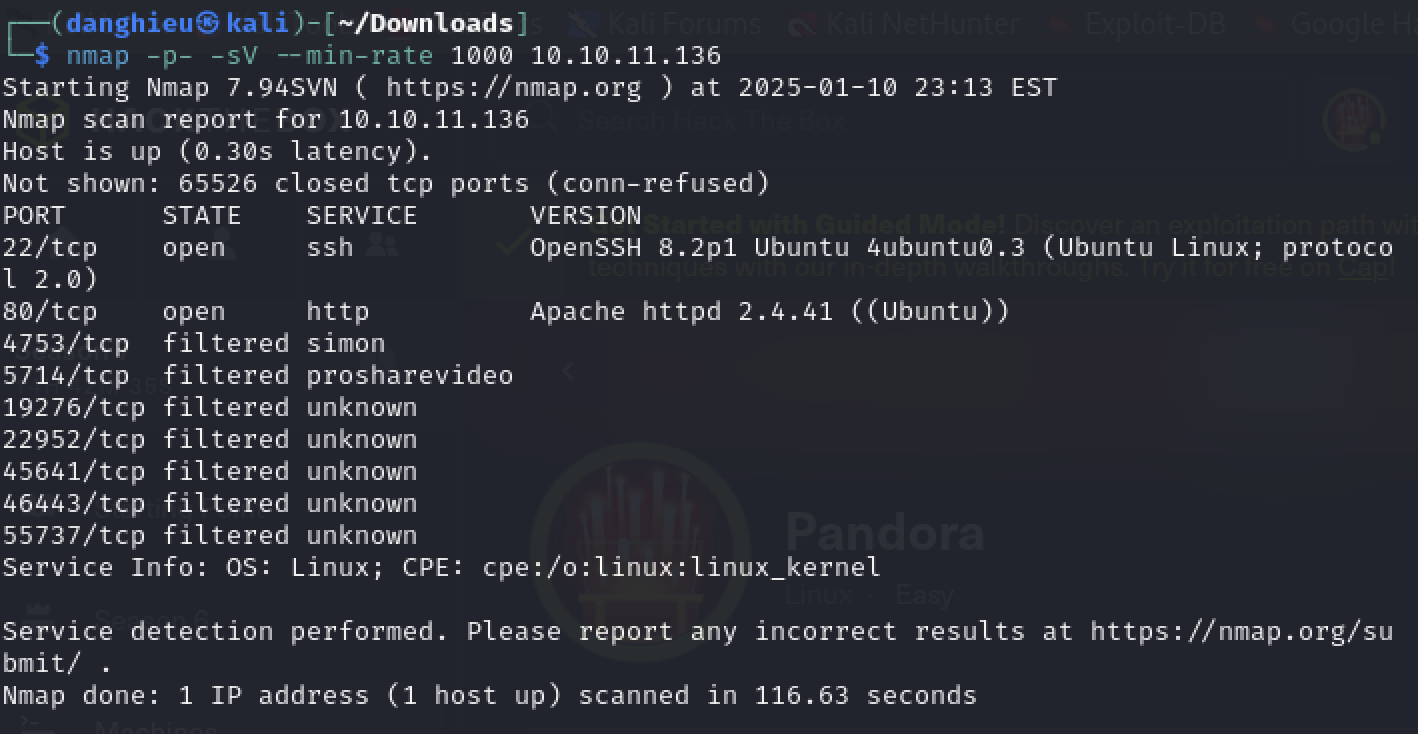
**Network**

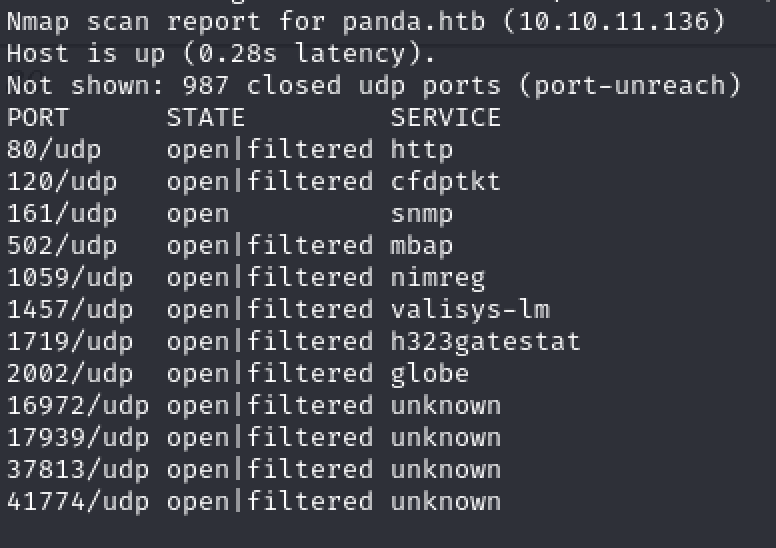


Thấy có hai dịch vụ lạ đang chạy: simon và prosharevideo

Nếu chúng ta đã làm hết các bước liệt kê mạng nhưng vẫn không tìm được manh mối để khai thác, có thể chúng ta đã bỏ qua các cổng UDP.

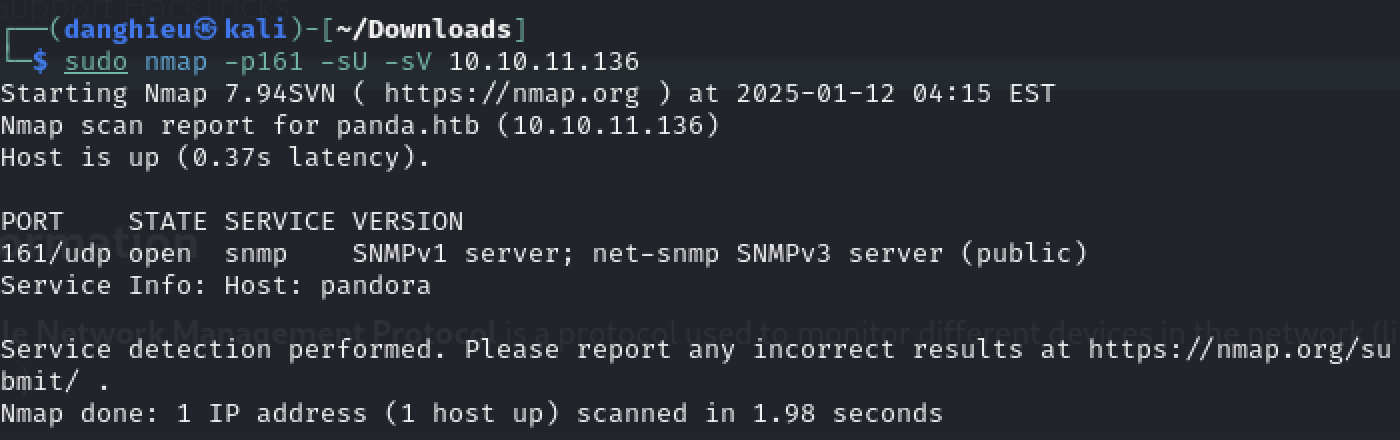
Mở rộng thêm: quét các cổng UDP

sudo nmap -sU 10.10.11.136



Phát hiện dịch vụ snmp chạy ở cổng 161

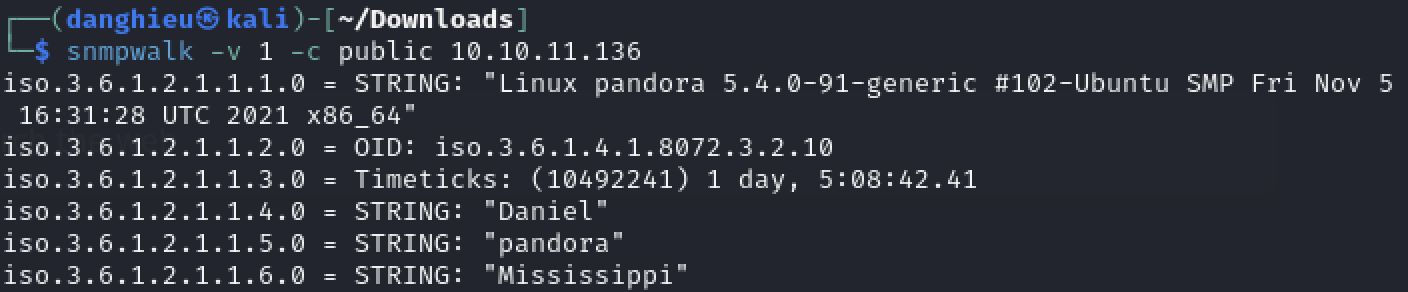
SNMP - Simple Network Management Protocol là 1 giao thức dùng để theo dõi các thiết bị khác nhau trong mạng (như routers, switches, máy in và IoTs)



SNMP có rất nhiều thông tin nhạy cảm về máy chủ như các giao diện mạng (IPv4 và IPv6), tên người dùng, phiên bản của hệ điều hành và các tiến trình đang chạy (có thể chứa mật khẩu).

Liệt kê dịch vụ SNMP:

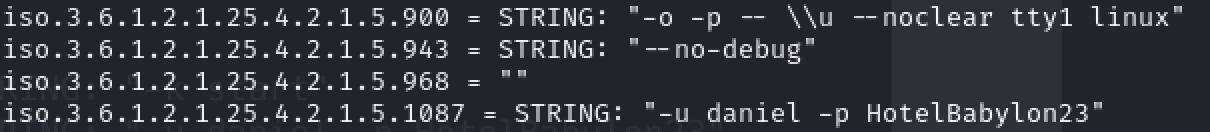
snmpwalk -v 1 -c public 10.10.11.136



Phiên bản của hệ điều hành: Linux pandora 5.4.0-91-generic #102-Ubuntu SMP Fri Nov 5 16:31:28 UTC 2021 x86\_64

Tên người dùng: Daniel, pandora, Mississippi

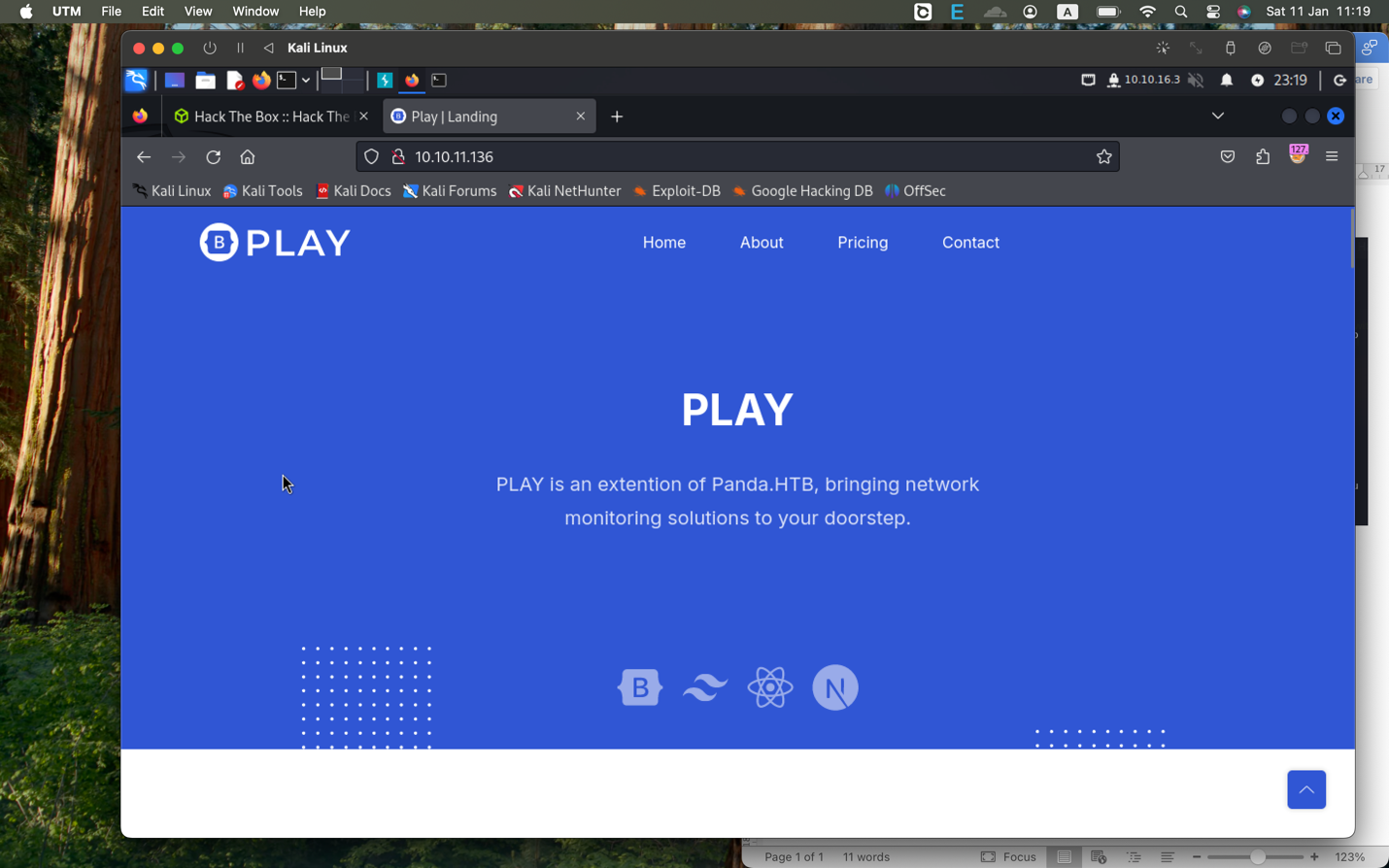
Phải đợi nó quét khá lâu mới tìm được mật khẩu của Daniel:



daniel : HotelBabylon23

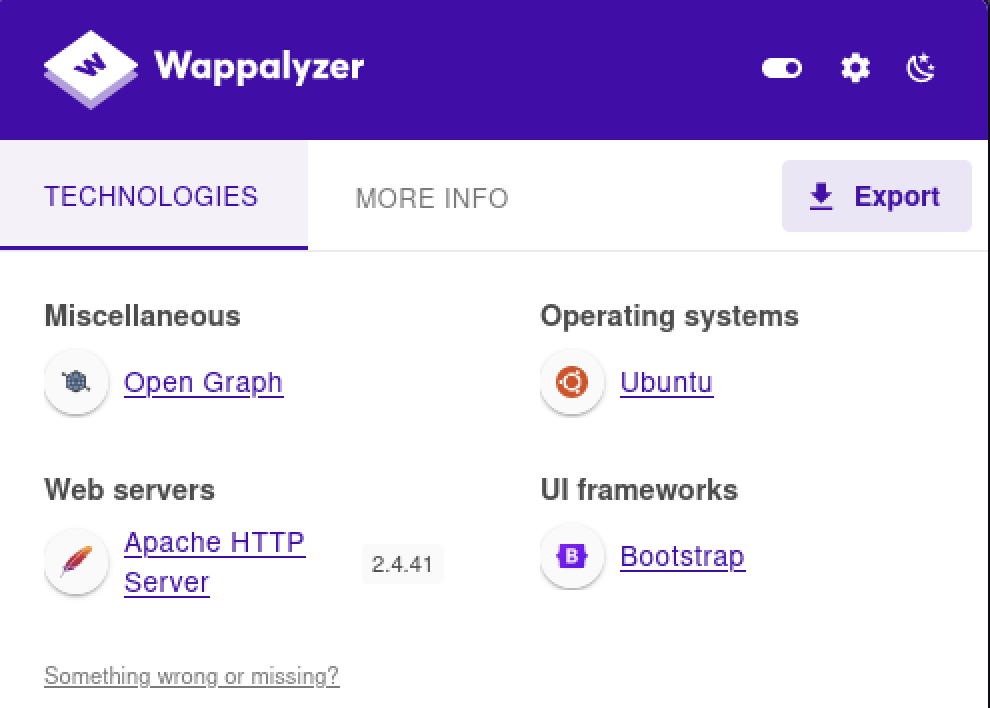
**Web**

Giao diện trang web:

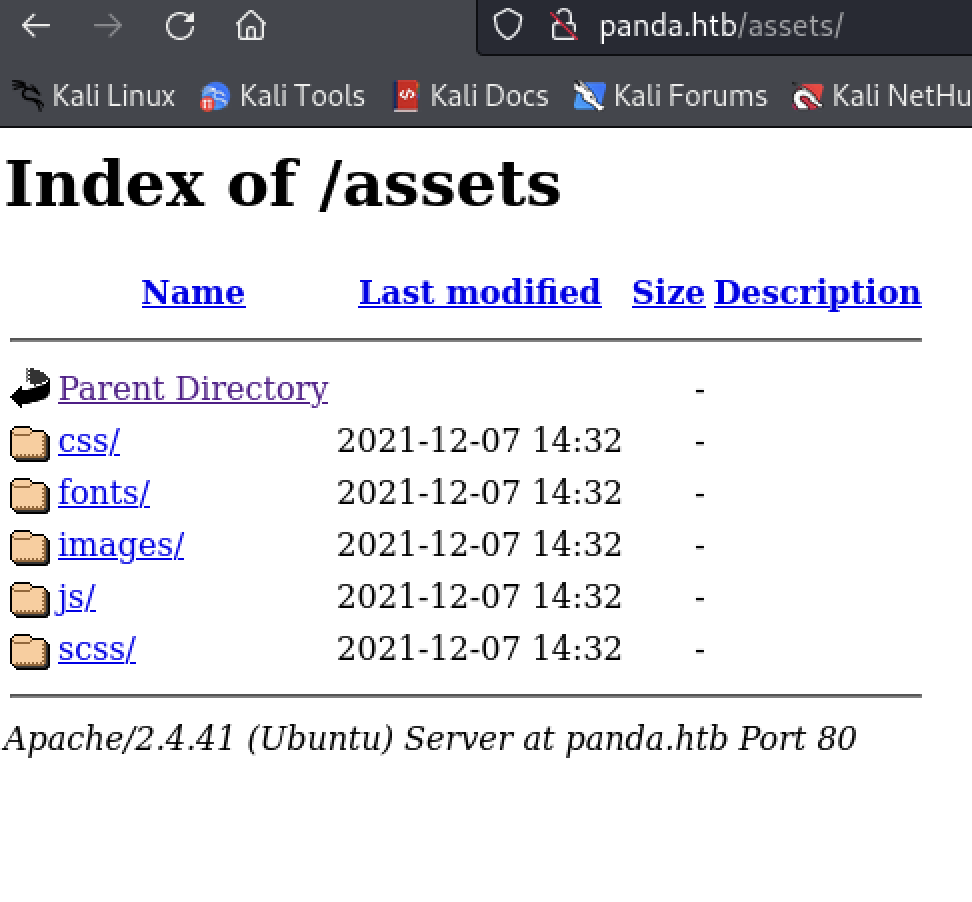




Công nghệ mà trang web sử dụng:



Lỗi hiển thị thư mục



support@panda.htb

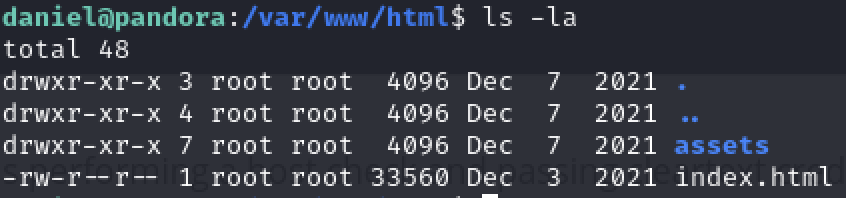
contact@panda.htb

Mình không tìm được đầu vào có thể tấn công trên trang web

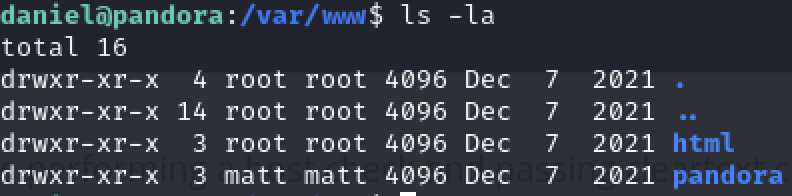
ssh daniel@10.10.11.136

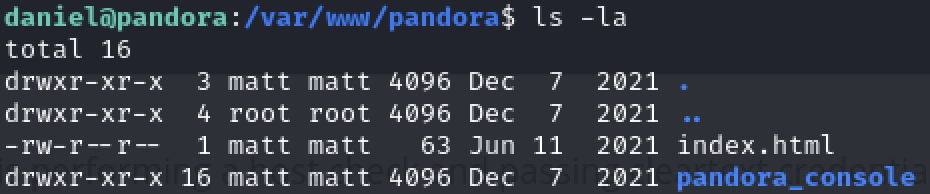


Trang web nhìn đơn giản quá



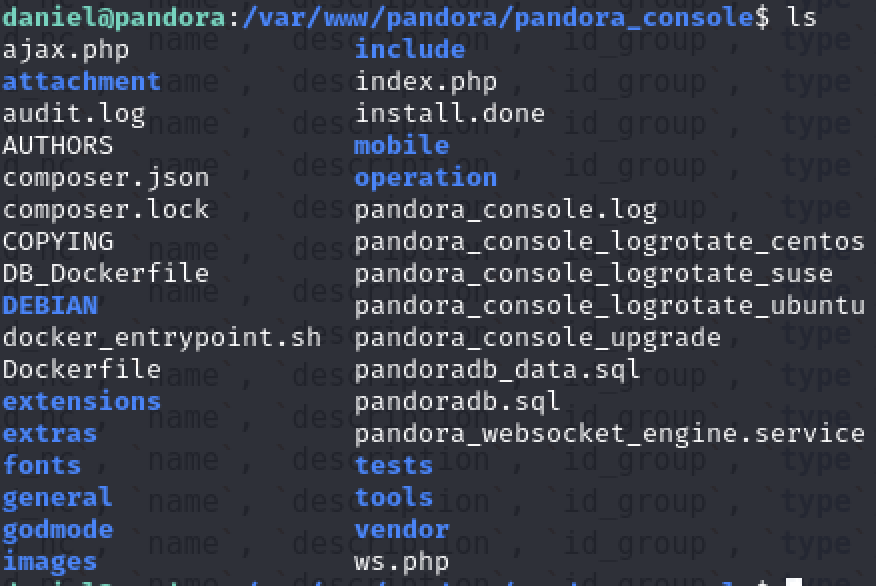
Thư mục pandora nhìn có vẻ thú vị

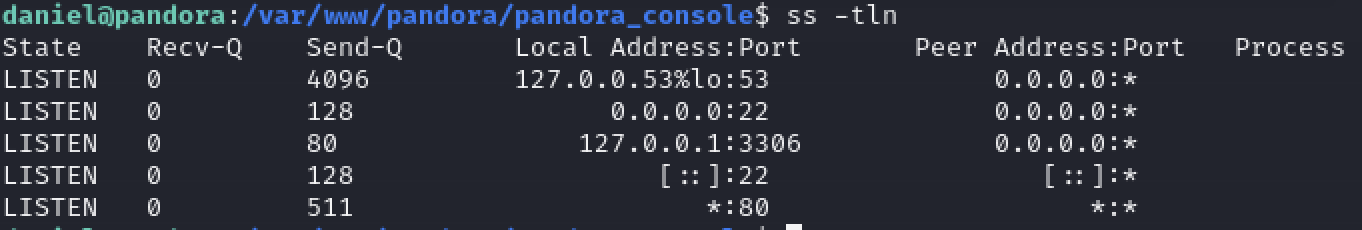




Có 1 số tập tin nhạy cảm trong thư mục pandora\_console

Giống 1 trang web đang hoạt động ngầm





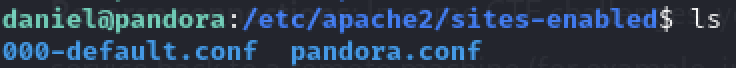
Địa chỉ 127.0.0.1; localhost: các cổng chỉ lắng nghe cục bộ trong máy ảo và không thể truy cập từ bên ngoài. Điều này giải thích tại sao Nmap không phát hiện được.

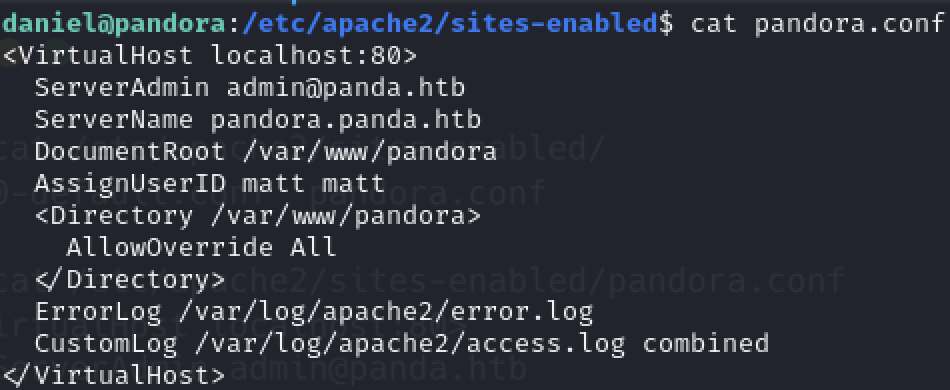
Địa chỉ 0.0.0.0 và [::] chỉ ra 1 cổng đang lắng nghe trên tất cả giao diện mạng, có thể truy cập từ bên ngoài

Thường chúng ta chỉ cần kiểm tra kết nối mạng bằng công cụ ss là biết có cần local port forwarding không. Nhưng trong trường hợp này thì hơi khó.

Kiểm tra cấu hình vhosts của máy chủ web (apache2) ở /etc/apache2/sites-enabled

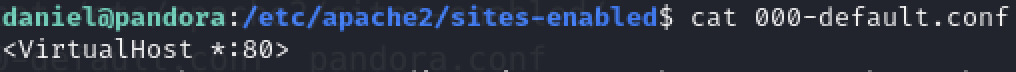
Có 2 tệp cấu hình ở đây: 1 cái mặc định và pandora.conf





Trang web đang chạy ở localhost:80 (chạy nội bộ)

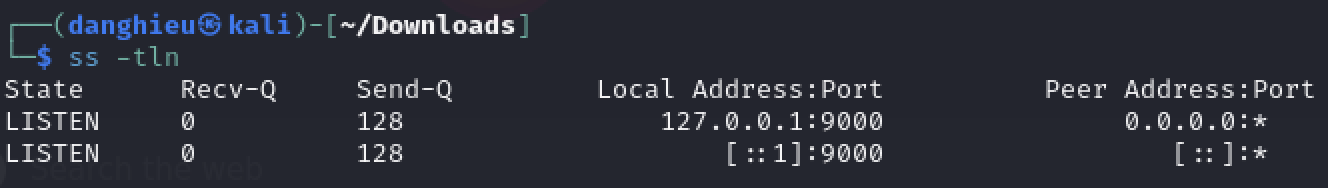
Còn mặc định lắng nghe trên tất cả giao diện mạng, có thể truy cập từ bên ngoài



Để truy cập được dịch vụ web đang chạy nội bộ, mình dùng kĩ thuật local port forwarding, chạy ở máy khách

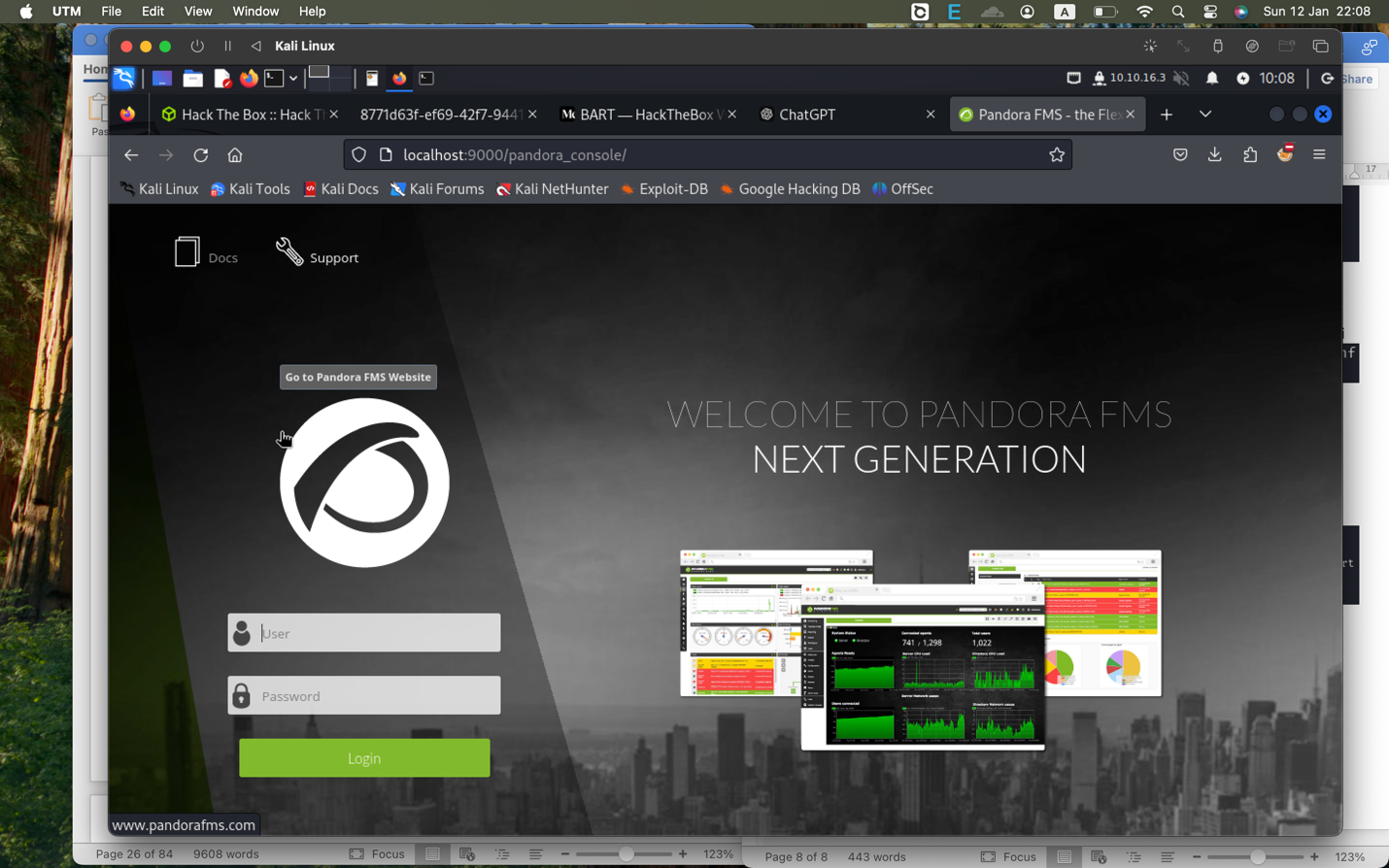
ssh daniel@10.10.11.136 -L 9000:127.0.0.1:80

Kiểm tra kết nối mạng ở máy khách, mình sẽ thấy cổng 9000 đang được mở



Bạn có thể truy cập được trang web Pandora bằng localhost:9000

Giao diện trang web:



Mình tìm được phiên bản của pandora fms là v7.0NG.742\_FIX\_PERL2020

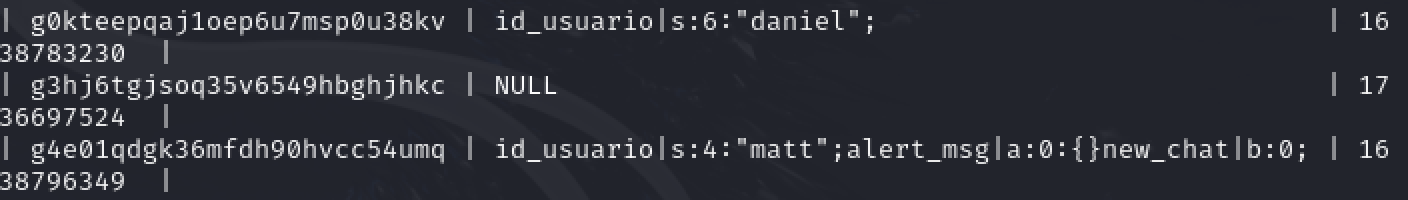
Bài này mình phải dùng rất nhiều CVE khác nhau để khai thác, nó xoay cho mình chóng mặt luôn

Mình biết có 1 lỗ hổng SQL Injection ở http://localhost:9000/pandora\_console/include/chart\_generator.php?session\_id=1

Mình có thể khai thác mà không cần xác thực

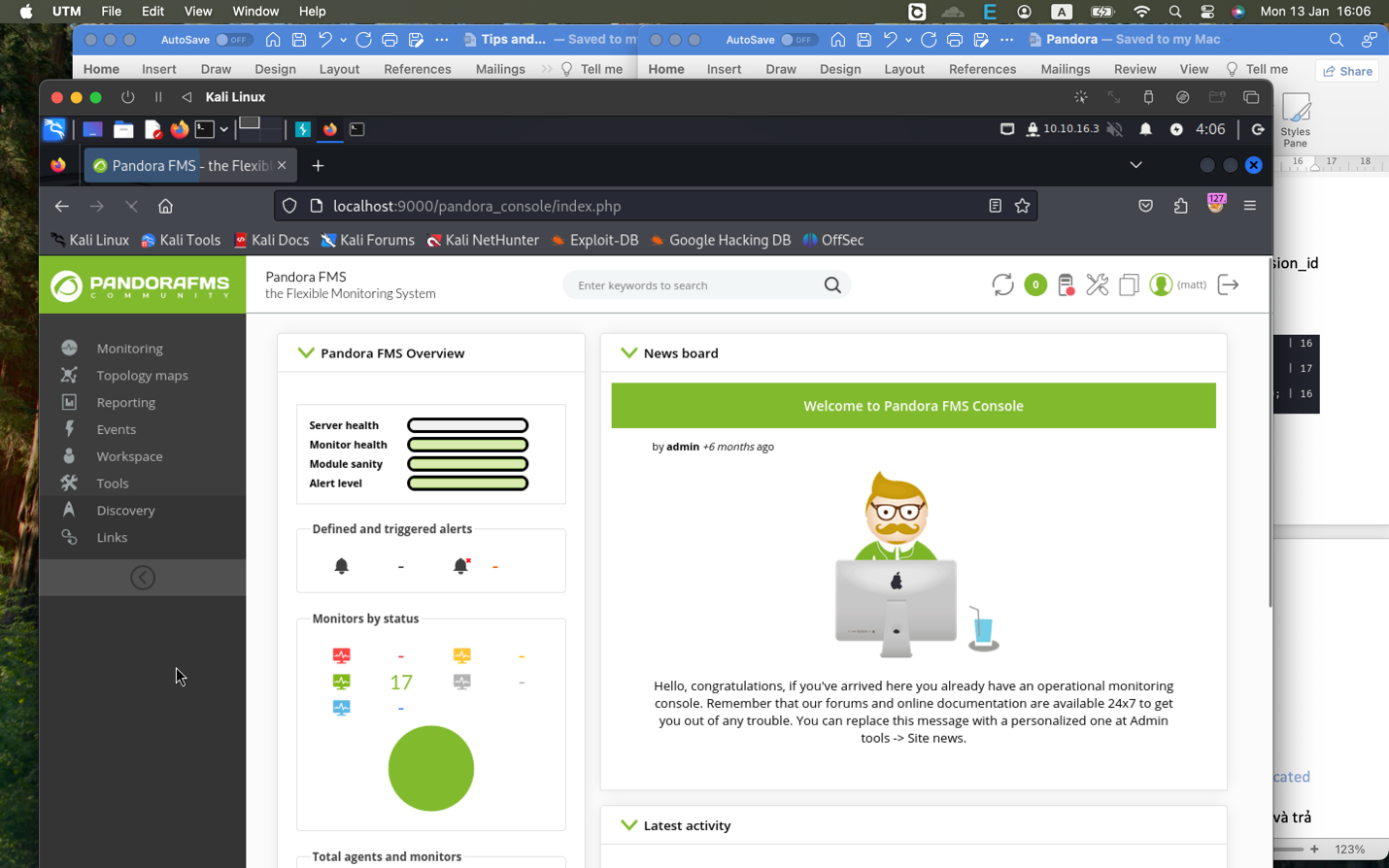
Cơ sở dữ liệu là pandora và bảng tsessions\_php

sqlmap -u "http://localhost:9000/pandora\_console/include/chart\_generator.php?session\_id=atnepnoh9ab0v84u1u2eqgup79" --threads=10 --dump -D pandora -T tsessions\_php



Bạn chỉ cần chỉnh sửa Cookie trong BurpSuite là đăng nhập được

Giao diện trang web

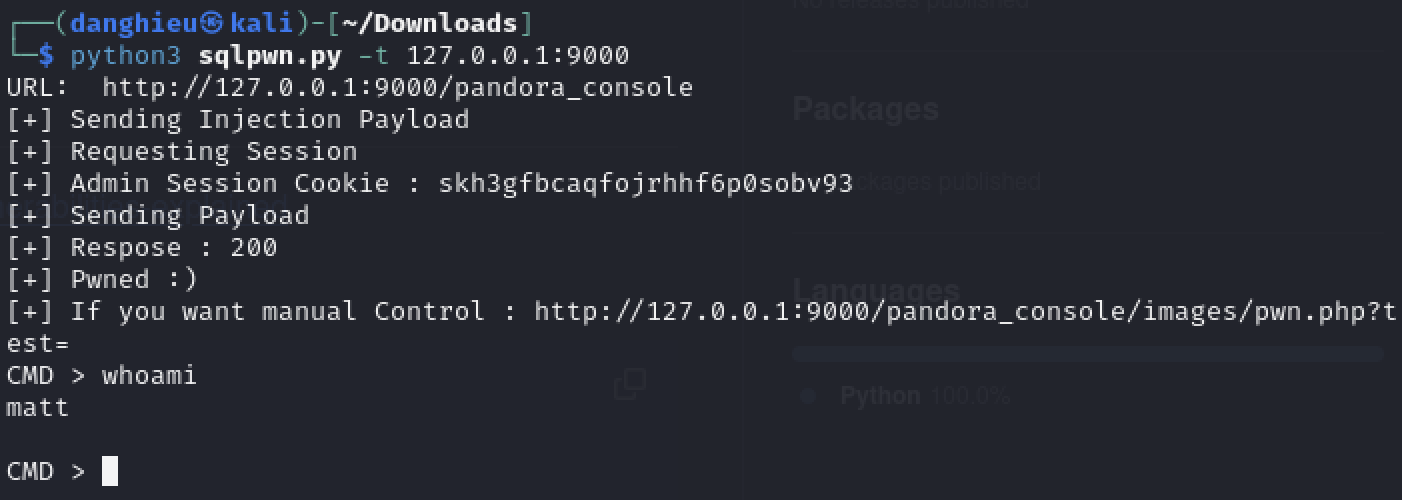


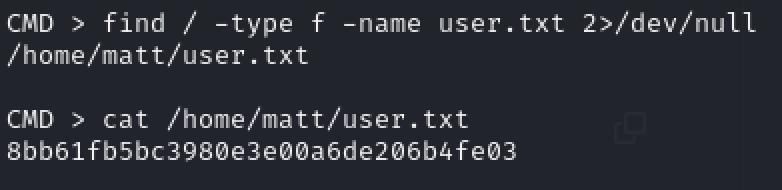
Người dùng matt bị hạn chế upload file nên mình không tìm được cách lấy file. Tìm kiếm khai thác thứ hai

Cũng lỗ hổng đó, nhưng lần này mình lấy được Cookie của admin nên reverse shell luôn

https://github.com/shyam0904a/Pandora\_v7.0NG.742\_exploit\_unauthenticated

Sql injection không cần xác thực có thể đẩy cơ sở dữ liệu, mạo danh Admin và trả về 1 shell tương tác

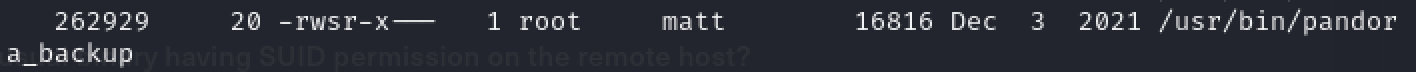




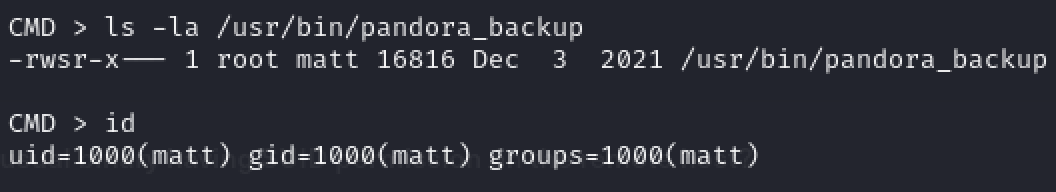
Tìm các tệp nhị phân có đặc quyền suid của root:

find / -type f -perm -04000 -ls 2>/dev/null

Mình tìm được 1 tập tin đáng nghi:



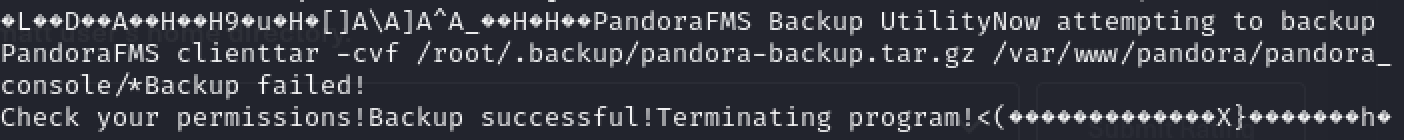
Người dùng matt có quyền đọc và thực thi tệp pandora\_backup



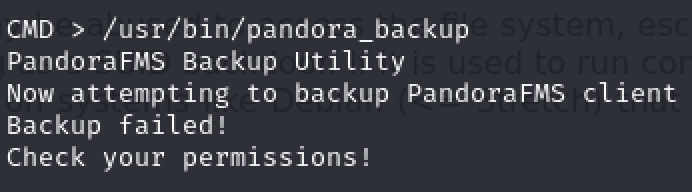
Đọc thử tệp thực thi trên

Nó đang muốn sao lưu thư mục /var/www/pandora/pandora\_console/\*

tar -cvf /root/.backup/pandora-backup.tar.gz /var/www/pandora/pandora\_console/\*



Khi chạy thử tệp nhị phân, chúng ta thấy lỗi sau:



Lỗi về đặc quyền không truy cập được tập tin trong thư mục root. Nhưng tệp nhị phân có đặc quyền SUID của root, phải chạy được chứ. Lỗi có thể nằm ở shell bị giới hạn.

Chúng ta có thể dùng tệp nhị phân /usr/bin/at để thoát khỏi shell bị giới hạn

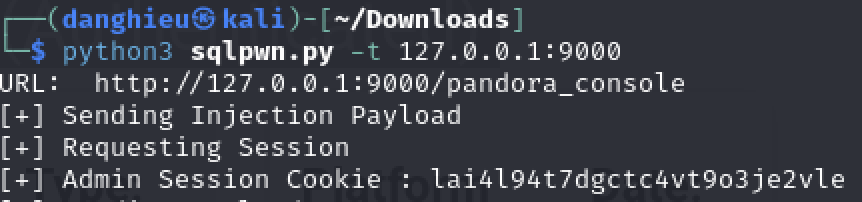
echo "/bin/sh <$(tty) >$(tty) 2>$(tty)" | at now; tail -f /dev/null

Shell do CVE lấy được không chạy được lệnh trên.

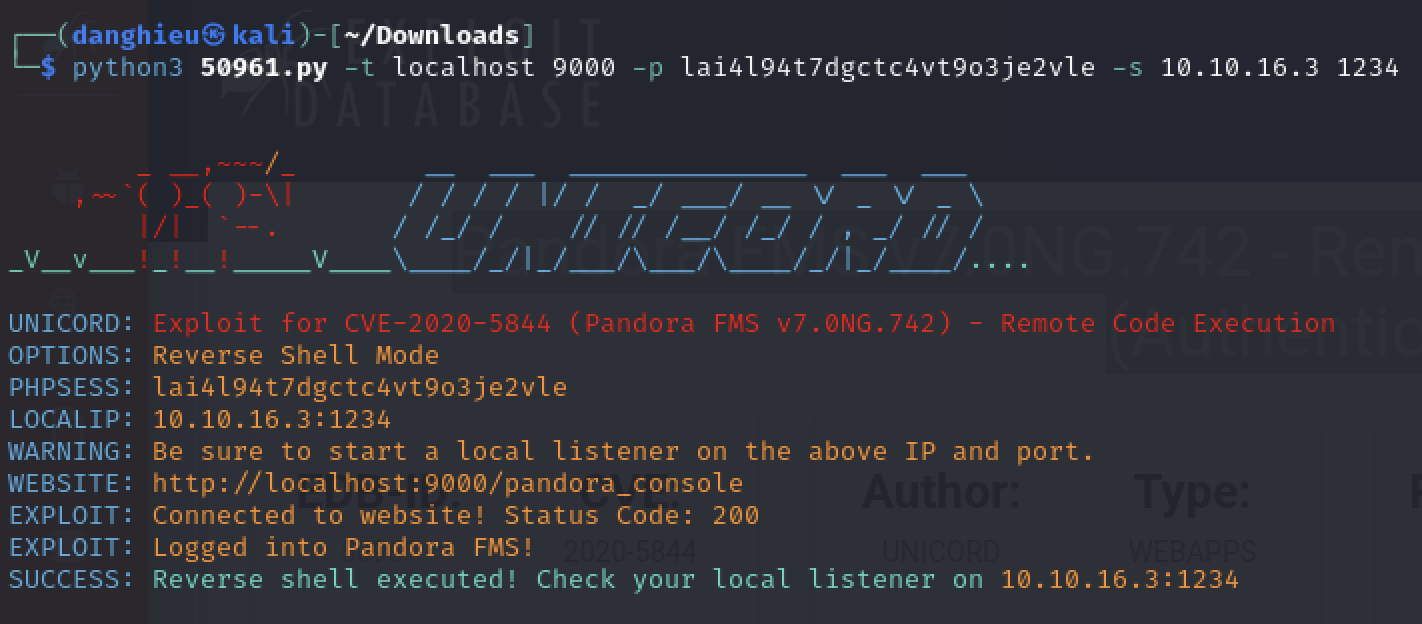
Mình muốn reverse shell bằng php cũng không được nên mình quyết định dùng 1 CVE khác

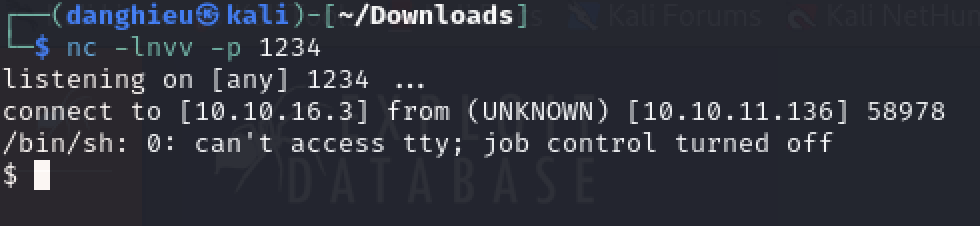
CVE-2020-5844 cho phép bạn thực thi lệnh từ xa nhưng yêu cầu phải xác thực (người dùng là quản trị viên)

Mình sẽ lấy cookie của admin ở CVE trước để khai thác

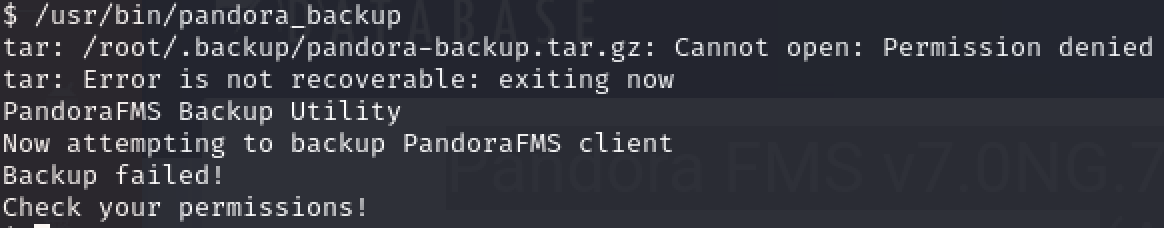


Admin Session Cookie : lai4l94t7dgctc4vt9o3je2vle



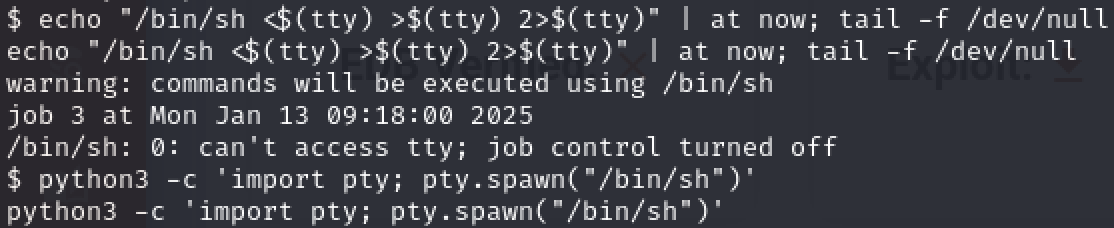


Dĩ nhiên, chúng ta chạy tệp thực thi pandora\_backup vẫn bị lỗi



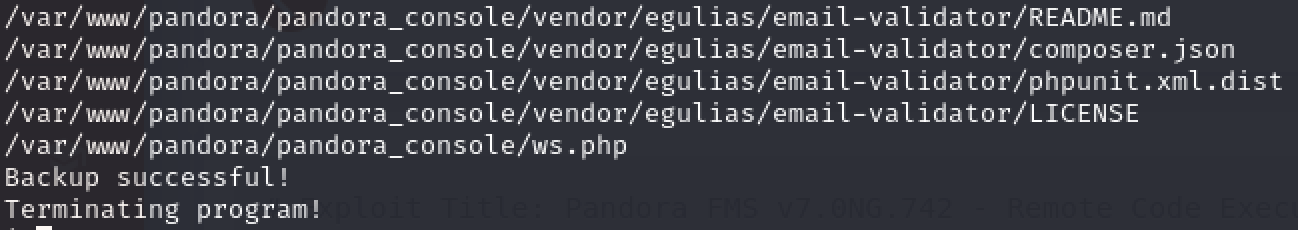
Nhưng ở shell mới, chúng ta có thể bật interactive mode:

echo "/bin/sh <$(tty) >$(tty) 2>$(tty)" | at now; tail -f /dev/null



Chạy lại tệp thực thi pandora\_backup

Nó đã backup thành công

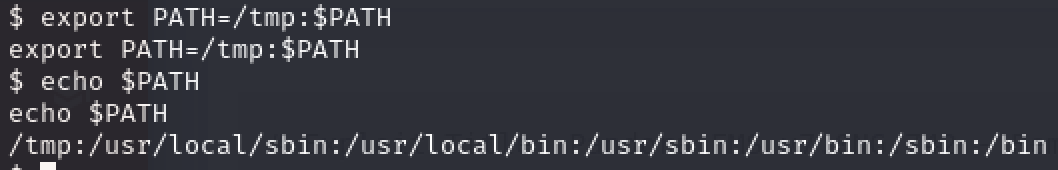


**Privilege Escalation**

Tệp thực thi pandora\_backup thực thi lệnh tar dưới quyền root nhưng đường dẫn không rõ ràng.

tar -cvf /root/.backup/pandora-backup.tar.gz /var/www/pandora/pandora\_console/\*

Để xem, chúng ta có chỉnh sửa được biến môi trường PATH không



Chúng ta sẽ thêm tệp nhị phân tar vào thư mục /tmp

Chỉnh sửa như nào để nhận được shell của root, vì tar được thực thi với nhiều đối số??

