**Security and Permissions commands in RedHat Linux**

In Red Hat Linux and other Linux distributions, security and permissions are managed using various commands and utilities. Here are some common commands for managing security and permissions:

* **chmod: Changes the permissions of files and directories.**
* **Symbolic notation:**

chmod u+x filename # Add execute permission for the owner

chmod go-w filename # Remove write permission for group and others

* **Numeric notation:**

chmod 755 filename # Give read, write, and execute permissions to owner; read and execute permissions to group and others

* **chown: Changes the owner and group of files and directories.**

chown username:groupname filename

* **chgrp: Changes the group ownership of files and directories.**

chgrp groupname filename

* **ls: Lists directory contents along with their permissions.**

ls -l

* **umask: Sets the default permissions for newly created files and directories.**

umask 555

* **passwd: Changes the password for a user.**

passwd username

* **su: Switches the user identity to another user, typically to root.**

su - username

* **sudo: Executes commands with superuser privileges.**

sudo command

* **getfacl: Displays file access control lists (ACLs) for files and directories.**

getfacl filename

* **setfacl: Sets file access control lists (ACLs) for files and directories.**

setfacl -m u:username:rw filename # Give read and write permissions to a specific user

These commands help in managing security and permissions on Red Hat Linux systems, ensuring that access to resources is controlled and secure.