Detailed Solution: How to Exploit and Solve the Challenge

Overview of the Challenge

This challenge involves analyzing a set of network packets (challenge.pcap) that contains hidden messages across different protocols (DNS, ICMP, and HTTP). The goal is to extract the full flag by piecing together hidden parts found in each protocol.

Steps to Solve the Challenge

Step 1: Analyze DNS Traffic

1. **Filter DNS Packets in Wireshark**: Open the challenge.pcap file in Wireshark and apply the following filter to focus on DNS traffic:

   dns

2. **Inspect DNS Query and Response**: Look for DNS queries for hidden.flag. In the corresponding DNS response, note the subdomain hidden.<encoded_message>.example.com.
3. **Decode the Subdomain**: The subdomain contains a BASE64-encoded hidden message. Extract and decode it using an online BASE64 decoder or Python:

   ```
   import base64
   encoded_message = "Q1RGX3BhcnRfMV9oaWRkZW4="    # Replace with the actual data
   print(base64.b64decode(encoded_message).decode())
   ```

   Result: CTF_part_1_hidden

Step 2: Extract Data from ICMP Packets

1. **Filter ICMP Packets in Wireshark**: Use the following filter to isolate ICMP traffic:

   icmp

2. **Inspect ICMP Payload**: Check the data field in the ICMP packets. The payload contains the second part of the flag: CTF_part_2_hidden.

Step 3: Analyze HTTP Traffic

1. **Filter HTTP Packets in Wireshark**: Apply the following filter to focus on HTTP traffic:

   http

2. **Inspect HTTP Responses**: Look for HTTP responses from the /response endpoint. The response body will include the third part of the flag: hidden_flag_part_3:CTF_hidden.

Step 4: Combine All Parts of the Flag

Once you've extracted all parts of the flag:

- From DNS: CTF_part_1_hidden
- From ICMP: CTF_part_2_hidden
- From HTTP: hidden_flag_part_3:CTF_hidden

Combine them into the final flag:

CTF{part_1_hidden_part_2_hidden_flag_part_3_hidden}

Tools Used

- **Wireshark**: For packet capture analysis.
- **Python**: For decoding BASE64.
- **Scapy**: For generating ICMP packets with embedded data.

Conclusion

The challenge is designed to test the participants' ability to analyze network traffic, decode hidden data, and piece together information across multiple protocols. The

challenge.pcap provides all the necessary data, so no additional setup is required by the participants.