|  |
| --- |
| BAN CƠ YẾU CHÍNH PHỦ  **HỌC VIỆN KỸ THUẬT MẬT MÃ**  ¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯  logo ATTT-02 |
| HỌC PHẦN  **TẤN CÔNG VÀ PHÒNG THỦ HỆ THỐNG** |
| BÁO CÁO THỰC HÀNH  **Metasploitable** |
| |  |  | | --- | --- | | ***Họ tên sinh viên:*** | Nguyễn Ngọc Anh | | ***Lớp:*** | ATM03 | | ***Mã sinh viên:*** | AT180304 | |  |  | | ***Giảng viên:*** | TS. Lại Minh Tuấn  **Hà Nội, 2024** | |
|  |

MỤC LỤC

**[I)](#_Toc184490358)****[Chuẩn bị](#_Toc184490358)** [3](#_Toc184490358)

[**II)** **Khai thác** 3](#_Toc184490359)

[**1.** **Port 21 vsftpd** 5](#_Toc184490360)

[**2.** **Port 22 SSH** 7](#_Toc184490361)

[**3.** **Port 23 telnet** 10](#_Toc184490362)

[**III)** **Kết quả** 11](#_Toc184490363)

1. **Chuẩn bị**

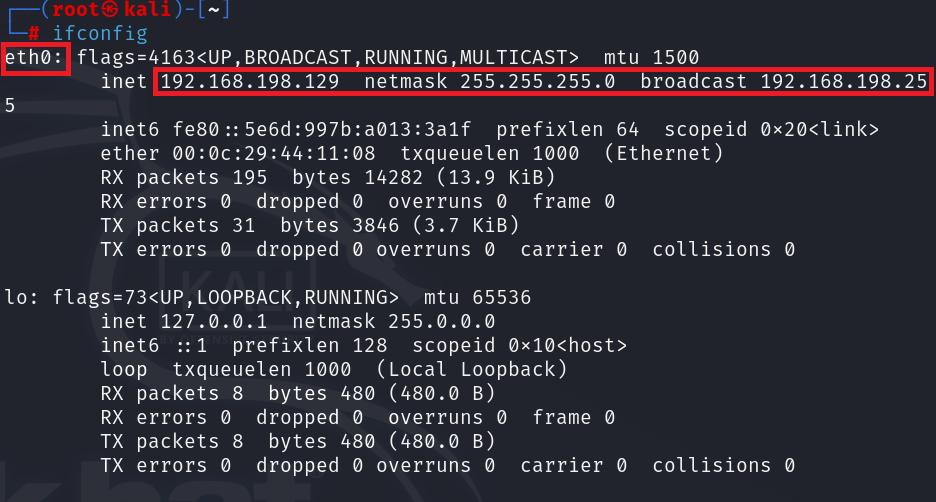
2 máy ảo:

* Máy attacker: kali linux hoặc parrotOS
* Máy victim: metasploitable

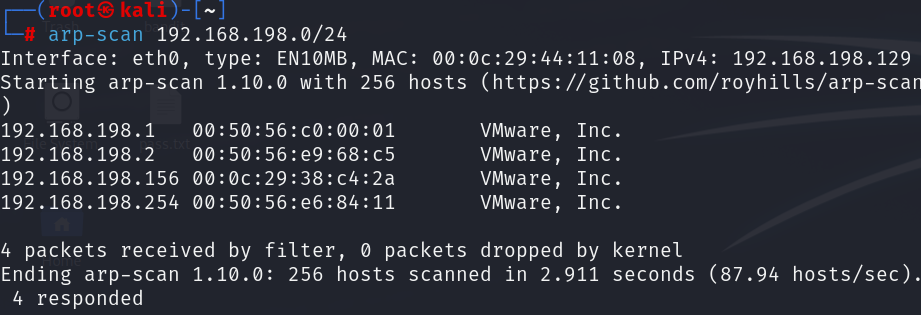
*Lưu ý: 2 máy phải cùng dải mạng*

1. **Khai thác**

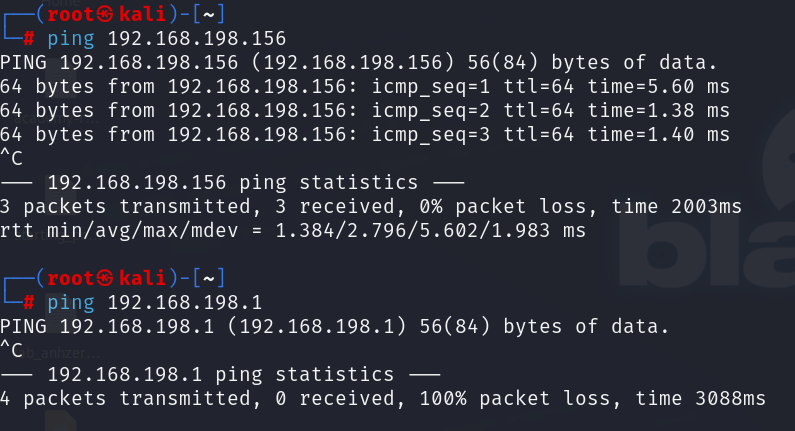
**B1**: Xác định dải ip address máy hacker. Từ đó tìm ra ip address máy victim.



Chạy câu lệnh sau để tìm IP address máy victim.



Ở đây, chúng ta thấy có 4 IP address. Vì vậy, để biết máy nào đang mở hay là cho chúng ta truy cập tới, ta có thể thực hiện câu lệnh ping.



Ta có thể thấy IP address victim là 192.168.198.156

**B2**: Scan port đang mở trên máy victim. Trước hết, hãy tạo một folder, file ghi lại quá trình attack.

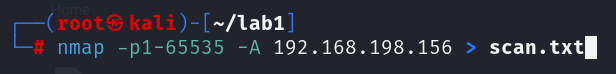
* Tạo folder có tên là lab1.



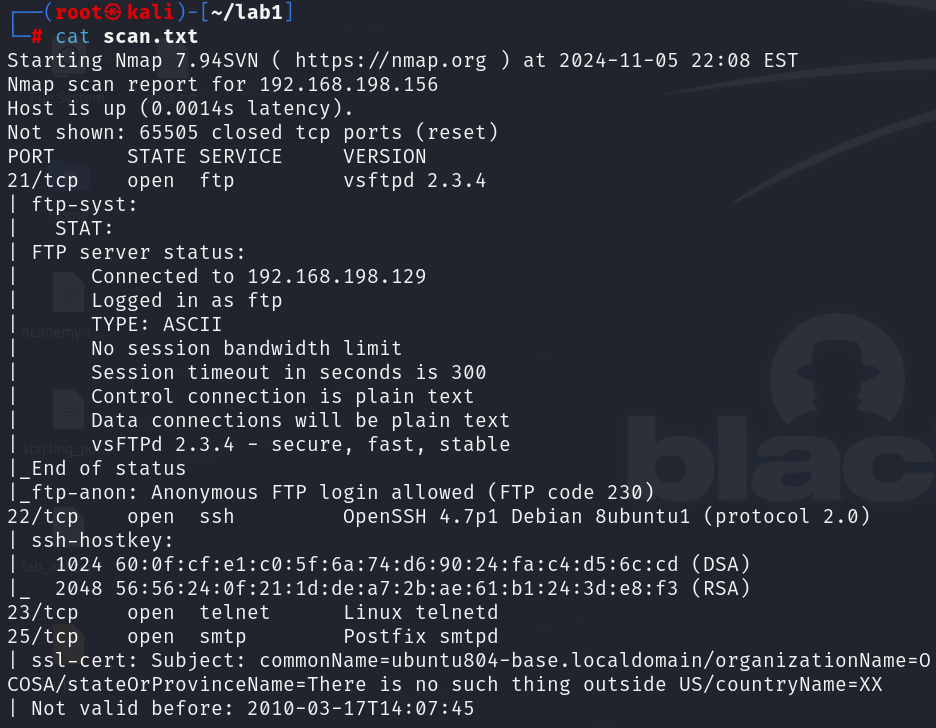
* Vào folder lab1, tạo file scan.txt.



Chạy câu lệnh sau để dò quét cổng port, dịch vụ đang chạy và lưu thông tin dò quét được vào file scan.txt



Đọc file scan.txt.



1. **Port 21 vsftpd**

**B1: Chạy tool msfconsole và bắt đầu khai thác:**

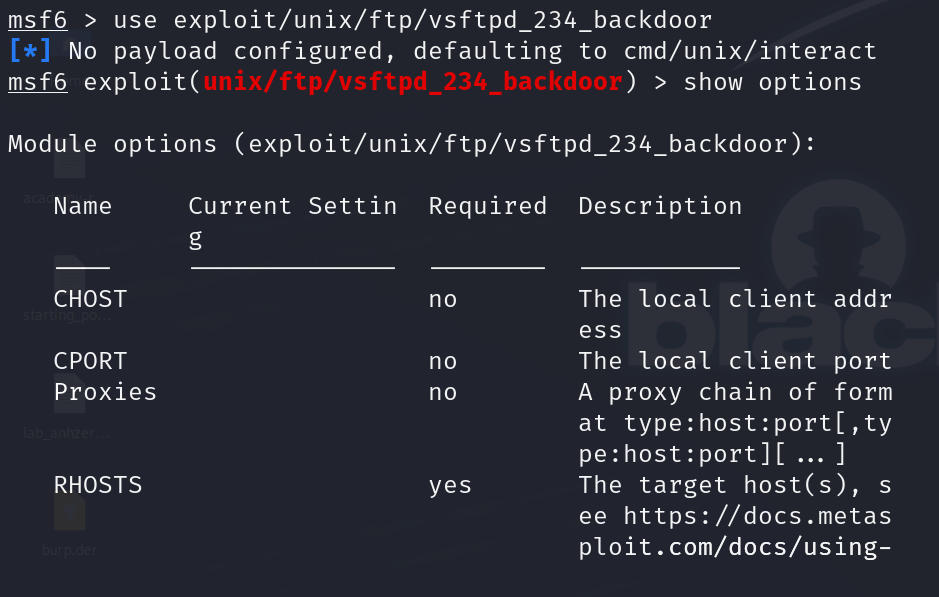
Trong Metasploit, phiên bản vsftpd có sẵn 1 lỗ hổng khai thác.



**VSFTPD v2.3.4 Backdoor Command Execution**

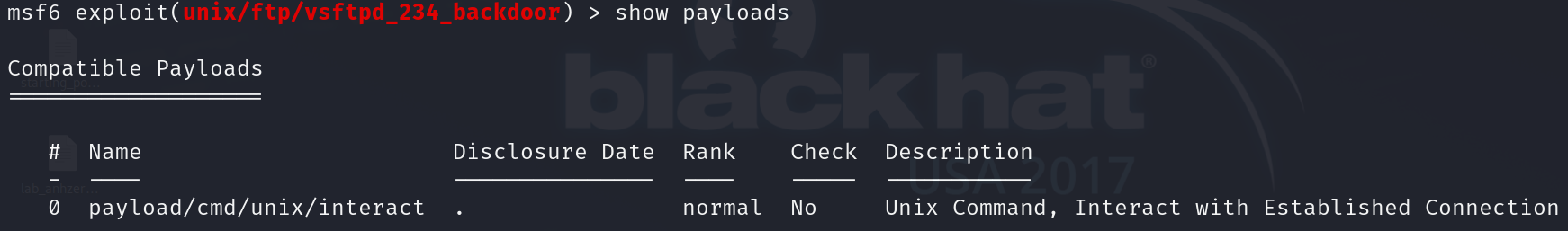
Một backdoor độc hại được đưa vào kho lưu trữ tải xuống VSFTPD bị khai thác bởi mô-đun này. Theo thông tin mới nhất có sẵn, backdoor này đã được thêm vào kho lưu trữ vsftpd-2.3.4.tar.gz trong khoảng thời gian từ ngày 30 tháng 6 năm 2011 đến ngày 1 tháng 7 năm 2011. Vào ngày 3 tháng 7 năm 2011, backdoor này đã bị loại bỏ.

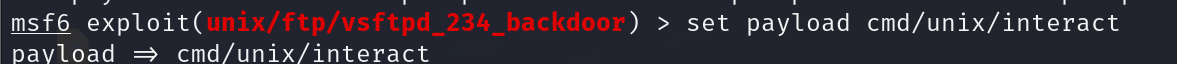
**B2: Chúng ta sẽ khai thác nó và lấy một shell:**

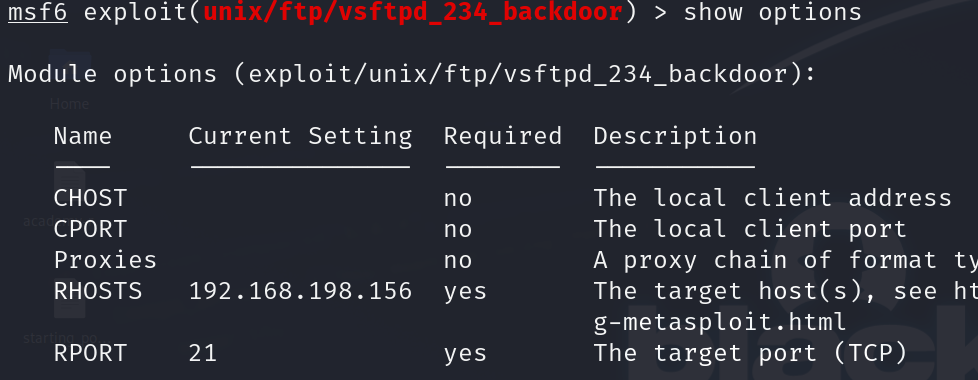


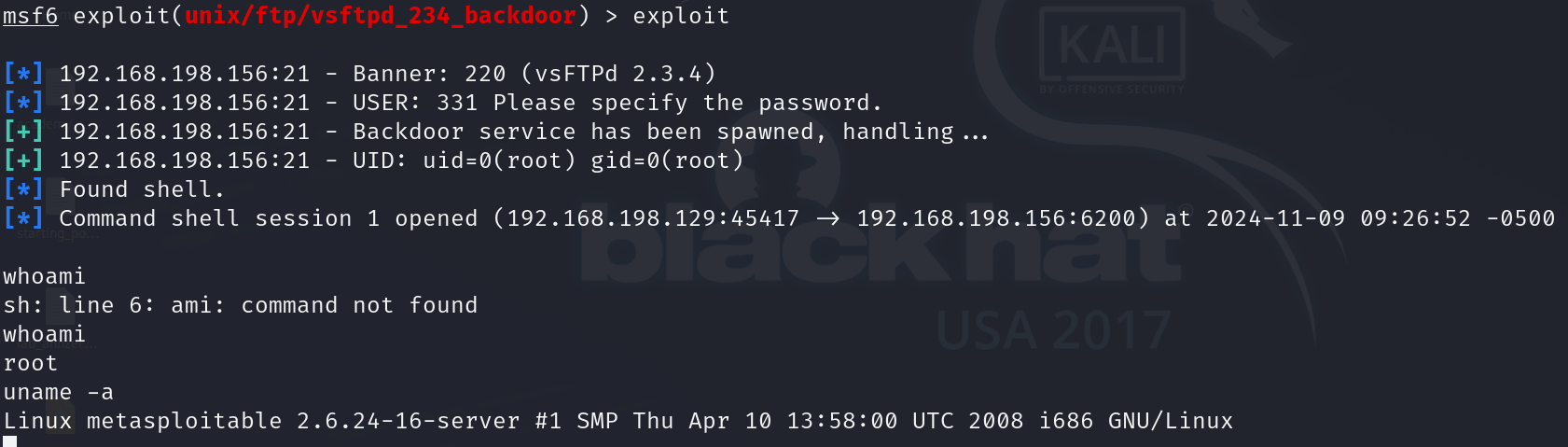












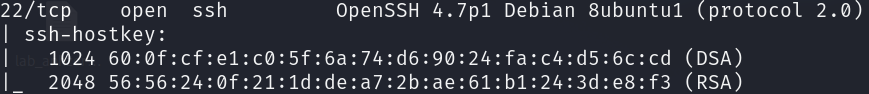
Bây giờ chúng ta đã sử hữu 1 máy victim.

1. **Port 22 SSH**

Bởi vì do một lỗ hổng của trình tạo số ngẫu nhiên, phần mềm OpenSSL được cài đặt trên hệ thống dễ bị tấn công bằng cách dùng brute-force. Sau đây là mô tả và số CVE:

**CVE-2008-0166**

Trên các hệ điều hành (OS) dựa trên Debian, OpenSSL 0.9.8c-1 cho đến các phiên bản trước 0.9.8g-9 sử dụng trình tạo số ngẫu nhiên tạo ra các con số có thể dự đoán được, giúp kẻ tấn công từ xa dễ dàng thực hiện các cuộc tấn công đoán khóa mật mã bằng cách dùng vũ lực.



Máy chủ này không sử dụng giao thức 1.0, giao thức này bị hỏng hoàn toàn và dễ bị đánh bại. Điều này có nghĩa là việc vượt qua SSH sẽ (ít nhất) là một thách thức nhẹ.

Có 2 cuộc tấn công SSH sử dụng metasploit:

* + Cuộc tấn công đầu tiên là *ssh\_login*, cho phép bạn sử dụng metasploit để đoán thông tin đăng nhập SSH bằng cách dùng phương pháp brute-force.

Module name is auxiliary/scanner/ssh/ssh\_login

* + Cuộc tấn công thứ hai yêu cầu một khóa riêng. Nếu bạn có quyền truy cập vào khóa SSH riêng trên máy nạn nhân, bạn có thể thử xác thực với một số lượng lớn máy chủ và dịch vụ bằng khóa riêng đó

Module name is auxiliary/scanner/ssh/ssh\_login\_pubkey

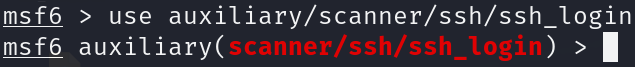
*Thứ 1:ssh\_login*

Có thể tấn công bằng brute force để đăng nhập bằng Hydra, Metasploitable/SSH/Brute Force.

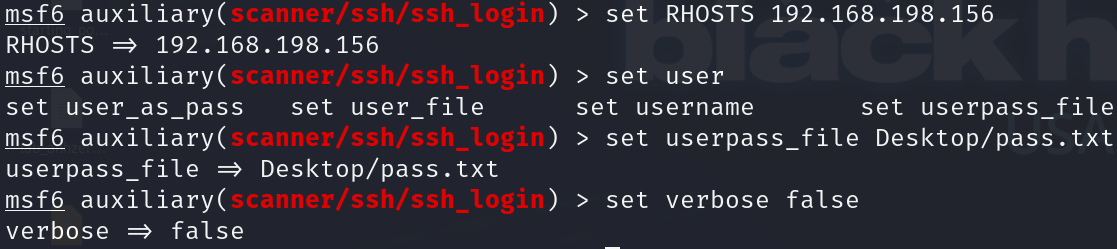
Nhưng ở đây chúng ta cũng có thể dùng brute force để đăng nhập SSH bằng Metasploitable. Sử dụng mô-đun auxiliary/scanner/ssh/ssh\_login.

**B1: Setting up the attack**

Chúng ta sẽ sử dụng module auxiliary/scanner/ssh/ssh\_login:

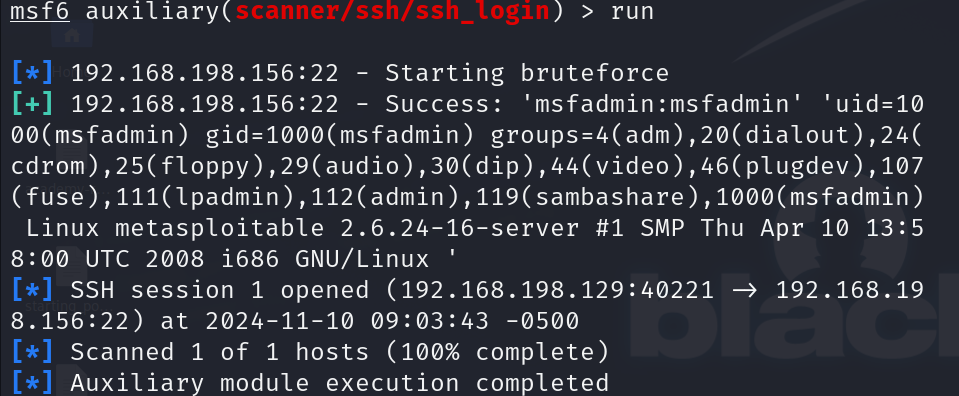


Thiết lập để chạy trên mục tiêu hộp ảo Metasploitable:



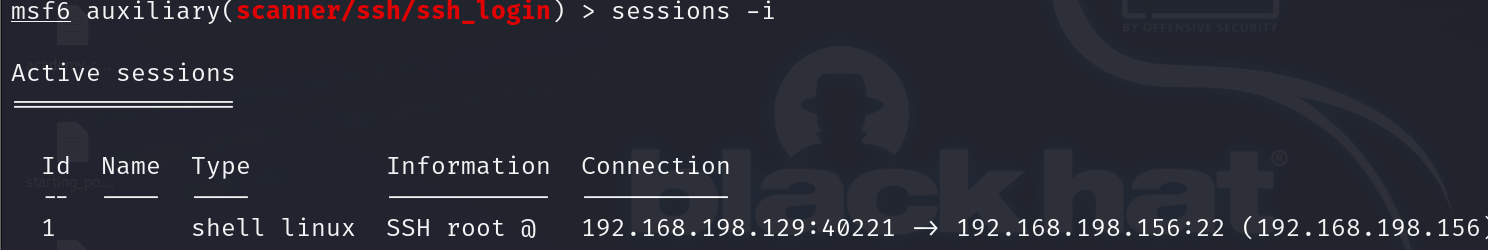
**B2: Running the attack**

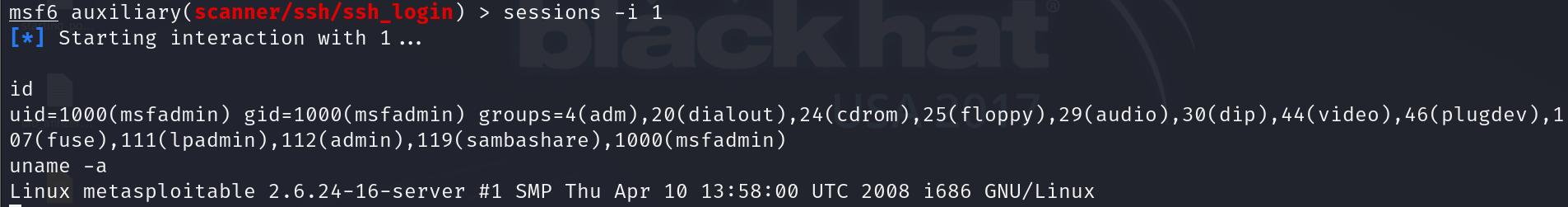
Bây giờ chạy cuộc tấn công:



**B3: Chúng ta có một shell**

Tại thời điểm này, chúng ta có thể tạo một phiên làm việc với máy mà chúng ta đã xâm phạm. Đăng nhập với tư cách là người dùng msfadmin:





*Thứ 2*: *ssh\_login\_pubkey*

Nếu bạn có thể lấy được khóa riêng của nạn nhân thì mô-đun auxiliary/scanner/ssh/ssh\_login\_pubkey chính là dành cho bạn!

Mô-đun này sử dụng khóa riêng để thực hiện hai việc:

* + Truy cập vào máy nạn nhân
  + Truy cập vào bất kỳ máy nào tin tưởng khóa riêng của nạn nhân (phải được liệt kê trong tệp SSH của máy nạn nhân)

**B1: Lấy khóa riêng**

Để thực hiện cuộc tấn công này, bạn sẽ cần có quyền truy cập vào hệ thống tệp và/hoặc có thể gắn hệ thống tệp từ xa (trên Metasploitable, điều này hoàn toàn có thể!): xem [Metasploitable/NFS](https://charlesreid1.com/wiki/Metasploitable/NFS)

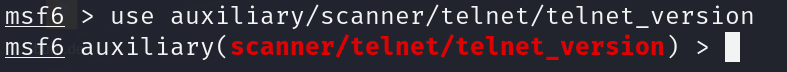
Khi đã có quyền truy cập vào hệ thống tập tin, bạn sẽ lấy một bản sao khóa riêng của máy từ xa và sử dụng chúng cùng với Metasploit để có quyền truy cập vào máy.

(Lưu ý rằng bạn cũng có thể cài khóa của mình vào mục tiêu bằng cách thêm khóa SSH công khai vào danh sách máy đáng tin cậy của máy mục tiêu, nhưng kỹ thuật này sẽ giới hạn bạn ở một máy cụ thể, trong khi phương pháp Metasploit có tính di động và ít xâm phạm hơn.)

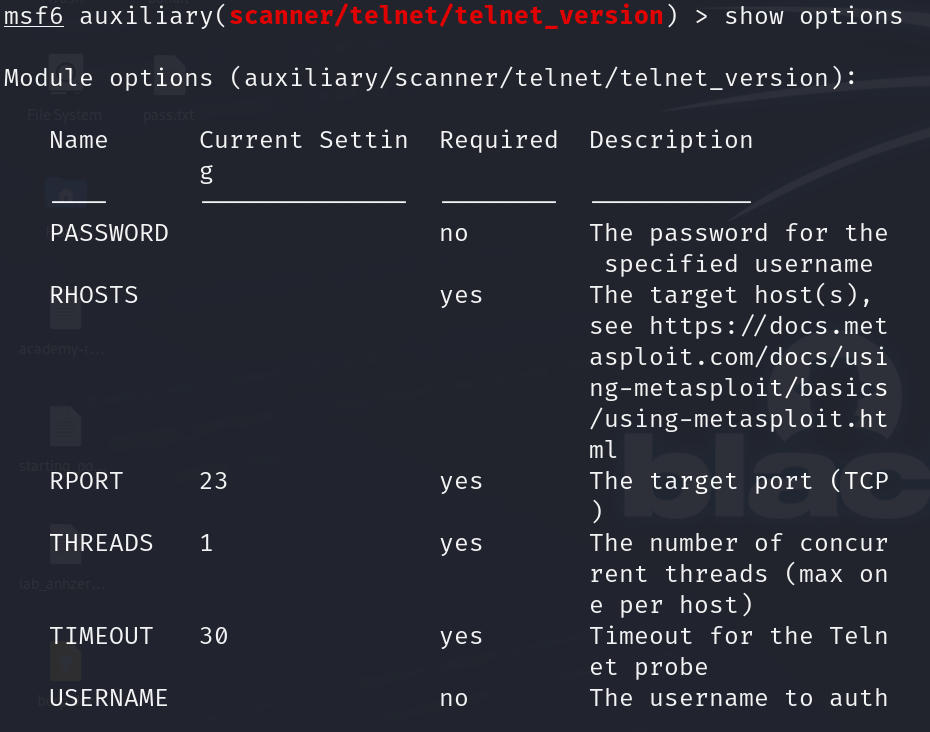
Để lấy cắp khóa riêng của mục tiêu:

1. **Port 23 telnet**

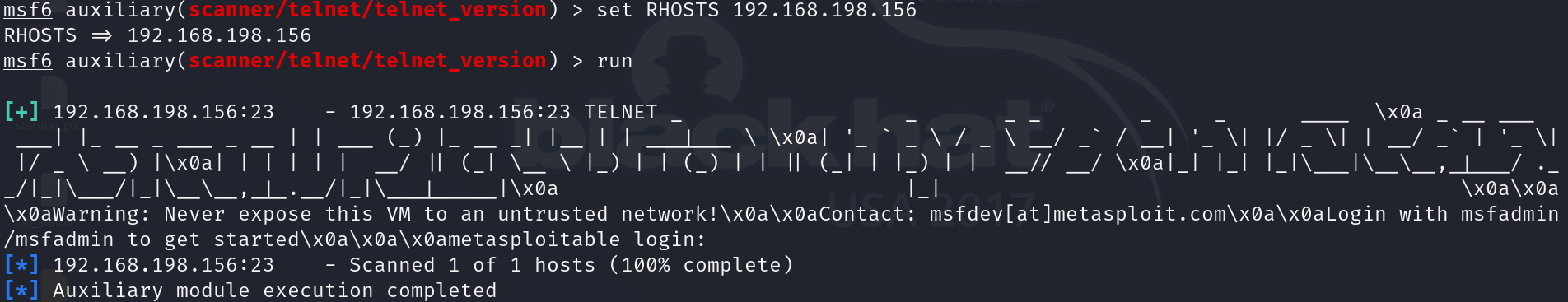
Telnet là một chương trình được sử dụng để phát triển kết nối giữa hai máy. Nó vốn dễ bị tấn công vì nó phân phối dữ liệu dưới dạng văn bản thuần túy, để lại nhiều lỗ hổng bảo mật. Chúng ta sử dụng Mô-đun phụ trợ cho cái này:



Hiển thị options:



Setting the attack and run.



Bây giờ bạn đã biết thông tin đăng nhập của tài khoản msfadmin và nếu bạn đăng nhập và thử nghiệm, bạn sẽ thấy rằng tài khoản này có quyền sudo nên bạn có thể thực thi lệnh với tư cách là root.

1. **Kết quả**

* Khai thác được lỗ hổng phổ biến thông qua các cổng dịch vụ
* Thực hiện việc lấy được shell root