**System Hacking through msfconsole**

1) Firstly, scan the system through nmap (nmap [ip] -v -sT -p 1-65535 -oX tcpscan.xml -sV ).

2) Then change the .xml file .html by (xsltproc tcpscan.xml -o tcpscan.html). It gives all the open ports and services that we will run in browser.

3) Now, type (service postgresql start) to start the service of msfconsole. Then type (msfconsole) run the console.

4) Then type (db\_status) to know that our system is connected to our database or not. You can also import the .xml file to this cosnsole by giving command (db\_import filename).

5) For enumeration :-- type search service (like ftp) auxiliary. It show varoius options like auxiliary/ftp/anonymous\_login. Then type show options and fill the blank spaces which stated yes and ignore the no options. For that set RHOSTS then give target system’s ip. Then type run/exploit to execute that auxiliary cmnd.

6) All these steps are also for exploitation. After all these steps there are some more commands written below.

7) After execution, type sessions to check session of that auxiliary. To access that session type (sessions -i [session no.]).

8) Now you got the system’s access. To check the machine name, you can type whoami/uname -a/hostname).

**Here are the various steps which I used to gain the access of a system**

**DESCRIPTION**

* System Hacking Process for Local Metasploitable Machine
* The local Metasploitable machine is a vulnerable system designed for penetration testing and learning ethical hacking. It is a virtual machine that can be installed on a computer to practice hacking techniques.
* To hack this machine, you would need to follow these steps:

1. Set up the Metasploitable machine on your computer.

2. Use tools like Nmap to scan the network and identify open ports and services.

3. Look for vulnerabilities in the services and applications running on the machine.

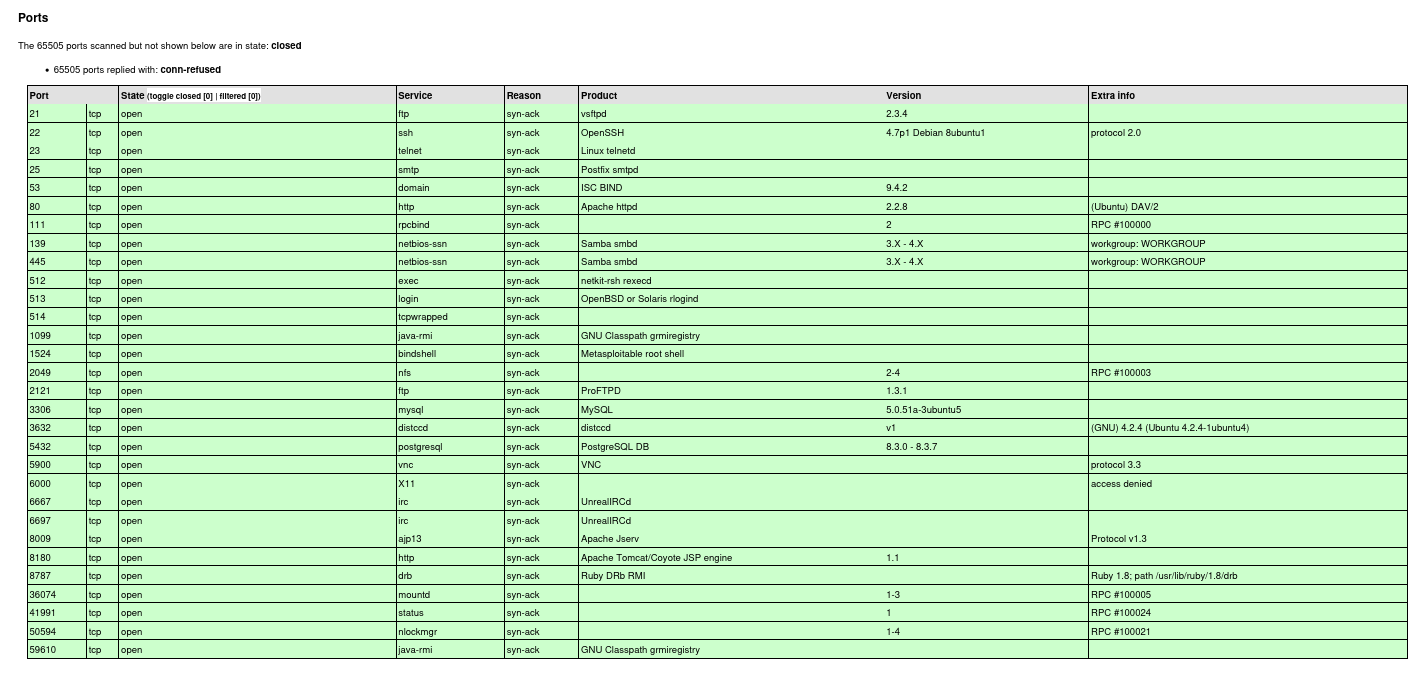
4. Use Metasploit to exploit any vulnerabilities found.

5. Gain access to the machine and install backdoors or malware.

6. Steal sensitive data and documents.

7. Maintain persistence and avoid detection by security measures.

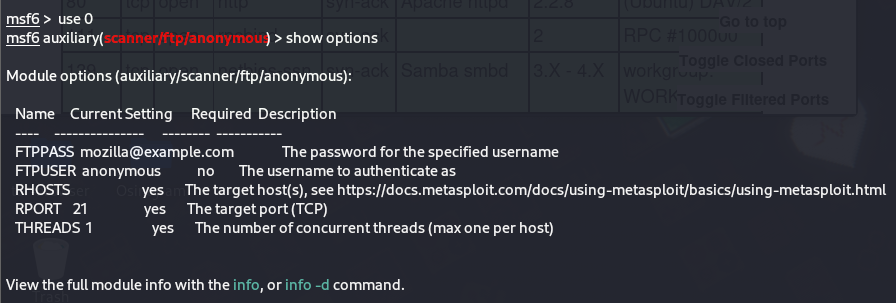
* The main steps of system hacking are written below :-
* **Open the tcpscan.html file in browser.**



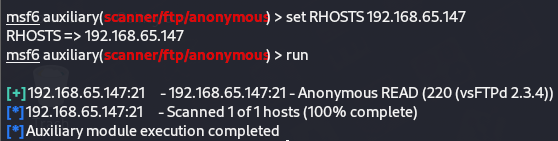
* **Now search (search ftp auxiliary) then :--**



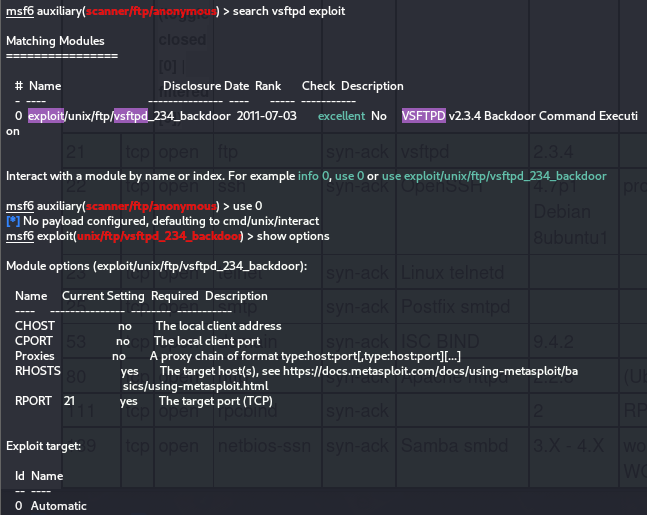
* **Type (use 0) because we select the first option and that’s name is 0.**

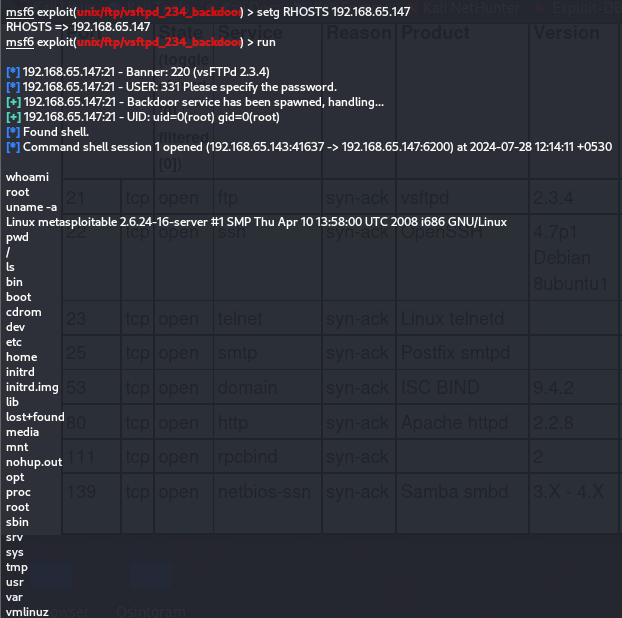


* **We got the username and password of the ftp. Now type set RHOSTS (ip of targeted system) because it stated yes. So it’s necessary to fill the blank space.**



* **It’s successfully completed now its time to exploit for that search (search ftp exploit). You can also search by their product name.**



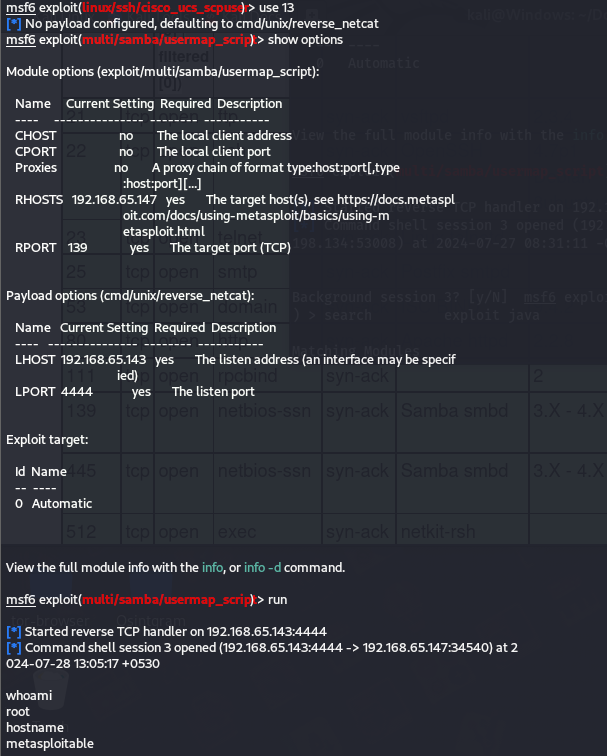
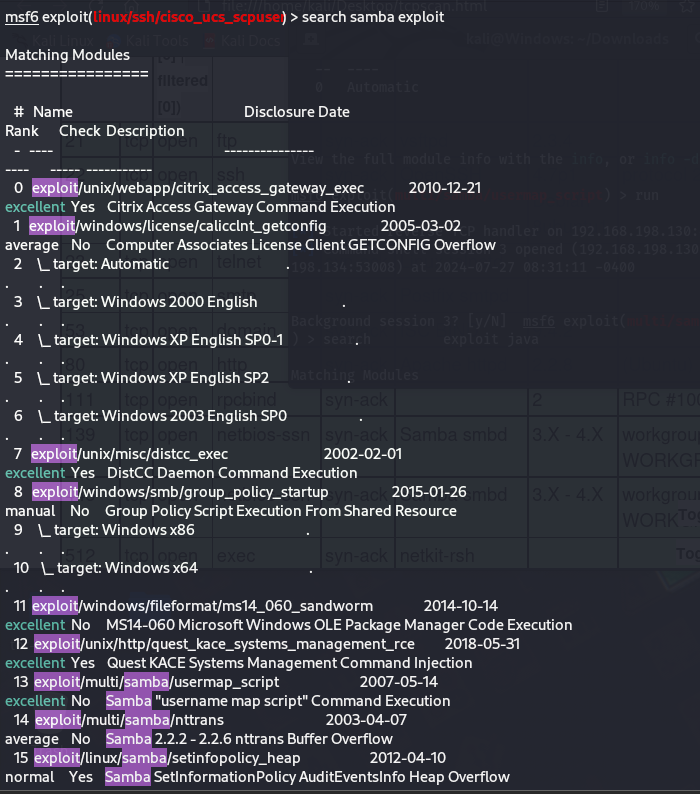


* **We successfully gain the access of a system through a port name called ftp.**
* **Now move into another port that is ssh.**

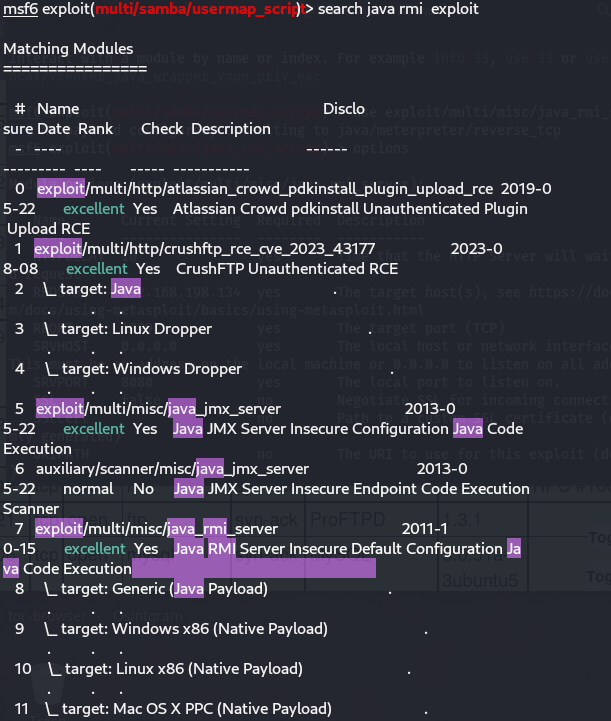


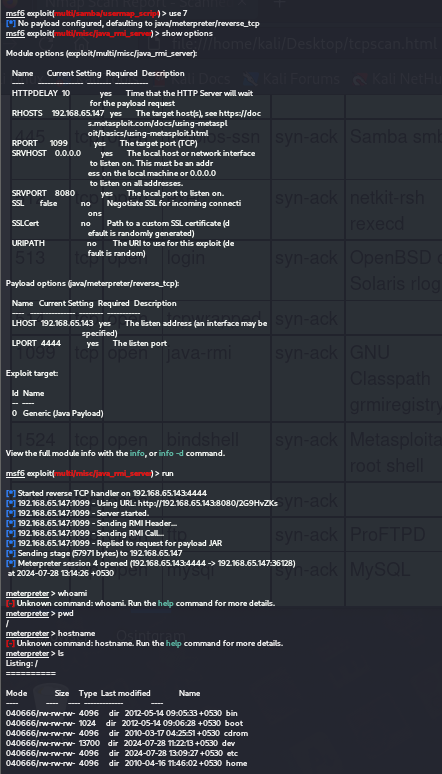


* **We know the default username and password of ssh that is user:user if we don’t know then, we search auxiliary and then put rockyou.txt in username and password section. We also got the access of ssh service of port number 22.**
* **Now move onto another service or port number.**
* **Search samba exploit, then choose an exploit**

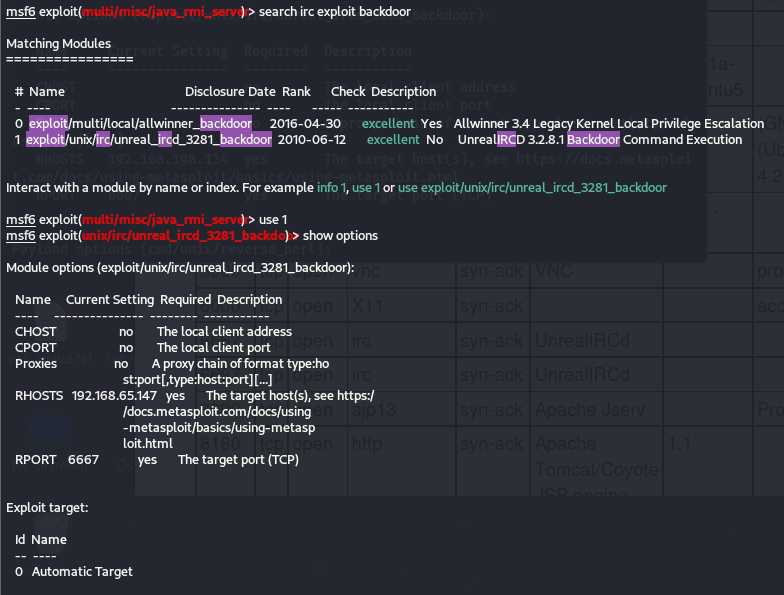


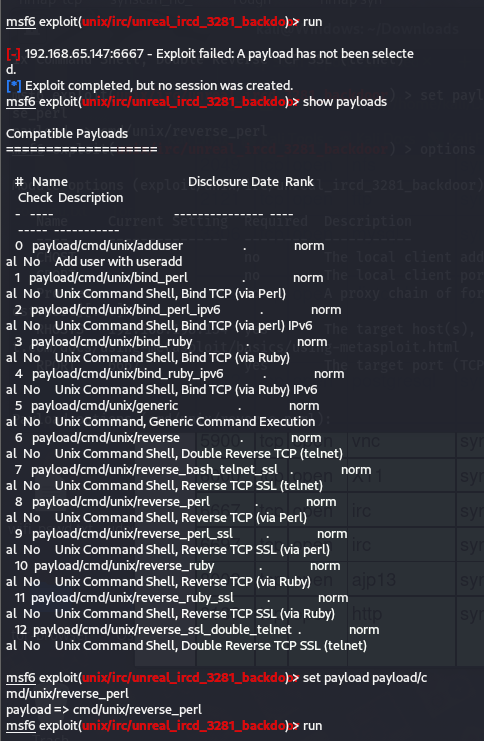
* **So we also got the access of samba service on port number 139.**
* **Move into another port number 1099.**



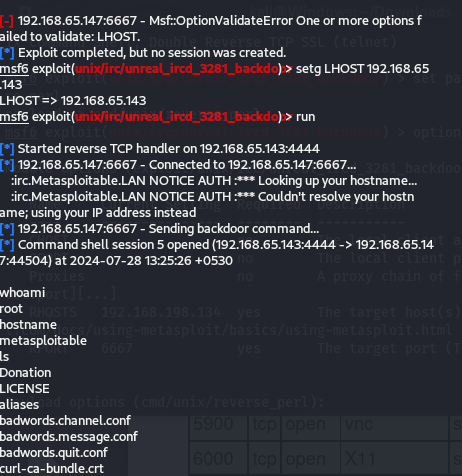


* **Here we got the access of another system through java-rmi service.**
* **Now, we move into another service called irc on port 6667.**





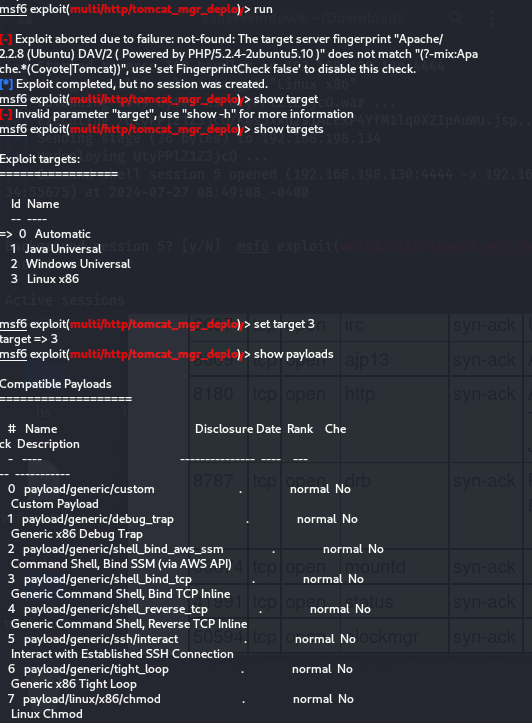
* **Here, we need to select a payload. For that type show payloads, then set payload by typing (set payloads [and name of that payload]).**



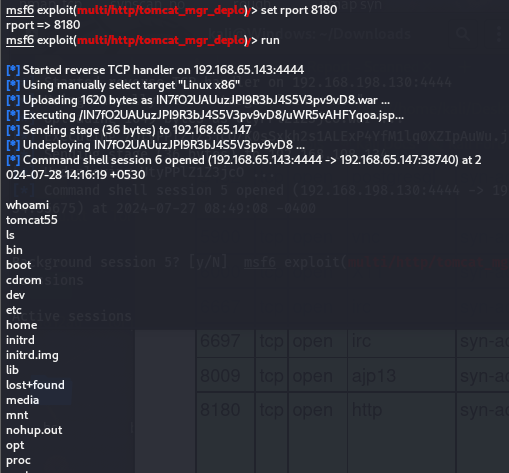
* **Now we got another error of not selecting the RHOSTS & LHOST. After giving these two then run the command and boom we got the access of targeted system.**
* **Let’s move onto another service called tomcat on port 8180.**



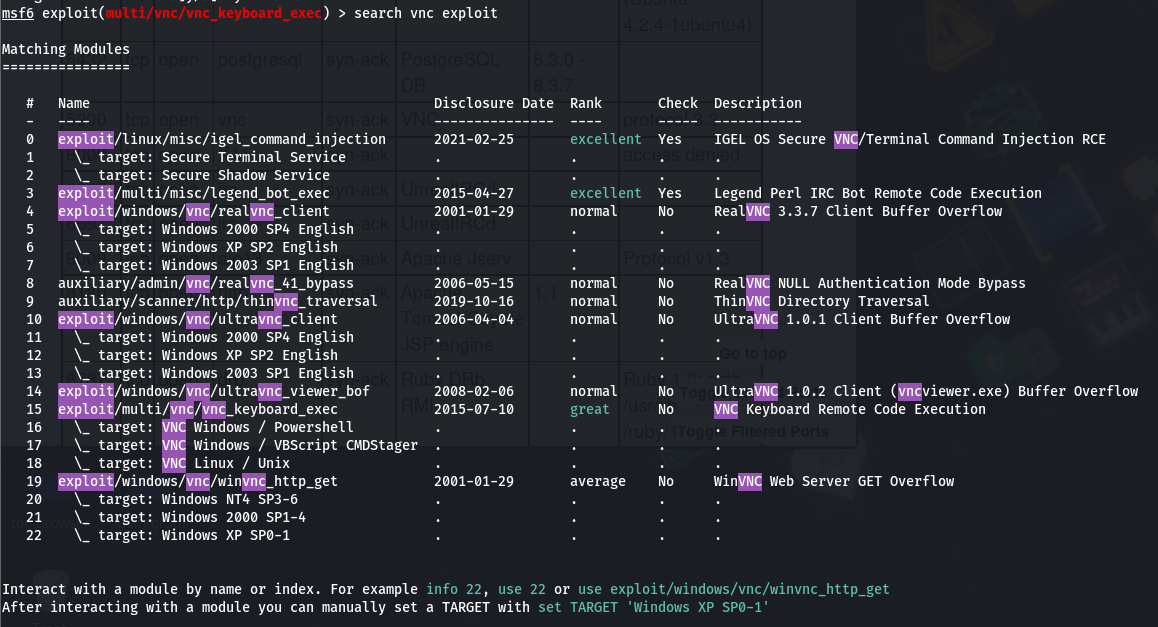
* **Then show options and fill the required options and run.**



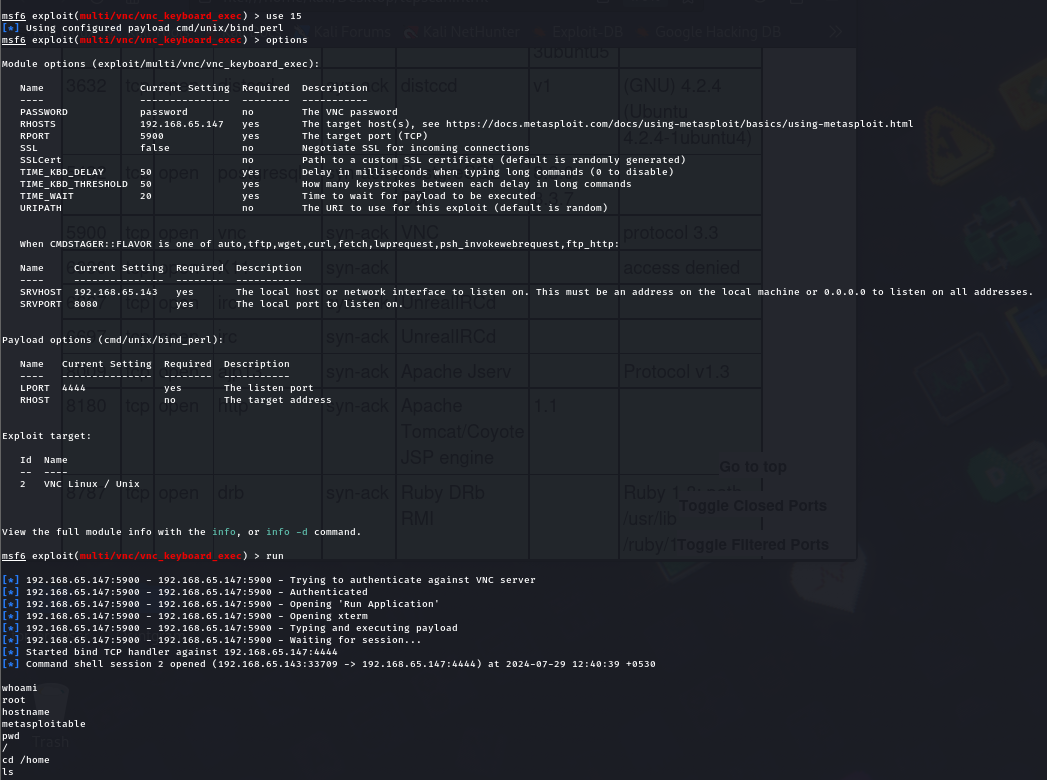
* **Then set payload, as we done previously.**



* **We got another access. Now search another exploit that name is vnc on port no. 5900.**



* **Now we type a exploit id/no. that we want to test.**



* **And we got the access. One thing is here that firstly we have to check the password for this exploit through auxiliaries.**

Ending note

* Please note that hacking into a system that is not your own is illegal and should only be done with the explicit permission of the system owner. Always use ethical hacking tools and methods for testing and learning purposes.
* The purpose of hacking into a local Metasploitable machine is to understand the process of ethical hacking and to practice ethical hacking techniques. It is not meant to cause any harm to the machine or its owner.
* Remember to only use this machine for educational and ethical hacking purposes, and never use it for any malicious activities.

THANKING YOU TO VIEW MY FILE AND GIVE ME SOME SUGGESTIONS.