**WLAN – Ataque y defensa en redes Wi-Fi**

Para la realización de la práctica, haremos uso de un **diccionario de clave**s como recurso para realizar la búsqueda de la contraseña a base de fuerza bruta.

Usaremos *xato-net-10-million-passwords-1000000.txt*

Una vez hemos capturado el tráfico en modo promiscuo (como es el caso del fichero utilizado, donde ya hemos encontrado el handshake), localizamos la **dirección MAC del punto de acceso** a atacar (en nuestro caso el dispositivo Xiaomi): **04:b1:67:3d:c5:90**

A close up of a computer screen

Description automatically generated

*Tramas de transmisión de clave Wi-Fi*

*A screenshot of a computer

Description automatically generated*

*MAC del AP*

Ejecutamos la herramienta **aircrack-ng** con la captura de tráfico y tras un tiempo de ejecución, si está en el diccionario, obtenemos la clave WPA2 utilizada en esa red Wi-Fi.

A black screen with white text

Description automatically generated

*La clave es “Pringles”*

Una vez tenemos la clave, pasaremos a desencriptar los mensajes, volviendo a la captura y buscando en los ajustes del protocolo 802.11, introducimos la clave para desencriptar los mensajes.

A screenshot of a computer

Description automatically generated

**La página web a la que accede es** [***http://demo.horde.org/login.php***](http://demo.horde.org/login.php)

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generatedAl igual que con la información de la página web a la que se ha accedido, podemos seguir indagando entre las tramas y encontrar la **información de inicio de sesión**.

A screenshot of a computer

Description automatically generated

**Usuario: guest / Contraseña: guest**

Podemos **evitar** todo esto cifrando los datos con una clave de sesión con más caracteres, pseudoalteatorios y con palabras de uso no frecuente.