EC-Council Certified Security Analyst v10

Código: ECSA-001

Propuesta de Valor: EC-COUNCIL

Duración: 40 Horas

En el presente curso, el participante obtiene la metodología para realizar Pruebas de Penetración, apegadas a las normas y estándares internacionales enfocadas a todos equipo y dispositivo de TI existentes en una organización; todo esto dentro del marco legal existente. El curso se desarrolla bajo un esquema práctico.

Mientras que la certificación Ethical Hacker expone al alumno a usar herramientas y tecnologías en piratería, el curso de Certified Security Analyst lleva un paso más allá mediante la forma de analizar los resultados de éstas herramientas y tecnologías.

A través de métodos de entrenamiento en pruebas de penetración de red innovadoras y técnicas, éstas pruebas de seguridad informática permiten a los estudiantes que llevan a cabo evaluaciones intensivas para identificar y mitigar riesgos en seguridad de la información de manera eficaz.
ECSA, es una certificación de formación avanzada en el hacking ético que complementa el Certified Ethical Hacker, la certificación CEH explora la fase analítica del hacking ético.

AUDIENCIA

- El curso está dirigido a profesionales técnicos de la seguridad en TI, principalmente aquellos enfocados a la valoración de la seguridad, las auditorias y evaluaciones de planes de continuidad del negocio, que tengan conocimientos en redes, sistemas operativos, base de datos, telefonía IP y seguridad en redes.

PRE REQUISITOS

- No hay requisitos previos.

OBJETIVOS

- Describir la metodología para realizar una Prueba de Penetración (Penetration Testing).
- Diseñar las pruebas de seguridad que se aplicarán a la infraestructura tecnológica de cualquier organización.
- Realizar un Pentesting Testing a los diferentes equipos que conforman la infraestructura de Tecnologías de Información y Comunicación, siguiendo los estándares y las cuestiones legales necesarias.
- Obtener la Licencia LPT (Licensed Penetration Tester), siempre que cumpla los requisitos necesarios para ello.

CERTIFICACIÓN DISPONIBLE

- Certificación emitida por COGNOS.

CONTENIDO

1. ANALISIS DE SEGURIDAD Y METODOLOGIAS DE PRUEBAS DE PENETRACION

2. ANALISIS DE PAQUETES TCP IP

3. PASOS PARA LA PRUEBA DE PRE-PENETRACION

4. METODOLOGIA DE RECOLECCION DE INFORMACION

5. ANALISIS DE VULNERABILIDAD

6. METODOLOGIA DE PRUEBAS DE PENETRACION EN REDES EXTERNAS

7. METODOLOGIA INTERNA DE LA PRUEBA DE LA PENETRACION DE LA RED

8. METODOLOGIA DE LA PRUEBA DE LA PENETRACION DEL CORTAFUEGO

9. METODOLOGIA DE PRUEBA DE PENETRACION DE IDS

10. METODOLOGIA DE LA PRUEBA DE LA PENETRACION DE LA APLICACION DEL WEB

11. METODOLOGIA DE LA PRUEBA DE LA PENETRACION DEL SQL

12. METODOLOGIA DE LA PRUEBA DE LA PENETRACION DE LA BASE DE DATOS

13. METODOLOGIA DE PRUEBAS DE PENETRACION DE REDES INALAMBRICAS

14. METODOLOGIA DE PRUEBAS DE PENETRACION DE DISPOSITIVOS MOVILES

15. METODOLOGIA DE LA PRUEBA DE LA PENETRACION DE LA NUBE

16. REDACCION DE INFORMES Y ACCIONES POSTERIORES A LA PRUEBA

BENEFICIOS

- Al terminar el curso el estudiante obtiene la metodología para realizar Pruebas de Penetración, apegadas a las normas y estándares internacionales enfocadas a todos equipo y dispositivo de TI existentes en una organización.