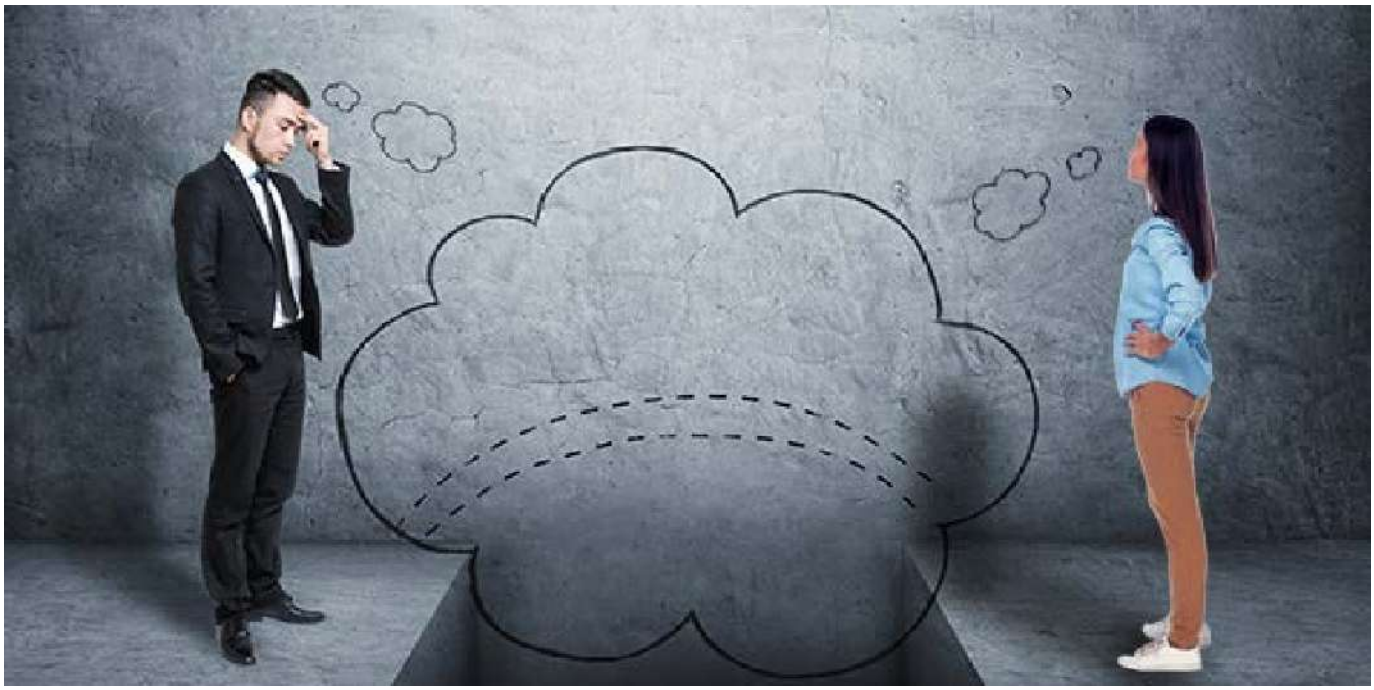
IR MÁS ALLÁ | KALI | HERRAMIENTAS AUTOMATIZADAS EN PLATAFORMAS DE PRUEBAS DE CIBERSEGURIDAD.

¿QUÉ ES EL CURSO C|PENT?

Un riguroso programa de prueba de penetración que, a diferencia de los cursos contemporáneos de prueba de penetración, le enseña cómo realizar una prueba de penetración efectiva en redes filtradas. C|PENT es un curso multidisciplinario con amplia capacitación práctica en una amplia gama de habilidades cruciales, incluidos ataques avanzados de Windows,Internet de las cosas (IoT) y sistemas de tecnología operativa (OT), técnicas de derivación de redes filtradas, escritura de exploits, doble pivote, escalada avanzada de privilegios y explotaciónbinaria. En resumen, ¡no existe un programa de este tipo en el mundo!

CUIDADO CON LA BRECHA

Años de investigación indican que la mayoría de los profesionales de pruebas de penetración tienen lagunas en sus habilidades cuando se trata de múltiples disciplinas. Las métricas también prueban que cuando los objetivos no están ubicados en el mismo segmento o en un segmento directamente conectadoy accesible, muy pocos pueden funcionar tan bien como cuando es directo y en una red plana.



Es por eso que, por primera vez en la industria, la evaluación para el Profesional certificado en pruebas de penetración (C|PENT) se trata de múltiples disciplinas y no solo de uno o dos tipos de especialidad.

01 El curso se presenta a través de un entorno de red empresarial que debe se ratacado, explotado, evadido y defendido.

02 El C|PENT de EC-Council evalúa las habilidades de un probador de penetración en un amplio espectro de "zonas de red".

03 Lo que hace que el C|PENT sea diferente es el requisito de que se le proporcione una variedad de diferentes ámbitos de trabajo para que el candidato pueda "pensar sobre la marcha".

04 El resultado de esto es que hay diferentes zonas que representan diferentes tipos de pruebas.

05 Cualquiera que intente la prueba deberá realizar su evaluación en estas diferentes zonas.

El rango C|PENT, cual es

donde nuestros probadores de penetración adquieren habilidades del mundo real, está diseñado para proporcionar desafíos en todos los niveles del espectro de ataque.
Además, el rango contiene varias capas de segmentación de red y, una vez que se obtiene acceso a un segmento, se requierenlas últimas técnicas de pivote para llegar al siguiente segmento. Muchos de los desafíos requerirán un pensamiento innovador y la personalización de scripts y exploits para ingresar a los segmentos más internos de la red.

La clave para ser un probador de penetración altamente calificado es enfrentarse a varios objetivos que están configurados en una variedad de formas. La C|PENT consta de segmentosde red completos que replican una red empresarial; esto no es una simulación de juego de computadora; esta es una representación precisa de una red empresarial que presentará los últimos desafíos para Penetration Tester. Dado que los objetivos y la tecnología continúan cambiando, el C|PENT es dinámico, se agregarán máquinas y defensas a medida que se observen en la naturaleza. Finalmente, los objetivos y segmentos son de naturaleza progresiva.Una vez que ingrese a una máquina o segmento, la siguiente lo desafiará aún más.

Con C|PENT, aprenda técnicas y metodologías de próxima generación para manejar situaciones de amenazas del mundo real

Las siguientes son 12 razones que hacen que el Programa C|PENT sea único. Este curso excepcional puede convertirlo en uno de los probadores de penetración más avanzados del mundo. El curso tieneun propósito: ayudarlo a superar algunos de los obstáculos más avanzados que enfrentan los profesionales del mundo real al realizar pruebas de penetración. Estos son algunos ejemplos de los desafíos que enfrentará cuando esté expuesto a la gama C|PENT:

ATAQUES AVANZADOS DE WINDOWS

1

Esta zona contiene un bosque completo al que primero debe acceder y, una vez que lo haga, su desafío es usar PowerShell y cualquier otro medio para ejecutar Silver y Gold Ticket y Kerberoasting. Las máquinas se configurarán con defensas en su lugar; por lo tanto, deberá usar técnicas de omisión de PowerShell y otros métodos avanzados para obtener puntos dentro de la zona.

SISTEMAS IOT ATAQUES

2

Con la popularidad de los dispositivos IOT, este es el primer programa que requiere que ubique los dispositivos IOT y luego obtenga acceso a la red. Una vez en la red, debe identificar el firmware del dispositivo IOT, extraerlo y luego revertir diseñarlo.

EXPLOTACIONES DE ESCRITURA: EXPLOTACIÓN DE BINARIOS AVANZADOS

3

Los desafíos que enfrentan los Penetration Testers hoy en día requieren que usen sus propias habilidades para encontrar una falla en el código. En esta zona, se le pedirá que encuentre los archivos binarios defectuosos, realice ingeniería inversa una vez que los encuentre y luego escriba exploits para tomar el control de la ejecución del programa.

La tarea es complicada y requiere Penetración desde el perímetro para obtener acceso y luegodescubrir los binarios. Una vez que tenga éxito, debe aplicar ingeniería inversa al código.

A diferencia de otras certificaciones, esta no será solo un simple código de 32 bits. Habrádesafíos de código de 32 y 64 bits, y parte del código se compilará con las protecciones básicas de las pilas no ejecutables.

Además, debe poder escribir un programa controlador para explotar estos binarios y luego descubriru método para escalar los privilegios. Esto requerirá habilidades avanzadas en explotación binaria que incluyan los últimos conceptos de depuración y técnicas de búsqueda de huevos. Debe crear el código de entrada primero para tomar el control de la ejecución del programa y segundo para mapear un área en la memoria para que su Shell code funcione y eluda las protecciones del sistema.

OMITIR UNA RED FILTRADA

4

La Certificación C|PENT se diferencia de las demás. Proporciona desafíos de zona web que existen dentro de una arquitectura de segmentación. Como resultado, debe identificar el filtrado de la arquitectura, aprovecharlo para obtener acceso a las aplicaciones web que tendrá que comprometer y luego extraer los datos necesarios para lograr puntos.

TECNOLOGÍA OPERACIONAL PENTESTING (OT)

5

Por primera vez en una certificación de prueba de penetración, el C|PENT contiene una zona dedicada a las redes ICS SCADA. El candidato deberá penetrarlos desde el lado de la red de TI, obtener acceso a la red de OT y, una vez allí, identificar el controlador lógico programable (PLC) y luego modificar los datos para impactar la red de OT. El candidato debe poder interceptar el protocolo de comunicación Mod Bus y la comunicación entre el PLC y otros nodos.

ACCEDE A REDES OCULTAS CON PIVOTE

6

Con base en estudios e investigaciones, pocos profesionales han podido identificar las reglas vigentes cuando se encuentran con una red en capas. Por lo tanto, en esta zona, deberá identificar las reglas de filtrado, luego penetrar en la red directa y, desde allí, intentar pivotar en la red oculta utilizando métodos de pivote único, pero a través de un filtro. La mayoría de las certificaciones no tienen un verdadero pivote entre redes dispares y algunas, si es que hay alguna, tienen el requisito de entrar y salir de un dispositivo de filtrado.

DOBLE PIVOTANTE

7

Una vez que haya desafiado y dominado los desafíos del pivote, el siguiente desafío es el doble pivote. Esto no es algo para lo que pueda usar una herramienta. En la mayoría de los casos, el pivote debe configurarse manualmente. C|PENT es la primera certificación en el mundo que requiere que acceda a redes ocultas mediante doble pivote.

ESCALADA DE PRIVILEGIOS

8

Se cubren los métodos más recientes de escalada de privilegios, así como también habrá desafíosq que requerirán que realice ingeniería inversa del código y tome el control de la ejecución, luego salga del shell limitado y obtenga acceso root/admin.

EVADIR MECANISMOS DE DEFENSA

9

Los diferentes métodos de evasión están cubiertos para que puedas tratar de hacer que tus hazañas atraviesen las defensas usándolas como armas.

AUTOMATIZACIÓN DE ATAQUES CON GUIONES

10 Prepárese para técnicas avanzadas de pruebas de penetración/secuencias de comandos con siete apéndices de autoaprendizaje: pruebas de penetración con Ruby, Python, PowerShell, Perl, BASH yaprenda sobre Fuzzing y Metasploit.

CONSTRUYE TU ARMERÍA: ARMA TUS HAZAÑAS

11 Lleve sus propias herramientas y construya su arsenal con su experiencia en codificación y pirateelos desafíos que se le presenten como lo haría en la vida real.

ESCRIBIR INFORMES PROFESIONALES

12 Experimente cómo un probador de penetración puede mitigar los riesgos y validar el informe presentado al cliente que tiene un impacto. La mejor parte de todo es que durante este riguroso proceso, llevaría sus propias herramientas, construiría su arsenal con su experiencia en codificación y piratearía los desafíos que se le presentaran como lo haría en la vida real.

PÚBLICO OBJETIVO

- Hackers éticos
- Probadores de penetración
- Administradores de servidores de red
- Administradores de cortafuegos
- Probadores de seguridad
- Administradores de sistemas y profesionales de evaluación de riesgos
- Analista Forense de Ciberseguridad
- Analista de ciberamenazas
- Seguridad en la nube
- Analista Consultor de Seguridad de la Información
- Analista de seguridad de aplicaciones
- Ingeniero de Aseguramiento de Ciberseguridad
- Analista del Centro de Operaciones de Seguridad (SOC)
- Ingeniero Técnico de Redes de Operaciones
- Ingeniero de Seguridad de la Información
- Probador de penetración de seguridad de red
- Ingeniero de Seguridad de Redes
- Arquitecto de seguridad de la información

DURACIÓN SUGERIDA

5 DIAS
(9:00 a. m. a 5:00 p. m.)

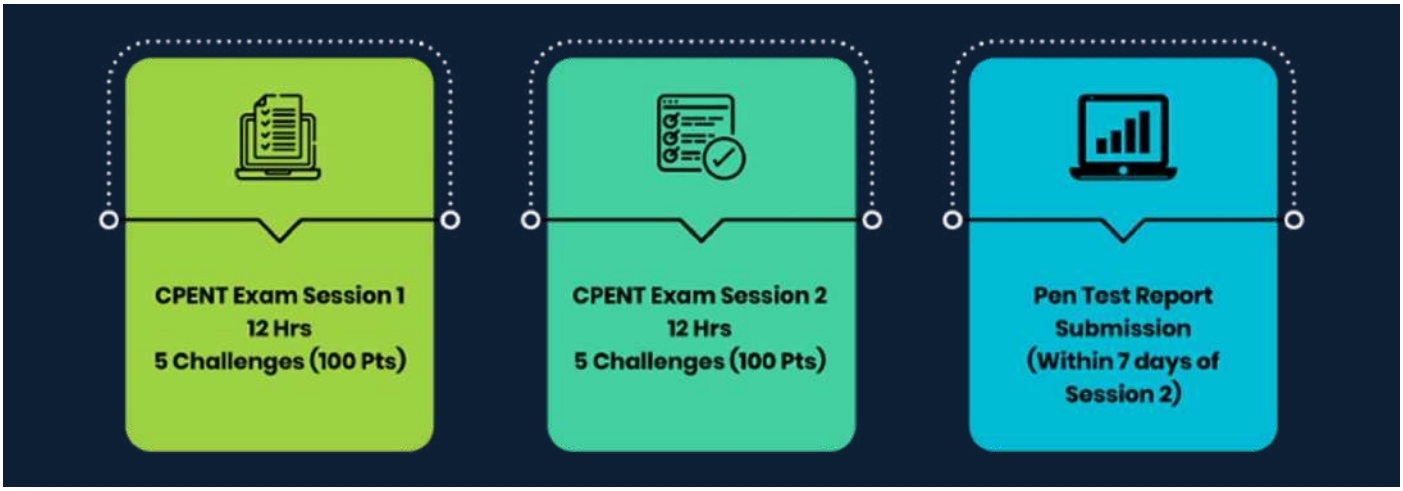
MÍNIMO 40h CAPACITACIÓN + 24h EXAMEN

LOGRAR LA CERTIFICACIÓN C|PENT

¿EXAMEN ÚNICO, CERTIFICACIÓN DOBLE?

Si obtiene al menos un 70% en el examen práctico C|PENT, obtendrá la credencial C|PENT. Sin embargo, si usted es uno de los pocos expertos raros en el planeta, ¡es posible que pueda alcanzar el 90% mínimo para obtener el derecho a ser llamado Probador de penetración con licencia (Maestro)!

C|PENT es un examen práctico completamente en línea supervisado de forma remota, que desafía a los candidatos a través de un extenuante examen práctico de 24 horas basado en el desempeño, categorizado en 2 exámenes prácticos de 12 horas cada uno, que pondrán a prueba su perseverancia y enfoque al obligándote a superarte a ti mismo con cada nuevo reto. Los candidatos tienen la opción de elegir entre dos exámenes de 12 horas o uno de 24 horas, según el nivel de esfuerzo que deseen para el examen.



¡Los candidatos que obtengan una puntuación superior al 90% se establecerán como Maestros en Pruebas de Penetración y obtendrán la prestigiosa credencial LPT (Maestro)!

C|PENT ESTÁ ORIENTADO A RESULTADOS

01

100% mapeado con el marco NICE.

02

Mapas para el puesto de trabajo de una penetración probador y seguridad analista, basado en principales portales de empleo

03

Metodología 100%- Penetración basada Programa de prueba.

04

Proporciona fuerte redacción de informes guía.

05

Mezclada con ambos manuales y automatizado Pruebas de penetración

06

Da un mundo real experiencia a través un avanzado Pruebas de penetración Rango.

07

Diseñado en base a los más comunes Pruebas de penetración servicios ofrecidos por el mejor servicio proveedores en el mercado.

08

Ofrece estándar plantillas que puede ayudar durante una prueba de penetración.

ESQUEMA DEL PROGRAMA

MÓDULO 01	Introducción a las pruebas de penetración	MÓDULO 08	Pruebas de penetración de aplicaciones web
MÓDULO 02	Alcance y compromiso de las pruebas de penetración	MÓDULO 09	Pruebas de penetración inalámbrica
MÓDULO 03	Inteligencia de código abierto (OSINT)	MÓDULO 10	Pruebas de penetración de IoT
MÓDULO 04	Pruebas de penetración de ingeniería social	MÓDULO 11	Pruebas de penetración OT/SCADA
MÓDULO 05	Prueba de penetración de red: externa	MÓDULO 12	Pruebas de penetración en la nube
MÓDULO 06	Prueba de penetración de red: interna	MÓDULO 13	Análisis binario y explotación
MÓDULO 07	Pruebas de penetración de red – Dispositivos perimetrales	MÓDULO 14	Redacción de informes y acciones posteriores

MÓDULOS ADICIONALES DE AUTOESTUDIO

A	Conceptos esenciales de las pruebas de penetración	GRAMO	Entorno Perl y secuencias de comandos
B	Fuzzing	H	Entorno Ruby y secuencias de comandos
C	Dominar el marco Metasploit	I	Pruebas de penetración de Active Directory
D	Secuencias de comandos de PowerShell	j	Pruebas de penetración de bases de datos
mi	Entorno Bash y secuencias de comandos	k	Pruebas de penetración de dispositivos móviles
F	Entorno Python y secuencias de comandos		

CURSO DE APRENDIZAJE DE LA ASOCIACIÓN EC-COUNCIL

EN EVALUACIÓN DE VULNERABILIDADES Y PRUEBAS DE PENETRACIÓN

C|PEN T Certificate Profesional de pruebas de penetración

RESULTADOS

> Dominio de las habilidades de Pruebas de Penetración.
> Realizar la metodología repetible.
> Compromiso con el código ético.
> Presentar los resultados analizados a través de

C|EH ETHICAL HACKER PRACTICAL

RESULTADOS

> Dominio de habilidades de hacking ético.
> Útil en escenarios de ataques cibernéticos

C|EH Certified Ethical Hacker

RESULTADOS

> Una introducción completa a la piratería ética.
> Exposición a vectores de amenazas y contramedidas.

C|ND Certified Network Defender

RESULTADOS

> Proteger, detectar, responder y predecir la aproximación.
> Certificación de proveedor neutral sin restricciones de herramientas/tecnologías.
> Aprenda los conceptos, herramientas y procedimientos generales de seguridad de la red. Diseñar, desarrollar y mantener redes seguras.

EC-Council

Envia un Correo a:
academiaciber@tgk.com.mx
Siguenos en nuestras redes