## Unix Access Control Basics,

## CE2 – HIM

## May 20, 2011

##### Login in to the Unix machine “paradox.sis.pitt.edu”

1. Click “Start” – and choose “All Programs”
2. Look for “SSH Secure Shell” – click on it and then click “SSH Secure Shell Client”
3. Click on “Quick Connect” in the client window that pops up.
4. Enter Hostname = paradox.sis.pitt.edu
5. Enter the Username/ Password given to you

##### Exercise 1 – access bits

1. Type “ls” and then “ls –al”

Discuss the various pieces of information you see

1. Create a director called “testDir”
2. Create a file called “testFile1.txt” in this subdirectory
3. See the directory listing

Discuss the various pieces of information you see

1. Do “cd testDir”
2. Do “ls –al”
3. Create a subdirectory called “testSubDir” (and check with “ls –al”)
4. Create a file called “testFile2.txt” in this subdirectory
5. Go to the testDir
6. Change modes of “testDir” with the following octal expressions

755 (then do “ls –l”) - what permissions are allowed ?

 Do : “ls –al” and “ls –al testDir” --- what do you see?

 Do: “cd testSubDir” -- what happens?

 If cd was successful then do the ls –al to see the info; if not discuss why?

Repeat these with the following changes to permission modes of testSubDir

 444

 700

1. Change permission setting of testFile.txt so that the following is allowed

1 2 3

Other write only read only read, execute

Group read, write write only read, write

Owner write, execute read, write read, write, execute

Bits are \_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

##### Exercise 2: umask

1. Type ‘umask” and “ls –al”
2. Discuss what is creation mask vs. umask and how to compute the final permissions setting
3. Set umask to 777
4. Create directory ts1 and file ts1.txt
5. See directory listing and discuss the permission setting
6. Set umask to 000
7. Create directory ts2 and file ts2.txt
8. See directory listing and discuss the permission setting
9. Set umask to 521
10. Create directory ts3 and file ts3.txt
11. See directory listing and discuss the permission setting
12. Change umask values such that the default *directory* permission setting is

713 [The umask value is \_\_\_\_\_\_\_\_\_\_\_\_\_\_ ]

222 [The umask value is \_\_\_\_\_\_\_\_\_\_\_\_\_\_ ]

321 [The umask value is \_\_\_\_\_\_\_\_\_\_\_\_\_\_ ]

1. Change umask values such that the default *file*  permission setting is

173 [The umask value is \_\_\_\_\_\_\_\_\_\_\_\_\_\_ ]

212 [The umask value is \_\_\_\_\_\_\_\_\_\_\_\_\_\_ ]

671 [The umask value is \_\_\_\_\_\_\_\_\_\_\_\_\_\_ ]

##### Exercise 3: other unix commands

 Try out other commands – cp, mv, rmdir, rm

 Use man command to see what each does.

##### Exercise 2: umask

1. Switch user roles as *user1* and then back to *root* using the su command
	1. whoami
	2. su user1
	3. su **OR** su root
2. Create a new file as root user
	1. touch /home/user2/HelloWorld
	2. ls –l /home/user2/HelloWorld (observe owner and group)
3. Change group ownership as well as user ownership of the file
	1. chgrp users /home/user2/HelloWorld
	2. chown user2:users /home/user2/HelloWorld
	3. ls –l /home/user2/HelloWorld (observe owner and group)

##### Part II: Exercise File and Folder Permissions

1. Log in as root user
2. Observe the results of *ls* and *cd* commands:
	1. su user1
	2. ls -al /home/user2 (Can you list directory?)
	3. cd /home/user2 (Can you change directory?)
3. Change directory permissions of *user2* directory and try again as *user1*:
	1. su root
	2. chmod 740 /home/user2
	3. Repeat step 2. (Can you list or change directory?)
	4. su root
	5. chmod 750 /home/user2
	6. Repeat step 2. (Can you list or change directory?)
	7. touch /home/user2/hello12.txt (Can you create the new file?)
	8. su root
	9. chmod 770 /home/user2
	10. su user1
	11. touch /home/user2/hello12.txt (Can you create the new file?)

##### Part III: Default File Permissions

1. Log in as root user
2. Use *umask* command to check the current mask permission and assign a new mask.
	1. umask
	2. What is the current mask? How is it interpreted?
	3. cd /test
	4. touch testmask1
	5. ls -al
	6. What are the permissions of the file *testmask1*?
	7. umask 0077
	8. touch testmask2
	9. Now what are the permissions of the file *testmask2*?

##### Part IV: *setuid* bit, *setgid* bit and *sticky* bit

1. Log in as root user
2. The following commands demonstrate how processes are affected when the *setuid* bit is set.
	1. which touch
	2. ls –l /bin/touch
	3. chmod 4755 /bin/touch
	4. ls –l /bin/touch
	5. ls –l /home/user2
	6. chmod 700 /home/user2/HelloWorld
	7. ls –l /home/user2 (observe timestamp and permissions)
	8. su user1
	9. touch /home/user2/HelloWorld
	10. ls –l /home/user2 (observe timestamp, is it updated?)
	11. su root
	12. chmod 0755 /bin/touch
	13. su user1
	14. touch /home/user2/HelloWorld
3. Why permission denied, while previously allowed?

##### *Restore the system*

1. su root
2. umask 0022
3. chmod 0755 /bin/touch
4. userdel user1
5. userdel user2
6. rm –rf /home/user1
7. rm –rf /home/user2
8. rm –rf /test
9. rm –rf /home/test/

## Port Redirection

###### Step I: Get the FTP server running

1. Run “FTPServer.exe” in the subfolder “1.0 PortRedirection”.
2. Check if the users include “anonymous”. You need to create the <user> if it does not exist.
3. Click the **Start** button on the top left of the FTP Server configuration panel.

###### Step II: Confirm that the FTP server is running on port 21

1. In command prompt, type “netstat –a”. See if the FTP server is running on port 21.
2. From another machine, type “ftp <ip-address>”. You should be able to log in.

###### Step III: Redirect the network traffic on port 21 to port 30

1. In command prompt, type “fpipe –l 30 –s 30 –r 21 –v <ip-address>”. Do not close the terminal.
2. Run “netstat –a -b” (requires elevation). What port is the executable “fpipe” running on?

###### Step IV: Start a ftp-client session and connect to the server through fpipe

1. On the FTP client machine, open up a new command prompt terminal.
2. At the prompt enter command: ftp
3. Enter command: open
4. At the “to” prompt, type: <ip-address> 30
5. At the “username” prompt, enter: anonymous
6. If you are connected, check the FPIPE terminal. What is the response?
7. At the “password” prompt, enter: (no password, just press Enter)
8. Type command: dir
9. Check the FPIPE terminal. What is the response?