[Đăng nhập metasploitable 2 2](#_Toc1)

[Quét các cổng và dịch vụ trên msf2 4](#_Toc2)

[Tấn công Port 21 vsftpd 7](#_Toc3)

[Tấn công porst 22 SSH 8](#_Toc4)

[Tấn công port 23 9](#_Toc5)

[Tấn công port 80 apche 10](#_Toc6)

[Tấn công port 445 12](#_Toc7)

[Tấn công port 514 13](#_Toc8)

[Tấn công port 1099 14](#_Toc9)

[Tấn công port 2049 NFS 14](#_Toc10)

[Tấn công port 3632 15](#_Toc11)

[Tấn công cổng 5432 PostgreSQL 16](#_Toc12)

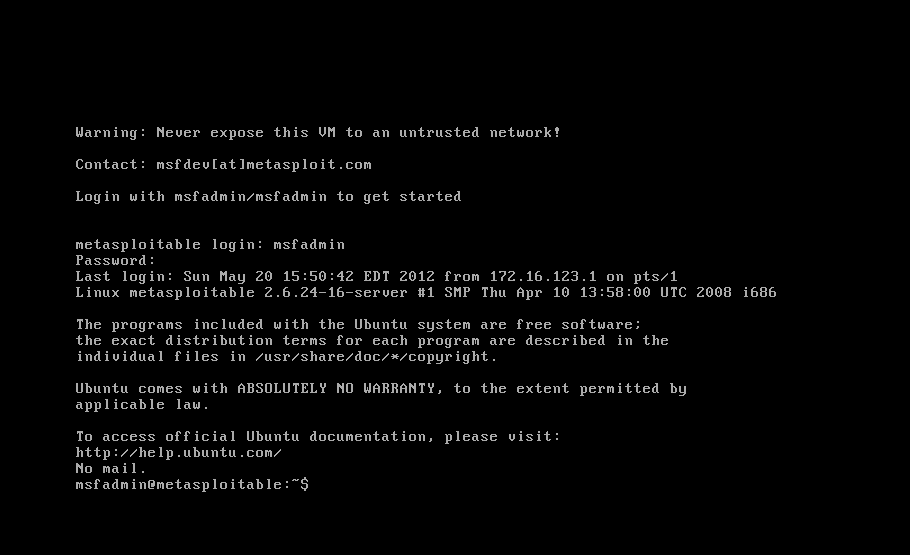
[Tấn công port 5900 vnc 18](#_Toc13)

[Tấn công port 667 IRC 19](#_Toc14)

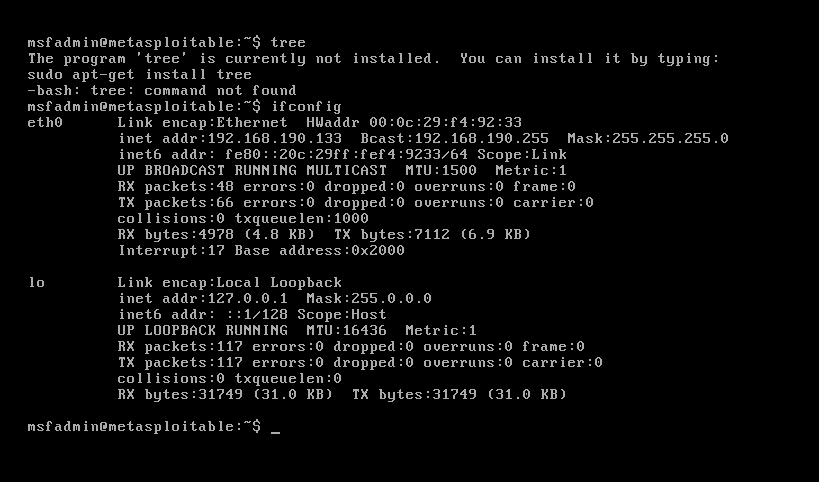
[Tấn công port 8180 19](#_Toc15)

[Tấn công port 6667 19](#_Toc16)

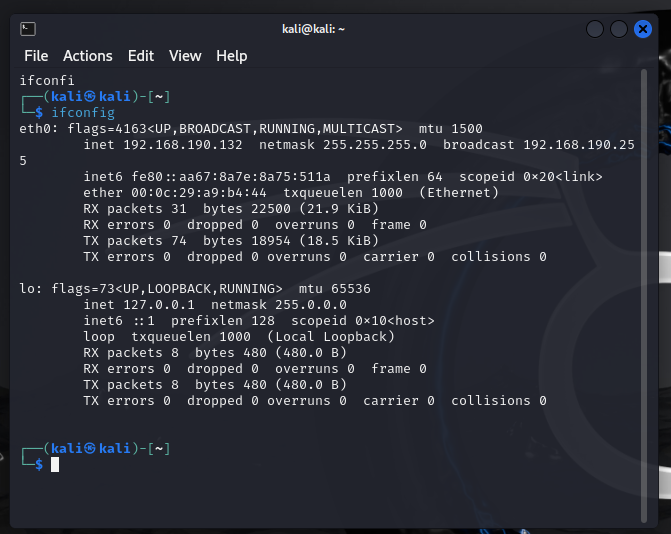
# Đăng nhập metasploitable 2



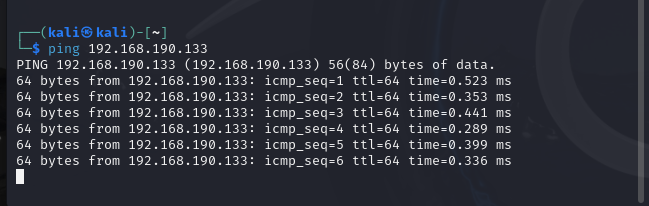
**IP máy msf2: 192.168.190.133**



**IP máy kali: 192.168.190.132**



Ktra ping dc lẫn nhau

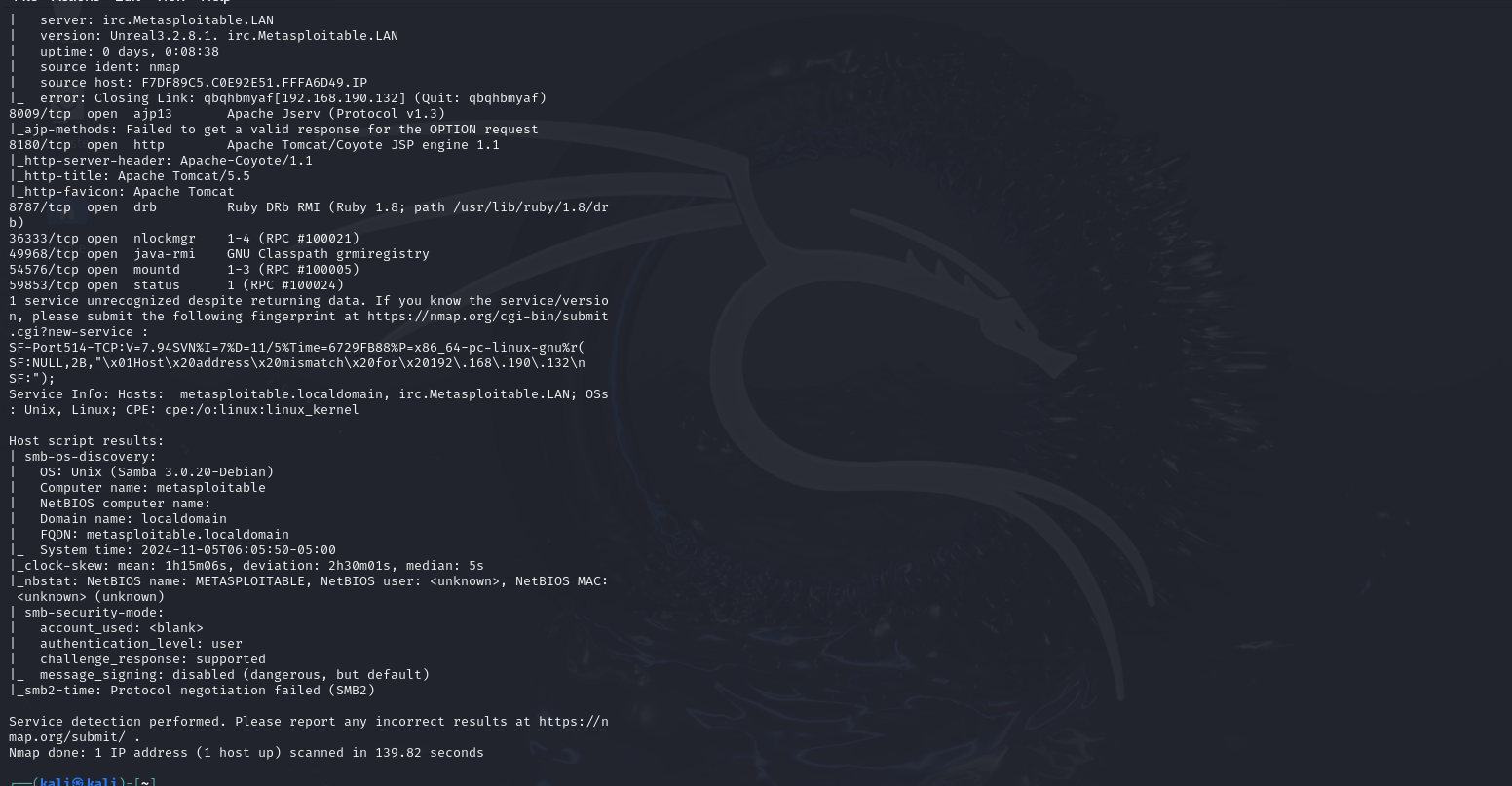


# Quét các cổng và dịch vụ trên msf2

* Câu lệnh



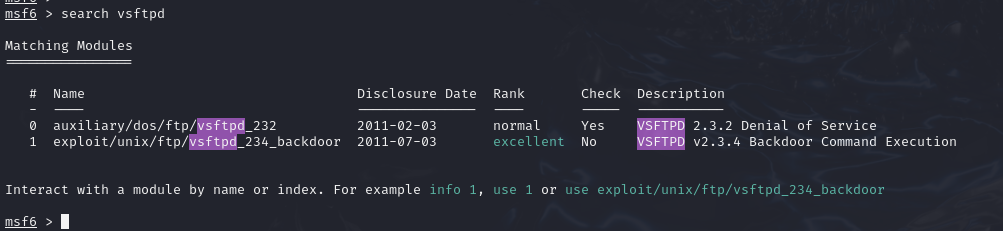
-Thông tin quét



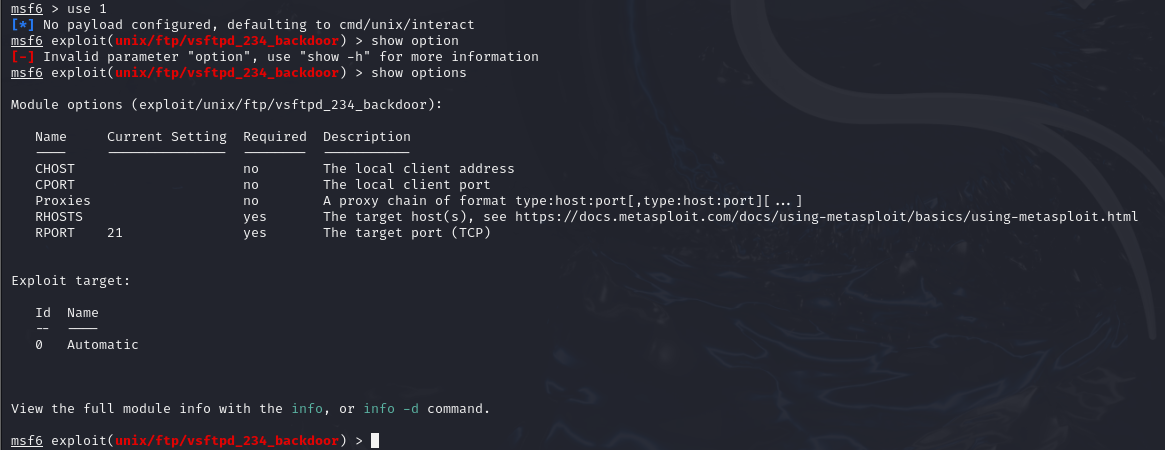
## Tấn công Port 21 vsftpd

* Mở Metasploit

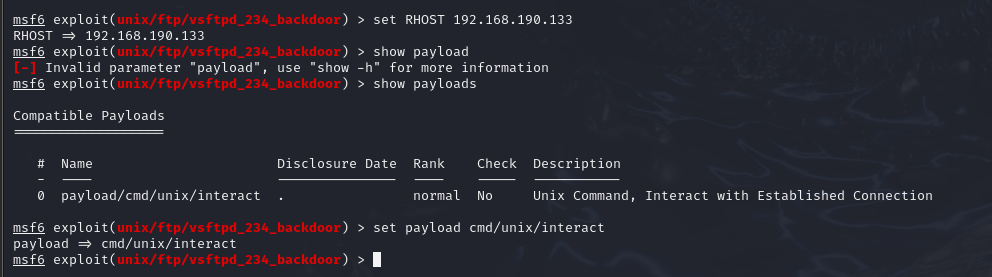
Tìm kiếm module vsftpd



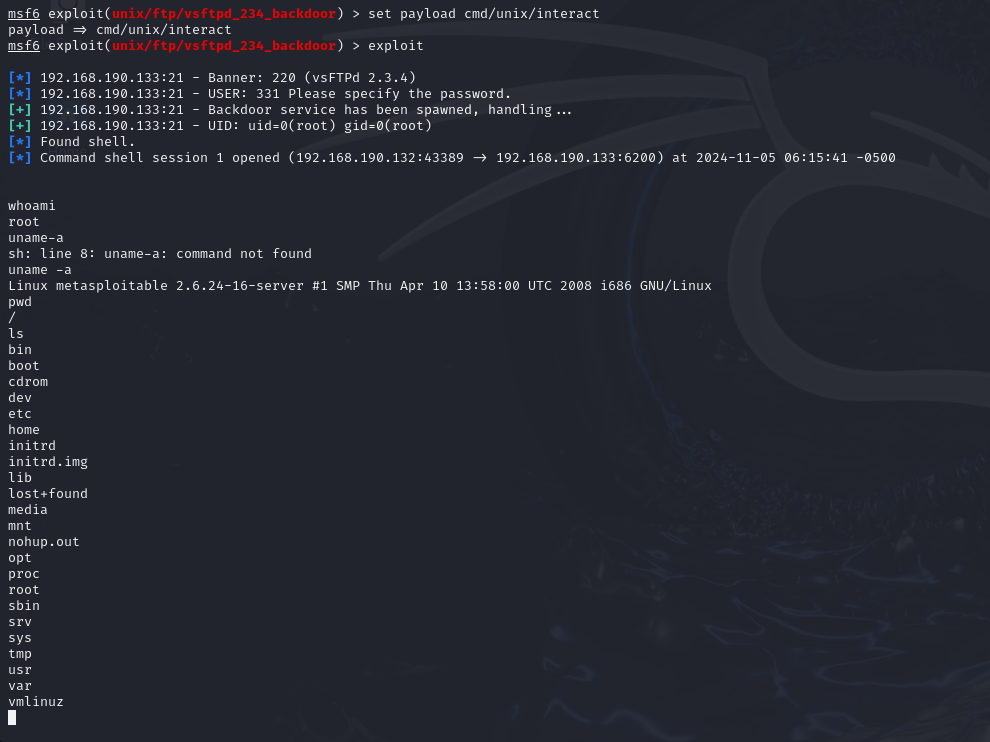
* Ta sẽ dùng cái 1 và hiển thị thông tin của module 1



* Đặt địa chỉ tấn công máy msf2 và set payload

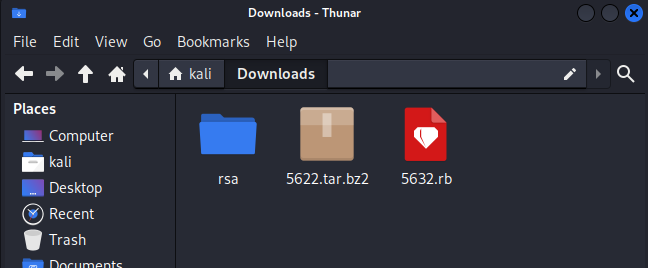


* Khai thác thành công



## Tấn công porst 22 SSH

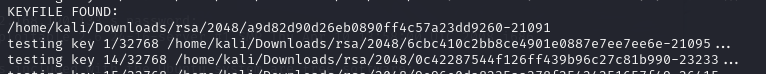
Cbi sẵn file để bruteforce



Câu lệnh thực hiện



* Key tìm thấy

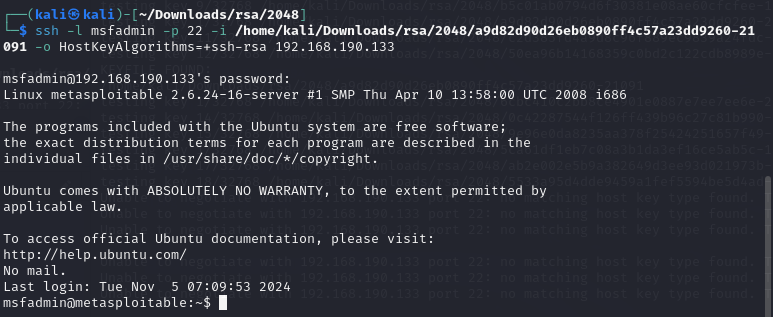


* Kết nối ssh tới qua câu lệnh

ssh -l msfadmin -p 22 -i /home/kali/Downloads/rsa/2048/a9d82d90d26eb0890ff4c57a23dd9260-21091 -o HostKeyAlgorithms=+ssh-rsa 192.168.190.133

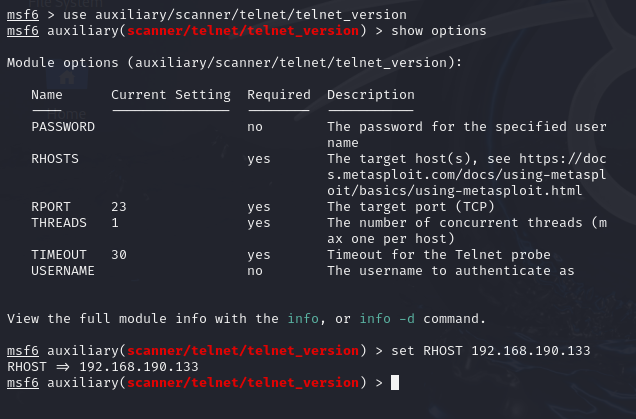
\*\*\* -o HostKeyAlgorithms=+ssh-rsa để ép dùng khóa là rsa do ssh cũ k còn dùng rsa

— kết quả



## Tấn công port 23

* Sử dụng module để tấn công



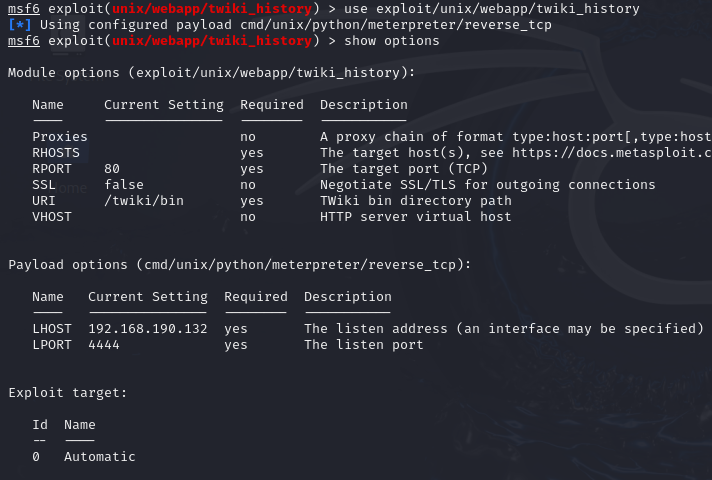
* Bắt đầu tần công



Ở đây đã lấy được thông tin tk có quyền sudo

## Tấn công port 80 apche

* Sử dụng module tấn công



* Cài đặt địa chỉ máy tấn công và set payload

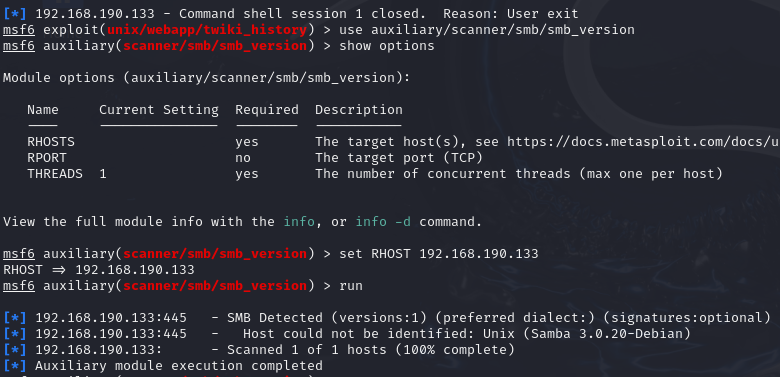


Tấn công thành công



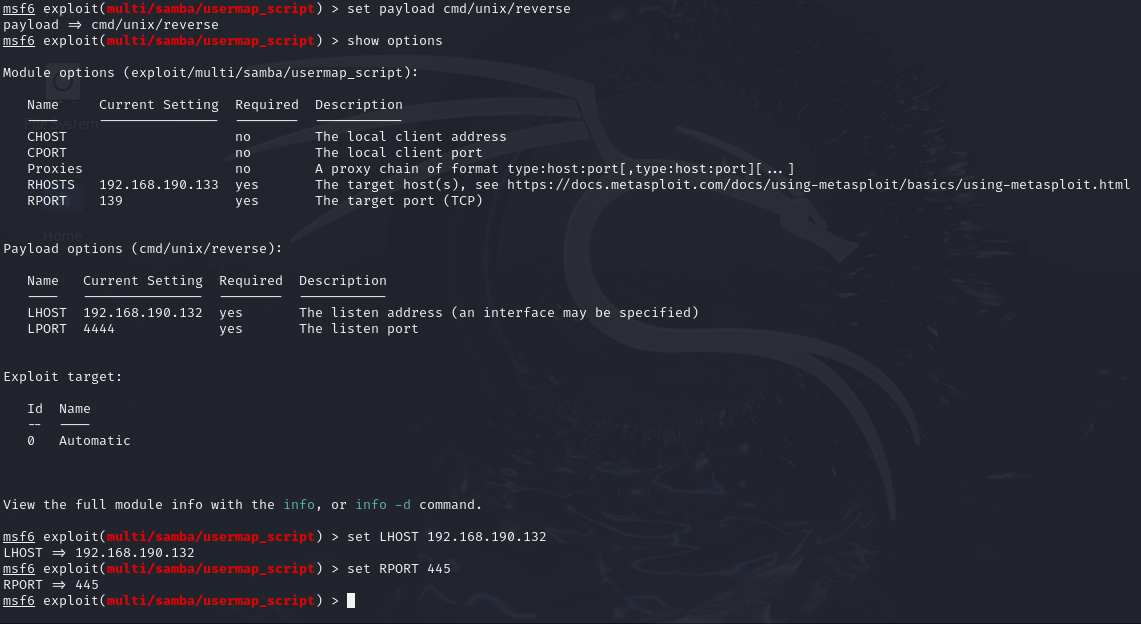
## Tấn công port 445

* Sử dụng module

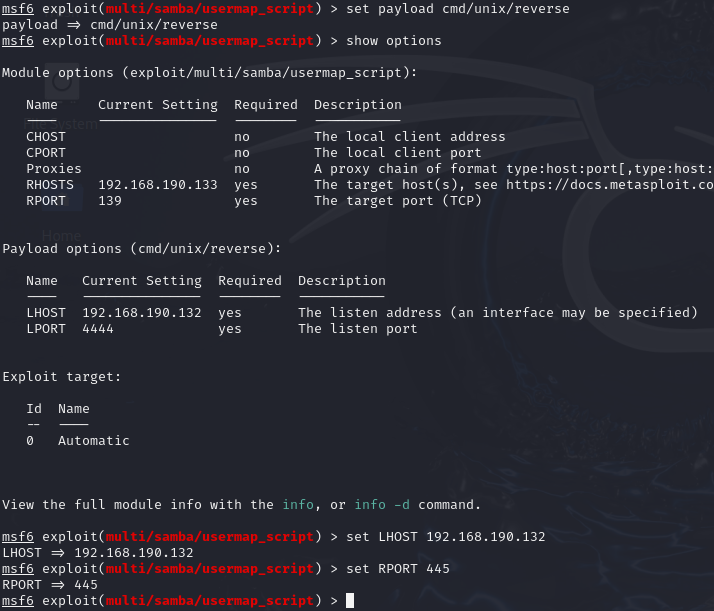


Đang chạy unix samba

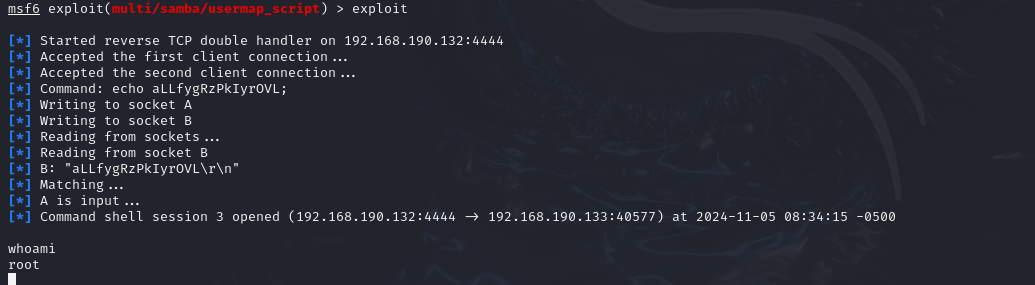
* Sử dụng username map script



* Cài đặt module (cài payload, host trả kết quả và cổng )

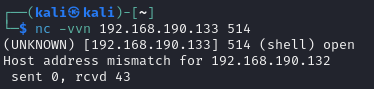


* Tấn công thành công



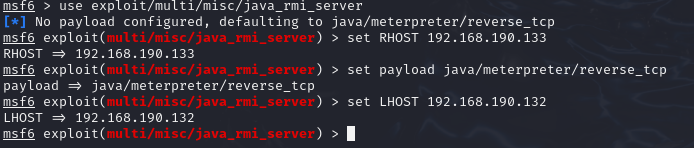
## Tấn công port 514

* Dùng netcat để quét cổng

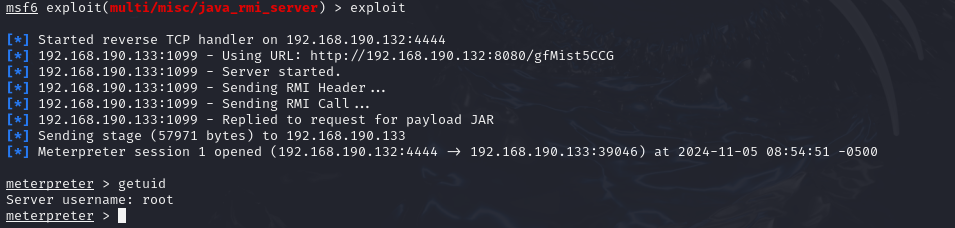


## Tấn công port 1099

* Cài đặt module tấn coongg

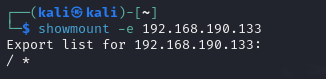


Khai thác thành công



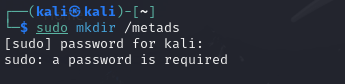
## Tấn công port 2049 NFS

* Xem danh sách suất của NFS server



Ở đây thư mục root cho phép mount

* Tạo thư mục bên kali để mount



Mount vào bên máy msf2

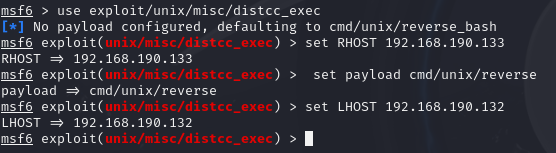


Cat mật khẩu ra

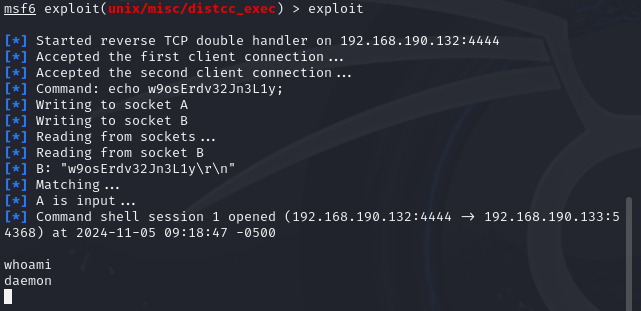


## Tấn công port 3632

* Thiết lập module tấn công



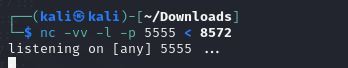
* Có được tài khoản mức thấp



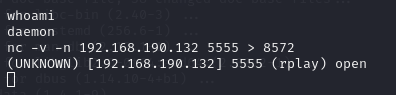
Compile mã về 32bit



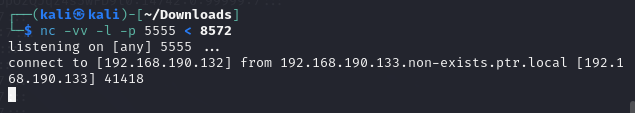
* Mở 1 cổng lắng nghe trên kali



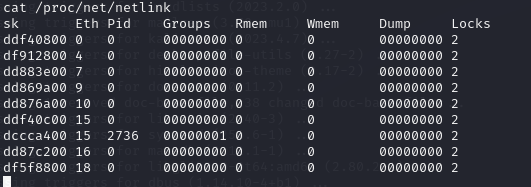
* Trên metasploit tạo công gửi thông tin từ máy nạn nhân



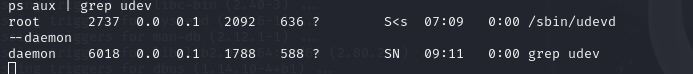
* Trên máy kali đã bắt dc kết nối



Ta vào tìm PID

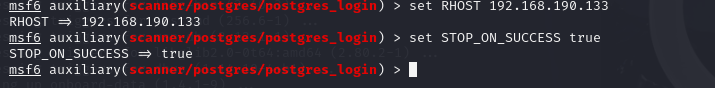


Kiểm tra Pid

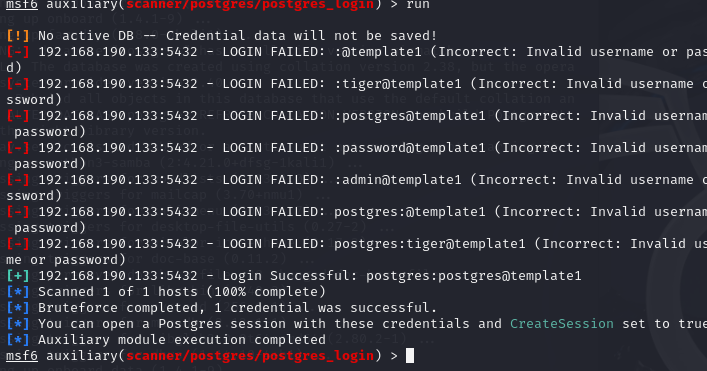


## Tấn công cổng 5432 PostgreSQL

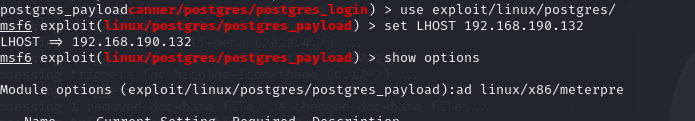
* Cài đặt module



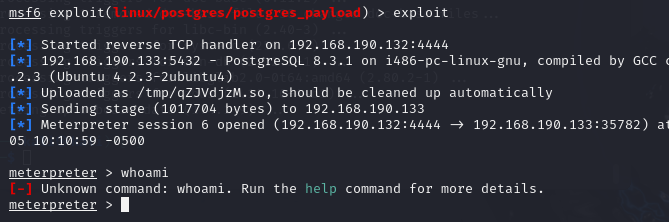
* Chạy



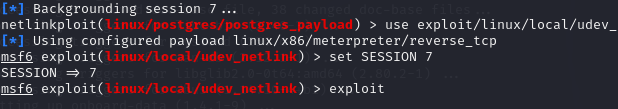
* Cấu hình module tiếp



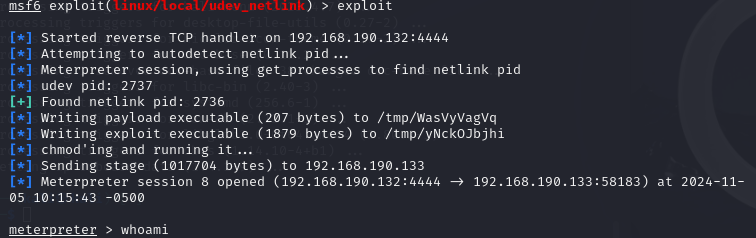
* Tấn công thành công



* Set up 1 module tiếp

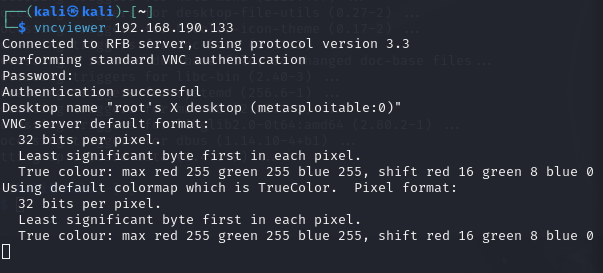


- Khai thác thành công

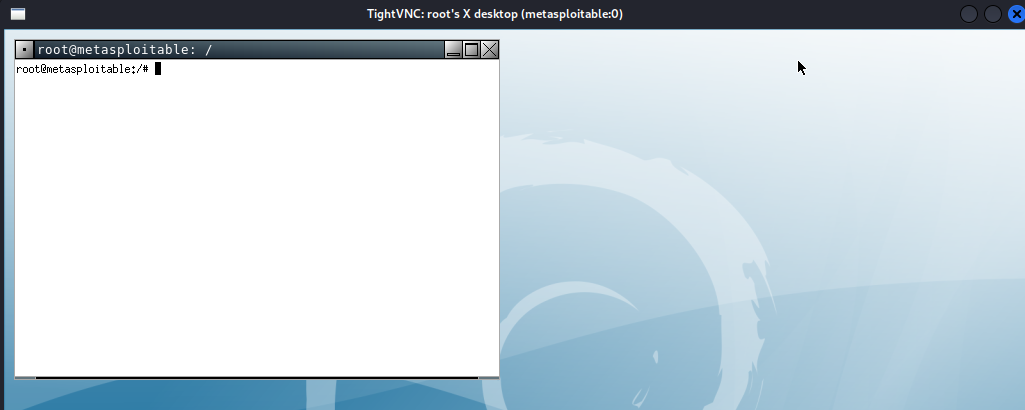


## Tấn công port 5900 vnc

* Đăng nhập với mật khẩu “password”

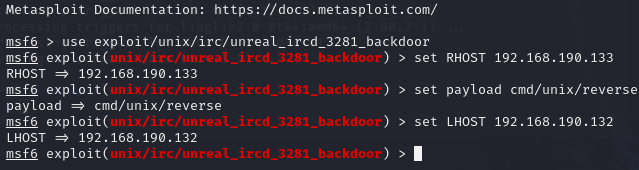


kq

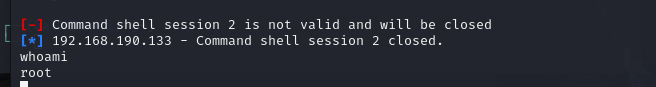


## Tấn công port 667 IRC

Câu lệnh

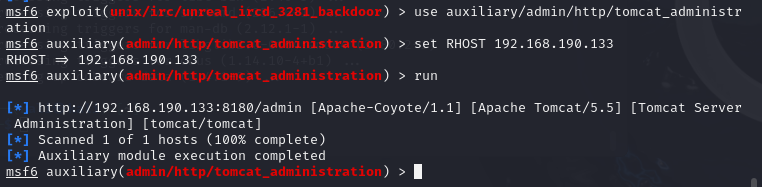


Kq thành công



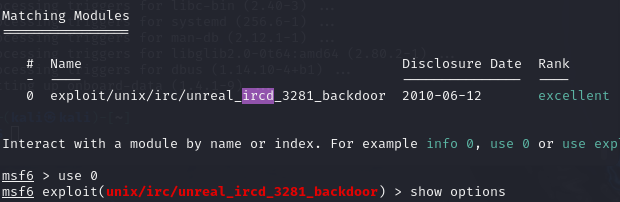
## Tấn công port 8180

-set up và hiển thị dc thông tin về tomcat



## Tấn công port 6667

* Chọn module



* Set up module và tấn công

