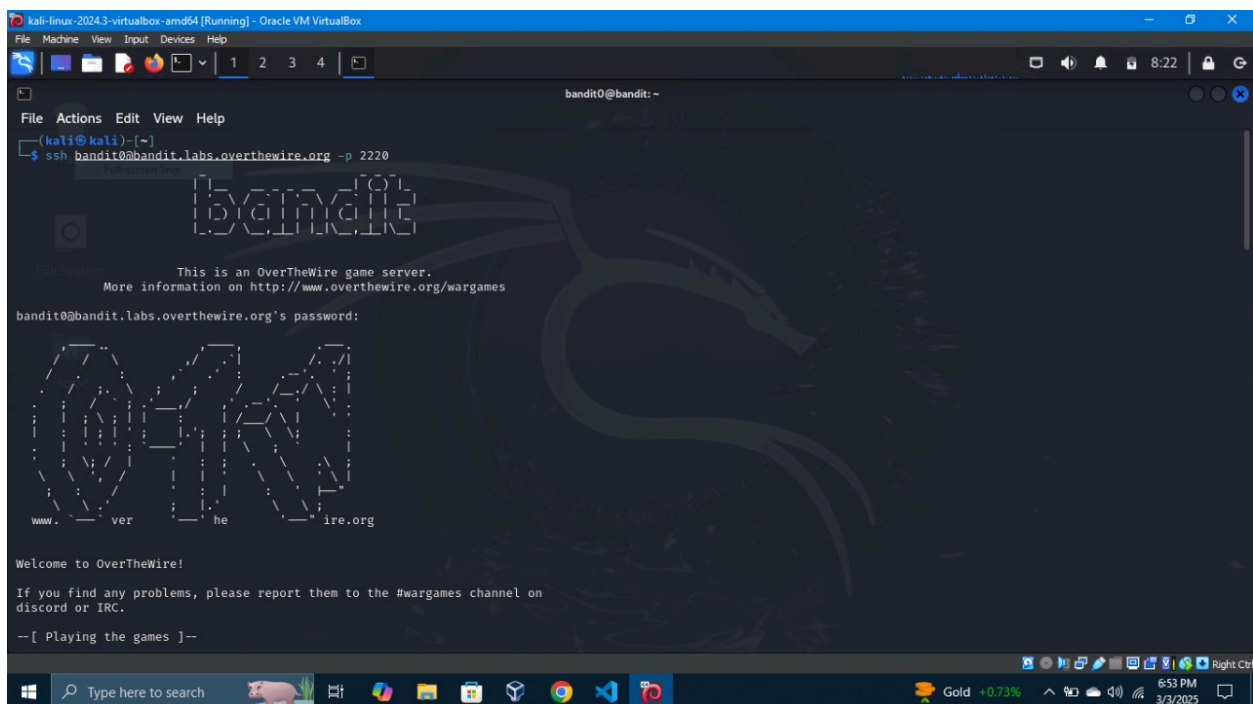


# Bandit OverTheWire Writeup:

## Level 0:

**Task :** 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.



Log into the level with ssh in server:bandit.labs.overthewire.org in the port 2220 .

**command :** `ssh bandit0@bandit.labs.overthewire.org -p 2220`

**username :** bandit0

**password :** bandit0

## Level 0 - 1:

**Task :** The password for the next level is stored in a file called **readme** located in the home directory. Use this password to log into bandit1 using SSH. Whenever

you find a password for a level, use SSH (on port 2220) to log into that level and continue the game.

```
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
Congratulations on your first steps into the bandit game!!
Please make sure you have read the rules at https://overthewire.org/rules/
If you are following a course, workshop, walkthrough or other educational activity,
please inform the instructor about the rules as well and encourage them to
contribute to the OverTheWire community so we can keep these games free!

The password you are looking for is: ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If
```

After entering the bandit0 use **ls** to view the directories.

Use **cat** to view the content of the readme file.

**command** : **ls** and **cat readme**

**password** : ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If

## Level 1 - 2:

**Task** : The password for the next level is stored in a file called **-** located in the home directory

```
bandit1@bandit:~$ ls -alps
total 24
4 -rw-r----- 1 bandit2 bandit1  33 Sep 19  2024 -
4 drwxr-xr-x  2 root    root    4096 Sep 19  2024 ./
4 drwxr-xr-x 70 root    root    4096 Sep 19  2024 ../
4 -rw-r--r--  1 root    root     220 Mar 31  2024 .bash_logout
4 -rw-r--r--  1 root    root    3771 Mar 31  2024 .bashrc
4 -rw-r--r--  1 root    root     807 Mar 31  2024 .profile
bandit1@bandit:~$ cat ./-
263JGJPfgU6LtdEvgfWU1XP5yac29mFx
bandit1@bandit:~$
```

Using the previous level passkey the current level is accessed and password for next level is in a file called **-**.

use **ls** and **cat** to get the password.

**command** : **ls -alps** and **cat ./-**

**password** : 263JGJPfgU6LtdEvgfWU1XP5yac29mFx

## Level 2 - 3:

**Task** : The password for the next level is stored in a file called **spaces in this filename** located in the home directory

```
bandit2@bandit:~$ ls -alps
total 24
4 drwxr-xr-x 2 root root 4096 Sep 19 2024 ./
4 drwxr-xr-x 70 root root 4096 Sep 19 2024 ../
4 -rw-r--r-- 1 root root 220 Mar 31 2024 .bash_logout
4 -rw-r--r-- 1 root root 3771 Mar 31 2024 .bashrc
4 -rw-r--r-- 1 root root 807 Mar 31 2024 .profile
4 -rw-r----- 1 bandit3 bandit2 33 Sep 19 2024 spaces in this filename
bandit2@bandit:~$ cat spaces\ in\ this\ filename
MNk8KNH3Usiio41PRUEoDFPqfxLPISmx
```

**command** : `cat spaces\ in\ this\ filename` \are used to show the space in the command

**password** : MNk8KNH3Usiio41PRUEoDFPqfxLPISmx

## Level 3 - 4:

**Task** : The password for the next level is stored in a hidden file in the **inhere** directory.

```
bandit3@bandit:~$ ls -alps
total 24
4 drwxr-xr-x 3 root root 4096 Sep 19 2024 ./
4 drwxr-xr-x 70 root root 4096 Sep 19 2024 ../
4 -rw-r--r-- 1 root root 220 Mar 31 2024 .bash_logout
4 -rw-r--r-- 1 root root 3771 Mar 31 2024 .bashrc
4 drwxr-xr-x 2 root root 4096 Sep 19 2024 inhere/
4 -rw-r--r-- 1 root root 807 Mar 31 2024 .profile
bandit3@bandit:~$ cd inhere/
bandit3@bandit:~/inhere$ ls -al
total 12
drwxr-xr-x 2 root root 4096 Sep 19 2024 .
drwxr-xr-x 3 root root 4096 Sep 19 2024 ..
-rw-r----- 1 bandit4 bandit3 33 Sep 19 2024 ... Hiding-From-You
bandit3@bandit:~/inhere$ cat ... Hiding-From-You
2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
bandit3@bandit:~/inhere$
```

In this level the password is hidden inside the directory inhere.

**command** : `cd` for changing directory

**password** : 2WmrDFRmJlq3lPxneAaMGhap0pFhF3NJ

## Level 4 - 5:

**Task** : The password for the next level is stored in the only human-readable file in the **inhere** directory. Tip: if your terminal is messed up, try the "reset" command.

```
bandit4@bandit:~$ ls -alps
total 24
4 drwxr-xr-x  3 root root 4096 Sep 19  2024 ./
4 drwxr-xr-x 70 root root 4096 Sep 19  2024 ../
4 -rw-r--r--  1 root root  220 Mar 31  2024 .bash_logout
4 -rw-r--r--  1 root root 3771 Mar 31  2024 .bashrc
4 drwxr-xr-x  2 root root 4096 Sep 19  2024 inhere/
4 -rw-r--r--  1 root root  807 Mar 31  2024 .profile
bandit4@bandit:~$ cd inhere/
bandit4@bandit:~/inhere$ ls
-file00 -file01 -file02 -file03 -file04 -file05 -file06 -file07 -file08 -file09
bandit4@bandit:~/inhere$ find . -type f | xargs file
./-file08: data
./-file02: data
./-file09: data
./-file01: data
./-file00: data
./-file05: data
./-file07: ASCII text
./-file03: data
./-file06: data
./-file04: data
bandit4@bandit:~/inhere$ man xarg
No manual entry for xarg
bandit4@bandit:~/inhere$ man xargs
bandit4@bandit:~/inhere$ cat ./-file07
4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw
bandit4@bandit:~/inhere$
```

In this level the directories as many files in which the password is in the human readable file. the command find is used to get the readable file in the directory.

**command** : `ls -alps`, `cd`, `find . -type f | xargs file` and `cat`

**password** : 4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw

## Level 5 - 6 :

**Task** : The password for the next level is stored in a file somewhere under the **inhere** directory and has all of the following properties:

- human-readable
- 1033 bytes in size
- not executable

```
File Actions Edit View Help
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere/
bandit5@bandit:~/inhere$ find . -type f -size 1033c ! -executable
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
```

the command `find . -type f -size 1033c ! executable` says the properties of the given directories.

**password** : HWasnPhtq9AVKe0dmk45nxy20cvUa6EG

## Level 6 - 7:

**Task** : The password for the next level is stored **somewhere on the server** and has all of the following properties:

- owned by user bandit7
- owned by group bandit6
- 33 bytes in size

```

bandit6@bandit:~$ find / -type f -user bandit7 -group bandit6 -size 33c
find: '/drifter/drifter14_src/axTLS': Permission denied
find: '/root': Permission denied
find: '/snap': Permission denied
find: '/tmp': Permission denied
find: '/proc/tty/driver': Permission denied
find: '/proc/1774579/task/1774579/fdinfo/6': No such file or directory
find: '/proc/1774579/fdinfo/5': No such file or directory
find: '/home/bandit31-git': Permission denied
find: '/home/ubuntu': Permission denied
find: '/home/bandit5/inhere': Permission denied
find: '/home/bandit30-git': Permission denied
find: '/home/drifter8/chroot': Permission denied
find: '/home/drifter6/data': Permission denied
find: '/home/bandit29-git': Permission denied
find: '/home/bandit28-git': Permission denied
find: '/home/bandit27-git': Permission denied
find: '/lost+found': Permission denied
find: '/etc/polkit-1/rules.d': Permission denied
find: '/etc/multipath': Permission denied
find: '/etc/stunnel': Permission denied
find: '/etc/xinetd.d': Permission denied
find: '/etc/credstore.encrypted': Permission denied
find: '/etc/ssl/private': Permission denied
find: '/etc/sudoers.d': Permission denied
find: '/etc/credstore': Permission denied
find: '/dev/shm': Permission denied
find: '/dev/mqueue': Permission denied
find: '/var/log/amazon': Permission denied
find: '/var/log/unattended-upgrades': Permission denied
find: '/var/log/chrony': Permission denied
find: '/var/log/private': Permission denied
find: '/var/tmp': Permission denied
find: '/var/spool/cron/crontabs': Permission denied
find: '/var/spool/bandit24': Permission denied
find: '/var/spool/rsyslog': Permission denied
find: '/var/cache/ldconfig': Permission denied
find: '/var/cache/apt/archives/partial': Permission denied
find: '/var/cache/pollinate': Permission denied
find: '/var/cache/private': Permission denied
find: '/var/cache/apparmor/2425d902.0': Permission denied
find: '/var/cache/apparmor/baad73a1.0': Permission denied
find: '/var/lib/polkit-1': Permission denied
find: '/var/lib/amazon': Permission denied
find: '/var/lib/dpkg/info/bandit7.password'
find: '/var/lib/apt/lists/partial': Permission denied
find: '/var/lib/chrony': Permission denied
find: '/var/lib/snapd/void': Permission denied
find: '/var/lib/snapd/cookie': Permission denied

```

```

find: '/run/user/11015': Permission denied
find: '/run/user/11003': Permission denied
find: '/run/user/11014': Permission denied
find: '/run/user/11009': Permission denied
find: '/run/user/11010': Permission denied
find: '/run/user/11019': Permission denied
find: '/run/user/11022': Permission denied
find: '/run/user/11002': Permission denied
find: '/run/user/11017': Permission denied
find: '/run/user/8002': Permission denied
find: '/run/user/11032': Permission denied
find: '/run/chrony': Permission denied
find: '/run/udisks2': Permission denied
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
morbNTDKSW6jIlUc0ymOdMaLnOlFVAaj
bandit6@bandit:~$ █

```

The password is stored somewhere in the server so the command `find / -type f -user bandit7 -group bandit6 -size 33c` is used to get the packets.

**command** : `find / -type f -user bandit7 -group bandit6 -size 33c`

**password** : morbNTDkSW6jIIUc0ymOdMaLnOIFVAaj

## Level 7 - 8 :

**Task** : The password for the next level is stored in the file **data.txt** next to the word **millionth**



```
bandit7@bandit:~$ ls -alps
total 4108
 4 drwxr-xr-x  2 root    root      4096 Sep 19  2024 ./
 4 drwxr-xr-x 70 root    root      4096 Sep 19  2024 ../
 4 -rw-r--r--  1 root    root       220 Mar 31  2024 .bash_logout
 4 -rw-r--r--  1 root    root     3771 Mar 31  2024 .bashrc
4088 -rw-r----- 1 bandit8 bandit7 4184396 Sep 19  2024 data.txt
 4 -rw-r--r--  1 root    root       807 Mar 31  2024 .profile
bandit7@bandit:~$ cat data.txt
momentary      MBLQ2x4SPU4Y6XIscWooXopjdSntWOhY
vicuña        6nKKKgZhbJvPFsEFQgzd2wqJWcv8TGGQ
equities       ZhOy86fNIP8sWs0LLYiHrtjRsrpu1bND
various        Eg1ZcmYmpvkXS10Vu04areb2hhT9Pkft
redefinition's vPzYXGDGwByIVBRIKQDRHn5xqoekZKME
Allison        4JPUMGRznD4JAyy1SX2Cf5zAwEhT7AP7
compels        8XgWaEyaUVmm1FLZksXE6vRBAKfm7xGB
misstep        0p0wfzDrUfyAbU6V5MVGLrvDKjmc6a0Z
coagulating    Ff0C46bf0Mzw0ojIDTWJAq9059WdKSdw
Onega's        YiR7TkXXHKpt00qs2EtFzRSXu8XGcQA
checkmate      XjaNSCEGpEdkJIMfCnwWGJURQ6fUIoUq
Lyndon         7m6zWzaFwemeBJ7jKzX01REfc9QtC9SQ
archivist      j1kdDmGHBGtcor81a2lIZzVd9ulFtifz
Jerri's        2fCe8FdpTJFt4gtanwmG7a8A1AYlEpDQ
underarms      ZSucs304S5mq2TONuDqpN5gwz7HsbCOQ
scrooge        SYI06iTGl1SdxwJV21kH4fty0AAer8Rv
Elnora         i1GGmWJChr5PUq8N8s9nt6nhYvoUtoRu
salver         uZf07mMWSaF4hLwFmGKIkt0qrSeTIPjy
hemorrhaged    rgsV70D3SHSx60IfJTpI4p60BApa0sEI
fount's        U4XHsnP97BgOI3v027KBrpwtMvR9qF1I
autograph's    00gaDupjr2Rbwo0A98oN4jzLYq2Q1Rwc
tranquillizes  5ncuXd3UAIy3S0QRnVS8s3Sp7iEb0hrX
edgiest        OJtPY7WKKVMFSkTHwYTUnWoZzRIQ76Ii
miles          C8GP1U4YQzLz6wdWbKsWBexSS361WShV
inconvenience's kJM03FuxWnwIyXyOQ3CgUjMM4RKpnyGc
hurled         fYt4KTYNxBpjsagDMXaggeaF1lj5TP1
strollers      Gf1nIa0aLC8w7MfeHQbFSRbmBdvK6MLk
Lincoln's      HoRRZZXAet2v03wM51A4sfCukDLHLMy
showerier      Qi4hcuzmFLfi79r0r1WqtE99n0CxiH5c
Head           ZoXDgeBUXPiKQIquLtWwqM1ZI8jzdkzF
Mormonism's    mQGJw2ifm0p6Y6jPBptLr679JY3gz0Mc
riming         fUq82Zhw36YYujQ0RhvzvXWEBH1E7ffM
eviscerating    55uIcX0b4z4JJ8n0rVsqIm2GUF4Swhom
fluoride's     GULiK1R5hxj9ZSCA3xhWGNCFsac7j44d
threnodies     2HEh1JzLBinyNbno1gW4UUp5SbQMTm4V
insecticide     V0gn5D80tLV3ksiTke5eM64RTPp0SE9W
muscat         1RuOF1vdEX0BrGNZqlrDsicRhcot0BnN
shortsightedly NKLJBXieAA8pcGwct19rAh91EAIIs2qcT
screen         HHW3ECeI3LTZE9qsIHVbQiW3YzBUaUxc
Adenauer      6nkup8SIXcOvtEToTgtqVf7srh9mxYCo
hedonists      iF2vetNKv6QIoFaMZZH99sWH30PMrtEF
insured        bKsaAcccEj9l35At2jqdbl5uFfS9w3js
```



```

pitgrills      CZX1qzyHMKFJPN5SugIKtyZdWNK63baq
endings        y1vEDG0S0mWfEa6mbo6Jh3fD8xXfgE11
initially      M9oo1rVmdR2HU1TLRtBzN85KvajmQgHc
centaurs       tmt78QAefsbdtQ0REnxxRUJUqsSqZTPj
abjure        Z1W4oog9188Qd8df3HW2reNri2aMxo26
renal          80cKdVMuGVVmIC6IZH39bx3rpDSkCbWv
sans          IzDQf2WJGG7nPugHbVIQKCbEPQwZIA3s
meting         mFY3wNpY9FvSVGZ1mgi5N8U83US5Ywzu
Franck        cErFvuq2Qsm1qvRoE9JIb3eP95XTD94b
reader's      uc94SAup0ckmTILYobI8t6LK4FXiopA0
tundra's      AMPxMOHtyyQyOSQ0eG819far1kJXkDAB
terminus      PTC11CY5EAoUu9vhU8Q3Rhvm55qvLLjH
subtotal      7a709N9ZIIYSETwdEGBR2mFSKMfKrxBTX
wrongfulness  mMDI21VOMyZxkV2R7b61ERqPIyBVslsV
whitens       0ryQZCxD3dXX60E9xMeDIgjeY0B2ivxj
treading       vmeULGaYMd69JwbAdEJtL2UiXZfgQ0JN
reimpose      XJubELpBFTp0wx0qybxfByHoKm1tE5C
battalions    hf3EPFD5eVFRedNnHLciwLH60iClh4rW
Soho's        uW70GRbkWX3CkzZjrU5KmIOdnd3paxTG
Mondays       TEzFxcQ7IC1VdsvqGs5fX4kwR22GwVnf
unsuccessfully 1aVW4qvBdy39Wkk15vyAZZV89qVkNSuW
Odessa        cMnmUf3hUk3zKizQQ9MygtjE0KBauwwN
jacket        sS3sDdschJbJfSN1d36VJLppXoYE3mW5
seeping       hhrdfoZgoMQmINOrmmZLL5t8sVhDGDWZ
renounces     H5pjlsprVRLLDbiSKtxAIG6NSBCKmzq2
impoverishment hwijIqvXQqbMMdW7Va80qMEZmcXXZL8i
bandit7@bandit:~$ strings data.txt | grep "millionth"
millionth     dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
bandit7@bandit:~$

```

the data.txt file has many strings which are difficult to find . so, the command `strings text_file | grep "word"` is given to get the password.

**command :** `strings data.txt | grep "millionth"`

**password :** `dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc`

## Level 8 - 9:

**Task :** The password for the next level is stored in the file **data.txt** and is the only line of text that occurs only once

```
bandit8@bandit:~$ cat data.txt
aMKlTMrptUxxTypCHocCTrqYRkR2gT8h
PRerp5EfTVxJHKuCZDXfAfRyCQSDpJMi
0BKVRLEJQcpNx8wnSPxDLfnFKlQafKK6
6Boy6esAjnIXCYN8uI6KZ7VD7zysDM8i
tgHSfEXcbYCeJWXfsWD04VXXbqtTVcqS
KZJOZECxhLxDhxDbGzdNy8m0uplZvP11
w6x5XtaoRWDqMCsYxgZIWuOKVdiGByAu
0kJ7XHD4gVtNSZIpqyP1V45sfz90BLFo
Wr4hWlUhGCKJpGDCEio8C1pLVt7DZm3X
Su9w1lri9UACf53cL1evAMKXVgI0nfqe
6Boy6esAjnIXCYN8uI6KZ7VD7zysDM8i
CgUjZiluCoMEvzNAge1Nbv3g9tpLQQj2
ysKmfYcysVfnViisRBcXzgjjXMDgnKKv
1VKPEkd0bCtIRwMFVQfY7Inulw0FyDsn
v1h4YD5vP5iFAwV6iF00PwTTLu5iS7lwC70
```

`cat` is used to view the `data.txt` file which is the only file.

```
bandit8@bandit:~$ sort data.txt
0BKVRLEJQcpNx8wnSPxDLfnFKlQafKK6
0BKVRLEJQcpNx8wnSPxDLfnFKlQafKK6
0BKVRLEJQcpNx8wnSPxDLfnFKlQafKK6
0BKVRLEJQcpNx8wnSPxDLfnFKlQafKK6
0BKVRLEJQcpNx8wnSPxDLfnFKlQafKK6
0BKVRLEJQcpNx8wnSPxDLfnFKlQafKK6
0BKVRLEJQcpNx8wnSPxDLfnFKlQafKK6
0BKVRLEJQcpNx8wnSPxDLfnFKlQafKK6
0BKVRLEJQcpNx8wnSPxDLfnFKlQafKK6
0BKVRLEJQcpNx8wnSPxDLfnFKlQafKK6
0eJPctF8gK96ykGBBaKydhJgxSpTlJtz
0eJPctF8gK96ykGBBaKydhJgxSpTlJtz
0eJPctF8gK96ykGBBaKydhJgxSpTlJtz
0eJPctF8gK96ykGBBaKydhJgxSpTlJtz
0eJPctF8gK96ykGBBaKydhJgxSpTlJtz
```

`sort` is used to arrange the strings in order to find the number of times the strings are repeated.

```
bandit8@bandit:~$ sort data.txt | uniq -c
10 0BKVRLEJQcpNx8wnSPxDLfnFKlQafKK6
10 0eJPctF8gK96ykGBBaKydhJgxSpTLJtz
10 0kJ7XHD4gVtNSZIpqyP1V45sfz90BLFo
10 0lP0vKhPHZebxji0gdjtGCd5GWiZnNBj
10 0REUhKk0yMqQ0wei6NK9ZqIpE5dVlWWM
10 1jfUH1m4XCjr7eWAeLeGdaNSxFXRtX0l
10 1VKPEkd0bCtIRwMFVQfY7Inulw0FyDsn
10 2u8fvAzvnaFlvQG3iPt4Wc1TFhPcGxhH
10 35l6mr3f6TvlJyDwU6aUgJX07cLhr6t9
10 3FIgajXBiaQAiTMVGo1gxRDSiACNyvvJ
10 3mNA2le0gfURQKNHVIhGkMNLqLwjyyLN
1 4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
10 4P8FsHcdr7d5WKnPtAaXY5SslKICd2gL
10 5EmwMKZHwF6Lwq5jHuaDlfFJBcHbcX0b
10 5hYz0028e1Q2TrtPVz5GZbpMzZNjebhh
10 5I2jWpqjtVp576xXI2TLh1UCyXJtGQ78
10 6Boy6esAjnIxCYn8uI6KZ7VD7zysDM8i
10 7cP8ssLElERHXq0Jc9T84bxsmJBjNXk2
10 7qHmEo1FEbzthgyNpKc38YofXjYKZv18
10 8FcUQLFXsJnNeyiDY5KfE3vRy6sZFEJ
10 8pePxs1MzXqA2mi87wFixd44qDBdrPiW
```

`uniq -c` is used to get the count of the unique strings present in the data.txt.

**command :** `sort data.txt | uniq -c`

**password :** 4CKMh1JI91bUIZZPXDqGanal4xvAg0JM

## Level 9 - 10 :

**Task :** The password for the next level is stored in the file **data.txt** in one of the few human-readable strings, preceded by several '=' characters.

```
bandit9@bandit:~$ strings data.txt | grep "="
}===== the
p\l=
;c<Q=.dEXU!
3JprD===== passwordi
qC(=
~fDV3===== is
7=oc
zP= le System
~de=
3k=fQ
~o=0
69}=
%=Y
=tZ~07
D9===== FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey
N=~[!N
zA=?0j
bandit9@bandit:~$
```

`strings data.txt` gives the whole strings content of the file but the `| grep "="` gives the strings which has the characters.

command : `strings data.txt | grep "="`

password : FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey

## Level 10 - 11 :

**Task :** The password for the next level is stored in the file **data.txt**, which contains base64 encoded data

```
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIGR0UjE3M2ZaS2IwUlJzREZTR3NnMlJXbnBOVm9kZmVjYyCg==
bandit10@bandit:~$ base64 -d data.txt
The password is dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr
bandit10@bandit:~$
```

the encoded data was in the data.txt file . We can also use other sources like cyberchief and base64 platform instead of `base64 -d` in linux.

command : `base64 -d data.txt`

**Tool :** base64

**password** : dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr

## Level 11 - 12 :

**Task** : The password for the next level is stored in the file **data.txt**, where all lowercase (a-z) and uppercase (A-Z) letters have been rotated by 13 positions

```
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf 7k16JArUVv5LxVuJfsSVdbbtaHGlw9D4
```

**rot13.com**

[About ROT13](#)

Gur cnffjbeq vf 7k16JArUVv5LxVuJfsSVdbbtaHGlw9D4



ROT13 ▼



The password is 7x16WNeHli5YklhWsfFIqoognUTyj9Q4

rot 13 is a tool used to decode the data. It is a online tool, the alternate for rot13 is cyberchief which is also a online platform.

**Tool** : rot13

**password** : 7x16WNeHli5YklhWsfFIqoognUTyj9Q4

## Level 12 - 13 :

**Task :** The password for the next level is stored in the file **data.txt**, which is a hexdump of a file that has been repeatedly compressed. For this level it may be useful to create a directory under /tmp in which you can work. Use mkdir with a hard to guess directory name. Or better, use the command "mktemp -d". Then copy the datafile using cp, and rename it using mv (read the manpages!)

```
bandit12@bandit:~$ mkdir /tmp/kalis
bandit12@bandit:~$ cp data.txt /tmp/kalis
bandit12@bandit:~$ cd /tmp/kalis
bandit12@bandit:/tmp/kalis$ ls
data.txt
bandit12@bandit:/tmp/kalis$ xxd -r data.txt > data
bandit12@bandit:/tmp/kalis$ ls
data  data.txt
bandit12@bandit:/tmp/kalis$ file data
data: gzip compressed data, was "data2.bin", last modified: Thu Sep 19 07:08:15 2024, max compression, from Unix, original size modulo 2^32 574
bandit12@bandit:/tmp/kalis$ mv data file.gz
bandit12@bandit:/tmp/kalis$ gzip -d file.gz
bandit12@bandit:/tmp/kalis$ ls
data.txt  file
bandit12@bandit:/tmp/kalis$ file file
file: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/kalis$ mv file file.bz2
bandit12@bandit:/tmp/kalis$ bzip2 -d file.bz2
bandit12@bandit:/tmp/kalis$ ls
data.txt  file
bandit12@bandit:/tmp/kalis$ file file
file: gzip compressed data, was "data4.bin", last modified: Thu Sep 19 07:08:15 2024, max compression, from Unix, original size modulo 2^32 20480
bandit12@bandit:/tmp/kalis$ mv file file.gz
bandit12@bandit:/tmp/kalis$ gzip -d file.gz
bandit12@bandit:/tmp/kalis$ ls
data.txt  file
bandit12@bandit:/tmp/kalis$ file file
file: POSIX tar archive (GNU)
bandit12@bandit:/tmp/kalis$ mv file file.tar
bandit12@bandit:/tmp/kalis$ tar xf file.tar
bandit12@bandit:/tmp/kalis$ ls
data5.bin  data.txt  file.tar
bandit12@bandit:/tmp/kalis$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/kalis$ rm file.tar
bandit12@bandit:/tmp/kalis$ rm data
rm: cannot remove 'data': No such file or directory
bandit12@bandit:/tmp/kalis$ rm data.txt
bandit12@bandit:/tmp/kalis$ ls
data5.bin
bandit12@bandit:/tmp/kalis$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/kalis$ mv data5.bin data.tar
bandit12@bandit:/tmp/kalis$ tar xf data.tar
bandit12@bandit:/tmp/kalis$ ls
data6.bin  data.tar
bandit12@bandit:/tmp/kalis$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
```

```

bandit12@bandit:/tmp/kalis$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/kalis$ mv data6.bin data.bz
bandit12@bandit:/tmp/kalis$ bzip2 -d data.bz2
bzip2: Can't open input file data.bz2: No such file or directory.
bandit12@bandit:/tmp/kalis$ mv data6.bin databz2
mv: cannot stat 'data6.bin': No such file or directory
bandit12@bandit:/tmp/kalis$ bzip2 -d data.bz
bandit12@bandit:/tmp/kalis$ ls
data  data.tar
bandit12@bandit:/tmp/kalis$ file file
file: cannot open `file' (No such file or directory)
bandit12@bandit:/tmp/kalis$ file data
data: POSIX tar archive (GNU)
bandit12@bandit:/tmp/kalis$ mv data data.tar
bandit12@bandit:/tmp/kalis$ ls
data.tar
bandit12@bandit:/tmp/kalis$ tar xf data.tar
bandit12@bandit:/tmp/kalis$ ls
data8.bin  data.tar
bandit12@bandit:/tmp/kalis$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Thu Sep 19 07:08:15 2024, max compression, from Unix, original size modulo 2^32 49
bandit12@bandit:/tmp/kalis$ mv data8.bin data.gz
bandit12@bandit:/tmp/kalis$ gzip -d data.gz
bandit12@bandit:/tmp/kalis$ ls
data  data.tar
bandit12@bandit:/tmp/kalis$ file data
data: ASCII text
bandit12@bandit:/tmp/kalis$ cat data
The password is FO5dwFsc0cbaliH0h8J2eUks2vdTDwAn
bandit12@bandit:/tmp/kalis$

```

Create a working directory and copy `data.txt`. **Convert Hexdump:** Use `xxd -r` to restore the binary file. Extract gzip, then bzip2, then another gzip. Extract multiple tar archives, decompressing as needed. **Retrieve Password:** Once the final file is ASCII text, use `cat` to display the password.

**commands :** `mkdir, tar, gzip, bzip2, xxd, cp, mv, file`

**password :** FO5dwFsc0cbaliH0h8J2eUks2vdTDwAn

## Level 13 - 15 :

**Task :** The password for the next level is stored in `/etc/bandit_pass/bandit14` and can only be read by user `bandit14`. For this level, you don't get the next password, but you get a private SSH key that can be used to log into the next level. **Note:** `localhost` is a hostname that refers to the machine you are working on. The password for the next level can be retrieved by submitting the password of the current level to **port 30000 on localhost**.



```

bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ ssh -i sshkey.private bandit14@localhost
The authenticity of host 'localhost (127.0.0.1)' 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 on port 22, which is not intended.

bandit14@localhost: Permission denied (publickey).
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

```

```

[ roots ]

For your convenience we have installed a few useful tools which you can find
in the following locations:

* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
MU4VWeTyJk8ROof1qqmcBPALh7IDCPvS
bandit14@bandit:~$ █

```

password for level 15 is derived here . The password is saved in the **ssh privatekey** by using **bandit14@localhost** the privatekey is derived from the same level.

command : **ssh -i sshkey.private bandit14@localhost -p 2220**

**cat /etc/bandit\_pass/bandit14**

**password of 14 : MU4VWeTyJk8ROof1qqmcBPALh7IDCPvS**

password of 15 : 8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo

```
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
MU4VWeTyJk8R0of1qqmcBPALh7lDCPvS
bandit14@bandit:~$ nc localhost 30000
MU4VWeTyJk8R0of1qqmcBPALh7lDCPvS
Correct!
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo
```

## Level 15 - 16 :

**Task :** The password for the next level can be retrieved by submitting the password of the current level to **port 30001 on localhost** using SSL/TLS encryption.

```
bandit15@bandit:~$ cat /etc/bandit_pass/bandit15
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo
bandit15@bandit:~$ man nc | grep ssl
bandit15@bandit:~$ man ncat | grep ssl
--ssl          Connect or listen with SSL
--ssl-cert     Specify SSL certificate file (PEM) for listening
--ssl-key      Specify SSL private key (PEM) for listening
--ssl-verify   Verify trust and domain name of certificates
--ssl-trustfile PEM file containing trusted SSL certificates
--ssl-ciphers  Cipherlist containing SSL ciphers to use
--ssl-servername Request distinct server name (SNI)
--ssl-alpn     ALPN protocol list to use

--ssl (Use SSL)
--ssl-verify (Verify server certificates)
    In client mode, --ssl-verify is like --ssl except that it also requires verification of the server
    available. Use --ssl-trustfile to give a custom list. Use -v one or more times to get details about
--ssl-cert certfile.pem (Specify SSL certificate)
    listen mode) or the client (in connect mode). Use it in combination with --ssl-key.
--ssl-key keyfile.pem (Specify SSL private key)
    named with --ssl-cert.
--ssl-trustfile cert.pem (List trusted certificates)
    has no effect unless combined with --ssl-verify. The argument to this option is the name of a PEM
--ssl-ciphers cipherlist (Specify SSL ciphersuites)
--ssl-servername name (Request distinct server name)
--ssl-alpn ALPN list (Specify ALPN protocol list)
    http://www.openssl.org
bandit15@bandit:~$ ncat --ssl localhost 30001
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo
Correct!
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
```

the password for next level is derived by giving the password fo current level.

**command :** `ncat --ssl localhost 30001`

**password** : kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx

## Level 16 - 17 :

**Task** : The credentials for the next level can be retrieved by submitting the password of the current level to **a port on localhost in the range 31000 to 32000**. First find out which of these ports have a server listening on them. Then find out which of those speak SSL/TLS and which don't. There is only 1 server that will give the next credentials, the others will simply send back to you whatever you send to it.

```
bandit16@bandit:~$ nc localhost 31790
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
bandit16@bandit:~$ ncat --ssl localhost 31790
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvM0kuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SudyJ
imZzeyGC0gtZPGUjUSxiJSWI/oTqexh+cAMTSMl0Jf7+BrJ0bArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl870Ri0+rW4LCDCNd2LUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW30ekePQAzL0VUYbW
JGTi65CxbCnzc/w4+mqQyvmzpWtMAzJTzAzQxNbK2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XF0JuaQIDAQABAoIBABagpxpM1aoLWfVd
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNUDE6SFth0ar69jp5RlLwD1NhPx3iBl
J9nOM80J0VToum43UOS8YxF8WwhXriYGnc1sskbwpX0UDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52yOQ9q0kwFTEQpjtF4uNtJom+asvlpMS8A
vLY9r60wYSvmZhNqBURj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOmama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxBgRRhORT
8c8hAuRbb2G82so8vUHK/fur850Efc9TncnCY2crpoqsgghifKLxrLgt+qDpfZnx
SatLdt8GfQ85yA7hnWJ2Mx3F3NaeSDm75Lsm+tBbA1yc9P2jGRNtMSkCgYEAypHd
HCctNi/FwJulhttFx/rHYKhLidZDFYeiE/v45bN4yFm8*7R/b0iE7KaszX+Exdvt
SghaTdcG0Kny1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enCIvGCSx+X3l5SiWg0A
R57hJglezIiVjv3aGwHwvLZvtszK6zV6oXFAu0ECgYAbjo46T4hyP5tJi93V5Hdi
TtieK7xRVxUL+iu7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFmly9FL2m9oQWCg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB30hYimtiG2Cg5JCqIZFHxD6MjEG0iu
L8ktHMPvodBwNsSBULPg0QKBgBAPLTfC1H0nWiMGOU3KPwYwt006CdTkMJOmL8Ni
blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAglHxbdLq/ZJQ7Yfz0KU4ZxEnabvXnvWkU
Y0djHdS0oKvDQNWu6ucyLRAWFuISeXw9a/9p7f7tpxm0TSgyvmfLF2MIAEwyZRqAM
77pBAoGAMmjmIJdjp+Ez8duyn3ieo36yrttF5NSsJLabxPpdlc1gvtGCWW+9Cq0b
dxviW8+TFVEBl104f7HVM6EpTscdDxU+bCXWkfjuRb7Dy9G0tt9JP5X8MBTakzh3
vBgysi/sN3RqRBCGU40f0oZyFAMT8s1m/uYv5206IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----
```

```
(kali㉿kali)-[~]
$ vim ch

(kali㉿kali)-[~]
$ vim key

(kali㉿kali)-[~]
$ chmod 400 key

(kali㉿kali)-[~]
$ ssh -i key bandit17@bandit.labs.overthewire.org -p 2220
```

┌─┐ ┌─┐ ┌─┐ ┌─┐ ┌─┐ ┌─┐  
│ │ \ / │ │ \ / │ │ \ / │ │  
│ │ │ │ │ │ │ │ │ │ │ │  
└─┬─┘ └─┬─┘ └─┬─┘ └─┬─┘  
└─┬─┘ └─┬─┘ └─┬─┘ └─┬─┘

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

The open ports are first checked between 31000 to 32000. nmap is used to find which port is open and which is active. The result is a private sshkey a file is created to store the private keys of the levels and that file only has the permission to the user.

**command** : nmap and nc.

## Level 17 - 18 :

**Task :** here are 2 files in the homedirectory: **passwords.old** and **passwords.new**. The password for the next level is in **passwords.new** and is the only line that has been changed between **passwords.old** and **passwords.new**

Find the one line that is different between the two files.