CS @CU COMPUTER SCIENCE

COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK

COMS 3102
Fall 2016

Dan Mechanic
Using Linux

Homework Assignment #2

Last Update: September 14, 2016

Submit a **tar file** named **YOURUNI-COMS3102-HW2.tar.gz**, replacing UNI with your actual UNI to courseworks by: **Wednesday September 21st @ 5PM**

Objective:

The objective of Homework2 is to make you comfortable with files, directories, permissions, your PATH, tar and copying files via the SSH protocol.

It can be convenient to write scripts for commands that we will use repeatedly. Since we are just a regular user, a good idea is to create a sub-directory of our home directory to store these files in. Additionally, our shell needs to be able to find these files AND we need to have the permissions to run them.

We will be writing simple bash scripts and showing one way that poorly written scripts can be "hacked".

tar

For Howework2, we are going to use the utility `tar` to create an archive file.

When you have completed the assignment, you should have a directory named `~/coms3102bin` This directory should contain the following files:

1. `hw2sourcethis`
2. `hw2hellohost.sh`
3. `hw2ans.txt`

   And optionally...

4. `whoami`
5. `hw2hack.sh`

We are going to put all of these files into a single "tar ball".

On the COMS3102 Server:

1. Make sure you are in your home directory: `cd`
2. Create the tarball:

```
tar cvzf ./YOURUNI-COMS3102-HW2.tar.gz ./coms3102bin
```

NOTE: You are asking **tar** to **c**reate **v**erbosely a **z**ipped **f**ile named ./YOURUNI-COMS3102-HW2.tar.gz from all the files in ./coms3102bin

Examine your tarball's **t**able of contents to make sure it has everything AND the permissions on the files within the tarball look correct:

```
tar tvzf ./YOURUNI-COMS3102-HW2.tar.gz
```

Using scp to Copy Files From our Server

We are using the SSH protocol to connect to our server. You may also use the SSH protocol to move files between computers.

OSX

From a terminal on YOUR OSX MACHINE:

```
scp UNI@104.196.122.167:~/YOURUNI-COMS3102-HW2.tar.gz ~/Desktop/
```

Windows using PSCP

From a cmdtool on YOUR WINDOWS MACHINE:

```
pscp -i privatekeyfile.ppk UNI@104.196.122.167:~/YOURUNI-COMS3102-HW2.tar.gz ~/Desktop/
```

Windows using WinSCP

A popular program which uses the SSH protocol for copying files is WinSCP.

Download WinSCP. Click on 'Installation Package'

You will need to configure WinSCP to use key authentication.

1. Launch WinSCP:
2. Use File Protocol 'SCP'
3. Enter your Username (uni)
4. Hostname is 104.196.122.167
5. Do not use a password
6. Click 'Advanced'
7. Click SSH-¿Authentication
8. Select your 'Private Key File'
9. Save the Session

Once you have launched, you should have a 'split screen' interface with your computer and the left and the COMS3102 server on the right. You can drag files from the COMS3102 server over to your machine.

What to Submit:

Submit to courseworks a **tar file** named **YOURUNI-COMS3102-HW2.tar.gz** , replacing UNI with your actual UNI.

Create Your ~/coms3102bin Directory: (20 POINTS)

1. Create a directory in your home directory named **coms3102bin**
2. Set the permissions on the **/coms3102bin** directory so that **ONLY YOU** have **any** permissions to the directory. You should be able to list files in this directory, create new files in this directory and cd into this directory. **No-one else** should have any of those permissions.
3. `ls -l` should show `drwx------`

Create a file that when sourced will add `~/coms3102bin` to your PATH (30 POINTS)

1. Using 'nano', or any editor you choose, create a file in the `~/coms3102bin` directory named `hw2sourcethis` which will **safely** update your PATH when sourced and allow commands in `~/coms3102bin` to be found by your shell no matter where you are in the filesystem.

   So, if you typed:

   `source ~/coms3102bin/hw2sourcethis`

   ...your PATH variable will now include `~/coms3102bin` and your shell would now find commands in `~/coms3102bin`

   ****NOTE**** This change would only affect the current shell, so you would have to source this file each time you logged in. Next week we will learn how to make these changes permanent.

2. Once you are confident this works, Set the permissions on this script so that **ONLY YOU** can read this script. `(-r--------)`

Write a `~/coms3102bin/hw2hellohost.sh` Bash Script: (40 POINTS)

We will now write a script named `hw2hellohost.sh` to place into our `~/coms3102bin` directory.

1. `cd` to `~/coms3102bin/` and using 'nano', or any other linux editor, write a bash script which will output:

   ```
   Hello World this machine is named coms3102server
   ```

   (a) ****NOTE**** Do **NOT** hardcode 'coms3102server' into your script, use a command to print the hostname. If I run your script on a machine named 'luddite', your script should output:

   ```
   Hello World this machine is named luddite
   ```

   (b) ****NOTE**** make sure the first line of your script is:

   ```
   #!/bin/bash
   ```

2. Once you are confident your script works, Set the permissions on this script so that **ONLY YOU** can run this script, remove all permissions for all other users. ****remove your own write permissions**** on this script so that it is 'write-protected' and cannot be edited by accident. `(-r-x------)`

3. Source your `~/coms3102bin/hw2sourcethis` file and confirm you can now run `hw2hellohost.sh` from any directory and that `which hw2hellohost.sh` reflects your script in `~/coms3102bin`

```
[~]$ hw2hellohost.sh
-bash: hw2hellohost.sh: command not found
[~]$ source ~/coms3102bin/hw2sourcethis
[~]$ hw2hellohost.sh
Hello World this machine is named coms3102server
[~]$ which hw2hellohost.sh
~/coms3102bin/hw2hellohost.sh
```

`hello.coms3102` Bash Script: (10 POINTS)

There is a script on the system named `hello.coms3102`.

1. Run this script.

   Using 'nano', or any editor you choose, create a text file in the `~/coms3102bin` directory named `hw2ans.txt` and answer:

2. Where is the script `hello.coms3102` located on our system?

3. What command did you use to discover where `hello.coms3102` is located?

EXTRA CREDIT: (10 POINTS)

Examine the `hello.coms3102` bash script. This script runs `whoami` to see if you are the all-powerful `root` user. However, it's trusting **your** PATH to find whoami. Can you hack it?

1. Write your own malicious `whoami` command and place it in `~/coms3102bin/`
2. Write a script named `hw2hack.sh` which tricks `hello.coms3102` into using your version of `whoami`

   ****NOTE**** Your PATH should NOT be affected when hw2hack.sh exits.

```
[~]$ whoami
dm2474
[~]$ ~/coms3102bin/whoami
root
[~]$ hello.coms3102
hello coms3102
You are NOT privileged: dm2474.
[~]$ hw2hack.sh
-bash: hw2hack.sh: command not found
[~]$ source ~/coms3102bin/hw2sourcethis
[~]$ hw2hack.sh
hello coms3102
root is ALL powerful.
[~]$  hello.coms3102
hello coms3102
You are NOT privileged: dm2474.
```