Linux Privilege Escalation

Recon
- find / -writable — id
- find / -perm -4000 — whoami
- ss -tulpn — uname -a
- ip a — hostname
- ps aux — sudo -l
- env

Kernel
- Linux Exploit Suggester — Kernel Exploits
- OverlayFS — Dirty COW
- Dirty Pipe

Sudo
- env_keep — NOPASSWD
- sudo version — GTFOBins

SUID & SGID
- Custom Binaries — Find SUID
- GTFOBins

Capabilities
- cap_sys_admin — getcap -r /
- cap_dac_override — cap_setuid

Cron Jobs
- Wildcard Injection — Writable Scripts
- PATH Hijacking

Services
- Systemd Units — Writable Service Files

PATH Hijacking
- Relative Paths — PATH Variable

Hardening
- Audit Capabilities — Patch Kernel
- Remove SUID — Restrict Sudo

LOLBins
- vim — bash
- tar — find
- python — awk
- perl

Persistence
- rc.local — Cron
- Systemd — SSH Keys

Tools
- LSE — LinPEAS
- GTFOBins — LinEnum
- pspy — Linux Exploit Suggester

Files
- Logs — /etc/passwd
- Backups — /etc/shadow

Containers
- Kubernetes — Docker Group
- LXD

Credentials
- Passwords — SSH Keys
- Config Files — .bash_history

NFS
- no_root_squash

www.hackingarticles.in