Linux Fundamentals Part 3

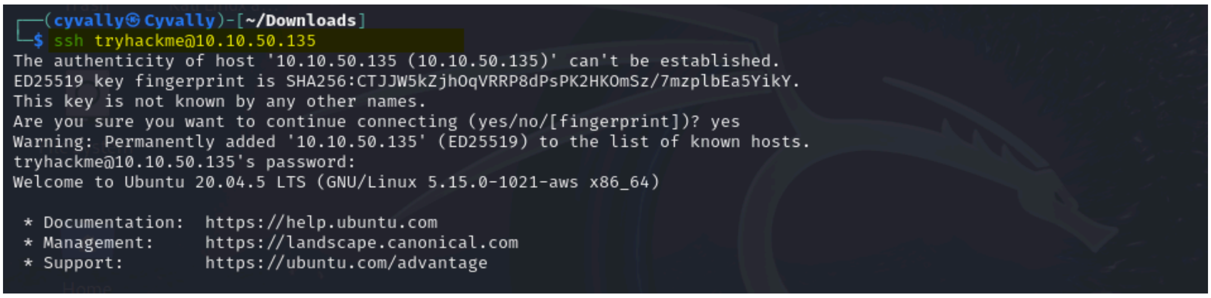
Power-up your Linux skills and get hands-on with some common utilities that you are likely to use day-to-day!

Connection

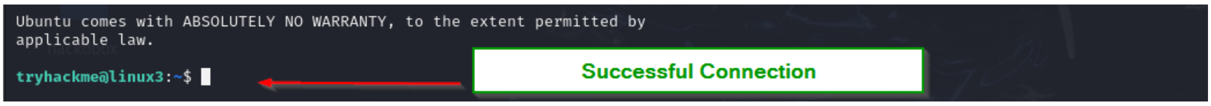
I ssh to this lab on my kali linux

Command: ssh tryhackme@10.10.50.135

Password: tryhackme



```
┌──(cyvally㉿Cyvally)-[~/Downloads]
└─$ ssh tryhackme@10.10.50.135
The authenticity of host '10.10.50.135 (10.10.50.135)' can't be established.
ED25519 key fingerprint is SHA256:CTJJW5kZjhOqVRRP8dPsPK2HKOmSz/7mzplbEa5YikY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.50.135' (ED25519) to the list of known hosts.
tryhackme@10.10.50.135's password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.15.0-1021-aws x86_64)

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



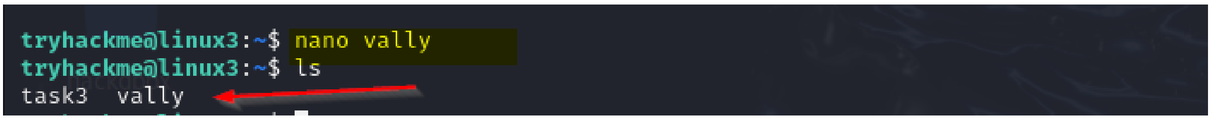
```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

tryhackme@linux3:~$
```

Task 3 Terminal Text Editors

Create a file using Nano

I created a file called vally

Command: nano vally

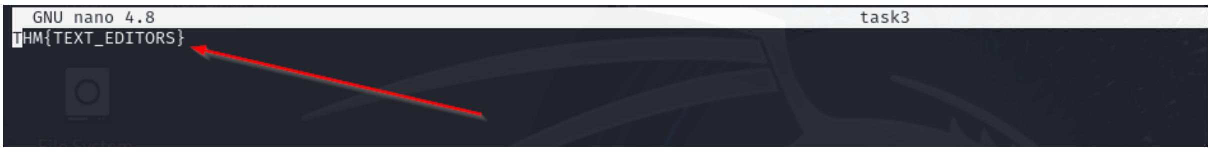


```
tryhackme@linux3:~$ nano vally
tryhackme@linux3:~$ ls
task3  vally
```

Edit "task3" located in "tryhackme"'s home directory using Nano. What is the flag?

Command: nano task3

Answer: thm{text_editors}

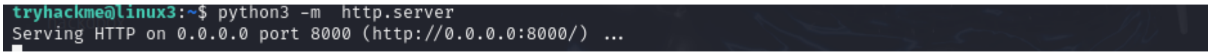


```
  GNU nano 4.8                                                                task3
THM{TEXT_EDITORS}
```

Task 4 General/Useful Utilities

Now, use Python 3's "HTTPServer" module to start a web server in the home directory of the "tryhackme" user on the deployed instance.

Command: python3 -m http.server



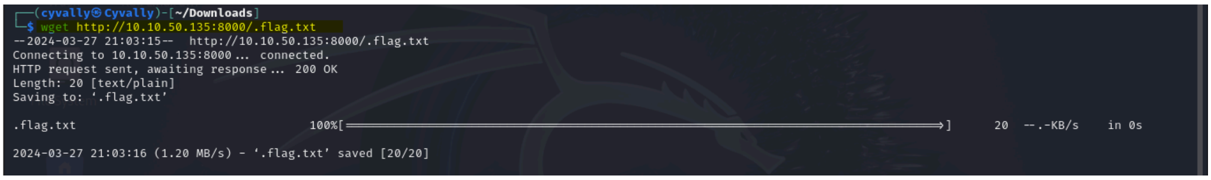
```
tryhackme@linux3:~$ python3 -m  http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Download the file http://10.10.50.135:8000/.flag.txt onto the TryHackMe AttackBox. Remember, you will need to do this in a new terminal.

What are the contents?

Using wget to download the file

Command: wget http://10.10.50.135:8000/.flag.txt

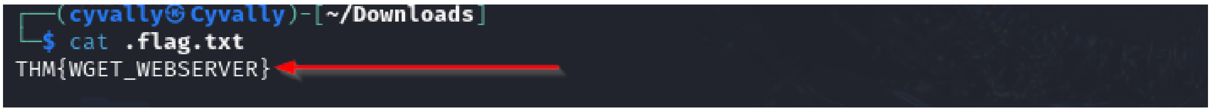


```
┌──(cyvally㉿Cyvally)-[~/Downloads]
└─$ wget http://10.10.50.135:8000/.flag.txt
--2024-03-27 21:03:15--  http://10.10.50.135:8000/.flag.txt
Connecting to 10.10.50.135:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 20 [text/plain]
Saving to: '.flag.txt'

.flag.txt                    100%[==========================================>]      20  --.-KB/s    in 0s

2024-03-27 21:03:16 (1.20 MB/s) - '.flag.txt' saved [20/20]
```

And cat command to output the content of .flag.txt

Command: cat .flag.txt

Answer: THM{WGET_WEBSERVER}



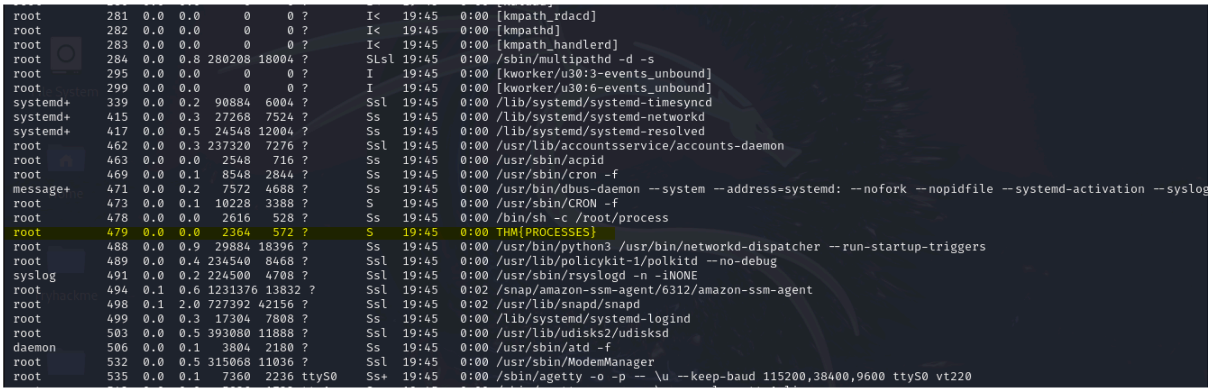
```
┌──(cyvally㉿Cyvally)-[~/Downloads]
└─$ cat .flag.txt
THM{WGET_WEBSERVER}
```

Task 5: Processes 101

Question	Answer
If we were to launch a process where the previous ID was "300", what would the ID of this new process be?	301
If we wanted to cleanly kill a process, what signal would we send it?	sigterm

Locate the process that is running on the deployed instance (10.10.50.135). What flag is given?

Command: ps aux
Answer: thm{processes}



```
root        281  0.0  0.0      0     0 ?        I<   19:45   0:00 [kmpath_rdacd]
root        282  0.0  0.0      0     0 ?        I<   19:45   0:00 [kmpathd]
root        283  0.0  0.0      0     0 ?        I<   19:45   0:00 [kmpath_handlerd]
root        284  0.0  0.8 280208 18004 ?        SLsl 19:45   0:00 /sbin/multipathd -d -s
root        295  0.0  0.0      0     0 ?        I    19:45   0:00 [kworker/u30:3-events_unbound]
root        299  0.0  0.0      0     0 ?        I    19:45   0:00 [kworker/u30:6-events_unbound]
systemd+    339  0.0  0.2  90884  6004 ?        Ssl  19:45   0:00 /lib/systemd/systemd-timesyncd
systemd+    415  0.0  0.3  27268  7524 ?        Ss   19:45   0:00 /lib/systemd/systemd-networkd
systemd+    417  0.0  0.5  24548 12004 ?        Ss   19:45   0:00 /lib/systemd/systemd-resolved
root        462  0.0  0.3 237320  7276 ?        Ssl  19:45   0:00 /usr/lib/accountsservice/accounts-daemon
root        463  0.0  0.0   2548   716 ?        Ss   19:45   0:00 /usr/sbin/acpid
root        469  0.0  0.1   8548  2844 ?        Ss   19:45   0:00 /usr/sbin/cron -f
message+    471  0.0  0.2   7572  4688 ?        Ss   19:45   0:00 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog
root        473  0.0  0.1  10228  3388 ?        S    19:45   0:00 /usr/sbin/CRON -f
root        478  0.0  0.0   2616   528 ?        Ss   19:45   0:00 /bin/sh -c /root/process
root        479  0.0  0.0   2364   572 ?        S    19:45   0:00 THM{PROCESSES}
root        488  0.0  0.9  29884 18396 ?        Ss   19:45   0:00 /usr/bin/python3 /usr/bin/networkd-dispatcher --run-startup-triggers
root        489  0.0  0.4 234540  8468 ?        Ssl  19:45   0:00 /usr/lib/policykit-1/polkitd --no-debug
syslog      491  0.0  0.2 224500  4708 ?        Ssl  19:45   0:00 /usr/sbin/rsyslogd -n -iNONE
root        494  0.1  0.6 1231376 13832 ?       Ssl  19:45   0:02 /snap/amazon-ssm-agent/6312/amazon-ssm-agent
root        498  0.1  2.0 727392 42156 ?        Ssl  19:45   0:02 /usr/lib/snapd/snapd
root        499  0.0  0.3  17304  7808 ?        Ss   19:45   0:00 /lib/systemd/systemd-logind
root        503  0.0  0.5 393080 11888 ?        Ssl  19:45   0:00 /usr/lib/udisks2/udisksd
daemon      506  0.0  0.1   3804  2180 ?        Ss   19:45   0:00 /usr/sbin/atd -f
root        532  0.0  0.5 315068 11036 ?        Ssl  19:45   0:00 /usr/sbin/ModemManager
root        535  0.0  0.1   7360  2236 ttyS0    Ss+  19:45   0:00 /sbin/agetty -o -p -- \u --keep-baud 115200,38400,9600 ttyS0 vt220
```

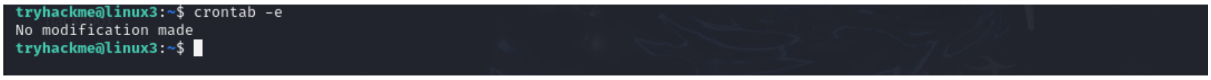
Question	Answer
What command would we use to stop the service "myservice"?	systemctl stop myservice
What command would we use to start the same service on the boot-up of the system?	systemctl enable myservice
What command would we use to bring a previously backgrounded process back	fg

to the foreground?	

Task 6 Maintaining Your System: Automation

Ensure you are connected to the deployed instance and look at the running crontabs.

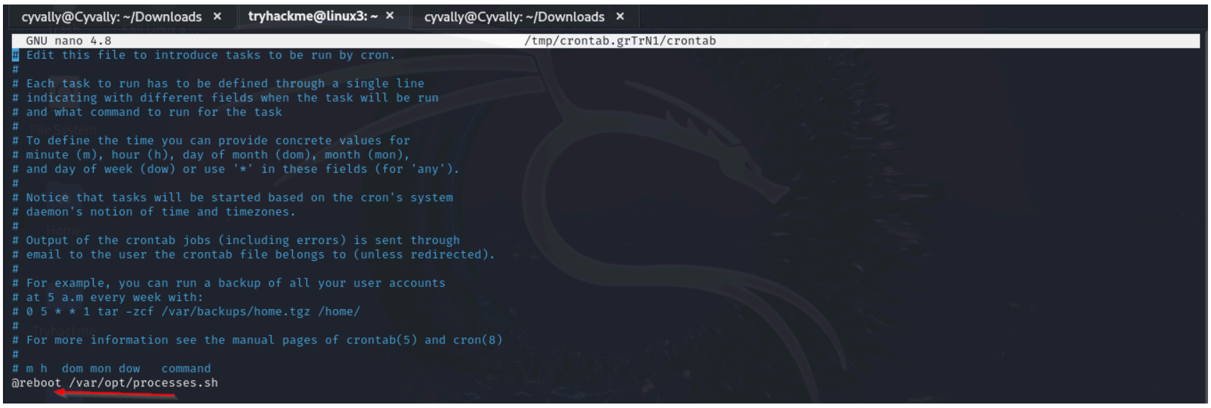
Command: crontab -e



```
tryhackme@linux3:~$ crontab -e
No modification made
tryhackme@linux3:~$ 
```

When will the crontab on the deployed instance (10.10.50.135) run?

Answer: @reboot


cyvally@Cyvally: ~/Downloads ×
tryhackme@linux3: ~ ×
cyvally@Cyvally: ~/Downloads ×

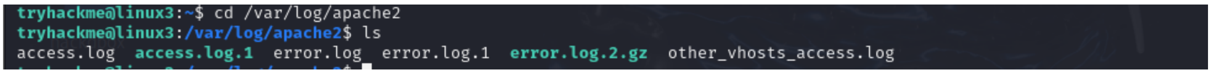
```
  GNU nano 4.8                                    /tmp/crontab.grTrN1/crontab
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
@reboot /var/opt/processes.sh
```

Task 8 Maintaining Your System: Logs

Look for the apache2 logs on the deployable Linux machine

I changed to the /var/log/apache2 directory

Command: cd /var/log/apache2

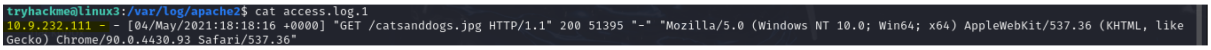


```
tryhackme@linux3:~$ cd /var/log/apache2
tryhackme@linux3:/var/log/apache2$ ls
access.log  access.log.1  error.log  error.log.1  error.log.2.gz  other_vhosts_access.log
```

What is the IP address of the user who visited the site?

Command: cat access.log.1

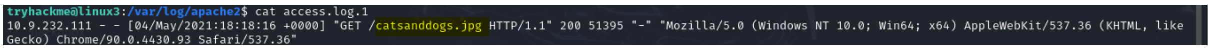
Answer:10.9.232.111



```
tryhackme@linux3:/var/log/apache2$ cat access.log.1
10.9.232.111 - - [04/May/2021:18:18:16 +0000] "GET /catsanddogs.jpg HTTP/1.1" 200 51395 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/90.0.4430.93 Safari/537.36"
```

What file did they access?

Answer: catsanddogs.jpg



```
tryhackme@linux3:/var/log/apache2$ cat access.log.1
10.9.232.111 - - [04/May/2021:18:18:16 +0000] "GET /catsanddogs.jpg HTTP/1.1" 200 51395 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/90.0.4430.93 Safari/537.36"
```

END!!!