Travaux pratiques
WiFi

Anaïs Gantet, Benoît Camredon

19 décembre 2019

Objectifs

- Savoir se connecter à
  - Un réseau ouvert
  - Un réseau `WEP`
  - Un réseau `WPA`
- Se familiariser avec la configuration de hostapd
- Casser un réseau `WEP`
- Casser un réseau `WPA`

1 Mise en place de la carte réseau

1. Branchez votre carte réseau WiFi USB et vérifiez qu'elle est bien reconnue par votre ordinateur.

2 Réseau ouvert

2.1 Mise en place d'un réseau ouvert

1. Vérifiez que votre carte réseau supporte bien le mode `AP`.
2. Créez une configuration de `hostapd` permettant la création d'un réseau ouvert.
3. Exécutez `hostapd` avec cette configuration.
4. Vérifiez que votre carte réseau est bien en mode `AP`.
5. Scannez les réseaux pour vérifier que votre réseau ouvert est bien visible. Pour cela vous pouvez utiliser divers outils : votre téléphone, `iw`, `airodump`, `kismet`…Attention vous devez utiliser une carte WiFi différente de la carte utilisée par `hostapd`. Alternez avec votre voisin pour faire cette vérification.

2.2 Connexion à un réseau ouvert

1. Listez les réseaux autour de vous en utilisant la commande `iw`.
2. Connectez-vous au réseau ouvert de votre voisin, en lui demandant son `SSID`, d'abord en utilisant la commande `iw` puis en utilisant `wpa_supplicant`.

2.3 Mise en place de services au-dessus de la connexion wifi établie

Le réseau WiFi peut être en place, cela ne veut pas dire que la connectivité fonctionne. Pour cela, il faut mettre des services au niveau IP, comme un serveur DHCP et un routeur par exemple.

1. Mettez en place un serveur DHCP sur votre machine. Vous pouvez utiliser `dnsmasq` qui est déjà installé sur votre machine.
2. Mettez en place le routage sur votre machine.

3 Réseau WEP

3.1 Mise en place d'un réseau WEP

1. Créez une configuration de `hostapd` permettant la création d'un réseau `WEP`.
2. Exécutez `hostapd` avec cette configuration.
3. Scannez les réseaux pour vérifier que votre réseau `WEP` est bien visible. Pour cela vous pouvez utiliser divers outils : votre téléphone, `iw`, `airodump`, `kismet`…Attention vous devez utiliser une carte WiFi différente de la carte utilisée par `hostapd`. Alternez avec votre voisin pour faire cette vérification.
4. Capturez les paquets d'une authentification sur un réseau `WEP` et un réseau ouvert et comparez-les.

3.2 Connexion à un réseau WEP

1. Connectez-vous au réseau `WEP` de votre voisin, en lui demandant son `SSID` et son mot de passe en utilisant `wpa_supplicant`.

3.3 Cassage d'un réseau WEP

1. Demandez à votre voisin de changer son mot de passe et générez du trafic sur le réseau `WEP` en utilisant `aireplay-ng`. Attention un client doit déjà être présent sur le réseau pour rejouer son trafic.
2. Une fois que suffisamment de trafic a été généré, casser la clé du réseau `WEP` avec `aircrack-ng`.

4 Réseau WPA-PSK

4.1 Mise en place d'un réseau WPA-PSK

1. Créez une configuration de `hostapd` permettant la création d'un réseau `WPA-PSK` (TKIP ou CCMP).
2. Exécutez `hostapd` avec cette configuration.
3. Scannez les réseaux pour vérifier que votre réseau `WPA` est bien visible. Pour cela vous pouvez utiliser divers outils : votre téléphone, `iw`, `airodump`, `kismet`…Attention vous devez utiliser une carte WiFi différente de la carte utilisée par `hostapd`. Alternez avec votre voisin pour faire cette vérification.
4. Capturez les paquets d'une authentification sur un réseau `WEP`, ouvert, `WPA-TKIP` et `WPA-CCMP`. Comparez-les.

4.2 Connexion à un réseau WPA-PSK

1. Connectez-vous au réseau WPA de votre voisin, en lui demandant son `SSID` et son mot de passe en utilisant `wpa_supplicant`.

4.3 Cassage d'un réseau WPA-PSK

1. Demandez à votre voisin de changer son mot de passe (Utiliser un mot de passe appartenant au dictionnaire…). Forcez la désauthentification d'un client connecté à ce réseau en utilisant `aireplay-ng`.
2. Capturez le *4 way-handshake* et cassez le mot de passe `WPA` du réseau en utilisant le dictionnaire fourni.

5 Pour aller plus loin

5.1 Filtrage d'adresses MAC

1. Mettez en place un nouveau réseau WiFi du niveau de sécurité de votre choix.
2. Configurez `hostapd` pour mettre en place un filtrage de MAC et faites en sorte que
   — Votre voisin le plus proche puisse se connecter à votre AP
   — Le reste de la promo ne le puisse pas.
3. Reconfigurez votre filtrage pour ne bloquer l'accès à votre AP qu'à votre plus proche voisin.

5.2 Masquage du SSID

Il est possible aux AP de ne pas diffuser leur SSID sur le réseau.

1. Mettez en place un nouvel AP avec le niveau de sécurité de votre choix.

2. Configurez `hostapd` de sorte que cet AP ne diffuse plus son SSID.
3. Demandez à votre voisin de scanner le réseau et vérifiez qu'il ne voit pas le SSID de votre AP.
4. Communiquez ensuite le SSID à votre voisin (et autres informations de connexion si nécessaire) et dites lui de s'y connecter, pour vérifier que l'AP existe bien.