Computer Networking

Basic Task

-Hirthick Diyan V

108124047

Analysis Questions:

1. **What types of traffic (HTTP, DNS, FTP, etc.) are present?**
   Types of traffic which were present:
   - DNS and mDNS traffic ran over UDP observed
   - HTTP traffic ran over TCP was observed
   - General TCP traffic was observed which consists of 3-way handshakes and some RESET and PUSH flags were also observed within TCP.
2. **How many DNS queries were made in total?**
   358 DNS queries were made in total in which one was a mDNS query.
3. **What types of DNS queries were made?**
   Types of DNS queries made:
   - A - To lookup an IPv4 address
   - AAAA - To lookup an IPv4 address
   - HTTPS - To discover metadata about how to securely connect to a service
   - PTR - used in reverse DNS lookups
4. **What is a Loopback Interface?**
   The loopback interface is a virtual interface on a machine that is used to send network traffic to itself without requiring a physical network connection.
5. **How many .txt files were requested? List their names.**
   3 were requested.
   - decoy1.txt
   - decoy2.txt
   - encoded.txt
6. **One .txt file contains base64-encoded content. Identify and decode it. What does it contain?**
   It contains “FLAG{spid3r_network_master}”
7. **Was any attempt made to distract the analyst using decoy files? Explain.**
   Yes along with the encoded file two decoy files with text “This is just a decoy.” And “Nothing to see here.” were given as distractions to distract the analyst.
8. **Are there any known ports being used for uncommon services?**
   We can say that localhost:8000 normally used for testing loopback are used to send and receive .txt files here but otherwise no known ports are being used for uncommon services.
9. **How many HTTP GET requests are visible in the capture?**
   3 HTTP GET requests are visible in the capture.
10. **What User-Agent was used to make the HTTP requests?**
    curl/8.5.0 was the User-Agent which was used to make the HTTP requests.