Cheatography

Linux Permissions (Hardening) Cheat Sheet

by hlhlhl (hlhlhl) via cheatography.com/218585/cs/48357/

Ownership & Permissions

Command	Purpose
`ls -l`	View permissions
`stat FILE`	Detailed file info
`chmod MODE FILE`	Change permissions
`chown USER FILE`	Change owner
`chgrp GROUP FILE`	Change group
`umask`	View default permissions
`umask 022`	Set default permissions

Common Permission Values

600	Owner RW
644	Owner RW, Others R
700	Owner RWX
755	Owner RWX, Others RX
777	Everyone RWX (Avoid)

ACL (Access Control Lists)

Command	Purpose
`getfacl FILE`	View ACL
`setfacl -m u:USER:rwx FILE`	Add ACL
`setfacl -x u:USER FILE`	Remove ACL
`setfacl -b FILE`	Remove all ACLs

Attributes

Command	Purpose
`lsattr`	View attributes
`chattr +i FILE`	Immutable
`chattr -i FILE`	Remove immutable
`chattr +a FILE`	Append only

Reference Box

r = Read
w = Write
x = Execute
4 = Read
2 = Write
1 = Execute

SUID = Run as Owner
SGID = Run as Group
Sticky = Only Owner Can Delete

SUID / SGID

Command	Purpose
`find / -perm -4000`	Find SUID files
`find / -perm -2000`	Find SGID files
`chmod u-s FILE`	Remove SUID
`chmod g-s FILE`	Remove SGID

Sticky Bit

Command	Purpose
`chmod +t DIR`	Set Sticky Bit
`chmod -t DIR`	Remove Sticky Bit

Security Checklist

Least Privilege
Avoid chmod 777
Secure ~/.ssh (700)
Secure private keys (600)
Protect /etc/shadow
Audit SUID files
Review ownership

By **hlhlhl** (hlhlhl)
cheatography.com/hlhlhl/

Published 7th August, 2026.
Last updated 7th August, 2026.