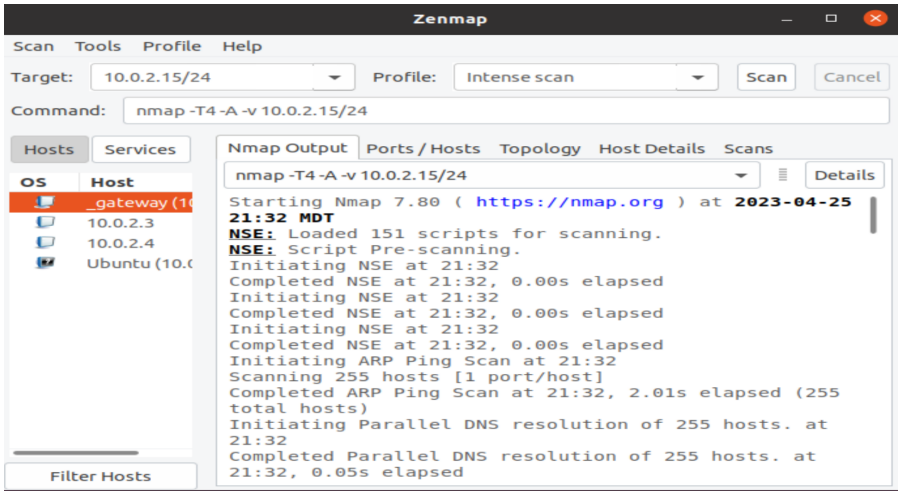
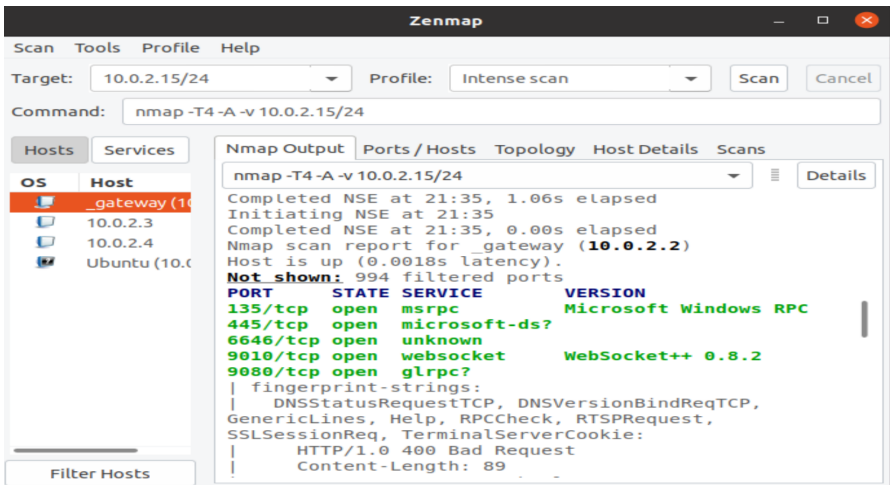
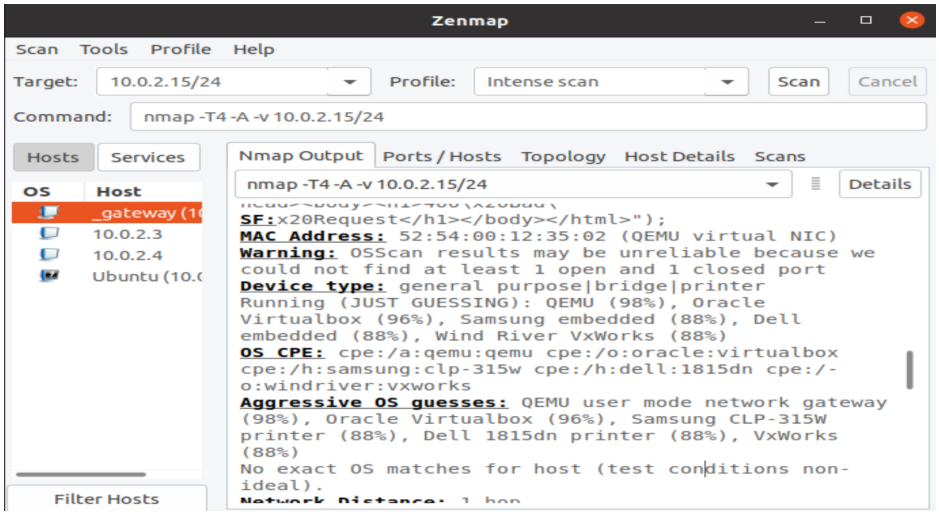
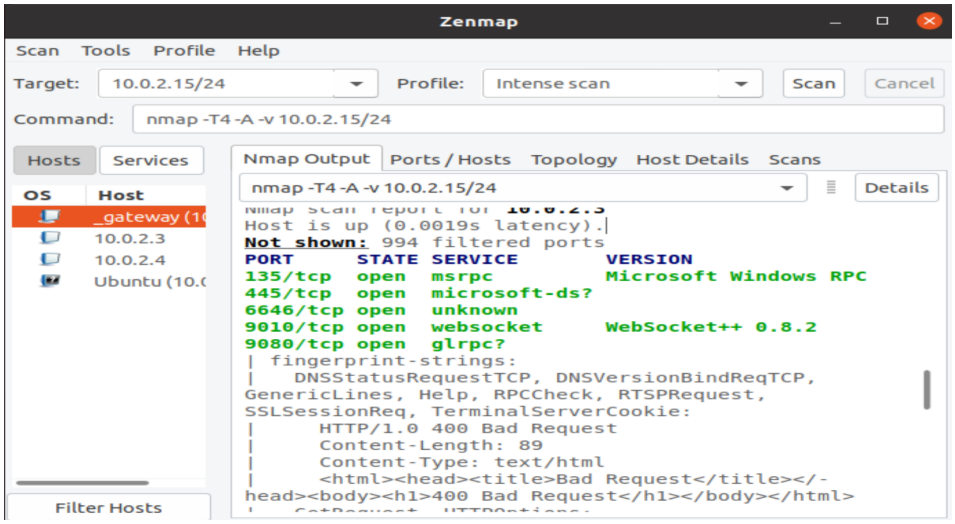
Part 1: Port Scanning to Map a Network

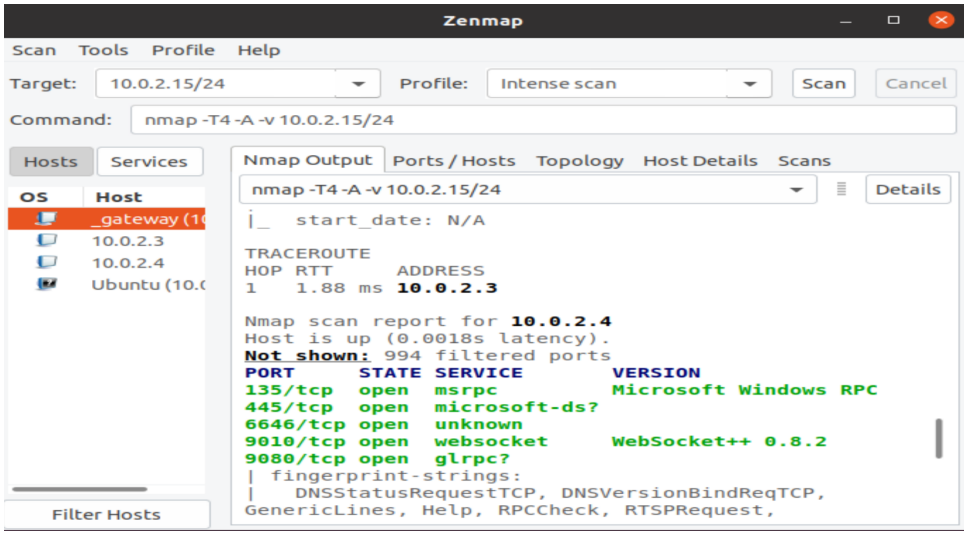
Sample Screenshots of Zenmap and Nmap:





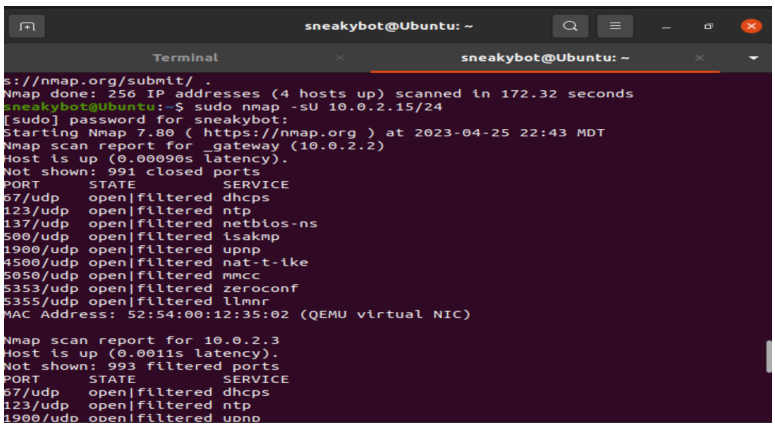



Zenmap
Scan Tools Profile Help
Target: 10.0.2.15/24
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 10.0.2.15/24
Hosts
Services
OS
Host
_gateway (1
10.0.2.3
10.0.2.4
Ubuntu (10.
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v 10.0.2.15/24
Details
Host is up (0.0019s latency).
Not shown: 994 filtered ports
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
445/tcp open microsoft-ds?
6646/tcp open unknown
9010/tcp open websocket WebSocket++ 0.8.2
9080/tcp open glrpc?
| fingerprint-strings:
| DNSStatusRequestTCP, DNSVersionBindReqTCP,
GenericLines, Help, RPCCheck, RTSPRequest,
SSLSessionReq, TerminalServerCookie:
| HTTP/1.0 400 Bad Request
| Content-Length: 89
| Content-Type: text/html
| <html><head><title>Bad Request</title></-
head><body><h1>400 Bad Request</h1></body></html>


Zenmap
Scan Tools Profile Help
Target: 10.0.2.15/24
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 10.0.2.15/24
Hosts
Services
OS
Host
_gateway (1
10.0.2.3
10.0.2.4
Ubuntu (10.
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v 10.0.2.15/24
Details
| start_date: N/A
TRACEROUTE
HOP RTT ADDRESS
1 1.88 ms 10.0.2.3
Nmap scan report for 10.0.2.4
Host is up (0.0018s latency).
Not shown: 994 filtered ports
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
445/tcp open microsoft-ds?
6646/tcp open unknown
9010/tcp open websocket WebSocket++ 0.8.2
9080/tcp open glrpc?
| fingerprint-strings:
| DNSStatusRequestTCP, DNSVersionBindReqTCP,
GenericLines, Help, RPCCheck, RTSPRequest,

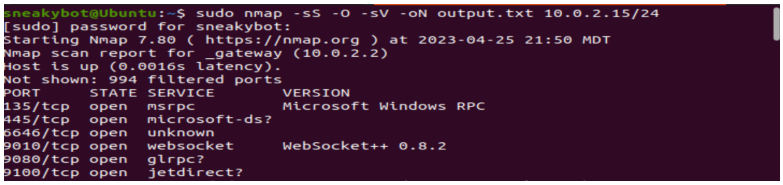
Utilized Several Nmap Scans:

- **Sudo nmap -sU <target IP address>**



- sU performs a UDP scan

- **sudo nmap -sS -O -sV -oN output.txt <target IP address or range>**



-sS: performs a SYN scan, which sends SYN packets to target ports to determine which are open.
-O: attempts to identify the OS on the target machine
-sV: performs version detection, finds the version of services running on open ports
-oN output.txt: saves the output of the scan in a file named "output.txt" in the current working directory.

- **List of all IP addresses of all machines in the network:**

Nmap scanned the IP address 10.0.2.2, 10.0.2.3, and 10.0.2.4 which had a latency of 0.0016 seconds.

- **OS and Version**

The host is likely running QEMU, Oracle Virtualbox, or Samsung embedded software.

- **Open Ports and services running on ports and versions**

PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
445/tcp open microsoft-ds?
6646/tcp open unknown
9010/tcp open websocket WebSocket++ 0.8.2
9080/tcp open glrpc?
9100/tcp open jetdirect?

- **List of all IP addresses of all machines in the network:**

Nmap also scanned Ubuntu (10.0.2.15) which had a 0.000059s latency

- **OS and Version**

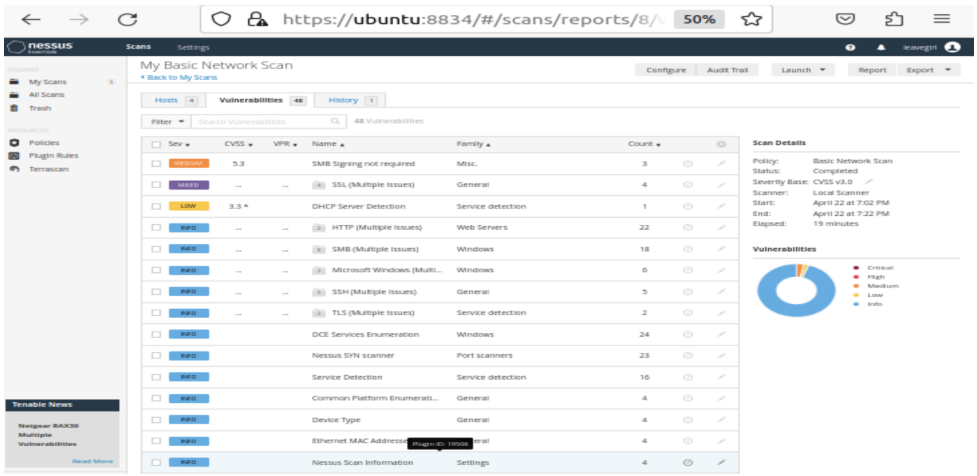
The host has too many matching fingerprints, which makes it impossible to provide specific details about its operating system.

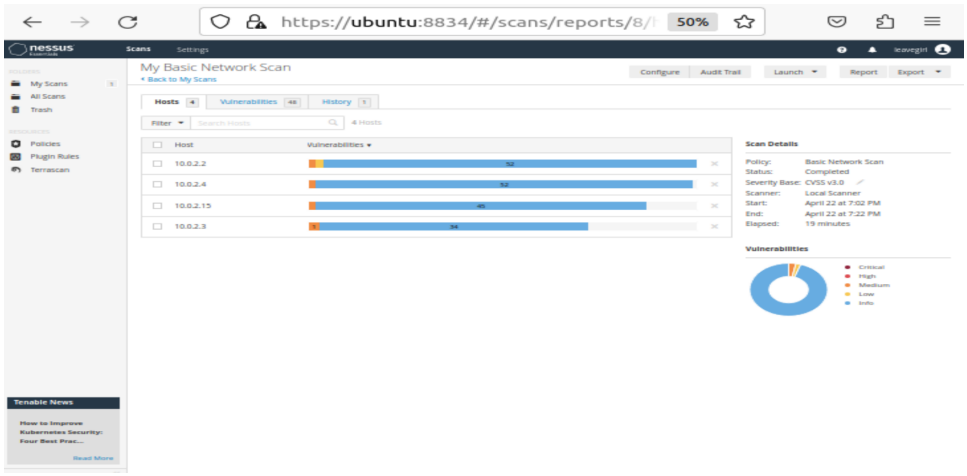
- **Open Ports and services running on ports and versions**

All 1000 scanned ports on Ubuntu (10.0.2.15) are closed

Part 2: Vulnerability Scanning

Nessus Screenshots:





Top 5 Vulnerabilities/Info:
**** My Nessus only displayed three vulnerabilities, which were low, medium, and mixed.**
**** Professor has given me permission to list out info as well that Nessus provided.**
****Information is taken from Nessus Scan and Nist Website that lists all CVEs.**

Low:
DHCP Server Detection
Description:
This script contacts the remote DHCP server to retrieve information about the network layout, which could include sensitive details such as the NIS domain name or network web server list. While this script does not exhibit any vulnerability, a local attacker may leverage DHCP to gain insights into the associated network. To prevent DHCP Server Detection, it is recommended to filter the network and eliminate any unused options. The primary vulnerability associated with this issue is CVE-2023-28488, which involves the client.c in gdhcp in ConnMan through version 1.41. Attackers operating a crafted DHCP server could exploit this vulnerability to trigger a stack-based buffer overflow and deny service, thereby terminating the connman process.

Medium:
SMB Signing not required
Description:
The remote SMB server has a weakness where it doesn't need message signing, allowing attackers to attack the server without authentication. To prevent these attacks, message signing should be turned on in the host's settings. On Windows, this can be done by enabling the 'Microsoft network server: Digitally sign communications (always)' policy setting. On Samba, it can be done by enabling the 'server signing' setting. The problem is called CVE-2016-2115, and it affects Samba 3.x and 4.x. Attackers can modify the client-server data stream and trick SMB clients without requiring SMB signing in a DCERPC session over ncacn_np.

Medium:
SSL Certificate Cannot Be Trusted
Description:
The message means that the server's X.509 certificate might not be trustworthy for three reasons. First, the certificate chain's top, which the server sent, might not be recognized by a well-known public certificate authority. Second, the certificate chain could have an expired invalid certificate. Third, the signature on the certificate might not be checkable. Any problem with the chain makes it hard to confirm if the web server is real, making it easy for attackers to trick the remote host with man-in-the-middle attacks. This security flaw is linked to CVE-2010-4340, which involves libcloud before version 0.4.1. It fails to check SSL certificates for HTTPS connections, allowing attackers to bypass access controls and make fake certificates with man-in-the-middle attacks.

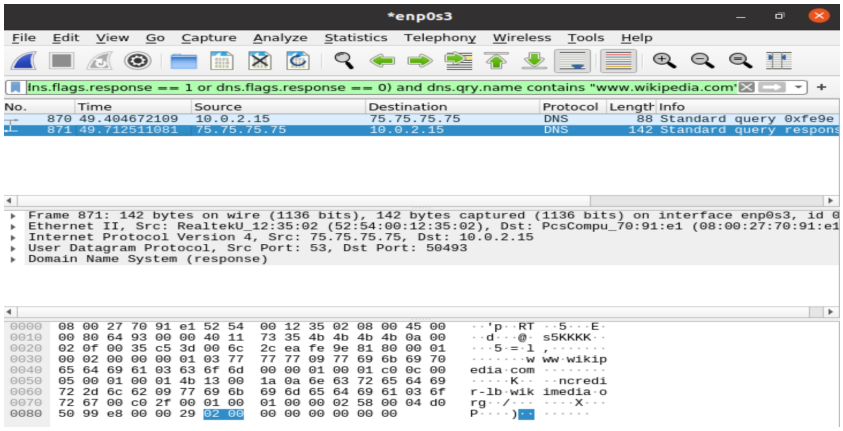
Info:
Nessus SYN scanner
Description:
This tool is a type of port scanner used by Nessus to quickly scan targets behind a firewall. It is not as strong as other scans that can break services, but it may still cause problems for weaker firewalls and may leave open connections on the target if the network is busy.
To keep your target safe, it is best to use an IP filter.

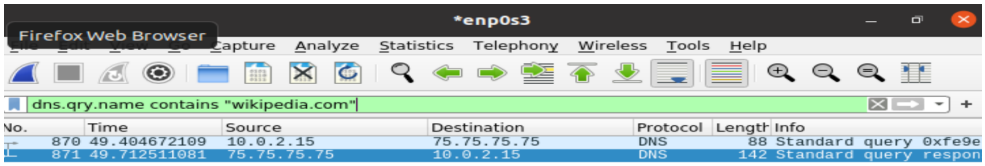
Info:
Enumerate IPv4 Interfaces via SSH
Description:
This message from Nessus says that it found out which network interfaces have IPv4 addresses on the remote computer by using SSH with the given login information. To make the computer safer, it's recommended to turn off any network interfaces that are not being used.

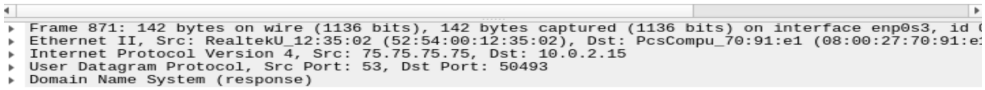
3.2

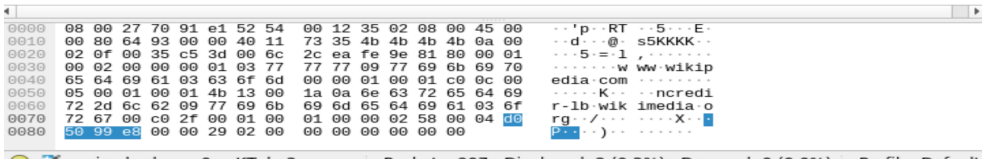
The transport layer protocol used in the DNS query packet is UDP, and the decimal number in the network layer header that identifies this protocol is 17.

3.3









3.4.

Raw Results:

1 0.000000000 PcsCompu_70:91:e1 Broadcast ARP 58 Who has 208.80.153.224? Tell 10.0.2.15

2 1.005063308 PcsCompu_70:91:e1 Broadcast ARP 58 Who has 208.80.153.224? Tell 10.0.2.15

3 2.010036189 PcsCompu_70:91:e1 Broadcast ARP 58 Who has 208.80.153.224? Tell 10.0.2.15

6 3.014411317 PcsCompu_70:91:e1 Broadcast ARP 58 Who has 208.80.153.224? Tell 10.0.2.15

7 4.015364477 PcsCompu_70:91:e1 Broadcast ARP 58 Who has 208.80.153.224? Tell 10.0.2.15

8 5.015483046 PcsCompu_70:91:e1 Broadcast ARP 58 Who has 208.80.153.224? Tell 10.0.2.15

682 22.057669131 PcsCompu_70:91:e1 Broadcast ARP 58 Who has 208.80.153.224? Tell 10.0.2.15

870 49.404672109 10.0.2.15 75.75.75.75 DNS 88 Standard query 0xfe9e A www.wikipedia.com OPT

871 49.712511081 75.75.75.75 10.0.2.15 DNS 142 Standard query response 0xfe9e A www.wikipedia.com CNAME ncredir-lb.wikimedia.org A 208.80.153.232 OPT

ARP Query/Response Pairs:
Query 1: "Who has 208.80.153.224? Tell 10.0.2.15"
Response 1: Not captured
Query 2: "Who has 208.80.153.224? Tell 10.0.2.15"
Response 2: Not captured
Query 3: "Who has 208.80.153.224? Tell 10.0.2.15"
Response 3: Not captured
Query 4: "Who has 208.80.153.224? Tell 10.0.2.15"
Response 4: Not captured
Query 5: "Who has 208.80.153.224? Tell 10.0.2.15"
Response 5: Not captured
Query 6: "Who has 208.80.153.224? Tell 10.0.2.15"
Response 6: Not captured
DNS Query/Response Pairs:

Query 1: "Standard query 0x15a9 A doh2.gslb2.xfinity.com OPT"
Query source: IP address 10.0.2.15
Query destination: IP address 75.75.75.75
Response 1: Not captured
Query 2: "Standard query 0xfe9e A www.wikipedia.com OPT"
Query source: IP address 10.0.2.15
Query destination: IP address 75.75.75.75
Response 2: "Standard query response 0xfe9e A www.wikipedia.com CNAME ncredir-lb.wikimedia.org A 208.80.153.232 OPT"
Response source: IP address 75.75.75.75
Response destination: IP address 10.0.2.15

DNS Query/Response Pairs:
Query 1: "Standard query 0x15a9 A doh2.gslb2.xfinity.com OPT"
Query source: IP address 10.0.2.15

Query destination: IP address 75.75.75.75
Response 1: Not captured

Query 2: "Standard query 0xfe9e A www.wikipedia.com OPT"
Query source: IP address 10.0.2.15
Query destination: IP address 75.75.75.75
Response 2: "Standard query response 0xfe9e A www.wikipedia.com CNAME ncredir-lb.wikimedia.org A 208.80.153.232 OPT"
Response source: IP address 75.75.75.75
Response destination: IP address 10.0.2.15

Questions for ARP:

- **Info on query, MAC address, IP address, who answered, info in answer**

The ARP query was asking for the MAC address associated with the IP address 208.80.153.224. The query was sent by the device with MAC address "PcsCompu_70:91:e1" and IP address 10.0.2.15, and was broadcasted to all devices on the network. There was no answer to the query in the captured packets.

The device with IP address 10.0.2.15 was trying to establish communication with the device associated with the IP address 208.80.153.224, but did not have the MAC address information necessary for the communication to occur. By sending an ARP query, it was waiting to obtain the MAC address of the device with the specified IP address.

Questions for DNS:

- **Info on query, MAC address, IP address, who answered, info in answer**

The query was asking for the IP address of "www.wikipedia.com" and was sent from IP address 10.0.2.15 with MAC address. The query was sent to the DNS server with IP address 75.75.75.75.

The response to the query was sent from the DNS server with IP address 75.75.75.75 and MAC address. It included the IP address of the CNAME "ncredir-lb.wikimedia.org" (208.80.153.232), which is the final destination for the query to resolve "www.wikipedia.com".

The query was made by a client device (with IP address 10.0.2.15) that was trying to access the website "www.wikipedia.com", and it needed to resolve the domain name to an IP address so it could establish a connection. The DNS server with IP address 75.75.75.75 was likely the primary DNS server configured on the client device.