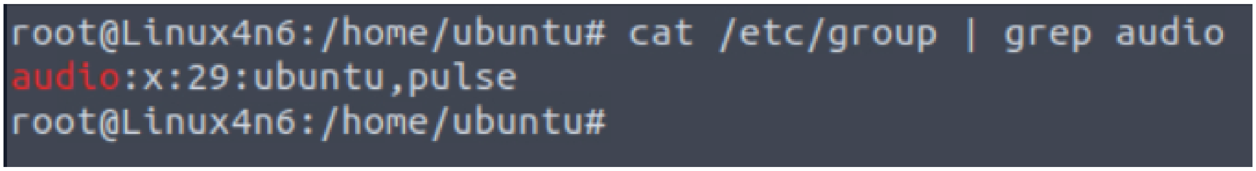
Linux Forensics

Task 3 OS and account information

Which two users are the members of the group audio?

Use cat /etc/group | grep audio

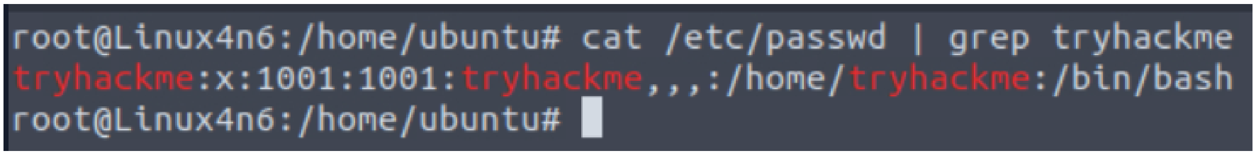


```
root@Linux4n6:/home/ubuntu# cat /etc/group | grep audio
audio:x:29:ubuntu,pulse
root@Linux4n6:/home/ubuntu#
```

ubuntu,pulse

In the attached VM, there is a user account named tryhackme. What is the uid of this account?

Run the command cat /etc/passwd | grep tryhackme

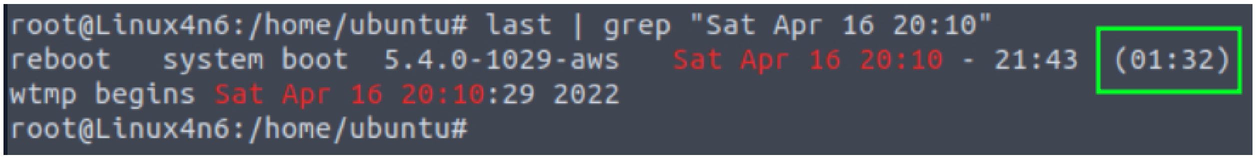


```
root@Linux4n6:/home/ubuntu# cat /etc/passwd | grep tryhackme
tryhackme:x:1001:1001:tryhackme,,,:/home/tryhackme:/bin/bash
root@Linux4n6:/home/ubuntu#
```

1001

A session was started on this machine on Sat Apr 16 20:10. How long did this session last?

last | grep "Sat Apr 16 20:10"

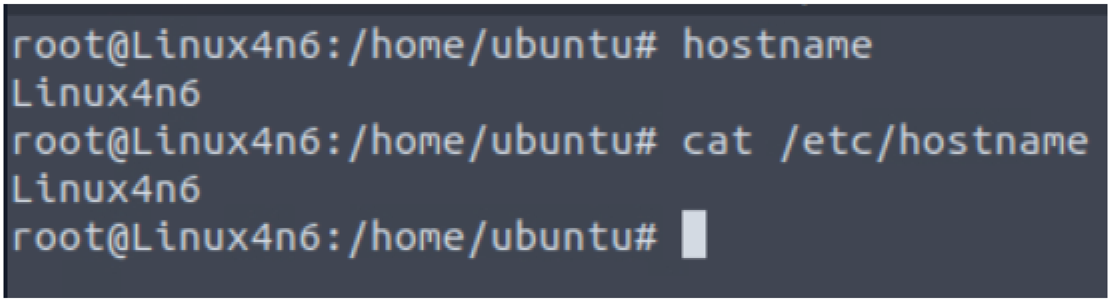


```
root@Linux4n6:/home/ubuntu# last | grep "Sat Apr 16 20:10"
reboot   system boot  5.4.0-1029-aws   Sat Apr 16 20:10 - 21:43  (01:32)
wtmp begins Sat Apr 16 20:10:29 2022
root@Linux4n6:/home/ubuntu#
```

01:32

Task 4 System Configuration

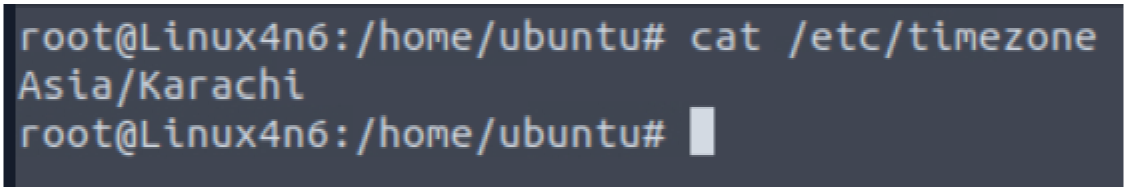
What is the hostname of the attached VM?



```
root@Linux4n6:/home/ubuntu# hostname
Linux4n6
root@Linux4n6:/home/ubuntu# cat /etc/hostname
Linux4n6
root@Linux4n6:/home/ubuntu# 
```

Linux4n6

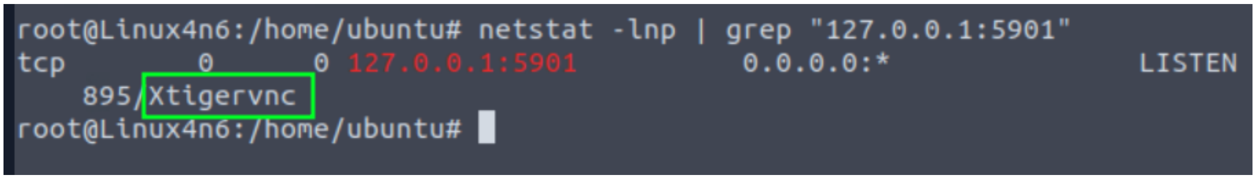
What is the timezone of the attached VM?



```
root@Linux4n6:/home/ubuntu# cat /etc/timezone
Asia/Karachi
root@Linux4n6:/home/ubuntu# 
```

Asia/Karachi

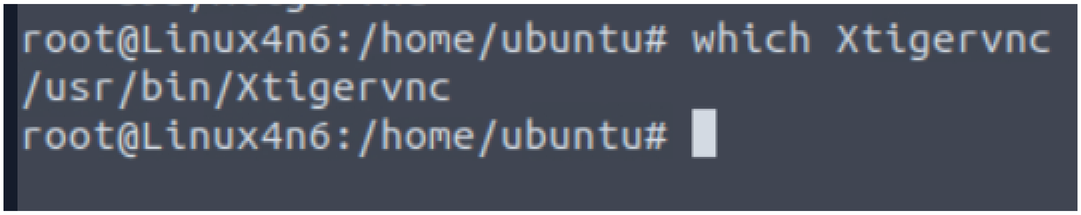
What program is listening on the address 127.0.0.1:5901?



```
root@Linux4n6:/home/ubuntu# netstat -lnp | grep "127.0.0.1:5901"
tcp        0      0 127.0.0.1:5901          0.0.0.0:*               LISTEN
    895/Xtigervnc
root@Linux4n6:/home/ubuntu# 
```

Xtigervnc

What is the full path of this program?

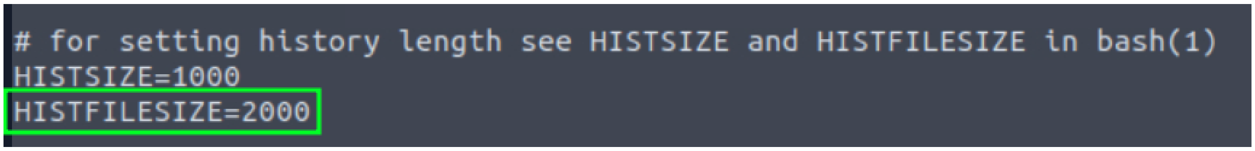


```
root@Linux4n6:/home/ubuntu# which Xtigervnc
/usr/bin/Xtigervnc
root@Linux4n6:/home/ubuntu# 
```

/usr/bin/Xtigervnc

Task 5 Persistence mechanisms

In the bashrc file, the size of the history file is defined. What is the size of the history file that is set for the user Ubuntu in the attached machine?

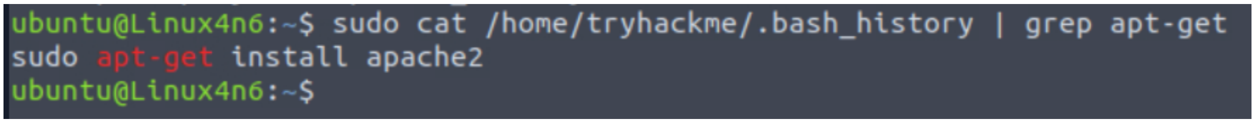


```
# for setting history length see HISTSIZE and HISTFILESIZE in bash(1)
HISTSIZE=1000
HISTFILESIZE=2000
```

2000

Task 6 Evidence of Execution

The user tryhackme used apt-get to install a package. What was the command that was issued?



```
ubuntu@Linux4n6:~$ sudo cat /home/tryhackme/.bash_history | grep apt-get
sudo apt-get install apache2
ubuntu@Linux4n6:~$
```

sudo apt-get install apache2

What was the current working directory when the command to install net-tools was issued?

/home/ubuntu

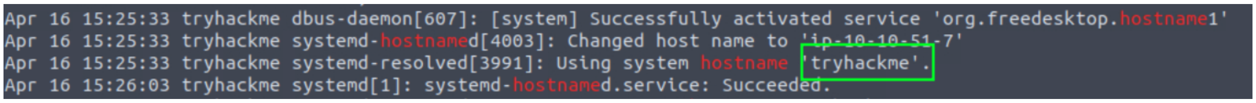
Task 7 Log files

Though the machine's current hostname is the one we identified in Task 4. The machine earlier had a different hostname. What was the previous hostname of the machine?

After executing the command cat /var/log/syslog* | grep hostname I didn’t find the answer later i found the some archive files in /var/log

syslog.2.gz and syslog.3.gz

Extract them and try again using gzip -d filename or gunzip filename



```
Apr 16 15:25:33 tryhackme dbus-daemon[607]: [system] Successfully activated service 'org.freedesktop.hostname1'
Apr 16 15:25:33 tryhackme systemd-hostnamed[4003]: Changed host name to 'ip-10-10-51-7'
Apr 16 15:25:33 tryhackme systemd-resolved[3991]: Using system hostname 'tryhackme'.
Apr 16 15:26:03 tryhackme systemd[1]: systemd-hostnamed.service: Succeeded.
```

tryhackme