BÁO CÁO BÀI TẬP

**Môn học:** Pháp chứng kĩ thuật số

**Tên chủ đề: Bài tập Queen of Stegano**

*GVHD: Nghi Hoàng Khoa*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT334.O21.ANTN

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Hà Thị Thu Hiền | 21522056 | 21522056@gm.uit.edu.vn |
| 2 | Phạm Ngọc Thơ | 21522641 | 21522641@gm.uit.edu.vn |
| 3 | Nguyễn Ngọc Nhung | 21521248 | 21521248@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | Câu 1 | 100% |

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

BÁO CÁO CHI TIẾT

1. **Câu 1:** **Queen of Stegano**

**Descriptions:**

**- My picture is corrupted**

**- My zip file lost password**

**- So sad :((**

**Format flag: W1{...}**

**A black background with white numbers

Description automatically generated**

* Ta có tài nguyên là 1 file zip và 1 ảnh dạng png, nhưng để chắc chắn ta thử xem file ảnh có thật sự được coi là png hay không.

**A screen shot of a computer

Description automatically generated**

* Điều này có nghĩa là lệnh file không nhận dạng được định dạng cụ thể của tệp Chall.png, và chỉ trả về "data". Thông thường, một tệp PNG sẽ được nhận dạng là image/png, nhưng trong trường hợp này, có thể tệp Chall.png không thực sự là một tệp hình ảnh hợp lệ hoặc bị hỏng.
* Bây giờ, ta sẽ kiểm tra trực tiếp nội dung nhị phân của tệp, bằng cách thực hiện lệnh **xxd Chall.png | head -n 20** dùng để hiển thị 20 dòng đầu tiên của tệp Chall.png dưới dạng hexdump.

A screenshot of a computer screen

Description automatically generated

* Thông thường, signature của tệp PNG chuẩn bao gồm 8 byte đầu tiên:

**89 50 4E 47 0D 0A 1A 0A**

* Nhưng theo kết quả trên thì chưa khớp với định dạng chuẩn của PNG.

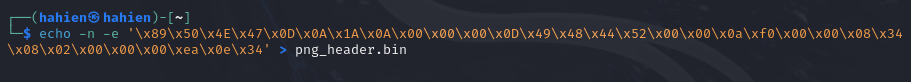
PNG là một định dạng tệp hình ảnh có cấu trúc cụ thể. Mỗi tệp PNG bao gồm các chunk (khối dữ liệu) bắt buộc, như IHDR (Image Header), IDAT (Image Data), và IEND (Image End). Dưới đây là cấu trúc cơ bản:

* Signature: 8 byte
* IHDR chunk: Mô tả thông tin cơ bản về hình ảnh (chiều rộng, chiều cao, độ sâu màu, v.v.)
* IDAT chunk: Chứa dữ liệu hình ảnh nén
* IEND chunk: Đánh dấu kết thúc tệp PNG

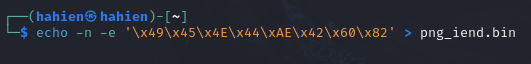
Trong đầu ra từ xxd, chunk IDAT bắt đầu từ byte thứ 16:

**00000010: 8400 0100 0049 4441 5478 9cec fd5d 97e4 .....IDATx...]..**

* Thiếu chunk IHDR và IEND.
* Bây giờ ta sẽ thêm signature và chunk cần thiết, ta thêm signature của file png là 89 50 4E 47 0D 0A 1A 0A, thấy rằng nó cũng thiếu một chunk quan trọng là IHDR, ta thêm 00 00 00 0D 49 48 44 52, và phần ở byte 0 đến chunk IDAT sẽ thuộc chunk IHDR. Và cuối cùng là thêm IEND là 49 45 4E 44 AE 42 60 82.
* Đầu tiên, tạo các file chứa signature, chunk IHDR, và chunk IEND.
  + Tạo file chứa signature và IHDR.



* + Tạo file chứa IEND.



* Tạo file tạm chứa phần IDAT hiện tại.

A computer screen shot of a computer code

Description automatically generated

* Kết hợp các file thành một tệp PNG hợp lệ.

A close up of a computer screen

Description automatically generated

* Thử lại với xxd xem kết quả.

**A screenshot of a computer screen

Description automatically generated**

**A close up of numbers

Description automatically generated**

* Kiểm tra lại với pngcheck và không có lỗi.

A close up of a computer screen

Description automatically generated

A screenshot of a computer game

Description automatically generated

* Sau một lúc thực hiện kiểm tra với các tool steganography và không có kết quả, và trong bức ảnh là con appa, chúng ta thử với tool appa, decode và có được phần đầu của flag: **W1-Y0u-4r3**.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generatedA screenshot of a computer program

Description automatically generated

* Tiến đến, xem thử file zip.

A screenshot of a computer

Description automatically generated

* Vì không giải nén được, nên em sử dụng lệnh **unzip -lv** để hiển thị thông tin chi tiết về các tệp trong một tệp nén (tệp zip) mà không cần giải nén chúng.

A screenshot of a computer

Description automatically generated

* Ở đây, ta thấy trong đây có file Chall.png và flag.txt, rất có thể đây là file Chall.png trước khi bị chỉnh sửa, từ đây có thể thực hiện crack file zip nhờ vào kỹ thuật plaintext-known.
* Kỹ thuật "plaintext-known" (hoặc "known-plaintext attack") là một phương pháp tấn công mật mã học trong đó kẻ tấn công có quyền truy cập vào cả văn bản gốc (plaintext) và văn bản mã hóa (ciphertext) của một hoặc nhiều thông điệp. Bằng cách sử dụng thông tin này, kẻ tấn công có thể cố gắng khám phá khóa mã hóa hoặc thu thập thêm thông tin để giải mã các thông điệp khác mã hóa bằng cùng một khóa.
* Đầu tiên, tạo 1 tệp zip mới chứa Fixed\_chall.png như sau:

A computer code with text

Description automatically generated

* **Tiếp theo,** **kiểm tra giá trị CRC của các tệp**:
  + Kiểm tra thông tin chi tiết của tệp Chall.png trong tệp zip ban đầu (CrackMe.zip) và so sánh giá trị CRC với tệp Fixed\_chall.png trong tệp zip mới (Fixed\_chall.zip).
  + Giá trị CRC là một giá trị kiểm tra (checksum) được sử dụng để xác minh tính toàn vẹn của dữ liệu. Nó đảm bảo rằng nội dung của hai tệp là giống nhau.

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

* Trong hình ảnh, chúng ta có thể thấy rằng giá trị CRC của cả hai tệp là AB6A1C78, điều này xác nhận rằng nội dung của Fixed\_chall.png và Chall.png là giống nhau.
* **Tiếp theo, sử dụng pkcrack:**
* Công cụ pkcrack có thể được sử dụng để thực hiện tấn công plaintext-known như sau:
  + Sử dụng tệp zip chứa plaintext đã biết (Fixed\_chall.zip với Fixed\_Chall.png).
  + Sử dụng tệp zip được mã hóa (CrackMe.zip với Chall.png và flag.txt).
  + Chạy pkcrack để tìm ra khóa mã hóa được sử dụng trong CrackMe.zip.

A screen shot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generatedA computer screen shot of a program

Description automatically generated

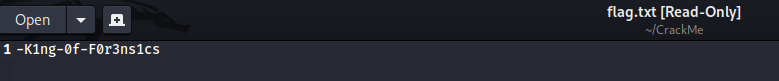
A screenshot of a computer

Description automatically generatedA computer screen shot of a number

Description automatically generated

A computer screen shot of a program

Description automatically generated



* ­Vậy nửa flag còn lại là: **-K1ng-0f-F0r3ns1cs**
* Kết luận, ta có **Flag: W1{Y0u-4r3-K1ng-0f-F0r3ns1cs}**

---

***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 bố).

*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, trễ, … sẽ được xử lý tùy mức độ vi phạm.*

**HẾT**

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-1)