

Domain 02 Demo 03

Investigating DoS and MITM Attacks Using Wireshark

Objective: To investigate DoS and MITM attacks using Wireshark and filter and analyze traffic for anomalies like excessive packets, IP duplication, and irregular ARP entries

Tools required: Wireshark

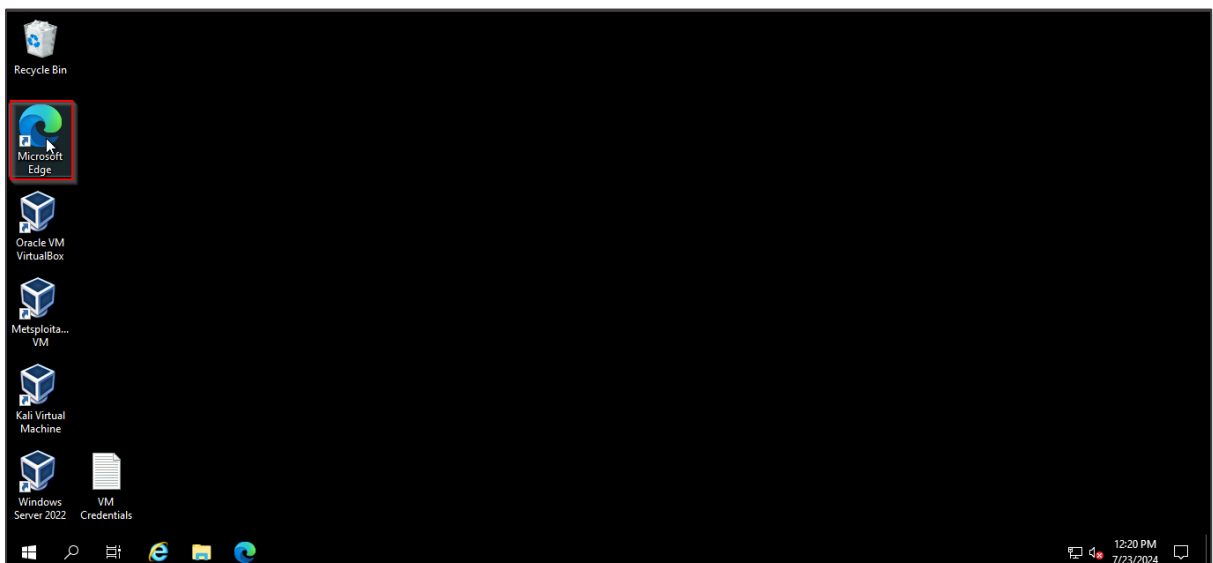
Prerequisites: None

Steps to be followed:

1. Analyze the **MITM.pcapng** file
2. Analyze the **NmapScanANDDoS.pcapng** file
3. Mitigate **MITM** and **DoS** attacks

Step 1: Analyze the MITM.pcapng file

1.1 Open the Microsoft Edge browser

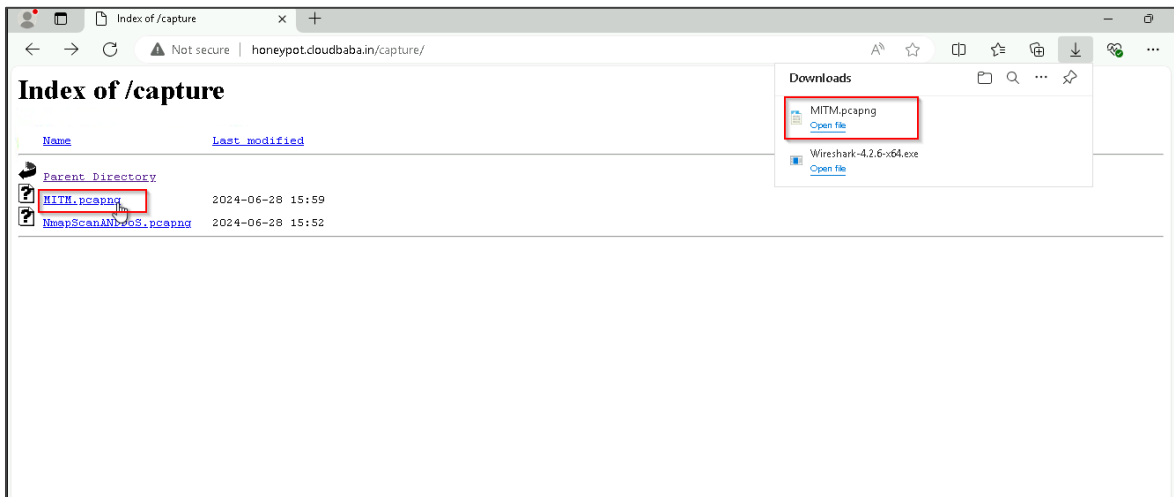


1.2 Browse to the following link:

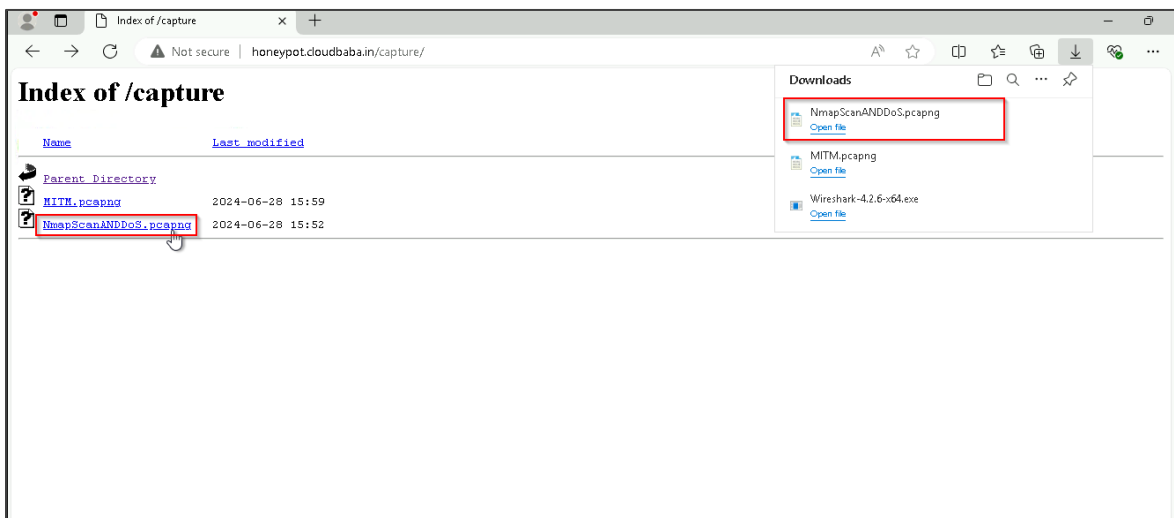
<http://honeypot.cloudbaba.in/capture>



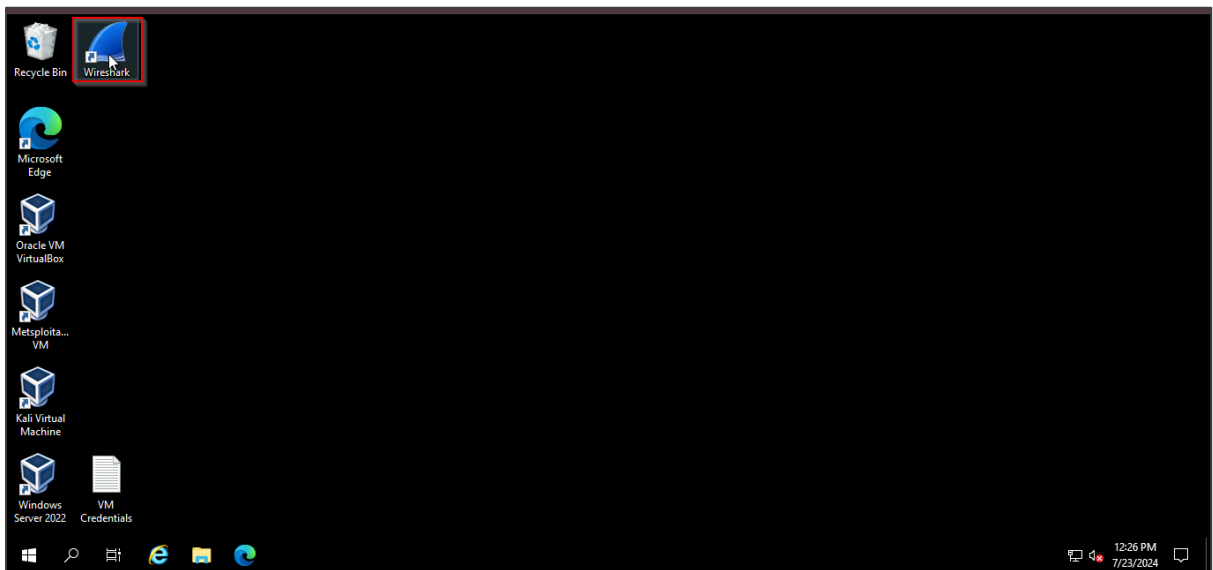
1.3 Click on the **MITM.pcapng** link to download the file



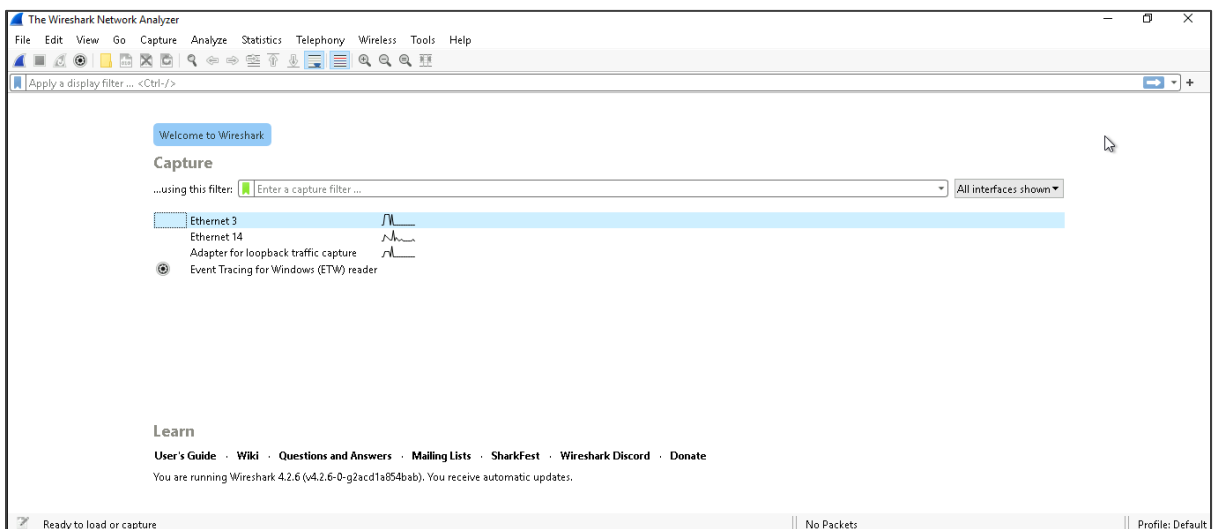
1.4 Further, click on the **NmapScanANDDoS.pcapng** link to download the file



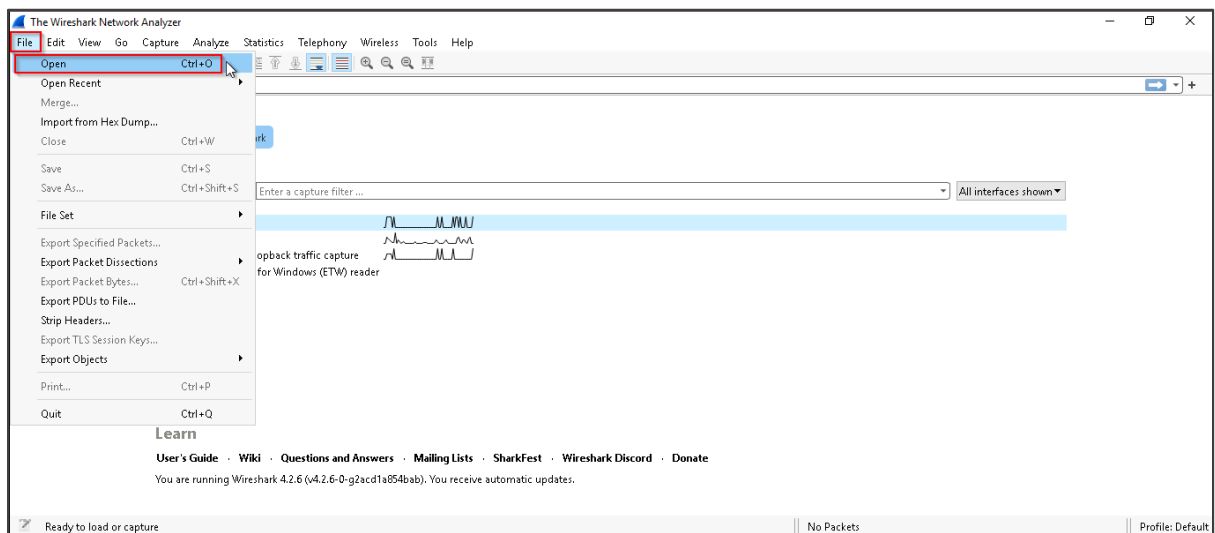
1.5 Navigate to the desktop and open the **Wireshark** application



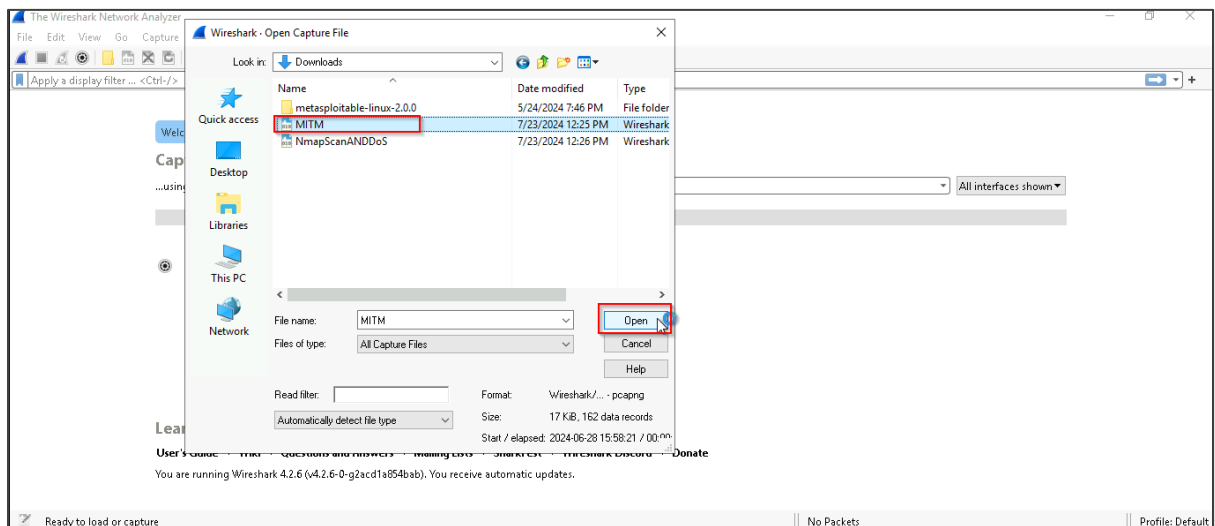
The **Wireshark Network Analyzer** interface opens as shown below:



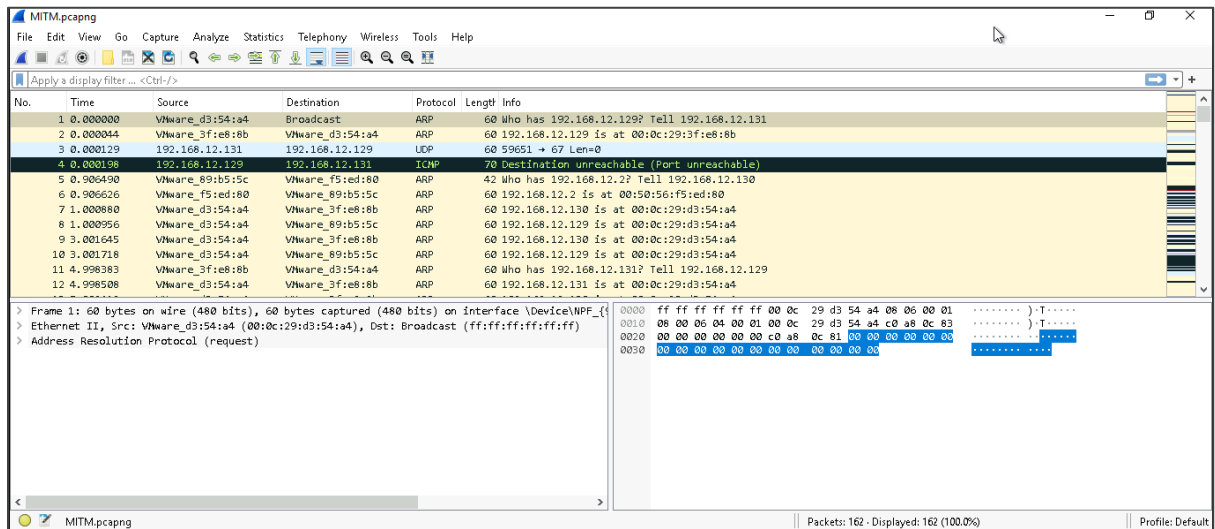
1.6 Click on the **File** option and select **Open**



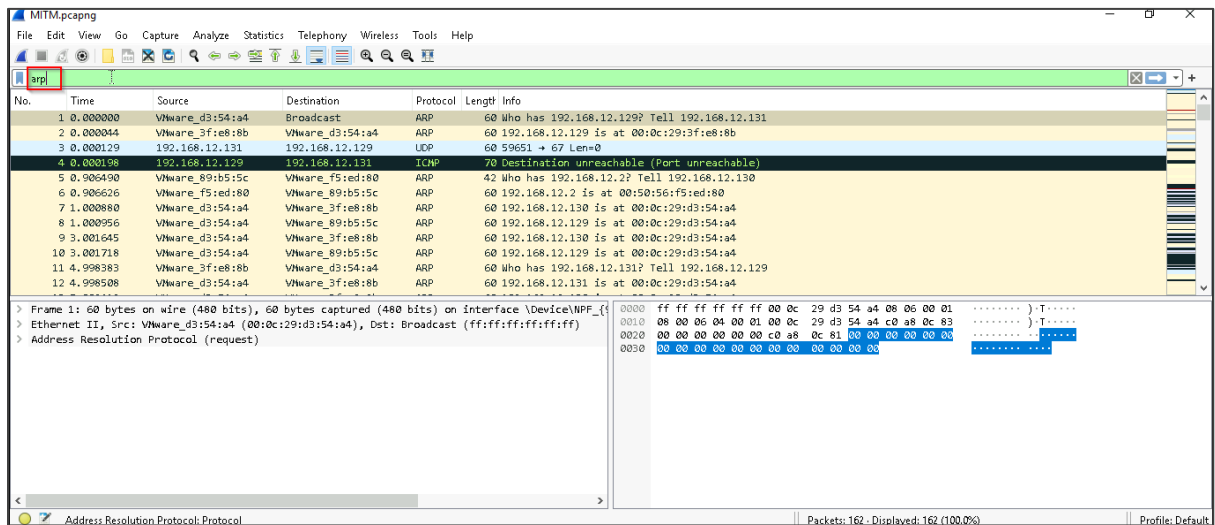
1.7 Select the **MITM** file and click on **Open**



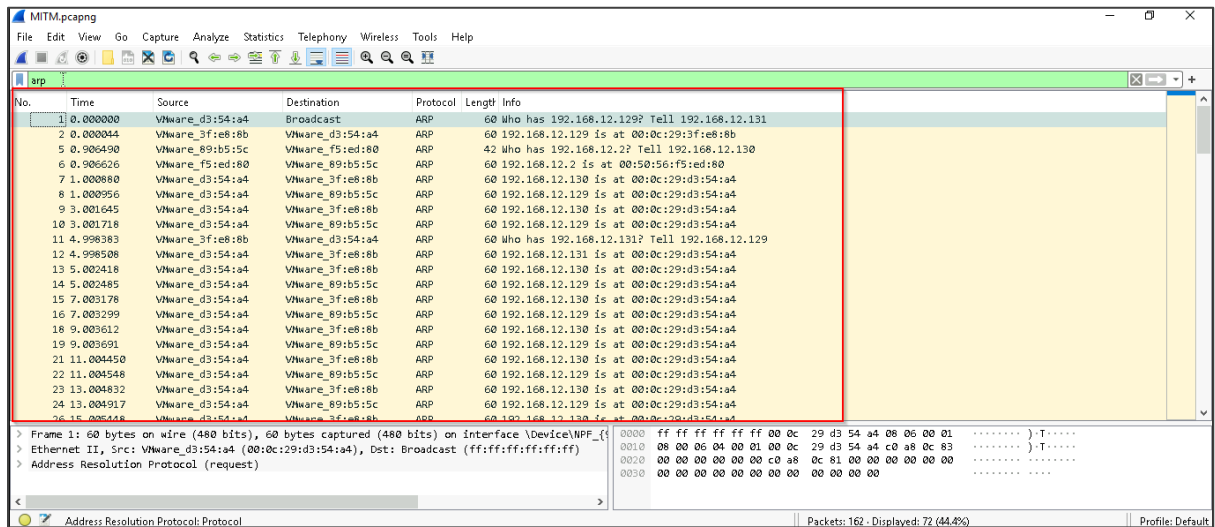
The MITM file opens in the Wireshark.



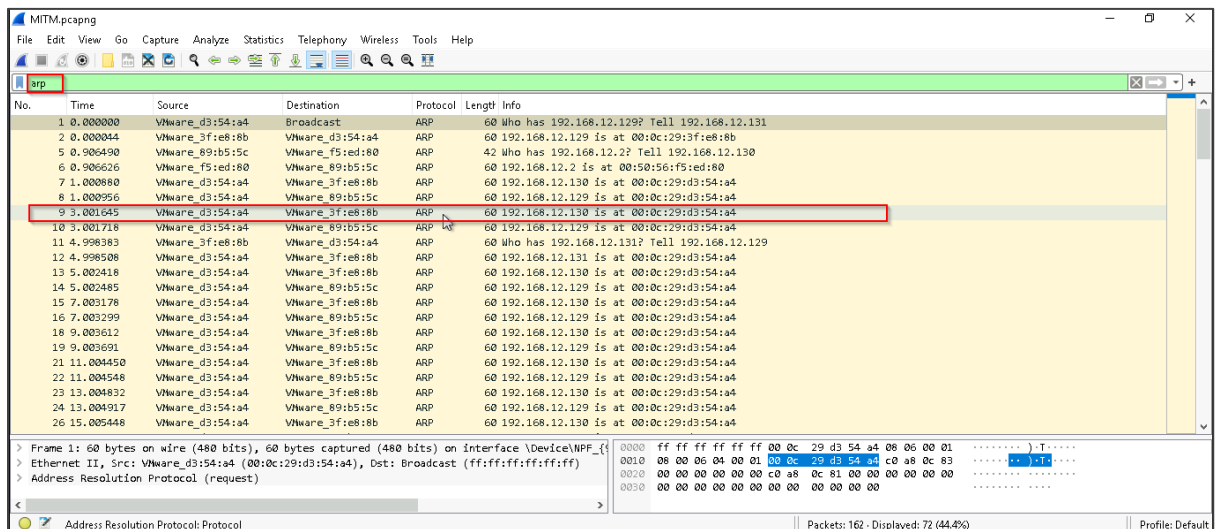
1.8 In the filter section, type **arp** and click **enter** to filter the unexpected ARP traffic



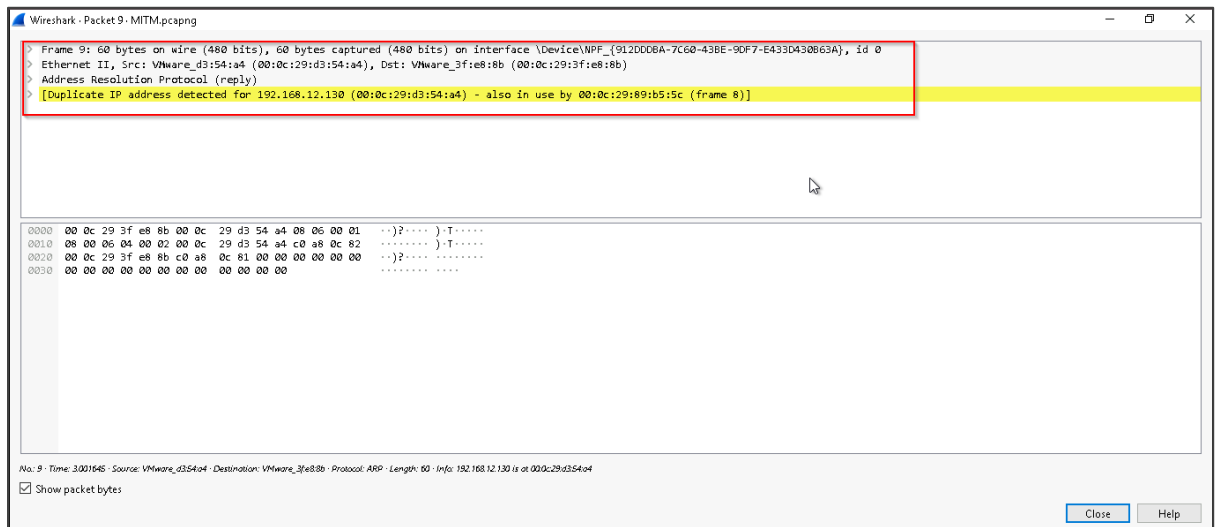
All the **ARP** traffic is filtered out as shown below:



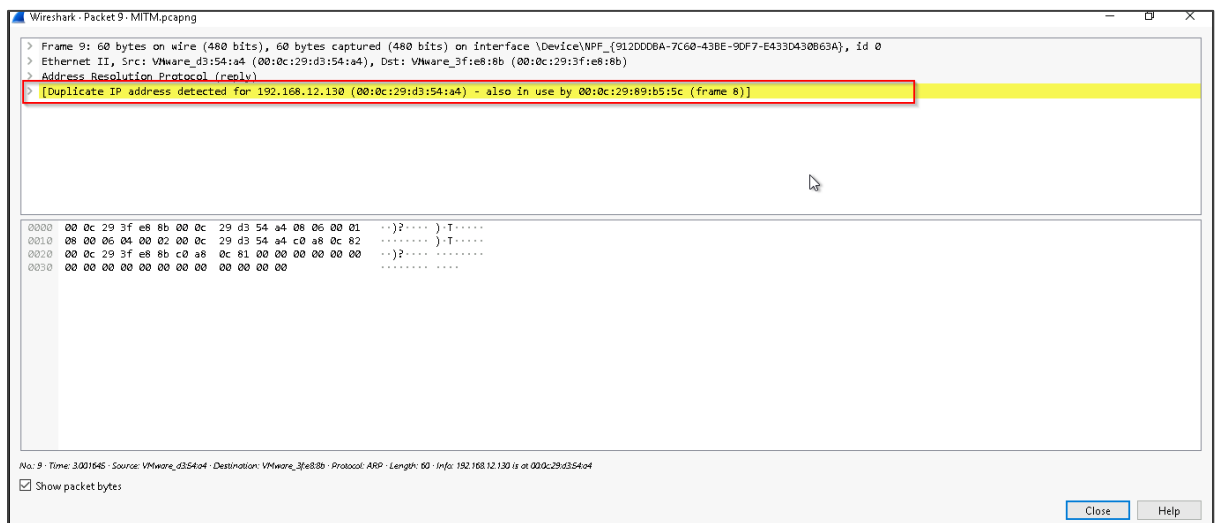
1.9 Double-click on any one **ARP** packet to see the details



The details of the selected ARP packet are available as shown below:



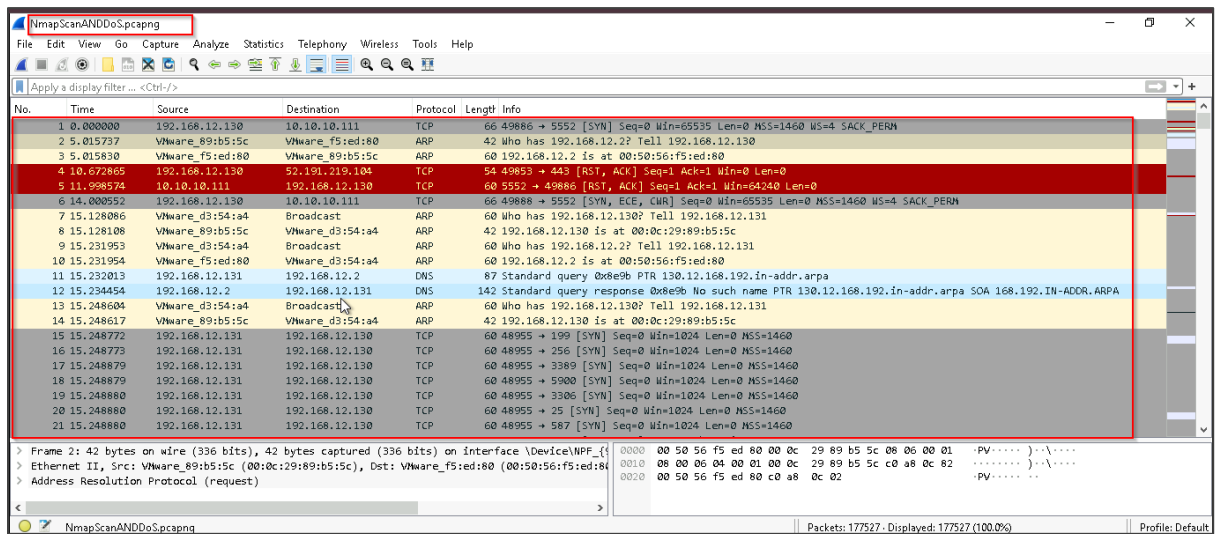
The warning for duplicate IP addresses is also shown below:



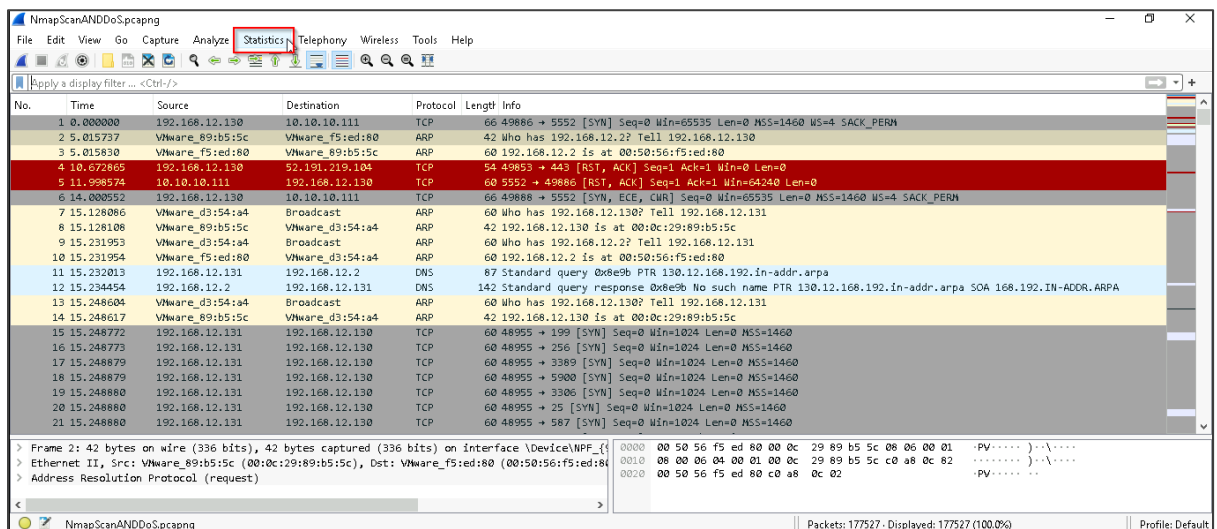
Note: Repeated IP addresses during an MITM attack are often caused by ARP spoofing. This indicates that network devices are receiving conflicting ARP responses, which leads to traffic being redirected to the attacker's MAC address, causing potential data interception and network disruptions.

Step 2: Analyze the NmapScanANDDoS.pcapng file

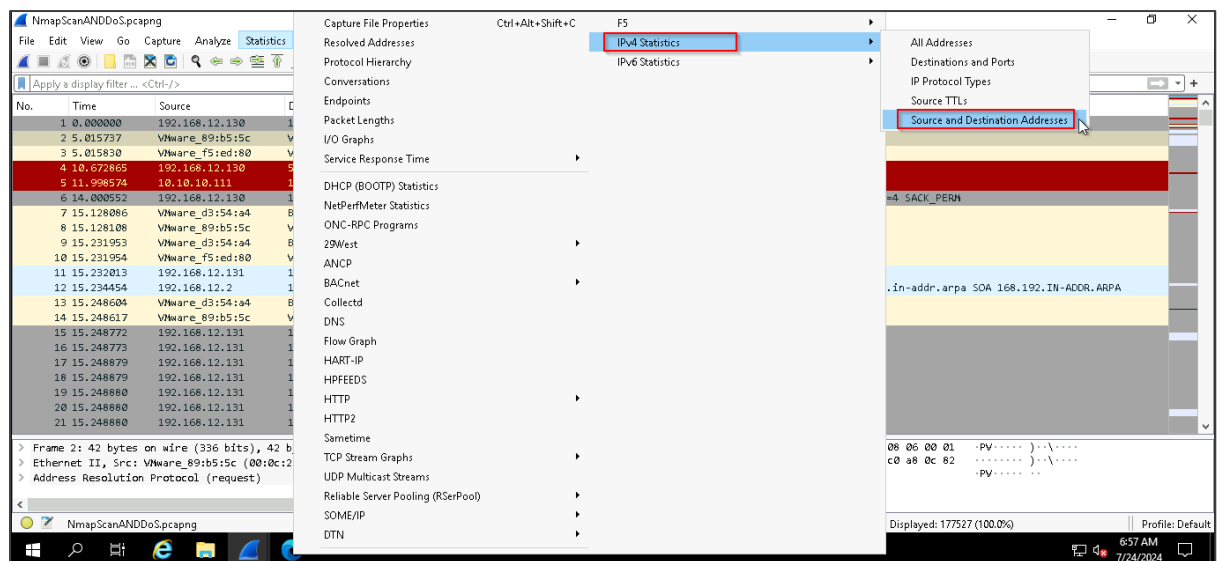
2.1 Open the NmapScanANDDoS.pcapng file in Wireshark



2.2 Click on the Statistics option in the menu bar



2.3 Further, click on **IPv4 Statistics** and select the **Source and Destination Addresses** option



The source IP, along with the packet transmission, is visible.

The screenshot shows the 'Source and Destination Addresses' statistics window in Wireshark. The window displays a table of IP addresses and their associated statistics, including count, average, min/max values, rate, percent, burst rate, and burst start.

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Source IPv4 Addresses	177478				2.1451	100%	46.7800	76.270
40.81.94.65	1				0.0000	0.00%	0.0100	20.164
20.118.138.130	26				0.0003	0.01%	0.0600	16.335
192.168.12.2	5				0.0001	0.00%	0.0200	15.821
192.168.12.131	99487				1.2025	56.08%	39.9600	76.201
192.168.12.130	77939				0.9420	43.91%	21.8700	71.995
192.168.12.1	16				0.0002	0.01%	0.0500	56.730
10.10.10.111	4				0.0000	0.00%	0.0100	11.999
Destination IPv4 Addresses	177478				2.1451	100%	46.7800	76.270
52.191.219.104	1				0.0000	0.00%	0.0100	10.673
40.81.94.65	1				0.0000	0.00%	0.0100	20.094
224.0.0.252	4				0.0000	0.00%	0.0100	55.729
224.0.0.251	12				0.0001	0.01%	0.0400	56.730
20.118.138.130	19				0.0002	0.01%	0.0300	16.335
192.168.12.2	5				0.0001	0.00%	0.0200	15.743
192.168.12.131	77905				0.9416	43.90%	21.8700	71.995
192.168.12.130	99521				1.2029	56.08%	39.9600	76.201
10.10.10.111	10				0.0001	0.01%	0.0100	0.000

2.4 In the Display filter field, enter the following filter and press **enter**:
tcp.flags.syn==1 and tcp.flags.ack==0

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Source IPv4 Addresses	177478				2.1451	100%	46.7800	76.270
40.81.94.65	1	0.0000			0.0000	0.00%	0.0100	20.164
20.118.138.130	26	0.0003			0.0003	0.01%	0.0600	16.335
192.168.12.2	5	0.0001			0.0001	0.00%	0.0200	15.821
192.168.12.131	99487	1.2025			56.06%	39.9600	76.201	
192.168.12.130	77939	0.9420			43.91%	21.8700	71.935	
192.168.12.1	16	0.0002			0.0002	0.01%	0.0500	56.730
10.10.10.111	4	0.0000			0.0000	0.00%	0.0100	11.999
Destination IPv4 Addresses	177478				2.1451	100%	46.7800	76.270
52.191.219.104	1	0.0000			0.0000	0.00%	0.0100	10.673
40.81.94.65	1	0.0000			0.0000	0.00%	0.0100	20.094
224.0.0.252	4	0.0000			0.0000	0.00%	0.0100	55.729
224.0.0.251	12	0.0001			0.0001	0.01%	0.0400	56.730
20.118.138.130	19	0.0002			0.0002	0.01%	0.0300	16.335
192.168.12.2	5	0.0001			0.0001	0.00%	0.0200	15.743
192.168.12.131	77905	0.9416			43.90%	21.8700	71.935	
192.168.12.130	99521	1.2029			56.08%	39.9600	76.201	
10.10.10.111	10	0.0001			0.0001	0.01%	0.0100	0.000

Display filter: **tcp.flags.syn==1 and tcp.flags.ack==0**

2.5 Copy the **source IP** that has the highest amount of packet transmission as shown below:

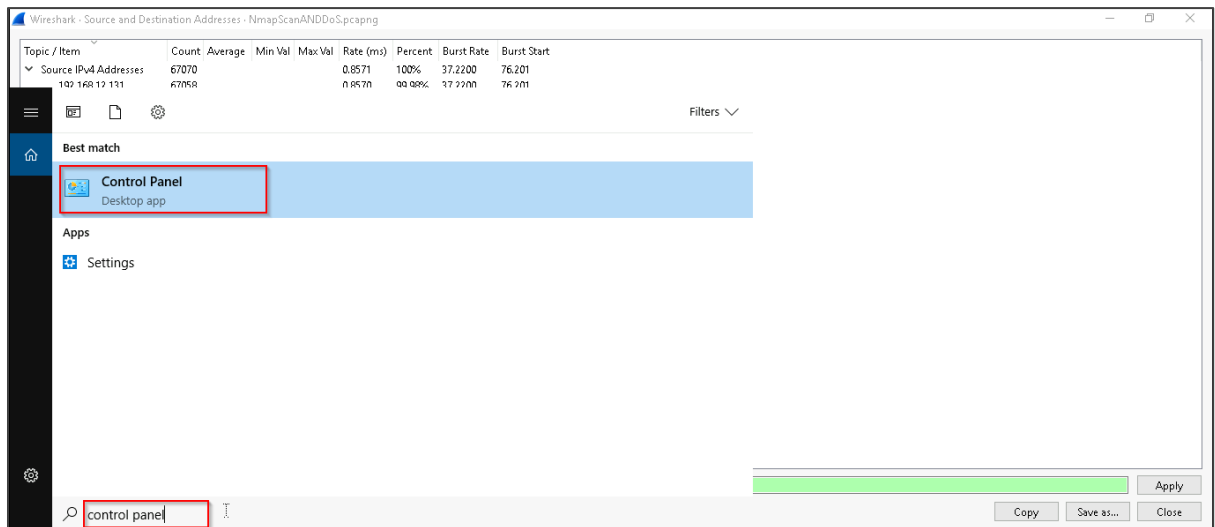
Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Source IPv4 Addresses	67070				0.8571	100%	37.2200	76.201
192.168.12.131	67058	0.8570			99.98%	37.2200	76.201	
192.168.12.130	12	0.0002			0.0002	0.02%	0.0100	0.000
Destination IPv4 Addresses	67070				0.8571	100%	37.2200	76.201
20.118.138.130	2	0.0000			0.0000	0.00%	0.0100	15.824
192.168.12.130	67058	0.8570			99.98%	37.2200	76.201	
10.10.10.111	10	0.0001			0.0001	0.01%	0.0100	0.000

Display filter: **tcp.flags.syn==1 and tcp.flags.ack==0**

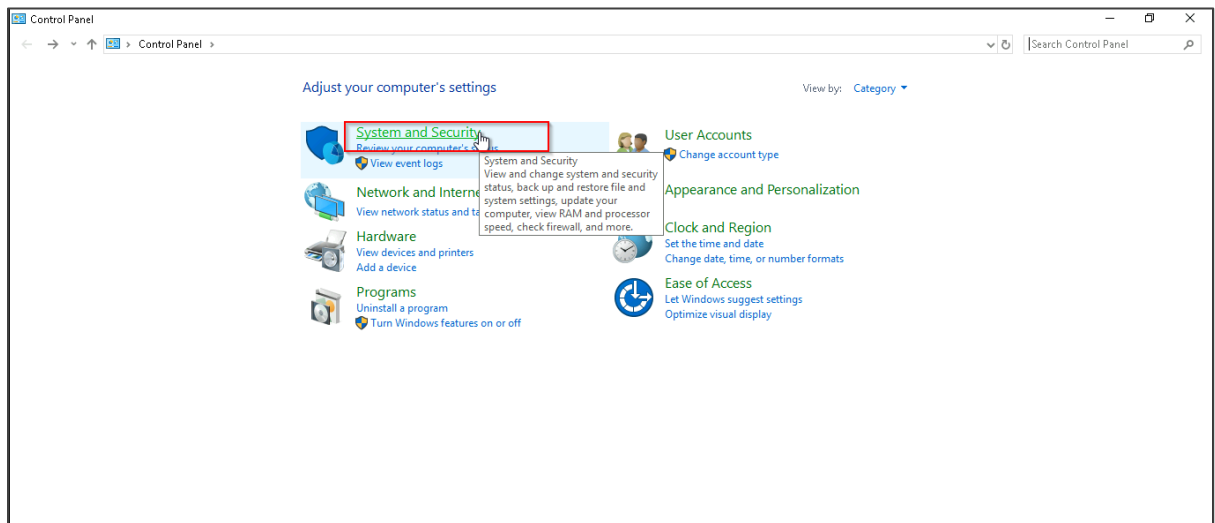
In this case, the **source IP** that has the highest amount of packet transmission is
192.168.12.131

Step 3: Mitigate MITM and DoS attacks

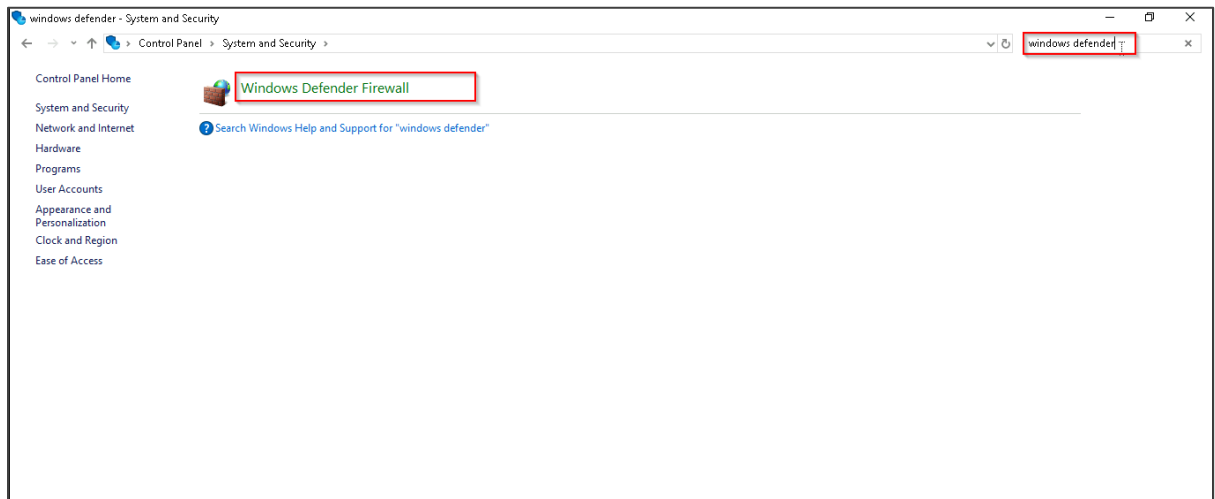
3.1 Open the **Control Panel** from the Windows search button



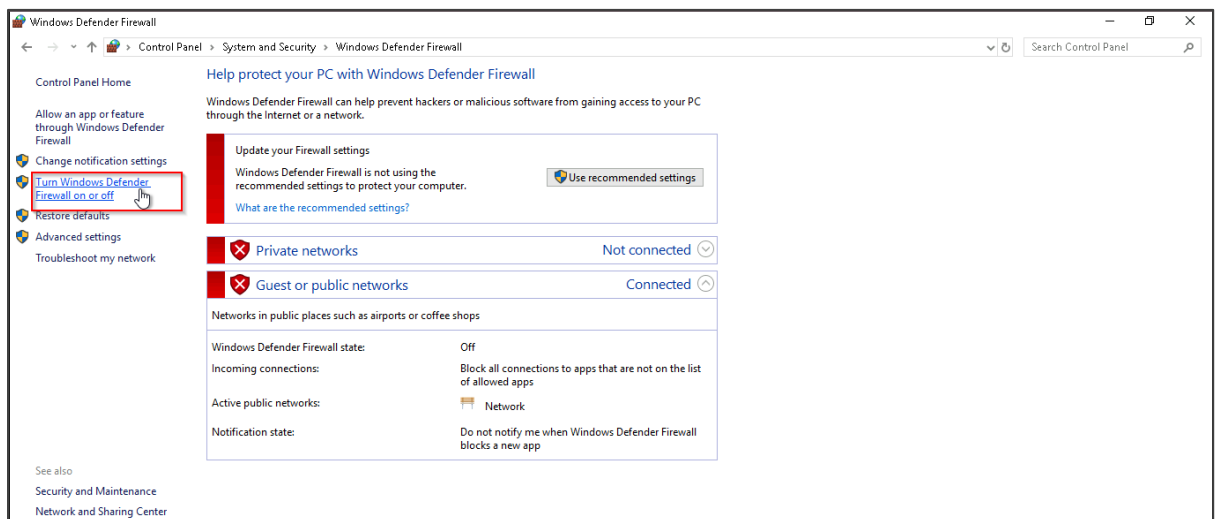
3.2 Select **System and Security**



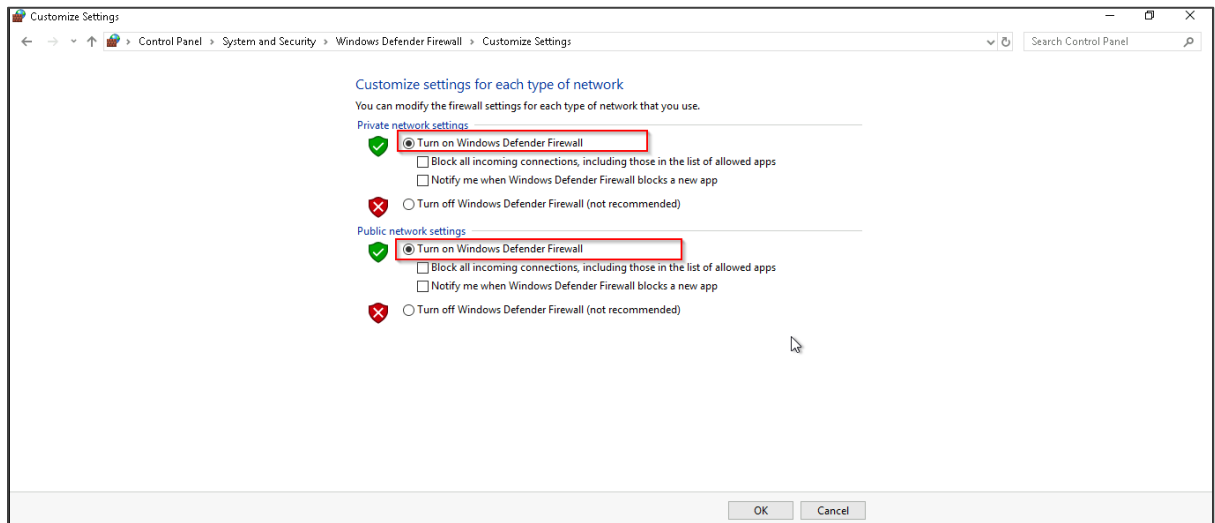
3.3 Search for windows defender and click on the Windows Defender Firewall option



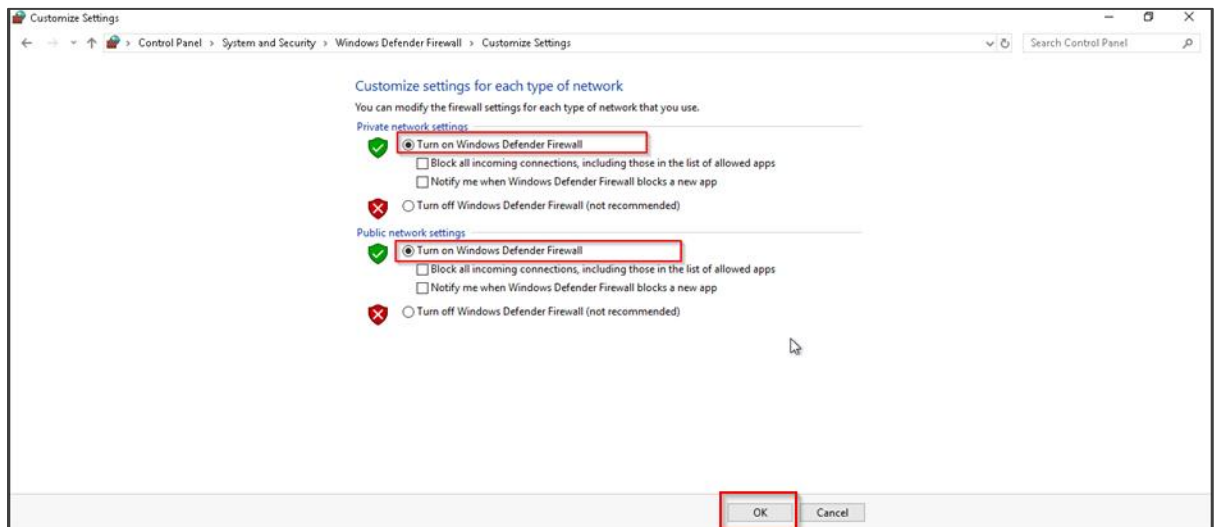
3.4 Click on Turn Windows Defender Firewall on or off



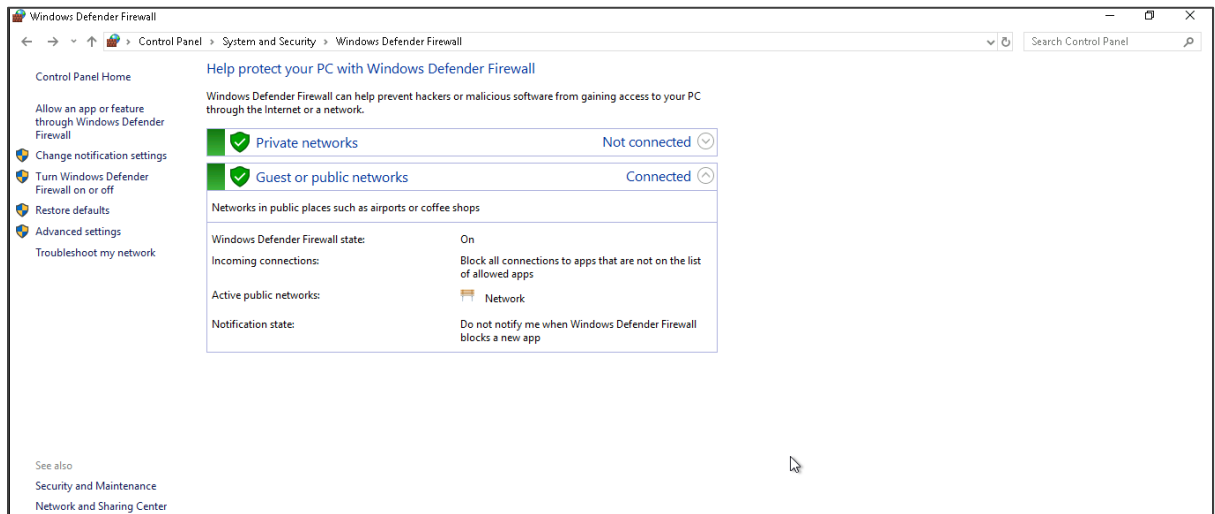
3.5 Select Turn on Windows Defender Firewall



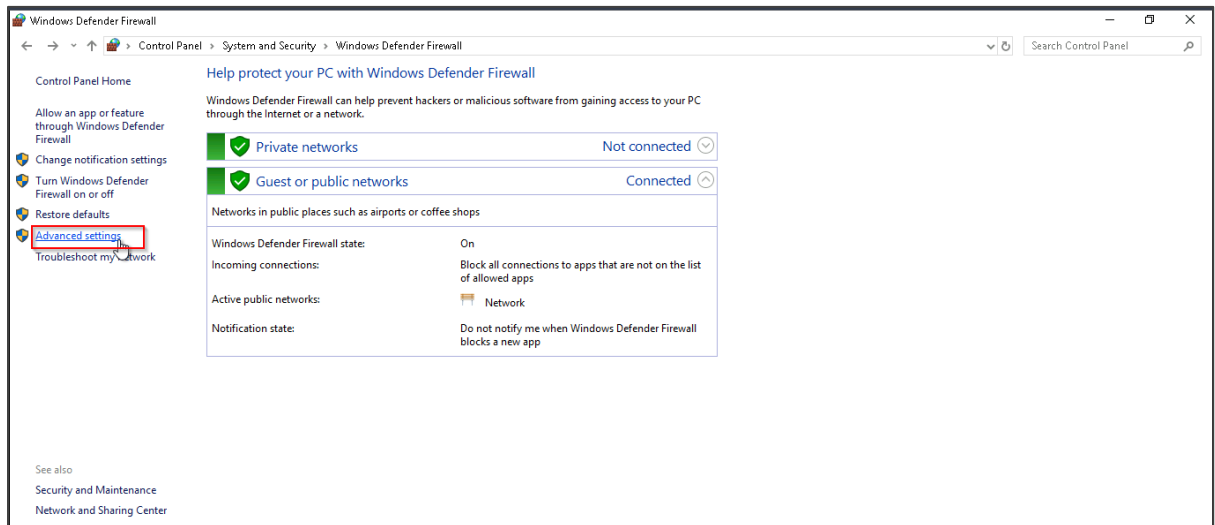
3.6 Click on OK



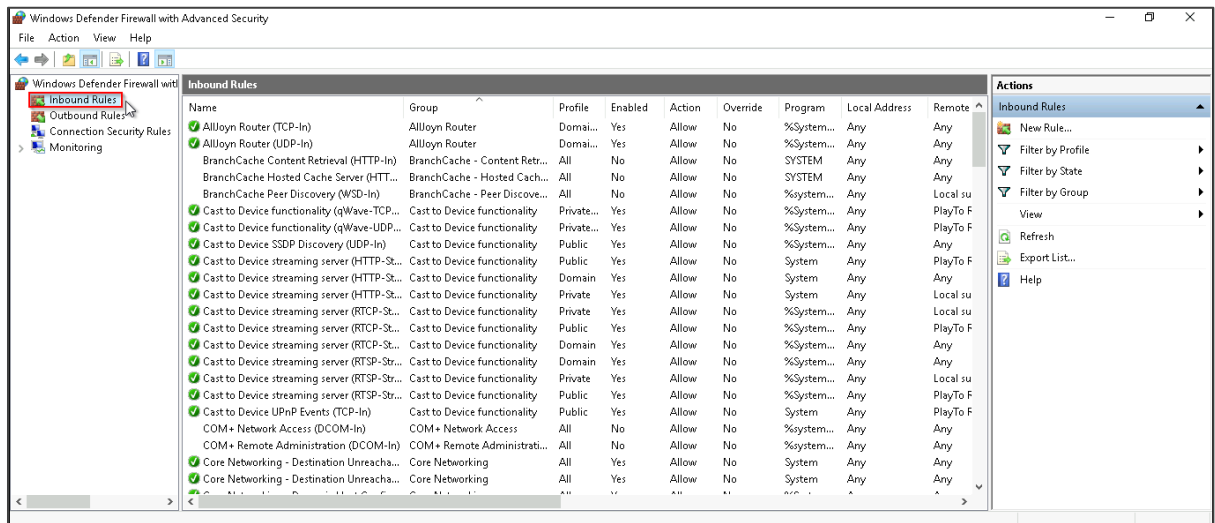
The changes are applied as shown below.



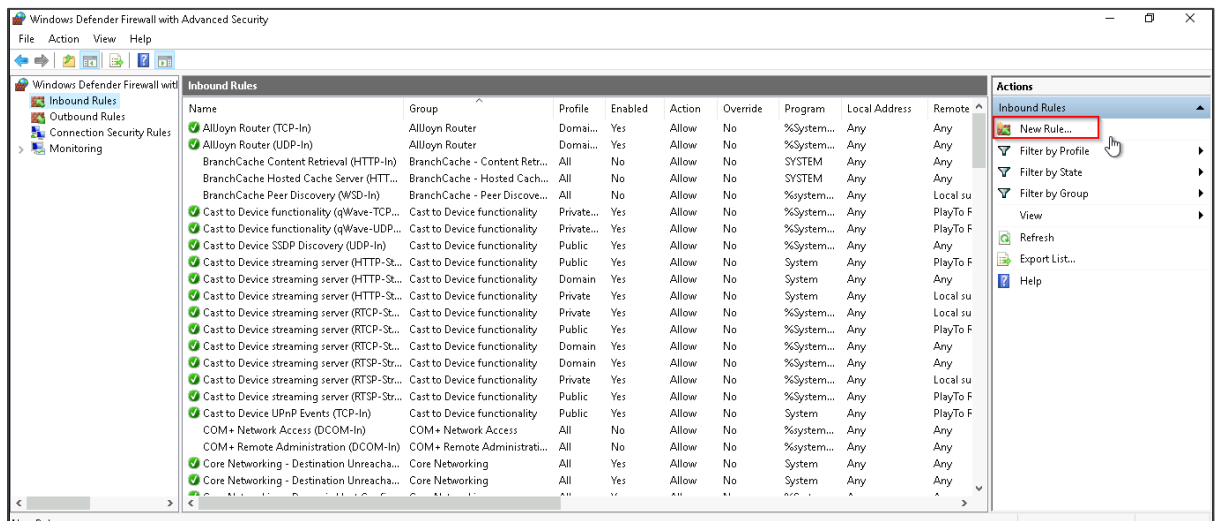
3.7 Click on **Advanced settings**



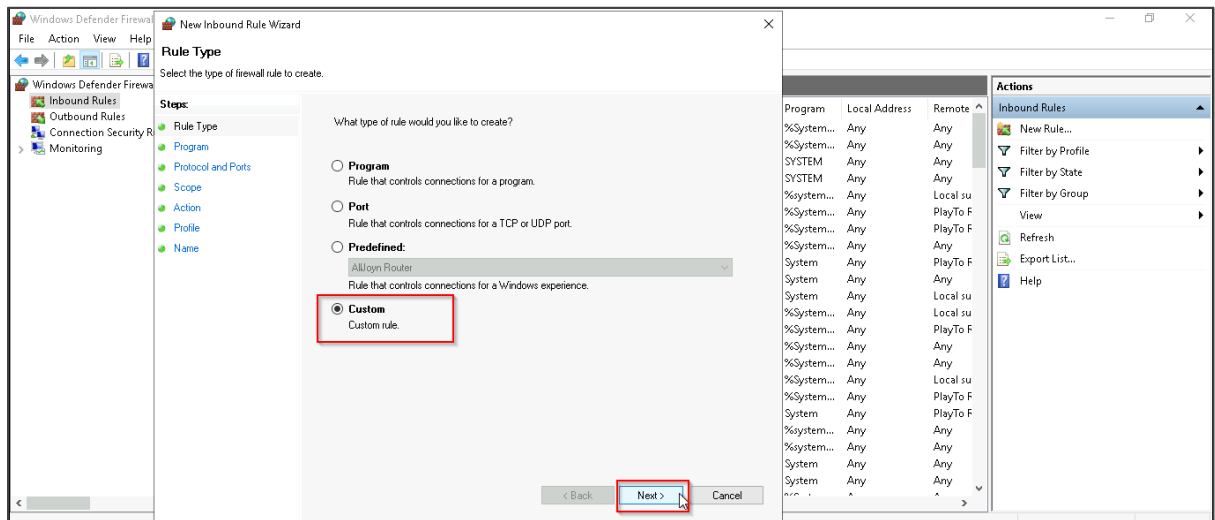
3.8 Click on Inbound Rules



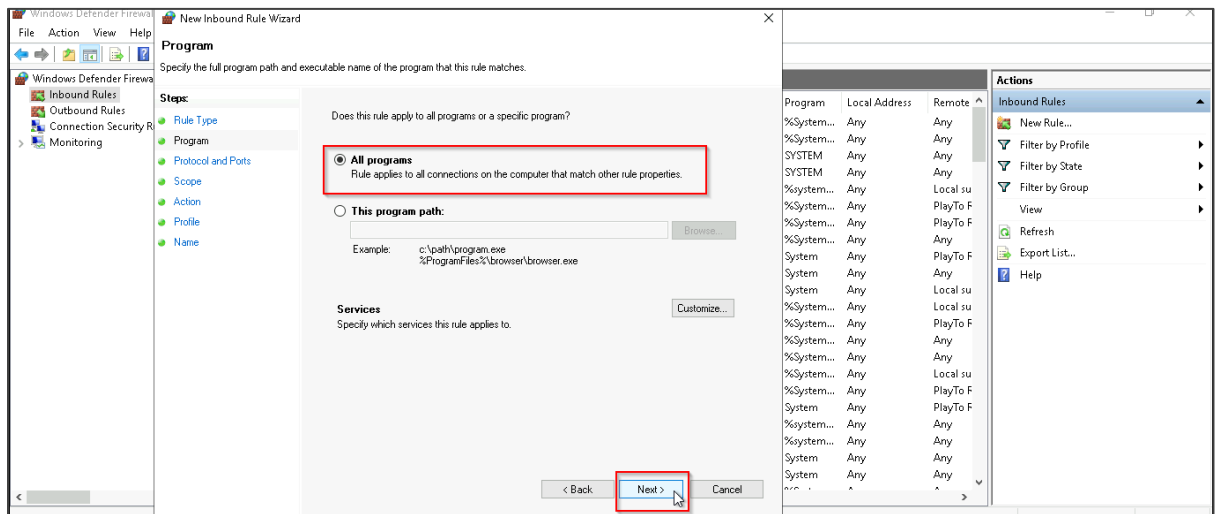
3.9 Further, click on New Rule



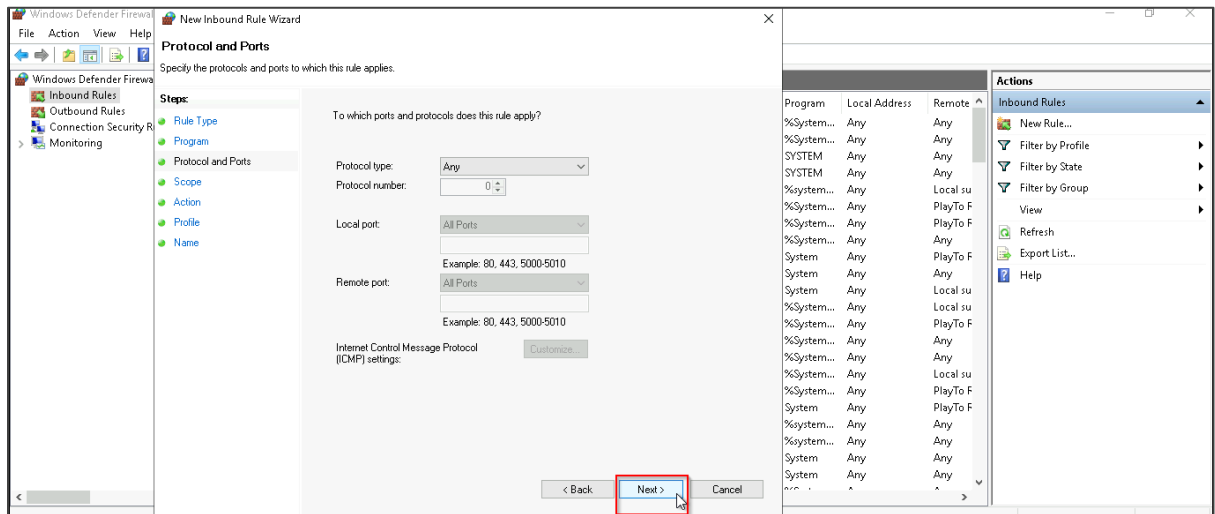
3.10 Select the **Custom** rule and click on **Next**



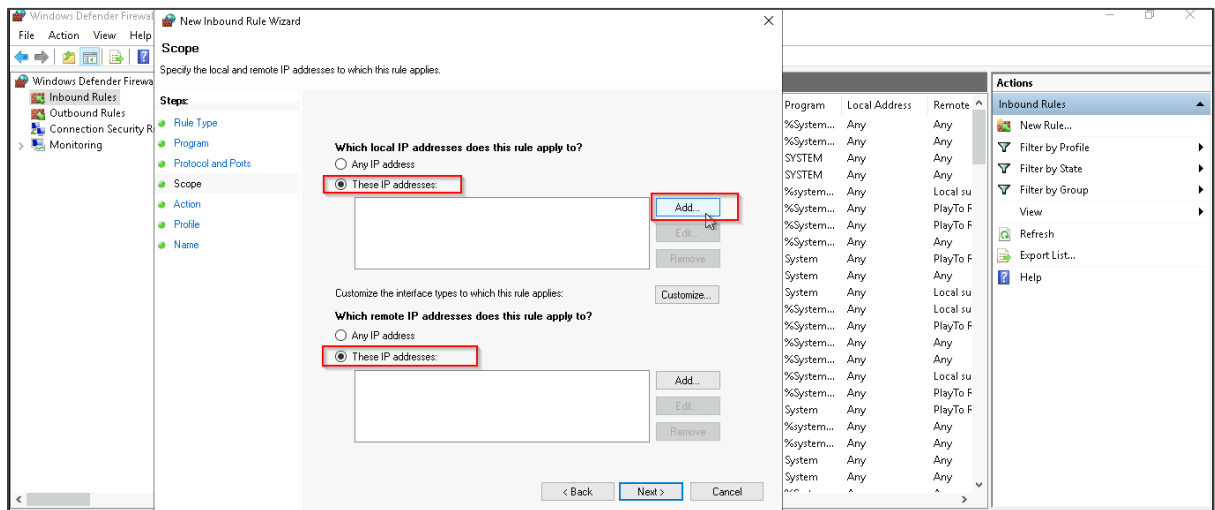
3.11 Select **All programs** and click on **Next**



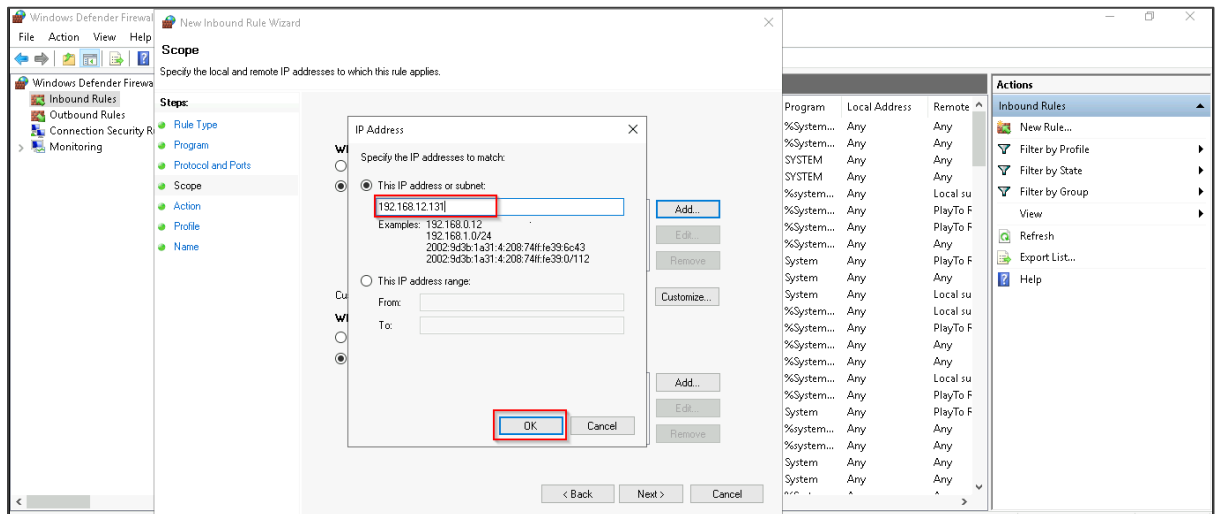
3.12 Further, click on **Next**



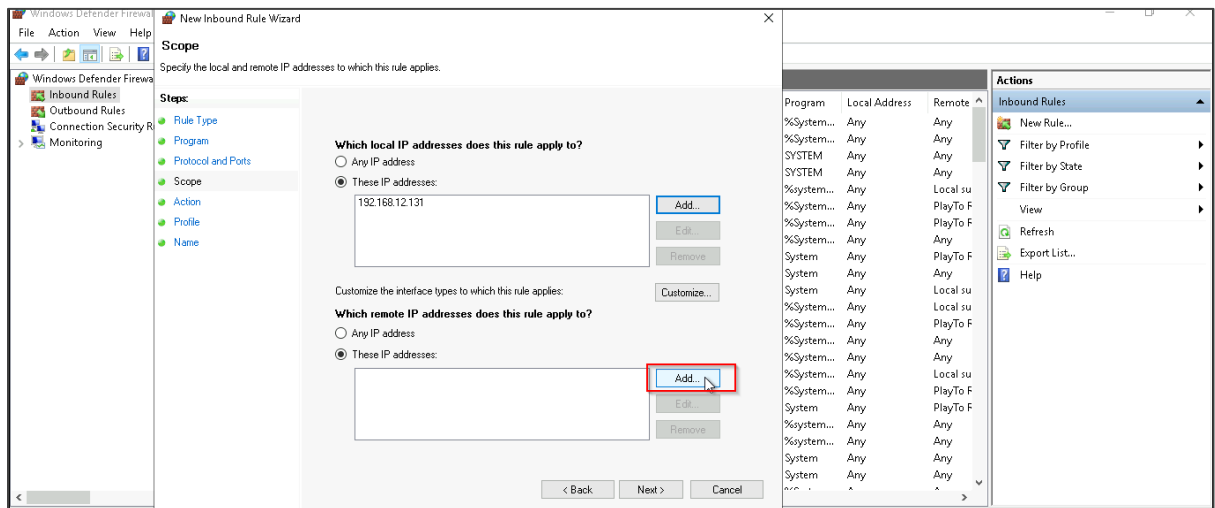
3.13 Click on the **Add** button to add the IP addresses



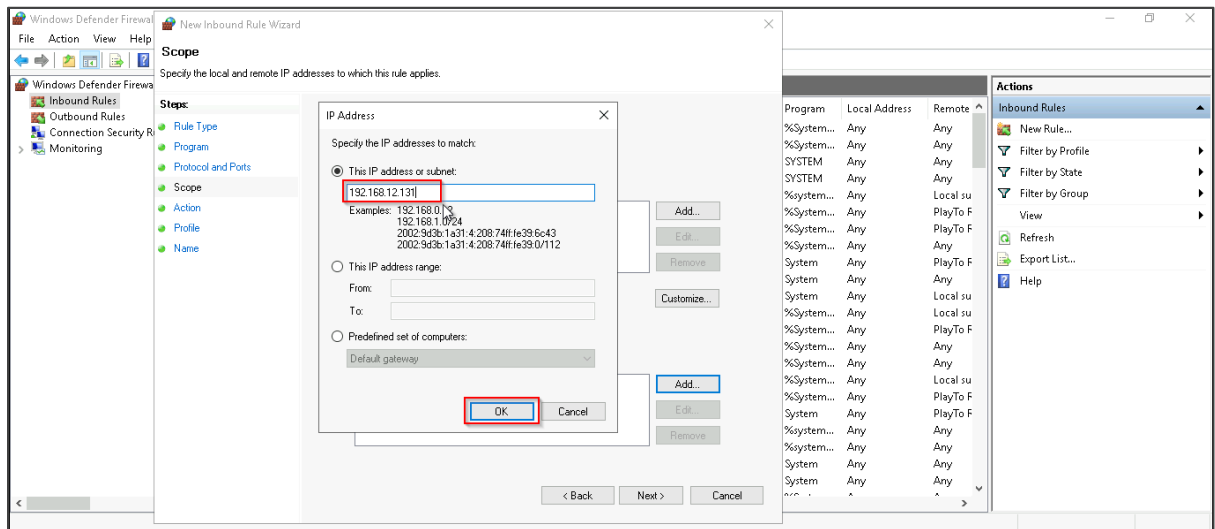
3.14 Add the IP address as **192.168.12.131** and click on **OK**



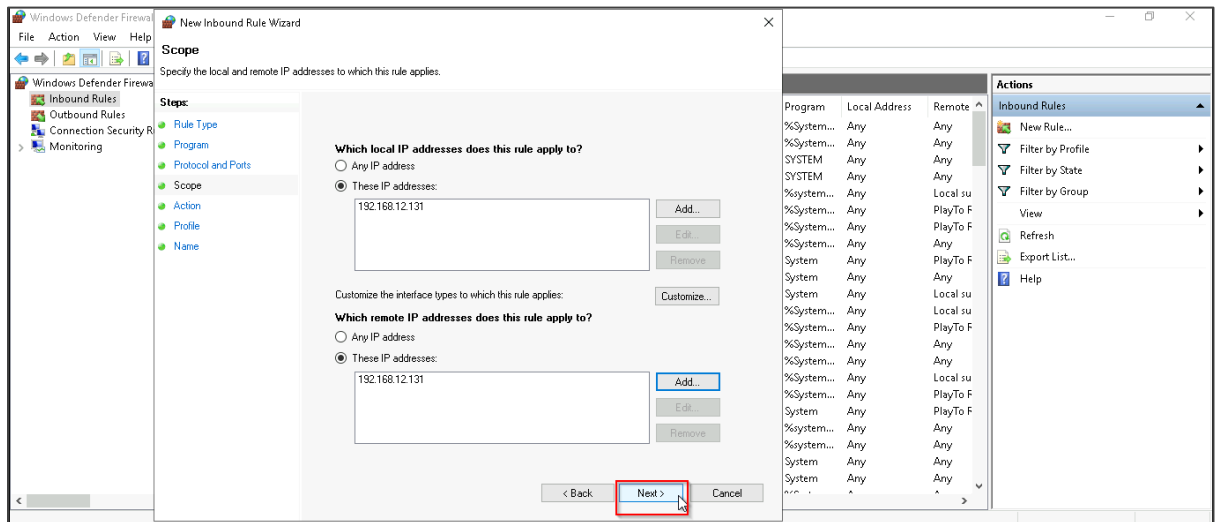
3.15 Further, click on the second **Add** button



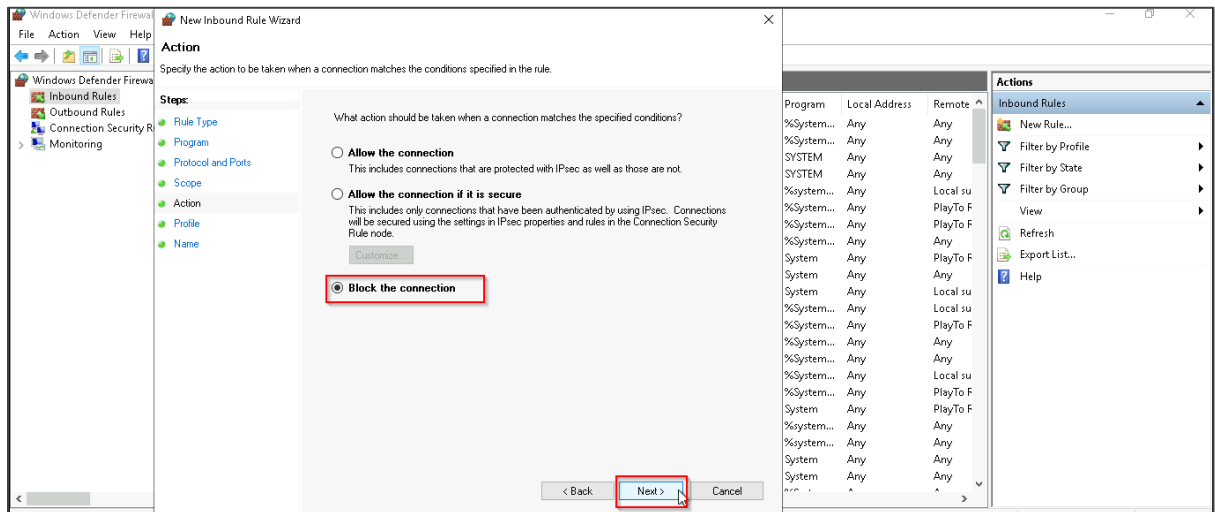
3.16 Add the IP address as **192.168.12.131** and click on **OK**



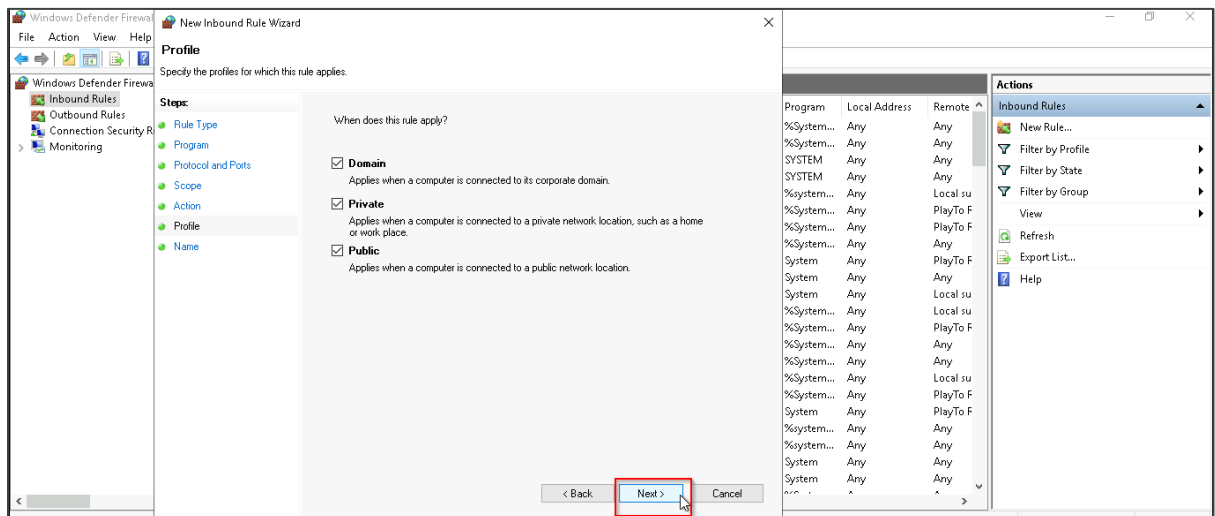
3.17 Click on **Next**



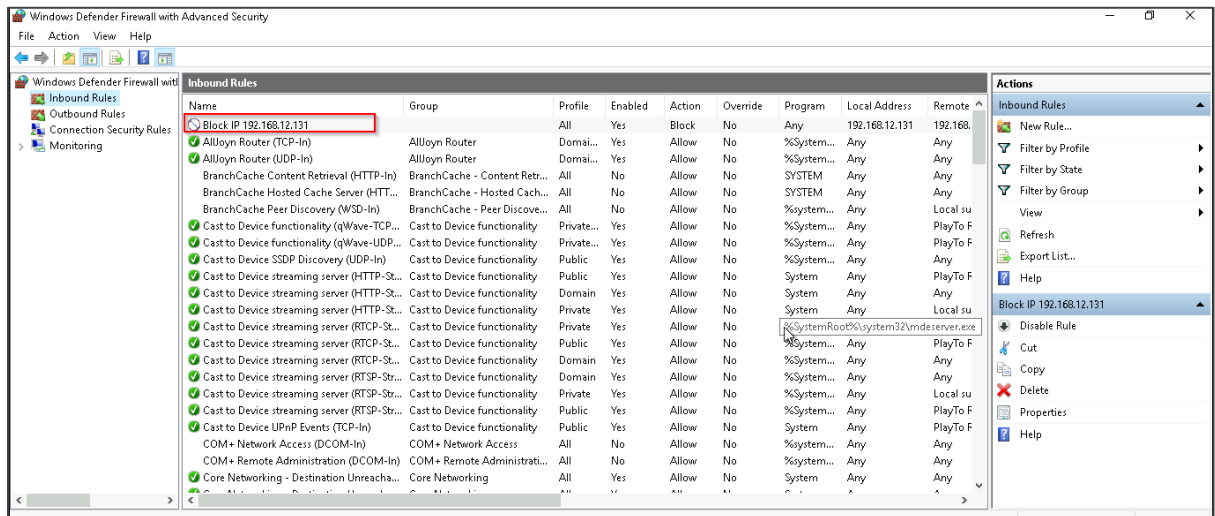
3.18 Select **Block the connection** and click on **Next**



3.19 Keep all default selections and click on **Next**



The rule with the blocked IP address **192.168.12.131** appears in the **Inbound Rules**.



Following the above steps, you have successfully investigated DoS and MITM attacks using a Wireshark capture file. You have filtered and analyzed traffic for signs of anomalies, such as excessive packets or IP duplication, which may indicate potential DoS and irregular ARP entries pointing to possible MITM activities.