



Test de conocimientos (Puntuación máxima 5)

Test de 20 preguntas. Cada pregunta correcta suma 0,25 puntos, las preguntas incorrectas restan 0,08 puntos. Las preguntas no contestadas ni suman ni restan.

PTP1. Decálogo de seguridad. (Puntuación máxima 2p, Cada pregunta 0.5p)

P1: Política de firewall.

Indica la política de actuación del firewall.

P2: Navegación por internet.

Explicar razonadamente si el equipo puede navegar por Internet.

P3: Quitar la línea "ufw allow 22/tcp"

Explicar qué ocurre si se elimina tal línea, si afecta al funcionamiento.

P4: Línea para poder servir páginas web.

Explicar la/s Línea/s para permitir el servicio de páginas web HTTP.

PTP2. Análisis de incidente de ciberseguridad.

P1: Análisis de equipo. (Puntuación máxima 1p)

Descripción de los pasos para el análisis del equipo en este caso práctico.

P2: Herramientas y técnicas. (Puntuación máxima 0.5p)

Herramientas y técnicas para llevar a cabo este análisis.

P3: Medidas preventivas. (Puntuación máxima 0.5p)

Medidas para evitar incidentes similares.

PTP3. Plan de respuestas ante incidentes.

P1: Playbook. (Puntuación máxima 0.4p)

Explicar qué es el playbook de un incidente.

P2: Fases de actuación ante incidentes reconocidos. (Puntuación máxima 0.6p)

Descripción de las fases tras la identificación del incidente.