Sreehari P J , 110124122 , ICE

Computer Networking Basic task

1. What types of traffic (HTTP, DNS, FTP, etc.) are present?
A. ipv6,ip,udp,tcp,http,frame,mdns,eth,dns,data-text-lines

2. How many DNS queries were made in total?
A. 714

3. What types of DNS queries were made?
A. A(IPv4), AAAA(IPv6), HTTPS

4. What is a Loopback Interface?
A. The loopback interface is a virtual network interface that allows a computer to communicate with itself.

5. How many .txt files were requested? List their names.
A.3 GET recorded, names are decoy2.txt,encoded.txt,decoy1.txt (in the order of time)

6. One .txt file contains base64-encoded content. Identify and decode it.
What does it contain?
A. FLAG{spid3r_network_master}

7. Was any attempt made to distract the analyst using decoy files? Explain.
A. Yes, 2 Get requests of decoy were made to distract, but it can be easily dealt with when time is ordered.
those decoy files contents were had "Nothing to see here.\n" and "This is just a decoy.\n"

8. Are there any known ports being used for uncommon services?
A. Yes, HTTP traffic on TCP 8000 "Host: localhost:8000"

9. How many HTTP GET requests are visible in the capture?
A. 3

10. What User-Agent was used to make the HTTP requests?
A. curl/8.5.0

c3JlZWhhcmlfc3BpZDNyX25ldHdva2luZ19iYXNpY190YXNr