Thông tin sinh viên

Võ Anh Kiệt - 20520605

Nguyễn Bùi Kim Ngân - 20520648

Nguyễn Bình Thục Trâm - 20520815

Bài làm

Cấu hình máy thực hiện:

Intel core i5 8250U 8th gen

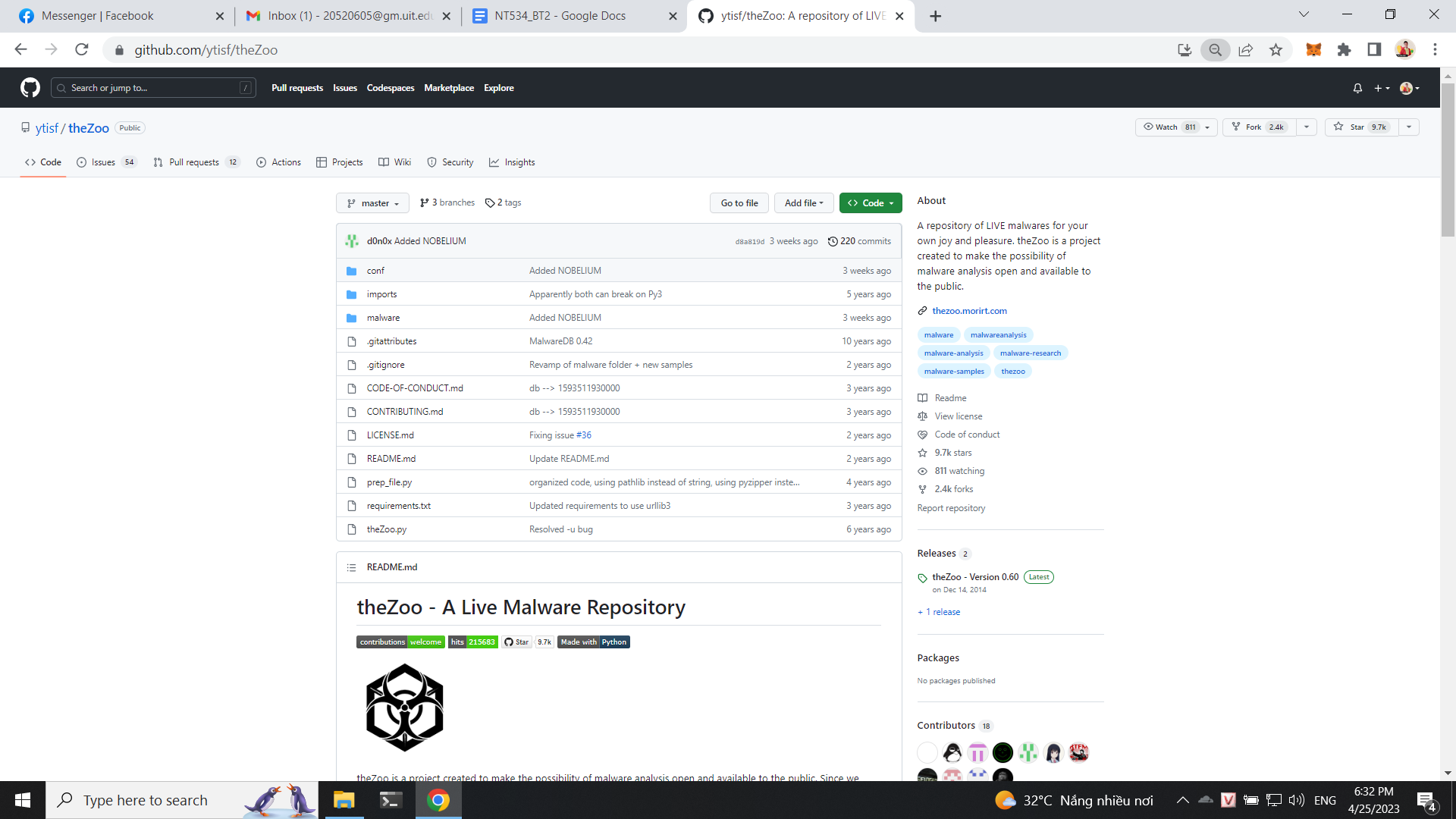
SSD 500GB

HDD 1000GB

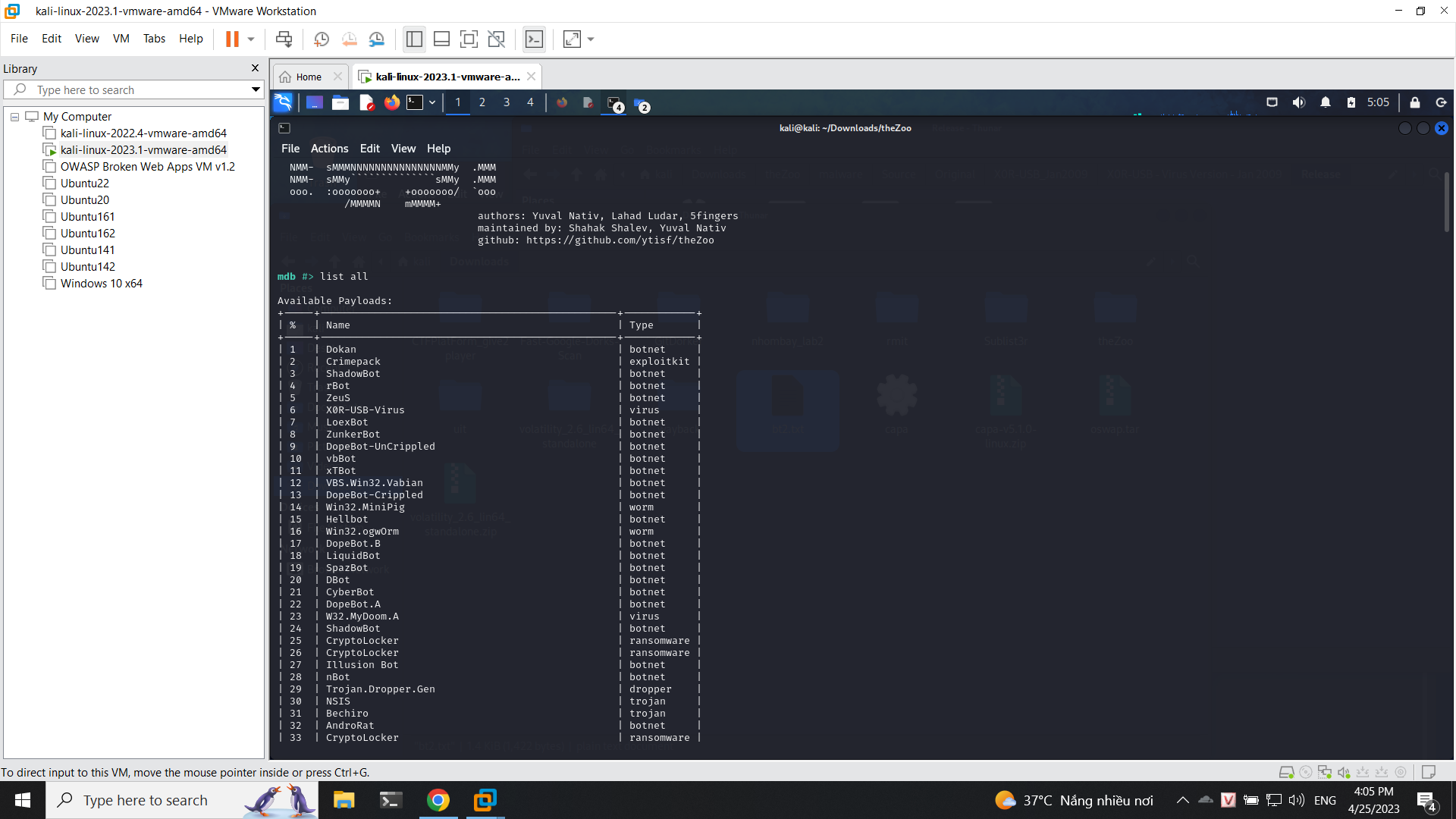
RAM 16GB DDR3L

OS Kali Linux 2023.1

Đầu tiên thực hiện clone repo theZoo để lấy mã độc



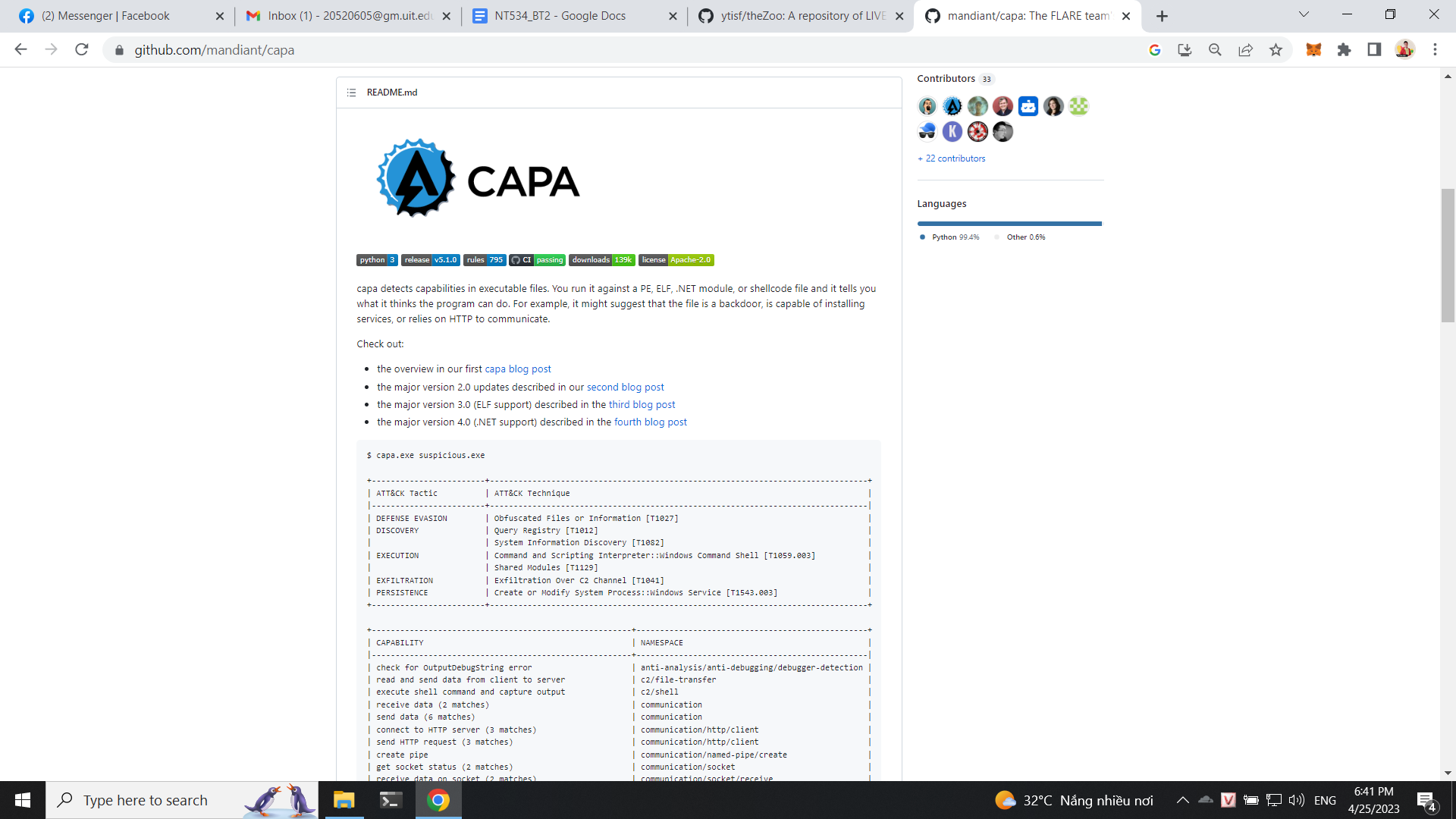
Tiếp theo thực hiện list các mã độc ra để xem



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

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

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



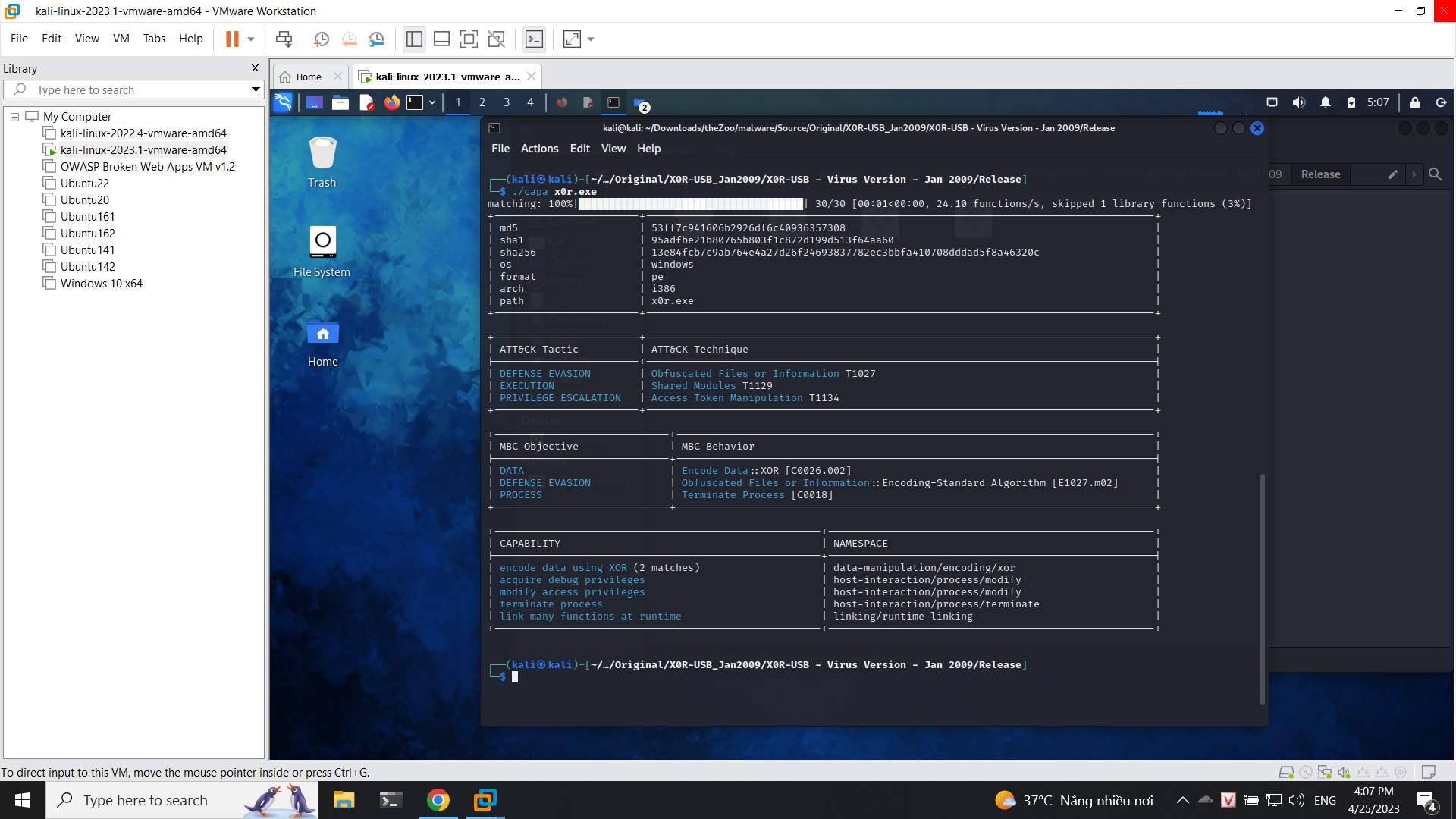
Đầu tiên ta sẽ tải Capa phiên bản standalone cho linux để thực hiện

Sau đó thực hiện quét

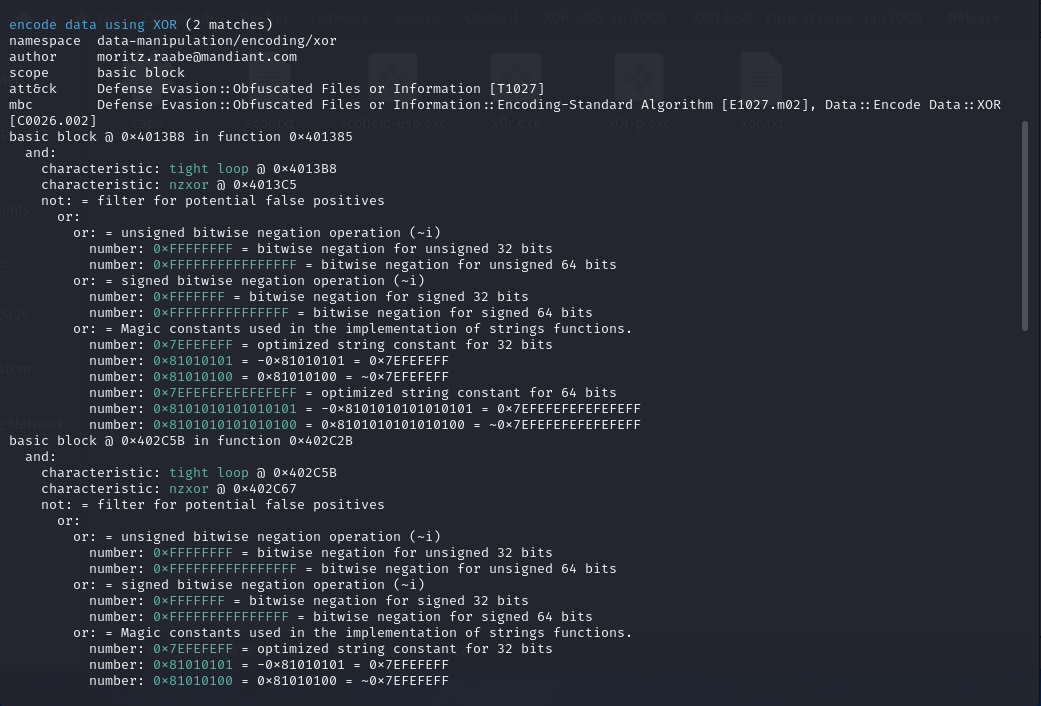
Với xor usb virus ta thấy được thông tin về kỹ thuật tấn công như obfuscate file, information, share module, access token manipulation. Ta thấy được các behavior như encode bằng xor, obfuscate file và terminal process

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



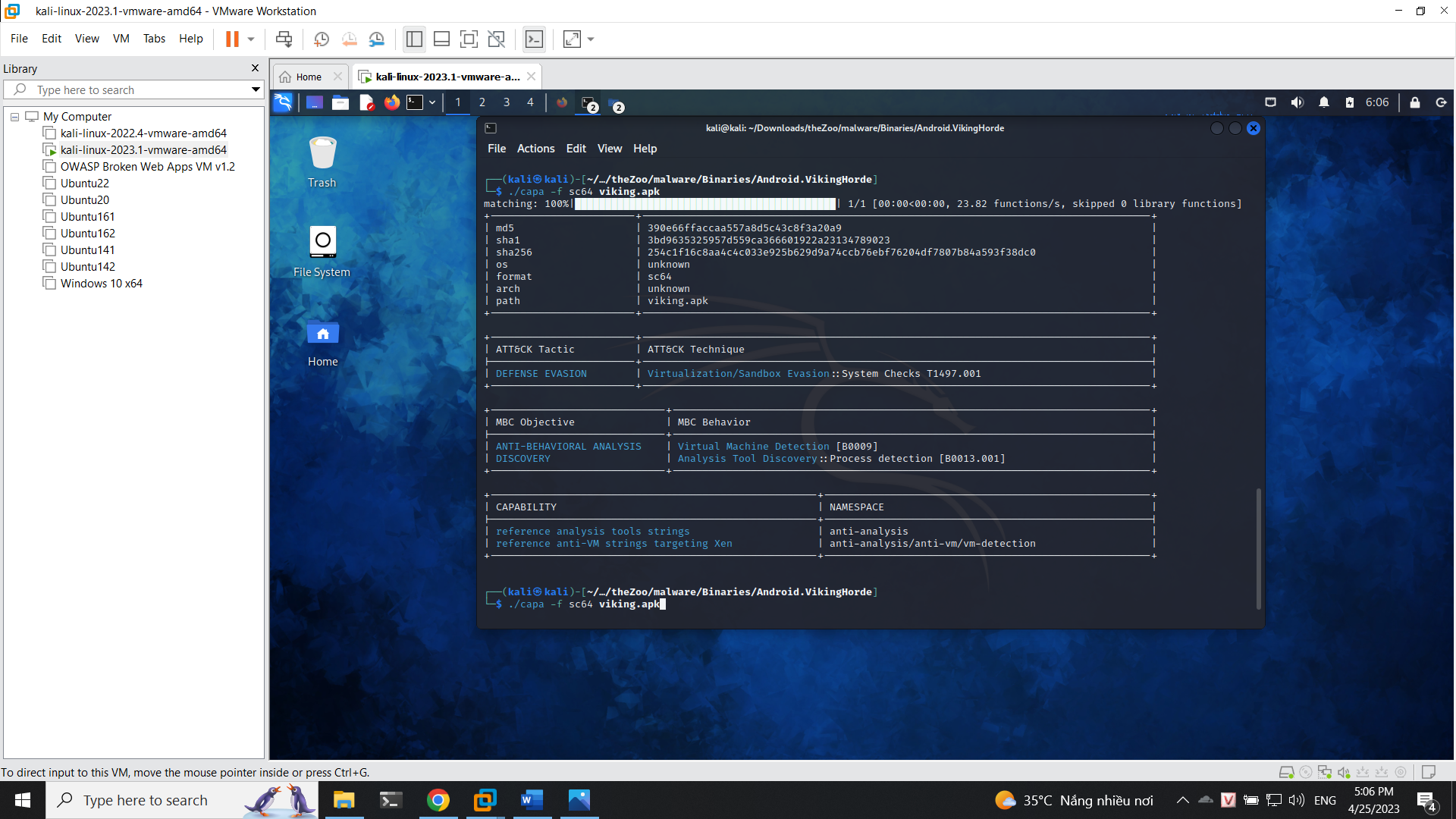
Ta có thể sử dụng thêm flag -vv để xem thêm thông tin



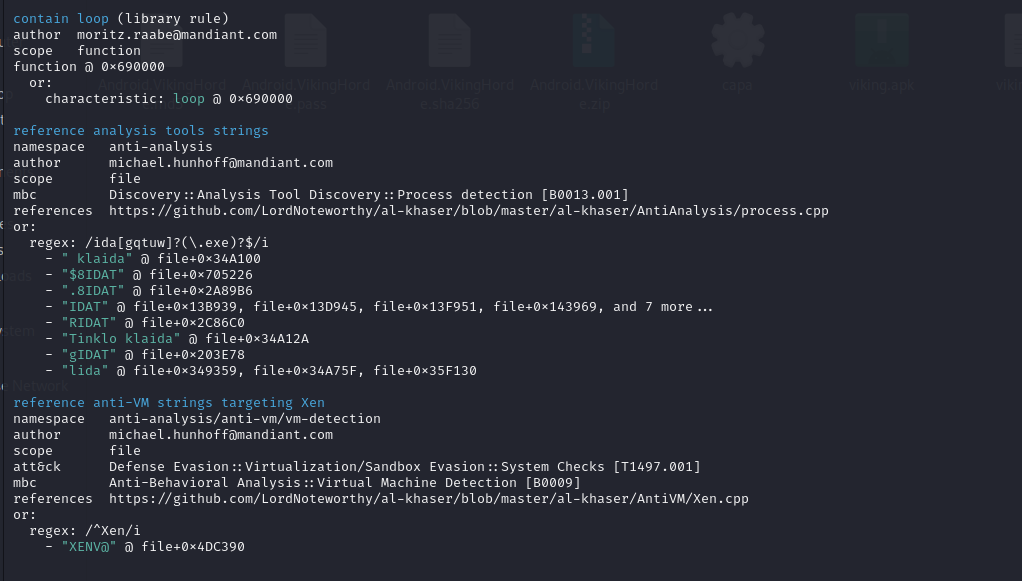
Tiếp tục với virus Viking Horde thì ta thấy được virus này có các hành vi:

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

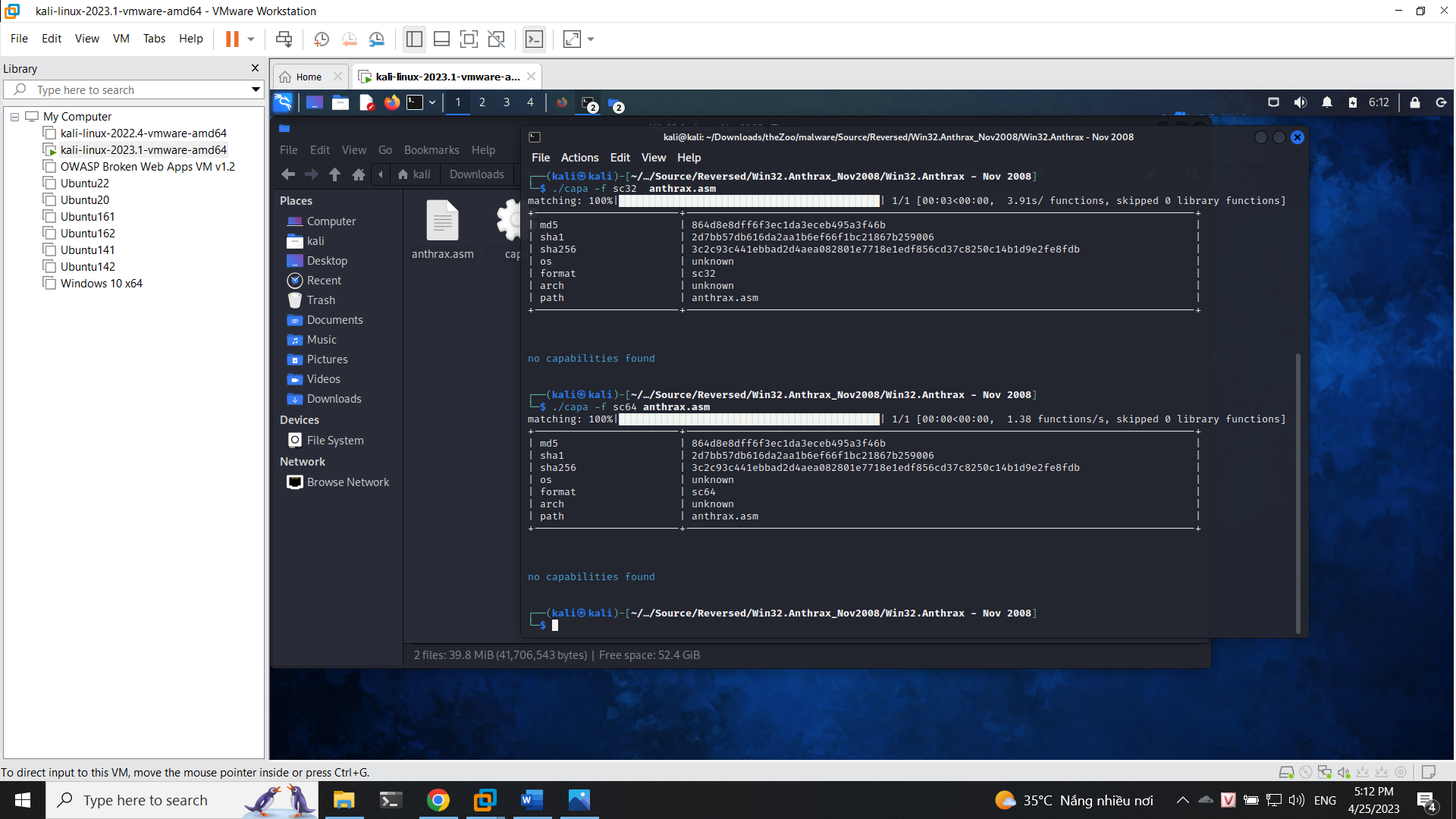
Ngoài ra cũng có các kỹ thuật tấn công được cung cấp là sandbox evasion



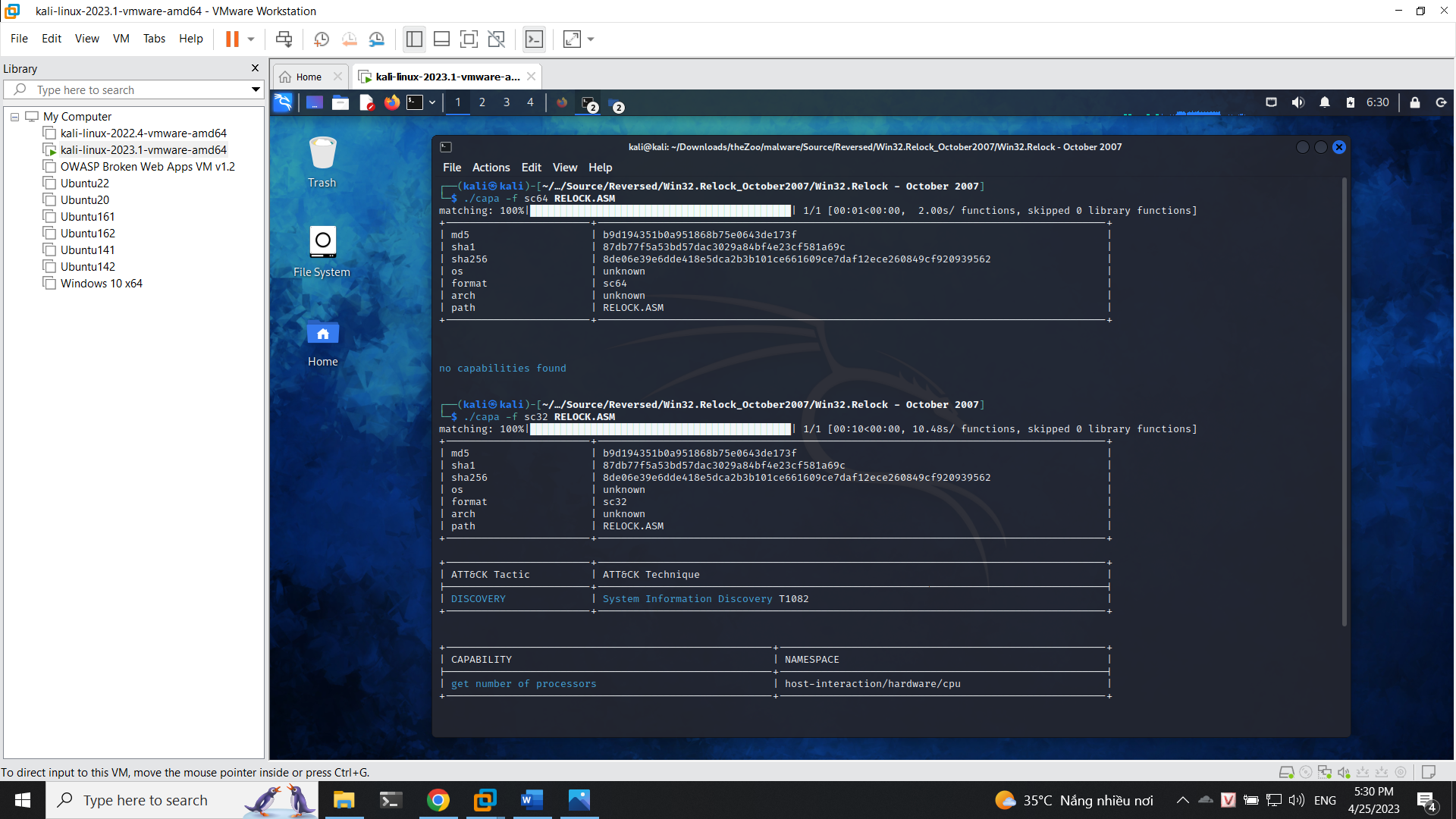
Sử dụng thêm flag -vv



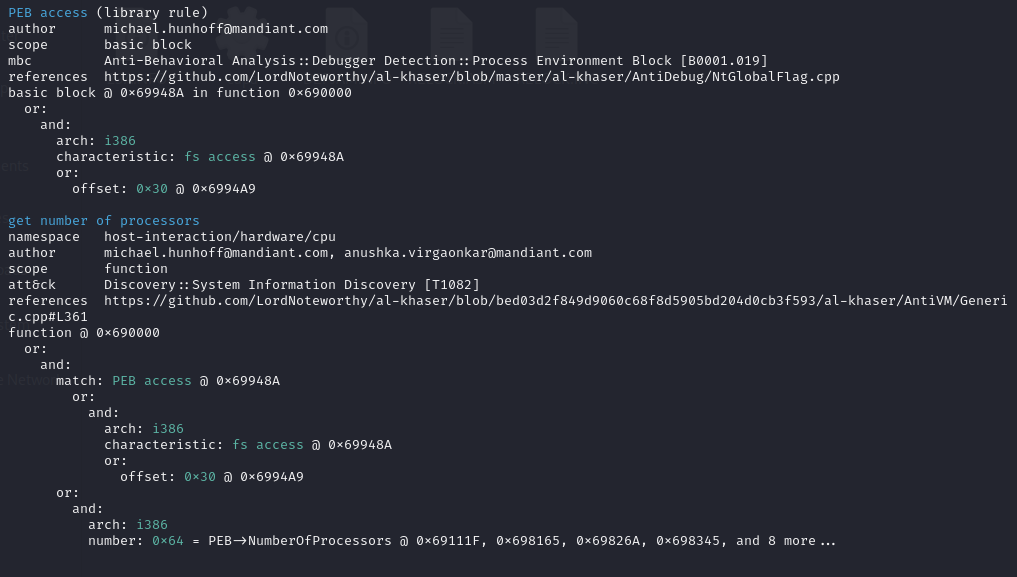
Tiếp tục với virus Anthrax thì ta không thấy có thông tin được cung cấp



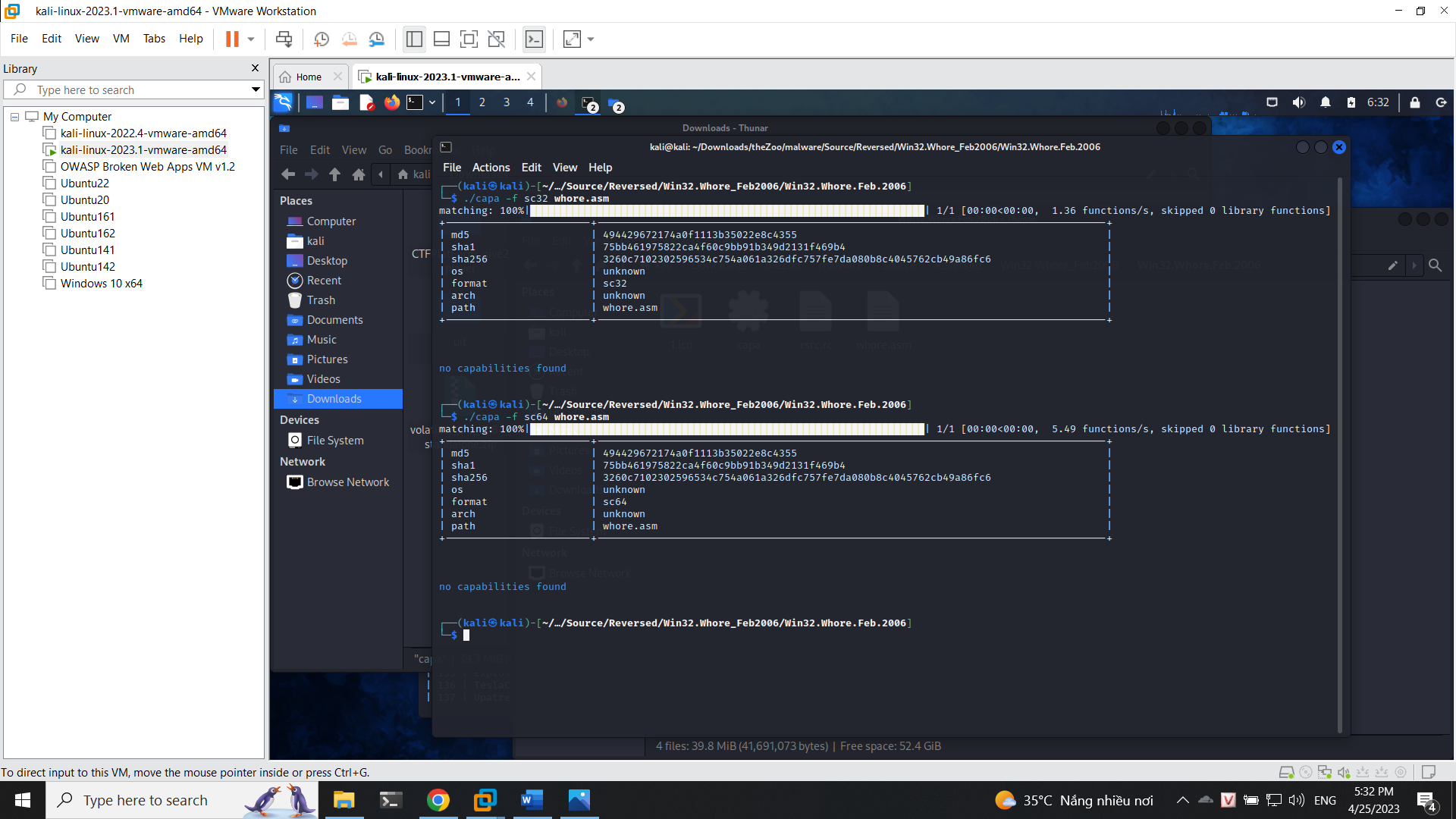
Tiếp tục với virus relock thì ta thấy được thông tin chính là virus có khả năng thực hiện get number of processor và kỹ thuật tấn công được cung cấp là System Info Discovery



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)