1

BÁO CÁO THỰC HÀNH

Môn học: Nhập môn mạng máy tính
Buổi báo cáo: Lab 01
Tên chủ đề: Làm quen với Wireshark
Bài tập về nhà
GVHD: Ngô Khánh Khoa
Ngày thực hiện: 06/03/2024
Ngày nộp báo cáo: 20/03/2024

1. THÔNG TIN CHUNG:

Lớp: IT005.O21.CTTN.1

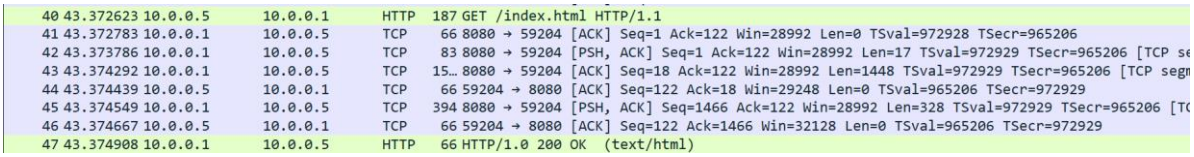
STT	Họ và tên	MSSV	Email
1	Đoàn Đức Anh	23520041	23520041@gm.uit.edu.vn

BÁO CÁO CHI TIẾT

I) Task 1:

*Quest 1: Find the password leak in the packet capture:

-Mở file task1.pcapng, ta chú ý bên trong có phần:



-Mở packet chứa text/html ta thấy được bên trong có nội dung quan trọng:

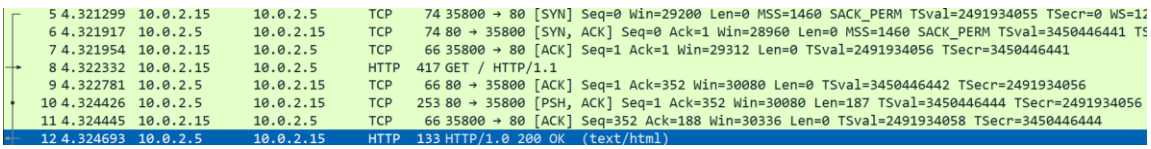
```
\t<td>Username</td>\r\n
    <td><input type="text" name="userid"/></td>\r\n
</tr>\r\n
<tr>\r\n
\t<td>Password</td>\r\n
    <td><input type="password" name="pswrd"/></td>\r\n
```

-Ta đã thấy được mật khẩu bị rò rỉ ra: pswrd

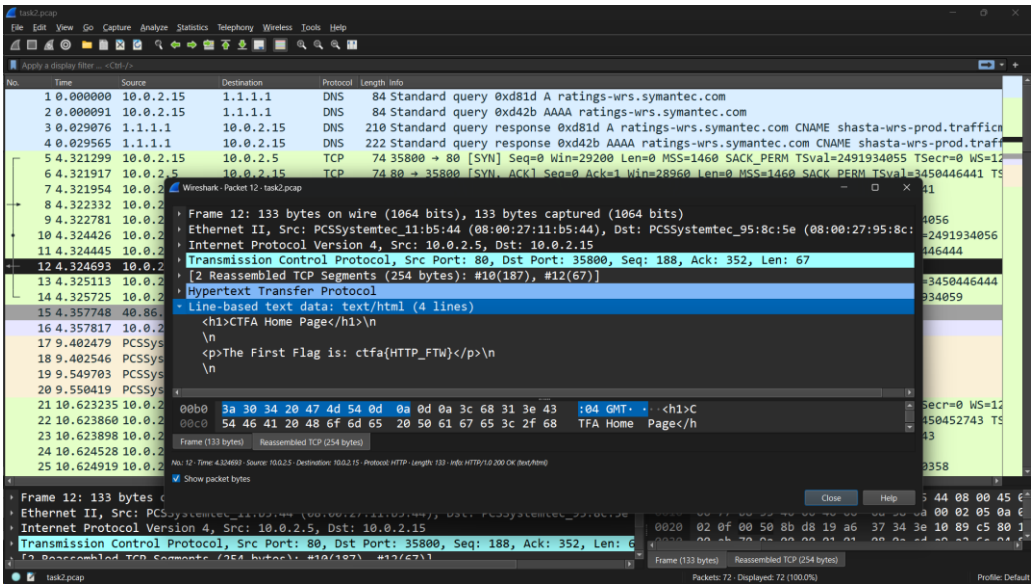
II) Task 2:

*Quest 2:What is the first flag in the packet capture?

-Tương tự như task 1, khi mở file task2.pcapng:



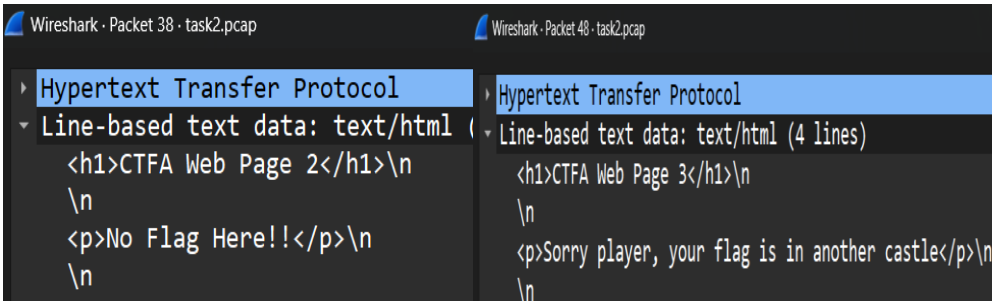
-Mở packet chứa text/html:

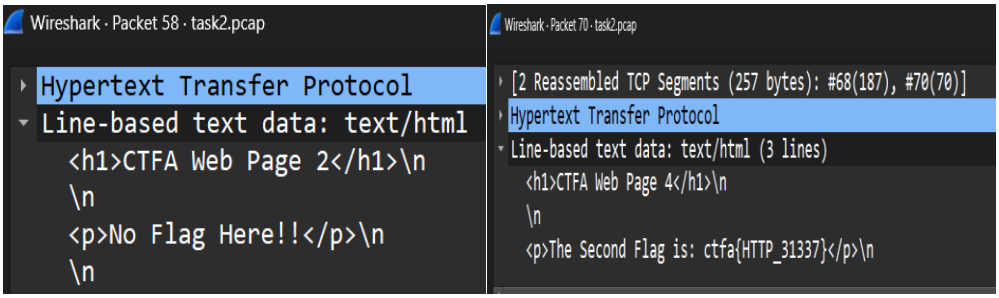


-Ta thấy flag là: ctfa{HTP_FTW}

***Quest 3:What is the second flag in the packet capture?**

-Tiếp tục tìm kiếm các packet chứa text/html bên dưới:





-Tuy nhiên ta sẽ không thấy flag ngay lập tức, ta cần tìm lần lượt và tìm thấy file flag ở packet 70.

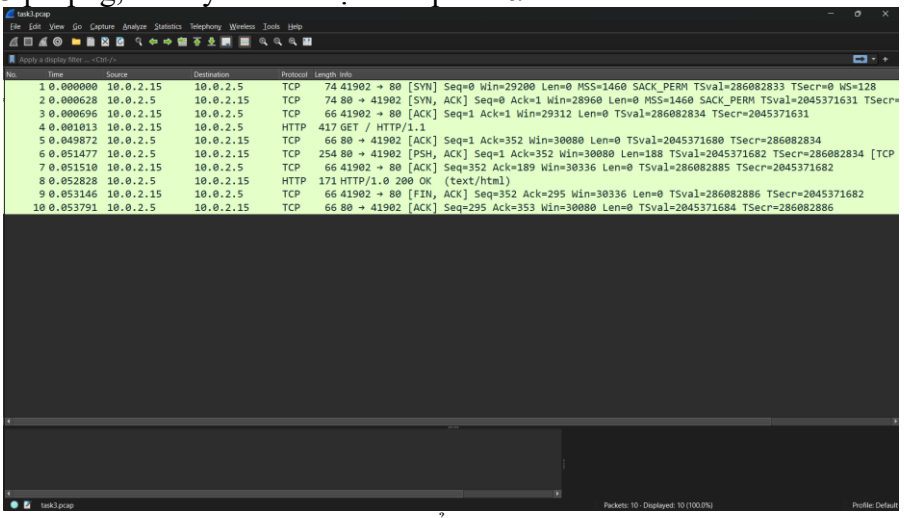
-Flag thứ 2 là : ctfa{HTTP_31337}

III) Task 3:

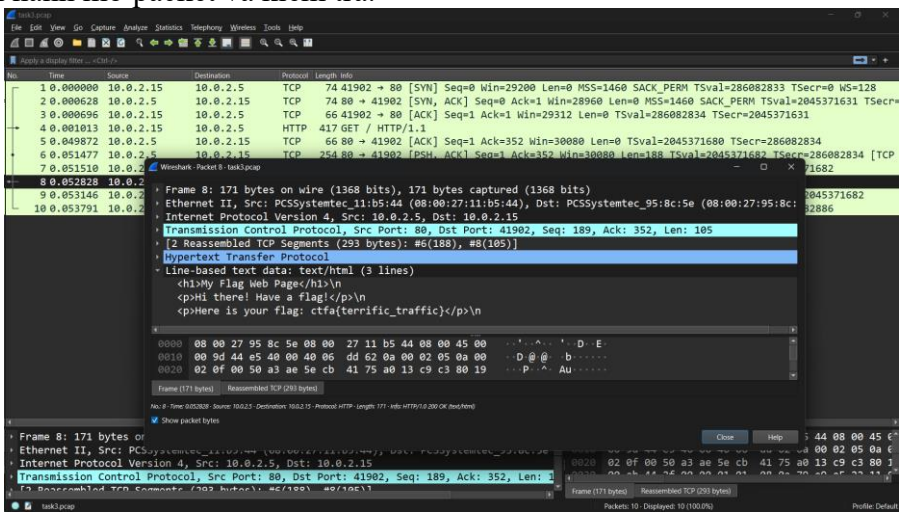
***Quest 4:What protocol was the flag transferred with?**

***Quest 5:What is the flag found in the capture file?**

-Mở file task3.pcapng, ta thấy chỉ có một số ít packet:



-Ta thấy rằng packet chứa text/html được chuyển với giao thức(protocol) là HTTP có khả năng cao chứa flag, ta tiến hành mở packet và kiểm tra.



-Ta có được flag: ctfa{terrific_traffic}