



Eric Mwenda

**Linux Fundamentals**

<https://academy.hackthebox.com/achievement/596337/18>

Process made to connect to my Virtual Machine:

1. I downloaded the vpn file provided in the module.
2. Opened my terminal.
3. Located to where the file was downloaded in, that is the Downloads folder.
4. Opened it with the command **sudo openvpn academy-regular.ovpn**

The screenshot shows a terminal window titled '- : sudo openvpn — Konsole'. The terminal has a menu bar with File, Edit, View, Bookmarks, Plugins, Settings, Help, and a toolbar with Copy, Paste, and Find. The terminal content shows a user named 'coderic' at a Kali Linux prompt. The user runs 'cd Downloads/htb\_academy' and then 'sudo openvpn academy-regular.ovpn'. The terminal then displays a log of the OpenVPN connection process, including various system messages and security details, such as certificate validation and TLS handshakes. The log ends with a successful connection message.

```
(coderic㉿kali)-[~] action    Show QUICK Commands set with QAction::setShortcut()! Use KActionCollection::setShortcut()
$ cd Downloads/htb_academy
(coderic㉿kali)-[~/Downloads/htb_academy]
$ sudo openvpn academy-regular.ovpn
[sudo] password for coderic:
2024-01-25 11:27:42 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent packets are not compressed unless "allow-compression yes" is also set.
2024-01-25 11:27:42 Note: --data-cipher-fallback with cipher 'AES-128-CBC' disables data channel offload.
2024-01-25 11:27:42 OpenVPN 2.6.0 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2024-01-25 11:27:42 library versions: OpenSSL 3.1.4 24 Oct 2023, LZO 2.10
2024-01-25 11:27:42 Outgoing Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication
2024-01-25 11:27:42 Incoming Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication
2024-01-25 11:27:42 TCP/UDP: Preserving recently used remote address: [AF_INET]23.106.59.92:1337
2024-01-25 11:27:42 Socket Buffers: R=[212992->212992] S=[212992->212992]
2024-01-25 11:27:42 UDPv4 link local: (not bound)
2024-01-25 11:27:42 UDPv4 link remote: [AF_INET]23.106.59.92:1337
2024-01-25 11:27:42 TLS: Initial packet from [AF_INET]23.106.59.92:1337, sid=c2ce9e0b b5bab627
2024-01-25 11:27:42 VERIFY OK: depth=1, C=UK, ST=City, L=London, O=HackTheBox, CN=HackTheBox CA, name=htb, emailAddress=info@hackthebox.eu
2024-01-25 11:27:42 VERIFY KU OK
2024-01-25 11:27:42 Validating certificate extended key usage
2024-01-25 11:27:42 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2024-01-25 11:27:42 VERIFY EKU OK
2024-01-25 11:27:42 VERIFY OK: depth=0, C=UK, ST=City, L=London, O=HackTheBox, CN=htb, name=htb, emailAddress=info@hackthebox.eu
2024-01-25 11:27:49 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 2048 bit RSA, signature: RSA-SHA1
2024-01-25 11:27:49 [htb] Peer Connection Initiated with [AF_INET]23.106.59.92:1337
2024-01-25 11:27:49 TLS: move_session: dest=TM_ACTIVE src=TM_INITIAL reinit_src=1
2024-01-25 11:27:49 TLS: tls_multi_process: initial untrusted session promoted to trusted
2024-01-25 11:27:50 SENT CONTROL [htb]: 'PUSH_REQUEST' (status=1)
2024-01-25 11:27:51 PUSH: Received control message: 'PUSH_REPLY, route 10.10.10.0 255.255.254.0,route 10.129.0.0 255.255.0.0,route-i
pv6 dead:beef::/64,explicit-exit-notify,tun-ipv6,route-gateway 10.10.14.1,topology subnet,ping 10,ping-restart 120,ifconfig-ipv6 de
ad:beef:2::116e/64 dead:beef:2::1,ifconfig 10.10.15.112 255.255.254.0,peer-id 185,cipher AES-256-CBC'
2024-01-25 11:27:51 OPTIONS IMPORT: timers and/or timeouts modified
2024-01-25 11:27:51 OPTIONS IMPORT: explicit notify param(s) modified
2024-01-25 11:27:51 OPTIONS IMPORT: --ifconfig/up options modified
2024-01-25 11:27:51 OPTIONS IMPORT: route_options modified
```

**Linux Fundamentals module location:**

After login into HackTheBox Academy, I searched for “Linux Fundamentals” under the search option hence landing on my assignment.

The screenshot shows the HTB Academy interface. On the left is a sidebar with a user profile for 'coderic' (Free, 60 cubes), sections for LEARN (Dashboard, Exams, Modules, Paths, Academy x HTB Labs), MY ACHIEVEMENTS (My Certificates, My Badges), and REFERRALS. The main content area is titled 'LINUX FUNDAMENTALS' and features a large image of Tux. Below it is the 'Linux Fundamentals' module summary, which includes a star rating of 5, a brief description, and a list of topics covered. To the right is a 'Module Sections' sidebar with links to various Linux concepts.

Starting to the htб virtual machine:

The screenshot shows a VNC session connected to a Parrot OS virtual machine. The desktop environment includes a menu bar with Applications, Places, System, and a terminal window titled 'Parrot Terminal'. The terminal displays network interface statistics for 'Pwnhole' and 'tun0'. The status bar at the bottom indicates a connection to 'htb-ac-596337' and shows 'Connected to htb-gqdhdlfr9t:1 (htb-ac-596337)'.

## Connection to the machine using ssh protocol:

username: htб-student

Password: HTB @cademy stdnt!

IP: 10.129.35.12

ssh htb-student@10.129.35.12

The screenshot shows a terminal window titled "htb-student@nixfund: ~". The session is connected to "htb-ac-596337" via port 22. The user has run the command "ssh htb-student@10.129.35.12 -p HTB\_academy\_stdnt!". The terminal displays the host's system information, including its load average (0.27), memory usage (51.0% of 6.76GB), and swap usage (0%). It also shows that Canonical Livepatch is available for installation. The user has run "htop" to view the process list, which shows 154 processes running. The terminal also displays the last login information: "Last login: Wed Sep 23 22:09:41 2020 from 10.10.14.6".

This screenshot is identical to the one above, showing the same terminal session and system information. The user has run "htop" again, and the terminal displays the same details about the system's load, memory usage, and process count.

Here is the Target shell.

## SYSTEM INFORMATION

**Find out the machine hardware name and submit it as the answer.**

To find out the machine name I used command “uname” and attribute “-n”

Command used:- uname -n

## ANS: x86\_64

my\_crede Last login: Wed Sep 23 22:09:41 2020 from 10.10.14.6  
htb-student@nixfund:~\$ ls  
htb-student@nixfund:~\$ whoami  
htb-student  
htb-student@nixfund:~\$ uname -a  
Linux nixfund 4.15.0-123-generic #126-Ubuntu SMP Wed Oct 21 09:40:11 UTC 2020 x8  
6 64 x86\_64 x86\_64 GNU/Linux  
htb-student@nixfund:~\$ uname -m  
htb-student@nixfund:~\$

Connected to htb-gqdhdlfr9t:1 (htb-ac-596337)

Life Left: 101m

**Questions**  
Answer the question(s) below to complete this Section and earn cubes!

Target: 10.129.35.12   
Life Left: 110 minute(s) +  X

💡 SSH to 10.129.35.12 with user "htb-student" and password "HTB\_@cademy\_stdnt!"  
+ 0   
x86\_64

Integrated Terminal

## What is the path to htb-student's home directory?

To navigate in the htb-student I went back one directory, then keyed in the command “ls” to view all files available in that directory. Here is where I found the “htb-student” directory and without much I could see the path was **ANS: /home/htb-student**

x86\_64  
htb-student@nixfund:~\$ cd ..  
htb-student@nixfund:/home\$ ls  
cry0l1t3 htb-student mrb3n  
htb-student@nixfund:/home\$

Connected to htb-gqdhdlfr9t:1 (htb-ac-596337)

Life Left: 99m

**Questions**  
Answer the question(s) below to complete this Section and earn cubes!

Target: 10.129.35.12   
Life Left: 108 minute(s) +  X

+ 1

+ 1   
/home/htb-student

## What is the path to the htb-student's mail?

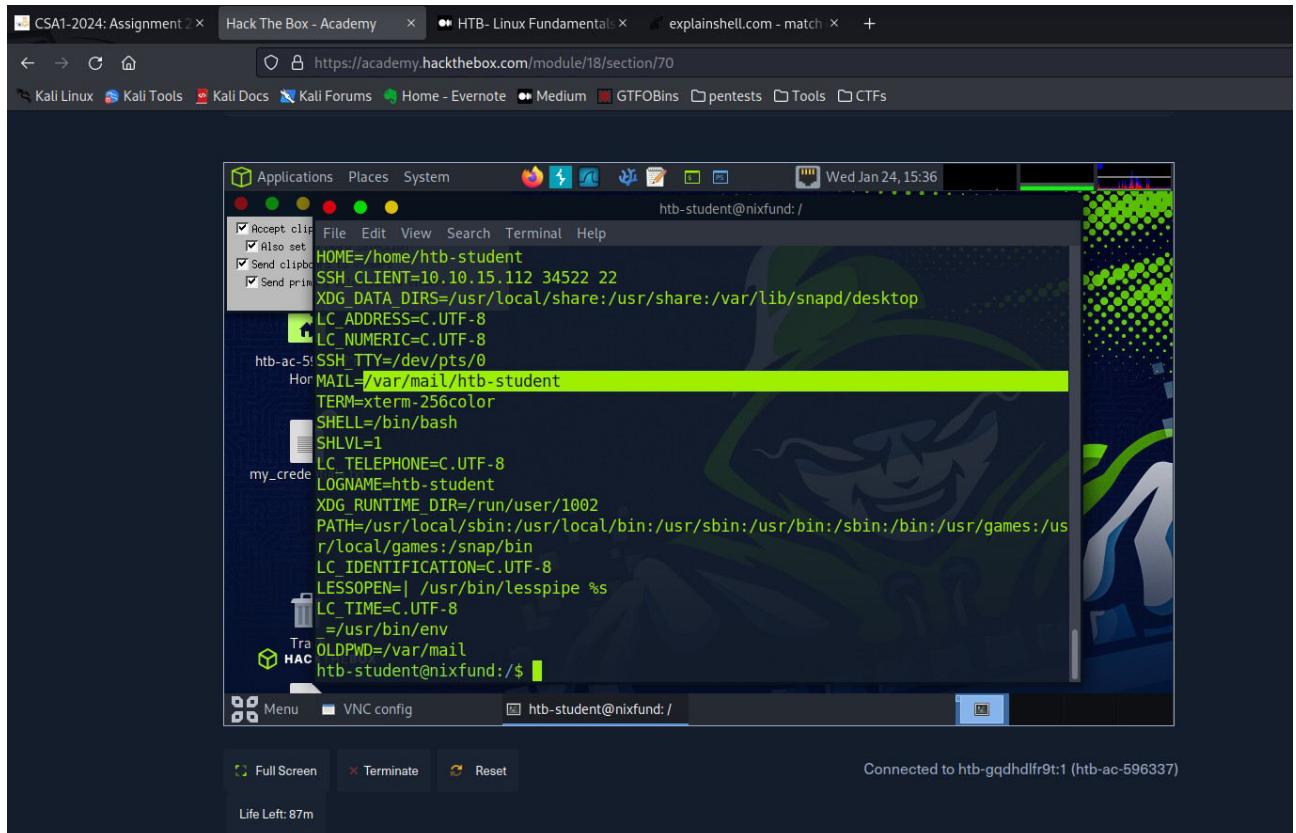
To get this path I used env and grep command

- env is a shell command used to either print a list of environment variables.

- Grep command can be used to find or search a regular expression or a string in a text file.

Command used:- env | grep MAIL

## ANS: /var/mail/htb-student



## Which shell is specified for the htb-student user?

The shell information is stored in the etc/passwd file we can open this file to view the information on which shell is specified to the user "htb-student"

I navigated to etc/passwd and run the file using the command "cat passwd" the file we are looking for is the one that has root permissions which is:- **ANS bin/bash**

A screenshot of a terminal window titled "htb-student@nixfund:~". The terminal shows a list of users and groups from the /etc/passwd file. The output includes:

```
htb-student:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
htb-ac-5:bin:x:2:2:bin:/bin:/usr/sbin/nologin
Hor:sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:0:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
```

### **Which kernel version is installed on the system? (Format: 1.22.3)**

The information of the installed kernel and OS can be seen with the 'uname' command. However, we can use additional attributes for specific information, such as '-a' for all the available information or '-r' for the release version of the installed version.

Command used:- uname -r

**ANS: 4.15.0**

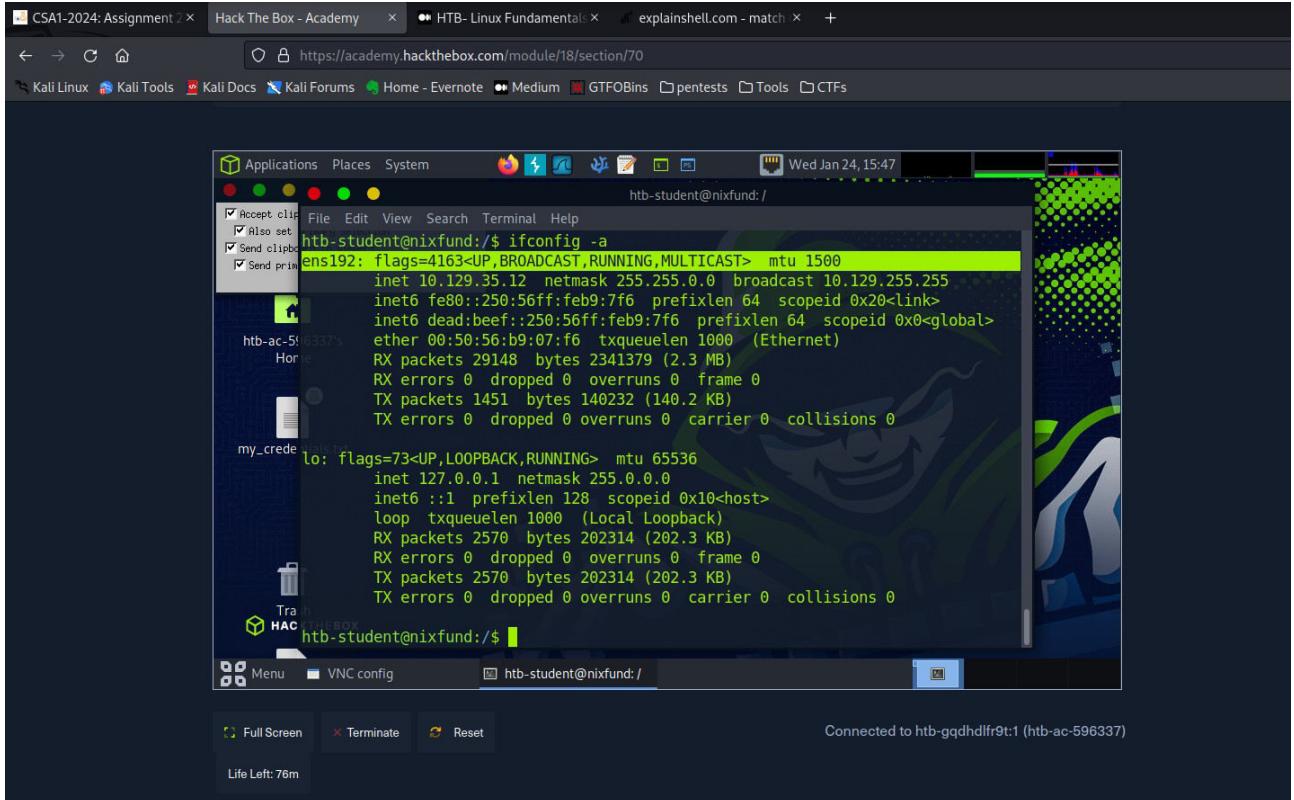
A screenshot of a terminal window titled "htb-student@nixfund:~". The terminal shows the output of the 'ls' command followed by the output of the 'uname -r' command. The output includes:

```
htb-student@nixfund:~$ ls
bin dev initrd.img lib64 mnt root snap tmp vmlinuz
boot etc initrd.img.old lost+found opt run srv usr vmlinuz.old
cdrom home lib media proc sbin sys var
htb-student@nixfund:~$ uname -r
4.15.0-123-generic
htb-student@nixfund:~$
```

### **What is the name of the network interface that MTU is set to 1500?**

To view network interfaces in linux environments we can use “ifconfig” command. By running this command I found the MTU for interface ens192 set to 1500

**ANS: ens192**



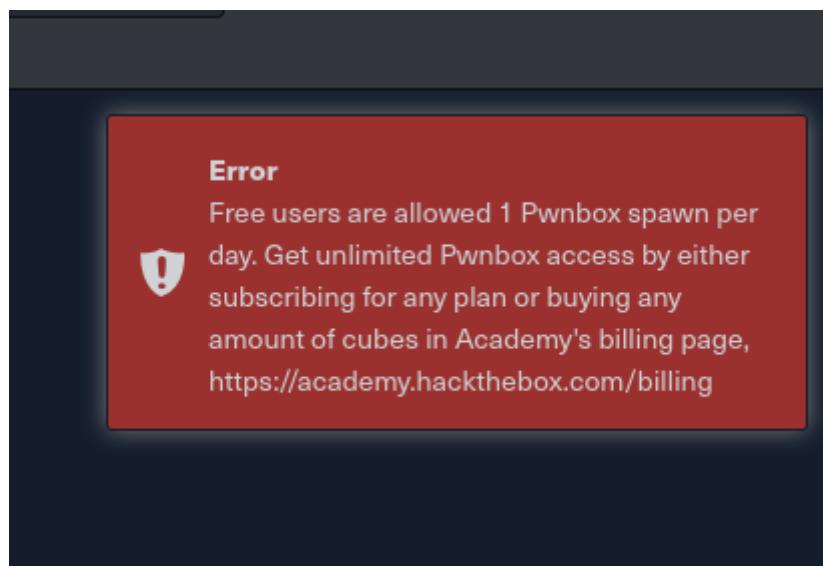
A screenshot of a Kali Linux desktop environment via VNC. The terminal window shows the output of the command `htb-student@nixfund:~$ ifconfig -a`. The output lists network interfaces and their configurations, including the MTU for ens192.

```
htb-student@nixfund:~$ ifconfig -a
ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.129.35.12 netmask 255.255.0.0 broadcast 10.129.255.255
              inet6 fe80::250:56ff:feb9:7f6 prefixlen 64 scopeid 0x20<link>
        inet6 dead:beef::250:56ff:feb9:7f6 prefixlen 64 scopeid 0x0<global>
          ether 00:50:56:b9:07:f6 txqueuelen 1000 (Ethernet)
            RX packets 29148 bytes 2341379 (2.3 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 1451 bytes 140232 (140.2 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

my_creds: lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
            RX packets 2570 bytes 202314 (202.3 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 2570 bytes 202314 (202.3 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
htb-student@nixfund:~$
```

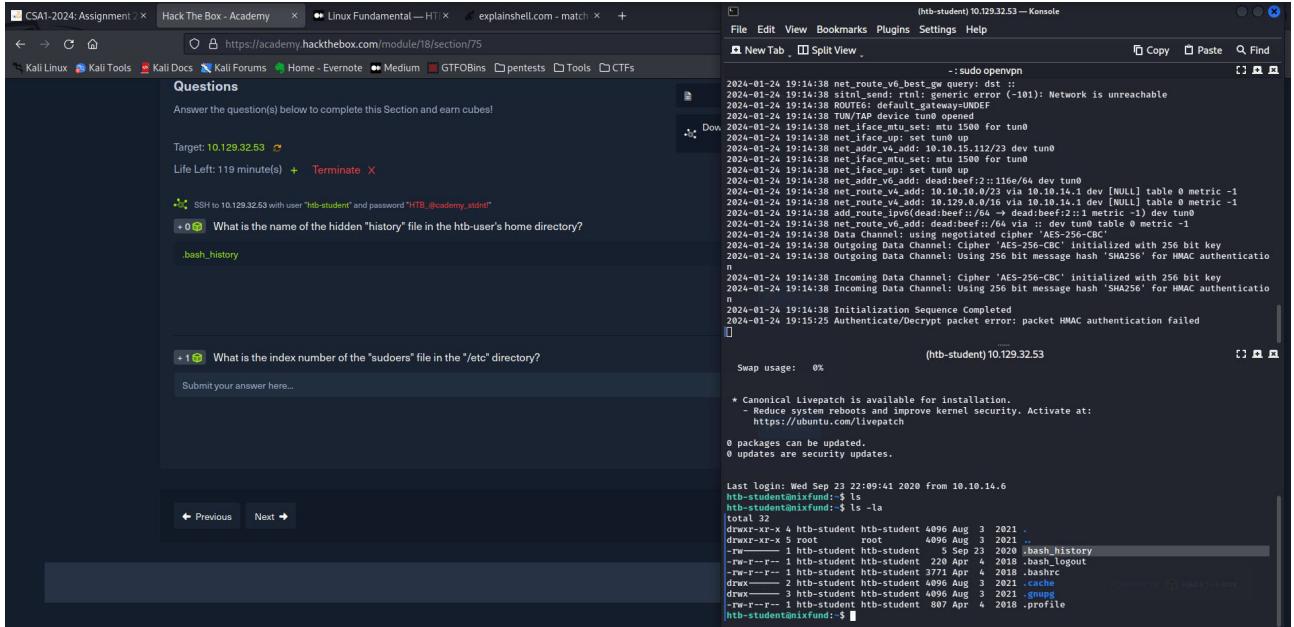
## NAVIGATION

After concluding the section on System Information, I terminated the virtual machine provided in htb academy and on powering it back on I got an error only to realize I have one offer per day to use the htb virtual machine therefore I had to switch to my Local virtual machine using the VPN file provided in the module hence from here my IP address will keep changing as I did the work in different timestamps.



## **What is the name of the hidden "history" file in the htб-user's home directory?**

I first did an “ls” on this directory but couldn’t find any file present therefore, I used ‘ls -la’ to list all items (including hidden) briefly of the home directory and with that I was able to see the hidden file that was lacking with an history file attached on it **ANS: .bash\_history**



The screenshot shows a terminal window titled '(htб-student) 10.129.32.53 — Konsole'. The window displays a history of commands run by the htб-student user. The commands include network configuration (net\_route, net\_iface), setting MTU for tun0, and various SSH sessions. The terminal also shows a warning about Canonical Livepatch and a successful initialization sequence. At the bottom, the user runs 'ls -la' in their home directory, which lists several files, including a hidden file named '.bash\_history'.

```
2024-01-24 19:14:38 net_route_v6_best_gw query: dst ::  
2024-01-24 19:14:38 sitnl_send: rtnl: generic error (-101): Network is unreachable  
2024-01-24 19:14:38 ROUTE6: default_gateway=UNDEF  
2024-01-24 19:14:38 TUN/tap0: MTU:1500 qdisc mq  
2024-01-24 19:14:38 net_iface_mtu set: mtu 1500 for tun0  
2024-01-24 19:14:38 net_iface_up: set tun0 up  
2024-01-24 19:14:38 net_addr_v4_add: 10.10.15.112/23 dev tun0  
2024-01-24 19:14:38 net_route_mtu_set: mtu 1500 for tun0  
2024-01-24 19:14:38 net_iface_mtu_set: mtu 1500 for tun0  
2024-01-24 19:14:38 net_addr_v6_add: dead:bee:f2::116e/64 dev tun0  
2024-01-24 19:14:38 net_route_v4_add: 10.10.10.0/23 via 10.10.14.3 dev [NULL] table 0 metric -1  
2024-01-24 19:14:38 net_route_v4_add: 10.10.10.0/16 via 10.10.14.3 dev [NULL] table 0 metric -1  
2024-01-24 19:14:38 net_route_v4_add: 10.10.10.0/24 via 10.10.14.3 dev [NULL] table 0 metric -1  
2024-01-24 19:14:38 net_route_v6_add: dead:bee:f2::/64 via :: dev tun0 table 0 metric -1  
2024-01-24 19:14:38 Data Channel: using negotiated cipher 'AES-256-CBC'  
2024-01-24 19:14:38 Outgoing Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key  
2024-01-24 19:14:38 Incoming Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key  
2024-01-24 19:14:38 Incoming Data Channel: Using 256 bit message hash 'SHA256' for HMAC authentication  
2024-01-24 19:14:38 Initialization Sequence Completed  
2024-01-24 19:15:25 Authenticate/Decrypt packet error: packet HMAC authentication failed  
[...]  
Swappiness: 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 from 10.10.14.6  
htб-student@htб-xfund:~$ ls -la  
htб-student@htб-xfund:~$ ls -la  
total 32  
drwxr-xr-x 4 htб-student htб-student 4096 Aug 3 2021 .  
drwxr-xr-x 5 root root 4096 Aug 3 2021 ..  
-rw-r--r-- 1 htб-student htб-student 23 Apr 4 2018 .bash_history  
-rw-r--r-- 1 htб-student htб-student 220 Apr 4 2018 .bash_logout  
-rw-r--r-- 1 htб-student htб-student 3771 Apr 4 2018 .bashrc  
drwxr--r-- 2 htб-student htб-student 4096 Aug 3 2021 .cache  
drwxr--r-- 3 htб-student htб-student 4096 Aug 3 2021 .groups  
-rw-r--r-- 1 htб-student htб-student 687 Apr 4 2018 .profile  
htб-student@htб-xfund:~$
```

## **What is the index number of the "sudoers" file in the "/etc" directory?**

Command used:- “ls -i”

The ls command is a command-line utility for listing the contents of a directory

-i will list the index for the files in the specified directory, with joining both “ls” and “-i” a files in the /etc directory all appear with their given indexes one of the files is sudoers appears with index no 147627

**ANS: 147627**

```

(hb-student) 10.129.32.53 — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
-: sudo openvpn
2024-01-24 19:14:38 net/route_v6_best_gw query: dst :: 0.0.0.0/0 metric 1 dev [NULL] table 0 metric -1
2024-01-24 19:14:38 ROUTE6I default_gateway_metric error (-101): Network is unreachable
2024-01-24 19:14:38 TUN/TAP device tun0 opened
2024-01-24 19:14:38 net_iface_mtu_set: stu 15000 for tun0
2024-01-24 19:14:38 net_iface_ip6_set: stu 10.15.1.12/23 dev tun0
2024-01-24 19:14:38 net_iface_mtu_set: stu 15000 for tun0
2024-01-24 19:14:38 net_iface_up set tun0 up
2024-01-24 19:14:38 net_addr_v6_add: dead:beef:2:116f:64 dev tun0
2024-01-24 19:14:38 net_route_v4_add: 10.129.0.0/16 via 10.10.14.1 dev [NULL] table 0 metric -1
2024-01-24 19:14:38 net_route_v6_add: 10.129.0.0/16 via 10.10.14.1 dev [NULL] table 0 metric -1
2024-01-24 19:14:38 addr_route_ipv6_(dead:beef::64 via :: dev tun0 table 0 metric -1)
2024-01-24 19:14:38 net_iface_ip6_set: stu 15000 for tun0
2024-01-24 19:14:38 outgoing Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
2024-01-24 19:14:38 Outgoing Data Channel: Using 256 bit message hash 'SHA256' for HMAC authentication
2024-01-24 19:14:38 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
2024-01-24 19:14:38 Incoming Data Channel: Using 256 bit message hash 'SHA256' for HMAC authentication
2024-01-24 19:15:25 Authenticate/Decrypt packet error: packet HMAC authentication failed
[...]
+ 1 2 What is the name of the hidden "history" file in the htb-user's home directory?
.bash_history

147627

← Previous Next →

```

## Working with Files and Directories

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

Command used:- ls -la -t

ls - lists the contents of a directory, la – lists all, -t shows the last time of modification. In our results apt.extended\_states.0 appears to be last modified on Nov 12 2020. **ANS: apt.extended\_states.0**

```

(hb-student) 10.129.32.53 — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
-: sudo openvpn
eived key id: 2, known key id: [key#0 state=S_GENERATED_KEYS auth=K5_AUTH TRUE id=0 sid=7d3282e9 f7 92a0c] [key#1 state=S_UNDEF auth=K5_AUTH FALSE id=0 sid=00000000 00000000] [key#2 state=S_UNDEF auth=K5_AUTH FALSE id=0 sid=00000000 00000000]
2024-01-24 19:29:24 Authenticate/Decrypt packet error: packet HMAC authentication failed
2024-01-24 19:29:24 TLS ECDHE-RSA-AES256-GCM-SHA384 keys are out of sync: AF 7d3282e9 100d 09:23:137 [enc 92a0c] [key#1 state=S_UNDEF auth=K5_AUTH FALSE id=0 sid=00000000 00000000] [key#2 state=S_UNDEF auth=K5_AUTH FALSE id=0 sid=00000000 00000000]
[...]
(hb-student) 10.129.32.53 — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
-: sudo openvpn
-rw—— 1 root shadow 716 Sep 23 2020 gshadow.bak
-rw—— 1 root root 860 Sep 23 2020 group.back
drwxr-xr-x 14 root root 4096 Sep 23 2020 ...
-rw-r--r-- 1 root root 437 Aug 5 2019 dpkg-diversions.0
-rw-r--r-- 1 root root 202 Aug 5 2019 dpkg-diversions.1.gz
-rw-r--r-- 1 root root 202 Aug 5 2019 dpkg-diversions.2.gz
-rw-r--r-- 1 root root 202 Aug 5 2019 dpkg-diversions.3.gz
-rw-r--r-- 1 root root 202 Aug 5 2019 dpkg-diversions.4.gz
-rw-r--r-- 1 root root 202 Aug 5 2019 dpkg-diversions.5.gz
-rw-r--r-- 1 root root 202 Aug 5 2019 dpkg-diversions.6.gz
total 2168
drwxr-xr-x 2 root root 4096 Aug 5 2019 alternatives.tar.0
-rw-r--r-- 1 root root 41872 Aug 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 742750 Nov 11 2020 upnp-status.0
-rw-r--r-- 1 root root 286270 Nov 5 2020 dpkg.status.0.gz
-rw-r--r-- 1 root root 286270 Nov 5 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 51200 Oct 29 2020 alternatives.tar.0
-rw-r--r-- 1 root root 4623 Oct 22 2020 apt.extended.states.2.gz
-rw-r--r-- 1 root root 2497 Oct 2020 alternative.tar.1.gz
-rw-r--r-- 1 root root 4002 Oct 2020 alternative.tar.2.gz
-rw-r--r-- 1 root root 2492 Sep 24 2020 alternative.tar.3.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.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
[...]
+ 1 2 What is the inode number of the "shadow.bak" file in the "/var/backups" directory?
apt.extended.states.0

Submit your answer here...

```

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

First is to navigate to the file “shadow.bak” then run the command ls -i | grep shadow.bak to get the inode number. **ANS: 265293**

The screenshot shows a Kali Linux desktop environment with several windows open. In the foreground, a terminal window titled '(htb-student) 10.129.32.53 — Konsole' displays a password dump from a Wi-Fi interface. The output includes several entries for 'key#1' and 'key#2' with various authentication status codes like 'S\_undef', 'K5\_AUTH\_FALSE', and 'K5\_AUTH\_TRUE'. Below this, a command-line search for 'shadow.bak' in the '/var/backups' directory is shown, resulting in a single file found: '265293 shadow.bak'.

```

(htb-student) 10.129.32.53 — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
-: sudo openvpn
92af0c] [key#1 state=S_undef auth=K5_AUTH_FALSE id=0 sid=00000000 00000000] [key#2 state=S_undef auth
=K5_AUTH_FALSE id=0 sid=00000000 00000000]
2024-01-24 19:30:19 TLS Error: local/remote TLS keys are out of sync: [AF_INET]23.106.59.92:1337 (rec
eived key id 1, known key ids: [key#1 state=S_GENERATED_KEYS auth=K5_AUTH_TRUE id=0 sid=7d3282e9 f7
=K5_AUTH_FALSE id=0 sid=00000000 00000000] [key#2 state=S_undef auth
=K5_AUTH_FALSE id=0 sid=00000000 00000000])
2024-01-24 19:30:50 TLS Error: local/remote TLS keys are out of sync: [AF_INET]23.106.59.92:1337 (rec
eived key id 1, known key ids: [key#1 state=S_GENERATED_KEYS auth=K5_AUTH_TRUE id=0 sid=7d3282e9 f7
=K5_AUTH_FALSE id=0 sid=00000000 00000000])
2024-01-24 19:32:53 TLS Error: local/remote TLS keys are out of sync: [AF_INET]23.106.59.92:1337 (rec
eived key id 1, known key ids: [key#1 state=S_GENERATED_KEYS auth=K5_AUTH_TRUE id=0 sid=7d3282e9 f7
=K5_AUTH_FALSE id=0 sid=00000000 00000000]) [key#2 state=S_undef auth
=K5_AUTH_FALSE id=0 sid=00000000 00000000]
[...]
(htb-student) 10.129.32.53
-rw-r--r-- 1 root root 286270 Nov 5 2020 dpgk.statuses.3.gz
-rw-r--r-- 1 root root 286270 Nov 5 2020 dpgk.statuses.4.gz
-rw-r--r-- 1 root root 286270 Nov 5 2020 dpgk.statuses.5.gz
-rw-r--r-- 1 root root 286270 Nov 5 2020 dpgk.statuses.6.gz
-rw-r--r-- 1 root root 51200 Oct 29 2020 alternatives.tar.gz
-rw-r--r-- 1 root root 4623 Oct 22 2020 apt.extended.states.7.gz
-rw-r--r-- 1 root root 2401 Sep 24 2020 apt.extended.states.8.gz
-rw-r--r-- 1 root root 4601 Oct 15 2020 apt.extended.states.9.gz
-rw-r--r-- 1 root root 2492 Sep 24 2020 alternatives.tar.2.gz
-rw-r--r-- 1 root root 367 Sep 23 2020 dpkg.statoverride.1.gz
-rw-r--r-- 1 root root 237 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.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.4.gz
-rw-r--r-- 1 root root 229 Sep 23 2020 dpkg.statoverride.5.gz
-rw-r--r-- 1 root root 4572 Sep 23 2020 apt.extended.states.1.gz
-rw-r--r-- 1 root root 2014 Sep 23 2020 passwd.bak
-rw-r--r-- 1 root root 1362 Sep 23 2020 shadow.bak
-rw-r--r-- 1 root shadow 1362 Sep 23 2020 shadow.bak
-rw-r--r-- 1 root root 860 Sep 23 2020 group.bak
drwxr-xr-x 14 root root 4096 Sep 23 2020 ...
-rw-r--r-- 1 root root 437 Aug 5 2019 dpkg.diversions.0
-rw-r--r-- 1 root root 202 Aug 5 2019 dpkg.diversions.1.gz
-rw-r--r-- 1 root root 202 Aug 5 2019 dpkg.diversions.2.gz
-rw-r--r-- 1 root root 202 Aug 5 2019 dpkg.diversions.3.gz
-rw-r--r-- 1 root root 202 Aug 5 2019 dpkg.diversions.3.gz
-rw-r--r-- 1 root root 202 Aug 5 2019 dpkg.diversions.4.gz
-rw-r--r-- 1 root root 202 Aug 5 2019 dpkg.diversions.4.gz
[...]
htb-student@htb:~$ find /var/backups -name "shadow.bak" -size +25k -size -28k --newermt 2020-03-03 2>/dev/null
265293 shadow.bak
htb-student@htb:~$ ls -l | grep shadow.bak
265293 shadow.bak
htb-student@htb:~$ ^C

```

## Editing files

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?

Command used is: find / -type f -name “\*.conf” -size +25k -size -28k --newermt 2020-03-03 2>/dev/null

- find - The command used for searching files and directories.
- /: The starting directory for the search, in this case, the root directory.
- -type f: Specifies that the search is for files (not directories).
- -name “\*.conf”: Specifies that the file names should match the pattern “\*.conf” (files with the “.conf” extension).
- -size +25k -size -28k: Filters files based on size. It searches for files larger than 25 kilobytes and smaller than 28 kilobytes.
- --newermt 2020-03-03: Filters files modified after the specified date (March 3, 2020).
- 2>/dev/null: Redirects error messages to /dev/null, discarding them. This is done to suppress any permission denied or other error messages that might occur during the search.

**ANS: 00-mesa-defaults.conf**

**Questions**

Answer the question(s) below to complete this Section and earn cubes!

Target: 10.129.29.51

Life Left: 113 minute(s) + Terminate X

SSH to 10.129.29.51 with user "htb-student" and password "HTB\_@cademy\_stdt!!"

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

00-mesa-defaults.conf

+ 0 How many files exist on the system that have the ".bak" extension?

Submit your answer here...

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

Submit your answer here...

(htb-student) 10.129.29.51

```
-:sudo openvpn
2024-01-24 19:58:57 net_route_v4_add: 10.129.0.0/16 via 10.10.14.1 dev [NULL] table 0 metric -1
2024-01-24 19:58:57 add_route_ipv6dead:beef::/64 via dead:beef::1 metric -1 dev tun0
2024-01-24 19:58:57 add_route_ip4dead:beef::/32 via dead:beef::1 metric -1 dev tun0
2024-01-24 19:58:57 Data Channel: Using negotiate cipher 'AES-256-CBC'
2024-01-24 19:58:57 Outgoing Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
2024-01-24 19:58:57 Incoming Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
2024-01-24 19:58:57 Incoming Data Channel: Using 256 bit message hash 'SHA256' for HMAC authentication
2024-01-24 19:58:57 Sequence Completed
2024-01-24 20:00:30 Authenticate/Decrypt packet error: packet HMAC authentication failed

[...]
```

Are you sure you want to continue connecting (yes/no/[Fingerprint])? yes

Warning: Permanently added '10.129.29.51' (ED25519) to the list of known hosts.

htb-student@10.129.29.51's password:

Permission denied, please try again.

htb-student@10.129.29.51'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 Wed Jan 24 17:00:04 UTC 2024
System load: 0.22 Processes: 155
Usage of /: 51.0% of 6.76GB Users logged in: 0
Memory usage: 21% IP address for ens192: 10.129.29.51
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 / -type f -name *.conf" -size +25k -size -28k -newermt 2020-03-03 2>/dev/null
htb-student@nixfund:~$ find / -type f -name *.conf -user root -size +25k -size -28k -newermt 2020-03-03 -exec ls -al {} ; 2>/dev/null
-rw-r--r-- 1 root root 27422 Jun 12 2020 /usr/share/drirc.d/00-mesa-defaults.conf
htb-student@nixfund:~$
```

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

Using command :- `find / -type f -iname *.bak 2>/dev/null | wc -l`

Here "wc-l" Counts the number of lines in the input it receives. In this context, it counts the number of files found by the find command.

**ANS: 4**

**Questions**

Answer the question(s) below to complete this Section and earn cubes!

Target: 10.129.29.51

Life Left: 110 minute(s) + Terminate X

SSH to 10.129.29.51 with user "htb-student" and password "HTB\_@cademy\_stdt!!"

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

00-mesa-defaults.conf

+ 0 How many files exist on the system that have the ".bak" extension?

4

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

Submit your answer here...

(htb-student) 10.129.29.51

```
-:sudo openvpn
2024-01-24 19:58:57 Incoming Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
2024-01-24 19:58:57 Initialization Sequence Completed
2024-01-24 20:00:30 Authenticate/Decrypt packet error: packet HMAC authentication failed
2024-01-24 20:04:19 TLS Error: local/remote TLS keys are out of sync: [AF_INET]23.106.59.92:1337 (received key id: 1, known key ids: [key#0 state=GENERATED_KEYS auth=KS_AUTH_TRUE id=0 sid=6402c30 40 TS=10659921337 auth=KS_AUTH_FALSE id#=00000000 00000000] [key#2 state=S_UNDER auth=KS_AUTH FALSE id#=00000000 00000000])
2024-01-24 20:04:53 Authenticate/Decrypt packet error: packet HMAC authentication failed
2024-01-24 20:05:54 Authenticate/Decrypt packet error: packet HMAC authentication failed
```

Warning: Permanently added '10.129.29.51' (ED25519) to the list of known hosts.

htb-student@10.129.29.51's password:

htb-student@10.129.29.51'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 Wed Jan 24 17:00:04 UTC 2024
System load: 0.22 Processes: 155
Usage of /: 51.0% of 6.76GB Users logged in: 0
Memory usage: 21% IP address for ens192: 10.129.29.51
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 / -type f -name *.conf" -size +25k -size -28k -newermt 2020-03-03 2>/dev/null
htb-student@nixfund:~$ find / -type f -name *.conf -user root -size +25k -size -28k -newermt 2020-03-03 -exec ls -al {} ; 2>/dev/null
-rw-r--r-- 1 root root 27422 Jun 12 2020 /usr/share/drirc.d/00-mesa-defaults.conf
htb-student@nixfund:~$
```

## **Submit the full path of the "xxd" binary.**

I used the “which” command that allows users to search the list of paths in the \$PATH environment variable and outputs the full path of the command specified as an argument.

Command used:- which xxd

**ANS: /usr/bin/xxd**

```
File Edit View Bookmarks Plugins Settings Help
File New Tab Split View
- :sudo openvpn
n
2024-01-24 19:58:57 Initialization Sequence Completed
2024-01-24 20:00:30 Authenticate/Decrypt packet error: packet HMAC authentication failed
2024-01-24 20:04:19 TLS Error: local/remote TLS keys are out of sync: [AF_INET]23.106.59.92:1337 (received key id: 0x[REDACTED] known key id: 0x[REDACTED] [key#0 state=5_GENERATED_KEYS auth=K5_AUTH_TRUE id#0 sid=66402c30 40 ms], auth=K5_AUTH_FALSE id#0 sid=00000000 00000000) [key#2 state=5_UNDEF auth=K5_AUTH_FALSE id#0 sid=00000000 00000000]
2024-01-24 20:04:53 Authenticate/Decrypt packet error: packet HMAC authentication failed
2024-01-24 20:05:28 Authenticate/Decrypt packet error: packet HMAC authentication failed
2024-01-24 20:07:12 Authenticate/Decrypt packet error: packet HMAC authentication failed
2024-01-24 20:07:45 Authenticate/Decrypt packet error: packet HMAC authentication failed
2024-01-24 20:08:40 Authenticate/Decrypt packet error: packet HMAC authentication failed
(htb-student)10.129.29.51
Permission denied, please try again.
htb-student@10.129.29.51'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 Wed Jan 24 17:00:04 UTC 2024

System load: 0.22 Processes: 155
Usage of /: 51.0% of 6.76GB Users logged in: 0
Memory usage: 2048MB IP address for ens192: 10.129.29.51
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@10.129.29.51:~$ find / -type f -name *.conf" -size +25k -size -28k -newermt 2020-03-03 2>/dev/null
htb-student@10.129.29.51:~$ find / -type f -name *.conf -user root -size +25k -size -28k -newermt 2020-03-03 2>/dev/null
-rw-r--r-- 1 root root 27422 Jun 12 2020 /usr/share/drirc.d/00-mesa-defaults.conf
htb-student@10.129.29.51:~$ find / -type f -iname *.bak 2>/dev/null | wc -l
4
htb-student@10.129.29.51:~$ which xxd
/usr/bin/xxd
htb-student@10.129.29.51:~$
```

## **How many files exist on the system that have the ".log" file extension?**

Command used: - find / -type f -iname \*.log 2>/dev/null | wc -l

**ANS:32**

```
File Edit View Bookmarks Plugins Settings Help
File New Tab Split View
- :sudo openvpn
fb5729] [key#1 state=5_UNDEF auth=K5_AUTH_FALSE id#0 sid=00000000 00000000) [key#2 state=5_UNDEF auth=K5_AUTH_FALSE id#0 sid=00000000 00000000)
2024-01-24 20:04:53 Authenticate/Decrypt packet error: packet HMAC authentication failed
2024-01-24 20:05:28 Authenticate/Decrypt packet error: packet HMAC authentication failed
2024-01-24 20:07:12 Authenticate/Decrypt packet error: packet HMAC authentication failed
2024-01-24 20:07:45 Authenticate/Decrypt packet error: packet HMAC authentication failed
2024-01-24 20:08:40 Authenticate/Decrypt packet error: packet HMAC authentication failed
2024-01-24 20:11:35 Authenticate/Decrypt packet error: packet HMAC authentication failed
2024-01-24 20:11:35 TLS Error: local/remote TLS keys are out of sync: [AF_INET]23.106.59.92:1337 (received key id: 0x[REDACTED] known key id: 0x[REDACTED] [key#1 state=5_GENERATED_KEYS auth=K5_AUTH_TRUE id#0 sid=66402c30 40 ms], auth=K5_AUTH_FALSE id#0 sid=00000000 00000000) [key#2 state=5_UNDEF auth=K5_AUTH_FALSE id#0 sid=00000000 00000000)
(htb-student)10.129.29.51
System information as of Wed Sep 23 22:09:41 2020 From 10.10.14.6
htb-student@10.129.29.51:~$ find / -type f -name *.conf" -size +25k -size -28k -newermt 2020-03-03 2>/dev/null
htb-student@10.129.29.51:~$ find / -type f -name *.conf -user root -size +25k -size -28k -newermt 2020-03-03 2>/dev/null
-rw-r--r-- 1 root root 27422 Jun 12 2020 /usr/share/drirc.d/00-mesa-defaults.conf
htb-student@10.129.29.51:~$ find / -type f -iname *.bak 2>/dev/null | wc -l
4
htb-student@10.129.29.51:~$ which xxd
/usr/bin/xxd
htb-student@10.129.29.51:~$ apt list - installed | grep -c "installed"
0
htb-student@10.129.29.51:~$ find / -type f -iname *.log 2>/dev/null | wc -l
32
htb-student@10.129.29.51:~$
```

**Took A break.**

**Lets Continue**

## How many total packages are installed on the target system?

Command used:- `apt list -- installed | grep -c installed`. This command will list all the installed packages in the target system.

**ANS:737**

```
+1 0 How many files exist on the system that have the ".log" file extension? 32
+0 0 How many total packages are installed on the target system? 737
+0 0
htb-student@nixfund:~$ apt list -- installed | grep -c installed
737
htb-student@nixfund:~$
```

## Filter Contents.

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

First I looked up at my target IPv4 address which came up as 127.0.0.1 therefore having this we can listen to all services on the target system.

Command used: `netstat -tlpn | grep -v tcp6 | grep -v "127.0.0." | grep -c LISTEN`

**ANS: 7**

```
+0 0 How many services are listening on the target system on all interfaces? (Not on localhost and IPv4 only) 7
+0 0 Determine what user the ProFTPD server is running under. Submit the username as the answer.
Submit your answer here...
+0 0
htb-student@nixfund:~$ netstat -tlpn | grep -v tcp6 | grep -v "127.0.0." | grep -c LISTEN
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
7
htb-student@nixfund:~$
```

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

Command used:- `ps aux | grep proftpd`

- ps aux: Lists information about currently running processes. The aux options provide a detailed listing of all processes owned by any user.

- |: Pipes the output of the ps aux command (the list of all processes) to the next command.

- grep proftpd: will search for lines in the output that contain the string "proftpd".

grep is a command-line utility for searching plain-text data using regular expressions.

**ANS: proftpd**

The screenshot shows a terminal window titled 'Konsole' with several tabs open. The current tab displays a command-line session where the user runs 'ifconfig' and 'netstat -ltn' to find listening ports. The output shows port 21 is listening on 0.0.0.0. The user then runs 'ps aux | grep proftpd' and highlights the resulting line: 'proftpd 1738 0.0 0.1 126440 3668 ? Ss 20:03 0:00 proftpd: (accepting connections)'. This line is highlighted with a red box. The terminal also shows a curl command being run against a domain, and a note at the bottom asking to submit the number of unique paths found.

## 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.

For this I'll use my host machine as instructed.

Command used:- `curl https://www.inlanefreight.com/ | grep -Po "https://www.inlanefreight.com/[^\/*]*" | sort -u | wc -l`

- curl command: Retrieves the HTML content of the specified website.

- grep -Po: Searches for lines in the HTML content that match the specified regular expression. This regular expression is designed to extract URLs that start with "<https://www.inlanefreight.com/>" and may contain characters other than single quotes or asterisks. The -P option enables Perl-compatible regular expressions, and the -o option only outputs the matched part of the line.

- sort -u: Sorts the extracted URLs in lexicographical order (sort) and removes duplicate URLs (-u option).

-wc -l: Counts the number of lines in the output, which corresponds to the number of unique URLs found.

**ANS: 34**

```

File Edit View Bookmarks
New Tab Split View
Flameshot Help
Hello, I'm here! Click icon in the tray to take a screenshot or click with a right button to see more options.
2024-01-25 08:50:20 Data Channel: using negotiated cipher 'AES-256-CBC'
2024-01-25 08:50:20 Outgoing Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
2024-01-25 08:50:20 Incoming Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
2024-01-25 08:50:20 Incoming Data Channel: Using 256 bit message hash 'SHA256' for HMAC authentication
2024-01-25 08:50:20 Initialization Sequence Completed
hb_academy:zsh
[+0] 0 [+] How many services are listening on the target system on all interfaces? (Not on localhost and IPv4 only)
7
[+0] 0 [+] Determine what user the ProFTPD server is running under. Submit the username as the answer.
proftpd
[+1] 0 [+] Use curl from your Pwnbox (not the target machine) to obtain the source code of the "https://www.inlanefreight.com/" and filter all unique paths of that domain. Submit the number of these paths as the answer.
34
[+0] 0 [+] Answer the question(s) below to complete this Section and earn cubes!
Mark Complete & Next

```

## User Management

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

**ANS: -m**

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

**ANS: --lock**

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

**ANS: --command**

```

File Edit View Bookmarks
New Tab Split View
Answer the question(s) below to complete this Section and earn cubes!
[+0] 0 [+] Which option needs to be set to create a home directory for a new user using "useradd" command?
-m
Submit
[+0] 0 [+] Which option needs to be set to lock a user account using the "usermod" command? (long version of the option)
--lock
Submit
[+0] 0 [+] Which option needs to be set to execute a command as a different user using the "su" command? (long version of the option)
--command
Submit
[+0] 0 [+] Answer the question(s) below to complete this Section and earn cubes!
Mark Complete & Next
Powered by HACKTHEBOX

```

## Service and Process Management

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.

Command Used:- systemctl list-units --type=service | grep Load AppArmor

- `systemctl list-units --type=service`: Lists all active systemd units of type "service" along with their current status and some additional information.
- `grep Load AppArmor`: Searches for lines in the output that contain both the words "Load" and "AppArmor". This would filter the results to only show lines related to services with "AppArmor" in their load information.

### ANS: snapd.apparmor.service

```

(htb-student) 10.129.2.219 — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
--:sudo openvpn
2024-01-25 08:50:20 Data Channel: using negotiated cipher 'AES-256-CBC'
2024-01-25 08:50:20 Outgoing Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
2024-01-25 08:50:20 Outgoing Data Channel: Using 256 bit message hash 'SHA256' for HMAC authentication
2024-01-25 08:50:20 Incoming Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
2024-01-25 08:50:20 Incoming Data Channel: Using 256 bit message hash 'SHA256' for HMAC authentication
2024-01-25 08:50:20 Initialization Sequence Completed
[...]
(htb-student) 10.129.2.219
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/adantage
System information as of Thu Jan 25 06:26:28 UTC 2024
System load: 0.51 Processes: 156
Usage of /: 51.0% of 6.76GB Users logged in: 0
Memory usage: 23% IP address for ens192: 10.129.2.219
Swap usage: 0%
[...]
* Canonical Livepatch is available for installation.
  Read https://patchwork.ubuntu.com 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@htbfund:~$ systemctl list-units --type=service | grep "Load AppArmor"
[...]
Warning: Journal has been rotated since unit was started. Log output is incomplete or unavailable.
grep: AppArmor*: No such file or directory
htb-student@htbfund:~$ systemctl list-units --type=service | grep "Load AppArmor profiles managed internally"
[...]
snapd.apparmor.service
[...]
(htb-student@htbfund:~$)

```

## Task Scheduling

### What is the type of the service of the "syslog.service"?

Command used:- `systemctl show syslog.service`

This command will display detailed information about the `syslog.service` unit, including its configuration settings and current status. This information also includes the type of service running. In this case Type=notify.

### ANS: notify

```

(htb-student) 10.129.2.219 — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
--:systemctl show syslog.service
[...]
Type=notify
[...]
(htb-student) 10.129.2.219

```

## Working with Web Services

**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).**

Here is the command to run http-server -p 8080

"-p" (specifying port 8080) **ANS: http-server -p 8080**

The screenshot shows a Kali Linux desktop environment. In the top-left corner, there is a browser window titled "Hack The Box - Academy" displaying the URL "https://academy.hackthebox.com/module/18/section/74". The page content is a challenge section for "Questions". It asks for a way to start an HTTP server using npm and provides a command input field with "http-server -p 8080". In the bottom-right corner, there is a terminal window titled "hb\_academy:node — Konsole". The terminal shows the output of the command "sudo openvpn" followed by the execution of "http-server -p 8080". The output indicates that the server is running on port 8080 with three available URLs: "http://127.0.0.1:8080", "http://10.0.2.15:8080", and "http://10.0.15.112:8080". A red box highlights the terminal output.

```
- sudo openvpn
2024-01-25 10:40:23 VERIFY KU OK
2024-01-25 10:40:23 Validating certificate extended key usage
2024-01-25 10:40:23 Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2024-01-25 10:40:23 VERIFY EKU OK
2024-01-25 10:40:23 VERIFY OK: depth=0, C=UK, ST=City, L=London, O=HackTheBox, CN=htb, name=htb, email=htb_email@hackthebox.eu
2024-01-25 10:40:23 Peer certificate initialized with 256 bit key
2024-01-25 10:40:23 Using 256 bit message hash 'SHA256' for HMAC authentication
2024-01-25 10:40:23 Control Channel: TLSv1.3, cipher 'AES-256-GCM' initialized with 256 bit key
2024-01-25 10:40:23 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
2024-01-25 10:40:23 Incoming Data Channel: Using 256 bit message hash 'SHA256' for HMAC authentication
2024-01-25 10:40:23 Control Channel: TLSv1.3, cipher 'AES-256-GCM' initialized with 256 bit key
2024-01-25 10:40:23 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
2024-01-25 10:40:23 Incoming Data Channel: Using 256 bit message hash 'SHA256' for HMAC authentication
hb_academy:node
[htb_email@htb ~]$ http-server -p 8080
Starting up http-server, serving ...
http-server version: 14.1.1
http-server settings:
  CORS: disabled
  Cache: 3600 seconds
  Connection Timeout: 120 seconds
  Directories Listings: visible
  Autoreload: false
  Serve GZIP Files: false
  Serve Brotli Files: false
  Default File Extension: none
Available on:
  http://127.0.0.1:8080
  http://10.0.2.15:8080
  http://10.0.15.112:8080
Hit Ctrl-C to stop the server
[htb_email@htb ~]$
```

**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.**

Command used:- php -S 127.0.0.1:8080

**ANS: php -S 127.0.0.1:8080**

The screenshot shows a Kali Linux desktop environment. In the top-left corner, there is a browser window titled "Hack The Box - Academy" displaying the URL "https://academy.hackthebox.com/module/18/section/74". The page content is a challenge section for "Questions". It asks for a way to start an HTTP server using php and provides a command input field with "php -S 127.0.0.1:8080". In the bottom-right corner, there is a terminal window titled "hb\_academy:zsh". The terminal shows the execution of "php -S 127.0.0.1:8080". The output indicates that the server is running on port 8080 with the URL "http://127.0.0.1:8080". A red box highlights the terminal output.

```
python3-m http.server
(htb-student)10.129.2.219
php -S 127.0.0.1:8080
php 7.2-24~Ubuntu18.04.1+deb10u1 httpd/2.2.24-1ubuntu1.15.10.0.1:8080
Listening on /var/www/htb-student
Document root is '/home/htb-student'
Press Ctrl-C to quit.
[htb-student@htb ~]$ php -S 127.0.0.1:8080
(htb-student)10.129.2.219
php 7.2-24~Ubuntu18.04.1+deb10u1 httpd/2.2.24-1ubuntu1.15.10.0.1:8080
Listening on /var/www/htb-student
Document root is '/home/htb-student'
Press Ctrl-C to quit.
[htb_stu@htb ~]$ http://127.0.0.1:8080
[htb_stu@htb ~]$
```

## File System Management

### How many partitions exist in our Pwnbox? (Format: 0)

lsblk command provides information like:

NAME: The name of the block device.

MAJ:MIN: The major and minor device numbers.

RM: Whether the device is removable or not (1 for removable, 0 for non-removable).

SIZE: The size of the block device.

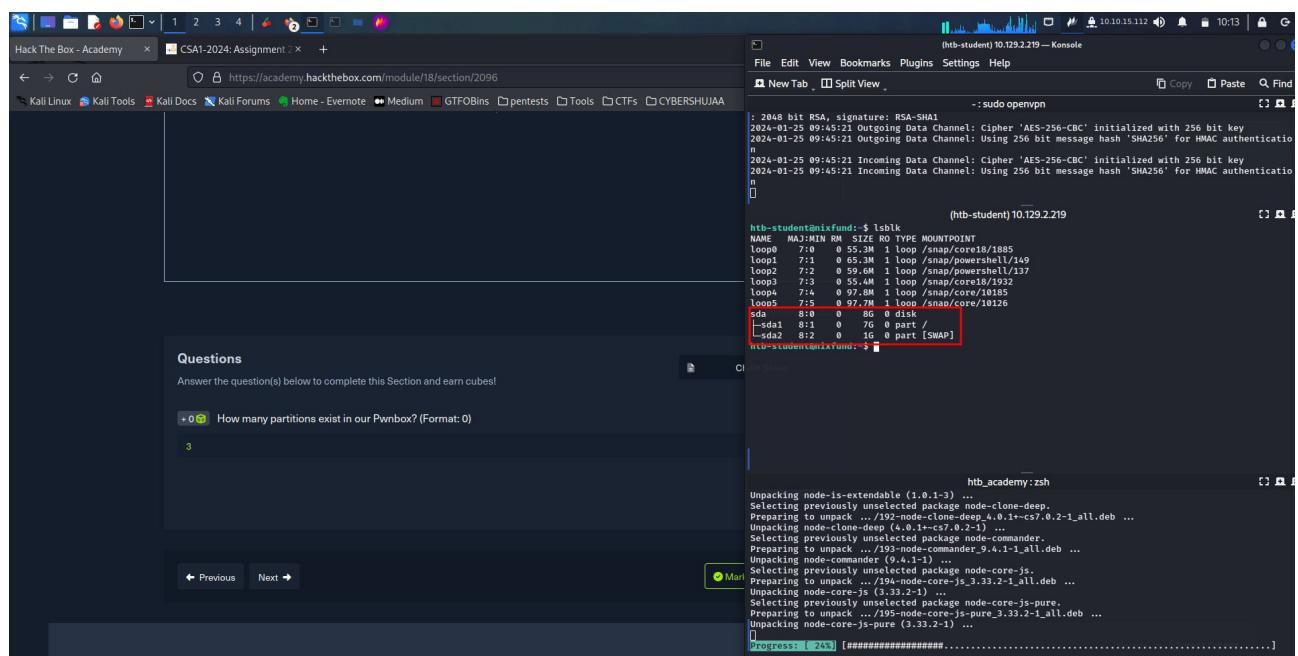
RO: Whether the device is read-only or read-write.

TYPE: The type of the block device (disk, partition, etc.).

MOUNTPOINT: The mount point of the device if it is mounted.

Therefore with this command we shall also get the number of partitions with the format of “0”

### ANS: 3



```
(htb-student)10.129.2.219 - Konsole
File Edit View Bookmarks Plugins Settings Help
Copy Paste Find
~: sudo openvpn
(htb-student)10.129.2.219
File Edit View Bookmarks Plugins Settings Help
Copy Paste Find
htb-student@mixfund:~$ lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
loop0 7:0 0 3.3M 1 loop /snap/cor10/1085
loop1 7:1 0 65.3M 1 loop /snap/powershell/149
loop2 7:2 0 59.6M 1 loop /snap/powershell/137
loop3 7:3 0 55.4M 1 loop /snap/core18/1932
loop4 7:4 0 97.8M 1 loop /snap/core/10185
loop5 7:5 0 97.8M 1 loop /snap/core/10186
sda 8:0 0 8G 0 disk
└─sda1 8:1 0 7G 0 part /
  └─sda2 8:2 0 1G 0 part [SWAP]
htb-student@mixfund:~$ █
```

Questions

Answer the question(s) below to complete this Section and earn cubes!

+ 0 0 How many partitions exist in our Pwnbox? (Format: 0)

3

◀ Previous Next ▶

Unpacking node-is-extensible (1.0.1-3) ...
Selecting previously unselected package node-clone-deep.
Preparing to unpack .../node-clone-deep\_1.0.1-3\_all.deb ...
Unpacking node-clone-deep (1.0.1-3) ...
Selecting previously unselected package node-commander.
Preparing to unpack .../node-commander\_9.4.1-1\_all.deb ...
Unpacking node-commander (9.4.1-1) ...
Selecting previously unselected package node-core-js.
Preparing to unpack .../node-core-js\_3.33.2-1\_all.deb ...
Unpacking node-core-js (3.33.2-1) ...
Selecting previously unselected package node-core-js-pure.
Preparing to unpack .../node-core-js-pure\_3.33.2-1\_all.deb ...
Unpacking node-core-js-pure (3.33.2-1) ...
Progress: [ 24%] [#####.....]

## Conclusion.

I have really enjoyed the course module, I have been able to lean on different ways to navigate through the directories and easier search of specific files using their extensions, name and size as well. I have also learnt on how to add users and remove users, grouping of users in Linux environments using the terminal and also to give permissions to who can read, write or execute a file.

In conclusion this module has opened up my eyes on new ways of approach on the Linux environment.

**Thank you.**