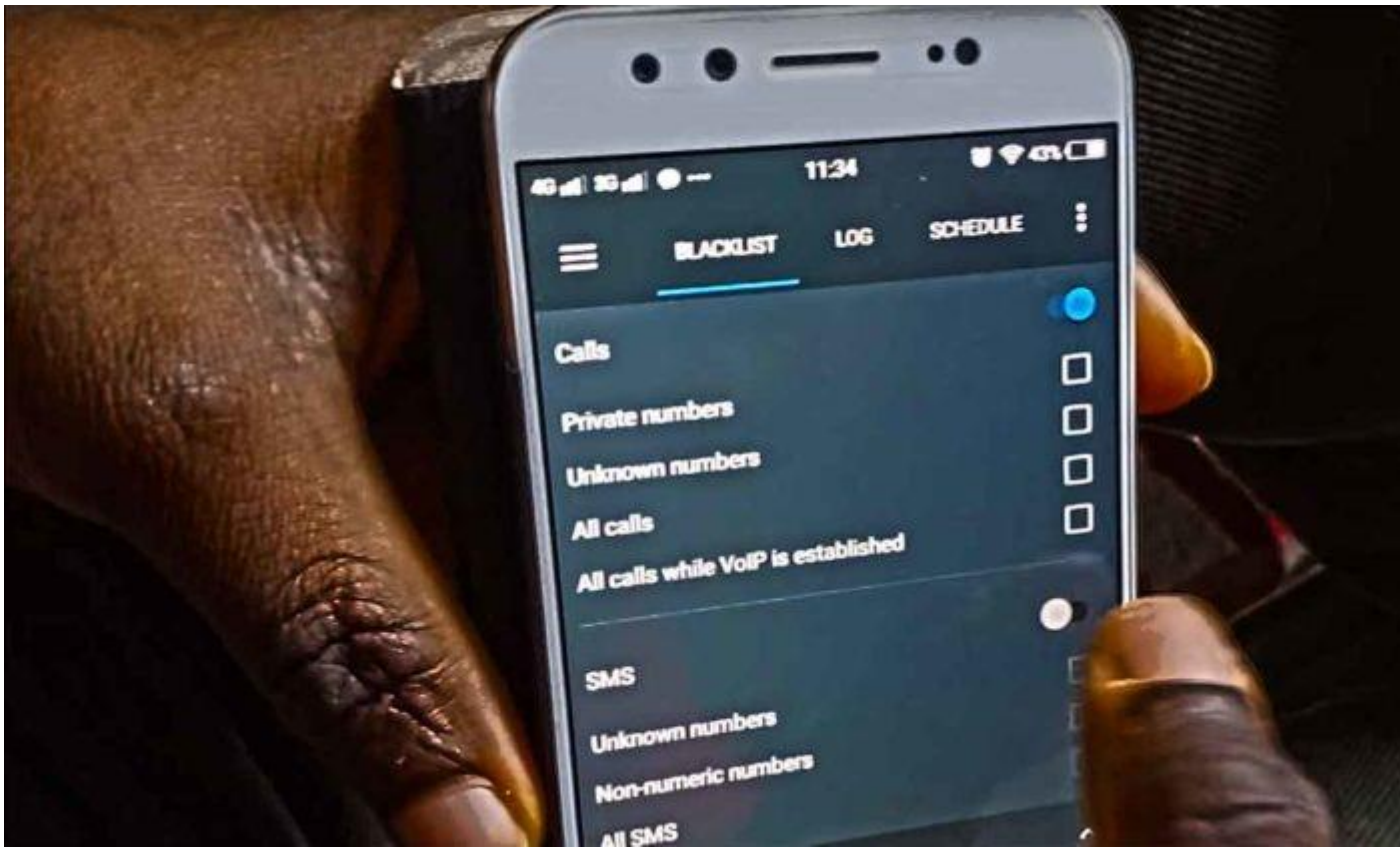
Un Téléphone

L'usage du téléphone par les hommes et les femmes

Guide pour pirater un portable par bluetooth

Publié le 19 septembre 2019 par Agnès Michaud



Sommaire

Donner le blues à votre téléphone

Le Bluetooth est une technologie merveilleuse. Elle vous permet de vous connecter à des écouteurs, un casque, de vous synchroniser avec votre voiture ou votre ordinateur, et bien plus encore. **Mais le Bluetooth est également l'une des principales failles de sécurité par lesquelles les pirates peuvent accéder à votre téléphone**.

Avant d'examiner les différentes failles possibles et les outils adéquats, attardons-nous sur ce qu'est vraiment le Bluetooth, principalement sur un téléphone mobile.

Les bases du Bluetooth : En quoi pirater le bluetooth peut-il être dangereux ?

Le Bluetooth est un protocole universel de communication à faible puissance, dans un champ fonctionnant entre 2,4 – 2,485 GHz et en utilisant un spectre étalé.

Le Bluetooth effectue un saut de fréquence de 1.600 sauts par seconde. Il a été développé en 1994 par Ericsson Corp en Suède et nommé d'après le roi Harald Bluetooth danois du 10ème siècle (la Suède et le Danemark ne formaient qu'un seul pays à cette époque).

La spécification minimale pour la portée Bluetooth est de **10 mètres**, mais il n'y a aucune limite à la portée que les fabricants peuvent mettre en œuvre dans leurs appareils. De nombreux appareils ont des portées allant jusqu'à 100 mètres. Avec des antennes spéciales, nous pouvons étendre cette portée à beaucoup plus loin.

Lorsque deux périphériques Bluetooth se connectent, on parle d'**appairage**. Deux appareils Bluetooth peuvent facilement se connecter l'un à l'autre. Tout périphérique Bluetooth détectable transmet les informations suivantes à son interlocuteur:

- Nom
- Catégorie
- Liste des services
- Informations techniques

Lorsque les deux appareils s'accouplent, ils échangent une clé secrète dite « clé de liaison pré-partagée ». Ils stockent cette clé secrètement pour s'identifier automatiquement l'un à l'autre lors des futurs appariements.

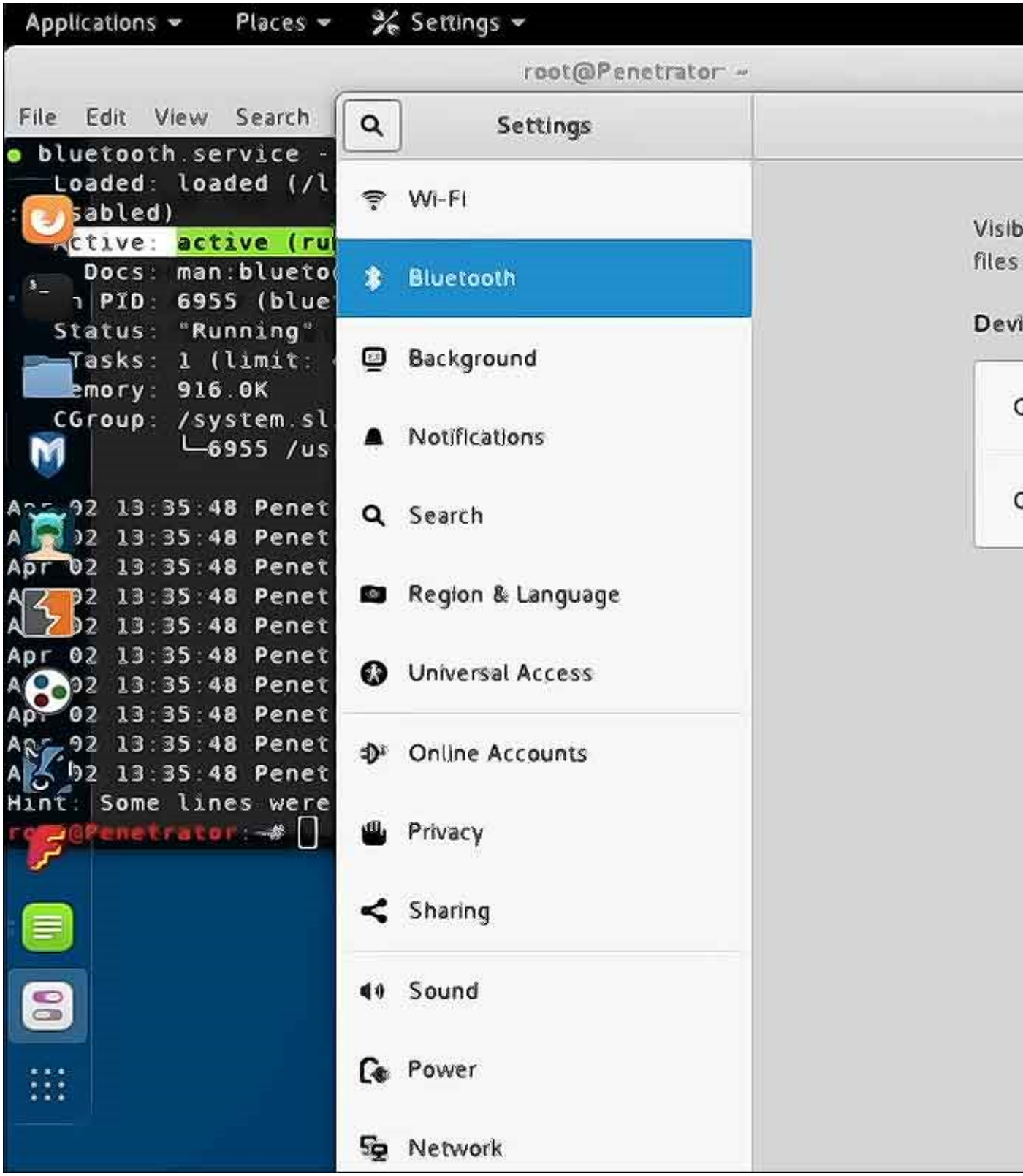
Chaque appareil Bluetooth possède un identificateur unique de 48 bits (une adresse de type MAC) ainsi qu'un nom attribué par son fabricant.

Quelles sont les sécurités du mode Bluetooth ?

La sécurité Bluetooth est basée sur quelques techniques. Deux sont principalement à connaître quand on cherche à pirater un portable par bluetooth:

> D'abord, **le saut de fréquence**. Les deux apparails appairés connaissent tous les deux l'algorithme de saut de fréquence, mais pas les étrangers.

> Deuxièmement, **une clé pré-partagée** échangée lors de l'appariement est utilisée pour l'authentification et le chiffrement (128 bits).



→ Agrandir l'image

Il existe cinq types d’attaques de base basées sur le Bluetooth :

1. Bluejacking

Le bluejacking est une attaque relativement inoffensive lors de laquelle un pirate envoie des messages non sollicités à des appareils détectables dans la zone.

L’attaque est menée en exploitant la fonction de carte de visite électronique Bluetooth comme support de message. Le pirate informatique ne peut accéder à aucune information ni intercepter aucun message. Vous pouvez vous protéger de ces spams non sollicités en mettant votre téléphone en mode « caché », en mode « invisible » ou en mode « non détectable ».

Le Bluejacking n’est donc ni plus ni moins qu’une méthode de piratage qui permet à un individu d’envoyer des messages anonymes à un appareil Bluetooth dans un certain rayon. Tout d’abord, le pirate analyse son environnement à l’aide d’un appareil compatible Bluetooth, à la recherche d’autres appareils. Ensuite il envoie un message non sollicité aux périphériques détectés.

Le **bluejacking** est aussi connu sous le nom de **bluehacking**.

Le Bluejacking exploite une fonction Bluetooth de base qui permet aux appareils d’envoyer des messages à des contacts à portée. Il ne permet pas le détournement complet de l’appareil. Le pirate ne peut qu’envoyer des messages non sollicités. Le détournement ne se produit pas réellement parce que l’agresseur n’a jamais le contrôle de l’appareil de la victime. Au pire, le bluejacking est juste une sorte de SPAM.

Le Bluesnarfing et le bluebugging, quant à eux, sont des attaques réelles qui peuvent entraîner une perte de contrôle totale de l’utilisateur.

2. Bluesnarfing

Le Bluesnarfing est bien pire que le bluejacking car il permet à un hacker d’accéder à certaines de vos informations privées.

Dans ce type d’attaque, un pirate informatique utilise un logiciel spécial pour demander des informations à un appareil via le profil Bluetooth *OBEX push*. Cette attaque peut être effectuée contre des périphériques en mode invisible, mais cela demande un temps considérable pour y parvenir sans connaître le nom du périphérique.

En résumé, le **Bluesnarfing** est donc un piratage de périphérique effectué lorsqu'un périphérique sans fil compatible Bluetooth reste constamment en mode découverte. Il permet aux pirates d'accéder à distance aux données des périphériques Bluetooth, telles que le calendrier, la liste de contacts, les emails et les textos de l'utilisateur. Cette attaque est perpétrée à l'insu de la victime.

Les périphériques Bluetooth sont vulnérables aux attaques de bluesnarfing lorsqu'ils sont en mode découvrable car les pirates peuvent répondre aux requêtes d'autres périphériques Bluetooth, obtenant ainsi un accès non autorisé aux informations.

La plupart des modes de découverte des téléphones mobiles sont activés par défaut. A moins que le mode ne soit désactivé, un dispositif est donc par défaut sensible aux attaques de bluesnarfing.

La seule façon de protéger complètement un appareil sans fil contre le bluesnarfing est de **désactiver le Bluetooth**. De même, le fait de garder son téléphone **en mode invisible** offre une certaine protection.

3. Bluebugging

Lorsque votre téléphone est en mode découverte, un pirate informatique peut utiliser le même point d'entrée que le bluejacking et le bluesnarfing pour prendre votre téléphone sous son contrôle. La plupart des téléphones ne sont pas vulnérables au bluebugging, mais certains des premiers modèles **dont le firmware est obsolète** peuvent être piratés de cette façon.

Un processus de transfert électronique est alors utilisé pour ajouter l'appareil du pirate en tant qu'appareil de confiance à l'insu de l'utilisateur. Cet état de confiance peut ensuite être utilisé pour prendre le contrôle du téléphone et des données qu'il contient.

Concrètement, le **Bluebugging** est donc une technique qui permet aux hackers expérimentés d'accéder aux commandes mobiles d'un appareil Bluetooth qui reste en en mode découverte.

Parce que le mode découvrable est un paramètre par défaut, la plupart des téléphones mobiles sont automatiquement vulnérables aux attaques de bluebugging. Certains outils – tels que *RedFang* et *BlueSniff* – permettent même aux pirates d'infiltrer des périphériques Bluetooth qui ne sont pas en mode découverte.

Les périphériques sont alors vulnérables à un ou plusieurs des scénarios suivants :

- Le téléphone portable peut être commandé à distance, ce qui permet aux pirates d'intercepter ou de réacheminer les communications.
- Les pirates informatiques peuvent envoyer et lire les SMS.
- Les pirates informatiques peuvent passer ou surveiller des appels téléphoniques.
- Les pirates informatiques peuvent faire tout ce qui précède sans laisser de trace.

4. Blueprinting

Le Blueprinting est un processus d'empreinte.

5. Bluesmack

Le Bluesmack est une attaque DoS contre un appareil Bluetooth.

Les outils pour pirater le Bluetooth de quelqu'un

Utiliser l'OS Kali (Linux)

→ Téléchargement de la version Kali de LInux

Kali est un système d'exploitation Linux. Il s'agit de la plus récente et la plus grande version du très populaire test de pénétration ***Backtrack Linux***.

Les créateurs de Backtrack ont gardé Kali dans un format très similaire à Backtrack.

Kali a été remanié pour devenir le meilleur et le plus riche des OS dédiés au hacking éthique. Vous trouvez sur cette plateforme des tests de sécurité faciles à utiliser, et des outils puissants pour tester et sécuriser votre système réseau.

Kali inclut plus de 300 outils de tests de sécurité classés par menus. Cela vous permet d'utiliser des outils et des techniques similaires à ceux qu'un hacker utiliserait pour tester la sécurité de votre ordinateur. Le but est de trouver et de corriger ces problèmes avant qu'un vrai hacker ne les trouve.

Les pirates informatiques exécutent généralement une combinaison d'étapes lorsqu'ils attaquent un réseau:

- Vérifier la cible en utilisant plusieurs sources de renseignements.
- Scanner et cartographier le réseau.
- Exploiter les trous d'attaque trouvés pendant le balayage.
- Élévation des privilèges – Éléver un accès inférieur au niveau racine ou au niveau système.
- Maintien de l'accès – Utiliser des techniques comme les portes dérobées pour conserver l'accès au réseau.
- Couvrir ses traces – Effacer les logs et masquer l'intrusion.

Les différents outils intégrés dans Kali pour pirater le Bluetooth

Plusieurs outils de piratage Bluetooth sont intégrés à Kali. Pour les trouver, il suffit de se rendre dans *Applications -> Kali Linux -> Wireless Attacks -> Bluetooth Tools*.

Là, nous trouvons plusieurs outils pour attaquer un réseau Bluetooth. Examinons-les brièvement:

- **Bluelog** : Un outil d'étude. Il scanne la zone pour trouver les périphériques découvrables et les enregistre ensuite dans un fichier.
- **Bluemahoho** : Une suite d'outils basée sur une interface graphique pour tester la sécurité des périphériques Bluetooth.
- **Blueranger** : Un script Python simple qui utilise les pings i2cap pour localiser les périphériques Bluetooth et déterminer leurs distances approximatives.
- **Btscanner** : Cet outil basé sur une interface utilisateur graphique recherche les périphériques détectables à portée de main.
- **Redfang** : Cet outil permet de **trouver un périphérique Bluetooth caché**.
- **Spooftooph** : il s'agit d'un outil de spoofing Bluetooth.
- **Bettercap** : Bettercap est le successeur d'Ettercap et comporte des modules d'attaque pour différents types de technologies radio et réseau, dont le Bluetooth. Précisons cependant que Bettercap fait beaucoup plus que du simple piratage Bluetooth. Bettercap peut traquer et attaquer des réseaux Wi-Fi, et par défaut, commence à énumérer les périphériques sur n'importe quel réseau sur lequel vous vous trouvez. Cette capacité est bien utile pour identifier et balayer des appareils Bluetooth.

Bettercap

→ Bettercap site officiel

Bettercap est livré avec la suite *Bluetooth Low Energy* qui nous permet de faire beaucoup plus que regarder les appareils Bluetooth à proximité.

Avec lui, nous pouvons rechercher l'adresse MAC de n'importe quel appareil à portée, puis utiliser cette adresse MAC pour nous connecter à l'appareil et obtenir des informations à son sujet.

Enfin, nous pouvons écrire des données sur le périphérique pour essayer de l'exploiter, comme une balise pour suivre le périphérique dans le temps même s'il change son adresse MAC.

Tous les appareils Bluetooth peuvent être découverts avec Bettercap. De nombreux fabricants ne choisissent pas de profiter de la sécurité des périphériques comme la randomisation des adresses MAC, ce qui fait que leurs périphériques Bluetooth diffusent la même adresse MAC partout où ils vont. Cela les rend très faciles à suivre.

→ Les possibilités offertes par Bettercap

L’information est le premier élément de toute attaque. Pour commencer, nous devrons connaître le fabricant de l’appareil afin d’acquérir des connaissances comme son code PIN d’appairage par défaut.

Une fois que nous avons identifié le modèle spécifique derrière la radio Bluetooth, nous pouvons commencer à rechercher des informations spécifiques qui pourraient être utilisées pour **détourner l’appareil par Bluetooth**.

Lors du balayage d’un périphérique Bluetooth, nous pouvons apprendre des informations que nous ne devrions pas savoir. Nous pouvons déterminer:

- la version du système d’exploitation de l’appareil cible,
- le nom de l’appareil,
- le fabricant,
- et même des détails comme le niveau actuel de la batterie.

Si nous apprenons qu’un appareil exécute un vieux logiciel, il devient beaucoup plus facile de rechercher les vulnérabilités à exploiter. La première étape consiste à découvrir l’appareil et à le scanner pour en savoir plus à son sujet.

Pour cela, commencez par faire une installation complète de Kali Linux. Bettercap peut être facilement installé sur plusieurs plates-formes, mais le module Bluetooth ne fonctionne pas sur MacOS.

→ Installer Bettercap

Si vous avez une version entièrement mise à jour de Kali, vous pouvez exécuter **apt install bettercap** pour installer Bettercap et les dépendances requises.

Si vous êtes sur un autre système Linux, vous pouvez **installer Bettercap** en exécutant les commandes suivantes dans une nouvelle fenêtre de terminal.

```
apt install golang
go get github.com/bettercap/bettercap
cd $GOPATH/src/github.com/bettercap/bettercap
make build
sudo make install
```

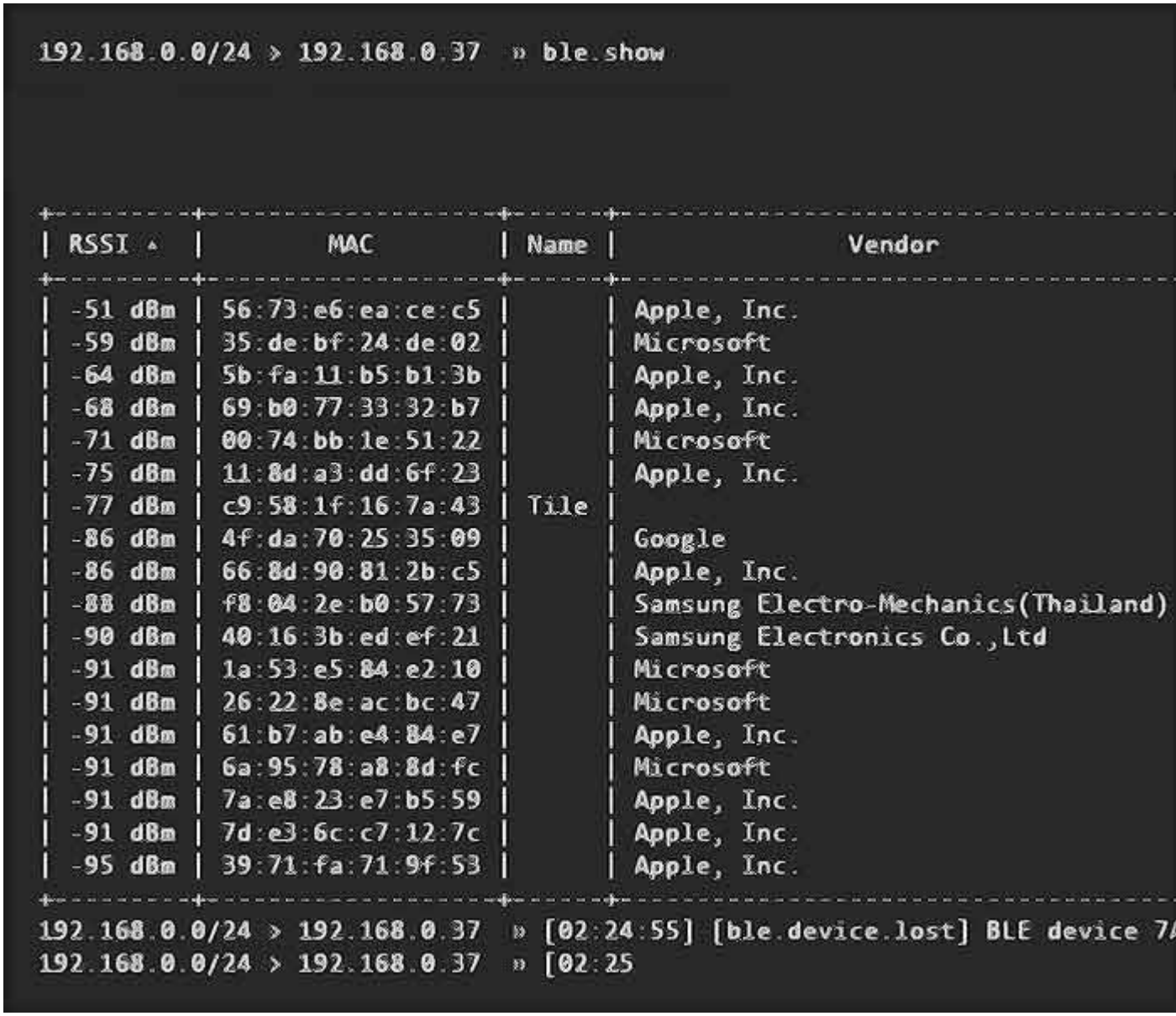
Pour démarrer Bettercap, vous pouvez simplement exécuter **sudo bettercap** dans une fenêtre de terminal. Le module réseau démarre par défaut et commence à détecter passivement les périphériques sur le même réseau. Plutôt cool ! Si nous

voulons voir la liste la plus à jour des périphériques que nous avons identifiés, nous pouvons la voir en tapant **net.show** et en appuyant sur Entrée.

→ Exécutez le module de Sniffing Bluetooth

Commençons la découverte Bluetooth ! Pour commencer, tapez **ble.recon on** et appuyez sur Entrée.

Après quelques secondes, la liste est longue. Dans un café même à 2 heures du matin, vous pouvez identifier de nombreux appareils. Pour voir les appareils que vous avez découverts, tapez **ble.show** et appuyez sur Retour.



Après avoir identifié un appareil intéressant, nous pouvons utiliser Bettercap pour l’interroger plus avant. La clé ici est de connaître l’adresse MAC de la cible.

Sur la base de l'analyse ci-dessus, le périphérique avec le signal le plus fort est un périphérique Apple dont l'adresse MAC est 56:73:e6:ea:ea:ce:c5. Nous pouvons diriger un scan de ce périphérique en tapant la commande **ble.enum 56:73:e6:ea:ea:ce:c5** pour énumérer les détails du périphérique.

A lire aussi sur notre blog :

→ la technique de spoofing MAC pour pirater Whatsapp

Un autre outil pour pirater un portable par Bluetooth

Un logiciel pour téléphone portable

Deux logiciels se distinguent pour pirater le Bluetooth d'un téléphone.

L'un d'entre eux localisera silencieusement le téléphone et enregistrera secrètement ses communications écrites (SMS, réseaux sociaux, keylogger, mots de passe, historiques, etc.). Il s'agit de cette application téléphonique :

→ L'appli spécialisée dans les messages et la localisation

Il vous faudra l'installer dans le téléphone portable.

L'autre application est la seule à proposer un enregistrement des communications téléphoniques, soit en direct, soit après enregistrement sur un serveur cloud. Cette appli peut également suivre à distance le téléphone et enregistrer ses textos. Il s'agit de celle-là :

→ L’appli spécialisée dans l’écoute des conversations