

Ownership & Permissions	
Command	Purpose
<code>ls -l</code>	View permissions
<code>stat FILE</code>	Detailed file info
<code>chmod MODE FILE</code>	Change permissions
<code>chown USER FILE</code>	Change owner
<code>chgrp GROUP FILE</code>	Change group
<code>umask</code>	View default permissions
<code>umask 022</code>	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)

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	

ACL (Access Control Lists)	
Command	Purpose
<code>getfacl FILE</code>	View ACL
<code>setfacl -m u:USER:rwX FILE</code>	Add ACL
<code>setfacl -x u:USER FILE</code>	Remove ACL
<code>setfacl -b FILE</code>	Remove all ACLs

Attributes	
Command	Purpose
<code>lsattr</code>	View attributes
<code>chattr +i FILE</code>	Immutable
<code>chattr -i FILE</code>	Remove immutable
<code>chattr +a FILE</code>	Append only

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

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

Sticky Bit	
Command	Purpose
<code>chmod +t DIR</code>	Set Sticky Bit
<code>chmod -t DIR</code>	Remove Sticky Bit

Secure Boot	
Command	Purpose
<code>mokutil --sb-state</code>	Check Secure Boot status
<code>mokutil --disable-validation</code>	Disable Secure Boot validation (MOK)
<code>mokutil --enable-validation</code>	Enable Secure Boot validation (MOK)

