Breaking into WiFi Networks*

*only when you have permission
Prerequisites

1. Kali Linux
2. A supported wireless card
3. A GPU or an AWS account (optional)
Types of WiFi Security

In order of effectiveness

1. No Encryption
2. Hidden SSID
3. WEP
4. WPA2 Personal with WPS
5. WPA2 Personal without WPS
6. WPA2 Enterprise
Getting Past Hidden SSIDs

1. Launch Kismet
2. Wait
3. or... aireplay-ng
   a. Floods clients with spoofed de-auths
4. Profit
Breaking WEP Encryption

1. Airodump-ng
   a. Capture around 15000 packets
   b. Takes around 10-15 minutes
      i. or... aireplay-ng

2. Aircrack-ng
   a. Takes 5 minutes max

3. Profit
Breaking WPA2 with WPS

1. Wash
   a. Finds networks with WPS enabled

2. Reaver
   a. WPS is an 8 digit base-10 password
   b. θ_θ
   c. 8th digit is a checksum so it's really a 7 digit password
   d. θ_θ
   e. Router tells you when you get the first 4 digits correct
   f. θ_θ

3. Profit
   a. Only works on most routers
Getting into WPA2 Personal

1. Airodump-ng
   a. Capture handshake
      i. Aireplay-ng if necessary

2. Aircrack-ng dictionary attack
   a. Key must be in dictionary
   b. Lenovo x201 i7 runs about 300 keys/sec
   c. GRAPHICS CARDS
   d. Other programs may be faster
   e. Can use AWS EC2 G2 in a pinch

3. Profit
Getting into WPA2 Enterprise

WPA2 Enterprise is the most secure

1. Set up fake AP
2. Connect fake AP to FreeRADIUS-WPE
3. Wait to capture an attempted authentication
   a. or... aireplay-ng
4. Brute force challenge response pair
5. Profit
NEVER TRUST WIRELESS COMMUNICATIONS
Bonus Round: WiFi Paywalls

1. Launch Kismet
2. Find a MAC address that's already paid
3. Spoof that MAC address
4. Wait for the other person to give up
5. Profit
Questions?