Tugas Training CaKru Day 5

Networking: OSI Layer 101 dan Wireshark

NAMA : Christian Valerioksana Laujerly Sebayang
NIM : 16523079

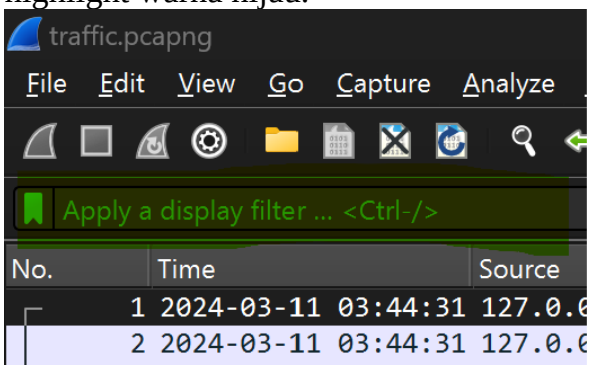
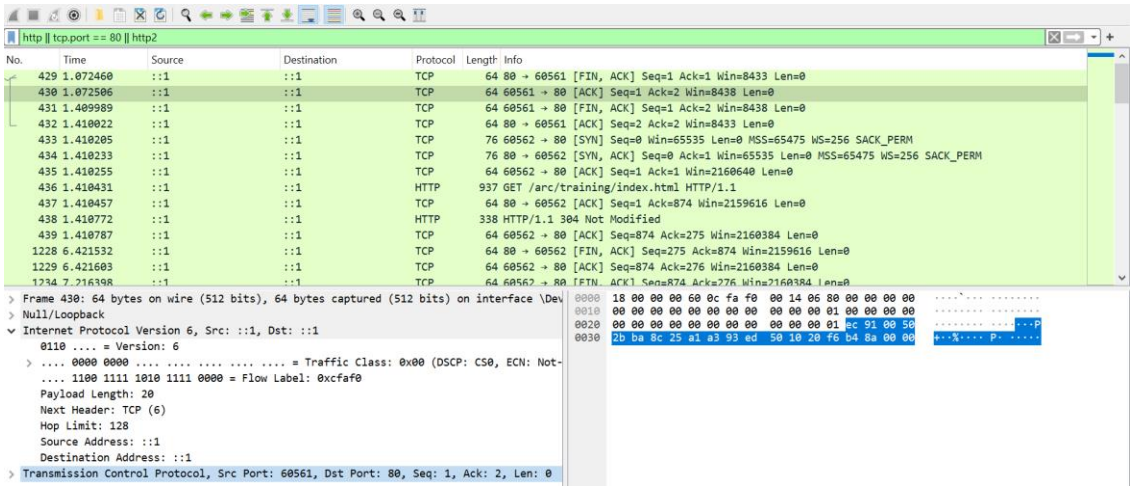
Cara Menjawab:
Pilih menu File > Make a copy, untuk dokumen ini. Isi pada kolom jawaban.
Deadline : **23 Maret 2024, pukul 23.59 WIB**
Pengumpulan: https://forms.gle/ckqLXcd7k2p9KpCt7

Anda diberikan sebuah captured traffic yang dapat diunduh pada link berikut:
traffic.zip

Tugas anda adalah menganalisis traffic network tersebut. Sebagai problem setter yang baik, kami memberikan langkah-langkah untuk menyelesaikan tugas tersebut. Silakan menambahkan screenshot gambar untuk mendukung penjelasan.

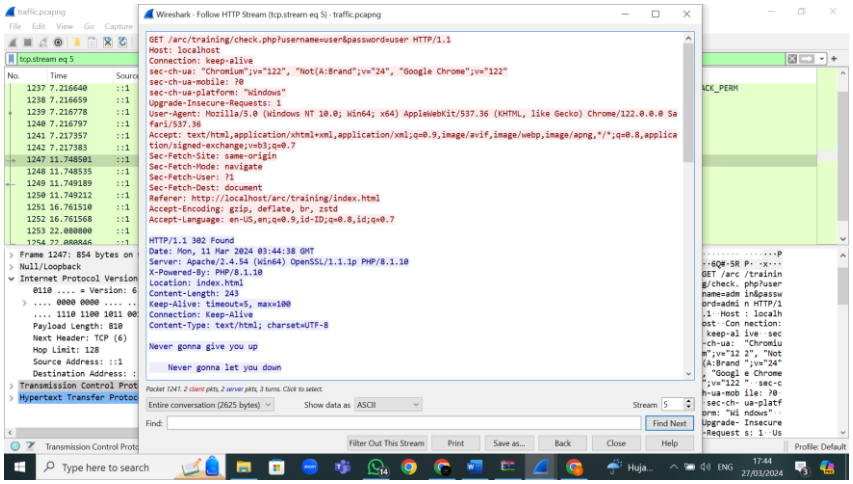
Tugas Day 5

1. Network Protocol Filter

Deskripsi
File di atas berisi 2407 paket. Tidak mungkin Anda menganalisis satu per satu. Oleh karena itu, lakukanlah penyaringan protokol jaringan pada kolom yang di-highlight warna hijau. 
Jawaban
 Protokol:TCP, HTTP Alasan: dengan Metode filtering yang disesuikan dengan color rules http || tcp.port == 80 || http2

2. Akun pengguna

Deskripsi
Tampaknya, pengguna melakukan beberapa percobaan login. Dapatkah kamu menemukan kredensial asli pengguna?
Jawaban



Username: user
Password: user
Alasan: Dengan View analisis dari HTTP yang sudah di filtering kita dapat tahu bahwa user menggunakan usrname dan password dan pengiriman metode apa , POST atau GET

3. Redirect

Deskripsi
Apabila berhasil login, halaman/lokasi manakah yang akan dikunjungi pengguna?

Jawaban

```
GET /arc/training/check.php?username=user&password=user HTTP/1.1
Host: localhost
Connection: keep-alive
sec-ch-ua: "Chromium";v="122", "Not(A:Brand";v="24", "Google Chrome";v="122"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Sa
fari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applica
tion/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/arc/training/index.html
Accept-Encoding: gzip, deflate, br, zstd
Accept-Language: en-US,en;q=0.9,id-ID;q=0.8,id;q=0.7

HTTP/1.1 302 Found
Date: Mon, 11 Mar 2024 03:44:38 GMT
Server: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/8.1.10
X-Powered-By: PHP/8.1.10
Location: index.html
Content-Length: 243
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

Never gonna give you up
```

Nama file atau full url: http://localhost/arc/training/index.html
Alasan: dengan HTTP scream dapat melihat page tujuan user

4. Extract File

Deskripsi
Pada halaman/lokasi di jawaban pertanyaan 3, seharusnya pengguna diberikan 3 buah url. Pengguna mengklik salah satu link sehingga mengunduh suatu file. File apa yang pengguna unduh? File yang benar adalah sebuah file yang dapat dijalankan dan memberikan suatu link. Link tersebut berisi sebuah **bendera** dengan format **FLAG{}**

Jawaban

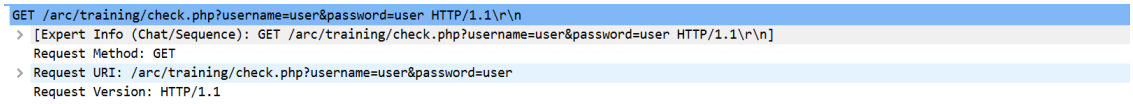
Nama file: image.png

Flag:

Alasan: di Accept terlihat tiga page dan salah satunya page yang berisi flag namun di komputer saya tidak dapat di ekstrak

5. Summary

Deskripsi
Jelaskan cara kerja web yang pengguna akses dan pengetahuan apa yang Anda dapatkan setelah mengerjakan tugas menggunakan Wireshark?
Jawaban



Cara kerja web:

Web di atas sepertinya memiliki 4 buah halaman, yaitu.

Halaman utama adalah Login Page

Mekanisme login adalah

Username dan password dikirim melalui PHP dan menggunakan METHOD GET

Wireshark:

Wireshark keren banget, Terima kasih Wireshark.

BONUS

Mungkin ada yang enjoy ngerjainnya. Jadi, kami menyiapkan soal BONUS, maksimal +15 poin.

Anda diberikan sebuah captured traffic yang dapat diunduh pada link berikut: bonus_day5.zip

Tugas anda adalah mendapatkan **FLAG** pada paket dengan format . Sebagai problem setter yang baik, kami memberikan langkah-langkah untuk menyelesaikan tugas tersebut.

1. Identifikasi ekstensi file bendera dengan pencocokan hex signature.
   Referensi: List of file signatures - Wikipedia
2. Lakukan filter dengan command berikut.
   ```
   data.data contains "ext123"
   ```
3. Extract setiap paket yang mengandung bendera
4. Langkah-langkah yang Anda lakukan dapat dirangkum dalam kolom di bawah

   Story telling aja jawabnya dan kalo bisa tambahkan screenshot gambar yang mendukung.

   Contoh writeup: Writeup-Netcomp CTF UGM.pdf

Jawaban