Uso de reportes de ethical hacking

Código: UREH

Propuesta de Valor: SEGURIDAD INFORMÁTICA

Duración: 16 Horas

Este curso esta diseñado para cualquier persona que quiera iniciarse en el mundo del Hacking y la Ciberseguridad comenzando desde un nivel muy básico, y avanzando a medida que se realiza el curso hasta niveles avanzados, en los que se muestran técnicas como la manipulación de tráfico de red en tiempo real o técnicas de Machine Learning aplicadas a Hacking. Aprende las técnicas más utilizadas por los hackers y cómo utilizarlas para analizar la seguridad de las redes empresariales, formulando reportes tanto para el personal técnico como gerencial, y asistiendo a las organizaciones en la mitigación de sus vulnerabilidades de seguridad.

AUDIENCIA

- Responsables de Seguridad IT
- Administradores de Sistemas y Administradores de Redes
- Operadores de Sistemas, y Auditores
- Técnicos de Soporte y programadores.

PRE REQUISITOS

- No tiene requisitos previos.

OBJETIVOS

- Conocer y desarrollar las fases de un ataque hacker.
- Conocer que son y cómo se llevan a cabo los ataques hackers más habituales.
- Conocer y aplicar programas orientados a Ethical Hacking.
- Conocer y desplegar contramedidas de protección de ataques hackers.
- Reforzar la seguridad de hosts y aplicaciones.

CERTIFICACIÓN DISPONIBLE

- Certificado oficial de **COGNOS**.

CONTENIDO

1. METODOLOGÍAS DE ETHICAL HACKING: OWASP, OSSTMM, ECCOUNCIL

2. CALIFICACIÓN DE RIESGOS: CVSS

3. TIPOS DE INFORMES DE ETHICAL HACKING

4. MALAS PRÁCTICAS EN INFORMES DE ETHICAL HACKING

5. CICLO DE CIERRE DE VULNERABILIDADES DE ETHICAL HACKING

6. RELACIÓN ENTRE VULNERABILIDADES DEL ETHICAL HACKING Y LA GESTIÓN DE RIESGOS TI

BENEFICIOS

- Al finalizar el curso, los participantes conoceran los conceptos, ámbito y limitaciones del Ethical Hacking