PCAP FILE ANALYSIS REPORT

BY-ABHAY PRATAP SINGH

COURSE- BTECH ICE

-------------------------------------------------------------------

Question 1

Type of traffic present?

Solution

Frame, Ethernet, Internet protocol version 4, Transmission control protocol, Internet protocol version 6, User Datagram protocol, Hypertext transfer protocol

------------------------------------------------------------------------

Question 2

How many DNS queries were made in total?

Solution

A total of 357 dns queries were made.

Question 3

What types of DNS queries were made?

Solution

A

AAAA

HTTPS

PTR

THESE TYPE OF QUERIES WERE MADE.

--------------------------------------------------------------------------------------------------------------------------------------

Question 4

What is a Loopback Interface?

Solution

A loopback interface is a virtual network interface that exists solely within a device that allows a device to test its own network software and functionality while ensuring a stable and reliable management address.

IP address: **127.0.0.1**

It’s often used for testing or local communication.

--------------------------------------------------------------------------------------------------------------------------------------

Question 5

**Number of .txt Files Requested and Their Names?**

Solution

1. Decoy2.txt
2. Encoded.txt
3. Decoy1.txt

---------------------------------------------------------------------------------------------------------

Question 6

One .txt file contains base64-encoded content. Identify and decode it. What does it contain?

Solution

A http protocol packet

Packet source destination protocol info

207 127.0.01 127.0.01 HTTP GET/encoded.txt HTTP/1.1

After decoding we get

a1GET /encoded.txt HTTP/1.1

Host: localhost:8000

User-Agent: curl/8.5.0

Accept: \*/\*

HTTP/1.0 200 OK

Server: SimpleHTTP/0.6 Python/3.12.3

Date: Sat, 10 May 2025 13:08:22 GMT

Content-type: text/plain

Content-Length: 41

---------------------------------------------------------------------------------------------------------

Question 7

**Evidence of Decoy Files Used to Distract the Analyst**

**Solution**

Yes, decoy1.txt and decoy2.txt

---------------------------------------------------------------------------------------------------------

Question 8

**Use of Known Ports for Uncommon Services**

**Solution**

port A:52400

port B:8000

-------------------------------------------------------------------------

Question 9

How many HTTP GET requests are visible in the capture?

Solution

Three requests are visible, packet number

180

207

752

---------------------------------------------------------------------------------

Question 10

What User-Agent was used to make the HTTP requests?

Solution

User agent used to make the HTTP request here is

Curl/8.5.0

-------------------------------------------------------------------------