EX.NO: 4 ANALYZE THE MALICIOUS NETWORK TRAFFIC USING WIRESHARK

DATE: 05.03.2025 ROLLNO:231901035 NAME: NITHEESH

KK

Aim:

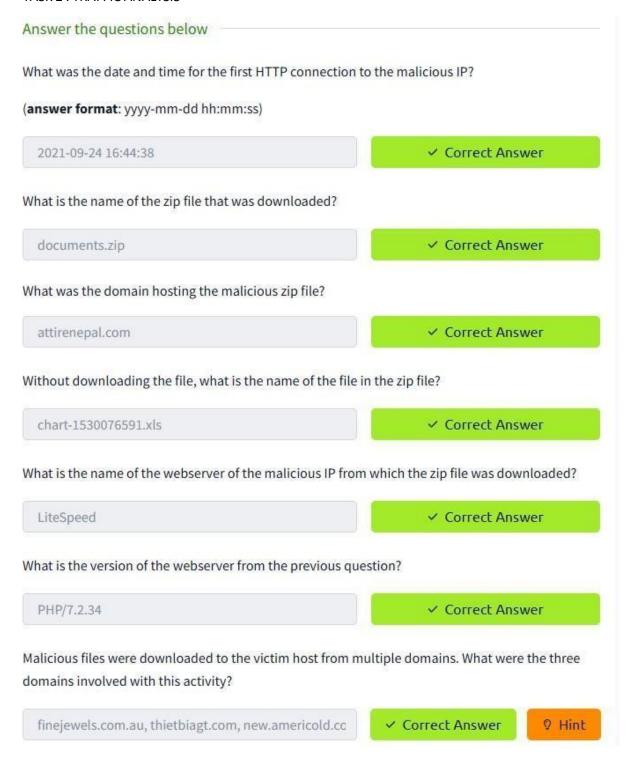
To analyze a **malicious pcap file** using **Wireshark** and investigate network traffic to uncover malicious activities, such as file downloads, Cobalt Strike servers, and post-infection communications.

Procedure:

- 1. Load the pcap file in Wireshark.
- 2. Identify the first HTTP connection to the malicious IP (http.request).
- 3. Find the downloaded zip file by analyzing HTTP GET requests.
- 4. Extract the hosting domain from the Host header.
- 5. Check the file inside the zip (Look at Content-Disposition).
- 6. Identify the web server and version (http.server filter).
- 7. Analyze SSL traffic to find certificate details (ssl.handshake).
- 8. Find the Cobalt Strike C2 servers using VirusTotal.
- 9. **Analyze post-infection traffic** (Check domains contacted after infection).
- 10. **Identify the victim's outbound connections** for possible data exfiltration.

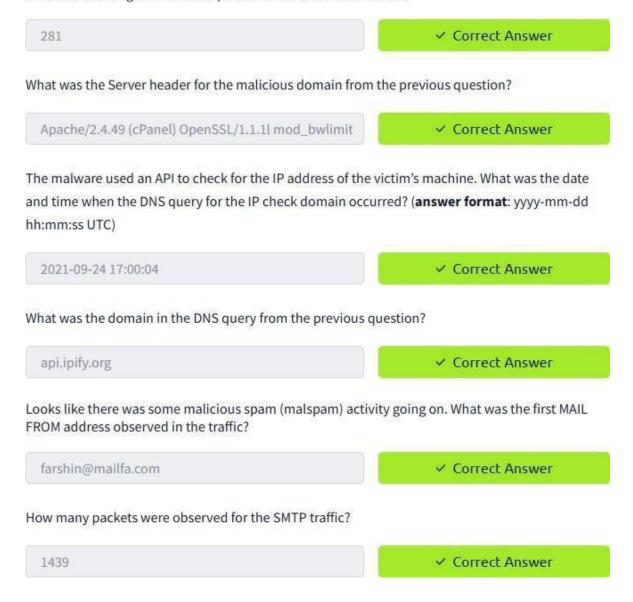


TASK 2: TRAFFIC ANALYSIS



Which certificate authority issued the SSL certificate to the first domain from the previous question? ✓ Correct Answer GoDaddy What are the two IP addresses of the Cobalt Strike servers? Use VirusTotal (the Community tab) to confirm if IPs are identified as Cobalt Strike C2 servers. (answer format: enter the IP addresses in sequential order) Hint 185.106.96.158, 185.125.204.174 ✓ Correct Answer What is the Host header for the first Cobalt Strike IP address from the previous question? ocsp.verisign.com ✓ Correct Answer What is the domain name for the first IP address of the Cobalt Strike server? You may use VirusTotal to confirm if it's the Cobalt Strike server (check the Community tab). survmeter.live ✓ Correct Answer 9 Hint What is the domain name of the second Cobalt Strike server IP? You may use VirusTotal to confirm if it's the Cobalt Strike server (check the Community tab). 9 Hint securitybusinpuff.com ✓ Correct Answer What is the domain name of the post-infection traffic? 9 Hint ✓ Correct Answer maldivehost.net What are the first eleven characters that the victim host sends out to the malicious domain involved in the post-infection traffic? zLlisQRWZI9 ✓ Correct Answer

What was the length for the first packet sent out to the C2 server?



Result:

TryHackMe platform **Carnage - Traffic Analysis using Wireshark** tasks have been successfully completed.