BÁO CÁO BÀI TẬP

**Môn học: An toàn mạng máy tính nâng cao**

**Kỳ báo cáo: Buổi 02 (Session 02)**

**Tên chủ đề: Malware**

*GV: Nguyễn Duy*

*Ngày báo cáo: 26/04/2023*

1. **THÔNG TIN CHUNG:**

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

Lớp: NT534.N21.ANTN

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

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

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** | **Người đóng góp** |
| 1 | Kịch bản 01: Malware: theZoo | 100% |  |
| 2 | Kịch bản 02: Capa: Mal analysis | 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 thực hiện:

Intel core i5 8250U 8th gen

SSD 500GB

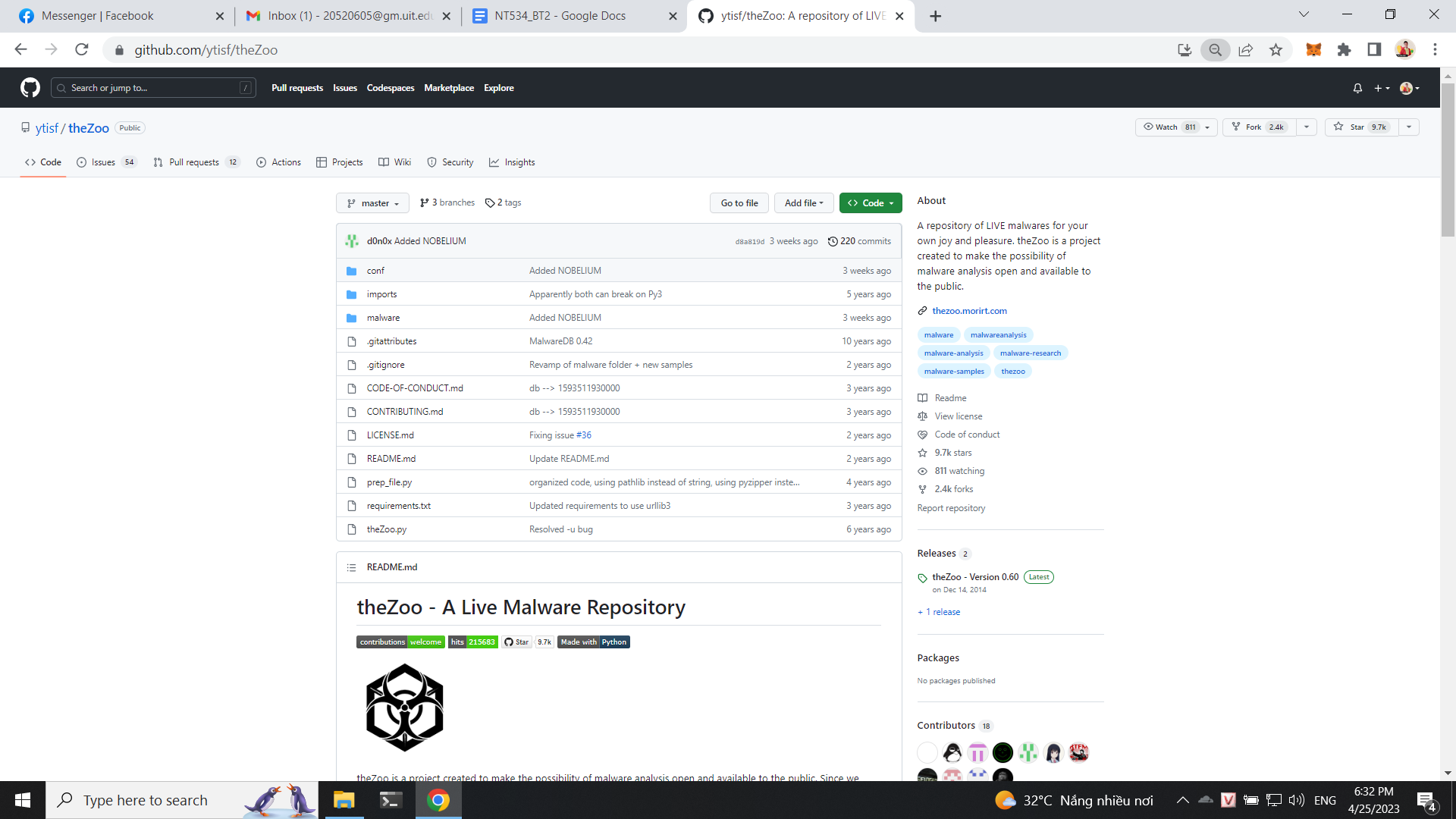
HDD 1000GB

RAM 16GB DDR3L

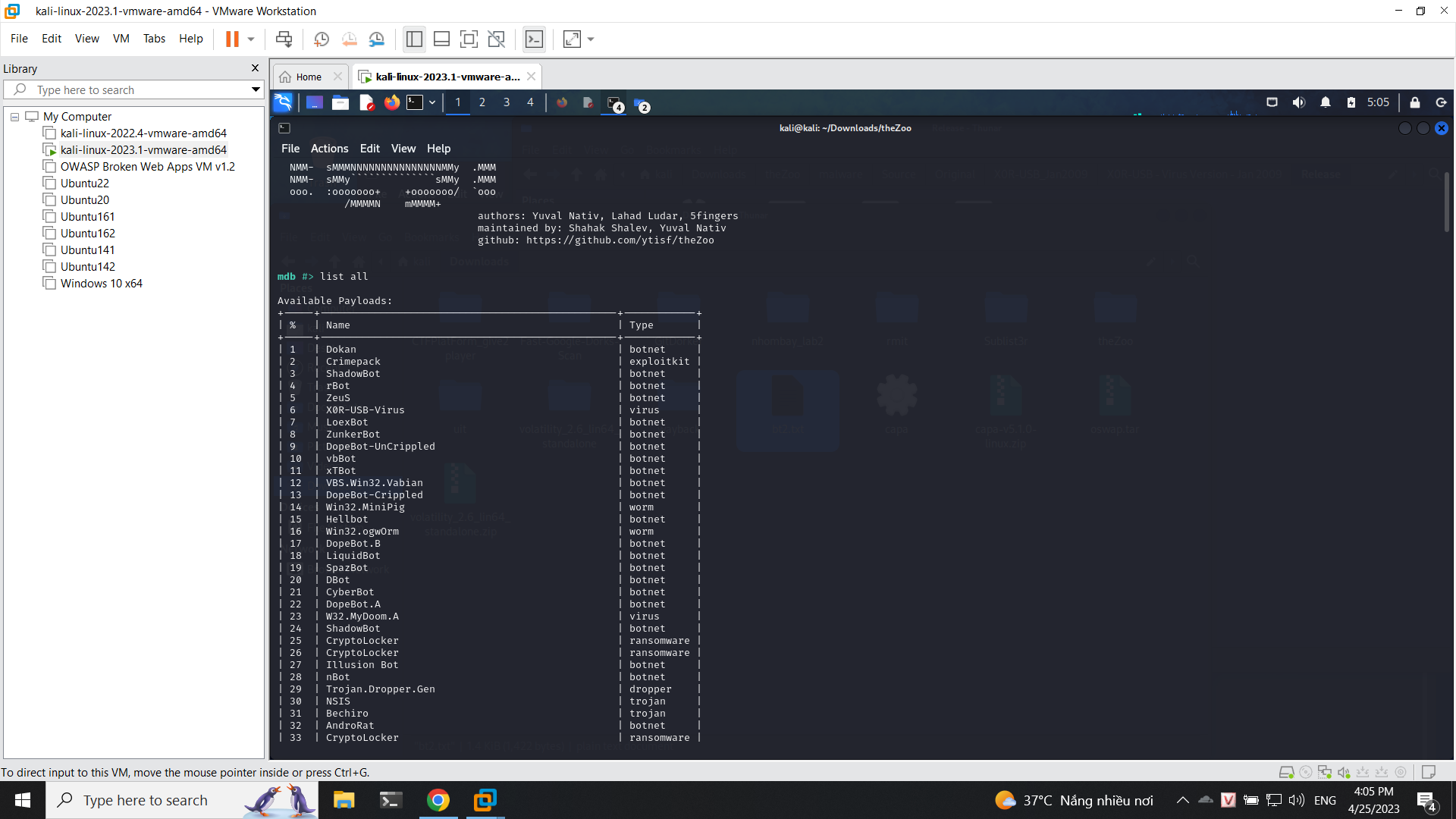
OS Kali Linux 2023.1

## Kịch bản 1

Đầu tiên thực hiện clone repo theZoo để lấy mã độc



Tiếp theo thực hiện list các mã độc ra để xem

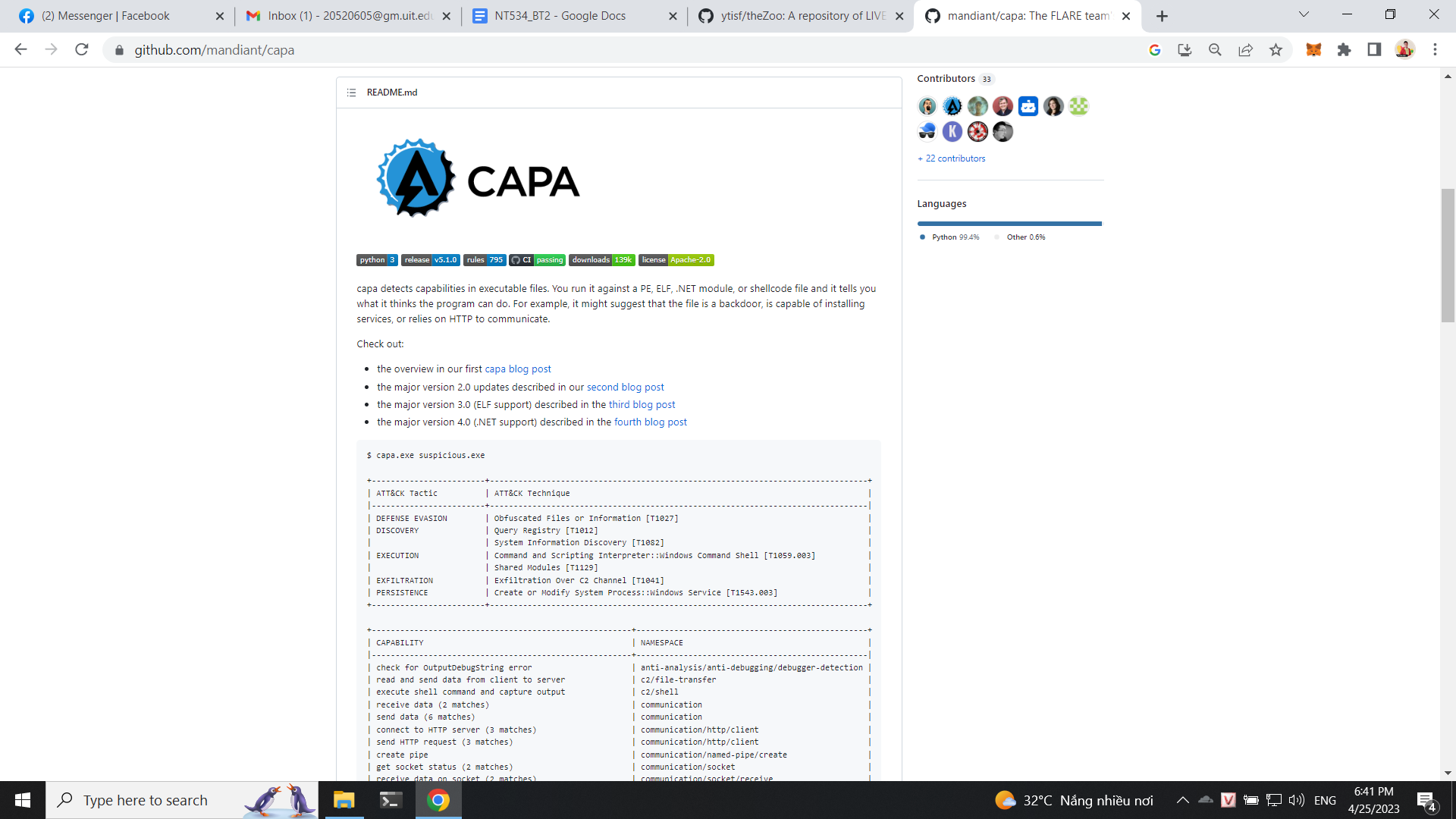


Với yêu cầu virus ta sẽ thực hiện 5 trường hợp virus bao gồm:

* Xor USB
* Viking Horde
* Anthrax
* Relock
* Whore

## Kịch bản 2

Tool thực hiện kiểm tra, phân tích mã độc: Capa



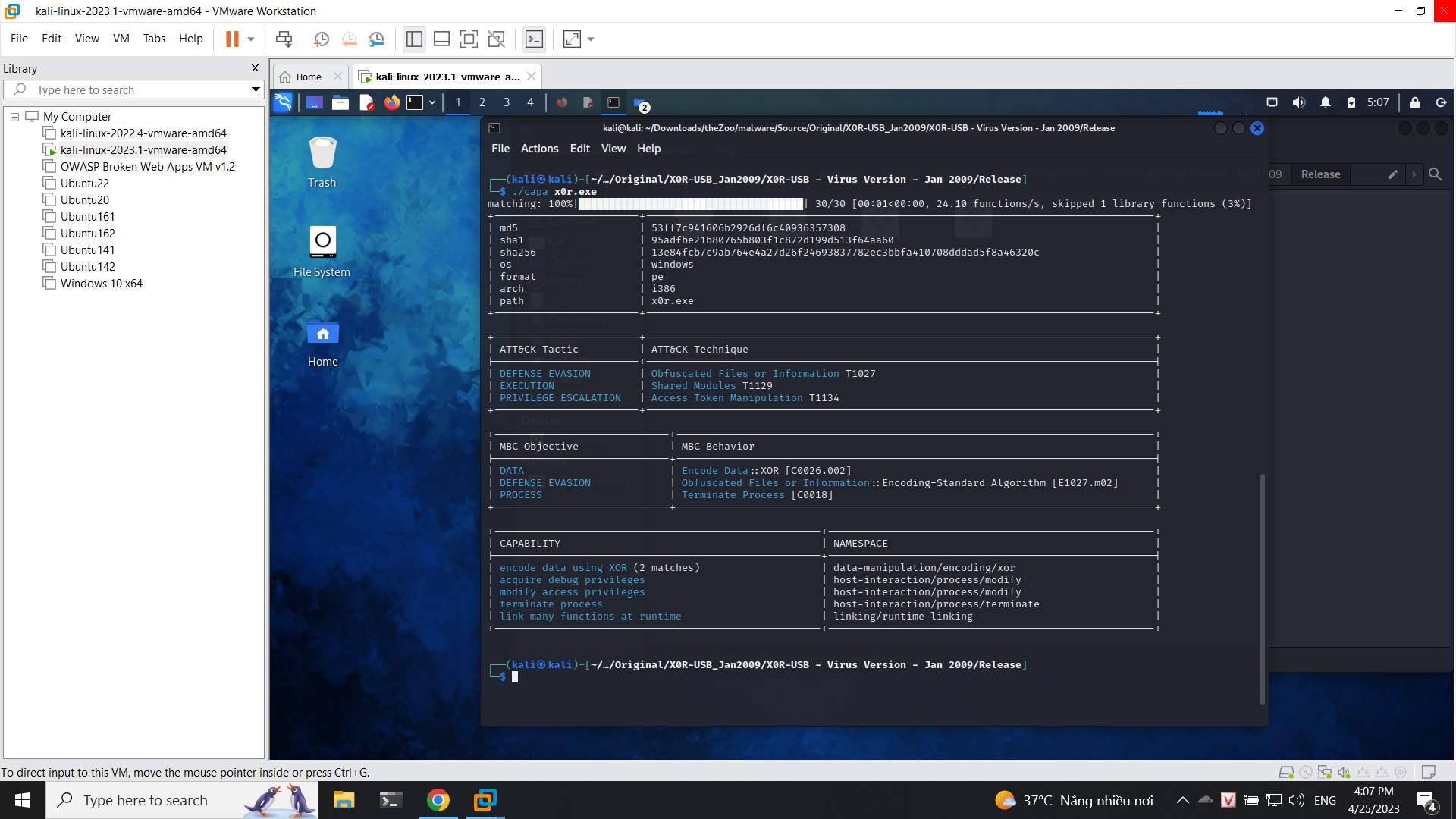
Đầu tiên ta sẽ tải Capa phiên bản standalone cho linux để thực hiện

Sau đó thực hiện quét

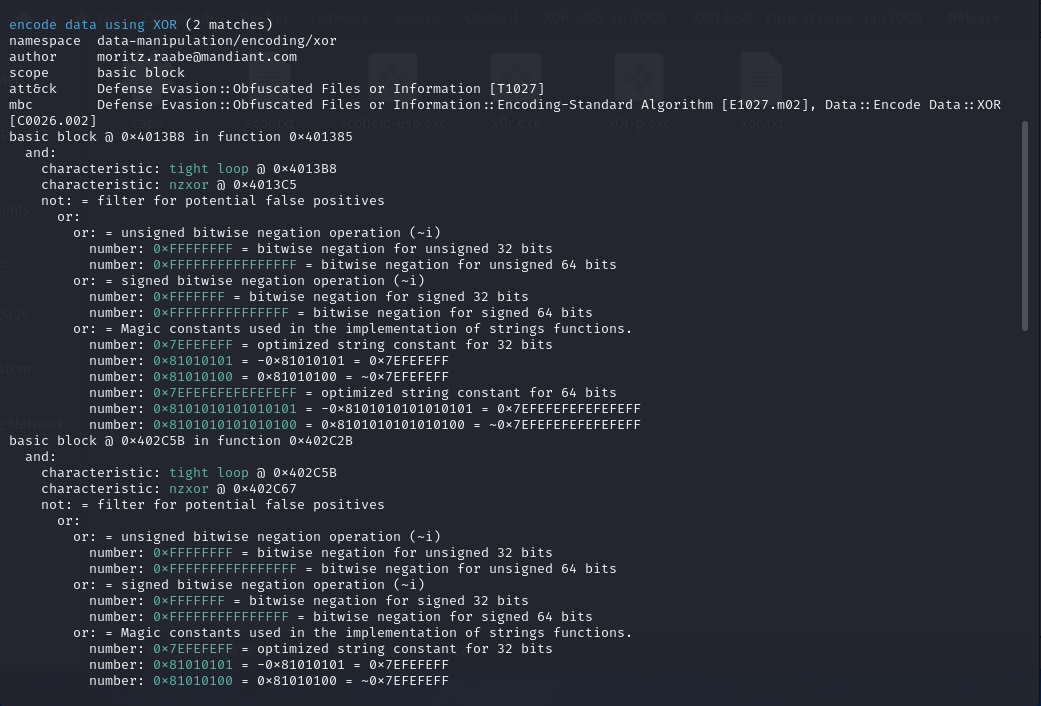
Với xor usb virus ta thấy được thông tin về kỹ thuật tấn công như obfuscate file, information, share module, access token manipulation. Ta thấy được các behavior như encode bằng xor, obfuscate file và terminal process

Cuối cùng ta thấy được các khả năng của virus:

* encode data using XOR (2 matches)
* acquire debug privileges
* modify access privileges
* terminate process
* link many functions at runtime



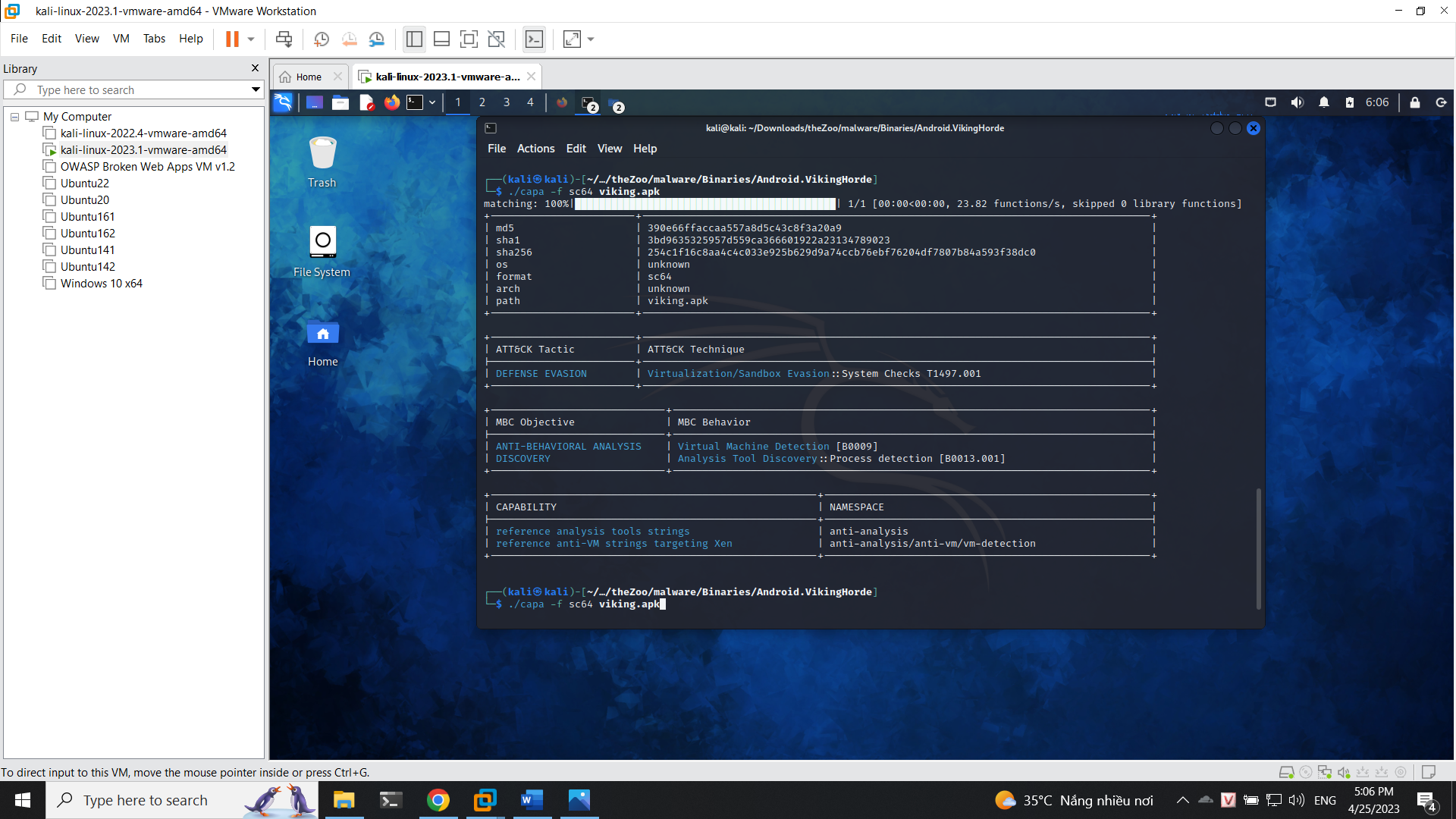
Ta có thể sử dụng thêm flag -vv để xem thêm thông tin



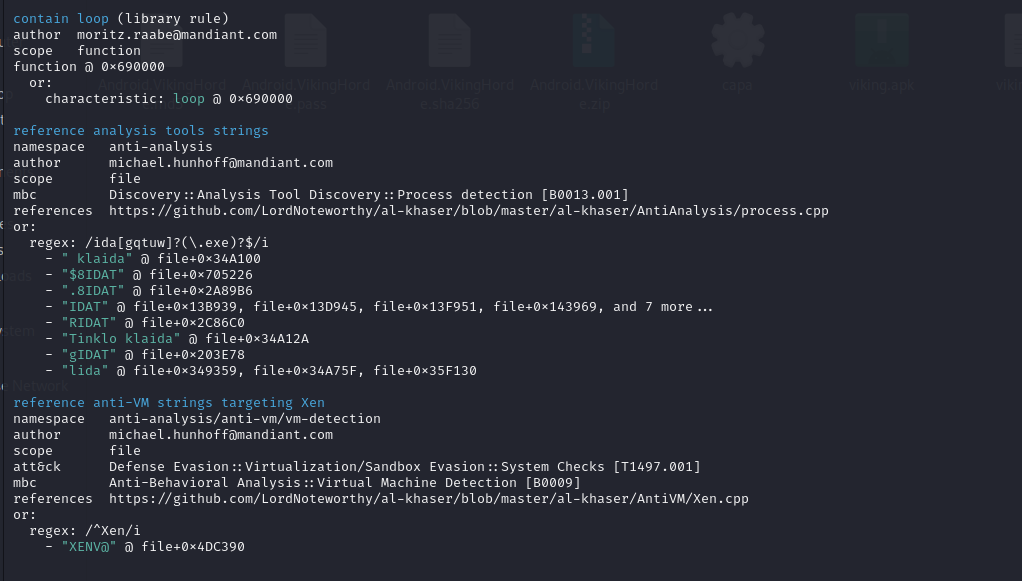
Tiếp tục với virus Viking Horde thì ta thấy được virus này có các hành vi:

* Phát hiện máy ảo
* Phát hiện các công cụ phân tích mã độc

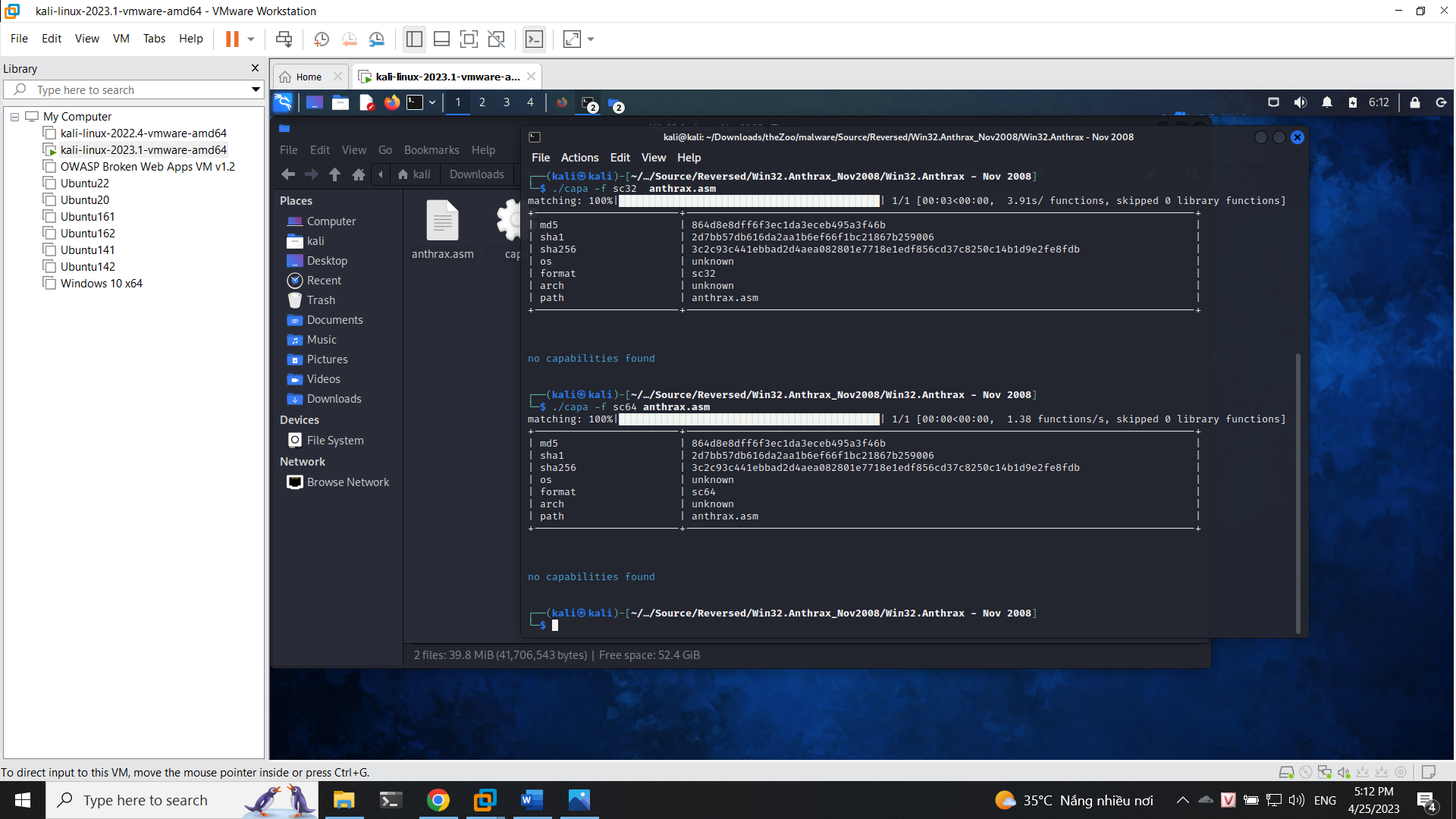
Ngoài ra cũng có các kỹ thuật tấn công được cung cấp là sandbox evasion



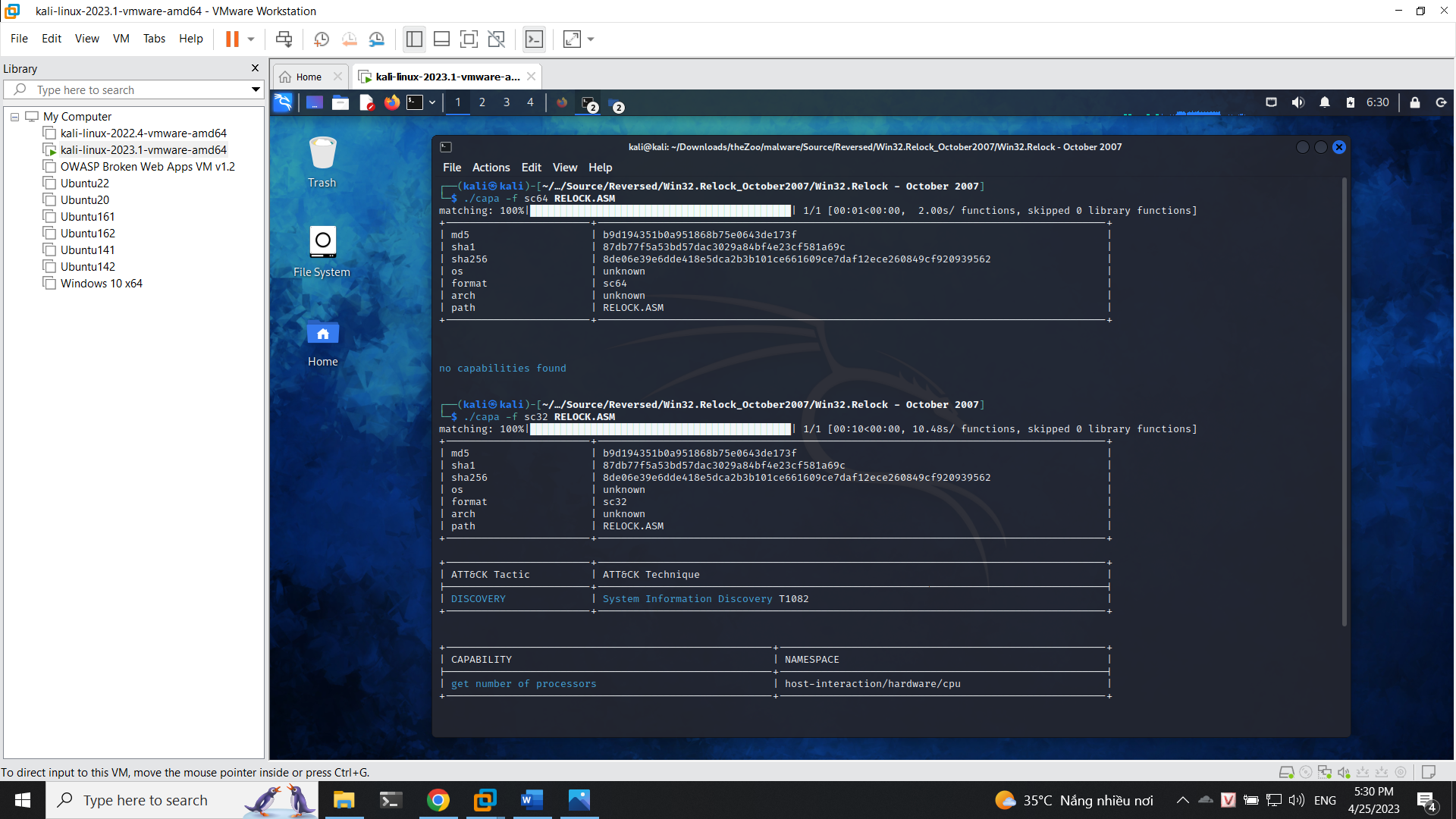
Sử dụng thêm flag -vv



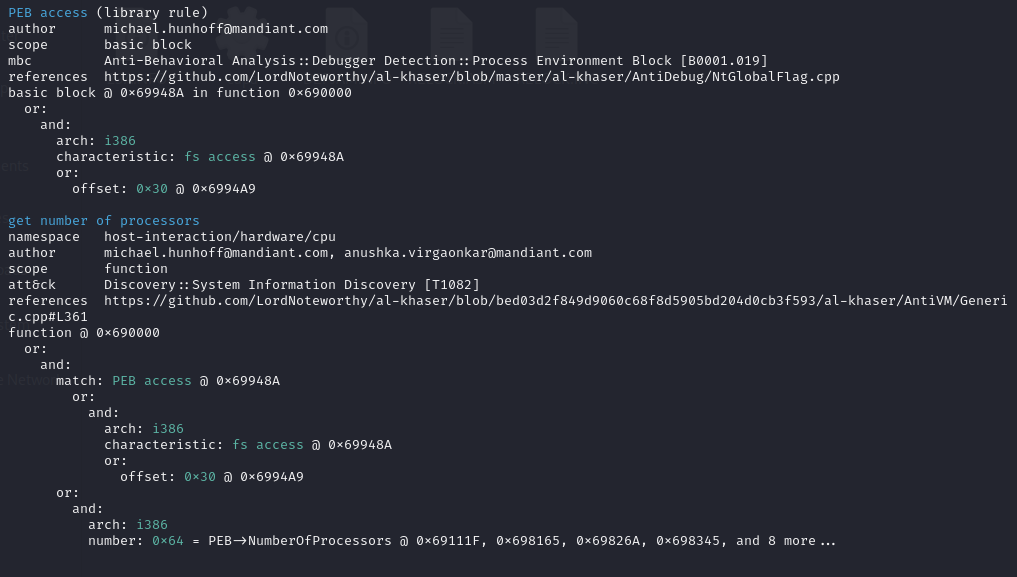
Tiếp tục với virus Anthrax thì ta không thấy có thông tin được cung cấp



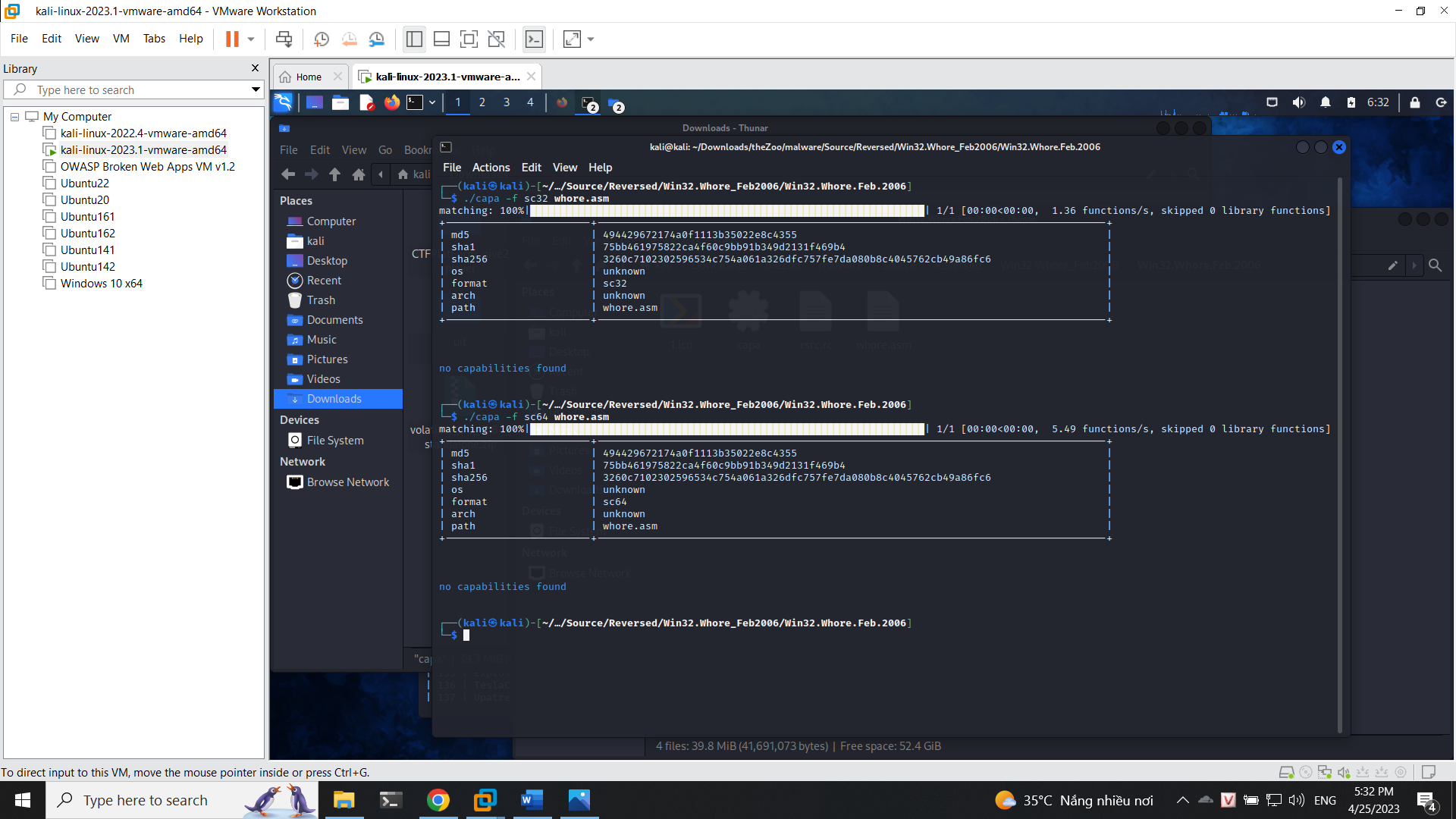
Tiếp tục với virus relock thì ta thấy được thông tin chính là virus có khả năng thực hiện get number of processor và kỹ thuật tấn công được cung cấp là System Info Discovery



Thêm flag -vv để xem



Cuối cùng với virus whore thì ta thấy được thông tin không được cung cấp như virus Anthrax



Kết luận

theZoo cung cấp được một lượng lớn malware cho phép thực hiện công việc học tập nghiên cứu

Capa là một ứng dụng hỗ trợ một phần công việc cho việc phân tích mã độc nhằm phục vụ học tập nghiên cứu

Hạn chế:

theZoo chỉ cung cấp known mal và unknown mal chưa cung cấp được advanced mal

Capa vẫn còn nhiều hạn chế trong việc phân tích mã độc (do kết quả thực nghiệm đã không cung cấp được một số trường hợp, hoặc chạy ra kết quả sai ở một số trường hợp)

---

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

# **YÊU CẦU CHUNG**

* Sinh viên tìm hiểu và thực hành theo 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]-SessionX\_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành/Tên Cá nhân đã đăng ký với GV).

*Ví dụ: [*NT101.K11.ANTT*]-Session1\_Group3.*

* 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.
* Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

**Đánh giá**: Sinh viên hiểu và tự thực hiện. Khuyến khích:

* Chuẩn bị tốt.
* Có nội dung mở rộng, ứng dụng trong kịch bản/câu hỏi phức tạp hơn, có đóng góp xây dựng.

*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)