**COMP 2766: Introduction to Linux**

**Assignment #6: System and User Security and Processes**

**This assignment consists of three parts: a dictionary attack, configuring the sudoers file, and managing processes.**

**PART 1: Dictionary Attack Exercise (SHA512)**

1. Start your CentOS Streaming 9 Linux virtual machine.
2. Login as **root**.
3. If needed, create a user based on **your first name and last initial** (ex: justint, if you are Justin Trudeau) by entering the following command line:

# useradd justint

1. Think of a word from the English language that starts with any letter **between h and p, inclusive**. If needed, confirm its spelling using an online dictionary (ex: [www.dictionary.com](http://www.dictionary.com)). **As the root user**, enter the following command line with your word in **lowercase** and enclosed in single quotation marks to check whether it is in Linux’s dictionary (**do *NOT* copy and paste this command line**):

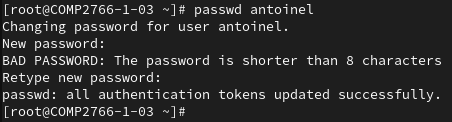
# egrep ‘^*yourword$’* /usr/share/dict/words



If your word is in the dictionary, then the above command line will output it. If your word is not in the dictionary, choose another English word until the above command line confirms that your chosen word is in the Linux dictionary.

1. **As the root user**, enter the following command line to change **your user’s** password to the word that you chose (***NOTE: ensure CapsLock is off and carefully enter your password using all lowercase letters; ignore any warnings about the password being a dictionary word, a bad choice, or too short***):

# passwd *justint*



1. Computers use algorithms to encrypt passwords and create password hashes. Enter the following command line to determine which hashing algorithm is currently being used. If the output is 6, then the algorithm is SHA512:

# head -1 /etc/shadow | cut -f2 -d\$



If the output is not 6, let the instructor know.

1. **As the root user**, enter the following command line to output **your user**’s encrypted password information:

# egrep ‘^*justint*:’ /etc/shadow

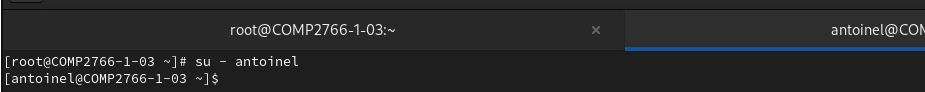


Field 2 in /etc/shadow contains 3 subfields delimited by the $ character: (1) the hashing algorithm, (2) the SALT, which is a random string used for encryption, and (3) the encrypted password hash. The SALT in /etc/shadow is between the 2nd and 3rd $ signs. In the following example, the SALT is **pGSSh2gz**



1. Open a new tab in your terminal window by clicking the + symbol enclosed in a square at the top-left of your terminal. **In that new tab**, enter this command line to switch to **your own user**:

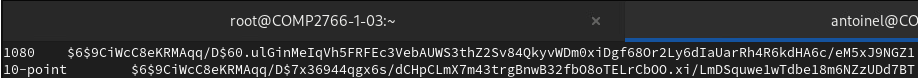
# su - *justint*



1. **In your user’s tab**, enter the following command line to encrypt the entire dictionary using SHA256 and insert your user’s SALT in single quotation marks in place of ***pGSSh2gz*** (***do NOT use pGSSh2gz***) (**do *NOT* copy and paste this command line**):

$ openssl passwd -table -in /usr/share/dict/words -6 -salt ‘***pGSSh2gz’*** | less

Examine the output which shows each dictionary word in plaintext on the left with its SHA512 encrypted hash on the right. Press Q to quit less and, then, Ctrl-C to terminate the command line.



1. Look up your user’s ciphertext (encrypted password hash) in /etc/shadow (it’s between the 3rd $ sign in field 2 and the next colon). In the following example, the ciphertext is **9G4Dloe45Q**



1. Press UpArrow to retrieve the command line that you entered in step 9, above. Modify that command line by piping to the egrep command and using your user’s ciphertext (encrypted password hash) enclosed in single quotation marks in place of **9G4Dloe45Q** (***do NOT use* 9G4Dloe45Q**) to find your password (**do *NOT* copy and paste this command line**):

$ openssl passwd -table -in /usr/share/dict/words -6 -salt ‘***pGSSh2gz’*** | egrep ‘***9G4Dloe45Q’***

After entering the above command line, the cursor will just sit on the next line. Be very patient as the search could take upwards of thirty minutes (as you’re waiting, do part 2 of this assignment). If you followed all the instructions correctly, the plaintext password will eventually be output with its encrypted hash in a line that is half white and half red.

If the command line prompt returns and you receive no output, then double-check that you used the correct SALT and the correct encrypted password hash in step #11, above. If they appear correct, then you very likely typed the password incorrectly when you set your user’s password and need to go back to step #5, above.

(**5 marks**) Capture and insert a screenshot, here, of your openssl command line and its output which includes your plaintext password and the ciphertext:

**PART 2: Configuring the /etc/sudoers file**

1. Open a new tab by clicking the + symbol enclosed in a square at the top-left corner of your terminal window. In that new tab, enter a command line to **switch to your user** using the login shell option. (See Chapter 15, section 15.2.1 for more information about the login shell option.)
2. (**1 mark**) **As your user**, enter the following command line and insert a screenshot, here, showing that command line (and your command line prompt) and its results (which should be permission denied):

$ head /var/log/secure



1. A non-root user is unable to view the contents of /var/log/secure because it is an authentication log. To allow users who are learning Linux to view the contents of that file, the root user can configure /etc/sudoers and specify which user(s) – and also which group(s) – can run command line(s) that only the root user normally has permission to execute. Enter the following command line to close your user’s shell and revert to the root user (**do *NOT* use the su command to switch to the root user**):

$ exit

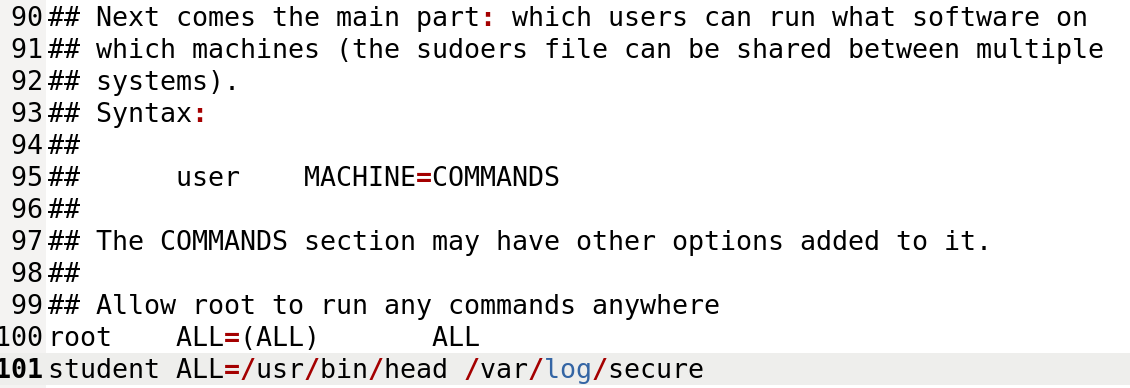
1. (**1 mark**) **As the root user**, enter a command line that forces commands such as visudo to use the gedit editor instead of vi. If you forgot how to do this, refer to Session 8 Lecture Slide Set 1. Insert a screenshot of your command line, here:



1. **As the root user**, enter the following command line to edit /etc/sudoers

# visudo

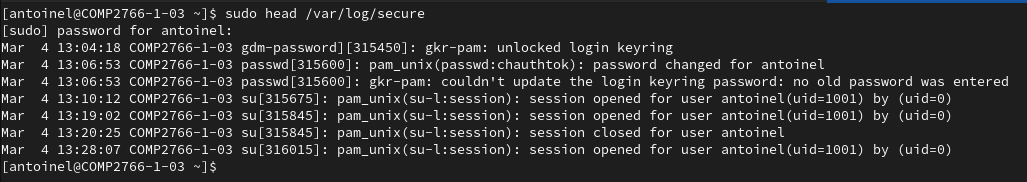
Then, enter line 101 shown in the screenshot below **using your own user name** **instead of student** (ex: justint, if you are Justin Trudeau). Save your changes and exit gedit.



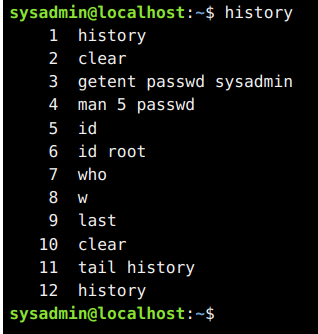
1. **As your user**, enter this command line and your password when prompted:

$ sudo head /var/log/secure

(**2 marks**) Insert a screenshot, here, showing the above command line (and your command line prompt) and the command line’s output **INCLUDING the first ten lines of /var/log/secure**



1. (**1 mark**) Do NDG Module 15’s **Lab 15**, sections 15.4.4 to 15.6.1, inclusive, on NDG’s Ubutun VM. Then, enter the history command and insert a screenshot of its output, here:



**\*\*\* IMPORTANT: Check on the progress of your dictionary attack and go back to PART 1 of this assignment. \*\*\***

**PART 3: Managing Processes**

1. (**3 marks**) Do NDG Module 13’s **Lab 13**, sections 13.1 to 13.7.2, inclusive, on NDG’s Ubuntu VM. Then, as the root user on NDG’s Ubuntu VM, enter the history command and insert a screenshot of its output, here:

**\*\*\* IMPORTANT: Check on the progress of your dictionary attack and go back to PART 1 of this assignment. \*\*\***