

Laboratory Exercise 7 – Password Cracking

Task 1: Merge the passwd and shadow files

Made sure I was in the passwords directory and merged the passwd and shadow fil in a file called target_hashes

```
student@amansha:~$ cd ~/passwords
student@amansha:~/passwords$ unshadow target_passwd target_shadow > target_hashes
Created directory: /home/student/.john
student@amansha:~/passwords$
```

Task 2: Crack the passwords

Ran john the ripper using the john command to crack the password and then used “—show+ to see the passwords

```
student@amansha:~$ cd ~/passwords
student@amansha:~/passwords$ unshadow target_passwd target_shadow > target_hashes
Created directory: /home/student/.john
student@amansha:~/passwords$ john target_hashes
stat: target_hashes: No such file or directory
student@amansha:~/passwords$ unshadow target_passwd target_shadow > target_hashes
student@amansha:~/passwords$ john target_hashes
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
joe      (joe)
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed for performance.
student  (student)
2g 0:00:00:00 DONE 1/3 (2021-09-29 18:10) 100.0g/s 300.0p/s 350.0c/s 350.0C/s student..joe
Use the "--show" option to display all of the cracked passwords reliably
Session completed
student@amansha:~/passwords$ john --show target_hashes
student:student:1001:1001::/home/student:
joe:joe:1002:1002::,,:/home/joe:/bin/bash

2 password hashes cracked, 0 left
student@amansha:~/passwords$ date
Wed Sep 29 18:11:48 UTC 2021
student@amansha:~/passwords$
```

I used “crunch” that is a built-in kali to make a dictionary. I set min and max character to 8-11 and used cyber security mason words saved in the file called list.txt.

Amir Mansha
Lab 3-7
CYSE 425
Fall 2021

```
student@amansha:~/passwords$ crunch 8 11 Cyber security mason > list.txt
Crunch will now generate the following amount of data: 716406250 bytes
683 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 60937500
student@amansha:~/passwords$ ls
list.txt  target  target_hashes  target_passwd  target_shadow
student@amansha:~/passwords$
```

Amir Mansha
Lab 3-7
CYSE 425
Fall 2021

```
Terminal - student@amansha: ~/passwords
File Edit View Terminal Tabs Help
eeCreCbeb
eeCreCbee
eeCreCber
eeCreCbrC
eeCreCbry
eeCreCbrb
eeCreCbre
eeCreCbrr
eeCreCeCC
eeCreCeCy
eeCreCeCb
eeCreCeCe
eeCreCeCr
eeCreCeyC
eeCreCeyy
eeCreCeyb
eeCreCeye
eeCreCeyr
eeCreCebC
eeCreCeby
eeCreCebb
eeCreCebe
eeCreCebr
eeCreCeeC
eeCreCeey
eeCreCeeb
eeCreCeee
eeCreCeer
eeCreCerC
eeCreCery
eeCreCerb
eeCreCere
eeCreCerr
eeCreCrCC
eeCreCrCy
eeCreCrCb
eeCreCrCe
eeCreCrCr
eeCreCryC
eeCreCryy
eeCreCryb
eeCreCrye
eeCreCryr
eeCreCrbC
eeCreCrby
eeCreCrbb
eeCreCrbe
```

Task 3: Test the cracked account

Used the ssh to go in system target system IP Address and then tested to see if student has sudo access and it did not.

```
student@amansha:~/passwords$ ssh student@10.1.143.79
student@10.1.143.79's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-1018-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Get cloud support with Ubuntu Advantage Cloud Guest:
http://www.ubuntu.com/business/services/cloud

38 packages can be updated.
0 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

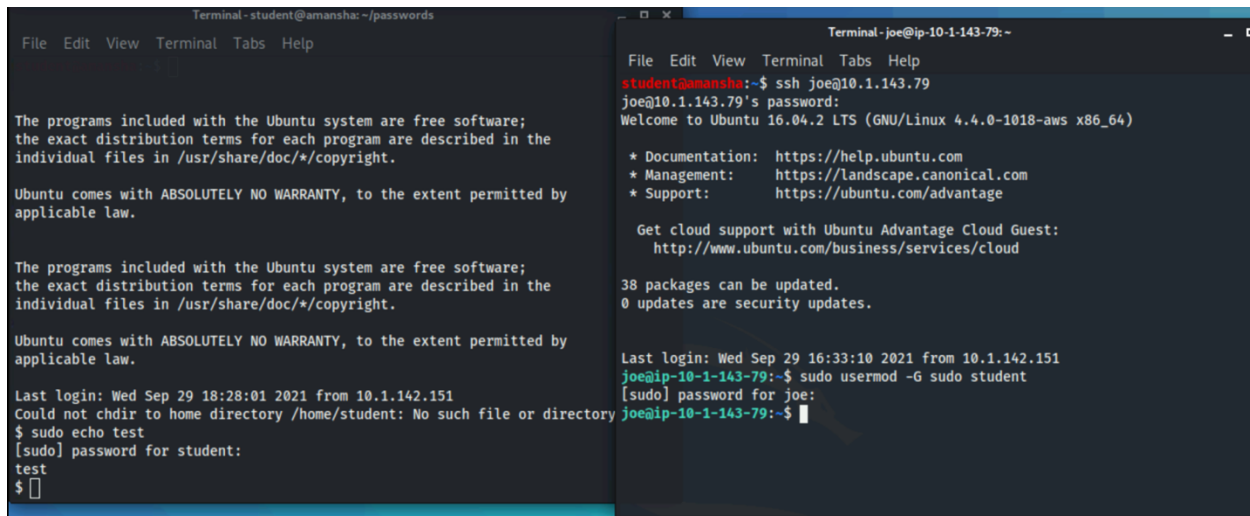
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Could not chdir to home directory /home/student: No such file or directory
$ sudo echo test
[sudo] password for student:
student is not in the sudoers file. This incident will be reported.
$
```

Amir Mansha
Lab 3-7
CYSE 425
Fall 2021

Task 4: Upgrade the cracked account Sudo



The image shows two terminal windows side-by-side. The left window is titled 'Terminal - student@amansha: ~/passwords' and shows the user 'student' running 'sudo echo test', which fails because 'student' is not in the sudoers file. The right window is titled 'Terminal - joe@ip-10-1-143-79: ~' and shows the user 'joe' running 'sudo usermod -G sudo student', which succeeds. Then, 'joe' runs 'sudo echo test' again, which succeeds, indicating that 'student' now has sudo access.

```
Terminal - student@amansha: ~/passwords
File Edit View Terminal Tabs Help

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Wed Sep 29 18:28:01 2021 from 10.1.142.151
Could not chdir to home directory /home/student: No such file or directory
$ sudo echo test
[sudo] password for student:
test
$

Terminal - joe@ip-10-1-143-79: ~
File Edit View Terminal Tabs Help

student@amansha:~$ ssh joe@10.1.143.79
joe@10.1.143.79's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-1018-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Get cloud support with Ubuntu Advantage Cloud Guest:
http://www.ubuntu.com/business/services/cloud

38 packages can be updated.
0 updates are security updates.

Last login: Wed Sep 29 16:33:10 2021 from 10.1.142.151
joe@ip-10-1-143-79:~$ sudo usermod -G sudo student
[sudo] password for joe:
joe@ip-10-1-143-79:~$
```

I ssh into joe and made student in the sudo group then I went back to ssh student and. Tried the sudo echo test command again and now student has sudo access in the target system
