

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:

40	43.372623	10.0.0.5	10.0.0.1	HTTP	187	GET /index.html HTTP/1.1
41	43.372783	10.0.0.1	10.0.0.5	TCP	66	8080 → 59204 [ACK] Seq=1 Ack=122 Win=28992 Len=0 TSval=972928 TSecr=965206
42	43.373786	10.0.0.1	10.0.0.5	TCP	83	8080 → 59204 [PSH, ACK] Seq=1 Ack=122 Win=28992 Len=17 TSval=972929 TSecr=965206 [TCP segn
43	43.374292	10.0.0.1	10.0.0.5	TCP	15...	8080 → 59204 [ACK] Seq=18 Ack=122 Win=28992 Len=1448 TSval=972929 TSecr=965206 [TCP segn
44	43.374439	10.0.0.5	10.0.0.1	TCP	66	59204 → 8080 [ACK] Seq=122 Ack=18 Win=29248 Len=0 TSval=965206 TSecr=972929
45	43.374549	10.0.0.1	10.0.0.5	TCP	394	8080 → 59204 [PSH, ACK] Seq=1466 Ack=122 Win=28992 Len=328 TSval=972929 TSecr=965206 [TC
46	43.374667	10.0.0.5	10.0.0.1	TCP	66	59204 → 8080 [ACK] Seq=122 Ack=1466 Win=32128 Len=0 TSval=965206 TSecr=972929
47	43.374908	10.0.0.1	10.0.0.5	HTTP	66	HTTP/1.0 200 OK (text/html)

-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

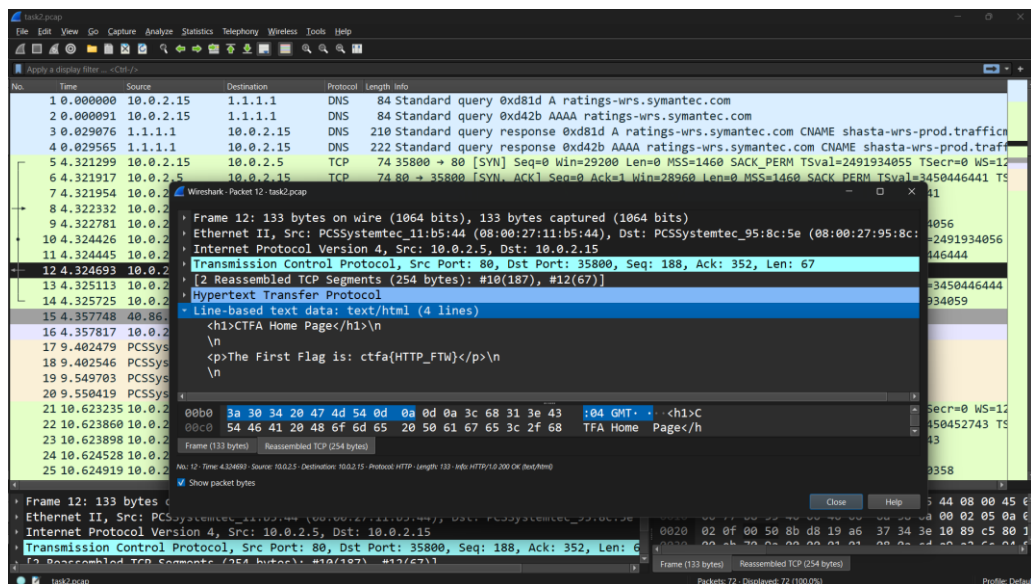
II) Task 2:

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

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

5	4.321299	10.0.2.15	10.0.2.5	TCP	74	35800 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=2491934055 TSecr=0 WS=12
6	4.321917	10.0.2.5	10.0.2.15	TCP	74	80 → 35800 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=3450446441 TS
7	4.321954	10.0.2.15	10.0.2.5	TCP	66	35800 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=2491934056 TSecr=3450446441
8	4.322332	10.0.2.15	10.0.2.5	HTTP	417	GET / HTTP/1.1
9	4.322781	10.0.2.5	10.0.2.15	TCP	66	80 → 35800 [ACK] Seq=1 Ack=352 Win=30080 Len=0 TSval=3450446442 TSecr=2491934056
10	4.324426	10.0.2.5	10.0.2.15	TCP	253	80 → 35800 [PSH, ACK] Seq=1 Ack=352 Win=30080 Len=187 TSval=3450446444 TSecr=2491934056
11	4.324445	10.0.2.15	10.0.2.5	TCP	66	35800 → 80 [ACK] Seq=352 Ack=188 Win=30336 Len=0 TSval=2491934058 TSecr=3450446444
12	4.324693	10.0.2.5	10.0.2.15	HTTP	133	HTTP/1.0 200 OK (text/html)

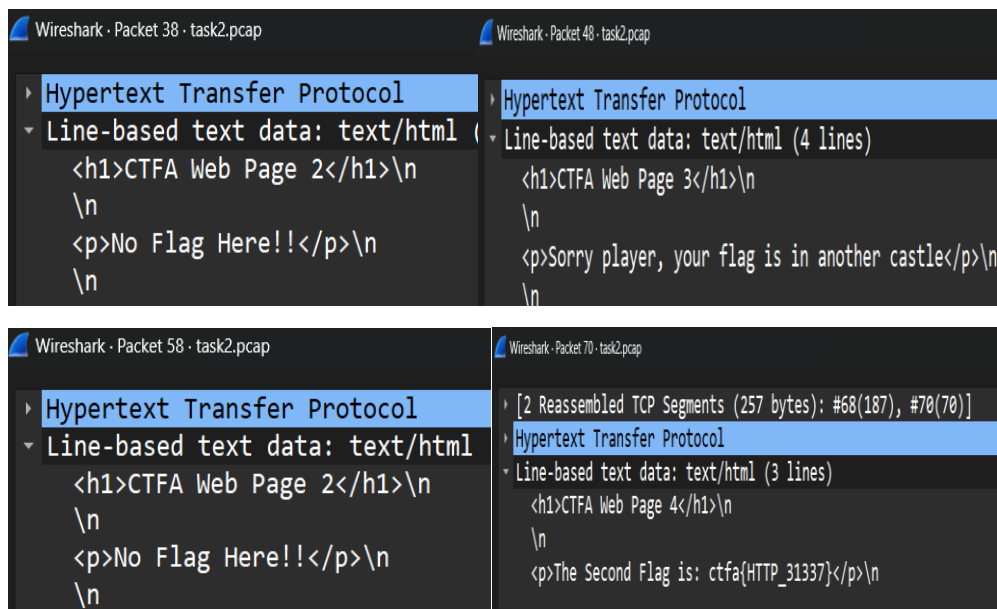
-Mở packet chứa text/html:



-Ta thấy flag là: ctfa{HTTP_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.

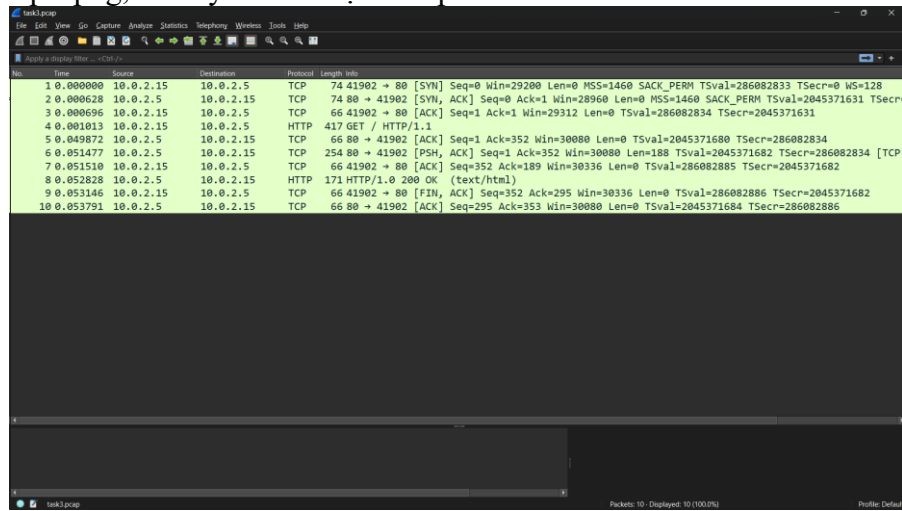
-Flag thứ 2 là : ctfa{HTTP_31337}

III) Task 3:

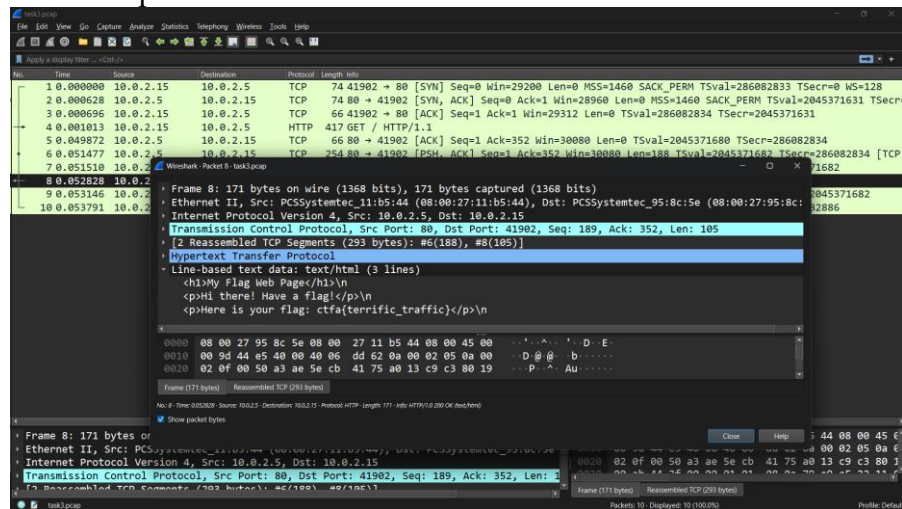
***Quest 4:What protocol was the flag transferred with?**

***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}