ARP Spoofing

- ARP Spoofing Explained: ARP spoofing involves manipulating the ARP (Address Resolution Protocol) entries in a device's ARP table, changing the MAC-to-IP address mapping to deceive the network into recognizing one device as another. This method is akin to MAC and IP spoofing, where the aim is to alter the network's perception of device identities.

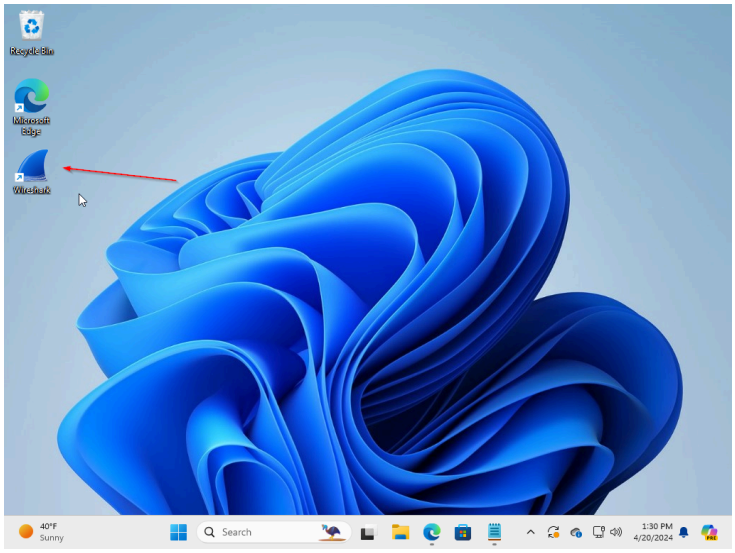
- Prevention Measures: To prevent ARP spoofing, as well as MAC and IP spoofing, implement DHCP snooping alongside Dynamic ARP Inspection (DAI). These techniques verify the integrity of both DHCP and ARP communications, ensuring the authenticity and reliability of device addressing within the network.

Equipment and Software Needed

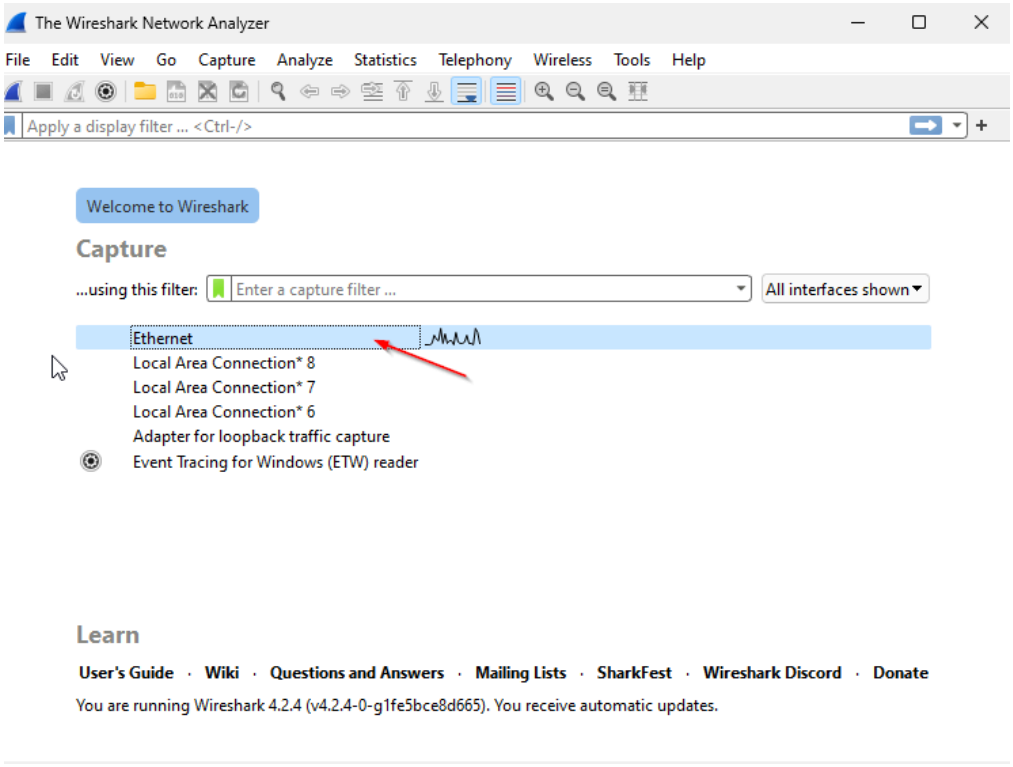
- Windows 11 virtual machine
- Network traffic capturing tool (Wireshark)
- Command Prompt with administrative privileges

Step 1: Capture Network Traffic

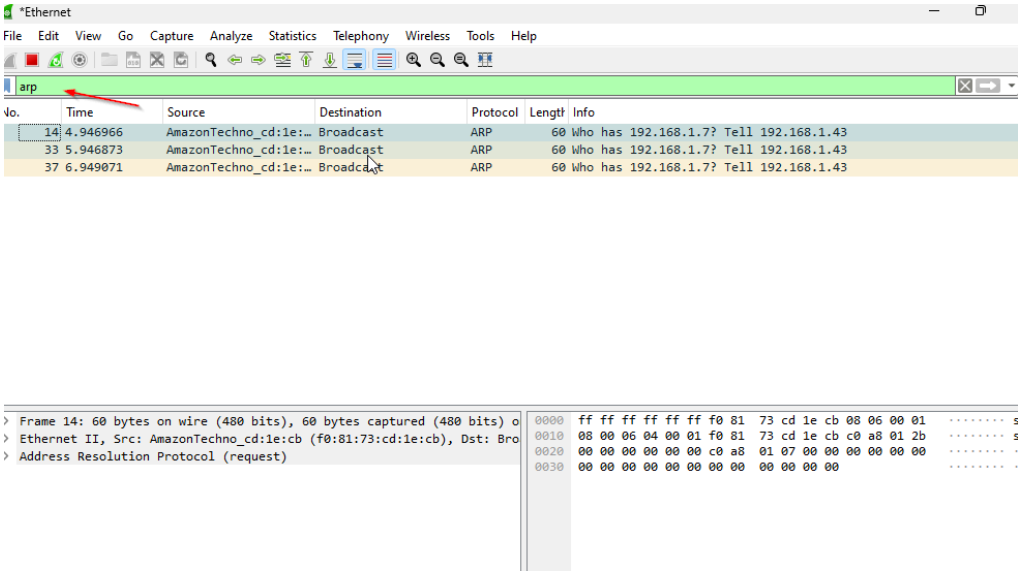
1. Open Wireshark:
    - Launch Wireshark on the Windows 11 virtual machine.



2. Select the Network Adapter:
    - Double-click on the network adapter you plan to monitor. If there's only one adapter available, select that one.

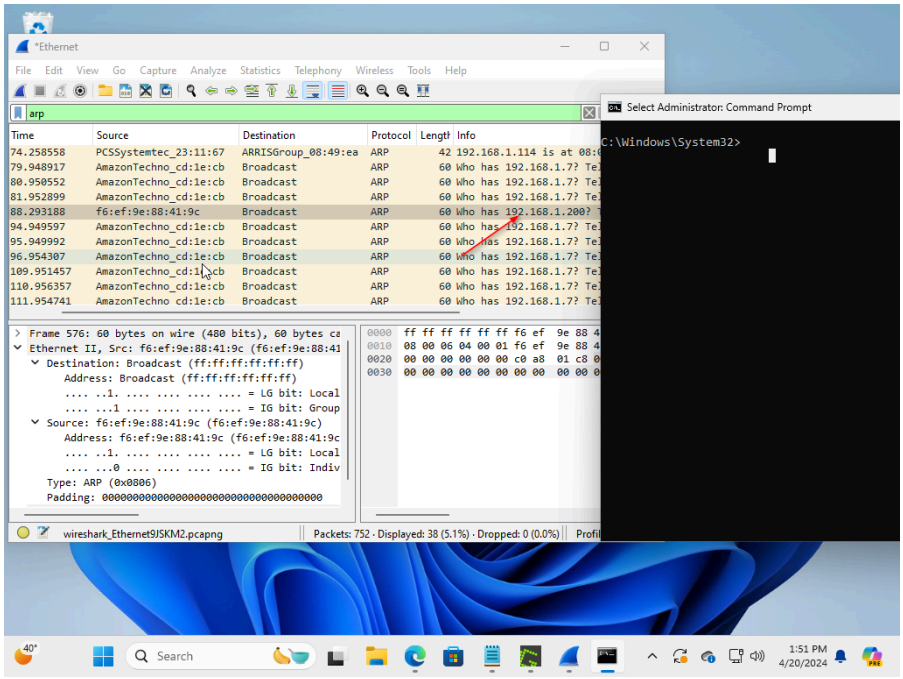


3. Filter for ARP Traffic:
    - Set a filter in Wireshark to display only ARP packets by typing `arp` in the filter bar.



4. Start Capturing Traffic:
    - Begin the capture and let it run briefly to collect sufficient ARP data.

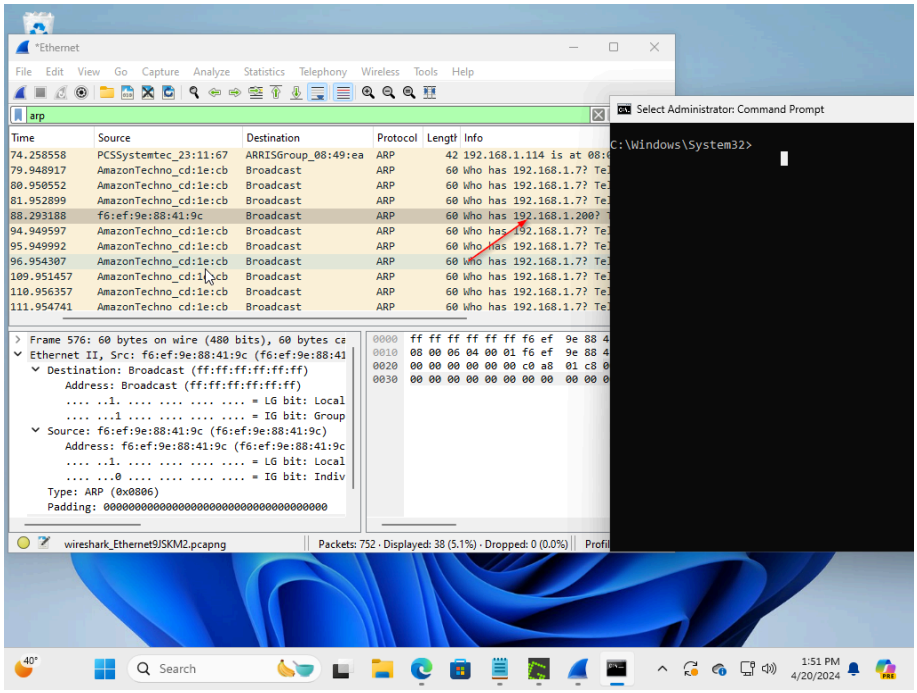
5. Identify a Target ARP Entry:
    - Look for an ARP packet that shows a MAC address and its associated IP address which isn't the IP of your virtual machine.



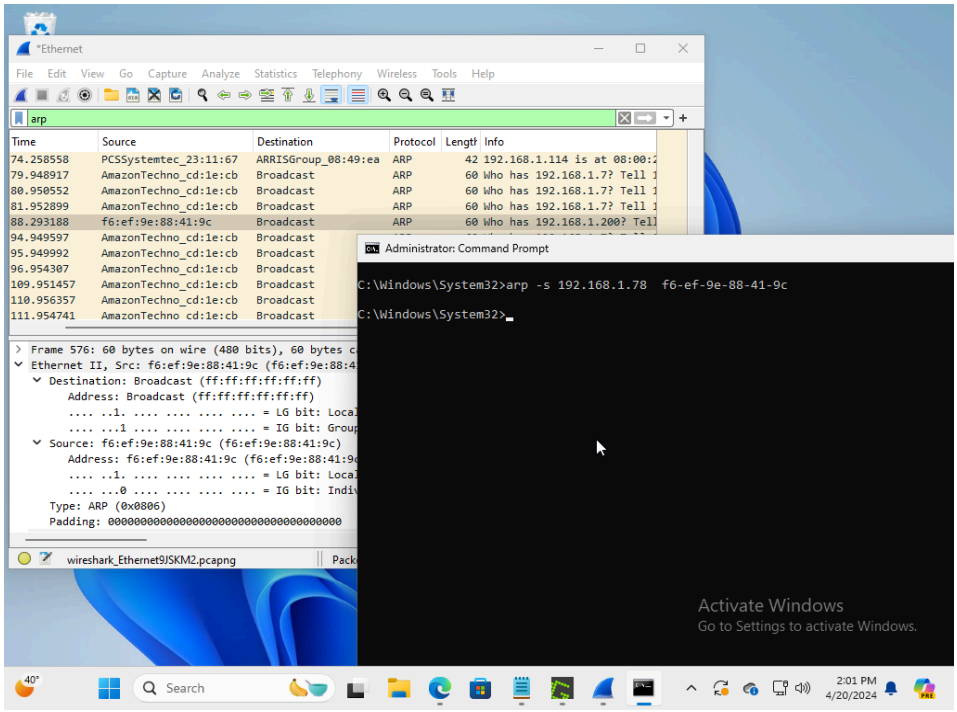
Step 2: Manipulate the ARP Table

1. Open Command Prompt as Administrator:
    - Click the Start button, type **cmd**, right-click on Command Prompt, and select 'Run as administrator'.
    - Click 'Yes' on the User Account Control prompt to proceed.

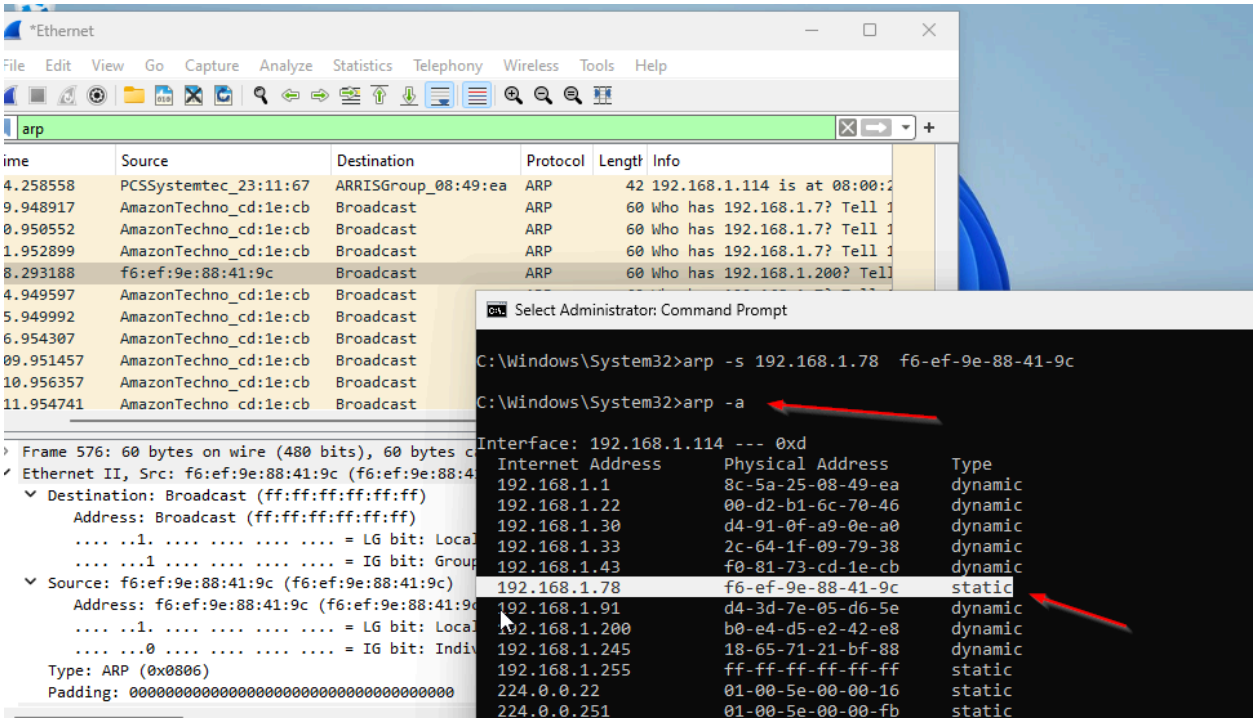
2. Prepare to Modify the ARP Entry:
    - Drag the Command Prompt window next to Wireshark (or have the MAC address written down) to easily read the MAC address you need to spoof.



3. Change the ARP Entry:
    - Use the ARP command to modify the ARP table. Type the following command:
      arp -s <IP address to spoof> <new MAC address>
    - Replace **`<IP address to spoof>`** with the new IP you want the original MAC to associate with (e.g., .78).
    - Replace **`<new MAC address>`** with the MAC address from the captured ARP packet, using dashes instead of colons between the hexadecimal numbers (e.g., 06-01-D4).



2. Verify the ARP Entry:
    - After entering the spoofing command, verify the new ARP entry by typing: arp -a
      This will display the current ARP table, and you should see the new entry with the IP address now associated with the spoofed MAC address.



Conclusion

This process demonstrates how ARP spoofing can be used to manipulate network traffic by altering the ARP table. This type of attack can redirect traffic to a malicious machine, posing significant security risks. This example serves to understand the mechanism and potential impact of ARP spoofing in network security testing or educational scenarios.