

LINUX FUNDAMENTALS TASKS

I.I System information

Questions

The screenshot shows the Hack The Box Academy interface for the 'System information' module. At the top, there is a warning banner: "There is an issue with a 3rd-party service provider, affecting the proper rendering of our platform. Our engineers are working with the third-party provider to resolve the issue as soon as possible." Below the banner, the interface displays the following questions and answers:

- Question 0: "Find out the machine hardware name and submit it as the answer." Answer: `x86_64`
- Question 1: "What is the path to htb-student's home directory?" Answer: `/home/htb-student`
- Question 0: "What is the path to the htb-student's mail?" Answer: `/var/mail/htb-student`

Each question has a "Submit" button and a "Hint" button (for Question 0). A "Life Left: 21 minute(s)" timer is visible at the top left of the question area.

The screenshot shows the Hack The Box Academy interface for the 'System information' module, continuing from the previous section. The warning banner is still present. The interface displays the following questions and answers:

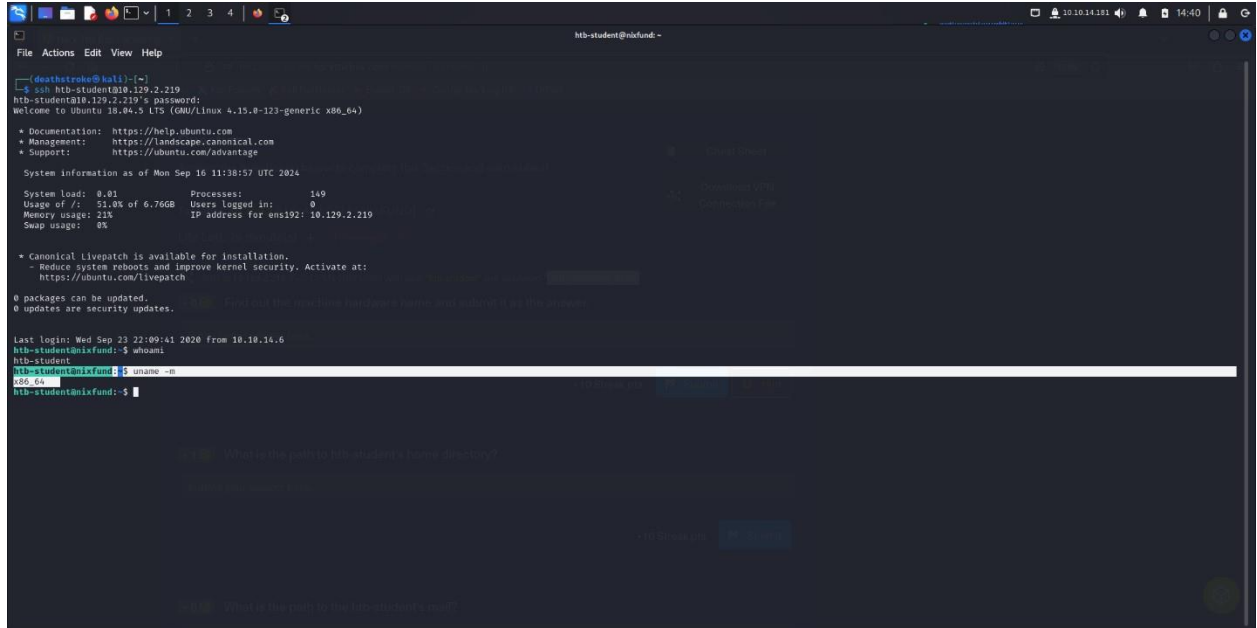
- Question 0: "Which shell is specified for the htb-student user?" Answer: `/bin/bash`
- Question 0: "Which kernel version is installed on the system? (Format: 1.22.3)" Answer: `4.15.0`
- Question 1: "What is the name of the network interface that MTU is set to 1500?" Answer: `ens192`

Each question has a "Submit" button. A green cube icon is visible in the bottom right corner of the interface.

Solution

I started off by connecting remotely to the target using SSH and target IP, Username and password

Used the `uname -m` found the machine hardware name.



```
deathstroke@kali:~$ ssh htb-student@10.129.2.219
htb-student@10.129.2.219's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-123-generic x86_64)

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

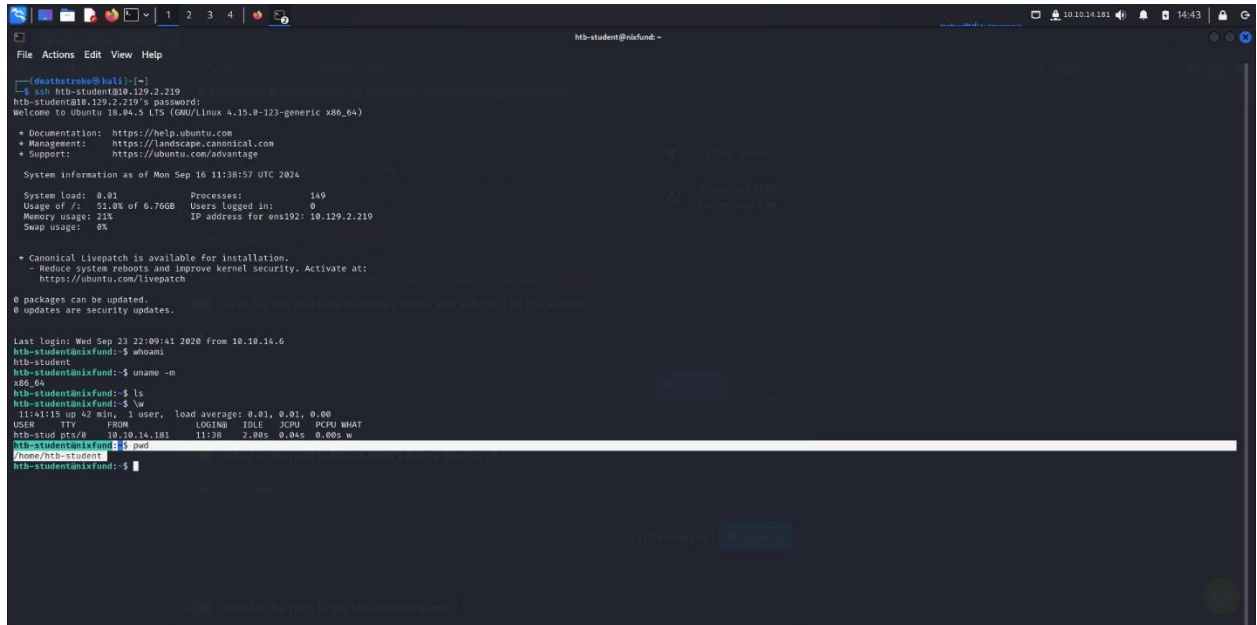
System information as of Mon Sep 16 11:38:57 UTC 2020
System load: 0.01          Processes: 149
Usage of /: 51.0% of 6.76GB Users logged in: 0
Memory usage: 21%         IP address for ens192: 10.129.2.219
Swap usage: 0%

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

0 packages can be updated.
0 updates are security updates.

Last login: Wed Sep 23 22:09:41 2020 from 10.10.14.6
htb-student@nixfund:~$ whoami
htb-student
htb-student@nixfund:~$ uname -m
x86_64
htb-student@nixfund:~$
```

Used the command `pwd`, it printed the working directory



```
htb-student@nixfund:~$ pwd
/home/htb-student
htb-student@nixfund:~$
```

Used the command `env` for printing the environment, found the path to mail

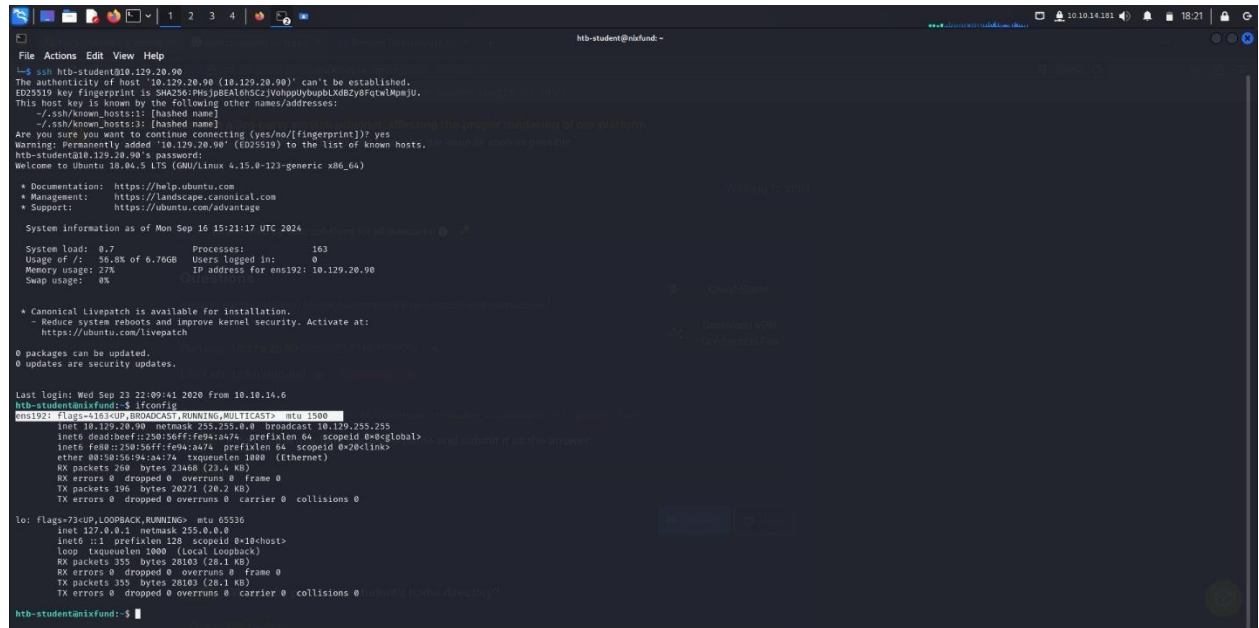
```
File Actions Edit View Help
0 packages can be updated.
0 updates are security updates.

Last login: Wed Sep 23 22:09:41 2020 from 10.10.14.6
htb-student@nixfund:~$ whoami
htb-student
htb-student@nixfund:~$ uname -m
x86_64
htb-student@nixfund:~$ ls
htb-student@nixfund:~$ w
   11:41:15 up 42 min, 1 user, load average: 0.01, 0.01, 0.00
USER      TTY      FROM            LOGIN#   IDLE   JCPU   PCPU   WHAT
htb-stud pts/0    10.10.14.101    11:38    2.00s  0.04s  0.00s  w
htb-student@nixfund:~$ pwd
/home/htb-student
htb-student@nixfund:~$ cd /var
htb-student@nixfund:/var$ ls
backups cache extra lib locale lock log mail opt rpm snap spoof top www
htb-student@nixfund:/var$ cd mail
htb-student@nixfund:/var/mail$ pwd
/var/mail
htb-student@nixfund:/var/mail$ ls
htb-student@nixfund:/var/mail$ env
IFS=
COLORTERM=true
HOME=/home/htb-student
LANG=en_US.UTF-8
LOGNAME=htb-student
MAIL=/var/mail/htb-student
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
PWD=/var/mail
SHELL=/bin/bash
SHVL=1
TERM=xterm-256color
USER=htb-student
XDG_DATA_DIRS=/usr/local/share:/usr/share:/var/lib/containers/desktop
XDG_SESSION_ID=1
XDG_USER_CONFIG_HOME=/home/htb-student/.config
_XDG_CURRENT_DESKTOP=XFCE
```

Used uname with -r I found the version of the kernel

[illegible]

used the ifconfig command, viewed the network interfaces, and found the one with MTU is set to 1500



```
File Actions Edit View Help
~$ ssh htb-student@10.129.20.90
The authenticity of host '10.129.20.90 (10.129.20.90)' can't be established.
ED25519 key fingerprint is SHA256:PHSjpeAEAlhsczjVohgpybupbLMBZy8FgtwLWpWJU.
This host key is known by the following other names/addresses:
  ./.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.20.90' (ED25519) to the list of known hosts.
htb-student@10.129.20.90's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-123-generic x86_64)

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

System information as of Mon Sep 16 15:21:17 UTC 2024

System load: 0.7          Processes:           163
Usage of /:  56.8% of 6.7GB  Users logged in:    0
Memory usage: 27%          IP address for ens192: 10.129.20.90
Swap usage:  0%

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

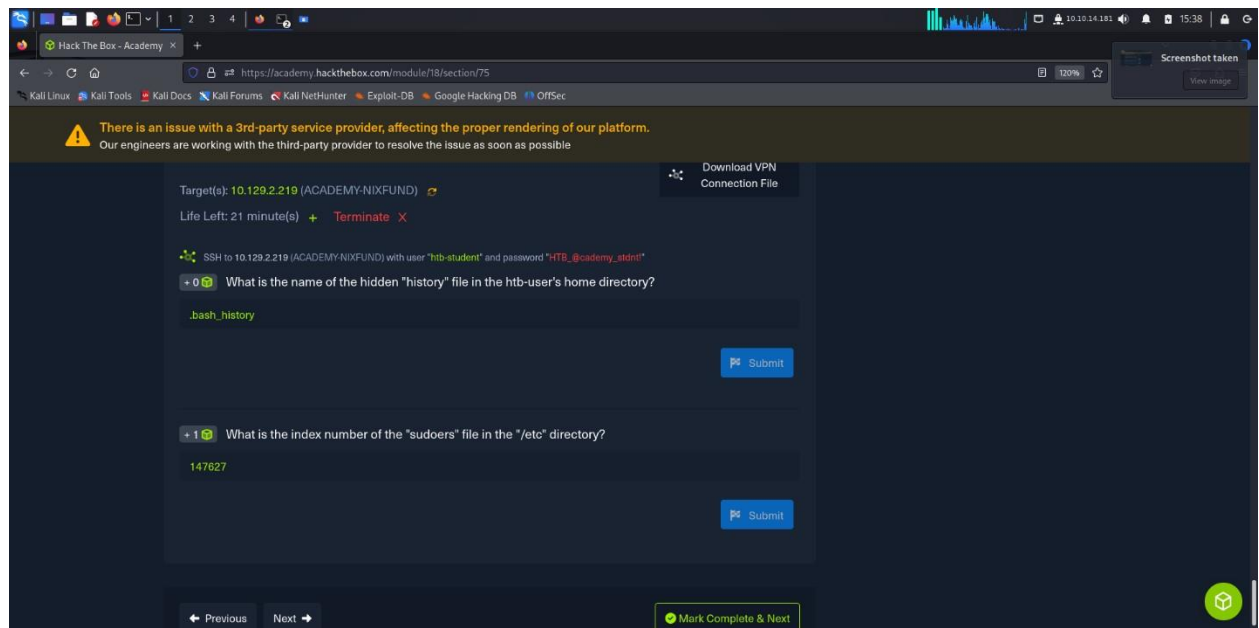
0 packages can be updated.
0 updates are security updates.

Last login: Wed Sep 22 22:09:41 2020 from 10.10.14.6
htb-student@nixfund:~$ ifconfig
ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.129.20.90 netmask 255.255.0.0 broadcast 10.129.255.255
    inet6 dead:beef::250:56ff:fe94:a474 prefixlen 64 scopeid 0<global>
    inet6 fe88::250:56ff:fe94:a474 prefixlen 64 scopeid 0<20<link>
    ether 8a:15:20:56:94:a474 txqueuelen 1000 (Ethernet)
    RX packets 268 bytes 23468 (23.4 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 196 bytes 20271 (20.2 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<localhost>
    loop 1:queuelen 1000 (local loopback)
    RX packets 355 bytes 28103 (28.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 355 bytes 28271 (28.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

1.2 Navigation

Questions



There is an issue with a 3rd-party service provider, affecting the proper rendering of our platform. Our engineers are working with the third-party provider to resolve the issue as soon as possible.

Target(s): 10.129.2.219 (ACADEMY-NIXFUND) [Download VPN Connection File](#)

Life Left: 21 minute(s) [+ Terminate](#)

SSH to 10.129.2.219 (ACADEMY-NIXFUND) with user "htb-student" and password "HTB_Academy_stdnt"

+0 What is the name of the hidden "history" file in the htb-user's home directory?

`.bash_history`

[Submit](#)

+1 What is the index number of the "sudoers" file in the "/etc" directory?

`147627`

[Submit](#)

[Previous](#) [Next](#) [Mark Complete & Next](#)

Solution

Used the ls command with -ls to view hidden files, found the hidden file

```
htb-student@nixfud:~$ ls
bin boot cdrom dev etc home initrd.img  initrd.img.old lib lib64 lost+found media mnt opt proc root run sbin snap srv sys  usr var vmlinuz vmlinuz.old
htb-student@nixfud:~$ cd home/htb-student
htb-student@nixfud:~/home/htb-student$ ls -la
total 92
drwxr-xr-x 4 htb-student htb-student 4096 Aug 3 2021 .
drwxr-xr-x 3 root        root        4096 Aug 3 2021 ..
-rw-r--r-- 1 htb-student htb-student 228 Apr 4 2018 .bash_history
-rw-r--r-- 1 htb-student htb-student 3771 Apr 4 2018 .bashrc
-rw-r--r-- 2 htb-student htb-student 4096 Aug 3 2021 .cache
-rw-r--r-- 3 htb-student htb-student 4096 Aug 3 2021 .gnupg
-rw-r--r-- 1 htb-student htb-student 887 Apr 4 2018 .profile
htb-student@nixfud:~/home/htb-student$
```

Used ls command an -i, list the files with their index numbers.

```
htb-student@nixfud:~$ ls -li
total 92
146877 drwxr-xr-x 4 htb-student htb-student 4096 Aug 3 2021 .
146878 drwxr-xr-x 3 root        root        4096 Aug 3 2021 ..
146879 -rw-r--r-- 1 htb-student htb-student 228 Apr 4 2018 .bash_history
146880 -rw-r--r-- 1 htb-student htb-student 3771 Apr 4 2018 .bashrc
146881 -rw-r--r-- 2 htb-student htb-student 4096 Aug 3 2021 .cache
146882 -rw-r--r-- 3 htb-student htb-student 4096 Aug 3 2021 .gnupg
146883 -rw-r--r-- 1 htb-student htb-student 887 Apr 4 2018 .profile
htb-student@nixfud:~/home/htb-student$
```

1.3 Working with directory

Question

There is an issue with a 3rd-party service provider, affecting the proper rendering of our platform. Our engineers are working with the third-party provider to resolve the issue as soon as possible.

Success
Congratulations! You earned 1 cubes!

SSH to 10.129.195.145 (ACADEMY-NIXFUND) with user "htb-student" and password "HTB_@cademy_student!"

What is the name of the last modified file in the "/var/backups" directory?

apt.extended_states.0

Submit

What is the inode number of the "shadow.bak" file in the "/var/backups" directory?

265293

Submit

Previous Next

Powered by HACKTHEBOX

Solution

Used ls and -la and the path /var/backups I found the file name and compared the dates

```
htb-student@nixfund:~$ ls -la /var/backups
total 2160
drwxr-xr-x 2 root root 4096 Aug 3 2021 .
drwxr-xr-x 14 root root 4096 Sep 23 2020 ..
-rw-r--r-- 1 root root 51200 Oct 29 2020 alternatives.tar.gz
-rw-r--r-- 1 root root 2497 Oct 16 2020 alternatives.tar.gz
-rw-r--r-- 1 root root 1492 Sep 24 2020 alternatives.tar.gz
-rw-r--r-- 1 root root 41872 Nov 12 2020 apt.extended_states.0
-rw-r--r-- 1 root root 4437 Nov 12 2020 apt.extended_states.1.gz
-rw-r--r-- 1 root root 4623 Oct 22 2020 apt.extended_states.1.gz
-rw-r--r-- 1 root root 4681 Oct 15 2020 apt.extended_states.3.gz
-rw-r--r-- 1 root root 4572 Sep 23 2020 apt.extended_states.4.gz
-rw-r--r-- 1 root root 437 Aug 5 2019 dpkg.diversions.0
-rw-r--r-- 1 root root 282 Aug 5 2019 dpkg.diversions.1.gz
-rw-r--r-- 1 root root 282 Aug 5 2019 dpkg.diversions.2.gz
-rw-r--r-- 1 root root 282 Aug 5 2019 dpkg.diversions.3.gz
-rw-r--r-- 1 root root 282 Aug 5 2019 dpkg.diversions.4.gz
-rw-r--r-- 1 root root 282 Aug 5 2019 dpkg.diversions.5.gz
-rw-r--r-- 1 root root 367 Sep 23 2020 dpkg.statoverride.0
-rw-r--r-- 1 root root 229 Sep 23 2020 dpkg.statoverride.1.gz
-rw-r--r-- 1 root root 229 Sep 23 2020 dpkg.statoverride.1.gz
-rw-r--r-- 1 root root 229 Sep 23 2020 dpkg.statoverride.3.gz
-rw-r--r-- 1 root root 229 Sep 23 2020 dpkg.statoverride.4.gz
-rw-r--r-- 1 root root 229 Sep 23 2020 dpkg.statoverride.5.gz
-rw-r--r-- 1 root root 229 Sep 23 2020 dpkg.statoverride.6.gz
-rw-r--r-- 1 root root 742750 Nov 11 2020 dpkg.status.0
-rw-r--r-- 1 root root 286270 Nov 11 2020 dpkg.status.1.gz
-rw-r--r-- 1 root root 286270 Nov 5 2020 dpkg.status.2.gz
-rw-r--r-- 1 root root 286270 Nov 5 2020 dpkg.status.3.gz
-rw-r--r-- 1 root root 286270 Nov 5 2020 dpkg.status.4.gz
-rw-r--r-- 1 root root 286270 Nov 5 2020 dpkg.status.5.gz
-rw-r--r-- 1 root root 286270 Nov 5 2020 dpkg.status.6.gz
-rw-r--r-- 1 root root 860 Sep 23 2020 group.bak
-rw-r--r-- 1 root root 716 Sep 23 2020 shadow.bak
-rw-r--r-- 1 root root 2816 Sep 23 2020 shadow.bak
-rw-r--r-- 1 root root 1362 Sep 23 2020 shadow.bak
```

Used ls with -i it listed the files in backup with their index number.

```
htb-student@nixfund:~$ ls -i /var/backups
262248 alternatives.tar.0      266430 apt.extended_states.2.gz  262264 dpkg.diversions.2.gz  262231 dpkg.statoverride.0  262258 dpkg.statoverride.5.gz  262241 dpkg.status.2.gz  265817 gshadow.bak
262559 alternatives.tar.1.gz  264827 apt.extended_states.3.gz  262257 dpkg.diversions.3.gz  262285 dpkg.statoverride.1.gz  262236 dpkg.statoverride.6.gz  262243 dpkg.status.4.gz  264399 password.bak
262561 alternatives.tar.2.gz  262233 apt.extended_states.4.gz  262246 dpkg.diversions.4.gz  262218 dpkg.statoverride.2.gz  263999 dpkg.status.5.gz  262228 dpkg.status.5.gz  255252.gshadow.bak
266334 apt.extended_states.0  262178 dpkg.diversions.0        262249 dpkg.diversions.5.gz  262311 dpkg.statoverride.3.gz  262179 dpkg.status.1.gz  262238 dpkg.status.6.gz
266335 apt.extended_states.1.gz  262203 dpkg.diversions.1.gz      262235 dpkg.diversions.0.gz  262247 dpkg.statoverride.4.gz  262234 dpkg.status.3.gz  265226 group.bak
htb-student@nixfund:~$
```

1.4 Find Files and Directories

Questions

Life Left: 94 minute(s) + Terminate X

SSH to 10.129.204.122 (ACADEMY-NIXFUND) with user "htb-student" and password "HTB_Academy_student"

+1 What is the name of the config file that has been created after 2020-03-03 and is smaller than 28k but larger than 25k?

00-mesa-defaults.conf

Submit

+1 How many files exist on the system that have the ".bak" extension?

4

Submit

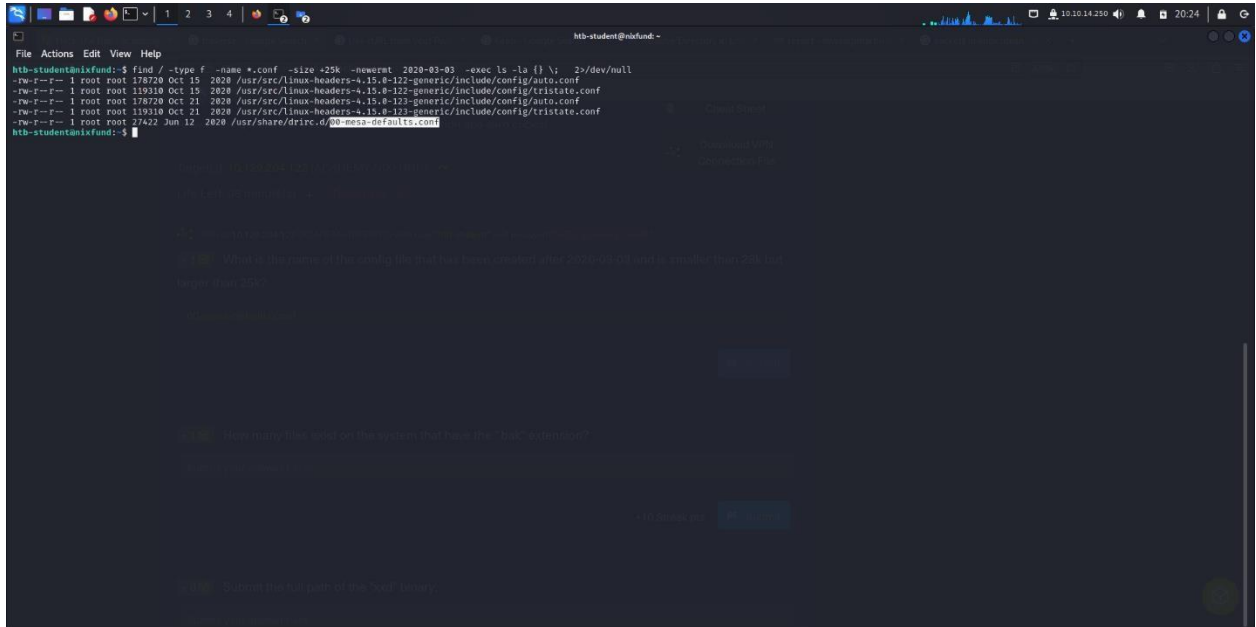
+0 Submit the full path of the "xxd" binary.

/usr/bin/xxd

Submit

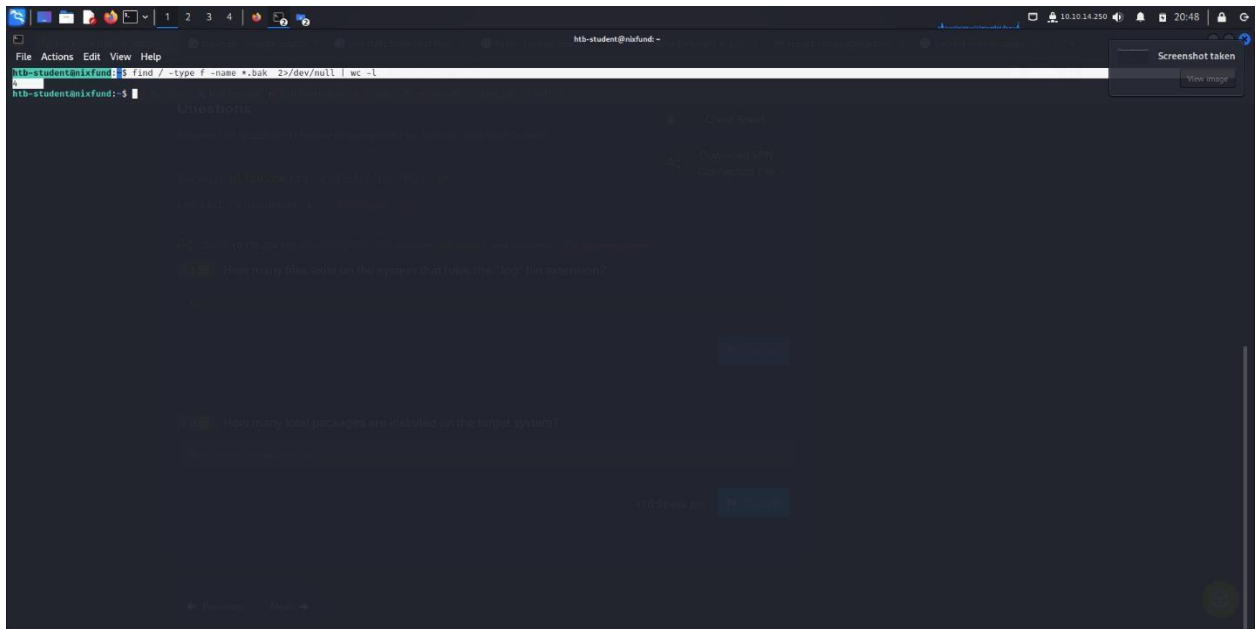
Solution

Used find command found the file that was new and more that 25k but less than 28k



```
htb-student@nixfund:~$ find / -type f -name *.conf -size +25k -newermt 2020-03-03 -exec ls -la {} \; 2>/dev/null
-rw-r--r-- 1 root root 178720 Oct 15 2020 /usr/src/linux-headers-4.15.0-122-generic/include/config/autos.conf
-rw-r--r-- 1 root root 119310 Oct 15 2020 /usr/src/linux-headers-4.15.0-122-generic/include/config/tristate.conf
-rw-r--r-- 1 root root 178720 Oct 21 2020 /usr/src/linux-headers-4.15.0-123-generic/include/config/autos.conf
-rw-r--r-- 1 root root 119310 Oct 21 2020 /usr/src/linux-headers-4.15.0-123-generic/include/config/tristate.conf
-rw-r--r-- 1 root root 27422 Jun 12 2020 /usr/share/doc/iptables-headers-1.4.21-1/include/config/tristate.conf
htb-student@nixfund:~$
```

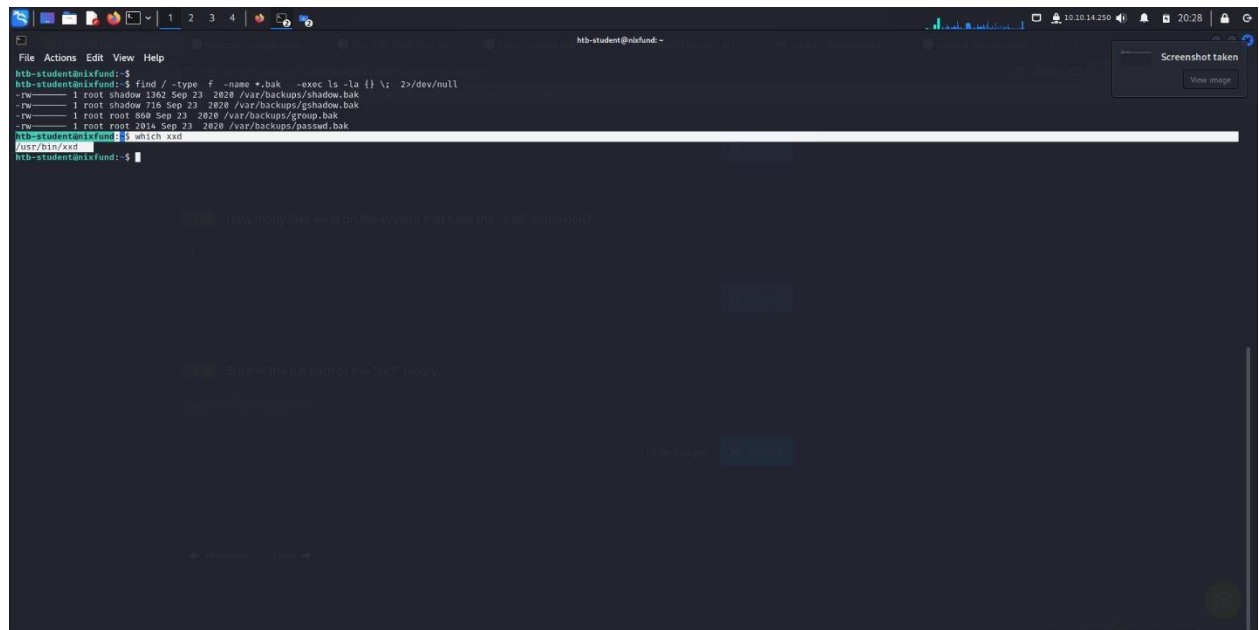
Used find and combining it with word count command (wc) found the number of files with .bak extension.



```
htb-student@nixfund:~$ find / -type f -name *.bak 2>/dev/null | wc -l
htb-student@nixfund:~$
```

Screenshot taken
View image

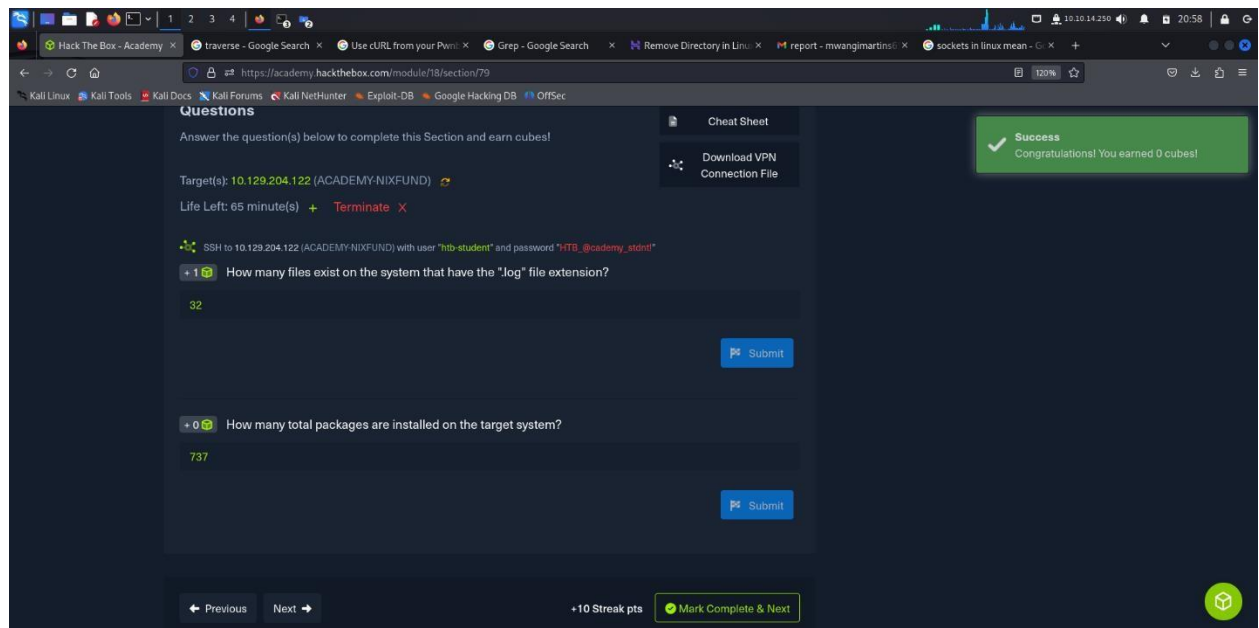
Used `find` which command found the path, to the file



```
htb-student@nixfund:~$ find / -type f -name *.bak -exec ls -la {} \; 2>/dev/null
-rw-r--r-- 1 root shadow 1362 Sep 23 2020 /var/backups/shadow.bak
-rw-r--r-- 1 root shadow 715 Sep 23 2020 /var/backups/gshadow.bak
-rw-r--r-- 1 root root 860 Sep 23 2020 /var/backups/group.bak
-rw-r--r-- 1 root root 2014 Sep 23 2020 /var/backups/passwd.bak
htb-student@nixfund:~$ which xxd
/usr/bin/xxd
htb-student@nixfund:~$
```

1.5 File Descriptors and Redirections

Questions



The screenshot shows the Hack The Box Academy interface. The page title is "Questions". The instructions state: "Answer the question(s) below to complete this Section and earn cubes!". The target is "10.129.204.122 (ACADEMY-NIXFUND)". The life left is "65 minute(s)". The user is "htb-student" and the password is "HTB_Academy_student!".

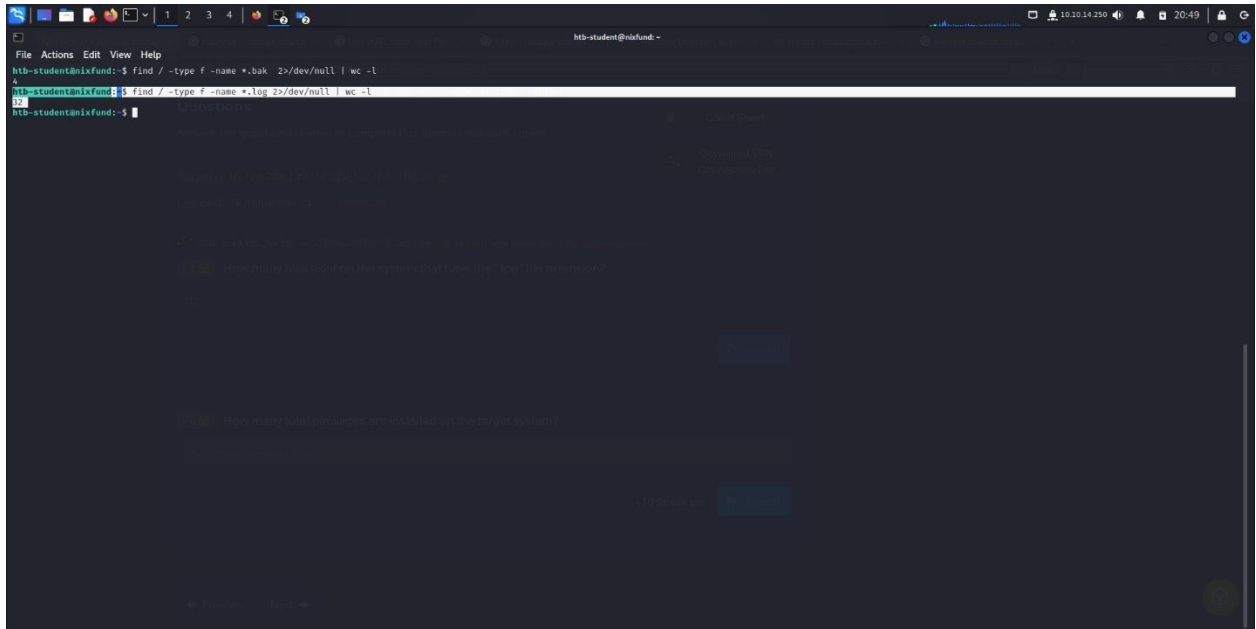
Question 1: "How many files exist on the system that have the '.log' file extension?". The answer is "32".

Question 2: "How many total packages are installed on the target system?". The answer is "737".

The interface includes a "Submit" button for each question and a "Success" message: "Congratulations! You earned 0 cubes!".

Solution

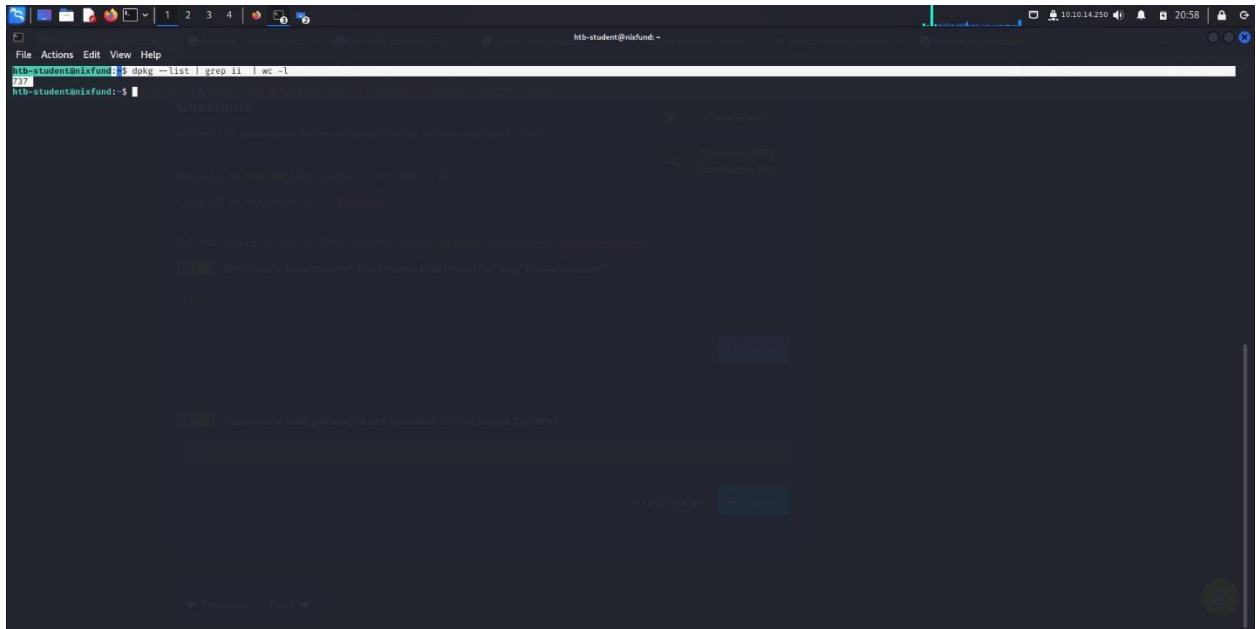
Used the find command and wc found number of files



A terminal window titled 'htb-student@nixfund: ~' showing a series of commands and their outputs. The user runs 'find / -type f -name *.bak 2>/dev/null | wc -l' which returns '4'. Then they run 'find / -type f -name *.log 2>/dev/null | wc -l' which returns '12'. The terminal also shows a 'Questions' section with a question about the number of total packages installed, with a 'Show Answer' button.

```
htb-student@nixfund:~$ find / -type f -name *.bak 2>/dev/null | wc -l
4
htb-student@nixfund:~$ find / -type f -name *.log 2>/dev/null | wc -l
12
htb-student@nixfund:~$
```

Used the command dpkg to check the number of installed packages in the system and combined with grep



A terminal window titled 'htb-student@nixfund: ~' showing a series of commands and their outputs. The user runs 'dpkg --get-selections | grep ii | wc -l' which returns '237'. The terminal also shows a 'Questions' section with a question about the number of total packages installed, with a 'Show Answer' button.

```
htb-student@nixfund:~$ dpkg --get-selections | grep ii | wc -l
237
htb-student@nixfund:~$
```

1.6 Filter Contents

Questions

Urgent maintenance required

Please use the EU VPN Servers until maintenance is completed.

How many services are listening on the target system on all interfaces? (Not on localhost and IPv4 only)

7

Submit

Determine what user the ProFTPD server is running under. Submit the username as the answer.

proftpd

Submit

Use curl from your Pwnbox (not the target machine) to obtain the source code of the "https://www.inlanefreight.com" website and filter all unique paths of that domain. Submit the number of these paths as the answer.

34

Submit

Solution

Used netstat got the results of the network status, and found the services listening,

File Actions Edit View Help

hth-student@nixfund:~\$ netstat -tlnp

Active Internet connections (only servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	localhost:domain	*.*.*.*.*	LISTEN	
tcp	0	0	0.0.0.0:ssh	0.0.0.0:*	LISTEN	
tcp	0	0	localhost:smtp	0.0.0.0:*	LISTEN	
tcp	0	0	0.0.0.0:microsoft-ds	0.0.0.0:*	LISTEN	
tcp	0	0	0.0.0.0:imap5	0.0.0.0:*	LISTEN	
tcp	0	0	0.0.0.0:pop3s	0.0.0.0:*	LISTEN	
tcp	0	0	localhost:mysql	0.0.0.0:*	LISTEN	
tcp	0	0	0.0.0.0:netbios-ssn	0.0.0.0:*	LISTEN	
tcp	0	0	0.0.0.0:pop3	0.0.0.0:*	LISTEN	
tcp	0	0	0.0.0.0:imap2	0.0.0.0:*	LISTEN	
tcp6	0	0	:::ftp	:::*	LISTEN	
tcp6	0	0	:::ssh	:::*	LISTEN	
tcp6	0	0	ip6-localhost:smtp	:::*	LISTEN	
tcp6	0	0	:::microsoft-ds	:::*	LISTEN	
tcp6	0	0	:::imap5	:::*	LISTEN	
tcp6	0	0	:::pop3s	:::*	LISTEN	
tcp6	0	0	:::netbios-ssn	:::*	LISTEN	
tcp6	0	0	:::pop3	:::*	LISTEN	
tcp6	0	0	:::imap2	:::*	LISTEN	
tcp6	0	0	:::netip	:::*	LISTEN	
udp	0	0	localhost:domain	*.*.*.*.*	LISTEN	
udp	0	0	0.0.0.0:bootpc	0.0.0.0:*	LISTEN	
udp	0	0	10.129.255.2:netbios-ns	0.0.0.0:*	LISTEN	
udp	0	0	10.129.97.40:netbios-ns	0.0.0.0:*	LISTEN	
udp	0	0	0.0.0.0:netbios-ns	0.0.0.0:*	LISTEN	
udp	0	0	10.129.255.2:netbios-dgm	0.0.0.0:*	LISTEN	
udp	0	0	10.129.97.4:netbios-dgm	0.0.0.0:*	LISTEN	
udp	0	0	0.0.0.0:netbios-dgm	0.0.0.0:*	LISTEN	

Active UNIX domain sockets (only servers)

Proto	RefCnt	Flags	Type	State	I-Node	Path
unix	2	[ACC]	SEQPACKET	LISTENING	281	/run/udev/control
unix	2	[ACC]	STREAM	LISTENING	38717	/run/user/1002/systemd/private
unix	2	[ACC]	STREAM	LISTENING	38721	/run/user/1002/gnupg/g.gpg-agent
unix	2	[ACC]	STREAM	LISTENING	38722	/run/user/1002/gnupg/g.gpg-agent.browser
unix	2	[ACC]	STREAM	LISTENING	26649	public/pipe
unix	2	[ACC]	STREAM	LISTENING	38723	/run/user/1002/gnupg/g.gpg-agent
unix	2	[ACC]	STREAM	LISTENING	38724	/run/user/1002/gnupg/g.gpg-agent.ssh
unix	2	[ACC]	STREAM	LISTENING	38725	/run/user/1002/gnupg/g.gpg-agent.extra
unix	2	[ACC]	STREAM	LISTENING	38726	/run/user/1002/snapd-session-agent.socket
unix	2	[ACC]	STREAM	LISTENING	16685	/var/run/udev/guestServicePipe
unix	2	[ACC]	STREAM	LISTENING	250	/run/systemd/private
unix	2	[ACC]	STREAM	LISTENING	267	/run/systemd/journal/stdout
unix	2	[ACC]	STREAM	LISTENING	22873	libqemu-ls173.sock
unix	2	[ACC]	STREAM	LISTENING	278	/run/lvm/lvmetad.socket
unix	2	[ACC]	STREAM	LISTENING	286	/run/lvm/lvmpolld.socket
unix	2	[ACC]	STREAM	LISTENING	26852	private/lsmer
unix	2	[ACC]	STREAM	LISTENING	18888	/run/snapd.socket
unix	2	[ACC]	STREAM	LISTENING	18886	/run/acpid.socket
unix	2	[ACC]	STREAM	LISTENING	26656	private/rewrite

Used the command ps to list running process and found user of proFTPd server

```
File Actions Edit View Help
htb-student@nixfund:~$ clear
htb-student@nixfund:~$ ps
  PID TTY          TIME CMD
 6153 pts/0    00:00:00 bash
 6153 pts/0    00:00:00 ps
htb-student@nixfund:~$ ps -aux
USER        PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.0 225544 9216 T        Ss   10:00  0:01 /sbin/init maybe-ubiquity
root         2  0.0  0.0      0   0 T        S    10:00  0:00 [kthreadd]
root         3  0.0  0.0      0   0 T        I    10:00  0:00 [kworker/0:0]
root         4  0.0  0.0      0   0 T        I    10:00  0:00 [kworker/0:0H]
root         6  0.0  0.0      0   0 T        I    10:00  0:00 [mm_percpu_wq]
root         7  0.0  0.0      0   0 T        S    10:00  0:00 [ksoftirqd/0]
root         8  0.0  0.0      0   0 T        I    10:00  0:00 [rcu_sched]
root         9  0.0  0.0      0   0 T        I    10:00  0:00 [rcu_bh]
root        10  0.0  0.0      0   0 T        S    10:00  0:00 [migration/0]
root        11  0.0  0.0      0   0 T        S    10:00  0:00 [watchdog/0]
root        12  0.0  0.0      0   0 T        S    10:00  0:00 [cpuhp/0]
root        13  0.0  0.0      0   0 T        S    10:00  0:00 [cpuhp/1]
root        14  0.0  0.0      0   0 T        S    10:00  0:00 [watchdog/1]
root        15  0.0  0.0      0   0 T        S    10:00  0:00 [migration/1]
root        16  0.0  0.0      0   0 T        S    10:00  0:00 [ksoftirqd/1]
root        18  0.0  0.0      0   0 T        I    10:00  0:00 [kworker/1:0H]
root        19  0.0  0.0      0   0 T        S    10:00  0:00 [cpuhp/2]
root        20  0.0  0.0      0   0 T        S    10:00  0:00 [watchdog/2]
root        21  0.0  0.0      0   0 T        S    10:00  0:00 [migration/2]
root        22  0.0  0.0      0   0 T        S    10:00  0:00 [ksoftirqd/2]
root        24  0.0  0.0      0   0 T        I    10:00  0:00 [kworker/2:0H]
root        25  0.0  0.0      0   0 T        S    10:00  0:00 [cpuhp/3]
root        26  0.0  0.0      0   0 T        S    10:00  0:00 [watchdog/3]
root        27  0.0  0.0      0   0 T        S    10:00  0:00 [migration/3]
root        28  0.0  0.0      0   0 T        S    10:00  0:00 [ksoftirqd/3]
root        30  0.0  0.0      0   0 T        I    10:00  0:00 [kworker/3:0H]
root        31  0.0  0.0      0   0 T        S    10:00  0:00 [kdevtmpfs]
root        32  0.0  0.0      0   0 T        I    10:00  0:00 [netns]
root        33  0.0  0.0      0   0 T        S    10:00  0:00 [rcu_tasks_kthre]
root        34  0.0  0.0      0   0 T        S    10:00  0:00 [kauditd]
root        36  0.0  0.0      0   0 T        I    10:00  0:00 [kworker/1:1]
root        37  0.0  0.0      0   0 T        S    10:00  0:00 [khumtaskd]
root        38  0.0  0.0      0   0 T        S    10:00  0:00 [oom_reaper]
root        39  0.0  0.0      0   0 T        I    10:00  0:00 [writeback]
root        40  0.0  0.0      0   0 T        S    10:00  0:00 [kcompactd0]
root        41  0.0  0.0      0   0 T        S    10:00  0:00 [kswapd]
root        42  0.0  0.0      0   0 T        S    10:00  0:00 [khugepaged]
root        43  0.0  0.0      0   0 T        I    10:00  0:00 [crypto]
root        44  0.0  0.0      0   0 T        I    10:00  0:00 [kintegrityd]
root        45  0.0  0.0      0   0 T        I    10:00  0:00 [kblockd]
root        46  0.0  0.0      0   0 T        I    10:00  0:00 [ata_sff]
root        47  0.0  0.0      0   0 T        I    10:00  0:00 [md]
root        48  0.0  0.0      0   0 T        I    10:00  0:00 [edac-poller]
root        49  0.0  0.0      0   0 T        I    10:00  0:00 [deferred_wq]
root        50  0.0  0.0      0   0 T        I    10:00  0:00 [watchdog]
```

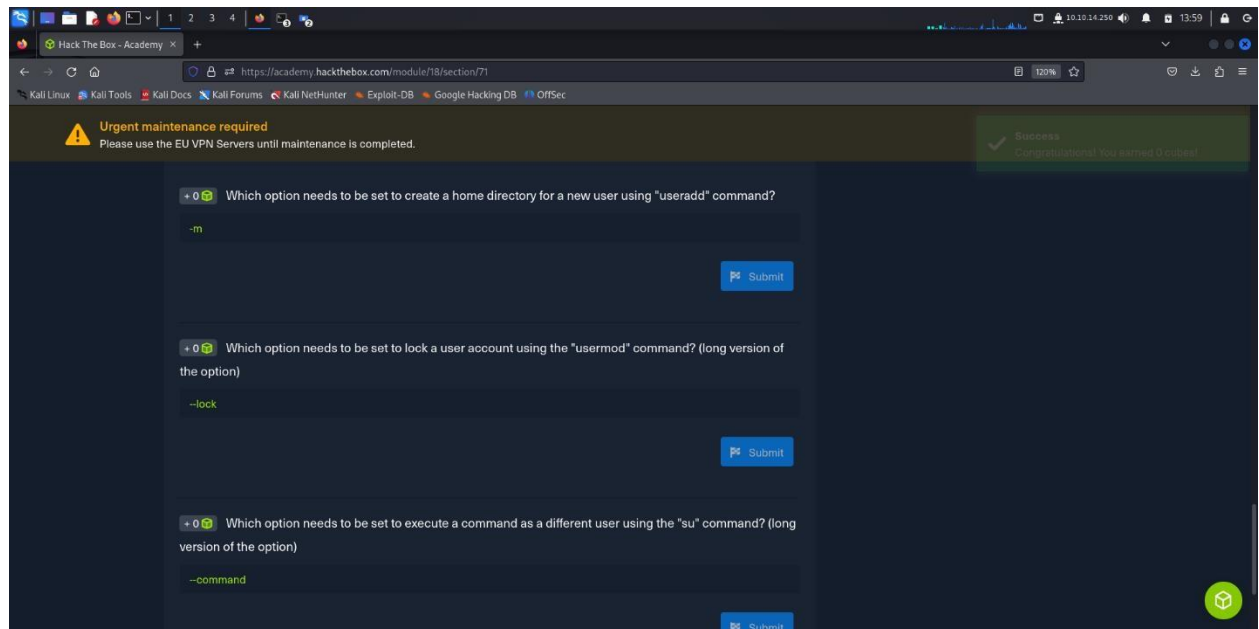
used curl, grep, sort, tr to specify the results I want then counted unique paths found 34

```
File Actions Edit View Help
deathstroke@kali:~$ curl https://www.inlanefreight.com | grep https://www.inlanefreight.com | tr '\n' '\n' | sort -u | grep -E "src|href" | wc -l
% Total    % Received % Xferd  Average Speed   Time    Time     Current
                                 Dload  Upload   Total   Spent    Left     Speed
100 22266  0 22266  0 0 26075  0 --:--:-- --:--:-- --:--:-- 26072
17

deathstroke@kali:~$ curl https://www.inlanefreight.com | grep https://www.inlanefreight.com | tr '\n' '\n' | sort -u | grep -E "src|href" | sort -u
href="https://www.inlanefreight.com/"
href="https://www.inlanefreight.com/wp-content/themes/ben_theme/css/animate.css?ver=5.6.14"
href="https://www.inlanefreight.com/wp-content/themes/ben_theme/css/bootstrap-progressbar.min.css?ver=5.6.14"
href="https://www.inlanefreight.com/wp-content/themes/ben_theme/css/bootstrap.css?ver=5.6.14"
href="https://www.inlanefreight.com/wp-content/themes/ben_theme/css/colors/default.css?ver=5.6.14"
href="https://www.inlanefreight.com/wp-content/themes/ben_theme/css/font-awesome.css?ver=5.6.14"
href="https://www.inlanefreight.com/wp-content/themes/ben_theme/css/jquery.smartmenus.bootstrap.css?ver=5.6.14"
href="https://www.inlanefreight.com/wp-content/themes/ben_theme/css/magnific-popup.css?ver=5.6.14"
href="https://www.inlanefreight.com/wp-content/themes/ben_theme/css/owl.carousel.css?ver=5.6.14"
href="https://www.inlanefreight.com/wp-content/themes/ben_theme/css/owl.transitions.css?ver=5.6.14"
href="https://www.inlanefreight.com/wp-content/themes/ben_theme/css/style.css?ver=5.6.14"
href="https://www.inlanefreight.com/wp-content/themes/ben_theme/css/dist/block-library/style.min.css?ver=5.6.14"
src="https://www.inlanefreight.com/wp-content/themes/ben_theme/js/bootstrap.min.js?ver=5.6.14"
src="https://www.inlanefreight.com/wp-content/themes/ben_theme/js/jquery.smartmenus.bootstrap.js?ver=5.6.14"
src="https://www.inlanefreight.com/wp-content/themes/ben_theme/js/jquery.smartmenus.js?ver=5.6.14"
src="https://www.inlanefreight.com/wp-content/themes/ben_theme/js/navigation.js?ver=5.6.14"
src="https://www.inlanefreight.com/wp-content/themes/ben_theme/js/owl.carousel.min.js?ver=5.6.14"
src="https://www.inlanefreight.com/wp-content/themes/ben_theme/js/jquery/jquery-migrate.min.js?ver=3.3.2"
src="https://www.inlanefreight.com/wp-content/themes/ben_theme/js/jquery/jquery.min.js?ver=3.5.1"
src="https://www.inlanefreight.com/wp-content/themes/ben_theme/js/wp-embed.min.js?ver=5.6.14"
```

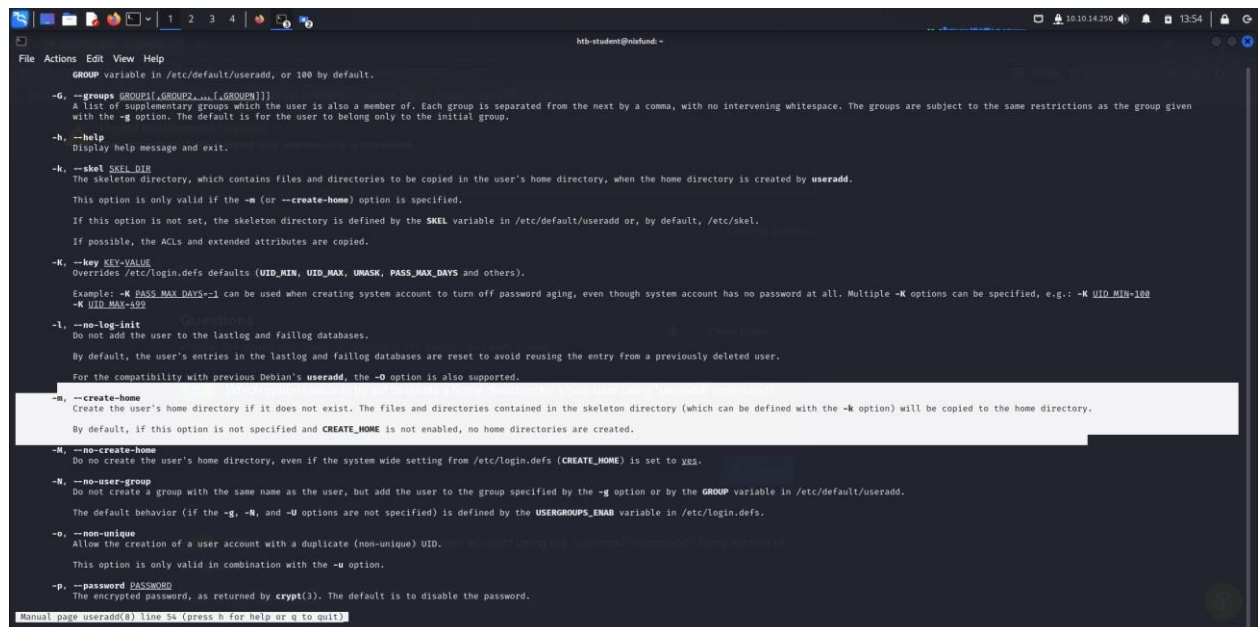
1.7 User Management

Questions



Solution

Used command `man useradd` found the command description and flags used with it



Used man command on usermod, this was the results

```
htb-student@nixfund: ~  
File Actions Edit View Help  
A value of 0 disables the account as soon as the password has expired, and a value of -1 disables the feature.  
This option requires a /etc/shadow file. A /etc/shadow entry will be created if there were none.  
-g, --gid GROUP  
The group name or number of the user's new initial login group. The group must exist.  
Any file from the user's home directory owned by the previous primary group of the user will be owned by this new group.  
The group ownership of files outside of the user's home directory must be fixed manually.  
-G, --groups GROUP1[,GROUP2,...[,GROUPN]]  
A list of supplementary groups which the user is also a member of. Each group is separated from the next by a comma, with no intervening whitespace. The groups are subject to the same restrictions as the group given with the -g option.  
If the user is currently a member of a group which is not listed, the user will be removed from the group. This behaviour can be changed via the -a option, which appends the user to the current supplementary group list.  
-l, --login NEW_LOGIN  
The name of the user will be changed from LOGIN to NEW_LOGIN. Nothing else is changed. In particular, the user's home directory or mail spool should probably be renamed manually to reflect the new login name.  
-L, --lock  
Lock a user's password. This puts a '!' in front of the encrypted password, effectively disabling the password. You can't use this option with -p or -u.  
Note: if you wish to lock the account (not only access with a password), you should also set the EXPIRE_DATE to 1.  
-m, --move-home  
Move the content of the user's home directory to the new location.  
This option is only valid in combination with the -d (or --home) option.  
usermod will try to adapt the ownership of the files and to copy the modes, ACL and extended attributes, but manual changes might be needed afterwards.  
-o, --non-unique  
When used with the -u option, this option allows to change the user ID to a non-unique value.  
-p, --password PASSWORD  
The encrypted password, as returned by crypt(3).  
Note: This option is not recommended because the password (or encrypted password) will be visible by users listing the processes.  
The password will be written in the local /etc/passwd or /etc/shadow file. This might differ from the password database configured in your PAM configuration.  
You should make sure the password respects the system's password policy.  
-R, --root CHROOT_DIR  
Apply changes in the CHROOT_DIR directory and use the configuration files from the CHROOT_DIR directory.  
-s, --shell SHELL  
The name of the user's new login shell. Setting this field to blank causes the system to select the default login shell.  
Manual page usermod(8) line 35/203 40% (press h for help or q to quit)
```

Used man command with su,

```
htb-student@nixfund: ~  
File Actions Edit View Help  
SU(1) User Commands SU(1)  
NAME  
su - change user ID or become superuser  
SYNOPSIS  
su [options] [username]  
DESCRIPTION  
The su command is used to become another user during a login session. Invoked without a username, su defaults to becoming the superuser. The optional argument - may be used to provide an environment similar to what the user would expect had the user logged in directly.  
Additional arguments may be provided after the username, in which case they are supplied to the user's login shell. In particular, an argument of -c will cause the next argument to be treated as a command by most command interpreters. The command will be executed by the shell specified in /etc/passwd for the target user.  
You can use the -- argument to separate su options from the arguments supplied to the shell.  
The user will be prompted for a password, if appropriate. Invalid passwords will produce an error message. All attempts, both valid and invalid, are logged to detect abuse of the system.  
The current environment is passed to the new shell. The value of $PATH is reset to /bin:/usr/bin for normal users, or /sbin:/bin:/usr/sbin:/usr/bin for the superuser. This may be changed with the ENV_PATH and ENV_SUPATH definitions in /etc/login.defs.  
A subsystem login is indicated by the presence of a "*" as the first character of the login shell. The given home directory will be used as the root of a new file system which the user is actually logged into.  
OPTIONS  
The options which apply to the su command are:  
-c, --command COMMAND  
Specify a command that will be invoked by the shell using its -c.  
The executed command will have no controlling terminal. This option cannot be used to execute interactive programs which need a controlling TTY.  
-l, --login  
Provide an environment similar to what the user would expect had the user logged in directly.  
When - is used, it must be specified before any username. For portability it is recommended to use it as last option, before any username. The other forms (-l and --login) do not have this restriction.  
-s, --shell SHELL  
The shell that will be invoked.  
The invoked shell is chosen from (highest priority first):  
The shell specified with --shell.  
If --preserve-environment is used, the shell specified by the $SHELL environment variable.  
The shell indicated in the /etc/passwd entry for the target user.  
/bin/sh if a shell could not be found by any above method.  
If the target user has a restricted shell (i.e. the shell field of this user's entry in /etc/passwd is not listed in /etc/shells), then the --shell option or the $SHELL environment variable won't be taken into account, unless su is called by root.  
Manual page su(1) line 1 (press h for help or q to quit)
```

I.8 Service and Process Management

Question

The screenshot shows a web browser window displaying the HackTheBox Academy interface. At the top, there is a navigation bar with links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. Below the navigation bar, a yellow warning banner states: "Urgent maintenance required. Please use the EU VPN Servers until maintenance is completed." The main content area is titled "Questions" and contains the following text: "Answer the question(s) below to complete this Section and earn cubes!". Below this, the target is listed as "10.129.97.49 (ACADEMY-NIXFUND)" with a status of "Life Left: 64 minute(s)". A "Terminate" button is visible. The question text reads: "SSH to 10.129.97.49 (ACADEMY-NIXFUND) with user 'htb-student' and password 'HTB_Academy_stdnt!'. Use the 'systemctl' command to list all units of services and submit the unit name with the description 'Load AppArmor profiles managed internally by snapd' as the answer." Below the question, the answer "snapd.apparmor.service" is entered. There are "Submit" and "Hint" buttons. At the bottom, there are "Previous" and "Next" navigation buttons, a "+10 Streak pts" indicator, and a "Mark Complete & Next" button. The page is powered by HackTheBox.

Solution

Used systemctl with grep to find name of the service

The screenshot shows a terminal window with the following commands and output:

```
htb-student@nixfund:~$ useradd htb-student
htb-student@nixfund:~$ man useradd
htb-student@nixfund:~$ man usermod
htb-student@nixfund:~$ man usermod
htb-student@nixfund:~$ man su
htb-student@nixfund:~$ systemctl | grep Load
snapd.apparmor.service loaded active exited AppArmor profiles managed internally by snapd
systemd-modules-load.service loaded active exited Load Kernel Modules
systemd-random-seed.service loaded active exited Load/Save Random Seed
systemd-rfkill.socket loaded active listening Load/Save RF Kill Switch Status /dev/rfkill Watch
```

The terminal window also shows the question text and the answer "snapd.apparmor.service" entered in the terminal.