BÁO CÁO THỰC HÀNH

**Môn học: Pháp chứng kỹ thuật số**

**Lab 6: CTF challenges cuối kỳ**

*GVHD: Đoàn Minh Trung*

1. **THÔNG TIN CHUNG:**

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

Lớp: NT334.O21.ATTN

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

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

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | Kịch bản 1 | 100% |
| 2 | Kịch bản 2 (còn câu g) | 100% |
| 3 | Kịch bản 3 (đã hoàn thành trên lớp) | 100% |
| 4 | Kịch bản 4 | 100% |

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

BÁO CÁO CHI TIẾT

Description:

**1. Memory (Easy to Hard):**

* 1. *memory.dmp* - Có một command chứa thông báo lạ trong bash history, liệu bạn có thể khôi phục thông báo đó? Bạn phải xây dựng volatility và tìm profile.

Tham khảo: <https://illuad.fr/2020/11/26/writeup-dga-ctf-bwing.html>

* 1. *dump.raw* - Dường như đã có hành vi bất thường trên laptop của NHK, bạn có thể giúp chúng tôi điều tra:

+ Thu thập các file bất thường để ghép mảnh flag.

+ Liệu họ có để lại những dấu vết trên trình duyệt web?

+ Và hình như kẻ xâm nhập bằng một cách nào đó đã lấy được password laptop của NHK. Hãy tìm password đó.

* 1. *Tiktoor-Erawlam.raw* - A critical document has been encrypted for some reason. Know that he always uses the same password. As an incident investigator, can you investigate and recover the file?

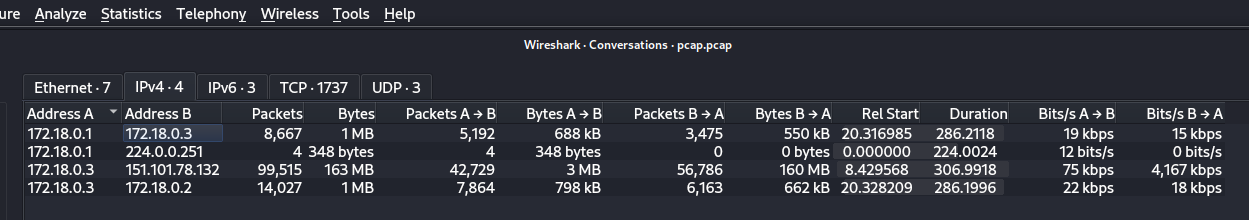
Format flag: flag{flag1-flag2-flag3)

**2. Network (Medium):**

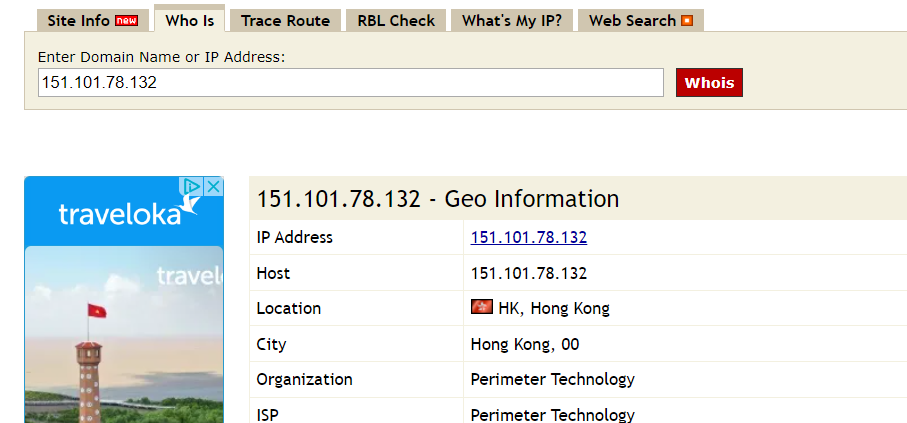
*pcap.pcap* - Vào lúc 3h sáng, trong khi tôi đang ngủ thì IDS của tôi cảnh báo rằng web server đang có cuộc tấn công, tôi nghe loáng thoáng mấy anh dev nói về việc “mù mờ” gì đó, nhưng họ không đủ năng lực để điều tra. Hãy giúp mấy anh dev nhà tôi nhé 😊

a. Tìm IP của web server.

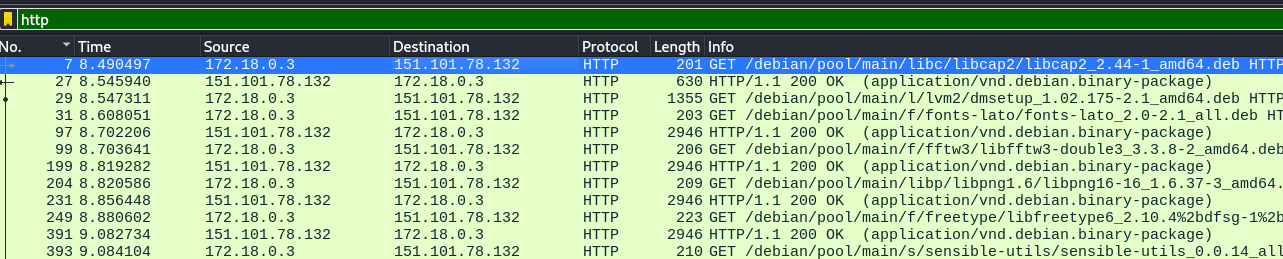
- Có 5 địa chỉ IP được tìm thấy:



- Trong đó, có IP 151.101.78.132 là ở HongKong:

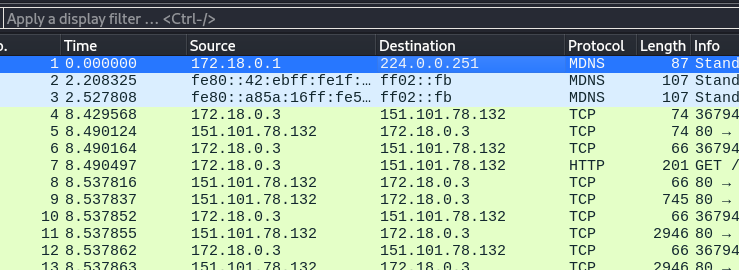


Quan sát IP này:



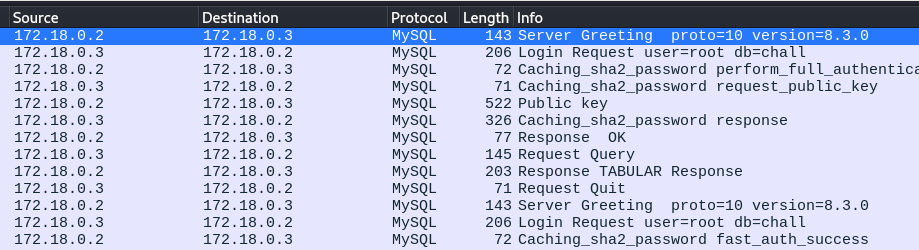
151.101.78.132 có hostname là deb.debian.org, 172.18.0.3 truy cập đến để GET các file với kích thước từ 23 – 113kB.

- Quan sát quá trình trao đổi gói tin:



224.0.0.251 sử dụng MDNS (multicast DNS) để trao đổi gói tin trong mạng nội bộ.

172.18.0.2 là Database vì sử dụng giao thức MySQL và 172.18.0.3 truy cập đến để lấy thông tin user:

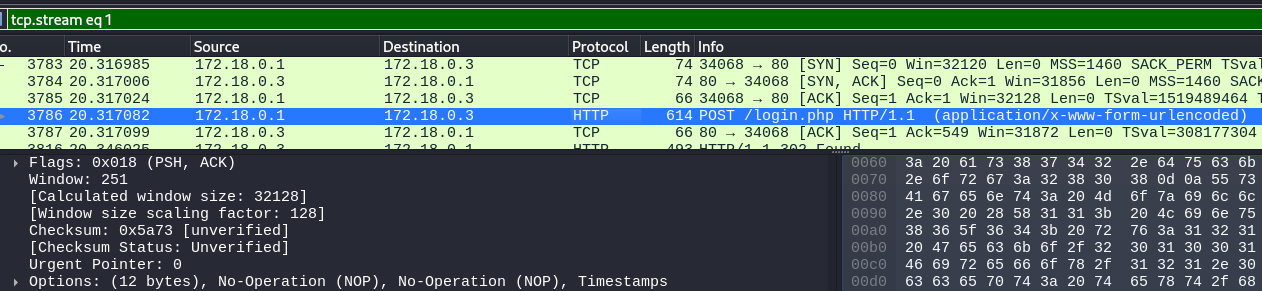


172.18.0.1 là IP của attacker.

Vậy 172.18.0.3 là IP của web server.

b. Tìm username và password của một tài khoản sử dụng server. Tôi nghe nói anh ta là một đặc vụ mật.

- Em tìm được gói tin dùng để truy cập đến *login.php*:



* Tìm được user và password là:

*username=agentp*

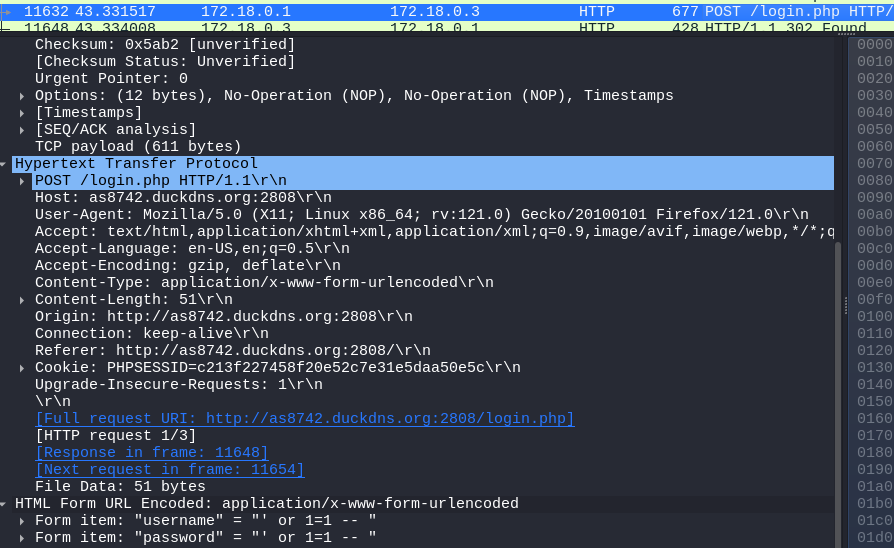
*password=perrytheplatypus*

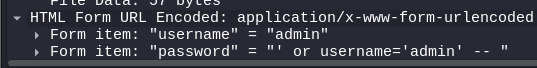
c. Hacker tấn công từ bên ngoài mạng hay là từ bên trong mạng.

Từ bên ngoài, thông qua gateway 172.18.0.1.

d. Lỗ hổng là hacker dùng để khai thác là gì?

SQL injection:





e. Hacker đã login vào tài khoản nào?

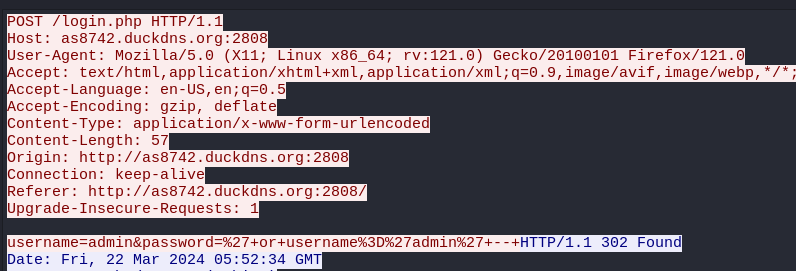
Admin.

f. Server mà hacker dùng để test là gì?

<http://as8742.duckdns.org:2808/>

g. Có vẻ là hacker đã lấy được mật khẩu của admin. Nhưng có người lại bảo là chưa. Vậy hacker đã lấy được mật khẩu của admin chưa? Mật khẩu của admin là gì? Hacker đã lấy được gì?

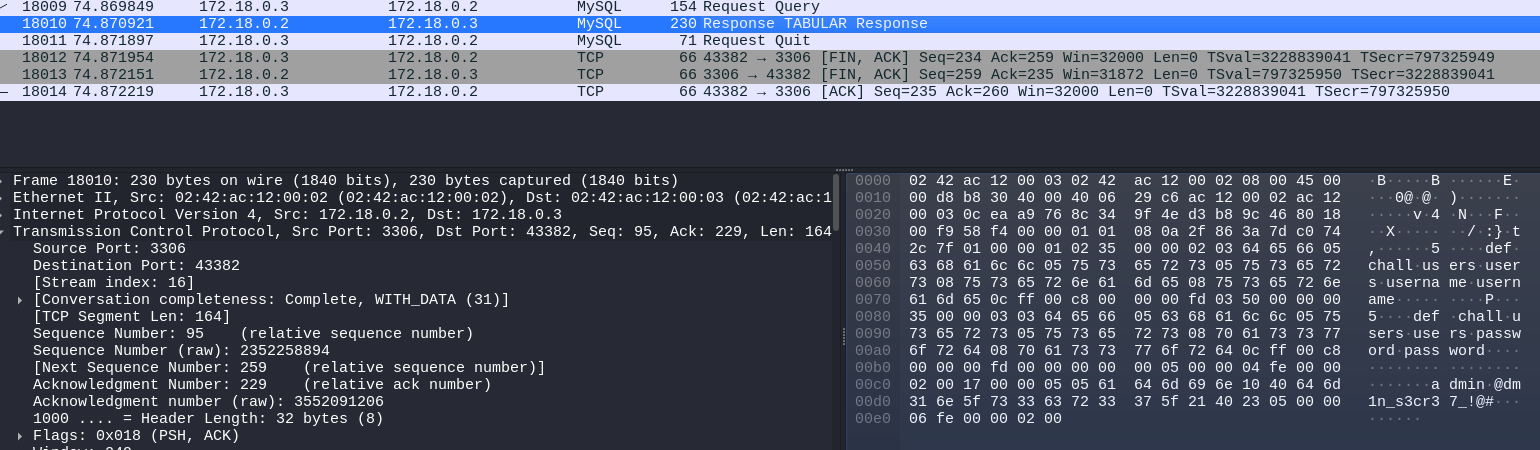
- Hacker chưa lấy được mật khẩu của admin:

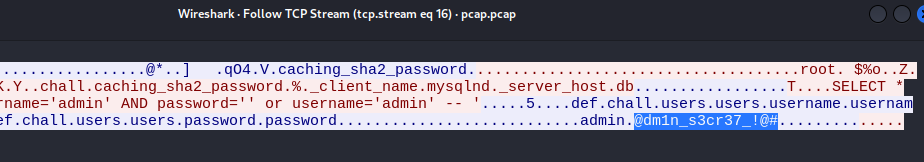


Đây là nội dung gói tin lấy được thông tin mật.

- Password: **@dm1n\_s3cr37\_!@#**

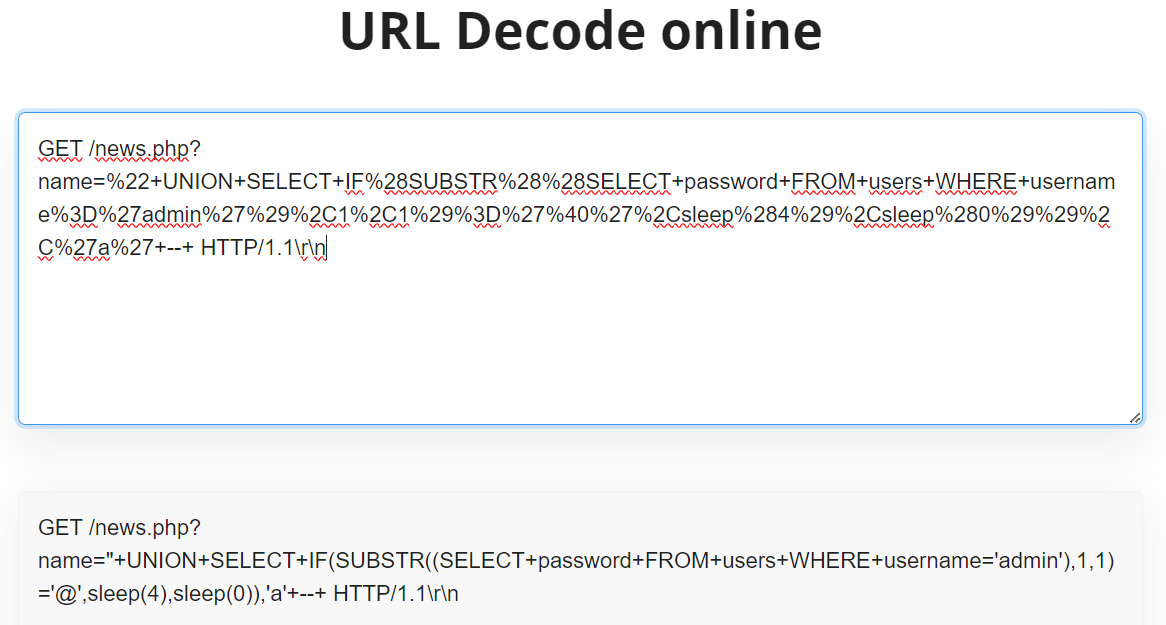
Tuy nhiên đây là gói tin do web server truy vấn đến database nên cuối cùng, attacker vẫn không dò được password:



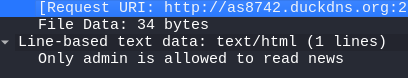


- j

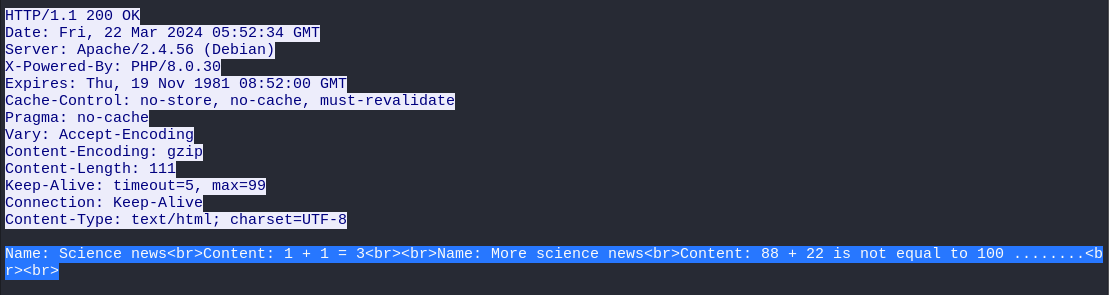
<https://www.urldecoder.io/>



- Ban đầu, khi chưa bypass được login, trang web được trả về sẽ hiển thị:

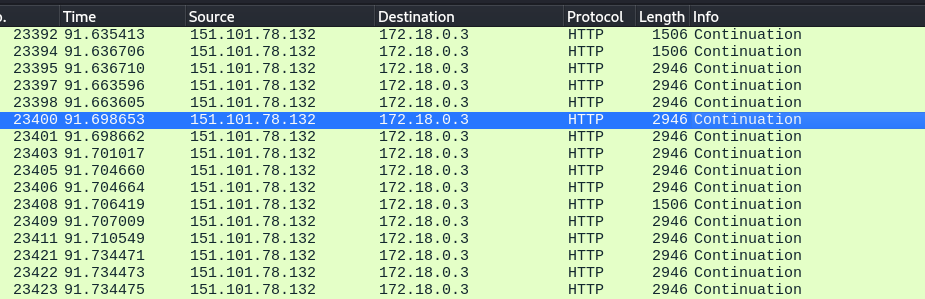


Nhưng sau khi bypass được, text tìm được là:



h. Có nên tình nghi đặc vụ đó là người đã thực hiện cuộc tấn công không? Tại sao?

- Có.

- Vì sau đó thì dường như trang web bị tấn công kểu floot: 

1. **Android (Easy):**

*bypass\_login.apk* - Như tên file, để tìm được flag hãy dịch ngược ứng dụng này và tìm cách bypass login. Đồng thời, cho biết dev đã mắc lỗi gì khi lập trình dẫn đến dễ dàng để lộ thông tin nhạy cảm như vậy. Đề xuất biện pháp khắc phục.

1. **Steganography (Maybe easy):**

*DecaoVsDatg.enc.png* - Hiện tại cộng đồng mạng chưa xác định được ai là võ sĩ mạnh nhất thời đại. Hãy tìm flag được giấu trong bức ảnh để xác định được ai là võ sĩ đấm đau nhất nhé :)) . Flag sẽ là một câu danh ngôn mà ai cũng biết…

Format flag: inseclab{...}

*Đáp án:*

---

***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)