

Date: 2019-09-03 Author: Ian Rash Index: #2

Before I work on sniffing the client communications, I wanted to try a little discovery first to see anything interesting with the device.

Nmap

Since the device was pretty much a black box to me, I wanted to see if I could discover any services/open ports beforehand. Nmap didn't notice any open ports when I scanned, which was a bit odd.

Setting up network sniffing

You can set this up one of two ways depending on the hardware.

Poor man's method

Two USB to Ethernet Dongles ([Recommended](#)) Two PCI Wired Ethernet Cards

Use a utility called [brctl](#), it's fairly straight forward to set this up, but I did have issues here and there with weird drops in connection.

These are the commands I used *brctl addbr br0 brctl addif br0 [camera-interface] * brctl addif br0 [sniffing-interface]*

Rich man's method

For this you need *One USB to Ethernet Dongle or PCI Wired Ethernet Card Enterprise level switch*

When I found out I could do this with my Cisco Catalyst 3750 I was ecstatic. For some reason, bridging didn't always work 100% as expected with the USB dongles and sometimes my internet would drop out while I was listening in on the camera. Once I found out you can use monitor session to forward packets from the camera to a one directional port, it saved me a lot of time and heart ache.

Just add this to your config. *monitor session 1 source interface Gi4/0/13 monitor session 1 destination interface Gi4/0/23*

You can then plug ther USB dongle into the switch on port 23, and all port 13 traffic will be routed there as well!

TAGGED SKILLS:

 Reverse Engineering  Security Research  Exploit PoC Development  C  Crystal

