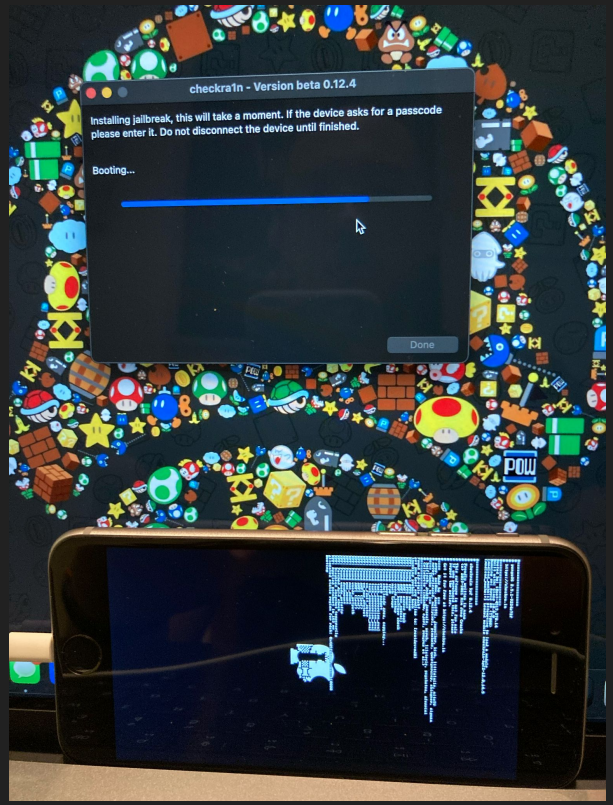
demo: iPhone bridging

demo: iPhone bridging – iPhone prep

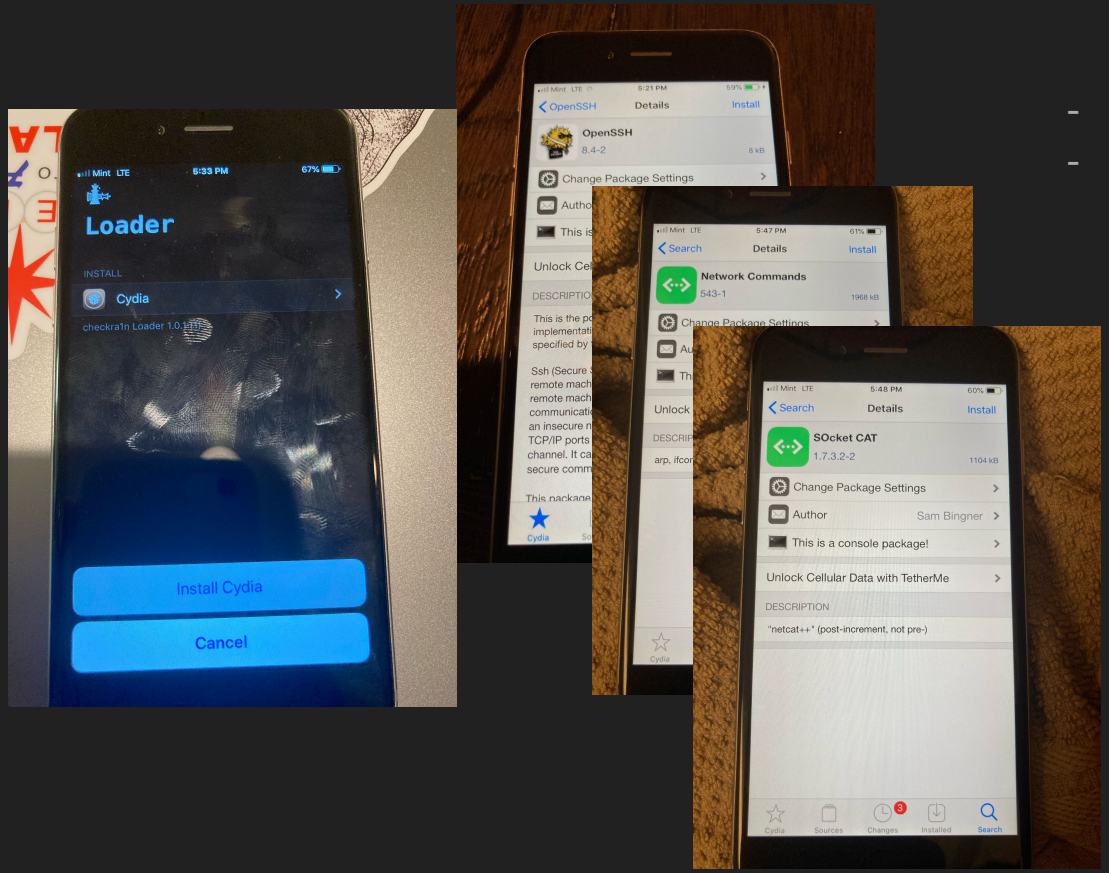
- Install WireGuard via app store

demo: iPhone bridging – iPhone prep



- Jailbreak (checkra1n pictured)

demo: iPhone bridging – iPhone prep

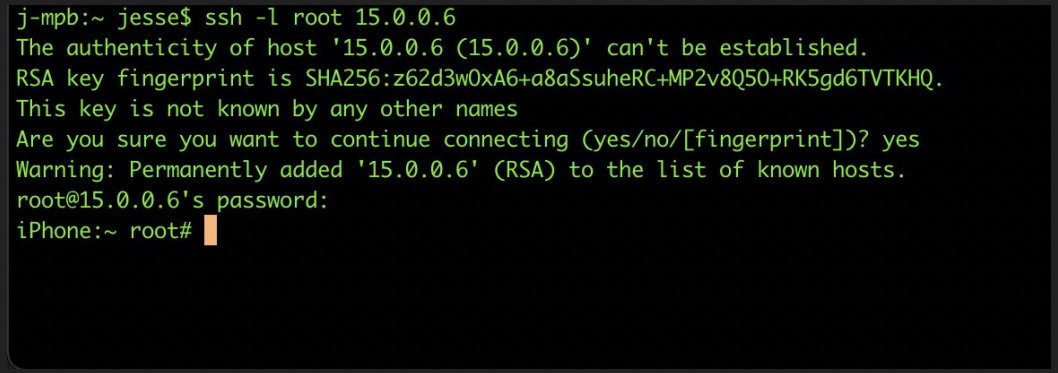


- Install Cydia via checkra1n app
- Install OpenSSH, network commands, socat and wifiutils

demo: iPhone bridging – iPhone prep

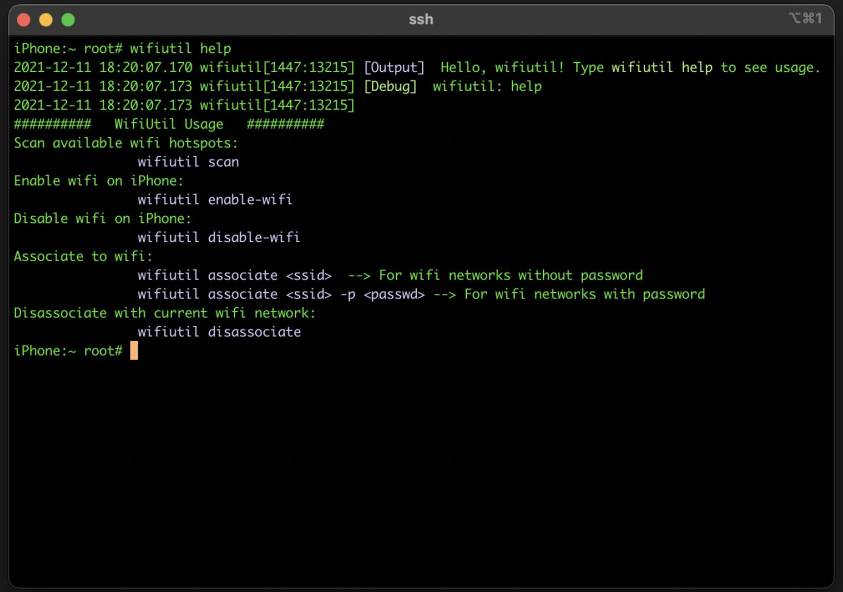
- Alternatively, you can install via SSH command line
- Pictured: apt update && apt install org.thebigboss.wifiutil

demo: iPhone bridging – Remote pentester



- You've now turned your phone into a pentesting tool.
- SSH into the iPhone

demo: iPhone bridging – Remote pentester



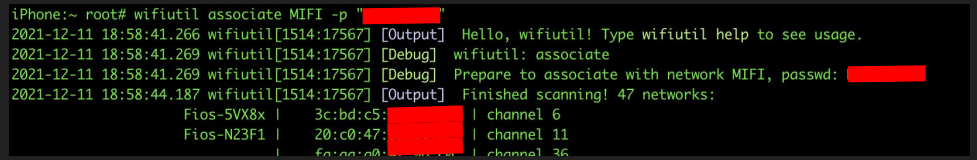
- Begin running wifiutil

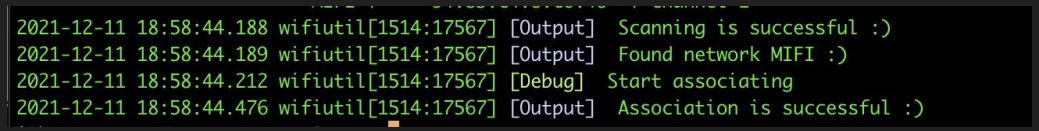
- wifiutil scan – helps you determine when you're in proximity of target AP

demo: iPhone bridging – Remote pentester

- wifiutil handles toggling the WiFi on and off on the iPhone
- At no point does the physical pentester/tiger team need to remove the iPhone from their pocket

demo: iPhone bridging – Remote pentester





- When you identify your target AP, run wifiutil associate command
- This is assuming you have captured password in a previous phase of your pentesting

demo: iPhone bridging – Remote pentester

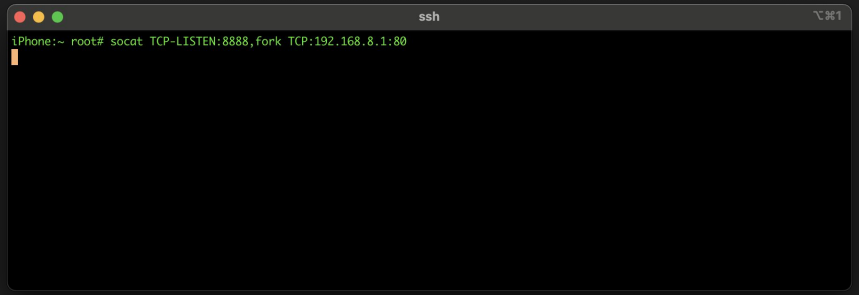
```
iPhone:~ root# ifconfig en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500 rtref 0 index 9
        eflags=412008c0<ACCEPT_RTADV,TXSTART,ARPLL,NOACKPRI,ECN_ENABLE,FASTLN_ON>
        options=400<CHANNEL_IO>
        ether cc:25:ef:[redacted]
        inet6 f[redacted] prefixlen 64 secured scopeid 0x9
        inet 192.168.8.232 netmask 0xffffff00 broadcast 192.168.8.255
        netif: 39DB3111-9E30-4[redacted]
        multistack: 100EE1BD-F0E3-4[redacted]
        media: autoselect
        status: active
        nd6 options=201<PERFORMNUD,DAD>
        type: Wi-Fi
        agent domain:Skywalk type:FlowSwitch flags:0x83 desc:"MultiStack"
        link quality: 100 (good)
        state availability: 0 (true)
        qosmarking enabled: yes mode: none
iPhone:~ root#
```

- Discover your environment

- Identify your target IP (in this example, I am targeting the upstream router)

```
iPhone:~ root# arp -a
console.gl-inet.com (192.168.8.1) at 94:83:c4:[redacted]0 ifscope [ethernet]
? (224.0.0.251) at 1:0:[redacted]en0 ifscope permanent [ethernet]
iPhone:~ root#
```

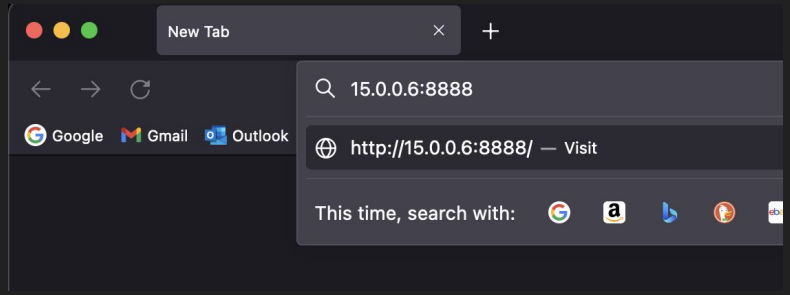
demo: iPhone bridging – Remote pentester



- Prepare your socat command

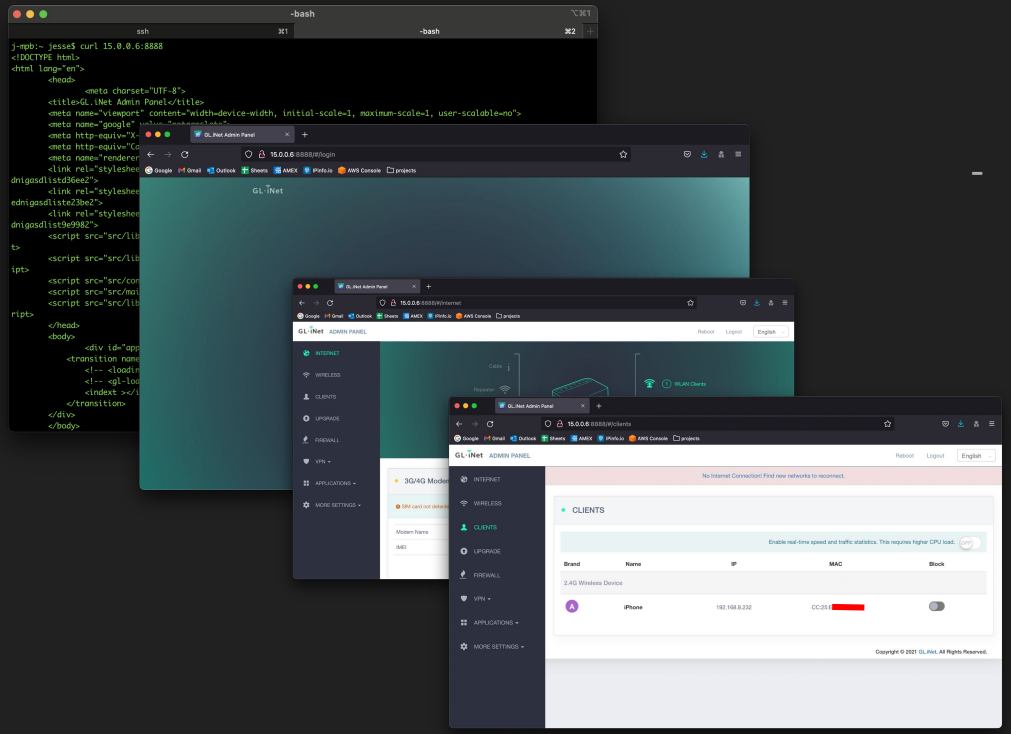
- Your mileage may vary targeting different protocols and services

demo: iPhone bridging – Remote pentester



- Navigate to iPhone WireGuard IP and socat port

demo: iPhone bridging – Success!



- Interact with target as if you were connected directly to the wireless LAN