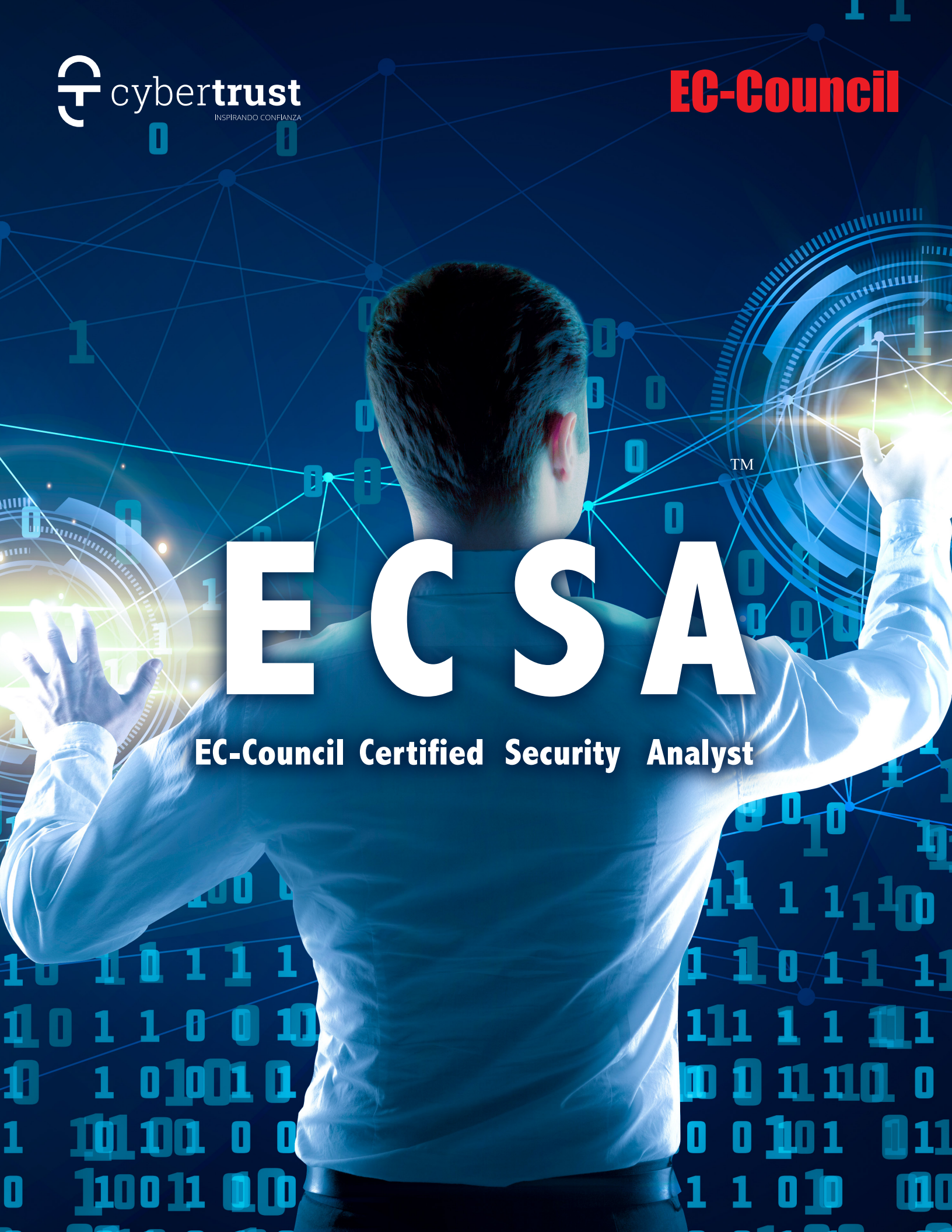
cybertrust
INSPIRANDO CONFIANZA

EC-Council



ECSA™

EC-Council Certified Security Analyst

EC-Council Security Analyst v10 (ECSA)v

El programa ECSA ofrece un progreso de aprendizaje continuo que continúa donde el programa CEH lo dejó.

El nuevo ECSAv10 incluye un currículo actualizado y una metodología integral de prueba de penetración paso a paso reconocida en la industria. Esto permite que un alumno eleve su capacidad para aplicar nuevas habilidades aprendidas a través de intensos laboratorios y desafíos prácticos.

A diferencia de la mayoría de los otros programas de pentesting que solo siguen una metodología genérica de "killchain"; ECSA presenta un conjunto de metodologías integrales distinguibles que pueden cubrir diferentes requisitos de pentesting en diferentes verticales.

Es un programa de capacitación, interactivo, integral, basado en estándares e intensivo de 5 días que enseña a los profesionales de la seguridad de la información cómo se llevan a cabo las pruebas profesionales de penetración en la vida real.

Sobre la base del conocimiento, las habilidades y las habilidades cubiertas en el nuevo programa CEH v10, hemos rediseñado simultáneamente el programa ECSA como una progresión desde el anterior.

Las organizaciones de hoy demandan un programa de pentesting de nivel profesional y no solo programas de pentesting que brinden capacitación sobre cómo atacar aplicaciones y redes.

Dichos programas de nivel profesional solo pueden lograrse cuando el núcleo de los planes de estudios se corresponde con y cumple con los marcos de pentesting publicados por el gobierno y / o la industria.

Este curso es parte de la VAPT Track del EC-Council. Este es un curso de nivel "Profesional", con el Certified Ethical Hacker como el "Core" y el Licensed Penetration Tester como certificación "Master".

En el nuevo curso ECSAv10, los estudiantes que aprueban el examen de conocimiento tienen la opción de realizar un examen totalmente práctico que les brinda una oportunidad para evaluar sus habilidades y obtener la credencial ECSA (Práctica). Esta nueva credencial permite a los empleadores validar fácilmente las habilidades del estudiante.

¿Qué hay de nuevo en ECSA v10?

1. Asigna mapas a NICE 2.0 Framework ECSAv10 maps

2. Nuevo Módulo para pruebas de ingeniería social

El plan de estudios de ECSA presenta una Metodología exhaustiva de pruebas de ingeniería social donde el programa de otros solo hace una mera referencia de esto. De acuerdo con el Informe de Investigación de Incumplimiento de Datos de Verizon 2017, en general, el 43% de las violaciones documentadas involucraron ataques de ingeniería social.

Vemos esto como una gran brecha y es allí donde el programa ECSA se diseña y desarrolla cuidadosamente para que sea completo en su cobertura del dominio pentesting.

3. Mayor enfoque en las metodologías

ECSA V10 brinda una mayor concentración en la metodología para pruebas de redes, aplicaciones web, bases de datos, inalámbricas y en la nube, mientras que otras certificaciones lo cubren superficialmente.

El nuevo programa ECSA v10 toma las herramientas que ha aprendido en la CEH e incluye una amplia gama de metodologías exhaustivas de pruebas de intrusión y penetración que mejoran lo mejor de las normas ISO 27001, OSSTMM y NIST.

4. Mezclado con enfoque de prueba de penetración tanto manual como automatizado

Hay muchas herramientas de prueba de penetración automáticas en el mercado que incluyen herramientas sofisticadas de alto precio, pero no son adecuadas. La mayoría de las herramientas avanzadas son de poco valor si nadie sabe cómo usarlas.

Las pruebas de penetración manual son el complemento perfecto para las pruebas automáticas de penetración. Ciertas pruebas de penetración, como las pruebas lógicas, no se pueden realizar con herramientas automatizadas. Requiere intervención humana para probar o encontrar tales vulnerabilidades

Según MITRE Corporation, las herramientas de pentesting automatizadas cubren solo el 45% de los tipos de vulnerabilidad conocidos. Por lo tanto, el 55% restante requiere intervención manual.

5. Diseñado en base a los servicios de pruebas de penetración más comunes provistos por los proveedores de servicios de prueba de penetración y firmas consultoras en el mercado, que incluyen:

Pruebas de penetración de red
Identificar problemas de seguridad en el diseño e implementación de la red.

Prueba de penetración de aplicaciones web
Detecta problemas de seguridad en aplicaciones web que existen debido a prácticas de diseño y desarrollo inseguras.

Pruebas de penetración en ingeniería social
Identifique a los empleados que no autentiquen, sigan, validen, manejen, los procesos y la tecnología correctamente.

Prueba de penetración inalámbrica
Identifique las configuraciones incorrectas en la infraestructura inalámbrica de la organización, incluyendo WLAN, móvil.

Prueba de penetración en la nube
Determine los problemas de seguridad en la infraestructura de la nube de la organización

Prueba de penetración de la base de datos
Identificar problemas de seguridad en la configuración del servidor de la base de datos y sus instancias.

6. Presenta una exhaustiva metodología de alcance y participación

Definir el alcance de la prueba de penetración es posiblemente uno de los componentes más importantes de una prueba de penetración, sin embargo, también es uno de los más ignorados en la mayoría de los programas de pruebas de penetración. Un módulo completo está dedicado en el curso para describir las actividades previas a la interacción en detalle, explica cómo iniciar y establecer el alcance y la Regla de participación (RoE) para la asignación de la prueba de penetración.

7. Proporciona una sólida guía de redacción de informes para redactar un informe de penetración valioso e integral

El informe es el resultado tangible del proceso de prueba y la única evidencia real de que realmente se realizó una prueba. En última instancia, es el informe que se puede vender en la asignación de prueba de penetración. Si no está bien planificado y redactado, el cliente puede estar en desacuerdo con los resultados de una prueba y no justificará los gastos de la prueba. Se dedica un módulo por separado en el curso para describir las habilidades requeridas para redactar un informe de prueba de penetración efectiva dependiendo de las audiencias objetivo.

8. Laboratorios prácticos que demuestran experiencia práctica y en tiempo real en cada área del examen de penetración.

El conocimiento práctico puede conducir a una comprensión más profunda de un concepto a través del acto de hacer. El curso también tiene como objetivo proporcionar experiencia práctica a través de laboratorios de control en el proceso de prueba de penetración exhaustiva, desde el alcance y el compromiso hasta la redacción de informes. El alumno obtendrá una experiencia directa trabajando en estos laboratorios prácticos.

9. Proporciona plantillas estándar que se requieren durante la prueba de penetración.

El curso se incluye con el conjunto de plantillas estándar que son necesarias para ayudar a los estudiantes durante el alcance y el proceso de participación, así como para recopilar e informar los resultados de las pruebas. Ningún otro programa ofrece un conjunto de plantillas integrales de penetración como ECSA.

El curso ECSA es un programa totalmente práctico con laboratorios y ejercicios que cubren escenarios del mundo real. Al practicar las habilidades que se le proporcionan en la clase ECSA, podemos ponerlo al día con las habilidades para descubrir las amenazas de seguridad a las que las organizaciones son vulnerables.

Esto se puede lograr de manera efectiva con el EC-Council iLabs Cyber Range. Le permite acceder dinámicamente a un host de máquinas virtuales preconfiguradas con vulnerabilidades, exploits, herramientas y scripts desde cualquier lugar con conexión a Internet.

Nuestro portal web le permite lanzar una gama completa de máquinas de destino y acceder a ellas de forma remota con un simple clic. Es la solución de laboratorio de rango en vivo más rentable y fácil de usar disponible.

Con iLabs, se puede acceder a los ejercicios de laboratorio 24 horas al día, 7 días a la semana, lo que permite al alumno practicar sus habilidades en una red segura y completamente funcional en cualquier momento que le resulte conveniente.

Nuestros laboratorios guiados paso a paso incluyen ejercicios con tareas detalladas, herramientas de soporte y materiales adicionales, así como nuestro "entorno abierto" de última generación, lo que le permite lanzar un rango completo en vivo abierto para las pruebas de penetracion.

Las máquinas de destino disponibles están completamente virtualizadas, lo que le permite controlar y restablecer las máquinas.

Criterios de elegibilidad para el examen ECSA

Asistir a la capacitación oficial a través de un canal de capacitación acreditado por el Consejo Ecológico O •

Tener un mínimo de 2 años de experiencia laboral en un dominio de InfoSec relacionado.

Descripción del curso

1. Introducción a las pruebas de penetración y metodologías
2. Metodología de determinación del alcance y prueba de penetración
3. Metodología de Open Source Intelligence (OSINT)
4. Metodología de prueba de penetración de ingeniería social
5. Metodología de prueba de penetración de red: externa
6. Metodología de prueba de penetración de red - interna
7. Metodología de prueba de penetración de red - Dispositivos perimetrales
8. Metodología de prueba de penetración de aplicaciones web
9. Metodología de prueba de penetración de bases de datos
10. Metodología de prueba de penetración inalámbrica
11. Metodología de prueba de penetración en la nube
12. Redacción de informes y acción de prueba posterior

Módulos de autoestudio

Se requiere que los pentesters profesionales continúen aprendiendo a lo largo de su carrera, manteniéndose estrechamente comprometidos con la industria de ciberseguridad que cambia rápidamente. Para permitir el aprendizaje continuo, el curso ECSA viene repleto de toneladas para recursos de autoaprendizaje.

1. Conceptos esenciales de la prueba de penetración Este es un requisito previo esencial, ya que te ayuda a prepararte el material didáctico de ECSA. Sirve como base para construir Conceptos avanzados de prueba de pluma
2. Pruebas de penetración de descifrado de contraseñas
3. Pruebas de penetración de negación de servicio
4. Computadoras portátiles, PDA y teléfonos celulares robados Pruebas de penetración
5. Pruebas de penetración de código fuente
6. Pruebas de penetración de cámaras de vigilancia
7. Pruebas de penetración de VoIP
8 Pruebas de penetración VPN
9. Pruebas de penetración de máquinas virtuales
10. Marcación de guerra
11. Detección de troyanos y virus
12. Pruebas de penetración de gestión de registros
13. Comprobación de integridad de archivos
14. Pruebas de penetración de telecomunicaciones y banda ancha
15. Pruebas de penetración de seguridad de correo electrónico
16. Penetración de parches de seguridad Pruebas
17. Pruebas de penetración de fugas de datos
18. Pruebas de penetración de SAP
19. Normas y cumplimiento
20. Principios de seguridad del sistema de información
21. Manejo y respuesta a incidentes del sistema de información
22. Auditoría y certificación del sistema de información
23. Pruebas de penetración de seguridad física

ECSA (Práctica) ECSA (Práctica) es un examen práctico riguroso de 12 horas. ECSA (Práctica) le presenta una organización simulada y sus redes subyacentes, cada una con múltiples hosts.
Los candidatos deben demostrar la aplicación de la metodología de prueba de penetración presentada en el programa ECSA para realizar una auditoría de seguridad integral de la organización. Comenzará con desafíos que le exigen realizar exploraciones de red avanzadas más allá de las defensas perimetrales, lo que lleva al análisis de vulnerabilidad manual y automatizado, la selección de exploits, la personalización, el lanzamiento y las maniobras posteriores a la explotación.
ECSA (Practical) también evalúa sus habilidades para realizar investigaciones de amenazas y explotación, habilidades para comprender exploits en la naturaleza, escribir sus propios exploits, personalizar payloads útiles y su capacidad para tomar decisiones críticas en diferentes fases de un pentesting .
También se le pedirá que cree un informe de pentesting profesional con elementos esenciales y orientación para la organización en el escenario en el que actuar.
La credencial ECSA (Práctica) proporciona una garantía de que el candidato posee las habilidades requeridas en el campo y será un testimonio de su capacidad para someterse al rigor de la profesión.

Analista de seguridad certificado del Consejo de EC

Consejo de la CE

Sobre el examen: 12 horas rigurosas, examen práctico supervisado en línea
Criterios de elegibilidad para el examen ECSA (práctico) Para ser elegible para presentar una solicitud para el examen ECSA (práctico),

El candidato debe:

- Ser un miembro de ECSA con buena reputación (no se cobrará su tarifa de solicitud de USD 100);
- Tener un mínimo de 2 años de experiencia laboral en el dominio de InfoSec (deberá abonar USD 100 como tarifa de solicitud no reembolsable);
- Tener otras certificaciones equivalentes de la industria, como OSCP o GPEN cert (tendrá que pagar USD 100 como una tarifa de solicitud no reembolsable).

www.cybertrust.cl

Av. Apoquindo 4775, Piso 3 - Las Condes, Santiago de Chile. Teléfono: +562 3224 3551 | +562 3224 3552 Email: contacto@cybertrust.cl