BÁO CÁO BÀI TẬP

**Môn học: Lập trình an toàn và khai thác lỗ hổng phần mềm**

**Tên chủ đề: Exercise 5**

*GVHD: Phan Thế Duy*

* **THÔNG TIN CHUNG:**

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

Lớp: ANTN2020

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Nguyễn Bùi Kim Ngân | 20520648 | 20520648@gm.uit.edu.vn |
| 2 | Nguyễn Bình Thục Trâm | 20520815 | 20520815@gm.uit.edu.vn |
| 3 | Võ Anh Kiệt | 20520605 | 20520605@gm.uit.edu.vn |

* **NỘI DUNG THỰC HIỆN:[[1]](#footnote-2)**

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | Yêu cầu a | 100% |
| 2 | Yêu cầu b | 100% |

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

BÁO CÁO CHI TIẾT

**Cấu hình máy**

+ Kali Linux 2022.3

+ 8GB Ram

+ 80GB HDD

+ 2 core 2 thread CPU intel core i5-8250U

**Cài đặt**

Đầu tiên ta sẽ cài đặt bộ công cụ fuzzing bằng lệnh:

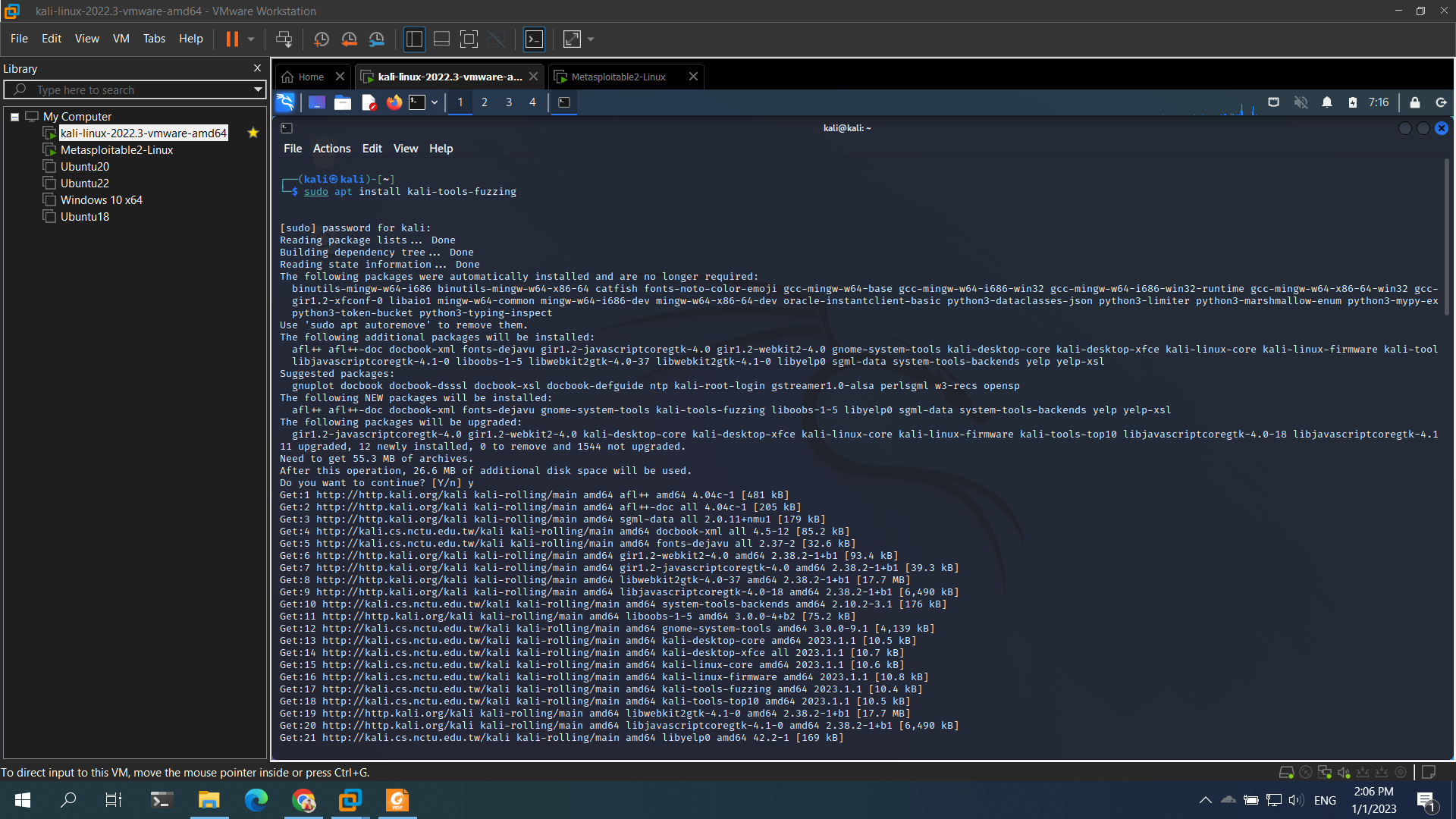
sudo apt install kali-tools-fuzzing

Bộ công cụ sẽ bao gồm công cụ

+ AFL++

+ sfuzz

+ wfuzz



**Yêu cầu A**

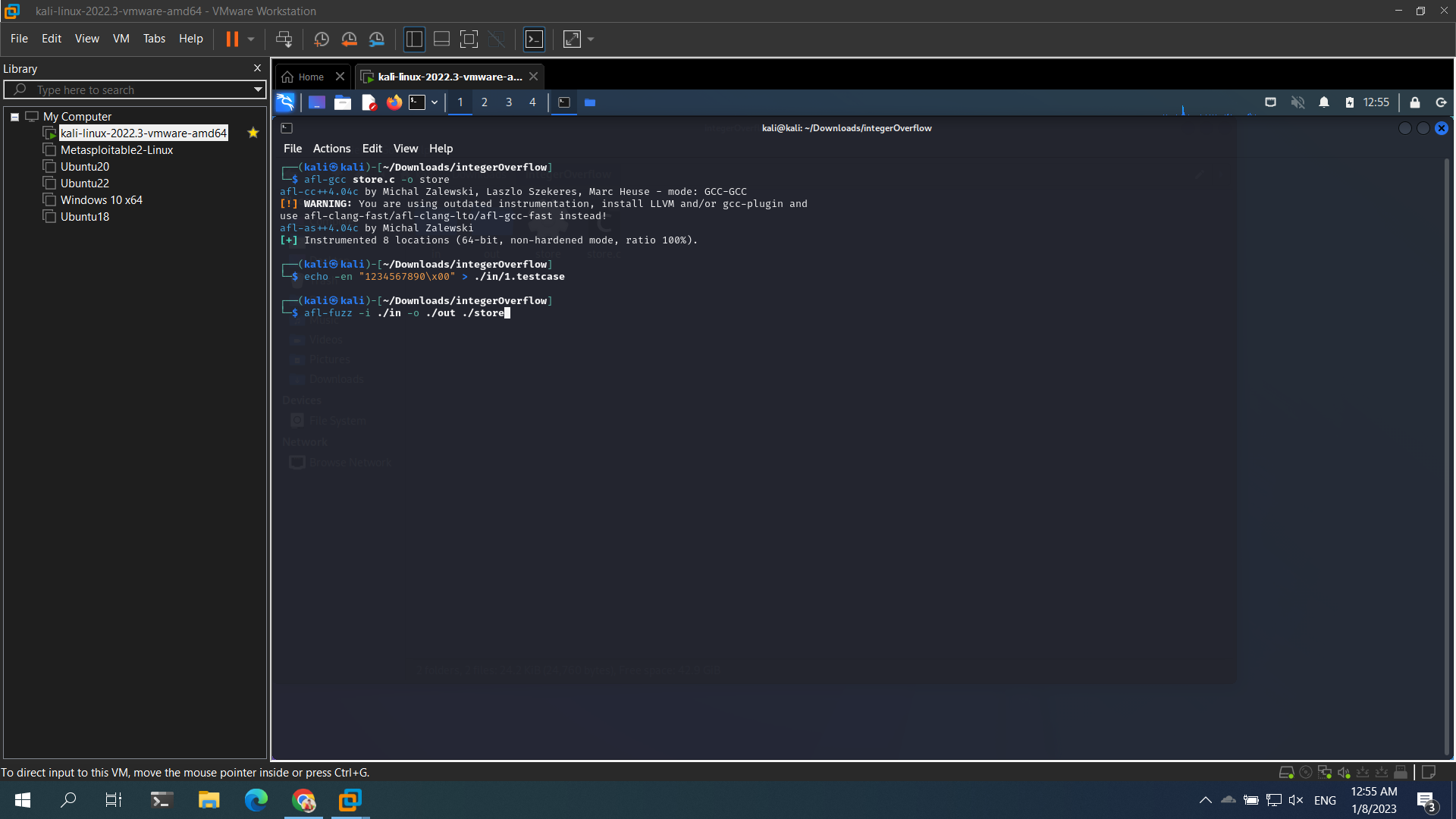
Nguồn: play.picoctf.org

Tạo folder input và output

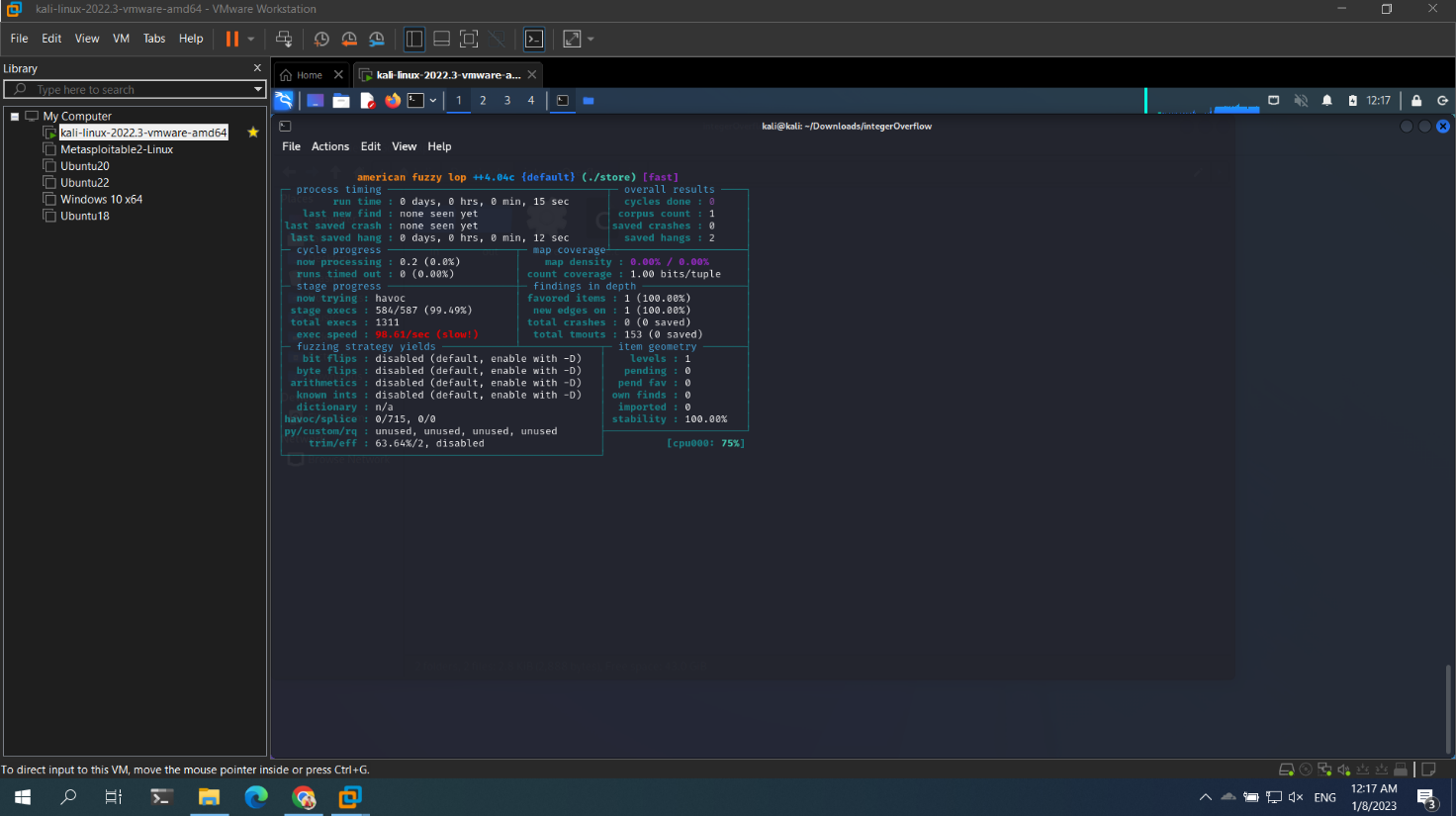
A screenshot of a computer

Description automatically generated

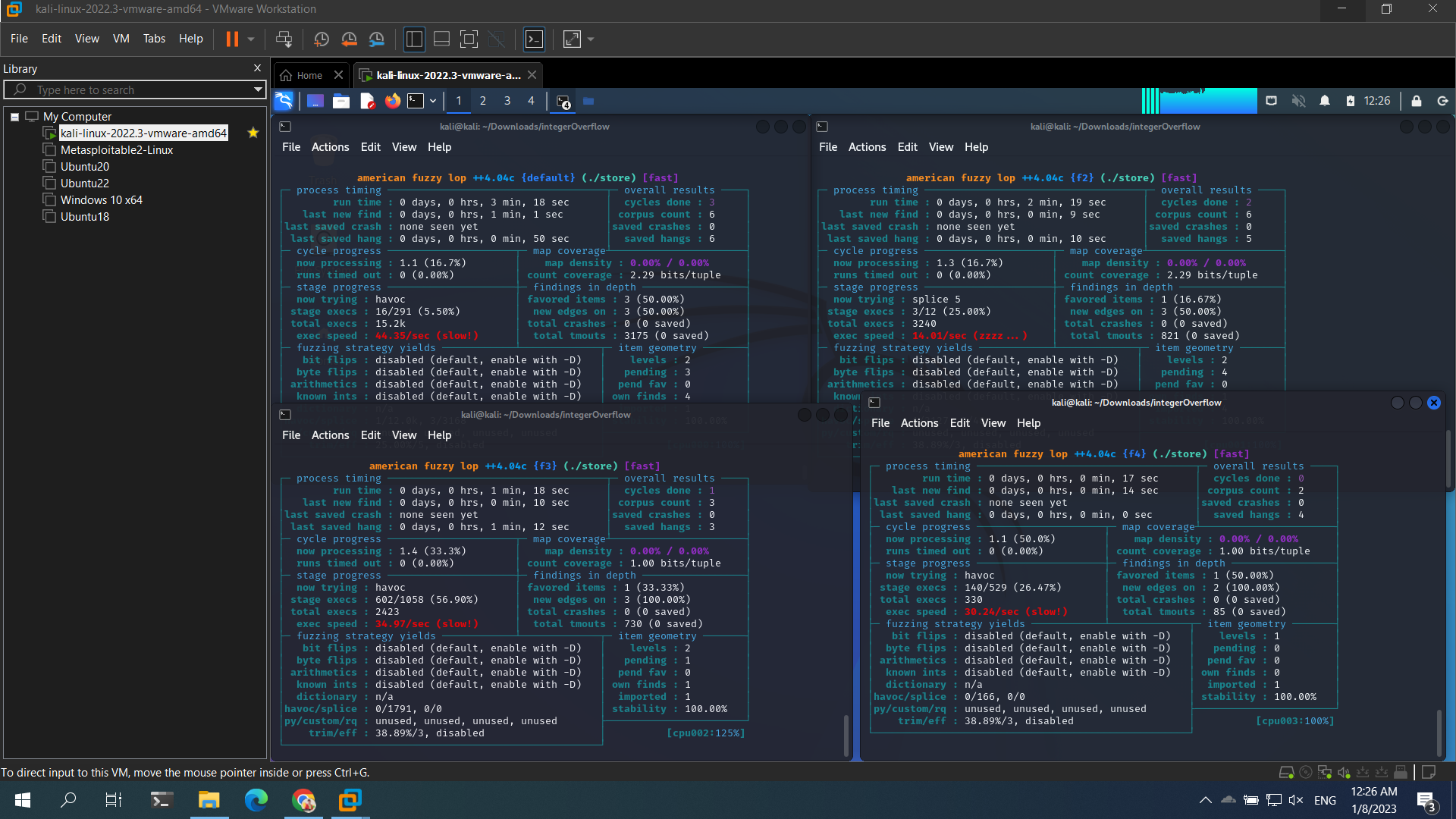
Tạo các testcase



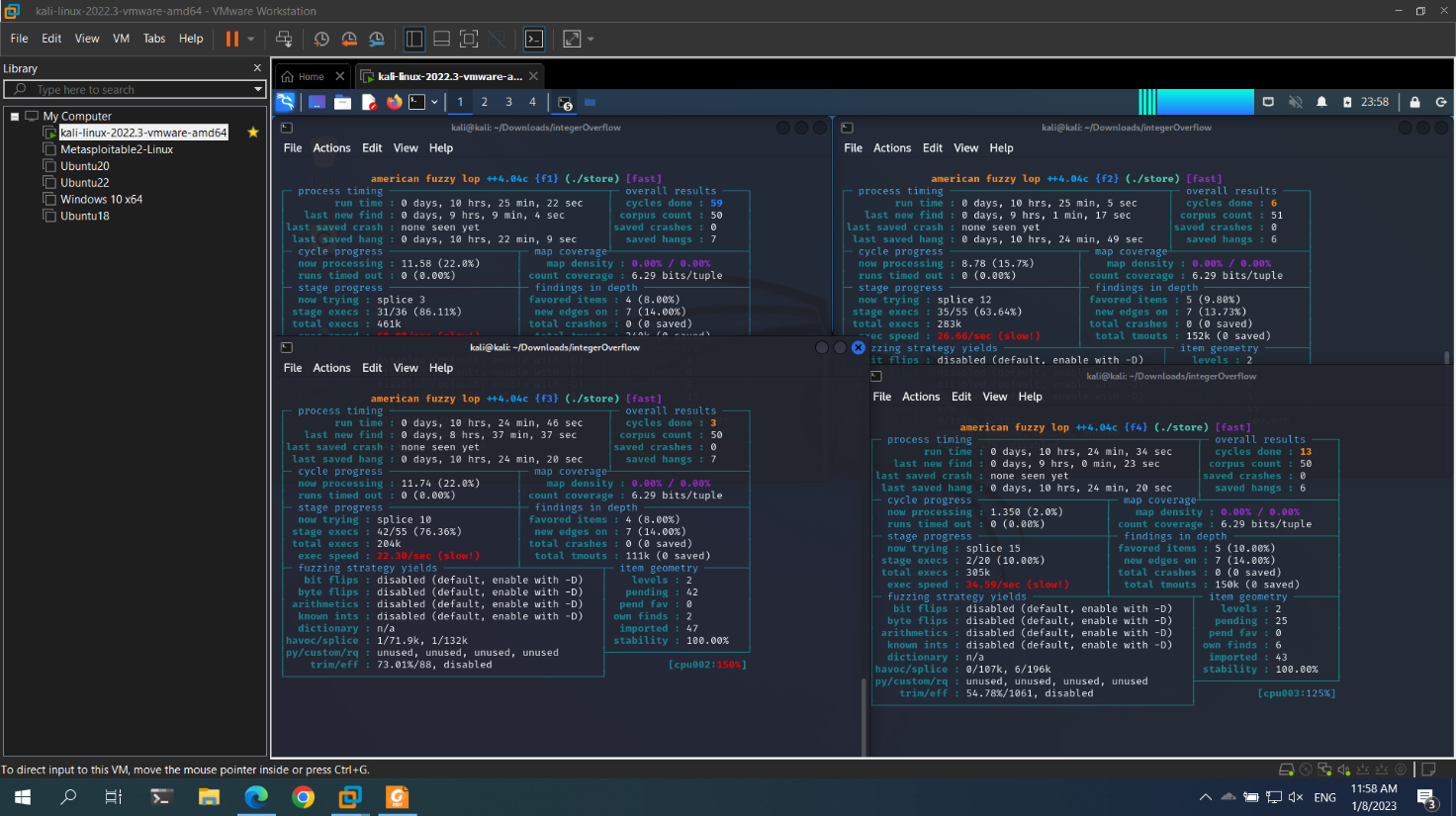
Thực hiện fuzzing (single thread)



Fuzzing multithread



Sau 10 tiếng fuzzing ta nhận thấy rằng là đây là lỗi integerOverflow (theo gợi ý) nên không được thể hiện trong phần crash, nên có thể thấy cách fuzzing chưa thực sự hiệu quả với file binary chứa lỗi này (sẽ hiệu quả hơn với những bài bufferOverflow, returnToLibC,…)



Kiểm tra lại trong file crash (không có kết quả)

A screenshot of a computer

Description automatically generated

**Yêu cầu b**

Công cụ thực hiện: sfuzz, wfuzz

Môi trường: <https://github.com/anhkiet1227/NT208_Web-Programming_Project>

So sánh

|  |  |  |
| --- | --- | --- |
|  | sfuzz | wfuzz |
| Cài đặt | Đều nằm trong bộ kali-tools-fuzzing | |
| Tính năng | Thực hiện fuzzing các yếu tố về network với các testcase có các giao thực http, imap, pop3,… | Thực hiện fuzzing các yếu tố về network với các testcase có các testcase về injection, webservice, vulns,… |
| Quy trình thực hiện | Giống: host service, cài đặt môi trường | |
| Câu lệnh chạy: sfuzz – S 192.168.1.3 -p 3000 -T -f /usr/share/sfuzz-db/bassic.http | Câu lệnh chạy: wfuzz -c -z file,/usr/share/wfuzz/wordlist/Injections/All\_attack.txt –hc 404, 400 “http://192.168.1.3:3000/FUZZ” |
| Giải thích câu lệnh | Fuzzing với ip 192.168.1.3 port 3000, tcp, và testcase bassic.http | Fuzzing với url là <http://102.168.1.3:3000/FUZZ>, testcase All\_attack.txt và tắt các respone 404, 400 |
| Thời gian | 6 phút 9 giây | < 1 giây |
| Kết quả | 194 respone 200 có thể khai thác  Do bộ testcase rộng hơn nên có thể quét được nhiều hơn | 64 respone 200 có thể khai thác  Do bộ testcase nhỏ hơn nên có thể quét được ít hơn |

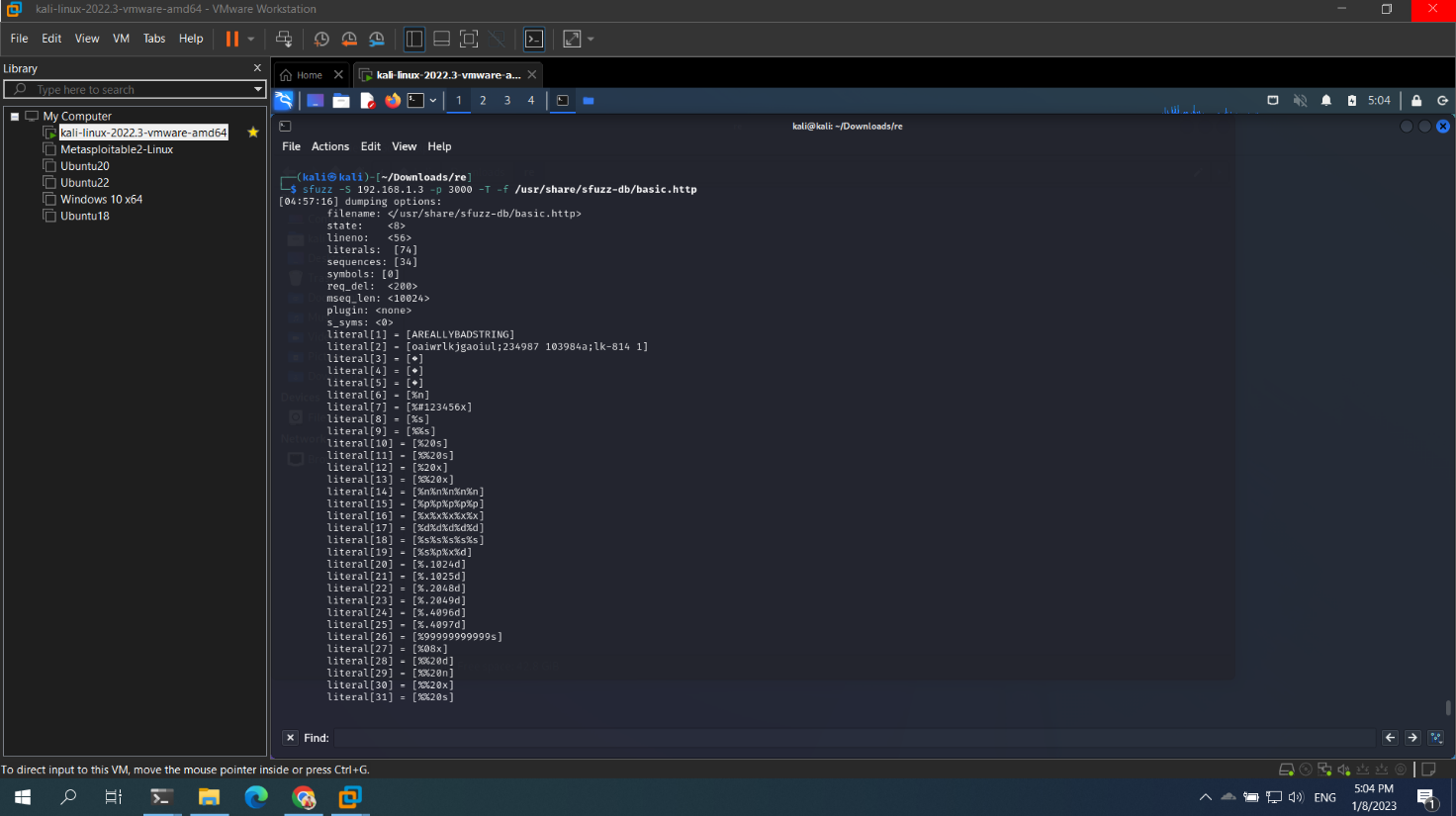
Minh chứng

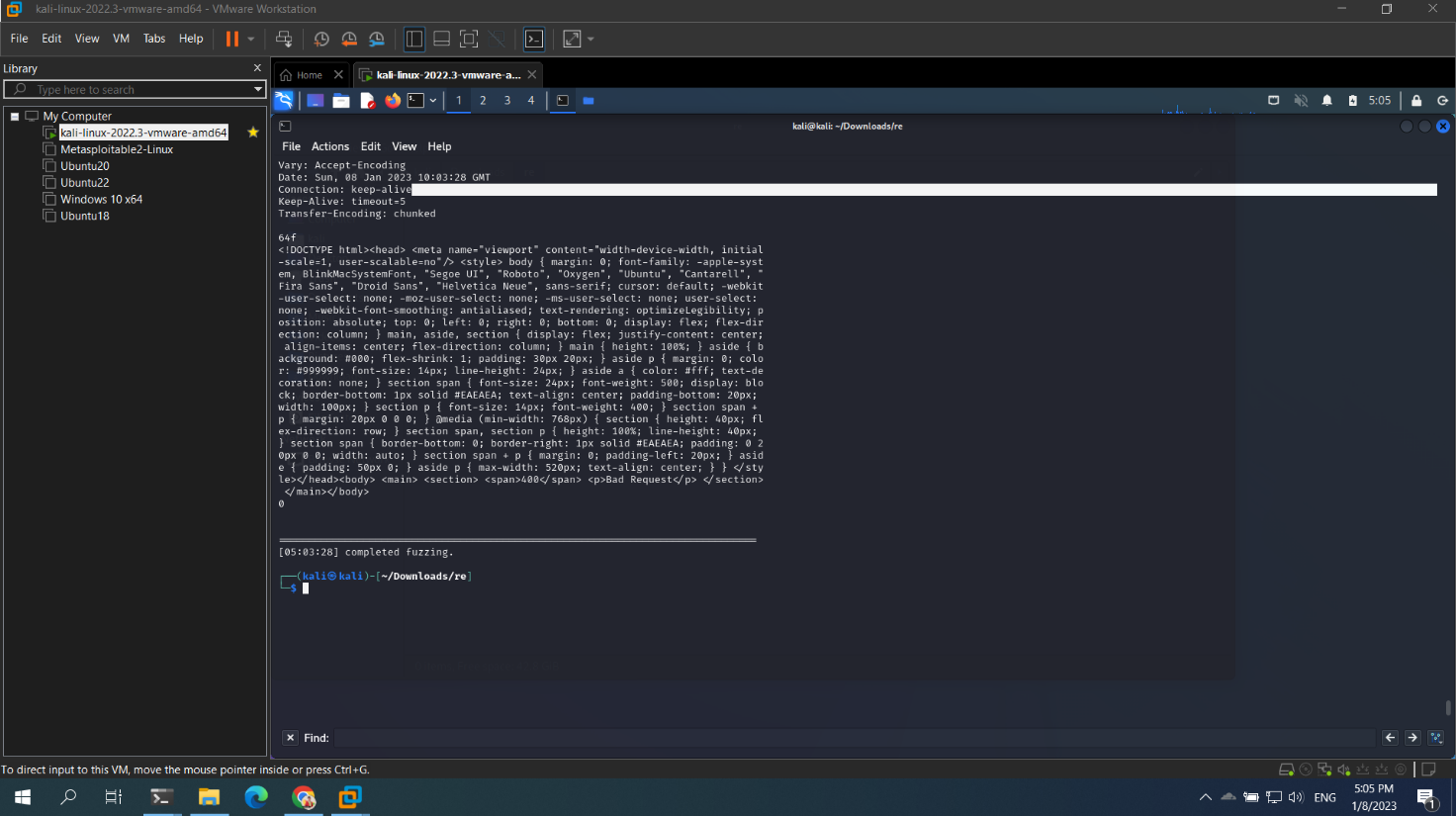
Service

Graphical user interface, text

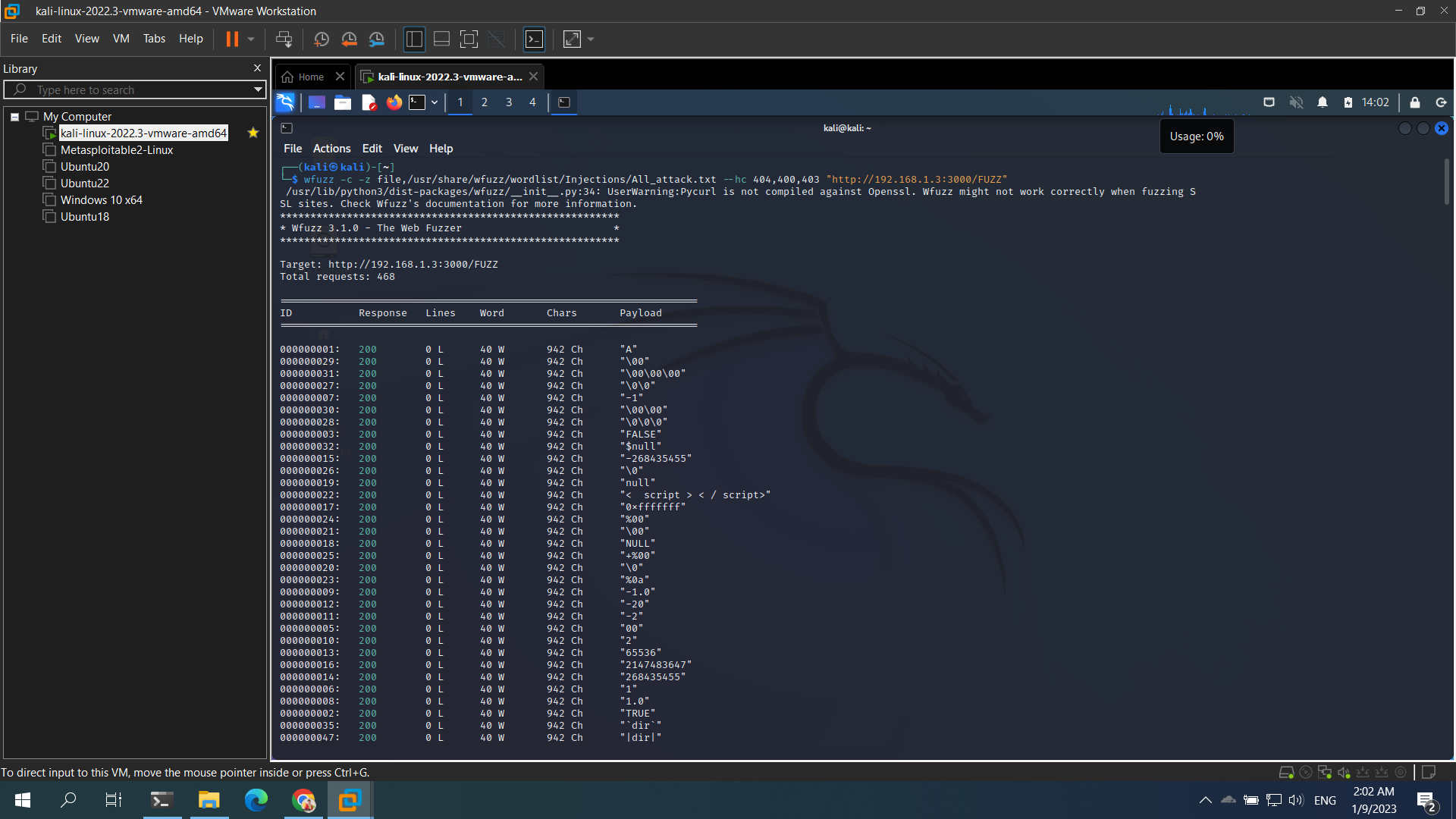
Description automatically generated

Sfuzz:





Wfuzz:



---

***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 .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**:

1. Hoàn thành tốt yêu cầu được giao.
2. 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-2)