Robert Carpenter
github.com/robertmcarpenter
Sat December 14th 2024

Lab 6.5.4 Analyzing an ARP Poisoning Attack with Wireshark

From TestOut CompTIA Security+ Course

In this lab I will be securing and hardening a Cisco Managed switch.

The scenario for this lab is as follows:

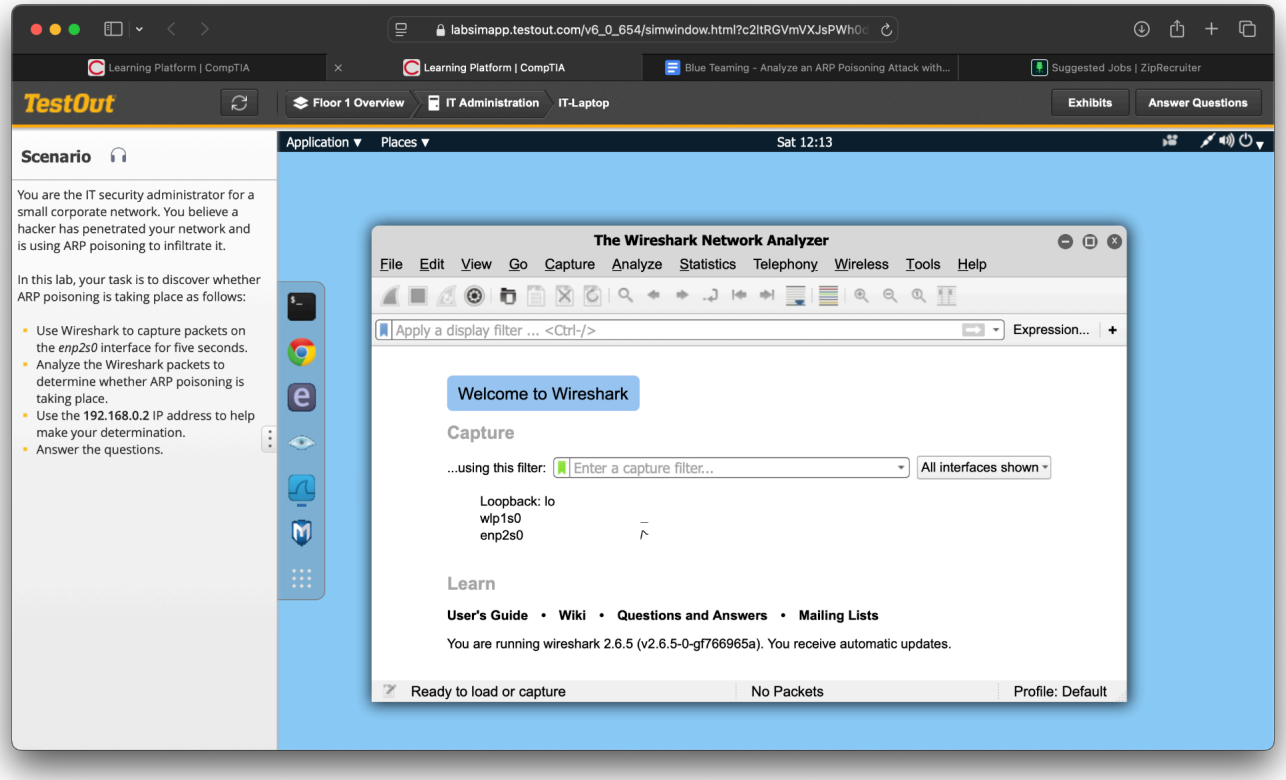
“You are the IT security administrator for a small corporate network. You believe a hacker has penetrated your network and is using ARP poisoning to infiltrate it.

In this lab, your task is to discover whether ARP poisoning is taking place as follows:

- Use Wireshark to capture packets on the *enp2s0* interface for five seconds.
- Analyze the Wireshark packets to determine whether ARP poisoning is taking place.
- Use the **192.168.0.2** IP address to help make your determination.
- Answer the questions:
    - What is the MAC Address of the First Responding Device
    - What is the MAC Address of the duplicate Responding device?”

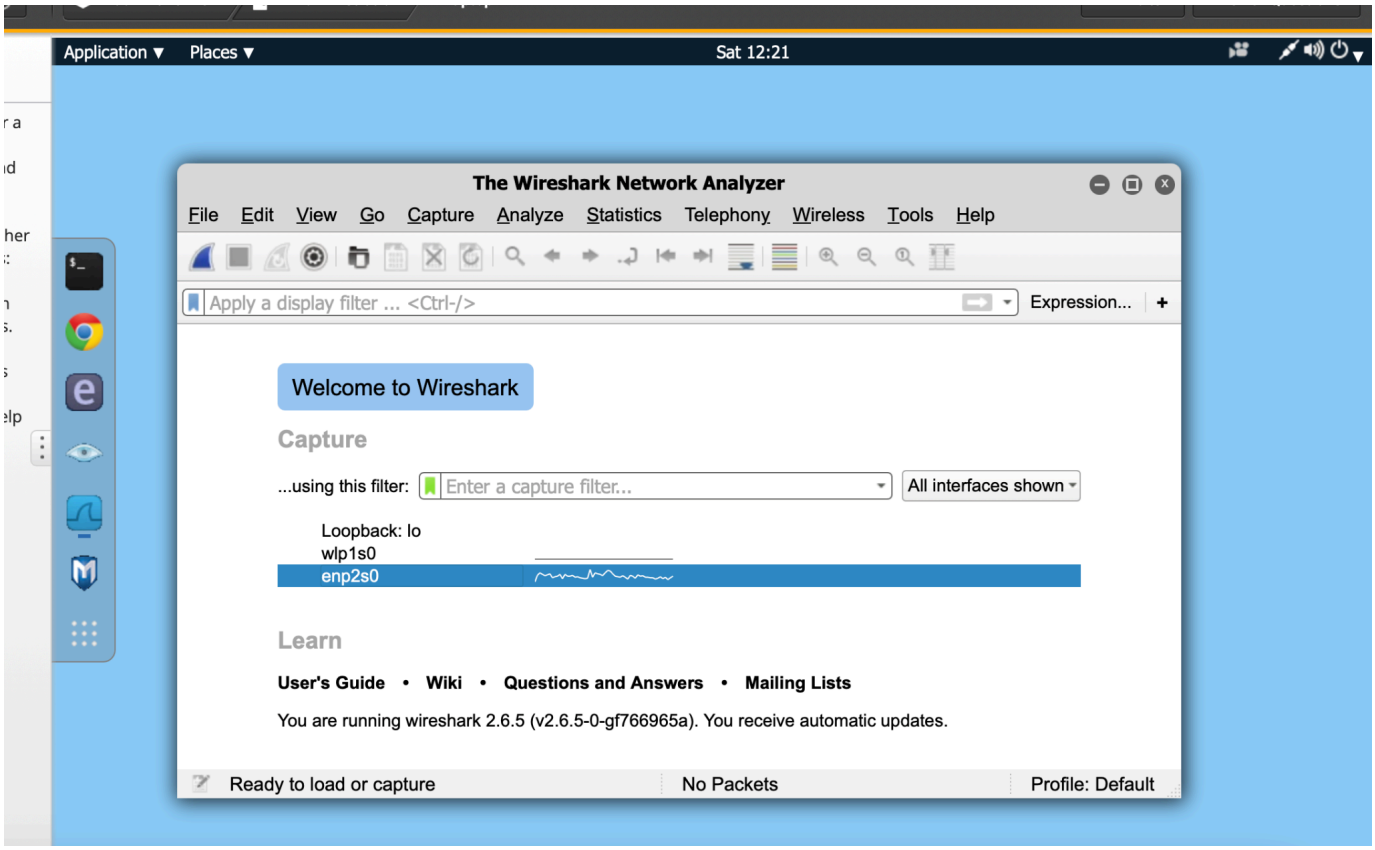
To start this lab, I will open up Wireshark within the Kali Linux box that is made available to me in this lab:

Robert Carpenter
github.com/robertmcarpenter
Sat December 14th 2024

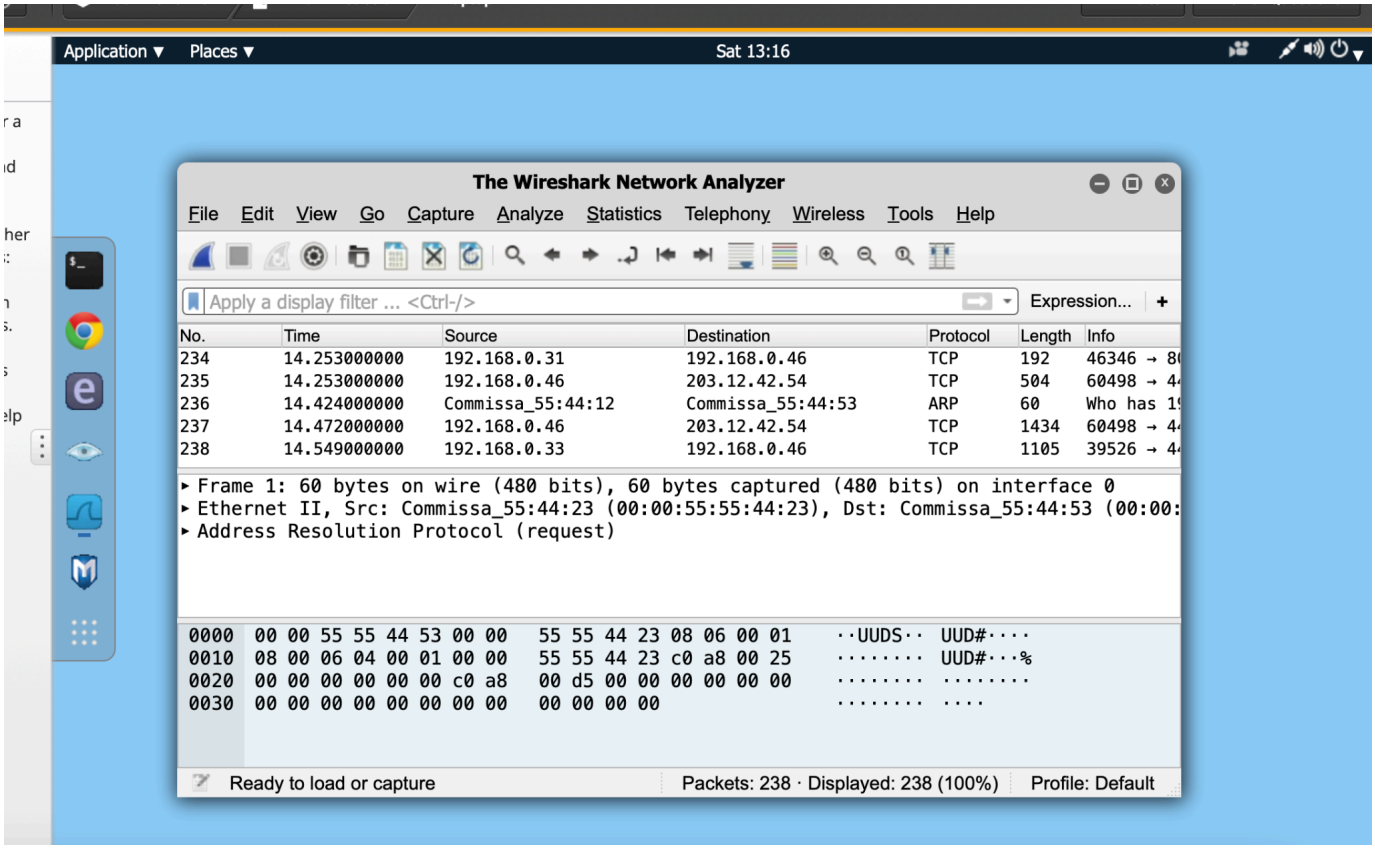


The Lab wants us to listen in on the **enp2s0** ethernet interface for 5 seconds and analyze the packets. TO do that, I'll click the interface in the window shown above so that its highlighted , then I'll click the Blue Fin in the top left corner to start capturing packets.

Robert Carpenter
github.com/robertmcarpenter
Sat December 14th 2024

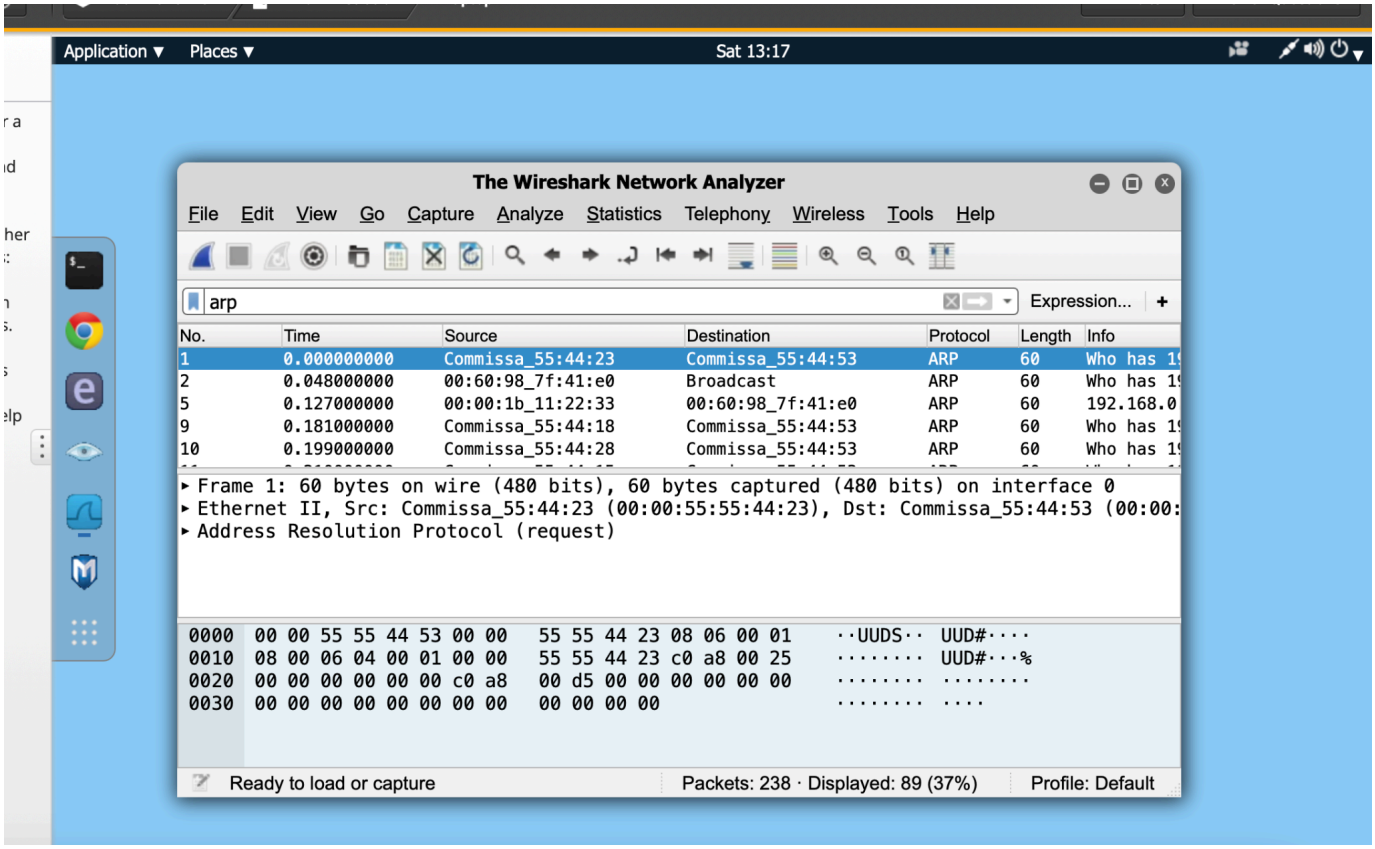


Robert Carpenter
github.com/robertmcarpenter
Sat December 14th 2024



As you can see many packets were captured in this mere 5 second period. This can be overwhelming but luckily Wireshark includes a way to filter packets by protocol. In the **Apply a display filter** field , I can enter **arp** to see all of the **ARP packets.**

Robert Carpenter
github.com/robertmcarpenter
Sat December 14th 2024

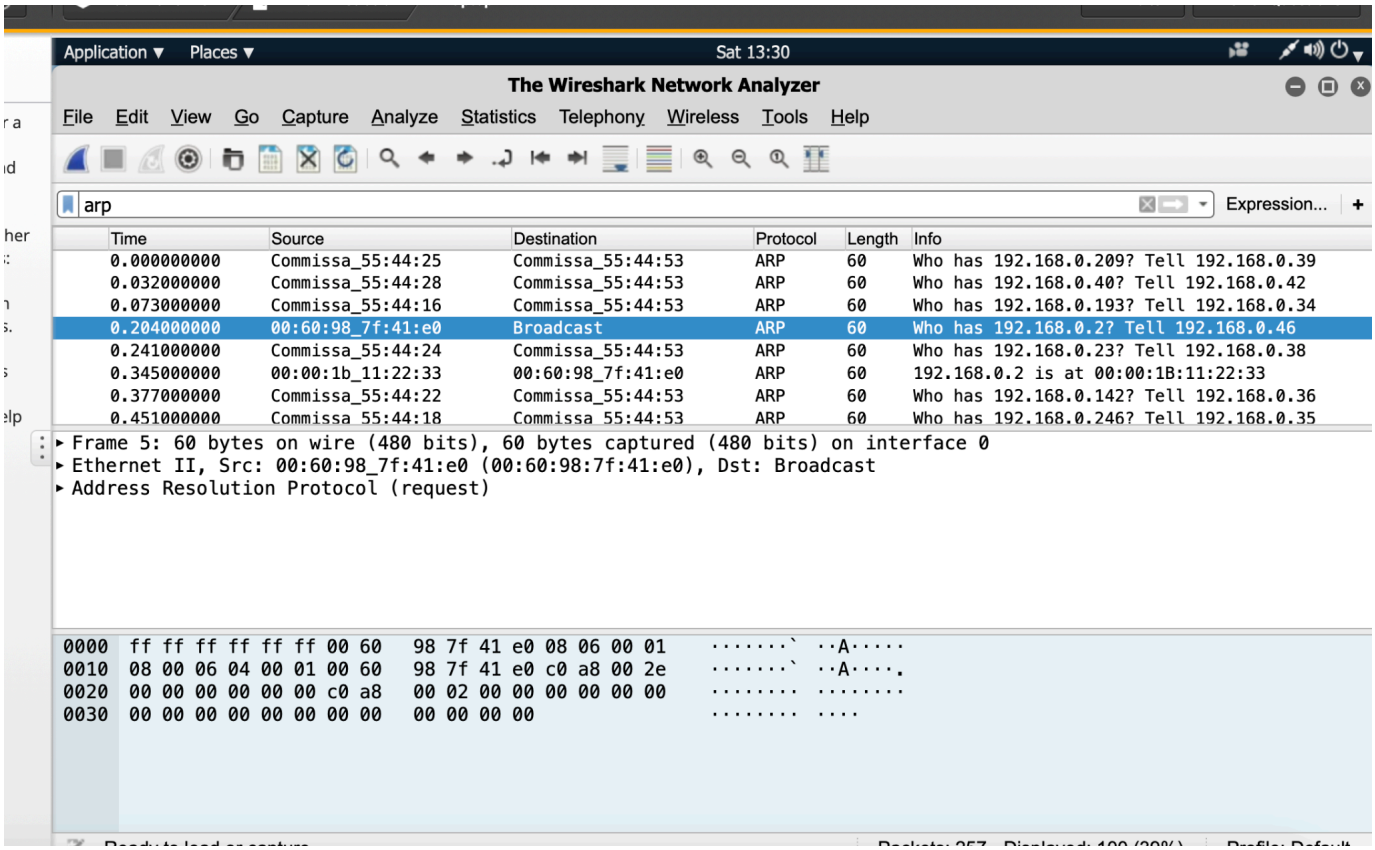


With the packets now filtered we can look for the IP address given to us by the lab.

They would like us to use the address **192.168.0.2** to make our determination. I only see about 2 entries asking the network “**Who has 192.168.0.2”**

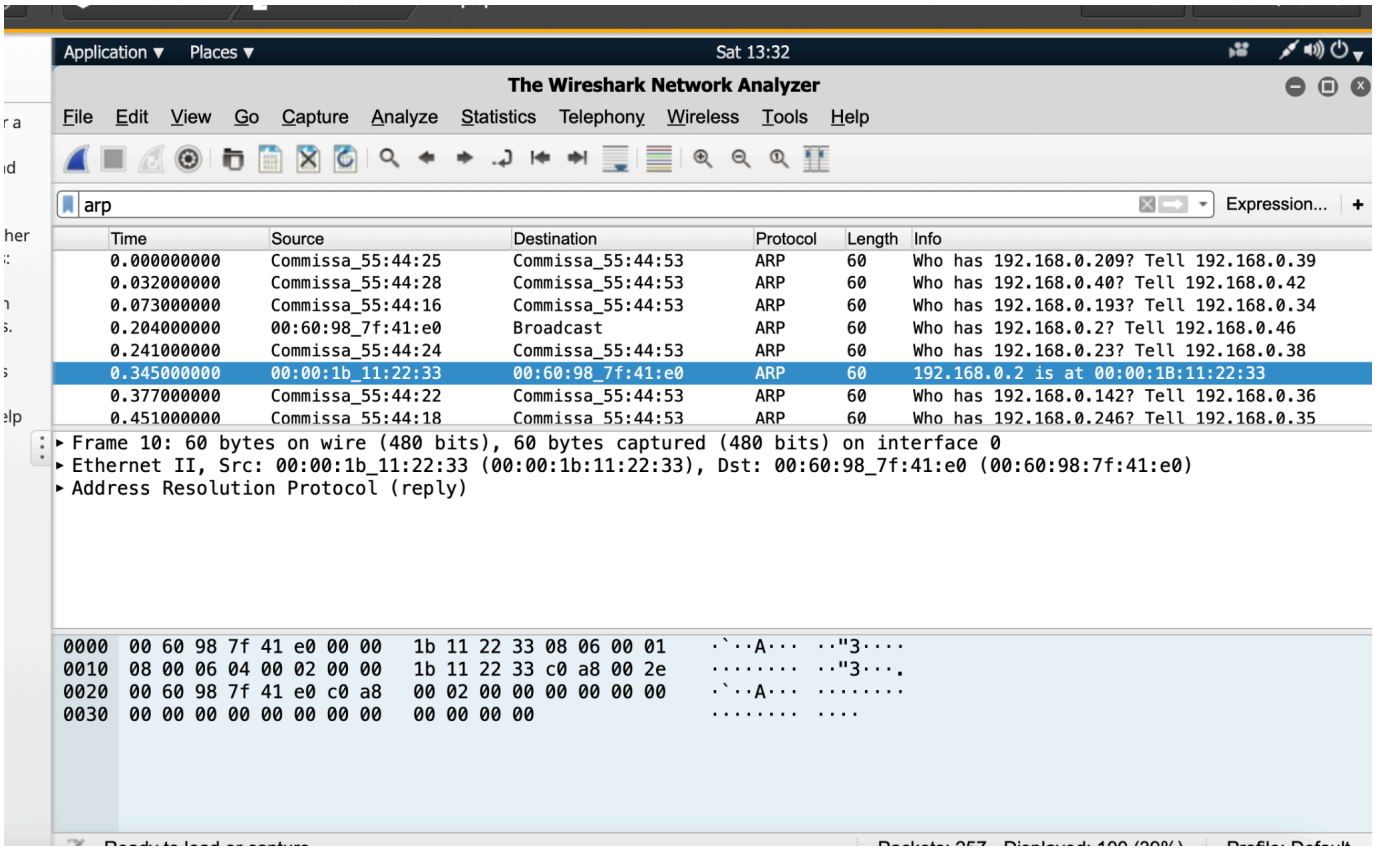
There is a suspicious entry I see which is a duplicate response to 198.168.0.2. This means an attacker is trying to overwrite the ARP table so that **198.168.0.2** points to **00:00:1b_11:22:33** instead of the real address which is **00:00:1b_33:22:11.**

Robert Carpenter
github.com/robertmcarpenter
Sat December 14th 2024

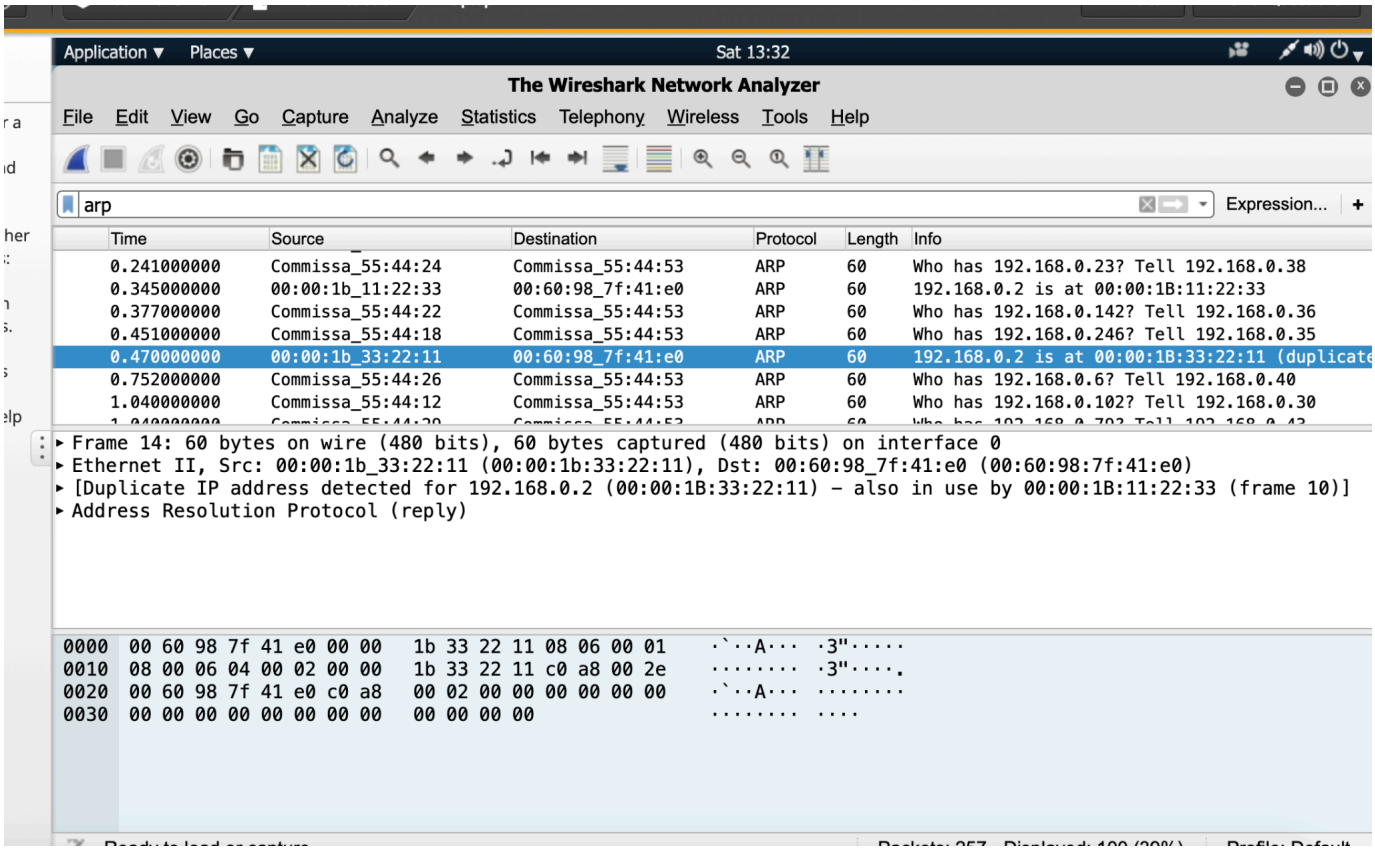


The highlighted packet is a broadcast message asking who has **198.168.0.2** . The next packet below is a response from: (see screenshot)

Robert Carpenter
github.com/robertmcarpenter
Sat December 14th 2024



Robert Carpenter
github.com/robertmcarpenter
Sat December 14th 2024



As you can see this packet tells us that this is a duplicate response meaning that there is a discrepancy between the original MAC address and the one thats listed in this packet. This means the attacker has replaced the MAC with theirs on the switch's ARP table and has now effectively hijacked the **198.168.0.2** Layer 3 address.

We can determine that this indeed is an ARP attack. I'll answer the following questions and then wrap up this lab.

- What is the MAC Address of the First Responding Device?
- What is the MAC Address of the duplicate Responding device?

Robert Carpenter
github.com/robertmcarpenter
Sat December 14th 2024