|  |
| --- |
| BAN CƠ YẾU CHÍNH PHỦ  **HỌC VIỆN KỸ THUẬT MẬT MÃ**  ¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯  logo ATTT-02 |
| HỌC PHẦN  **TẤN CÔNG VÀ PHÒNG THỦ HỆ THỐNG** |
| BÁO CÁO THỰC HÀNH  **CHRONOS** |
| |  |  | | --- | --- | | ***Họ tên sinh viên:*** | Nguyễn Ngọc Anh | | ***Lớp:*** | ATM03 | | ***Mã sinh viên:*** | AT180304 | |  |  | | ***Giảng viên:*** | TS. Lại Minh Tuấn  **Hà Nội, 2024** | |
|  |

Mục lục

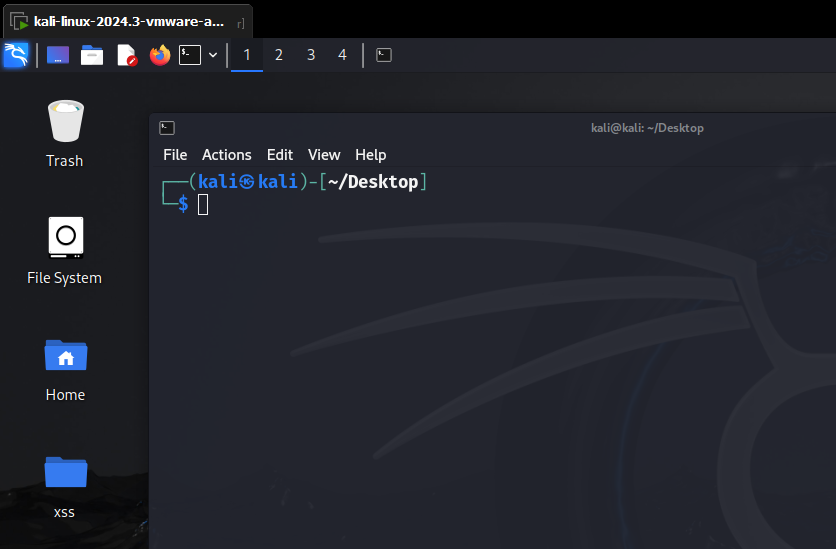
[**I)** **Chuẩn bị** 3](#_Toc185801340)

[**II)** **Khai thác** 4](#_Toc185801341)

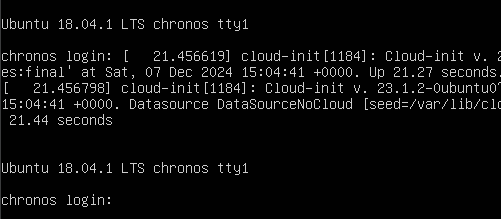
[**III)** **Kết quả** 20](#_Toc185801342)

1. **Chuẩn bị**

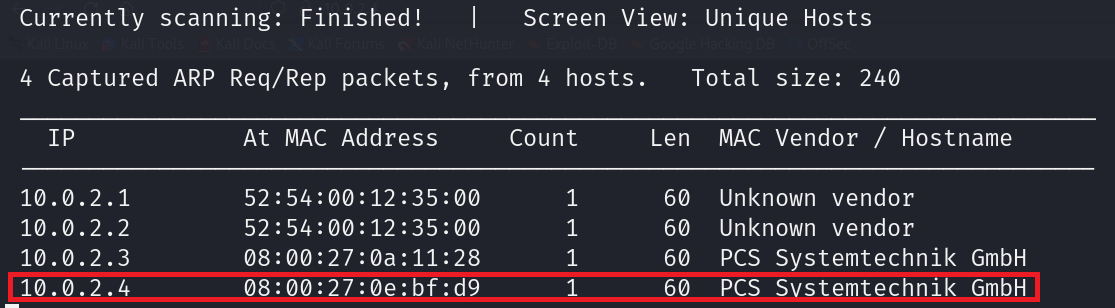
Cài máy ảo Kali trên WMware làm máy attacker để chế độ Briged Adapter



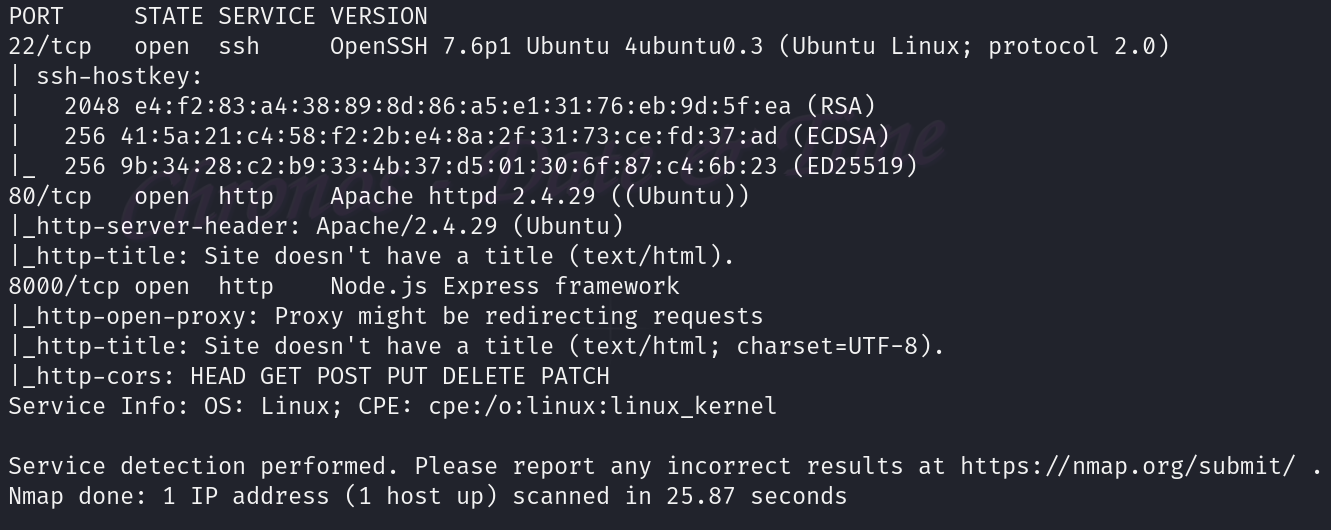
Dựng máy ảo Chronos trên Virtualbox để chế độ Bridged Adapter để có thể kết nối đến máy kali



Tìm máy victim trong phân vùng mạng của mình sử dụng netdiscover



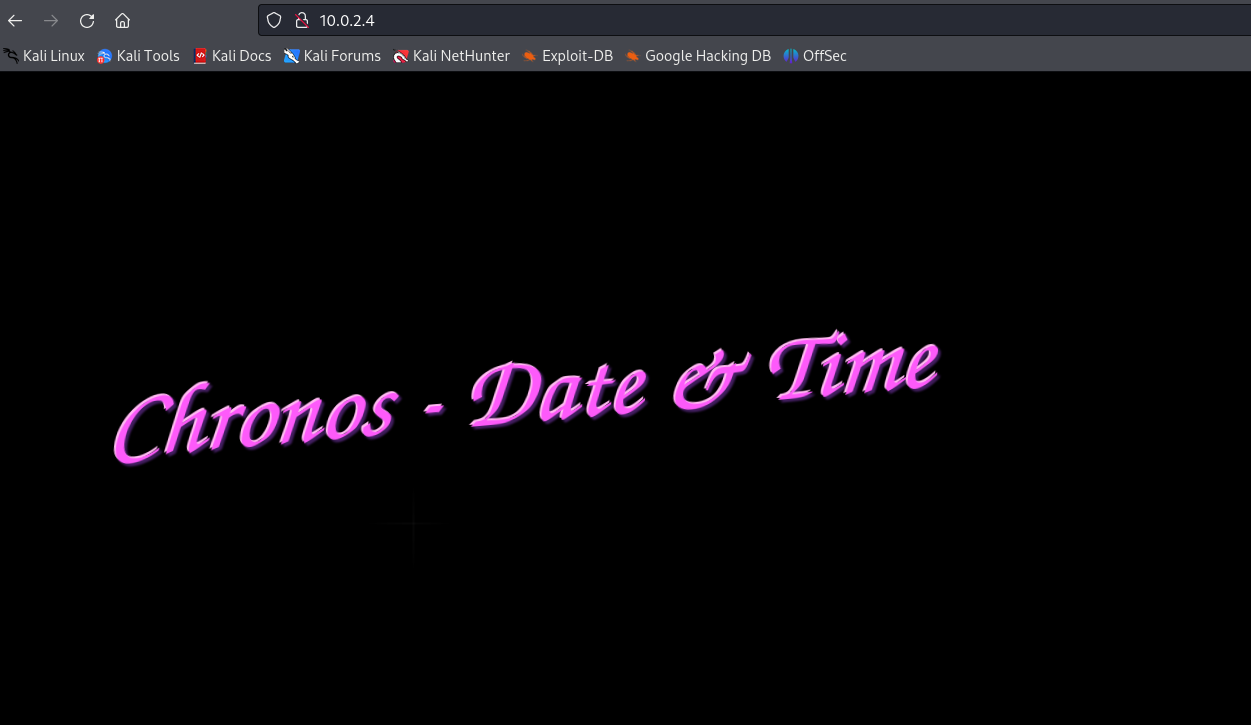
Sử dụng nmap để tìm kiêm các dịch vụ của nó



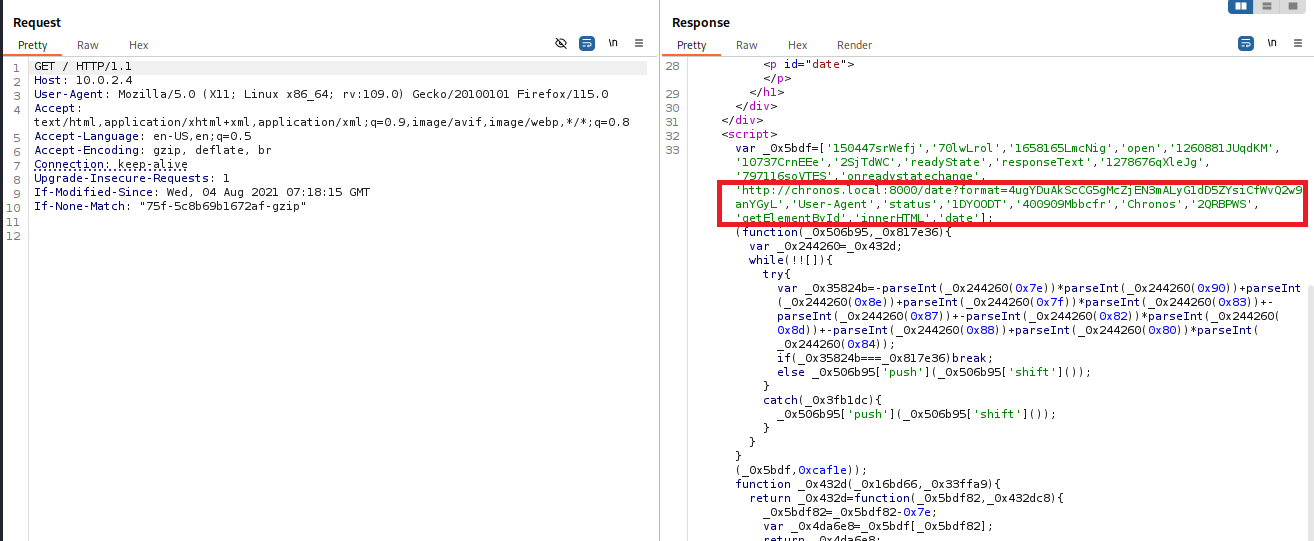
Kết quả trả về cho biết máy ảo đang có các dịch vụ được mở như ssh ở cổng 22, http ở cổng 80 và 8000.

1. **Khai thác**

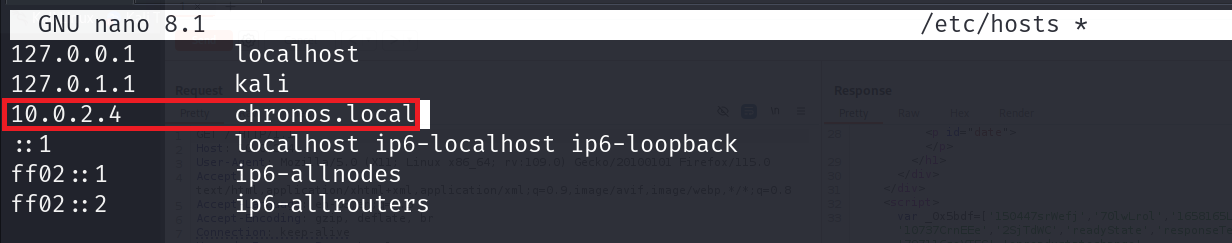
Truy cập vào trang web:



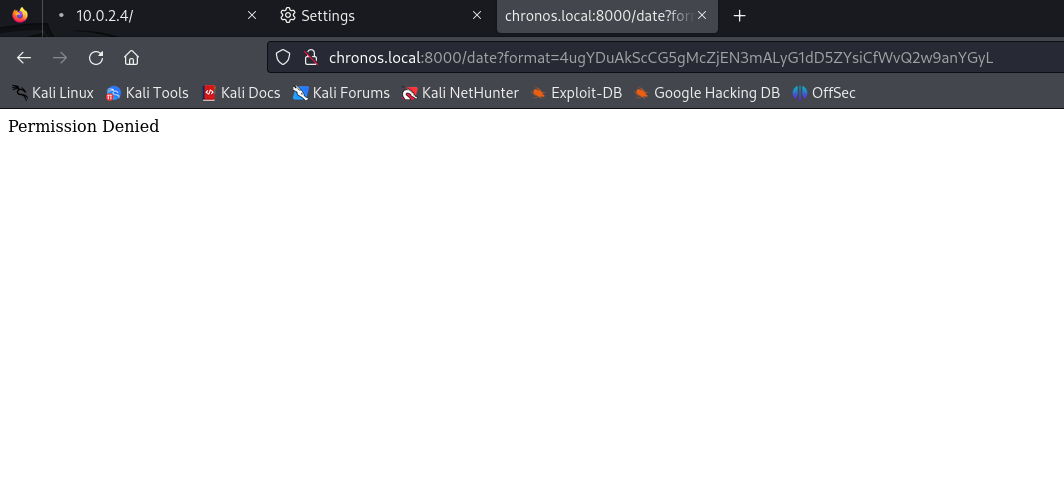
Kết quả chỉ có một hình ảnh, không có gì có thể khai thác. Tiếp theo xem mã nguồn của trang web:



Trong phần response có gợi ý rằng sẽ sử dụng javascript để làm gì đó liên quan đến url là chronos.local có cổng 8000 (có thể thực hiện gọi hoặc chuyển hướng đến nó). Dựa vào những gì nmap quét được máy lab cũng tồn tại một cổng 8000 chạy dịch vụ http, vì vậy vào file /etc/hosts để thêm chronos.local với ip của máy lab:

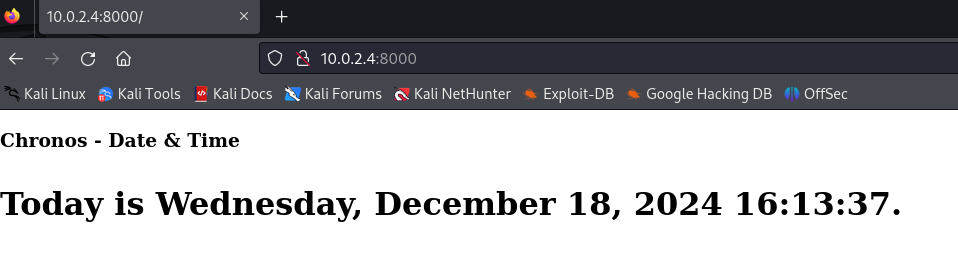


Truy cập vào url đó:

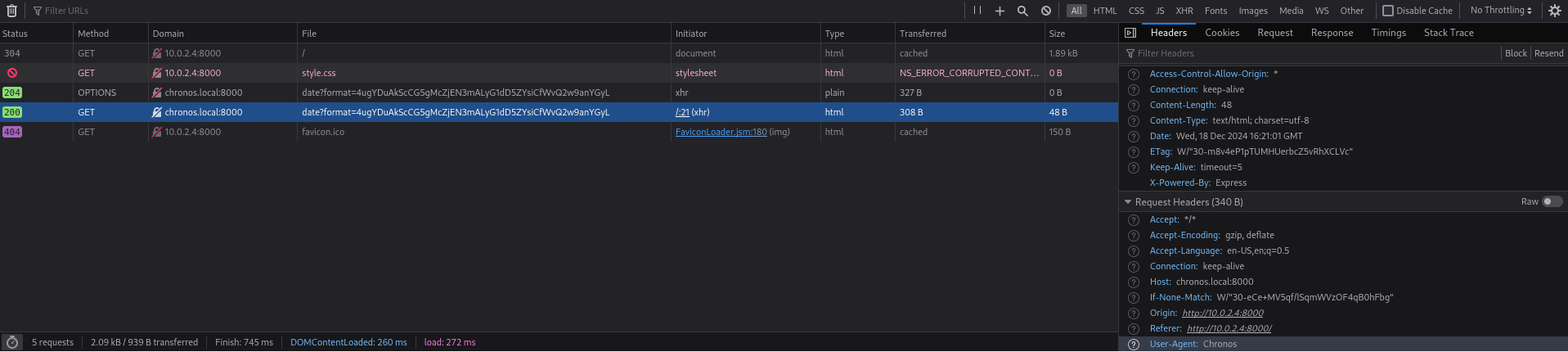


Kết quả trả về cho thấy rằng người dùng ko đủ quyền.

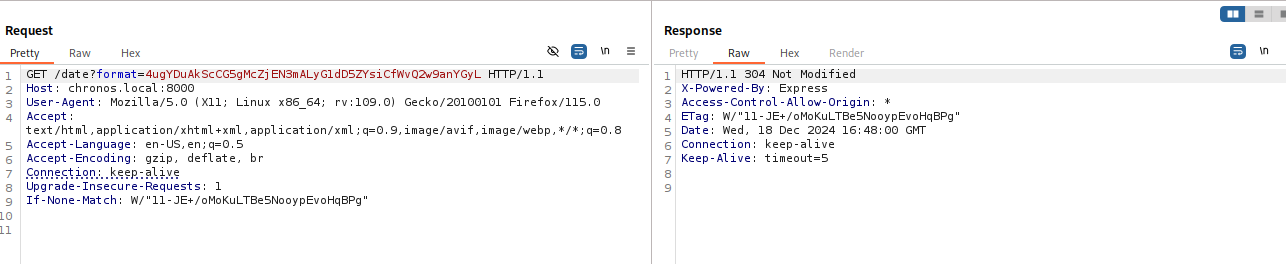
Thử truy cập vào trang web cơ bản:



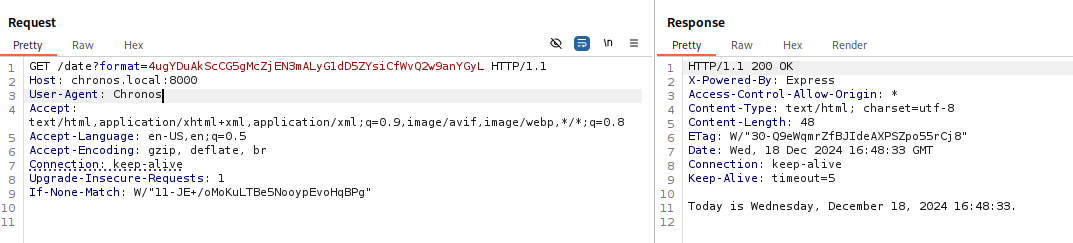
Kết quả trả về cho thấy rằng trang web có chức năng đọc thời gian hiện tại, thực hiện vào network để kiểm tra:



Kết quả cho thấy trang web có thực hiện gửi thêm request đến chronos.local:8000/date?format=4ugYDuAkScCG5gMcZjEN3mALyG1dD5ZYsiCfWvQ2w9anYGyL để thực hiện lấy thông tin về thời gian hiện tại. Ngoài ra user-agent ở đây đc đặt là Chronos chứ ko phải là thông tin của trình duyệt. Thử gửi request tới nó bằng user-agent của trình duyệt

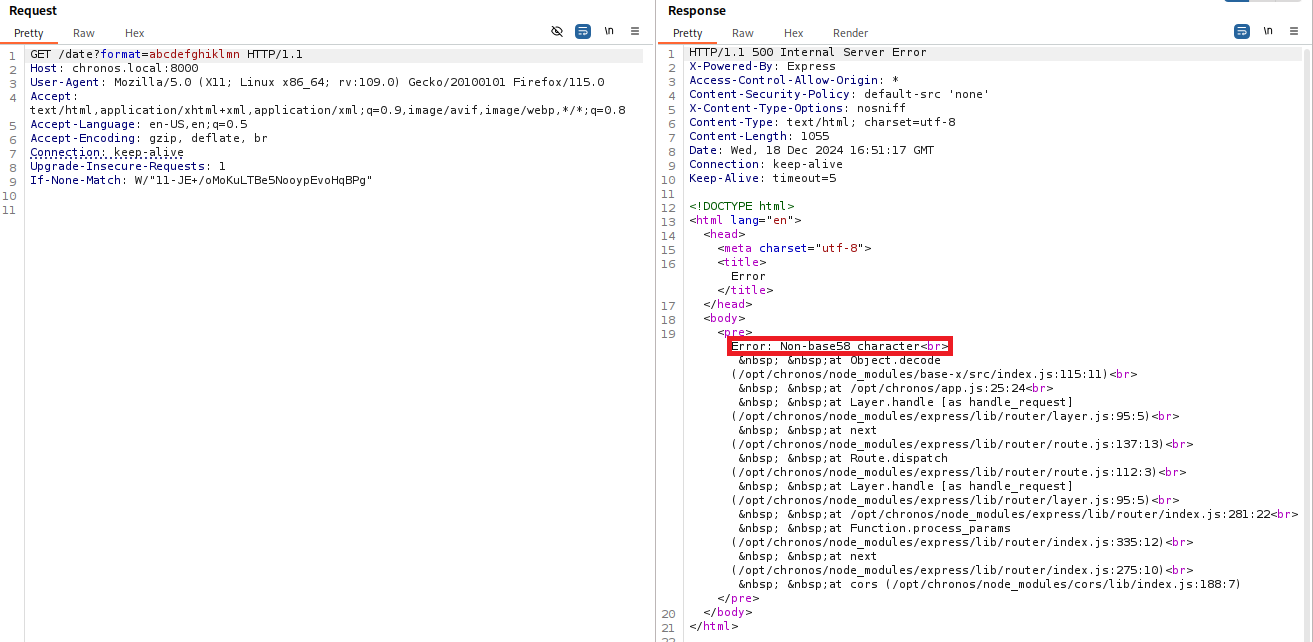


Bằng user-agent là Chronos



Kết qua cho thấy nếu dùng user-agent là chronos thì trang web trả về thông tin về thời gian hiện tại và ngược lại thì là 304 code.

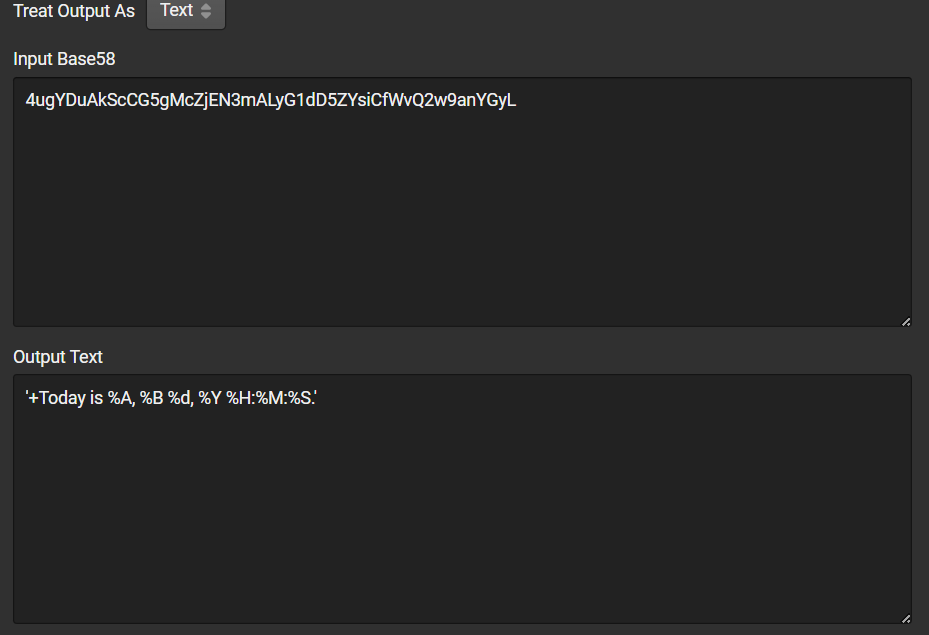
Sau khi liên tục đưa vào một vài kí tự ngẫu nhiên, đã có 1 thông báo lỗi cho biết rằng trang web sử dụng base58:



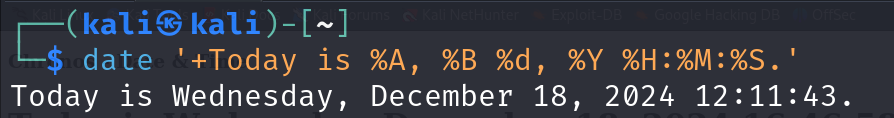
Ngoài ra, sử dụng chuỗi kí tự được gọi đến trong tham số format khi trang web thực hiện gọi đến chronos.local:8000/date?format=4ugYDuAkScCG5gMcZjEN3mALyG1dD5ZysiCfWvQ2w9anYGyL cũng xác định được rằng đây là base58



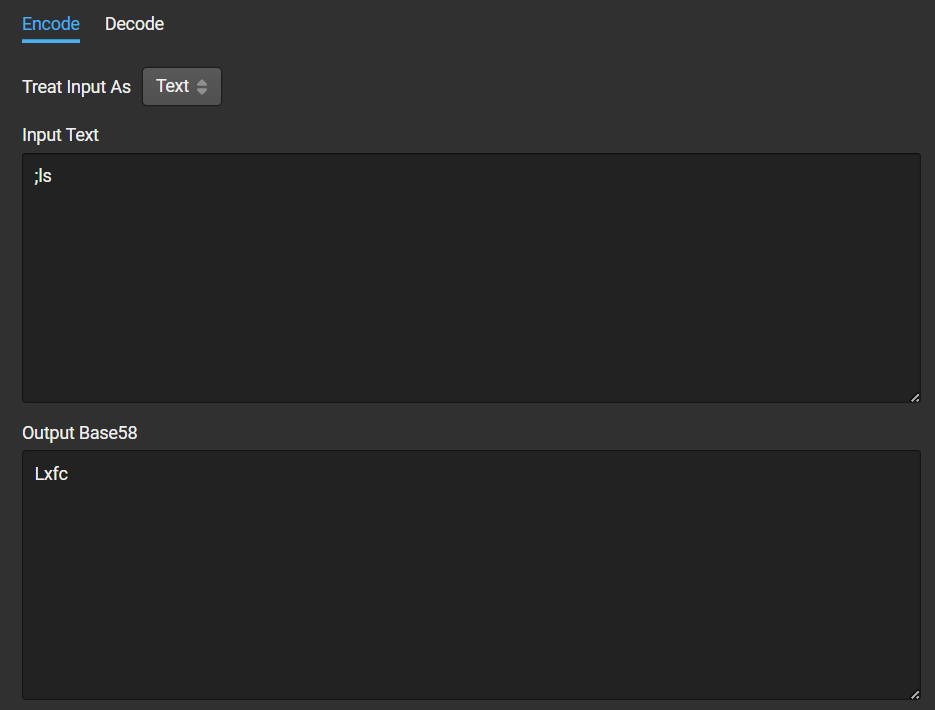
Thực hiện decode nó:

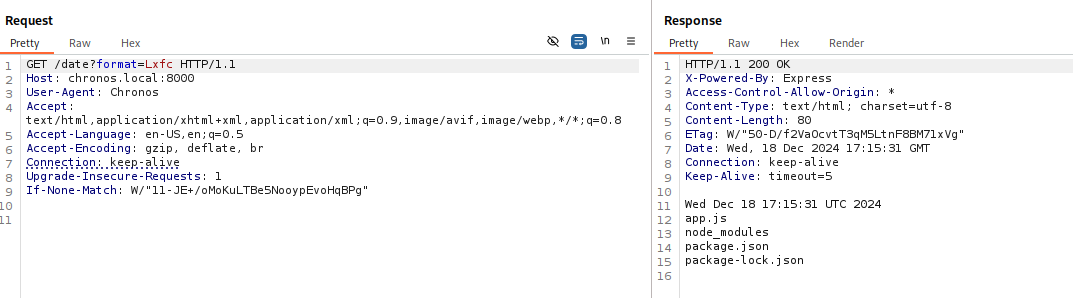


Kết quả trả về cho thấy 1 chuỗi với các tham số liên quan đến ngày tháng năm giờ phút giây, ngoài gia đây là một đối số cho lệnh Linux “date”. Ví dụ, nếu sử dụng lệnh date trên máy kali sẽ có kết quả như sau:



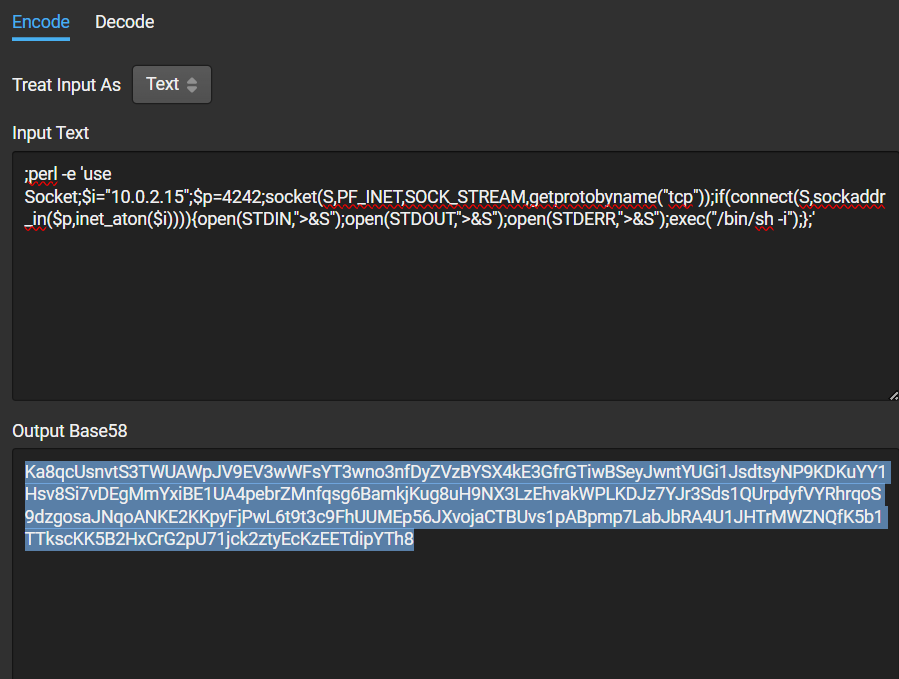
Vì vậy, đây có thể là một vị trí tiềm năng để khai thác command injection, thử thực hiện kiểm tra bằng cách đưa vào một dấu ; và câu lệnh ls, mã hóa base58 cho nó và đưa vào tham số format





Kết quả cho thấy lệnh ls đã được thực thi thành công, điều này chứng minh rằng trang web tồn tại lỗ hổng command injection. Tiếp đó, có thể thực hiện reverse shell bằng cách sử dụng lần lượt các câu lệnh reverse shell trên các trang chear sheet, sau 1 hồi thì mình cũng đã tìm thấy đc 1 câu lệnh và thực thi thành công.

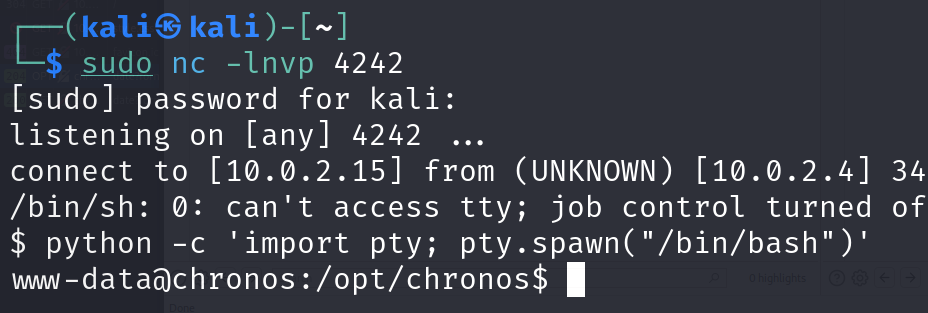
Mã hóa base58:



Đưa vào tham số format:

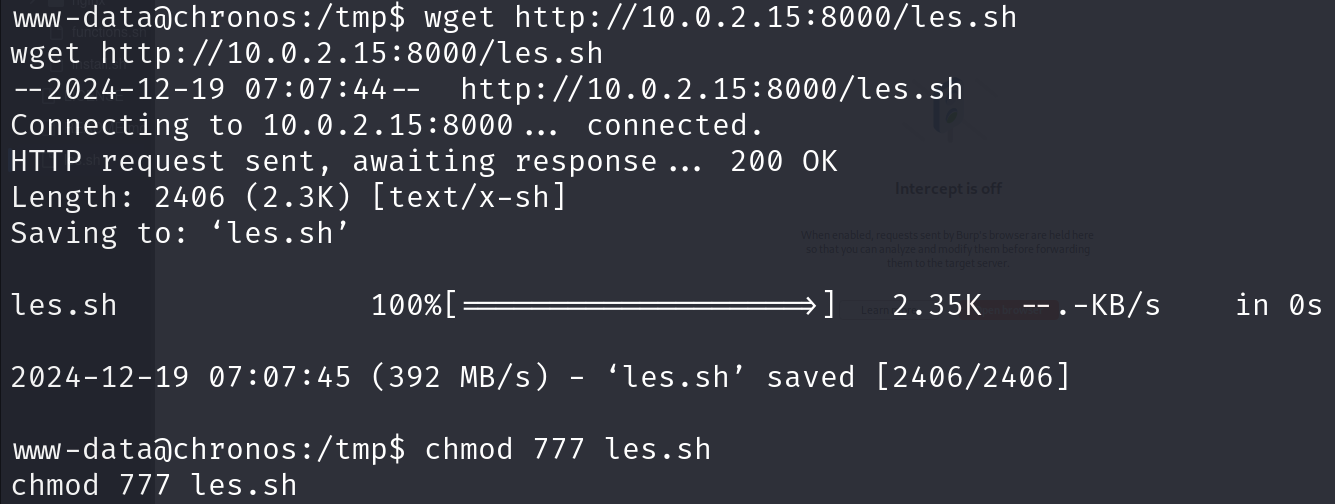


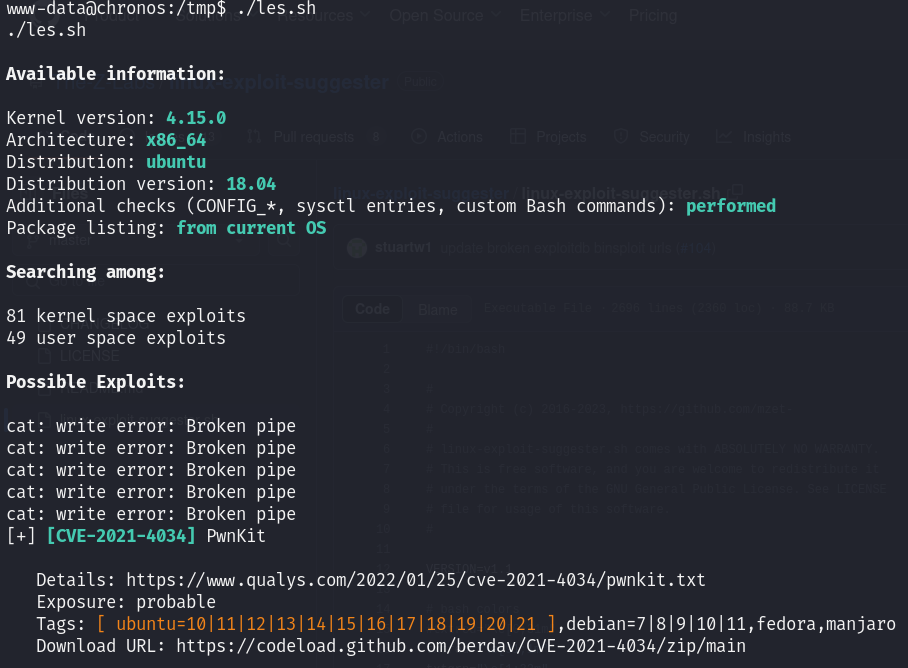
Vào shell thành công và nâng cấp shell:

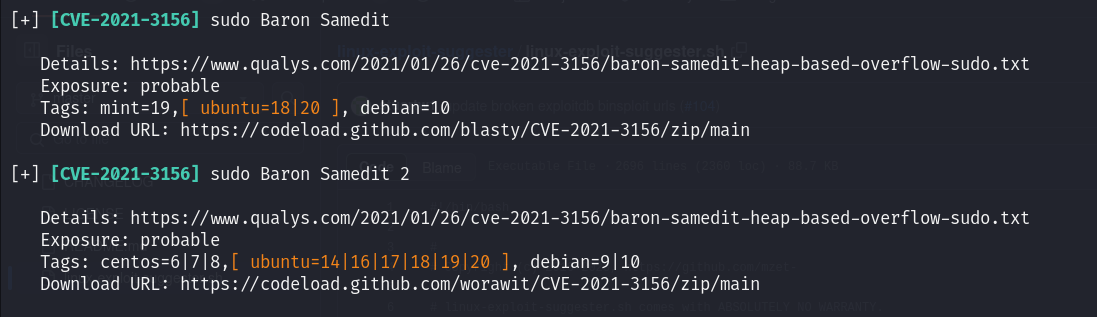


\* **Leo thang đặc quyền bằng file exploit**

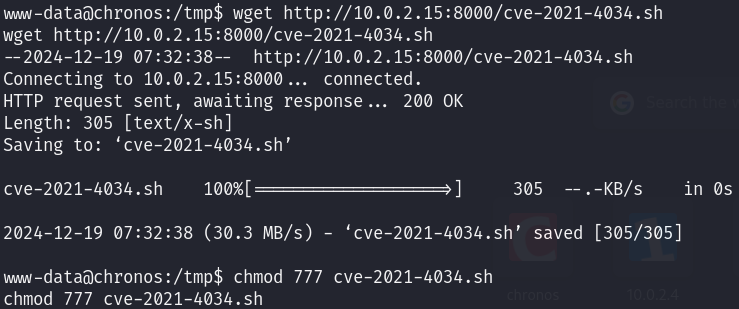
Sử dụng file les.sh, đây là một file có khả năng kiểm tra phiên bản của kernel và đưa ra các cve đã phát hiện của phiên bản đó để có thể thực hiện khai thác:



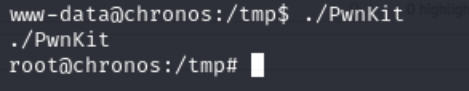




Sau khi chạy và xem xét thì chọn CVE 2021 4034 PWNKIT để thực hiện khai thác, Tải về máy kali và gửi nó qua máy lab:

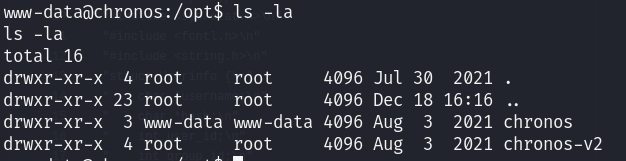


Thực thi file và thành công vào root:

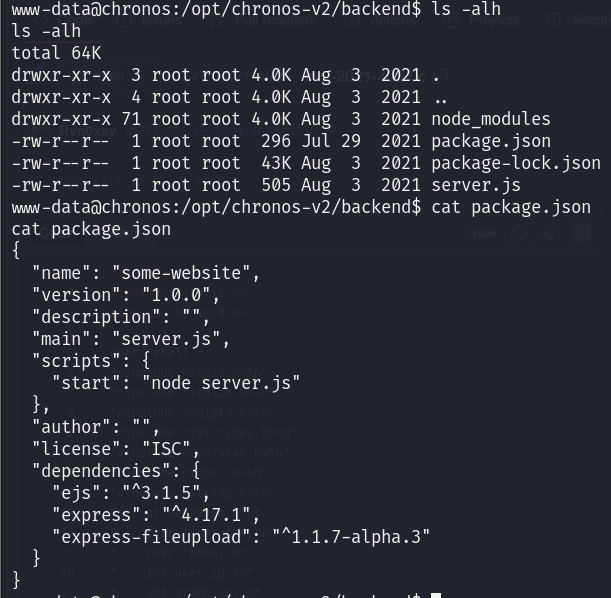


\* **Cách leo thang đặc quyền thứ 2 :**

Lùi ra khỏi thư mục hiện tại thì thấy còn một thu mục khác nữa mang tên v2:



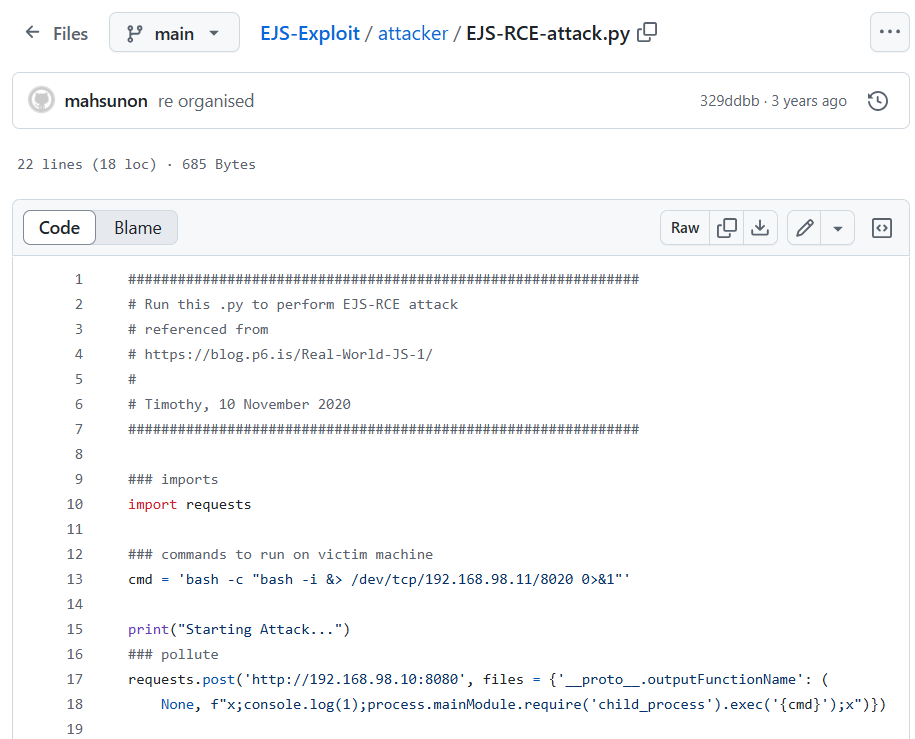
Truy cập vào trong và đọc các file trong đó thì tìm thấy thông tin liên quan đến express-fileupload phiên bản 1.1.7:

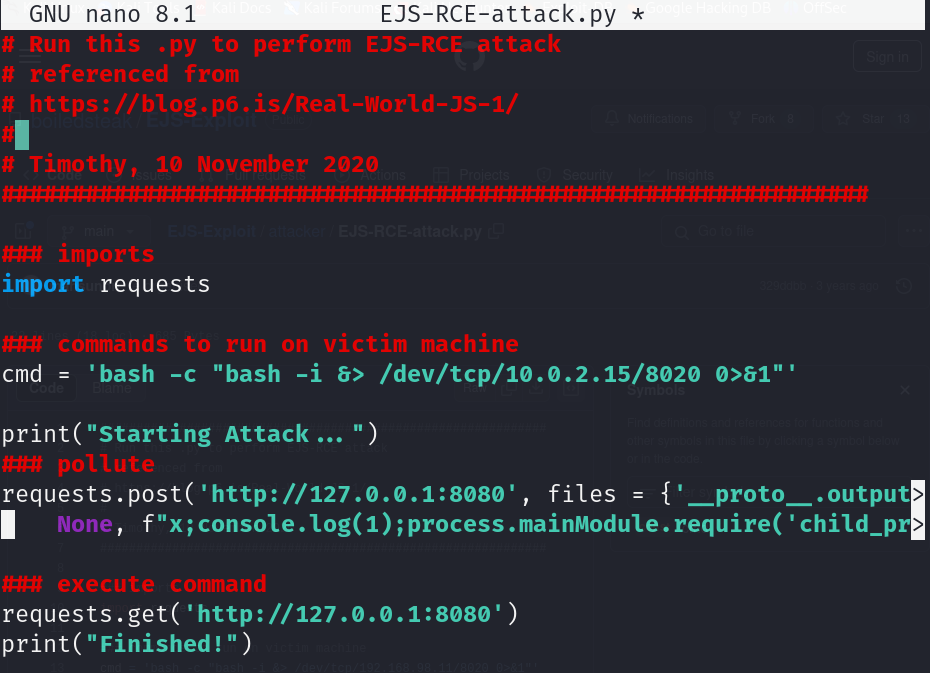


Sau một hồi tìm kiếm thì phát hiện 1 cve liên quan tới rce với phiên bản 1.1.8 trở xuống:

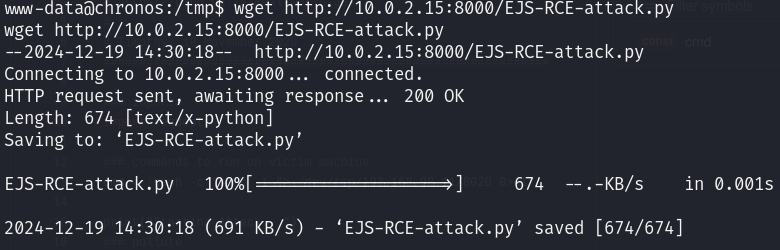


Tìm kiếm file khai thác và lưu nó vào kali:

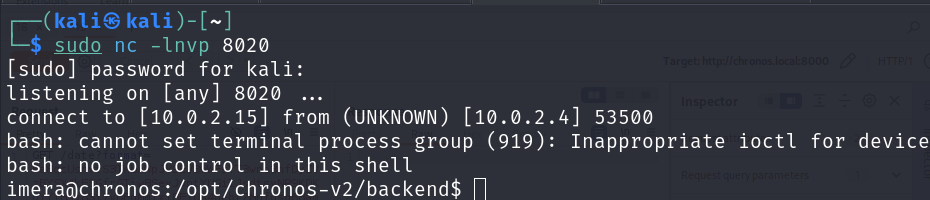




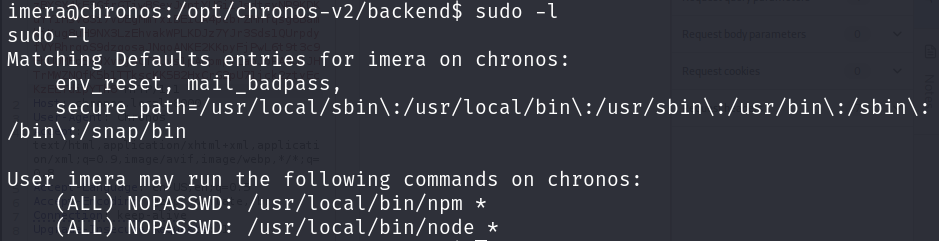
Đưa file khai thác sang máy target:



Thực hiện file khai thác và truy cập thành công vào shell của user khác tên là imera:

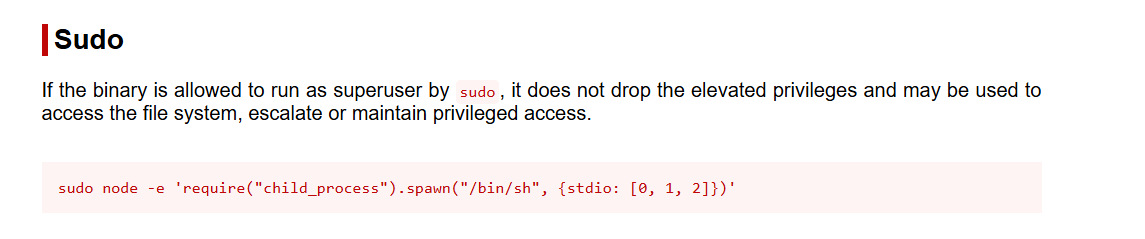


Sử dụng sudo -l để xem các quyền:

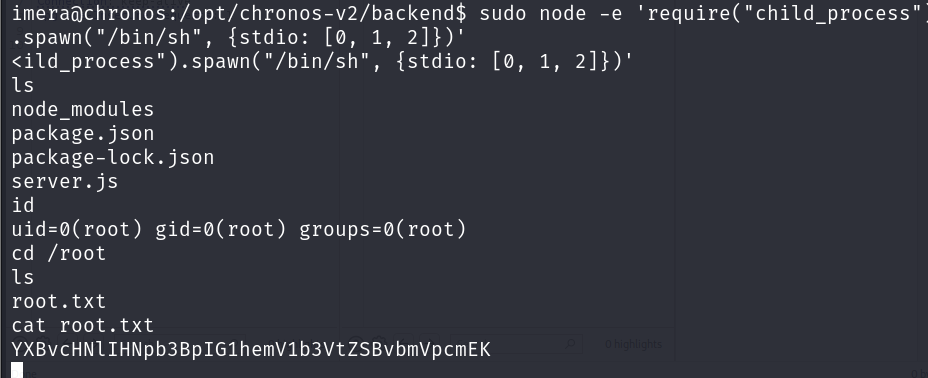


Kết quả trả về cho thấy người dùng imera có thể thực thi 2 lệnh là node và npm dưới quyền sudo mà ko cần mật khẩu.

Thực hiện tìm kiếm và phát hiện có cách leo thang đặc quyền qua node với quyền sudo:



Thực hiện theo hướng dẫn và thanh công lên được root:



1. **Kết quả**

Attacker leo được lên quyền root và lấy được flag tại file root.txt trong thư mục /root

