Appendix E: Bash Environment and Scripting

Note: The screens might differ while performing the labs.

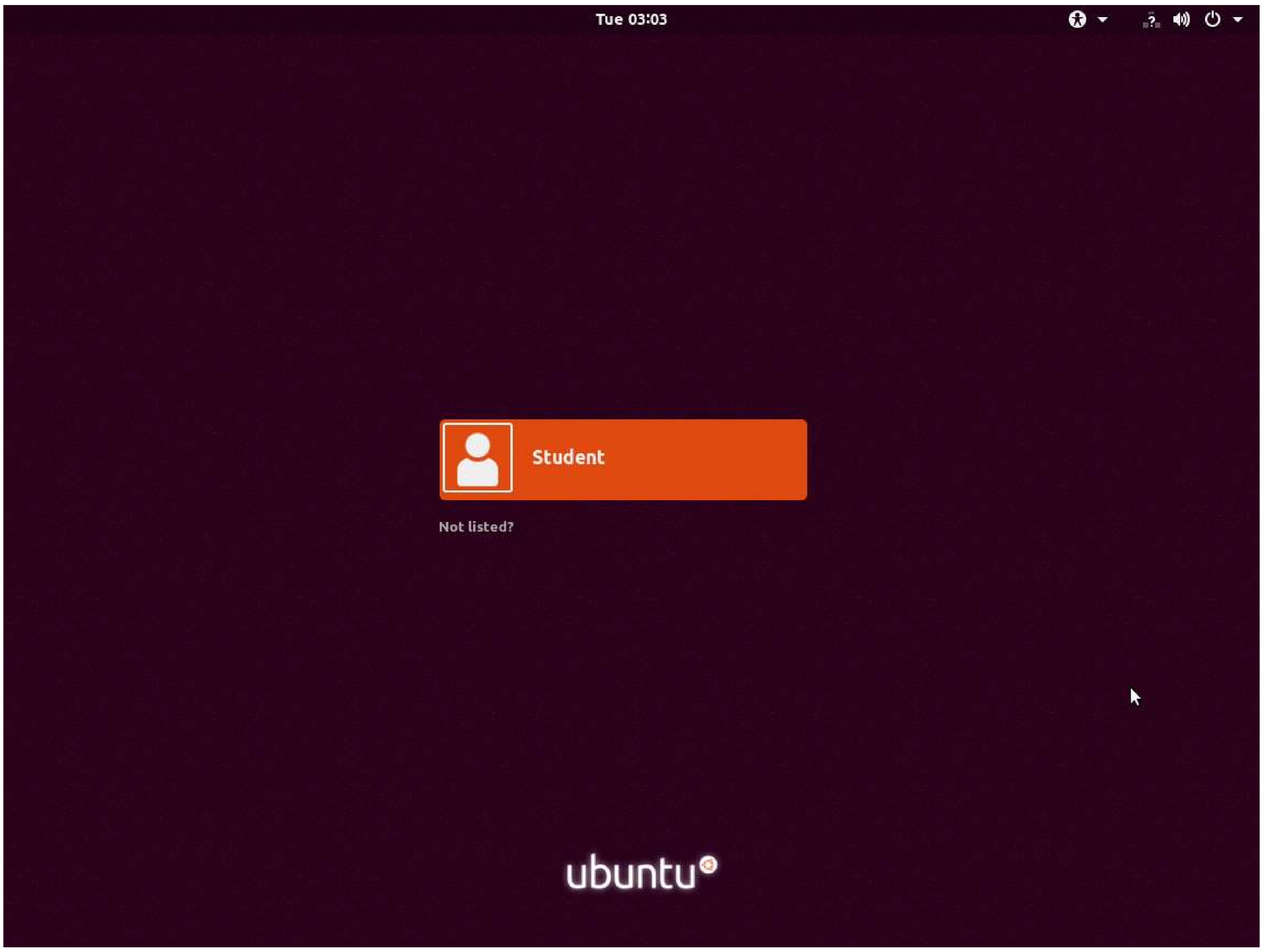
Exercise 1: Basic BASH Queries

Objectives

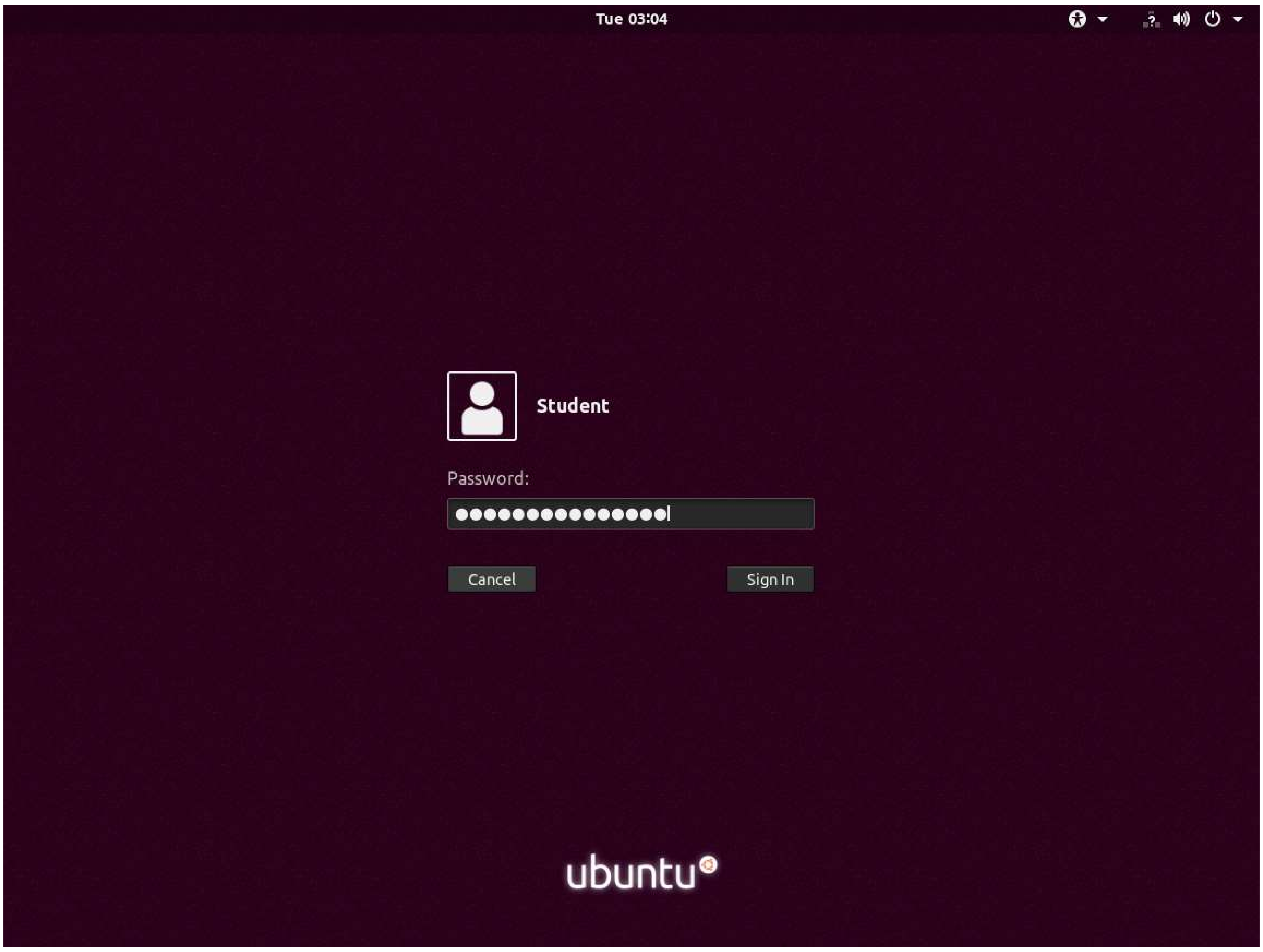
- Create basic BASH queries, extract data, and explore the features and components of BASH

Lab Duration: **20** Minutes

1. By default **CPENT Bash Machine** machine selected, click **Student** profile to login.

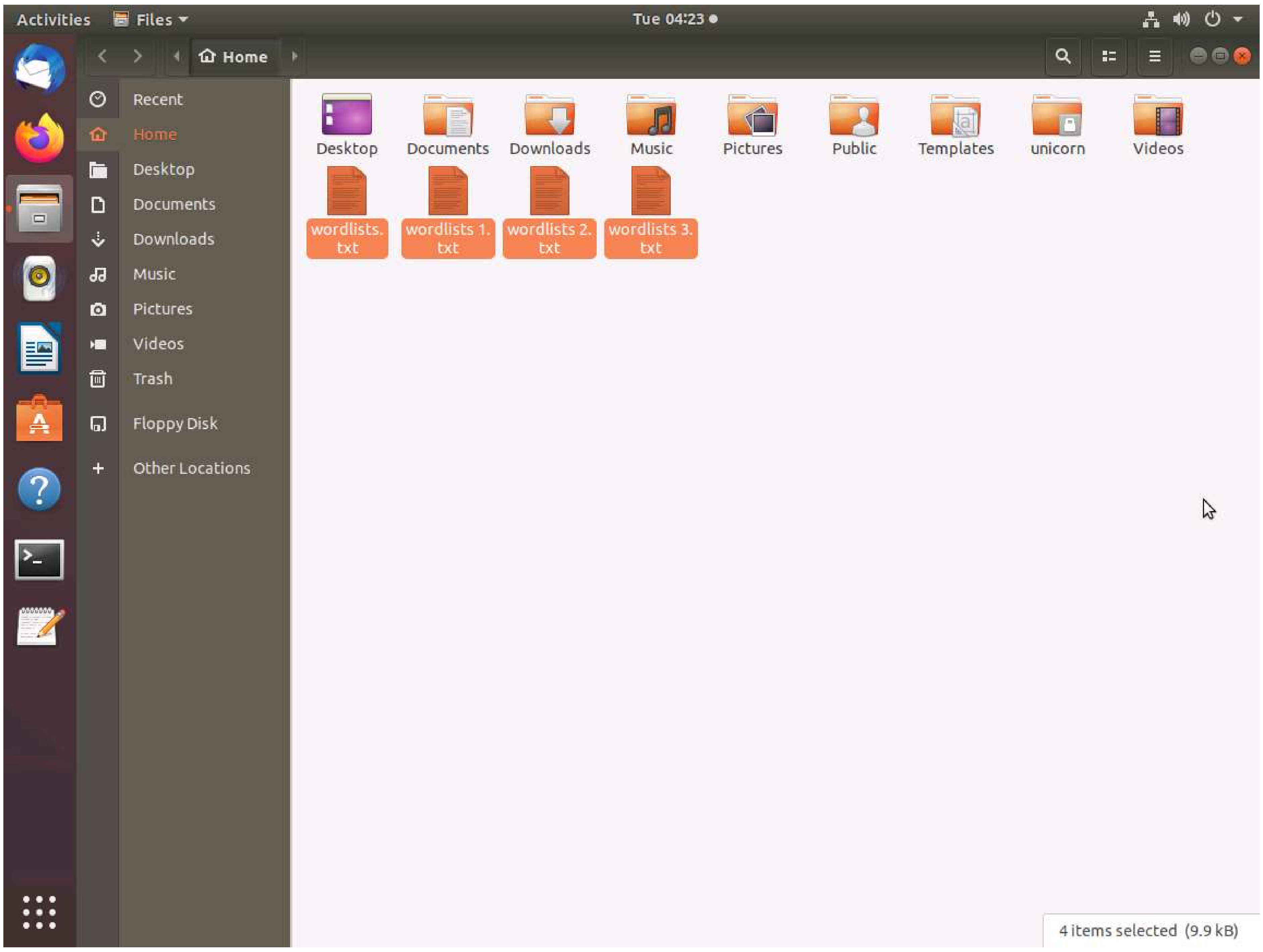


2. Type **password** in the Password field and click **Sign In**.

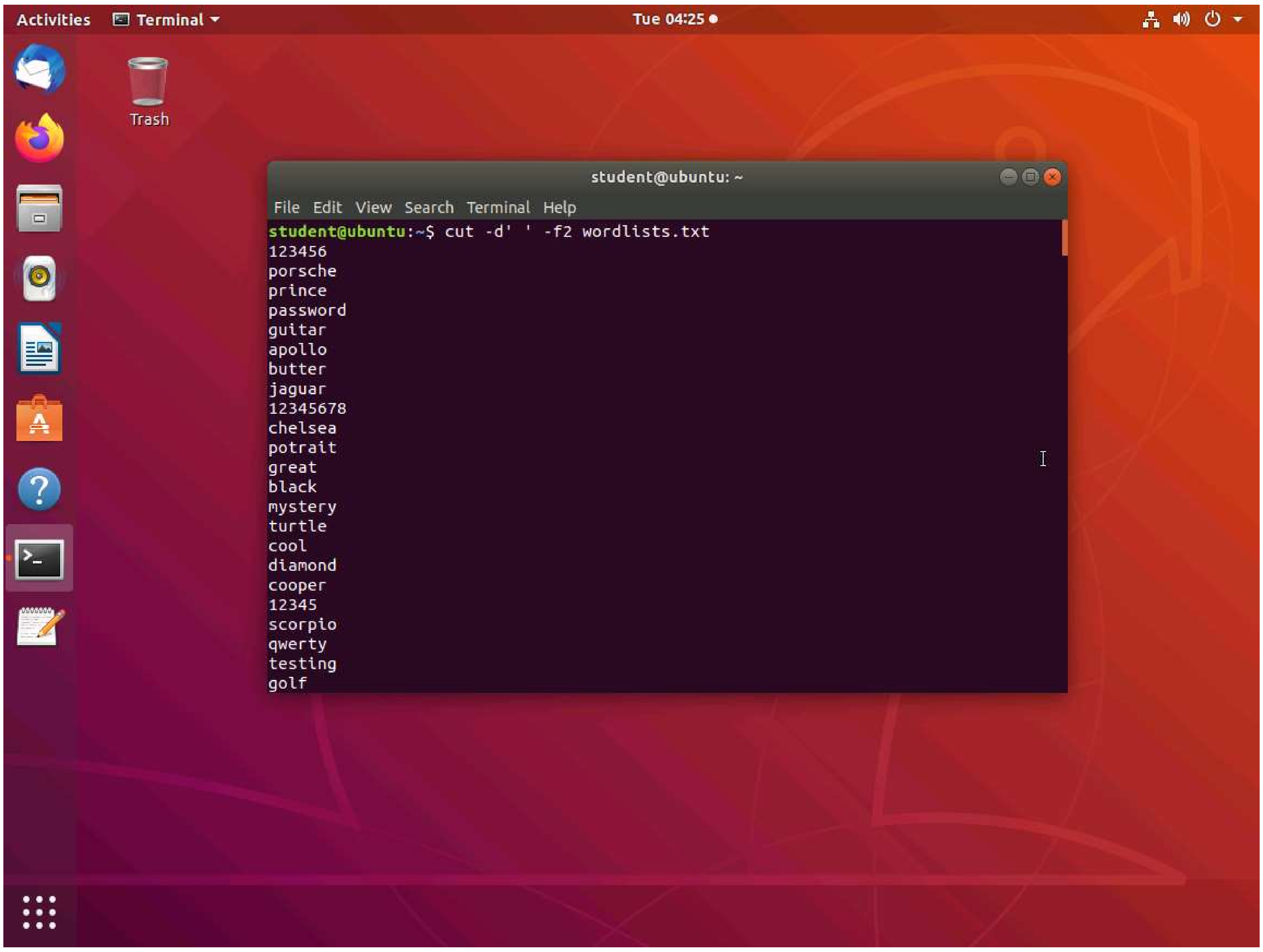


3. In this exercise, we will review the different methods of extracting data using **BASH**. First, we want to create several files with passwords in them. You can create your own or open one of the files on the machine, copy parts of it, and create multiple files. We need at least three files to work with.

4. In this exercise we have already created **wordlists.txt** file in the Home directory and made a copy of those files in the Home directory, as shown in the screenshot.

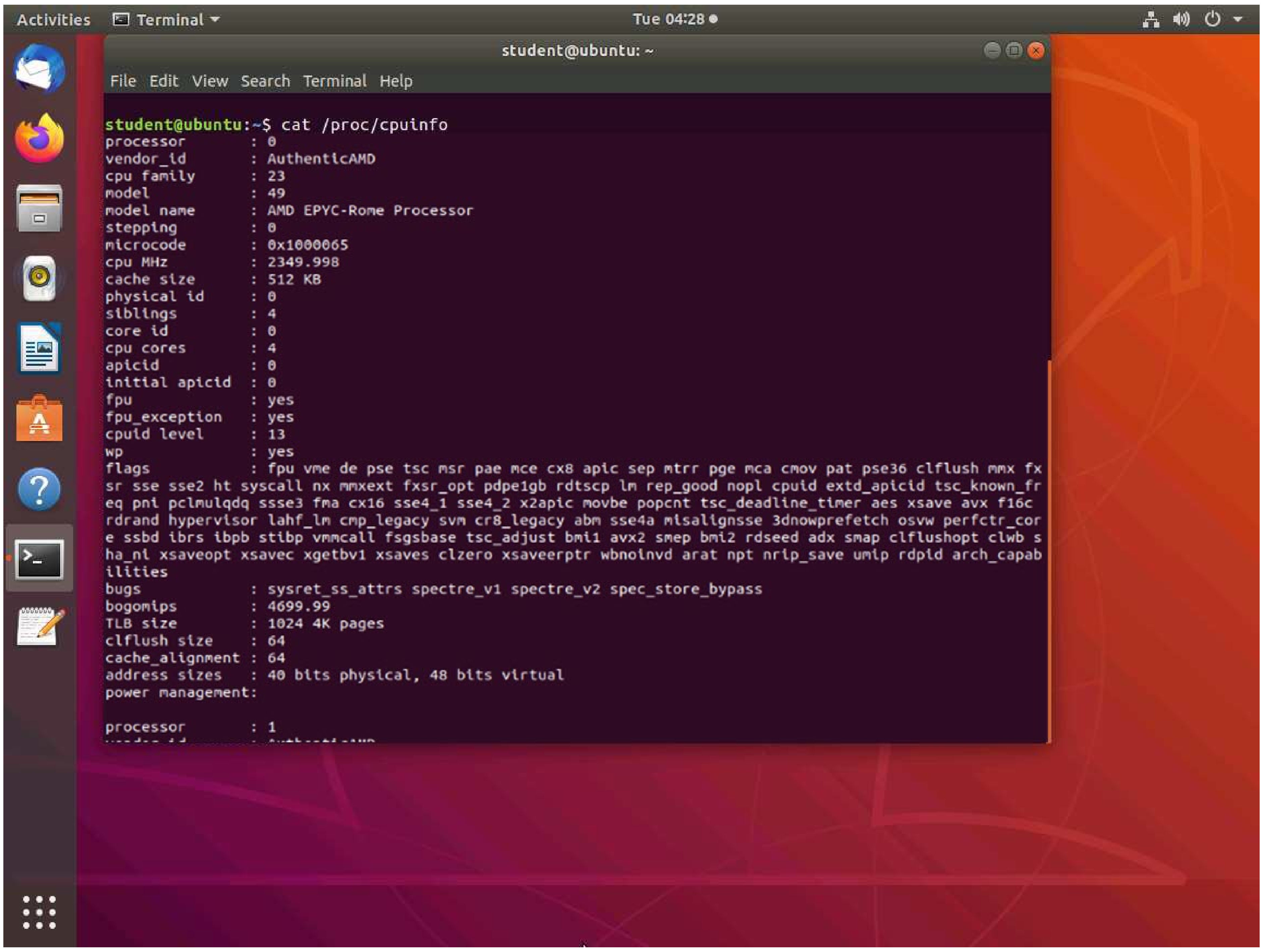


5. First, try the command **cut -d' ' -f2 wordlists.txt**. Launch a terminal, type **cut -d' ' -f2 wordlists.txt** and press **Enter**. An example of the output of the command is shown in the screenshot.



```
student@ubuntu:~$ cut -d' ' -f2 wordlists.txt
123456
porsche
prince
password
guitar
apollo
butter
jaguar
12345678
chelsea
potrait
great
black
mystery
turtle
cool
diamond
cooper
12345
scorpio
qwerty
testing
golf
```

6. Next, you can view the info on the **CPU**. Type **cat /proc/cpuinfo** and press **Enter**. An example of the output of the command is shown in the screenshot. Take a few minutes and review the results.



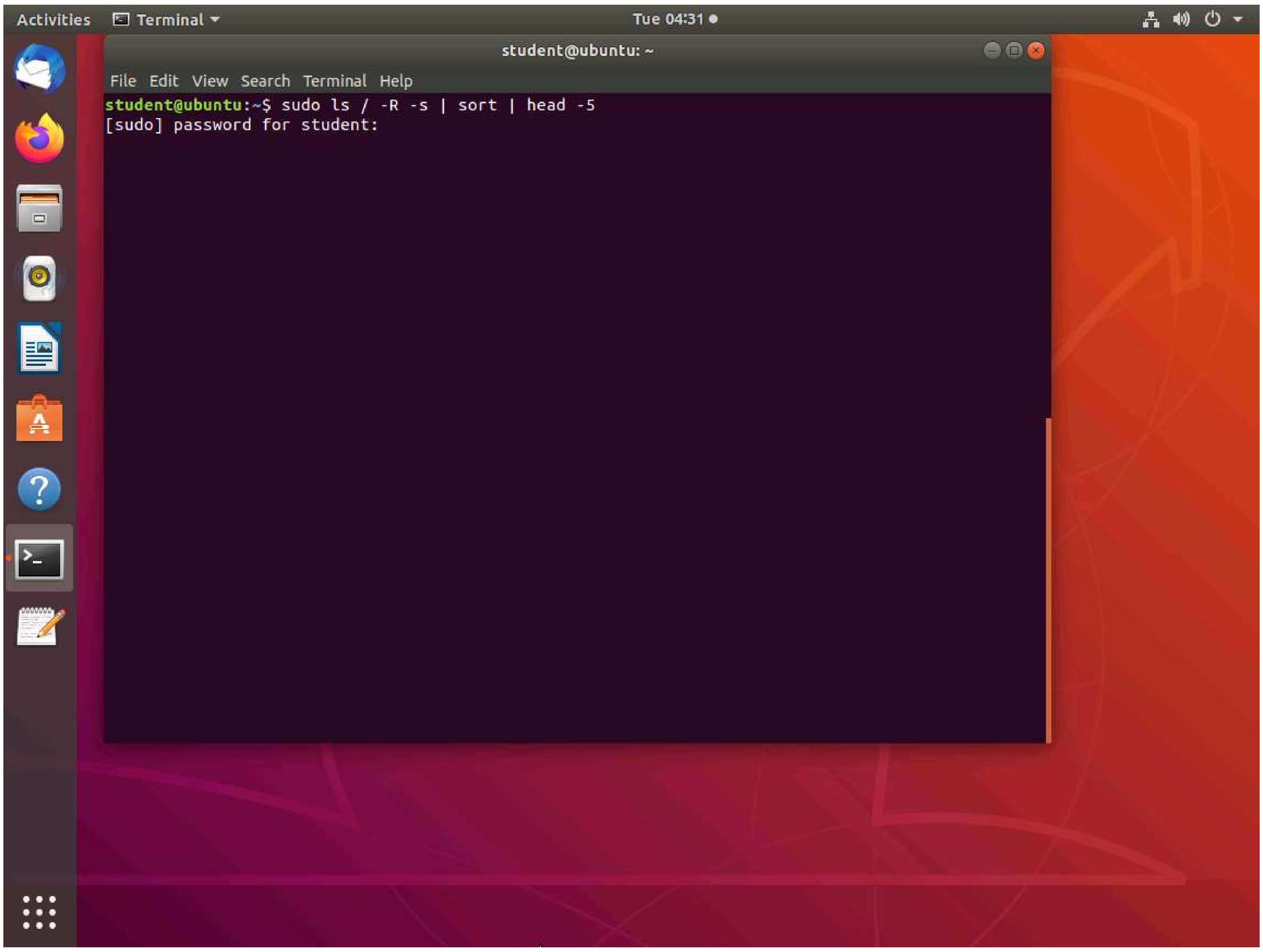
```
student@ubuntu:~$ cat /proc/cpuinfo
processor       : 0
vendor_id       : AuthenticAMD
cpu family      : 23
model           : 49
model name      : AMD EPYC-Rome Processor
stepping        : 0
microcode       : 0x1000065
cpu MHz         : 2349.998
cache size      : 512 KB
physical id     : 0
siblings        : 4
core id         : 0
cpu cores       : 4
apicid          : 0
initial apicid  : 0
fpu             : yes
fpu_exception   : yes
cpuid level     : 13
wp              : yes
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fx
sr sse sse2 ht syscall nx mmxext fxsr_opt pdpe1gb rdtscp lm rep_good nopl cpuid extd_apicid tsc_known_fr
eq pni pclmulqdq ssse3 fma cx16 sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave avx f16c
rdrand hypervisor lahf_lm cmp_legacy svm cr8_legacy abm sse4a misalignsse 3dnowprefetch osvw perfctr_cor
e ssbd ibrs ibpb stibp vmmcall fsgsbase tsc_adjust bmi1 avx2 smep bmi2 rdseed adx smap clflushopt clwb s
ha_ni xsaveopt xsavec xgetbv1 xsaves clzero xsaveerptr wbnoinvd arat npt nrip_save umip rdpid arch_capab
ilities
bugs            : sysret_ss_attrs spectre_v1 spectre_v2 spec_store_bypass
bogomips        : 4699.99
TLB size        : 1024 4K pages
clflush size    : 64
cache_alignment : 64
address sizes   : 40 bits physical, 48 bits virtual
power management:

processor       : 1
```

7. Next, we will review the sort command. Type **sudo ls / -R -s | sort | head -5** and press **Enter**. Type **password** and press **Enter**.

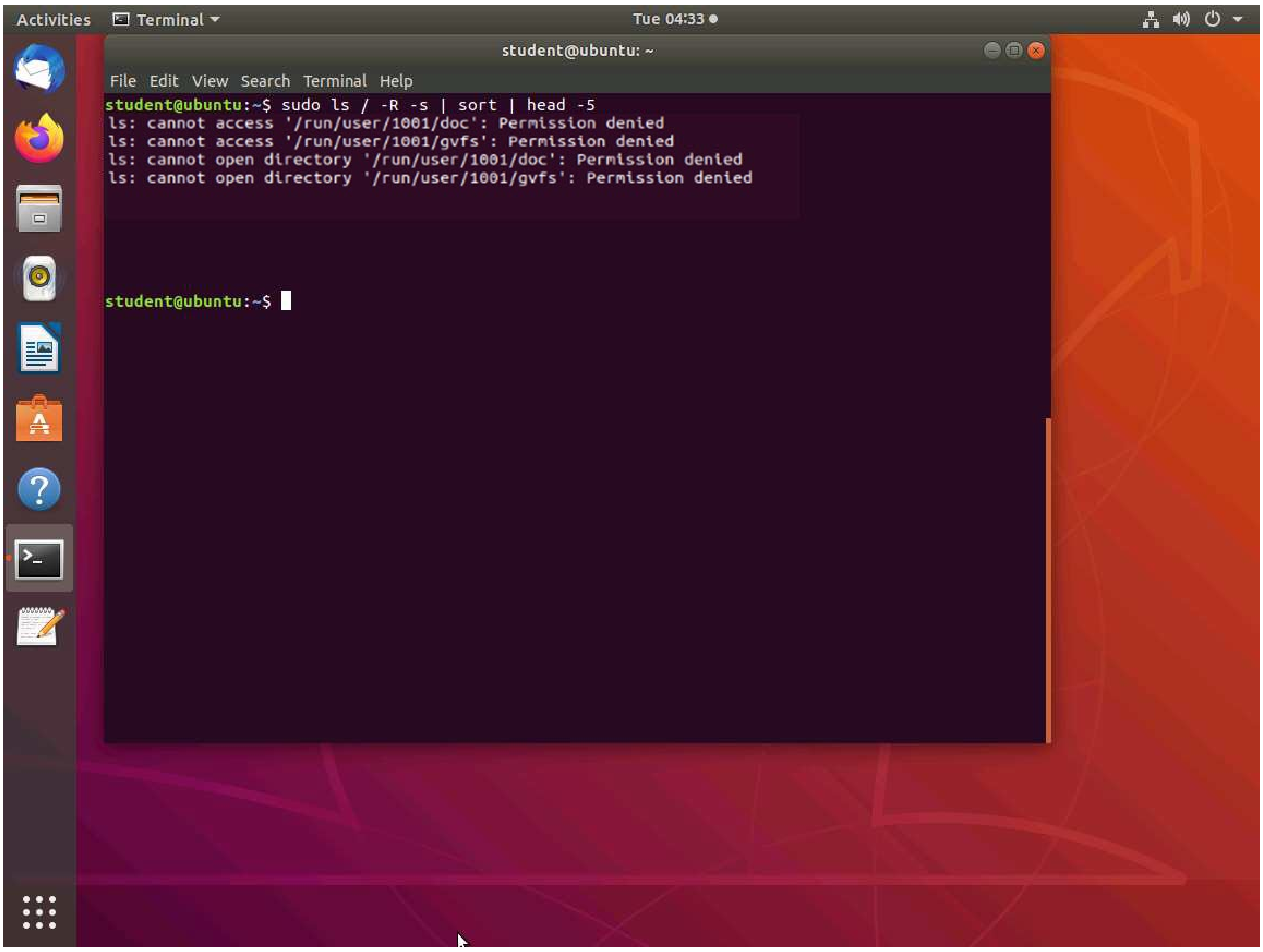
   - R option for ls, which will cause it to recursively list the files under the specified directory.
   - The power of piping is demonstrated. An example of the output of this command is shown in the following screenshot.

8. There are many different ways to work with the output. If you have time, feel free to explore more.

9. Press **Ctrl+C** to terminate the execution of the command.



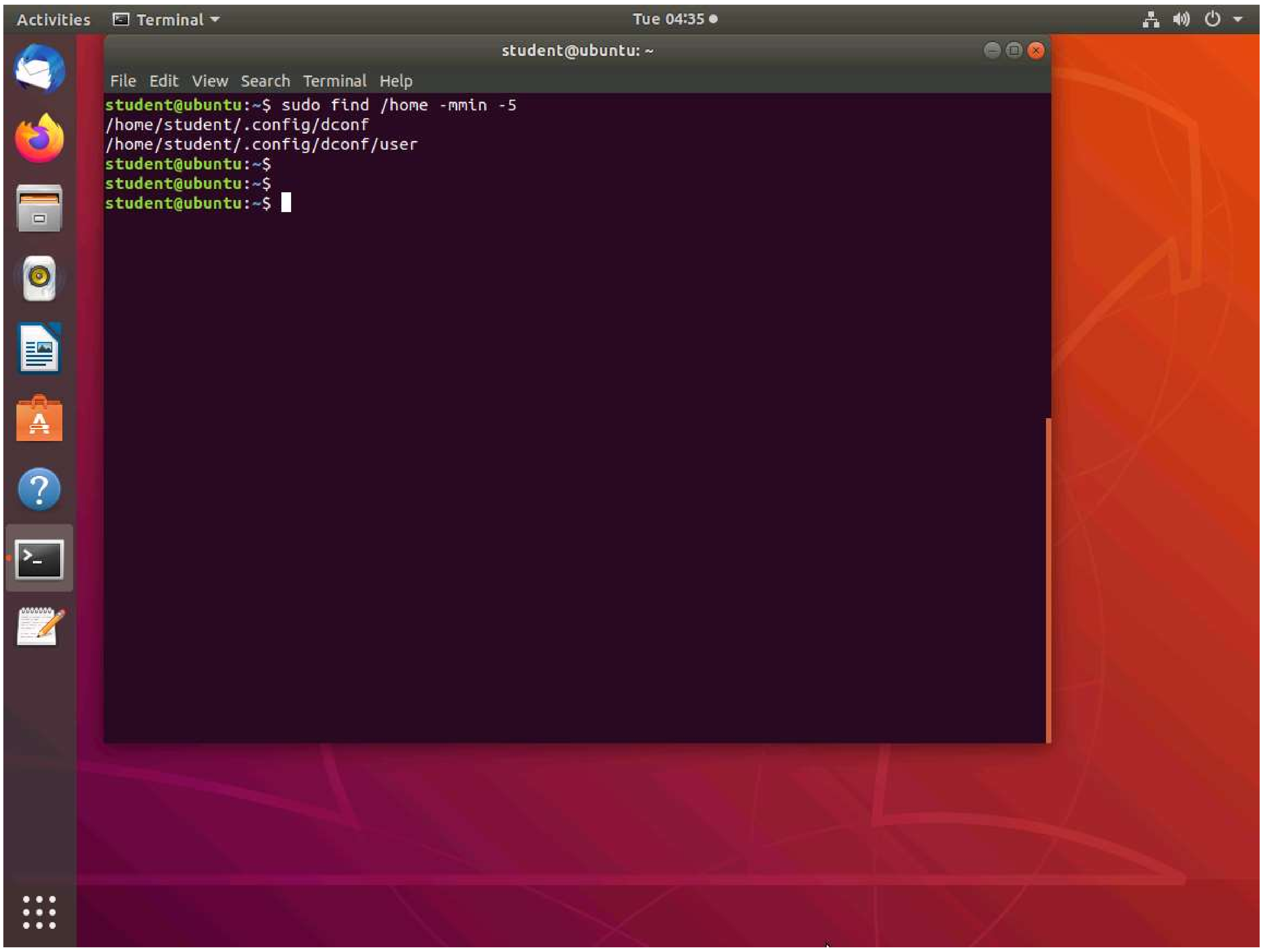
```
student@ubuntu:~$ sudo ls / -R -s | sort | head -5
[sudo] password for student:
```



```
student@ubuntu:~$ sudo ls / -R -s | sort | head -5
ls: cannot access '/run/user/1001/doc': Permission denied
ls: cannot access '/run/user/1001/gvfs': Permission denied
ls: cannot open directory '/run/user/1001/doc': Permission denied
ls: cannot open directory '/run/user/1001/gvfs': Permission denied



student@ubuntu:~$
```

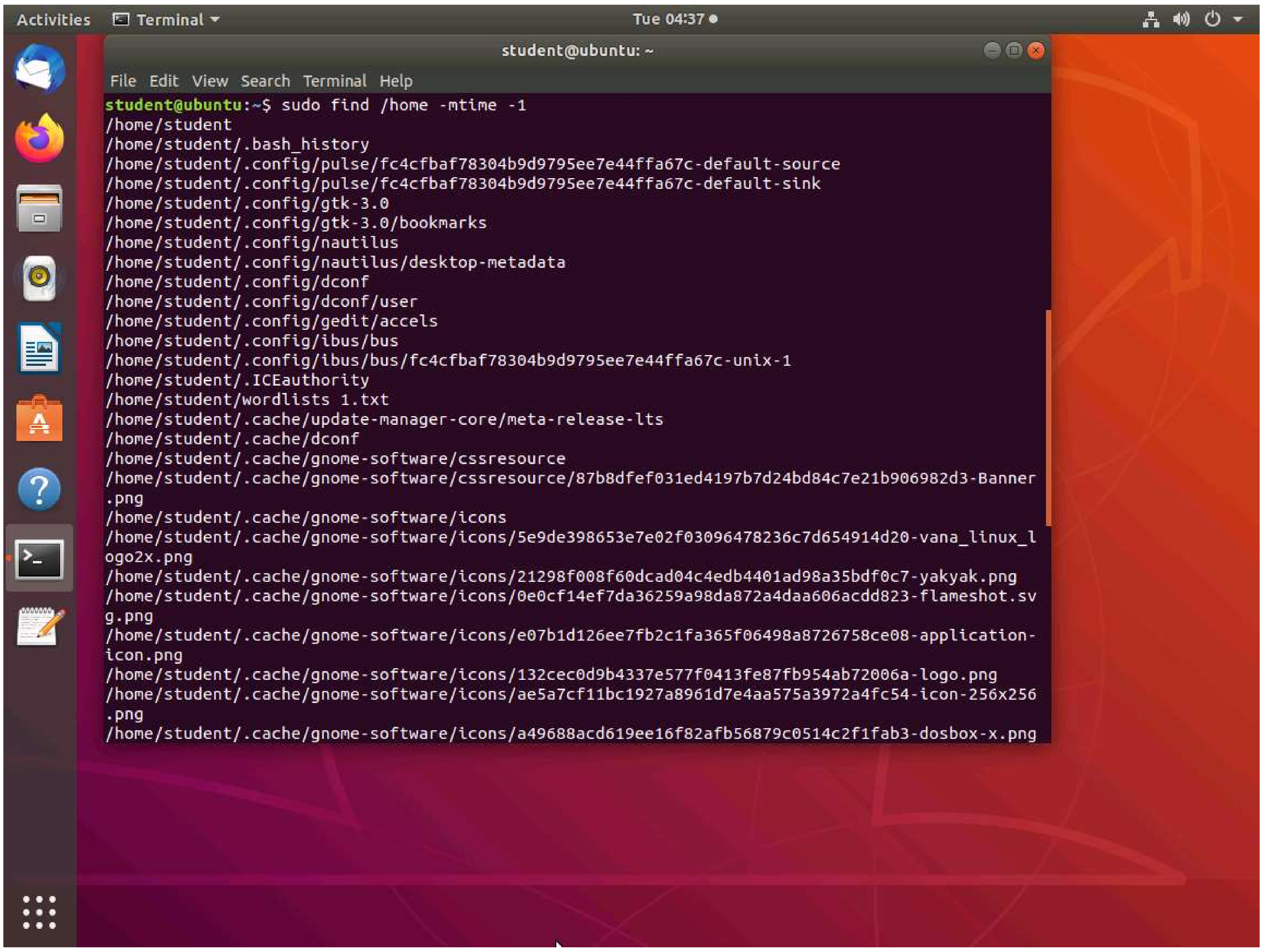
10. Next, type **sudo find /home -mmin -5** and press **Enter**. The output of this command is shown in the following screenshot.

Note: The result might differ when you perform this lab exercise..



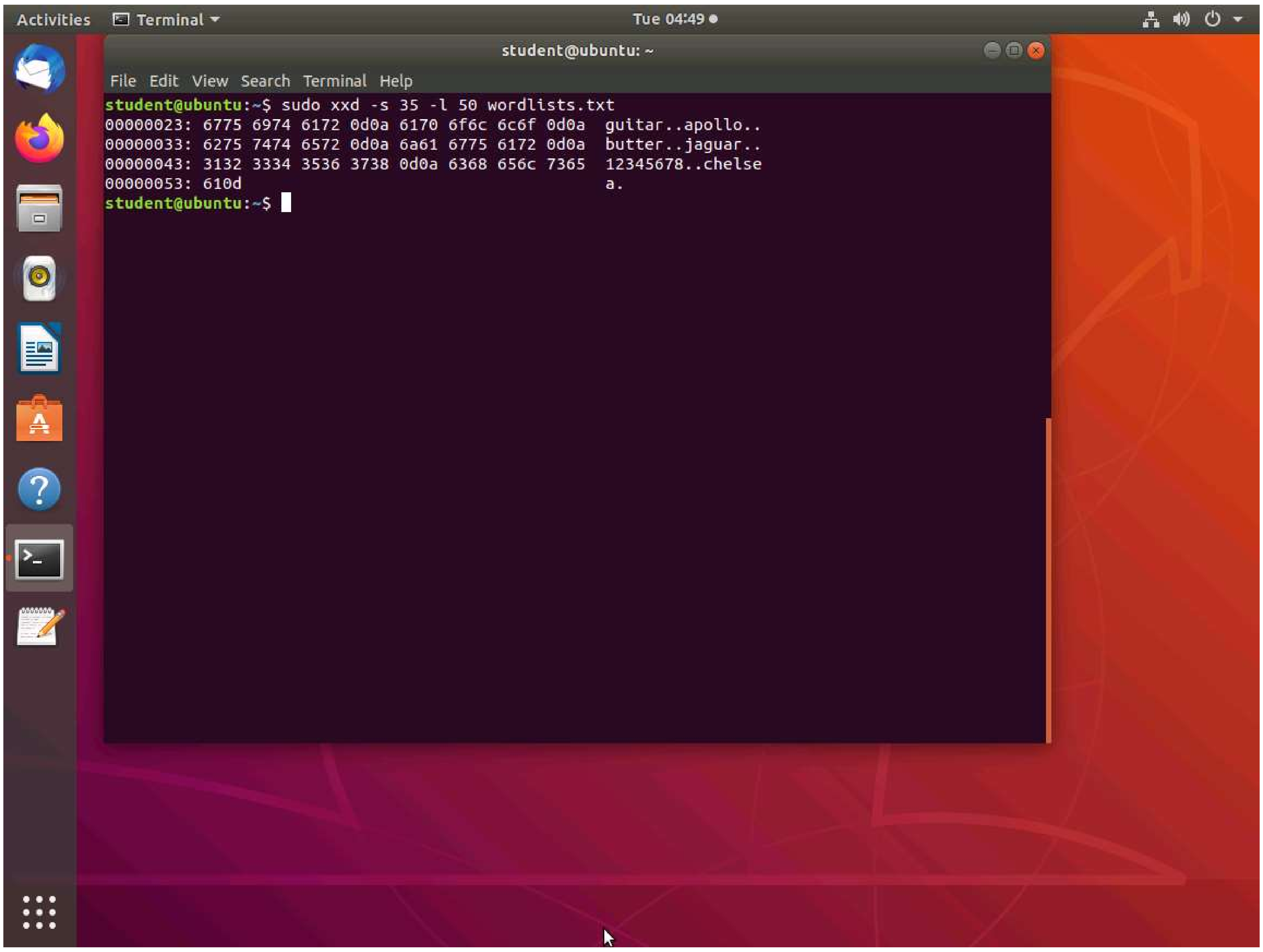
```
student@ubuntu:~$ sudo find /home -mmin -5
/home/student/.config/dconf
/home/student/.config/dconf/user
student@ubuntu:~$
student@ubuntu:~$
student@ubuntu:~$
```

11. To view the files modified in the last **24** hours, type **sudo find /home -mtime -1** and press **Enter**.



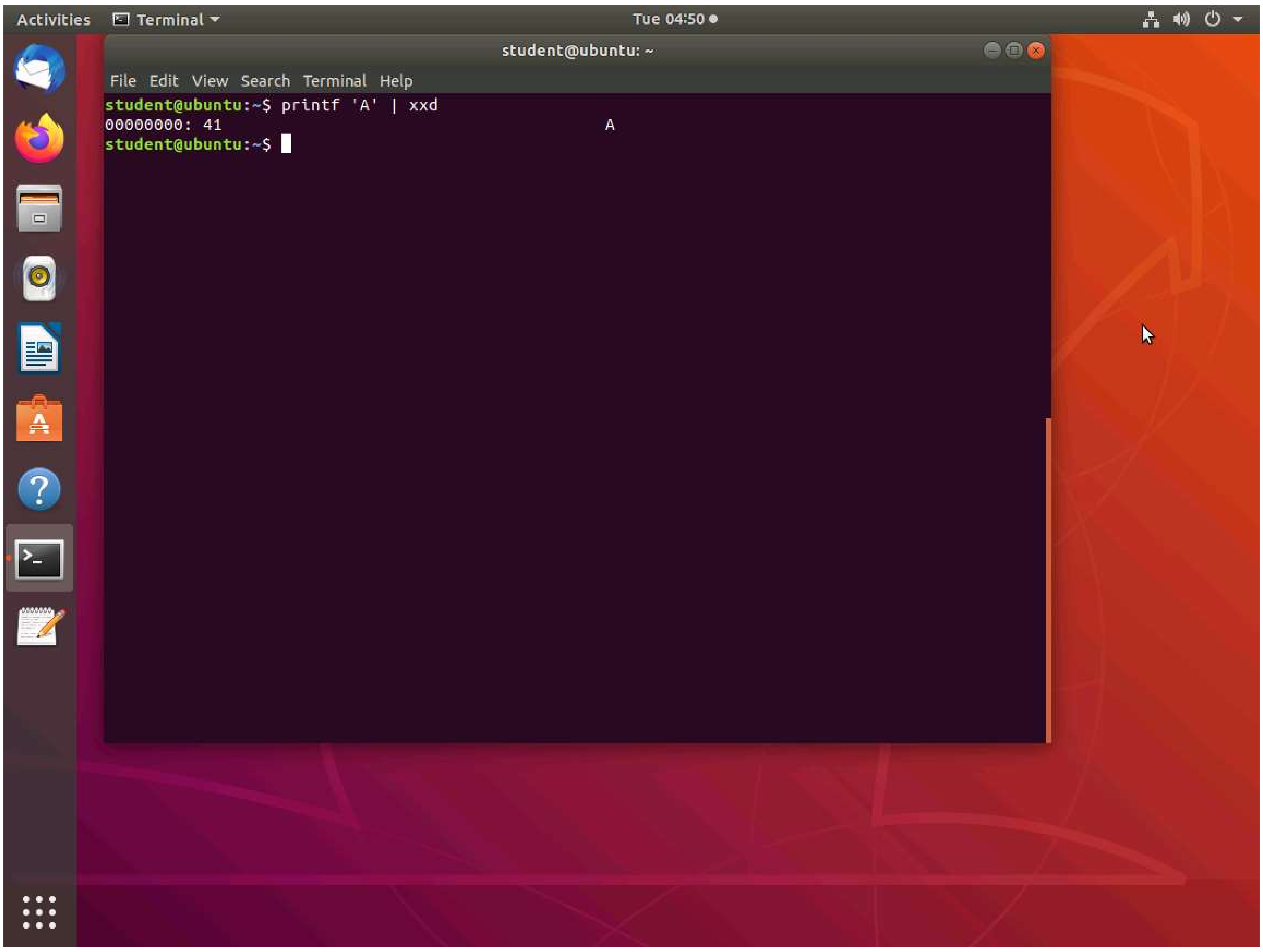
```
student@ubuntu:~$ sudo find /home -mtime -1
/home/student
/home/student/.bash_history
/home/student/.config/pulse/fc4cfbaf78304b9d9795ee7e44ffa67c-default-source
/home/student/.config/pulse/fc4cfbaf78304b9d9795ee7e44ffa67c-default-sink
/home/student/.config/gtk-3.0
/home/student/.config/gtk-3.0/bookmarks
/home/student/.config/nautilus
/home/student/.config/nautilus/desktop-metadata
/home/student/.config/dconf
/home/student/.config/dconf/user
/home/student/.config/gedit/accels
/home/student/.config/ibus/bus
/home/student/.config/ibus/bus/fc4cfbaf78304b9d9795ee7e44ffa67c-unix-1
/home/student/.ICEauthority
/home/student/wordlists 1.txt
/home/student/.cache/update-manager-core/meta-release-lts
/home/student/.cache/dconf
/home/student/.cache/gnome-software/cssresource
/home/student/.cache/gnome-software/cssresource/87b8dfef031ed4197b7d24bd84c7e21b906982d3-Banner
.png
/home/student/.cache/gnome-software/icons
/home/student/.cache/gnome-software/icons/5e9de398653e7e02f03096478236c7d654914d20-vana_linux_l
ogo2x.png
/home/student/.cache/gnome-software/icons/21298f008f60dcad04c4edb4401ad98a35bdf0c7-yakyak.png
/home/student/.cache/gnome-software/icons/0e0cf14ef7da36259a98da872a4daa606acdd823-flameshot.sv
g.png
/home/student/.cache/gnome-software/icons/e07b1d126ee7fb2c1fa365f06498a8726758ce08-application-
icon.png
/home/student/.cache/gnome-software/icons/132cec0d9b4337e577f0413fe87fb954ab72006a-logo.png
/home/student/.cache/gnome-software/icons/ae5a7cf11bc1927a8961d7e4aa575a3972a4fc54-icon-256x256
.png
/home/student/.cache/gnome-software/icons/a49688acd619ee16f82afb56879c0514c2f1fab3-dosbox-x.png
```

12. Another command we can use is the tool **xxd**. Type **sudo xxd -s 35 -l 50 wordlists.txt** and press **Enter**. An example of the output of the command is shown in the following screenshot.



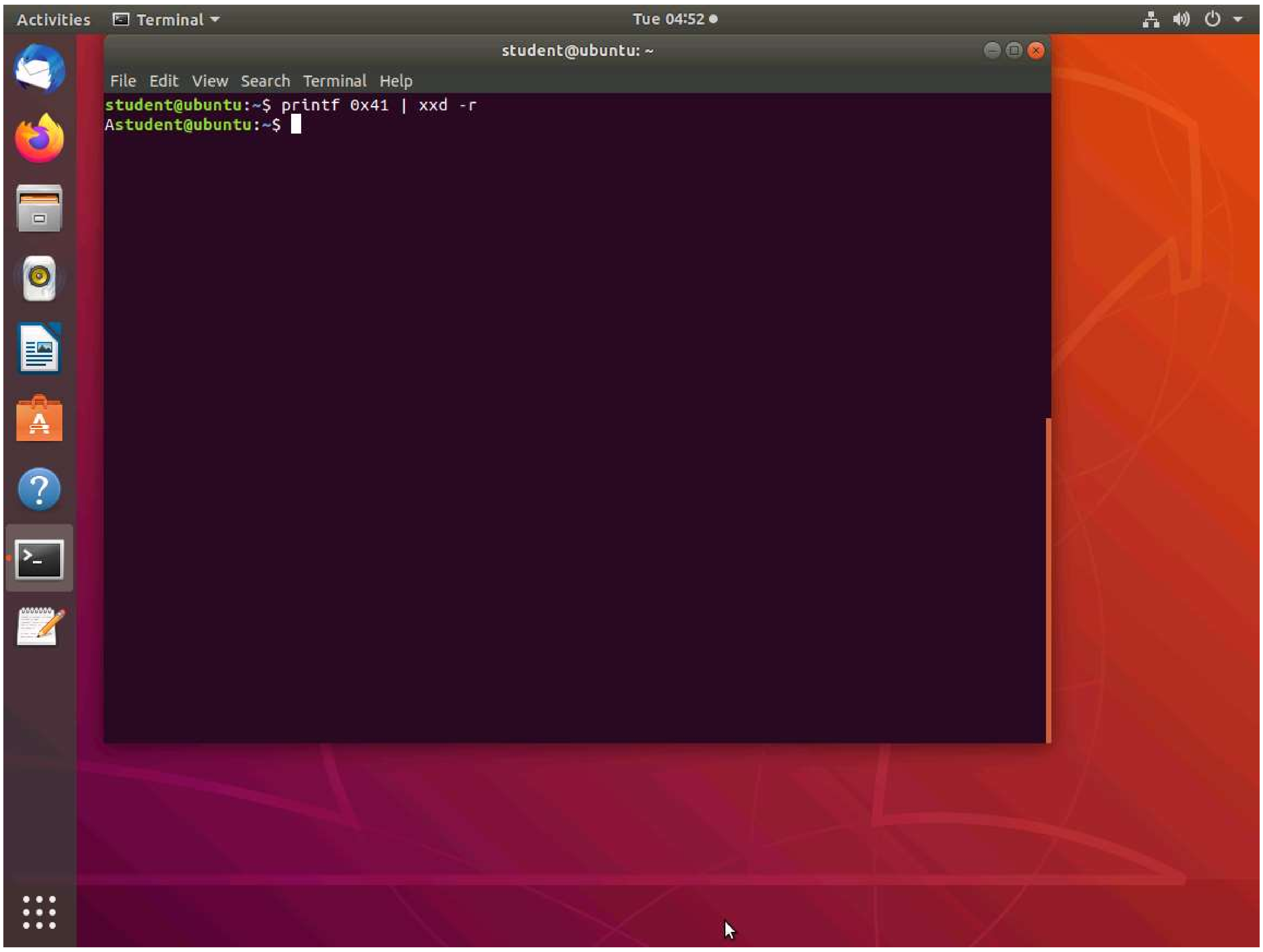
```
student@ubuntu:~$ sudo xxd -s 35 -l 50 wordlists.txt
00000023: 6775 6974 6172 0d0a 6170 6f6c 6c6f 0d0a  guitar..apollo..
00000033: 6275 7474 6572 0d0a 6a61 6775 6172 0d0a  butter..jaguar..
00000043: 3132 3334 3536 3738 0d0a 6368 656c 7365  12345678..chelse
00000053: 610d                                     a.
student@ubuntu:~$
```

13. Next, type **printf 'A' | xxd** and press **Enter** to convert **A** into hex.



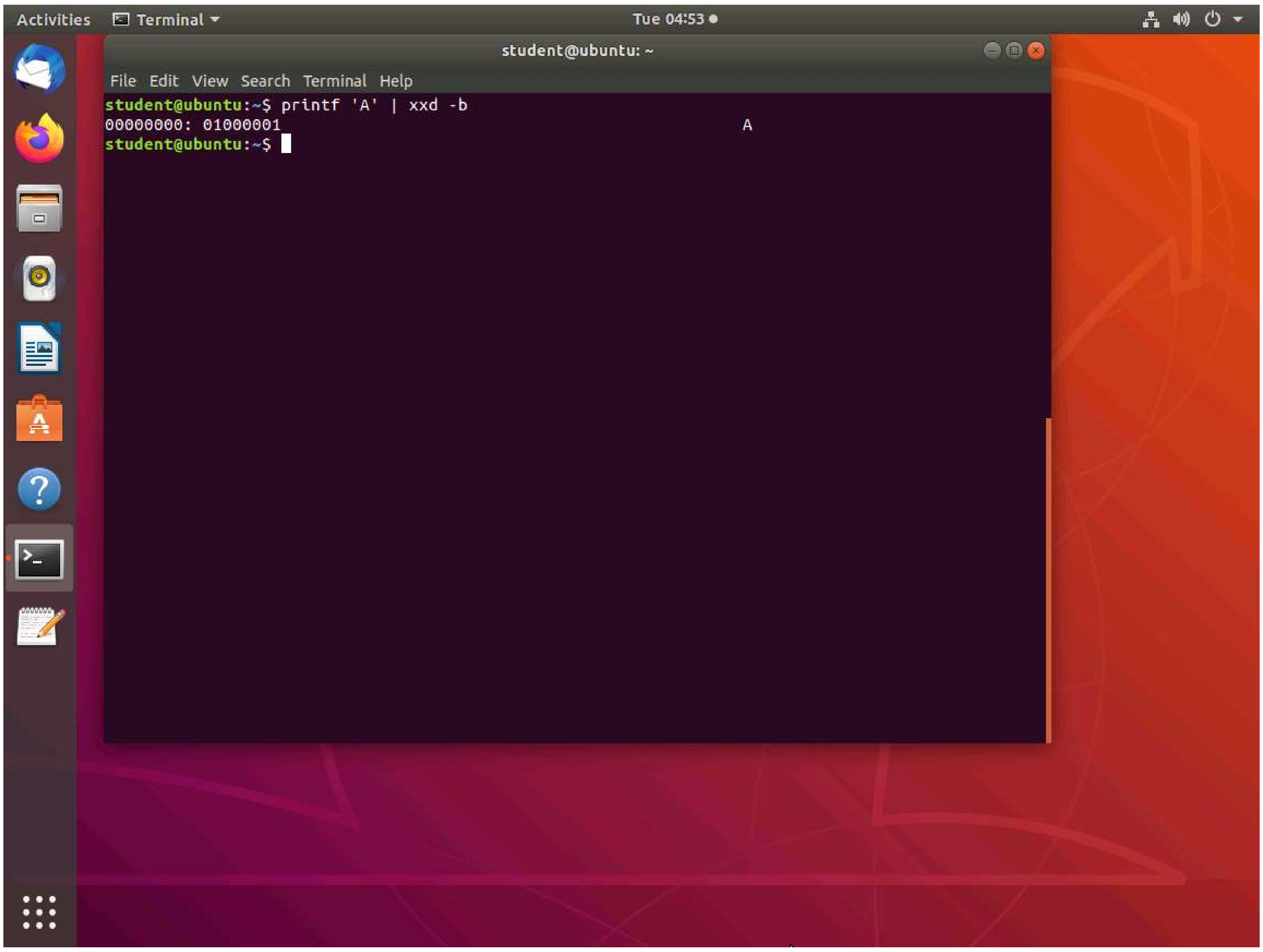
```
student@ubuntu:~$ printf 'A' | xxd
00000000: 41                                       A
student@ubuntu:~$
```

14. To convert from hex to ASCII, type **printf 0x41 | xxd -r** and press **Enter**.



```
student@ubuntu:~$ printf 0x41 | xxd -r
Astudent@ubuntu:~$ 
```

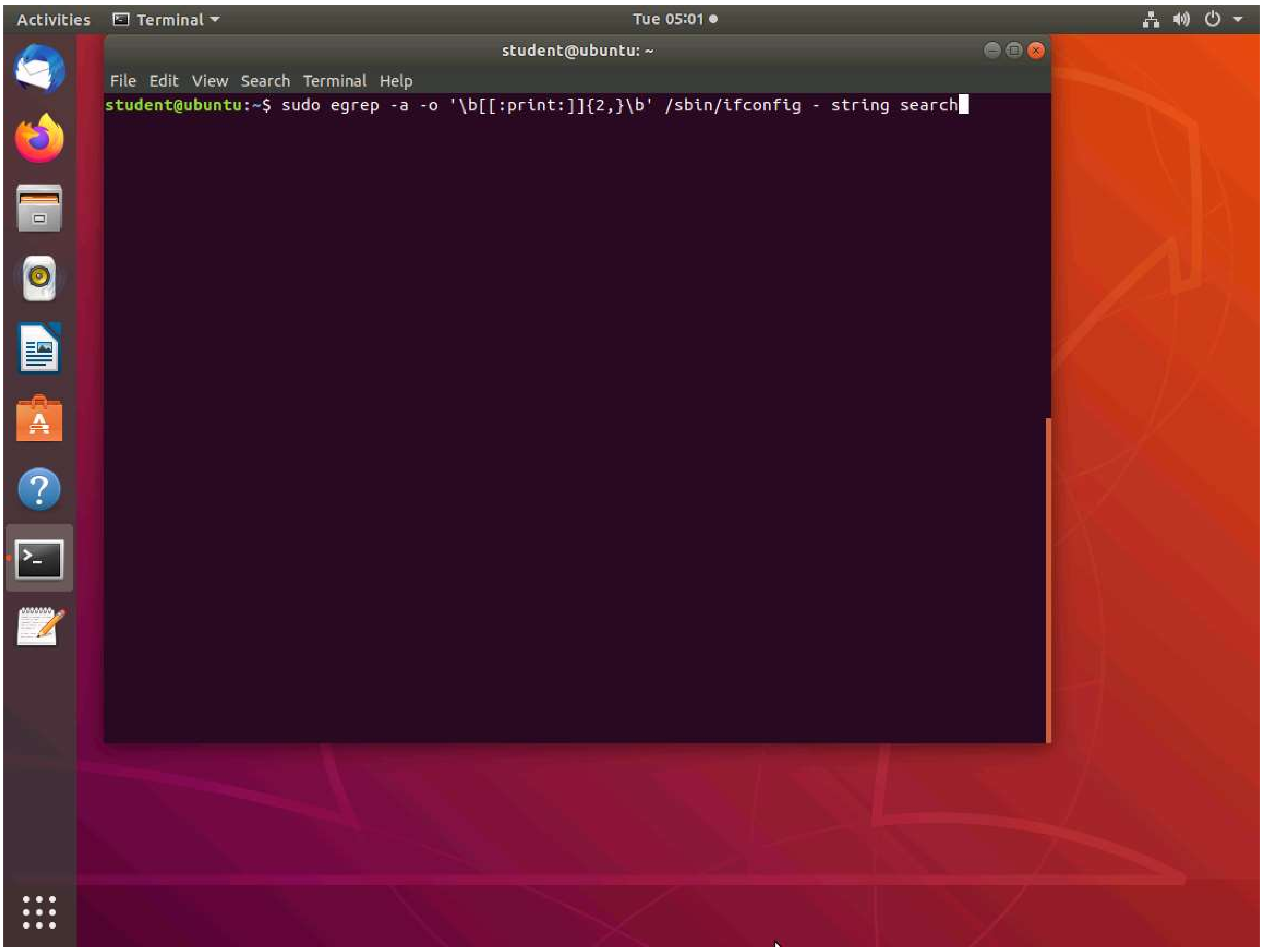
15. To output in binary, type **printf 'A' | xxd -b** and press **Enter**. The output of the command is shown in the following screenshot.



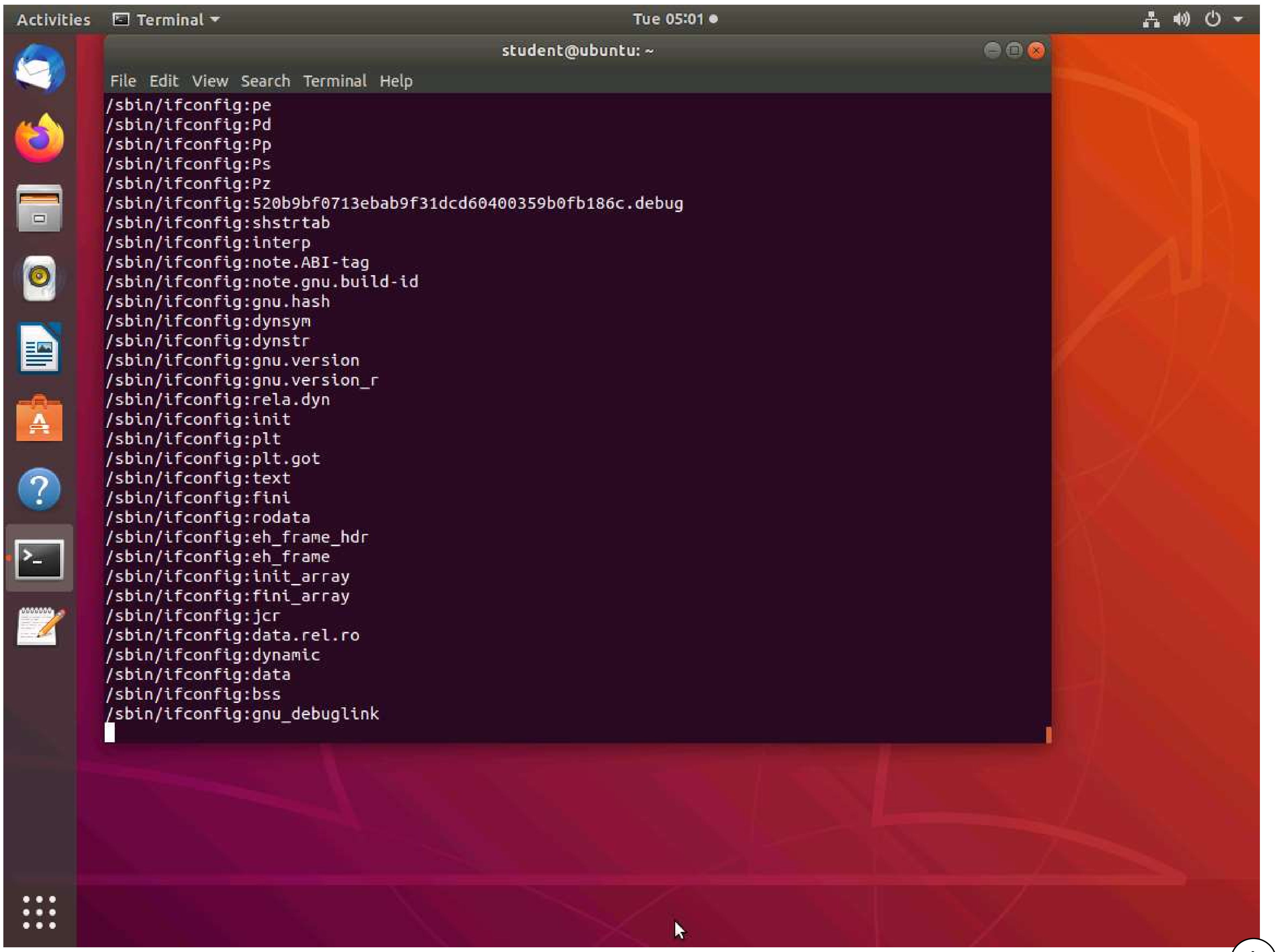
```
student@ubuntu:~$ printf 'A' | xxd -b
00000000: 01000001                                          A
student@ubuntu:~$ 
```

16. We will now explore the string search capability. Type **sudo egrep -a -o '\b[[:print:]]{2,}\b' somefile.exe – string search** and press **Enter**.

17. By replacing the **somefile.exe** with a binary file, you can use the file command to find one if needed or use **/sbin/ifconfig** as shown in the following screenshot. An example of the output of the command is shown in the following screenshot.

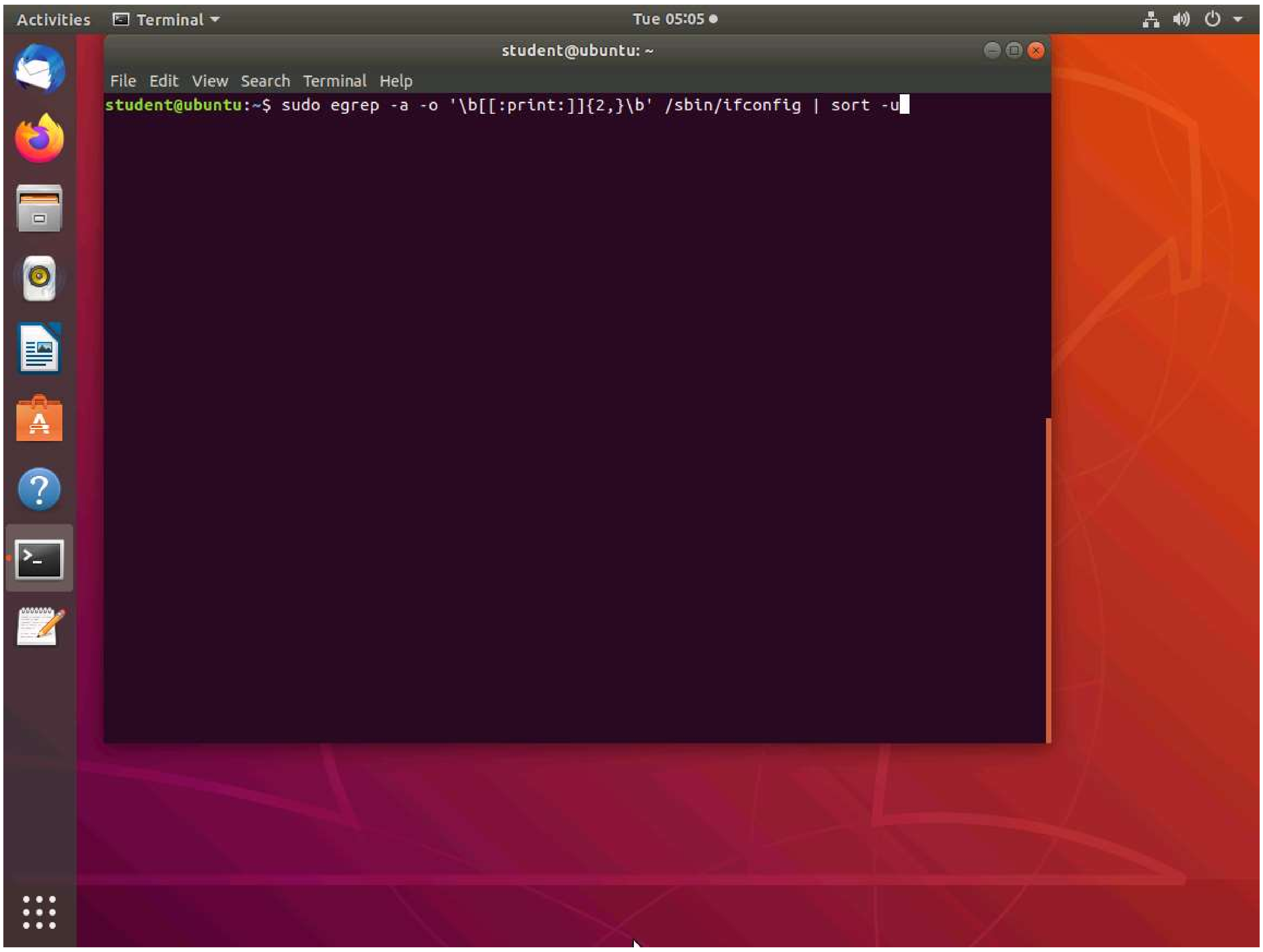


```
student@ubuntu:~$ sudo egrep -a -o '\b[[:print:]]{2,}\b' /sbin/ifconfig - string search
```

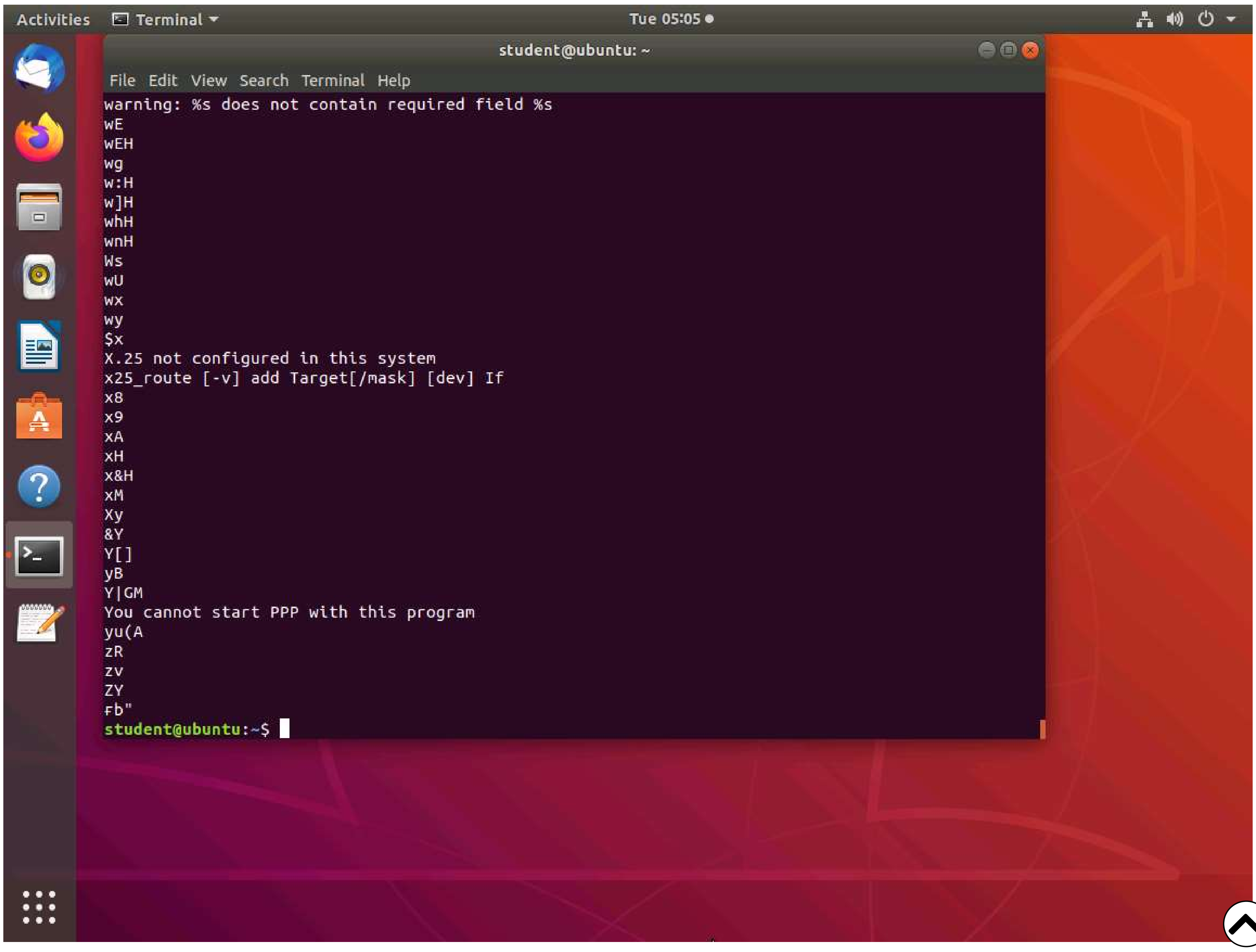


```
/sbin/ifconfig:pe
/sbin/ifconfig:Pd
/sbin/ifconfig:Pp
/sbin/ifconfig:Ps
/sbin/ifconfig:Pz
/sbin/ifconfig:520b9bf0713ebab9f31dcd60400359b0fb186c.debug
/sbin/ifconfig:shstrtab
/sbin/ifconfig:interp
/sbin/ifconfig:note.ABI-tag
/sbin/ifconfig:note.gnu.build-id
/sbin/ifconfig:gnu.hash
/sbin/ifconfig:dynsym
/sbin/ifconfig:dynstr
/sbin/ifconfig:gnu.version
/sbin/ifconfig:gnu.version_r
/sbin/ifconfig:rela.dyn
/sbin/ifconfig:init
/sbin/ifconfig:plt
/sbin/ifconfig:plt.got
/sbin/ifconfig:text
/sbin/ifconfig:fini
/sbin/ifconfig:rodata
/sbin/ifconfig:eh_frame_hdr
/sbin/ifconfig:eh_frame
/sbin/ifconfig:init_array
/sbin/ifconfig:fini_array
/sbin/ifconfig:jcr
/sbin/ifconfig:data.rel.ro
/sbin/ifconfig:dynamic
/sbin/ifconfig:data
/sbin/ifconfig:bss
/sbin/ifconfig:gnu_debuglink
```

18. Another useful feature is removing duplicates. Type **sudo egrep -a -o '\b[[:print:]]{2,}\b' /sbin/ifconfig | sort –u** and press **Enter**. We are piping the output into sort, which will remove any duplicates. This is another common feature of the files found during testing or competitions.



```
student@ubuntu:~$ sudo egrep -a -o '\b[[:print:]]{2,}\b' /sbin/ifconfig | sort -u
```



```
warning: %s does not contain required field %s
wE
wEH
wg
w:H
w]H
whH
wnH
Ws
wU
wx
wy
$x
X.25 not configured in this system
x25_route [-v] add Target[/mask] [dev] If
x8
x9
xA
xH
x&H
xM
Xy
&Y
Y[]
yB
Y|GM
You cannot start PPP with this program
yu(A
zR
zv
ZY
Fb"
student@ubuntu:~$
```

19. The lab objectives have been achieved.

Exercise 2: Basic cURL Queries

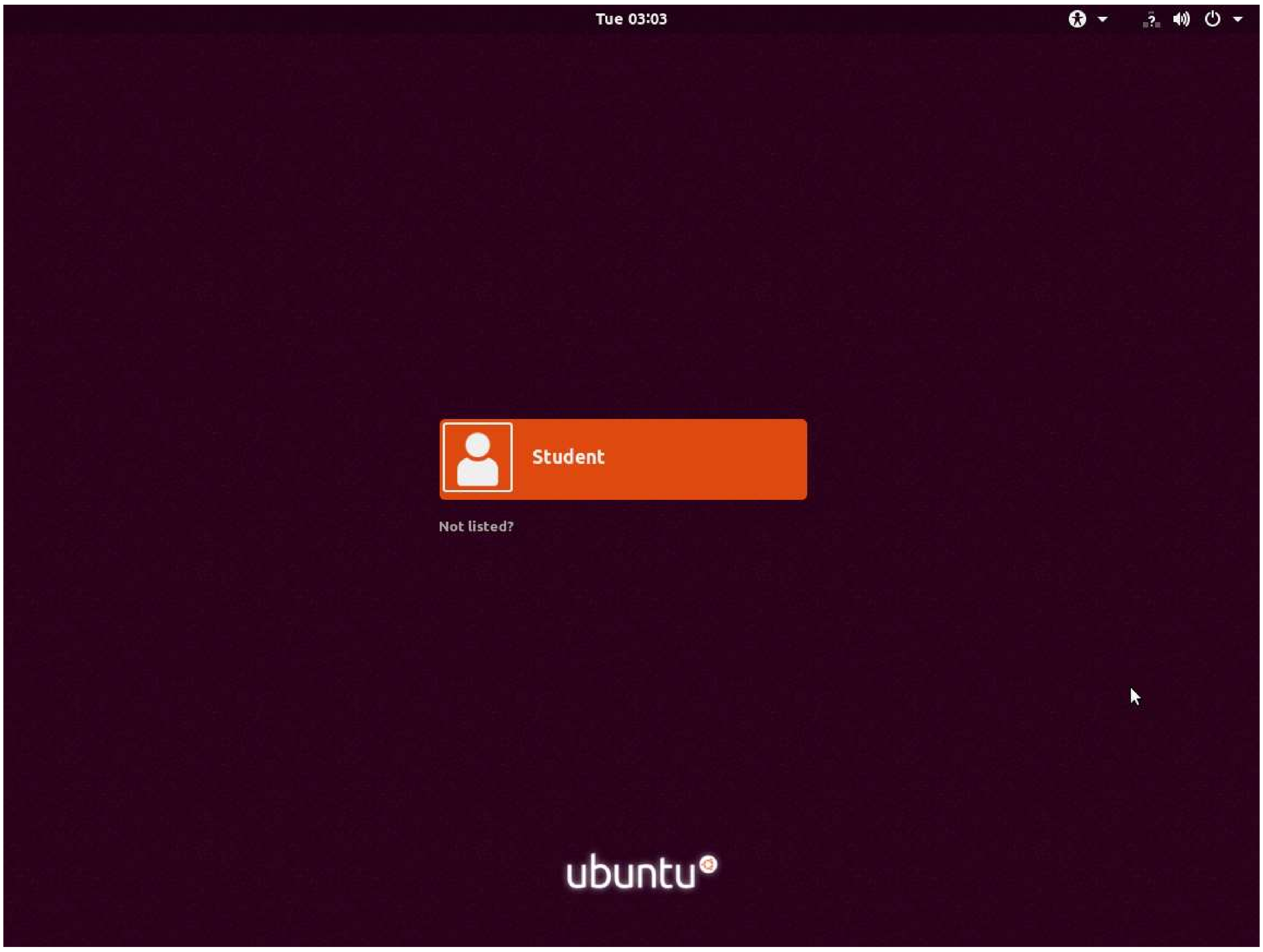
Objectives

- Create basic cURL queries, extract the data, and explore the features and components of cURL

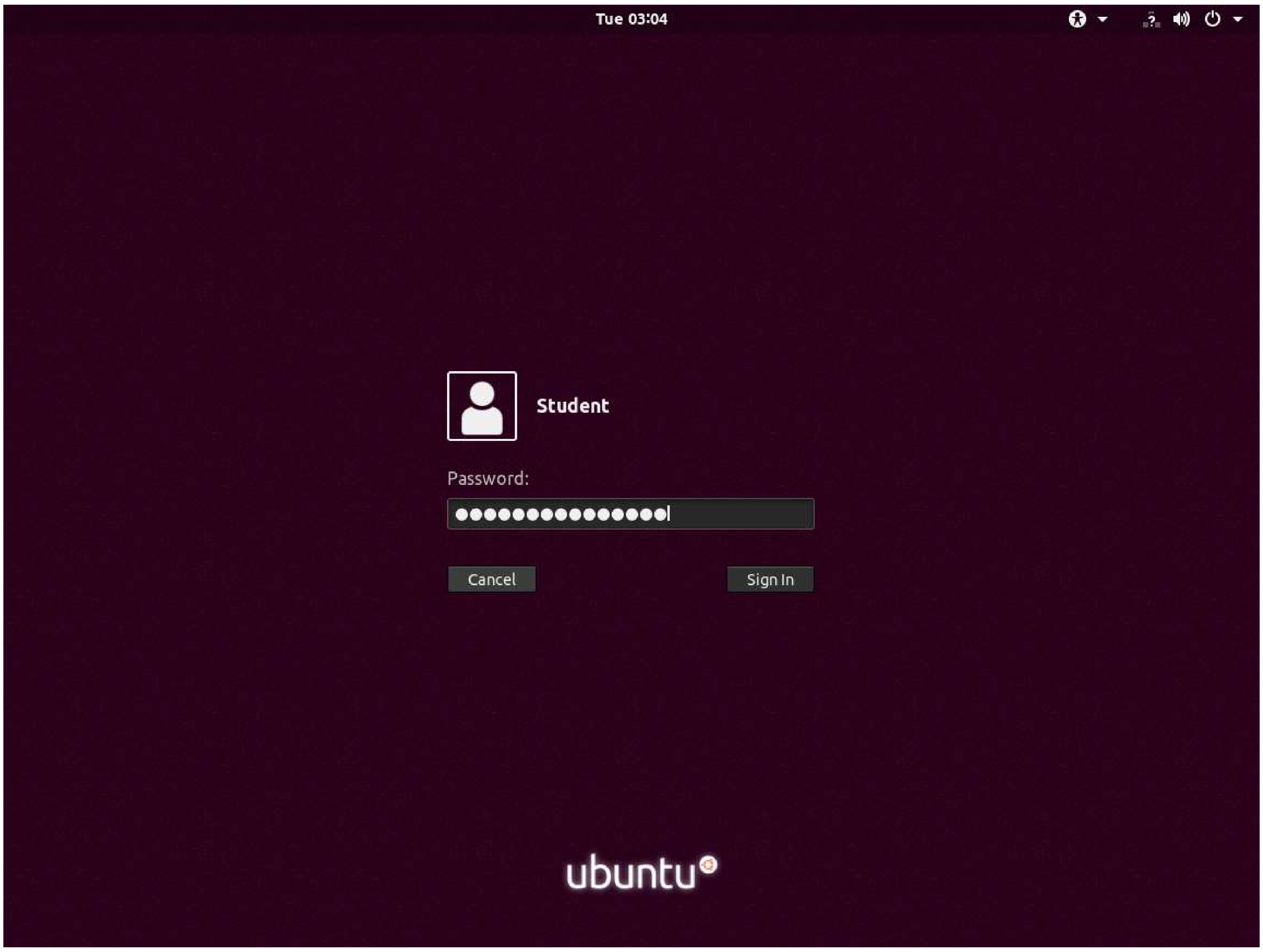
Lab Duration: **20** Minutes

1. **cURL** is a command line tool and a library that can be used to receive and send data between a client and a server or any two machines connected over the internet. It supports a wide range of protocols such as HTTP, FTP, IMAP, LDAP, POP3, and SMTP.
2. Due to its **versatile nature**, cURL is used in many applications and for many use cases. For example, the command line tool can be used to download files, testing Application Program Interfaces (APIs), and debugging network problems. In this lab, we shall look at how the cURL command line tool can be used to perform various tasks.
3. As a penetration tester, you need to be familiar with this tool. We will cover some of the usage examples in this lab, but this tool can be used in many ways.
4. In this exercise, we will review the different methods of extracting data using **cURL**.
5. By default **CPENT Bash Machine** machine selected, click Student profile to login.

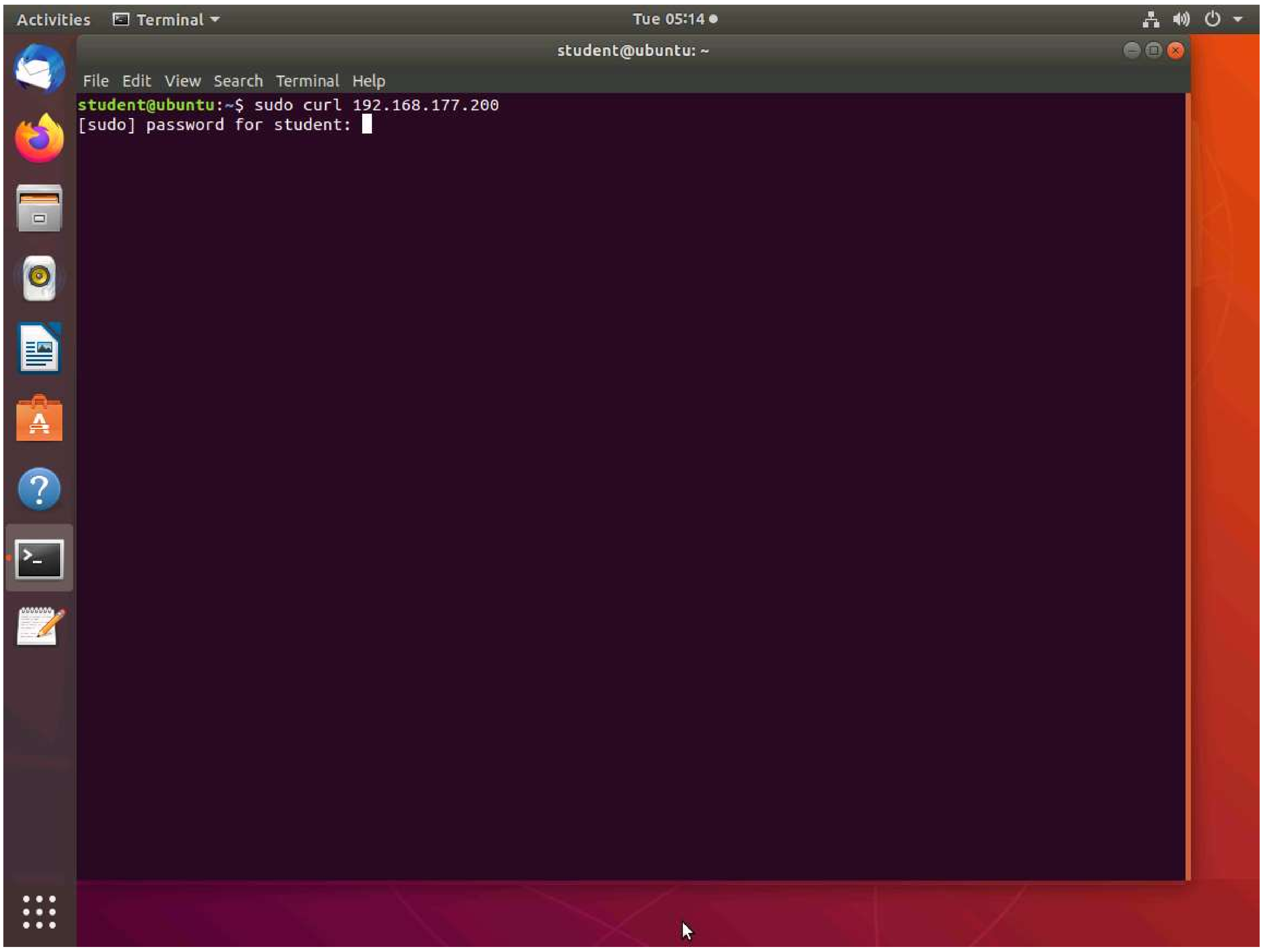
Note: If you are already logged in skip to step **7**.



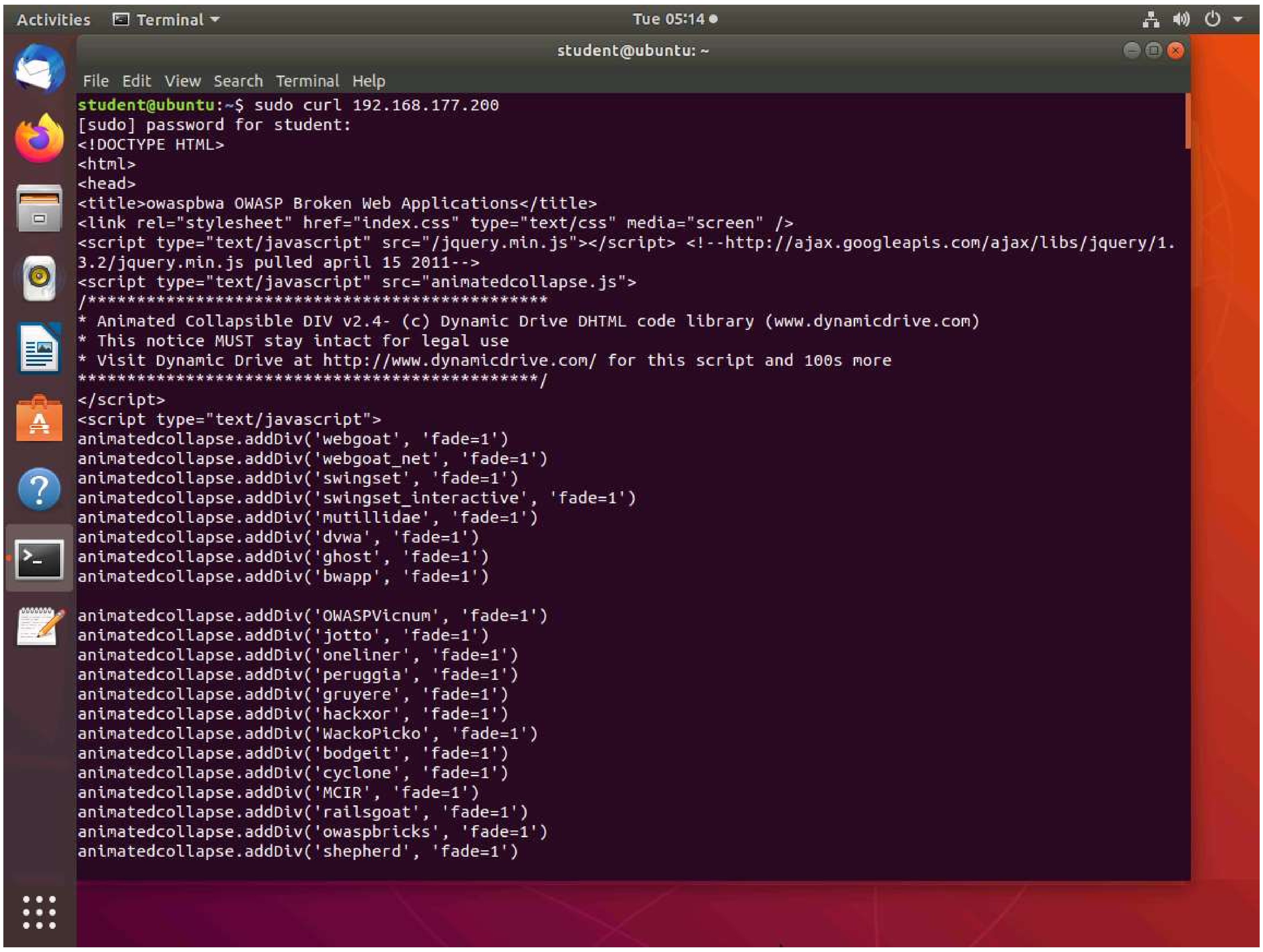
6. Type **password** in the Password field and click **Sign In**.



7. Launch Wireshark and click start capturing. For our first example, we will connect to the website. Type **sudo curl 192.168.177.200** and press **Enter**. Type **password** and press **Enter**.



```
student@ubuntu:~$ sudo curl 192.168.177.200
[sudo] password for student:
```

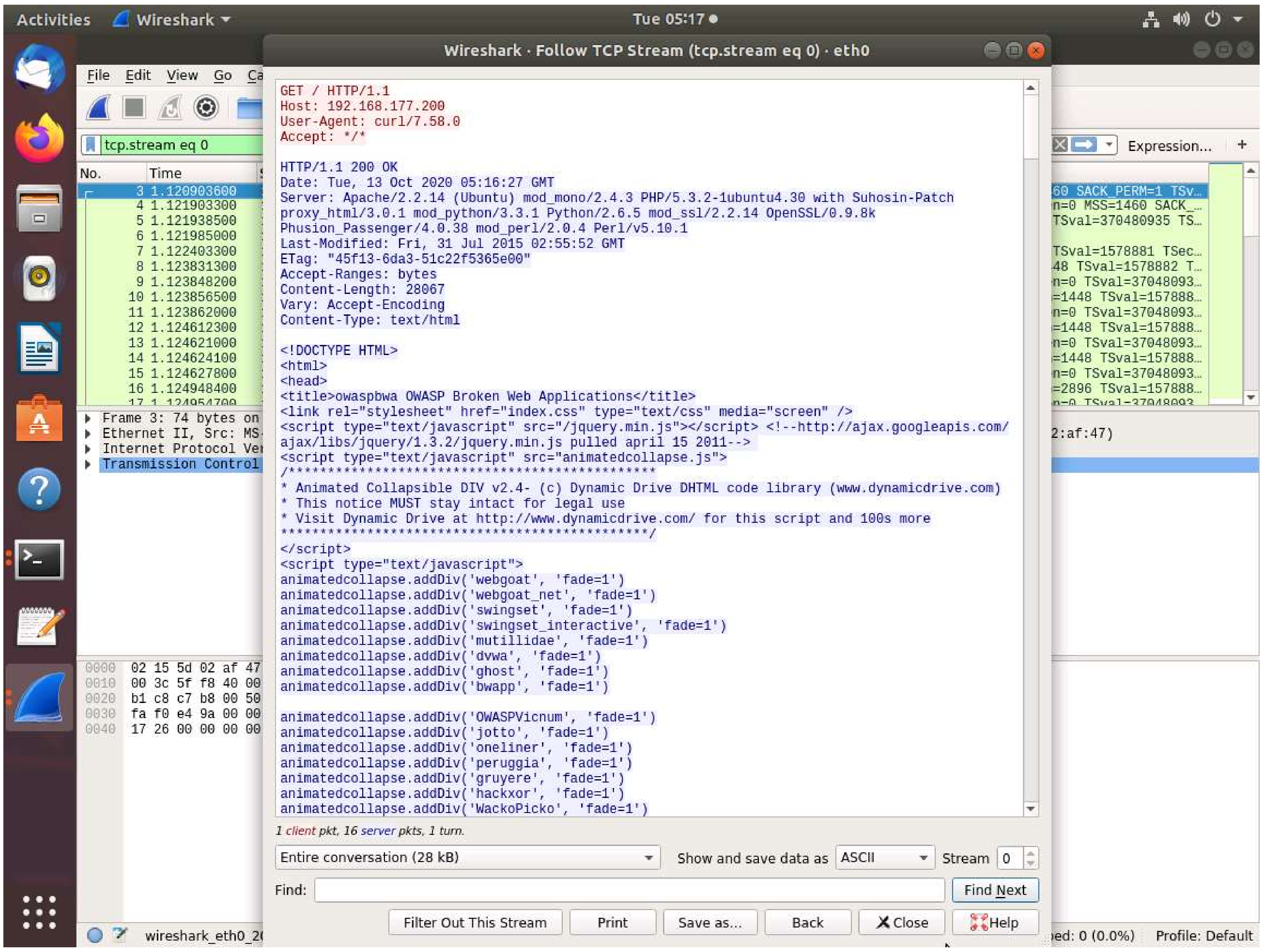


```
student@ubuntu:~$ sudo curl 192.168.177.200
[sudo] password for student:
<!DOCTYPE HTML>
<html>
<head>
<title>owaspbwa OWASP Broken Web Applications</title>
<link rel="stylesheet" href="index.css" type="text/css" media="screen" />
<script type="text/javascript" src="/jquery.min.js"></script> <!--http://ajax.googleapis.com/ajax/libs/jquery/1.
3.2/jquery.min.js pulled april 15 2011-->
<script type="text/javascript" src="animatedcollapse.js">
/***********************************************
* Animated Collapsible DIV v2.4- (c) Dynamic Drive DHTML code library (www.dynamicdrive.com)
* This notice MUST stay intact for legal use
* Visit Dynamic Drive at http://www.dynamicdrive.com/ for this script and 100s more
***********************************************/
</script>
<script type="text/javascript">
animatedcollapse.addDiv('webgoat', 'fade=1')
animatedcollapse.addDiv('webgoat_net', 'fade=1')
animatedcollapse.addDiv('swingset', 'fade=1')
animatedcollapse.addDiv('swingset_interactive', 'fade=1')
animatedcollapse.addDiv('mutillidae', 'fade=1')
animatedcollapse.addDiv('dvwa', 'fade=1')
animatedcollapse.addDiv('ghost', 'fade=1')
animatedcollapse.addDiv('bwapp', 'fade=1')

animatedcollapse.addDiv('OWASPVicnum', 'fade=1')
animatedcollapse.addDiv('jotto', 'fade=1')
animatedcollapse.addDiv('oneliner', 'fade=1')
animatedcollapse.addDiv('peruggia', 'fade=1')
animatedcollapse.addDiv('gruyere', 'fade=1')
animatedcollapse.addDiv('hackxor', 'fade=1')
animatedcollapse.addDiv('WackoPicko', 'fade=1')
animatedcollapse.addDiv('bodgeit', 'fade=1')
animatedcollapse.addDiv('cyclone', 'fade=1')
animatedcollapse.addDiv('MCIR', 'fade=1')
animatedcollapse.addDiv('railsgoat', 'fade=1')
animatedcollapse.addDiv('owaspbricks', 'fade=1')
animatedcollapse.addDiv('shepherd', 'fade=1')
```

8. In this form, the cURL tool is acting as a simple client. We have the capability to do this using **Telnet** and **netcat**, but the tool makes it in one go.

9. Let us now see what it looks like at the packet level. We need to know this in case we use it in testing. An example of the Wireshark session is shown in the following screenshot. The default User-Agent shows that the request comes from cURL. This could alert monitoring on different networks, so you might want to use the tools capability to customize the UA if this is included in the scope of work (evasion) or you are acting as a red team member.

Note: To open **Wireshark - Follow TCP Stream** window, click **Analyze** in the menu bar and navigate to **Follow** --> **TCP Stream**.

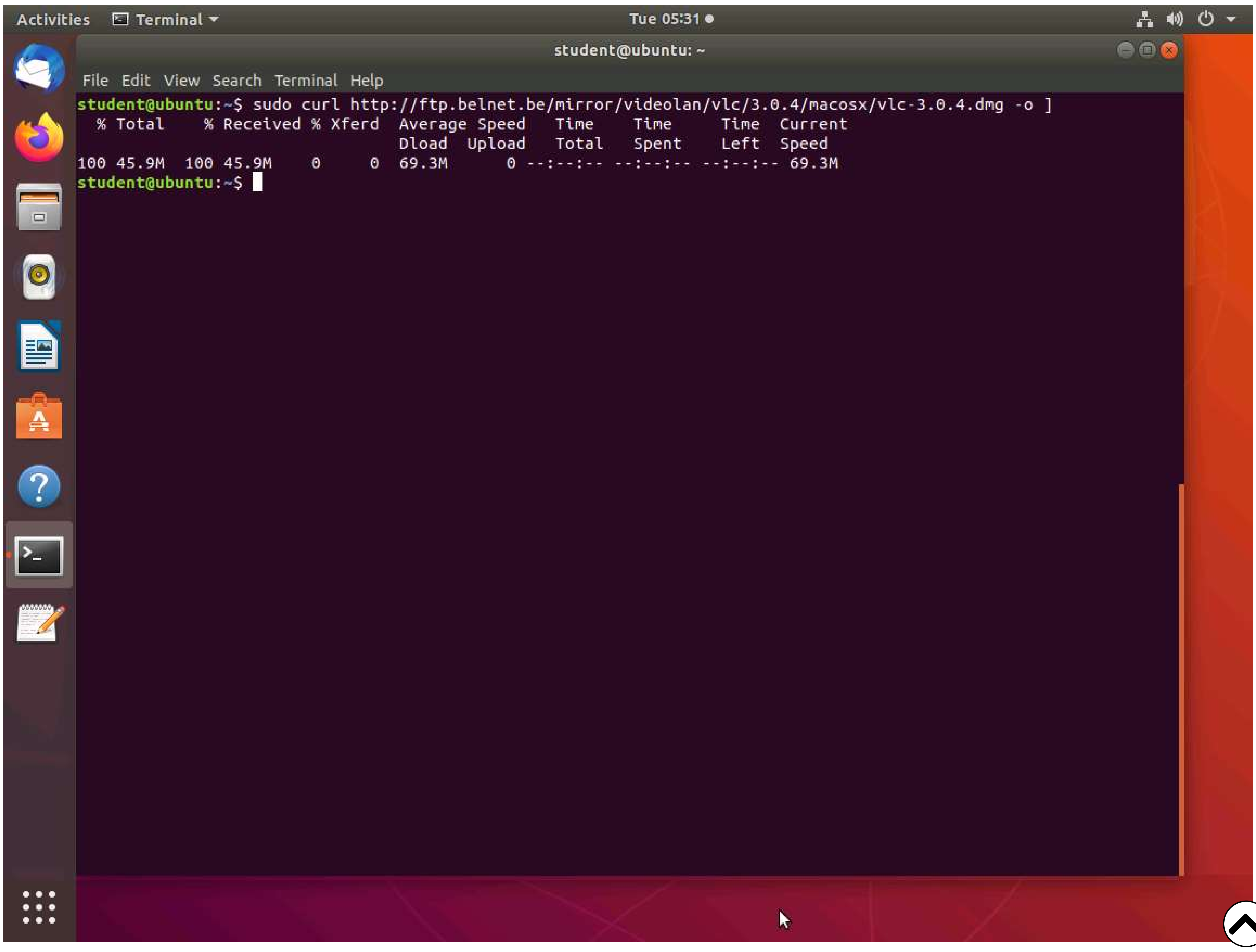


```
GET / HTTP/1.1
Host: 192.168.177.200
User-Agent: curl/7.58.0
Accept: */*

HTTP/1.1 200 OK
Date: Tue, 13 Oct 2020 05:16:27 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch
proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k
Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
Last-Modified: Fri, 31 Jul 2015 02:55:52 GMT
ETag: "45f13-6da3-51c22f5365e00"
Accept-Ranges: bytes
Content-Length: 28067
Vary: Accept-Encoding
Content-Type: text/html

<!DOCTYPE HTML>
<html>
<head>
<title>owaspbwa OWASP Broken Web Applications</title>
<link rel="stylesheet" href="index.css" type="text/css" media="screen" />
<script type="text/javascript" src="/jquery.min.js"></script> <!--http://ajax.googleapis.com/
ajax/libs/jquery/1.3.2/jquery.min.js pulled april 15 2011-->
<script type="text/javascript" src="animatedcollapse.js">
/***********************************************
* Animated Collapsible DIV v2.4- (c) Dynamic Drive DHTML code library (www.dynamicdrive.com)
* This notice MUST stay intact for legal use
* Visit Dynamic Drive at http://www.dynamicdrive.com/ for this script and 100s more
***********************************************/
</script>
<script type="text/javascript">
animatedcollapse.addDiv('webgoat', 'fade=1')
animatedcollapse.addDiv('webgoat_net', 'fade=1')
animatedcollapse.addDiv('swingset', 'fade=1')
animatedcollapse.addDiv('swingset_interactive', 'fade=1')
animatedcollapse.addDiv('mutillidae', 'fade=1')
animatedcollapse.addDiv('dvwa', 'fade=1')
animatedcollapse.addDiv('ghost', 'fade=1')
animatedcollapse.addDiv('bwapp', 'fade=1')

animatedcollapse.addDiv('OWASPVicnum', 'fade=1')
animatedcollapse.addDiv('jotto', 'fade=1')
animatedcollapse.addDiv('oneliner', 'fade=1')
animatedcollapse.addDiv('peruggia', 'fade=1')
animatedcollapse.addDiv('gruyere', 'fade=1')
animatedcollapse.addDiv('hackxor', 'fade=1')
animatedcollapse.addDiv('WackoPicko', 'fade=1')
```

Activities
Wireshark
Tue 05:17
Wireshark · Follow TCP Stream (tcp.stream eq 0) · eth0
tcp.stream eq 0
1 client pkt, 16 server pkts, 1 turn.
Entire conversation (28 kB)
Show and save data as ASCII
Stream 0
Find:
Find Next
Filter Out This Stream
Print
Save as…
Back
Close
Help

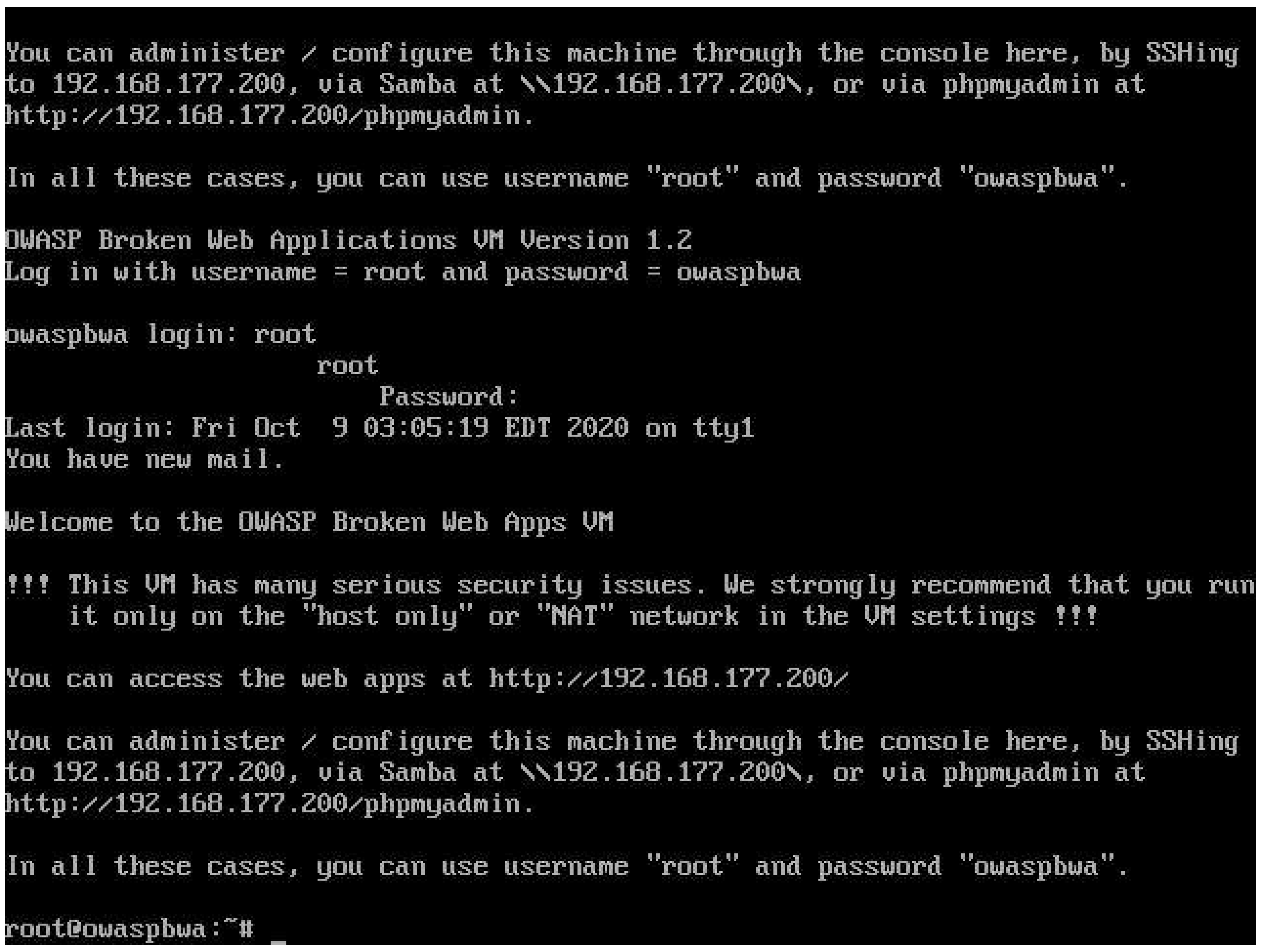
10. Similar to most tools, the cURL utility has the ability to output to a file. cURL uses the **-o** option. The tool can download, and when it does, a progress bar shows the download statistics. An example of this is shown in the following screenshot.

11. If you have a partially downloaded file, you can resume the file download with the -C – option.



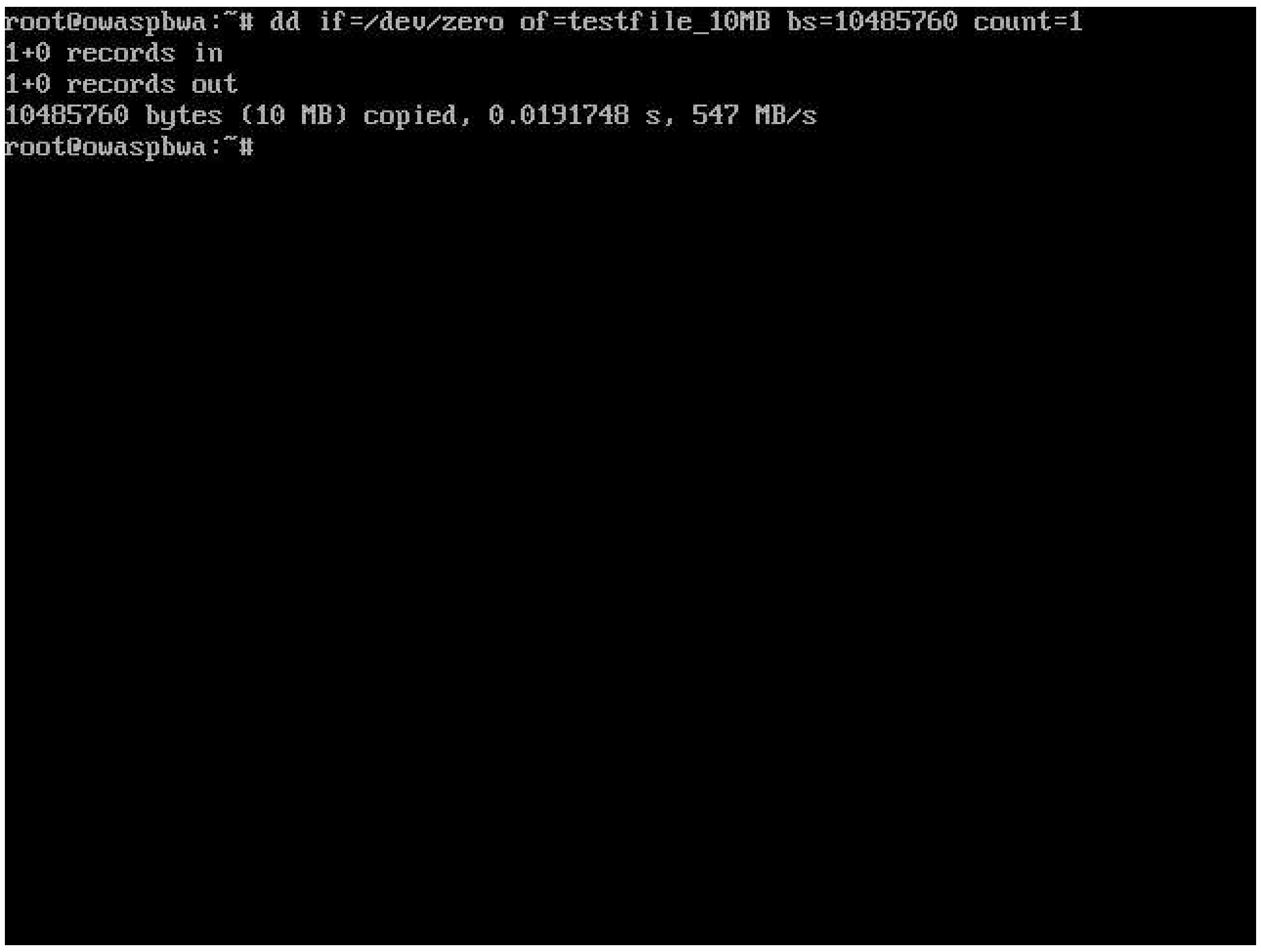
```
student@ubuntu:~$ sudo curl http://ftp.belnet.be/mirror/videolan/vlc/3.0.4/macosx/vlc-3.0.4.dmg -o ]
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 45.9M  100 45.9M    0     0  69.3M      0 --:--:-- --:--:-- --:--:-- 69.3M
student@ubuntu:~$ 
```

12. We can test this now. Log in to the **Target_CPENT Bash-Web** machine with the username as **root** and password as **owaspbwa**.



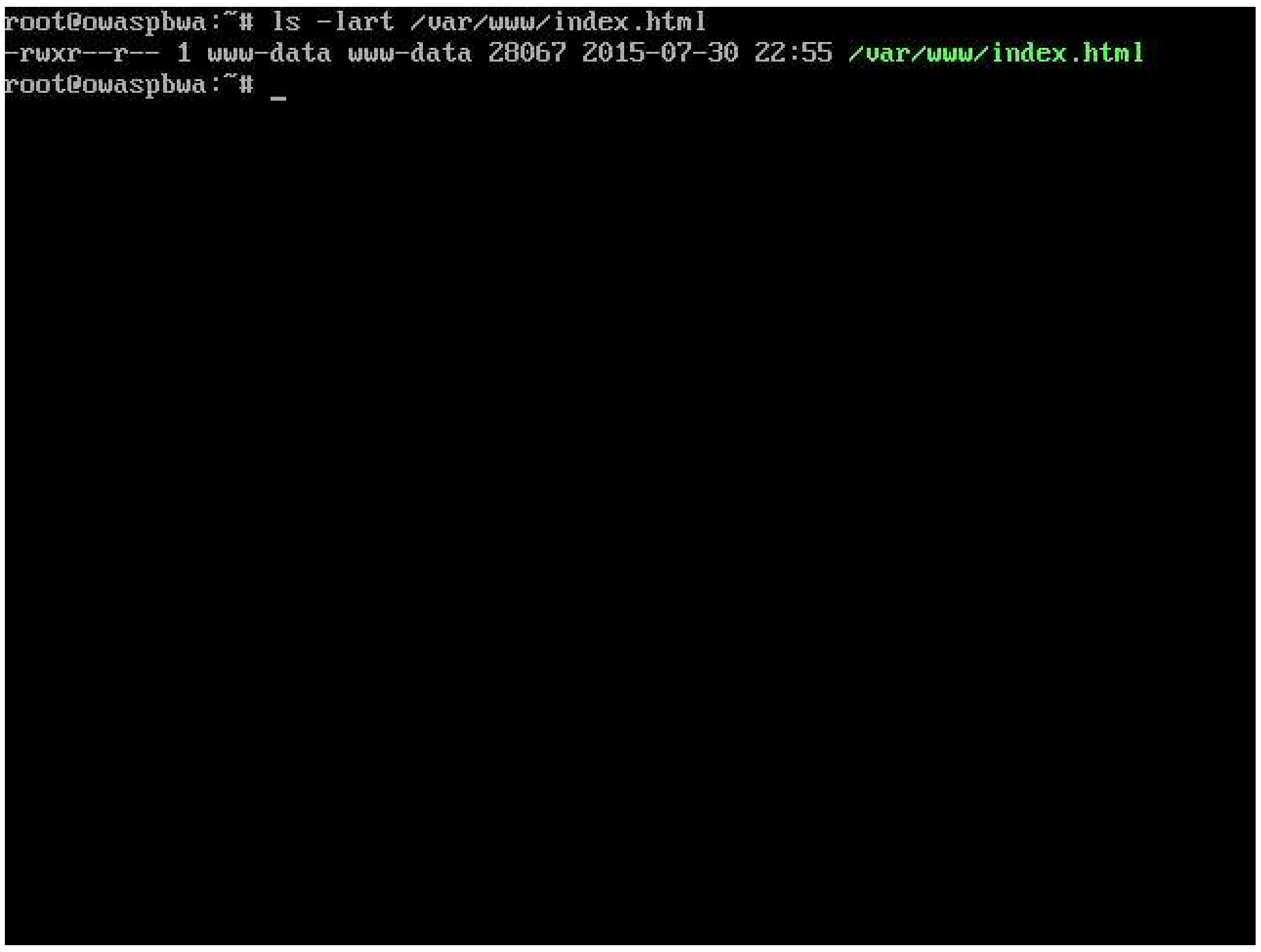
```
You can administer / configure this machine through the console here, by SSHing
to 192.168.177.200, via Samba at \\192.168.177.200\, or via phpmyadmin at
http://192.168.177.200/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

OWASP Broken Web Applications VM Version 1.2
Log in with username = root and password = owaspbwa

owaspbwa login: root
                    root
                        Password:
Last login: Fri Oct  9 03:05:19 EDT 2020 on tty1
You have new mail.

Welcome to the OWASP Broken Web Apps VM

!!! This VM has many serious security issues. We strongly recommend that you run
    it only on the "host only" or "NAT" network in the VM settings !!!

You can access the web apps at http://192.168.177.200/

You can administer / configure this machine through the console here, by SSHing
to 192.168.177.200, via Samba at \\192.168.177.200\, or via phpmyadmin at
http://192.168.177.200/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

root@owaspbwa:~# _
```

13. Once you are in the machine, you can use the **dd** command to create the file. Type **dd if=/dev/zero of=testfile_10MB bs=10485760 count=1** and press **Enter**.



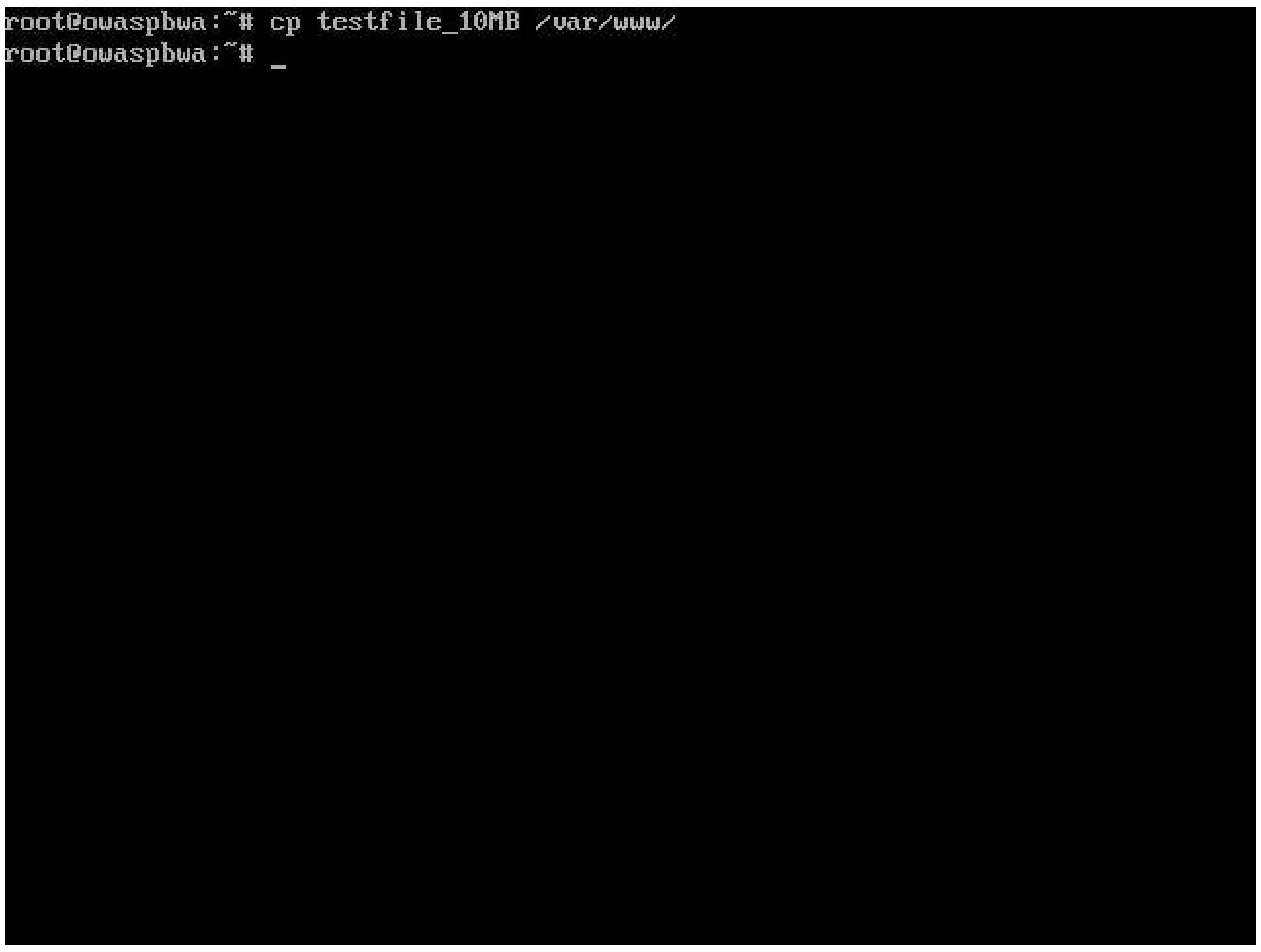
```
root@owaspbwa:~# dd if=/dev/zero of=testfile_10MB bs=10485760 count=1
1+0 records in
1+0 records out
10485760 bytes (10 MB) copied, 0.0191748 s, 547 MB/s
root@owaspbwa:~#
```

14. Next, we need to copy the file to the root folder for the web server. First, we need to identify its location. In most cases, the **root** folder is in a default location. So let us see if this is the case. Type **ls -lart /var/www/index.html** and press **Enter**. An example of the output of the command is shown in the following screenshot.



```
root@owaspbwa:~# ls -lart /var/www/index.html
-rwxr--r-- 1 www-data www-data 28067 2015-07-30 22:55 /var/www/index.html
root@owaspbwa:~# _
```

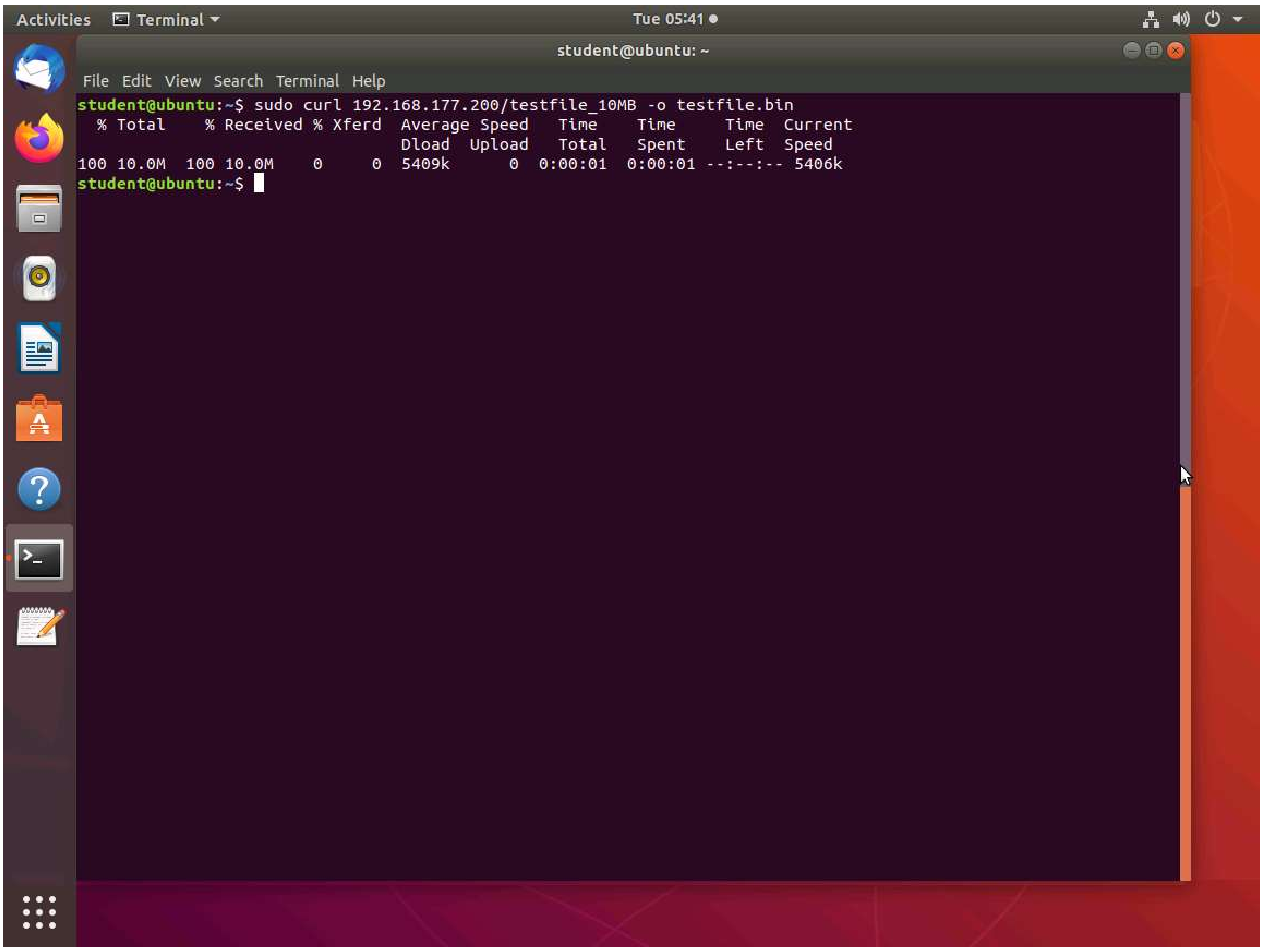
15. Now that the file has been verified along with the path, we can copy our created file there. Type **cp testfile_10MB /var/www/** and press **Enter**.



```
root@owaspbwa:~# cp testfile_10MB /var/www/
root@owaspbwa:~# _
```

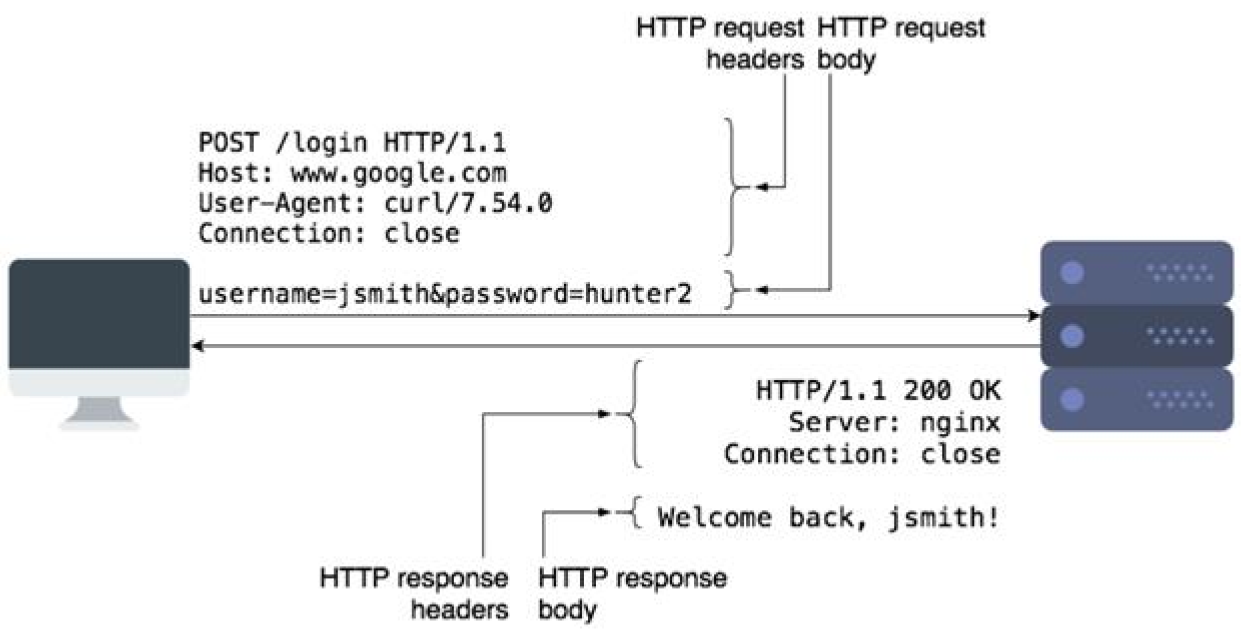
16. Switch to **CPENT Bash Machine** machine and type **sudo curl 192.168.177.200/testfile_10MB -o testfile.bin** and press **Enter**.

Note: 192.168.177.200 is the IP of the **Target_CPENT Bash-Web** machine.



```
student@ubuntu:~$ sudo curl 192.168.177.200/testfile_10MB -o testfile.bin
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 10.0M  100 10.0M    0     0  5409k      0  0:00:01  0:00:01 --:--:-- 5406k
student@ubuntu:~$ 
```

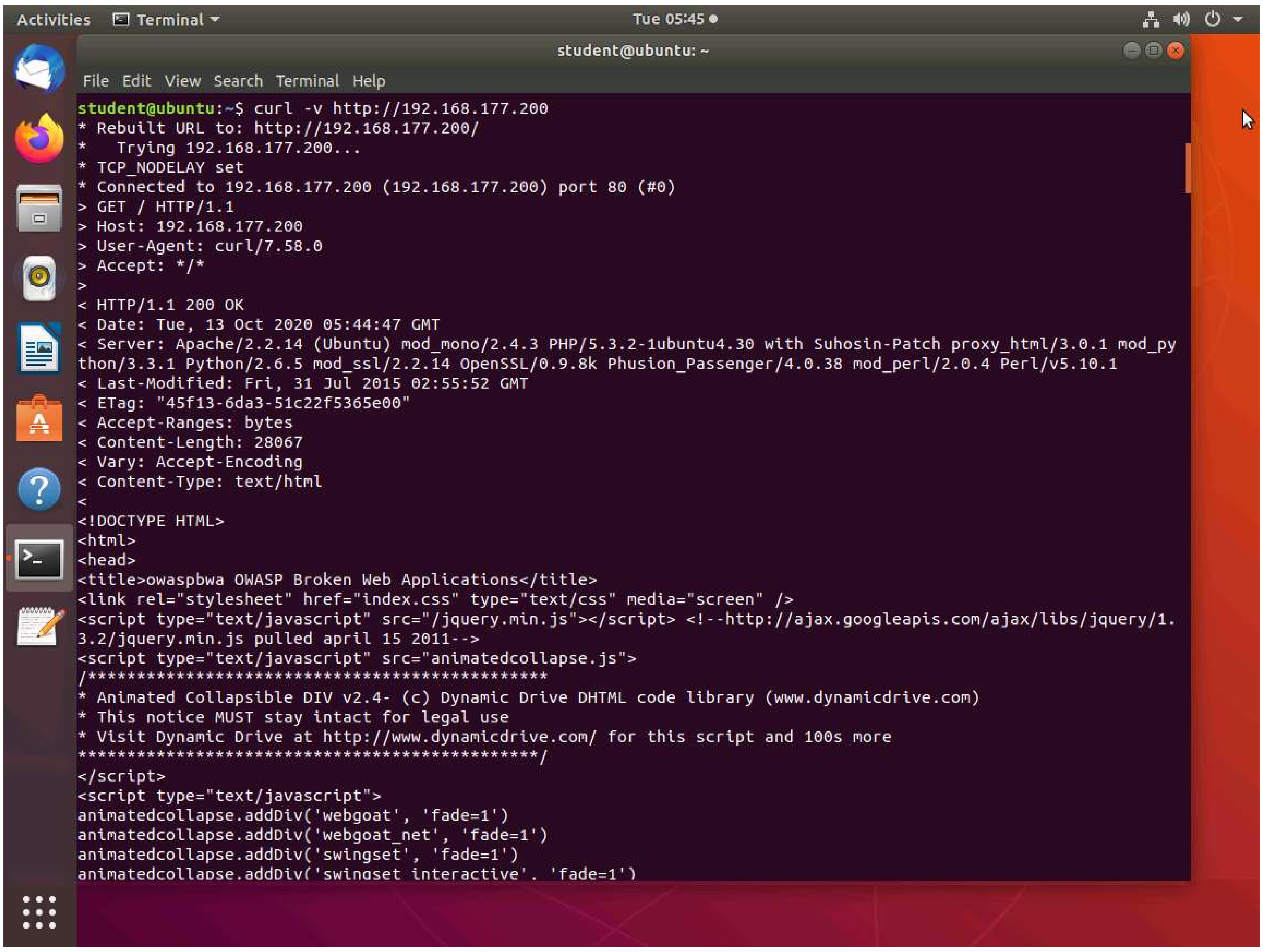
17. Before we delve further into the features supported by cURL, we will discuss HTTP requests and responses in more detail. If you are familiar with these concepts, you can skip to Step **20**. As per the RFC, to request a resource such as a web page or to submit data to a server, an HTTP client (such as a browser or cURL) makes an HTTP request to the server. The server responds with an HTTP response, which contains the "contents" of that page. An example of this is shown in the following screenshot.



18. HTTP requests contain the request method, URL, some headers, and some optional data as part of the "request body." The request method controls how a certain request should be processed. The most common types of request methods are "GET" and "POST." Typically, we use "GET" requests to retrieve a resource from the server and "POST" to submit data to the server for processing. "POST" requests generally contain some data in the request body, which the server can use.

19. HTTP responses are similar and contain the status code, some headers, and a body. The body contains the actual data that clients can display or save to a file. The status code is a three-digit code, which tells the client if the request succeeded or failed, and how to proceed further. Common status codes are 2xx (success), 3xx (redirect to another page), and 4xx/5xx (for errors).

20. To review the request headers and connection details, you can use the verbose option. Type **curl -v http://192.168.177.200** and press **Enter**. An example of the output from the command is shown in the following screenshot.

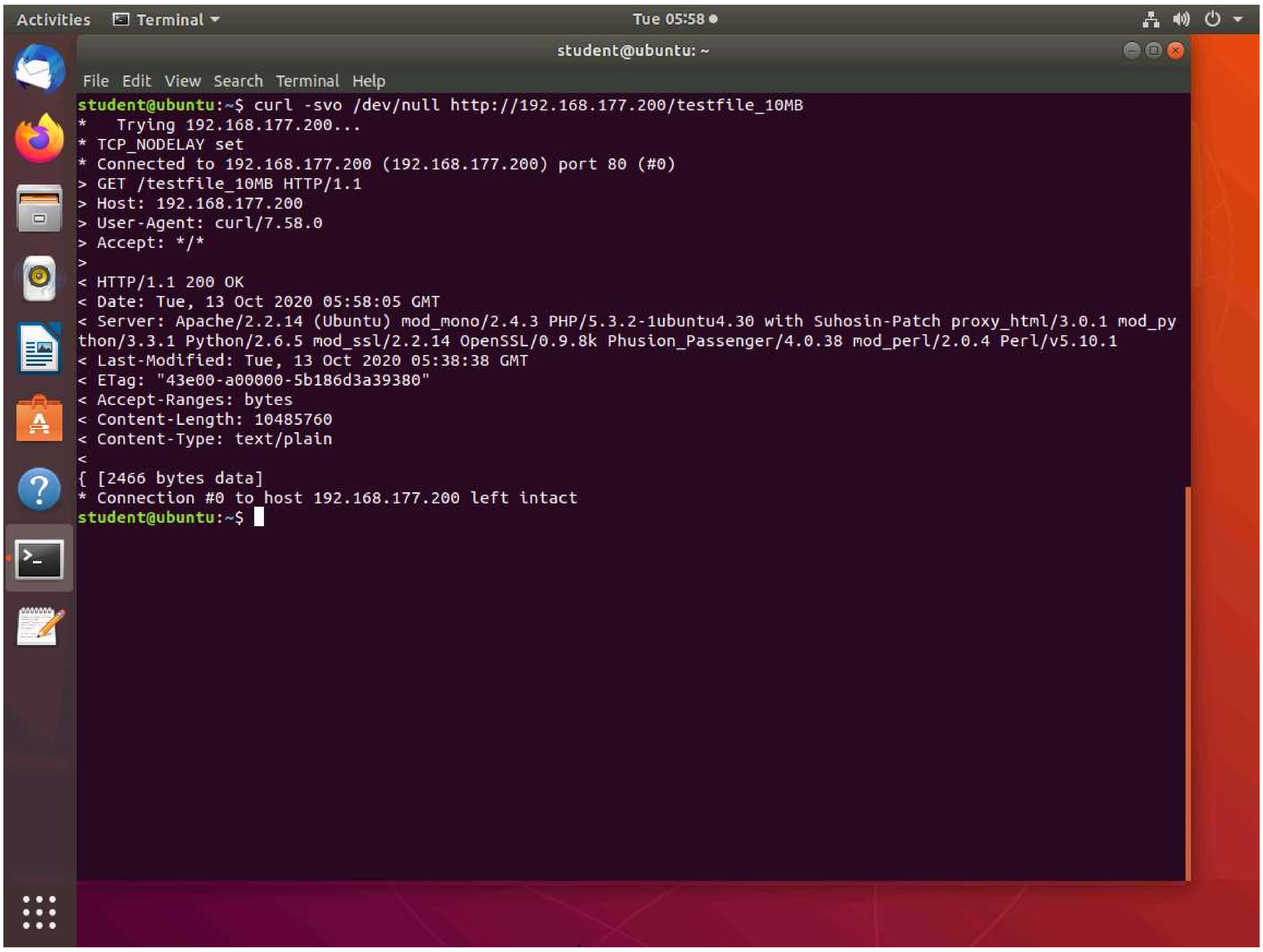


```
student@ubuntu:~$ curl -v http://192.168.177.200
* Rebuilt URL to: http://192.168.177.200/
*   Trying 192.168.177.200...
* TCP_NODELAY set
* Connected to 192.168.177.200 (192.168.177.200) port 80 (#0)
> GET / HTTP/1.1
> Host: 192.168.177.200
> User-Agent: curl/7.58.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Tue, 13 Oct 2020 05:44:47 GMT
< Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_py
thon/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
< Last-Modified: Fri, 31 Jul 2015 02:55:52 GMT
< ETag: "45f13-6da3-51c22f5365e00"
< Accept-Ranges: bytes
< Content-Length: 28067
< Vary: Accept-Encoding
< Content-Type: text/html
<
<!DOCTYPE HTML>
<html>
<head>
<title>owaspbwa OWASP Broken Web Applications</title>
<link rel="stylesheet" href="index.css" type="text/css" media="screen" />
<script type="text/javascript" src="/jquery.min.js"></script> <!--http://ajax.googleapis.com/ajax/libs/jquery/1.
3.2/jquery.min.js pulled april 15 2011-->
<script type="text/javascript" src="animatedcollapse.js">
/***********************************************
* Animated Collapsible DIV v2.4- (c) Dynamic Drive DHTML code library (www.dynamicdrive.com)
* This notice MUST stay intact for legal use
* Visit Dynamic Drive at http://www.dynamicdrive.com/ for this script and 100s more
***********************************************/
</script>
<script type="text/javascript">
animatedcollapse.addDiv('webgoat', 'fade=1')
animatedcollapse.addDiv('webgoat_net', 'fade=1')
animatedcollapse.addDiv('swingset', 'fade=1')
animatedcollapse.addDiv('swingset interactive', 'fade=1')
```

21. Take a few minutes to review the output. If you so prefer, you can output the command to a file and review it there as well later. The output contains **request data** (marked with >), **response headers** (marked with <), and other details about the request such as the IP used and the SSL handshake process (marked with *). When the HTTPS protocol is used.

22. Most often, we are not interested in the response body. You can simply hide it by "saving" the output to the null device, which is /dev/null (the bit bucket).

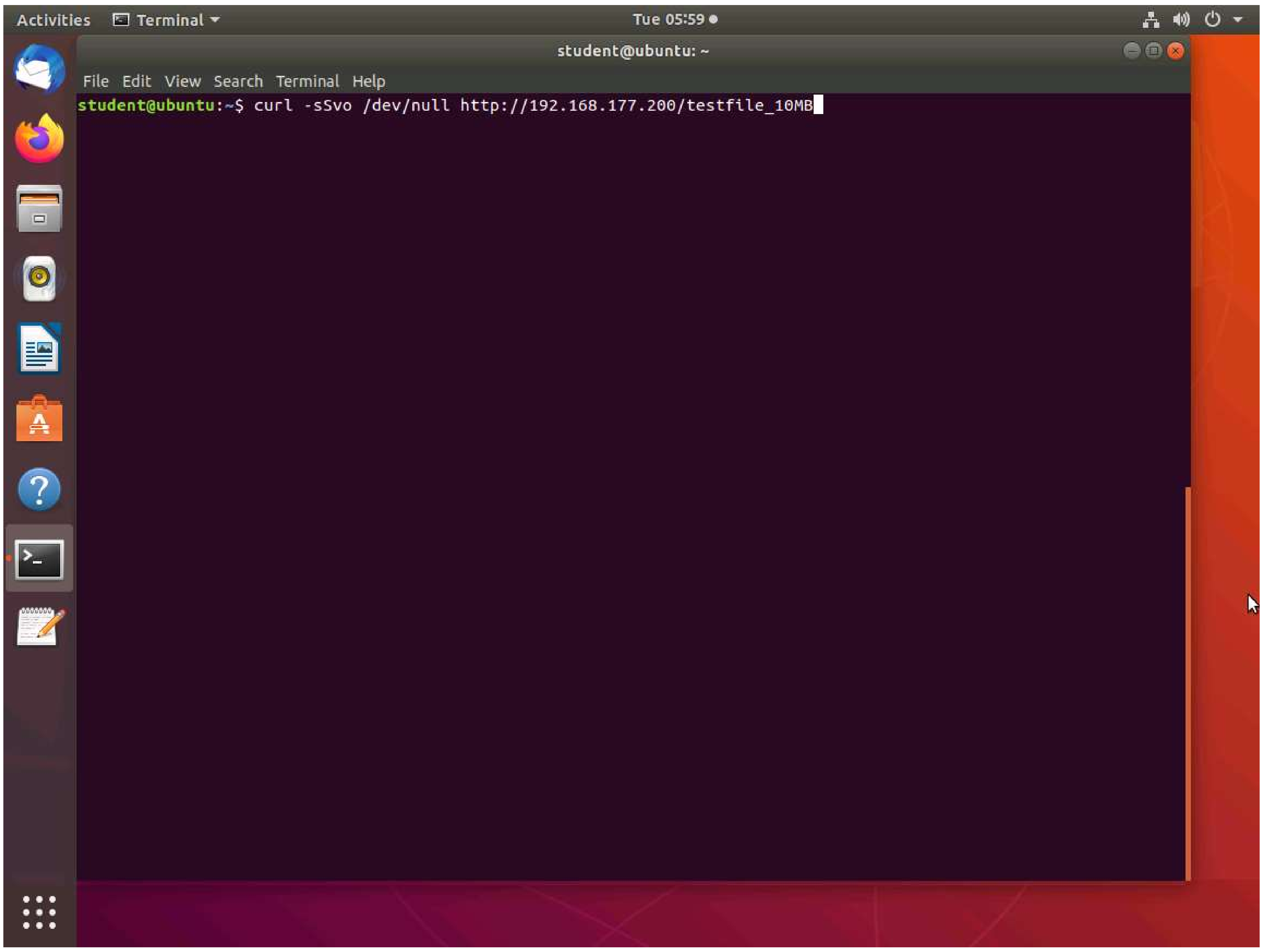
23. If you want to perform the **recon** without seeing the output of errors, you can use the **-s** option. Type **curl -svo /dev/null http://192.168.177.200/testfile_10MB** and press **Enter**.



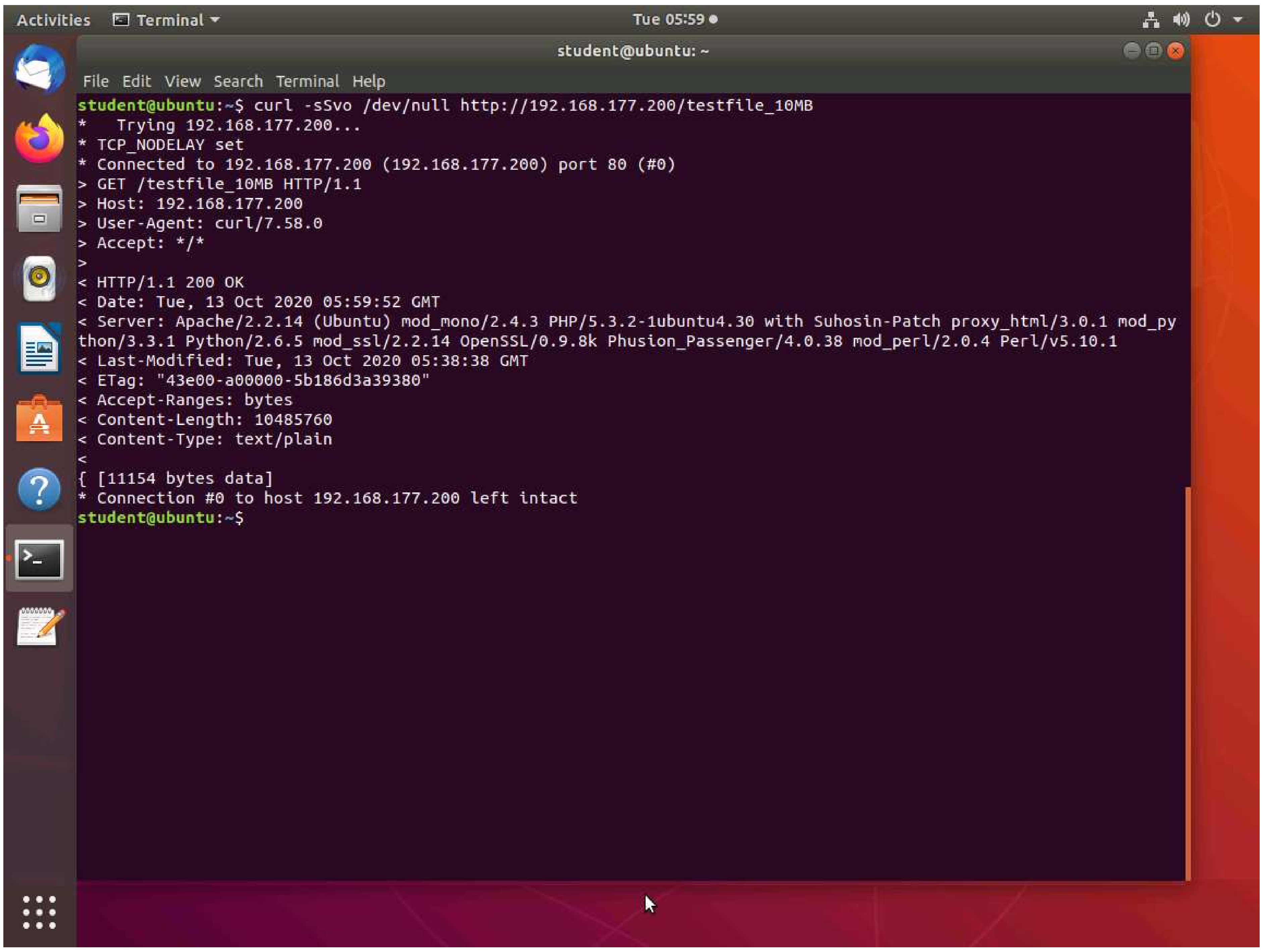
```
student@ubuntu:~$ curl -svo /dev/null http://192.168.177.200/testfile_10MB
*   Trying 192.168.177.200...
* TCP_NODELAY set
* Connected to 192.168.177.200 (192.168.177.200) port 80 (#0)
> GET /testfile_10MB HTTP/1.1
> Host: 192.168.177.200
> User-Agent: curl/7.58.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Tue, 13 Oct 2020 05:58:05 GMT
< Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_py
thon/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
< Last-Modified: Tue, 13 Oct 2020 05:38:38 GMT
< ETag: "43e00-a00000-5b186d3a39380"
< Accept-Ranges: bytes
< Content-Length: 10485760
< Content-Type: text/plain
<
{ [2466 bytes data]
* Connection #0 to host 192.168.177.200 left intact
student@ubuntu:~$
```

24. The **-s** option is slightly aggressive, since it hides even error messages. For your use case, if you want to hide the progress bar but still view any errors, you can combine the **-S** option.

25. Therefore, if you are trying to save the cURL output to a file but simply want to hide the progress bar, you can type **curl -sSvo /dev/null http://192.168.177.200/testfile_10MB** and press **Enter**.



```
student@ubuntu:~$ curl -sSvo /dev/null http://192.168.177.200/testfile_10MB
```

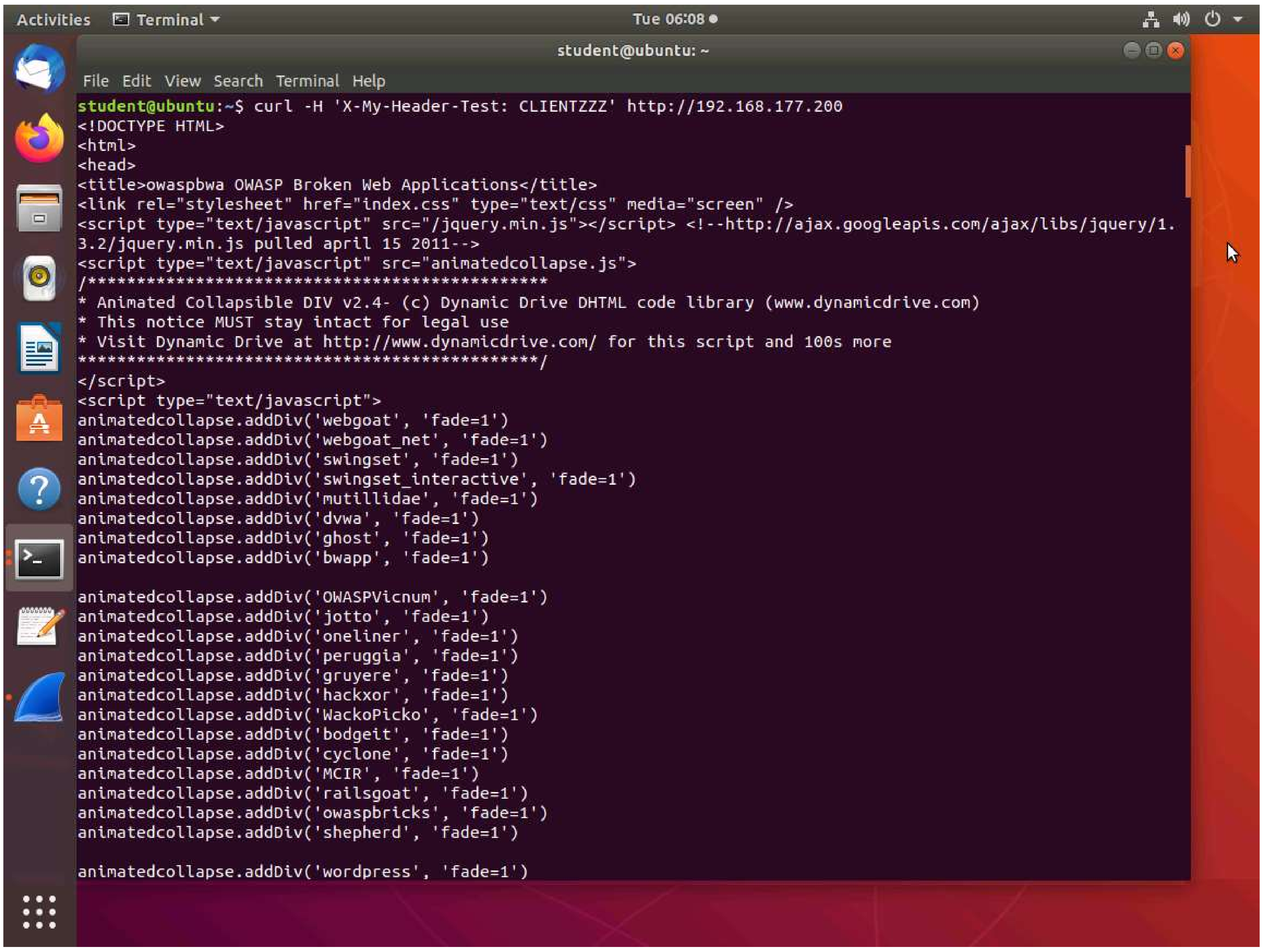


```
student@ubuntu:~$ curl -sSvo /dev/null http://192.168.177.200/testfile_10MB
*   Trying 192.168.177.200...
* TCP_NODELAY set
* Connected to 192.168.177.200 (192.168.177.200) port 80 (#0)
> GET /testfile_10MB HTTP/1.1
> Host: 192.168.177.200
> User-Agent: curl/7.58.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Tue, 13 Oct 2020 05:59:52 GMT
< Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_py
thon/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
< Last-Modified: Tue, 13 Oct 2020 05:38:38 GMT
< ETag: "43e00-a00000-5b186d3a39380"
< Accept-Ranges: bytes
< Content-Length: 10485760
< Content-Type: text/plain
<
{ [11154 bytes data]
* Connection #0 to host 192.168.177.200 left intact
student@ubuntu:~$
```

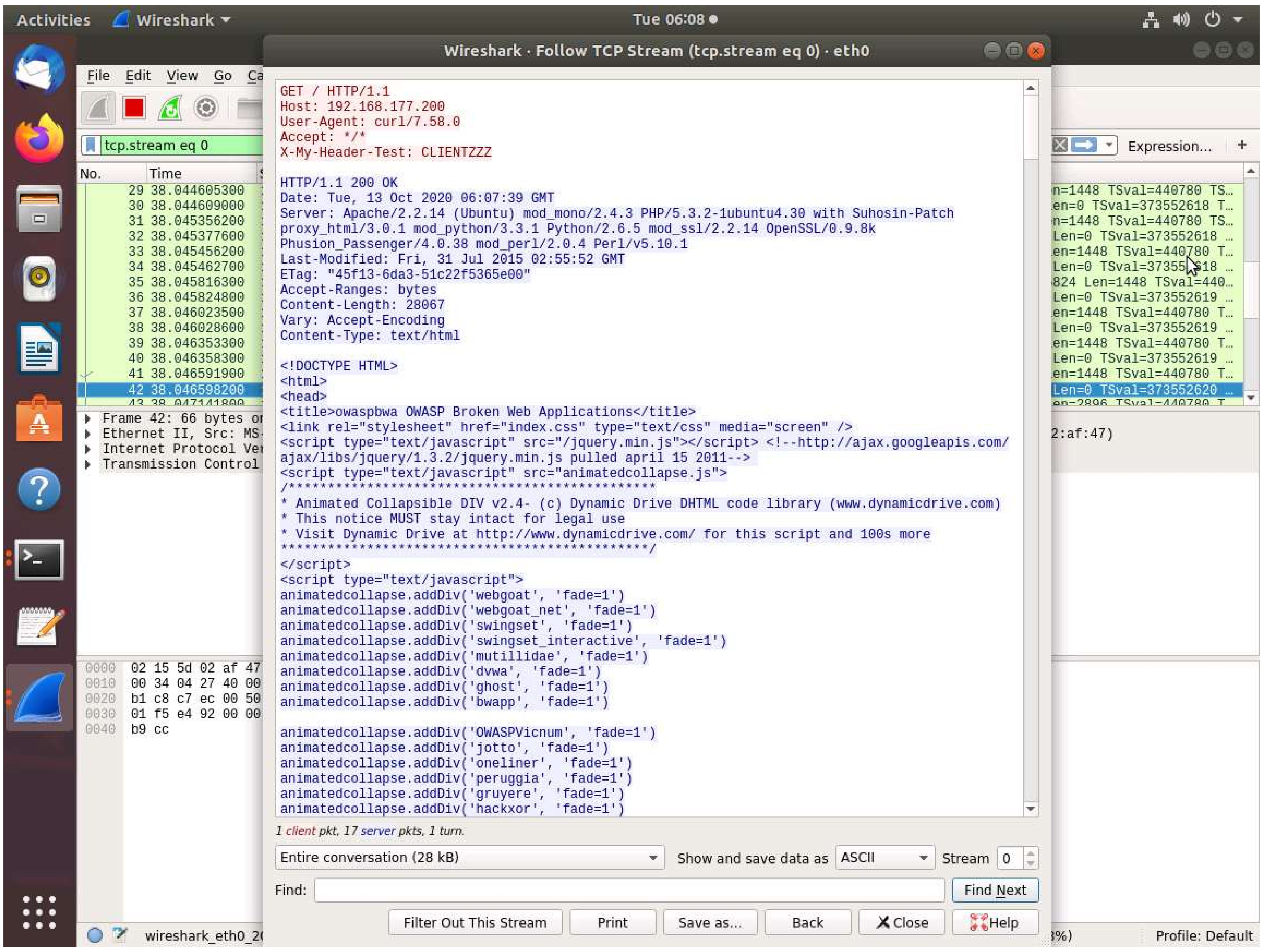
26. Now, we address the fact that the command shows the name curl in the **User-Agent**. When testing APIs, you may need to set custom headers on the HTTP request. You can use the **-H** option of cURL for this purpose. Ensure that you are capturing on Wireshark before entering the next command. If you want to send the custom header X-My-Custom-Header, type **curl -H 'X-My-**

Header-Test: CLIENTZZZ' http://192.168.177.200 and press **Enter**. The output of the command is shown in the following screenshot.

Note: To open **Wireshark - Follow TCP Stream** window, click **Analyze** in the menu bar and navigate to **Follow** --> **TCP Stream**.



```
student@ubuntu:~$ curl -H 'X-My-Header-Test: CLIENTZZZ' http://192.168.177.200
<!DOCTYPE HTML>
<html>
<head>
<title>owaspbwa OWASP Broken Web Applications</title>
<link rel="stylesheet" href="index.css" type="text/css" media="screen" />
<script type="text/javascript" src="/jquery.min.js"></script> <!--http://ajax.googleapis.com/ajax/libs/jquery/1.
3.2/jquery.min.js pulled april 15 2011-->
<script type="text/javascript" src="animatedcollapse.js">
/***********************************************
* Animated Collapsible DIV v2.4- (c) Dynamic Drive DHTML code library (www.dynamicdrive.com)
* This notice MUST stay intact for legal use
* Visit Dynamic Drive at http://www.dynamicdrive.com/ for this script and 100s more
***********************************************/
</script>
<script type="text/javascript">
animatedcollapse.addDiv('webgoat', 'fade=1')
animatedcollapse.addDiv('webgoat_net', 'fade=1')
animatedcollapse.addDiv('swingset', 'fade=1')
animatedcollapse.addDiv('swingset_interactive', 'fade=1')
animatedcollapse.addDiv('mutillidae', 'fade=1')
animatedcollapse.addDiv('dvwa', 'fade=1')
animatedcollapse.addDiv('ghost', 'fade=1')
animatedcollapse.addDiv('bwapp', 'fade=1')

animatedcollapse.addDiv('OWASPVicnum', 'fade=1')
animatedcollapse.addDiv('jotto', 'fade=1')
animatedcollapse.addDiv('oneliner', 'fade=1')
animatedcollapse.addDiv('peruggia', 'fade=1')
animatedcollapse.addDiv('gruyere', 'fade=1')
animatedcollapse.addDiv('hackxor', 'fade=1')
animatedcollapse.addDiv('WackoPicko', 'fade=1')
animatedcollapse.addDiv('bodgeit', 'fade=1')
animatedcollapse.addDiv('cyclone', 'fade=1')
animatedcollapse.addDiv('MCIR', 'fade=1')
animatedcollapse.addDiv('railsgoat', 'fade=1')
animatedcollapse.addDiv('owaspbricks', 'fade=1')
animatedcollapse.addDiv('shepherd', 'fade=1')

animatedcollapse.addDiv('wordpress', 'fade=1')
```



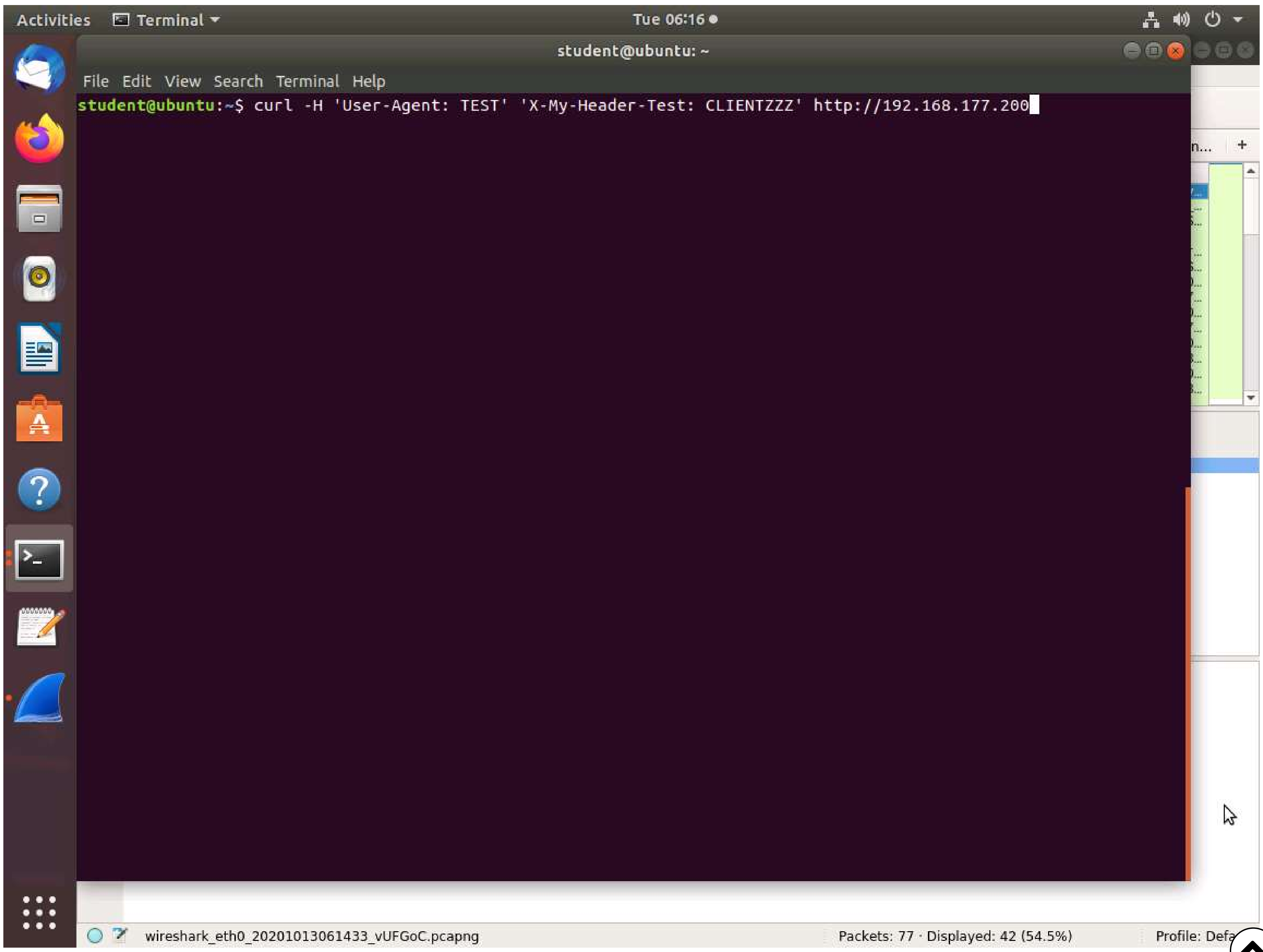
```
GET / HTTP/1.1
Host: 192.168.177.200
User-Agent: curl/7.58.0
Accept: */*
X-My-Header-Test: CLIENTZZZ

HTTP/1.1 200 OK
Date: Tue, 13 Oct 2020 06:07:39 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch
proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k
Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
Last-Modified: Fri, 31 Jul 2015 02:55:52 GMT
ETag: "45f13-6da3-51c22f5365e00"
Accept-Ranges: bytes
Content-Length: 28067
Vary: Accept-Encoding
Content-Type: text/html

<!DOCTYPE HTML>
<html>
<head>
<title>owaspbwa OWASP Broken Web Applications</title>
<link rel="stylesheet" href="index.css" type="text/css" media="screen" />
<script type="text/javascript" src="/jquery.min.js"></script> <!--http://ajax.googleapis.com/
ajax/libs/jquery/1.3.2/jquery.min.js pulled april 15 2011-->
<script type="text/javascript" src="animatedcollapse.js">
/***********************************************
* Animated Collapsible DIV v2.4- (c) Dynamic Drive DHTML code library (www.dynamicdrive.com)
* This notice MUST stay intact for legal use
* Visit Dynamic Drive at http://www.dynamicdrive.com/ for this script and 100s more
***********************************************/
</script>
<script type="text/javascript">
animatedcollapse.addDiv('webgoat', 'fade=1')
animatedcollapse.addDiv('webgoat_net', 'fade=1')
animatedcollapse.addDiv('swingset', 'fade=1')
animatedcollapse.addDiv('swingset_interactive', 'fade=1')
animatedcollapse.addDiv('mutillidae', 'fade=1')
animatedcollapse.addDiv('dvwa', 'fade=1')
animatedcollapse.addDiv('ghost', 'fade=1')
animatedcollapse.addDiv('bwapp', 'fade=1')

animatedcollapse.addDiv('OWASPVicnum', 'fade=1')
animatedcollapse.addDiv('jotto', 'fade=1')
animatedcollapse.addDiv('oneliner', 'fade=1')
animatedcollapse.addDiv('peruggia', 'fade=1')
animatedcollapse.addDiv('gruyere', 'fade=1')
animatedcollapse.addDiv('hackxor', 'fade=1')
```

1 client pkt, 17 server pkts, 1 turn.

Entire conversation (28 kB) · Show and save data as ASCII · Stream 0

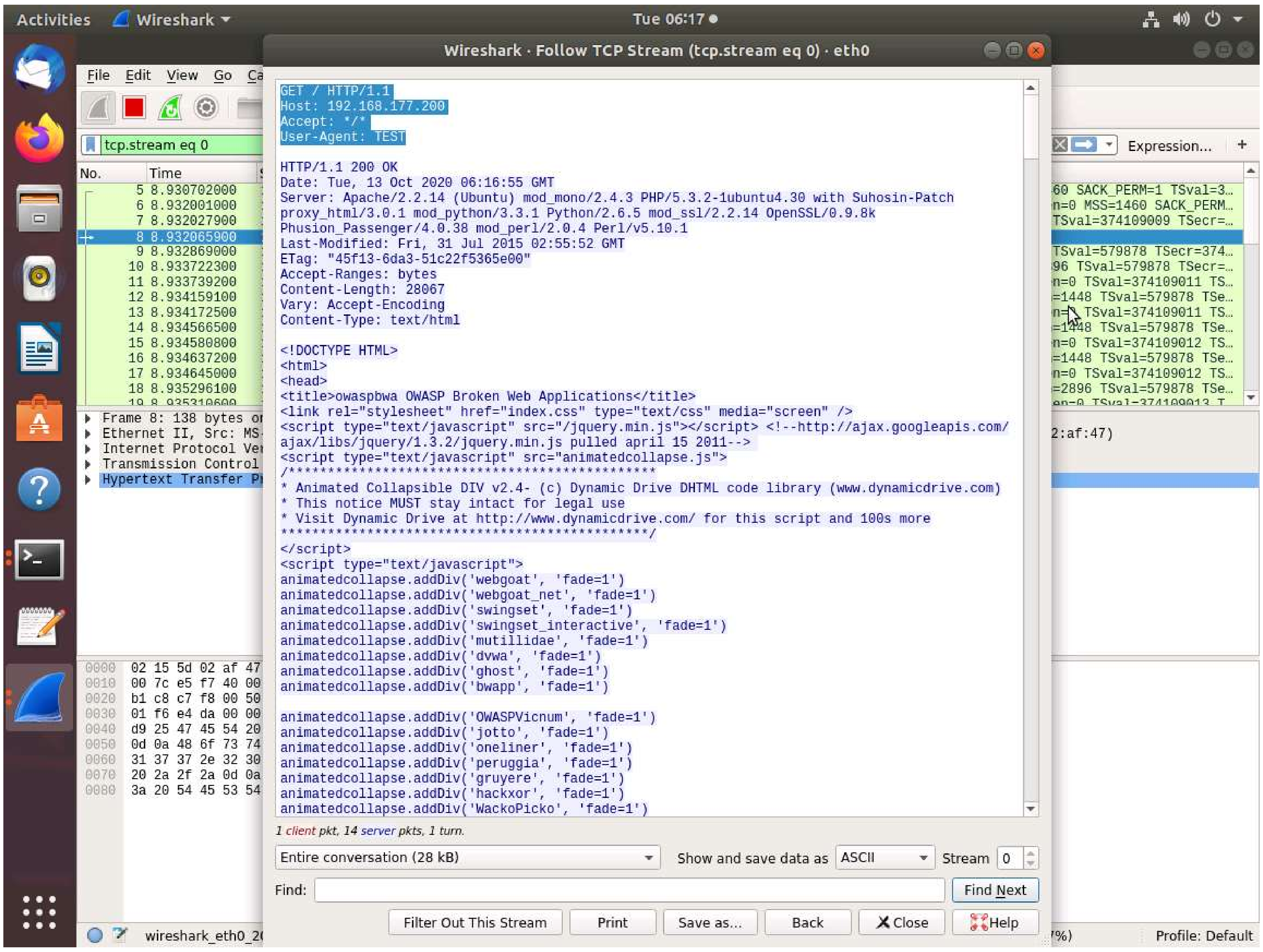
Find:

27. Wait a minute! We have our custom header, but we still have the announcement that we are using curl. This needs to be addressed. Restart the Wireshark capture and then type **curl -H 'User-Agent: TEST' 'X-My-Header-Test: CLIENTZZZ' http://192.168.177.200** and press **Enter**.



```
student@ubuntu:~$ curl -H 'User-Agent: TEST' 'X-My-Header-Test: CLIENTZZZ' http://192.168.177.200
```

wireshark_eth0_20201013061433_vUFGoC.pcapng · Packets: 77 · Displayed: 42 (54.5%) · Profile: Default

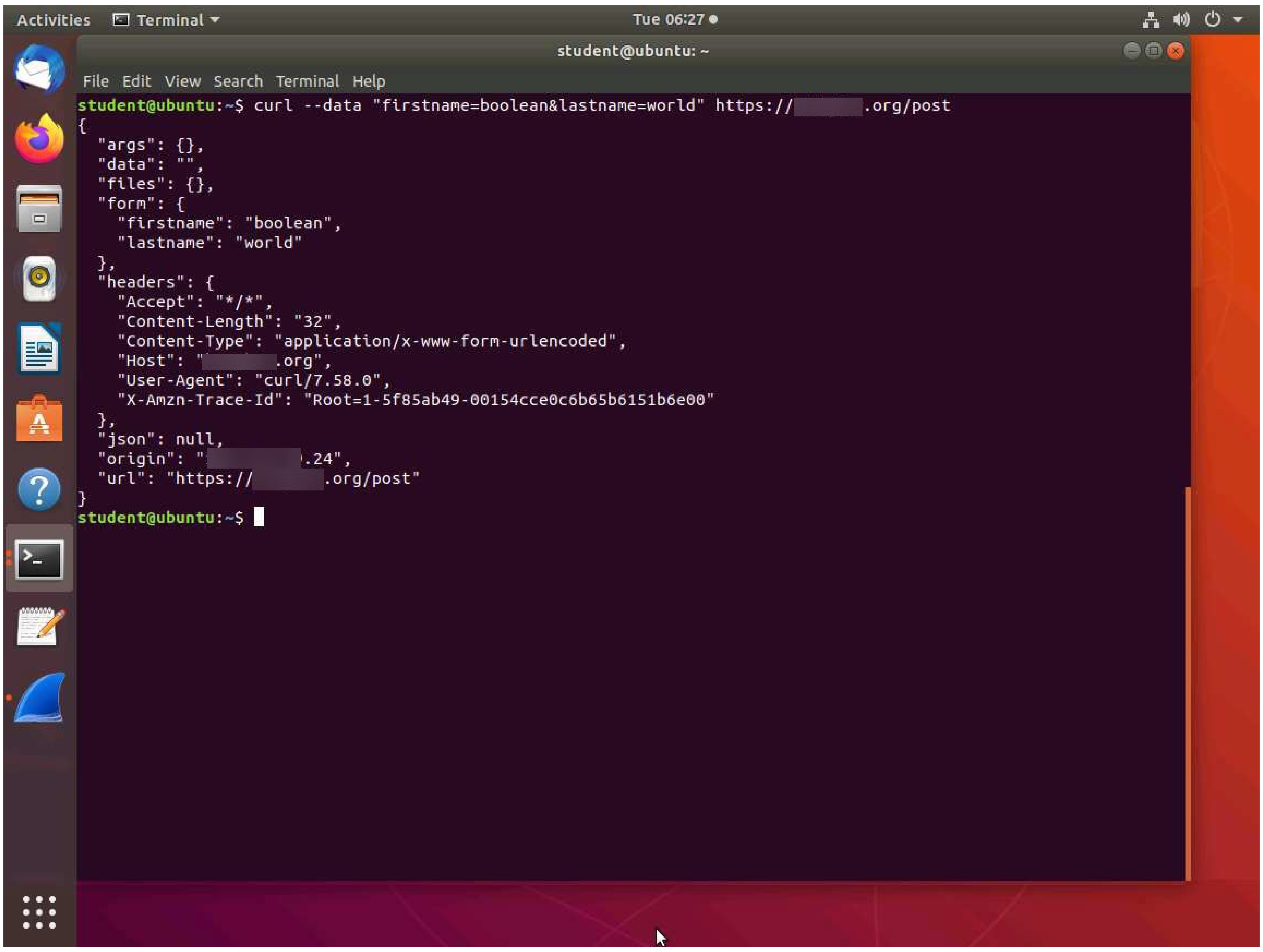

Wireshark · Follow TCP Stream (tcp.stream eq 0) · eth0
Entire conversation (28 kB)
Show and save data as ASCII
Stream 0
Find:
Find Next
Filter Out This Stream
Print
Save as…
Back
Close
Help

```
GET / HTTP/1.1
Host: 192.168.177.200
Accept: */*
User-Agent: TEST

HTTP/1.1 200 OK
Date: Tue, 13 Oct 2020 06:16:55 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch
proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k
Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
Last-Modified: Fri, 31 Jul 2015 02:55:52 GMT
ETag: "45f13-6da3-51c22f5365e00"
Accept-Ranges: bytes
Content-Length: 28067
Vary: Accept-Encoding
Content-Type: text/html

<!DOCTYPE HTML>
<html>
<head>
<title>owaspbwa OWASP Broken Web Applications</title>
<link rel="stylesheet" href="index.css" type="text/css" media="screen" />
<script type="text/javascript" src="/jquery.min.js"></script> <!--http://ajax.googleapis.com/
ajax/libs/jquery/1.3.2/jquery.min.js pulled april 15 2011-->
<script type="text/javascript" src="animatedcollapse.js">
/***********************************************
* Animated Collapsible DIV v2.4- (c) Dynamic Drive DHTML code library (www.dynamicdrive.com)
* This notice MUST stay intact for legal use
* Visit Dynamic Drive at http://www.dynamicdrive.com/ for this script and 100s more
***********************************************/
</script>
<script type="text/javascript">
animatedcollapse.addDiv('webgoat', 'fade=1')
animatedcollapse.addDiv('webgoat_net', 'fade=1')
animatedcollapse.addDiv('swingset', 'fade=1')
animatedcollapse.addDiv('swingset_interactive', 'fade=1')
animatedcollapse.addDiv('mutillidae', 'fade=1')
animatedcollapse.addDiv('dvwa', 'fade=1')
animatedcollapse.addDiv('ghost', 'fade=1')
animatedcollapse.addDiv('bwapp', 'fade=1')

animatedcollapse.addDiv('OWASPVicnum', 'fade=1')
animatedcollapse.addDiv('jotto', 'fade=1')
animatedcollapse.addDiv('oneliner', 'fade=1')
animatedcollapse.addDiv('peruggia', 'fade=1')
animatedcollapse.addDiv('gruyere', 'fade=1')
animatedcollapse.addDiv('hackxor', 'fade=1')
animatedcollapse.addDiv('WackoPicko', 'fade=1')
```

1 client pkt, 14 server pkts, 1 turn.

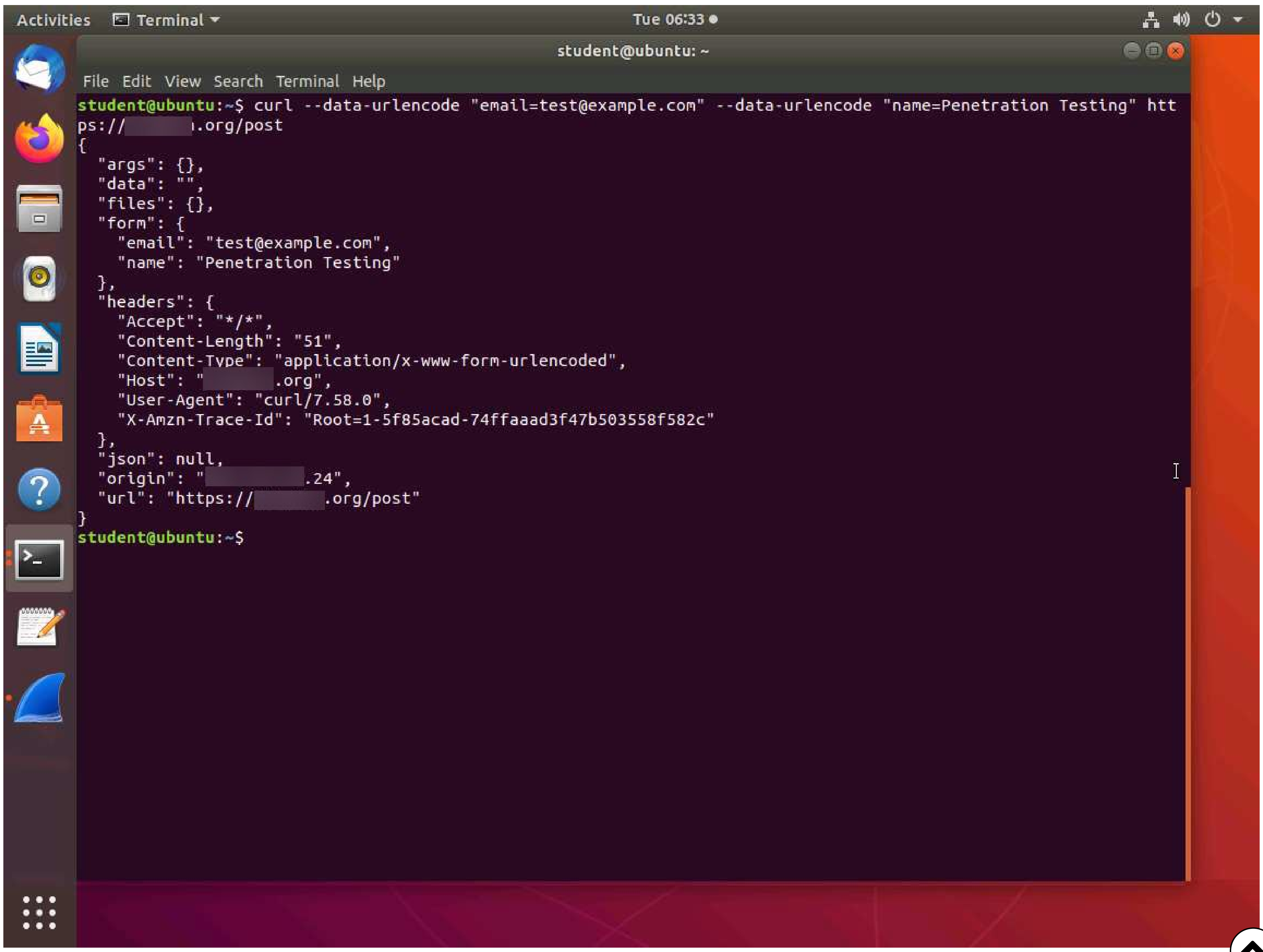
28. As you can see, we have now successfully obfuscated our client connection. You can do a lot more and are encouraged to explore. By default, cURL sends **GET requests**, but it can also be used to send **POST requests** with the **-d** or **--data** option. All fields must be given as key=value pairs separated by the ampersand (&) character. Type **curl --data "firstname=boolean&lastname=world" https://httpbin.org/post** and press **Enter**.

29. The output clearly indicates that we have posted two parameters that are identified with the form data.



```
student@ubuntu:~$ curl --data "firstname=boolean&lastname=world" https://[redacted].org/post
{
  "args": {},
  "data": "",
  "files": {},
  "form": {
    "firstname": "boolean",
    "lastname": "world"
  },
  "headers": {
    "Accept": "*/*",
    "Content-Length": "32",
    "Content-Type": "application/x-www-form-urlencoded",
    "Host": "[redacted].org",
    "User-Agent": "curl/7.58.0",
    "X-Amzn-Trace-Id": "Root=1-5f85ab49-00154cce0c6b65b6151b6e00"
  },
  "json": null,
  "origin": "[redacted].24",
  "url": "https://[redacted].org/post"
}
student@ubuntu:~$
```

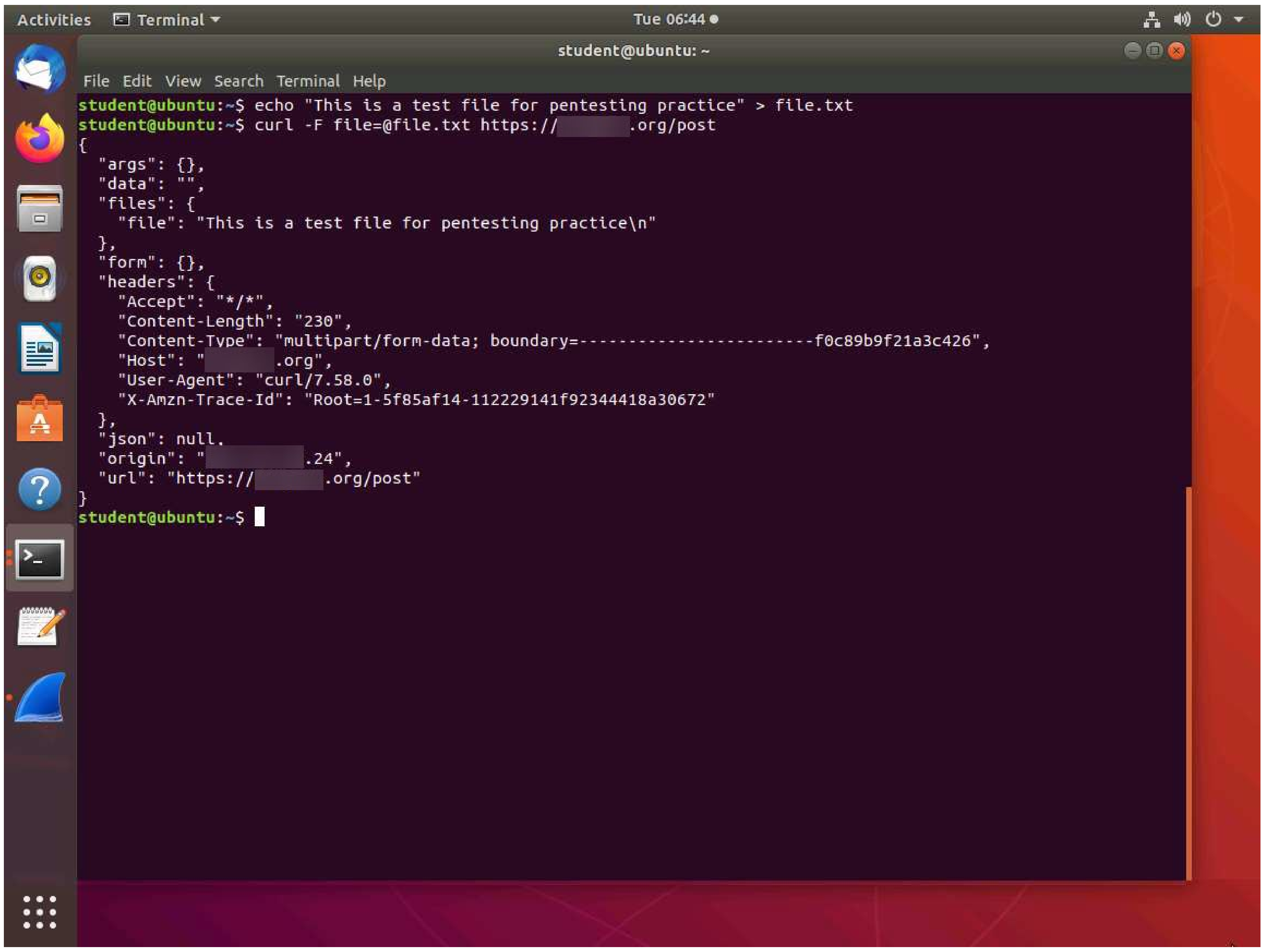
30. As a refresher, characters that are considered special characters must be encoded. This can be done manually, but it is easier to use the cURL tool. Now, type **curl --data-urlencode "email=test@example.com" --data-urlencode "name=Penetration Testing" https://httpbin.org/post** and press **Enter**.



```
student@ubuntu:~$ curl --data-urlencode "email=test@example.com" --data-urlencode "name=Penetration Testing" htt
ps://[redacted].org/post
{
  "args": {},
  "data": "",
  "files": {},
  "form": {
    "email": "test@example.com",
    "name": "Penetration Testing"
  },
  "headers": {
    "Accept": "*/*",
    "Content-Length": "51",
    "Content-Type": "application/x-www-form-urlencoded",
    "Host": "[redacted].org",
    "User-Agent": "curl/7.58.0",
    "X-Amzn-Trace-Id": "Root=1-5f85acad-74ffaaad3f47b503558f582c"
  },
  "json": null,
  "origin": "[redacted].24",
  "url": "https://[redacted].org/post"
}
student@ubuntu:~$
```

31. If you want to upload files using a POST request, you can use the **-F** ("form") option. Here, we will submit the file.txt under the parameter name file.

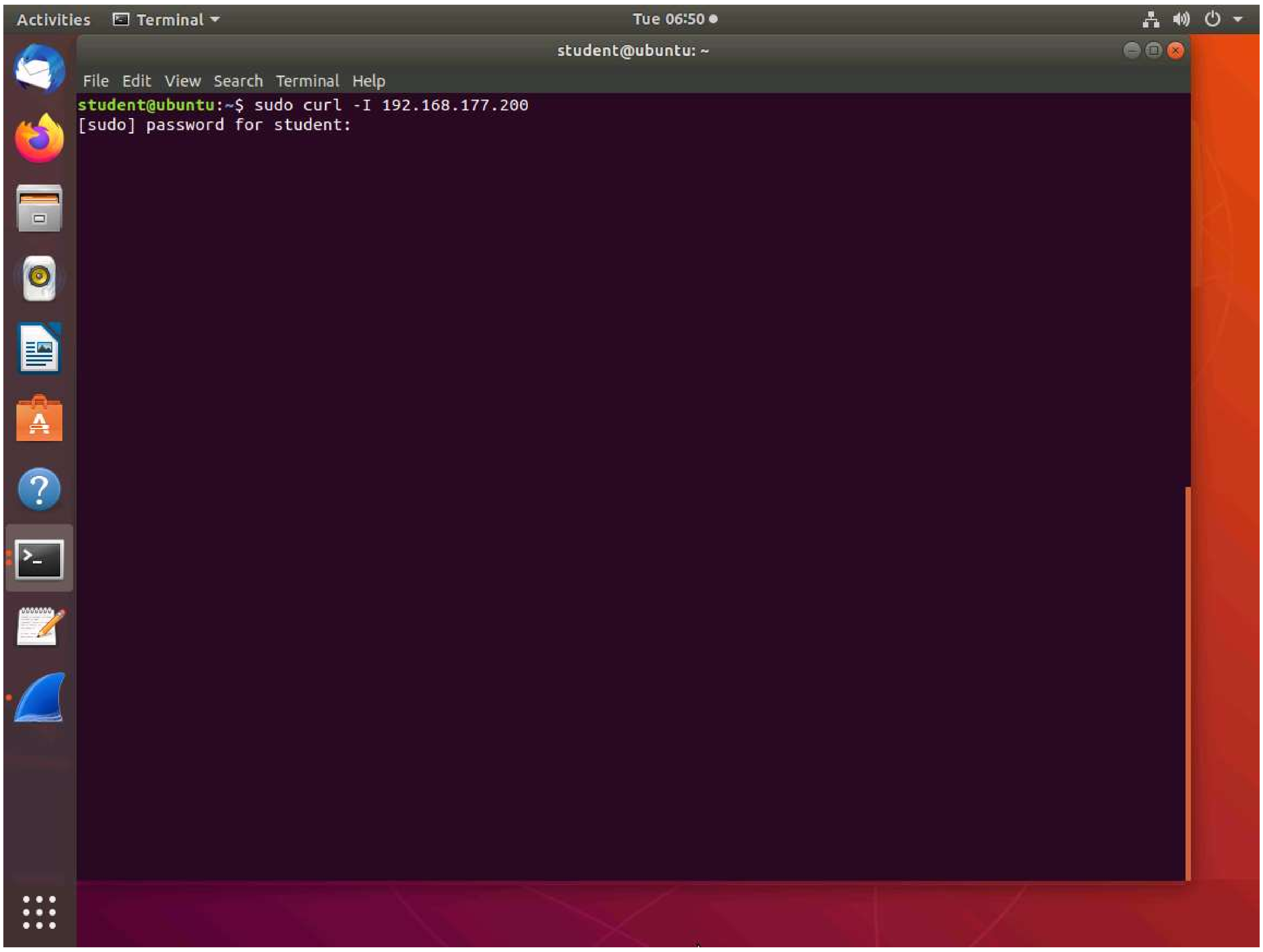
   - Type **echo "This is a test file for pentesting practice" > file.txt** and press **Enter**.
   - Type **curl -F file=@file.txt https://httpbin.org/post** and press **Enter**.



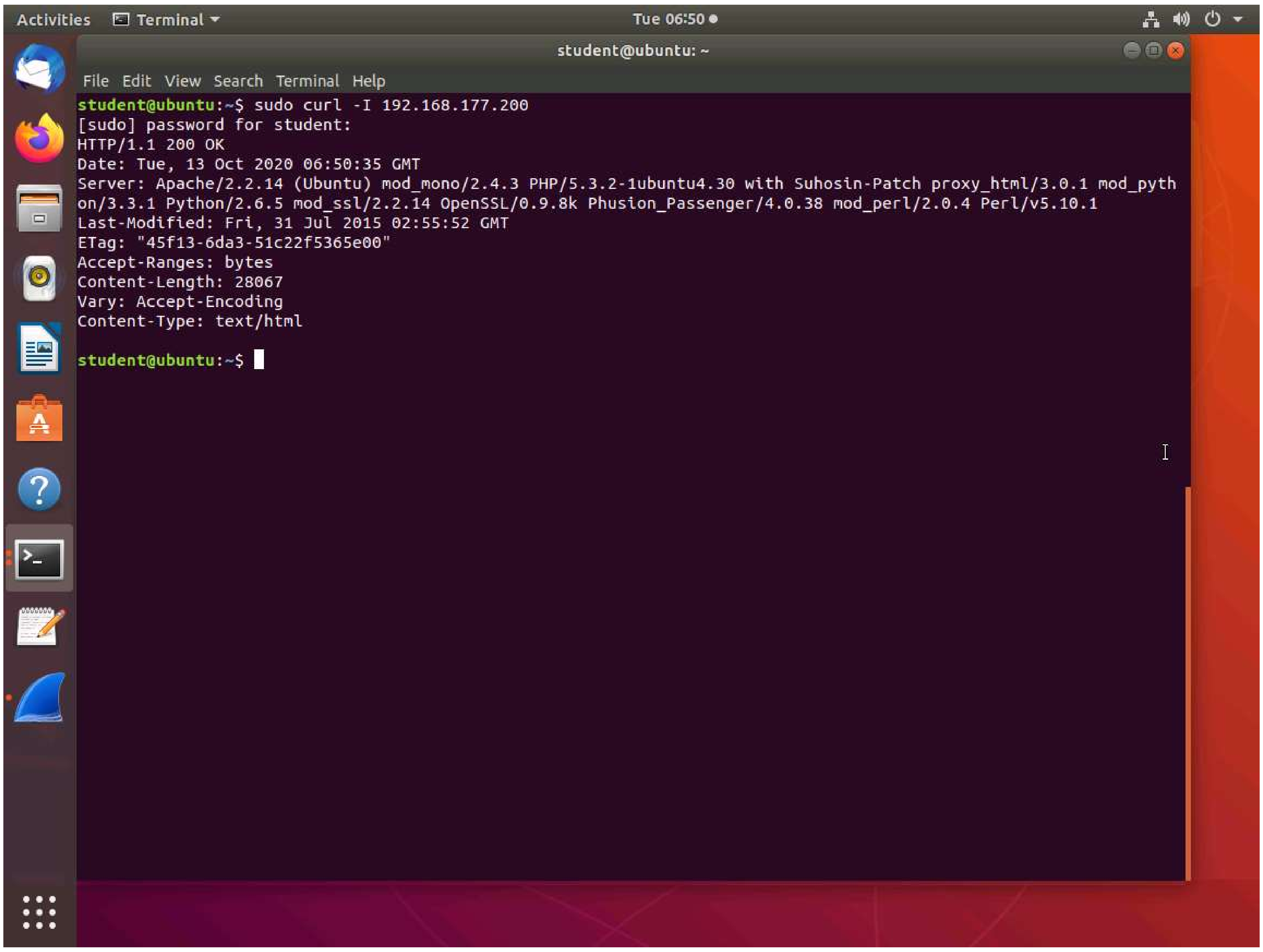
```
student@ubuntu:~$ echo "This is a test file for pentesting practice" > file.txt
student@ubuntu:~$ curl -F file=@file.txt https://[redacted].org/post
{
  "args": {},
  "data": "",
  "files": {
    "file": "This is a test file for pentesting practice\n"
  },
  "form": {},
  "headers": {
    "Accept": "*/*",
    "Content-Length": "230",
    "Content-Type": "multipart/form-data; boundary=------------------------f0c89b9f21a3c426",
    "Host": "[redacted].org",
    "User-Agent": "curl/7.58.0",
    "X-Amzn-Trace-Id": "Root=1-5f85af14-112229141f92344418a30672"
  },
  "json": null,
  "origin": "[redacted].24",
  "url": "https://[redacted].org/post"
}
student@ubuntu:~$ 
```

32. Previously, we have seen how to send POST requests with cURL. Sometimes, you may need to send a POST request with no data at all. In that case, simply change the request method to POST with the -X option.

33. The request method can also be changed to anything else such as **PUT**, **DELETE** or **PATCH**. One notable exception is the HEAD method, which cannot be set with the -X option. The HEAD method is used to check if a document is present on the server, but without downloading the document. To use the HEAD method, we use the **-I** option. Type **sudo curl -I 192.168.177.200** and press **Enter**. Type **password** and press **Enter**.



```
student@ubuntu:~$ sudo curl -I 192.168.177.200
[sudo] password for student:
```

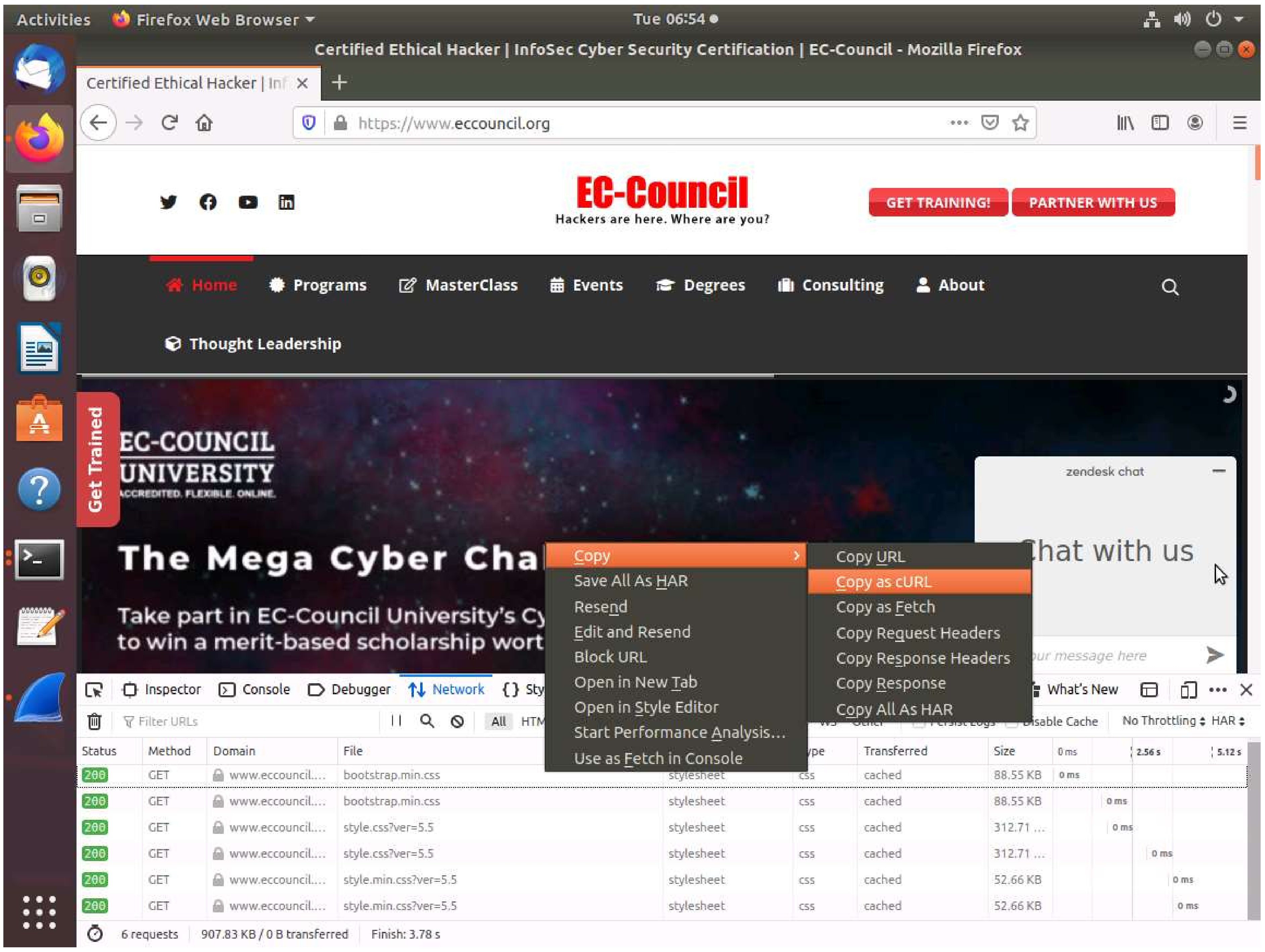


```
student@ubuntu:~$ sudo curl -I 192.168.177.200
[sudo] password for student:
HTTP/1.1 200 OK
Date: Tue, 13 Oct 2020 06:50:35 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_pyth
on/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
Last-Modified: Fri, 31 Jul 2015 02:55:52 GMT
ETag: "45f13-6da3-51c22f5365e00"
Accept-Ranges: bytes
Content-Length: 28067
Vary: Accept-Encoding
Content-Type: text/html

student@ubuntu:~$
```

34. As the above screenshot shows, we have only returned the header. Using the **HEAD** method has been demonstrated.

35. We can also access the **Firefox** developer tools. Launch Firefox browser and open any web site. Press **F12** to open the developer tools, and then click on the **Network** Tab. Select a **GET** request. Right-click on this to bring up another menu.

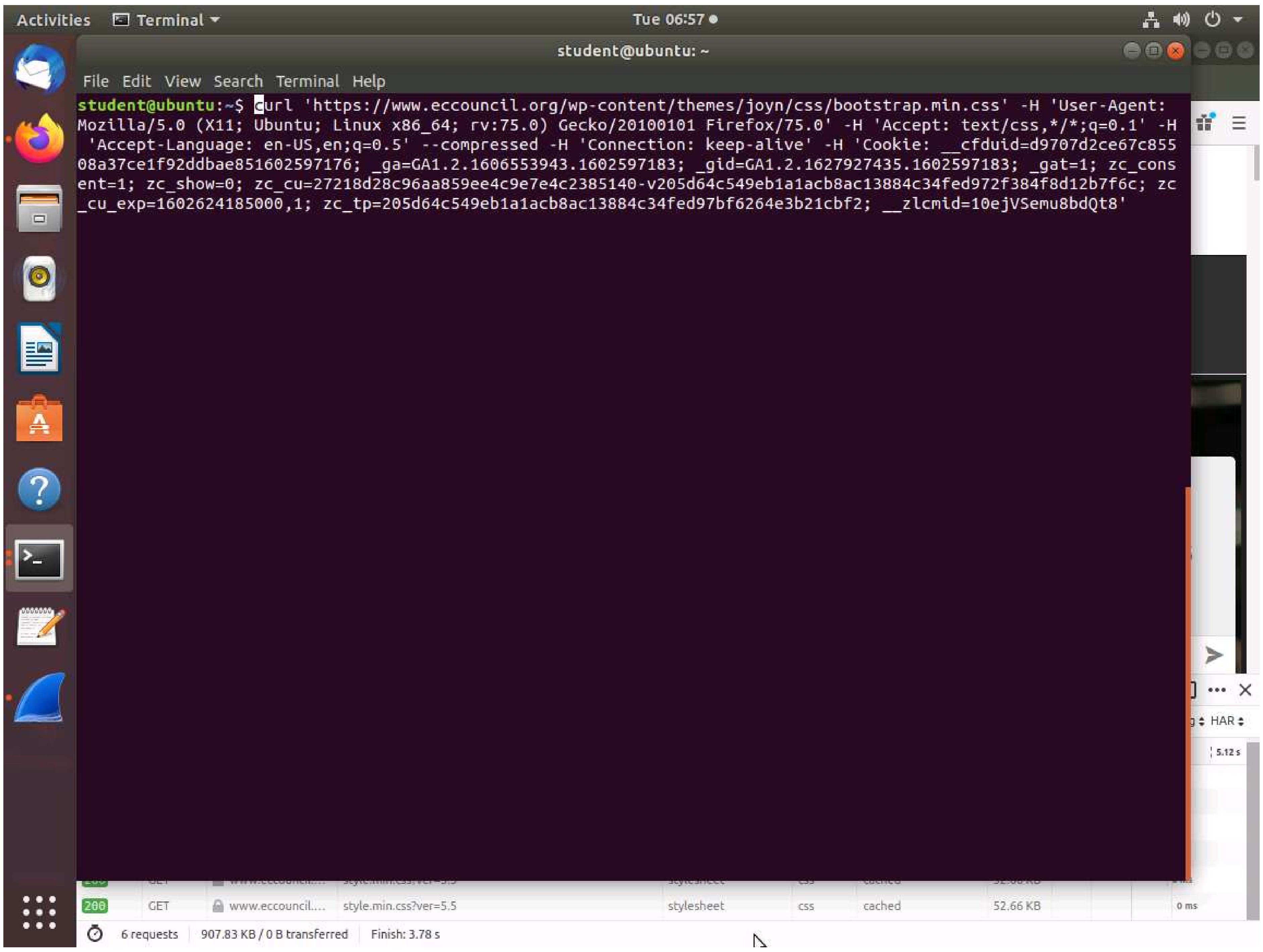
36. Click **Copy as cURL**. We have the option to copy for both Windows and POSIX, select the appropriate one, and then paste it.



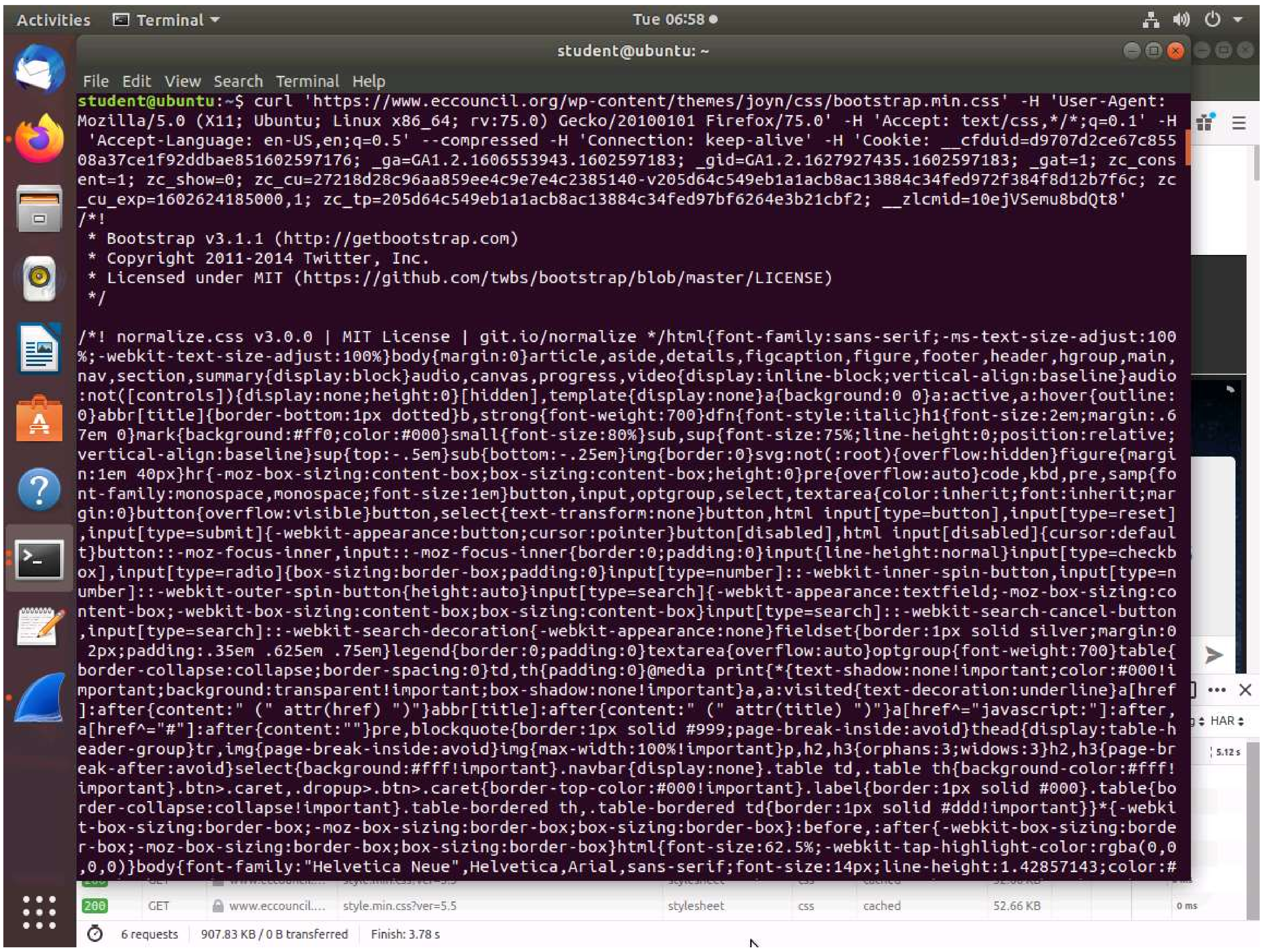
Status	Method	Domain	File	Type		Transferred	Size
200	GET	www.eccouncil.…	bootstrap.min.css	stylesheet	css	cached	88.55 KB
200	GET	www.eccouncil.…	bootstrap.min.css	stylesheet	css	cached	88.55 KB
200	GET	www.eccouncil.…	style.css?ver=5.5	stylesheet	css	cached	312.71 …
200	GET	www.eccouncil.…	style.css?ver=5.5	stylesheet	css	cached	312.71 …
200	GET	www.eccouncil.…	style.min.css?ver=5.5	stylesheet	css	cached	52.66 KB
200	GET	www.eccouncil.…	style.min.css?ver=5.5	stylesheet	css	cached	52.66 KB

6 requests | 907.83 KB / 0 B transferred | Finish: 3.78 s

37. Switch to cURL terminal and paste the copied cURL in the terminal and press **Enter**. You can try this by connecting to any web server machine.

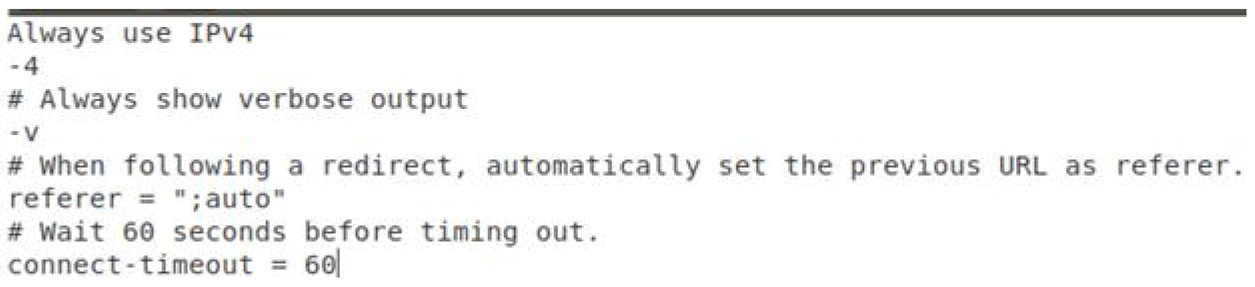


```
student@ubuntu:~$ curl 'https://www.eccouncil.org/wp-content/themes/joyn/css/bootstrap.min.css' -H 'User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0' -H 'Accept: text/css,*/*;q=0.1' -H 'Accept-Language: en-US,en;q=0.5' --compressed -H 'Connection: keep-alive' -H 'Cookie: __cfduid=d9707d2ce67c85508a37ce1f92ddbae851602597176; _ga=GA1.2.1606553943.1602597183; _gid=GA1.2.1627927435.1602597183; _gat=1; zc_consent=1; zc_show=0; zc_cu=27218d28c96aa859ee4c9e7e4c2385140-v205d64c549eb1a1acb8ac13884c34fed972f384f8d12b7f6c; zc_cu_exp=1602624185000,1; zc_tp=205d64c549eb1a1acb8ac13884c34fed97bf6264e3b21cbf2; __zlcmid=10ejVSemu8bdQt8'
```



```
student@ubuntu:~$ curl 'https://www.eccouncil.org/wp-content/themes/joyn/css/bootstrap.min.css' -H 'User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0' -H 'Accept: text/css,*/*;q=0.1' -H 'Accept-Language: en-US,en;q=0.5' --compressed -H 'Connection: keep-alive' -H 'Cookie: __cfduid=d9707d2ce67c85508a37ce1f92ddbae851602597176; _ga=GA1.2.1606553943.1602597183; _gid=GA1.2.1627927435.1602597183; _gat=1; zc_consent=1; zc_show=0; zc_cu=27218d28c96aa859ee4c9e7e4c2385140-v205d64c549eb1a1acb8ac13884c34fed972f384f8d12b7f6c; zc_cu_exp=1602624185000,1; zc_tp=205d64c549eb1a1acb8ac13884c34fed97bf6264e3b21cbf2; __zlcmid=10ejVSemu8bdQt8'
/*!
 * Bootstrap v3.1.1 (http://getbootstrap.com)
 * Copyright 2011-2014 Twitter, Inc.
 * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE)
 */

/*! normalize.css v3.0.0 | MIT License | git.io/normalize */html{font-family:sans-serif;-ms-text-size-adjust:100%;-webkit-text-size-adjust:100%}body{margin:0}article,aside,details,figcaption,figure,footer,header,hgroup,main,nav,section,summary{display:block}audio,canvas,progress,video{display:inline-block;vertical-align:baseline}audio:not([controls]){display:none;height:0}[hidden],template{display:none}a{background:0 0}a:active,a:hover{outline:0}abbr[title]{border-bottom:1px dotted}b,strong{font-weight:700}dfn{font-style:italic}h1{font-size:2em;margin:.67em 0}mark{background:#ff0;color:#000}small{font-size:80%}sub,sup{font-size:75%;line-height:0;position:relative;vertical-align:baseline}sup{top:-.5em}sub{bottom:-.25em}img{border:0}svg:not(:root){overflow:hidden}figure{margin:1em 40px}hr{-moz-box-sizing:content-box;box-sizing:content-box;height:0}pre{overflow:auto}code,kbd,pre,samp{font-family:monospace,monospace;font-size:1em}button,input,optgroup,select,textarea{color:inherit;font:inherit;margin:0}button{overflow:visible}button,select{text-transform:none}button,html input[type=button],input[type=reset],input[type=submit]{-webkit-appearance:button;cursor:pointer}button[disabled],html input[disabled]{cursor:default}button::-moz-focus-inner,input::-moz-focus-inner{border:0;padding:0}input{line-height:normal}input[type=checkbox],input[type=radio]{box-sizing:border-box;padding:0}input[type=number]::-webkit-inner-spin-button,input[type=number]::-webkit-outer-spin-button{height:auto}input[type=search]{-webkit-appearance:textfield;-moz-box-sizing:content-box;-webkit-box-sizing:content-box;box-sizing:content-box}input[type=search]::-webkit-search-cancel-button,input[type=search]::-webkit-search-decoration{-webkit-appearance:none}fieldset{border:1px solid silver;margin:0 2px;padding:.35em .625em .75em}legend{border:0;padding:0}textarea{overflow:auto}optgroup{font-weight:700}table{border-collapse:collapse;border-spacing:0}td,th{padding:0}@media print{*{text-shadow:none!important;color:#000!important;background:transparent!important;box-shadow:none!important}a,a:visited{text-decoration:underline}a[href]:after{content:" (" attr(href) ")"}abbr[title]:after{content:" (" attr(title) ")"}a[href^="javascript:"]:after,a[href^="#"]:after{content:""}pre,blockquote{border:1px solid #999;page-break-inside:avoid}thead{display:table-header-group}tr,img{page-break-inside:avoid}img{max-width:100%!important}p,h2,h3{orphans:3;widows:3}h2,h3{page-break-after:avoid}select{background:#fff!important}.navbar{display:none}.table td,.table th{background-color:#fff!important}.btn>.caret,.dropup>.btn>.caret{border-top-color:#000!important}.label{border:1px solid #000}.table{border-collapse:collapse!important}.table-bordered th,.table-bordered td{border:1px solid #ddd!important}}*{-webkit-box-sizing:border-box;-moz-box-sizing:border-box;box-sizing:border-box}:before,:after{-webkit-box-sizing:border-box;-moz-box-sizing:border-box;box-sizing:border-box}html{font-size:62.5%;-webkit-tap-highlight-color:rgba(0,0,0,0)}body{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;font-size:14px;line-height:1.42857143;color:#
```

38. Sometimes, you may wish to ensure that all cURL requests use the same options. Passing these options manually is not a feasible solution. Therefore, cURL allows you to specify options in a configuration file. The default configuration file is located in **~/.curlrc** in **Linux/MacOS**. An example of a configuration file is shown in the following screenshot.



```
Always use IPv4
-4
# Always show verbose output
-v
# When following a redirect, automatically set the previous URL as referer.
referer = ";auto"
# Wait 60 seconds before timing out.
connect-timeout = 60
```

39. If you want to use a custom configuration file instead of the default one, then you can use -K option to point curl to your configuration file. To learn more about the tool, enter man curl. Take a few minutes to read about the tool.

40. We have shown multiple ways to use the tool, and there are many more. The lab objectives have been achieved.

Exercise 3: Log Analysis with BASH

Objectives

- Create BASH queries, extract data from log files, and modify log data

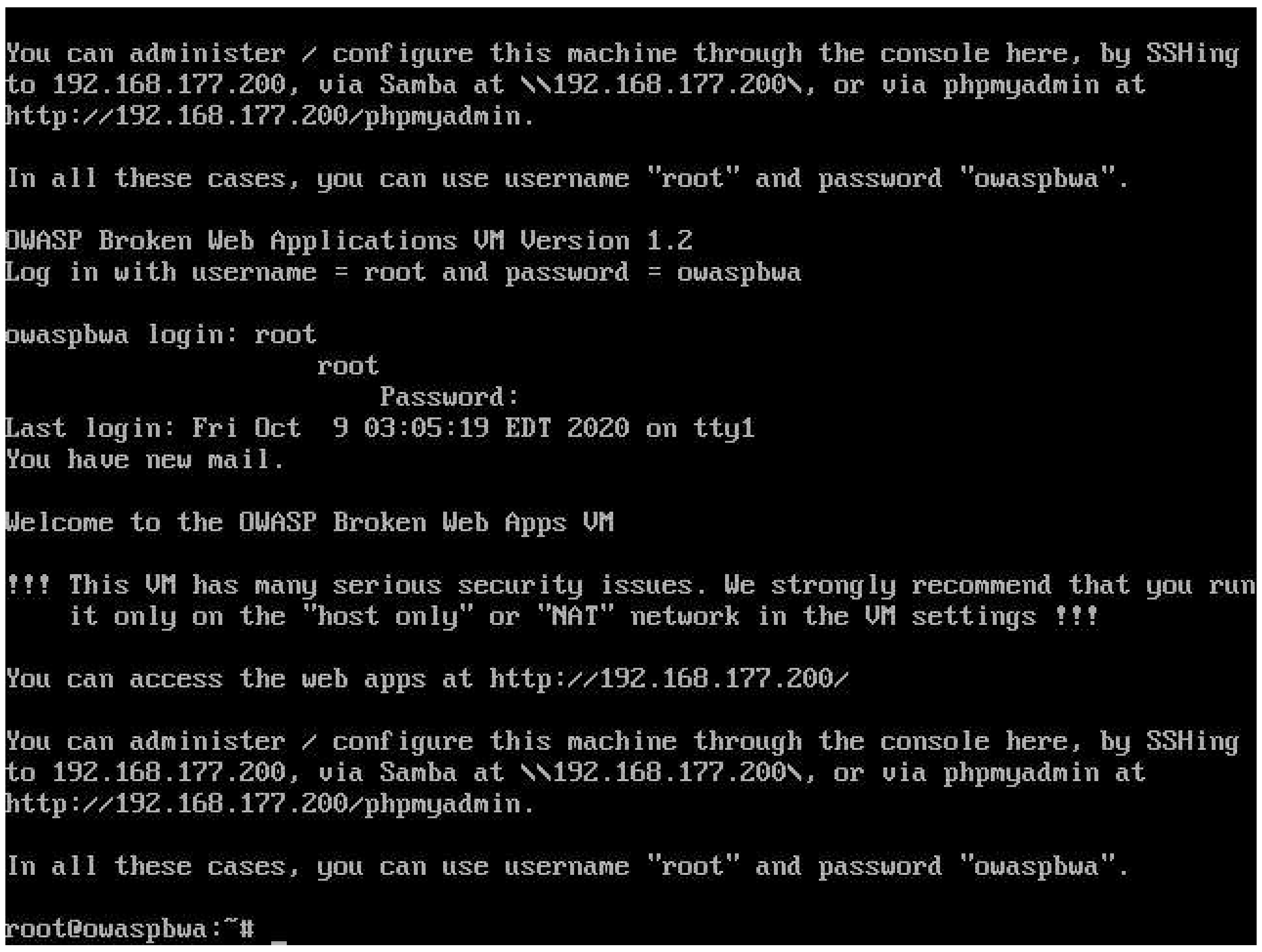
Lab Duration: **20** Minutes

1. In this exercise, we will review the different methods of extracting data from log files using different BASH methods.

2. By default **CPENT Bash Machine** machine selected, click **Target_CPENT Bash-Web** to switch.

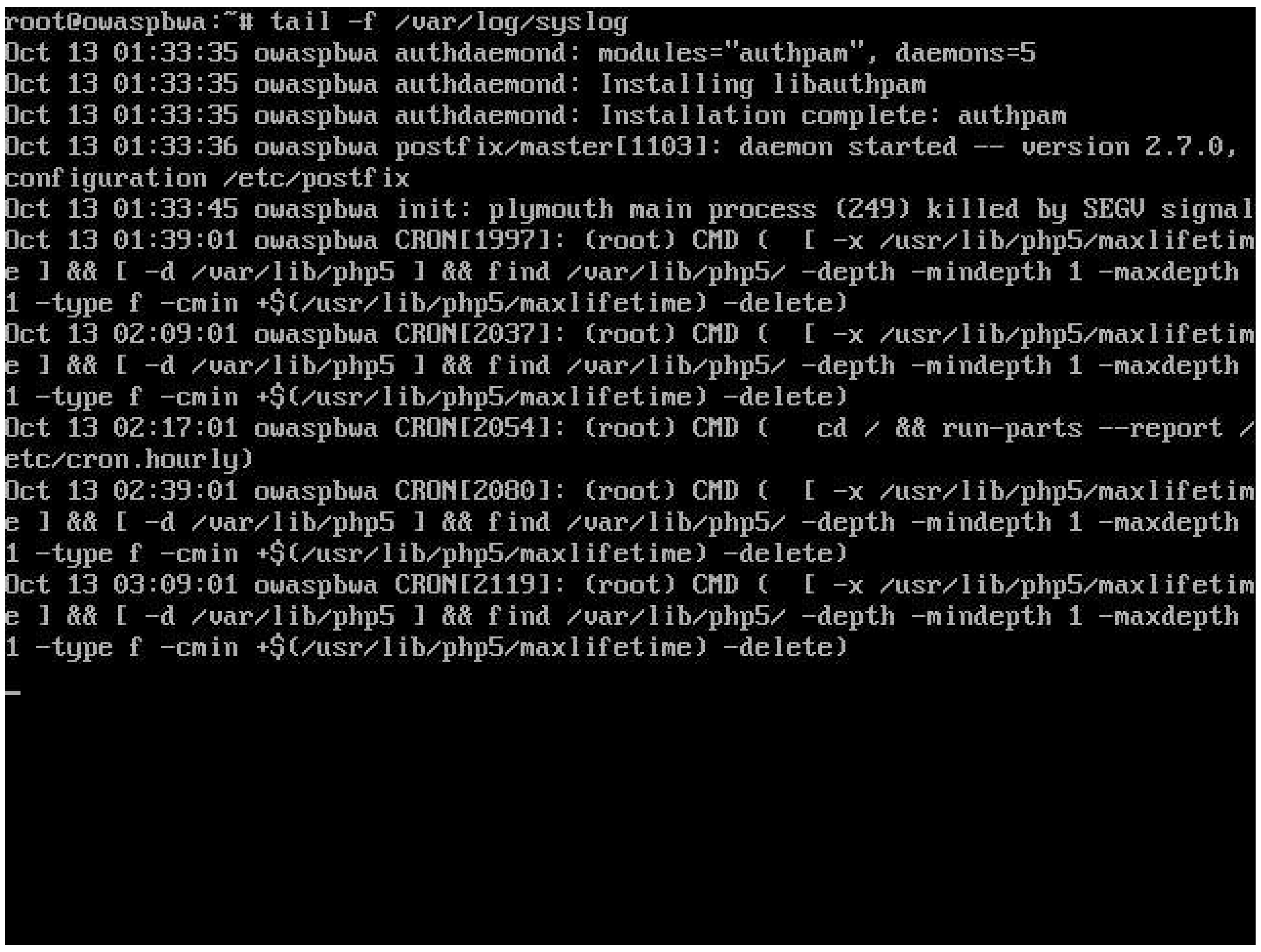
   Note: If you are already logged in skip to step **4**.

3. Login to the machine with the username as **root** and password as **owaspbwa**.



```
You can administer / configure this machine through the console here, by SSHing
to 192.168.177.200, via Samba at \\192.168.177.200\, or via phpmyadmin at
http://192.168.177.200/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

OWASP Broken Web Applications VM Version 1.2
Log in with username = root and password = owaspbwa

owaspbwa login: root
                   root
                       Password:
Last login: Fri Oct  9 03:05:19 EDT 2020 on tty1
You have new mail.

Welcome to the OWASP Broken Web Apps VM

!!! This VM has many serious security issues. We strongly recommend that you run
    it only on the "host only" or "NAT" network in the VM settings !!!

You can access the web apps at http://192.168.177.200/

You can administer / configure this machine through the console here, by SSHing
to 192.168.177.200, via Samba at \\192.168.177.200\, or via phpmyadmin at
http://192.168.177.200/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

root@owaspbwa:~# _
```

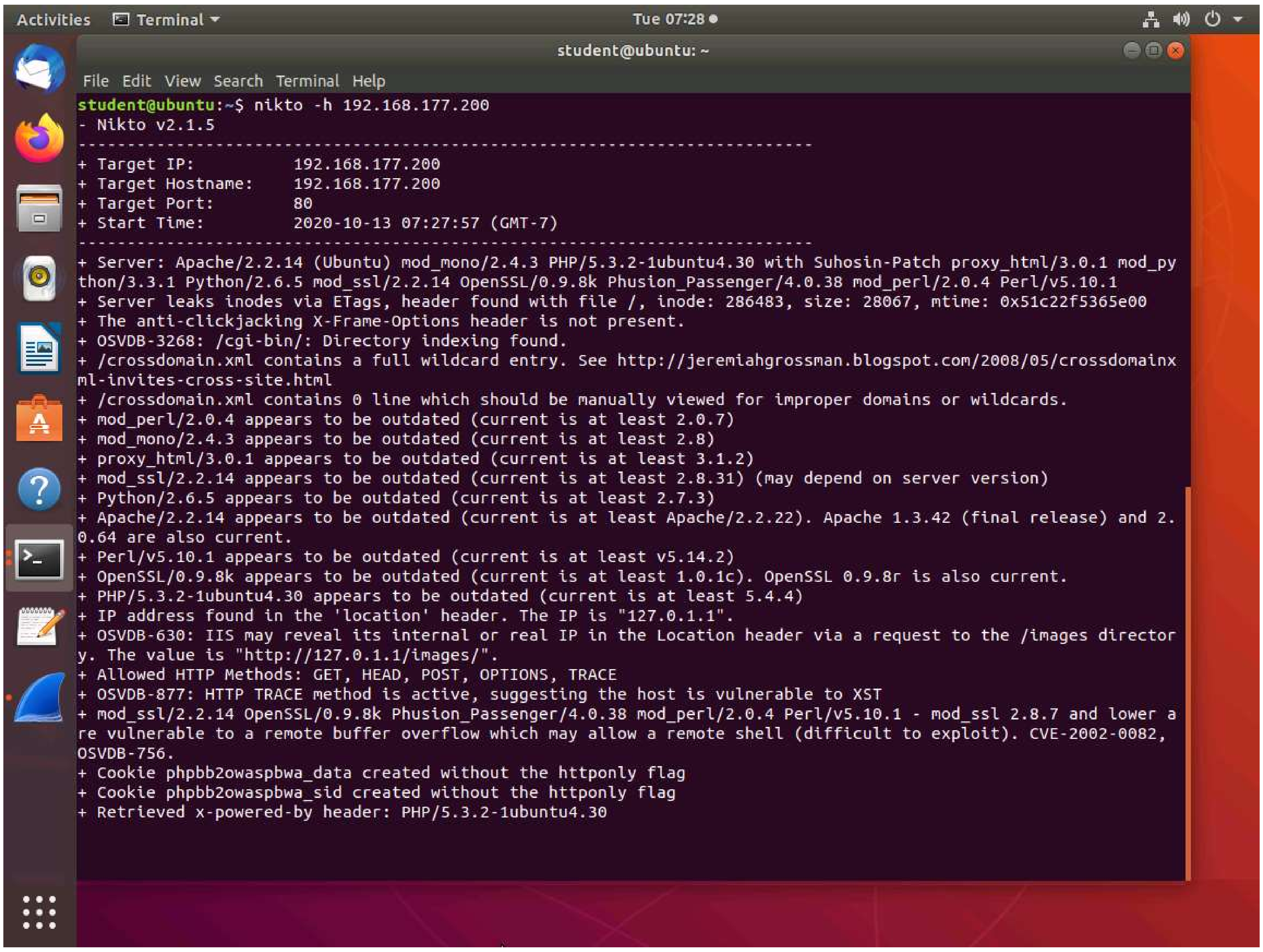
4. In the terminal, type **tail -f /var/log/syslog** and press **Enter**.



```
root@owaspbwa:~# tail -f /var/log/syslog
Oct 13 01:33:35 owaspbwa authdaemond: modules="authpam", daemons=5
Oct 13 01:33:35 owaspbwa authdaemond: Installing libauthpam
Oct 13 01:33:35 owaspbwa authdaemond: Installation complete: authpam
Oct 13 01:33:36 owaspbwa postfix/master[1103]: daemon started -- version 2.7.0,
configuration /etc/postfix
Oct 13 01:33:45 owaspbwa init: plymouth main process (249) killed by SEGV signal
Oct 13 01:39:01 owaspbwa CRON[1997]: (root) CMD (  [ -x /usr/lib/php5/maxlifetim
e ] && [ -d /var/lib/php5 ] && find /var/lib/php5/ -depth -mindepth 1 -maxdepth
1 -type f -cmin +$(/usr/lib/php5/maxlifetime) -delete)
Oct 13 02:09:01 owaspbwa CRON[2037]: (root) CMD (  [ -x /usr/lib/php5/maxlifetim
e ] && [ -d /var/lib/php5 ] && find /var/lib/php5/ -depth -mindepth 1 -maxdepth
1 -type f -cmin +$(/usr/lib/php5/maxlifetime) -delete)
Oct 13 02:17:01 owaspbwa CRON[2054]: (root) CMD (   cd / && run-parts --report /
etc/cron.hourly)
Oct 13 02:39:01 owaspbwa CRON[2080]: (root) CMD (  [ -x /usr/lib/php5/maxlifetim
e ] && [ -d /var/lib/php5 ] && find /var/lib/php5/ -depth -mindepth 1 -maxdepth
1 -type f -cmin +$(/usr/lib/php5/maxlifetime) -delete)
Oct 13 03:09:01 owaspbwa CRON[2119]: (root) CMD (  [ -x /usr/lib/php5/maxlifetim
e ] && [ -d /var/lib/php5 ] && find /var/lib/php5/ -depth -mindepth 1 -maxdepth
1 -type f -cmin +$(/usr/lib/php5/maxlifetime) -delete)

_
```

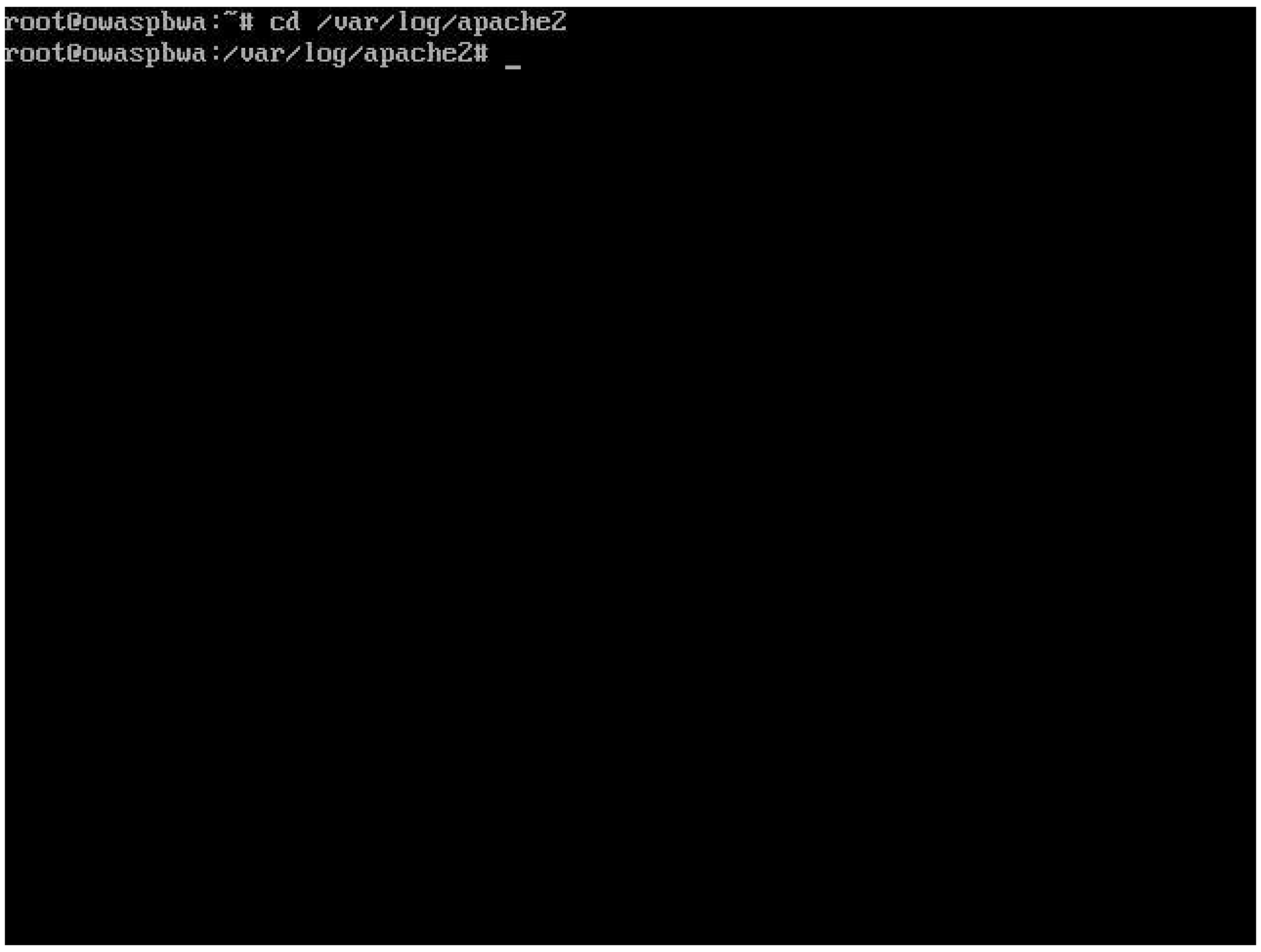
5. Switch to **CPENT Bash Machine** and in the terminal type **nikto -h 192.168.177.200** and press **Enter**.

Note: If the machine is locked, move your cursor in the upward direction and type **password** in the Password field and press **Enter**.



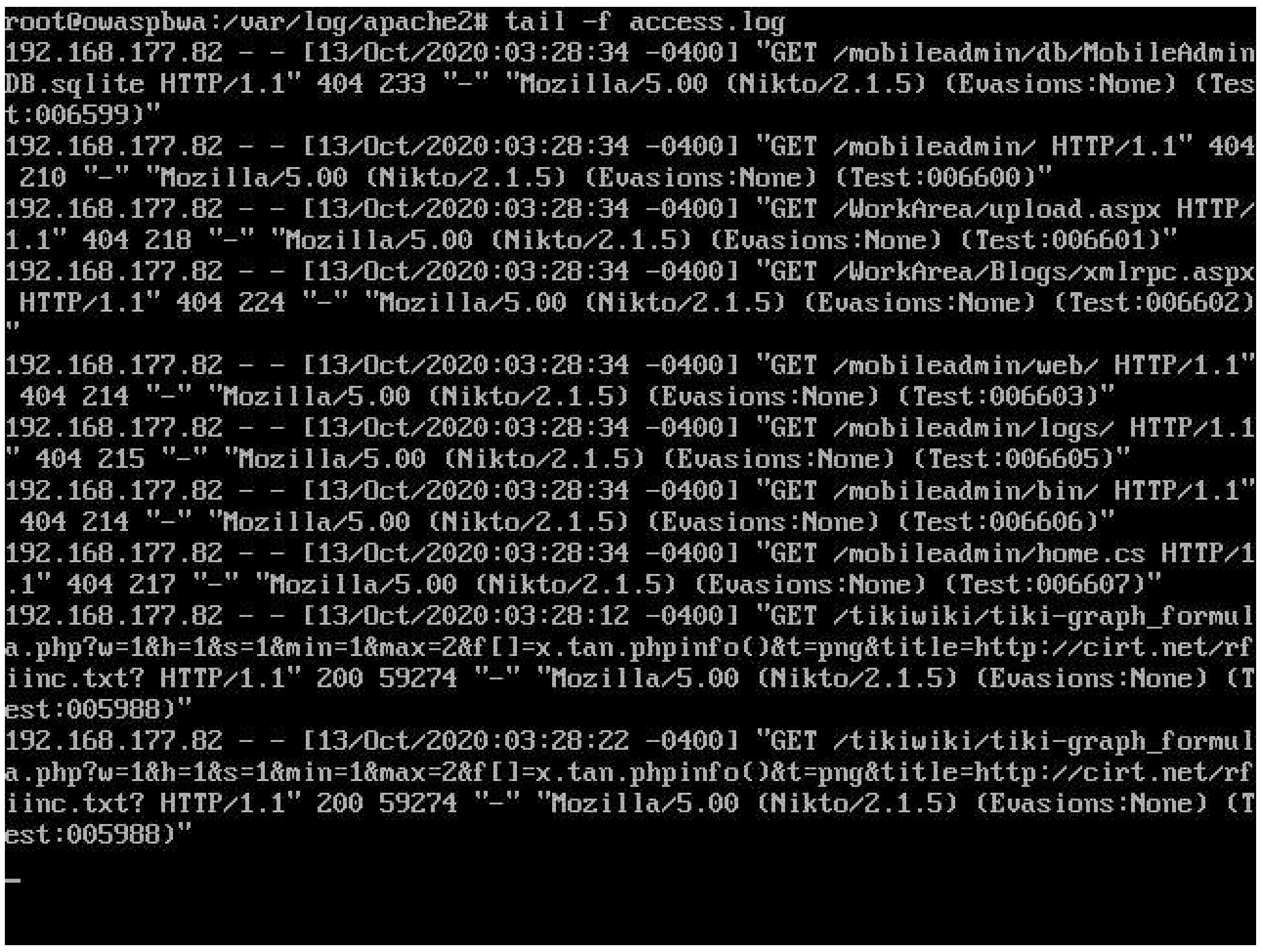
```
student@ubuntu:~$ nikto -h 192.168.177.200
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          192.168.177.200
+ Target Hostname:    192.168.177.200
+ Target Port:        80
+ Start Time:         2020-10-13 07:27:57 (GMT-7)
---------------------------------------------------------------------------
+ Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_py
thon/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
+ Server leaks inodes via ETags, header found with file /, inode: 286483, size: 28067, mtime: 0x51c22f5365e00
+ The anti-clickjacking X-Frame-Options header is not present.
+ OSVDB-3268: /cgi-bin/: Directory indexing found.
+ /crossdomain.xml contains a full wildcard entry. See http://jeremiahgrossman.blogspot.com/2008/05/crossdomainx
ml-invites-cross-site.html
+ /crossdomain.xml contains 0 line which should be manually viewed for improper domains or wildcards.
+ mod_perl/2.0.4 appears to be outdated (current is at least 2.0.7)
+ mod_mono/2.4.3 appears to be outdated (current is at least 2.8)
+ proxy_html/3.0.1 appears to be outdated (current is at least 3.1.2)
+ mod_ssl/2.2.14 appears to be outdated (current is at least 2.8.31) (may depend on server version)
+ Python/2.6.5 appears to be outdated (current is at least 2.7.3)
+ Apache/2.2.14 appears to be outdated (current is at least Apache/2.2.22). Apache 1.3.42 (final release) and 2.
0.64 are also current.
+ Perl/v5.10.1 appears to be outdated (current is at least v5.14.2)
+ OpenSSL/0.9.8k appears to be outdated (current is at least 1.0.1c). OpenSSL 0.9.8r is also current.
+ PHP/5.3.2-1ubuntu4.30 appears to be outdated (current is at least 5.4.4)
+ IP address found in the 'location' header. The IP is "127.0.1.1".
+ OSVDB-630: IIS may reveal its internal or real IP in the Location header via a request to the /images director
y. The value is "http://127.0.1.1/images/".
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1 - mod_ssl 2.8.7 and lower a
re vulnerable to a remote buffer overflow which may allow a remote shell (difficult to exploit). CVE-2002-0082,
OSVDB-756.
+ Cookie phpbb2owaspbwa_data created without the httponly flag
+ Cookie phpbb2owaspbwa_sid created without the httponly flag
+ Retrieved x-powered-by header: PHP/5.3.2-1ubuntu4.30
```

6. Switch to **Target_CPENT Bash-Web** and press **Ctrl+C**. The main log for **Apache** is located in the folder **/var/log/apache2**. Change into the directory with **cd /var/log/apache2**.



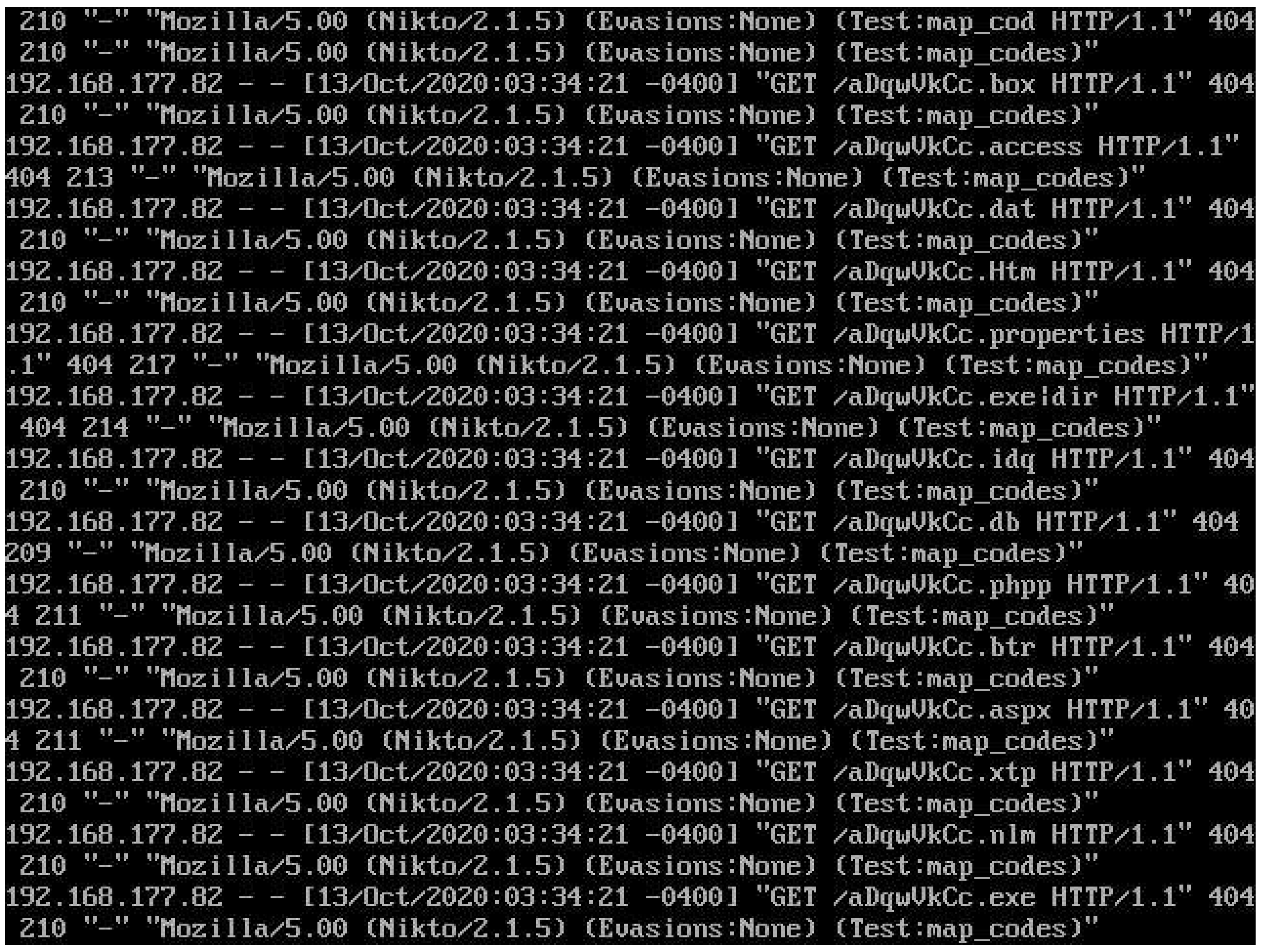
```
root@owaspbwa:~# cd /var/log/apache2
root@owaspbwa:/var/log/apache2# _
```

7. Next, type **tail -f access.log** and press **Enter** and leave the machine intact.



```
root@owaspbwa:/var/log/apache2# tail -f access.log
192.168.177.82 - - [13/Oct/2020:03:28:34 -0400] "GET /mobileadmin/db/MobileAdmin
DB.sqlite HTTP/1.1" 404 233 "-" "Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Tes
t:006599)"
192.168.177.82 - - [13/Oct/2020:03:28:34 -0400] "GET /mobileadmin/ HTTP/1.1" 404
 210 "-" "Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:006600)"
192.168.177.82 - - [13/Oct/2020:03:28:34 -0400] "GET /WorkArea/upload.aspx HTTP/
1.1" 404 218 "-" "Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:006601)"
192.168.177.82 - - [13/Oct/2020:03:28:34 -0400] "GET /WorkArea/Blogs/xmlrpc.aspx
 HTTP/1.1" 404 224 "-" "Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:006602)
"
192.168.177.82 - - [13/Oct/2020:03:28:34 -0400] "GET /mobileadmin/web/ HTTP/1.1"
 404 214 "-" "Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:006603)"
192.168.177.82 - - [13/Oct/2020:03:28:34 -0400] "GET /mobileadmin/logs/ HTTP/1.1
" 404 215 "-" "Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:006605)"
192.168.177.82 - - [13/Oct/2020:03:28:34 -0400] "GET /mobileadmin/bin/ HTTP/1.1"
 404 214 "-" "Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:006606)"
192.168.177.82 - - [13/Oct/2020:03:28:34 -0400] "GET /mobileadmin/home.cs HTTP/1
.1" 404 217 "-" "Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:006607)"
192.168.177.82 - - [13/Oct/2020:03:28:12 -0400] "GET /tikiwiki/tiki-graph_formul
a.php?w=1&h=1&s=1&min=1&max=2&f[]=x.tan.phpinfo()&t=png&title=http://cirt.net/rf
iinc.txt? HTTP/1.1" 200 59274 "-" "Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (T
est:005988)"
192.168.177.82 - - [13/Oct/2020:03:28:22 -0400] "GET /tikiwiki/tiki-graph_formul
a.php?w=1&h=1&s=1&min=1&max=2&f[]=x.tan.phpinfo()&t=png&title=http://cirt.net/rf
iinc.txt? HTTP/1.1" 200 59274 "-" "Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (T
est:005988)"

_
```

8. Now, switch to the **CPENT Bash Machine** and run the Nikto scan again. Then switch to the **Target_CPENT Bash-Web** and review the output of the scan. This is shown in the following screenshot.

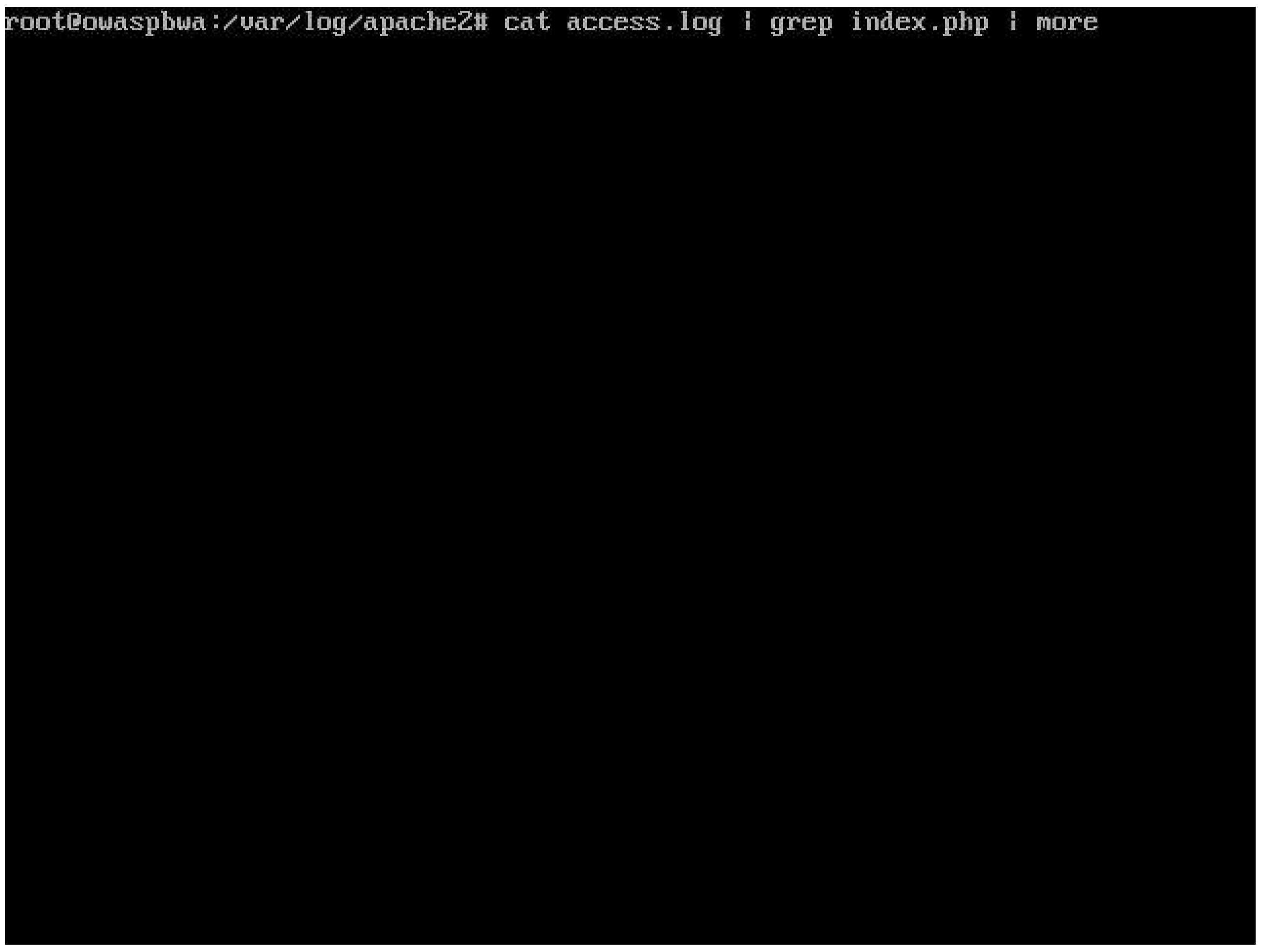


```
 210 "-" "Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:map_cod HTTP/1.1" 404
 210 "-" "Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
192.168.177.82 - - [13/Oct/2020:03:34:21 -0400] "GET /aDqwVkCc.box HTTP/1.1" 404
 210 "-" "Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
192.168.177.82 - - [13/Oct/2020:03:34:21 -0400] "GET /aDqwVkCc.access HTTP/1.1"
404 213 "-" "Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
192.168.177.82 - - [13/Oct/2020:03:34:21 -0400] "GET /aDqwVkCc.dat HTTP/1.1" 404
 210 "-" "Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
192.168.177.82 - - [13/Oct/2020:03:34:21 -0400] "GET /aDqwVkCc.Htm HTTP/1.1" 404
 210 "-" "Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
192.168.177.82 - - [13/Oct/2020:03:34:21 -0400] "GET /aDqwVkCc.properties HTTP/1
.1" 404 217 "-" "Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
192.168.177.82 - - [13/Oct/2020:03:34:21 -0400] "GET /aDqwVkCc.exe|dir HTTP/1.1"
 404 214 "-" "Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
192.168.177.82 - - [13/Oct/2020:03:34:21 -0400] "GET /aDqwVkCc.idq HTTP/1.1" 404
 210 "-" "Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
192.168.177.82 - - [13/Oct/2020:03:34:21 -0400] "GET /aDqwVkCc.db HTTP/1.1" 404
209 "-" "Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
192.168.177.82 - - [13/Oct/2020:03:34:21 -0400] "GET /aDqwVkCc.phpp HTTP/1.1" 40
4 211 "-" "Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
192.168.177.82 - - [13/Oct/2020:03:34:21 -0400] "GET /aDqwVkCc.btr HTTP/1.1" 404
 210 "-" "Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
192.168.177.82 - - [13/Oct/2020:03:34:21 -0400] "GET /aDqwVkCc.aspx HTTP/1.1" 40
4 211 "-" "Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
192.168.177.82 - - [13/Oct/2020:03:34:21 -0400] "GET /aDqwVkCc.xtp HTTP/1.1" 404
 210 "-" "Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
192.168.177.82 - - [13/Oct/2020:03:34:21 -0400] "GET /aDqwVkCc.nlm HTTP/1.1" 404
 210 "-" "Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
192.168.177.82 - - [13/Oct/2020:03:34:21 -0400] "GET /aDqwVkCc.exe HTTP/1.1" 404
 210 "-" "Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
```

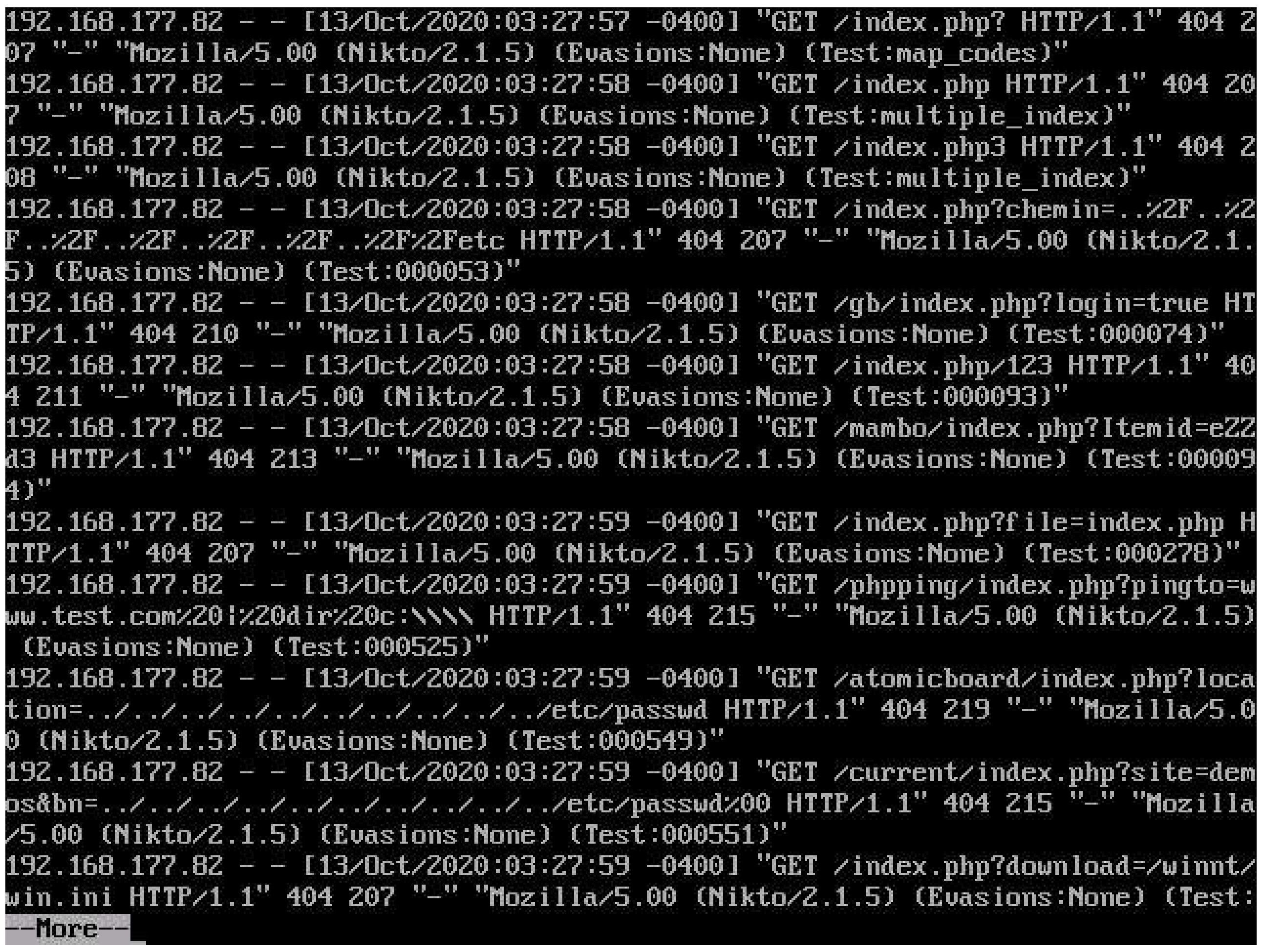
9. The scan results are being tracked in our **access.log** file. However, since we only scanned the default page, we do not see a lot of information. Again, the above screenshot reveals that we are being logged when we access the web server and not only that our IP address is being logged as well. Therefore, we need to identify a method to modify the logs and change what is located there. We could delete the log, but this will be obvious and not ideal in a professional test. If the log is removed, it could cause a problem for our clients.

10. In cases of logs with a smaller size or if we are looking for a specific keyword, then we can spend some time observing the logs manually using things such as grep expressions.

11. As we have done earlier, we can use the cat command to pipe the output into grep and look for specific keywords. Press **Ctrl+C** in the **Target_CPENT Bash-Web** machine to stop the traffic. Type **cat access.log | grep index.php | more** and press **Enter**. The output from this command is shown in the following screenshot. Press **Enter** to review until you get the terminal.



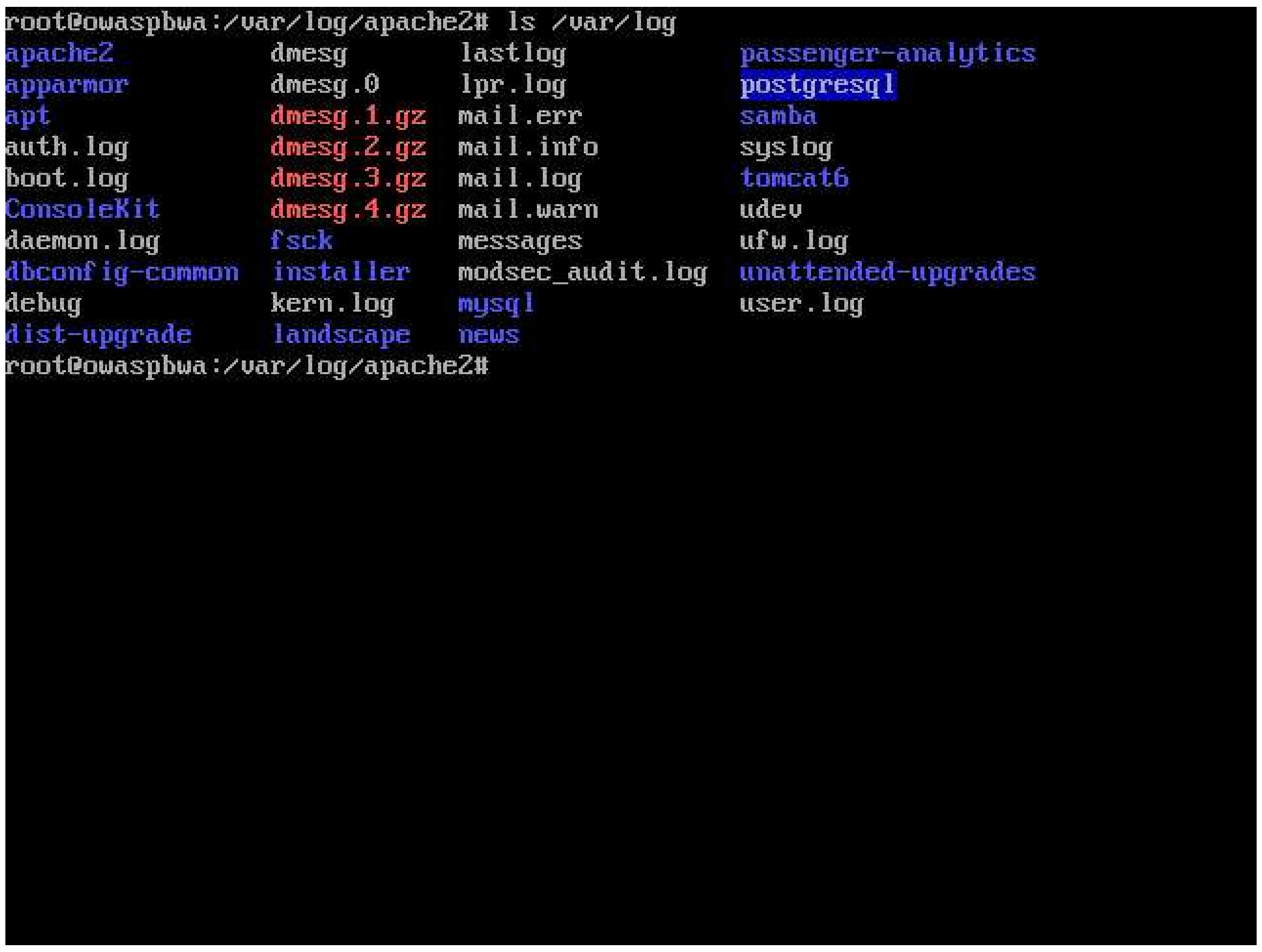
```
root@owaspbwa:/var/log/apache2# cat access.log | grep index.php | more
```



```
192.168.177.82 - - [13/Oct/2020:03:27:57 -0400] "GET /index.php? HTTP/1.1" 404 2
07 "-" "Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:map_codes)"
192.168.177.82 - - [13/Oct/2020:03:27:58 -0400] "GET /index.php HTTP/1.1" 404 20
7 "-" "Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:multiple_index)"
192.168.177.82 - - [13/Oct/2020:03:27:58 -0400] "GET /index.php3 HTTP/1.1" 404 2
08 "-" "Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:multiple_index)"
192.168.177.82 - - [13/Oct/2020:03:27:58 -0400] "GET /index.php?chemin=..%2F..%2
F..%2F..%2F..%2F..%2F..%2F%2Fetc HTTP/1.1" 404 207 "-" "Mozilla/5.00 (Nikto/2.1.
5) (Evasions:None) (Test:000053)"
192.168.177.82 - - [13/Oct/2020:03:27:58 -0400] "GET /gb/index.php?login=true HT
TP/1.1" 404 210 "-" "Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:000074)"
192.168.177.82 - - [13/Oct/2020:03:27:58 -0400] "GET /index.php/123 HTTP/1.1" 40
4 211 "-" "Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:000093)"
192.168.177.82 - - [13/Oct/2020:03:27:58 -0400] "GET /mambo/index.php?Itemid=eZZ
d3 HTTP/1.1" 404 213 "-" "Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:00009
4)"
192.168.177.82 - - [13/Oct/2020:03:27:59 -0400] "GET /index.php?file=index.php H
TTP/1.1" 404 207 "-" "Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:000278)"
192.168.177.82 - - [13/Oct/2020:03:27:59 -0400] "GET /phpping/index.php?pingto=w
ww.test.com%20|%20dir%20c:\\\\ HTTP/1.1" 404 215 "-" "Mozilla/5.00 (Nikto/2.1.5)
 (Evasions:None) (Test:000525)"
192.168.177.82 - - [13/Oct/2020:03:27:59 -0400] "GET /atomicboard/index.php?loca
tion=../../../../../../../../../../etc/passwd HTTP/1.1" 404 219 "-" "Mozilla/5.0
0 (Nikto/2.1.5) (Evasions:None) (Test:000549)"
192.168.177.82 - - [13/Oct/2020:03:27:59 -0400] "GET /current/index.php?site=dem
os&bn=../../../../../../../../../../etc/passwd%00 HTTP/1.1" 404 215 "-" "Mozilla
/5.00 (Nikto/2.1.5) (Evasions:None) (Test:000551)"
192.168.177.82 - - [13/Oct/2020:03:27:59 -0400] "GET /index.php?download=/winnt/
win.ini HTTP/1.1" 404 207 "-" "Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:
--More--
```

12. As the above screenshot shows, one of the problems is that we have a header with the **User-Agent** of nikto as well. In addition to the IP address and the obvious attack strings, this is another concerning aspect.

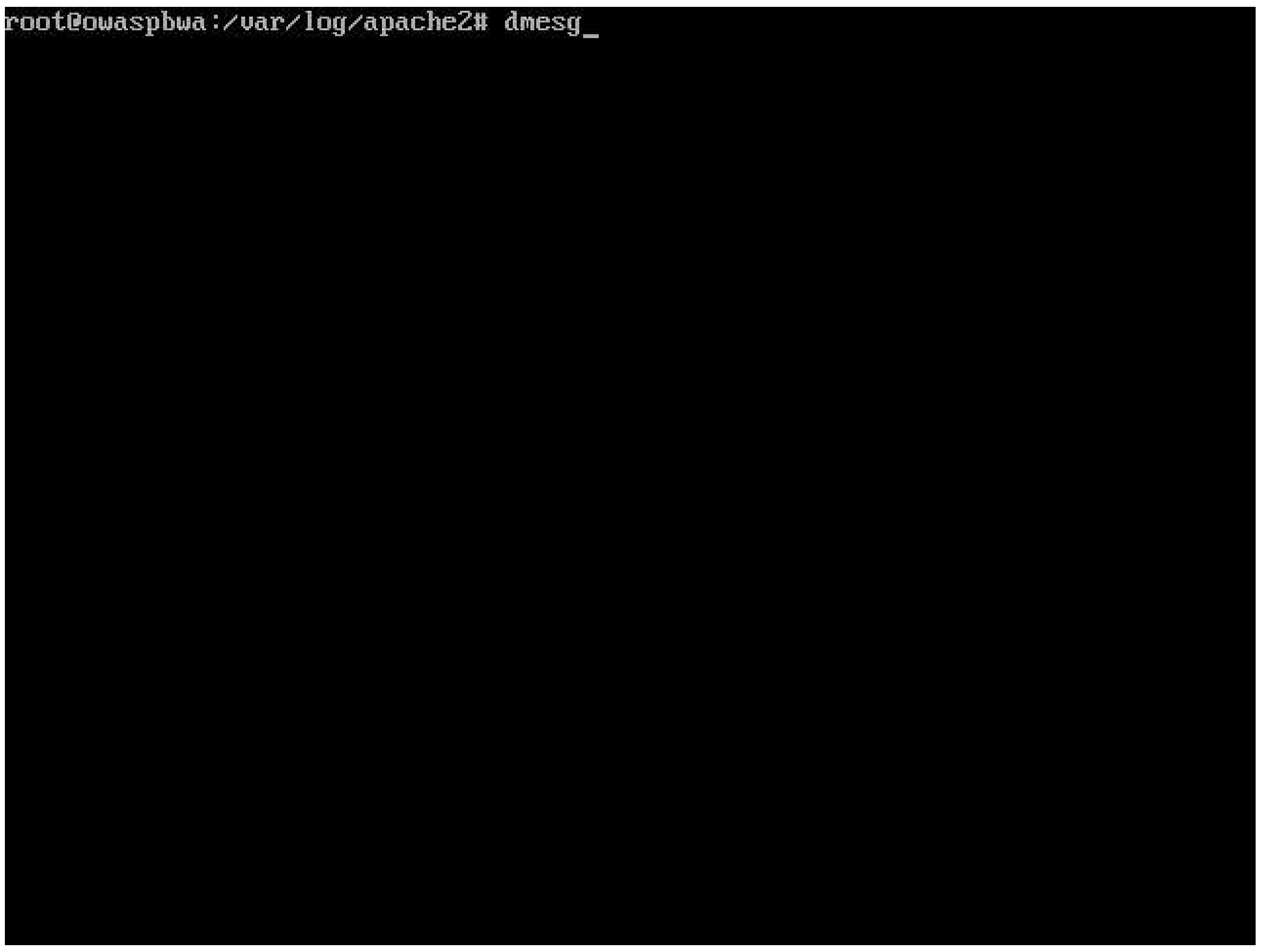
13. Let us now take a look at all logs in the folder. Type **ls /var/log** and press **Enter**.



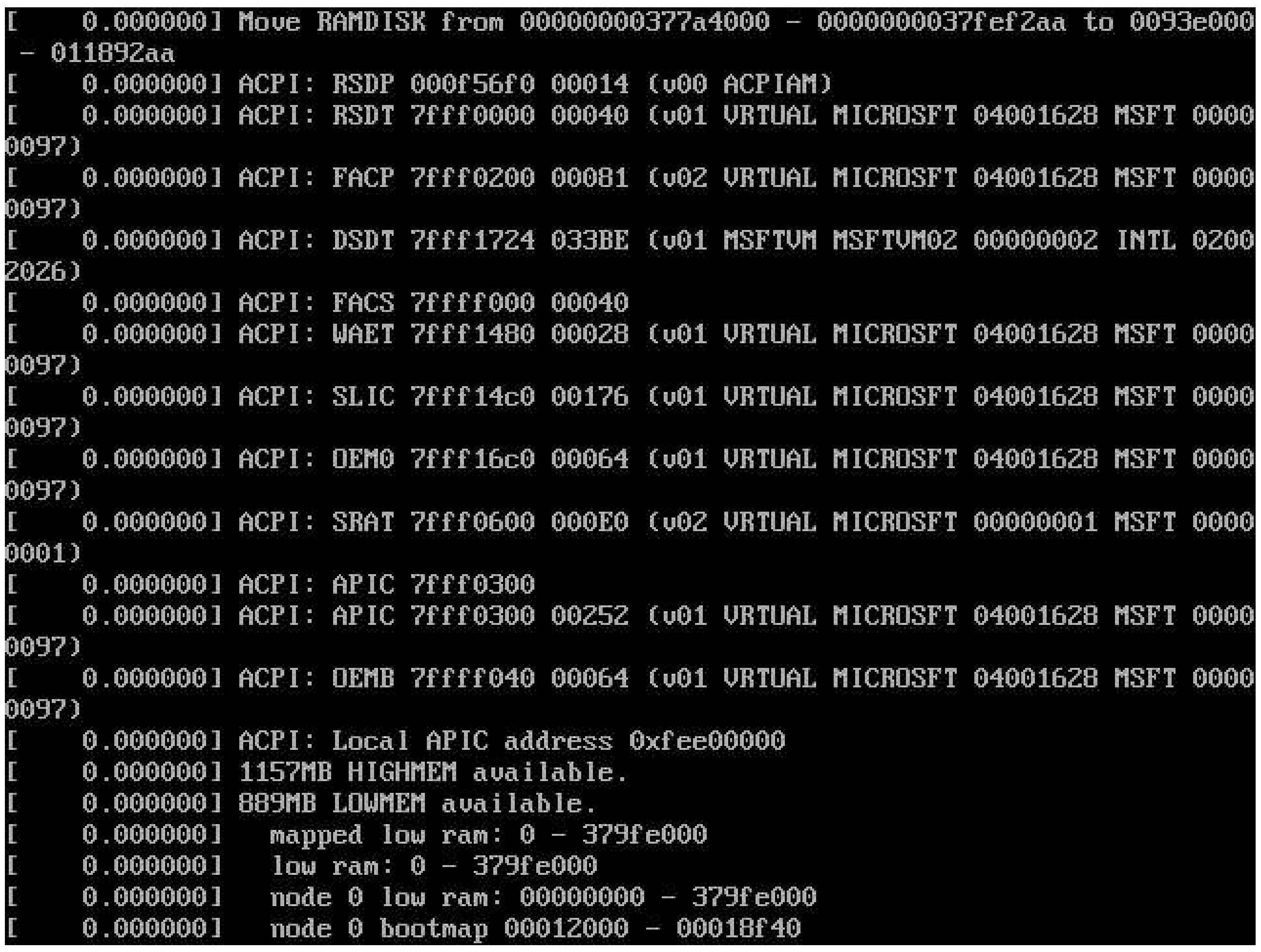
```
root@owaspbwa:/var/log/apache2# ls /var/log
apache2          dmesg       lastlog          passenger-analytics
apparmor         dmesg.0     lpr.log          postgresql
apt              dmesg.1.gz  mail.err         samba
auth.log         dmesg.2.gz  mail.info        syslog
boot.log         dmesg.3.gz  mail.log         tomcat6
ConsoleKit       dmesg.4.gz  mail.warn        udev
daemon.log       fsck        messages         ufw.log
dbconfig-common  installer   modsec_audit.log unattended-upgrades
debug            kern.log    mysql            user.log
dist-upgrade     landscape   news
root@owaspbwa:/var/log/apache2#
```

14. As the above image shows, there are several log files, and investigating them is beyond the scope of this lab. However, the process of log analysis is the same, and which log you review is irrelevant.

15. The **dmesg** command prints the **kernel** ring buffer. By default, the command will display all messages from the kernel ring buffer. In the terminal, type **dmesg** and press **Enter**, and the entire kernel ring buffer will print. An example of the output is shown in the following screenshot.

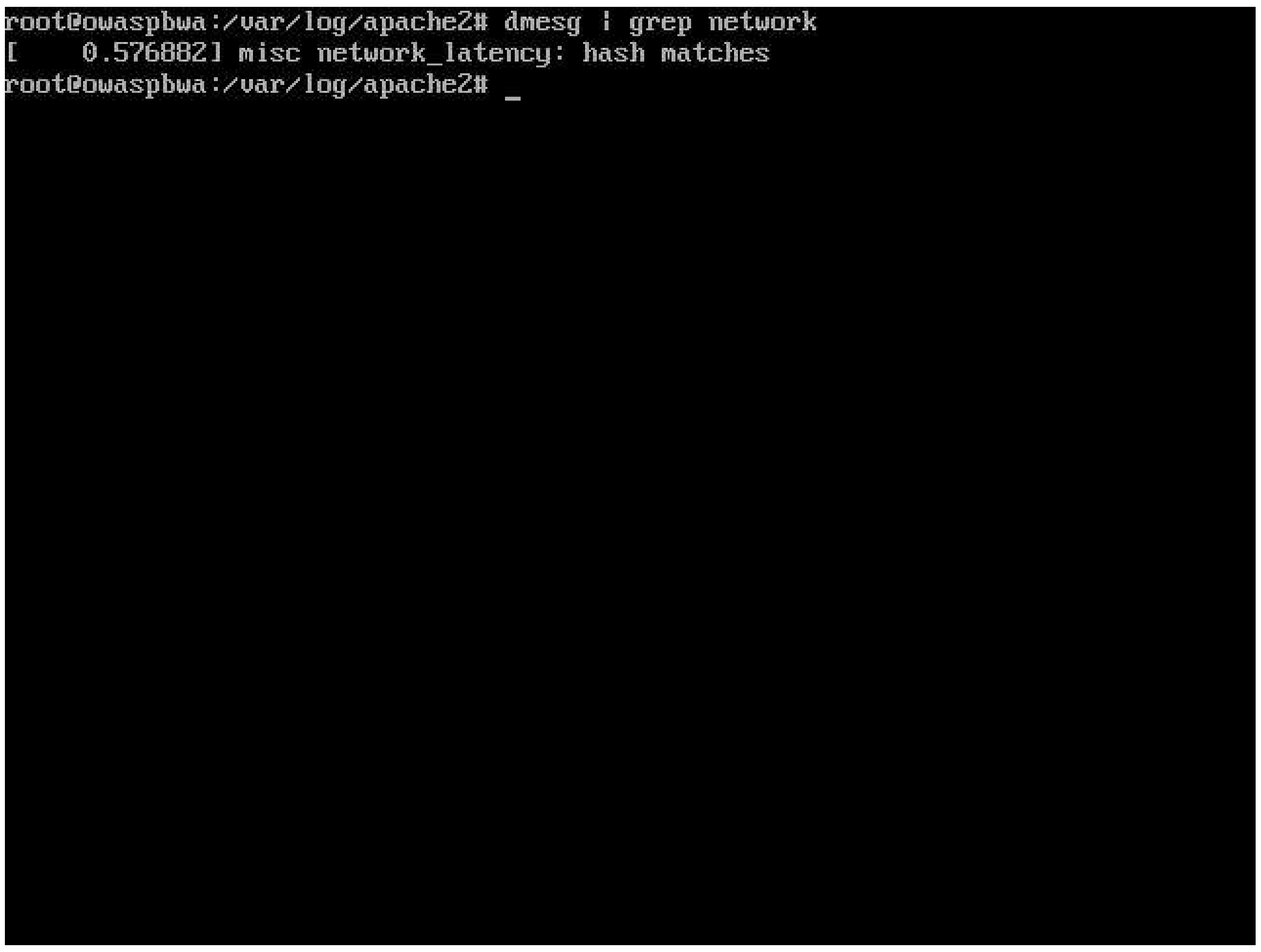


```
root@owaspbwa:/var/log/apache2# dmesg_
```



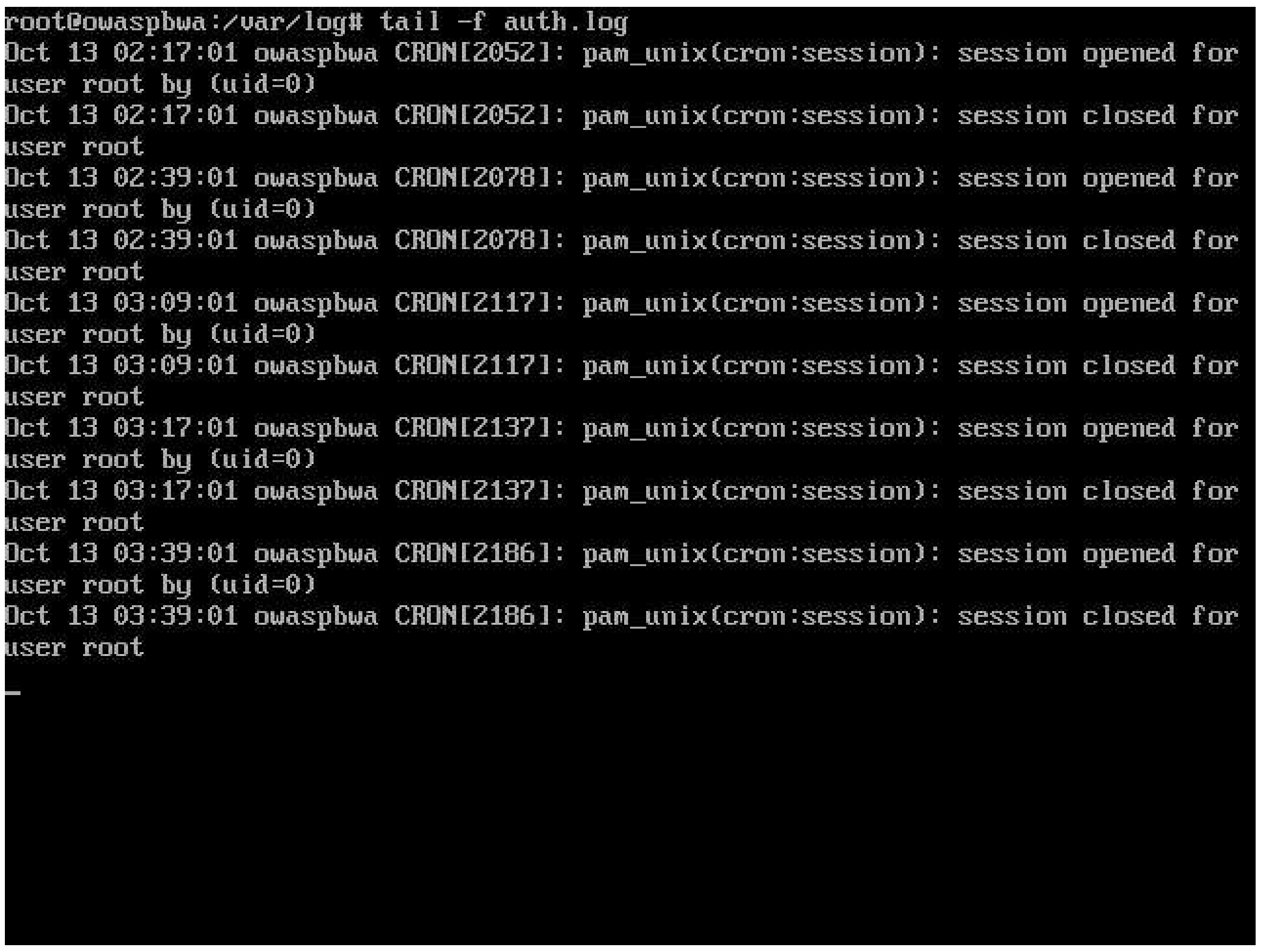
```
[    0.000000] Move RAMDISK from 00000000377a4000 - 0000000037fef2aa to 0093e000
 - 011892aa
[    0.000000] ACPI: RSDP 000f56f0 00014 (v00 ACPIAM)
[    0.000000] ACPI: RSDT 7fff0000 00040 (v01 VRTUAL MICROSFT 04001628 MSFT 0000
0097)
[    0.000000] ACPI: FACP 7fff0200 00081 (v02 VRTUAL MICROSFT 04001628 MSFT 0000
0097)
[    0.000000] ACPI: DSDT 7fff1724 033BE (v01 MSFTVM MSFTVM02 00000002 INTL 0200
2026)
[    0.000000] ACPI: FACS 7ffff000 00040
[    0.000000] ACPI: WAET 7fff1480 00028 (v01 VRTUAL MICROSFT 04001628 MSFT 0000
0097)
[    0.000000] ACPI: SLIC 7fff14c0 00176 (v01 VRTUAL MICROSFT 04001628 MSFT 0000
0097)
[    0.000000] ACPI: OEM0 7fff16c0 00064 (v01 VRTUAL MICROSFT 04001628 MSFT 0000
0097)
[    0.000000] ACPI: SRAT 7fff0600 000E0 (v02 VRTUAL MICROSFT 00000001 MSFT 0000
0001)
[    0.000000] ACPI: APIC 7fff0300
[    0.000000] ACPI: APIC 7fff0300 00252 (v01 VRTUAL MICROSFT 04001628 MSFT 0000
0097)
[    0.000000] ACPI: OEMB 7ffff040 00064 (v01 VRTUAL MICROSFT 04001628 MSFT 0000
0097)
[    0.000000] ACPI: Local APIC address 0xfee00000
[    0.000000] 1157MB HIGHMEM available.
[    0.000000] 889MB LOWMEM available.
[    0.000000]   mapped low ram: 0 - 379fe000
[    0.000000]   low ram: 0 - 379fe000
[    0.000000]   node 0 low ram: 00000000 - 379fe000
[    0.000000]   node 0 bootmap 00012000 - 00018f40
```

16. The output file can be long, so you can pipe it to less and review it there. We can also pipe the log into the grep tool. Type **dmesg | grep network** and press **Enter**. If anything has been logged, it will print. An example of this is shown in the following screenshot.



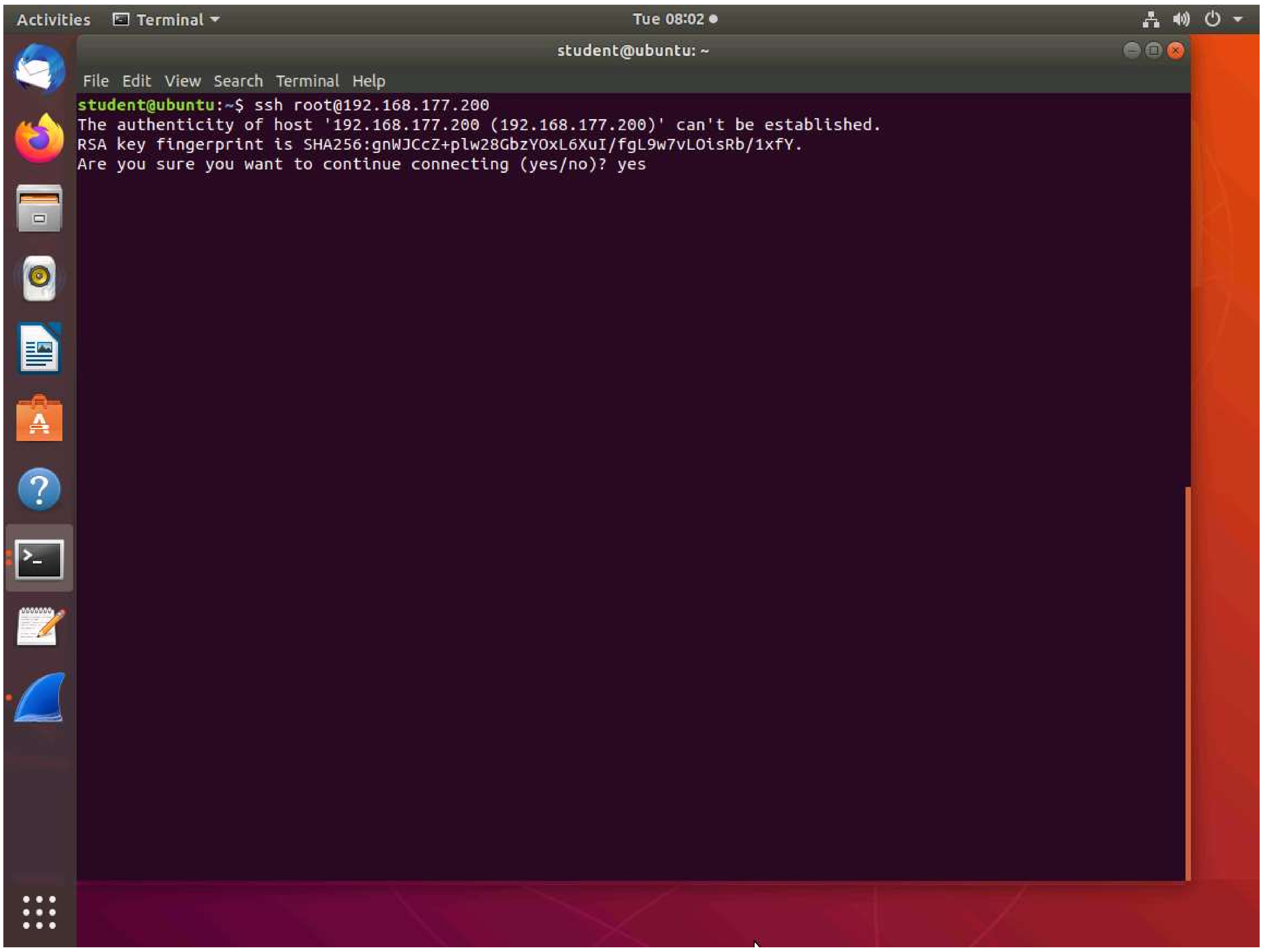
```
root@owaspbwa:/var/log/apache2# dmesg | grep network
[    0.576882] misc network_latency: hash matches
root@owaspbwa:/var/log/apache2# _
```

17. Next, we will review the **auth log**. In the terminal type **cd /var/log** and press **Enter** to change the directory to log. Type **tail -f auth.log** and press **Enter**. This will show the login sessions.



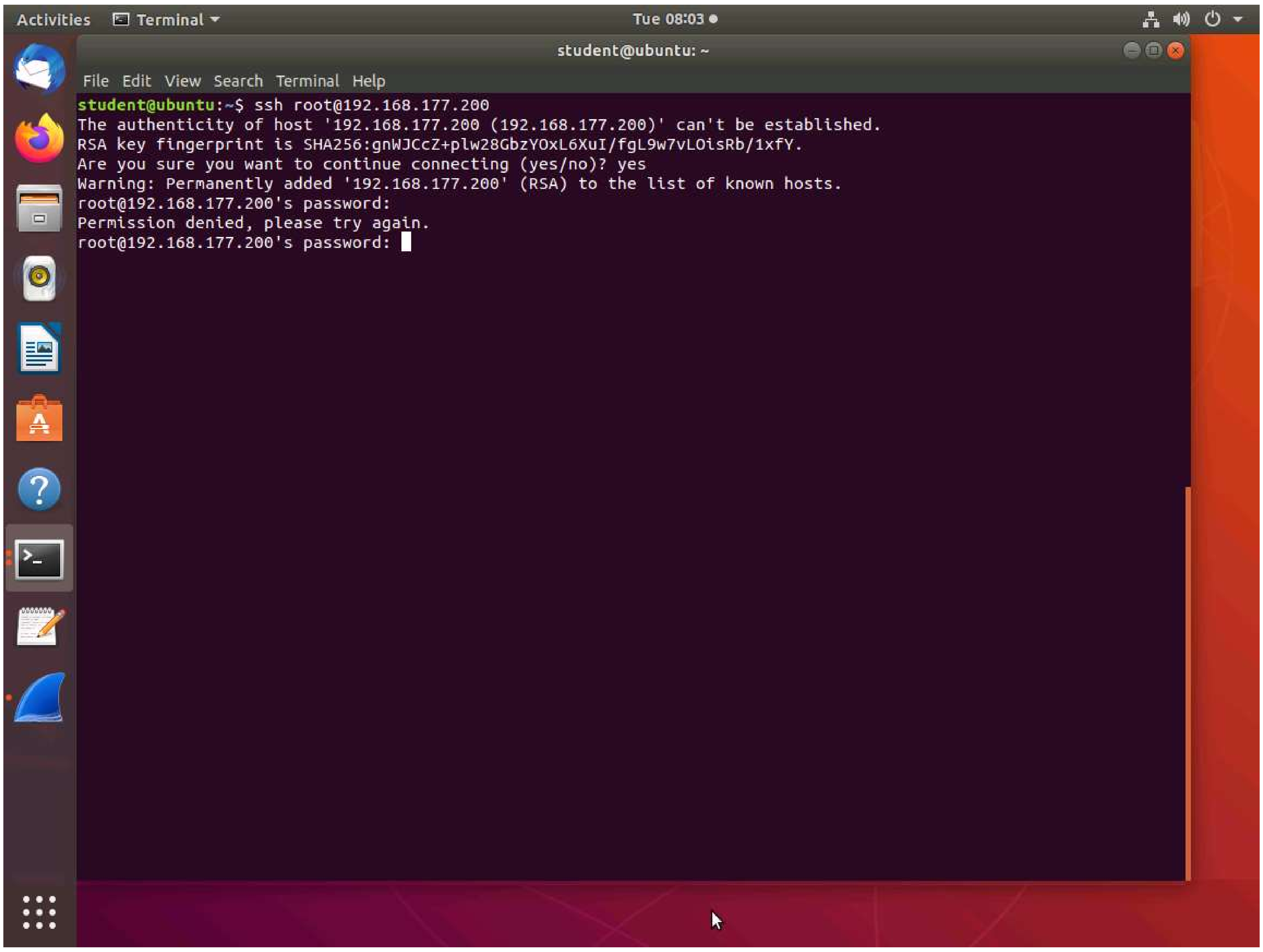
```
root@owaspbwa:/var/log# tail -f auth.log
Oct 13 02:17:01 owaspbwa CRON[2052]: pam_unix(cron:session): session opened for
user root by (uid=0)
Oct 13 02:17:01 owaspbwa CRON[2052]: pam_unix(cron:session): session closed for
user root
Oct 13 02:39:01 owaspbwa CRON[2078]: pam_unix(cron:session): session opened for
user root by (uid=0)
Oct 13 02:39:01 owaspbwa CRON[2078]: pam_unix(cron:session): session closed for
user root
Oct 13 03:09:01 owaspbwa CRON[2117]: pam_unix(cron:session): session opened for
user root by (uid=0)
Oct 13 03:09:01 owaspbwa CRON[2117]: pam_unix(cron:session): session closed for
user root
Oct 13 03:17:01 owaspbwa CRON[2137]: pam_unix(cron:session): session opened for
user root by (uid=0)
Oct 13 03:17:01 owaspbwa CRON[2137]: pam_unix(cron:session): session closed for
user root
Oct 13 03:39:01 owaspbwa CRON[2186]: pam_unix(cron:session): session opened for
user root by (uid=0)
Oct 13 03:39:01 owaspbwa CRON[2186]: pam_unix(cron:session): session closed for
user root

_
```

18. Switch to **CPENT Bash Machine** machine, and type **ssh root@192.168.177.200** and press **Enter**. Accept the storage of the key message, and enter **yes**.



```
student@ubuntu:~$ ssh root@192.168.177.200
The authenticity of host '192.168.177.200 (192.168.177.200)' can't be established.
RSA key fingerprint is SHA256:gnWJCcZ+plw28GbzYOxL6XuI/fgL9w7vLOisRb/1xfY.
Are you sure you want to continue connecting (yes/no)? yes
```

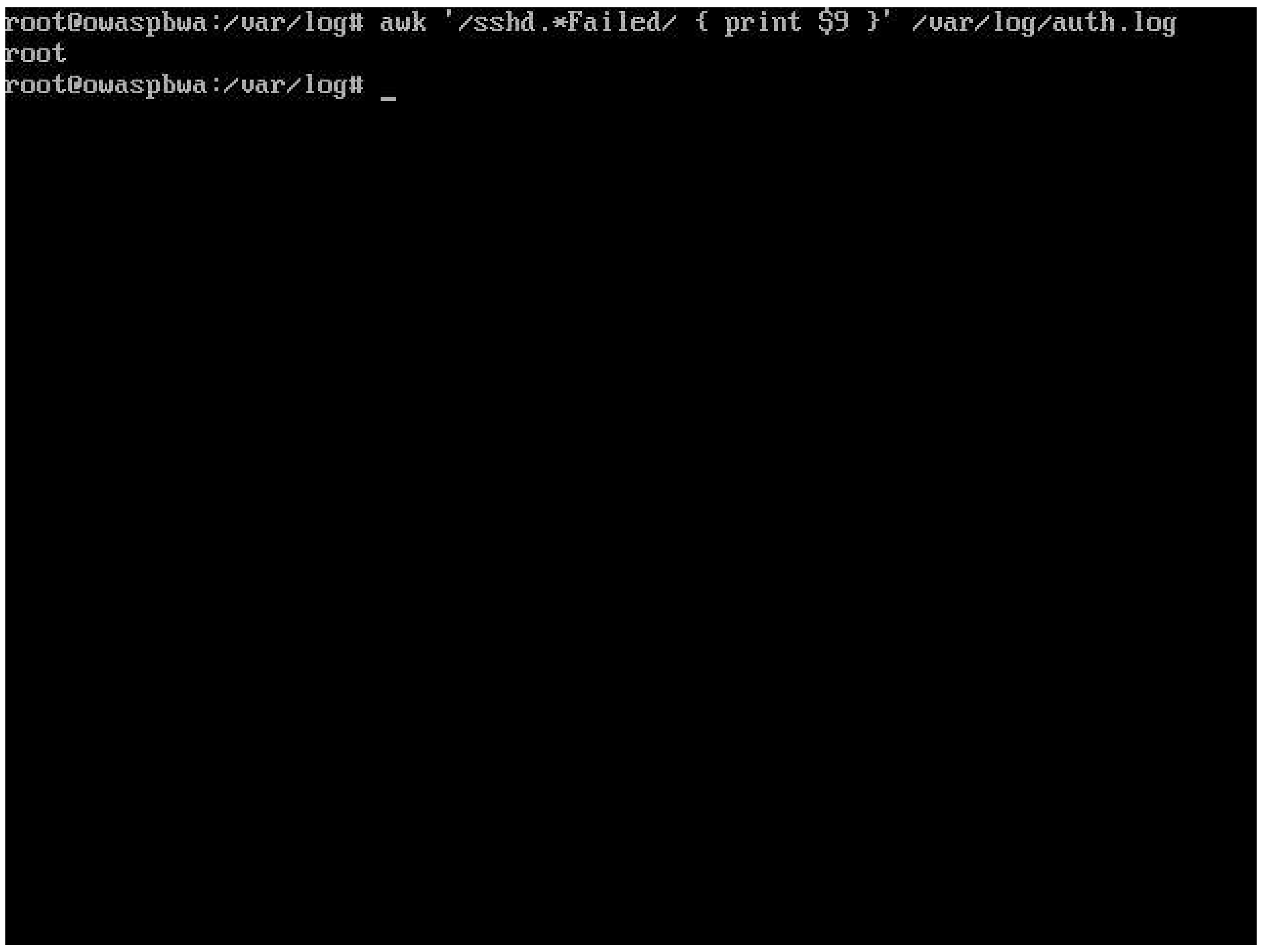
19. Enter the wrong password.



```
student@ubuntu:~$ ssh root@192.168.177.200
The authenticity of host '192.168.177.200 (192.168.177.200)' can't be established.
RSA key fingerprint is SHA256:gnWJCcZ+plw28GbzYOxL6XuI/fgL9w7vLOisRb/1xfY.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.177.200' (RSA) to the list of known hosts.
root@192.168.177.200's password:
Permission denied, please try again.
root@192.168.177.200's password:
```

20. Now, switch to **Target_CPENT Bash-Web** machine, and type **awk '/sshd.*Failed/ { print $9 }' /var/log/auth.log** and press **Enter**. An example of the output of the command is shown in the following screenshot.

21. As the screenshot shows, the login has failed.

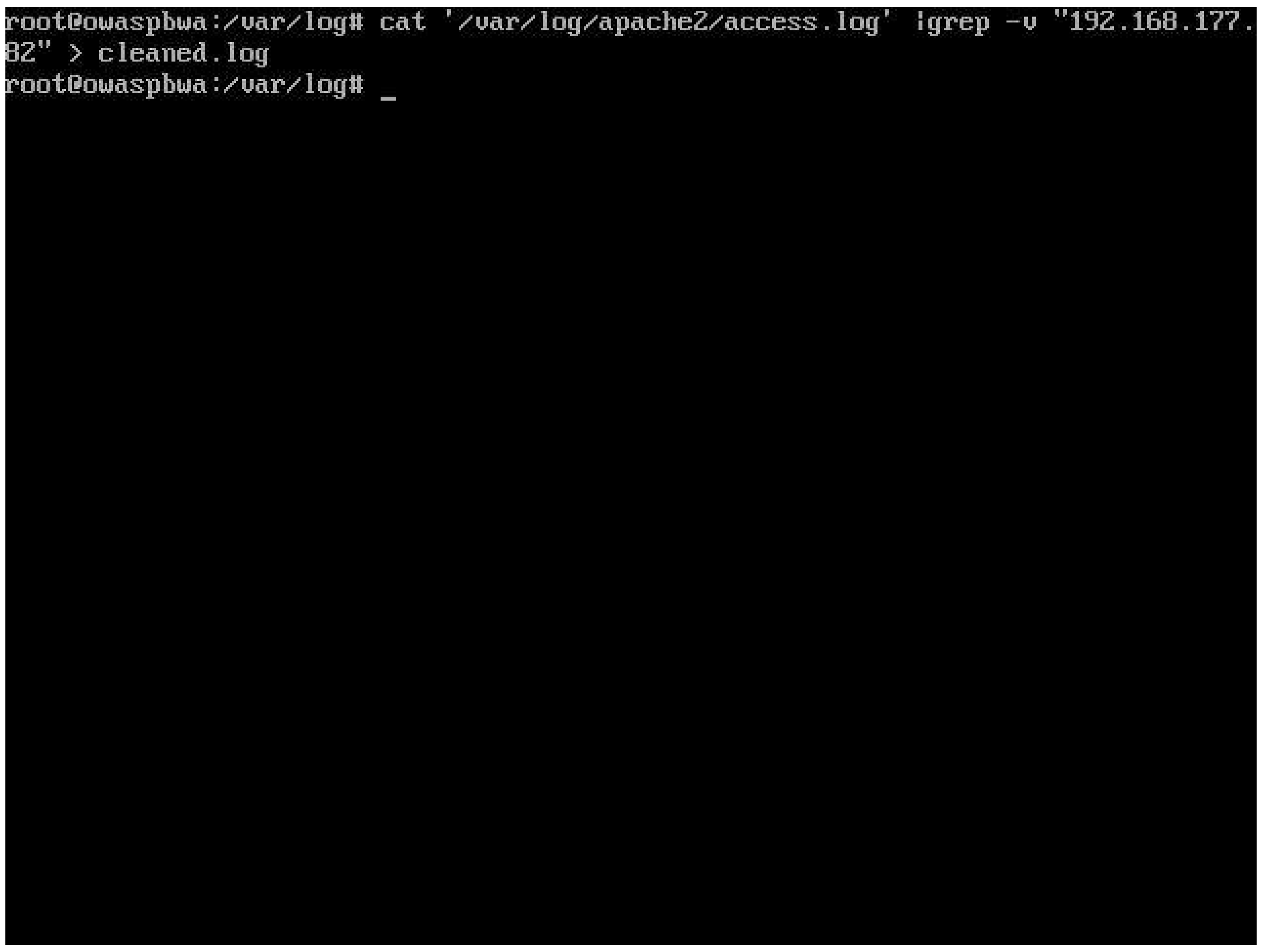


```
root@owaspbwa:/var/log# awk '/sshd.*Failed/ { print $9 }' /var/log/auth.log
root
root@owaspbwa:/var/log# _
```

22. We are now ready to modify the log and change our access so that it does not show us making access. Type the following command and change the address if required to your address:

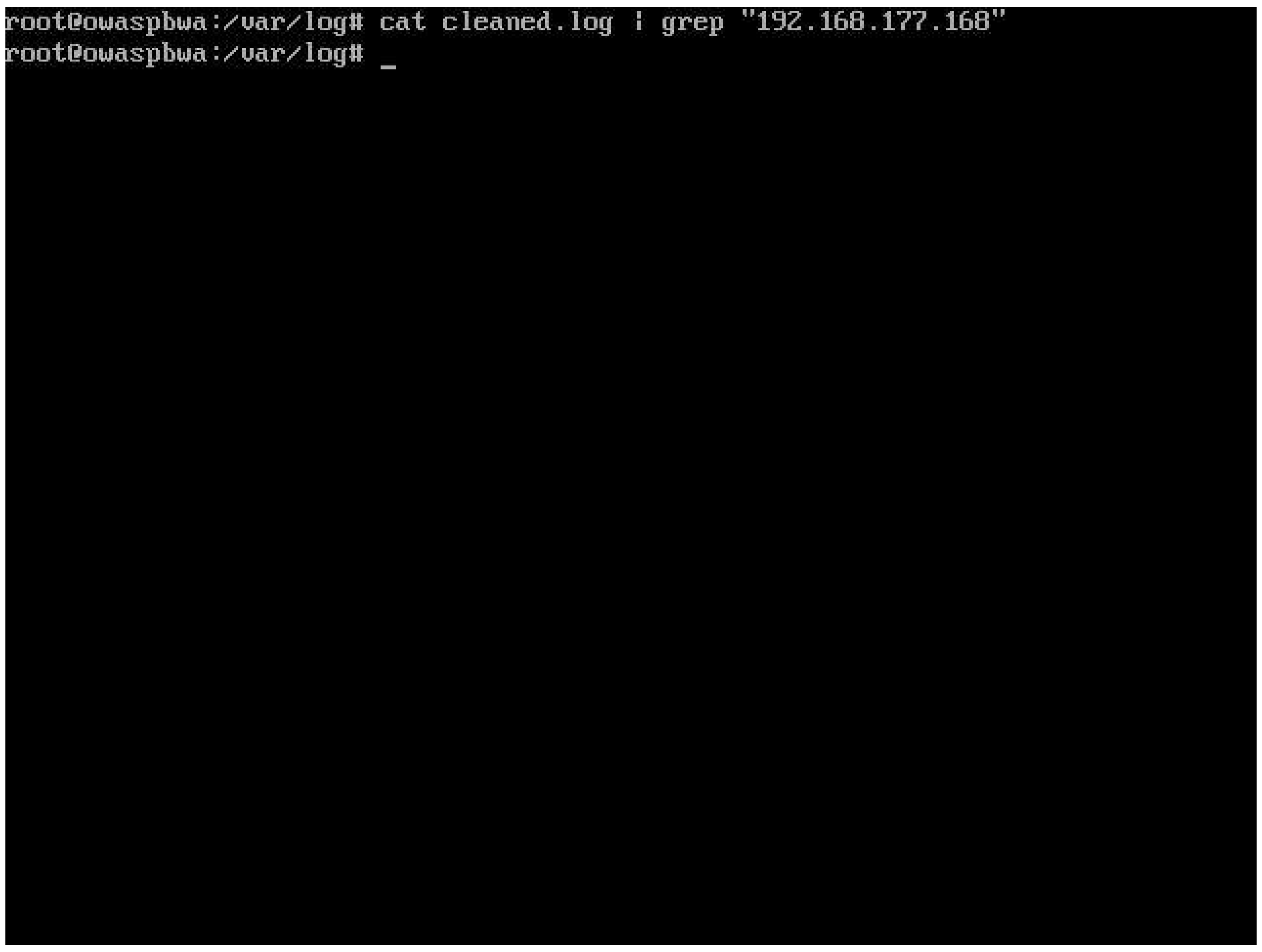
    cat '/var/log/apache2/access.log' |grep -v “192.168.177.82” > cleaned.log

    Note: 192.168.177.82 is the IP address of the CPENT Bash Machine.



```
root@owaspbwa:/var/log# cat '/var/log/apache2/access.log' |grep -v "192.168.177.
82" > cleaned.log
root@owaspbwa:/var/log# _
```

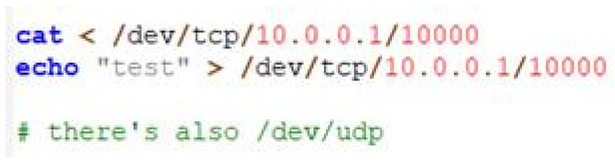
23. Now, you want to grep for your IP address to see if it is still there. Type **cat cleaned.log | grep "192.168.177.168"** and press **Enter**. The output of the command is shown in the following screenshot.



```
root@owaspbwa:/var/log# cat cleaned.log | grep "192.168.177.168"
root@owaspbwa:/var/log# _
```

24. As the above screenshot shows, we are successful, and there is no evidence of our IP address in the log.

25. The last task of this lab is using **BASH** to connect to a socket. This is accomplished by entering the code shown in the following screenshot.



```
cat < /dev/tcp/10.0.0.1/10000
echo "test" > /dev/tcp/10.0.0.1/10000

# there's also /dev/udp
```

26. Depending on the version of the OS, the Transmission Control Protocol (TCP) location may or may not be the same.

27. The lab objectives have been achieved.