TASK 7 LINUX GAMES

OVERTHEWIRE -BANDIT

BANDIT LV 0:

PASS: bandit0

The goal of this level is for you to log into the game using SSH. The host to which you need to connect is **bandit.labs.overthewire.org**, on port 2220. The username is **bandit0** and the password is **bandit0**. Once logged in, go to the Level 1 page to find out how to beat Level 1.

BANDIT LV 0-1:

PASS: boJ9jbbUNNfktd78OOpsqOltutMc3MY1

```
bandit0@bandit:~$ cat readme
boJ9jbbUNNfktd78OOpsqOltutMc3MY1
```

BANDIT LV 1-2:

PASS: CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9

```
bandit1@bandit:~$ cat ./"-"
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
```

BANDIT LV 2-3:

PASS: UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK

```
bandit2@bandit:~$ cat ./"spaces in this filename"
UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK
bandit2@bandit:~$
```

BANDIT LV 3-4:

PASS: pIwrPrtPN36QITSp3EQaw936yaFoFgAB

```
bandit3@bandit:~/inhere$ ls -a
.   ..   .hidden
bandit3@bandit:~/inhere$ cat .hidden
pIwrPrtPN36QITSp3EQaw936yaFoFgAB
```

BANDIT LV 4-5:

PASS: koReBOKuIDDepwhWk7jZC0RTdopnAYKh

```
bandit4@bandit:~/inhere$ cat ./-file07
koReBOKuIDDepwhWk7jZC0RTdopnAYKh
```

BANDIT LV 5-6:

PASS: DXjZPULLxYr17uwoI01bNLQbtFemEgo7

```
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7
```

BANDIT LV 6-7:

PASS: HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs

```
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs
```

BANDIT LV 7-8:

PASS: cvX2JJa4CFALtqS87jk27qwqGhBM9plV

```
bandit7@bandit:~$ cat data.txt|grep millionth
millionth        cvX2JJa4CFALtqS87jk27qwqGhBM9plV
```

BANDIT LV 8-9:

PASS: UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR

```
bandit8@bandit:~$ sort data.txt|uniq -u
UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR
```

BANDIT LV 9-10:

PASS: truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk

```
bandit9@bandit:~$ strings data.txt | grep =
========= the*2i"4
=:G e
========= password
<I=zsGi
Z)========= is
A=|t&E
Zdb=
c^ LAh=3G
*SF=s
δ========= truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk
S=A.H&^
```

BANDIT LV 10-11:

PASS: IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR

```
bandit10@bandit:~$ cat data.txt| base64 --decode
The password is IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR
```

BANDIT LV 11-12:

PASS: 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu

```
bandit11@bandit:~$ cat data.txt| tr "A-Za-z" "N-ZA-Mn-za-m"
The password is 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu
```

BANDIT LV 12-13:

PASS: 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL

```
bandit12@bandit:/tmp/xxd$ cat f5
The password is 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
```

BANDIT LV 13-14:

Since this a secure connection we have to tell to check the pvt key so we use ssh -i sshkey.private

```
bandit13@bandit:~$ ls
sshkey.private
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/wb2bfidNpwbB8rsJ4sZIDZQ7XuIh4LfygoAQSS+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
GC83sOs3D7n5Mj8×3NdO8xFit7dT9a245TvaoYQ7KgmqpSg/ScKCw4c3eiLava+J
3btnJeSIU+8ZXq9XjPRpKwUCgYA7z6LiOQKxNeXH3qHXcnHok855maUj5fJNpPbY
iDkyZ8ySF8GlcFsky8Yw6fWCqfG3zDrohJ5l9JmEsBh7SadkwsZhvecQcS9t4vby
9/8X4jS0P8ibfcKS4nBP+dT81kkkg5Z5MohXBORA7VWx+ACohcDEkprsQ+w32xeD
qT1EvQKBgQDKm8ws2ByvSUVs9GjTilCajFqLJ0eVYzRPaY6f++Gv/UVfAPV4c+S0
kAWpXbv5tbkkzbS0eaLPTKgLzavXtQoTtKwrjpolHKIHUz6Wu+n4abfAIRFubOdN
/+aLoRQ0yBDRbdXMsZN/jvY44eM+xRLdRVyMmdPtP8belRi2E2aEzA==
-----END RSA PRIVATE KEY-----
```

After logging into lv 14 we can extract it's password..

PASS: 4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e

```
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
bandit14@bandit:~$
```

BANDIT LV 14-15:

PASS: BfMYroe26WYalil77FoDi9qh59eK5xNr

```
bandit14@bandit:~$ nc localhost 30000
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
Correct!
BfMYroe26WYalil77FoDi9qh59eK5xNr
```

BANDIT LV 15:

PASS: cluFn7wTiGryunymYOu4RcffSxQluehd

```
bandit15@bandit:~$ openssl s_client -connect localhost:30001
CONNECTED(00000003)
depth=0 CN = localhost
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = localhost
verify return:1
---
Certificate chain
 0 s:/CN=localhost
   i:/CN=localhost
```

After establishing the connection submit the current pass to get the pass foe next level..

```
BfMYroe26WYalil77FoDi9qh59eK5xNr
Correct!
cluFn7wTiGryunymYOu4RcffSxQluehd
```

-----------------------------------THANKYOU FOR GOING THROUGH MY WORK-------------------------------------

DONE BY

A.SANJAY KUMAAR