Rapport d’avancement Jalon 2

### **Configuration de la borne Linksys pour l'épreuve**

## 1. Configuration matérielle

La borne utilisée pour cette épreuve était un modèle **Linksys** compatible avec le protocole WPS et offrant des options de configuration avancées. Voici les étapes techniques détaillées :

### a. Accès à l’interface d’administration

1. Connexion à la borne avec l’adresse IP 192.168.1.1
2. Authentification sur l’interface avec les identifiants administrateurs par défaut.

### b. Création du réseau Wi-Fi caché

1. Accès au menu **Wireless Settings** > **Basic Wireless Settings** :
   * **SSID** : Configuration du nom du réseau, SSIDCaché.
   * **SSID Broadcast** : Désactivation pour rendre le réseau non visible aux scanners classiques.
2. **Canal** :
   * Réglage manuel sur un canal peu encombré, le 6, pour éviter les interférences.
3. **Puissance du signal** :
   * Ajustée à 50 % dans les paramètres avancés pour limiter la portée excessive tout en restant accessible aux participants.

### c. Activation et configuration du protocole WPS

1. Accès au menu **Wireless Settings** > **Wireless Security (WPS)** :
   * **Mode WPS** : Activé avec l’option *PIN* comme méthode d’authentification.
   * **PIN WPS** : Utilisation du PIN généré par défaut par la borne. Ce PIN a été noté et vérifié avant le déploiement pour assurer qu’il fonctionnait avec des outils d’exploitation comme reaver.
   * **Lockout WPS** : Désactivé pour permettre un nombre illimité de tentatives sur le PIN.

### d. Sécurisation du réseau

1. **Cryptage WPA2-PSK** :
   * Accès au menu **Wireless Security** :
     + **Security Mode** : WPA2-PSK (AES).
     + **Passphrase** : Une clé, ctfwifi2025, qui est ensuite hashée en ascii : 99 116 102 119 105 102 105 50 48 50 53
2. **Filtrage MAC** (désactivé pour l’épreuve) :
   * Le filtrage d’adresse MAC a été désactivé pour permettre à tous les participants de tenter une connexion après récupération des informations.

## 2. Validation des paramètres réseau

Après la configuration, des tests ont été réalisés pour valider le bon fonctionnement de la borne dans les conditions de l’épreuve :

1. **Test du réseau caché** :
   * Utilisation de l’outil **airodump-ng** pour vérifier que le SSID caché apparaissait sous forme de balises avec un nom non visible.
   * Confirmation que le réseau était identifiable via son BSSID et son canal.
2. **Test de la fonctionnalité WPS** :
   * Exploitation du PIN WPS avec reaver pour s’assurer que la borne répondait correctement aux requêtes WPS sans se bloquer.
3. **Test du mot de passe WPA2** :
   * Une fois le PIN WPS validé, extraction de la clé WPA2-PSK et connexion au réseau pour valider l’accès.

Comme prochaine épreuve, nous avons comme objectif de mettre en place le serveur FTP présentant des vulnérabilités. Pour l’instant, nous avons des difficultés pour trouver une bonne version exploitable de ce serveur.