CONESTOGA

Connect Life and Learning

Student Name:	Aagam Sanjay Shah
Deliverable:	In-Class Tasks Week 11 Assignment
Course Name:	NTWK8141-24S-Sec3-Linux Server

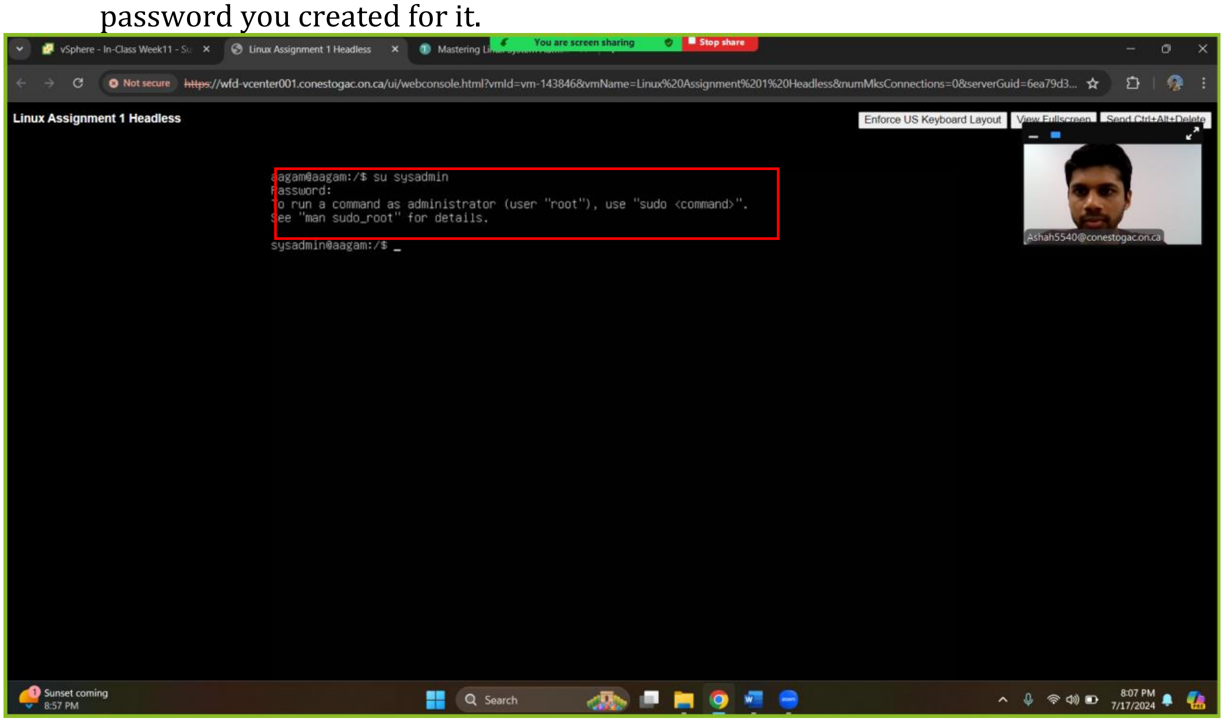
Date Assigned:	17/07/2024
Date Due:	18/07/2024
Rules:	• Individual. • Cheating is not allowed. • Plagiarism counts as cheating! • That FAILURE to submit work in the course can result in a grade of 'F' or 'I' for failure to complete the course!

1. Week 11 Slide 8

Complete the Real World Scenario: Determining Your Privilege Elevation Status in Ch 17

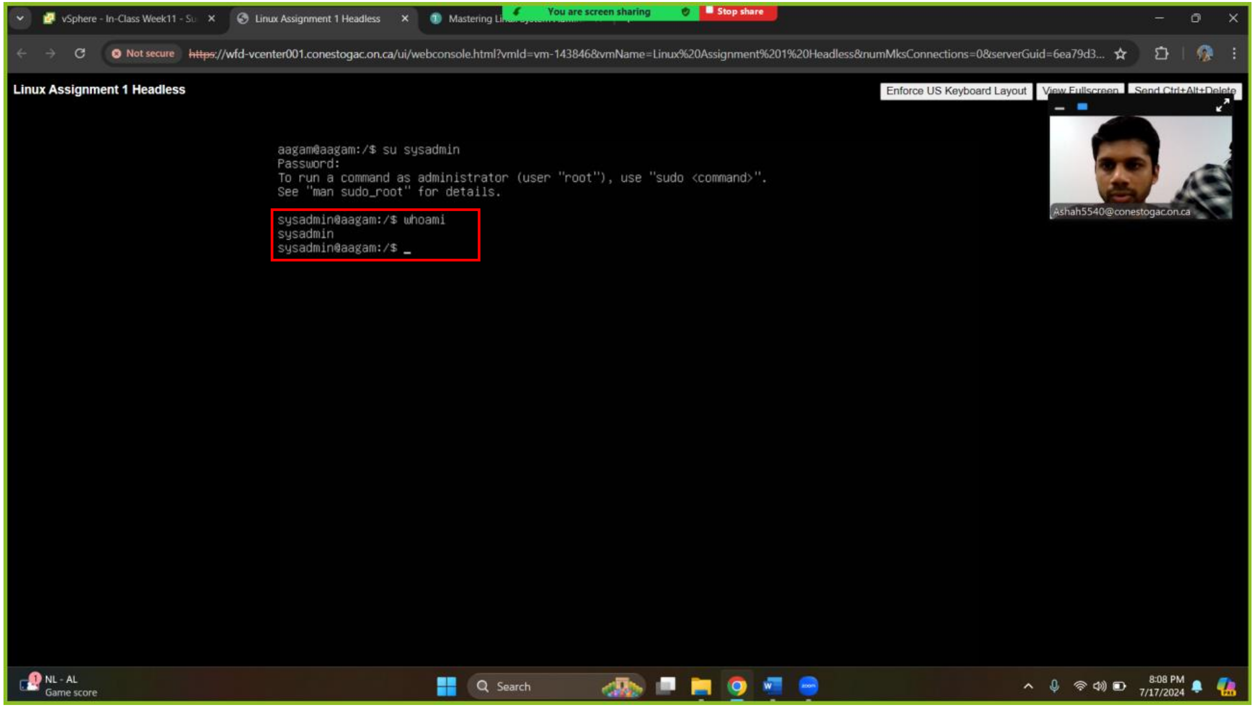
DETERMINING YOUR PRIVILEGE ELEVATION STATUS

1. Using your Ubuntu Linux distribution, log into the `sysadmin` account and enter the password you created for it.


vSphere - In-Class Week11 - Su
Linux Assignment 1 Headless
Mastering Lin
You are screen sharing
Stop share
Not secure
https://wfd-vcenter001.conestogac.on.ca/ui/webconsole.html?vmId=vm-143846&vmName=Linux%20Assignment%201%20Headless&numMksConnections=0&serverGuid=6ea79d3...
Linux Assignment 1 Headless
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Ashah5540@conestogac.on.ca
Sunset coming
8:57 PM
Search
8:07 PM
7/17/2024

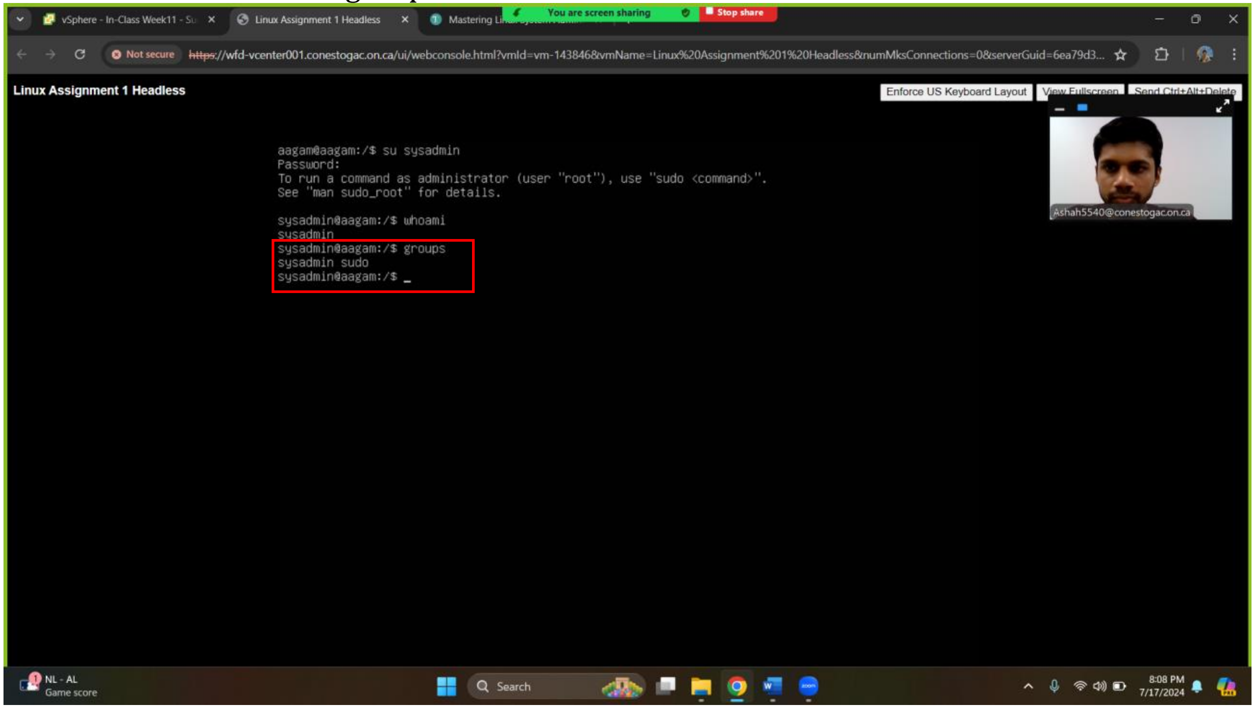
```
aagam@aagam:/$ su sysadmin
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

sysadmin@aagam:/$ _
```

2. Look at your account name by typing **whoami** and pressing Enter. The account name should be `sysadmin`.


vSphere - In-Class Week11 - Su
Linux Assignment 1 Headless
Mastering Li
You are screen sharing
Stop share
Not secure
https://wfd-vcenter001.conestogac.on.ca/ui/webconsole.html?vmId=vm-143846&vmName=Linux%20Assignment%201%20Headless&numMksConnections=0&serverGuid=6ea79d3...
Linux Assignment 1 Headless
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Ashah5540@conestogac.on.ca
NL - AL
Game score
Search
8:08 PM
7/17/2024

```
aagam@aagam:/$ su sysadmin
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

sysadmin@aagam:/$ whoami
sysadmin
sysadmin@aagam:/$ _
```

3. Determine the groups to which this account belongs by typing **groups** and pressing Enter. Record the group names.



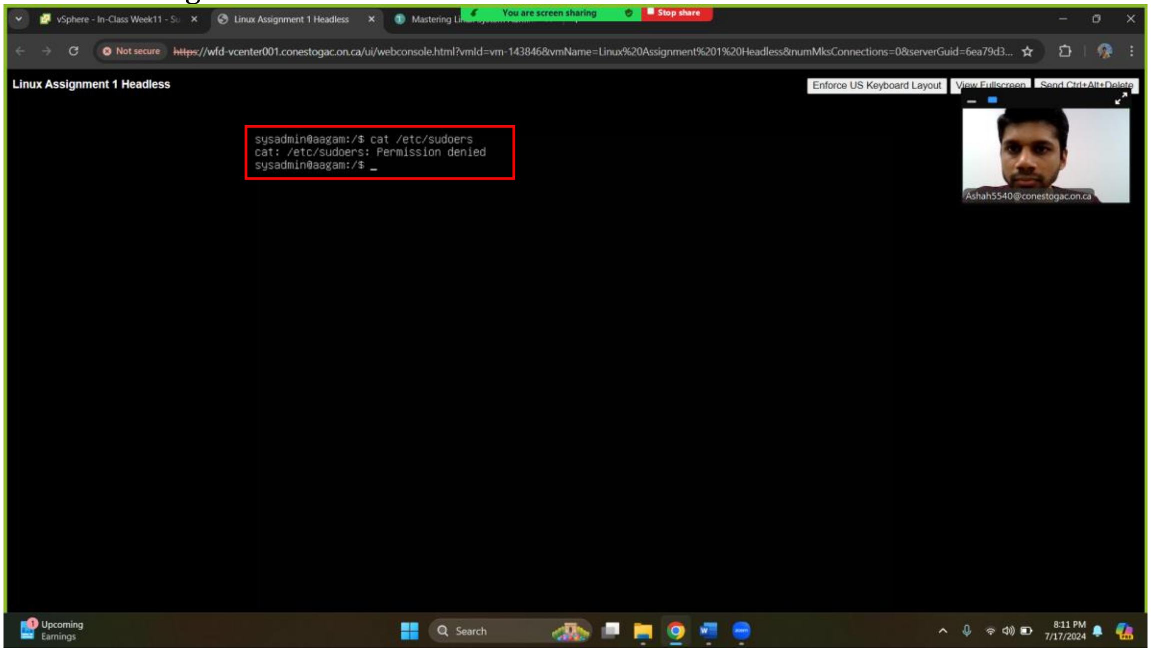
Linux Assignment 1 Headless
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Ashah5540@conestogac.on.ca

```
aagam@aagam:/$ su sysadmin
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

sysadmin@aagam:/$ whoami
sysadmin
sysadmin@aagam:/$ groups
sysadmin sudo
sysadmin@aagam:/$ _
```

4. Typically, Ubuntu Linux allows those users who belong to the group `sudo` to access full super user privileges. From the names you recorded in the previous step, determine if you belong to that group. Record your finding.

Yes, sysadmin is a user of group sudo

5. Try to display the `/etc/sudoers` file without using escalated privileges by typing **cat /etc/sudoers** and pressing Enter. You should receive a "permission denied" error message and not be able to view the file.

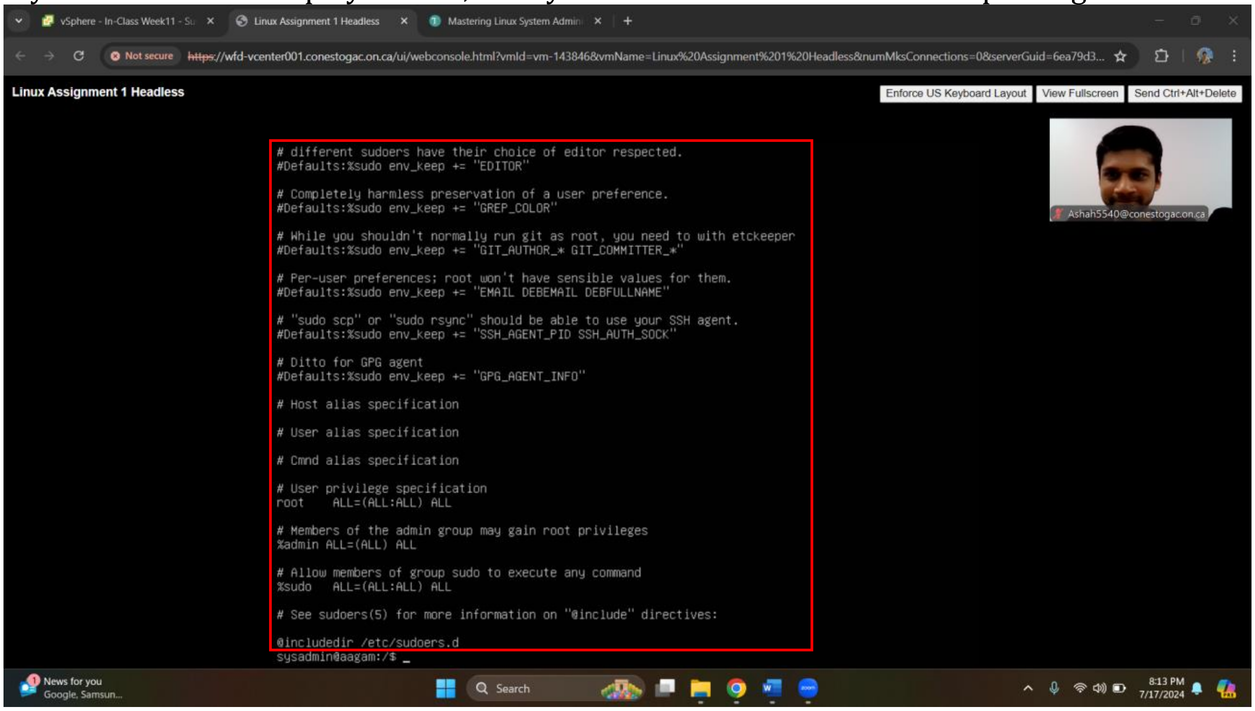


Linux Assignment 1 Headless
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Ashah5540@conestogac.on.ca

```
sysadmin@aagam:/$ cat /etc/sudoers
cat: /etc/sudoers: Permission denied
sysadmin@aagam:/$ _
```

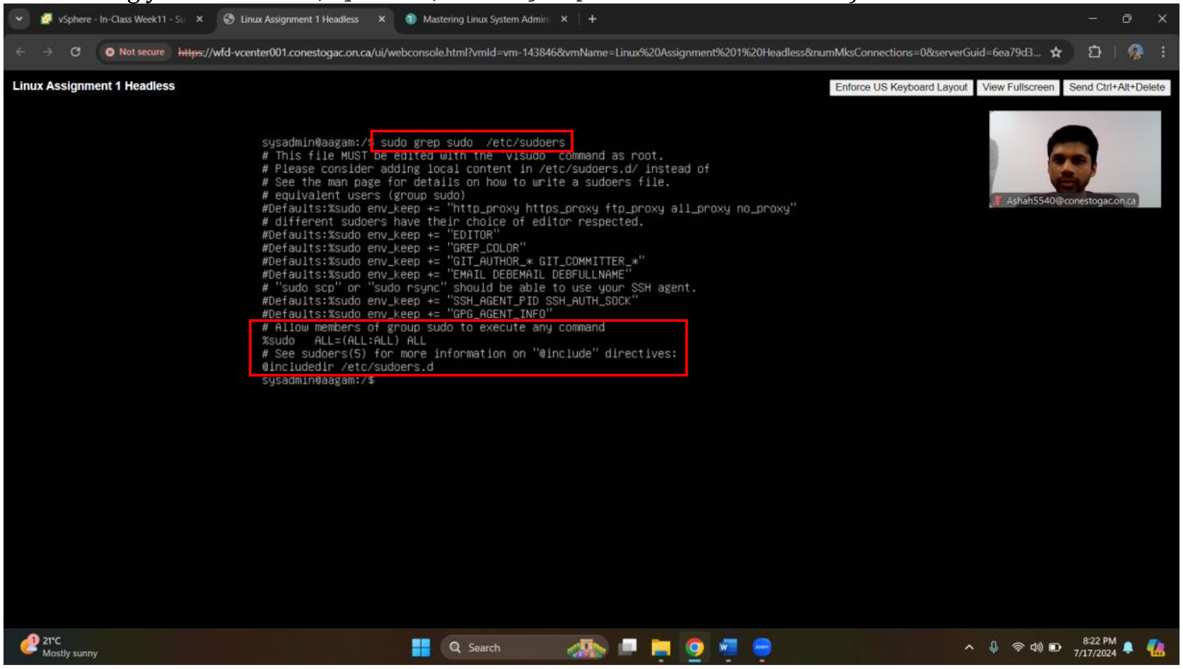
6. Now attempt to display the file by using escalated privileges by typing **sudo cat /etc/sudoers** and pressing Enter. If asked, enter your account's password. Record whether you were able to display the file.

If you were able to display the file, then you do have access to escalated privileges.



```
# different sudoers have their choice of editor respected.
#Defaults:%sudo env_keep += "EDITOR"

# Completely harmless preservation of a user preference.
#Defaults:%sudo env_keep += "GREP_COLOR"

# While you shouldn't normally run git as root, you need to with etckeeper
#Defaults:%sudo env_keep += "GIT_AUTHOR_* GIT_COMMITTER_*"

# Per-user preferences; root won't have sensible values for them.
#Defaults:%sudo env_keep += "EMAIL DEBEMAIL DEBFULLNAME"

# "sudo scp" or "sudo rsync" should be able to use your SSH agent.
#Defaults:%sudo env_keep += "SSH_AGENT_PID SSH_AUTH_SOCK"

# Ditto for GPG agent
#Defaults:%sudo env_keep += "GPG_AGENT_INFO"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "@include" directives:

@includedir /etc/sudoers.d
sysadmin@aagam:/$ _
```

7. Assuming you do have access to escalated privileges, use the group names you recorded in step 3 to search for a record in the `/etc/sudoers` file that shows what escalated privileges you are allowed to use, by typing **grep *group-name* `/etc/sudoers`** and pressing Enter. Continue to enter this command until `grep` finds a record for one of your groups, if any. (If you cannot find a group record, try substituting your username, `sysadmin`, for the *`group-name`* in the command.)



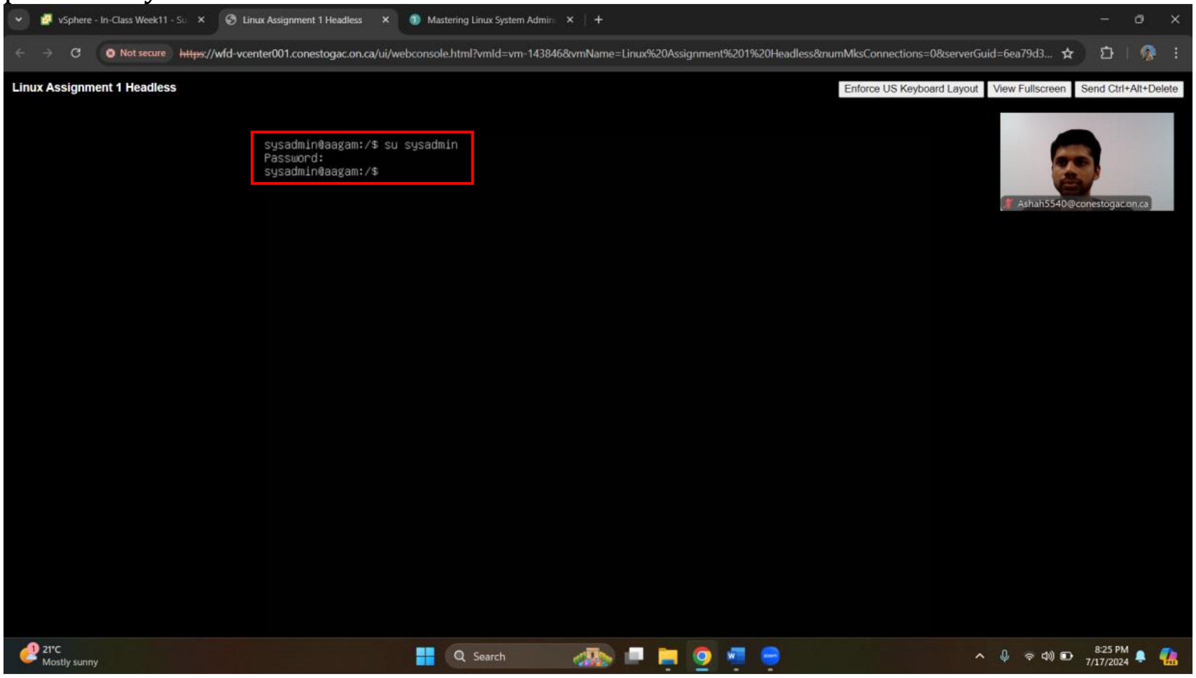
```
sysadmin@aagam:/$ sudo grep sudo  /etc/sudoers
# This file MUST be edited with the 'visudo' command as root.
# Please consider adding local content in /etc/sudoers.d/ instead of
# See the man page for details on how to write a sudoers file.
# equivalent users (group sudo)
#Defaults:%sudo env_keep += "http_proxy https_proxy ftp_proxy all_proxy no_proxy"
# different sudoers have their choice of editor respected.
#Defaults:%sudo env_keep += "EDITOR"
#Defaults:%sudo env_keep += "GREP_COLOR"
#Defaults:%sudo env_keep += "GIT_AUTHOR_* GIT_COMMITTER_*"
#Defaults:%sudo env_keep += "EMAIL DEBEMAIL DEBFULLNAME"
# "sudo scp" or "sudo rsync" should be able to use your SSH agent.
#Defaults:%sudo env_keep += "SSH_AGENT_PID SSH_AUTH_SOCK"
#Defaults:%sudo env_keep += "GPG_AGENT_INFO"
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
# See sudoers(5) for more information on "@include" directives:
@includedir /etc/sudoers.d
sysadmin@aagam:/$
```

2. Week 11 Slide 13

Complete the Real World Scenario: Using OpenSSH to Log Into a System in Ch 17
Also, generate a user authentication key, use ssh-copy-id to transfer to a remote server, and remote login using the key.

USING OpenSSH TO LOG INTO A SYSTEM

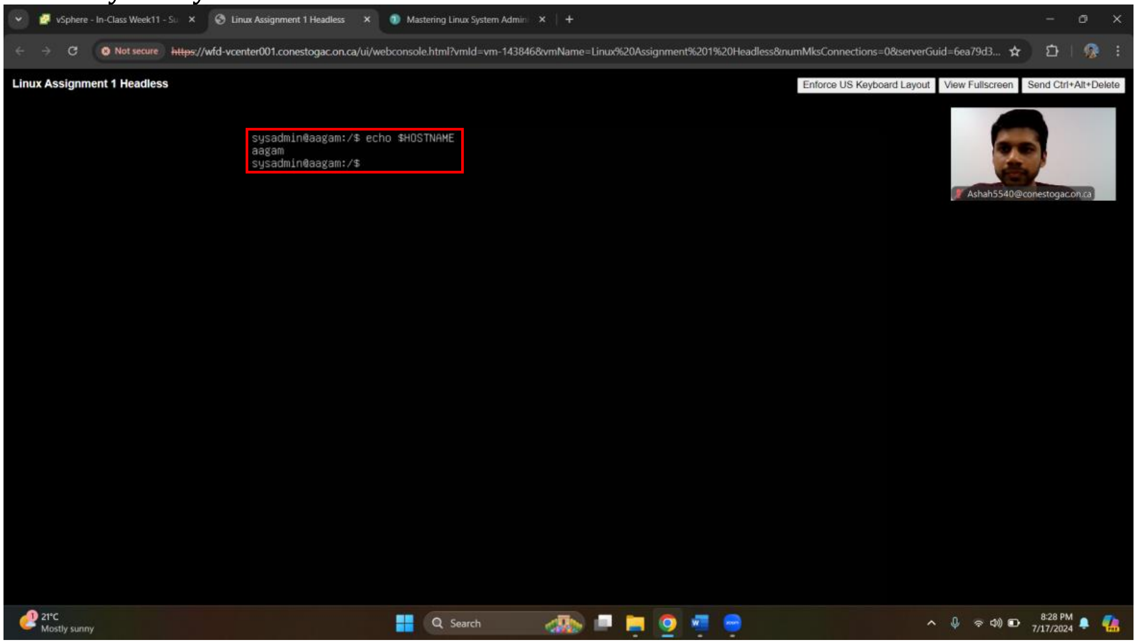
1. Using your Ubuntu Linux distribution, log into the `sysadmin` account and the password you created for it.



vSphere - In-Class Week11 - Su
Linux Assignment 1 Headless
Mastering Linux System Admin
Not secure
https://wfd-vcenter001.conestogac.on.ca/ui/webconsole.html?vmId=vm-143846&vmName=Linux%20Assignment%201%20Headless&numMksConnections=0&serverGuid=6ea79d3...
Linux Assignment 1 Headless
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Ashah5540@conestogac.on.ca
21°C
Mostly sunny
Search
8:25 PM
7/17/2024

```
sysadmin@aagam:/$ su sysadmin
Password:
sysadmin@aagam:/$
```

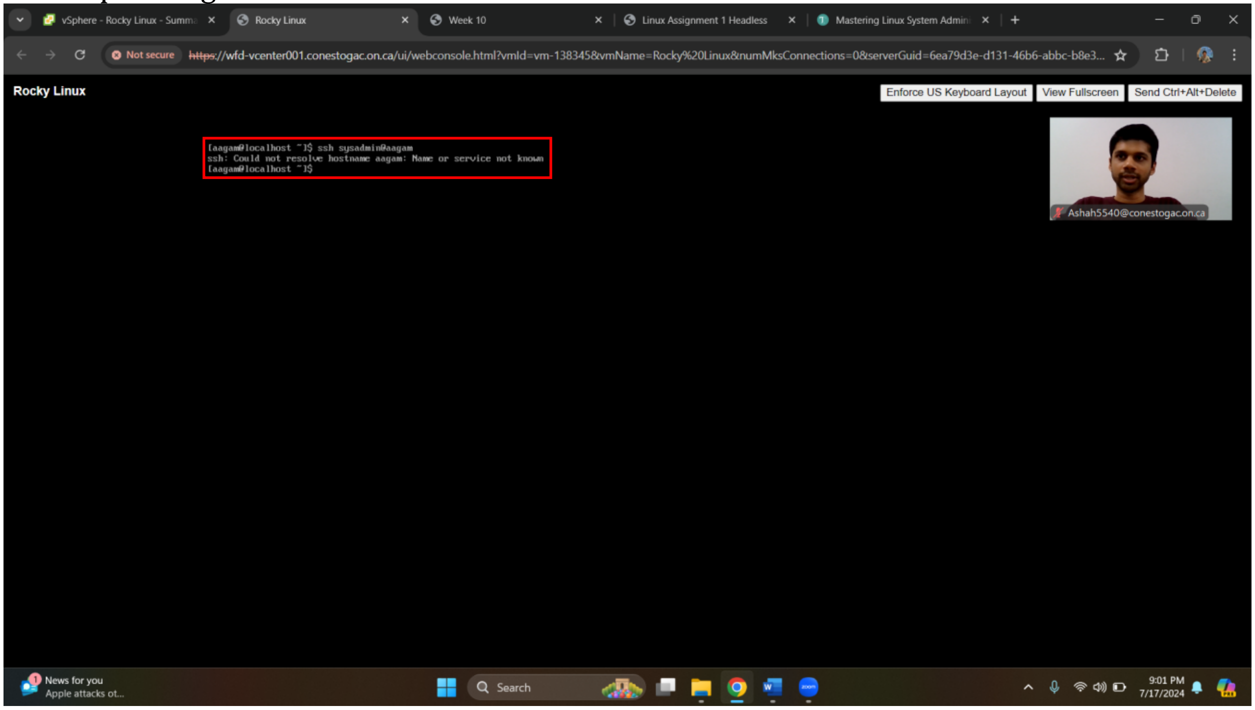
2. Determine your system's hostname by typing **echo $HOSTNAME** and pressing Enter. Record your system's hostname.



vSphere - In-Class Week11 - Su
Linux Assignment 1 Headless
Mastering Linux System Admin
Not secure
https://wfd-vcenter001.conestogac.on.ca/ui/webconsole.html?vmId=vm-143846&vmName=Linux%20Assignment%201%20Headless&numMksConnections=0&serverGuid=6ea79d3...
Linux Assignment 1 Headless
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Ashah5540@conestogac.on.ca
21°C
Mostly sunny
Search
8:28 PM
7/17/2024

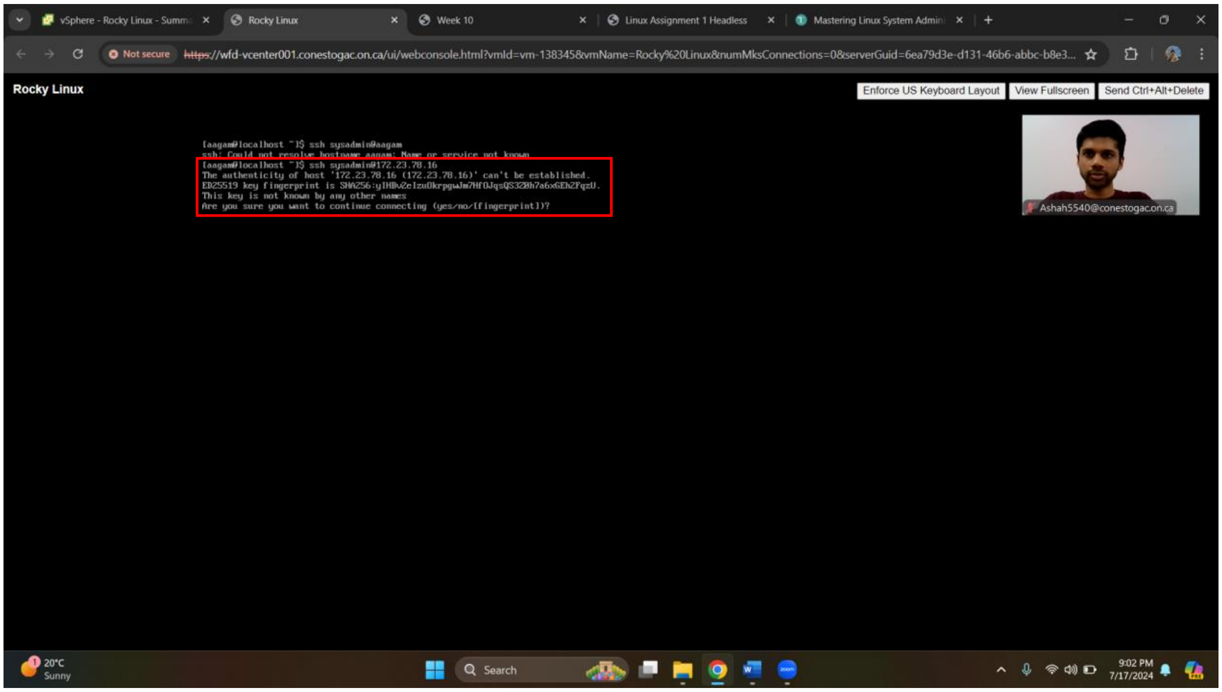
```
sysadmin@aagam:/$ echo $HOSTNAME
aagam
sysadmin@aagam:/$
```

3. You will be logging into the current system by going out onto the network and back into the system via OpenSSH. Do this by typing **ssh sysadmin@ *hostname*** , where *hostname* is the system's hostname you recorded in the previous step, and pressing Enter.



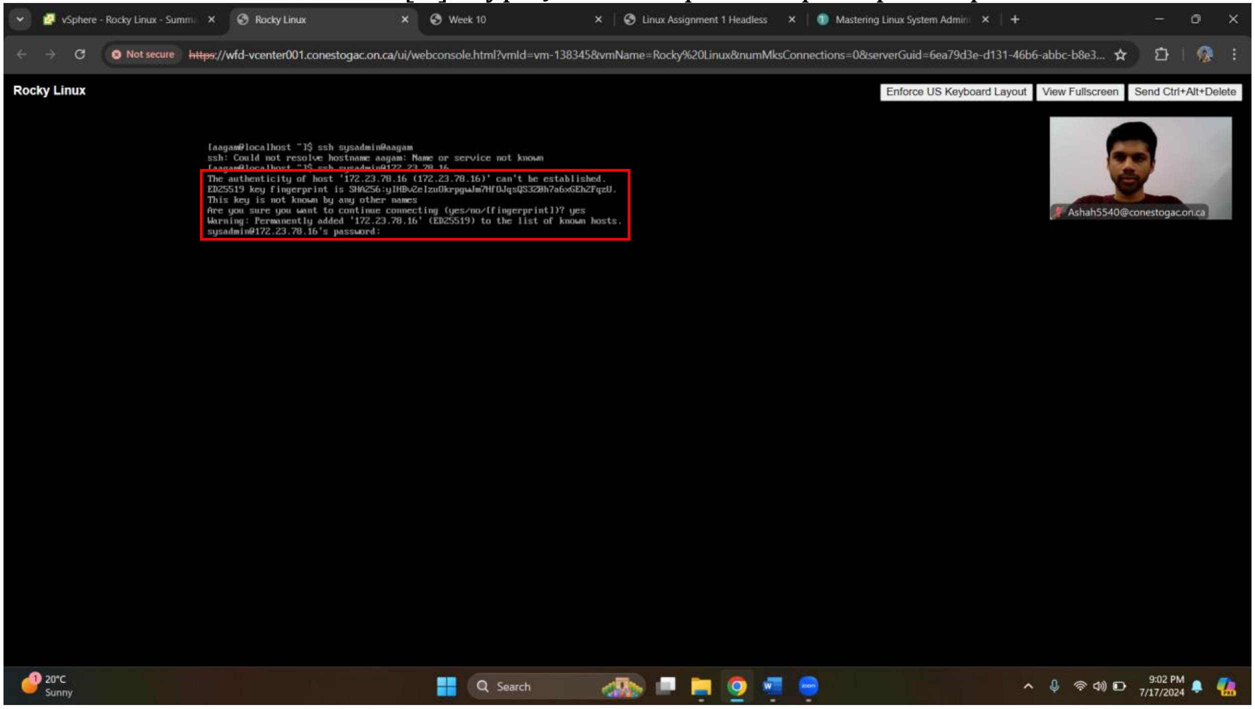
```
[aagam@localhost ~]$ ssh sysadmin@aagam
ssh: Could not resolve hostname aagam: Name or service not known
[aagam@localhost ~]$
```

Note that if you have problems in this step, you may need to enter the system's IP address instead of its hostname. If after using the IP address you continue to have problems, there may be a firewall setting blocking your access. (Firewalls are covered later in this chapter.)



```
[aagam@localhost ~]$ ssh sysadmin@aagam
ssh: Could not resolve hostname aagam: Name or service not known
[aagam@localhost ~]$ ssh sysadmin@172.23.78.16
The authenticity of host '172.23.78.16 (172.23.78.16)' can't be established.
ED25519 key fingerprint is SHA256:yIHDv2cIzuOkrpgwJm7HfOJqsQS328h7a6xGEh2FqzU.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

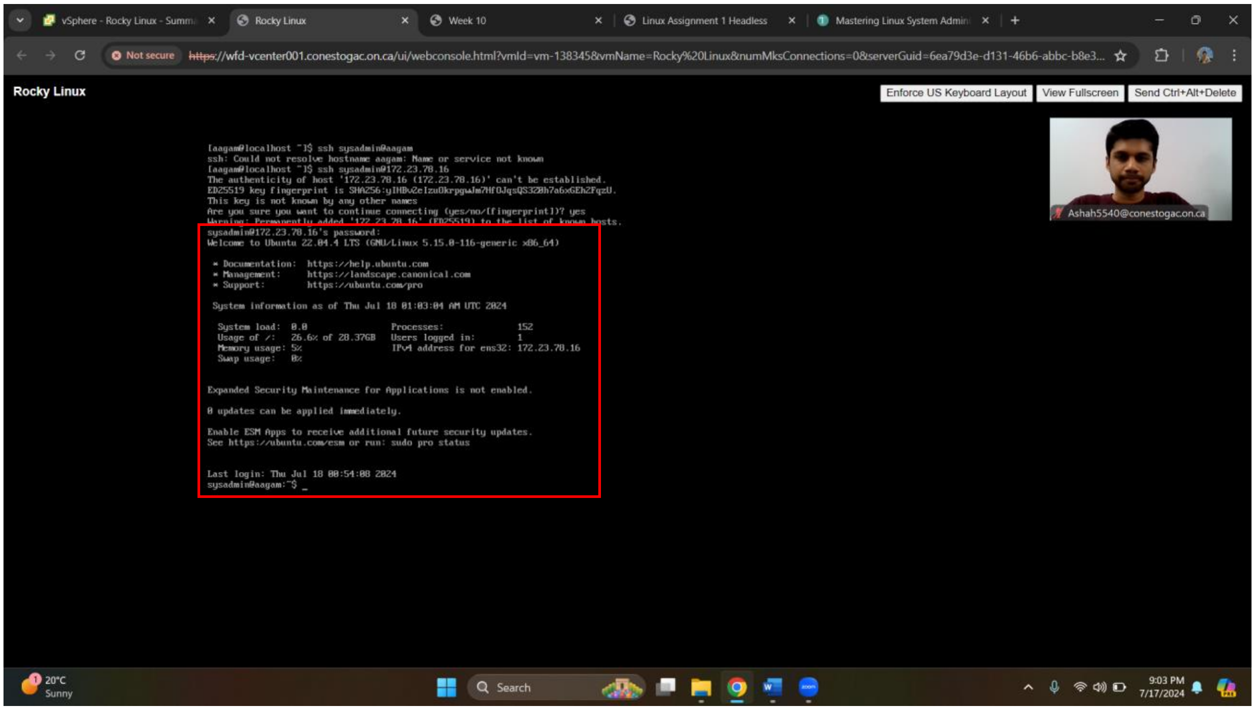
4. If you receive a message stating something similar to “The authenticity of host […] cannot be established […],” type **yes** at the question prompt and press Enter.


vSphere - Rocky Linux - Summ
Rocky Linux
Week 10
Linux Assignment 1 Headless
Mastering Linux System Admin
Not secure
~~https~~://wfd-vcenter001.conestogac.on.ca/ui/webconsole.html?vmId=vm-138345&vmName=Rocky%20Linux&numMksConnections=0&serverGuid=6ea79d3e-d131-46b6-abbc-b8e3...
Rocky Linux
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Ashah5540@conestogac.on.ca
20°C
Sunny
Search
9:02 PM
7/17/2024

```
[aagam@localhost ~]$ ssh sysadmin@aagam
ssh: Could not resolve hostname aagam: Name or service not known
[aagam@localhost ~]$ ssh sysadmin@172.23.78.16
The authenticity of host '172.23.78.16 (172.23.78.16)' can't be established.
ED25519 key fingerprint is SHA256:yIHBv2eIzuOkrpgwJm7HfOJqsQS320h7a6xGEh2FqzU.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.23.78.16' (ED25519) to the list of known hosts.
sysadmin@172.23.78.16's password:
```

5. At the password prompt, enter the password for the `sysadmin` account.

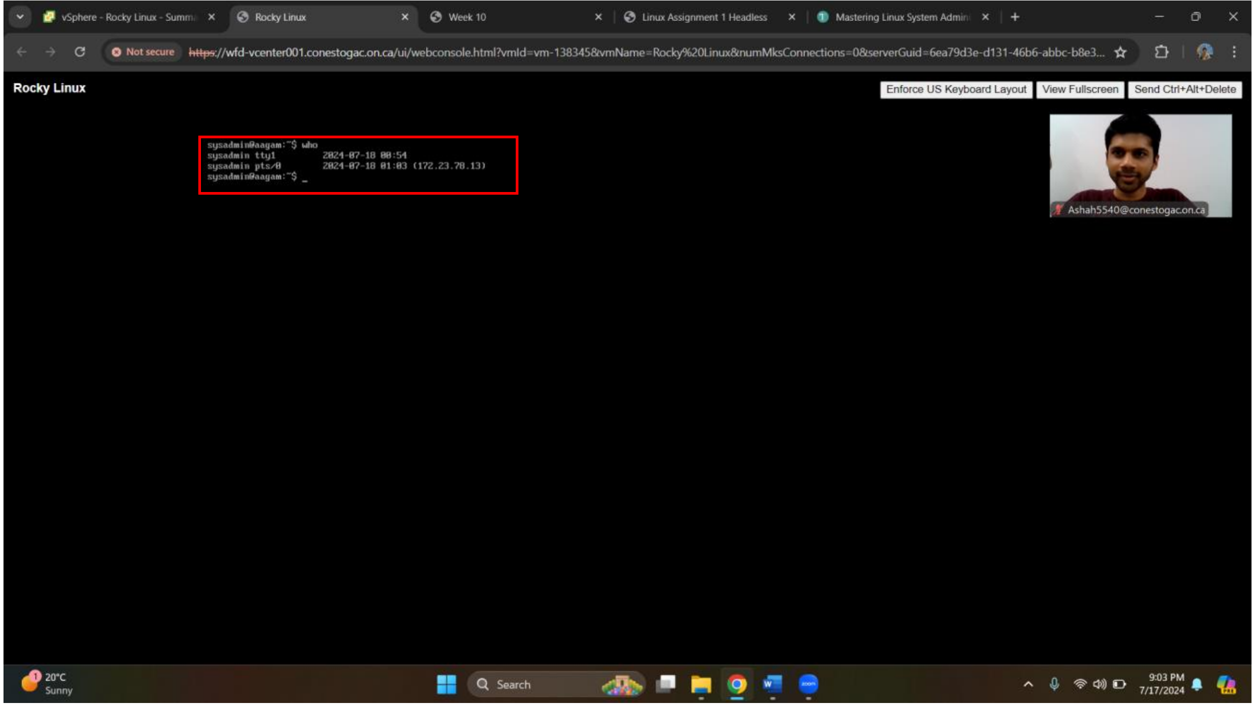
   If you receive a prompt, you have successfully used OpenSSH to log into a system. Congratulations.


vSphere - Rocky Linux - Summ
Rocky Linux
Week 10
Linux Assignment 1 Headless
Mastering Linux System Admin
Not secure
~~https~~://wfd-vcenter001.conestogac.on.ca/ui/webconsole.html?vmId=vm-138345&vmName=Rocky%20Linux&numMksConnections=0&serverGuid=6ea79d3e-d131-46b6-abbc-b8e3...
Rocky Linux
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Ashah5540@conestogac.on.ca
20°C
Sunny
Search
9:03 PM
7/17/2024

```
[aagam@localhost ~]$ ssh sysadmin@aagam
ssh: Could not resolve hostname aagam: Name or service not known
[aagam@localhost ~]$ ssh sysadmin@172.23.78.16
The authenticity of host '172.23.78.16 (172.23.78.16)' can't be established.
ED25519 key fingerprint is SHA256:yIHBv2eIzuOkrpgwJm7HfOJqsQS320h7a6xGEh2FqzU.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.23.78.16' (ED25519) to the list of known hosts.
sysadmin@172.23.78.16's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-116-generic x86_64)

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

 System information as of Thu Jul 18 01:03:04 AM UTC 2024

  System load:  0.0               Processes:              152
  Usage of /:   26.6% of 28.37GB   Users logged in:        1
  Memory usage: 5%                IPv4 address for ens32: 172.23.78.16
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


Last login: Thu Jul 18 00:54:08 2024
sysadmin@aagam:~$ _
```

6. At the command prompt, type **who** to see all the accounts that are currently logged into the system and from what IP address they have accessed the system, if any.

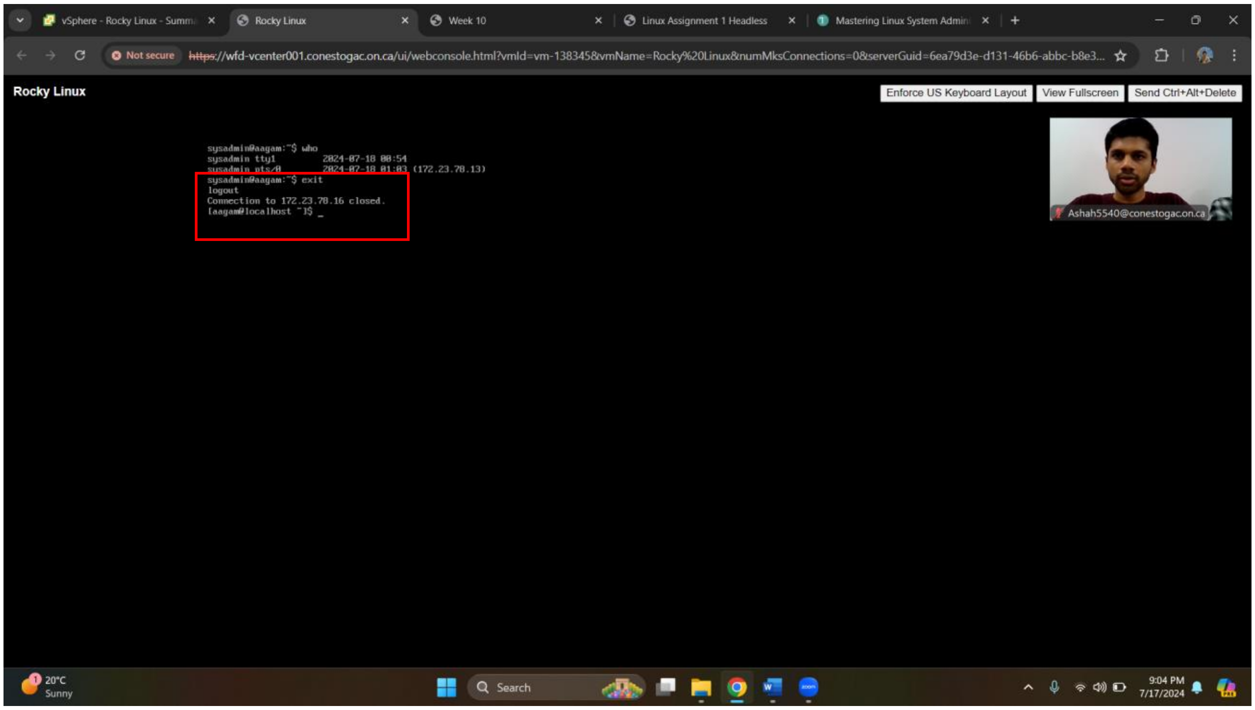
More than likely, you will see that you accessed this system from `127.0.0.1` (IPv4) or `::1` (IPv6).



vSphere - Rocky Linux - Summ
Rocky Linux
Week 10
Linux Assignment 1 Headless
Mastering Linux System Admin
Not secure
https://wfd-vcenter001.conestogac.on.ca/ui/webconsole.html?vmId=vm-138345&vmName=Rocky%20Linux&numMksConnections=0&serverGuid=6ea79d3e-d131-46b6-abbc-b8e3...
Rocky Linux
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Ashah5540@conestogac.on.ca
20°C
Sunny
Search
9:03 PM
7/17/2024

```
sysadmin@aagam:~$ who
sysadmin tty1         2024-07-18 00:54
sysadmin pts/0        2024-07-18 01:03 (172.23.78.13)
sysadmin@aagam:~$ _
```

7. Type **exit** and press Enter to log out of the connection.



vSphere - Rocky Linux - Summ
Rocky Linux
Week 10
Linux Assignment 1 Headless
Mastering Linux System Admin
Not secure
https://wfd-vcenter001.conestogac.on.ca/ui/webconsole.html?vmId=vm-138345&vmName=Rocky%20Linux&numMksConnections=0&serverGuid=6ea79d3e-d131-46b6-abbc-b8e3...
Rocky Linux
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Ashah5540@conestogac.on.ca
20°C
Sunny
Search
9:04 PM
7/17/2024

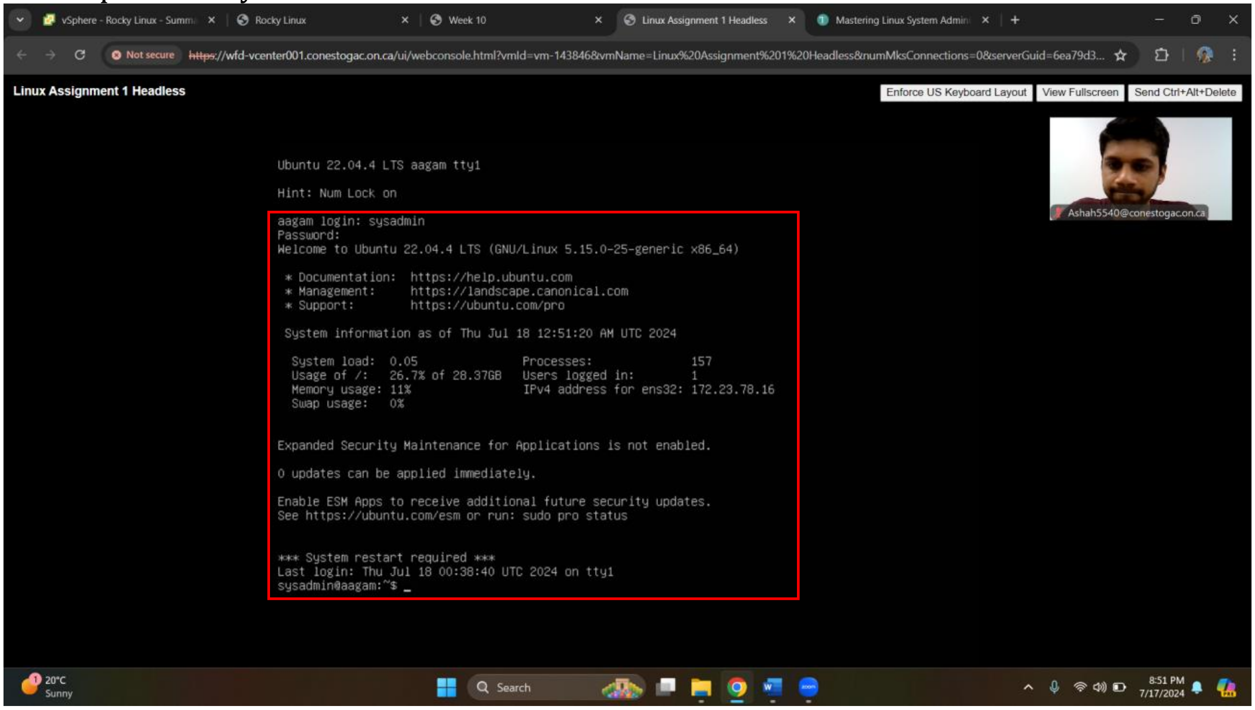
```
sysadmin@aagam:~$ who
sysadmin tty1         2024-07-18 00:54
sysadmin pts/0        2024-07-18 01:03 (172.23.78.13)
sysadmin@aagam:~$ exit
logout
Connection to 172.23.78.16 closed.
[aagam@localhost ~]$ _
```

3. Week 11 Slide 22

Complete the Real World Scenario: Viewing and Configuring UFW in Ch17

VIEWING AND CONFIGURING UFW

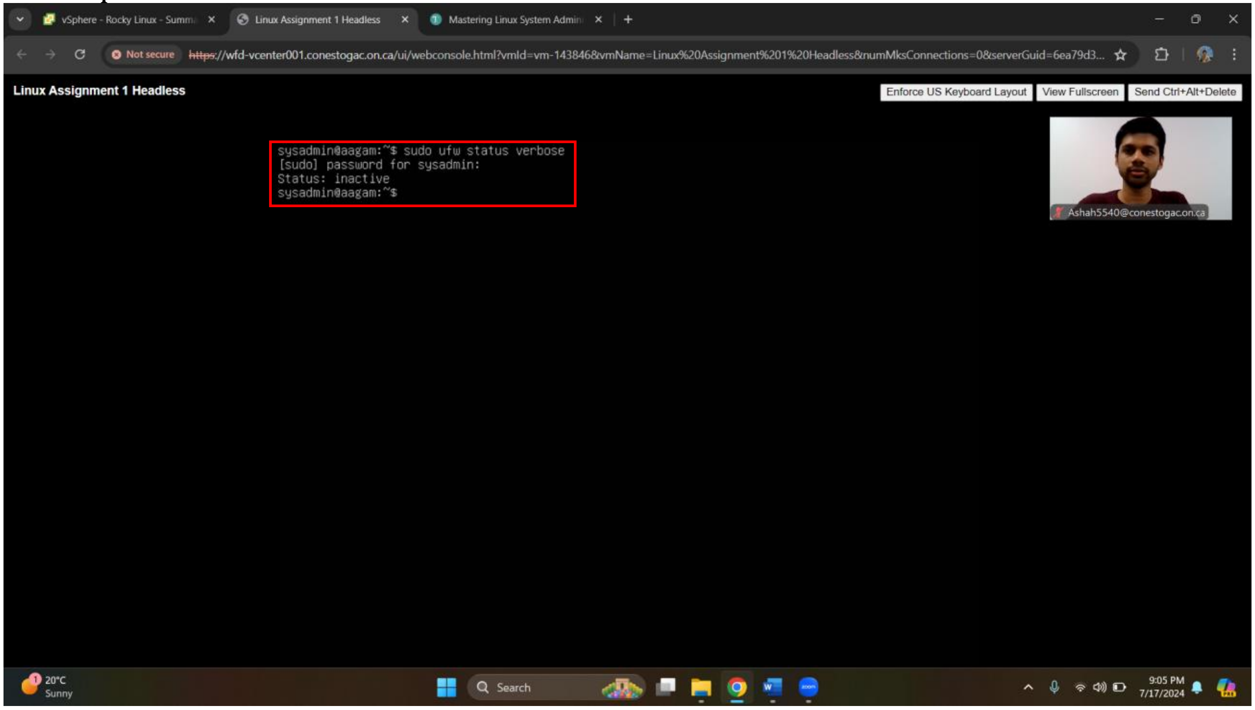
1. Using your Ubuntu Linux distribution, log into the `sysadmin` account and enter the password you created for it.



Linux Assignment 1 Headless

```
Ubuntu 22.04.4 LTS aagam tty1

Hint: Num Lock on

aagam login: sysadmin
Password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-25-generic x86_64)

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

 System information as of Thu Jul 18 12:51:20 AM UTC 2024

  System load:  0.05              Processes:             157
  Usage of /:   26.7% of 28.37GB   Users logged in:       1
  Memory usage: 11%               IPv4 address for ens32: 172.23.78.16
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


*** System restart required ***
Last login: Thu Jul 18 00:38:40 UTC 2024 on tty1
sysadmin@aagam:~$ _
```

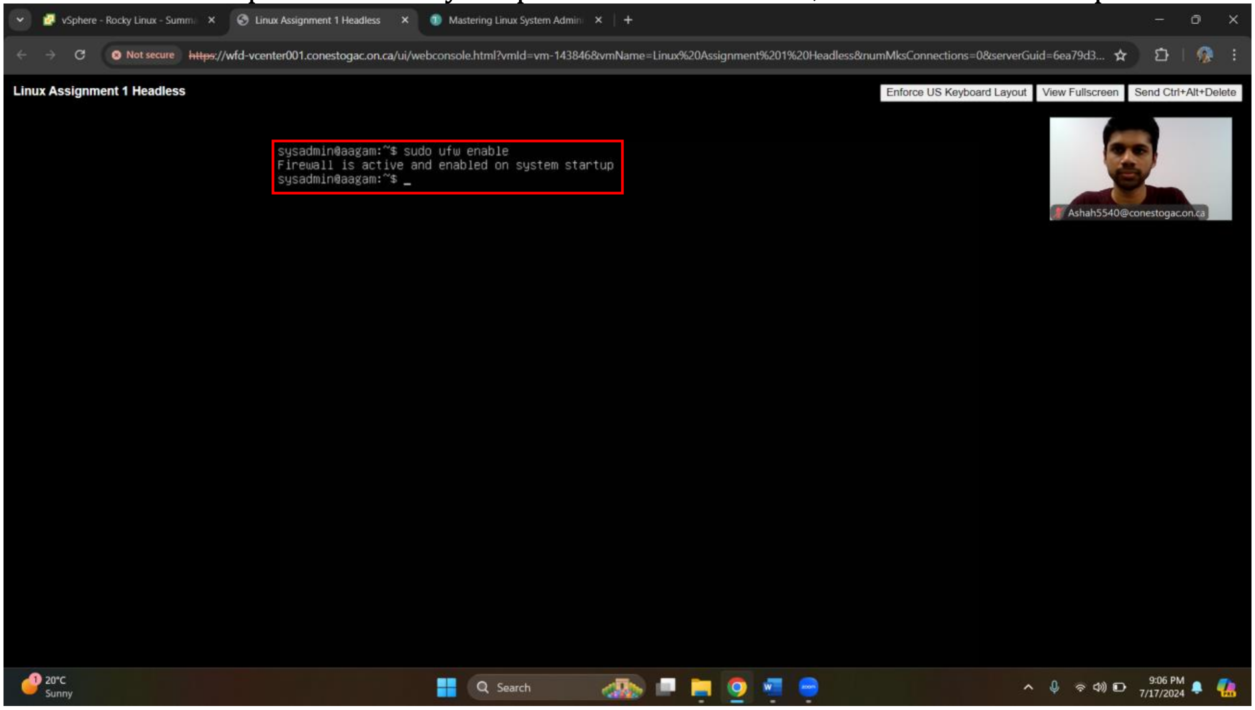
2. Determine if your system's UFW firewall application is enabled by typing **sudo ufw status verbose** and pressing Enter. If your password is asked for, enter the account's password. Record the status.



Linux Assignment 1 Headless

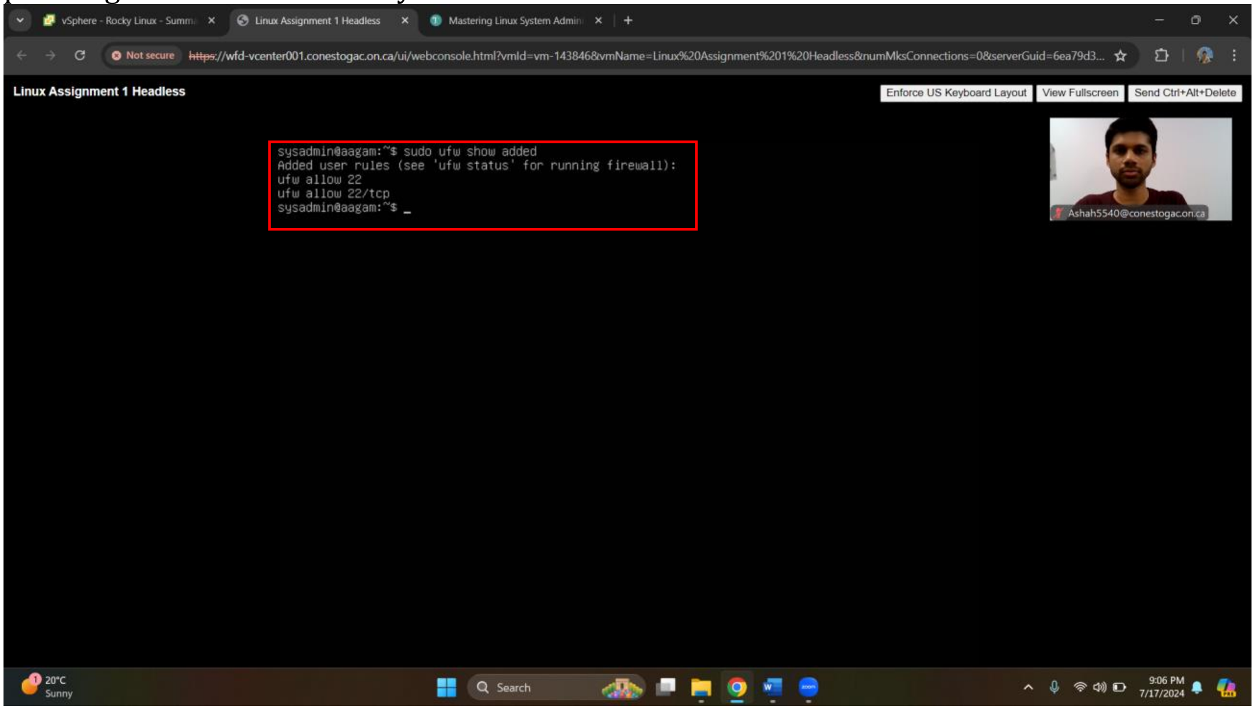
```
sysadmin@aagam:~$ sudo ufw status verbose
[sudo] password for sysadmin:
Status: inactive
sysadmin@aagam:~$
```

3. If the status you determined in the previous step is `inactive`, type **sudo ufw enable** and press Enter. If your password is asked for, enter the account's password.


vSphere - Rocky Linux - Summ
Linux Assignment 1 Headless
Mastering Linux System Admin
Not secure
https://wfd-vcenter001.conestogac.on.ca/ui/webconsole.html?vmId=vm-143846&vmName=Linux%20Assignment%201%20Headless&numMksConnections=0&serverGuid=6ea79d3...
Linux Assignment 1 Headless
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Ashah5540@conestogac.on.ca
20°C
Sunny
Search
9:06 PM
7/17/2024

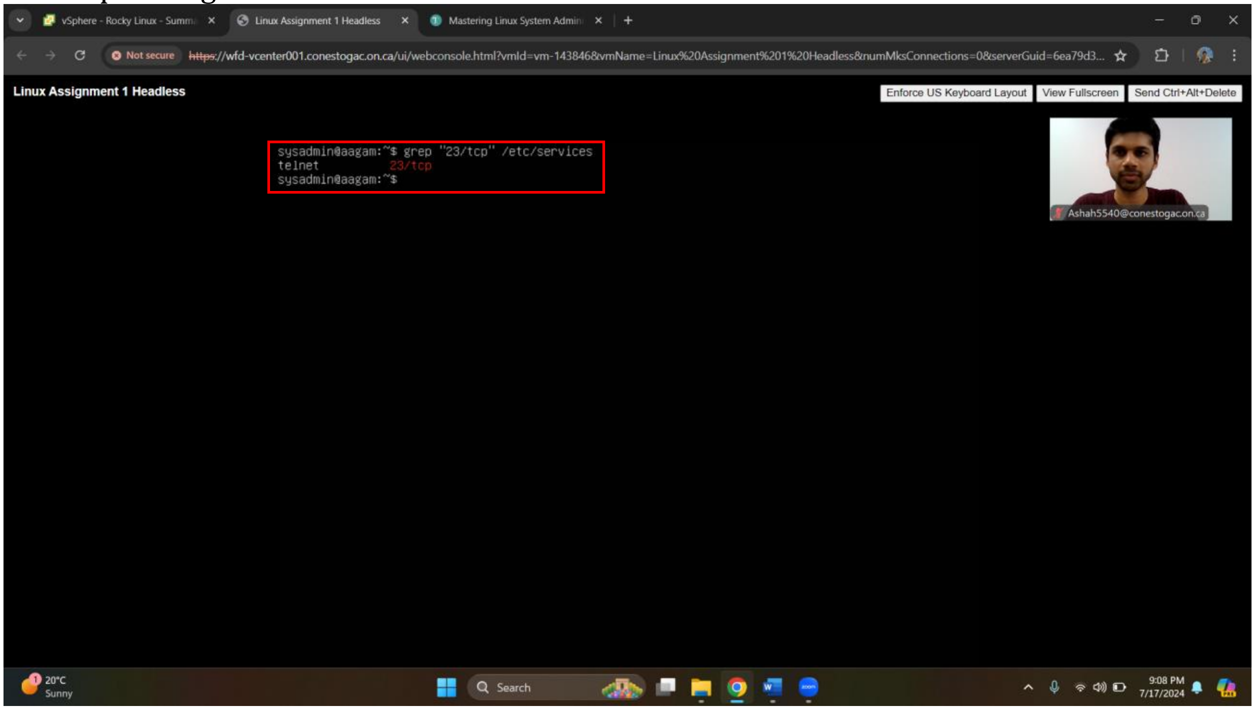
```
sysadmin@aagam:~$ sudo ufw enable
Firewall is active and enabled on system startup
sysadmin@aagam:~$ _
```

4. View any added rules (there may be none) in UFW by typing **sudo ufw show added** and pressing Enter. Record what you find.


vSphere - Rocky Linux - Summ
Linux Assignment 1 Headless
Mastering Linux System Admin
Not secure
https://wfd-vcenter001.conestogac.on.ca/ui/webconsole.html?vmId=vm-143846&vmName=Linux%20Assignment%201%20Headless&numMksConnections=0&serverGuid=6ea79d3...
Linux Assignment 1 Headless
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Ashah5540@conestogac.on.ca
20°C
Sunny
Search
9:06 PM
7/17/2024

```
sysadmin@aagam:~$ sudo ufw show added
Added user rules (see 'ufw status' for running firewall):
ufw allow 22
ufw allow 22/tcp
sysadmin@aagam:~$ _
```

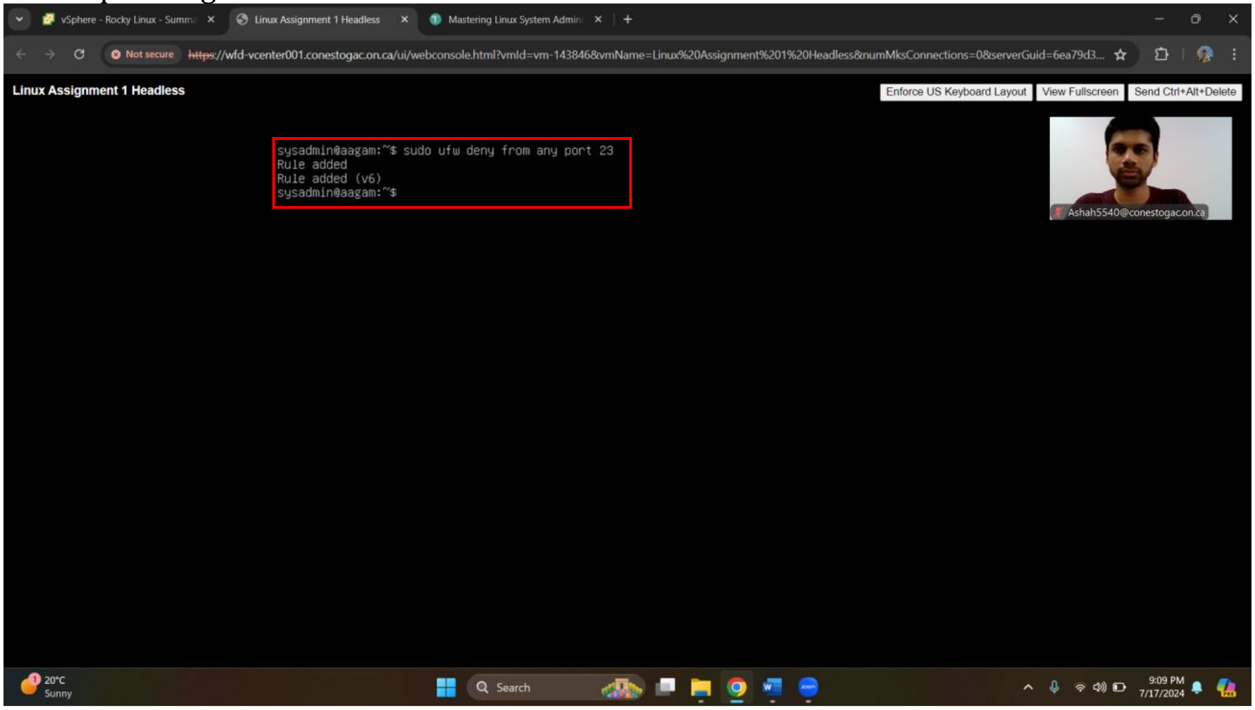
5. Determine what service may use port 23 by typing **grep "23/tcp" /etc/services** and pressing Enter. Record the service name.



Linux Assignment 1 Headless
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Ashah5540@conestogac.on.ca
9:08 PM
7/17/2024

```
sysadmin@aagam:~$ grep "23/tcp" /etc/services
telnet          23/tcp
sysadmin@aagam:~$
```

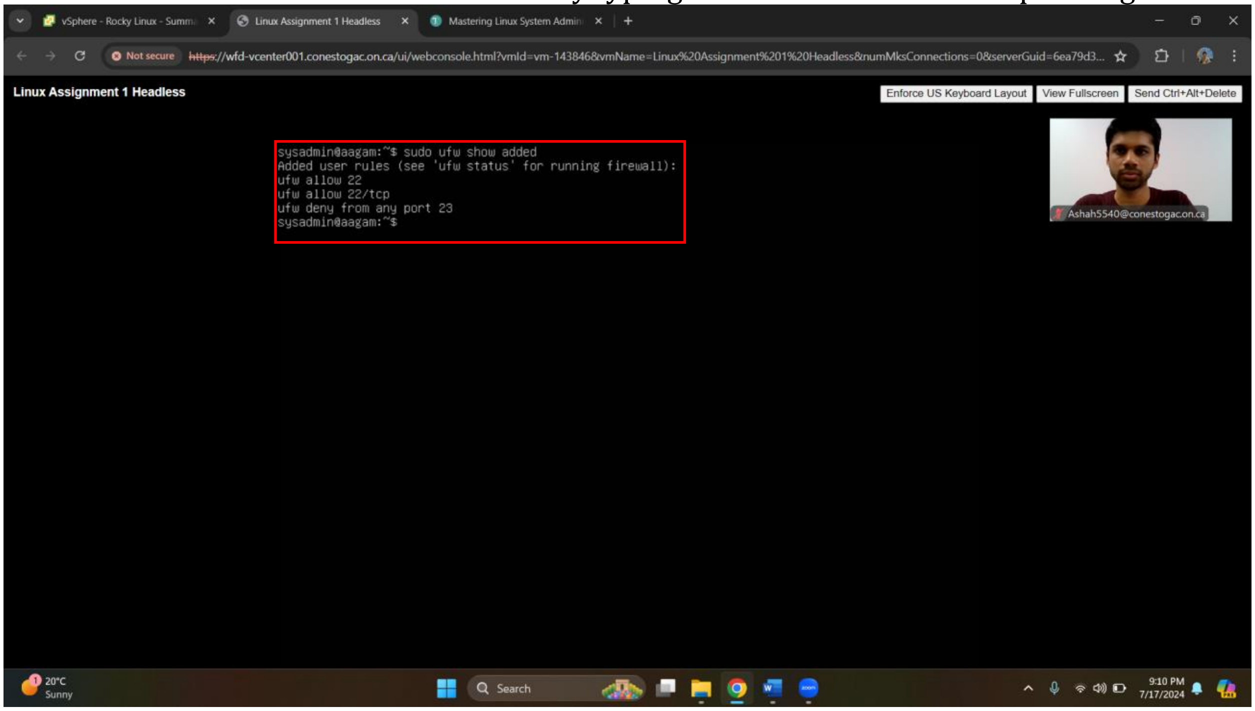
6. Block the service using port 23 you discovered in the previous step from any incoming network traffic via UFW by typing **sudo ufw deny from any port 23** and pressing Enter.



Linux Assignment 1 Headless
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Ashah5540@conestogac.on.ca
9:09 PM
7/17/2024

```
sysadmin@aagam:~$ sudo ufw deny from any port 23
Rule added
Rule added (v6)
sysadmin@aagam:~$
```

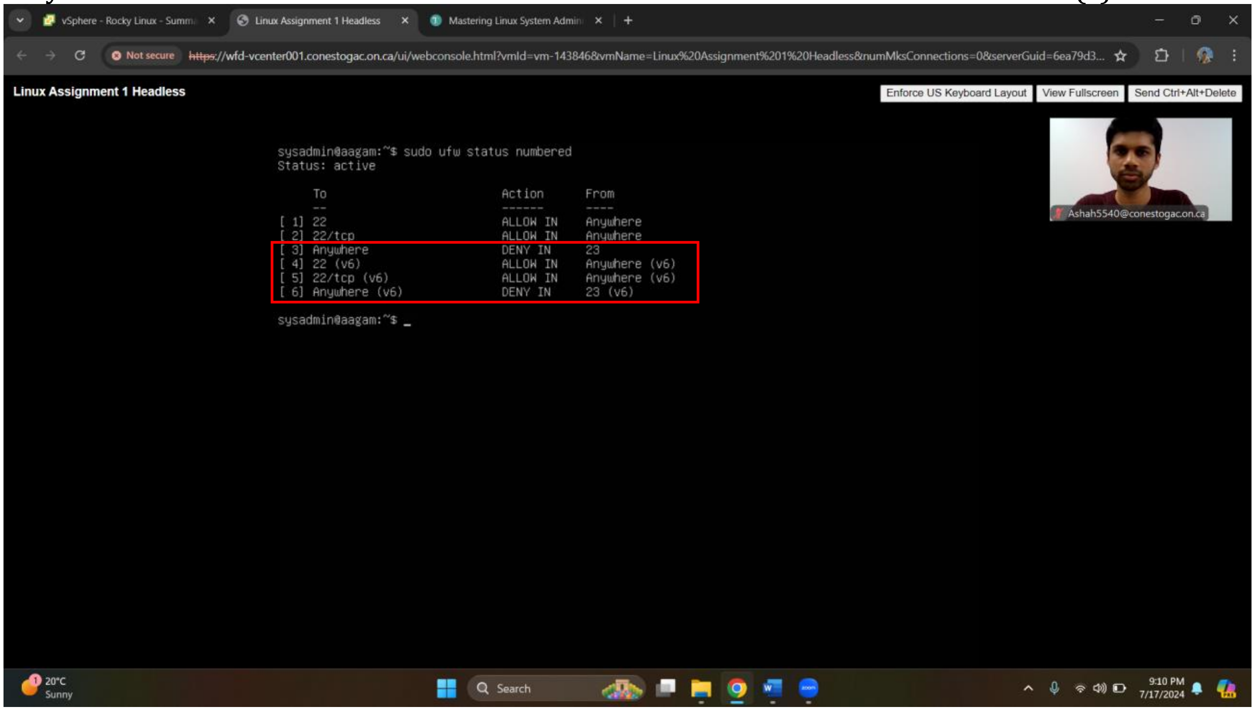
7. See if the rule was added to UFW by typing **sudo ufw show added** and pressing Enter.



vSphere - Rocky Linux - Summ
Linux Assignment 1 Headless
Mastering Linux System Admin
Not secure
https://wfd-vcenter001.conestogac.on.ca/ui/webconsole.html?vmId=vm-1438468vmName=Linux%20Assignment%201%20Headless&numMksConnections=0&serverGuid=6ea79d3...
Linux Assignment 1 Headless
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Ashah5540@conestogac.on.ca
20°C
Sunny
Search
9:10 PM
7/17/2024

```
sysadmin@aagam:~$ sudo ufw show added
Added user rules (see 'ufw status' for running firewall):
ufw allow 22
ufw allow 22/tcp
ufw deny from any port 23
sysadmin@aagam:~$
```

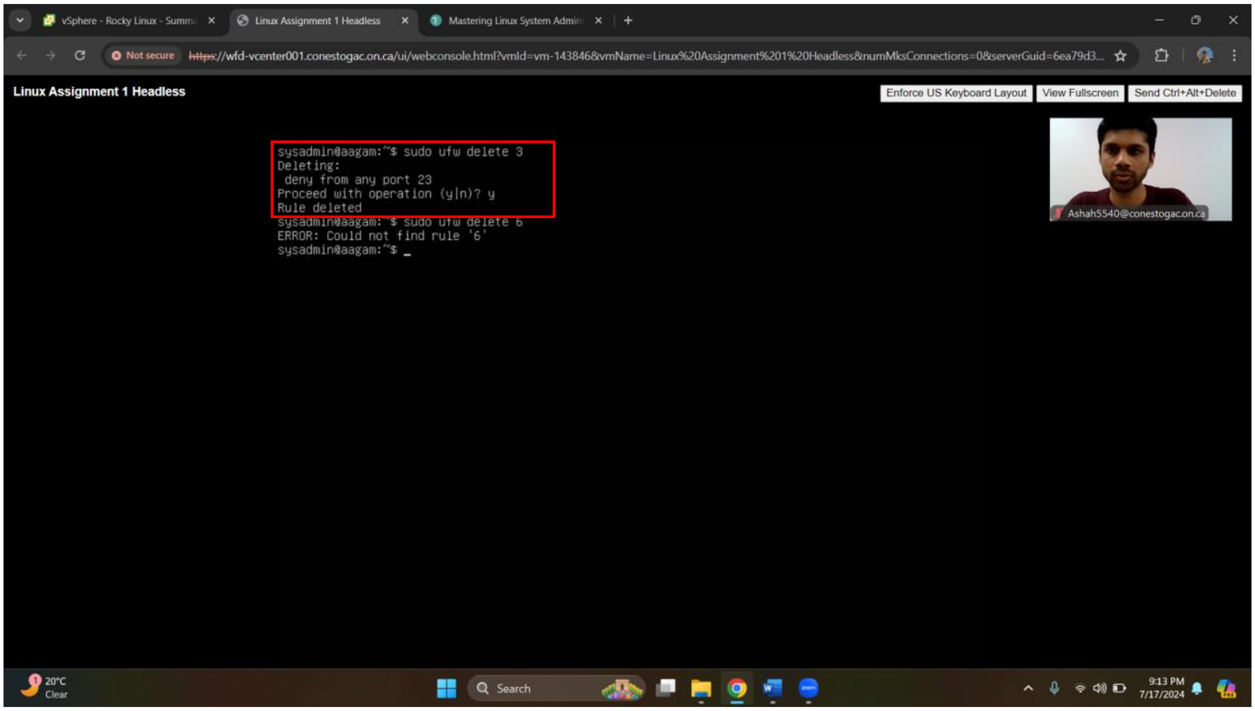
8. Now determine your new rule's number by typing **sudo ufw status numbered** and pressing Enter. The rule number will appear in the first column within brackets. You may see two different rules—one for IPv4 and one for IPv6. Record its number(s).



vSphere - Rocky Linux - Summ
Linux Assignment 1 Headless
Mastering Linux System Admin
Not secure
https://wfd-vcenter001.conestogac.on.ca/ui/webconsole.html?vmId=vm-1438468vmName=Linux%20Assignment%201%20Headless&numMksConnections=0&serverGuid=6ea79d3...
Linux Assignment 1 Headless
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Ashah5540@conestogac.on.ca
20°C
Sunny
Search
9:10 PM
7/17/2024

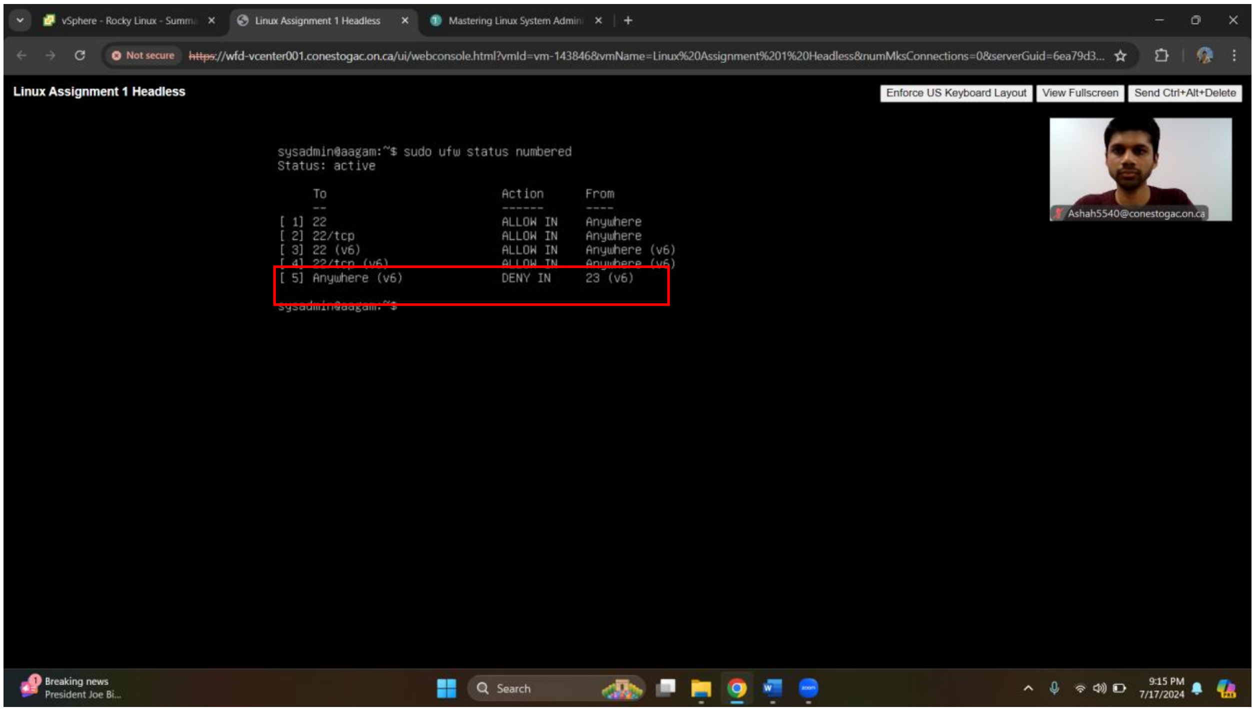
```
sysadmin@aagam:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 22                         ALLOW IN    Anywhere
[ 2] 22/tcp                     ALLOW IN    Anywhere
[ 3] Anywhere                   DENY IN     23
[ 4] 22 (v6)                    ALLOW IN    Anywhere (v6)
[ 5] 22/tcp (v6)                ALLOW IN    Anywhere (v6)
[ 6] Anywhere (v6)              DENY IN     23 (v6)

sysadmin@aagam:~$ _
```

9. Remove the new rule by typing **sudo ufw delete *rule#*** and pressing Enter, where *rule#* is the first number you recorded in the previous step. When you receive the message `Proceed with operation (y|n)?`, type **y** and press Enter.


Linux Assignment 1 Headless
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Ashah5540@conestogac.on.ca

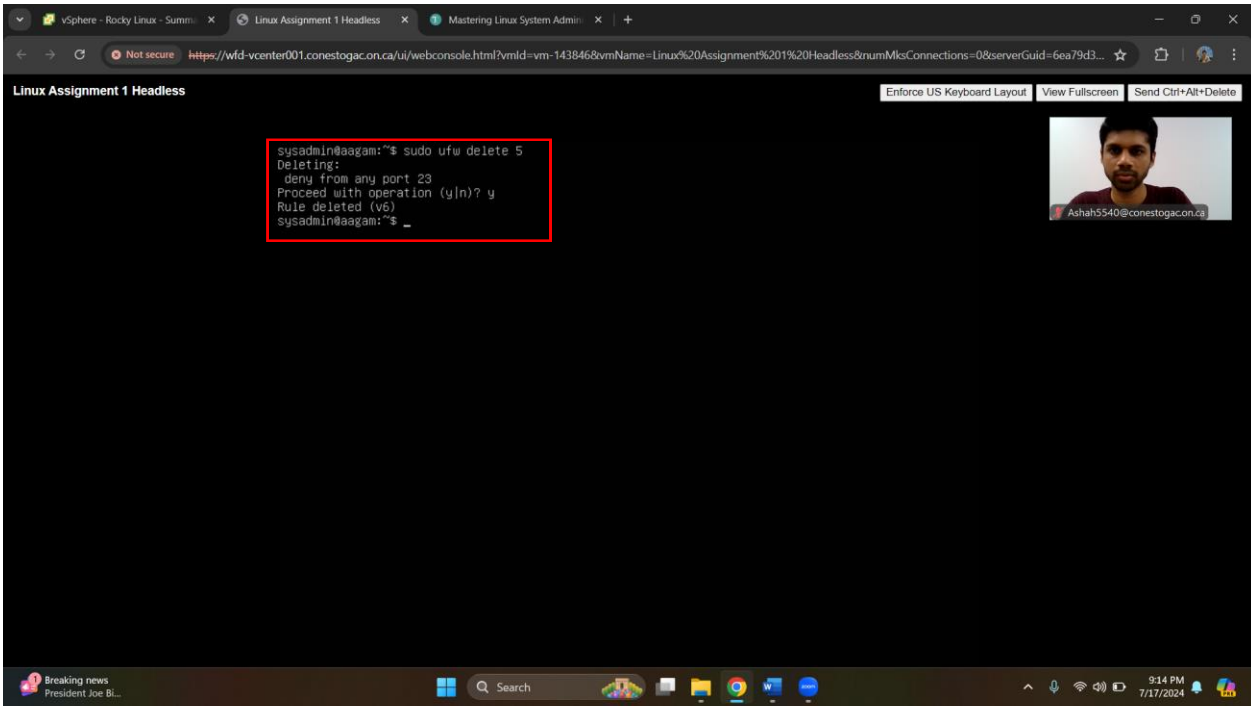
```
sysadmin@aagam:~$ sudo ufw delete 3
Deleting:
 deny from any port 23
Proceed with operation (y|n)? y
Rule deleted
sysadmin@aagam:~$ sudo ufw delete 6
ERROR: Could not find rule '6'
sysadmin@aagam:~$ _
```

10. If you recorded two rules in step 8, be aware that the rule number will change after a rule deletion. To delete the second rule, if you have one:
    1. Type **sudo ufw status numbered** and press Enter. The rule number will appear in the first column within brackets. Record its number.


Linux Assignment 1 Headless
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Ashah5540@conestogac.on.ca

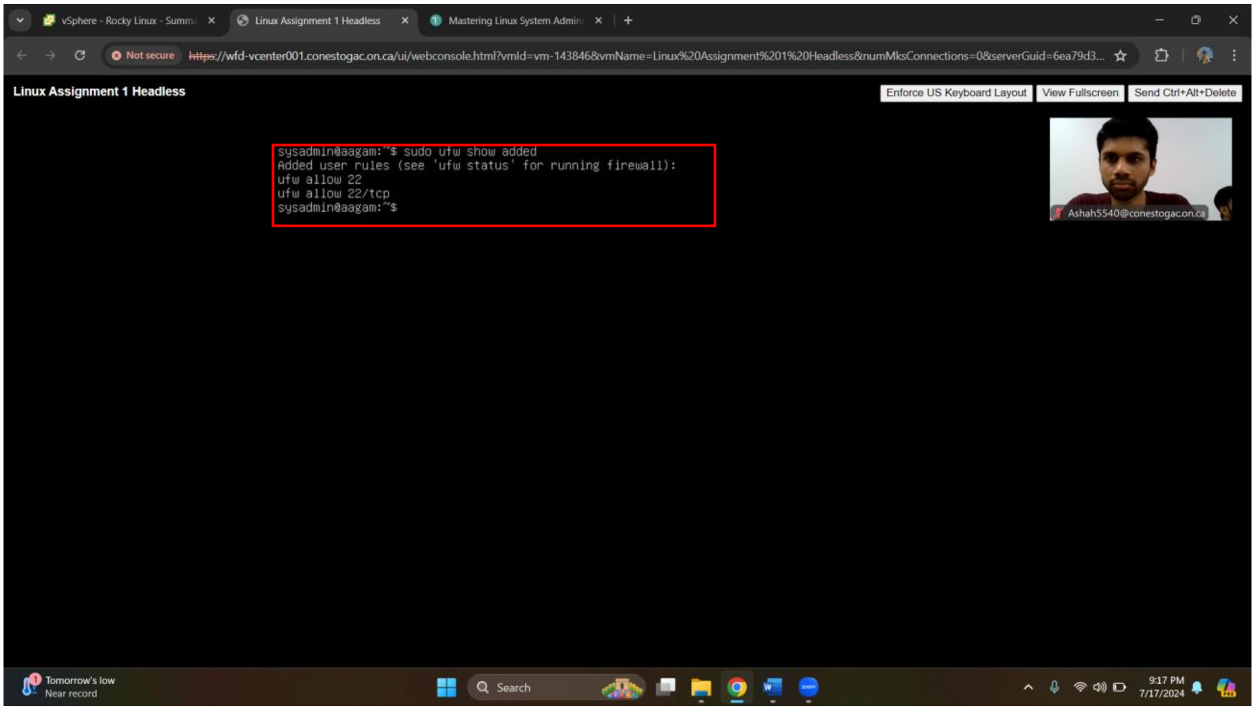
```
sysadmin@aagam:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 22                         ALLOW IN    Anywhere
[ 2] 22/tcp                     ALLOW IN    Anywhere
[ 3] 22 (v6)                    ALLOW IN    Anywhere (v6)
[ 4] 22/tcp (v6)                ALLOW IN    Anywhere (v6)
[ 5] Anywhere (v6)              DENY IN     23 (v6)

sysadmin@aagam:~$
```

2. Remove the second rule by typing **sudo ufw delete *rule#*** and pressing Enter, where *rule#* is the number you recorded in the previous step. When you receive the message `Proceed with operation (y|n)?`, type **y** and press Enter.


vSphere - Rocky Linux - Summ
Linux Assignment 1 Headless
Mastering Linux System Admin
Not secure
https://wfd-vcenter001.conestogac.on.ca/ui/webconsole.html?vmId=vm-143846&vmName=Linux%20Assignment%201%20Headless&numMksConnections=0&serverGuid=6ea79d3...
Linux Assignment 1 Headless
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Ashah5540@conestogac.on.ca
Breaking news
President Joe Bi...
Search
9:14 PM
7/17/2024

```
sysadmin@aagam:~$ sudo ufw delete 5
Deleting:
 deny from any port 23
Proceed with operation (y|n)? y
Rule deleted (v6)
sysadmin@aagam:~$ _
```

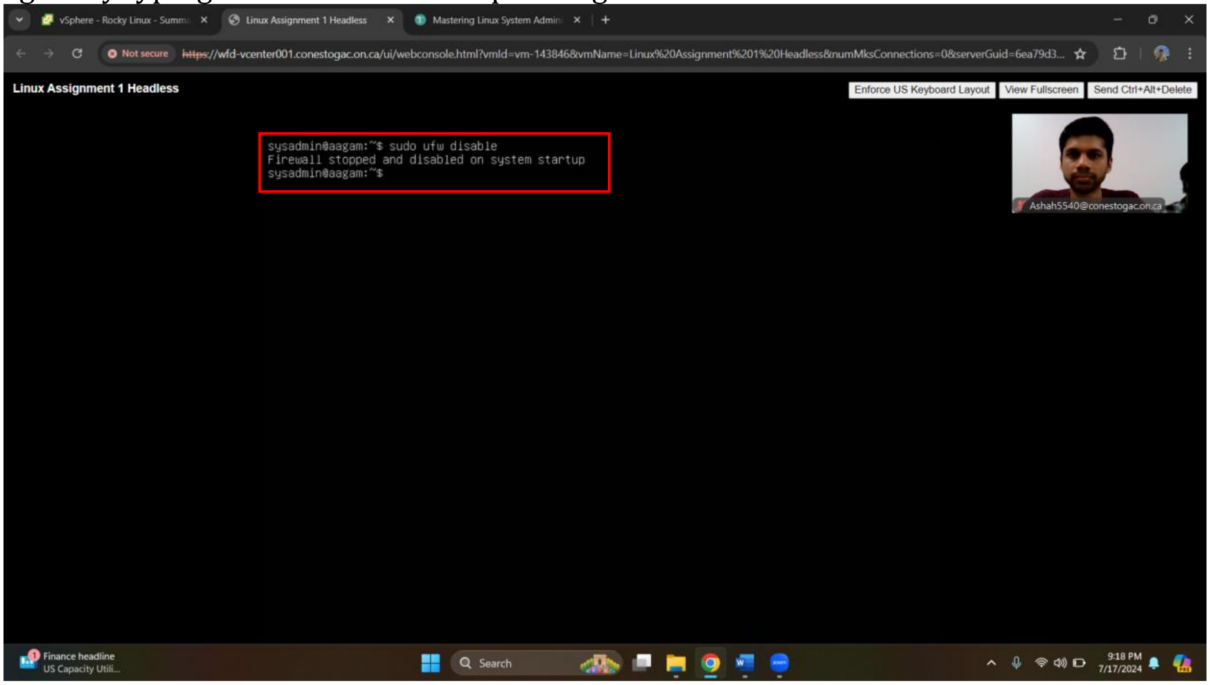
11. Ensure the new rule(s) was deleted by typing **sudo ufw show added** and pressing Enter.


vSphere - Rocky Linux - Summ
Linux Assignment 1 Headless
Mastering Linux System Admin
Not secure
https://wfd-vcenter001.conestogac.on.ca/ui/webconsole.html?vmId=vm-143846&vmName=Linux%20Assignment%201%20Headless&numMksConnections=0&serverGuid=6ea79d3...
Linux Assignment 1 Headless
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Ashah5540@conestogac.on.ca
Tomorrow's low
Near record
Search
9:17 PM
7/17/2024

```
sysadmin@aagam:~$ sudo ufw show added
Added user rules (see 'ufw status' for running firewall):
ufw allow 22
ufw allow 22/tcp
sysadmin@aagam:~$
```

12. Compare the output of the previous step's command with what you recorded for step 4. You should find that they are now identical. →**Yes, its showing identical**

13. If you determined that your UFW firewall was `inactive` in step 2, disable it again by typing **sudo ufw disable** and pressing Enter.


Linux Assignment 1 Headless
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Ashah5540@conestogac.on.ca

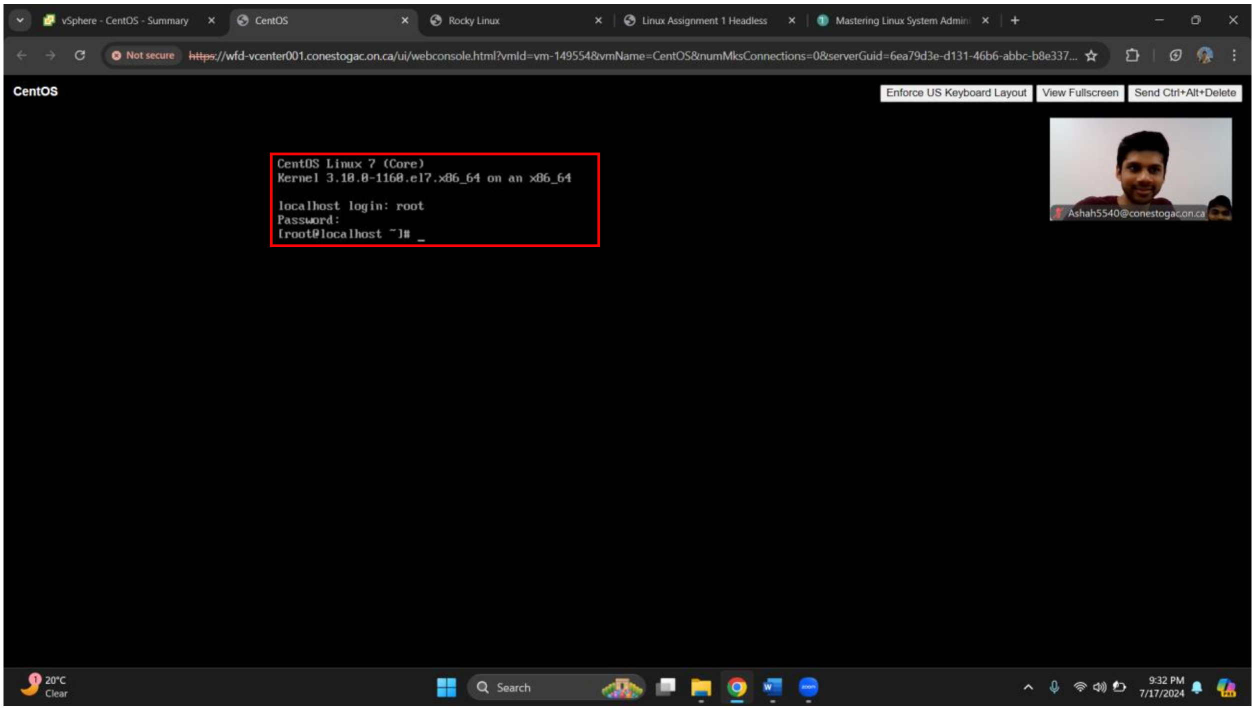
```
sysadmin@aagam:~$ sudo ufw disable
Firewall stopped and disabled on system startup
sysadmin@aagam:~$
```

4. Week 11 Slide 28

Complete the Real World Scenario: Testing the Timeout Feature in Ch 18

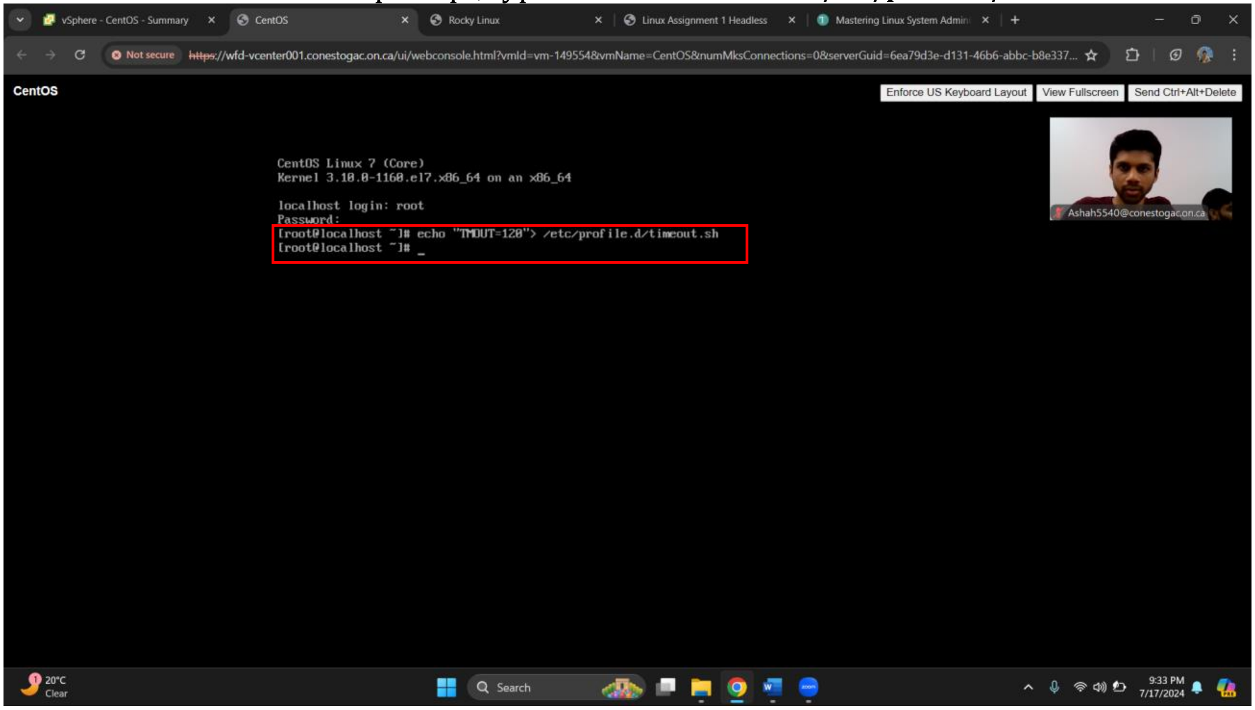
TESTING THE TIMEOUT FEATURE

1. Log into your CentOS server either as the root user account or as a user account that has root privileges.



```
CentOS Linux 7 (Core)
Kernel 3.10.0-1160.el7.x86_64 on an x86_64

localhost login: root
Password:
[root@localhost ~]# _
```

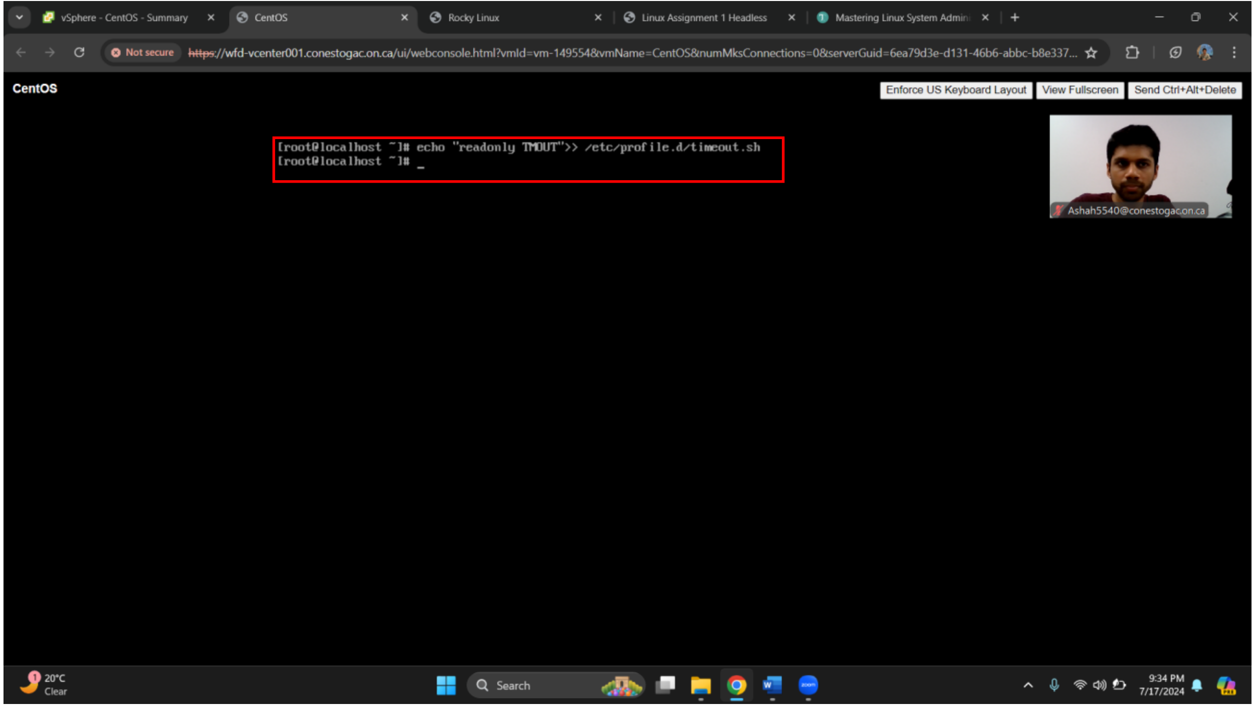
2. From the command prompt, type **echo "TMOUT=120"> /etc/profile.d/timeout.sh.**



vSphere - CentOS - Summary
CentOS
Rocky Linux
Linux Assignment 1 Headless
Mastering Linux System Admin
Not secure
https://wfd-vcenter001.conestogac.on.ca/ui/webconsole.html?vmId=vm-149554&vmName=CentOS&numMksConnections=0&serverGuid=6ea79d3e-d131-46b6-abbc-b8e337...
CentOS
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Ashah5540@conestogac.on.ca
20°C
Clear
Search
9:33 PM
7/17/2024

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1160.el7.x86_64 on an x86_64

localhost login: root
Password:
[root@localhost ~]# echo "TMOUT=120"> /etc/profile.d/timeout.sh
[root@localhost ~]# _
```

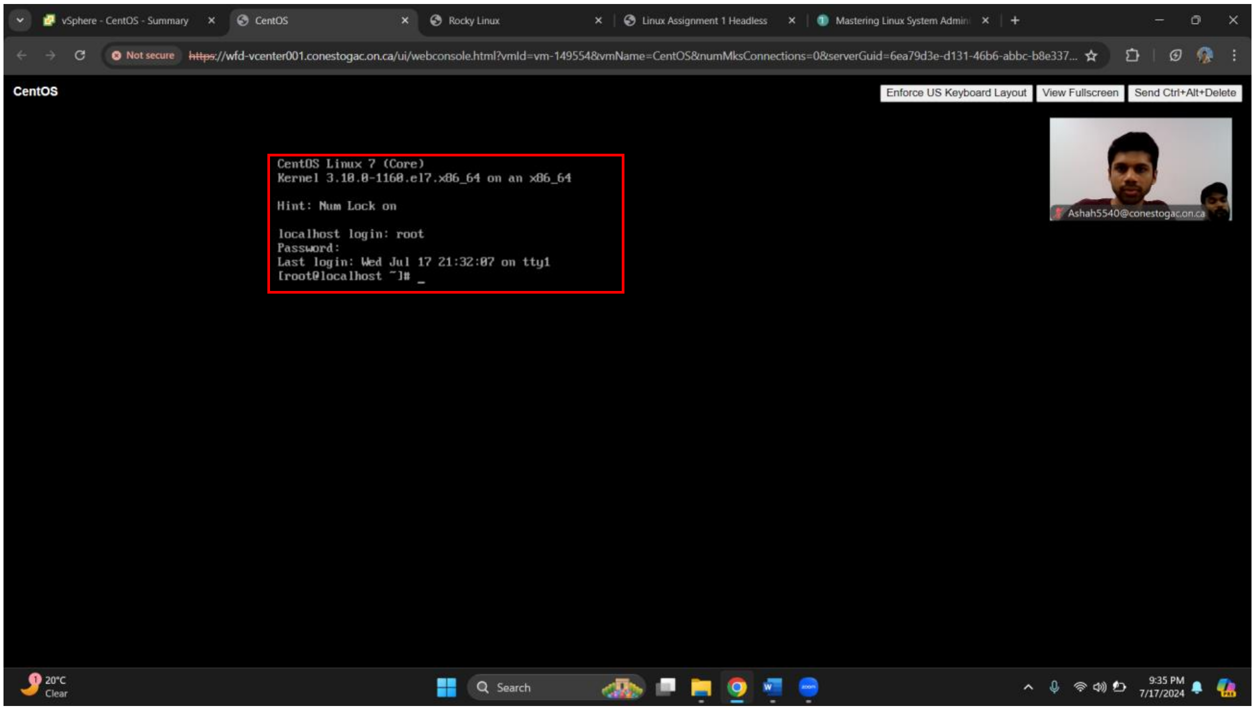
3. Again from the command prompt, type **echo "readonly TMOUT" >> /etc/profile.d/timeout.sh.**



vSphere - CentOS - Summary
CentOS
Rocky Linux
Linux Assignment 1 Headless
Mastering Linux System Admin
Not secure
https://wfd-vcenter001.conestogac.on.ca/ui/webconsole.html?vmId=vm-149554&vmName=CentOS&numMksConnections=0&serverGuid=6ea79d3e-d131-46b6-abbc-b8e337...
CentOS
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Ashah5540@conestogac.on.ca
20°C
Clear
Search
9:34 PM
7/17/2024

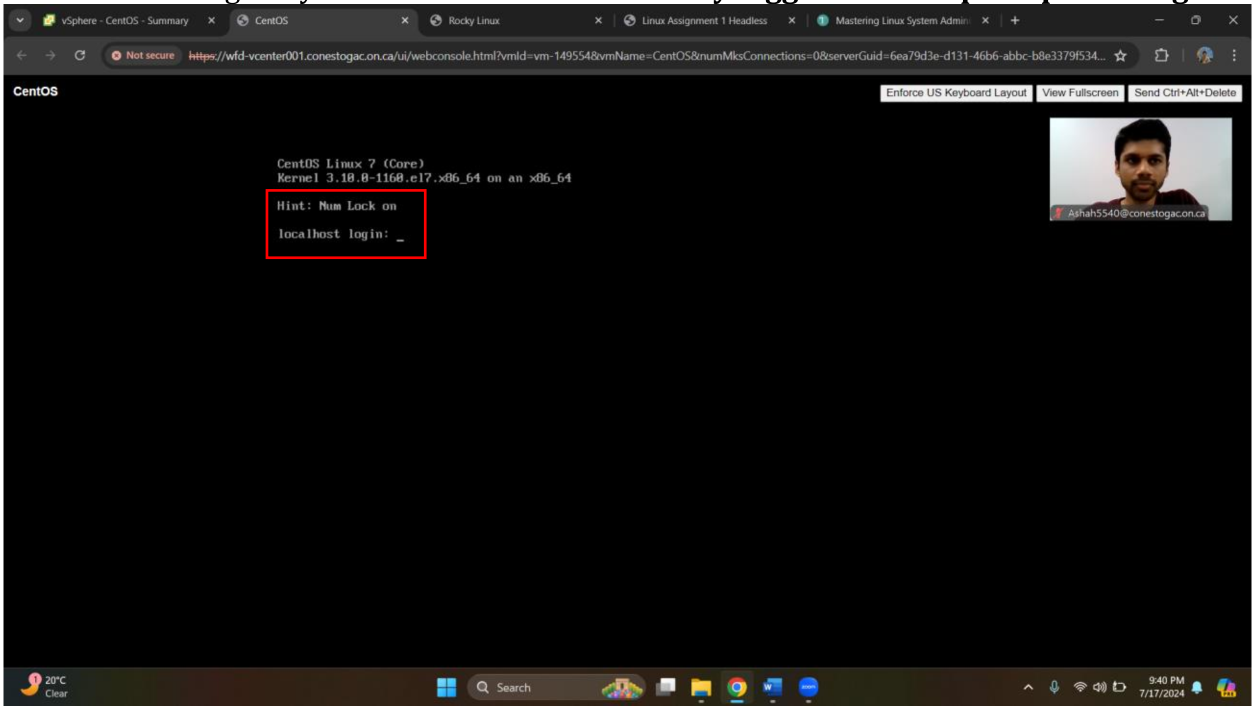
```
[root@localhost ~]# echo "readonly TMOUT">> /etc/profile.d/timeout.sh
[root@localhost ~]# _
```

4. Log out from the terminal session, and then log back in.


vSphere - CentOS - Summary
CentOS
Rocky Linux
Linux Assignment 1 Headless
Mastering Linux System Admin
Not secure
https://wfd-vcenter001.conestogac.on.ca/ui/webconsole.html?vmId=vm-149554&vmName=CentOS&numMksConnections=0&serverGuid=6ea79d3e-d131-46b6-abbc-b8e337...
CentOS
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Ashah5540@conestogac.on.ca
20°C
Clear
Search
9:35 PM
7/17/2024

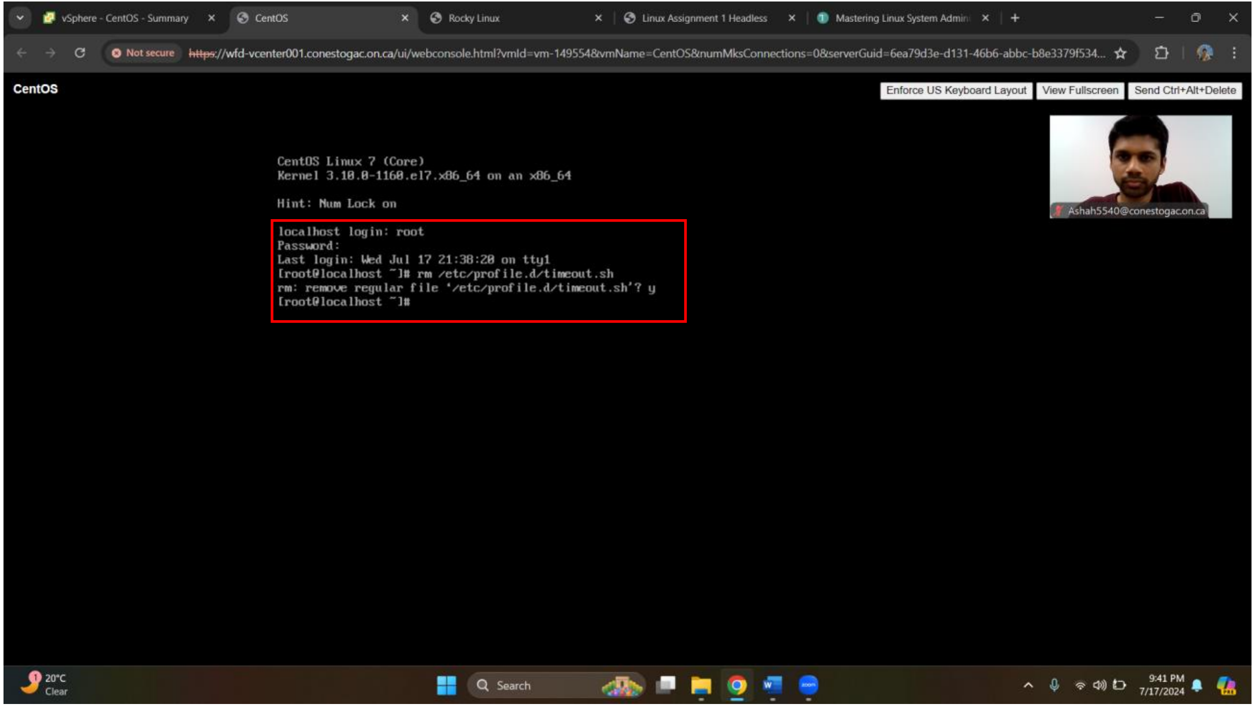
```
CentOS Linux 7 (Core)
Kernel 3.10.0-1160.el7.x86_64 on an x86_64

Hint: Num Lock on

localhost login: root
Password:
Last login: Wed Jul 17 21:32:07 on tty1
[root@localhost ~]# _
```

5. Let the session sit idle at the command prompt for more than 2 minutes. The system should log out your session. → **Automatically logged out and prompts for login**


vSphere - CentOS - Summary
CentOS
Rocky Linux
Linux Assignment 1 Headless
Mastering Linux System Admin
Not secure
https://wfd-vcenter001.conestogac.on.ca/ui/webconsole.html?vmId=vm-149554&vmName=CentOS&numMksConnections=0&serverGuid=6ea79d3e-d131-46b6-abbc-b8e3379f534...
CentOS
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Ashah5540@conestogac.on.ca
20°C
Clear
Search
9:40 PM
7/17/2024

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1160.el7.x86_64 on an x86_64

Hint: Num Lock on

localhost login: _
```

6. If you want to remove the timeout feature, from the command prompt, type **rm /etc/profile.d/timeout.sh.**



vSphere - CentOS - Summary
CentOS
Rocky Linux
Linux Assignment 1 Headless
Mastering Linux System Admin
Not secure
https://wfd-vcenter001.conestogac.on.ca/ui/webconsole.html?vmId=vm-149554&vmName=CentOS&numMksConnections=0&serverGuid=6ea79d3e-d131-46b6-abbc-b8e3379f534...
CentOS
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Ashah5540@conestogac.on.ca
20°C
Clear
Search
9:41 PM
7/17/2024

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1160.el7.x86_64 on an x86_64

Hint: Num Lock on

localhost login: root
Password:
Last login: Wed Jul 17 21:38:20 on tty1
[root@localhost ~]# rm /etc/profile.d/timeout.sh
rm: remove regular file '/etc/profile.d/timeout.sh'? y
[root@localhost ~]#
```