

Name: Amit Raj

Roll no.: 110124014

Task: Computer networking basic task

1. What types of traffic (HTTP, DNS, FTP, etc.) are present?

⇒ DNS, HTTP, TCP, MDNS

2. How many DNS queries were made in total?

⇒ 357(358 including mDNS)

3. What types of DNS queries were made?

⇒ A, AAAA, HTTPS, PTR

4. What is a Loopback Interface?

⇒ A loopback interface is a virtual network interface on a computer or network device that is used to communicate with itself.

5. How many .txt files were requested? List their names.

⇒ 3

Names: decoy2.txt, encoded.txt, decoy1.txt

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

⇒ encoded.txt has.

FLAG{spid3r\_network\_master}

7. Was any attempt made to distract the analyst using decoy files? Explain.

⇒ Yes, other two files had unrelated info.

decoy2.txt - Nothing to see here.

decoy1.txt - This is just a decoy.

8. Are there any known ports being used for uncommon services?

⇒ In TCP analysis all are targeting port 8000 which isn't standard in general internet traffic compared to port 80 or 443.

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

⇒ 3

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

⇒ curl/8.5.0\r\n