

Marie to the	Mission Name: Users and Permissions	
	30 3	
*	In order to protect the integrity of the computer and to	
	In order to protect the integrity of the computer and to protect users from each other, the concept of users arouse.	
	Every user has their own set of permissions.	
*	Commands to see, which user we are coverently working in:	
	i) whoami	
	i) who ami ii) id -un	
1		
1/	Both command gives same output.	
	, size	
*	groups are a mechanism used to facilitate granting and	
	revoking permissions from the user.	
*	Command to check group's associated with the user: "groups"	
*	N. I. C.	
	* When a user creater a file or directory ownership is attributed to the user who created it.	
	Service of the servic	
*	By default, the group ownership is given to the primary.	
	group of the users who created the file	
9	A primary group is simply a group that is associated with a	
	user. It will typically have the same name & group	
	number as that of the uses.	
	Permissions	
	remarked administration of the second	
	I vient or vy man mining in a constant	
	owner avner group Everyone else	
	LANCE Was been to be a	
163	musing among A court de like of	
100	Constituting when a best ? ? I will	
Section	on or there we there is a surface	

Pate	
Date	
0/2010	

	DatePage				
*	Sometimes were need to inchange permissions of the existing files.				
*	* To do so, we use the following command:				
	chmod permission file.				
Chem	remove read [ugoa][+-=][rwx] Execute user group others out				
1	Eg:-				
	Before Command After command				
V = - ()	Deen't matter chmod g=xx, u=wxx== rwxy=xy=- r-xy= chmod g+x, o+r r-xy=- t-xy=xy= chmod u+w, g-x, o-r rwxy= chmod u+w, g-x, o-r rwxy= chmod g=xx, u=xwxy= r-xy=xy=				
	poesii matter chimod a= YWX YWXYWXYWX				
*	"stat" command can be used to know the stats of a file.				
	Stats includes permissions, uid and gid.				
*	Octal Notation:				
•	x: 1 (only execution permission) -w-: 2 (write only permission)				
•	· T: 4 (read only permissions) · T-X: 5 (read & execute permissions)				
•	r-x: 5 (read & execute permissions) rw-: 6 (read & write permissions) rwx: 7 (read, write & execute permissions)				

Date	0
Page	/

	487	Date	
	e.	(Tago	
	Eg:-		
	Symbolic Notation	Octal Notation	
	0	DC124 MITAFION	
	TW-TW-T	66 4	
	3MX1M-1-	764	
	XXX	7.50	
	YWXY-X-WX	753	
*	A user that has full access to all files and commands is		
	called a root user.		
×	soot is the administrator/superuser.		
4	To run a program/command with mot priveledge, "sudo"		
	(command) can be used.		
*	Eg:- sudo mkdir oop		
1/14	Suido ago only ha wood has wood of a reconstruction		
1	Sudo can only be used by users who are part of sudo group.		
*	Ownership of a file can be changed by:		
	chown [new_owner][:new_group].file		
Ĭ.	Jan		
	die deux and can also be also		
	optional i e any one can also be given. Not a mandate to give both.		
(L)		0	