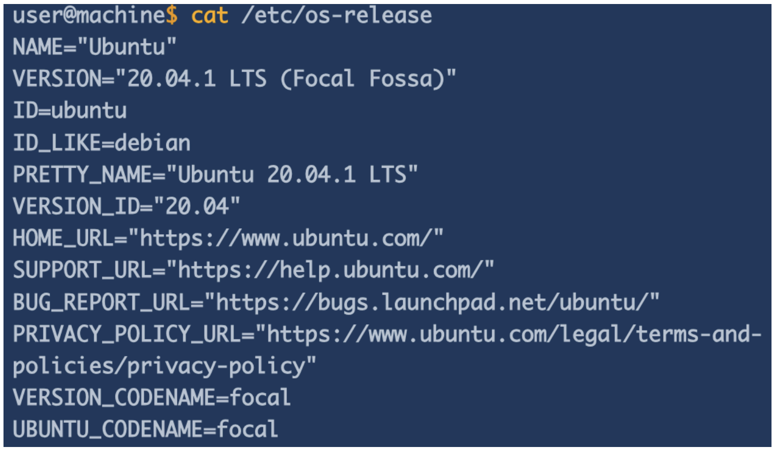
Linux Forensics

Linux challenge on TryHackme:

- Finding OS, account, and system information on a Linux machine
- Finding information about running processes, executed processes, and processes that are scheduled to run
- Finding system log files and identifying information from them
- Common third-party applications used in Linux and their logs

OS Release Information

Use cat utility to read the file located at /etc/os-release

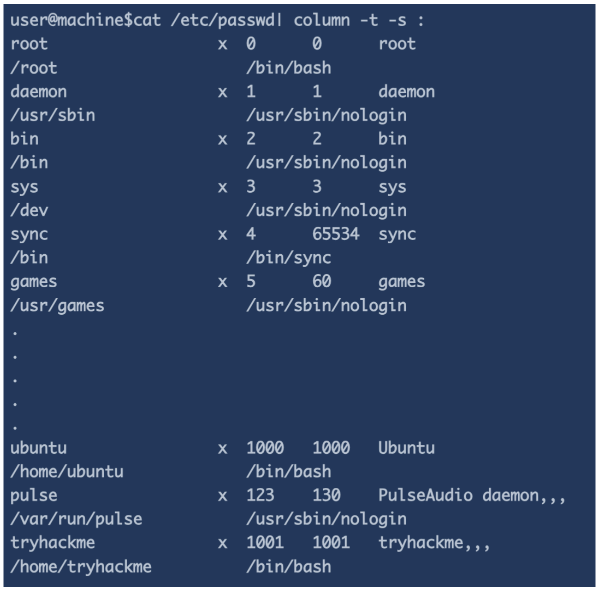


```
user@machine$ cat /etc/os-release
NAME="Ubuntu"
VERSION="20.04.1 LTS (Focal Fossa)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 20.04.1 LTS"
VERSION_ID="20.04"
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-
policies/privacy-policy"
VERSION_CODENAME=focal
UBUNTU_CODENAME=focal
```

User Accounts

The /etc/passwd file contains information about the user accounts that exist on a Linux system. Use the cat utility to read this file.

The output contains 7 colon-separated fields, describing username, password information, user id (uid), group id (gid), description, home directory information, and the default shell that executes when the user logs in. Like Windows, the user-created user accounts have uids 1000 or above. Use this command to make it more readable cat /etc/passwd| column -t -s :

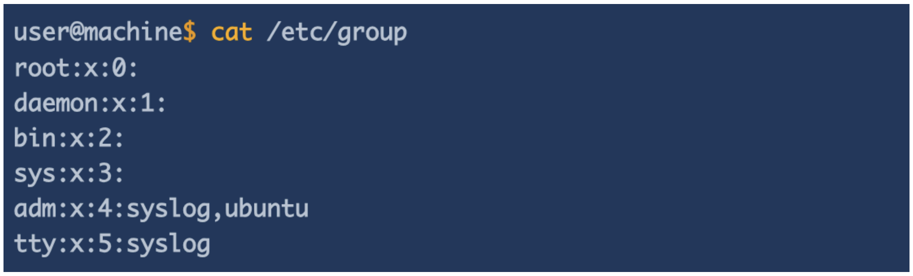


```
user@machine$cat /etc/passwd| column -t -s :
root                  x  0      0      root
/root                    /bin/bash
daemon                x  1      1      daemon
/usr/sbin                /usr/sbin/nologin
bin                   x  2      2      bin
/bin                     /usr/sbin/nologin
sys                   x  3      3      sys
/dev                     /usr/sbin/nologin
sync                  x  4      65534  sync
/bin                     /bin/sync
games                 x  5      60     games
/usr/games               /usr/sbin/nologin
.
.
.
.
.
ubuntu                x  1000   1000   Ubuntu
/home/ubuntu             /bin/bash
pulse                 x  123    130    PulseAudio daemon,,,
/var/run/pulse           /usr/sbin/nologin
tryhackme             x  1001   1001   tryhackme,,,
/home/tryhackme          /bin/bash
```

Group Information

The /etc/group file contains information about the different user groups present on the host. It can be read using the cat utility.

Linux Forensics

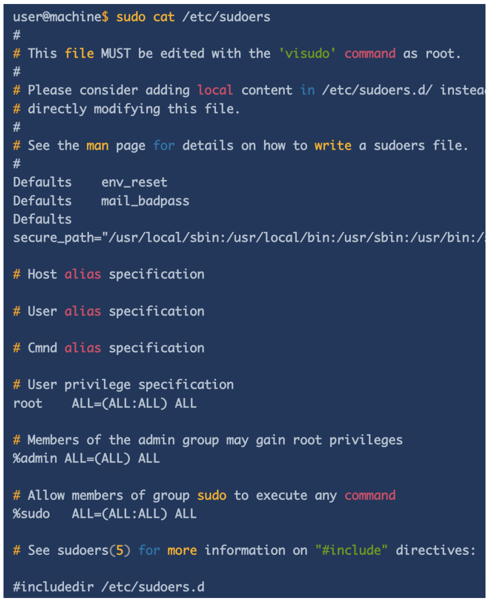


```
user@machine$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,ubuntu
tty:x:5:syslog
```

The user ubuntu belongs to the adm group, which has a password stored in the /etc/shadow file, signified by the x character. The gid is 4, and the group contains 2 users, Syslog, and ubuntu.

Sudoers List

Stored in the file /etc/sudoers and can be read using the cat utility. Needs to elevate privileges to access the file.

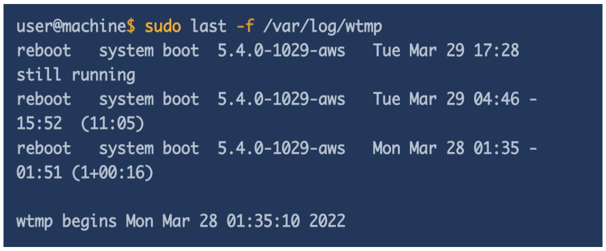


```
user@machine$ sudo cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instea
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults    env_reset
Defaults    mail_badpass
Defaults
secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/

# 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
```

Login Information

In the /var/log directory, log files of all kinds including wtmp and btmp. The btmp file saves information about failed logins, while the wtmp keeps historical data of logins. These files are not regular text files that can be read using cat, less or vim; instead, they are binary files, which have to be read using the last utility.

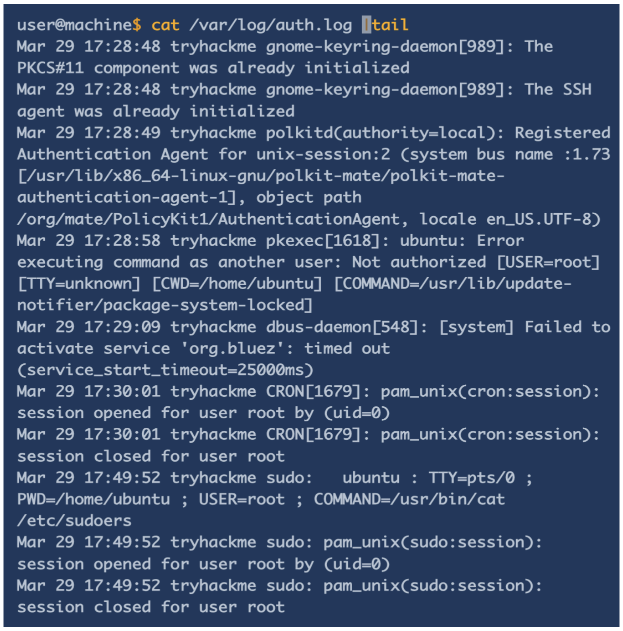
man last
The following terminal shows the contents of wtmp being read using the last utility.



```
user@machine$ sudo last -f /var/log/wtmp
reboot   system boot  5.4.0-1029-aws   Tue Mar 29 17:28
still running
reboot   system boot  5.4.0-1029-aws   Tue Mar 29 04:46 -
15:52  (11:05)
reboot   system boot  5.4.0-1029-aws   Mon Mar 28 01:35 -
01:51 (1+00:16)

wtmp begins Mon Mar 28 01:35:10 2022
```

Authentication Logs

Every user that authenticates on a Linux host is logged in the auth log. The auth log is a file placed in the location /var/log/auth.log. It can be read using the cat utility, however, given the size of the file, we can use tail, head, more or less utilities to make it easier to read.



```
user@machine$ cat /var/log/auth.log |tail
Mar 29 17:28:48 tryhackme gnome-keyring-daemon[989]: The
PKCS#11 component was already initialized
Mar 29 17:28:48 tryhackme gnome-keyring-daemon[989]: The SSH
agent was already initialized
Mar 29 17:28:49 tryhackme polkitd(authority=local): Registered
Authentication Agent for unix-session:2 (system bus name :1.73
[/usr/lib/x86_64-linux-gnu/polkit-mate/polkit-mate-
authentication-agent-1], object path
/org/mate/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Mar 29 17:28:58 tryhackme pkexec[1618]: ubuntu: Error
executing command as another user: Not authorized [USER=root]
[TTY=unknown] [CWD=/home/ubuntu] [COMMAND=/usr/lib/update-
notifier/package-system-locked]
Mar 29 17:29:09 tryhackme dbus-daemon[548]: [system] Failed to
activate service 'org.bluez': timed out
(service_start_timeout=25000ms)
Mar 29 17:30:01 tryhackme CRON[1679]: pam_unix(cron:session):
session opened for user root by (uid=0)
Mar 29 17:30:01 tryhackme CRON[1679]: pam_unix(cron:session):
session closed for user root
Mar 29 17:49:52 tryhackme sudo:   ubuntu : TTY=pts/0 ;
PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/cat
/etc/sudoers
Mar 29 17:49:52 tryhackme sudo: pam_unix(sudo:session):
session opened for user root by (uid=0)
Mar 29 17:49:52 tryhackme sudo: pam_unix(sudo:session):
session closed for user root
```

Linux Forensics

The user ‘ubuntu’ elevated privileges on Mar 29 17:49:52 using sudo to run the command cat /etc/sudoers. The subsequent session opened and closed events for the root user, which were a result of the above-mentioned privilege escalation.

QUESTIONS

1. **Which two users are the members of the group audio?**

ubuntu, pulse

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

1001

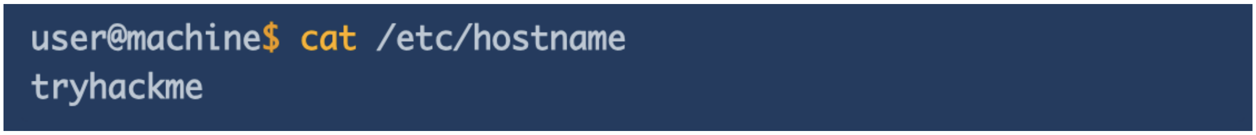
3. **A session was started on this machine on Sat Apr 16 20:10. How long did this session last?**

01:32

SYSTEM CONFIGURATION

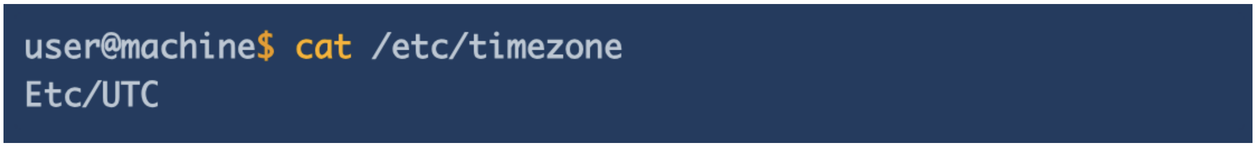
Hostname

The hostname is stored in the /etc/hostname file on a Linux Host. It can be accessed using the cat utility.



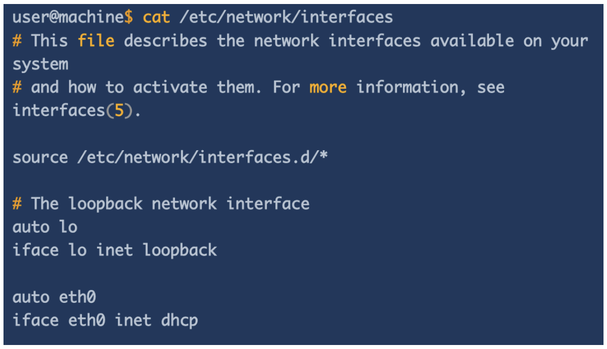
```
user@machine$ cat /etc/hostname
tryhackme
```

Timezone



```
user@machine$ cat /etc/timezone
Etc/UTC
```

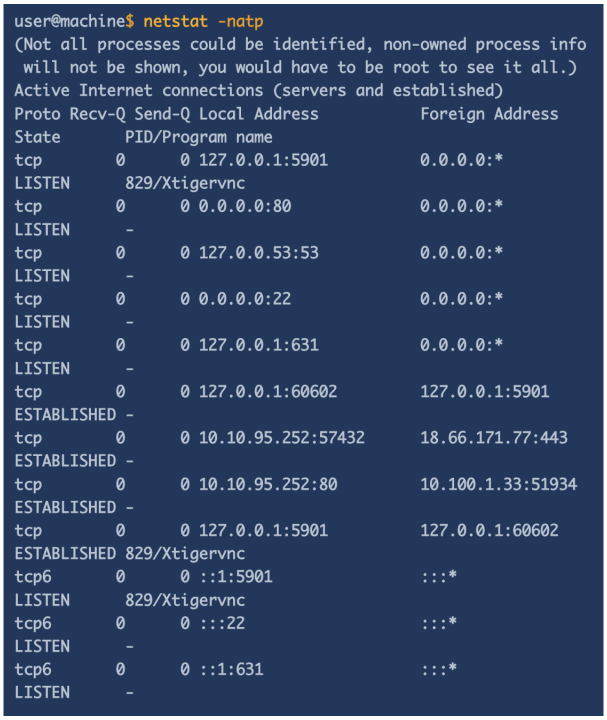
Network Configuration



```
user@machine$ cat /etc/network/interfaces
# This file describes the network interfaces available on your
system
# and how to activate them. For more information, see
interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet dhcp
```

Linux Forensics

To find information about the network interfaces, we can cat the /etc/network/interfaces file. The output on your machine might be different from the one shown here, depending on configuration.



```
user@machine$ netstat -natp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address
State       PID/Program name
tcp        0      0 127.0.0.1:5901          0.0.0.0:*
LISTEN      829/Xtigervnc
tcp        0      0 0.0.0.0:80              0.0.0.0:*
LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*
LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*
LISTEN      -
tcp        0      0 127.0.0.1:631           0.0.0.0:*
LISTEN      -
tcp        0      0 127.0.0.1:60602         127.0.0.1:5901
ESTABLISHED -
tcp        0      0 10.10.95.252:57432      18.66.171.77:443
ESTABLISHED -
tcp        0      0 10.10.95.252:80         10.100.1.33:51934
ESTABLISHED -
tcp        0      0 127.0.0.1:5901          127.0.0.1:60602
ESTABLISHED 829/Xtigervnc
tcp6       0      0 ::1:5901                :::*
LISTEN      829/Xtigervnc
tcp6       0      0 :::22                   :::*
LISTEN      -
tcp6       0      0 ::1:631                 :::*
LISTEN      -
```

Active network connections

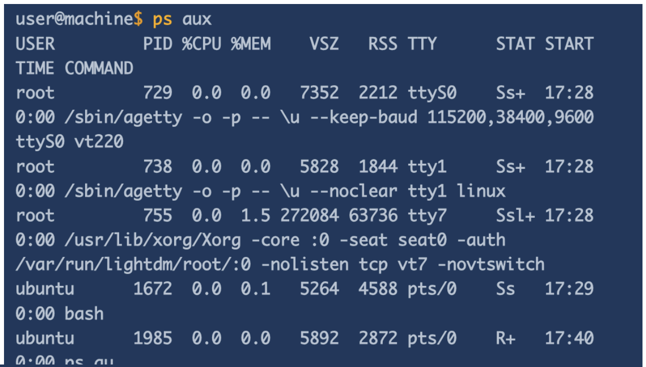
On a live system, knowing the active network connections provides additional context to the investigation. Use the netstat utility to find active network connections on a Linux host.

man netstat

The terminal below shows the usage of the netstat utility.

Running processes

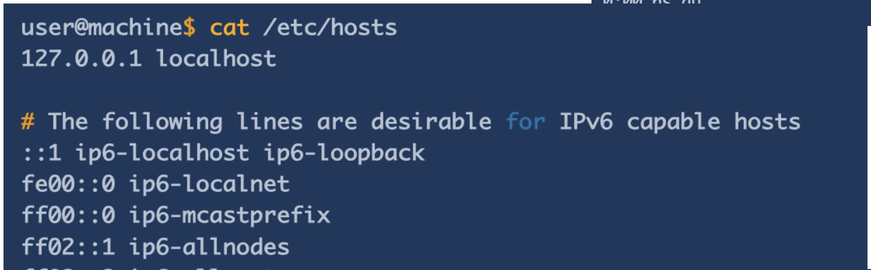
If performing forensics on a live system, it is helpful to check the running processes. The ps utility shows details about the running processes. man p The below terminal shows the usage of the ps utility.



```
user@machine$ ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START
TIME COMMAND
root         729  0.0  0.0   7352  2212 ttyS0    Ss+  17:28
0:00 /sbin/agetty -o -p -- \u --keep-baud 115200,38400,9600
ttyS0 vt220
root         738  0.0  0.0   5828  1844 tty1     Ss+  17:28
0:00 /sbin/agetty -o -p -- \u --noclear tty1 linux
root         755  0.0  1.5 272084 63736 tty7     Ssl+ 17:28
0:00 /usr/lib/xorg/Xorg -core :0 -seat seat0 -auth
/var/run/lightdm/root/:0 -nolisten tcp vt7 -novtswitch
ubuntu      1672  0.0  0.1   5264  4588 pts/0    Ss   17:29
0:00 bash
ubuntu      1985  0.0  0.0   5892  2872 pts/0    R+   17:40
0:00 ps au
```

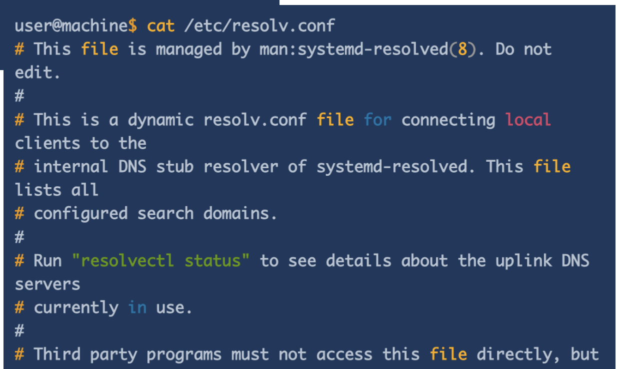
DNS Information

The file /etc/hosts contains the configuration for the DNS name assignment. Use the cat utility to read the hosts file. man hosts The terminal shows a sample output of the hosts file.



```
user@machine$ cat /etc/hosts
127.0.0.1 localhost

# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
```

The information about DNS servers that a Linux host talks to for DNS resolution is



```
user@machine$ cat /etc/resolv.conf
# This file is managed by man:systemd-resolved(8). Do not
edit.
#
# This is a dynamic resolv.conf file for connecting local
clients to the
# internal DNS stub resolver of systemd-resolved. This file
lists all
# configured search domains.
#
# Run "resolvectl status" to see details about the uplink DNS
servers
# currently in use.
#
# Third party programs must not access this file directly, but
```

stored in the *resolv.conf* file. Its location is /etc/resolv.conf. Use the cat utility to read this file.

QUESTIONS

1. **What is the hostname of the attached VM?**

Linux4n6

2. **What is the timezone of the attached VM?**

Asia/Karachi

3. **What program is listening on the address 127.0.0.1:5901?**

Xtigervnc

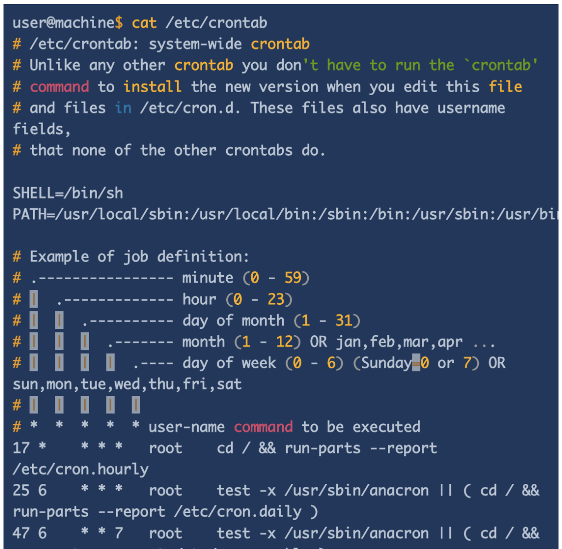
4. **What is the full path of this program?**

/usr/bin/Xtigervnc

PERSISTENCE MECHANISMS

Cron jobs

Cron jobs are commands that run periodically after a set amount of time. A Linux host maintains a list of Cron jobs in a file located at /etc/crontab. Read the file using the cat utility.

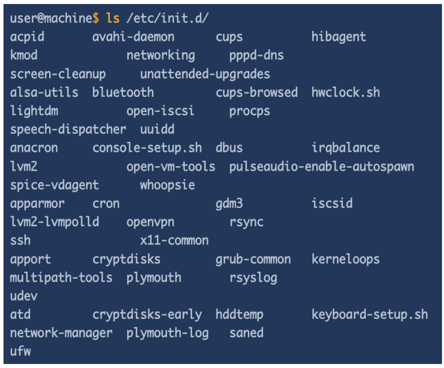


```
user@machine$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username
fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bi

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR
sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report
/etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / &&
run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / &&
```

Linux Forensics

Service Startup

Like Windows, services can be set up in Linux that will start and run in the background after every system boot. A list of services can be found in the /etc/init.d directory. Check the contents of the directory by using the ls utility.

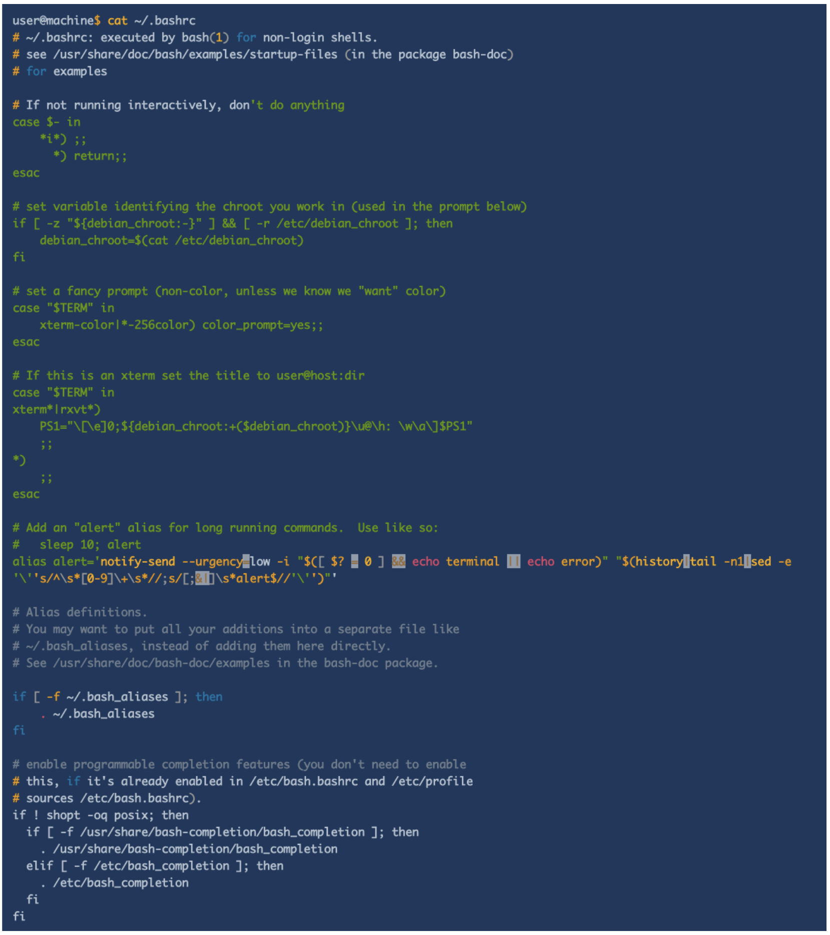


```
user@machine$ ls /etc/init.d/
acpid       avahi-daemon      cups          hibagent
kmod             networking     pppd-dns
screen-cleanup     unattended-upgrades
alsa-utils  bluetooth         cups-browsed  hwclock.sh
lightdm          open-iscsi     procps
speech-dispatcher  uuidd
anacron     console-setup.sh  dbus          irqbalance
lvm2             open-vm-tools  pulseaudio-enable-autospawn
spice-vdagent      whoopsie
apparmor    cron              gdm3          iscsid
lvm2-lvmpolld    openvpn        rsync
ssh                x11-common
apport      cryptdisks        grub-common   kerneloops
multipath-tools  plymouth       rsyslog
udev
atd         cryptdisks-early  hddtemp       keyboard-setup.sh
network-manager  plymouth-log   saned
ufw
```

.Bashrc

When a bash shell is spawned, it runs the commands stored in the .bashrc file. This file can be considered as a startup list of actions to be performed. Hence it can prove to be a good place to look for persistence.

Example .bashrc file



```
user@machine$ cat ~/.bashrc
# ~/.bashrc: executed by bash(1) for non-login shells.
# see /usr/share/doc/bash/examples/startup-files (in the package bash-doc)
# for examples

# If not running interactively, don't do anything
case $- in
    *i*) ;;
      *) return;;
esac

# set variable identifying the chroot you work in (used in the prompt below)
if [ -z "${debian_chroot:-}" ] && [ -r /etc/debian_chroot ]; then
    debian_chroot=$(cat /etc/debian_chroot)
fi

# set a fancy prompt (non-color, unless we know we "want" color)
case "$TERM" in
    xterm-color|*-256color) color_prompt=yes;;
esac

# If this is an xterm set the title to user@host:dir
case "$TERM" in
xterm*|rxvt*)
    PS1="\[\e]0;${debian_chroot:+($debian_chroot)}\u@\h: \w\a\]$PS1"
    ;;
*)
    ;;
esac

# Add an "alert" alias for long running commands.  Use like so:
#   sleep 10; alert
alias alert='notify-send --urgency=low -i "$([ $? = 0 ] && echo terminal || echo error)" "$(history|tail -n1|sed -e
'\''s/^\s*[0-9]\+\s*//;s/[;&|]\s*alert$//'\'')"'

# Alias definitions.
# You may want to put all your additions into a separate file like
# ~/.bash_aliases, instead of adding them here directly.
# See /usr/share/doc/bash-doc/examples in the bash-doc package.

if [ -f ~/.bash_aliases ]; then
    . ~/.bash_aliases
fi

# enable programmable completion features (you don't need to enable
# this, if it's already enabled in /etc/bash.bashrc and /etc/profile
# sources /etc/bash.bashrc).
if ! shopt -oq posix; then
  if [ -f /usr/share/bash-completion/bash_completion ]; then
    . /usr/share/bash-completion/bash_completion
  elif [ -f /etc/bash_completion ]; then
    . /etc/bash_completion
  fi
fi
```

QUESTIONS

1. **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?**

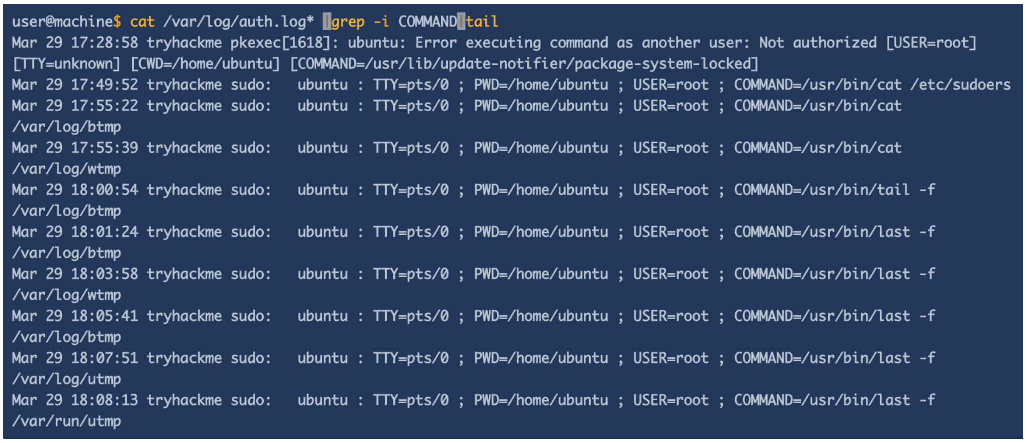
2000

Linux Forensics

EVIDENCE OF EXECUTION

Sudo execution history

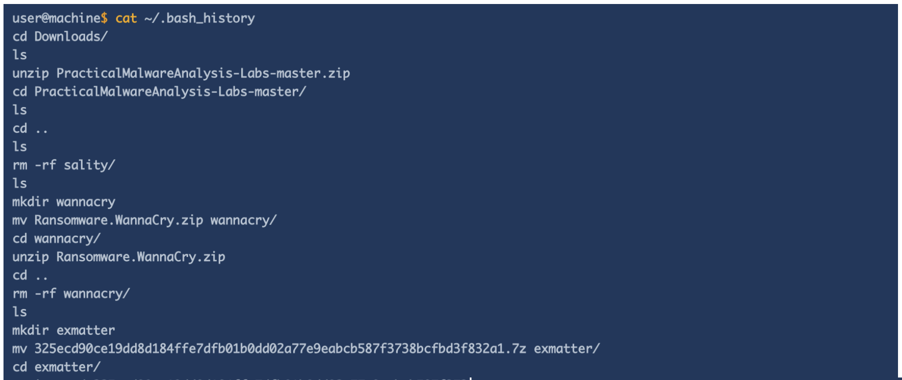
All the commands that are run on a Linux host using sudo are stored in the auth log. Use the grep utility to filter out only the required information from the auth log.



```
user@machine$ cat /var/log/auth.log* |grep -i COMMAND|tail
Mar 29 17:28:58 tryhackme pkexec[1618]: ubuntu: Error executing command as another user: Not authorized [USER=root]
[TTY=unknown] [CWD=/home/ubuntu] [COMMAND=/usr/lib/update-notifier/package-system-locked]
Mar 29 17:49:52 tryhackme sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/cat /etc/sudoers
Mar 29 17:55:22 tryhackme sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/cat
/var/log/btmp
Mar 29 17:55:39 tryhackme sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/cat
/var/log/wtmp
Mar 29 18:00:54 tryhackme sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/tail -f
/var/log/btmp
Mar 29 18:01:24 tryhackme sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/last -f
/var/log/btmp
Mar 29 18:03:58 tryhackme sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/last -f
/var/log/wtmp
Mar 29 18:05:41 tryhackme sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/last -f
/var/log/btmp
Mar 29 18:07:51 tryhackme sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/last -f
/var/log/utmp
Mar 29 18:08:13 tryhackme sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/last -f
/var/run/utmp
```

Bash history

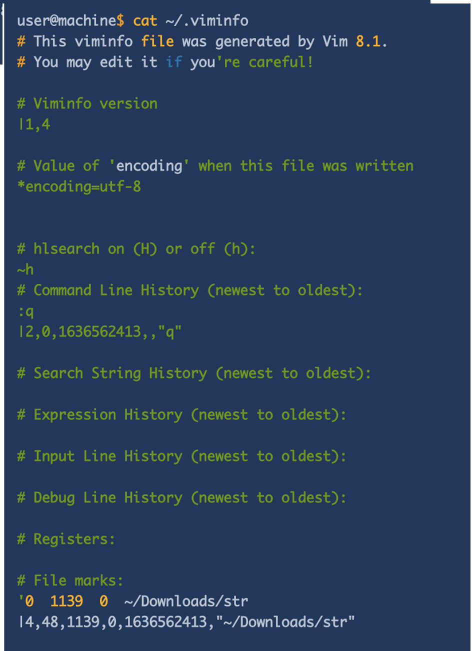
Any commands other than the ones run using sudo are stored in the bash history. Every user's bash history is stored separately in that user's home folder. Therefore, when examining bash history, we need to get the bash_history file from each user's home directory. Examine the bash history from the root user to make note of all the commands run using the root user too.



```
user@machine$ cat ~/.bash_history
cd Downloads/
ls
unzip PracticalMalwareAnalysis-Labs-master.zip
cd PracticalMalwareAnalysis-Labs-master/
ls
cd ..
ls
rm -rf sality/
ls
mkdir wannacry
mv Ransomware.WannaCry.zip wannacry/
cd wannacry/
unzip Ransomware.WannaCry.zip
cd ..
rm -rf wannacry/
ls
mkdir exmatter
mv 325ecd90ce19dd8d184ffe7dfb01b0dd02a77e9eabcb587f3738bcfbd3f832a1.7z exmatter/
cd exmatter/
strings -d 325ecd90ce19dd8d184ffe7dfb01b0dd02a77e9eabcb587f373
cd ..
ls
```

File accessed using vim

The Vim text editor stores logs for opened files in Vim in the file named .viminfo in the home directory. This file contains command line history, search string history, etc. for the opened files. Use the cat utility to open .viminfo



```
user@machine$ cat ~/.viminfo
# This viminfo file was generated by Vim 8.1.
# You may edit it if you're careful!

# Viminfo version
|1,4

# Value of 'encoding' when this file was written
*encoding=utf-8


# hlsearch on (H) or off (h):
~h
# Command Line History (newest to oldest):
:q
|2,0,1636562413,,"q"

# Search String History (newest to oldest):

# Expression History (newest to oldest):

# Input Line History (newest to oldest):

# Debug Line History (newest to oldest):

# Registers:

# File marks:
'0  1139  0  ~/Downloads/str
|4,48,1139,0,1636562413,"~/Downloads/str"
```

Linux Forensics

QUESTIONS

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

sudo apt-get install apache2

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

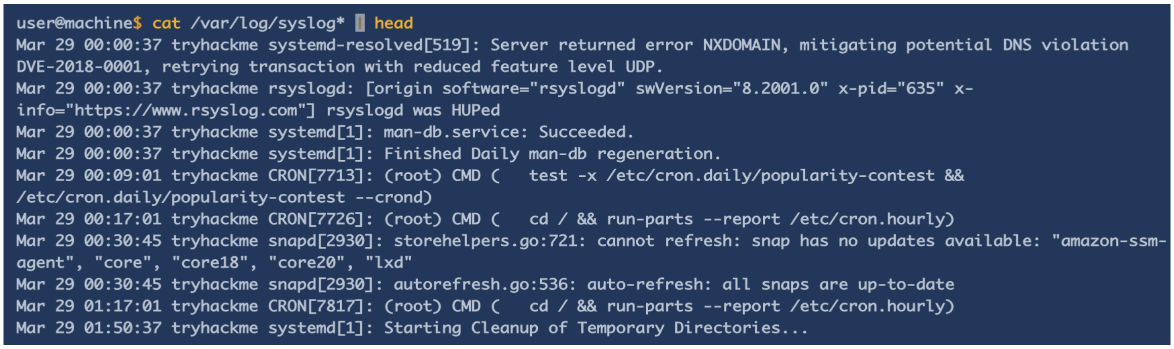
/home/ubuntu

LOG FILES

Syslog

/var/log directory

The Syslog contains messages that are recorded by the host about system activity. The detail which is recorded in these messages is configurable through the logging level. We can use the cat utility to view the Syslog, which can be found in the file /var/log/syslog. Since the Syslog is a big file, it is easier to use tail, head, more or less utilities to help make it more readable.



```
user@machine$ cat /var/log/syslog* | head
Mar 29 00:00:37 tryhackme systemd-resolved[519]: Server returned error NXDOMAIN, mitigating potential DNS violation
DVE-2018-0001, retrying transaction with reduced feature level UDP.
Mar 29 00:00:37 tryhackme rsyslogd: [origin software="rsyslogd" swVersion="8.2001.0" x-pid="635" x-
info="https://www.rsyslog.com"] rsyslogd was HUPed
Mar 29 00:00:37 tryhackme systemd[1]: man-db.service: Succeeded.
Mar 29 00:00:37 tryhackme systemd[1]: Finished Daily man-db regeneration.
Mar 29 00:09:01 tryhackme CRON[7713]: (root) CMD (   test -x /etc/cron.daily/popularity-contest &&
/etc/cron.daily/popularity-contest --crond)
Mar 29 00:17:01 tryhackme CRON[7726]: (root) CMD (   cd / && run-parts --report /etc/cron.hourly)
Mar 29 00:30:45 tryhackme snapd[2930]: storehelpers.go:721: cannot refresh: snap has no updates available: "amazon-ssm-
agent", "core", "core18", "core20", "lxd"
Mar 29 00:30:45 tryhackme snapd[2930]: autorefresh.go:536: auto-refresh: all snaps are up-to-date
Mar 29 01:17:01 tryhackme CRON[7817]: (root) CMD (   cd / && run-parts --report /etc/cron.hourly)
Mar 29 01:50:37 tryhackme systemd[1]: Starting Cleanup of Temporary Directories...
```

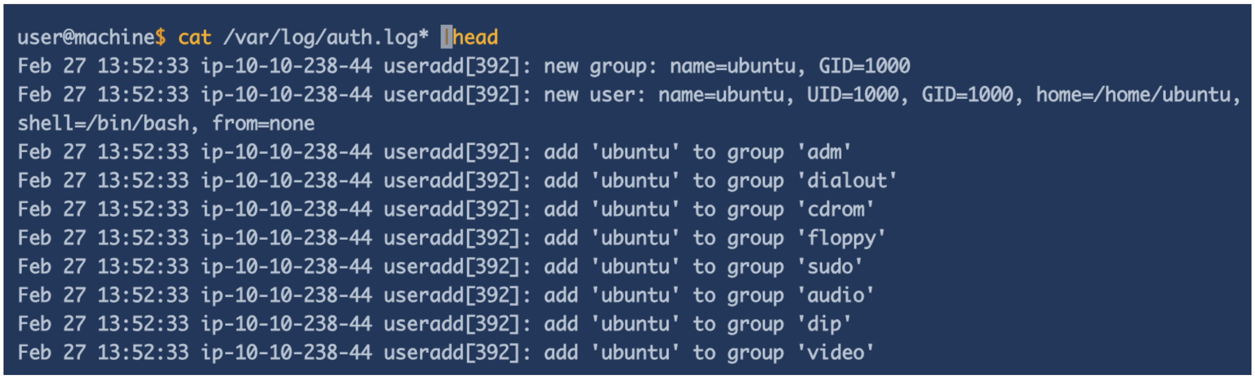
The above terminal shows the system time, system name, the process that sent the log [the process id], and the details of the log.

Linux Forensics

See a couple of cron jobs being run here in the logs above, apart from some other activity.
See an asterisk(*) after the syslog. This is to include rotated logs as well. With the passage of time, the Linux machine rotates older logs into files such as syslog.1, syslog.2 etc, so that the syslog file doesn't become too big.
In order to search through all of the syslogs, use the asterisk(*) wildcard.

Auth logs

The auth logs contain information about users and authentication-related logs. The below terminal shows a sample of the auth logs.

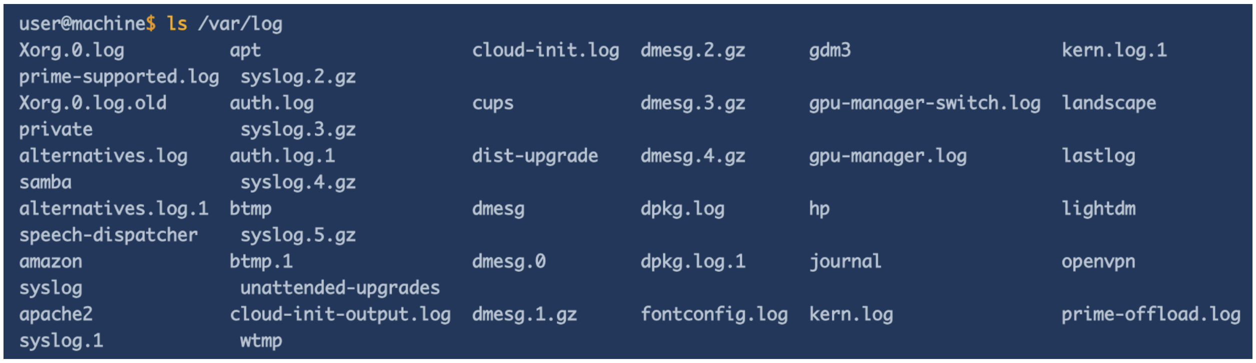


```
user@machine$ cat /var/log/auth.log* |head
Feb 27 13:52:33 ip-10-10-238-44 useradd[392]: new group: name=ubuntu, GID=1000
Feb 27 13:52:33 ip-10-10-238-44 useradd[392]: new user: name=ubuntu, UID=1000, GID=1000, home=/home/ubuntu,
shell=/bin/bash, from=none
Feb 27 13:52:33 ip-10-10-238-44 useradd[392]: add 'ubuntu' to group 'adm'
Feb 27 13:52:33 ip-10-10-238-44 useradd[392]: add 'ubuntu' to group 'dialout'
Feb 27 13:52:33 ip-10-10-238-44 useradd[392]: add 'ubuntu' to group 'cdrom'
Feb 27 13:52:33 ip-10-10-238-44 useradd[392]: add 'ubuntu' to group 'floppy'
Feb 27 13:52:33 ip-10-10-238-44 useradd[392]: add 'ubuntu' to group 'sudo'
Feb 27 13:52:33 ip-10-10-238-44 useradd[392]: add 'ubuntu' to group 'audio'
Feb 27 13:52:33 ip-10-10-238-44 useradd[392]: add 'ubuntu' to group 'dip'
Feb 27 13:52:33 ip-10-10-238-44 useradd[392]: add 'ubuntu' to group 'video'
```

See above that the log stored information about the creation of a new group, a new user, and the addition of the user into different groups.

Third-party logs

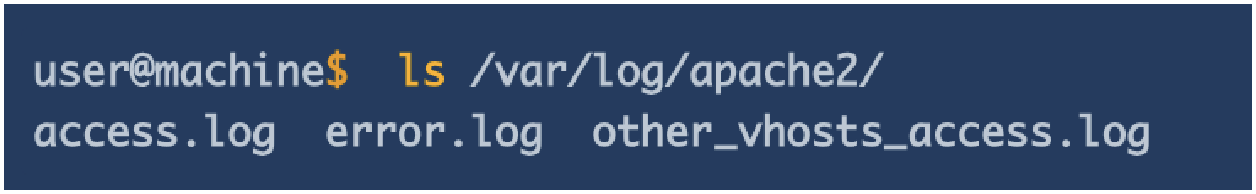
Similar to the syslog and authentication logs, the /var/log/ directory contains logs for third-party applications such as webserver, database, or file share server logs. Investigate these by looking at the /var/log/ directory.



```
user@machine$ ls /var/log
Xorg.0.log          apt                    cloud-init.log  dmesg.2.gz      gdm3                    kern.log.1
prime-supported.log  syslog.2.gz
Xorg.0.log.old      auth.log               cups            dmesg.3.gz      gpu-manager-switch.log  landscape
private              syslog.3.gz
alternatives.log    auth.log.1             dist-upgrade    dmesg.4.gz      gpu-manager.log         lastlog
samba                syslog.4.gz
alternatives.log.1  btmp                   dmesg           dpkg.log        hp                      lightdm
speech-dispatcher    syslog.5.gz
amazon              btmp.1                 dmesg.0         dpkg.log.1      journal                 openvpn
syslog               unattended-upgrades
apache2             cloud-init-output.log  dmesg.1.gz      fontconfig.log  kern.log                prime-offload.log
syslog.1             wtmp
```

Find the apache logs in the apache2 directory and samba logs in the samba directory.

Linux Forensics



```
user@machine$  ls /var/log/apache2/
access.log  error.log  other_vhosts_access.log
```

If any database server like MySQL is installed on the system, find the logs in this directory.

QUESTIONS

1. **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?**

tryhackme