

RESOLUCIÓN DE PROBLEMAS EN LA SEGURIDAD INFORMÁTICA (80 HORAS)

Todos los contenidos de la presente acción formativa están directamente extraídos del módulo formativo MEO408.3: Gestión de Incidencias de Seguridad Informática del Certificado de Profesionalidad. ITCT0109: Seguridad Informática de la Familia Profesional de Informática y Comunicaciones: Sistemas y Telemática

TEORÍA: (30 HORAS)

GESTION DE INCIDENCIAS DE SEGURIDAD : 10 HORAS

- Justificación de la necesidad de gestionar incidencias de seguridad.
- Identificación y caracterización de los datos de funcionamiento del sistema.
- Sistemas de detección de intrusos:
 - Sistemas basados en equipo (HIDS)
 - Sistemas basados en red (NIDS)
 - Sistemas de prevención de intrusiones (IPS)
 - Señuelos

RESPUESTA ANTE INCIDENTES DE SEGURIDAD : 10 HORAS

- Recolección de información.
- Análisis y correlación de eventos.
- Verificación de la intrusión.
- Organismos de gestión de incidentes:
 - Nacionales IRIS-CERT, es CERT
 - Internacionales. CERT, FIRST

ANALISIS FORENSE INFORMATICO: 10 HORAS

- Objetivos de análisis forense. Principio de Lockard
- Recogida de evidencias. Principio de indeterminación
 - Evidencias volátiles
 - Evidencias no volátiles
 - Etiquetado de evidencias
 - Cadena de custodia.

- Análisis de evidencias:
 - Ficheros y directorios ocultos.
 - Información oculta en el sistema de ficheros. Slack-sàce
 - recuperación de ficheros borrados
 - Herramientas de análisis forense.
- Análisis de evidencias:
 - Desensambladores
 - Entornos de ejecución controlada

PRACTICA: (50 HORAS)

1. Planificar e implantar los sistemas de detección de intrusos según las normas de seguridad.

- Describir las técnicas de detección y prevención de intrusos, exponiendo los principales parámetros que pueden emplearse como criterios de detección.
- Determinar el número, tipo y ubicación de los sistemas de detección de intrusos, garantizando la monitorización del tráfico indicado en el plan de implantación.
- Seleccionar las reglas del sistema de detección de intrusos, en función del sistema informático a monitorizar.
- Determinar los umbrales de alarma del sistema, teniendo en cuenta los parámetros de uso del sistema.

2. Aplicar los procedimientos de análisis de la información y contención del ataque ante una incidencia detectada.

- Analizar la información de los sistemas de detección de intrusos, extrayendo aquellos eventos relevantes para la seguridad.
- Analizar los indicios de intrusión, indicando los condicionantes necesarios para que la amenaza pueda materializarse.
- Clasificar los elementos de las alertas del sistema de detección de intrusiones, estableciendo las posibles correlaciones existentes entre ellos, distinguiendo las alertas por tiempos y niveles de seguridad.

3. Analizar el alcance de los daños y determinar los procesos de recuperación ante una incidencia detectada.

- Describir las fases del plan de actuación frente a incidentes de seguridad, describiendo los objetivos de cada fase.
- Indicar las fases del análisis forense de equipos informáticos, describiéndolos objetivos de cada fase.
- Clasificar los tipos de evidencias del análisis forense de sistemas, indicando sus características, métodos de recolección y análisis.