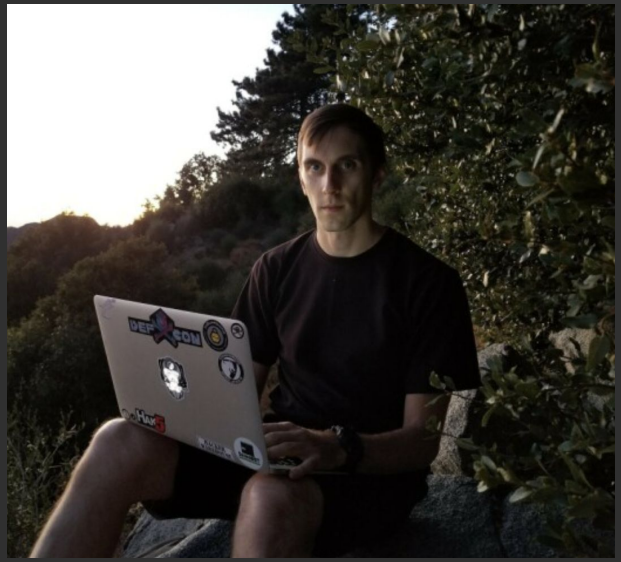
Wi-Fi Self Defense

Cat Got Your password

Who Am I?

Hi! I’m Kody Kinzie:

- Security researcher specializing in Wi-Fi hacking, microcontrollers, and open source investigations
- Teach ethical hacking on my YouTube channels: Retia
- Find more at hack.gay



Resources

- Example Github Repo: github.com/skickar/CatGotYourPassword
- Serial terminal: serialterminal.com
- Flashing Tool: nugget.dev
- Retia Discord: https://discord.gg/rjVJbauAUX

Learn

⛔ Getting attacked in the wild
⛔ Attacking Others to Learn What Vulnerable Systems Look Like

How do we Learn Safely and Ethically?

✅ Use Our Own Devices as a Lab
✅ Also Makes Your System More Secure

What are we learning?

- **Detect jamming attacks** - Find out if someone is attacking your network
- **Hunt down suspicious Wi-Fi devices** - Learn about scanning, isolating, & tracking
- **Beacon Swarm** - Extract information from devices with a beacon swarm
- **Catch a Wi-Fi Pineapple** - Learn Karma attack, uncover hacker tools nearby!
- **QR Code attacks** - Explore the dangers of hidden Wi-Fi networks in QR codes
- **Wi-Fi Phishing** - Learn what Wi-Fi Phishing looks like and try it yourself

What is a Microcontroller?

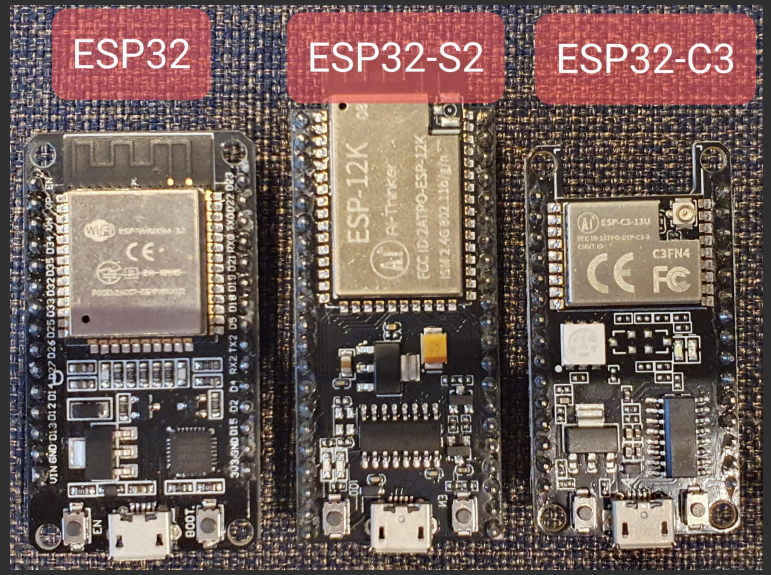
Inexpensive Systems on Chips With A Variety Of Strengths and Weaknesses

<u>Examples:</u>

ESP8266 - Wi-Fi Injection Capable, no USB

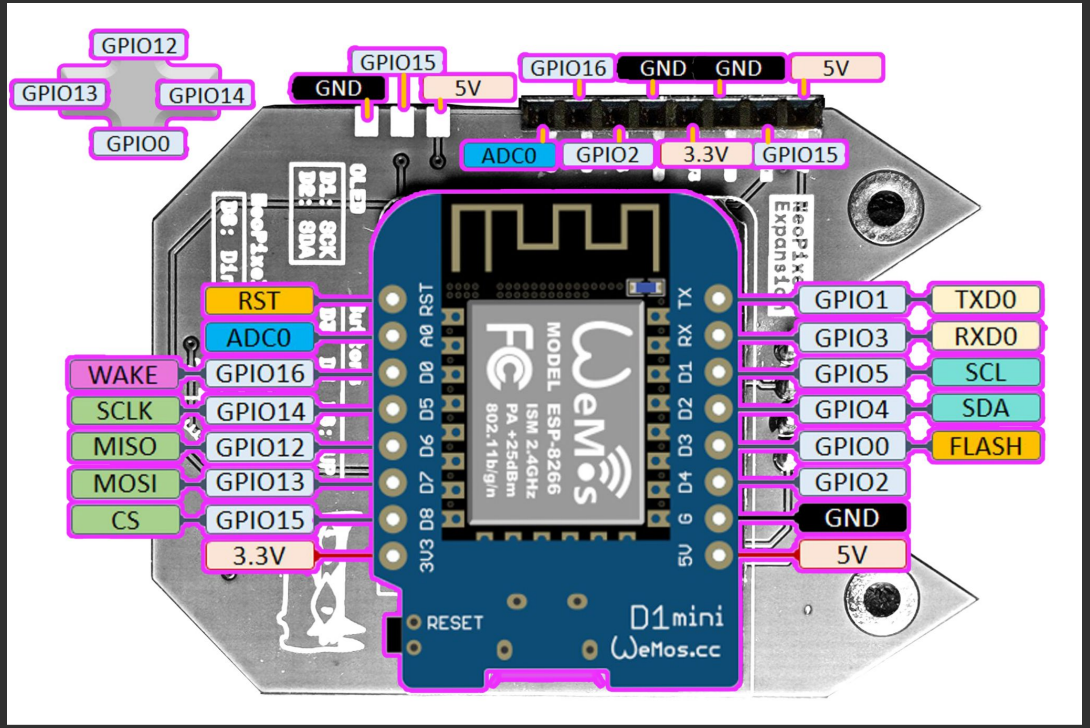
ESP32 - Bluetooth & Wi-Fi, no USB

ESP32-S2 - Wi-Fi Enabled Microcontroller with HID + USB



What is The Wi-Fi Nugget?

- Cute, cat-shaped microcontroller breakout for beginners
- Based on ESP8266
- Uses D1 Mini development boards
- Designed to be a tool for learning
- Flashes firmware of programs over USB/website



Lab #1: Detect jamming attacks

Let’s catch hackers jamming Wi-Fi networks!

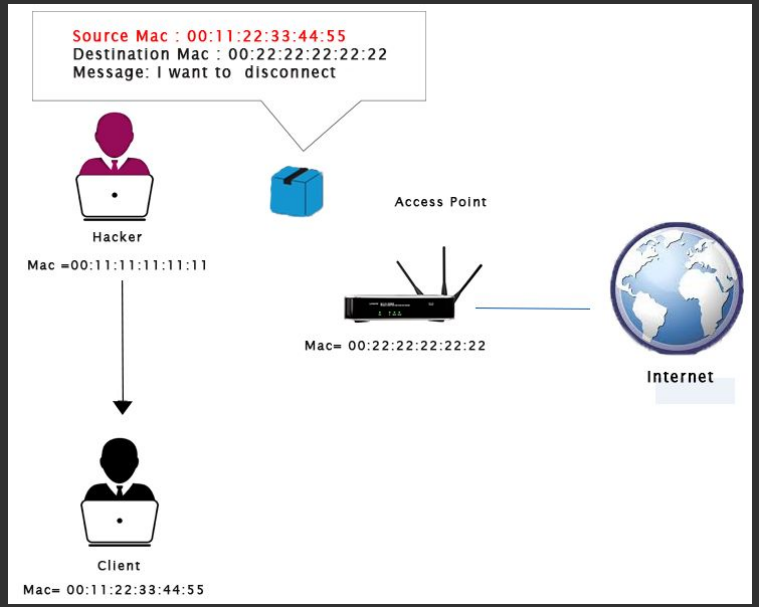
- This attack is unsophisticated, anyone can do it
- Mostly affects 2.4 GHz using older security protocols but can affect 5 GHz
- We’ll configure the nugget to act as a sentry and monitor for these attacks

What is a Deauthentication Attack?

- Kicks devices off of a Wi-Fi network
- Protocol jamming
- Can target one device or all devices
- Sends valid packets to terminate connection
- Most modern Wi-Fi does protect against this!

Exception:

- WPA3 +
- Enabling protected management frames



Why does this matter?

Wi-Fi jamming to knock out cameras suspected in nine Minnesota burglaries -- smart security systems vulnerable as tech becomes cheaper and easier to acquire

News By Mark Tyson published 5 days ago

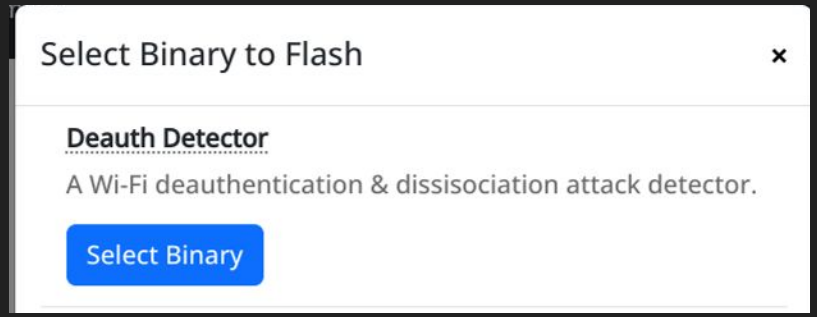
Police believe a string of nine robberies in Edina have used this tech.

Comments (51)

Setting Up Your Nugget to Detect Jamming

- Navigate to our flashing website www.nugget.dev in Chrome-based browser
- Plug in your Nugget via USB cable & click “Connect Your Nugget”
- Select your Nugget from the dropdown menu of serial devices

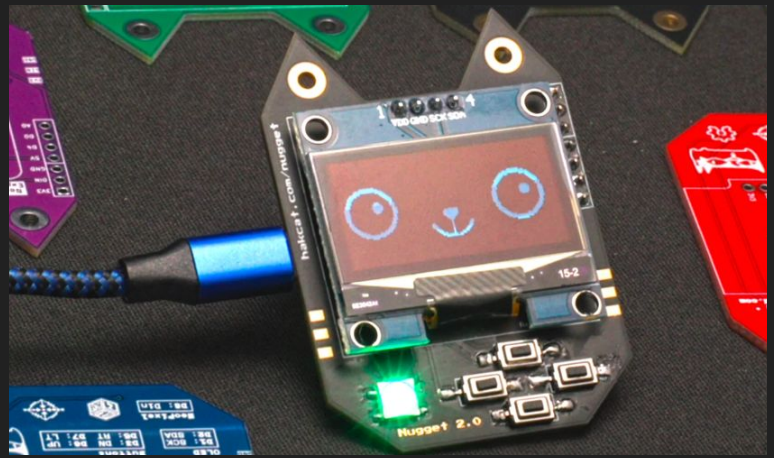
Flash the Deauth Detector Binary



- Open Select Program Menu
- Select **Deauth Detector**
- Close Menu and “Program”
- Wait for the Completion Bar
- Unplug and replug your Nugget

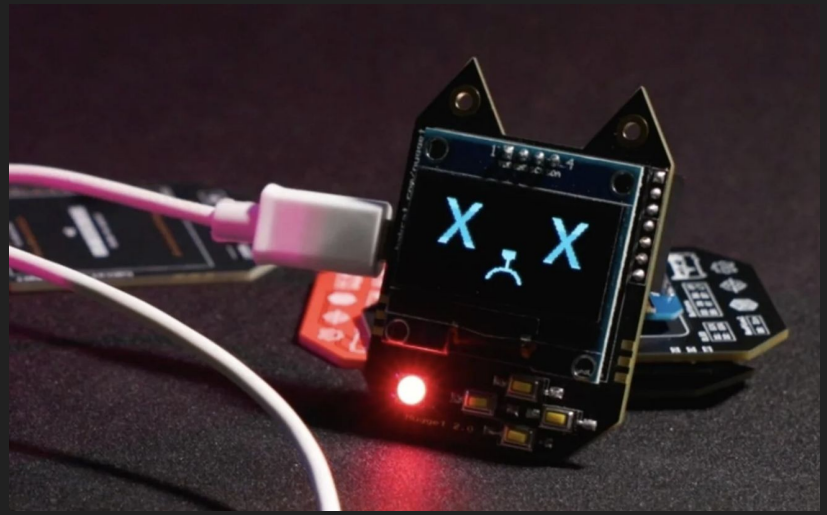
*Certain Systems may need to have Dialout Group added

Your Nugget is On Guard



- Nugget is sniffing every Wi-Fi packet
- Doesn’t know if attack is on your network or one nearby
- Deauth packets are part of normal operations but can be abused
- Nugget alerts if too many deauthentication packets are detected
- Open source code - Change if you want

Hacker Alert!



- Nugget glows red on detecting hacker
- The face also becomes attacked
- The longer this lasts, the more likely it’s malicious

About Deauth Attacks

- Deauthentication is normal and more common in crowded environments
- You can’t tell without modification which network is under attack
- Not as easy against 5ghz networks
- WPA3 and protected management frames disable this attack

Lab #2: Hunt down suspicious Wi-Fi devices

- In this section, we'll flash a new program to our Wi-Fi Nugget
- After flashing the Advanced V3 Deauther, we'll learn to scan for Wi-Fi devices
- Next, we'll learn to identify and hone in on suspicious devices
- Finally, we'll track down a device by signal strength

Setting Up Your Nugget For Hunting

- Once again, go to our flashing website www.nugget.dev
- Plug in your Nugget via USB cable & click “Connect Your Nugget”
- Select your Nugget from the dropdown menu of serial devices

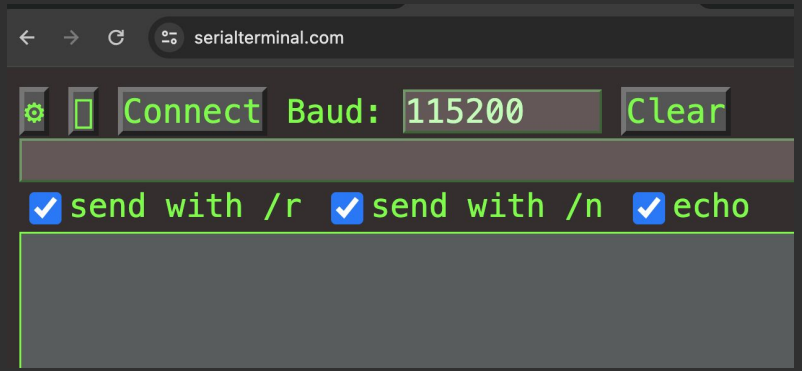
Flash the Headless Advanced Wi-Fi Deauther Binary

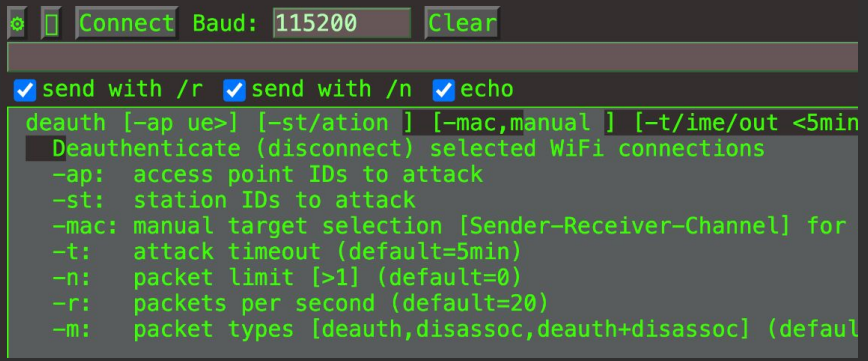
- Open a Chromium based browser and navigate to: nugget.dev
- Plug in Wi-Fi Nugget & Click “Connect”
- Select Serial Port of Nugget
- Open Select Program Menu And Select Advanced Deauther V3
- Close Menu and “Program”

*Certain Systems may need to have Dialout Group added

Connect Via Serial terminal

- Navigate to serialterminal.com in a Chrome browser
- Unplug & Plug in your Nugget, set Baud to 115200, click “Connect”
- Select your Nugget from the dropdown menu of serial devices
- Type “help” and press return to test if the connection is working

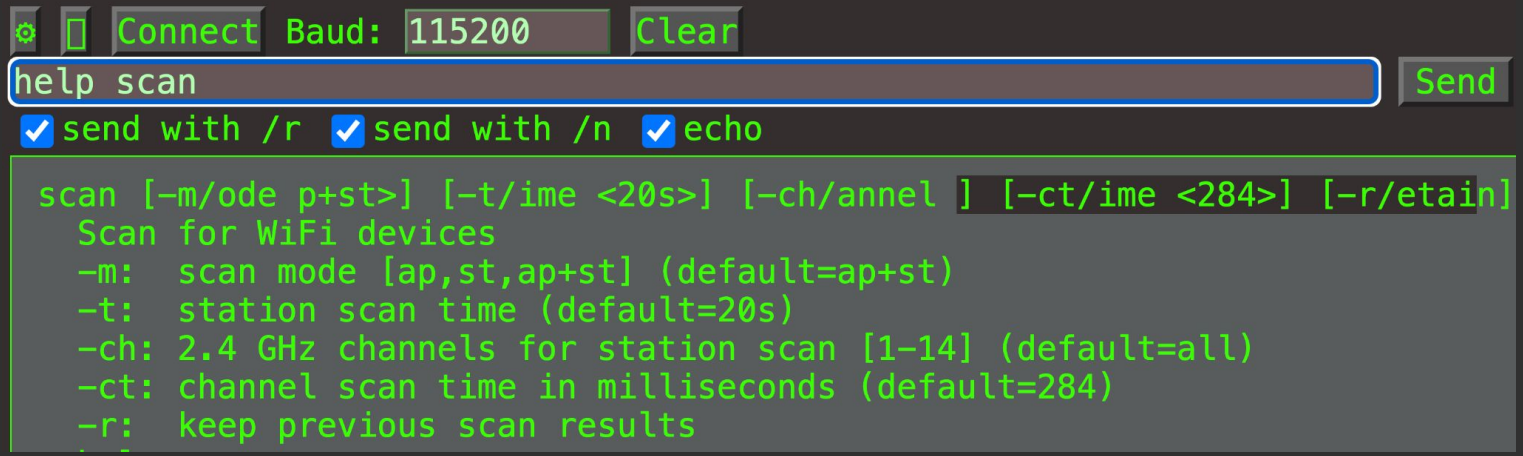




We’re set up!

Use the “help” command to get more information on how to use each command:

- Scan - search the airwaves for Wi-Fi signals, display devices & access points
- Beacon - create the appearance of Wi-Fi networks that can’t be joined
- AP - create an evil Wi-Fi access point that can be joined



Let’s try a scan!

- We’ll scan the airwaves to listen in on networks devices are calling out for
- Try a basic scan - just type “Scan”
- We’ll do a more advanced scan to learn more about what’s around us
- What might we not see? Connected Wi-Fi devices that aren’t being used

```
[ ========== Scan Results ========== ]

[ ===== Access Points ===== ]
 ID SSID (Network Name)                RSSI Mode Ch BSSID (MAC Addr.) Vendor
=============================================================================

  0 *HIDDEN-NETWORK*                    -85 WPA2  6 90:4c:81:fa:bd:e0 HewlettP
  1 "POS411"                            -84 WPA*  6 90:4c:81:fa:bd:e1 HewlettP

  2 "CCA411"                            -86 WPA2  6 90:4c:81:fa:bd:e3 HewlettP
  3 "H-Rewards by IntercityHotel"       -85 Open  6 90:4c:81:fa:bd:e4 HewlettP

  4 "CORP"                              -86 WPA2  6 90:4c:81:fa:bd:e5 HewlettP
  5 *HIDDEN-NETWORK*                    -63 WPA2  1 90:4c:81:fc:03:80 HewlettP

  6 "POS411"                            -63 WPA*  1 90:4c:81:fc:03:81 HewlettP
  7 "DHOffice"                          -62 ?     1 90:4c:81:fc:03:82 HewlettP

  8 "CCA411"                            -62 WPA2  1 90:4c:81:fc:03:83 HewlettP
  9 "H-Rewards by IntercityHotel"       -61 Open  1 90:4c:81:fc:03:84 HewlettP

 10 "CORP"                              -63 WPA2  1 90:4c:81:fc:03:85 HewlettP
 11 "CORP-IoT"                          -63 WPA2  1 90:4c:81:fc:03:86 HewlettP

=============================================================================
Ch = 2.4 GHz Channel  ,  RSSI = Signal strengh  ,  WPA* = WPA & WPA2 auto mode
```

Advanced Scan for Suspicious Devices

- Use this advanced scan to look for stations we may want to track down: **scan -m st -ch 1-12 -t 60 -ct 5000**

```
# help scan

scan [-m/ode p+st>] [-t/ime <20s>] [-ch/annel ] [-ct/ime <284>] [-r/etain]
  Scan for WiFi devices
  -m:  scan mode [ap,st,ap+st] (default=ap+st)
  -t:  station scan time (default=20s)
  -ch: 2.4 GHz channels for station scan [1-14] (default=all)
  -ct: channel scan time in milliseconds (default=284)
  -r:  keep previous scan results
```

Specify a device to track with RSSI

When we decide what we want to track, we need:

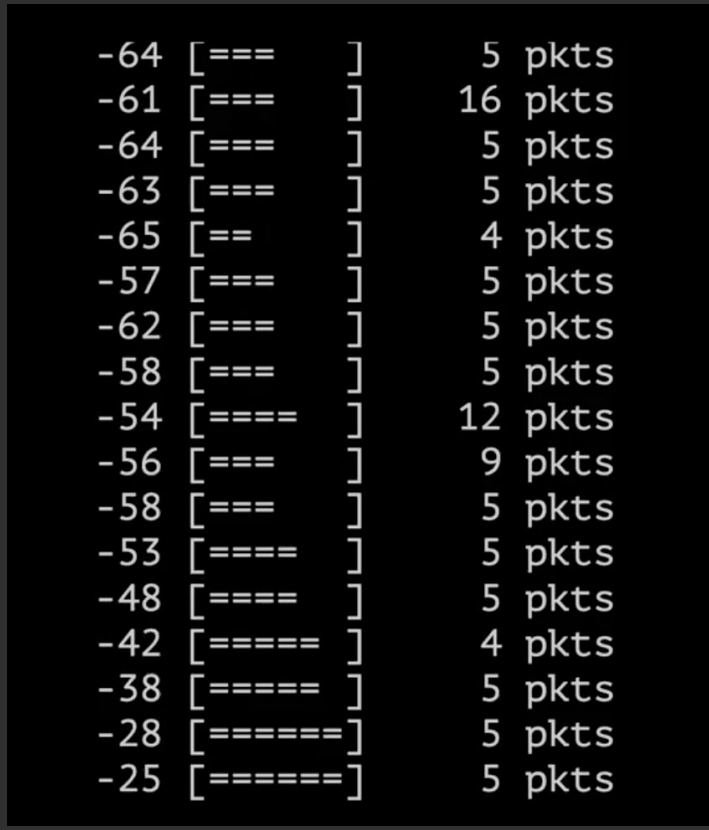
- Index number
- Channel it’s operating on

```
rssi [-mac ue>] [-ap ] [-st/ation alue>] [-ch/annel ] [-ct/ime <120>] [-ut,u/pdate/time <1s>]
  Signal Strength scan
  -mac: filter by MAC(s)
  -ap:  filter by AP(s)
  -st:  filter by Station(s)
  -ch:  2.4 GHz channel(s) for scan [1-14] (default=all)
  -ct:  channel scan time in milliseconds (default=120)
  -ut:  update time (default=1s)
================================================================================
Pkts = Recorded packets , RSSI = Average signal strength
================================================================================
```

Track down by signal

With a command like:
rssi -st 0 -ch 1

You can start displaying the signal strength of the first station we found in our scan live.



Next: Tracking With Beacon Swarms

- Beacons - Like a “billboard” advertising a Wi-Fi network
- Beacon Swarm - Creating up to hundreds of fake networks to see if nearby devices have joined them before
- We can uncover VIPs or places someone has been by listening for which of our beacons a smartphone trusts

beacon "SSID_1","SSID_2" -mon

- beacon - Loops sending of target beacons to create beacon swarm
- “SSID_x” - Sets the target names, can add 20+ network names
- -mon - Tells the tool to scan for devices attempting to join the advertised networks
- Try the “beacon swarm” command in the resources - https://github.com/skickar/CatGotYourPassword

```
> help beacon

# help beacon

beacon -ssid/s  [-bssid,from ] [-receiver,to ] [-enc/ryption ] [-ch/annel <1>] [-r/ate <10>] [-auth,m/on/itor]
  Send WiFi network advertisement beacons
  -ssid: network names (SSIDs) for example: "test A","test B"
  -from: BSSID or sender MAC address (default=random)
  -to:   receiver MAC address (default=broadcast)
  -enc:  encryption [open,wpa2] (default=open)
  -ch:   2.4 GHz channel(s) [1-14] (default=1)
  -r:    packets per second per SSID (default=10)
  -m:    scan for authentications
  -save: save probe requests from auth. scan
  -t:    attack timeout (default=5min)
```

```
[ ===== Authentication Scan ===== ]
Scan time:     5min
Channels:      1,
Channel time:  -
Beacon Mode:   On

Save stations: No
BSSID filter:  0

Type 'stop auth' to stop the scan

RSSI Ch Vendor   MAC-Address       SSID                                BSSID
================================================================================
 -74  1          fe:23:2d:09:0e:53 "Ace Hotel"                         00:0a:73:a2:dd:d3
 -72  1          fe:23:2d:09:0e:53 "Ace Hotel"                         00:0a:73:a2:dd:d3
 -74  1          fe:23:2d:09:0e:53 "Ace Hotel"                         00:0a:73:a2:dd:d3
 -71  1          fe:23:2d:09:0e:53 "Ace Hotel"                         00:0a:73:a2:dd:d3
 -66  1          fe:23:2d:09:0e:53 "Ace Hotel"                         00:0a:73:a2:dd:d3
 -71  1          fe:23:2d:09:0e:53 "Ace Hotel"                         00:0a:73:a2:dd:d3
 -68  1          fe:23:2d:09:0e:53 "Ace Hotel"                         00:0a:73:a2:dd:d3
 -70  1          fe:23:2d:09:0e:53 "Ace Hotel"                         00:0a:73:a2:dd:d3
 -69  1          fe:23:2d:09:0e:53 "Ace Hotel"                         00:0a:73:a2:dd:d3
 -70  1          fe:23:2d:09:0e:53 "Ace Hotel"                         00:0a:73:a2:dd:d3
 -67  1          fe:23:2d:09:0e:53 "Ace Hotel"                         00:0a:73:a2:dd:d3
 -68  1          fe:23:2d:09:0e:53 "Ace Hotel"                         00:0a:73:a2:dd:d3
 -67  1          fe:23:2d:09:0e:53 "Ace Hotel"                         00:0a:73:a2:dd:d3
 -48  1          06:06:e7:96:78:50 "Americas Best Value Inn"           00:0a:73:a2:dd:d4
 -49  1          06:06:e7:96:78:50 "Americas Best Value Inn"           00:0a:73:a2:dd:d4
 -50  1          06:06:e7:96:78:50 "Americas Best Value Inn"           00:0a:73:a2:dd:d4
 -53  1          06:06:e7:96:78:50 "Americas Best Value Inn"           00:0a:73:a2:dd:d4
 -52  1          06:06:e7:96:78:50 "Americas Best Value Inn"           00:0a:73:a2:dd:d4
 -52  1          06:06:e7:96:78:50 "Americas Best Value Inn"           00:0a:73:a2:dd:d4
 -49  1          06:06:e7:96:78:50 "Americas Best Value Inn"           00:0a:73:a2:dd:d4
 -49  1          06:06:e7:96:78:50 "Americas Best Value Inn"           00:0a:73:a2:dd:d4
 -50  1          06:06:e7:96:78:50 "Americas Best Value Inn"           00:0a:73:a2:dd:d4
 -50  1          06:06:e7:96:78:50 "Americas Best Value Inn"           00:0a:73:a2:dd:d4
 -52  1          06:06:e7:96:78:50 "Americas Best Value Inn"           00:0a:73:a2:dd:d4
 -50  1          06:06:e7:96:78:50 "Americas Best Value Inn"           00:0a:73:a2:dd:d4
```

Example Attack Result

Lab #3: Catch a Wi-Fi Pineapple

Hackers can use hacking tools like a Wi-Fi Pineapple to attack Wi-Fi devices.

In this lab, we'll trick these hacking tools into revealing their presence!

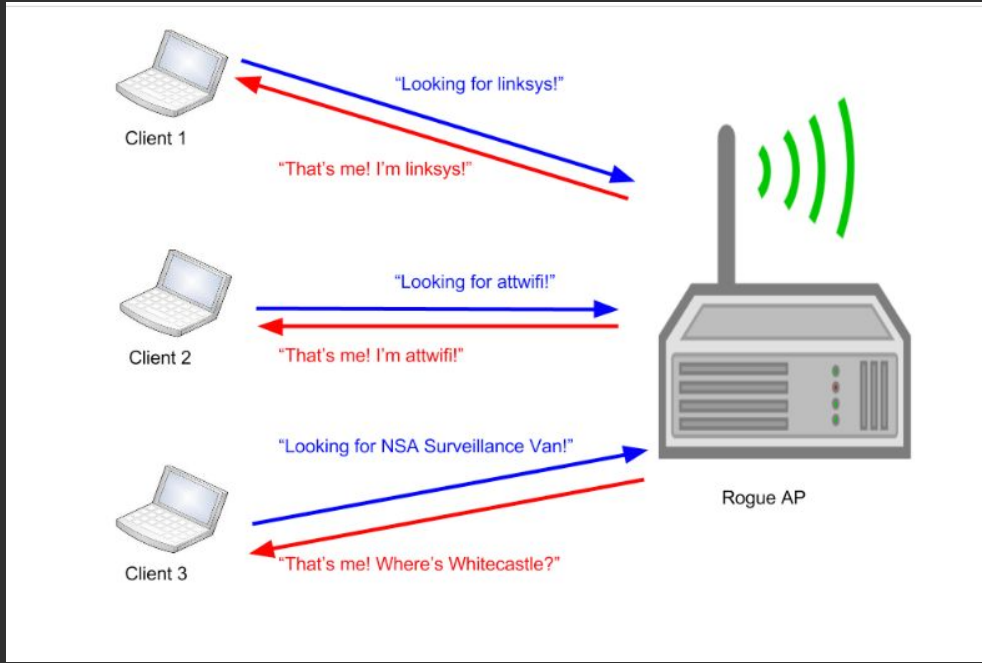
What is a Wi-Fi Pineapple?

- Wi-Fi Pentesting tool
- Creates evil access points
- Listens in on Wi-Fi traffic to find devices to attack
- Customizes attacks based on what it sees

What is the Karma Attack?

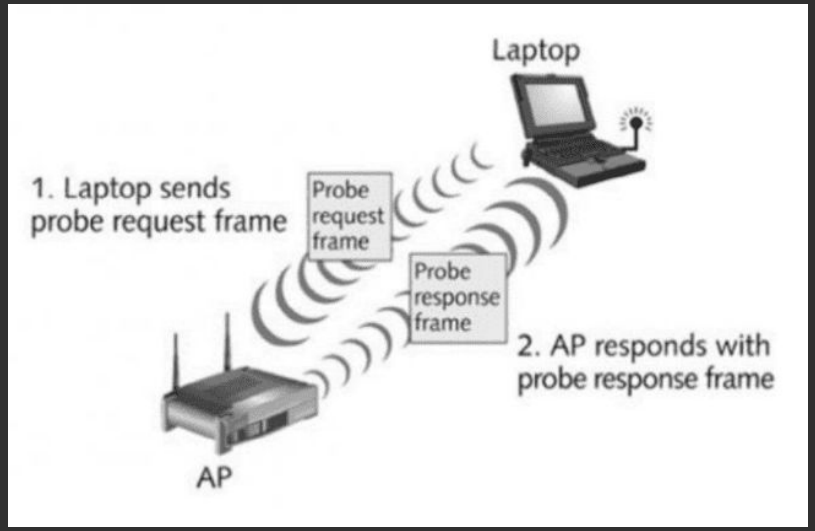
In a Karma attack:

- Attacker listens for nearby Wi-Fi devices calling for trusted network names.
- Creates fake networks based on the names it sees nearby devices calling out for
- Tries to lure victim devices into connecting to these fake networks



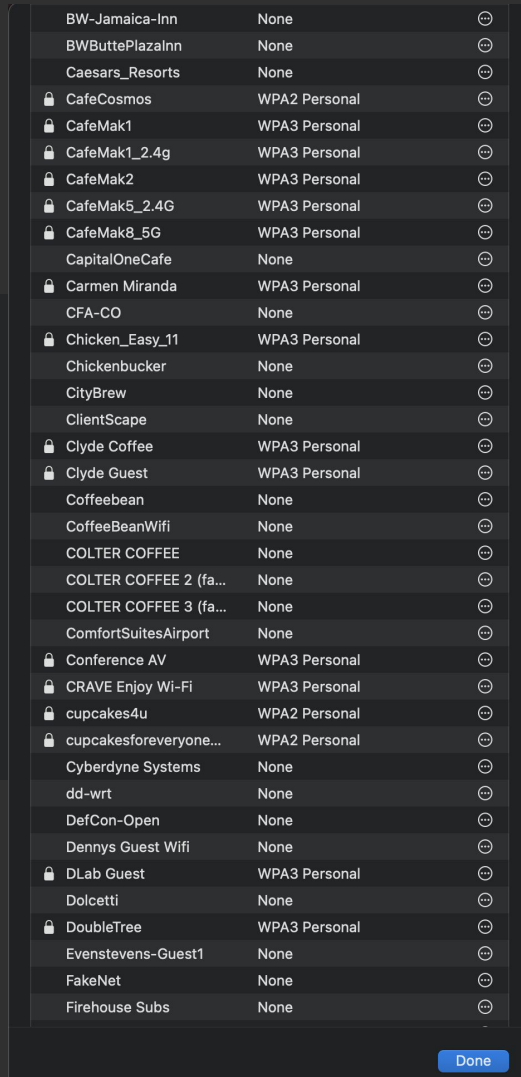
What is a probe request?

- A type of packet Wi-Fi devices send out periodically
- Contains the names of recently connected-to networks in plain text
- The pineapple sniffs for these messages and makes evil twin networks in response



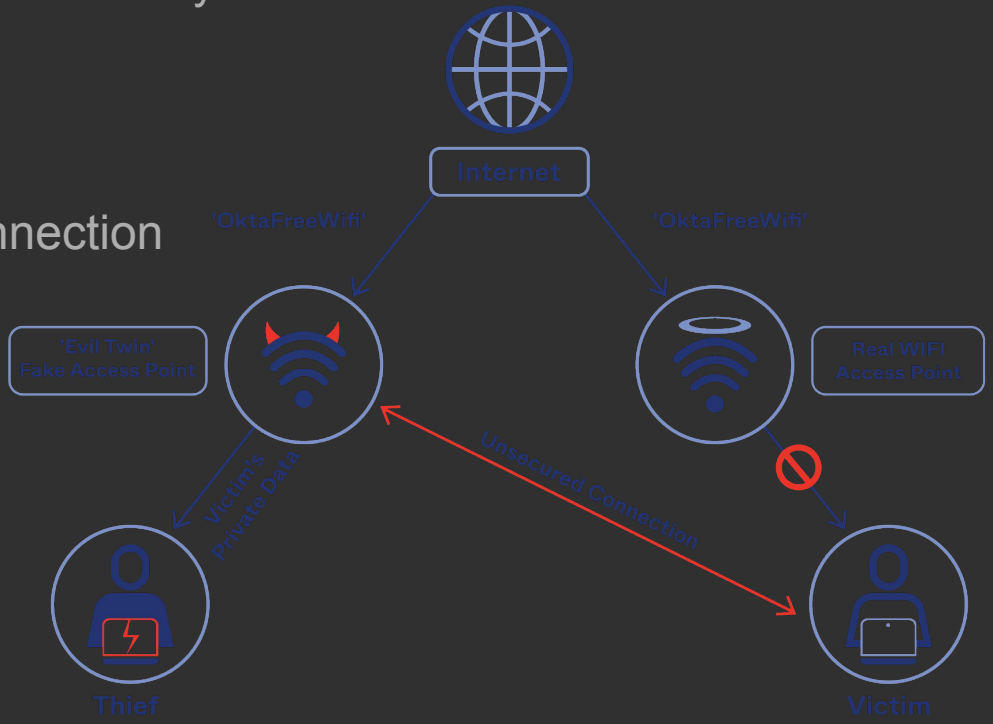
How many networks are in your phone?

- Check your device’s trusted network list
- I am the instructor of this class and I still had 4 vulnerable networks when I checked
- You should delete any open Wi-Fi networks or set them not to auto-connect
- Do this. We’ll wait.
- ANY of these networks can sell you out, It only takes one



When does a Karma attack work?

- Pineapple creates a fake network with the same name as an open Wi-Fi network you've joined before
- Device joins the evil AP.
- Hacker controls your data connection



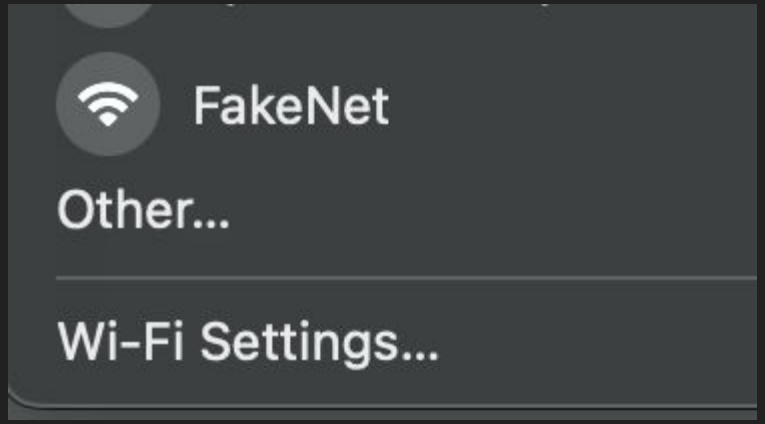
Unmasking the Pineapple

- We can force the pineapple to reveal itself by sending out fake probe requests
- Let’s make up stupid fake network names and call out for them with probe requests
- If we see those fake networks appear out of thin air, there’s a pineapple afoot!

probe "FakeNet","PineAppleBuddy"

- probe - Loops sending of probe requests to entice pineapple
- “FakeNet” - Sets the target names, works 20 or (sometimes)more networks
- Pineapples should react to this!

```
probe -ssid/s  [-sender,from ] [-receiver,to ] [-ch/annel/s <1>] [-r/ate <10>] [-t/ime/out <5min>]
  Send probe requests for WiFi networks
  -ssid: network names (SSIDs) for example: "test A","test B"
  -from: sender MAC address (default=random)
  -to:   receiver MAC address (default=broadcast)
  -ch:   2.4 GHz channel(s) [1-14] (default=1)
  -r:    packets per second per SSID (default=10)
  -t:    attack timeout (default=5min)
```



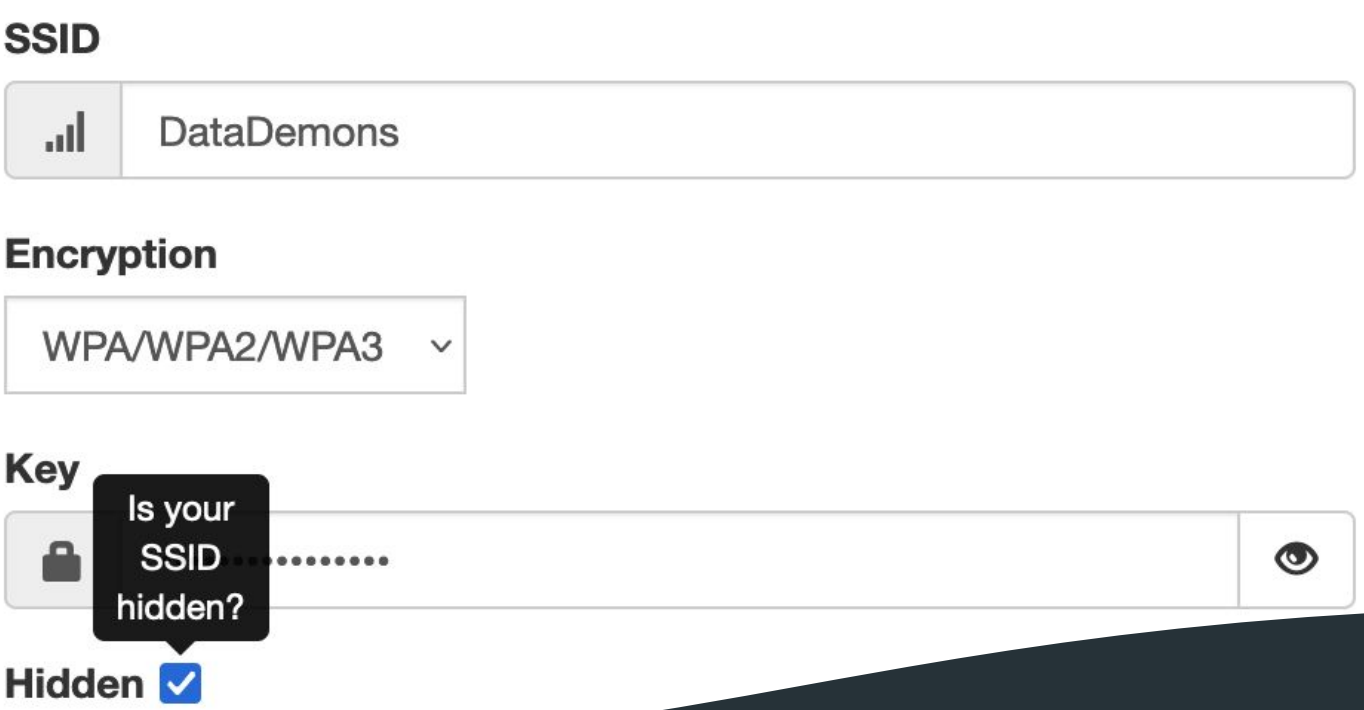
Look For FakeNet appearing!

Lab #4: Detect If You've Been Tagged by Evil QR codes

- We can encode different information in QR codes
- For this example, we'll be showing how hackers can make an Evil Wi-Fi QR code
- This format is sneaky because we can add data the user can't see
- We're going to add the "hidden" flag to this QR code

Wi-Fi

WIFI:S:DataDemons;T:WPA;P:mysecretpassword;H:true;



Qifi.org: Browser Based QR Generator

Let’s Tag Our Device - Create Your Own QR Code

Run this while scanning your QR code to see what happens:
scan -m st -ch 1-12 -t 60 -ct 5000

```
[ ===== Scan for Stations ===== ]
Scan time:    1min

Channel time: 5s
Channels:     1,2,3,4,5,6,7,8,9,10,11,12,

Type 'stop scan' to stop the scan

 ID Pkts RSSI Vendor   MAC-Address       AccessPoint-SSID                  AccessPoint-BSSID Probe-Requests
=============================================================================================================
  -    4  -59          52:4f:f5:b1:ec:31                                                     "HiddenNet"
                                                                                            "IrishTracker"
  -    2  -63          2e:b8:b6:36:12:18                                                     "DataDemons"
  -    6  -60          36:9e:63:6f:d7:cd                                                     "DataDemons"
                                                                                            "HiddenNet"
                                                                                            "IrishTracker"
  -    2  -53          ae:8d:47:50:db:34                                                     "DataDemons"
  -    6  -49          82:dd:99:f4:3d:db                                                     "DataDemons"
                                                                                            "HiddenNet"
                                                                                            "IrishTracker"
```

Takeaways from QR attack

If you've joined a hidden network in the past (from a QR code or otherwise) your device will always be screaming out the hidden network's name.

Hackers can:

- Take over your data connection and change what loads
- Detect when you're nearby
- Make pop-ups appear on your phone

Remediation

- Don’t scan QR codes you don’t trust
- Regularly check your saved networks and delete any unrecognized nets to ensure System Security

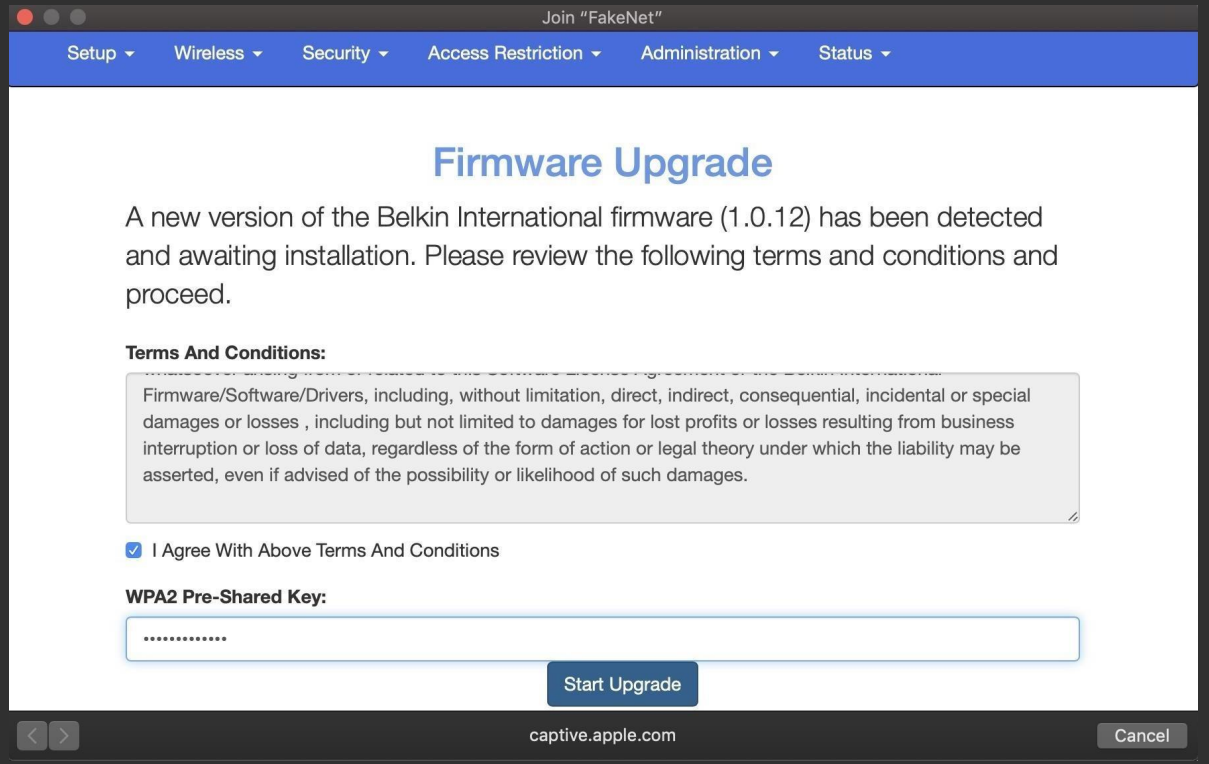
❗You Just Backdoored Your Device, Clear that Tracker out

Lab #5: Catching Wi-Fi phishing attacks

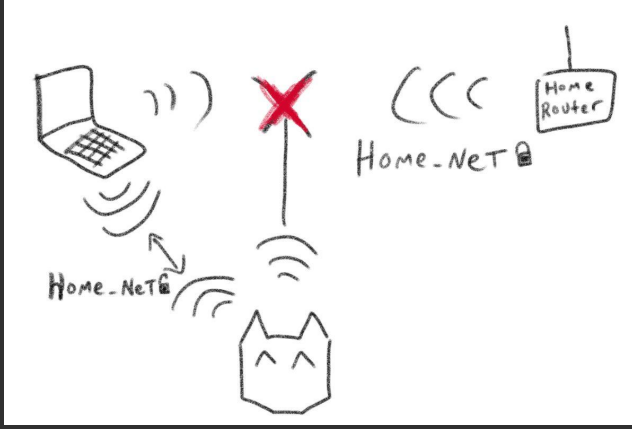
Wi-Fi phishing is part social engineering, part hacking. If you don’t know the Wi-Fi password, you can often trick someone into giving it to you!

Real Phishing Page

- A security researcher was compromised by this phishing Network Page in the wild
- Captive portal popup on mobile makes this look authentic
- Often customized to the brand of router



Anatomy of Wi-Fi Phishing



How phishing works:

- First, the hacker kicks the victim off their real network
- Next, the hacker makes an evil AP with the same name as the target network
- The evil AP has no password and pretends to be the router needing an update
- When the victim connects to the evil AP, they see a phishing page
- If the victim enters the Wi-Fi password, the attacker stops blocking the legitimate Wi-Fi network
- The victim feels a warm fuzzy feeling from updating their router and staying safe. In reality, they let the hacker in!

AP Command - Make a joinable Wi-Fi Network

```
# help ap

ap -s/sid  [-p/assword ] [-hidden] [-ch/annel <1>] [-b/ssid >]
  Start access point
  -s:  SSID network name
  -p:  Password with at least 8 characters
  -h:  Hidden network
  -ch: Channel (default=1)
  -b:  BSSID MAC address (default=random)
```

Let’s create a phishing network

Type this command, replacing the SSID with your own:
ap “RotSehenAberGehen”

Now, connect with your phone to the AP.
Do you get a “captive portal” popup?

Once you connect, you should see a notification like this from your Nugget.

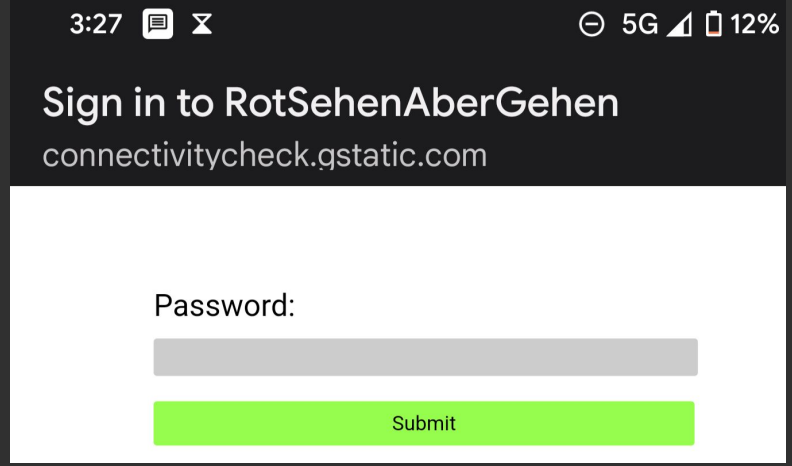
```
# ap RotSehenAberGehen

[ ========== Access Point ========== ]
SSID:       RotSehenAberGehen
Password:
Mode:       Open
Hidden:     False
Channel:    1
BSSID:      00:00:2c:c6:14:cd

Type 'stop ap' to stop the access point
[ ==================== Connections ==================== ]
IP-Address    MAC-Address       URL
=======================================================

192.168.4.100 92:f6:99:15:ba:2f /generate_204
192.168.4.100 92:f6:99:15:ba:2f /generate_204
192.168.4.100 92:f6:99:15:ba:2f /generate_204
192.168.4.100 92:f6:99:15:ba:2f /favicon.ico
192.168.4.100 92:f6:99:15:ba:2f /generate_204
```

Password Stealing Time

On your smartphone, type in a fake password and hit submit.

You should see the password you submitted appear in your serial terminal!

Remember this example any time you're asked to type passwords or login information into a captive portal!




```
# ap RotSehenAberGehen

> Stopped access point

[ ========= Access Point ========= ]
SSID:       RotSehenAberGehen
Password:
Mode:       Open
Hidden:     False
Channel:    1
BSSID:      00:03:2a:b6:78:cd

Type 'stop ap' to stop the access point
[ ================== Connections ================== ]
IP-Address     MAC-Address        URL
=================================================
192.168.4.100 92:f6:99:15:ba:2f /generate_204
192.168.4.100 92:f6:99:15:ba:2f /generate_204
192.168.4.100 92:f6:99:15:ba:2f /generate_204
192.168.4.100 92:f6:99:15:ba:2f /favicon.ico
192.168.4.100 92:f6:99:15:ba:2f /generate_204
192.168.4.100 92:f6:99:15:ba:2f /generate_204?password=ILoveToJaywalk4Lyfe
192.168.4.100 92:f6:99:15:ba:2f /favicon.ico
192.168.4.100 92:f6:99:15:ba:2f /generate_204
192.168.4.100 92:f6:99:15:ba:2f /generate_204
```

Self Defense Tips - Wi-Fi Habits

- Never join an open network with the same Wi-Fi name as your protected home or work network - it’s a trick!
- Never type your Wi-Fi network password into a website
- Delete any saved open Wi-Fi networks in your phone
- Set saved Wi-Fi networks to not auto-join
- Use a VPN to prevent an evil network from snooping or modifying your traffic

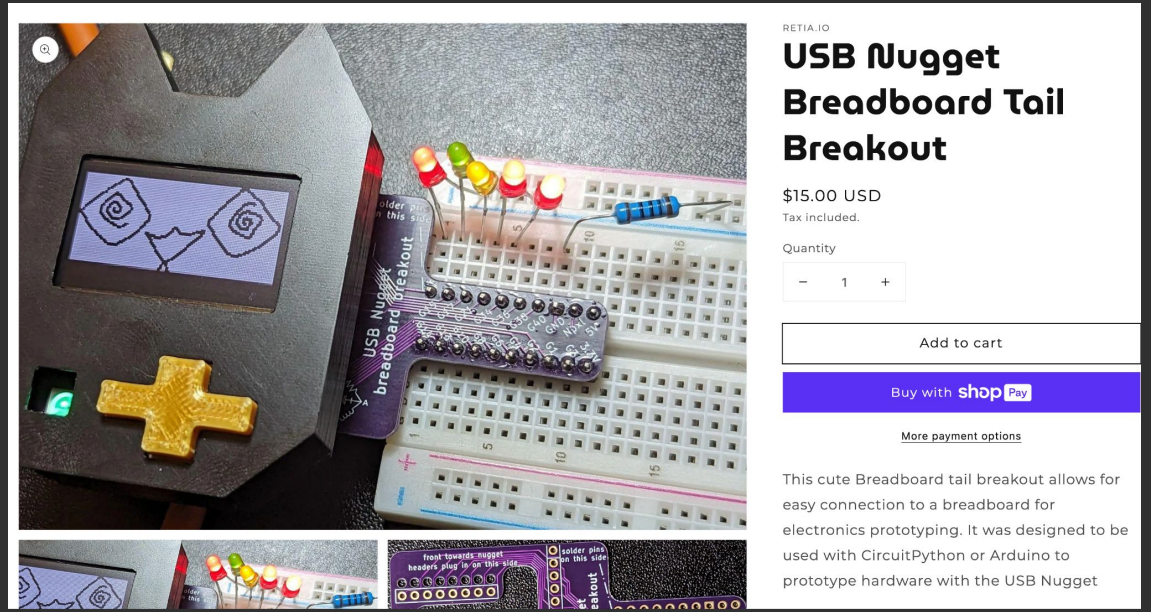
Self Defense Tips - Hidden Networks

- Do not add networks via QR code.
- If you must, use a QR scanner that shows the raw text and verify it isn’t a hidden network
- Don’t use hidden networks

Teach a friend!

We have kits on Retia.io and discounts for instructors teaching classes!

- Nuggets
- Add-ons
- Online classes



Keep in Touch

Want to learn more? You can find us here:

- Discord: https://discord.gg/rjVJbauAUX
- Store: Retia.io
- Nugget Flasher: Nugget.dev
- Livestreams: youtube.com/@SecurityFWD