OverTheWire - Bandit

Minh Giang

2021-10-30

Contents

Level 0 -> Level 1

`bandit0:bandit0`

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.

This level is fairly straightforward, I just displayed the contents in the `readme` file.

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

The password is `boJ9jbbUNNfktd78OOpsqOltutMc3MY1`.

Level 1 -> Level 2

`bandit1:boJ9jbbUNNfktd78OOpsqOltutMc3MY1`

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

Since the file is called −, we need to provide the relative path to it, as − will be interpreted as an option for `cat`.

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

The password is `CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9`.

Level 2 -> Level 3

`bandit2:CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9`

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

When dealing with spaces in a file name, we need to use \ to take the spaces.

```
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat spaces\ in\ this\ filename
UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK
```

The password is `UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK`.

Level 3 -> Level 4

`bandit3:UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK`

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

First we need to change the directory to `inhere`.

```
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere
```

Then we can use `ls -al` to view all files in the directory (including hidden files).

```
bandit3@bandit:~/inhere$ ls -al
total 12
drwxr-xr-x 2 root    root    4096 May  7  2020 .
drwxr-xr-x 3 root    root    4096 May  7  2020 ..
-rw-r----- 1 bandit4 bandit3   33 May  7  2020 .hidden
bandit3@bandit:~/inhere$ cat .hidden
pIwrPrtPN36QITSp3EQaw936yaFoFgAB
```

The password is `pIwrPrtPN36QITSp3EQaw936yaFoFgAB`.

Level 4 -> Level 5

`bandit4:pIwrPrtPN36QITSp3EQaw936yaFoFgAB`

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.

First we need to change the directory to `inhere`.

```
bandit4@bandit:~$ ls
bandit4@bandit:~$ cd inhere
```

Then we can use `ls -al` to list all the files.

```
bandit4@bandit:~/inhere$ ls -al
total 48
drwxr-xr-x 2 root    root    4096 May  7  2020 .
drwxr-xr-x 3 root    root    4096 May  7  2020 ..
-rw-r----- 1 bandit5 bandit4   33 May  7  2020 -file00
-rw-r----- 1 bandit5 bandit4   33 May  7  2020 -file01
-rw-r----- 1 bandit5 bandit4   33 May  7  2020 -file02
-rw-r----- 1 bandit5 bandit4   33 May  7  2020 -file03
```

```
-rw-r----- 1 bandit5 bandit4   33 May  7  2020 -file04
-rw-r----- 1 bandit5 bandit4   33 May  7  2020 -file05
-rw-r----- 1 bandit5 bandit4   33 May  7  2020 -file06
-rw-r----- 1 bandit5 bandit4   33 May  7  2020 -file07
-rw-r----- 1 bandit5 bandit4   33 May  7  2020 -file08
-rw-r----- 1 bandit5 bandit4   33 May  7  2020 -file09
```

It appears that there are 10 files, where we can choose to look through one-by-one, or just simply print all of the contents of each file at once. That can be done with `cat ./*`.

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

The password is `koReBOKuIDDepwhWk7jZC0RTdopnAYKh`.

Level 5 -> Level 6

`bandit5:koReBOKuIDDepwhWk7jZC0RTdopnAYKh` > 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

First we should change the directory to `inhere` and list the files/directories in it.

```
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls
maybehere00  maybehere04  maybehere08  maybehere12  maybehere16
maybehere01  maybehere05  maybehere09  maybehere13  maybehere17
maybehere02  maybehere06  maybehere10  maybehere14  maybehere18
maybehere03  maybehere07  maybehere11  maybehere15  maybehere19
```

To find the file that we are looking for, we can use `find` and include `-size 1033c` to find a file that is 1033 bytes in size, and `! -executable` to find non-executable files.

```
bandit5@bandit:~/inhere$ find . -size 1033c ! -executable
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7
```

The password is `DXjZPULLxYr17uwoI01bNLQbtFemEgo7`.

Level 6 -> Level 7

`bandit6:DXjZPULLxYr17uwoI01bNLQbtFemEgo7` > 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

To find the file that we are interested in, we can use a command called `find`. We can add `-user bandit7` to find the file that is owned by user bandit7, `-group bandit6` for file that is owned by group bandit6, and `-size 32c` for files that is 33 bytes in size. I also provided `2> /dev/null` because I want to redirect any errors that occurs.

```
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c 2> /dev
    /null
/var/lib/dpkg/info/bandit7.password
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs
```

The password is `HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs`.

Level 7 -> Level 8

`bandit7:HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs` > The password for the next level is stored in the file data.txt next to the word millionth

```
bandit7@bandit:~$ ls
data.txt
bandit7@bandit:~$ grep "millionth" data.txt
millionth   cvX2JJa4CFALtqS87jk27qwqGhBM9plV
```

The password is `cvX2JJa4CFALtqS87jk27qwqGhBM9plV`.

Level 8 -> Level 9

`bandit8:cvX2JJa4CFALtqS87jk27qwqGhBM9plV` > 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:~$ ls
data.txt
bandit8@bandit:~$ sort data.txt | uniq -u
UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR
```

The password is `UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR`.

Level 9 -> Level 10

`bandit9:UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR` > 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:~$ ls
data.txt
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
&========== truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk
S=A.H&^
```

The password is `truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk`.

Level 10 -> Level 11

`bandit10:truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk` > The password for the next level is stored in the file data.txt, which contains base64 encoded data

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

The password is `IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR`.

Level 11 -> Level 12

`bandit11:IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR` > 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:~$ ls
data.txt
bandit11@bandit:~$ cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'
The password is 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu
```

The password is `5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu`.

Level 12 -> Level 13

bandit12:5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu > 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 using mkdir. For example: mkdir /tmp/myname123. Then copy the datafile using cp, and rename it using mv (read the manpages!)

```
bandit12@bandit:~$ ls
data.txt
bandit12@bandit:~$ cd /tmp
bandit12@bandit:~/tmp$ mkdir blackjackk
bandit12@bandit:~/tmp$ cd blackjackk
bandit12@bandit:~/tmp/blackjackk$ cp ~/data.txt .
bandit12@bandit:~/tmp/blackjackk$ head -2 data.txt
00000000: 1f8b 0808 0650 b45e 0203 6461 7461 322e  .....P.^..data2.
00000010: 6269 6e00 013d 02c2 fd42 5a68 3931 4159  bin..=...BZh91AY
bandit12@bandit:~/tmp/blackjackk$ xxd -r data.txt > data2.bin
bandit12@bandit:~/tmp/blackjackk$ file data2.bin
data2.bin: gzip compressed data, was "data2.bin", last modified: Thu
    May  7 18:14:30 2020, max compression, from Unix
bandit12@bandit:~/tmp/blackjackk$ mv data2.bin data2.bin.gz
bandit12@bandit:~/tmp/blackjackk$ gunzip data2.bin.gz
bandit12@bandit:~/tmp/blackjackk$ file data2.bin
data2.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:~/tmp/blackjackk$ mv data2.bin data2.bin.bz2
bandit12@bandit:~/tmp/blackjackk$ bzip2 -d data2.bin.bz2
bandit12@bandit:~/tmp/blackjackk$ file data2.bin
data2.bin: gzip compressed data, was "data4.bin", last modified: Thu
    May  7 18:14:30 2020, max compression, from Unix
bandit12@bandit:~/tmp/blackjackk$ mv data2.bin data4.bin.gz
bandit12@bandit:~/tmp/blackjackk$ gunzip data4.bin.gz
bandit12@bandit:~/tmp/blackjackk$ file data4.bin
data4.bin: POSIX tar archive (GNU)
bandit12@bandit:~/tmp/blackjackk$ mv data4.bin data4.bin.tar
bandit12@bandit:~/tmp/blackjackk$ tar -xf data4.bin.tar
bandit12@bandit:~/tmp/blackjackk$ ls
data4.bin.tar  data5.bin  data.txt
bandit12@bandit:~/tmp/blackjackk$ file data5.bin
data4.bin: POSIX tar archive (GNU)
bandit12@bandit:~/tmp/blackjackk$ mv data5.bin data5.bin.tar
bandit12@bandit:~/tmp/blackjackk$ tar -xf data5.bin.tar
bandit12@bandit:~/tmp/blackjackk$ ls
data4.bin.tar  data5.bin.tar  data6.bin  data.txt
bandit12@bandit:~/tmp/blackjackk$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:~/tmp/blackjackk$ mv data6.bin data6.bin.bz2
bandit12@bandit:~/tmp/blackjackk$ bzip2 -d data6.bin.bz2
bandit12@bandit:~/tmp/blackjackk$ file data6.bin
data6.bin: POSIX tar archive (GNU)
bandit12@bandit:~/tmp/blackjackk$ mv data6.bin data6.bin.tar
```

```
bandit12@bandit:~/tmp/blackjackk$ tar -xf data6.bin.tar
bandit12@bandit:~/tmp/blackjackk$ ls
data4.bin.tar  data5.bin.tar  data6.bin.tar  data8.bin  data.txt
bandit12@bandit:~/tmp/blackjackk$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Thu
    May  7 18:14:30 2020, max compression, from Unix
bandit12@bandit:~/tmp/blackjackk$ mv data8.bin data9.bin.gz
bandit12@bandit:~/tmp/blackjackk$ gunzip data9.bin.gz
bandit12@bandit:~/tmp/blackjackk$ file data9.bin
data9.bin: ASCII text
bandit12@bandit:~/tmp/blackjackk$ cat data9.bin
The password is 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
```

Level 13 -> Level 14

bandit13:8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL > 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

```
bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ ssh -i sshkey.private bandit14@localhost
Could not create directory '/home/bandit13/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98
    UL0ZWr85496EtCRkKlo20X3OPnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
```

Level 14 -> Level 15

bandit14:4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e > The password for the next level can be retrieved by submitting the password of the current level to port 30000 on localhost.

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

Level 15 -> Level 16

`bandit15:BfMYroe26WYalil77FoDi9qh59eK5xNr` > The password for the next level can be retrieved by submitting the password of the current level to port 30001 on localhost using SSL encryption. Helpful note: Getting “HEARTBEATING” and “Read R BLOCK”? Use -ign_eof and read the “CONNECTED COMMANDS” section in the manpage. Next to ‘R’ and ‘Q’, the ‘B’ command also works in this version of that command

```
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
---
Server certificate
-----BEGIN CERTIFICATE-----
MIICBjCCAW+gAwIBAgIEZOzuVDANBgkqhkiG9w0BAQUFADAUMRIwEAYDVQQDDAls
b2NhbGhvc3QwHhcNMjEwOTMwMDQ0NTU0WhcNMjIwOTMwMDQ0NTU0WjAUMRIwEAYD
VQQDDAlsb2NhbGhvc3QwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAM9En7CC
uPr6cVPATLAVhWMU1hggfIJEp5sZN9RPUbK0zKBv802yD54ObHYmIge6lqqkgXOz
2AuI4UfCG4iMb0UYUCA/wISwNqUQrjcja0OnqzCTRscXzzoIsHbC8lGFzMDRz3Jw
8nBD6/2jvFt1rnBtZ4ghibNn5rFHRi5EC+K/AgMBAAGjZTBjMBQGA1UdEQQNMAuC
CWxvY2FsaG9zdDBLBglghkgBhvhCAQ0EPhY8QXV0b21hdGljYWxseSBnZW5lcmF0
ZWQgYnkgTmNhdC4gU2VlIGh0dHBzOi8vbm1hcC5vcmcvbmNhdC8uMA0GCSqGSIb3
DQEBBQUAA4GBAD7/moj14DUI6/D6imJ8pQlAy/8lZlsrbyRnqpzjWaATShDYr7k3
umdRg+36MciNFAglE7nGYZroTSDCm650D81+797owSXLPAdp1Q6JfQH5LOni2kbw
UHcO9hwQ+rJzEgIlfGOic7dC5lj8DBU5tugY87RZGKiZ2GG77WXas9Iz
-----END CERTIFICATE-----
subject=/CN=localhost
issuer=/CN=localhost
---
No client certificate CA names sent
Peer signing digest: SHA512
Server Temp Key: X25519, 253 bits
---
SSL handshake has read 1019 bytes and written 269 bytes
Verification error: self signed certificate
---
New, TLSv1.2, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 1024 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
```

```
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES256-GCM-SHA384
    Session-ID:
       BA203CEEBC6E40DF43DEC962889B74A13C2CEDDA98A1CFB931545BB3CA1A178C
    Session-ID-ctx:
    Master-Key: 6
       CAF057AA473CE8D5C965F1C0A524AFE705FE5138E5517FE421DD0DC3D9523F7983F566313AC5

    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
    0000 - 8a eb e8 f5 31 15 46 ad-b2 a8 10 c1 51 b9 66 14   ....1.F
       .....Q.f.
    0010 - ab bb 84 e7 d3 4f 5f bb-94 cc 47 11 ae 0f d4 8b   .....O_...
       G.....
    0020 - 87 3d 64 77 b2 51 ad 37-cf 3a f0 43 91 54 1f 08   .=dw.Q
       .7.:.C.T..
    0030 - e5 d6 6c 67 40 0e 08 c7-15 b2 59 1c 56 bc a7 52   ..lg@.....
       Y.V..R
    0040 - c5 e3 e0 7d cc b2 31 09-58 2b 08 ca 45 87 0f 64   ...}..1.X
       +..E..d
    0050 - 18 ff 6e 74 74 9f 3f a8-12 f1 6e fe 0f 79 a0 59   ..ntt.?...
       n..y.Y
    0060 - d3 fe 26 c2 c2 4a 0c d7-86 77 d8 4b a8 d7 af c0   ..&..J...w
       .K....
    0070 - 2b 6a 4e 7d eb 04 d4 11-59 4c ca d9 a1 03 3f 06   +jN}....YL
       ....?.
    0080 - 48 cd ad 82 65 16 62 67-b5 36 0f 1d d0 4b c2 95   H...e.bg
       .6...K..
    0090 - e3 e3 be ed 12 6a a0 4f-65 33 ab 86 f2 af 6e b3   .....j.Oe3
       ....n.

    Start Time: 1633343145
    Timeout   : 7200 (sec)
    Verify return code: 18 (self signed certificate)
    Extended master secret: yes
---
BfMYroe26WYalil77FoDi9qh59eK5xNr
Correct!
cluFn7wTiGryunymYOu4RcffSxQluehd

closed
```

Level 16 -> Level 17

`bandit16:cluFn7wTiGryunymYOu4RcffSxQluehd` > 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 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:~$ nmap -p31000-32000 -sV localhost
Starting Nmap 7.40 ( https://nmap.org ) at 2021-10-04 12:28 CEST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00038s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE     VERSION
31046/tcp open  echo
31518/tcp open  ssl/echo
31691/tcp open  echo
31790/tcp open  ssl/unknown
31960/tcp open  echo
1 service unrecognized despite returning data. If you know the service/
    version, please submit the following fingerprint at https://nmap.org
    /cgi-bin/submit.cgi?new-service :
SF-Port31790-TCP:V=7.40%T=SSL%I=7%D=10/4%Time=615AD75A%P=x86_64-pc-
    linux-g
SF:nu%r(GenericLines,31,"Wrong!\x20Please\x20enter\x20the\x20correct\
    x20cu
SF:rrent\x20password\n")%r(GetRequest,31,"Wrong!\x20Please\x20enter\
    x20the
SF:\x20correct\x20current\x20password\n")%r(HTTPOptions,31,"Wrong!\
    x20Plea
SF:se\x20enter\x20the\x20correct\x20current\x20password\n")%r(
    RTSPRequest,
SF:31,"Wrong!\x20Please\x20enter\x20the\x20correct\x20current\
    x20password\
SF:n")%r(Help,31,"Wrong!\x20Please\x20enter\x20the\x20correct\
    x20current\x
SF:20password\n")%r(SSLSessionReq,31,"Wrong!\x20Please\x20enter\x20the\
    x20
SF:correct\x20current\x20password\n")%r(TLSSessionReq,31,"Wrong!\
    x20Please
SF:\x20enter\x20the\x20correct\x20current\x20password\n")%r(Kerberos
    ,31,"W
SF:rong!\x20Please\x20enter\x20the\x20correct\x20current\x20password\n"
    )%r
SF:(FourOhFourRequest,31,"Wrong!\x20Please\x20enter\x20the\x20correct\
    x20c
SF:urrent\x20password\n")%r(LPDString,31,"Wrong!\x20Please\x20enter\
    x20the
SF:\x20correct\x20current\x20password\n")%r(LDAPSearchReq,31,"Wrong!\
```

```
    x20Pl
SF:ease\x20enter\x20the\x20correct\x20current\x20password\n")%r(
    SIPOptions
SF:,31,"Wrong!\x20Please\x20enter\x20the\x20correct\x20current\
    x20password
SF:\n");

Service detection performed. Please report any incorrect results at
    https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 88.06 seconds
bandit16@bandit:~$ openssl s_client -connect localhost:31790
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
---
Server certificate
-----BEGIN CERTIFICATE-----
MIICBjCCAW+gAwIBAgIESHcOOjANBgkqhkiG9w0BAQUFADAUMRIwEAYDVQQDDAls
b2NhbGhvc3QwHhcNMjEwOTMwMDQ0NjAyWhcNMjIwOTMwMDQ0NjAyWjAUMRIwEAYD
VQQDDAlsb2NhbGhvc3QwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAPQcF7d1
ID9LNKC+iUC3Yc6kW3j8S5ZLNi8ZiYa+gtUH5ruwqyC/QMME3/JiY/nzYXZO2X0o
1ANrcaGCDgFNFbNYBxNSdRLNhfQeXX7OfJh7+MTJ/PHBR2kXeSJJES2DjdlxjK4i
ZmnfJSIK9pziiygDwYKSIkkZfkza9YJttGZ1AgMBAAGjZTBjMBQGA1UdEQQNMAuC
CWxvY2FsaG9zdDBLBglghkgBhvhCAQ0EPhY8QXV0b21hdGljYWxseSBnZW5lcmF0
ZWQgYnkgTmNhdC4gU2VlIGh0dHBzOi8vbm1hcC5vcmcvbmNhdC8uMA0GCSqGSIb3
DQEBBQUAA4GBAIxX2OYx2fzO1PsKOjDcTgCEerfX512NxALJjf8EQuro+mUjxCfy
yNzIzYDRx+sGTeolfqwNZXgWIURjJYHGxhvGRPAnf6HisDrAluLwC0qZE+A6Ez5q
Zx9QvjOFHk8uXkmhW5sIeoPV1a0/vf5RpJFptLZz/Gm+Og5cG23sjPL/
-----END CERTIFICATE-----
subject=/CN=localhost
issuer=/CN=localhost
---
No client certificate CA names sent
Peer signing digest: SHA512
Server Temp Key: X25519, 253 bits
---
SSL handshake has read 1019 bytes and written 269 bytes
Verification error: self signed certificate
---
New, TLSv1.2, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 1024 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
```

```
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES256-GCM-SHA384
    Session-ID: 12
       BDD84FBF21DC3F92205398E066980091A4809E6A9B59757036C4C9EA86BEB6
    Session-ID-ctx:
    Master-Key: 0
       C0B4901ACFFB03795EE216654CD48E3C34E02186B57A744277B4309333E4BF49946D9369EC22

    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
    0000 - 27 6a 7e ce 82 82 53 7f-56 22 fc 0b 04 d0 99 b7   'j~...S.V
       "......
    0010 - 1f ff 78 c3 c9 15 4b a0-90 9f fe a3 8b c9 80 7d   ..x...K
       ........}
    0020 - 40 59 0d 54 10 24 e3 4a-0f 93 7d 88 fa ff 08 3a   @Y.T.$.J
       ..}....:
    0030 - 09 75 67 53 d8 62 01 13-dd c8 52 18 45 9b 60 c6   .ugS.b....
       R.E.`.
    0040 - a8 0a 54 7d 48 31 b9 07-c2 df 3c 31 45 1b f2 00   ..T}H1
       ....<1E...
    0050 - 99 f8 b0 d3 5a 3e 55 4b-ed 54 b8 3f 9f 53 2e ab   ....Z>UK.T
       .?.S..
    0060 - 2a de d0 e7 b0 0f a6 b9-8f f0 5a 61 7e 88 9b ce   *.........
       Za~...
    0070 - 9a 3e 5f 73 8d fd ee 5c-9a 6a a0 b0 98 1f 98 6d   .>_s...\.j
       .....m
    0080 - 87 10 ab 82 3e 8f 17 17-56 b8 9e 64 15 19 1f 34   ....>...V
       ..d...4
    0090 - 3c 0e 28 be 76 21 c1 49-00 6d 14 38 15 9e bc 34   <.(.v!.I.m
       .8...4

    Start Time: 1633343458
    Timeout   : 7200 (sec)
    Verify return code: 18 (self signed certificate)
    Extended master secret: yes
---
cluFn7wTiGryunymYOu4RcffSxQluehd
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
```

Level 17 -> Level 18

```
-----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-----
```

> There 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 NOTE: if you have solved this level and see 'Byebye!' when trying to log into bandit18, this is related to the next level, bandit19

```
bandit17@bandit:~$ diff passwords.old passwords.new
42c42
< w0Yfolrc5bwjS4qw5mq1nnQi6mF03bii
---
> kfBf3eYk5BPBRzwjqutbbfE887SVc5Yd
```

Level 18 -> Level 19

`bandit18:kfBf3eYk5BPBRzwjqutbbfE887SVc5Yd` > The password for the next level is stored in a file readme in the homedirectory. Unfortunately, someone has modified .bashrc to log you out when you log in with SSH.

```
blackjackk@local:~$ ssh -p2220 bandit18@bandit.labs.overthewire.org "ls
"
This is a OverTheWire game server. More information on http://www.
    overthewire.org/wargames

bandit18@bandit.labs.overthewire.org's password:
    kfBf3eYk5BPBRzwjqutbbfE887SVc5Yd
readme

blackjackk@local:~$ ssh -p2220 bandit18@bandit.labs.overthewire.org "
    cat readme"
This is a OverTheWire game server. More information on http://www.
    overthewire.org/wargames

bandit18@bandit.labs.overthewire.org's password:
    kfBf3eYk5BPBRzwjqutbbfE887SVc5Yd
IueksS7Ubh8G3DCwVzrTd8rAVOwq3M5x
```

Level 19 -> Level 20

`bandit19:IueksS7Ubh8G3DCwVzrTd8rAVOwq3M5x` > To gain access to the next level, you should use the setuid binary in the homedirectory. Execute it without arguments to find out how to use it. The password for this level can be found in the usual place (/etc/bandit_pass), after you have used the setuid binary.

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

Level 20 -> Level 21

bandit20:GbKksEFF4yrVs6il55v6gwY5aVje5f0j > There is a setuid binary in the homedirectory that does the following: it makes a connection to localhost on the port you specify as a commandline argument. It then reads a line of text from the connection and compares it to the password in the previous level (bandit20). If the password is correct, it will transmit the password for the next level (bandit21). NOTE: Try connecting to your own network daemon to see if it works as you think

```
bandit20@bandit:~$ echo "GbKksEFF4yrVs6il55v6gwY5aVje5f0j" | nc -lp
    6666&
[1] 17729
bandit20@bandit:~$ ./suconnect 6666
Read: GbKksEFF4yrVs6il55v6gwY5aVje5f0j
Password matches, sending next password
gE269g2h3mw3pwgrj0Ha9Uoqen1c9DGr
```

Level 21 -> Level 22

bandit21:gE269g2h3mw3pwgrj0Ha9Uoqen1c9DGr > A program is running automatically at regular intervals from cron, the time-based job scheduler. Look in /etc/cron.d/ for the configuration and see what command is being executed.

```
bandit21@bandit:~$ cd /etc/cron.d
bandit21@bandit:/etc/cron.d$ ls
cronjob_bandit15_root  cronjob_bandit22  cronjob_bandit24
cronjob_bandit17_root  cronjob_bandit23  cronjob_bandit25_root
bandit21@bandit:/etc/cron.d$ cat cronjob_bandit22
@reboot bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
* * * * * bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
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:~$ cat /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv
Yk7owGAcWjwMVRwrTesJEwB7WVOiILLI
```

Level 22 -> Level 23

bandit22:Yk7owGAcWjwMVRwrTesJEwB7WVOiILLI > A program is running automatically at regular intervals from cron, the time-based job scheduler. Look in /etc/cron.d/ for the configuration and see what command is being executed. NOTE: Looking at shell scripts written by other people is a very useful skill. The script for this level is intentionally made easy to read. If you are having problems understanding what it does, try executing it to see the debug information it prints.

```
bandit22@bandit:~$ cd /etc/cron.d/
bandit22@bandit:/etc/cron.d$ ls
cronjob_bandit15_root  cronjob_bandit22  cronjob_bandit24
cronjob_bandit17_root  cronjob_bandit23  cronjob_bandit25_root
bandit22@bandit:/etc/cron.d$ cat cronjob_bandit23
@reboot bandit23 /usr/bin/cronjob_bandit23.sh  &> /dev/null
* * * * * bandit23 /usr/bin/cronjob_bandit23.sh  &> /dev/null
bandit22@bandit:/etc/cron.d$ 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:/etc/cron.d$ echo $(echo I am user bandit23 | md5sum |
   cut -d ' ' -f 1)
8ca319486bfbbc3663ea0fbe81326349
bandit22@bandit:/etc/cron.d$ cat /tmp/8ca319486bfbbc3663ea0fbe81326349
jc1udXuA1tiHqjIsL8yaapX5XIAI6i0n
```

Level 23 -> Level 24

bandit23:jc1udXuA1tiHqjIsL8yaapX5XIAI6i0n > A program is running automatically at regular intervals from cron, the time-based job scheduler. Look in /etc/cron.d/ for the configuration and see what command is being executed. NOTE: This level requires you to create your own first shell-script. This is a very big step and you should be proud of yourself when you beat this level! NOTE 2: Keep in mind that your shell script is removed once executed, so you may want to keep a copy around…

```
bandit23@bandit:~$ cd /etc/cron.d
bandit23@bandit:/etc/cron.d$ ls
cronjob_bandit15_root  cronjob_bandit22  cronjob_bandit24
cronjob_bandit17_root  cronjob_bandit23  cronjob_bandit25_root
bandit23@bandit:/etc/cron.d$ cat cronjob_bandit24
@reboot bandit24 /usr/bin/cronjob_bandit24.sh &> /dev/null
* * * * * bandit24 /usr/bin/cronjob_bandit24.sh &> /dev/null
bandit23@bandit:/etc/cron.d$ cat /usr/bin/cronjob_bandit24.sh
```

```
#!/bin/bash

myname=$(whoami)

cd /var/spool/$myname
echo "Executing and deleting all scripts in /var/spool/$myname:"
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
```