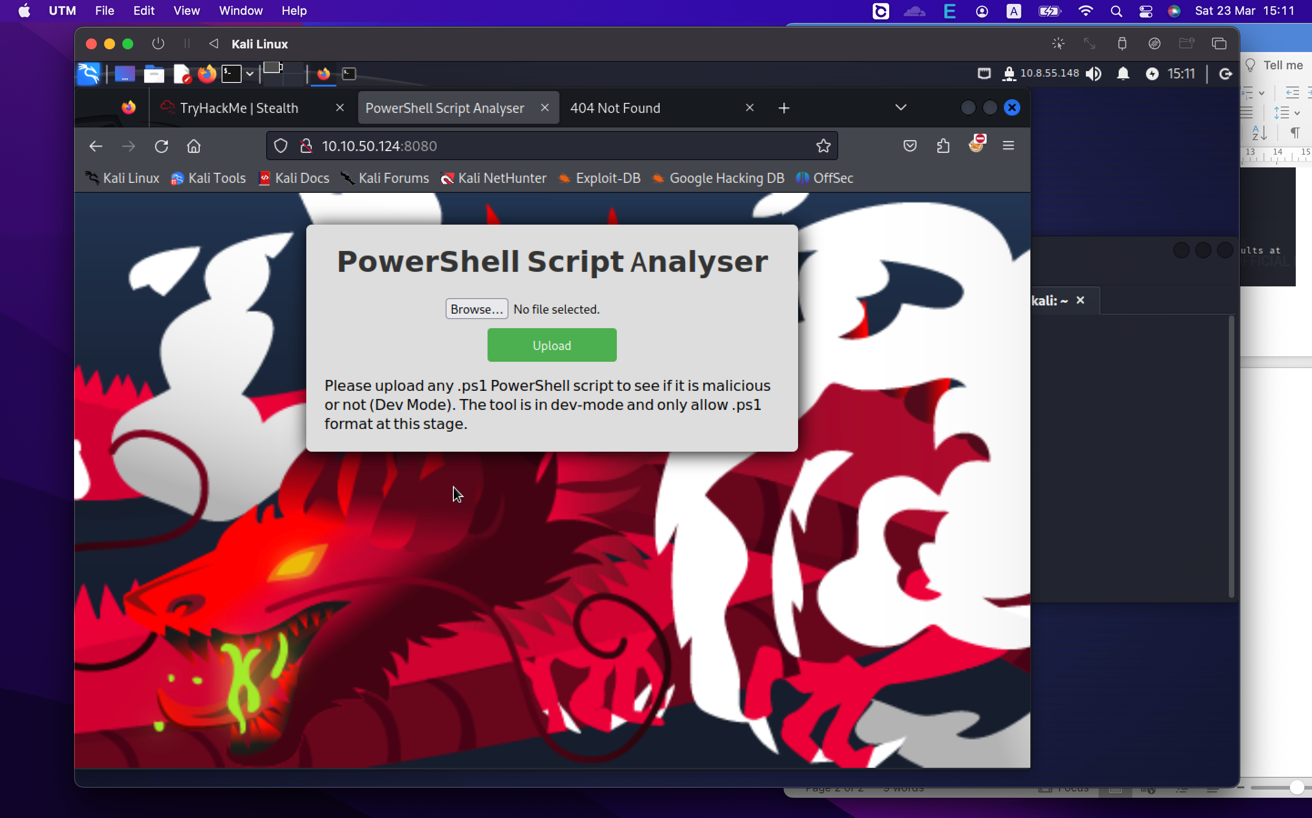
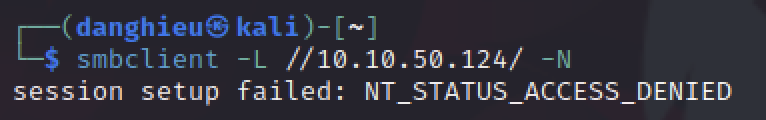
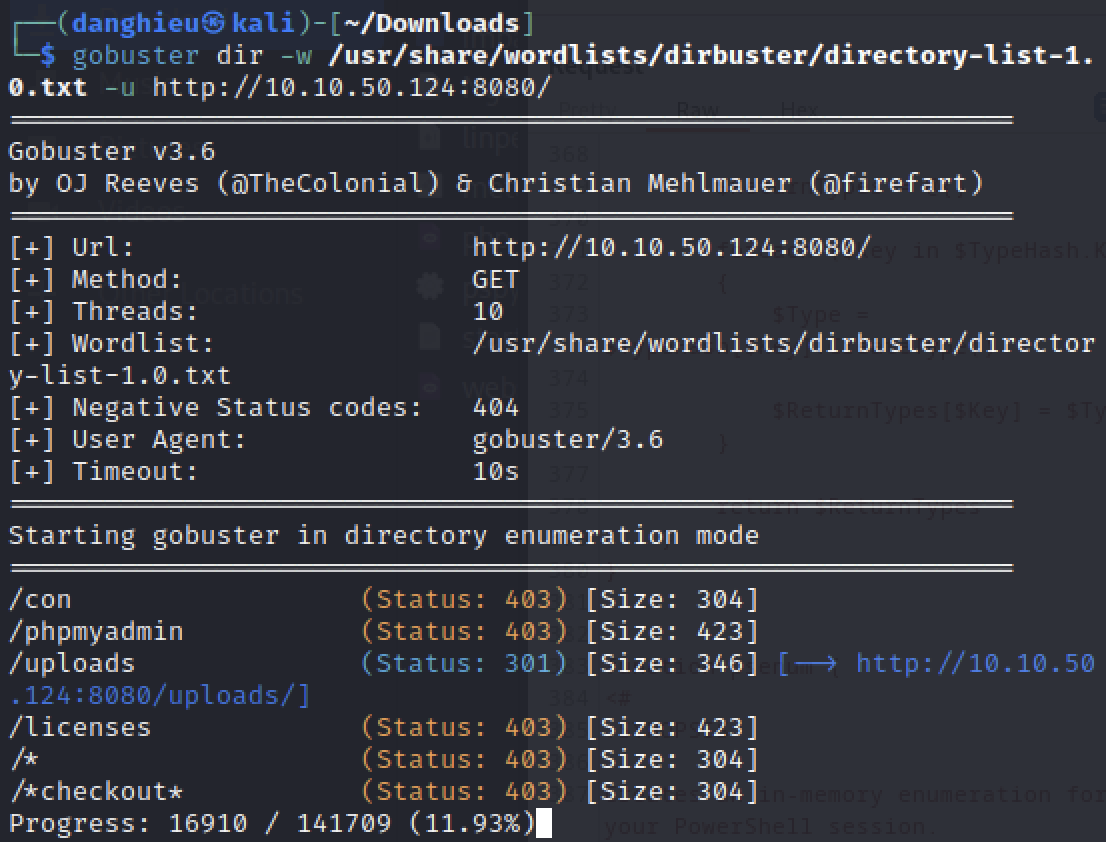


Mình có 1 trang web phân tích Powershell Script:

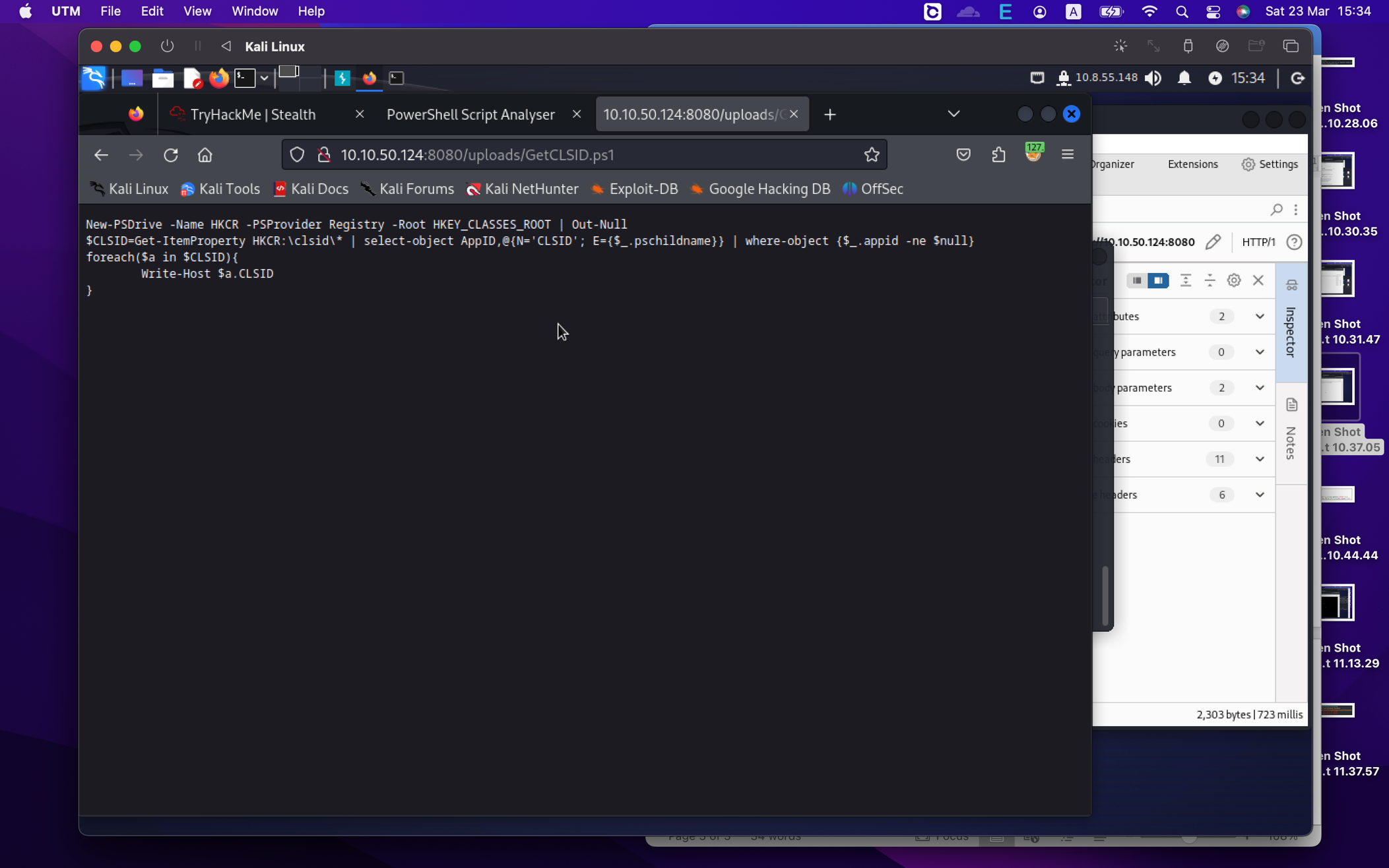


Dịch vụ SMB bị từ chối truy cập:





Bạn có thể đăng tải tập tin nhưng trong thư mục uploads nó sẽ không thực thi:



Ứng dụng bị dính lỗ hổng upload file!

Không mình đã sai ý tưởng ngay từ đầu, làm sao ứng dụng biết tập tin đó có độc hại không? Chắc chắn ứng dụng đã thực thi nó trên hệ thống mới biết. Còn thư mục uploads chỉ chứa source code.

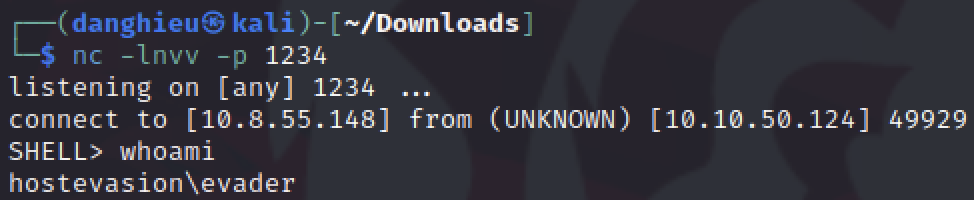
Nếu vậy cũng không thực tế, chưa biết tập tin độc hại như thế nào mà máy chủ dám thực thi. Chỉ có một khả năng, máy chủ sẽ kiểm tra tập tin có độc hại không rồi mới thực thi. Vậy mình chỉ cần tìm Powershell script để máy chủ không phát hiện ra.

Có 1 powershell reverse shell script không bị phát hiện độc hại:

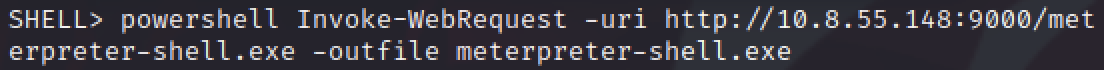
https://github.com/martinsohn/PowerShell-reverse-shell/blob/main/powershell-reverse-shell.ps1

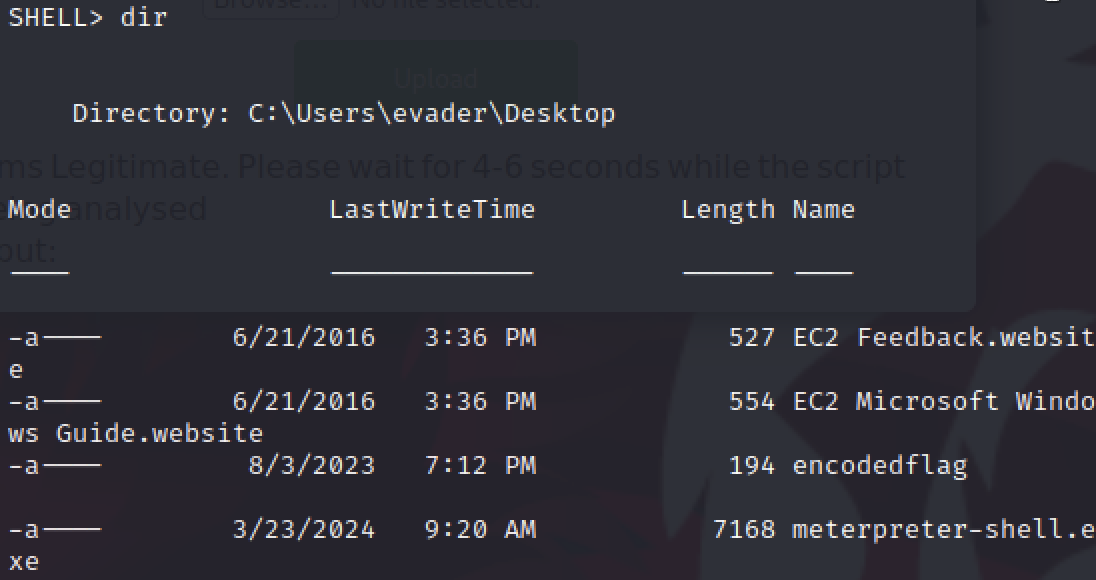
Mình so sánh nó với Invoke-PowerShellTcp.ps1

* Giống là nó trả về cho mình 1 Powershell
* powershell-reverse-shell.ps1 giống như reverse-shell.exe vậy, bạn chỉ cần thực thi là nhận được shell, còn Invoke-PowerShellTcp.ps1 bạn phải xác định địa chỉ ip, cổng lắng nghe.
* Đối với Invoke-PowerShellTcp.ps1, bạn phải có shell hoặc được thực thi lệnh, powershell-reverse-shell.ps1 phù hợp để bạn upload file.

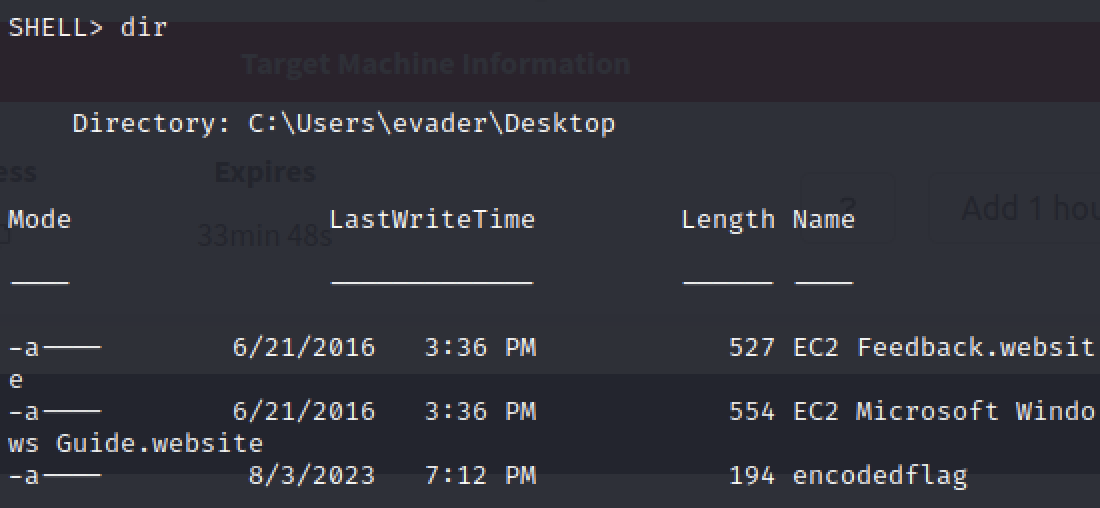


Mình sẽ switch lên meterpreter shell để khai thác cho dễ.

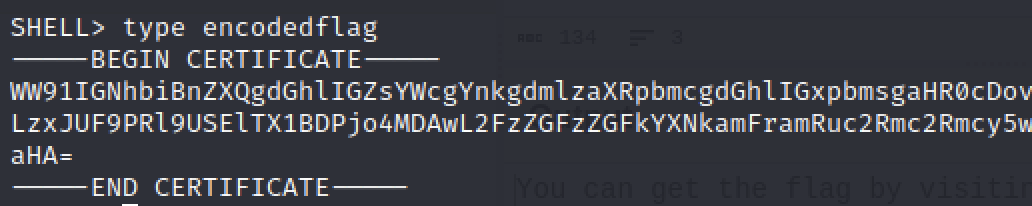




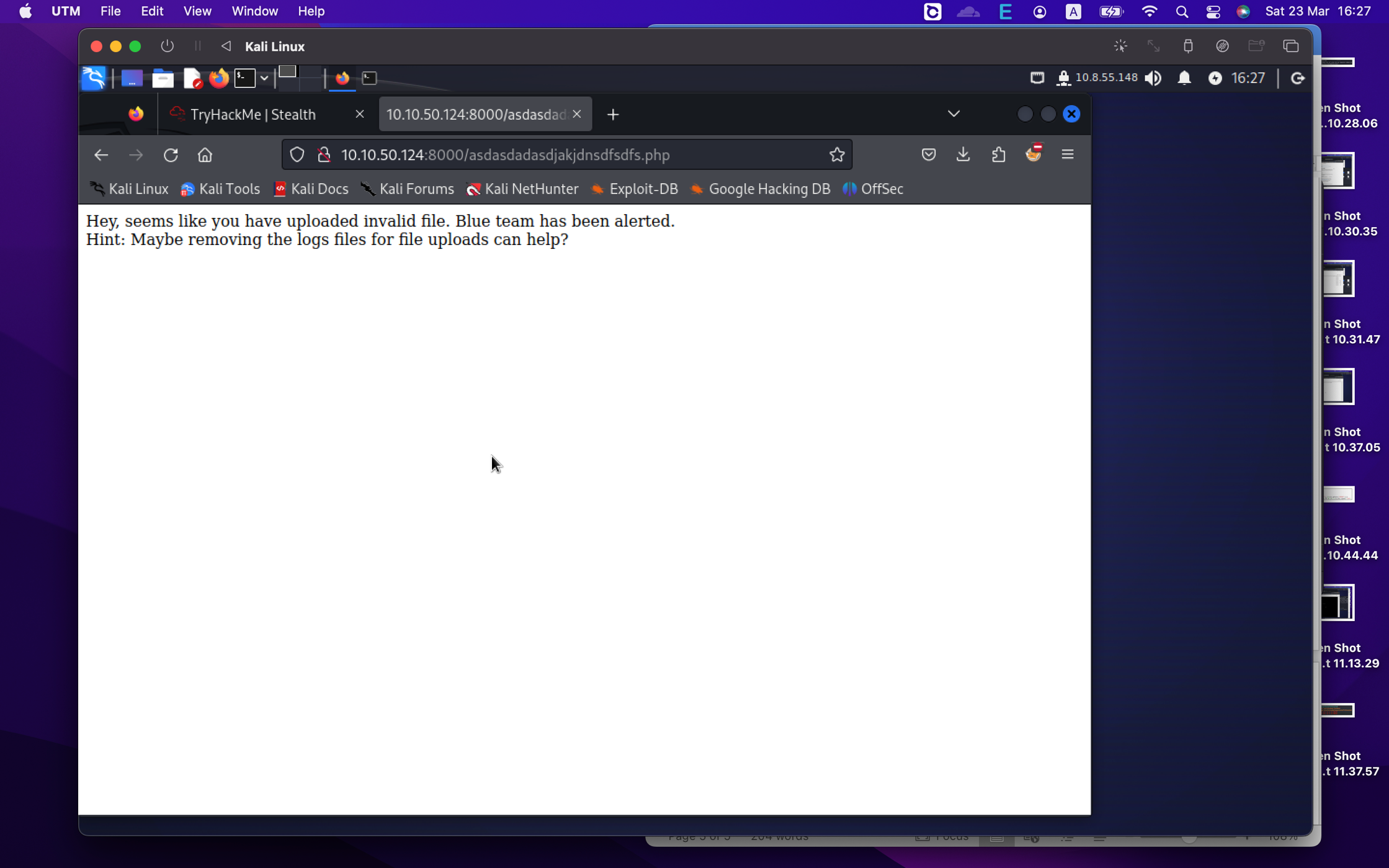
Mình quên mất, máy chủ triển khai rất nhiều phương pháp bảo mật, mình mới vận chuyển reverse-shell thì máy chủ tự động xóa.



Mình tìm được flag đầu tiên:

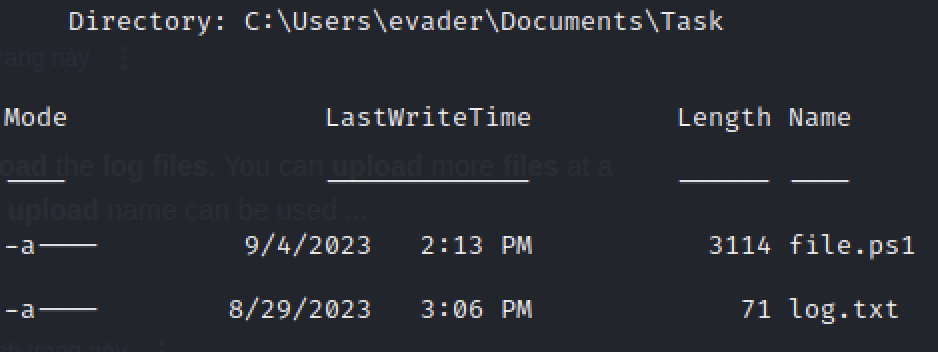


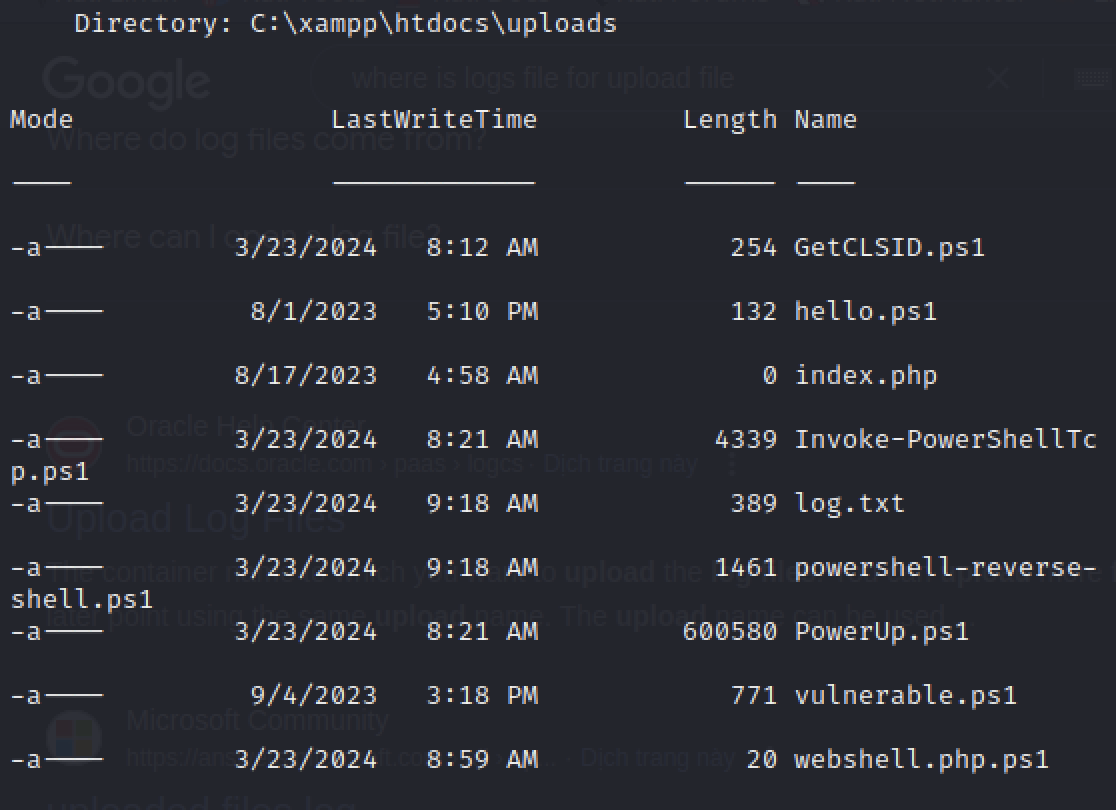
You can get the flag by visiting the link http://<IP\_OF\_THIS\_PC>:8000/asdasdadasdjakjdnsdfsdfs.php



Mình không biết các file logs để upload tập tin ở đâu?

file.ps1 trong thư mục C:\Users\evader\Documents\Task chỉ rằng có 1 tập log trong C:\xampp\htdocs\uploads

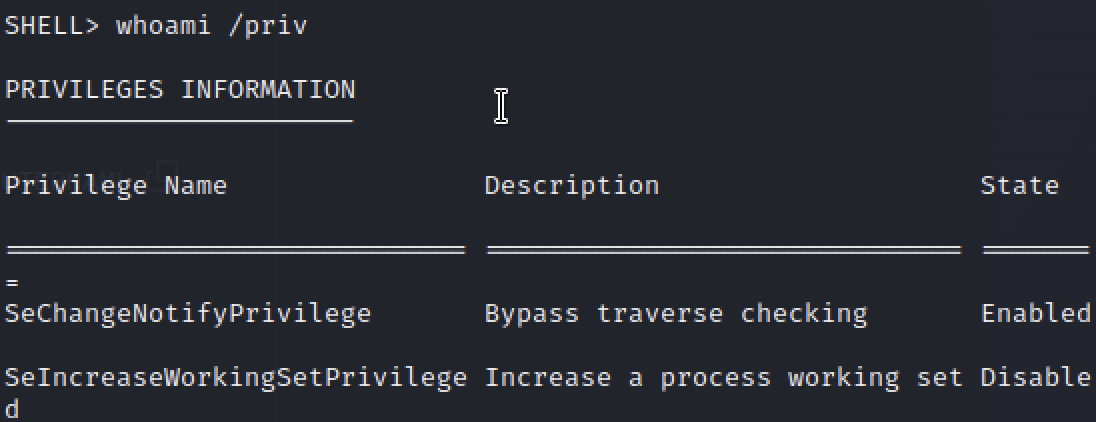




Mình sẽ xóa log.txt. Sau khi xóa, tải lại trang web mình sẽ thấy flag.

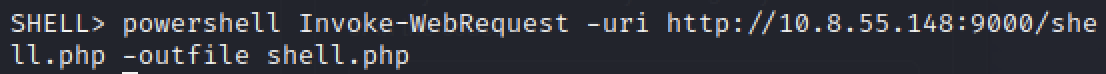
**Flag: THM{1010\_EVASION\_LOCAL\_USER}**

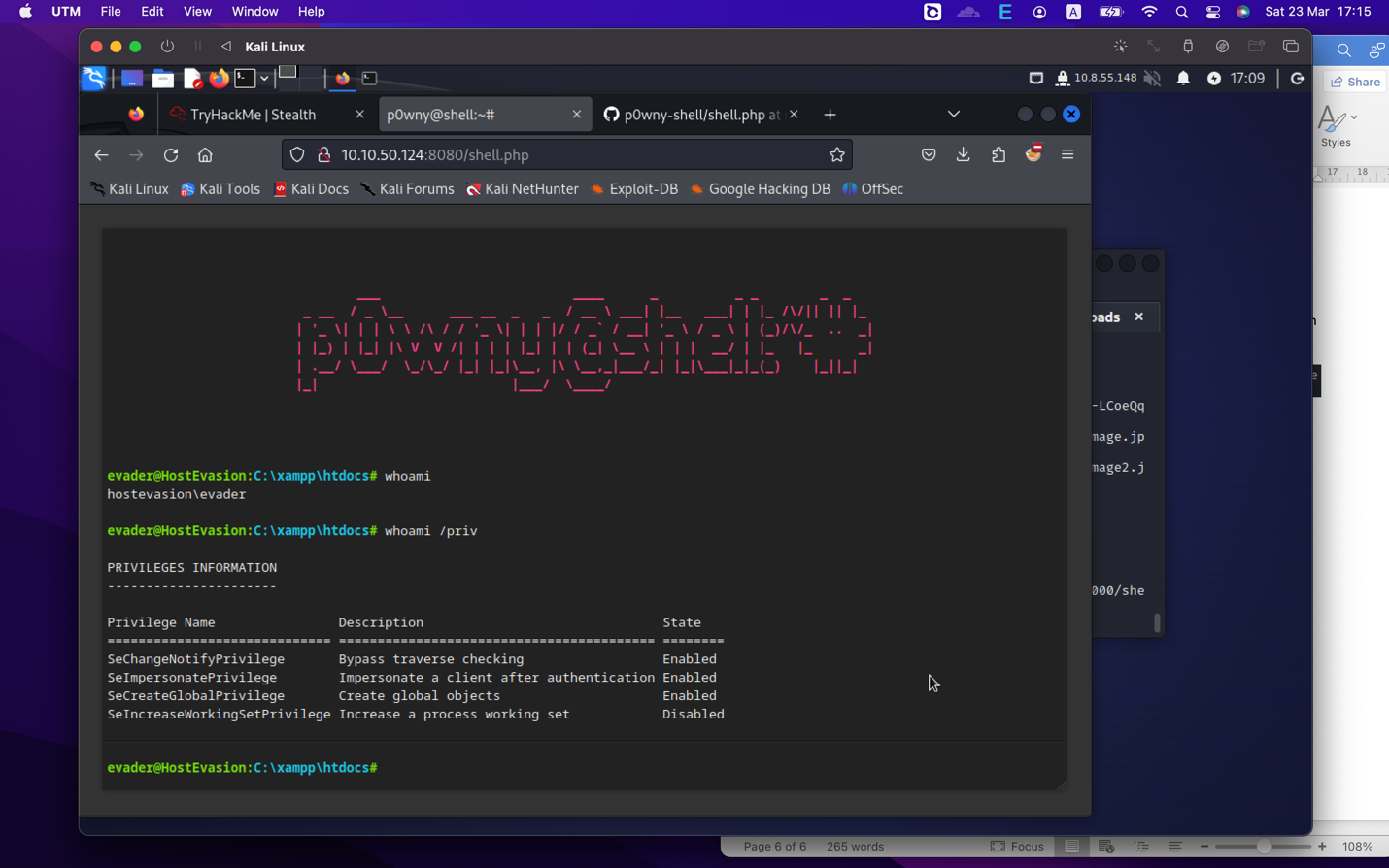
**Leo thang đặc quyền**



Mình sẽ vận chuyển p0wny-shell đến thư mục xampp/htdocs để lấy shell của dịch vụ web.

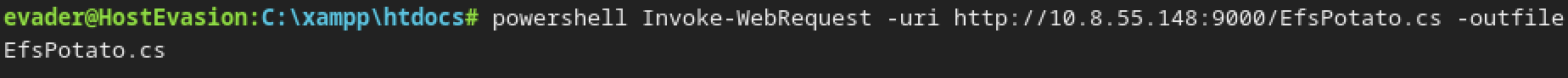
p0wny-shell giống như php reverse shell, nhưng bạn không cần thay đổi địa chỉ ip, cổng lắng nghe. Vì nó cho bạn 1 web-based shell. Bạn chỉ cần thực thi nó.



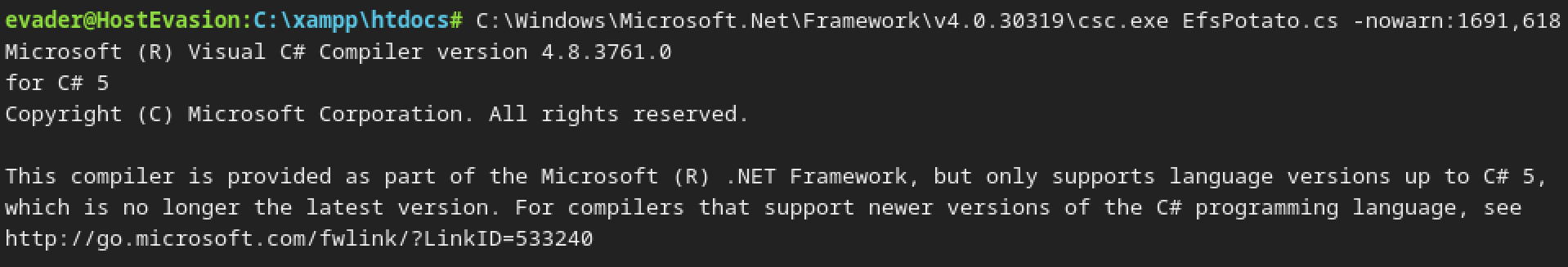


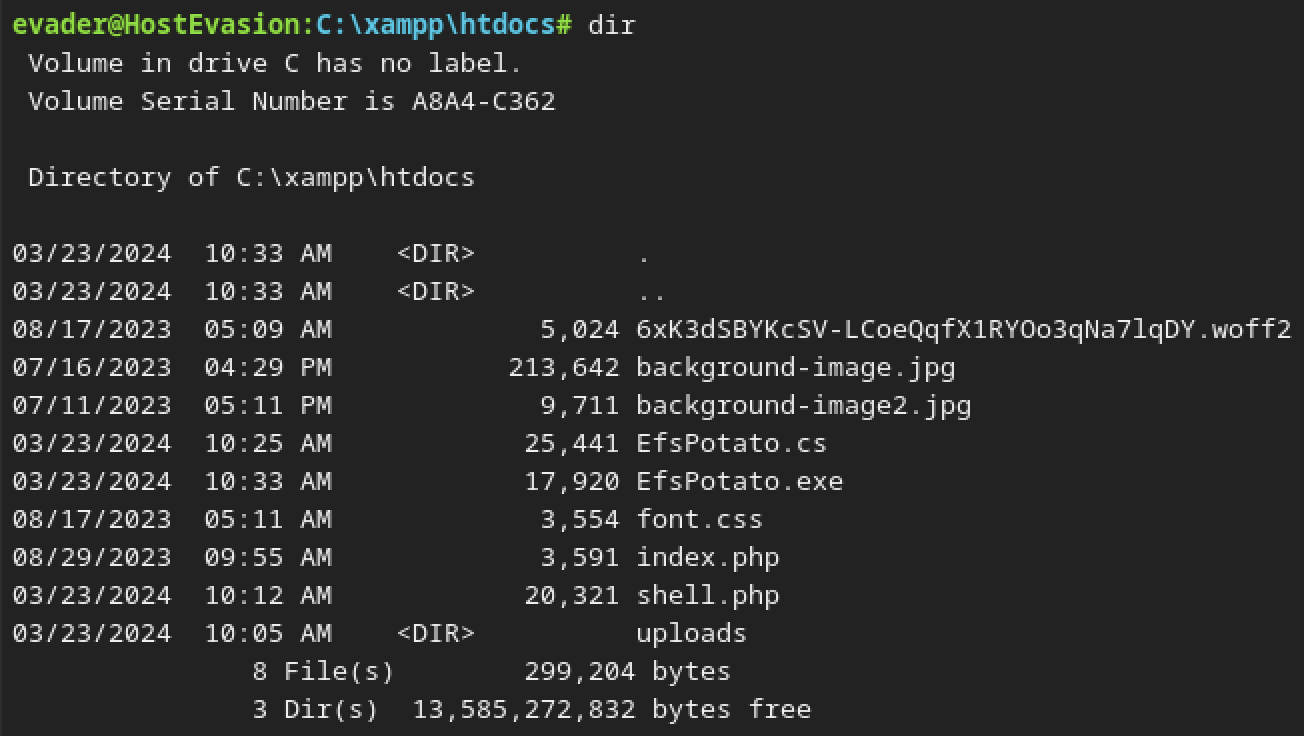
Cùng 1 người dùng, nhưng ở dịch vụ web bạn có thêm đặc quyền Seimpersonate. Mình sẽ dùng công cụ Efspotato để leo thang đặc quyền.

Vận chuyển tập tin đến máy nạn nhân:

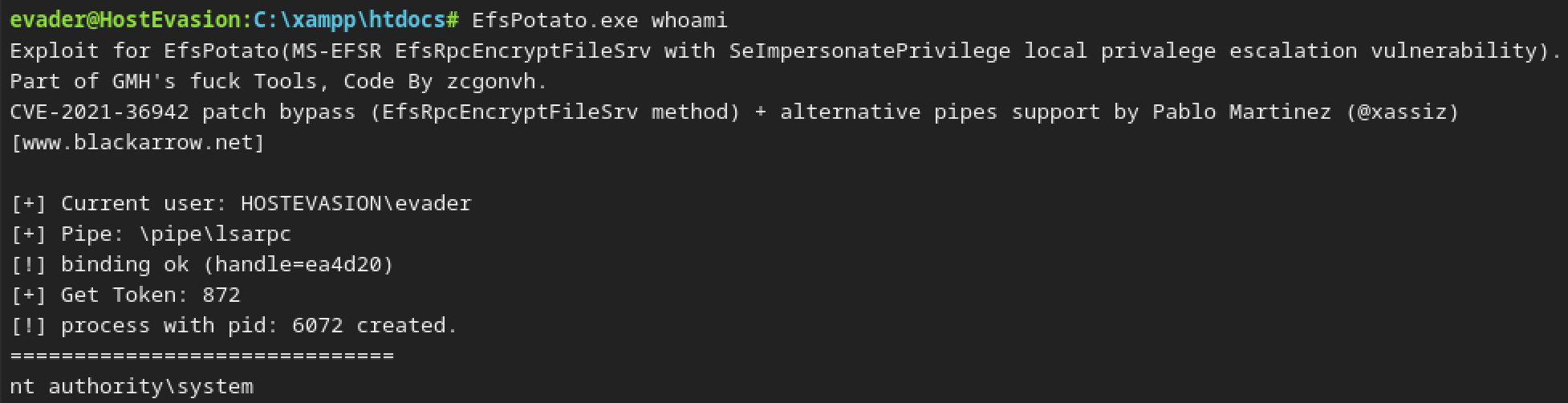


Biên dịch tập tin:



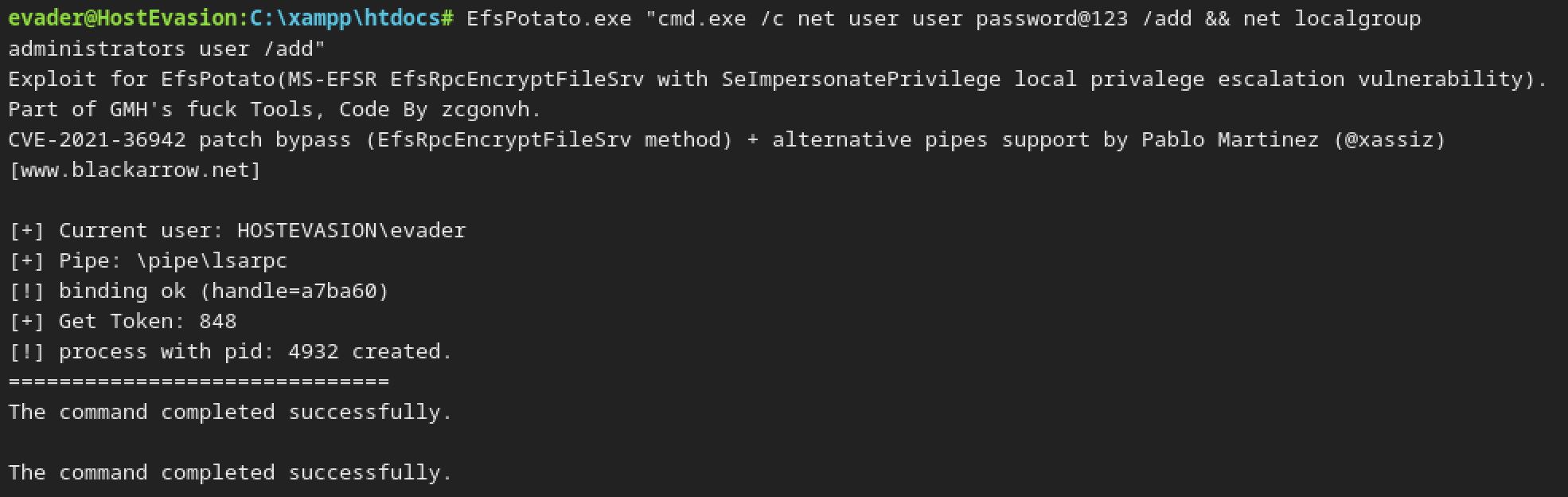


Dùng EfsPotato.exe để chạy lệnh với đặc quyền cao:



Thêm người dùng mới vào nhóm Administrators:

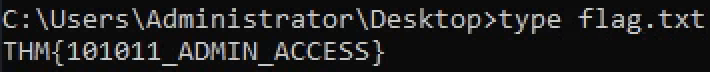
EfsPotato.exe "cmd.exe /c net user user password@123 /add && net localgroup Administrators user /add"



Dùng thông tin đăng nhập mới để kết nối RDP:

xfreerdp /u:user /p:password@123 /cert:ignore /v:10.10.50.124

Run as Administrator



**Flag: THM{101011\_ADMIN\_ACCESS}**