Intro to Wi-Fi Hacking

Capture, Cracking, & Scanning of Wireless Networks

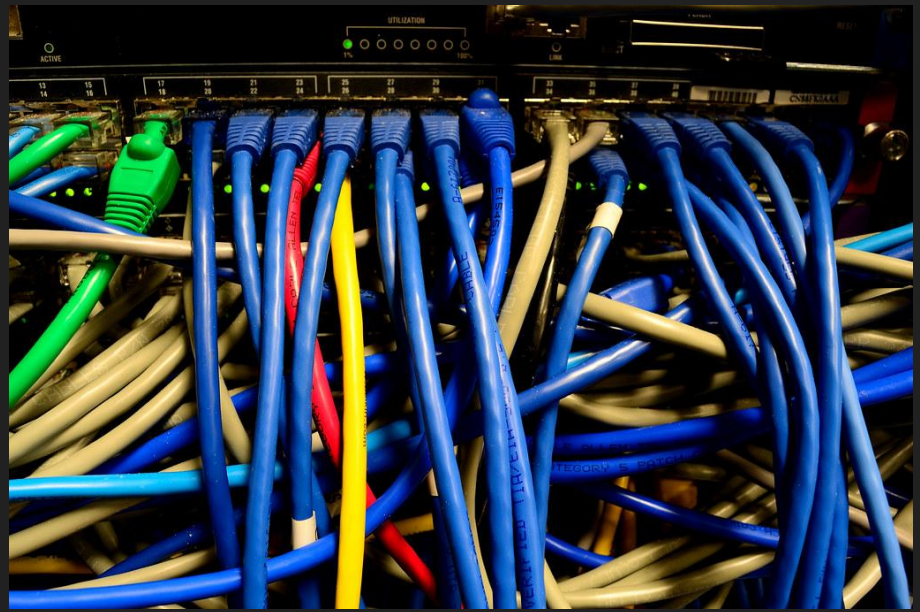
By Kody Kinzie, Security Researcher at Varonis

What are we doing today:

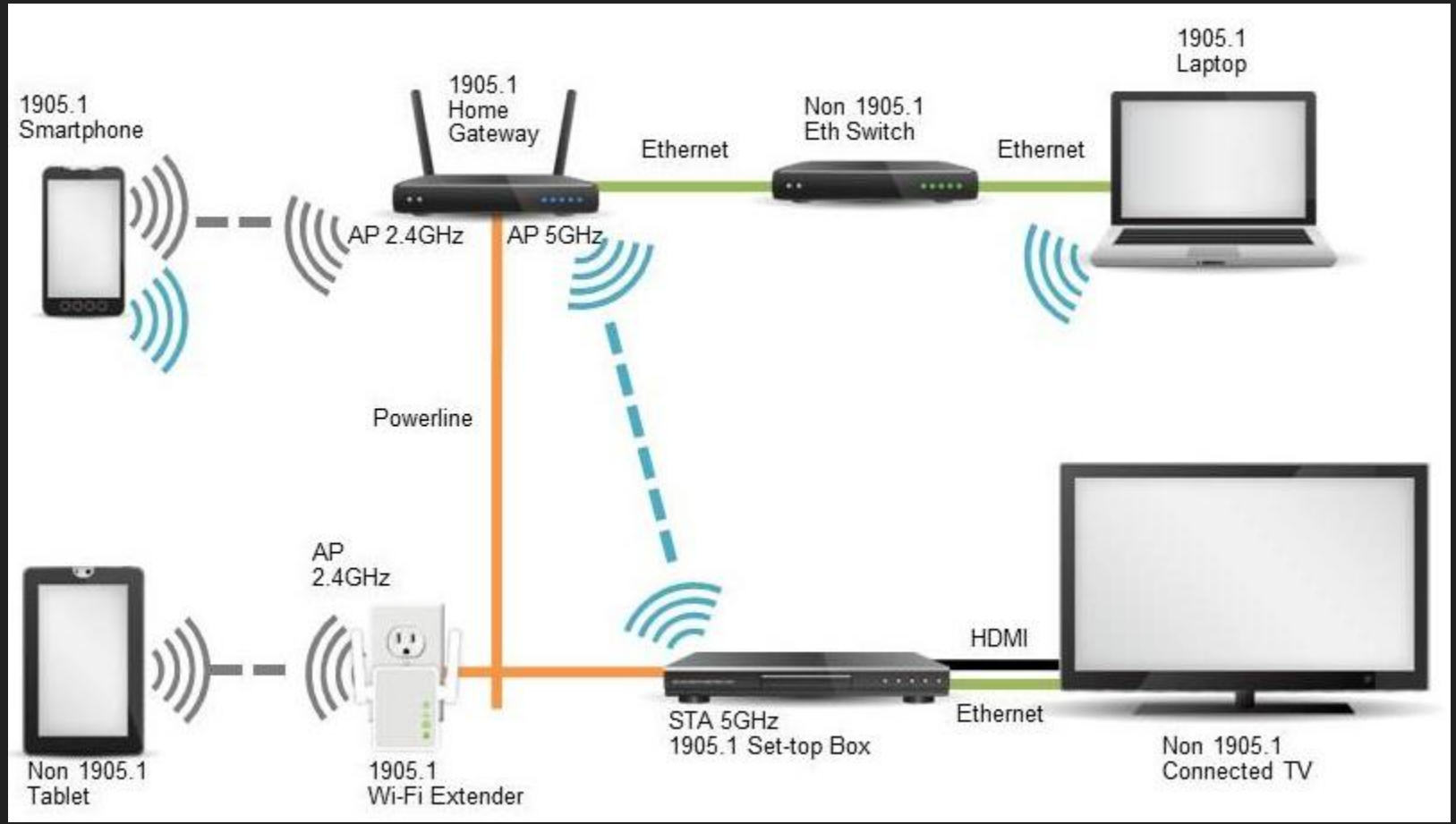
- Learn how Wi-Fi works under normal conditions
- Learn what kind of attacks exist against Wi-Fi
- Learn about WPA2 password cracking
- Use monitor mode to listen to Wi-Fi traffic
- Learn about Raspberry Pi & Arduino-programmed microcontrollers
- Compete in a Wi-Fi hacking challenge

What is Wi-Fi?

Wi-Fi connects devices together much like ethernet, but has a few important differences. It uses radio signals sent from a transmitter to a receiver instead of wires.



Wi-Fi is riskier: Anyone in range can try to join

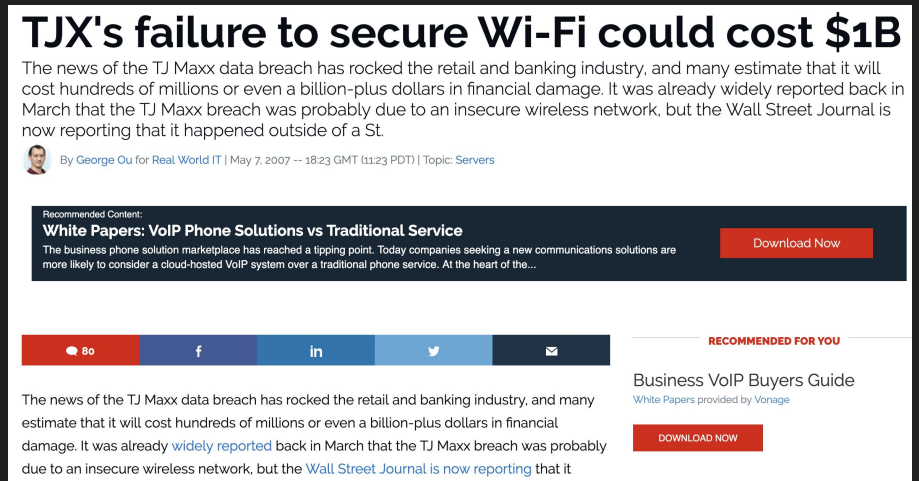


Types of Wi-Fi Network Security

- Open - No Password, no encryption. Anyone can see what websites you are requesting. All HTTP traffic is plain text. Insecure.
- WEP - Outdated, easy to crack. Almost worse than open. Takes 15 minutes to crack.
- WPA - Better encryption, not used as often
- WPA2 - Modern Wi-Fi, vulnerable to brute force or workarounds
- WPA3 - Just came out - Optional standard, so lots of holes. Dragonblood is the first exploit discovered

While Wi-Fi is convenient, it had disadvantages

- Wi-Fi is half-duplex while ethernet is full duplex - one device talks at a time
- Routers have convenience features that break security
- The encryption protecting it is vulnerable if you use weak passwords
- Anyone can jam a device from connecting to a Wi-Fi network
- Devices can lie or pretend to be someone else on the network



TJX's failure to secure Wi-Fi could cost $1B

The news of the TJ Maxx data breach has rocked the retail and banking industry, and many estimate that it will cost hundreds of millions or even a billion-plus dollars in financial damage. It was already widely reported back in March that the TJ Maxx breach was probably due to an insecure wireless network, but the Wall Street Journal is now reporting that it happened outside of a St.

By George Ou for Real World IT | May 7, 2007 -- 18:23 GMT (11:23 PDT) | Topic: Servers

Recommended Content:

White Papers: VoIP Phone Solutions vs Traditional Service

The business phone solution marketplace has reached a tipping point. Today companies seeking a new communications solutions are more likely to consider a cloud-hosted VoIP system over a traditional phone service. At the heart of the...

Download Now

80

RECOMMENDED FOR YOU

Business VoIP Buyers Guide

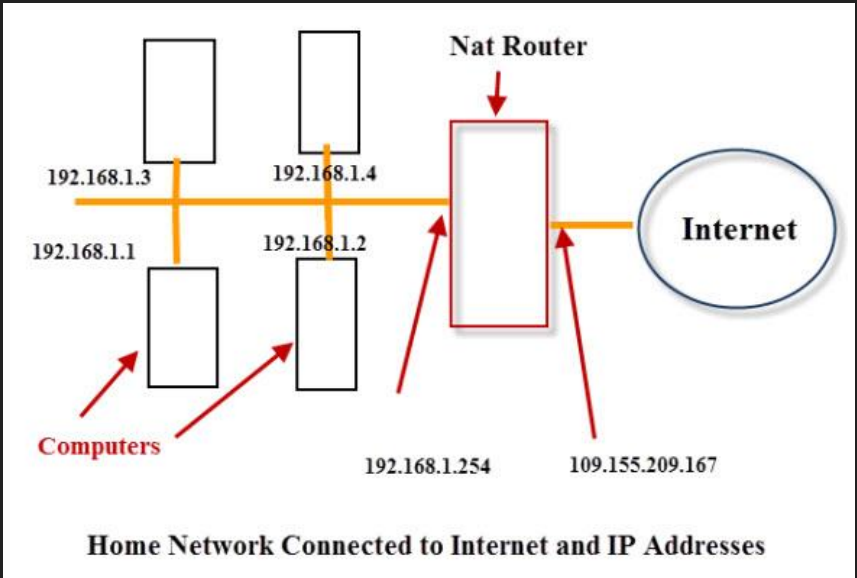
White Papers provided by Vonage

DOWNLOAD NOW

The news of the TJ Maxx data breach has rocked the retail and banking industry, and many estimate that it will cost hundreds of millions or even a billion-plus dollars in financial damage. It was already widely reported back in March that the TJ Maxx breach was probably due to an insecure wireless network, but the Wall Street Journal is now reporting that it

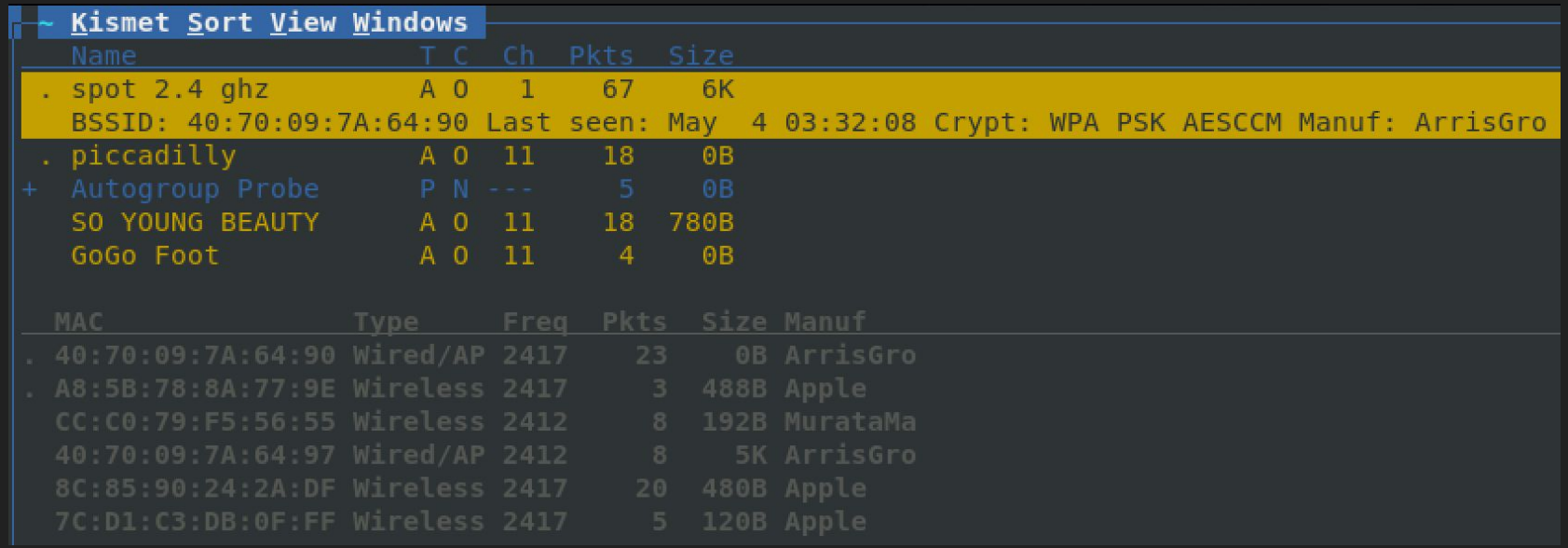
How does Wi-Fi work normally?

- An IP address is set by the network you connect to, like a parking space
- The router assigns every device that connects to the network a unique IP
- Two kinds of IP addresses, internal and external
- Without the password, you can’t see the IP address of devices on encrypted Wi-Fi



How do we identify devices like phones and laptops?

- Your MAC is set by your device and rarely changes, like a car's license plate
- Every Wi-Fi device has a MAC address, any outsider can see it
- Devices have to use their MAC address to transmit on a Wi-Fi network



What happens when you join a Wi-Fi network?

- When you join a Wi-Fi network, your device's MAC gets paired with an IP address
- The router uses this to deliver traffic from your device to the internet and back

```
Dell-3:rpi-hunter skickar$ arp-scan -l
Interface: en0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9.5 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.0.2     e8:11:32:dc:39:80       Samsung Electronics Co.,Ltd
192.168.0.5     00:09:1b:0c:62:0f       Digital Generation Inc.
192.168.0.1     40:70:09:7a:64:97       ARRIS Group, Inc.
192.168.0.7     d4:95:24:c2:36:27       Clover Network, Inc.
192.168.0.4     c8:85:50:f4:20:fa       Apple, Inc.
192.168.0.3     3c:dc:bc:05:77:d4       (Unknown)
192.168.0.6     10:8e:e0:ef:5d:f2       (Unknown)
192.168.0.28    cc:c0:79:f5:56:55       (Unknown)
192.168.0.28    cc:c0:79:f5:56:55       (Unknown) (DUP: 2)
192.168.0.154   7c:d1:c3:db:0f:ff       Apple, Inc.
```

Your IP may change, but your MAC will not

- You can think of this like parking a car in parking space, it may change depending on who gets there first and which are available
- The exception is MAC address randomization, which happens when your device is not connected to the network.

What can you see without the password?

- How many devices are out there, who made them, and which network they are connected to
- The real MAC address of any device, so you can track it when it comes and goes
- Which devices are sending data or being used and which are not
- Kick anyone or any device off the network

What can you do with the network password?

- Pretend to be the router and hijack ALL network traffic
- Watch what people are doing
- Redirect requests to any website to a password stealing version
- Inject things into the browser like keyloggers
- Scan devices on the network and connect to them!

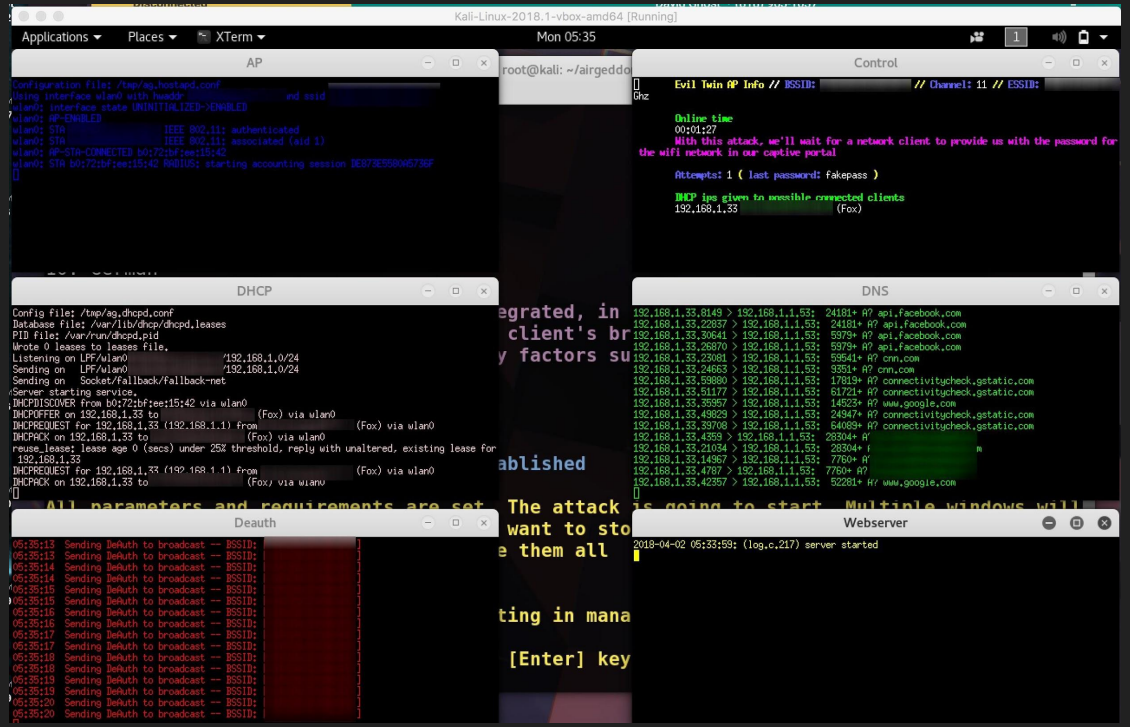
Let’s talk attacks!

There are three main categories we will cover today:

- WPS Setup pin attacks
- WPA handshake cracking
- Social engineering & phishing

Social Engineering attacks rely on user error

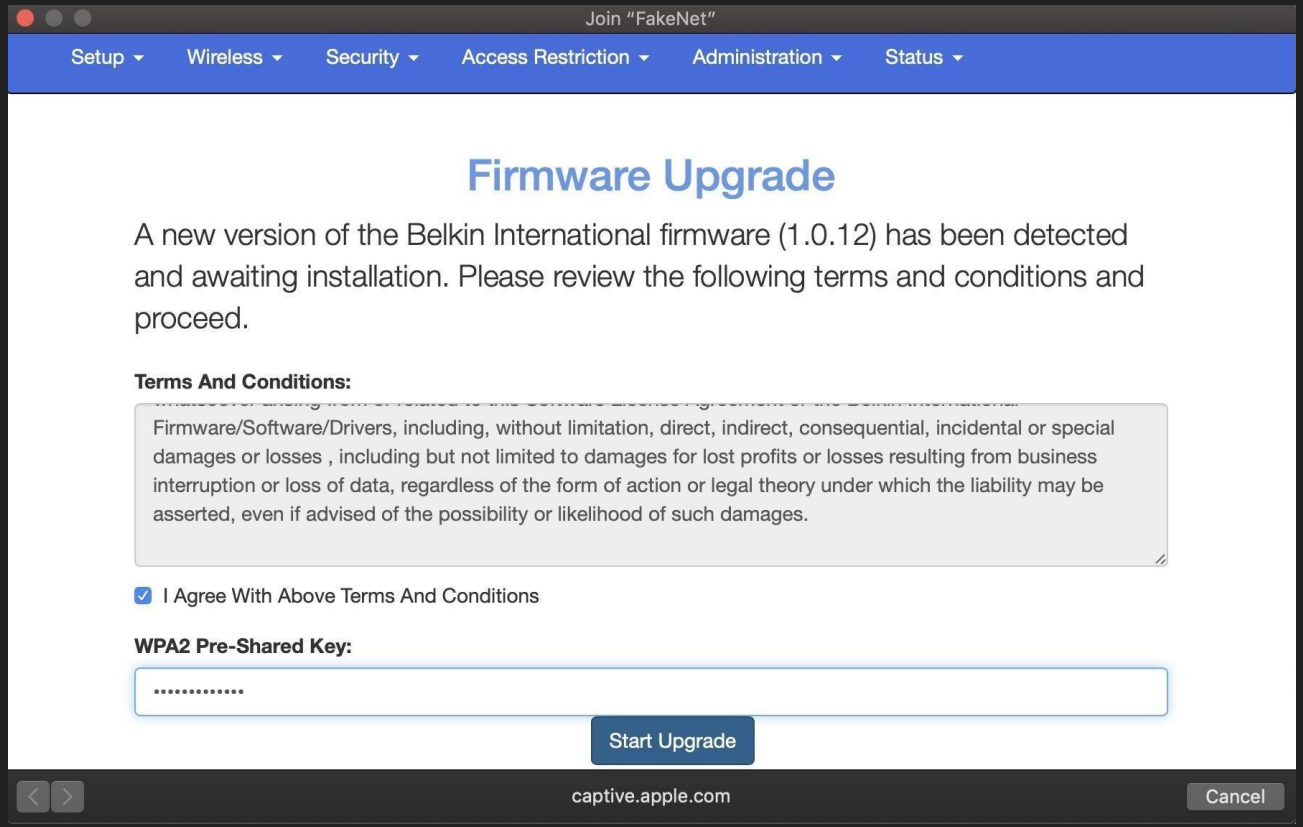
In a social engineering attack, we create an “evil” network for someone to join.



What does social engineering look like?

- Copy the name of the target Wi-Fi network, and make a fake network with no password
- Jam the real Wi-Fi network, and create a fake router update page asking for the password on the open network
- When the user cannot connect, they see the fake network with the same name as their usual network.
- The user connects and sees the page explaining an update is in progress. They enter the password.
- The attacker gets the password

What does the victim see?



WPS Setup Pin Attacks

These attacks are based on a feature that allows you to connect with a PIN to your router if you forget your password.

Many routers use a bad random seed for this that makes it possible to crack in 15 seconds.

Only about 40% of routers are vulnerable, only about 50% of routers have this enabled.

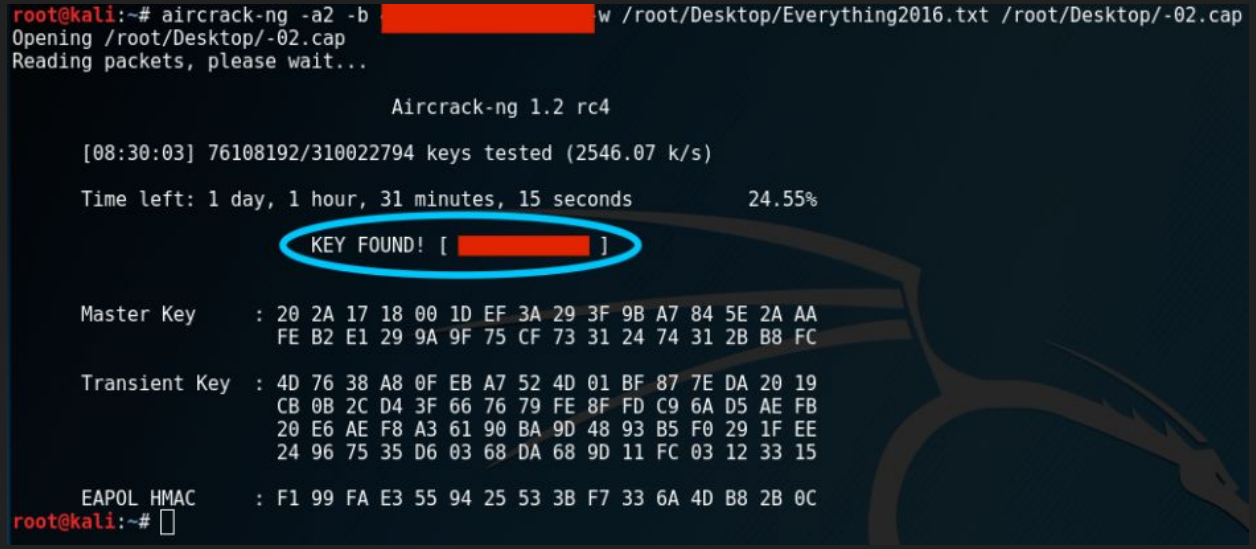
WPS Attacks don’t always work but are powerful

This doesn’t work if WPS is disabled or the wrong version, but if it does, you get backdoor access to the router even if they change the password.

WPA Handshake Brute Force Attacks!

This is the tried and true method of getting a modern Wi-Fi password.

Even though we can't grab a password out of the air, we can use a computer's processing power to figure it out.



What makes modern WPA2 vulnerable to this?

If you capture the handshake that occurs when a device joins a Wi-Fi network, you can use that captured information to crack the password.

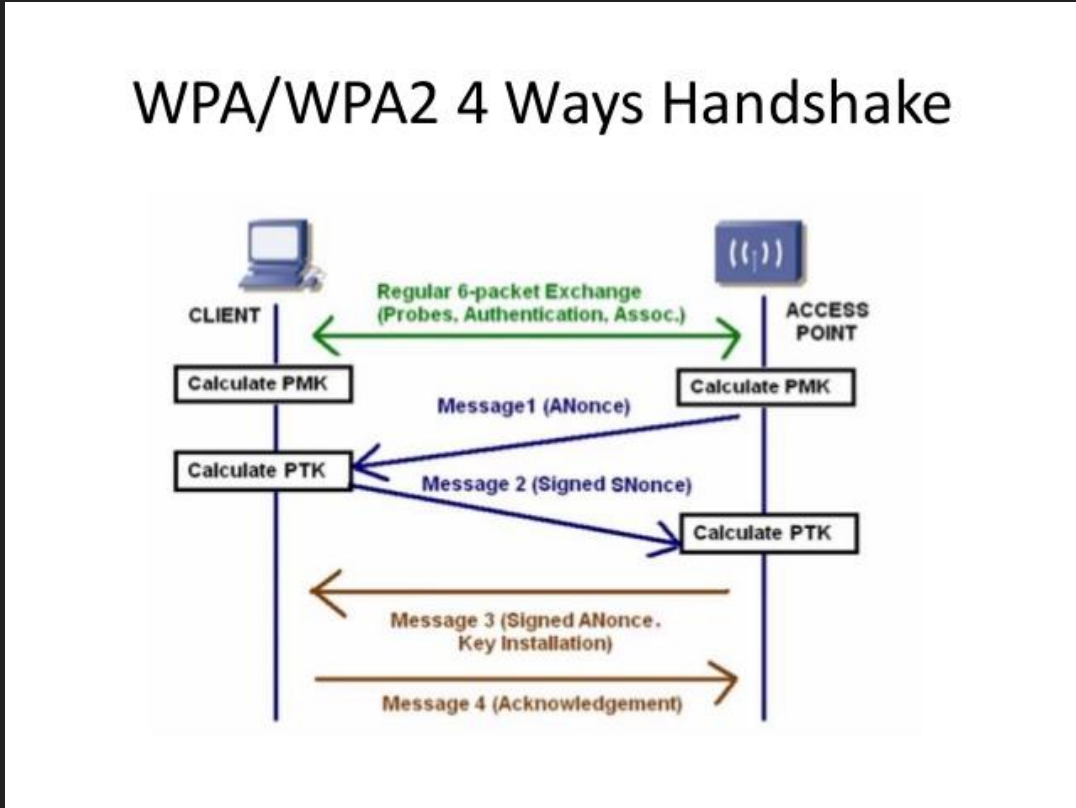
Anyone can kick a client off of a Wi-Fi network, even if you don’t know the password.

That means, provided at least one device is connected to a Wi-Fi network, anyone can kick that device off the network and capture the handshake when the device reconnects.

How do we capture a handshake?

To capture a handshake, we can either wait for a device to connect to the network, or we can kick a device off and record the handshake when it reconnects.

We need to be on the same channel to capture the handshake as well



What do we do with a handshake?

A handshake is a hashed version of the Wi-Fi password. A hash takes the password and converts it into a unique number via a fixed formula.

If we take a password guess and run it with the same formula, it will come out to the same number as the handshake if the password is correct.

A computer can convert several thousand password guesses per second into a hash, and compare them to see if it matches

WPA Cracking Workflow

- Identify the network you are attacking, switch your wireless network adapter to capture on that channel - **airmon-ng tool**
- Record Wi-Fi traffic on that channel until you capture a handshake and save it - **airodump-ng tool**
- Load the file of captured traffic containing the handshake into a cracking program - **aircrack-ng tool**
- Load a big list of password guesses
- Let the computer guess passwords until it succeeds or runs out of passwords

What do you need to do this?

A wireless network adapter that can “listen” in monitor mode. Usually, Wi-Fi is like a one on one conversation.

Some network cards can be switched to “monitor mode” which allows them to listen to traffic that wasn’t meant for them.

Yours may work, but we be can use a Raspberry Pi, or Panda Wireless network adapter. We made one for you!

Technical section overview

Core skills review:

Denial of service/deauthing

Creating fake networks to unmask devices

Objectives:

Attack a single device on a network

Create a cloned fake network

Workflow: Connect to ESP via serial

Step 1: Help

Step 2: Scanning:

scan [<all/aps/stations/wifi>] [-t <time>] [-c <continue-time>] [-ch <channel>]

Scan for all AP’s on channel 6: **scan aps -ch 6**

Scan for all clients on channel 11: **scan stations -t 20s -ch 11**

Draw packet graph: **draw**

Step 3: Compound Commands

Can use DELAY and :: to combine commands.

scan for 60 seconds on channel 6 and show all stations after a 65-second delay:

scan wifi -t 60s -ch 6;;DELAY 65s;;show stations

Step 4: Showing scan results

Show detected stations/AP’s: **show [<all/aps/stations/names/ssids>]**

Show all client devices: **show stations**

Show all AP’s: **show aps**

Step 5: Select a target from scan:

Select a target: **select [<all/aps/stations/names>] [<id>]**

Deselect a target: **deselect [<all/aps/stations/names>] [<id>]**

select **[<all/aps/stations/names>] [<id>]**

Select all AP's: **select aps**

Select all stations: **select stations**

Select AP number 5 from our list of scanned APs: **select aps 5**

Select client 3 from our list of detected clients: **select stations 3**

Show targets selected: **show selected**

Step 6: Attack a target

Attack command: **attack [beacon] [deauth] [deauthall] [probe] [nooutput] [-t <timeout>]**

Attack all selected targets: **attack -d**

Attack all networks in range: **attack -da**

Check status of attack: **attack status [on/off]**

Stop an attack in progress: **stop -a**

Wireless AP Interface:

Enable: startap [-p <path][-s <ssid>] [-pswd <password>] [-ch <channel>] [-h] [-cp]

Disable: stopap

Create false networks:

Remove command: **remove <ap/station/names/ssids> [all]**

Remove default SSIDs: **remove ssids all**

Add AP #0 from our scan, cloned 20 times: **add ssid -ap 0 -cl 20**

Check our list of ssids: **show ssids**

Start our beacon attack: **attack -b**

Stop attack: **stop -a**

Add custom fake network (must escape spaces): **add ssid “Dokdo\ Proud\ to\ Island” [-wpa2] -cl 20 [-f]**

Demo Time!

Let’s play the game we’ll be playing today and show how Wi-Fi hacking works.

After the demo, we’ll grab some food, and when we come back we’ll start the game!