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

## Answer the questions below

What was the date and time for the first HTTP connection to the malicious IP?

(**answer format**: yyyy-mm-dd hh:mm:ss)

2021-09-24 16:44:38 ✓ Correct Answer

What is the name of the zip file that was downloaded?

documents.zip ✓ Correct Answer

What was the domain hosting the malicious zip file?

attirenepal.com ✓ Correct Answer

Without downloading the file, what is the name of the file in the zip file?

chart-1530076591.xls ✓ Correct Answer

What is the name of the webserver of the malicious IP from which the zip file was downloaded?

LiteSpeed ✓ Correct Answer

What is the version of the webserver from the previous question?

PHP/7.2.34 ✓ Correct Answer

Malicious files were downloaded to the victim host from multiple domains. What were the three domains involved with this activity?

finejewels.com.au, thietbiagt.com, new.americold.cc ✓ Correct Answer Hint

Which certificate authority issued the SSL certificate to the first domain from the previous question?

GoDaddy ✓ Correct Answer

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)

185.106.96.158, 185.125.204.174 ✓ Correct Answer Hint

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 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).

securitybusinpuff.com ✓ Correct Answer Hint

What is the domain name of the post-infection traffic?

maldivehost.net ✓ Correct Answer Hint

What are the first eleven characters that the victim host sends out to the malicious domain involved in the post-infection traffic?

zLIisQRWZI9 ✓ Correct Answer

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

281 ✓ Correct Answer

What was the Server header for the malicious domain from the previous question?

Apache/2.4.49 (cPanel) OpenSSL/1.1.1l mod_bwlimit ✓ Correct Answer

The malware used an API to check for the IP address of the victim's machine. What was the date and time when the DNS query for the IP check domain occurred? (**answer format**: yyyy-mm-dd hh:mm:ss UTC)

2021-09-24 17:00:04 ✓ Correct Answer

What was the domain in the DNS query from the previous question?

api.ipify.org ✓ Correct Answer

Looks like there was some malicious spam (malspam) activity going on. What was the first MAIL FROM address observed in the traffic?

farshin@mailfa.com ✓ Correct Answer

How many packets were observed for the SMTP traffic?

1439 ✓ Correct Answer

**Result:**

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