🔍

OverTheWire Bandit Level 0-20

Level 0: Initial Access

1. Launch your terminal
2. Establish a connection via SSH :

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

3. Enter password:

Level 0 → 1

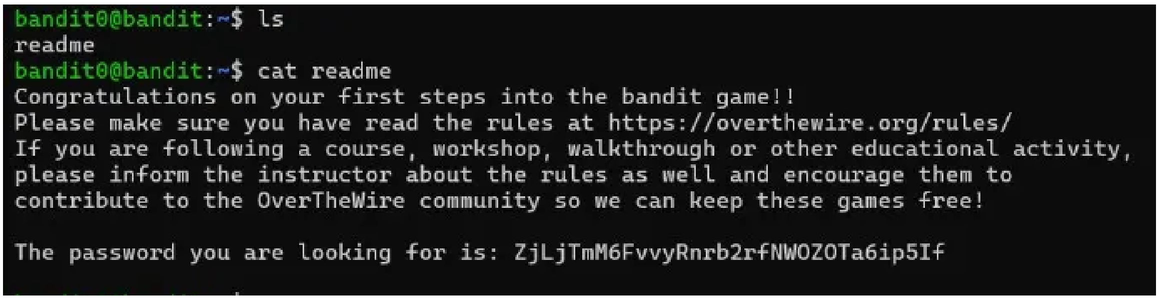
1. Check for the README file by listing the directory contents:

```
ls
```

2. Open and read the contents of the README file:

```
cat readme
```

3. Note down the displayed password



```
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
```

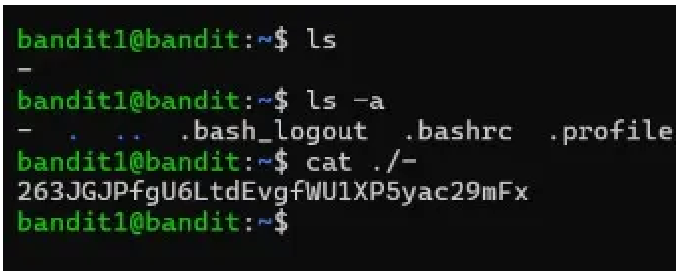
Level 1 → 2

1. The file is named "-", which requires special handling to access it properly.

2. Use the following command to read its contents:

```
cat ./-
```

3. Save the password shown



```
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ ls -a
-  .  ..  .bash_logout  .bashrc  .profile
bandit1@bandit:~$ cat ./-
263JGJPfgU6LtdEvgfWU1XP5yac29mFx
bandit1@bandit:~$
```

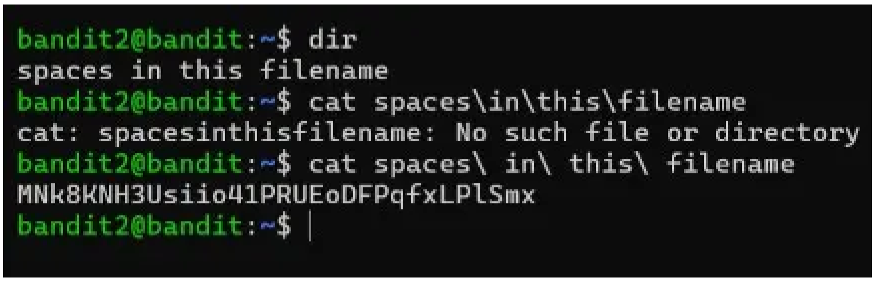
Level 2 → 3

1. The filename includes spaces, so it requires special handling.

2. Read the file by enclosing the filename in quotes:

```
cat "spaces in this filename"
```

3. Save the password shown



```
bandit2@bandit:~$ dir
spaces in this filename
bandit2@bandit:~$ cat spaces\in\this\filename
cat: spacesinthisfilename: No such file or directory
bandit2@bandit:~$ cat spaces\ in\ this\ filename
MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx
bandit2@bandit:~$ |
```

Level 3 → 4

1. Navigate to the **inhere** directory:

```
cd inhere
```

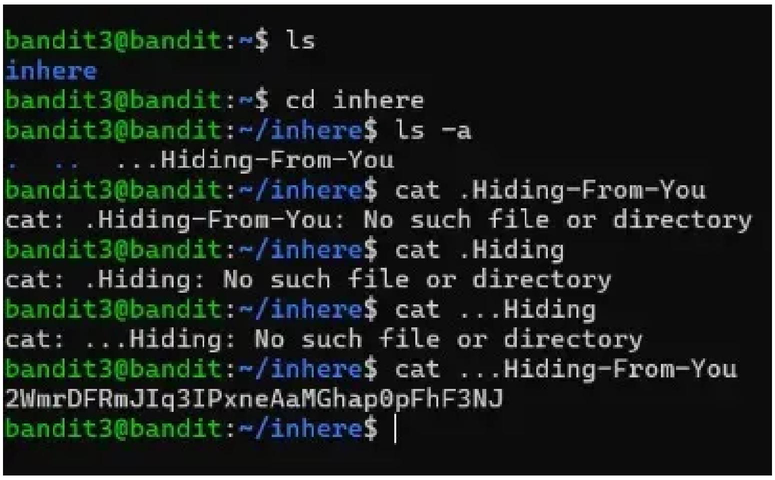
2. List all files including hidden:

```
ls -la
```

3. Read the hidden file:

```
cat .hidden
```

4. Save the password shown



```
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls -a
.  ..  ...Hiding-From-You
bandit3@bandit:~/inhere$ cat .Hiding-From-You
cat: .Hiding-From-You: No such file or directory
bandit3@bandit:~/inhere$ cat .Hiding
cat: .Hiding: No such file or directory
bandit3@bandit:~/inhere$ cat ...Hiding
cat: ...Hiding: No such file or directory
bandit3@bandit:~/inhere$ cat ...Hiding-From-You
2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
bandit3@bandit:~/inhere$ |
```

Level 4 → 5

1. Change to inhere directory

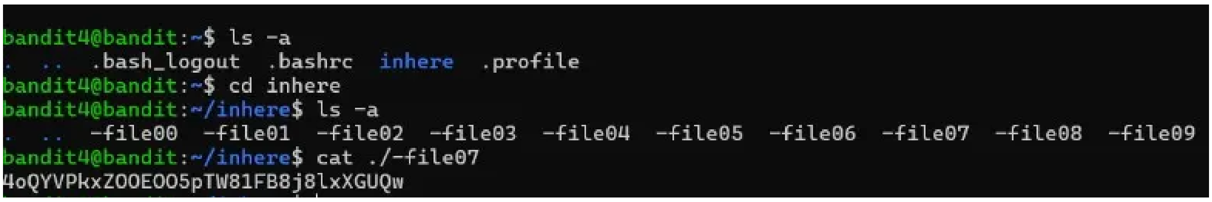
2. Check file types:

```
file ./*
```

3. Find and read the human-readable file:

```
cat ./-file07
```

4. Save the password shown



```
bandit4@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  inhere  .profile
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls -a
.  ..  -file00  -file01  -file02  -file03  -file04  -file05  -file06  -file07  -file08  -file09
bandit4@bandit:~/inhere$ cat ./-file07
4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw
```

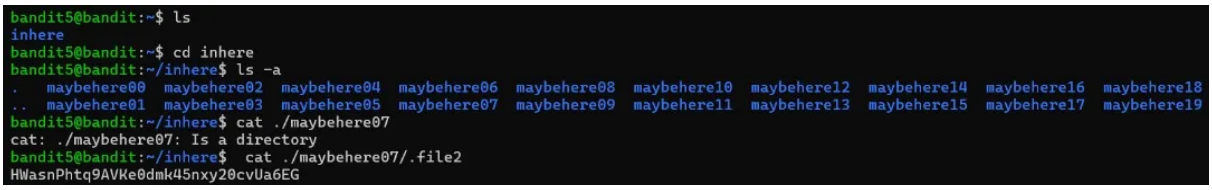
Level 5 → 6

1. Navigate to inhere directory

2. Find file with specific properties:

```
find . -type f -size 1033c ! -executable
```

3. save the password shown



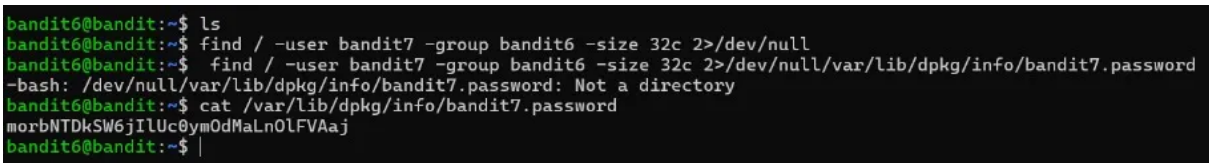
```
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls -a
.   maybehere00  maybehere02  maybehere04  maybehere06  maybehere08  maybehere10  maybehere12  maybehere14  maybehere16  maybehere18
..  maybehere01  maybehere03  maybehere05  maybehere07  maybehere09  maybehere11  maybehere13  maybehere15  maybehere17  maybehere19
bandit5@bandit:~/inhere$ cat ./maybehere07
cat: ./maybehere07: Is a directory
bandit5@bandit:~/inhere$  cat ./maybehere07/.file2
HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
```

Level 6 → 7

1. Search entire system with specific criteria:

```
find / -user bandit7 -group bandit6 -size 33c 2>/dev/null
```

2. Save the password shown



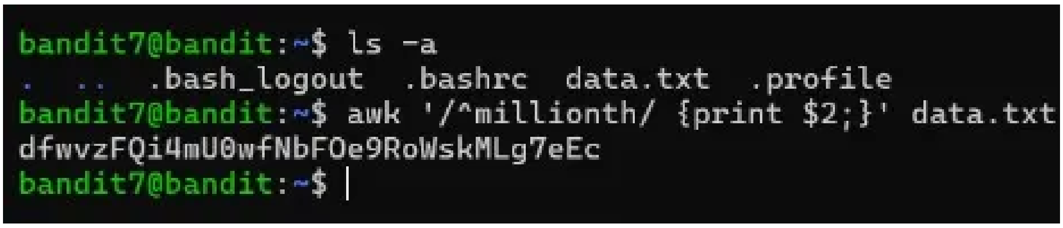
```
bandit6@bandit:~$ ls
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 32c 2>/dev/null
bandit6@bandit:~$  find / -user bandit7 -group bandit6 -size 32c 2>/dev/null/var/lib/dpkg/info/bandit7.password
-bash: /dev/null/var/lib/dpkg/info/bandit7.password: Not a directory
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj
bandit6@bandit:~$ |
```

Level 7 → 8

1. Search for "millionth" in data.txt:

```
cat data.txt | grep millionth
```

2. Save the password shown



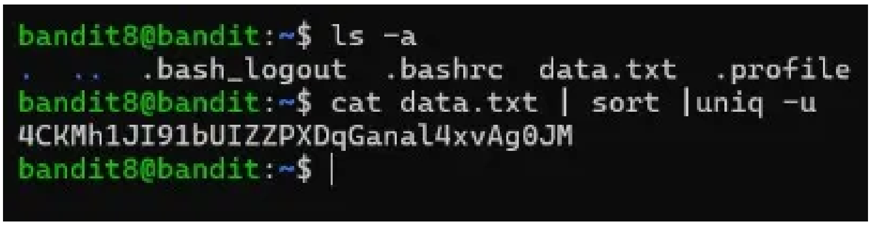
```
bandit7@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  data.txt  .profile
bandit7@bandit:~$ awk '/^millionth/ {print $2;}' data.txt
dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
bandit7@bandit:~$ |
```

Level 8 → 9

1. Find unique line:

```
sort data.txt | uniq -u
```

2. Save the password shown



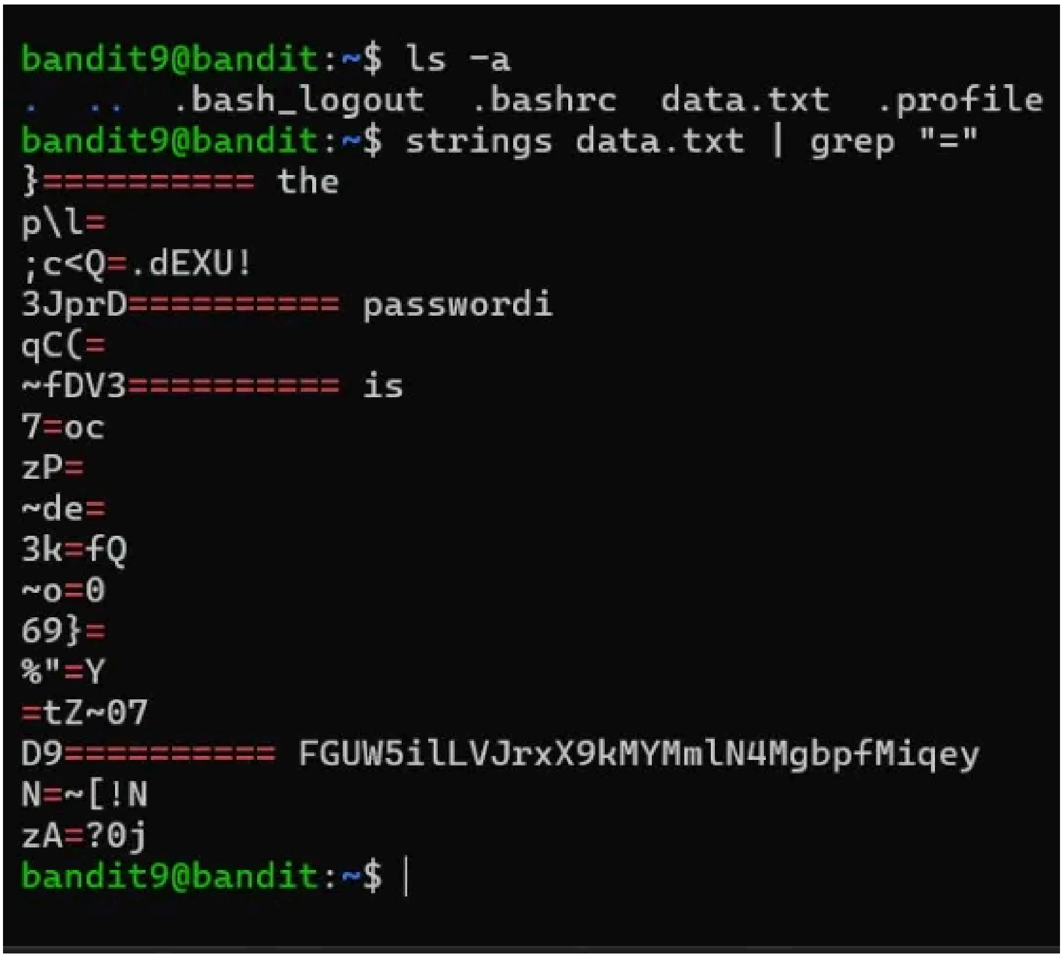
```
bandit8@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  data.txt  .profile
bandit8@bandit:~$ cat data.txt | sort |uniq -u
4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
bandit8@bandit:~$ |
```

Level 9 → 10

1. Search for human-readable strings with "=":

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

2. Save the password shown



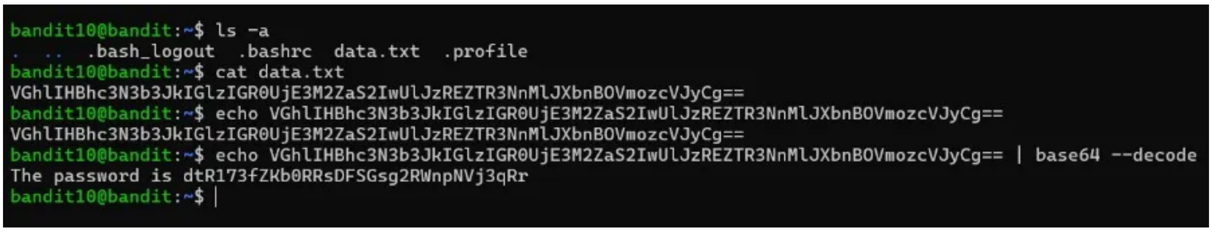
```
bandit9@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  data.txt  .profile
bandit9@bandit:~$ strings data.txt | grep "="
}========== the
p\l=
;c<Q=.dEXU!
3JprD========== passwordi
qC(=
~fDV3========== is
7=oc
zP=
~de=
3k=fQ
~o=0
69}=
%"=Y
=tZ~07
D9========== FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey
N=~[!N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

Level 10 → 11

1. Decode base64 content:

```
base64 -d data.txt
```

2. Save the password shown



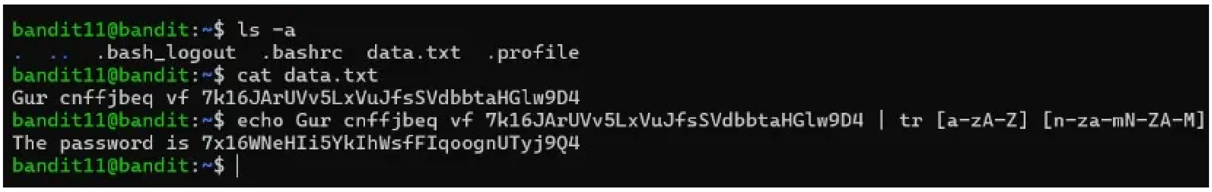
```
bandit10@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  data.txt  .profile
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIGR0UjE3M2ZaS2IwUlJzREZTR3NnMlJXbnBOVmozcVJyCg==
bandit10@bandit:~$ echo VGhlIHBhc3N3b3JkIGlzIGR0UjE3M2ZaS2IwUlJzREZTR3NnMlJXbnBOVmozcVJyCg==
VGhlIHBhc3N3b3JkIGlzIGR0UjE3M2ZaS2IwUlJzREZTR3NnMlJXbnBOVmozcVJyCg==
bandit10@bandit:~$ echo VGhlIHBhc3N3b3JkIGlzIGR0UjE3M2ZaS2IwUlJzREZTR3NnMlJXbnBOVmozcVJyCg== | base64 --decode
The password is dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr
bandit10@bandit:~$ |
```

Level 11 → 12

1. Decode ROT13:

```
cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'
```

2. Save the password shown



```
bandit11@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  data.txt  .profile
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf 7k16JArUVv5LxVuJfsSVdbbtaHGlw9D4
bandit11@bandit:~$ echo Gur cnffjbeq vf 7k16JArUVv5LxVuJfsSVdbbtaHGlw9D4 | tr [a-zA-Z] [n-za-mN-ZA-M]
The password is 7x16WNeHIi5YkIhWsfFIqoognUTyj9Q4
bandit11@bandit:~$ |
```

Level 12 → 13

1. Create temporary directory:

```
mkdir /tmp/myname123
```

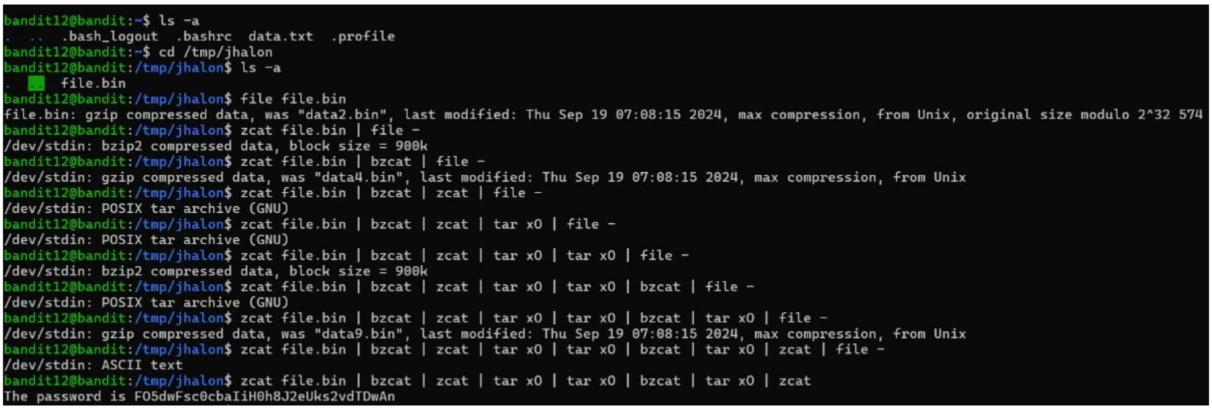
2. Copy and navigate:

```
cp data.txt /tmp/myname123
cd /tmp/myname123
```

3. Convert hex dump:

```
xxd -r data.txt > data
```

4. Save the password shown



```
bandit12@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  data.txt  .profile
bandit12@bandit:~$ cd /tmp/jhalon
bandit12@bandit:/tmp/jhalon$ ls -a
.  ..  file.bin
bandit12@bandit:/tmp/jhalon$ file file.bin
file.bin: 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/jhalon$ zcat file.bin | file -
/dev/stdin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/jhalon$ zcat file.bin | bzcat | file -
/dev/stdin: gzip compressed data, was "data4.bin", last modified: Thu Sep 19 07:08:15 2024, max compression, from Unix
bandit12@bandit:/tmp/jhalon$ zcat file.bin | bzcat | zcat | file -
/dev/stdin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/jhalon$ zcat file.bin | bzcat | zcat | tar xO | file -
/dev/stdin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/jhalon$ zcat file.bin | bzcat | zcat | tar xO | tar xO | file -
/dev/stdin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/jhalon$ zcat file.bin | bzcat | zcat | tar xO | tar xO | bzcat | file -
/dev/stdin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/jhalon$ zcat file.bin | bzcat | zcat | tar xO | tar xO | bzcat | tar xO | file -
/dev/stdin: gzip compressed data, was "data9.bin", last modified: Thu Sep 19 07:08:15 2024, max compression, from Unix
bandit12@bandit:/tmp/jhalon$ zcat file.bin | bzcat | zcat | tar xO | tar xO | bzcat | tar xO | zcat | file -
/dev/stdin: ASCII text
bandit12@bandit:/tmp/jhalon$ zcat file.bin | bzcat | zcat | tar xO | tar xO | bzcat | tar xO | zcat
The password is FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn
```

Level 13 → 14

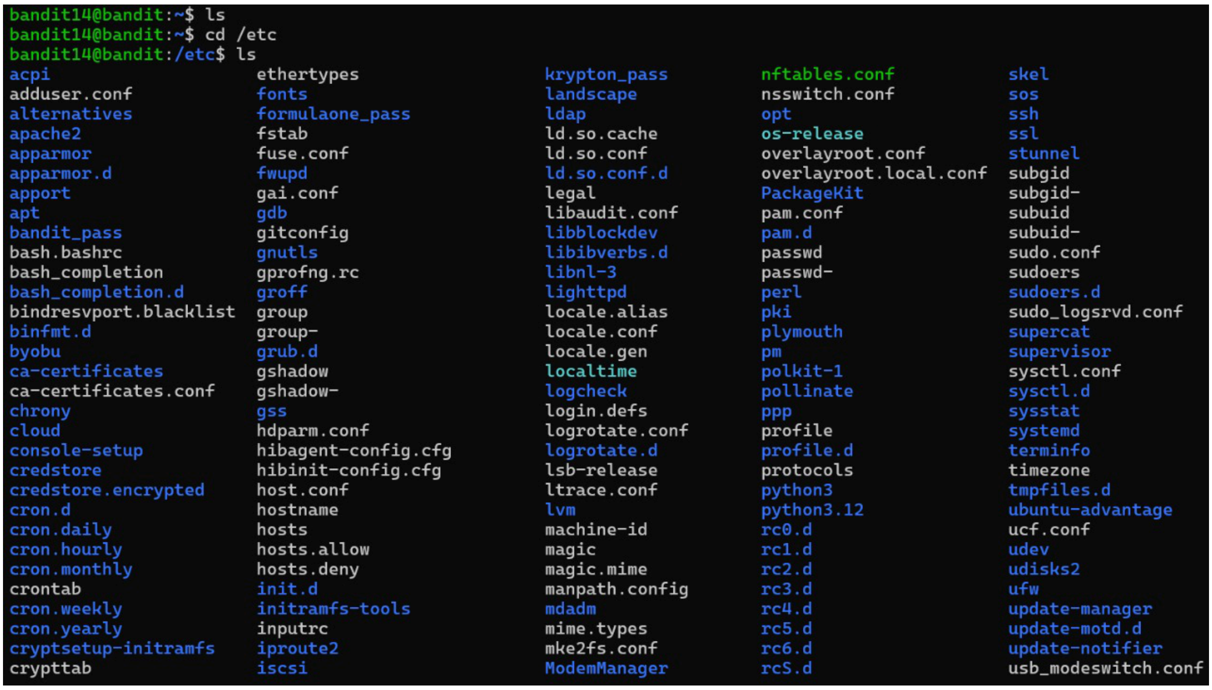
1. Use private key to login:

```
ssh -i sshkey.private bandit14@localhost
```

2. Read password from:

```
cat /etc/bandit_pass/bandit14
```

3. Save the password shown



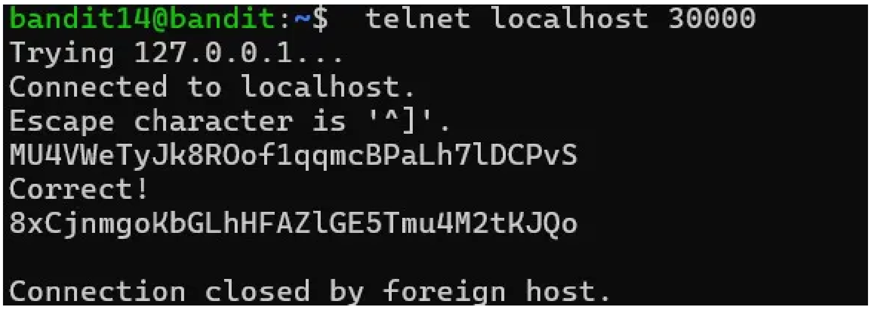
```
bandit14@bandit:~$ ls
bandit14@bandit:~$ cd /etc
bandit14@bandit:/etc$ ls
acpi                    ethertypes                  krypton_pass         nftables.conf           skel
adduser.conf            fonts                       landscape            nsswitch.conf           sos
alternatives            formulaone_pass             ldap                 opt                     ssh
apache2                 fstab                       ld.so.cache          os-release              ssl
apparmor                fuse.conf                   ld.so.conf           overlayroot.conf        stunnel
apparmor.d              fwupd                       ld.so.conf.d         overlayroot.local.conf  subgid
apport                  gai.conf                    legal                PackageKit              subgid-
apt                     gdb                         libaudit.conf        pam.conf                subuid
bandit_pass             gitconfig                   libblockdev          pam.d                   subuid-
bash.bashrc             gnutls                      libibverbs.d         passwd                  sudo.conf
bash_completion         gprofng.rc                  libnl-3              passwd-                 sudoers
bash_completion.d       groff                       lighttpd             perl                    sudoers.d
bindresvport.blacklist  group                       locale.alias         pki                     sudo_logsrvd.conf
binfmt.d                group-                      locale.conf          plymouth                supercat
byobu                   grub.d                      locale.gen           pm                      supervisor
ca-certificates         gshadow                     localtime            polkit-1                sysctl.conf
ca-certificates.conf    gshadow-                    logcheck             pollinate               sysctl.d
chrony                  gss                         login.defs           ppp                     sysstat
cloud                   hdparm.conf                 logrotate.conf       profile                 systemd
console-setup           hibagent-config.cfg         logrotate.d          profile.d               terminfo
credstore               hibinit-config.cfg          lsb-release          protocols               timezone
credstore.encrypted     host.conf                   ltrace.conf          python3                 tmpfiles.d
cron.d                  hostname                    lvm                  python3.12              ubuntu-advantage
cron.daily              hosts                       machine-id           rc0.d                   ucf.conf
cron.hourly             hosts.allow                 magic                rc1.d                   udev
cron.monthly            hosts.deny                  magic.mime           rc2.d                   udisks2
crontab                 init.d                      manpath.config       rc3.d                   ufw
cron.weekly             initramfs-tools             mdadm                rc4.d                   update-manager
cron.yearly             inputrc                     mime.types           rc5.d                   update-motd.d
cryptsetup-initramfs    iproute2                    mke2fs.conf          rc6.d                   update-notifier
crypttab                iscsi                       ModemManager         rcS.d                   usb_modeswitch.conf
```

Level 14 → 15

1. Connect to port 30000:

```
nc localhost 30000
```

2. Save the password shown



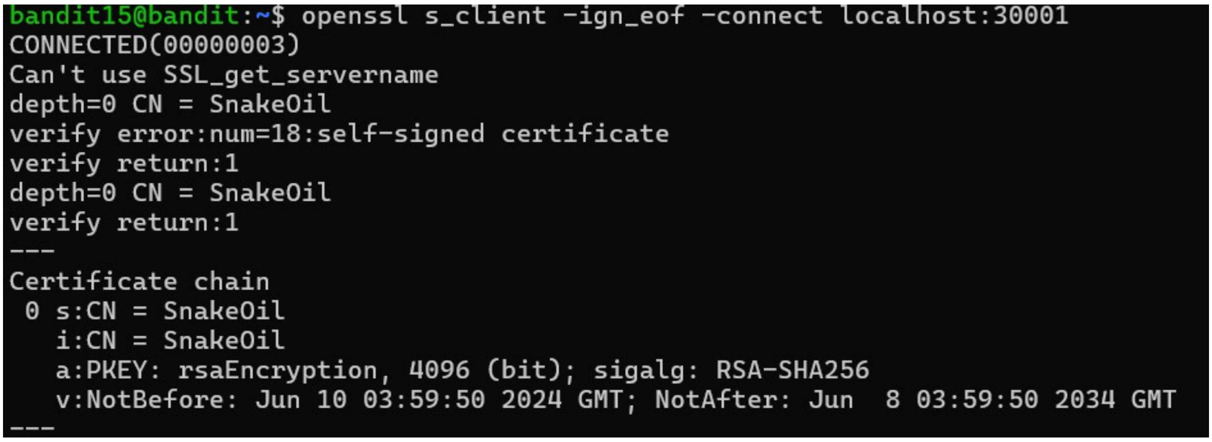
```
bandit14@bandit:~$  telnet localhost 30000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS
Correct!
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo

Connection closed by foreign host.
```

Level 15 → 16

1. Connect using SSL:

```
openssl s_client -connect localhost:30001
```

2. Save the password shown



```
bandit15@bandit:~$ openssl s_client -ign_eof -connect localhost:30001
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 CN = SnakeOil
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN = SnakeOil
verify return:1
---
Certificate chain
 0 s:CN = SnakeOil
   i:CN = SnakeOil
   a:PKEY: rsaEncryption, 4096 (bit); sigalg: RSA-SHA256
   v:NotBefore: Jun 10 03:59:50 2024 GMT; NotAfter: Jun  8 03:59:50 2034 GMT
---
```

Level 16 → 17

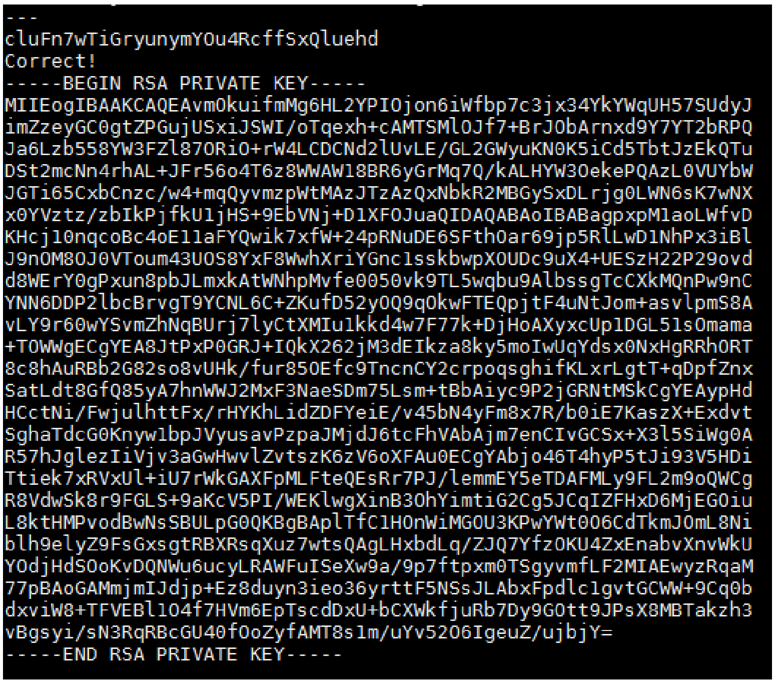
1. Scan ports:

```
nmap -p 31000-32000 localhost
```

2. Connect to correct SSL port:

```
openssl s_client -connect localhost:31790
```

3. Save the password shown



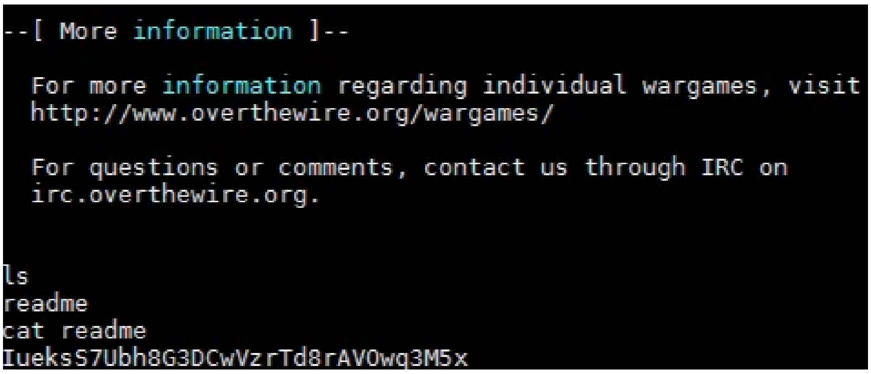
```
---
cluFn7wTiGryunymYOu4RcffSxQluehd
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMlOJf7+BrJObArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl87ORiO+rW4LCDCNd2lUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW3OekePQAzL0VUYbW
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-----
```

Level 17 → 18

1. Compare password files:

```
diff passwords.old passwords.new
```

2. Save the password shown



```
--[ More information ]--

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

  For questions or comments, contact us through IRC on
  irc.overthewire.org.


ls
readme
cat readme
IueksS7Ubh8G3DCwVzrTd8rAVOwq3M5x
```

Level 18 → 19

1. Execute command directly via SSH:

```
ssh bandit18@localhost "cat readme"
```

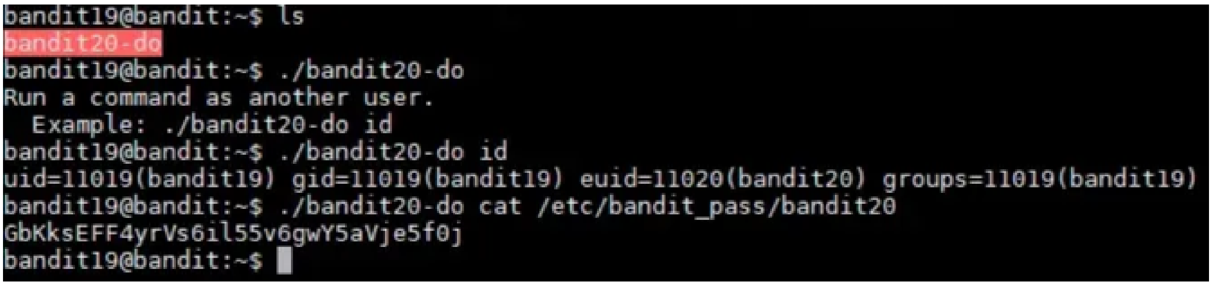
2. Save the password shown

Level 19 → 20

1. Use setuid binary:

```
./bandit20-do cat /etc/bandit_pass/bandit20
./bandit20-do cat /etc/bandit_pass/bandit20
```

2. Save the password shown



```
bandit19@bandit:~$ ls
bandit20-do
bandit19@bandit:~$ ./bandit20-do
Run a command as another user.
  Example: ./bandit20-do id
bandit19@bandit:~$ ./bandit20-do id
uid=11019(bandit19) gid=11019(bandit19) euid=11020(bandit20) groups=11019(bandit19)
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
GbKksEFF4yrVs6il55v6gwY5aVje5f0j
bandit19@bandit:~$ 
```