

Alexei Hooks

Cyber 440

Professor Moeller

September 15, 2022

Individual Analytic Lab – Network Analytic via PCAP

BLUF to Management

When working through the PCAP file that was provided to me, I noticed that there was a TCP ping sweep within the packet capture. The packet numbers in question are from frame 868716 to frame 1008718. A TCP ping sweep is a way for attackers to scan all available TCP ports that map to used hosts. This could potentially be used against the company as a foreign actor to the network now might be able to tell what live service we use, and therefore could concoct a plan against a found vulnerability. The use of port sweeps is a reconnaissance tactic used by hackers in order to better plan their next move. Being able to pick this up in the PCAP file should be able to give us the right details to be on high alert moving forward as a cyber-attack may be imminent.

As I started out in my investigation of the network, I had to split the PCAP file up in order to better analyze the data. To do this, I used the program Splitcap which is run through Linux systems. For this, I used Kali and broke up the original PCAP into about 2 million frames per file, making 5 separate packet captures to analyze.

I was hoping that searching for Dynamic Host Configuration Protocol (dhcp) traffic to enable me to more easily search through potentially suspicious IP addresses, but no such traffic came back from filtering. Next, I filtered the PCAP files for NetBIOS Name Server (nbns) traffic, but none of the split files had any on each of them. This would have let me see if this was organizational network traffic, and if there were any hosts within it. Since there were no hits when filtering the packets, this meant that the network was not part of an organization. After each of these, I filtered for ARP (Address Resolution Protocol) Requests which actually resulted in a successful search. An ARP filter search looks for hosts with changing or static IP addresses, and their MAC addresses in a Local-area Network (LAN). With this information, I was able to look at the hosts on the network, included below, and how each communicated through the network captures.

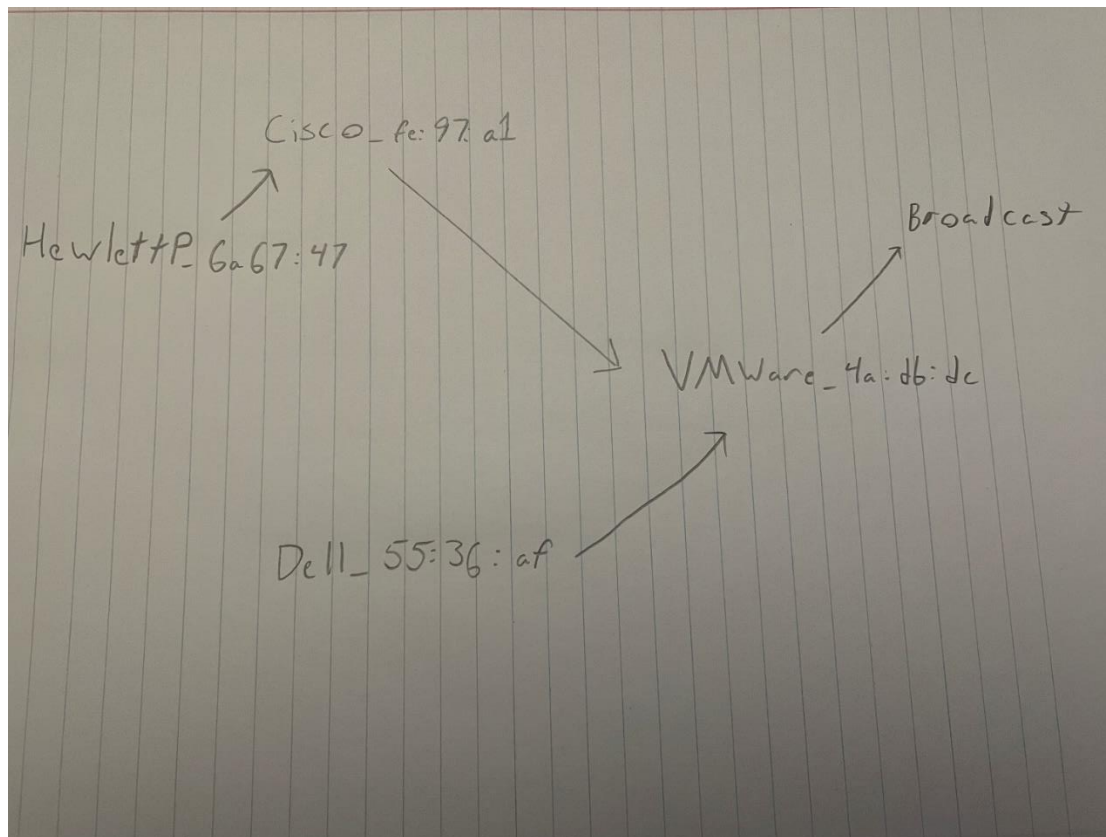
List of Hosts and List of Port Numbers that Offer Services

By manually running through packet frames and running a filter to search for ARP Requests, I was able to put a list of 5 hosts together. They read as such:

<u>Host</u>	<u>IP Address</u>	<u>Port Number</u>
HewlettP_6a:67:47	192.168.1.--	514 (TCP)
Cisco_fe:97:a1	10.200.150.--	80 (HTTP)
Dell_55:36:af	192.168.1.--	443 (HTTPS)
VMware_4a:db:dc	172.20.1.--	80 (HTTP)

Each of these hosts contacted at least one of the others throughout my viewing of the PCAP file. It seemed as if the hosts all run though VMware to a broadcast. I am unsure what this means at this time.

Network Diagram



Included Screen Captures as Evidence of HP being a host:

45 0.000526	192.168.1.1	192.168.1.50	UDP	231 514 → 514 Len=189[Packet size limited during capture]
46 0.000538	10.200.150.209	172.20.1.5	TCP	73 4101 → 80[Packet size limited during capture]
47 0.000545	10.200.150.209	172.20.1.5	TCP	73 4101 → 80[Packet size limited during capture]
48 0.000556	10.200.150.208	172.20.1.5	TCP	73 3502 → 80[Packet size limited during capture]
49 0.000564	10.200.150.208	172.20.1.5	TCP	73 3502 → 80[Packet size limited during capture]
50 0.000579	192.168.1.1	192.168.1.50	UDP	231 514 → 514 Len=189[Packet size limited during capture]
51 0.000599	192.168.1.1	192.168.1.50	UDP	231 514 → 514 Len=189[Packet size limited during capture]
52 0.000611	10.200.150.206	172.20.1.5	TCP	60 1808 → 80[Packet size limited during capture]

```

[Coloring Rule String: udp]
ethernet II, Src: Cisco_fe:97:a0 (d0:d0:fd:fe:97:a0), Dst: HewlettP_6a:67:47 (00:16:35:6a:67:47)
  Destination: HewlettP_6a:67:47 (00:16:35:6a:67:47)
    Address: HewlettP_6a:67:47 (00:16:35:6a:67:47)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
  Source: Cisco_fe:97:a0 (d0:d0:fd:fe:97:a0)
    Address: Cisco_fe:97:a0 (d0:d0:fd:fe:97:a0)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
  
```

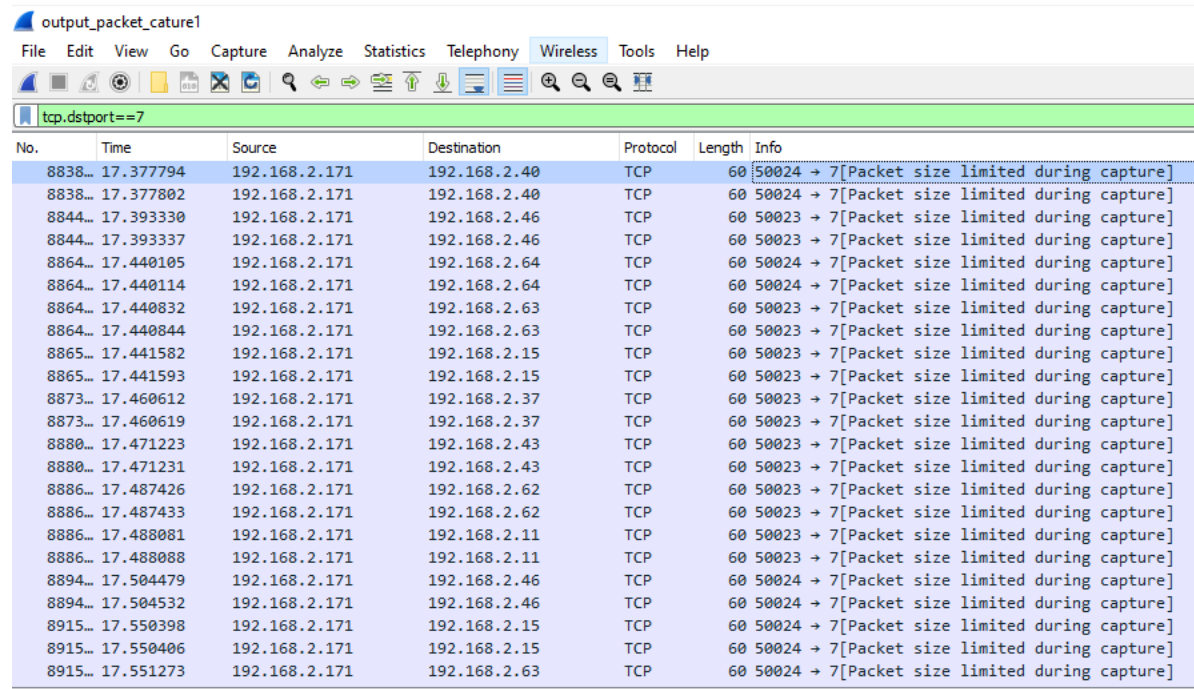
MAC Prefix	Vendor / Company	Address	Country
00-16-35 / 001635	Hewlett Packard	20555 State Highway 249 Houston TX 77070	US

Indicators of Compromise

TCP Ping Sweep:

This sweep is an IOC being that it shows the users that the network has been tampered with unknowingly. Having someone in the system is an issue, but one who now knows the landscape of your network is much more of a threat. Being that this sweep happened, high alert status should be in effect and an audit of the network should take place.

Below is only a part of the sweep that I was able to find, as it was too big to fit in one screen capture.



No.	Time	Source	Destination	Protocol	Length	Info
8838...	17.377794	192.168.2.171	192.168.2.40	TCP	60	50024 → 7[Packet size limited during capture]
8838...	17.377802	192.168.2.171	192.168.2.40	TCP	60	50024 → 7[Packet size limited during capture]
8844...	17.393330	192.168.2.171	192.168.2.46	TCP	60	50023 → 7[Packet size limited during capture]
8844...	17.393337	192.168.2.171	192.168.2.46	TCP	60	50023 → 7[Packet size limited during capture]
8864...	17.440105	192.168.2.171	192.168.2.64	TCP	60	50024 → 7[Packet size limited during capture]
8864...	17.440114	192.168.2.171	192.168.2.64	TCP	60	50024 → 7[Packet size limited during capture]
8864...	17.440832	192.168.2.171	192.168.2.63	TCP	60	50023 → 7[Packet size limited during capture]
8864...	17.440844	192.168.2.171	192.168.2.63	TCP	60	50023 → 7[Packet size limited during capture]
8865...	17.441582	192.168.2.171	192.168.2.15	TCP	60	50023 → 7[Packet size limited during capture]
8865...	17.441593	192.168.2.171	192.168.2.15	TCP	60	50023 → 7[Packet size limited during capture]
8873...	17.460612	192.168.2.171	192.168.2.37	TCP	60	50023 → 7[Packet size limited during capture]
8873...	17.460619	192.168.2.171	192.168.2.37	TCP	60	50023 → 7[Packet size limited during capture]
8880...	17.471223	192.168.2.171	192.168.2.43	TCP	60	50023 → 7[Packet size limited during capture]
8880...	17.471231	192.168.2.171	192.168.2.43	TCP	60	50023 → 7[Packet size limited during capture]
8886...	17.487426	192.168.2.171	192.168.2.62	TCP	60	50023 → 7[Packet size limited during capture]
8886...	17.487433	192.168.2.171	192.168.2.62	TCP	60	50023 → 7[Packet size limited during capture]
8886...	17.488081	192.168.2.171	192.168.2.11	TCP	60	50023 → 7[Packet size limited during capture]
8886...	17.488088	192.168.2.171	192.168.2.11	TCP	60	50023 → 7[Packet size limited during capture]
8894...	17.504479	192.168.2.171	192.168.2.46	TCP	60	50024 → 7[Packet size limited during capture]
8894...	17.504532	192.168.2.171	192.168.2.46	TCP	60	50024 → 7[Packet size limited during capture]
8915...	17.550398	192.168.2.171	192.168.2.15	TCP	60	50024 → 7[Packet size limited during capture]
8915...	17.550406	192.168.2.171	192.168.2.15	TCP	60	50024 → 7[Packet size limited during capture]
8915...	17.551273	192.168.2.171	192.168.2.63	TCP	60	50024 → 7[Packet size limited during capture]

Unsecure Ports:

When looking through what ports the hosts used, seeing that port 80 is continually being used is concerning. As there is a secure version of this port, it almost always should be in use. Transfer all port 80 (HTTP) traffic to port 443 (HTTPS).