**sese**

**ABANS DE COMENÇAR**

1. **Ves a menú Fitxer i sel·lecciona l'opció Fes una còpia… i desa-la a la carpeta corresponent dins de la professora té compartida amb tu.**
2. **Reanomena el fitxer de la següent manera:**

**"SMX MP05 UF2 NF2 A1.3 Seguretat WiFi Nom Cognoms"**

1. **Senyala la resposta correcta:**
   * Quina tecnologia de protecció de xarxes WiFi és més segura?
     1. WPA2-TKIP
     2. WPA-AES
     3. WEP
     4. **WPA2-AES**
   * En quant temps pot un atacant obtenir la contrasenya d’una xarxa WiFi basada en WEP? (escollir l’opció que requereix menys temps per part de l’atacant)
     1. **Menys d’un minut**
     2. Entre 1 i 30 minuts
     3. Entre 30 i 60 minuts
     4. Més de 60 minuts
   * En què consisteix l’atac sobre clients WiFi conegut com punt d’accés fals o evil twin?
     1. Introduir un punt d’accés WiFi no autoritzat a la xarxa de l’empresa
     2. **Suplantar una xarxa WiFi utilitzant el mateix nom de xarxa i configuració**
     3. Atacar un punt d’accés WiFi per modificar la seva configuració
     4. Fer ús de la xarxa WiFi d’un tercer sense autorització
   * Quin dels següents mecanismes de seguretat de xarxes WiFi està desaconsellat?
     1. **Filtrat per adreça MAC**
     2. Reduir la intensitat i abast de la senyal
     3. Ocultació del nom de la xarxa WiFi
     4. Sistema de detecció d’intrusos inalàmbrics (WIDS)
2. **Què creieu que podria ser un mètode de seguretat: activar o desactivar el DHCP d’un punt d’accés? Justifica la teva resposta.**

**Desactivar. Perque al final et pot entrar una persona no autoritzada i aixi podem evitar-ho.**

1. **Si tenim un router Wi-Fi amb IP: 192.168.0.1, per qüestions de seguretat, modificaríeu la IP del router, o bé, aquesta no es pot canviar?**

**Si es pot canviar, garanteix la seguretat de persones no autoritzades a la nostra xarxa.**

1. **Si el router ve amb un nom d’usuari i una contrasenya per poder gestionar l’administració d’aquest dispositiu, creieu que seria millor deixar les dades per defecte o bé modificar-les?**

**Modificar-les. Perquè si es un usuari o contrasenya predeterminats qualsevol persona que sàpiga una mica podria entrar.**

1. **Investigueu els següents sistemes de seguretat:** 
   * **OSA (*Open System Authentication*) Permet la conexió sense autentificació.**
   * **CNAC (*Close Network Access Control*) Restringeix l'accés a dispositius autoritzats.**
   * **SKA (*Shared Key Authentication*) Té una clau compartida per poder veure tots els dispositius autoritzats.**
   * **SSID (*Service Set Identifier*) Identificador de xarxa que diferencia una de l’altra.**
2. **Busca per Internet alguna notícia sobre la vulnerabilitat de la wifi (WPA2) que ha passat al 2020 i fes-ne un resum amb les teves paraules.**

[Noticia](https://www.forbes.com/sites/kateoflahertyuk/2020/11/29/iphone-weak-security-wi-fi-warning-heres-what-it-means/)

**Diferents dispositius estan afectats per una fallida del sistema de seguretat que comprometen els documents i les dades de les persones afectades. Apple va fer una actualització per poder combatre aquest cyberattack i han recomanat mantenir tots els dispositius actualitzats i també els routers.**

1. **Cerca per Internet 3 eines que descobreixin contrasenyes i comenta-les amb les teves paraules. Digues quin tipus de xarxes descobreixen, si l'autenticació es per WEP, WPA, WPA2, etc.**

**Wireshark: Analitza el tràfic de la xarxa.**

**Aircrack-ng: Avalua la seguretat de la xarxa.**

**Hashcat: Descobreix contrasenyes emmagatzemades.**