www.darFe.es

info@darfe.es

Temario del curso "Especialista en Ciberseguridad de Redes y Sistemas"

TEMAS

1. Telefonía fija y móvil.
2. Las redes de acceso, agregación, transporte y Core (red Fija y red Móvil).
3. Aspectos de detalle sobre el protocolo IP.
4. Switching y Protocolos de la familia IEEE: 802.x.
5. Redes WiFi IEEE: 801.11i
6. Routing y Protocolos de ruteo estáticos y dinámicos.
7. Firewalls.
8. Sistemas de detección de Intrusiones.
9. Autenticación y control de accesos.
10. Zero trust.
11. Gestión de Logs.
12. Gestión de incidentes.
13. Infraestructuras de Supervisión y Monitorización.
14. Riesgos, Política y Plan director de seguridad.
15. Resiliencia.
16. La privacidad de la información.
17. Familia ISO 27000.
18. Criptografía de clave pública y certificados digitales.
19. Infraestructura de Clave pública (PKI).
20. Empleo de Secure SHell (SSH).

Ejercicios:

Breve descripción de Temario

1. Telefonía fija y móvil.

   Hoy en día, toda la infraestructura de nuestra organización dependerá de estas dos redes públicas, pues sobre ellas configuraremos todas las comunicaciones hacia y desde el exterior.

2. Las redes de acceso, agregación, transporte y Core (red Fija y red Móvil).

   El entendimiento de estas redes, desde el punto de vista de Ciberseguridad, nos permite identificar y operar sobre cada segmento en las trazas de "extremo a extremo" de una comunicación.

Es decir, cuando se tiene el detalle de los diferentes caminos a seguir por nuestros paquetes, se puede identificar cada uno de sus saltos y analizar los puntos débiles de esta trayectoria.
Todo esto es fundamental pues cuando establecemos conexiones desde y hacia nuestras sedes, o más aún, cuando hoy en día implantamos medidas de acceso remoto a cualquiera de las zonas de nuestra organización, es imprescindible reconocer con máximo detalle cada uno de los protocolos, rutas y medidas de autenticación y control de acceso para el "establecimiento, mantenimiento y cierre" de la comunicación.

3. Aspectos de detalle sobre el protocolo IP.

   Más allá de lo desarrollado hasta ahora, el protocolo IP, en su encabezado, como también en su campo "opciones" permite o no una serie de parámetros que deben ser conocidos y abordados metodológicamente para su adecuada operación desde el punto de vista de ciberseguridad.

4. Switching y Protocolos de la familia IEEE: 802.x.

   El nivel de enlace, como ya se ha visto es el más importante de nuestras redes y sistemas, pues en el mismo, viajan "empaquetados" el resto de los niveles. Existen una serie de medidas que no pueden ser dejadas de lado hoy en día para asegurar este nivel.
   Es muy importante también, saber auditar la configuración de nuestros switchs para poder valorar el cumplimiento o no de las medidas de ciberseguridad que están establecidas.

5. Redes WiFi IEEE: 801.11i
   Hoy en día estas redes son una realidad en toda organización. No basta solamente con implementar WPA3, existen un conjunto de medidas a tomar en cuenta para la adecuada gestión de las mismas si deseamos que sean tan seguras como nuestras redes cableadas.

6. Routing y Protocolos de ruteo estáticos y dinámicos.

   Al igual que en el nivel 2, el concepto de switching nos habla de las medidas adecuadas para este nivel, en el nivel de red, sucede lo mismo. La elección de una ruta u otra puede impactar de forma directa, tanto el rendimiento de nuestras redes, como su interceptación y/o escucha, para minimizar el riesgo en este nivel, es necesario conocer los protocolos de enrutamiento, tanto estáticos como dinámicos y las medidas de bastionado o hardening de nuestros routers, que son los dispositivos clave de este nivel.
   El adecuado empleo de listas de control de acceso (ACLs) son una de las medidas fundamentales a considerar en el nivel 3.

7. Firewalls.

En este punto nos centraremos en los firewalls de red, comenzando por el más importante de sus referentes "iptables" de Linux, pues quien entienda y sepa operarlo debidamente, no tendrá ningún inconveniente en escalar su lógica o empleo en cualquier otro producto comercial.

8. Sistemas de detección de Intrusiones.

   Debemos reconocer que somos unos fanáticos obsesivos con "Snort", esta decisión viene desde el año 2001, en el que hicimos nuestros primeros trabajos con esta maravilla de la ingeniería (ver artículo "Nivel de inmadurez de los NIDS"). Estamos convencidos que la potencia, flexibilidad y sobre todo la "personalización" granular y específica que nos ofrece toda la configuración de este IDS no tiene ninguna comparación, ni siquiera con el producto más costoso del mercado, por ello centraremos toda la atención sobre "Snort".

9. Autenticación y control de accesos.

   Reconocer que "es quien dice ser" y luego encaminarlo hacia las zonas e infraestructuras a las que únicamente debe acceder son una de las principales medidas a la hora de establecer la ciberseguridad de nuestra organización.

10. Zero trust.

    Este concepto o arquitectura (ZTA: Zero Trust Architecture) es un tema que debe ser desarrollado y entendido, para poder aplicarlo en las políticas y entidades que gestionan y regulan, justamente la "Autenticación y el control de accesos". No solo es una idea teórica, sino que se trata de un conjunto de medidas, políticas e infraestructuras que deben relacionarse entre sí para que justamente en cada zona de nuestras redes, podamos asegurar quién puede o no acceder y qué acciones podrá o no realizar dentro de cada una de ellas.

11. Gestión de Logs.

    La "huella" de lo que se hace o deja de hacerse nos la dejan los registros o "Logs" de la organización. Lo primero que buscará un intruso (como cualquier delincuente), es no dejar rastros de su accionar delictivo, para evitar que eso suceda, existen una serie de acciones y medidas que deben ser tenidas en cuenta, y mucho más aún cuando esto desencadena en un incidente de seguridad que debemos "reconstruir".

12. Gestión de incidentes.

    Aparte de la certeza que todos algún día moriremos y es ineludible, en la vida de un informático y/o teleco, existe otra certeza absoluta y tan ineludible como la muerte física: "**Sí o sí"** tendré al

menos un incidente de ciberseguridad. Intencionado o no, por fallo humano o material, por catástrofes, incendios, enfermedades o pandemias, p ero tarde o temprano llegará…
No pensar así, es tan absurdo como confiar en no morir físicamente.

13. Infraestructuras de Supervisión y Monitorización.

Los ojos de nuestras redes son este tipo de plataformas e infraestructuras que nos permiten, tanto verificar en tiempo real su funcionamiento y rendimiento, como reconocer fallos en el menor tiempo posible, también nos permiten acceder a los diferentes dispositivos de forma segura y centralizada. Este tipo de plataformas, son las que en general se operan desde los NOC (Network Operation Center) y los SOC (Security Operation Center), así que también hablaremos de estos últimos.

14. Riesgos, Política y Plan director de seguridad.

Cualquier responsable de Ciberseguridad debe ser consciente de la importancia que tiene el "medio y largo plazo". La improvisación es el peor enemigo de la ciberseguridad. Diseñar, planificar, cuantificar, monitorizar y mantener viva la política y el plan director de seguridad, basado eminentemente en un "Análisis de Riesgo", es su principal responsabilidad.

15. Resiliencia.

La capacidad de recuperación, no una sino todas las veces que sea necesario, ante estos incidentes debe ser uno de los objetivos principales del plan y la política de seguridad. Esto es lo que denominamos Resiliencia, y se trata, no solo de una serie de copias de respaldo y recuperación, sino de mucho más.

16. La privacidad de la información.

Hoy en día la Unión Europea, ha puesto especial interés en este aspecto de la privacidad de los datos personales. Es un tema que se viene gestando desde hace años, pero que a partir de un par de años atrás no puede ser dejado de lado. El RGPD (Reglamento General de Protección de Datos) que promovió la UE está siendo un referente internacional, y en particular para todo el mundo de habla hispana, así que este será uno de los pilares sobre los que se desarrollo este punto.

17. Familia ISO 27000.

Más allá de que se desee o no obtener una certificación en ISO/UNE 27001, esta norma, o mejor dicho "familia" de normas, pues se trata de un conjunto de ellas bajo el encabezado 27xxx, es la verdadera guía para establecer un SGSI (Sistema de Gestión de la Seguridad de la Información).

El SGSI, debe ser la estructura y pilara sobre el que diseñar nuestra Ciberseguridad. Se trata de una serie de recomendaciones que lleva ya más de veinte años de madurez y se ha demostrado su eficiencia y robustez a lo largo de estos años. Por lo tanto, no importa tanto la obtención de su certificación, o no, sino la organización de nuestra Ciberseguridad, tomando como guía lo que establecen estos estándares, tanto en "cuerpo" de los mismos, reflejado en la norma ISO/UNE 27001, como su métricas y controles que figuran en ISO/UNE 27002. Sobre estas dos últimas, centraremos este punto.

18. Criptografía de clave pública y certificados digitales.

Hoy en día estos algoritmos criptográficos son los más robustos a emplear. Como veremos en este punto, muchos de los procesos y configuraciones de las comunicaciones y accesos a nuestras infraestructuras, pueden ser mejorados substancialmente si conocemos y sabemos aplicar los mismos. En este punto, desarrollaremos los mecanismos y comandos necesarios para comprender y aplicar los mismos.

19. Infraestructura de Clave pública (PKI).

Habiendo comprendido la criptografía de clave pública y certificados digitales, ahora podemos seguir avanzando hasta montar toda una PKI)Public Key Infraestructure) que gestione, emita, y mantenga el manejo de claves de nuestra organización.

20. Empleo de Secure SHell (SSH).

Este protocolo de comunicación segura, es uno de los pilares para la gestión de nuestros dispositivos, como así también a la hora de poder gestionar accesos remotos a través de Internet. El nivel criptográfico y de tunelización que nos ofrece, si sabemos configurarlo adecuadamente es de lo más robusto que se puede implementar, a su vez dentro de los entornos Linux, nos lo ofrece de forma gratuita como un recurso inmejorable para este tipo de tareas.