Berrikuntza Profesionalen Eskola
Escuela de Innovación Profesional

Especialización en ciberseguridad

Zer ikasiko duzu? / ¿Qué aprenderás?

- **Aplicar seguridad en capa de red,** mediante:
    - El establecimiento de protocolos para garantizar la confidencialidad e integridad de la información durante el proceso de la administración de conmutadores y routers.
    - La utilización de técnicas de autenticidad, confidencialidad e integridad de la información.
    - Evitar malas prácticas a la hora de configurar y administrar routers y conmutadores.
    - Implantación de Vlans y segmentación de las redes a través de conmutadores.
    - La gestión de listas de control de acceso ACLs.

- **Protección endpoint y servidor,** mediante
    - El estudio de las distintas políticas que se pueden emplear a través de Active Directory.
    - La aplicación de políticas para alinear las organizaciones con las medidas solicitadas en los controles de la ISO 27002.
    - Gestionar sistemas antivirus centralizados planificando actualizaciones, escaneos, listas blancas, negras y otras configuraciones.
    - Gestionar una plataforma Wsus vinculando equipos, servidores y estableciendo políticas que tengan por objeto mantener un parque de equipos totalmente actualizado.

- **Seguridad Perimetral,** mediante
    - La segmentación de redes y seguridad multicapa
    - La configuración de un firewall perimetral con inspección de estado que incluya
        - Reglas de filtrado
        - Reglas de NAT
        - Reglas de prerouting
    - La configuración de reglas de filtrado a nivel de host
    - La configuración de un Proxy Web basado en Squid
    - La configuración de acceso VPN mediante OpenVPN y RAS/Radius

- **Monitorización y Gestión de LOGS**, mediante

    - El análisis de registros de eventos.
    - La Configuración de los distintos sistemas de información independientemente de su sistema operativo para adecuar el registro de eventos a las necesidades de cualquier organización.
    - El análisis de herramientas SIEM para evaluar cual es la más adecuada para cualquier organización.
    - La Consulta de eventos, parseo de los mismos y posterior tratamiento para generar cuadros de mando, informes y alertas.
    - Conocimiento de las herramientas de monitorización de red más importantes de la actualidad, los protocolos que emplean y su configuración.

- **Pentesting Web y hacking ético,** mediante el conocimiento sobre

    - Que es una inyección SQL y cómo se emplean.
    - Que es un Cross-Site Scripting y cómo se emplean.
    - La finalidad y proceso de ataques de denegación de servicio.
    - Otros ataques, como Directory Traversal y ataques de tipo Misconfiguration.
    - Como emplear herramientas para el análisis de las vulnerabilidades en aplicaciones Web.

Nola ikasiko duzu? / ¿Cómo aprenderás?

1. **Mediante metodología activa PBL**: basada en resolución de retos y trabajo colaborativo.
2. **Con clases 100% prácticas**: trabajando en máquina desde el primer día.
3. **Utilizando un entorno de virtualización profesional:** sobre VMware vSphere y Diseño de redes virtuales y seguridad perimetral con VMware NSX
4. **Configurando complejos laboratorios**: replicando la estructura de una red local con acceso a Internet, donde se configuran más de 10 equipos entre servidores y clientes.
5. **Con profesionales expertos en ciberseguridad**: entre el equipo de profesores contarás con expertos con más de 12 años de experiencia profesional en empresas de ciberseguridad.

Zertarako ikasiko duzu? / ¿Para qué aprenderás?

1. **Formarte como profesional de ciberseguridad**:
    a. Adquiriendo conocimientos y habilidades específicas en esta área para…
2. **Mejorar tu empleabilidad:**
    a. Mejorando tu perfil profesional con competencias en ciberseguridad que supondrán un criterio diferenciador con el que poder…
3. **Atender la creciente demanda de especialistas en ciberseguridad**:
    a. Solicitada por las empresas para cubrir la falta de profesionales en el sector.