FORMACIÓN

UC0488_3

DETECTAR Y RESPONDER ANTE INCIDENTES DE SEGURIDAD

MF0488_3

GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

Capacidades y Criterios de Realización

* C1: Planificar e implantar los sistemas de detección de intrusos según las normas de seguridad.
* C2: Aplicar los procedimientos de análisis de la información y contención del ataque ante una incidencia detectada.
* C3: Analizar el alcance de los daños y determinar los procesos de recuperación ante una incidencia detectada.

C1 - Teoría

* CE1.1 Describir las técnicas de detección y prevención de intrusos, exponiendo los principales parámetros que pueden emplearse como criterios de detección.
* CE1.2 Determinar el número, tipo y ubicación de los sistemas de detección de intrusos, garantizando la monitorización del tráfico indicado en el plan de implantación.
* CE1.3 Seleccionar las reglas del sistema de detección de intrusos, en función del sistema informático a monitorizar.
* CE1.4 Determinar los umbrales de alarma del sistema, teniendo en cuenta los parámetros de uso del sistema.
* CE1.5 Elaborar reglas de detección, partiendo de la caracterización de las técnicas de intrusión.

C1 - Práctica

* CE1.6 A partir de un supuesto práctico convenientemente caracterizado en el que se ubican servidores con posibilidad de accesos locales y remotos:
  * - Instalar y configurar software de recolección de alarmas.
  * - Configurar diferentes niveles de recolección de alarmas.
* CE1.7 En una colección de supuestos prácticos en un entorno controlado de servidores en varias zonas de una red departamental con conexión a Internet:
  * - Decidir áreas a proteger.
  * - Instalar un sistema de detección de intrusos.
  * - Definir y aplicar normas de detección.
  * - Verificar funcionamiento del sistema atacando áreas protegidas.
  * - Elaborar un informe detallando conclusiones.

C2 - Teoría

* CE2.1 Analizar la información de los sistemas de detección de intrusos, extrayendo aquellos eventos relevantes para la seguridad.
* CE2.2 Analizar los indicios de intrusión, indicando los condicionantes necesarios para que la amenaza pueda materializarse.
* CE2.3 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.
* CE2.5 Establecer procesos de actualización de las herramientas de detección de intrusos para asegurar su funcionalidad según especificaciones de los fabricantes.

C2 - Práctica

* CE2.4 A partir de un supuesto práctico, en el que realizan intentos de intrusión al sistema informático:
  * - Recopilar las alertas de los sistemas de detección de intrusiones.
  * - Relacionar los eventos recogidos por los sistemas de detección de intrusiones.
  * - Determinar aquellas alertas significativas.
  * - Elaborar el informe correspondiente indicando las posibles intrusiones y el riesgo asociado para la seguridad del sistema informático de la organización.

C3 -Teoría

* CE3.1 Describir las fases del plan de actuación frente a incidentes de seguridad, describiendo los objetivos de cada fase.
* CE3.2 Indicar las fases del análisis forense de equipos informáticos, describiendo los objetivos de cada fase.
* CE3.3 Clasificar los tipos de evidencias del análisis forense de sistemas, indicando sus características, métodos de recolección y análisis.
* CE3.4 Describir las distintas técnicas para análisis de programas maliciosos, indicando casos de uso.
* CE3.6 Estandarizar métodos de recuperación de desastres de equipos informáticos ante la detección de intrusiones.

C4. Práctica

* CE3.5 En un supuesto práctico, en el que se ha producido una intrusión en un sistema informático:
  * - Realizar la recogida de evidencias volátiles.
  * - Realizar la recogida de evidencias no volátiles.
  * - Análisis preliminar de las evidencias.
  * - Análisis temporal de actividad del sistema de ficheros.
  * - Elaborar el informe final, recogiendo las evidencias encontradas, las posibles vulnerabilidades utilizadas para la intrusión y la actividad realizada por el intruso que ha sido detectada en el sistema.

Contenidos

1. Sistemas de detección y prevención de intrusiones (IDS/IPS)
2. Implantación y puesta en producción de sistemas IDS/IPS
3. Control de código malicioso
4. Respuesta ante incidentes de seguridad
5. Proceso de notificación y gestión de intentos de intrusión
6. Análisis forense informático