

Linux File Permissions Reference

CHMOD & CHOWN Cheat Sheet
For Ethical Hackers

Basic Concepts

Permission Types

- r (read) - Value 4: View file contents
- w (write) - Value 2: Modify files
- x (execute) - Value 1: Run programs

User Categories

- u (user/owner) - File's owner
- g (group) - Group members
- o (others) - All other users
- a (all) - All three categories

Viewing Permissions

```
# List with permissions
ls -l

# Show hidden files
ls -la

# Numeric permissions
stat -c '%a %n' filename
```

CHMOD Syntax

Symbolic Mode

Format: chmod [who] [operator] [perms] file

Operators

- + Add permissions
- - Remove permissions
- = Set exact permissions

Examples

```
# Add execute for owner
chmod u+x script.sh

# Remove write from group/others
chmod go-w config.conf

# Set exact permissions
chmod u=rw,go=r file.txt

# Add execute for all
chmod a+x tool
```

Numeric Mode

Format: chmod [numeric] file

Calculate by adding values: r(4) + w(2) + x(1)

Common Permission Sets

Num	Sym	Usage
777	rwxrwxrwx	DANGER! Full access
755	rwxr-xr-x	Public executables
750	rwxr-x--	Group-shared tools
700	rwx----	Private scripts
644	rw-r-r-	Public config files
640	rw-r---	Restricted configs
600	rw----	Private data/keys
400	r----	Read-only secrets

CHOWN Syntax

Basic Usage

```
# Change user owner
chown username file
```

```
# Change user and group
chown user:group file
```

```
# Change only group
chown :groupname file
```

```
# Recursive
chown -R user:group dir/
```

Advanced Options

```
# Follow symlinks
chown -L user:group link
```

```
# No dereference symlinks
chown -h user:group link
```

```
# Reference file ownership
chown --reference=ref target
```

```
# Numeric UID/GID
chown 1000:1000 file
```

Special Permissions

SUID (4000)

Runs with owner's permissions

```
# Set SUID
chmod 4755 binary # rwsr-xr-x
```

```
# Find SUID files
find / -perm -4000 2>/dev/null
```

Security Risk

SUID files owned by root are privilege escalation vectors!

SGID (2000)

- Files: Run with group permissions
- Dirs: New files inherit group

```
# Set SGID
chmod 2755 file      # rwxr-sr-x
chmod 2775 dir/       # rwxrwsr-x

# Find SGID files
find / -perm -2000 2>/dev/null
```

Sticky Bit (1000)

Users can only delete own files

```
# Set sticky bit
chmod 1777 /tmp/      # rwxrwxrwt

# Find sticky directories
find / -type d -perm -1000 2>/dev/null
```

Security Configurations

Critical Files

File	Owner:Group	Perms
/etc/passwd	root:root	644
/etc/shadow	root:shadow	640
/etc/sudoers	root:root	440
~/.ssh/id_rsa	user:user	600
~/.ssh/authorized_keys	user:user	600

Secure SSH Keys

```
chown user:user ~/.ssh/id_rsa
chmod 600 ~/.ssh/id_rsa
chmod 700 ~/.ssh/
```

Web Application

```
# Set ownership
chown -R www-data:www-data /var/www/

# Directory permissions
chmod 750 /var/www/html/

# File permissions
find /var/www/ -type f -exec chmod 640 {} \;
```

Vulnerability Detection

Finding Security Issues

```
# World-writable files
find / -type f -perm -o+w 2>/dev/null

# SUID binaries
find / -perm -4000 -ls 2>/dev/null

# World-writable dirs w/o sticky
find / -type d -perm -o+w ! -perm -1000 2>/dev/null

# Files with no owner
find / -nouser -o -nogroup 2>/dev/null

# Find by owner
find / -user targetuser 2>/dev/null

# Find by group
find / -group groupname 2>/dev/null
```

Check Critical Files

```
# Verify shadow file perms
[ $(stat -c %a /etc/shadow) -ne 640 ] &&
echo "WARNING!"

# Check if readable
[ -r /etc/shadow ] && echo "Shadow readable!
"

# List critical files
ls -la /etc/passwd /etc/shadow /etc/sudoers
```

Advanced Techniques

Recursive Operations

```
# Set dirs only
find /path -type d -exec chmod 750 {} \;

# Set files only
find /path -type f -exec chmod 640 {} \;

# Change ownership recursively
chown -R user:group /path/
```

Copy Permissions

```
# Copy permissions
chmod --reference=source target

# Copy ownership
chown --reference=source target
```

Default Permissions (umask)

```
# View current umask
umask

# High security (700/600)
umask 077

# Team environment (750/640)
```

```
umask 027

# Calculate final permissions
# Files: 666 - umask
# Dirs: 777 - umask
```

ACLs & Extended Attributes

Access Control Lists

```
# View ACLs
getfacl filename

# Set user ACL
setfacl -m u:username:rwx file

# Set group ACL
setfacl -m g:groupname:rx file

# Remove ACLs
setfacl -b file
```

Extended Attributes

```
# View attributes
getfattr -d file

# Make immutable
chattr +i critical_file

# Make append-only
chattr +a /var/log/audit.log

# View file attributes
lsattr file
```

Capabilities

```
# View capabilities
getcap file

# Set capability (bind to port <1024)
```

```
setcap 'cap_net_bind_service=+ep' /usr/bin/
       service

# Find files with capabilities
find / -type f -exec getcap {} \; 2>/dev/
       null
```

Exploitation Techniques

Privilege Escalation

```
# Writable cron jobs
find /etc/cron* -type f -perm -o+w 2>/dev/
       null

# Writable service files
find /etc/systemd -perm -o+w 2>/dev/null

# Config files with credentials
find / -name "*.conf" -perm -o+r 2>/dev/null
       | xargs grep -l "password"
```

Lateral Movement

```
# Readable home directories
find /home -maxdepth 1 -type d -perm -o+rx

# Service account files
find /tmp -user www-data 2>/dev/null

# Check running processes
ps aux | grep targetuser
```

Permission Interpretation

Symbolic Format

String	Numeric	Description
rwxrwxrwx	777	All permissions
rwxr-xr-x	755	Owner full, others r+x
rxw----	700	Owner only
rw-r-r-	644	Owner r+w, others r
rw-r--	640	Owner r+w, group r
rw----	600	Owner r+w only
r----	400	Owner read-only
rwsr-xr-x	4755	SUID + 755
rwxr-sr-x	2755	SGID + 755
rwxrwrxrwt	1777	Sticky + 777

File Type Indicators

- - Regular file
- d Directory
- l Symbolic link
- s Socket
- p Named pipe
- c Character device
- b Block device

User & Group Management

User Operations

```
# Create user
useradd -m -s /bin/bash username

# Change primary group
usermod -g groupname user

# Add to groups
usermod -aG group1,group2 user

# Display user info
id username
```

Group Operations

```
# Create group  
groupadd groupname  
  
# Add user to group  
gpasswd -a username group  
  
# Remove from group  
gpasswd -d username group  
  
# Display groups  
groups username
```

Quick Reference

Essential Commands

```
# Add execute  
chmod +x file  
  
# Private to owner  
chmod 600 file  
  
# Secure config  
chmod 640 file  
  
# Shared directory  
chmod 1775 dir  
  
# Change owner  
chown user:group file  
  
# Recursive change  
chown -R user:group dir/
```

Risk Assessment

Critical: World-writable system files, readable /etc/shadow
High: Incorrect SSH key permissions, SUID vulnerabilities
Medium: Weak directory permissions, group access issues

Mount Options

```
# Disable execution  
mount -o noexec /dev/sda2 /mnt/data  
  
# Disable SUID  
mount -o nosuid /dev/sda3 /mnt/untrusted  
  
# Read-only  
mount -o ro /dev/sda1 /mnt/readonly
```

Forensics & Incident Response

Timeline Analysis

```
# Recent permission changes  
find /etc -type f -mtime -7 -ls  
  
# New SUID files  
find / -perm -4000 -mtime -7 2>/dev/null  
  
# Permission timeline  
find / -exec stat -c '%y %U:%G %a %n' {} \;  
2>/dev/null | sort
```

Restore Secure Permissions

```
# Reset critical files  
chmod 644 /etc/passwd  
chmod 640 /etc/shadow  
chmod 440 /etc/sudoers  
  
# Reset home directory  
chown -R user:user /home/user/  
find /home/user -type d -exec chmod 750 {}   
\;  
find /home/user -type f -exec chmod 640 {}   
\;
```