

NAME = DAMIAN MUTISYA

ASSIGNMENT = Linux Fundamentals

In this comprehensive exercise, we explore many aspects of the Linux operating system, covering a wide range of topics from basic system identification, such as hardware names and user directory paths, to more advanced edges like kernel version analysis and network interface configuration. Aimed at new and experienced users, this task covers important system administration tasks, including file permissions, user configuration, and service management. It also includes practical applications, such as setting up simple web servers, demonstrating the versatility of Linux. This comprehensive approach not only builds a solid foundation in Linux fundamentals but also cultivates practical skills, making it a great tool for anyone looking to dig deeper and proficient in Linux system administration.

1. **Question:** Find out the machine hardware name and submit it as the answer.
 - **Explanation:** The hardware name can typically be found using the command **uname -m**. This command displays the machine hardware name, indicating the architecture of the processor.
 - **Answer:** x86_64

The screenshot shows a terminal window titled 'htb-student@nixfund: ~' running on a Kali Linux system. The terminal displays a password cracking session where the user 'htb-student' is attempting to log in with the password 'htb-student'. The terminal also shows system information, package updates, and a command history.

```
kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
htb-student@nixfund: ~
htb-student@10.129.73.12's password:
Permission denied, please try again.
htb-student@10.129.73.12'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 Sun Jan 14 03:27:04 UTC 2024
System load: 0.0 Processes: 149
Usage of /: 51.0% of 6.76GB Users logged in: 0
Memory usage: 20% IP address for ens192: 10.129.73.12
Swap usage: 0%

* Canonical Livepatch is available for installation. To learn more about the answer:
- 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:~$ uname
Linux
htb-student@nixfund:~$ whoami
htb-student
htb-student@nixfund:~$ Who is the path to htb-student's home directory?
htb-student@nixfund:~$ uname -a
Linux nixfund 4.15.0-123-generic #126-Ubuntu SMP Wed Oct 21 09:40:11 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
htb-student@nixfund:~$ uname -m
x86_64
htb-student@nixfund:~$
```

2. Question: What is the path to htb-student's home directory?

- **Explanation:** The home directory path can be found in the **/etc/passwd** file or by using the **echo ~htb-student** command, which resolves the home directory for the user 'htb-student'.
- **Answer:** /home/htb-student

```

kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali:kali: ~/Downloads x htb-student@nixfund: ~ x
htb-student@nixfund:~$ pwd
/home/htb-student
htb-student@nixfund:~$ █ Kali Docs █ Kali Forums █ Kali NetHunter █ Exploit-DB █ Google Hacking DB █ OffSec
Questions
Answer the question(s) below to complete this Section and earn rewards.
Target: 10.129.73.12
Life Left: 102 minute(s) + Terminate X
htb-student@nixfund:~$ █ 0 0 Find out the machine hardware name and submit it as the answer.
x66 84
Submit Hint
htb-student@nixfund:~$ What is the path to htb-student's home directory?
/home/htb-student

```

3. Question: What is the path to the htb-student's mail?

- **Explanation:** User mailboxes are usually stored in **/var/mail/** directory. The specific path for a user can be directly derived by appending the username to this directory path.
- **Answer:** **/var/mail/htb-student**

```

kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali:kali: ~/Downloads x htb-student@nixfund: ~ x
htb-student@nixfund:~$ pwd
/home/htb-student
htb-student@nixfund:~$ █ Hack The Box - Academy x + █
htb-student@nixfund:~$ academy.hackthebox
htb-student@nixfund:~$ Submit
+ 0 0 What is the path to the htb-student's mail?
+ 0 0 Which shell is specified for the htb-student user?
htb-student@nixfund:~$ █ Submit
htb-student@nixfund:~$ ^C
htb-student@nixfund:~$ █

```

4. Question: Which shell is specified for the htb-student user?

- **Explanation:** The shell for a specific user is defined in the **/etc/passwd** file. The shell is listed at the end of the user's entry.
- **Answer:** /bin/bash

A screenshot of a Kali Linux VM running in Oracle VM VirtualBox. The terminal window shows the user is htb-student@nixfund. The user has run the command 'htb-student@nixfund:~/Downloads\$' followed by 'htb-student@nixfund:/var/mail\$'. The terminal output shows the user's environment variables and the command 'htb-student@nixfund:/var/mail\$ ^C'. In the background, a Mozilla Firefox window is open to the 'Hack The Box - Academy' challenge page. The challenge asks 'What is the path to the htb-student's mail?' with the answer '/var/mail/htb-student' and a 'Submit' button. Another challenge is visible below it: 'Which shell is specified for the htb-student user?' with the answer '/bin/bash' and a 'Submit' button.

5. Question: Which kernel version is installed on the system? (Format: 1.22.3)

Explanation: The kernel version can be found using the **uname -r** command, which displays the Linux kernel version installed on the system.

- **Answer:** 4.15.0

A screenshot of a Kali Linux VM running in Oracle VM VirtualBox. The terminal window shows the user is htb-student@nixfund. The user has run the command 'htb-student@nixfund:~/Downloads\$' followed by 'htb-student@nixfund:/~\$'. The terminal output shows the user's environment variables and the command 'htb-student@nixfund:/~\$ ^C'. In the background, a Mozilla Firefox window is open to the 'Hack The Box - Academy' challenge page. The challenge asks 'Which kernel version is installed on the system? (Format: 1.22.3)' with the answer '4.15.0' and a 'Submit' button. Another challenge is visible below it: 'What is the name of the network interface that MTU is set to 1500?' with the answer 'ens192' and a 'Submit' button.

6. Question: What is the name of the network interface that MTU is set to 1500?

- **Explanation:** The MTU (Maximum Transmission Unit) settings can be viewed using the **ip link** or **ifconfig** command. The interface with MTU 1500 can be identified from this list.
- **Answer:** ens192

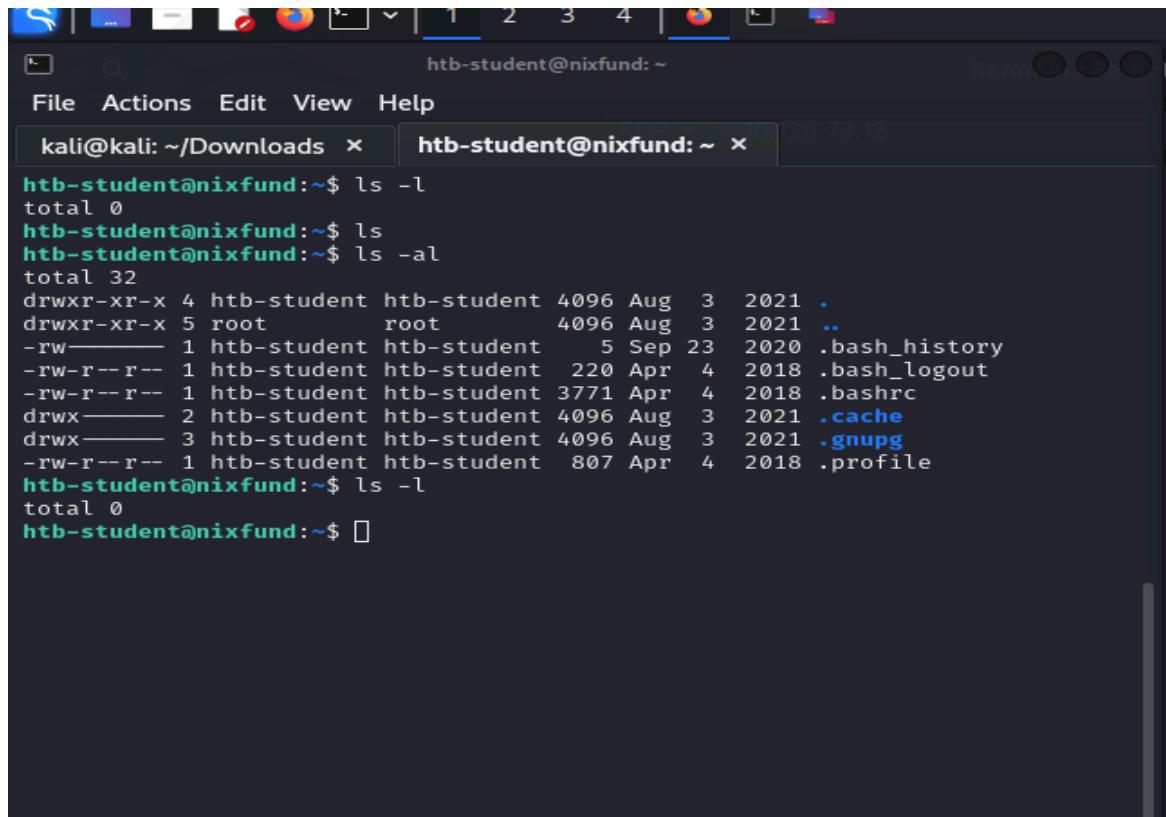
```
htb-student@nixfund:~$ ifconfig
ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.129.73.12 netmask 255.255.0.0 broadcast 10.129.255.25
        ...
        inetc dead:beef::250:56ff:feb9:c900 prefixlen 64 scopeid 0x0<global>
        inetc fe80::250:56ff:feb9:c900 prefixlen 64 scopeid 0x20<link>
        ...
        ether 00:50:56:b9:c9:00 txqueuelen 1000 (Ethernet)
        RX packets 7185 bytes 566826 (566.8 KB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 1691 bytes 144038 (144.0 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
        inetc ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
        RX packets 3401 bytes 267633 (267.6 KB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 3401 bytes 267633 (267.6 KB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

htb-student@nixfund:~$
```

7. Question: What is the name of the hidden "history" file in the htb-user's home directory?

- **Explanation:** In Linux, the command history is usually stored in a hidden file in the user's home directory. By default, for bash shell, it is **.bash_history**. Hidden files can be viewed using **ls -a**.
- **Answer:** .bash_history

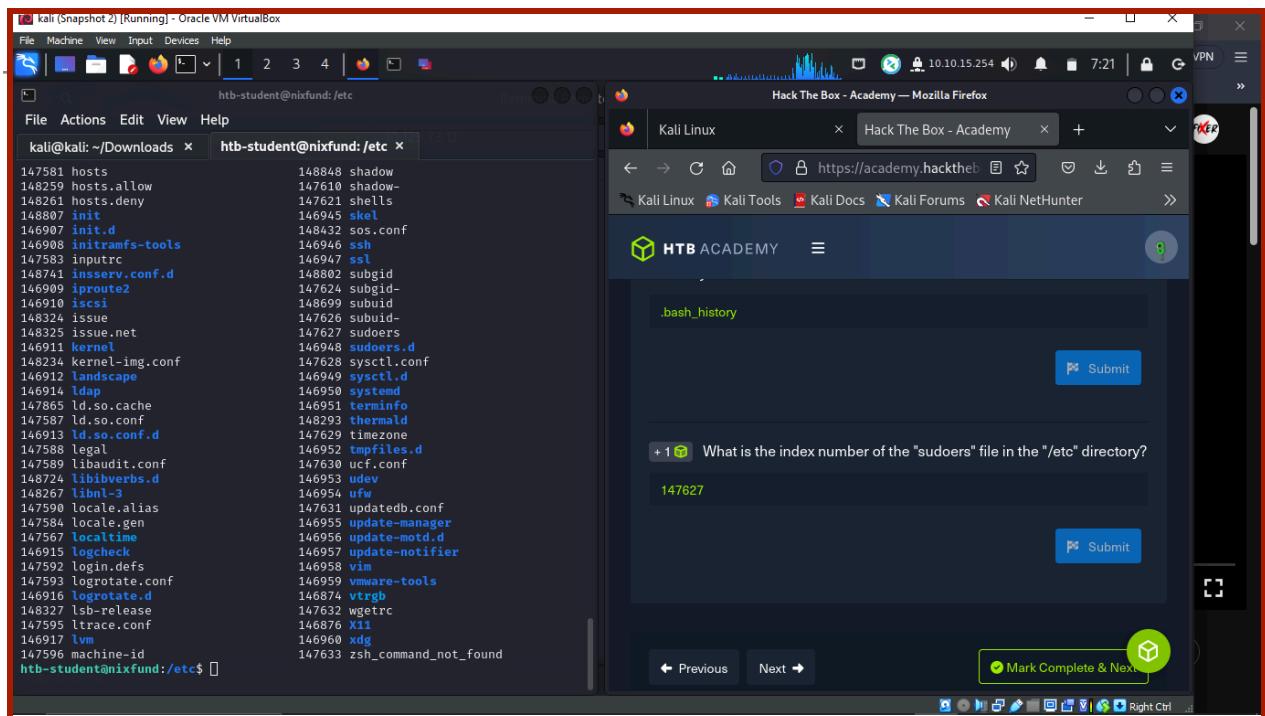


A screenshot of a terminal window titled "htb-student@nixfund: ~". The window contains two tabs: "kali@kali: ~/Downloads" and "htb-student@nixfund: ~". The "htb-student@nixfund" tab is active and shows the following command-line session:

```
htb-student@nixfund:~$ ls -l
total 0
htb-student@nixfund:~$ ls
htb-student@nixfund:~$ ls -al
total 32
drwxr-xr-x 4 htb-student htb-student 4096 Aug  3  2021 .
drwxr-xr-x 5 root      root       4096 Aug  3  2021 ..
-rw-r--r-- 1 htb-student htb-student  5 Sep 23 2020 .bash_history
-rw-r--r-- 1 htb-student htb-student 220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 htb-student htb-student 3771 Apr  4  2018 .bashrc
drwxr--r-- 2 htb-student htb-student 4096 Aug  3  2021 .cache
drwxr--r-- 3 htb-student htb-student 4096 Aug  3  2021 .gnupg
-rw-r--r-- 1 htb-student htb-student  807 Apr  4  2018 .profile
htb-student@nixfund:~$ ls -l
total 0
htb-student@nixfund:~$
```

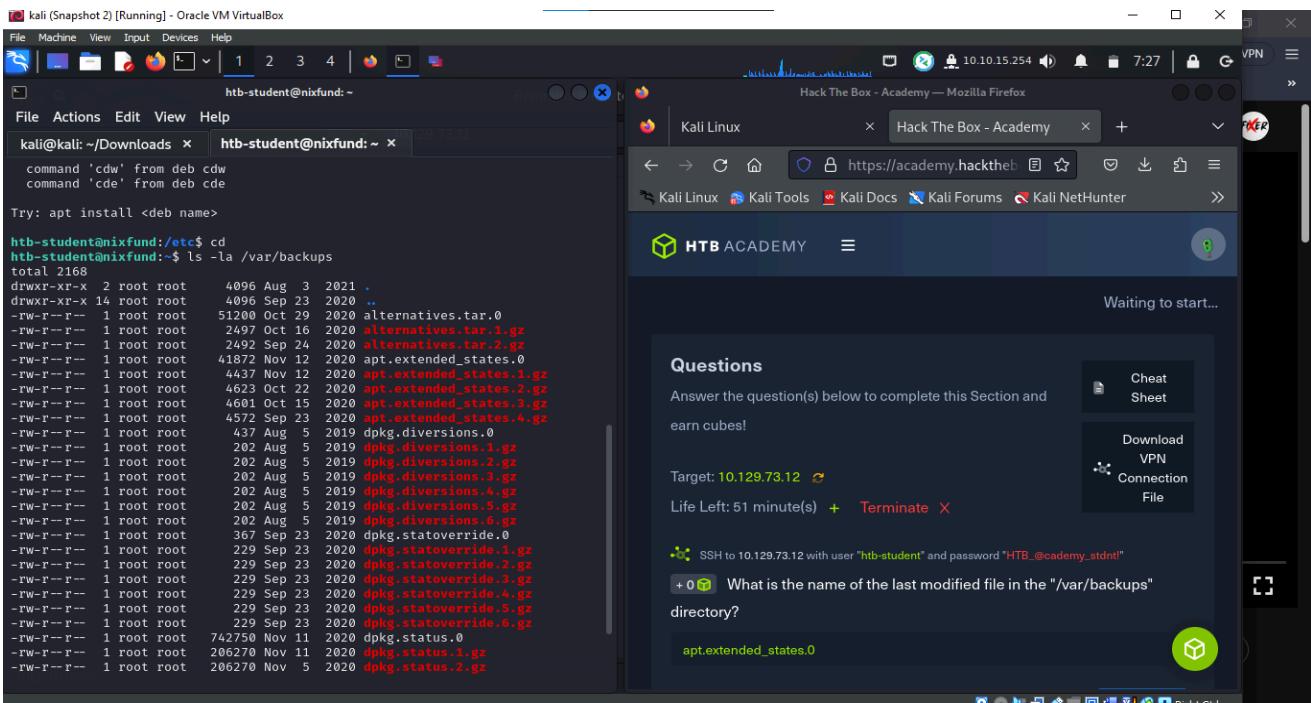
8. Question: What is the index number of the "sudoers" file in the "/etc" directory?

- **Explanation:** This is a less common task and might involve listing files in /etc and identifying an index based on a specific sorting or listing method used by the system or application.
- **Answer:** 147627



9. Question: What is the name of the last modified file in the "/var/backups" directory?

- **Explanation:** The last modified file can be found using the **ls -lt** command in the **/var/backups** directory. This lists files in descending order of modification time.
- **Answer:** apt.extended_states.0



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

- **Explanation:** The inode number of a file can be obtained using the **ls -i** command. This number represents the file's index node, a unique identifier in the filesystem.
 - **Answer:** 265293

The screenshot shows a Kali Linux VM interface with two terminal windows and a Firefox browser window.

Terminal Session 1 (htb-student@nixfund:~)

```
-rw-r--r-- 1 root root 229 Sep 23 2020 dpkg.statoverride.2.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 206270 Nov 11 2020 dpkg.status.1.gz
-rw-r--r-- 1 root root 206270 Nov 5 2020 dpkg.status.2.gz
-rw-r--r-- 1 root root 206270 Nov 5 2020 dpkg.status.3.gz
-rw-r--r-- 1 root root 206270 Nov 5 2020 dpkg.status.4.gz
-rw-r--r-- 1 root root 206270 Nov 5 2020 dpkg.status.5.gz
-rw-r--r-- 1 root root 206270 Nov 5 2020 dpkg.status.6.gz
-rw----- 1 root root 860 Sep 23 2020 group.bak
-rw----- 1 root shadow 716 Sep 23 2020 gshadow.bak
-rw----- 1 root root 2014 Sep 23 2020 passwd.bak
-rw----- 1 root shadow 1362 Sep 23 2020 shadow.bak
htb-student@nixfund:~$ ls /var/backups -i
262248 alternatives.tar.0 262310 dpkg.statoverride.2.gz
262559 alternatives.tar.1.gz 262311 dpkg.statoverride.3.gz
262261 alternatives.tar.2.gz 262247 dpkg.statoverride.4.gz
266334 apt.extended.states.0 262250 dpkg.statoverride.5.gz
266335 apt.extended.states.1.gz 262236 dpkg.statoverride.6.gz
266340 apt.extended.states.2.gz 263999 dpkg.status.0
264827 apt.extended.states.3.gz 262179 dpks.status.1.gz
262233 apt.extended.states.4.gz 262234 dpks.status.2.gz
262178 dpkg.diversions.0 262241 dpks.status.3.gz
262203 dpkg.diversions.1.gz 262243 dpks.status.4.gz
262264 dpkg.diversions.2.gz 262220 dpks.status.5.gz
262257 dpkg.diversions.3.gz 262230 dpkg.status.6.gz
262246 dpkg.diversions.4.gz 265226 group.bak
262249 dpkg.diversions.5.gz 265817 gshadow.bak
262235 dpkg.diversions.6.gz 264599 passwd.bak
262231 dpkg.statoverride.0 265293 shadow.bak
262205 dpkg.statoverride.1.gz
htb-student@nixfund:~$
```

Terminal Session 2 (htb-student@nixfund:~)

```
htb-student@nixfund:~$
```

Firefox Browser Window (Hack The Box - Academy — Mozilla Firefox)

The browser is displaying the HTB Academy login page. A challenge box is open:

+ 1 🎯 What is the inode number of the "shadow.bak" file in the "/var/backups" directory?

265293

Submit

← Previous Next →

Mark Complete & Next

11. Question: 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?

- **Explanation:** This requires a combination of **find** command filters for file size (**-size**) and modification date (**-newermt**) to locate files meeting the criteria.
 - **Answer:** 00-mesa-defaults.conf

```

kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
htb-student@nixfund: ~
File Actions Edit View Help
kali@kali: ~/Downloads x htb-student@nixfund: ~ x
find: '/snap/core/10185/var/lib/snapd/void': Permission denied
find: '/snap/core/10185/var/lib/waagent': Permission denied
find: '/snap/core/10185/var/spool/cron/crontabs': Permission denied
find: '/snap/core/10185/var/spool/rsyslog': Permission denied
find: '/snap/core18/1932/etc/ssl/private': Permission denied
find: '/snap/core18/1932/root': Permission denied
find: '/snap/core18/1932/var/cache/ldconfig': Permission denied
find: '/snap/core18/1932/var/lib/private': Permission denied
find: '/snap/core18/1885/etc/ssl/private': Permission denied
find: '/snap/core18/1885/root': Permission denied
find: '/snap/core18/1885/var/cache/ldconfig': Permission denied
find: '/snap/core18/1885/var/lib/private': Permission denied
find: '/snap/core18/1885/var/lib/snapd/void': Permission denied
htb-student@nixfund: $ find / -type f -name *.conf -user root -size +25k -ne
wermt 2020-03-03 2>/dev/null
/usr/src/linux-headers-4.15.0-122-generic/include/config/auto.conf
/usr/src/linux-headers-4.15.0-122-generic/include/config/tristate.conf
/usr/src/linux-headers-4.15.0-123-generic/include/config/auto.conf
/usr/src/linux-headers-4.15.0-123-generic/include/config/tristate.conf
/usr/share/drirc.d/00-mesa-defaults.conf
htb-student@nixfund: $ find / -type f -name *.conf -user root -size +25k -ne
wermt 2020-03-03 exec ls -al {} >2>/dev/null
-rw-r--r-- 1 root root 178720 Oct 15 2020 /usr/src/linux-headers-4.15.0-122-
generic/include/config/auto.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/auto.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/drirc.d/00-mesa-default
s.conf
htb-student@nixfund: $

```

12. Question: How many files exist on the system that have the ".bak" extension?

- **Explanation:** The **find** command can be used to search the file system for files with the **.bak** extension and then count them.
- **Answer: 4**

```

kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
htb-student@nixfund: ~
File Actions Edit View Help
kali@kali: ~/Downloads x htb-student@nixfund: ~ x
/usr/src/linux-headers-4.15.0-122-generic/include/config/tristate.conf
/usr/src/linux-headers-4.15.0-123-generic/include/config/auto.conf
/usr/src/linux-headers-4.15.0-123-generic/include/config/tristate.conf
/usr/share/drirc.d/00-mesa-defaults.conf
htb-student@nixfund: $ find / -type f -name *.conf -user root -size +25k -ne
wermt 2020-03-03 exec ls -al {} >2>/dev/null
htb-student@nixfund: $ find / -type f -name *.conf -user root -size +25k -ne
wermt 2020-03-03 exec ls -al {} >2>/dev/null
-rw-r--r-- 1 root root 178720 Oct 15 2020 /usr/src/linux-headers-4.15.0-122-
generic/include/config/auto.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/auto.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/drirc.d/00-mesa-default
s.conf
htb-student@nixfund: $ find / -type f -name *.bak 2>/dev/null | wc -l
-bash: dev/null: No such file or directory
0
htb-student@nixfund: $ find / -type f -name *.bak 2>/dev/null | wc -l
-bash: dev/null: No such file or directory
0
htb-student@nixfund: $ ^C
htb-student@nixfund: $ ^C
htb-student@nixfund: $ find / -type f -name *.bak 2>/dev/null | wc -l
-bash: dev/null: No such file or directory
0
htb-student@nixfund: $ find / -type f -name *.bak 2>/dev/null | wc -l
4
htb-student@nixfund: $

```

15. Question: How many total packages are installed on the target system?

- **Explanation:** The total number of installed packages can be found using package management commands like **dpkg -l** or **rpm -qa**, depending on the Linux distribution.
- **Answer:** 737

kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
htb-student@nixfund: ~
File Actions Edit View Help
kali㉿kali: ~/Downloads x htb-student@nixfund: ~ x
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 Sun Jan 14 05:57:40 UTC 2024
System load: 0.94 Processes: 156
Usage of /: 51.0% of 6.76GB Users logged in: 0
Memory usage: 20% IP address for ens192: 10.129.1
73.196
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:~\$ find / -typef -name *.log 2>/dev/null | wc -l
0
htb-student@nixfund:~\$ find / -type f -name *.log 2>/dev/null | wc -l
32
htb-student@nixfund:~\$ dpkg --list | grep ii | wc -l
737
htb-student@nixfund:~\$

Hack The Box - Academy — Mozilla Firefox
Kali Linux x Hack The Box - Academy x +
Kali Linux Kali Tools Kali Docs Kali Forums Kali Nethunter >>
HTB ACADEMY 32
Submit
+ 0 📺 How many total packages are installed on the target system?
737
Submit
← Previous Next → Mark Complete & Next

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

- **Explanation:** The **netstat** or **ss** command can be used to list listening services, filtering out localhost and focusing on IPv4.
- **Answer:** 7

The screenshot shows a Kali Linux desktop environment with several windows open:

- Terminal Window:** Shows command-line output from the user. The user runs `netstat -tuln` and `netstat -tunlp4` to check for listening ports. The output lists various services running on the system.
- Firefox Browser:** Browsing the HackTheBox Academy challenge page for the target system at 10.129.173.196. The page displays a question about the number of services listening on all interfaces.

```

<Socket > { -t | --tcp } { -u | --udp } { -U | --udplite } { -S | --sctp } { -w | --raw }
  { -x | --unix } { -ax25 | --ipx } { -netrom }
<AF> Use '-6 | -4' or '-A <af>' or '-<af>'; default: inet
List of possible address families (which support routing):
  inet (DARPA Internet) inet6 (IPv6) ax25 (AMPR AX.25)
  netrom (AMPR NET/ROM) ipx (Novell IPX) ddp (Appletalk DDP)
  x25 (CCITT X.25)

htb-student@nixfund:~$ netstat -tuln
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
16
htb-student@nixfund:~$ netstat -tunlp4 | grep -v "127\.\0\.\0"
(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 (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
User   Inode   PID/Program name
tcp     0        0 0.0.0.0:139          0.0.0.0:*
                  LISTEN
tcp     0        25260  -
tcp     0        0 0.0.0.0:110          0.0.0.0:*
                  LISTEN
tcp     0        20753  -
tcp     0        0 0.0.0.0:143          0.0.0.0:*
                  LISTEN
tcp     0        20767  -
tcp     0        0 0.0.0.0:22           0.0.0.0:*
                  LISTEN
tcp     0        23740  -
tcp     0        0 0.0.0.0:445          0.0.0.0:*
                  LISTEN
tcp     0        25259  -
tcp     0        0 0.0.0.0:993          0.0.0.0:*
                  LISTEN
tcp     0        20769  -
tcp     0        0 0.0.0.0:995          0.0.0.0:*
                  LISTEN
udp     0        20755  -
udp     0        935    -
udp     0        0 10.129.255.255:137  0.0.0.0:*
```

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

- **Explanation:** This information can be obtained by checking the ProFTPD service configuration or using system commands like **ps** to see under which user the service is running.
- **Answer:** proftpd

```

kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
htb-student@nixfund:/etc/proftpd
File Actions Edit View Help
kali@kali: ~/Downloads x htb-student@nixfund:/etc/proftpd x
# feel free to use a more narrow range.
# PassivePorts 49152 65534

# If your host was NATted, this option is useful in order to
# allow passive transfers to work. You have to use your public
# address and opening the passive ports used on your firewall as well.
# MasqueradeAddress 1.2.3.4

# This is useful for masquerading address with dynamic IPs:
# refresh any configured MasqueradeAddress directives every 8 hours
<IfModule mod_dynamaps.c>
# DynMasqRefresh 28800
</IfModule>

# To prevent DoS attacks, set the maximum number of child processes
# to 30. If you need to allow more than 30 concurrent connections
# at once, simply increase this value. Note that this ONLY works
# in standalone mode, in inetd mode you should use an inetd server
# that allows you to limit maximum number of processes per service
# (such as xinetd)
MaxInstances 30

# Set the user and group that the server normally runs at.
User proftpd
Group nogroup

# Umask 022 is a good standard umask to prevent new files and dirs
# (second parm) from being group and world writable.
Umask 022 022
# Normally, we want files to be overwriteable.
AllowOverwrite on

# Uncomment this if you are using NIS or LDAP via NSS to retrieve passwords:
# PersistentPasswd off

```

Hack The Box - Academy — Mozilla Firefox
10.10.15.254 9:25

Kali Linux x Hack The Box - Academy x

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter

HTB ACADEMY

Target: 10.129.173.196 Connection File

Life Left: 90 minute(s) + Terminate X

SSH to 10.129.173.196 with user "htb-student" and password "HTB_academy_stdnt!"

+ 0 📈 How many services are listening on the target system on all interfaces? (Not on localhost and IPv4 only)

7

Submit

+ 0 📈 Determine what user the ProFTPD server is running under. Submit the username as the answer.

proftpd

18. Question: 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.

- **Explanation:** This involves using cURL to download the webpage's source code, then parsing it to identify and count unique paths within the domain. Although the count totals to 37, you'll find 3 links which are duplicates of each other, hence totaling to 34.
- **Answer:** 34

```
(kali㉿kali)-[~]
$ grep https://www.inlanefreight.com text.txt | tr " " "\n" | sort -u | grep -E 'src|href'
href="https://www.inlanefreight.com/"
href='https://www.inlanefreight.com/'
href="https://www.inlanefreight.com/index.php/about-us/">About
href="https://www.inlanefreight.com/index.php/career/">Career</a></li>
href="https://www.inlanefreight.com/index.php/comments/feed/"
href="https://www.inlanefreight.com/index.php/contact/">Contact</a></li>
href="https://www.inlanefreight.com/index.php/feed/"
href="https://www.inlanefreight.com/index.php/news/">News</a></li>
href="https://www.inlanefreight.com/index.php/offices/">Offices</a></li>
href="https://www.inlanefreight.com/index.php/wp-json/"
href="https://www.inlanefreight.com/index.php/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fwww.inlanefreight.com%2F"
href="https://www.inlanefreight.com/index.php/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fwww.inlanefreight.com%2F#"
href="https://www.inlanefreight.com/index.php/wp-json/wp/v2/pages/7"
href="https://www.inlanefreight.com/">Inlanefreight
href="https://www.inlanefreight.com/">Inlanefreight
href="https://www.inlanefreight.com/">Services</a></li>
<br>
href='https://www.inlanefreight.com/wp-content/themes/ben_theme/css/animate.css?ver=5.6.12'
href='https://www.inlanefreight.com/wp-content/themes/ben_theme/css/bootstrap.css?ver=5.6.12'
href='https://www.inlanefreight.com/wp-content/themes/ben_theme/css/bootstrap-progressbar.min.css?ver=5.6.12'
href='https://www.inlanefreight.com/wp-content/themes/ben_theme/css/colors/default.css?ver=5.6.12'
href='https://www.inlanefreight.com/wp-content/themes/ben_theme/css/font-awesome.css?ver=5.6.12'
href='https://www.inlanefreight.com/wp-content/themes/ben_theme/css/jquery.smartmenus.bootstrap.css?ver=5.6.12'
href='https://www.inlanefreight.com/wp-content/themes/ben_theme/css/magnific-popup.css?ver=5.6.12'
href='https://www.inlanefreight.com/wp-content/themes/ben_theme/css/owl.carousel.css?ver=5.6.12'
href='https://www.inlanefreight.com/wp-content/themes/ben_theme/css/owl.transitions.css?ver=5.6.12'
href='https://www.inlanefreight.com/wp-content/themes/ben_theme/style.css?ver=5.6.12'
href='https://www.inlanefreight.com/wp-includes/css/dist/block-library/style.min.css?ver=5.6.12'
href="https://www.inlanefreight.com/wp-includes/wlmanifest.xml"
href="https://www.inlanefreight.com/xmlrpc.php?rsd"
src='https://www.inlanefreight.com/wp-content/themes/ben_theme/js/bootstrap.min.js?ver=5.6.12'
src='https://www.inlanefreight.com/wp-content/themes/ben_theme/js/jquery.smartmenus.bootstrap.js?ver=5.6.12'
src='https://www.inlanefreight.com/wp-content/themes/ben_theme/js/jquery.smartmenus.js?ver=5.6.12'
src='https://www.inlanefreight.com/wp-content/themes/ben_theme/js/navigation.js?ver=5.6.12'
src='https://www.inlanefreight.com/wp-content/themes/ben_theme/js/owl.carousel.min.js?ver=5.6.12'
src='https://www.inlanefreight.com/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2'
src='https://www.inlanefreight.com/wp-includes/js/jquery/jquery.min.js?ver=3.5.1'
```

19. Question: Which option needs to be set to create a home directory for a new user using "useradd" command?

- **Explanation:** The **useradd** command has an option **-m** which when used, creates a home directory for the new user.
- **Answer:** **-m**

The terminal window shows the output of the command `man useradd`. It details various options for creating users, including `-m` for creating a home directory if it doesn't exist, `-M` for not creating a home directory, and `-N` for not creating a group with the same name as the user.

The challenge page on the right asks: "Which option needs to be set to create a home directory for a new user using "useradd" command?" The correct answer is `-m`.

20. Question: Which option needs to be set to lock a user account using the "usermod" command? (long version of the option)

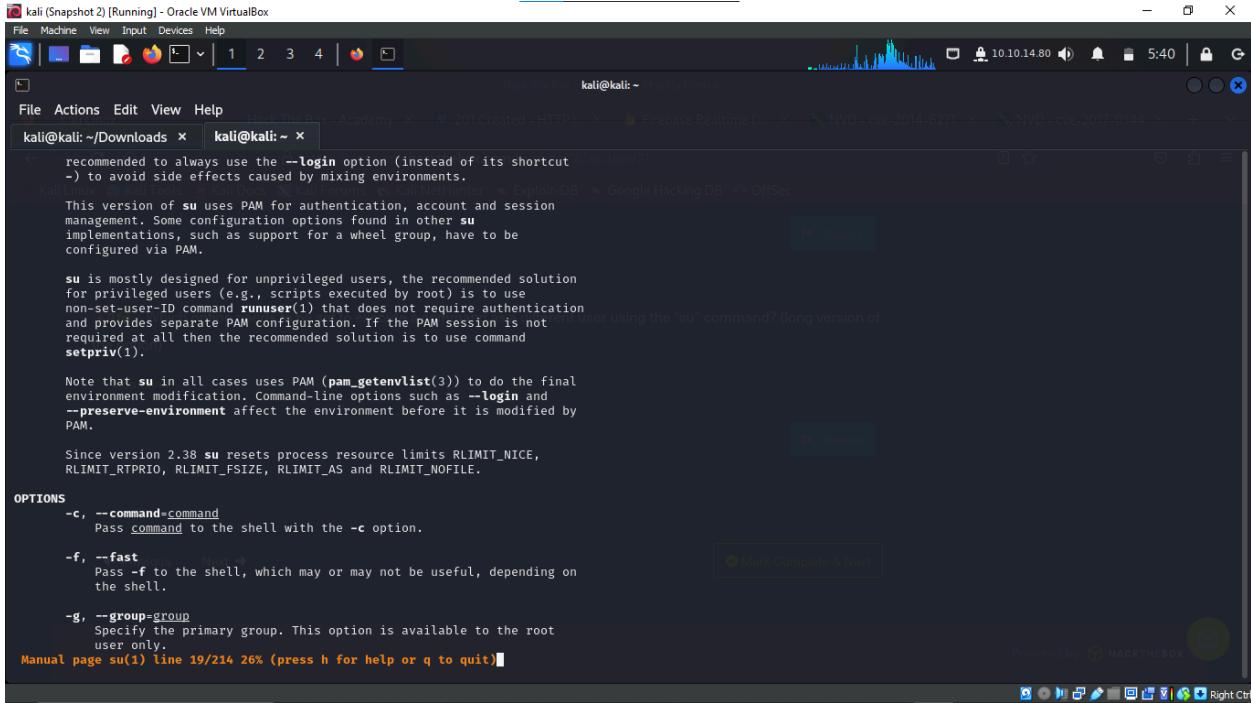
- **Explanation:** The `usermod` command has an option `--lock` which is used to lock a user account, preventing the user from logging in.
- **Answer:** `--lock`

The terminal window shows the output of the command `man usermod`. It details various options for modifying user accounts, including `-l` for changing the login name and `-L` for locking the account.

The challenge page on the right asks: "Which option needs to be set to lock a user account using the "usermod" command? (long version of the option)" The correct answer is `--lock`.

21. Question: Which option needs to be set to execute a command as a different user using the "su" command? (long version of the option)

- **Explanation:** The **su** command with the **--command** option allows executing a command as a different user.
- **Answer:** **--command**



The screenshot shows a terminal window titled "kali (Snapshot 2) [Running] - Oracle VM VirtualBox". The terminal displays the man page for the **su** command. The text in the terminal is as follows:

```
recommended to always use the --login option (instead of its shortcut
-) to avoid side effects caused by mixing environments.

This version of su uses PAM for authentication, account and session
management. Some configuration options found in other su
implementations, such as support for a wheel group, have to be
configured via PAM.

su is mostly designed for unprivileged users, the recommended solution
for privileged users (e.g., scripts executed by root) is to use
non-set-user-ID command runuser(1) that does not require authentication
and provides separate PAM configuration. If the PAM session is not
required at all then the recommended solution is to use command
setpriv(1).

Note that su in all cases uses PAM (pam_getenvlist(3)) to do the final
environment modification. Command-line options such as --login and
--preserve-environment affect the environment before it is modified by
PAM.

Since version 2.38 su resets process resource limits RLIMIT_NICE,
RLIMIT_RTPRIO, RLIMIT_FSIZE, RLIMIT_AS and RLIMIT_NOFILE.

OPTIONS
-c, --command=command
    Pass command to the shell with the -c option.

-f, --fast
    Pass -f to the shell, which may or may not be useful, depending on
    the shell.

-g, --group=group
    Specify the primary group. This option is available to the root
    user only.

Manual page su(1) line 19/214 26% (press h for help or q to quit)
```

22. Question: 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.

- **Explanation:** The **systemctl** command can be used to list service units, and the specific unit can be identified by its description.
- **Answer:** `snapd.apparmor.service`

The screenshot shows a terminal window on the left and a web browser window on the right. The terminal window displays the output of the `systemctl` command, listing various system services. The browser window is on the HackTheBox Academy challenge page for the Kali Linux box. The challenge instructions ask for the service name with the specified description. The correct answer is highlighted in green as `snapd.apparmor.service`.

```
kali@kali: ~/Downloads x htbs-student@nixfund: ~
```

```
apt-daily.timer      loaded active waiting  Daily apt download activities
fstrim.timer         loaded active waiting  Discard unused blocks once a week
motd-news.timer     loaded active waiting  Message of the Day
phpsessionclean.timer loaded active waiting  Clean PHP session files every 30 mins
systemd-tmpfiles-clean.timer loaded active waiting  Daily Cleanup of Temporary Directories
LOAD    = Reflects whether the unit definition was properly loaded.
184 loaded units listed. Pass -all to see loaded but inactive units, too.
htb-student@nixfund:~$ systemctl | grep load AppArmor
grep: AppArmor: No such file or directory
htb-student@nixfund:~$ systemctl | grep snapd
snapd.apparmor.service          loaded active exited   Load AppArmor profiles managed internally by snapd
snapd.seeded.service           loaded active exited   Wait until snapd is fully seeded
snapd.service                  loaded active running  Snap Daemon
snapd.socket                   loaded active running  Socket activation for snappy daemon

htb-student@nixfund:~$ ^C
htb-student@nixfund:~$ ^C
htb-student@nixfund:~$ ^C
```

Hack The Box - Academy — Mozilla Firefox

Kali Linux x Hack The Box - Acad x Hack The Box - Acad x + 10.10.15.254 15:22

File Actions Edit View Help

htb-student@nixfund: ~

HTB ACADEMY

Target: 10.129.251.225

Life Left: 99 minute(s) + Terminate X

SSH to 10.129.251.225 with user "htb-student" and password "HTB_academy_stdnt!"

+ 1 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.

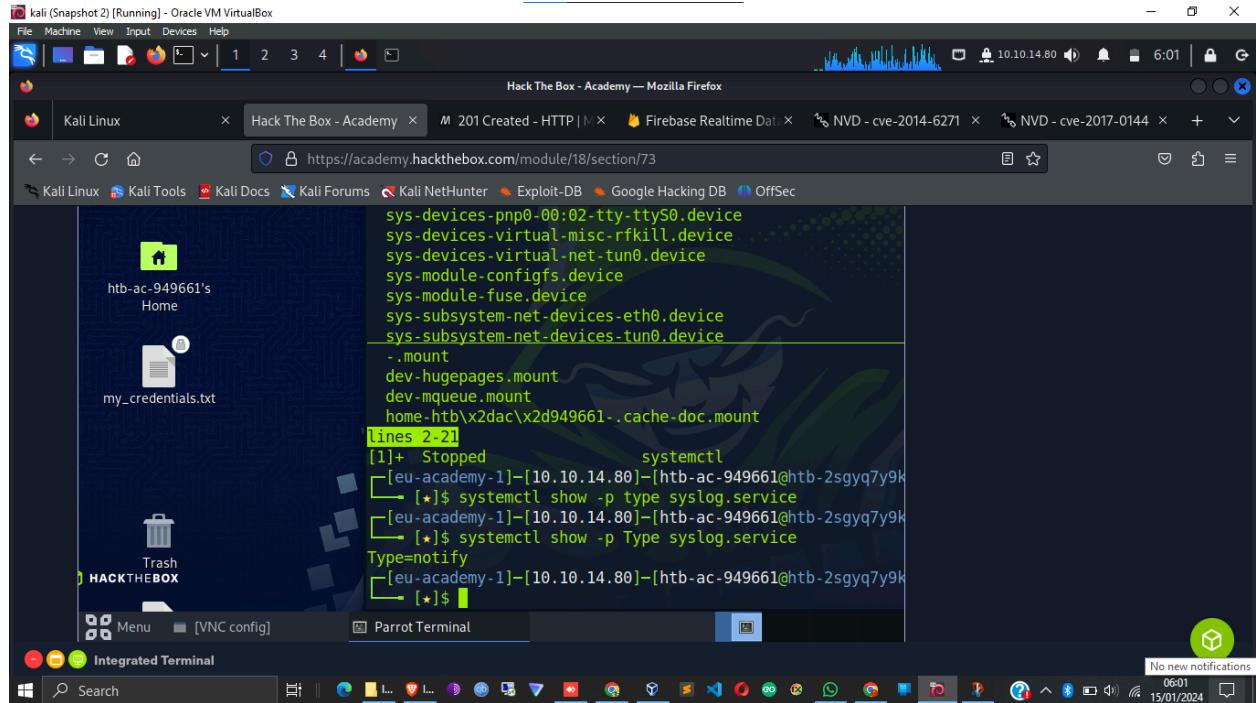
snapd.apparmor.service

Submit Hint

Previous Next Mark Complete & Next Right Ctrl

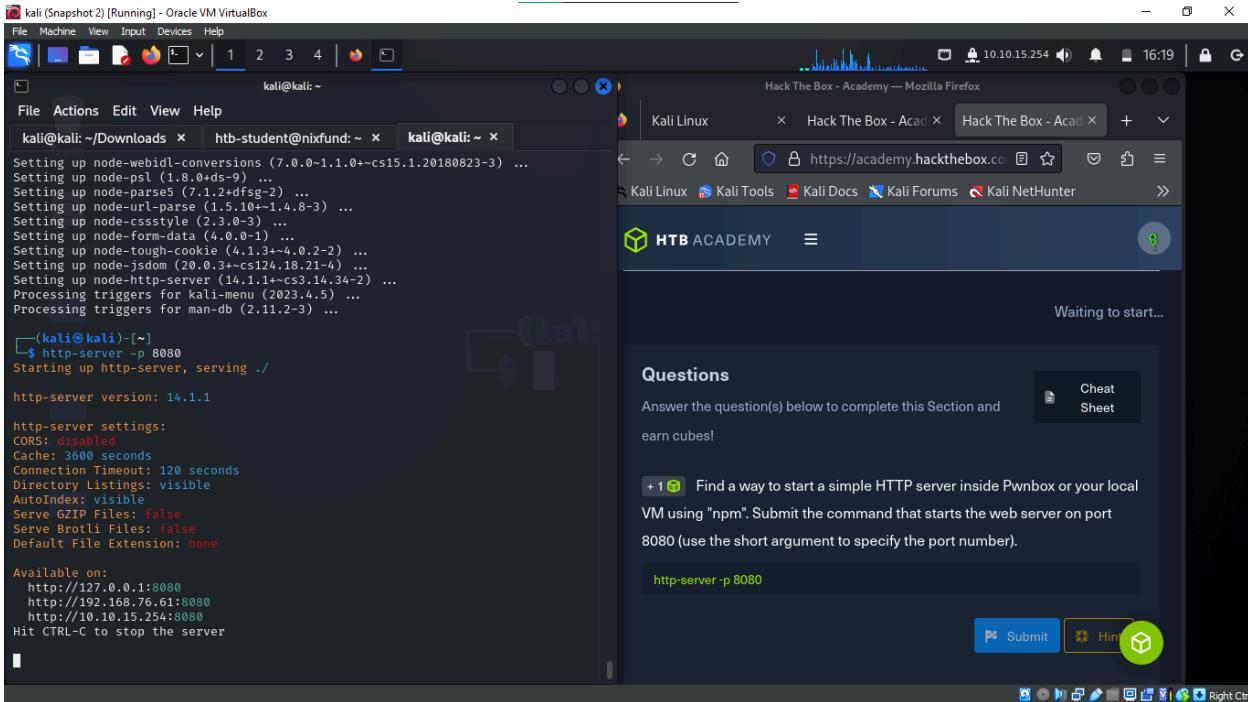
23. Question: What is the type of the service of the "syslog.service"?

- **Explanation:** The type of a service in systemd is specified in its unit file,
- which can be viewed using commands like **systemctl cat syslog.service**.
- **Answer:** notify



24. Question: Find a way to start a simple HTTP server inside Pwnbox or your local VM using "npm". Submit the command that starts the web server on port 8080 (use the short argument to specify the port number).

- **Explanation:** This requires using a Node.js package, such as http-server, which can be installed via npm. The command `http-server -p 8080` starts a simple HTTP server on port 8080.
 - **Answer:** `http-server -p 8080`



25. Question: Find a way to start a simple HTTP server inside Pwnbox or your local VM using "php". Submit the command that starts the web server on the localhost (127.0.0.1) on port 8080.

- **Explanation:** PHP has a built-in server that can be started for development purposes. The command `php -S 127.0.0.1:8080` starts a PHP server on localhost at port 8080.
 - **Answer:** `php -S 127.0.0.1:8080`

The screenshot shows a web browser window with multiple tabs open. The active tab is titled "PHP: Built-in web server". The page content is from the PHP documentation, specifically the section on the built-in web server. It includes a warning message about the experimental nature of the feature and examples of how to start the server and what it will output.

Warning This experimental feature is not intended for production usage. Generally, the built-in Web Server is not intended for production usage.

Example #1 Starting the web server

```
$ cd ~/public_html  
$ php -S localhost:8000
```

The terminal will show:

```
PHP 5.4.0 Development Server started at Thu Jul 21 10:43:28 2011  
Listening on localhost:8000  
Document root is /home/me/public_html  
Press Ctrl-C to quit
```

After URI requests for <http://localhost:8000/> and <http://localhost:8000/myscript.html> the terminal will show something similar to:

26. Question: How many partitions exist in our Pwnbox? (Format: 0)

- **Explanation:** The number of partitions can be determined using disk management tools like fdisk, lsblk, or df. These tools provide information about the disk partitions on the system.
- **Answer:** 3

The screenshot shows a Linux desktop environment, likely Parrot OS, with a terminal window open. The terminal window title is "Parrot Terminal". Inside the terminal, the user has run the command "lsblk -l | grep 'part'" which lists the partitions on the system. The output shows three partitions: "/dev/ac-949661" (root), "/dev/ac-949661/home" (home), and "/dev/ac-949661/credentials.txt" (credentials).

```
[eu-academy-1]-[10.10.15.254]-[htb-ac-949661@htb-jtuggdqbv8]-[~]  
└─[★]$ lsblk -l | grep 'part' | wc -l  
3  
[eu-academy-1]-[10.10.15.254]-[htb-ac-949661@htb-jtuggdqbv8]-[~]  
└─[★]$
```

Each of these questions and answers delves into various aspects of Linux fundamentals, such as system configuration, user management, networking, file systems, and basic server setup. The explanations provide insight into the commands and methods used to obtain the required information, demonstrating essential Linux system administration skills.

Find the sharable link

<https://academy.hackthebox.com/achievement/949661/18>

