SEGURIDAD EN REDES DE COMUNICACIONES
5º curso Ing. Telecomunicación

APELLIDOS.....

NOMBRE.....

DNI.....

No rellenar este espacio

LEEME:

- **El examen consta de 7 cuestiones de teoría y 5 cuestiones de prácticas.**
- **La duración del examen es de 3 horas.**
- **<u>No se admitirá ninguna respuesta a lápiz</u>.**

TEORIA [10 puntos]

1. [1 punto] Supongamos que alguien sugiere la siguiente manera de confirmar que dos de vosotros estáis en posesión de la misma clave secreta. Crea una secuencia aleatoria de bits del mismo tamaño que la clave, aplícale el XOR con la clave y envía el resultado por el canal. Tu receptor hace XOR del bloque entrante con la clave (que debería ser la misma que la tuya) y envía el resultado de vuelta. Observas lo que te devuelve y si coincide con tu secuencia aleatoria entonces has verificado que tu receptor tiene la misma clave secreta que tú, aunque ninguno ha transmitido la clave. ¿Hay algún defecto en este esquema?
2. [1,5 punto] De un ejemplo de amenaza procedente de personas explicando en qué consiste.
3. [1,5 punto] Compare los métodos de cifrado AES y RSA indicando sus características más relevantes.
4. [1,5 puntos] Expllique los diferentes métodos que existen para crear un autentificador y aporte un ejemplo de cada uno de ellos.
5. [1,5 punto] Indique, ayudándose de un dibujo o esquema, en qué consiste una firma digital y un certificado digital.
6. [1,5 puntos] Explique de forma clara y concisa la finalidad de los protocolos que conforman el SSL.
7. [1,5 punto] Compare los modos de funcionamiento tunel y transporte en ESP y AH.

PRACTICAS [10 puntos]

1. [2,5 puntos] Indique si NMAP trabaja como cliente y servidor, y dos servicios que ofrezca.
2. [2,5 puntos] Interprete estas reglas de Nessus: reject 192.168.4.254/32, accept 192.168.4.0/24, default reject.
3. [2,5 puntos] Dibuje un esquema de autenticación con EAP y RADIUS.
4. [2,5 puntos] Explique el proceso de obtención e instalación de un certificado de una CA para un servidor Apache en tres lineas.
5. [2,5 puntos] Explique brevemente porqué la generación manual de claves, al configurar un tunel IPSec, es más débil ante un intruso con cierto acceso al sistema.