Computer Networking Task

Spider (Common Tasks)

Submitted by: Parth Patidar

Roll Number: 114124072

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

The capture primarily contains **DNS (93.5%)**, **UDP (93.6%)**, and **IPv4 (99.2%)** traffic, with minor HTTP (0.8%) and TCP (5.6%) activity. No FTP or HTTPS was detected, though DNS dominance suggests heavy domain-name resolution activity. Also, IPv6 (0.8%) and Multicast DNS (0.1%) appeared in trace amounts.

2. How many DNS queries were made in total?

There were **357 DNS queries** observed. This high volume indicates frequent domain-name lookups, possibly due to web browsing or automated scripts.

3. What types of DNS queries were made?

All DNS queries were either:

- **A records:** Requests for IPv4 addresses (e.g., 192.0.2.1)
- **AAAA records:** Requests for IPv6 addresses (e.g., 2001:db8::1)

No other query types (like MX or TXT) were found, indicating basic domain lookups without email or security checks.

4. What is a Loopback Interface?

he loopback interface (IP address **127.0.0.1** or **::1** in IPv6) allows a computer to send network traffic to itself. It's commonly used for testing services locally without needing an external network. For example, a developer might run a website on http://localhost:8000.

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

Three files were fetched via HTTP GET:

1. **decoy1.txt**
2. **decoy2.txt**
3. **encoded.txt**

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

The file **encoded.txt** contained a Base64 string. Decoding it revealed:
FLAG{spid3r_network_master}

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

Two files were clearly meant to mislead anyone analyzing the traffic:

- **decoy1.txt** contained the text: *"This is just a decoy."*
- **decoy2.txt** contained: *"Nothing to see here."*

Meanwhile, the real payload was hidden in **encoded.txt**, showing an attempt to hide important data among fake files.

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

No unusual ports were detected. **Port 8000** (HTTP alternate) and ephemeral ports (e.g., 37216) are typical for local testing and client-side connections.

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

Only **3 HTTP GET requests** were made in the entire capture, all requesting text files:

1. GET /decoy1.txt HTTP/1.1
2. GET /decoy2.txt HTTP/1.1
3. GET /encoded.txt HTTP/1.1.

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

The HTTP requests were made using **curl/8.5.0**, a command-line tool for transferring data. This indicates automated or scripted downloads, as opposed to a web browser which would show a User-Agent like *Mozilla/5.0*.