SECURE SCRIPTING (Python)

**ADVANCED CONTROL**

# LAB: FILE SYSTEM SCANNER

This lab walks you through building a simple file system scanner. The scanner will be able to do three things. First, it will generate a list of files and file attributes, including a checksum of each file’s contents. Second, it can compare the files and file attributes of the files in the directory with that list. Third, it can delete that list.

For this lab, you will need the four files in the current directory. Please do not change anything in these files — one of the tests you need to run depends on those files being unchanged.

* abcde
* demofor
* demofor2
* demofor3

### Lab exercise 1

This exercise starts you off. You do not need to write any scripts until Part D. First, list the attributes of the files in the directory “sample”, one per line.

1. When you execute the command *dir (filename)* with the option, which of the desired attributes are printed?
2. What does the command *certutil -hashfile (filename)* print?
3. How would you cause both outputs to be printed at the same time?
4. Write a shell script that uses a *for* loop to list the attributes of the files in the directory “sample”, one per line. Call this script “scan1.py”.

Run your script. You should get information for four files. The checksums of the files “abcde” and “demofor” are:

5cb19ad82ef34ea11bd909702fe3cdddbdf26951 – abcde,py

9aa856b1f7d9a6b8e8a364064a63a63e4492c376 - demofor.py

### Lab Exercise 2

You are now going to modify the script you wrote for Lab Exercise 1D to see if a master file exists and, if it doesn’t, create one. Then, in the loop, you will ignore any non-regular files and the master file.

1. At the beginning of the script, add a line that defines a variable called MASTER, and give it the initial value “MasterList”. Call this script “scan2a.py”. When you are done, save a copy because you will use this in Lab Exercise 3.
2. After the variable definition but before your loop, test to see if the file named by the value of the variable MASTER exists. If so, print the message that the file “exists; please delete it” and exit, giving exit status code 1. If not, create it. Call this script “scan2b.py”.
3. In the *for* loop, before you print the file attributes, check to see if the file being examined is either a regular file or the MasterList file. If it is neither, immediately go to the next file (that is, do not get the file attributes). Call this script “scan2c.py”.
4. Modify your script so that the attributes are stored in the file named by the value of the variable MASTER. Call this script “scan2d.py”.
5. Finally, if everything works, have the script exit with an exit status code of 0. Call this script “scan2e.py”.

Run your script. There should be no output. Then look for a file called MasterList and compare its contents to what you got for the output of scan1.py. The outputs for the files abcde, demofor, demofor2, and demofor3 should be the same. The other files that are present should all be ones you created or put there.

### Lab Exercise 3

This exercise uses the copy of the script you saved after completing Lab Exercise 2A. We will be modifying it in a way similar to the rest of Lab Exercise 2.

1. At the beginning of the script, add a line that defines a variable called TMP, and give it the initial value “tmp+processID+”.txt”. Then add another line that creates the file named by the value of TMP. Call this script “scan3a.py”. What is the actual name of the file created?
2. In the *for* loop, before you print the file attributes, check to see if the file being examined is the file named by the value of TMP, and if so, *immediately* go to the next file (that is, do not get the file attributes). Call this script “scan3b.py”.
3. Modify your script so that the attributes are stored in the file named by the value of the variable TMP. Call this script “scan3c.py”.
4. After the loop, print the message “Changed files:”, and then compare the contents of the files named by TMP and MASTER. Use *fc.exe* to generate the comparison. Call this script “scan3d.py”. What happens if the file named by the value of MASTER does not exist?
5. Before the loop, check that the master file (the file named by the value of MASTER) exists. If it does not, print an error message saying “Master file does not exist; please generate it” and exit with an exit status code of 1. Call this script “scan3e.py”.
6. Conclude by using the command *del* to delete the file named by the value of TMP after the comparison in Part D. Again, have the script exit with an exit status code of 0. Call this script “scan3f.py”.

When you test this script, the MasterList file must already exist. If it does not, execute the script you wrote in Lab Exercise 2 (scan2e.py).

You should get at least one line for the file MasterList. You will also get other lines corresponding to the scripts you wrote. As long as you get the line for MasterList, you’re doing it right.

Also, from the command interpreter, check the exit code. Immediately after you execute your script, type

echo $lastExitCode

This prints the exit status code of the command that finished most recently. That command is your script. So, you should see True.

Play around with these scan2e and scan3f files with your sample files. Try changing one of the files in the sample folder to see if scan3f prints that a file has changed. To reset the Master file, simply execute scan2e.

### Lab Exercise 4

Now combine the scripts you wrote for Lab Exercises 2 and 3. Your script, which you are to call “scan4.py”, should define the variables TMP and MASTER, then do the parts of Lab Exercises 2 and 3 in the following order:

2A, 3A, 3B, 2C, 3C, 3D, 3E, 2E

Do not include Exercises 2B or 2D in this script.

Run your script twice to test it. First, just run it. The list of changed files should have only the ones you have written and left in the directory. Then change the time of last modification of the file “abcde” by going into the file typing something, deleting it, and then saving it.

Now rerun the script. The list should be the same as before but with the addition of “abcde”.

### Lab Exercise 5

Now you will modify the script from Lab Exercise 4 to handle two options. First we will handle the option –g, which creates the master file, then -d, which deletes the master file. If the script is called with no arguments, it will generate a list of files the attributes or contents of which have changed since the master list was created.

For the –g option:

1. Create a variable called GENMASTER and, at the beginning of the script, set it to “False”. Call this script “scan5a.py”.
2. If the –g option is given, set GENMASTER to “yes”. Call this script “scan5b.py”. What happens if you give some other argument or option, like “-m”?
3. After the argument processing loop, check to see whether GENMASTER is “True”. If it is, do what you do in the script that was the answer to Lab Exercise 2; you can just copy it into this script if you like, but if you do, don’t copy the line setting the variable MASTER. Then exit with an exit status code of 0. If it is “False”, do what you do in the script that was the answer to Lab Exercise 3; again, you can just copy it into this script if you like, but don’t copy the lines setting the variables MASTER and TMP. Exit with an exit status code of 0. Call this script “scan5c.py”.

Test your script by running it in the sample directory. First, do not give the –g option; you should get a list of files that have changed, most likely including abcde (from Lab Exercise 4). Then run it again giving the –g option. You should get the error message saying the master file exists, please delete it.

For the –d option:

1. Create a variable called DELMASTER and, at the beginning of the script, set it to “no”. Call this script “scan5d.py”.
2. If the –d option is given, set DELMASTER to “yes”. If any command-line option (or argument) other than –d or –g is given, print the error message “Unknown option” followed by the option, and exit with an exit status code of 1. Call this script “scan5e.py”.
3. Before you check the value of the variable GENMASTER, if the value of DELMASTER is “yes”, check that the master file exists. If it does, delete the master file and exit with an exit status code of 0. If it does not, print “Master file does not exist; please generate it” and exit with a status code of 1. Otherwise, if the –d option is not given, continue. Call this script “scan5f.py”.

Test your script by running it in the parent director of the sample directory. First, do not give the –d option; you should get a list of files that have changed, most likely including abcde (from Lab Exercise 4). Then run it again giving the –d option. You should get the error message saying the master file exists, please delete it.

Finally, do some sanity checking. It makes no sense to give both the –d and –g options, so we need to give an error message if both are set.

1. Right after you process the arguments (options), check the values of DELMASTER and GENMASTER. If both DELMASTER and GENMASTER are “yes”, print the error message “Only one of –d, -g allowed” and exit with an exit status code of 1. Call this script “scan5g.py”.

## What to Submit

For the parts of the exercises that do not require you to write a script, put your answers in a PDF or text file numbered appropriately, and call that file “Unit2answers.pdf” or “Unit2answers.txt” respectively. For the parts of the exercises that do require scripts, create plain text files to hold your script, and name the file containing your script as indicated in the problem.