***Forensics***

*Liberate - 50pts*

* Bài 50 điểm -> thử các cách đơn giản trước -> bật terminal trong linux lên và dùng lệnh strings với file ảnh 30\_4.jpg để tìm kiếm các chuỗi có thể đọc được trong file ảnh: strings “30\_4.jpg”. Trong các kết quả xuất ra màn hình, có một dòng đáng chú ý đến là: CI think it should be flag 84-\*O;\_:@97XK8VARo.6;aX,J3&P&SDI[TqATE2
* Từ dòng trên, có thể đoán trong đống lộn xộn ở cuối dòng sẽ là flag -> tuy nhiên, từ đề bài, cũng như trong đoạn trên, hay trong file ảnh không tìm được thêm manh mối về chuyện giải mã đống mã hóa đó -> thử coi trong đó có gì có thể dùng được.
* Trong một đống lộn xộn đó, chúng ta thấy 84 ngăn cách với cácc kí tự ở sau bằng dấu gạch nối -> có thể đây là manh mối giải mã -> search 84 decode -> thấy kiểu mã hóa base 85 -> thử decode với kiểu mã hóa base 85 -> ra flag.
* **Flag:** HCMUS-CTF{uSed\_ASCII85\_encoder}

*Worker’s Day - 50pts*

* Tìm kiếm bằng strings không thấy có đoạn mã hóa nào có thể khai thác, ngoài một đoạn nghi vấn là 2 dòng đầu, với các kí tự được sắp xếp liền nhau như một bảng tra. -> Có thể đã dùng công cụ để che dấu thông tin -> tìm kiếm một số côgn cụ steganography phổ biến -> steghide.
* Sử dụng steghide đối với hình ảnh iwd\_e.jpg theo lệnh: steghide extract -sf iwd\_e.jpg

Vì đề không cung cấp password -> thử bỏ trống password -> trên màn hình console xuất ra là dữ liệu đã được trích xuất ra tập tin flag.txt. -> mở tập tin flag.txt là có flag.

* **Flag:** HCMUS-CTF{simply\_use\_steghide\_to\_hiding\_something}

*AtLeast - 50pts*

* Sử dụng strings tìm được đoạn nghi vấn -> sử dụng steghide không được vì không phải là jpg -> tìm kiếm một phần mềm khác để giải các ảnh png -> tìm được stegsolve, một công cụ chứa nhiều cách phân tích một ảnh png để trích xuất thông tin.
* Stegsolve là một công cụ được viết bằng java -> khởi động qua file .jar bằng câu lệnh: java -jar ./stegsolve.jar. -> cửa sổ hiện lên, chọn file -> open -> chọn hình ảnh cần mở.
* Sau khi hình ảnh mở lên, nhấn nút mũi tên tiến tới (nút > ) để đi qua các lớp ảnh có thể phân tích từ ảnh gốc -> trong lớp ảnh Red Plane 0, tất cả đều màu đen, tuy nhiên, nếu để ý kĩ thì trên góc trên, bên trái có một số đốm trắng xếp thành hàng. -> bất thường, Green Plane 0 và Blue Plane 0 cũng có tình trạng tương tự như vậy.
* Trích xuất thông tin bằng cách vào Analyse -> Data Extract -> chọn xuất từ bit 0 của Red, Green, Blue -> thấy được một đoạn text, trong đó có flag.
* **Flag:** HCMUS-CTF{there\_is\_somthing\_I\_wanna\_hide}

*InsideMe - 100pts*

* Đây là một file ảnh về yoda, thử dùng các phần mềm zsteg để coi có thông điệp gì mã hóa không -> không tìm thấy, thử dùng steghide, duyệt qua các bit ở vị trí thấp, vì hình ảnh yoda có vẻ không bị nhiễu nhiều -> không tìm thấy gì có thể dẫn đến flag -> có thể trong tập tin đang ẩn chứa một tập tin khác.
* Mở một trình hex editor (cóc thể dùng online tại: hexed.it) và import file ảnh vào. Qua xem xét một số file ảnh png thì có thể biết file ảnh sẽ luôn kết thúc với 2 giá trị FF D9. Tìm trong file ảnh có thể thấy giá trị này xuất hiện 2 lần, tại lần xuất hiện thứ nhất thì đi ngay sau đó sẽ là RAR -> rất có thể bắt đầu một file nén RAR mới. -> chọn các byte từ vị trí RAR đó đến cuối file và xuất ra một file mới với tên là nen.rar -> dùng WinRAR để giải nén file trên, ta được thư mục Content với 2 file là secret.rtf và light.pdf.
* Dùng notepad hoặc các trình đọc text cấp thấp thì chúng ta không thấy được secret.rtf có thông tin gì thú vị -> dùng trình đọc pdf thì không mở được file light.pdf -> bỏ file light.pdf vào hex editor -> thấy nhiều điểm giống như là file ảnh như JFIF, GIMP, ... -> thử tìm magic number của file -> đây là file ảnh jpeg -> đổi đuôi thành file ảnh jpg mà mở lên -> được flag.
* **Flag:** HCMUS-CTF{1t\_is\_a\_s1mpl3\_BinWalk}

*Unknown - 100pts*

* Tập tin được nhận là một tập tin nhị phân. Không có thông tin về loại tập tin, thử dùng lệnh file của Ubuntu để tìm hiểu thông tin về file cũng không nhận được thông tin của file -> không có cách để đọc file.
* Xem mô tả đề bài, tập tin này đã bị hư -> cần tìm cách sửa. Lệnh file sử dụng magic number của tập tin để biết chính xác cách tổ chức của nội dung bên trong tập tin, mà lệnh file không trả ra được loại tập tin -> có thể magic number đã bị hư -> bật hexed.it để xem nội dung tập tin -> thấy PNG ở đầu tập tin -> xem magic number của file PNG bình thường -> sửa lại magic number của tập tin unknown -> được một file ảnh -> nội dung file ảnh có cờ.
* **Flag:** HCMUS-CTF{l0l\_CMU\_da\_b3s}

*Galaxy - 100pts*

* Được cho một đoạn âm thanh, 3 phút -> nghe thử -> đây là một bài nhạc bắt tai, nhưng có một đoạn khoảng 5-10 giây bất thường, gây khó chịu cho người nghe -> thử dùng phần mềm để phân tích spectrum -> tua đến đoạn bất thường -> thấy spectrum của âm thanh tạo thành một dãy các ký tự đọc được: HCMUS-CTF...
* **Flag:** HCMUS-CTF{sound\_likes\_Outer\_Space}

*Qemu - 150pts*

* Theo như đề cho, chúng ta nhận được một file có đuôi là qcow2. Và theo như mô tả của đề bài cũng như google search thì đây là file lưu trữ của máy ảo chạy bằng Qemu. Tuy nhiên, trên máy của người chơi đã có sẵn máy ảo Oracle VirtualBox, và tài nguyên của máy thì có hạn -> việc cài đặt và sử dụng máy ảo Qemu có thể sẽ khá lâu.
* Tải về phần mềm qemu và cài đặt bằng cách Next, next, install -> cài đặt xong, sử dụng qemu và bỏ file qcow2 vào chạy -> ó nhiều file qemu với nhiều cấu hình khác nhau -> dùng thử qemu x86-64 để chạy file qcow2 đề cho -> không boot được, qemu báo không tìm thấy bootable device -> có thể cài đặt sai -> sẽ cần thời gian để tìm hiểu nguyên nhân và cài đặt đúng -> có thể sẽ phải gỡ ra cài lại -> hơi lười :( .
* qcow2 là file lưu trữ của máy ảo, một hard drive ảo, phần mềm VirtualBox cũng có file tương tự vậy đó là file \*.vdi -> nếu có cách chuyển qcow2 sang vdi thì chúng ta có thể sử dụng VirtualBox để chạy máy ảo mà bài thi cho. -> tìm được cách chuyển bằng phần mềm qemu-img, đây là phần mềm đã được cài đặt chung với phần mềm Qemu -> sử dụng câu lệnh:

qemu-img convert -O vdi <<INPUT\_QCOW2\_FILE>> <<OUTPUT\_VDI\_FILE>>

* Chuyển đổi thành công, người chơi nhận được file vdi -> bật Oracle VirtualBox, vào mục Machine -> New… hoặc nhấn nút New -> type: Linux, Version: Ubuntu 64bit. -> chọn Use an existing virtual hard drive -> chọn file vdi vừa được chuyển đổi -> Create.
* Chạy máy ảo lên, chúng ta thấy cần phải có mật khẩu để đăng nhập -> đọc lại đề bài thì chúng ta hiểu rằng mật khẩu ở đâu đó trên màn hình máy ảo -> thử mật khẩu giống tên người dùng -> đã truy cập được vào máy ảo -> cờ có thể được lưu trong máy ảo, cần phải tìm kiếm trong máy ảo -> bật phần mềm duyệt file -> đầu tiên là thử vào folder người dùng hcmus-ctf -> trong các thư mục có thư mục Secret rất khêu gợi -> thử vào Secret, tìm thấy tập tin Secret -> mở tập tin Secret -> đã tìm được cờ.
* **Flag:** HCMUS-CTF{just\_try\_to\_teach\_you\_learn\_qemu}

*Crime - 150pts*

* Tập tin nhận được có đuôi là 001, tức là có thể đây là một tập tin lưu trữ, đọc magic number của tập tin ta thấy chuỗi NTFS -> rất có thể đây là file dump của một ổ đĩa được lưu trữ -> Sử dụng một phần mềm (OSFMount) để mount giả lập tập tin lưu trữ trên thành một ổ đĩa của máy tình -> nhận được một ổ đĩa chứa các tập tin.
* Ta có 3 tập tin, 1 tập tin zip được bảo vệ bằng mật khẩu -> không biết mật khẩu để unzip -> 2 tập tin còn lại là 2 file ảnh, 1 file có các kí tự khó hiểu, 1 file là ảnh của một tên tội phạm Zodiac Killer -> thử search về Zodiac Killer, ta biết được một loại cipher có liên quan đến một tên tội phạm -> dùng dcode.fr để giải mã các kí tự trong file language.png ta được: FITPASS, có thể đây là mật khẩu để unzip -> thử unzip, ta được file flag.txt.
* **Flag:** HCMUS-CTF{social\_distancing\_for\_this\_pandamic}

*Actual\_At\_Least - 150pts*

* Nhận được một tập tin ảnh png -> quét strings, zsteg không tìm ra được thông tin hữu ích -> nhìn vào mô tả của đề bài, có đề cập đến Red và Row -> có thể sẽ phải cần dùng đến stegsolve để trích xuất thông tin từ các bit.
* Dùng lệnh: java -jar ./stegsolve.jar để chạy công cụ stegsolve lên, coi sơ qua một lượt các plane, chúng ta không tìm thấy được plane có vẻ bị sai -> thử vào Analyse và chọn data extract để trích ra một số bit thông dụng như bit 0 ở các kênh RGB -> không tìm thấy -> nhớ lại đề bài là Red và Row -> nhìn kĩ ở những plane Red -> thấy một hàng bất thường tại Red Plane 7 -> có thể thông tin chỉ bị che dấu bằng cách sử dụng bit số 7 của các bit red. -> có được cờ
* **Flag:** HCMUS-CTF{You\_should\_learn\_LSB\_embeded\_system}

***Crypto***

Dot and Underscore - 50pts

* Nhìn đoạn cipher thì có thể thấy 2 kí tự để mã hóa là chấm và gạch. Các kí tự nối kiền nhau tạo thành khối, cách nhau bởi dấu cách. Bài 50 điểm -> các loại mã hóa phổ biến như nhị phân, morse code,... -> có một số khối độ dài ngắn -> không thể là nhị phân -> thử morse code -> ra: NOODTOLEARNMORSECODE.
* **Flag:** HCMUS-CTF{NOODTOLEARNMORSECODE}