

Họ và tên: Phùng Thị Linh – Ngô Phương Thanh

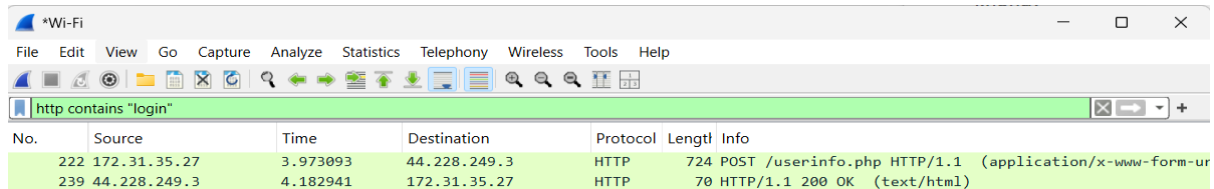
Lớp : DHKL16A1HN

BÀI KIỂM TRA SỐ 2

Bước 1: Mở Wireshark, chọn card mạng, bắt gói khi truy cập một trang web.

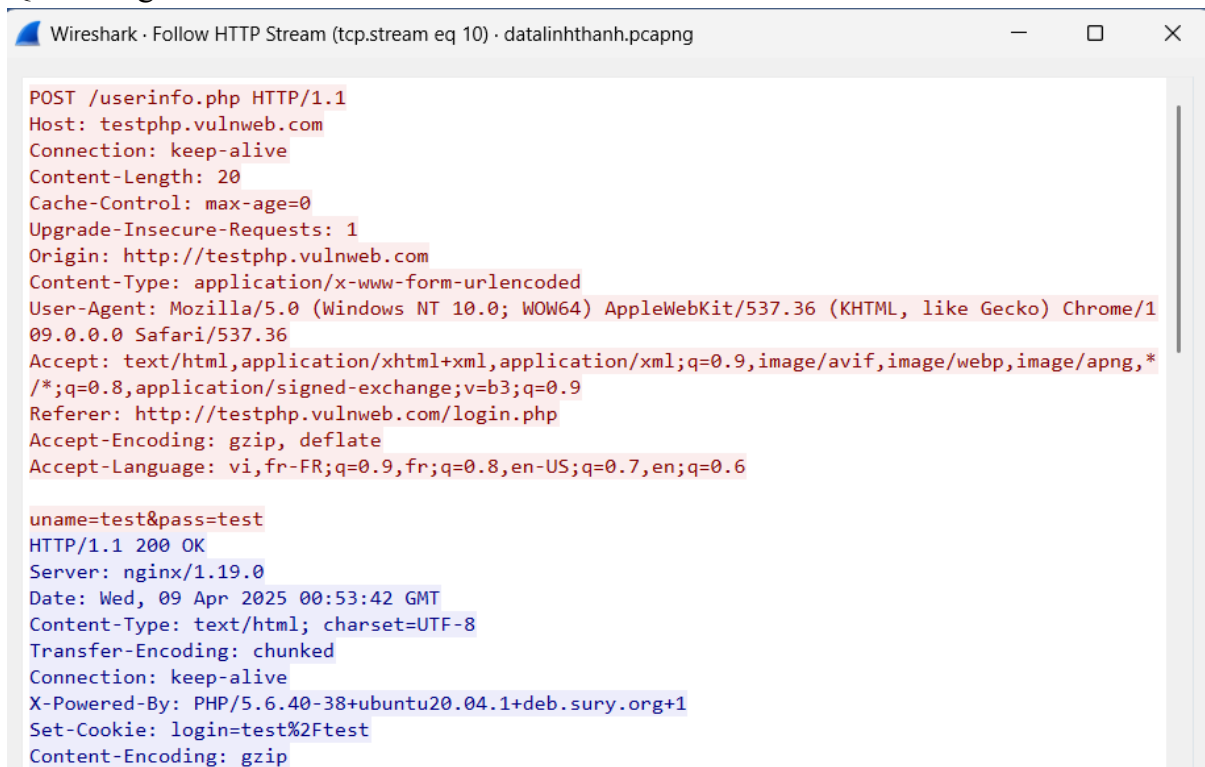
Bước 2: Lọc giao thức HTTP, truy cập một trang login, quan sát gói gửi dữ liệu.

Trang sử dụng : <http://testphp.vulnweb.com/userinfo.php>



No.	Source	Time	Destination	Protocol	Length	Info
222	172.31.35.27	3.973093	44.228.249.3	HTTP	724	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
239	44.228.249.3	4.182941	172.31.35.27	HTTP	70	HTTP/1.1 200 OK (text/html)

Quan sát gói POST:



- POST /userinfo.php HTTP/1.1
- Dữ liệu gửi: `uname=test&pass=test`

Bước 3: Lưu file kết quả bắt gói (.pcapng).

Lưu file với tên `datalinhthanh.pcapng`

Bước 4: Mở lại file đã lưu, phân tích theo từng lớp trong mô hình OSI.

Wireshark · Follow HTTP Stream (tcp.stream eq 10) · datalinhthanh.pcapng

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Connection: keep-alive
Content-Length: 20
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: vi,fr-FR;q=0.9,fr;q=0.8,en-US;q=0.7,en;q=0.6

uname=test&pass=test
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Wed, 09 Apr 2025 00:53:42 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Set-Cookie: login=test%2Ftest
Content-Encoding: gzip
```

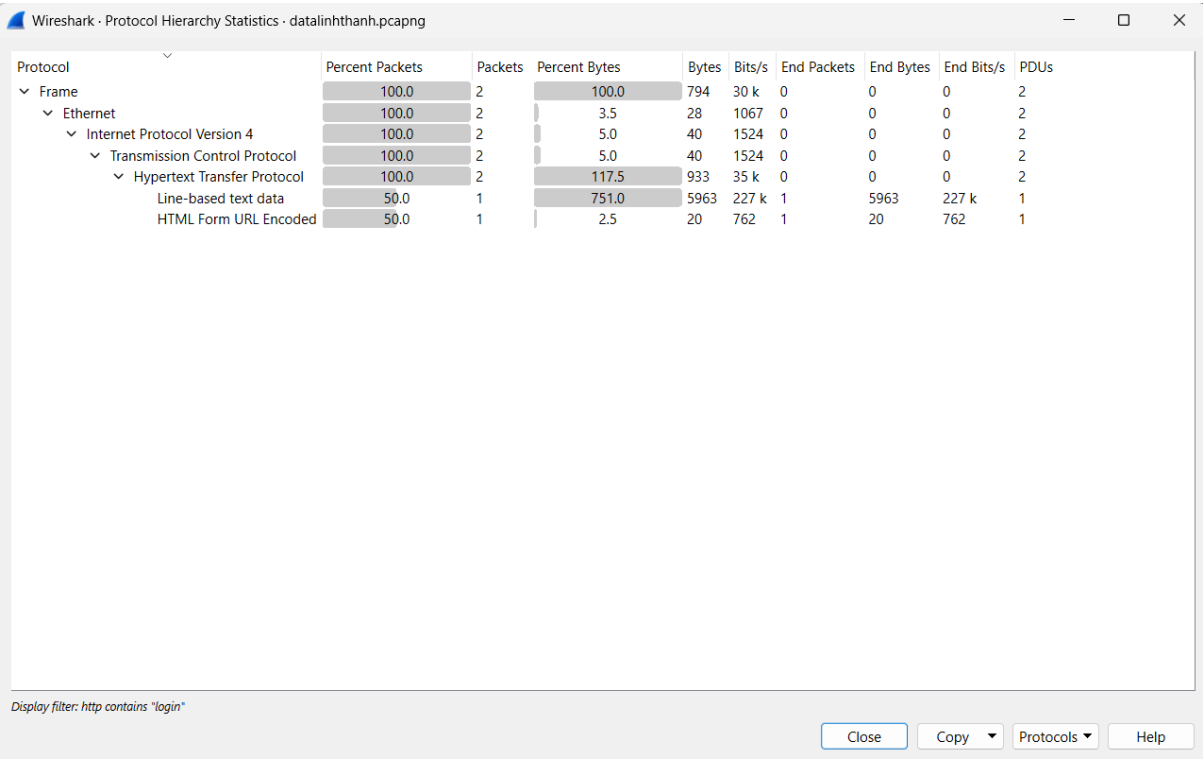
Tầng	Mô tả	Dữ liệu chính
1. Physical	Truyền tín hiệu vật lý	Cáp/Wi-Fi (không hiển thị)
2. Data Link	Frame Ethernet, địa chỉ MAC	MAC nguồn/đích (giả định)
3. Network	Gói IP, định tuyến	IP nguồn/đích (giả định)
4. Transport	TCP, truyền dữ liệu	Cổng 80, Connection: keep-alive
5. Session	Quản lý phiên	Cookie: login=test%2Ftest
6. Presentation	Định dạng, nén dữ liệu	Gzip, UTF-8, URL-encoded
7. Application	Giao thức HTTP	POST uname=test&pass=test, HTML trả về

Mô tả chi tiết lớp 7: Application (HTTP):

- Phương thức: POST
- URL: /userinfo.php
- Host: testphp.vulnweb.com
- Headers: gồm User-Agent, Content-Type, Referer, v.v.
- Body: uname=test&pass=test → dữ liệu đăng nhập
- Response: HTTP/1.1 200 OK, có Set-Cookie: login=test/test, nội dung trả về HTML

Bước 5: Sử dụng tính năng Protocol Hierarchy hoặc Follow TCP Stream để quan sát toàn cục.

Protocol Hierarchy



Giao thức	Số gói	Tỷ lệ gói (%)	Bytes	Tỷ lệ Bytes (%)	Ghi chú
Frame	2	100.0	794	100.0	Tổng số frame trong file.
Ethernet	2	100.0	794	100.0	Tầng 2: Frame Ethernet chứa gói IP.
IPv4	2	100.0	754	94.5	Tầng 3: Gói IP, 40 bytes header.
TCP	2	100.0	714	89.9	Tầng 4: TCP, 40 bytes header.
HTTP	2	100.0	674	84.9	Tầng 7: HTTP request và response.
- Line-based text data	1	50.0	5963	751.0	HTML phản hồi (nén gzip).
- HTML Form URL Encoded	1	50.0	20	2.5	Yêu cầu POST (uname=test&pass=test).

Phân tích:

- Tổng quan: Chỉ có 2 gói tin, 1 yêu cầu POST (uname=test&pass=test) và 1 phản hồi HTML (nén gzip).
- HTTP: Chiếm 84.9% dữ liệu, gồm 674 bytes (header HTTP + dữ liệu).

- HTML Form URL Encoded: 20 bytes, đúng với `uname=test&pass=test`.
- Line-based text data: 5963 bytes, phản hồi HTML nén gzip, lớn hơn thực tế do Wireshark giải nén.

Follow TCP Stream

Wireshark - Follow TCP Stream (tcp.stream eq 10) · datalinhthanh.pcapng

```

POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Connection: keep-alive
Content-Length: 20
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: vi,fr-FR;q=0.9,fr;q=0.8,en-US;q=0.7,en;q=0.6

uname=test&pass=test
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Wed, 09 Apr 2025 00:53:42 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Set-Cookie: login=test%2Ftest
Content-Encoding: gzip

a41
.....Xks.6..l.
.;[.3.(..$.6~d...xk.i?y .....%....=. )Z...t.....s.....Og7.^].w7....0....X.F....(:.9.....
h^i.*x.E...^Y[.h.Z.W.)....Qf..a.+eD?.i0.M..t.M.....H.....Y.(snE.D7..&ZpY..../dr....+./..2`.J
.....
R...T..H....F.,..@.S.,.....J...L.V.6.Y.X..Q.X.`..',..6.....}.E*--AO...Z@...6..z^..
...2B3Y..I.?<x.Q.<....{.E....sa2!l.2-../...Y\.....W6n.z=.0B....#.Z.....i....&....,....s..
.._k.....^..]U$.N...[.U..
..d!>..cQ...f3.V.H...;../.a.#...i....'....>....|)..*
Q.b...GrU.|..$......{%.}ai.gX.....>.A6c.c.P....eQ..Y.6;..{... 9.. S.W1~t.....+....
..o.....#d0.%n...g.J8.....=g..^9GF.Y..Q."3....7I..Id.e.%_..0.zqP*...c>3*..8..q....|8a.
...x..).6b.....dC'...9!.N....);M.!<.
a.C?Q..k.b..N.@.....2W.....qp08FV8.c.*`3...q0...m...%.....!...?.N.d..q..{$j0....a.H..X(..
v fN ..... r d C v k f "v OT \ x F x : v ^ 4 T3v ^ o i BR K

```

1 client pkt, 3 server pkts, 1 turn.

Entire conversation (3590 bytes) Show as ASCII No delta times Stream 10

Find: ☐ Case sensitive

Follow TCP Stream hiển thị luồng TCP đầy đủ:

- Yêu cầu POST gửi thông tin đăng nhập (`uname=test&pass=test`) tới `/userinfo.php`.
- Phản hồi trả về mã 200 OK, kèm nội dung HTML (nén gzip) chứa thông tin người dùng và cookie phiên (`login=test%2Ftest`).

Bước 6: Viết mã Python dùng thư viện PyShark để truy xuất thông tin tầng 2 và tầng 3 từ file .pcapng.

```
import pyshark

# Đường dẫn đến file .pcapng
file_path = "datalinhthanh.pcapng"

# Đọc file .pcapng
capture = pyshark.FileCapture(file_path)

# Biến đếm để giới hạn 10 gói tin đầu tiên
count = 0
max_packets = 10

# Duyệt qua từng gói tin
for packet in capture:
    if count >= max_packets:
        break # Thoát sau khi xử lý 10 gói tin

    try:
        # Tầng 2: Ethernet (Data Link)
        if "eth" in packet:
            eth_src = packet.eth.src # Địa chỉ MAC nguồn
            eth_dst = packet.eth.dst # Địa chỉ MAC đích
            print(f"Packet {packet.number}:")
            print(f"  Tầng 2 - Ethernet:")
            print(f"    MAC Nguồn: {eth_src}")
            print(f"    MAC Đích: {eth_dst}")

            # Tầng 3: IP (Network)
            if "ip" in packet:
                ip_src = packet.ip.src # Địa chỉ IP nguồn
                ip_dst = packet.ip.dst # Địa chỉ IP đích
                print(f"  Tầng 3 - IP:")
                print(f"    IP Nguồn: {ip_src}")
                print(f"    IP Đích: {ip_dst}")
                print("-" * 50)

            count += 1 # Tăng biến đếm

    except AttributeError:
        # Bỏ qua nếu gói tin không có thông tin tầng 2 hoặc 3
        continue

# Đóng file capture
capture.close()
```

Kết quả chạy code:

Packet 1:

Tầng 2 - Ethernet:

MAC Nguồn: 52:2d:60:4c:f4:52

MAC Đích: cc:47:40:70:7c:c0

Tầng 3 - IP:

IP Nguồn: 172.31.35.18

IP Đích: 224.0.0.251

Packet 2:

Tầng 2 - Ethernet:

MAC Nguồn: b2:ee:b5:b3:14:d1

MAC Đích: cc:47:40:70:7c:c0

Tầng 3 - IP:

IP Nguồn: 172.31.33.205

IP Đích: 224.0.0.251

Packet 3:

Tầng 2 - Ethernet:

MAC Nguồn: d6:03:27:31:e7:06

MAC Đích: cc:47:40:70:7c:c0

Tầng 3 - IP:

IP Nguồn: 172.31.34.164

IP Đích: 224.0.0.251

Packet 4:

Tầng 2 - Ethernet:

MAC Nguồn: cc:47:40:70:7c:c0

MAC Đích: ec:c0:18:b7:18:5d

Tầng 3 - IP:

IP Nguồn: 172.31.35.27

IP Đích: 20.167.82.225

Packet 5:

Tầng 2 - Ethernet:

MAC Nguồn: 02:5b:30:4d:60:f6

MAC Đích: cc:47:40:70:7c:c0

Tầng 3 - IP:

IP Nguồn: 172.31.34.47

IP Đích: 224.0.0.251

Packet 6:

Tầng 2 - Ethernet:

MAC Nguồn: 66:ea:6a:f7:80:a7

MAC Đích: ff:ff:ff:ff:ff:ff

Packet 7:

Tầng 2 - Ethernet:

MAC Nguồn: 66:ea:6a:f7:80:a7

MAC Đích: ff:ff:ff:ff:ff:ff

Packet 8:

Tầng 2 - Ethernet:

MAC Nguồn: 66:ea:6a:f7:80:a7

MAC Đích: ff:ff:ff:ff:ff:ff

Packet 9:

Tầng 2 - Ethernet:

MAC Nguồn: 6e:cf:f9:40:74:8e

MAC Đích: cc:47:40:70:7c:c0

Tầng 3 - IP:

IP Nguồn: 172.31.35.147

IP Đích: 224.0.0.251

Packet 10:

Tầng 2 - Ethernet:

MAC Nguồn: 12:1a:5a:82:ae:52

MAC Đích: ff:ff:ff:ff:ff:ff