www.darFe.es

info@darfe.es

# Temario del curso "Experto en Ciberseguridad de Redes y Sistemas"

Paso previo: Instalación de Máquina Virtual Kali.

Requerimiento 1: Instalación máquina virtual Kali.
Requerimiento 2: Trabajando con FWs (IPtables)
Requerimiento 3: Instalación de máquina virtual OSSIM

## TEMAS

1. Gestión de Firewalls y listas de control de acceso
2. Redirección de puertos
3. Análisis de Switchs y Routers
4. Auditorías y evaluaciones de Seguridad
5. Seguridad en grandes redes
6. Funciones, responsabilidad y obligaciones de Seguridad
7. Principales procesos de Seguridad
8. Seguridad en Centrales o CPDs
9. Sistemas de Prevención de Intrusiones
10. Análisis de Riesgo
11. Plan Director de Seguridad
12. Familia IPSec
13. Seguridad en VoIP
14. Guías CIS

## Breve descripción de Temario

1. Gestión de Firewalls y listas de control de acceso

   Cuando trabajamos con cierto número de FWs y/o el número de reglas comienza a superar los cientos de ellas, es necesario contar con infraestructuras o plataformas que nos permitan la gestión adecuada de cada uno de ellos, sin este tipo de herramientas, la gestión de los FWs puede presentar fallos de seguridad importantes.

2. Redirección de puertos.

El concepto de "SSH forwarding", para el acceso y trabajo de las redes de gestión o la securización de accesos, es una de las mejores metodologías a emplear en la gestión de ciberseguridad.

3. Análisis de Switchs y Routers

   Estas dos plataformas son claves en los niveles 2 y 3 del modelo TCP/IP. Es muy frecuente encontrara debilidades en sus configuraciones, por lo que el área de Ciberseguridad debe conocer la metodología de auditoría y análisis de los mismos.

4. Auditorías y evaluaciones de Seguridad.

   El área de Ciberseguridad debe ser la responsable de la realización de estos trabajos, para hacerlos de forma metódica, debe contar con una buena base de formación para poder hacer este tipo de tareas de forma técnica, sin que sea una mera auditoría procedimental.

5. Seguridad en grandes redes.

   Cuando la envergadura de la organización, comienza a tener despliegues regionales, accesos WAN, telefonía IP, diferentes zonas y accesos, etc. Se deben considerar un conjunto de medidas adicionales a una red LAN estándar.

6. Funciones, responsabilidad y obligaciones de Seguridad.

   Si bien este tema parece ser procedimental, en este punto se desarrollan las medidas técnicas a tener en cuenta por esta área.

7. Principales procesos de Seguridad.

   El desarrollo e implantación adecuada de los principales procesos relacionados a ciberseguridad, son una de las claves de éxito de una organización. No solo el desarrollo y confección de los mismos, sino su integración al día a día de la empresa.

8. Seguridad en Centrales o CPDs.

   Cuando se cuenta con este tipo de salas o edificios, hay un conjunto de medidas de seguridad física, medioambiental, energía, vigilancia, etc. Que están bastante estandarizadas y no pueden ser dejadas de lado.

9. Sistemas de Prevención de Intrusiones.

   Estos dispositivos, junto con los IDS, son los verdaderos ojos de la infraestructura de red y TI. Hoy en día son una pieza fundamental. El trabajo cotidiano con los mismos, requiera un especial ciclo de vida para que sean de verdad eficientes.

10. Análisis de Riesgo.

    Este es uno de los pasos más importantes a la hora de poder determinar el conjunto de medidas y acciones que nos permitirá desarrollar el punto que sigue. Sin un riguroso Análisis de Riesgo, es muy difícil poder cuantificar las necesidades que tiene la organización en cuanto a Ciberseguridad.

11. Plan Director de Seguridad.

    Este es el verdadero documento resultante de un trabajo metódico del área de ciberseguridad, pensado a medio/largo plazo. Existen bastantes guías y documentos de apoyo que nos facilitan esta tarea. La alta dirección debe recibir este documento como un "Plan de ciberseguridad" u hoja de ruta a seguir por su empresa u organización, y el mismo debe demostrar que el área de ciberseguridad ha sido capaz de analizar el tema con máximo detalle.

12. Familia IPSec.

    Esta familia de normas, nos permite aplicar un robusto sistema de "Autenticación, integridad y confidencialidad" en todas las comunicaciones de la empresa. Es probable que a futuro, se implante por medio de algún producto comercial, pero en general, hoy en día cualquiera de ellos, se basa en el empleo de IPSec, por lo que el conocimiento de estos estándares es la clave de un adecuado control de las comunicaciones seguras.

13. Seguridad en VoIP.

    Hoy en día es muy frecuento el empleo de VoIP en los sistemas de telefonía de toda empresa. Esta red, no deja ser parte de la arquitectura de red de la organización. Cuando no se securiza debidamente es una de las mejores puertas de entrada para los intrusos.

14. Guías CIS.

    El "Center for Internet Security" es una de las organizaciones más importantes a la hora de considerara guías de bastionado. Las guías CIS son un referente internacional para la implantación de seguridad de dispositivos, sistemas operativos y aplicaciones. El entendimiento de cómo se aplican las mismas es el punto que se desarrollará aquí, sobre ejemplos concretos.