Department of Computer Science and Engineering

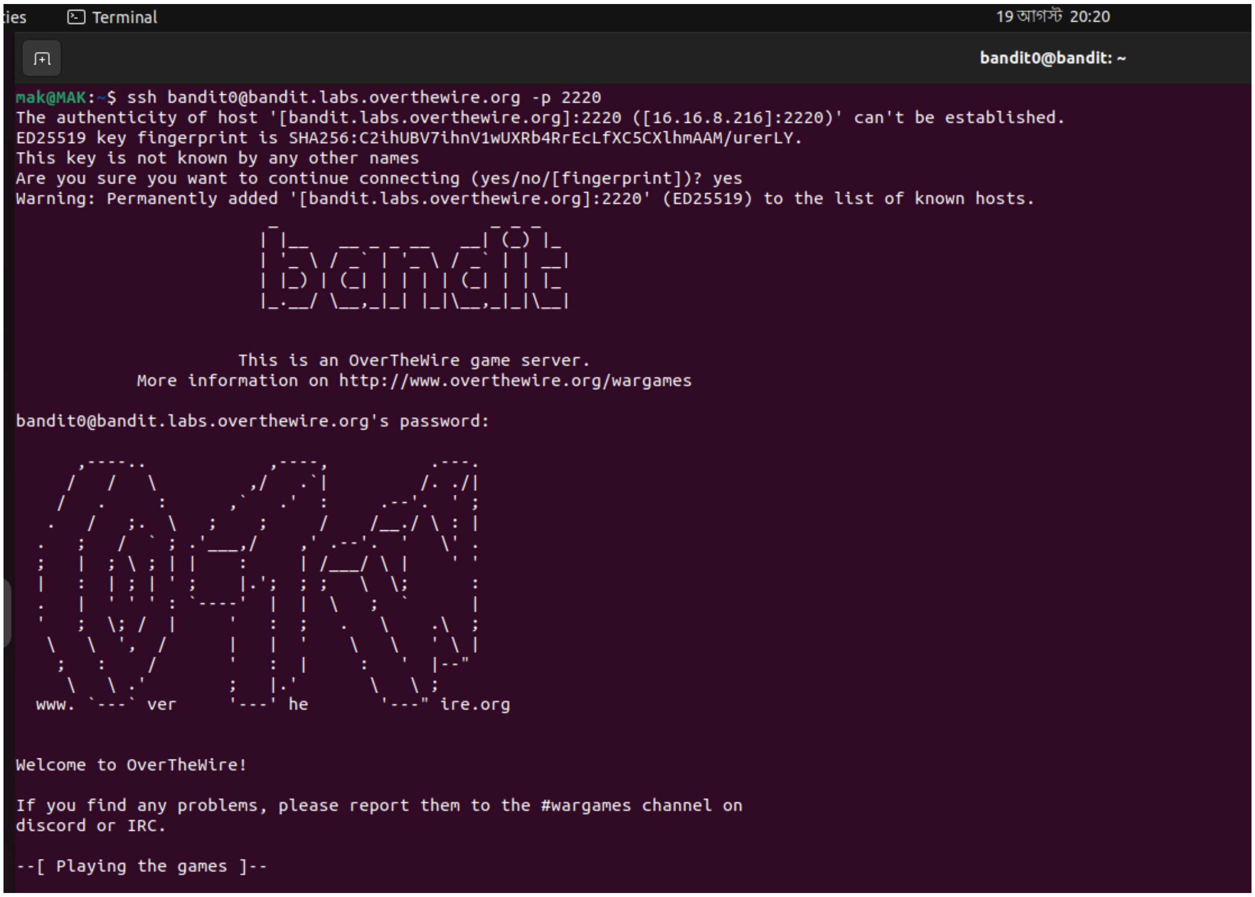
Islamic University of Technology (IUT)

A subsidiary organ of OIC

Laboratory Report

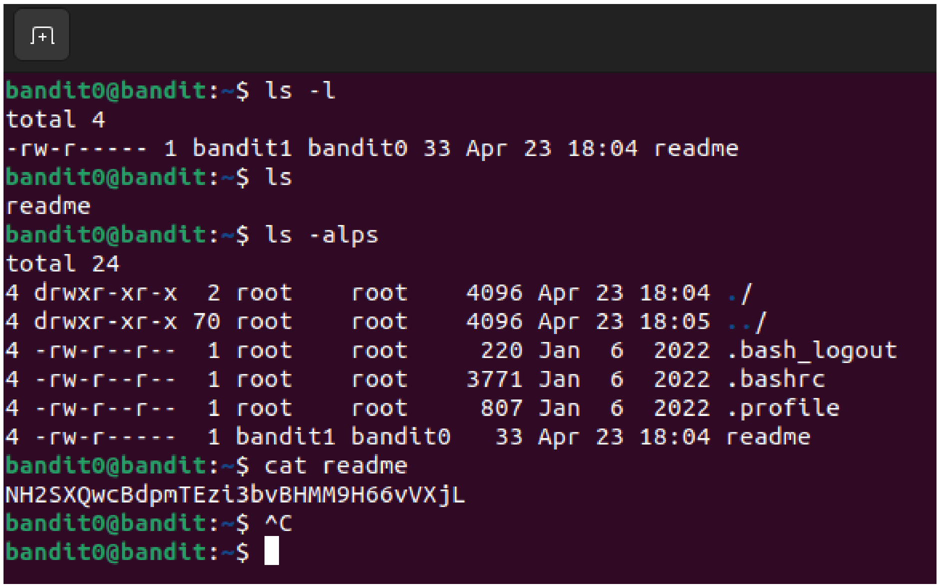
CSE 4504 : Software Security Lab

Name	**: Mashrur Ahsan**
Student ID	**: 200042115**
Section	**: 1 (SWE)**
Semester	**: Summer (5th)**
Academic Year	**: 2022-23**
Date of Submission	**: 22/08/2023**
Lab No	**: 1**



```
mak@MAK:~$ ssh bandit0@bandit.labs.overthewire.org -p 2220
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([16.16.8.216]: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
Warning: Permanently added '[bandit.labs.overthewire.org]:2220' (ED25519) to the list of known hosts.
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit0@bandit.labs.overthewire.org's password:

      ,----..            ,----,          .---.
     /   /   \         ,/   .`|         /. ./|
    /   .     :      ,`   .'  :     .--'.  ' ;
   .   /   ;.  \   ;    ;     /    /__./ \ : |
  .   ;   /  ` ; .'___,/    ,' .--'.  '   \' .
  ;   |  ; \ ; | |    :     | /___/ \ |    ' '
  |   :  | ; | ' ;    |.';  ; ;   \  \;      :
  .   |  ' ' ' : `----'  |  |  \   ;  `      |
  '   ;  \; /  |     '   :  ;   .   \    .\  ;
   \   \  ',  /      |   |  '    \   \   ' \ |
    ;   :    /       '   :  |     :   '  |--"
     \   \ .'        ;   |.'       \   \ ;
  www. `---` ver     '---' he       '---" ire.org


Welcome to OverTheWire!

If you find any problems, please report them to the #wargames channel on
discord or IRC.

--[ Playing the games ]--
```

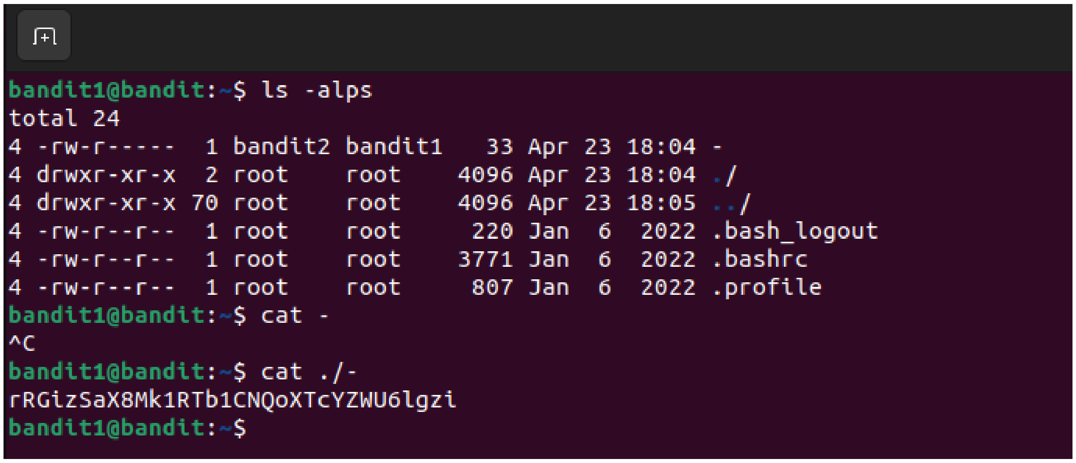
Level 0:



```
bandit0@bandit:~$ ls -l
total 4
-rw-r----- 1 bandit1 bandit0 33 Apr 23 18:04 readme
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ ls -alps
total 24
4 drwxr-xr-x  2 root    root    4096 Apr 23 18:04 ./
4 drwxr-xr-x 70 root    root    4096 Apr 23 18:05 ../
4 -rw-r--r--  1 root    root     220 Jan  6  2022 .bash_logout
4 -rw-r--r--  1 root    root    3771 Jan  6  2022 .bashrc
4 -rw-r--r--  1 root    root     807 Jan  6  2022 .profile
4 -rw-r-----  1 bandit1 bandit0   33 Apr 23 18:04 readme
bandit0@bandit:~$ cat readme
NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL
bandit0@bandit:~$ ^C
bandit0@bandit:~$ 
```

Password: bandit0

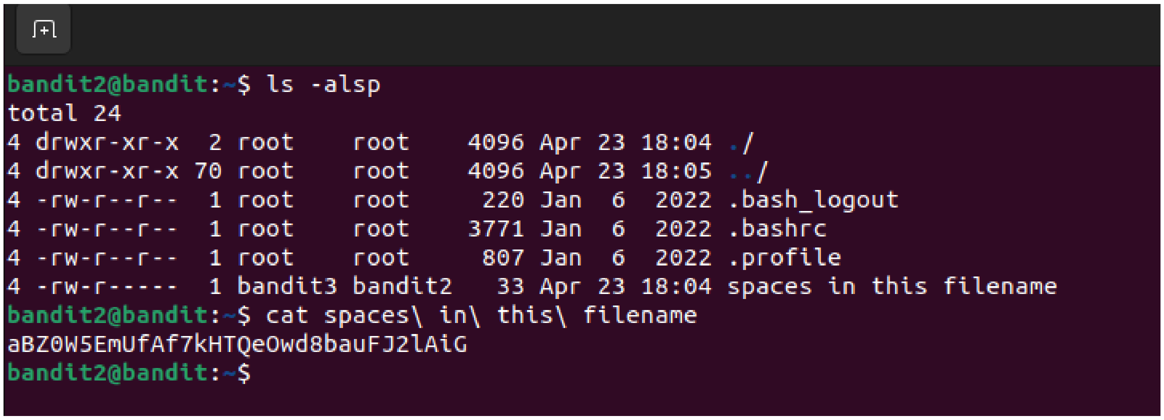
Level 1:



```
bandit1@bandit:~$ ls -alps
total 24
4 -rw-r-----  1 bandit2 bandit1   33 Apr 23 18:04 -
4 drwxr-xr-x  2 root    root    4096 Apr 23 18:04 ./
4 drwxr-xr-x 70 root    root    4096 Apr 23 18:05 ../
4 -rw-r--r--  1 root    root     220 Jan  6  2022 .bash_logout
4 -rw-r--r--  1 root    root    3771 Jan  6  2022 .bashrc
4 -rw-r--r--  1 root    root     807 Jan  6  2022 .profile
bandit1@bandit:~$ cat -
^C
bandit1@bandit:~$ cat ./-
rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi
bandit1@bandit:~$
```

Password: NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL

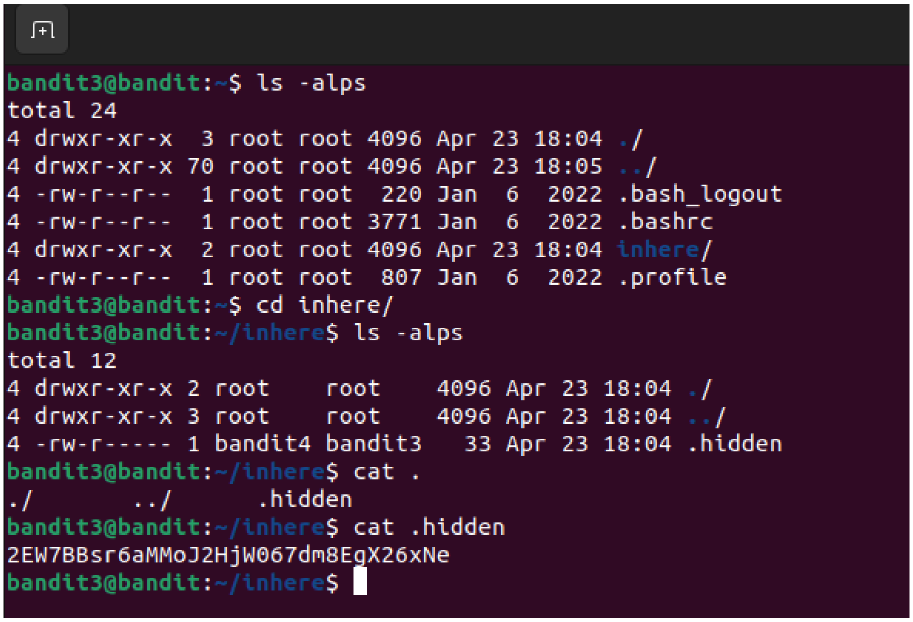
Level 2:



```
bandit2@bandit:~$ ls -alsp
total 24
4 drwxr-xr-x  2 root    root    4096 Apr 23 18:04 ./
4 drwxr-xr-x 70 root    root    4096 Apr 23 18:05 ../
4 -rw-r--r--  1 root    root     220 Jan  6  2022 .bash_logout
4 -rw-r--r--  1 root    root    3771 Jan  6  2022 .bashrc
4 -rw-r--r--  1 root    root     807 Jan  6  2022 .profile
4 -rw-r-----  1 bandit3 bandit2   33 Apr 23 18:04 spaces in this filename
bandit2@bandit:~$ cat spaces\ in\ this\ filename
aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG
bandit2@bandit:~$
```

Password: rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi

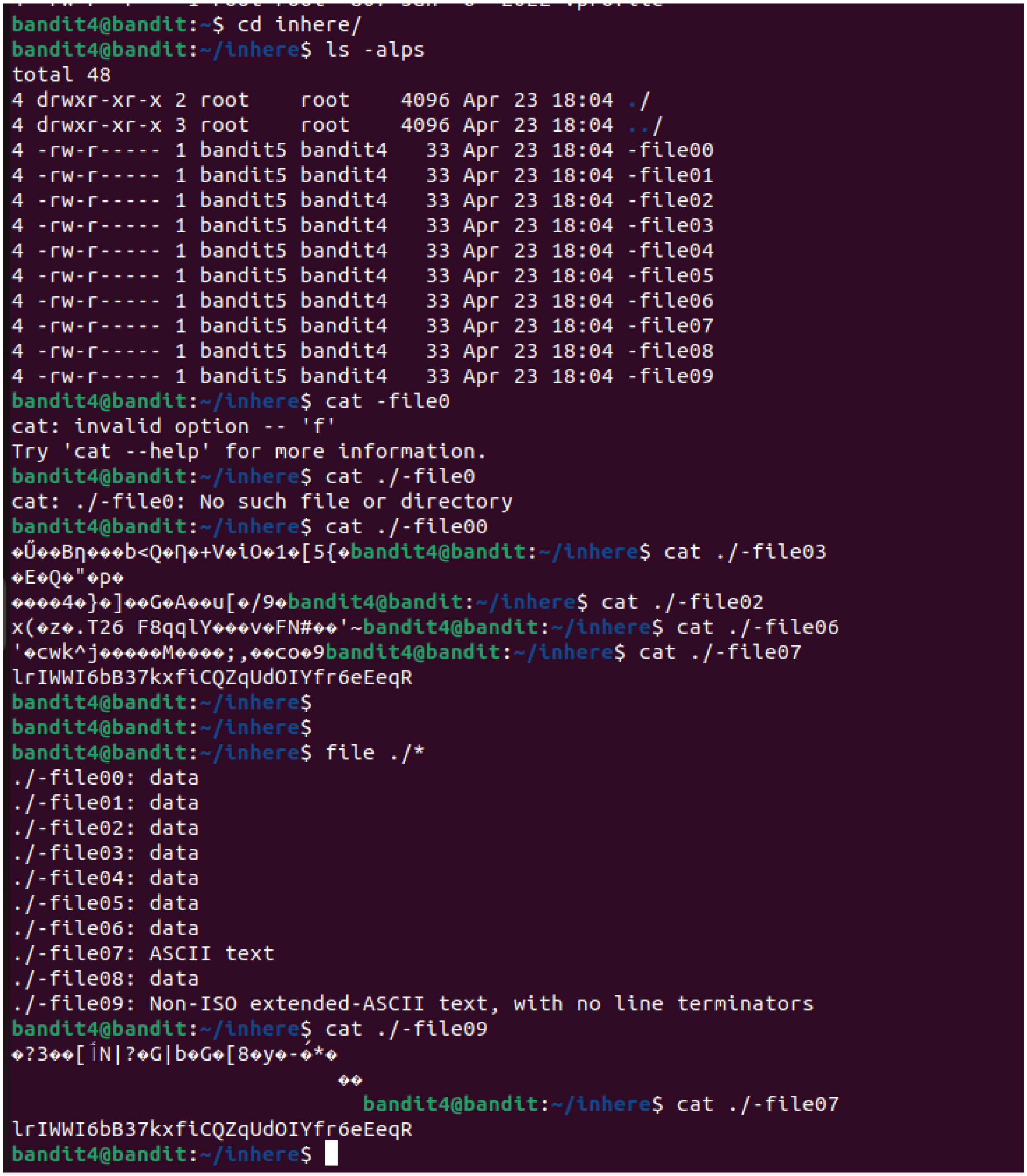
Level 4:



```
bandit3@bandit:~$ ls -alps
total 24
4 drwxr-xr-x  3 root root 4096 Apr 23 18:04 ./
4 drwxr-xr-x 70 root root 4096 Apr 23 18:05 ../
4 -rw-r--r--  1 root root  220 Jan  6  2022 .bash_logout
4 -rw-r--r--  1 root root 3771 Jan  6  2022 .bashrc
4 drwxr-xr-x  2 root root 4096 Apr 23 18:04 inhere/
4 -rw-r--r--  1 root root  807 Jan  6  2022 .profile
bandit3@bandit:~$ cd inhere/
bandit3@bandit:~/inhere$ ls -alps
total 12
4 drwxr-xr-x 2 root    root    4096 Apr 23 18:04 ./
4 drwxr-xr-x 3 root    root    4096 Apr 23 18:04 ../
4 -rw-r----- 1 bandit4 bandit3   33 Apr 23 18:04 .hidden
bandit3@bandit:~/inhere$ cat .
./         ../        .hidden
bandit3@bandit:~/inhere$ cat .hidden
2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe
bandit3@bandit:~/inhere$ 
```

Password: aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG

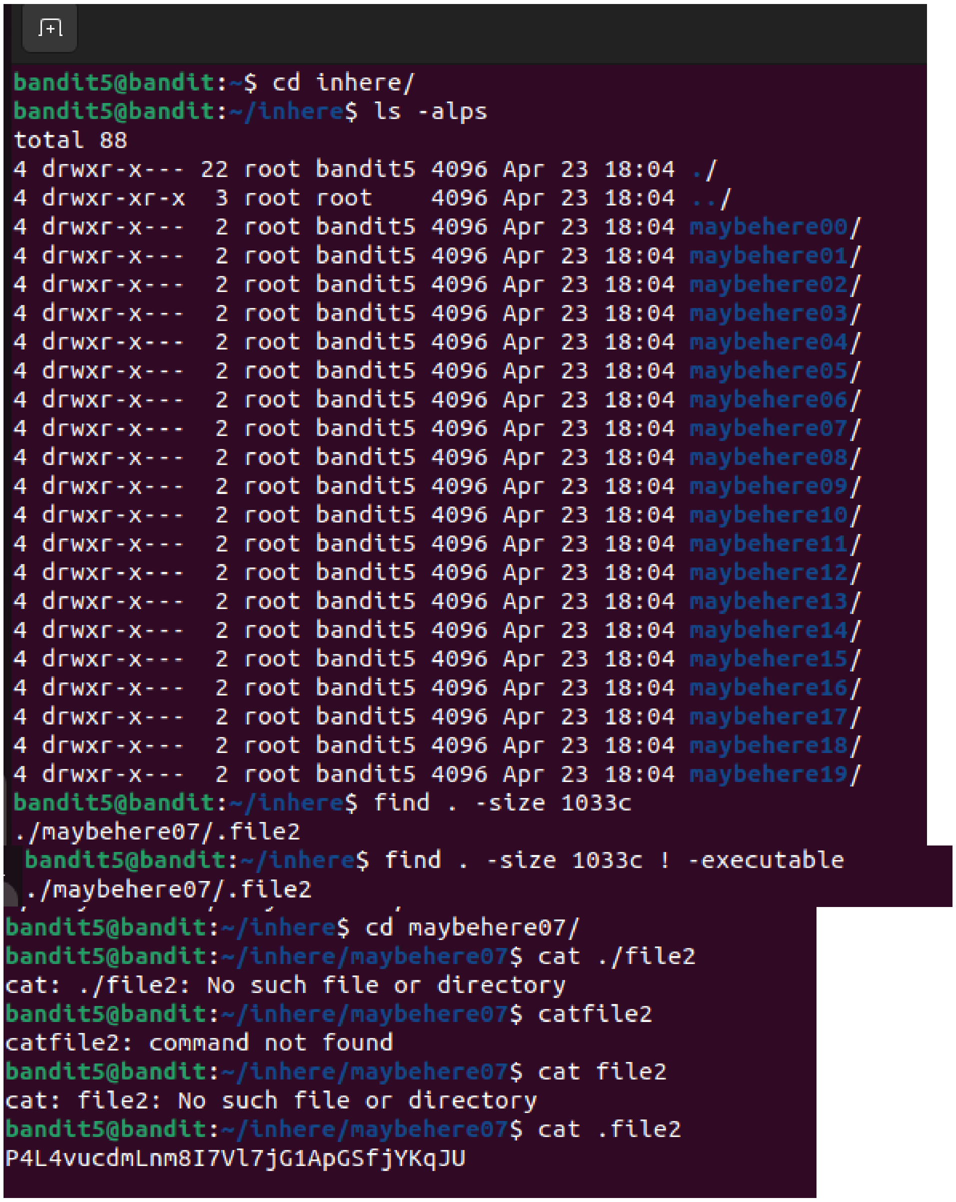
Level 5:



```
bandit4@bandit:~$ cd inhere/
bandit4@bandit:~/inhere$ ls -alps
total 48
4 drwxr-xr-x 2 root    root    4096 Apr 23 18:04 ./
4 drwxr-xr-x 3 root    root    4096 Apr 23 18:04 ../
4 -rw-r----- 1 bandit5 bandit4   33 Apr 23 18:04 -file00
4 -rw-r----- 1 bandit5 bandit4   33 Apr 23 18:04 -file01
4 -rw-r----- 1 bandit5 bandit4   33 Apr 23 18:04 -file02
4 -rw-r----- 1 bandit5 bandit4   33 Apr 23 18:04 -file03
4 -rw-r----- 1 bandit5 bandit4   33 Apr 23 18:04 -file04
4 -rw-r----- 1 bandit5 bandit4   33 Apr 23 18:04 -file05
4 -rw-r----- 1 bandit5 bandit4   33 Apr 23 18:04 -file06
4 -rw-r----- 1 bandit5 bandit4   33 Apr 23 18:04 -file07
4 -rw-r----- 1 bandit5 bandit4   33 Apr 23 18:04 -file08
4 -rw-r----- 1 bandit5 bandit4   33 Apr 23 18:04 -file09
bandit4@bandit:~/inhere$ cat -file0
cat: invalid option -- 'f'
Try 'cat --help' for more information.
bandit4@bandit:~/inhere$ cat ./-file0
cat: ./-file0: No such file or directory
bandit4@bandit:~/inhere$ cat ./-file00
�Ű��Bη���b<Q�Ŋ�+V�iO�1�[5{�bandit4@bandit:~/inhere$ cat ./-file03
�E�Q�"�p�
����4�}�]��G�A��u[�/9�bandit4@bandit:~/inhere$ cat ./-file02
x(�z�.T26 F8qqlY���v�FN#��'~bandit4@bandit:~/inhere$ cat ./-file06
'�cwk^j�����M����;,��co�9bandit4@bandit:~/inhere$ cat ./-file07
lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR
bandit4@bandit:~/inhere$
bandit4@bandit:~/inhere$
bandit4@bandit:~/inhere$ file ./*
./-file00: data
./-file01: data
./-file02: data
./-file03: data
./-file04: data
./-file05: data
./-file06: data
./-file07: ASCII text
./-file08: data
./-file09: Non-ISO extended-ASCII text, with no line terminators
bandit4@bandit:~/inhere$ cat ./-file09
�?3��[ÍN|?�G|b�G�[8�y�-�́*�
                          ��
                            bandit4@bandit:~/inhere$ cat ./-file07
lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR
bandit4@bandit:~/inhere$ █
```

Password: aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG

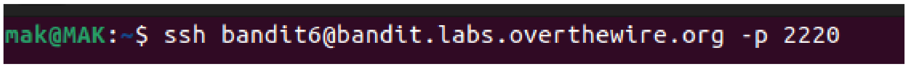
Level 6:



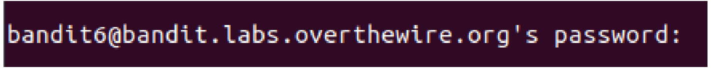
```
bandit5@bandit:~$ cd inhere/
bandit5@bandit:~/inhere$ ls -alps
total 88
4 drwxr-x--- 22 root bandit5 4096 Apr 23 18:04 ./
4 drwxr-xr-x  3 root root    4096 Apr 23 18:04 ../
4 drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere00/
4 drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere01/
4 drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere02/
4 drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere03/
4 drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere04/
4 drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere05/
4 drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere06/
4 drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere07/
4 drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere08/
4 drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere09/
4 drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere10/
4 drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere11/
4 drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere12/
4 drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere13/
4 drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere14/
4 drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere15/
4 drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere16/
4 drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere17/
4 drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere18/
4 drwxr-x---  2 root bandit5 4096 Apr 23 18:04 maybehere19/
bandit5@bandit:~/inhere$ find . -size 1033c
./maybehere07/.file2
bandit5@bandit:~/inhere$ find . -size 1033c ! -executable
./maybehere07/.file2
bandit5@bandit:~/inhere$ cd maybehere07/
bandit5@bandit:~/inhere/maybehere07$ cat ./file2
cat: ./file2: No such file or directory
bandit5@bandit:~/inhere/maybehere07$ catfile2
catfile2: command not found
bandit5@bandit:~/inhere/maybehere07$ cat file2
cat: file2: No such file or directory
bandit5@bandit:~/inhere/maybehere07$ cat .file2
P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU
```

Password: lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR

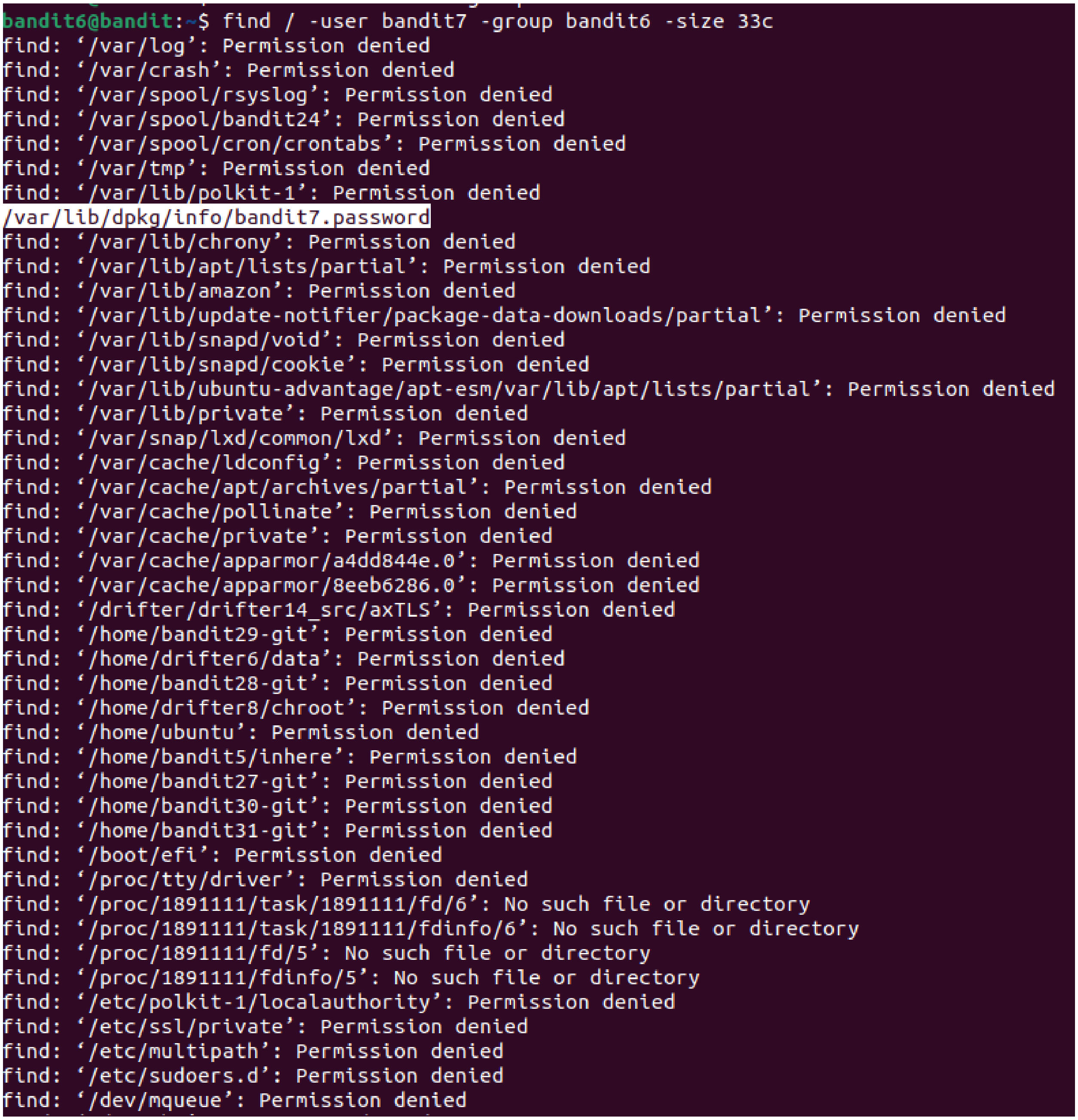
Level 7:



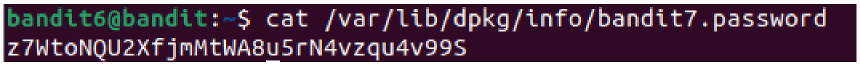
```
mak@MAK:~$ ssh bandit6@bandit.labs.overthewire.org -p 2220
```



```
bandit6@bandit.labs.overthewire.org's password:
```



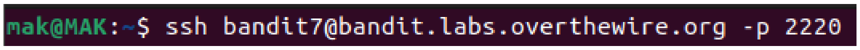
```
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c
find: ‘/var/log’: Permission denied
find: ‘/var/crash’: Permission denied
find: ‘/var/spool/rsyslog’: Permission denied
find: ‘/var/spool/bandit24’: Permission denied
find: ‘/var/spool/cron/crontabs’: Permission denied
find: ‘/var/tmp’: Permission denied
find: ‘/var/lib/polkit-1’: Permission denied
/var/lib/dpkg/info/bandit7.password
find: ‘/var/lib/chrony’: Permission denied
find: ‘/var/lib/apt/lists/partial’: Permission denied
find: ‘/var/lib/amazon’: Permission denied
find: ‘/var/lib/update-notifier/package-data-downloads/partial’: Permission denied
find: ‘/var/lib/snapd/void’: Permission denied
find: ‘/var/lib/snapd/cookie’: Permission denied
find: ‘/var/lib/ubuntu-advantage/apt-esm/var/lib/apt/lists/partial’: Permission denied
find: ‘/var/lib/private’: Permission denied
find: ‘/var/snap/lxd/common/lxd’: 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/a4dd844e.0’: Permission denied
find: ‘/var/cache/apparmor/8eeb6286.0’: Permission denied
find: ‘/drifter/drifter14_src/axTLS’: Permission denied
find: ‘/home/bandit29-git’: Permission denied
find: ‘/home/drifter6/data’: Permission denied
find: ‘/home/bandit28-git’: Permission denied
find: ‘/home/drifter8/chroot’: Permission denied
find: ‘/home/ubuntu’: Permission denied
find: ‘/home/bandit5/inhere’: Permission denied
find: ‘/home/bandit27-git’: Permission denied
find: ‘/home/bandit30-git’: Permission denied
find: ‘/home/bandit31-git’: Permission denied
find: ‘/boot/efi’: Permission denied
find: ‘/proc/tty/driver’: Permission denied
find: ‘/proc/1891111/task/1891111/fd/6’: No such file or directory
find: ‘/proc/1891111/task/1891111/fdinfo/6’: No such file or directory
find: ‘/proc/1891111/fd/5’: No such file or directory
find: ‘/proc/1891111/fdinfo/5’: No such file or directory
find: ‘/etc/polkit-1/localauthority’: Permission denied
find: ‘/etc/ssl/private’: Permission denied
find: ‘/etc/multipath’: Permission denied
find: ‘/etc/sudoers.d’: Permission denied
find: ‘/dev/mqueue’: Permission denied
```



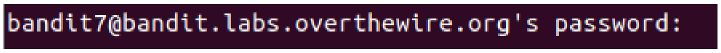
```
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S
```

Password: P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU

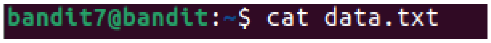
Level 8:



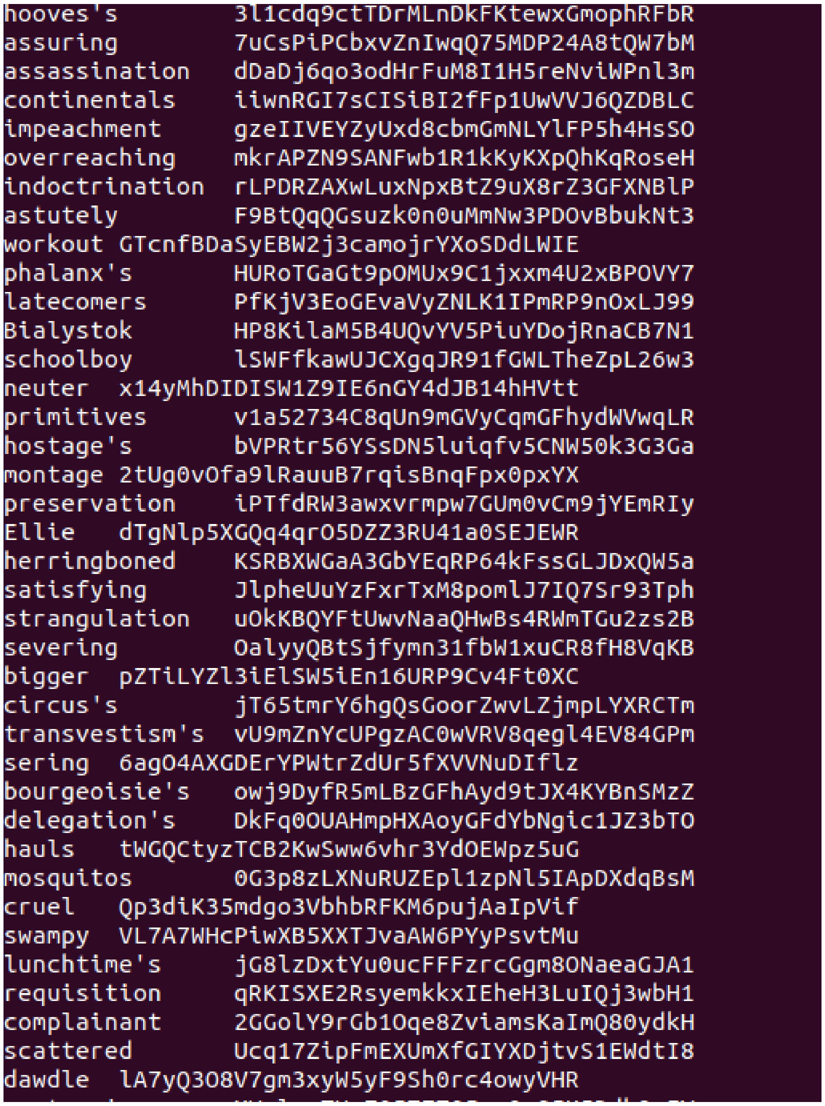
```
mak@MAK:~$ ssh bandit7@bandit.labs.overthewire.org -p 2220
```



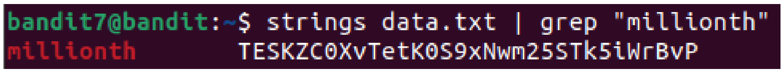
```
bandit7@bandit.labs.overthewire.org's password:
```



```
bandit7@bandit:~$ cat data.txt
```



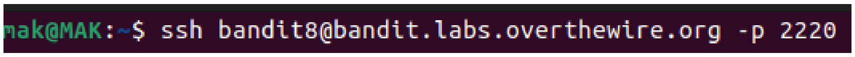
```
hooves's        3l1cdq9ctTDrMLnDkFKtewxGmophRFbR
assuring        7uCsPiPCbxvZnIwqQ75MDP24A8tQW7bM
assassination   dDaDj6qo3odHrFuM8I1H5reNviWPnl3m
continentals    iiwnRGI7sCISiBI2fFp1UwVVJ6QZDBLC
impeachment     gzeIIVEYZyUxd8cbmGmNLYlFP5h4HsSO
overreaching    mkrAPZN9SANFwb1R1kKyKXpQhKqRoseH
indoctrination  rLPDRZAXwLuxNpxBtZ9uX8rZ3GFXNBlP
astutely        F9BtQqQGsuzk0n0uMmNw3PDOvBbukNt3
workout GTcnfBDaSyEBW2j3camojrYXoSDdLWIE
phalanx's       HURoTGaGt9pOMUx9C1jxxm4U2xBPOVY7
latecomers      PfKjV3EoGEvaVyZNLK1IPmRP9nOxLJ99
Bialystok       HP8KilaM5B4UQvYV5PiuYDojRnaCB7N1
schoolboy       lSWFfkawUJCXgqJR91fGWLTheZpL26w3
neuter  x14yMhDIDISW1Z9IE6nGY4dJB14hHVtt
primitives      v1a52734C8qUn9mGVyCqmGFhydWVwqLR
hostage's       bVPRtr56YSsDN5luiqfv5CNW50k3G3Ga
montage 2tUg0vOfa9lRauuB7rqisBnqFpx0pxYX
preservation    iPTfdRW3awxvrmpw7GUm0vCm9jYEmRIy
Ellie   dTgNlp5XGQq4qrO5DZZ3RU41a0SEJEWR
herringboned    KSRBXWGaA3GbYEqRP64kFssGLJDxQW5a
satisfying      JlpheUuYzFxrTxM8pomlJ7IQ7Sr93Tph
strangulation   uOkKBQYFtUwvNaaQHwBs4RWmTGu2zs2B
severing        OalyyQBtSjfymn31fbW1xuCR8fH8VqKB
bigger  pZTiLYZl3iElSW5iEn16URP9Cv4Ft0XC
circus's        jT65tmrY6hgQsGoorZwvLZjmpLYXRCTm
transvestism's  vU9mZnYcUPgzAC0wVRV8qegl4EV84GPm
sering  6agO4AXGDErYPWtrZdUr5fXVVNuDIflz
bourgeoisie's   owj9DyfR5mLBzGFhAyd9tJX4KYBnSMzZ
delegation's    DkFq0OUAHmpHXAoyGFdYbNgic1JZ3bTO
hauls   tWGQCtyzTCB2KwSww6vhr3YdOEWpz5uG
mosquitos       0G3p8zLXNuRUZEpl1zpNl5IApDXdqBsM
cruel   Qp3diK35mdgo3VbhbRFKM6pujAaIpVif
swampy  VL7A7WHcPiwXB5XXTJvaAW6PYyPsvtMu
lunchtime's     jG8lzDxtYu0ucFFFzrcGgm8ONaeaGJA1
requisition     qRKISXE2RsyemkkxIEheH3LuIQj3wbH1
complainant     2GGolY9rGb1Oqe8ZviamsKaImQ80ydkH
scattered       Ucq17ZipFmEXUmXfGIYXDjtvS1EWdtI8
dawdle  lA7yQ3O8V7gm3xyW5yF9Sh0rc4owyVHR
```



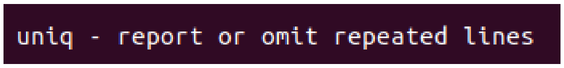
```
bandit7@bandit:~$ strings data.txt | grep "millionth"
millionth       TESKZC0XvTetK0S9xNwm25STk5iWrBvP
```

Password: z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S

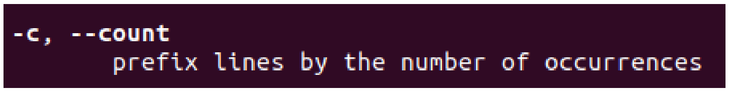
Level 9:



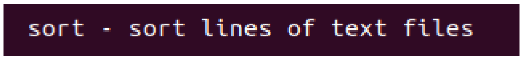
```
mak@MAK:~$ ssh bandit8@bandit.labs.overthewire.org -p 2220
```



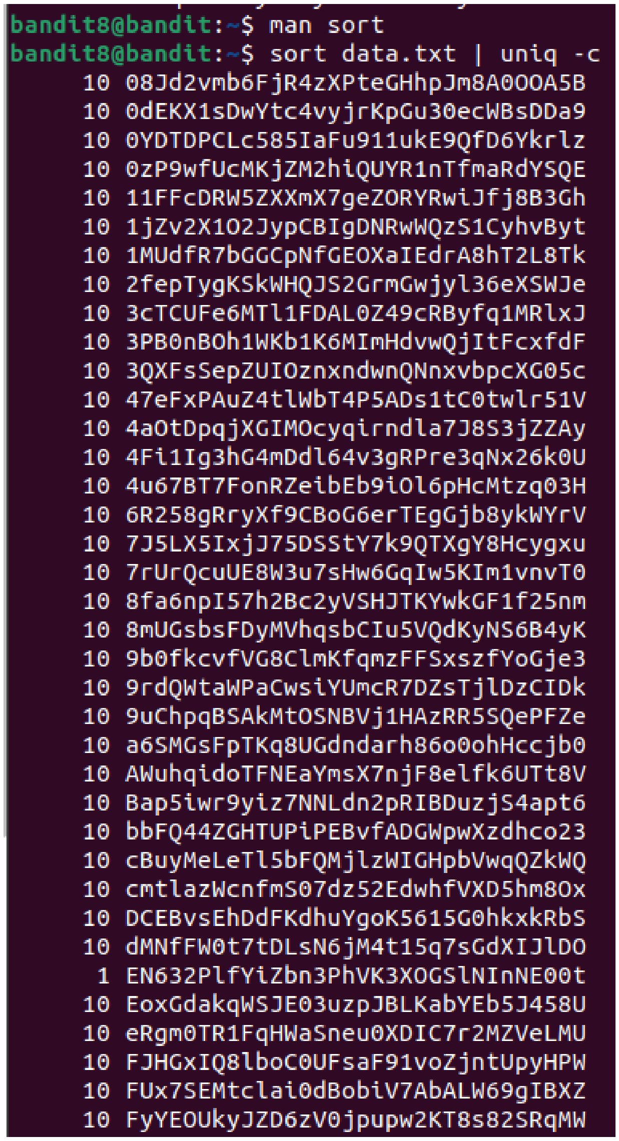
```
uniq - report or omit repeated lines
```



```
-c, --count
       prefix lines by the number of occurrences
```



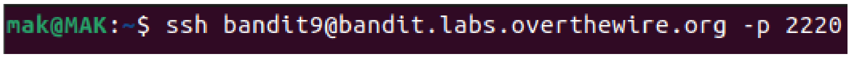
```
sort - sort lines of text files
```



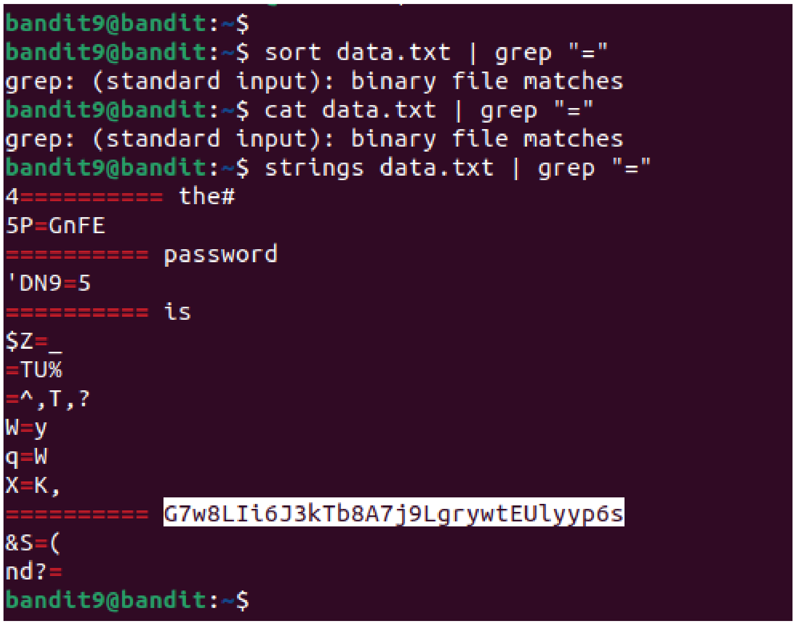
```
bandit8@bandit:~$ man sort
bandit8@bandit:~$ sort data.txt | uniq -c
     10 08Jd2vmb6FjR4zXPteGHhpJm8A0OOA5B
     10 0dEKX1sDwYtc4vyjrKpGu30ecWBsDDa9
     10 0YDTDPCLc585IaFu911ukE9QfD6Ykrlz
     10 0zP9wfUcMKjZM2hiQUYR1nTfmaRdYSQE
     10 11FFcDRW5ZXXmX7geZORYRwiJfj8B3Gh
     10 1jZv2X1O2JypCBIgDNRwWQzS1CyhvByt
     10 1MUdfR7bGGCpNfGEOXaIEdrA8hT2L8Tk
     10 2fepTygKSkWHQJS2GrmGwjyl36eXSWJe
     10 3cTCUFe6MTl1FDAL0Z49cRByfq1MRlxJ
     10 3PB0nBOh1WKb1K6MImHdvwQjItFcxfdF
     10 3QXFsSepZUIOznxndwnQNnxvbpcXG05c
     10 47eFxPAuZ4tlWbT4P5ADs1tC0twlr51V
     10 4aOtDpqjXGIMOcyqirndla7J8S3jZZAy
     10 4Fi1Ig3hG4mDdl64v3gRPre3qNx26k0U
     10 4u67BT7FonRZeibEb9iOl6pHcMtzq03H
     10 6R258gRryXf9CBoG6erTEgGjb8ykWYrV
     10 7J5LX5IxjJ75DSStY7k9QTXgY8Hcygxu
     10 7rUrQcuUE8W3u7sHw6GqIw5KIm1vnvT0
     10 8fa6npI57h2Bc2yVSHJTKYwkGF1f25nm
     10 8mUGsbsFDyMVhqsbCIu5VQdKyNS6B4yK
     10 9b0fkcvfVG8ClmKfqmzFFSxszfYoGje3
     10 9rdQWtaWPaCwsiYUmcR7DZsTjlDzCIDk
     10 9uChpqBSAkMtOSNBVj1HAzRR5SQePFZe
     10 a6SMGsFpTKq8UGdndarh86o0ohHccjb0
     10 AWuhqidoTFNEaYmsX7njF8elfk6UTt8V
     10 Bap5iwr9yiz7NNLdn2pRIBDuzjS4apt6
     10 bbFQ44ZGHTUPiPEBvfADGWpwXzdhco23
     10 cBuyMeLeTl5bFQMjlzWIGHpbVwqQZkWQ
     10 cmtlazWcnfmS07dz52EdwhfVXD5hm8Ox
     10 DCEBvsEhDdFKdhuYgoK5615G0hkxkRbS
     10 dMNfFW0t7tDLsN6jM4t15q7sGdXIJlDO
      1 EN632PlfYiZbn3PhVK3XOGSlNInNE00t
     10 EoxGdakqWSJE03uzpJBLKabYEb5J458U
     10 eRgm0TR1FqHWaSneu0XDIC7r2MZVeLMU
     10 FJHGxIQ8lboC0UFsaF91voZjntUpyHPW
     10 FUx7SEMtclai0dBobiV7AbALW69gIBXZ
     10 FyYEOUkyJZD6zV0jpupw2KT8s82SRqMW
```

Password: TESKZC0XvTetK059xNwm25STk5iWrBvP

Level 10:



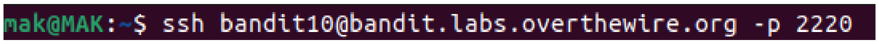
```
mak@MAK:~$ ssh bandit9@bandit.labs.overthewire.org -p 2220
```



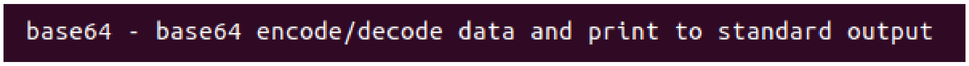
```
bandit9@bandit:~$
bandit9@bandit:~$ sort data.txt | grep "="
grep: (standard input): binary file matches
bandit9@bandit:~$ cat data.txt | grep "="
grep: (standard input): binary file matches
bandit9@bandit:~$ strings data.txt | grep "="
4========== the#
5P=GnFE
========== password
'DN9=5
========== is
$Z=_
=TU%
=^,T,?
W=y
q=W
X=K,
========== G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s
&S=(
nd?=
bandit9@bandit:~$
```

Password: EN632PlfYiZbn3PhVK3XOGSlNInNE00t

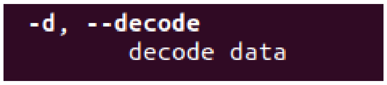
Level 11:



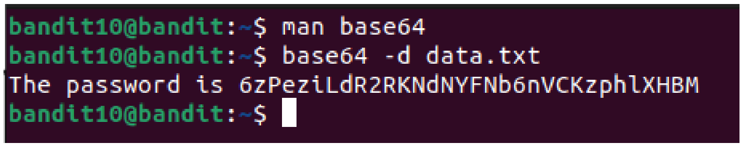
```
mak@MAK:~$ ssh bandit10@bandit.labs.overthewire.org -p 2220
```



```
base64 - base64 encode/decode data and print to standard output
```



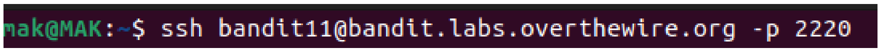
```
-d, --decode
       decode data
```



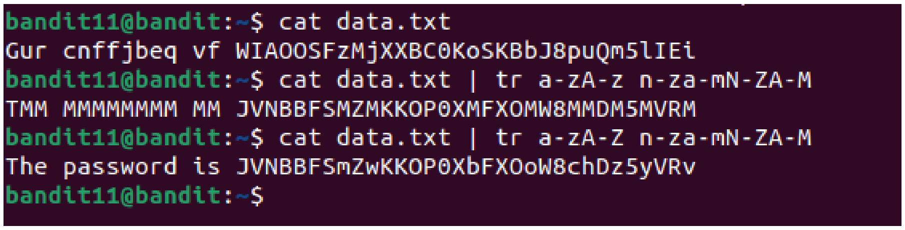
```
bandit10@bandit:~$ man base64
bandit10@bandit:~$ base64 -d data.txt
The password is 6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM
bandit10@bandit:~$ 
```

Password: G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s

Level 12:



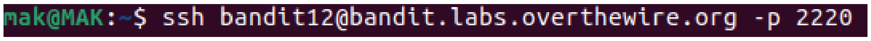
```
mak@MAK:~$ ssh bandit11@bandit.labs.overthewire.org -p 2220
```



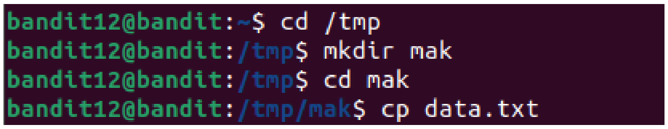
```
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf WIAOOSFzMjXXBC0KoSKBbJ8puQm5lIEi
bandit11@bandit:~$ cat data.txt | tr a-zA-z n-za-mN-ZA-M
TMM MMMMMMMM MM JVNBBFSMZMKKOP0XMFXOMW8MMDM5MVRM
bandit11@bandit:~$ cat data.txt | tr a-zA-Z n-za-mN-ZA-M
The password is JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv
bandit11@bandit:~$
```

Password: 6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM

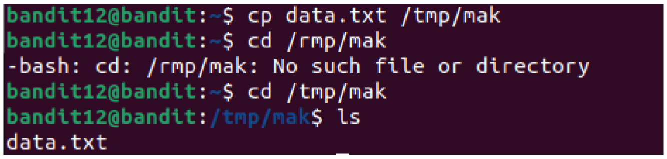
Level 13:



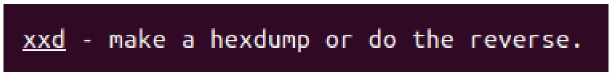
```
mak@MAK:~$ ssh bandit12@bandit.labs.overthewire.org -p 2220
```



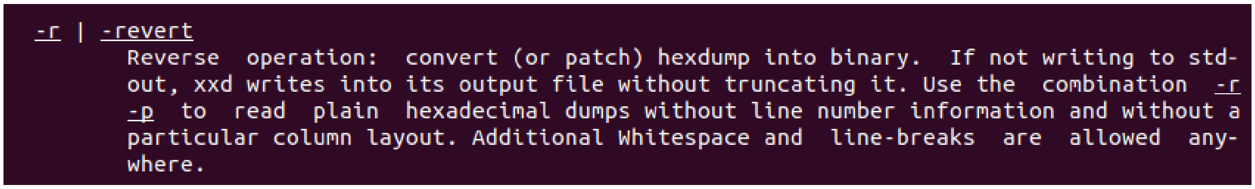
```
bandit12@bandit:~$ cd /tmp
bandit12@bandit:/tmp$ mkdir mak
bandit12@bandit:/tmp$ cd mak
bandit12@bandit:/tmp/mak$ cp data.txt
```



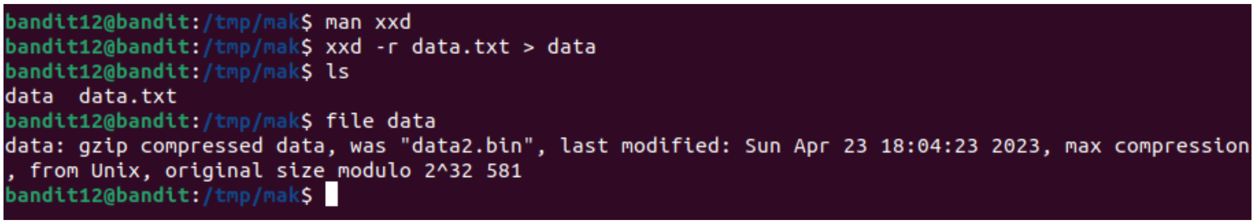
```
bandit12@bandit:~$ cp data.txt /tmp/mak
bandit12@bandit:~$ cd /rmp/mak
-bash: cd: /rmp/mak: No such file or directory
bandit12@bandit:~$ cd /tmp/mak
bandit12@bandit:/tmp/mak$ ls
data.txt
```



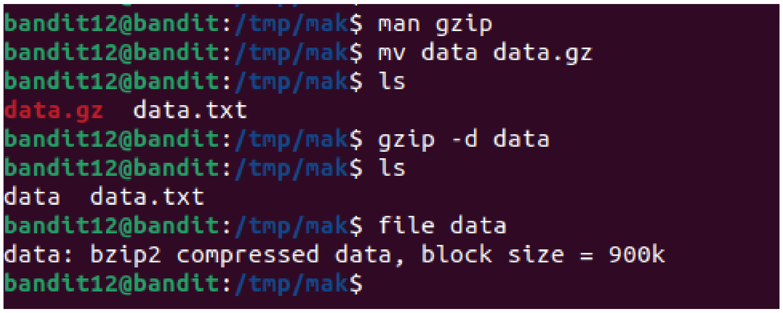
```
xxd - make a hexdump or do the reverse.
```



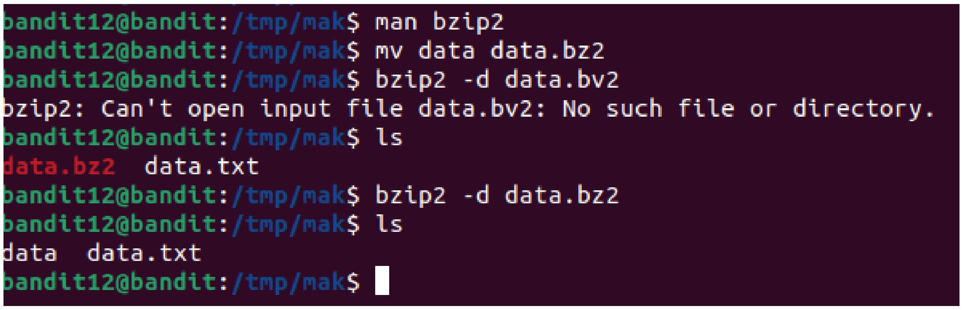
```
 -r | -revert
        Reverse  operation:  convert (or patch) hexdump into binary.  If not writing to std-
        out, xxd writes into its output file without truncating it. Use the  combination  -r
        -p  to  read  plain  hexadecimal dumps without line number information and without a
        particular column layout. Additional Whitespace and  line-breaks  are  allowed  any-
        where.
```



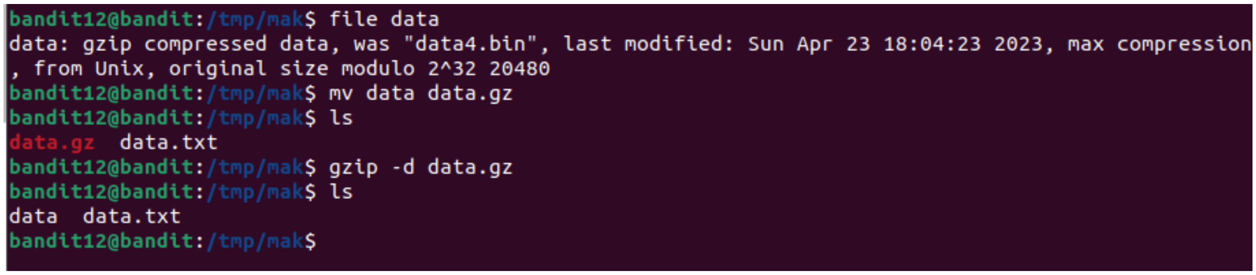
```
bandit12@bandit:/tmp/mak$ man xxd
bandit12@bandit:/tmp/mak$ xxd -r data.txt > data
bandit12@bandit:/tmp/mak$ ls
data  data.txt
bandit12@bandit:/tmp/mak$ file data
data: gzip compressed data, was "data2.bin", last modified: Sun Apr 23 18:04:23 2023, max compression
, from Unix, original size modulo 2^32 581
bandit12@bandit:/tmp/mak$
```



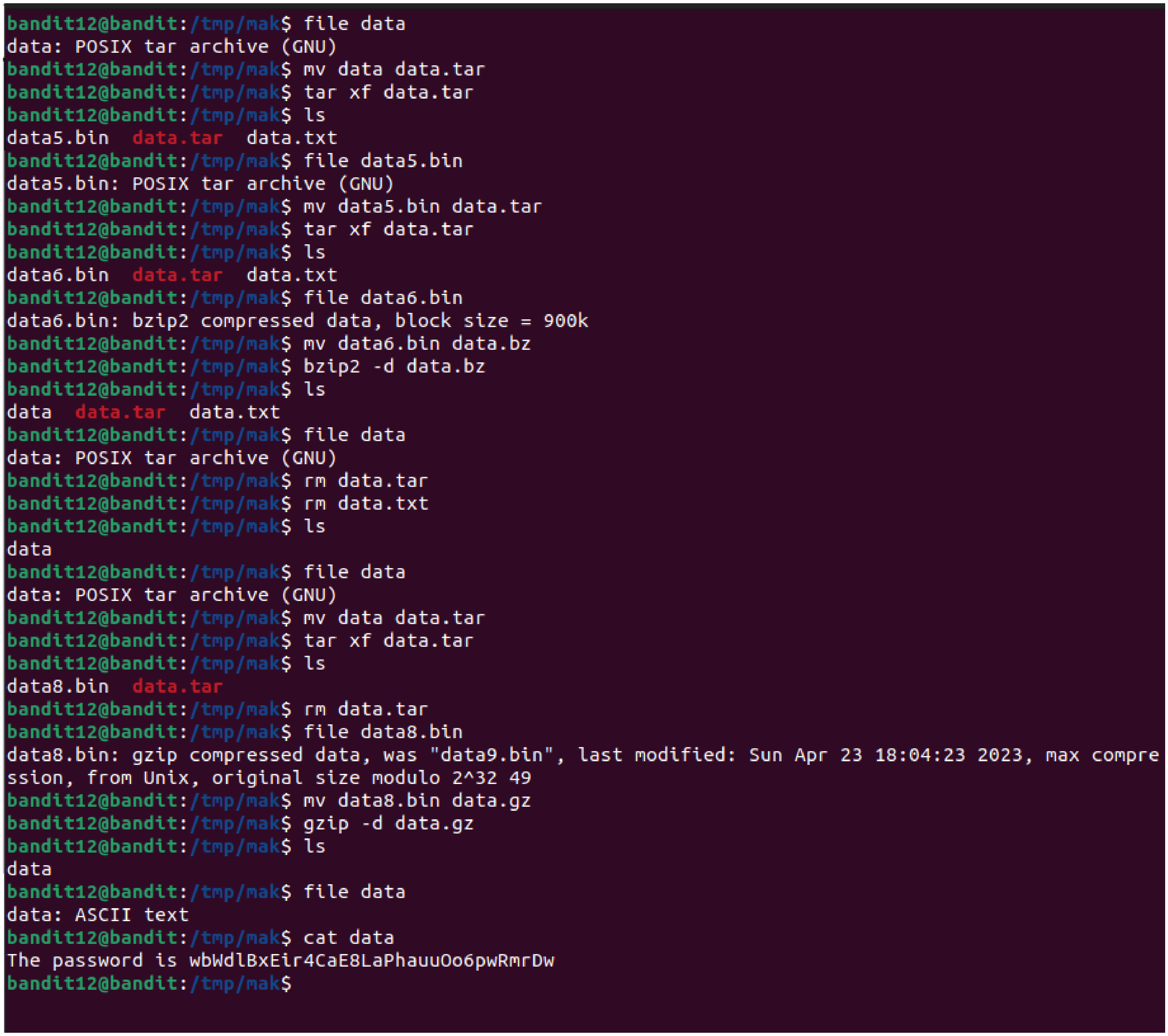
```
bandit12@bandit:/tmp/mak$ man gzip
bandit12@bandit:/tmp/mak$ mv data data.gz
bandit12@bandit:/tmp/mak$ ls
data.gz  data.txt
bandit12@bandit:/tmp/mak$ gzip -d data
bandit12@bandit:/tmp/mak$ ls
data  data.txt
bandit12@bandit:/tmp/mak$ file data
data: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/mak$
```



```
bandit12@bandit:/tmp/mak$ man bzip2
bandit12@bandit:/tmp/mak$ mv data data.bz2
bandit12@bandit:/tmp/mak$ bzip2 -d data.bv2
bzip2: Can't open input file data.bv2: No such file or directory.
bandit12@bandit:/tmp/mak$ ls
data.bz2  data.txt
bandit12@bandit:/tmp/mak$ bzip2 -d data.bz2
bandit12@bandit:/tmp/mak$ ls
data  data.txt
bandit12@bandit:/tmp/mak$
```



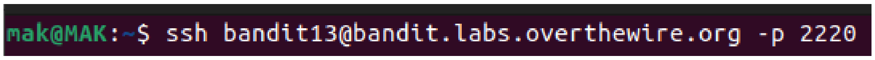
```
bandit12@bandit:/tmp/mak$ file data
data: gzip compressed data, was "data4.bin", last modified: Sun Apr 23 18:04:23 2023, max compression
, from Unix, original size modulo 2^32 20480
bandit12@bandit:/tmp/mak$ mv data data.gz
bandit12@bandit:/tmp/mak$ ls
data.gz  data.txt
bandit12@bandit:/tmp/mak$ gzip -d data.gz
bandit12@bandit:/tmp/mak$ ls
data  data.txt
bandit12@bandit:/tmp/mak$
```



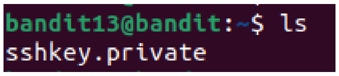
```
bandit12@bandit:/tmp/mak$ file data
data: POSIX tar archive (GNU)
bandit12@bandit:/tmp/mak$ mv data data.tar
bandit12@bandit:/tmp/mak$ tar xf data.tar
bandit12@bandit:/tmp/mak$ ls
data5.bin  data.tar  data.txt
bandit12@bandit:/tmp/mak$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/mak$ mv data5.bin data.tar
bandit12@bandit:/tmp/mak$ tar xf data.tar
bandit12@bandit:/tmp/mak$ ls
data6.bin  data.tar  data.txt
bandit12@bandit:/tmp/mak$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/mak$ mv data6.bin data.bz
bandit12@bandit:/tmp/mak$ bzip2 -d data.bz
bandit12@bandit:/tmp/mak$ ls
data  data.tar  data.txt
bandit12@bandit:/tmp/mak$ file data
data: POSIX tar archive (GNU)
bandit12@bandit:/tmp/mak$ rm data.tar
bandit12@bandit:/tmp/mak$ rm data.txt
bandit12@bandit:/tmp/mak$ ls
data
bandit12@bandit:/tmp/mak$ file data
data: POSIX tar archive (GNU)
bandit12@bandit:/tmp/mak$ mv data data.tar
bandit12@bandit:/tmp/mak$ tar xf data.tar
bandit12@bandit:/tmp/mak$ ls
data8.bin  data.tar
bandit12@bandit:/tmp/mak$ rm data.tar
bandit12@bandit:/tmp/mak$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Sun Apr 23 18:04:23 2023, max compre
ssion, from Unix, original size modulo 2^32 49
bandit12@bandit:/tmp/mak$ mv data8.bin data.gz
bandit12@bandit:/tmp/mak$ gzip -d data.gz
bandit12@bandit:/tmp/mak$ ls
data
bandit12@bandit:/tmp/mak$ file data
data: ASCII text
bandit12@bandit:/tmp/mak$ cat data
The password is wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw
bandit12@bandit:/tmp/mak$
```

Password: JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRV

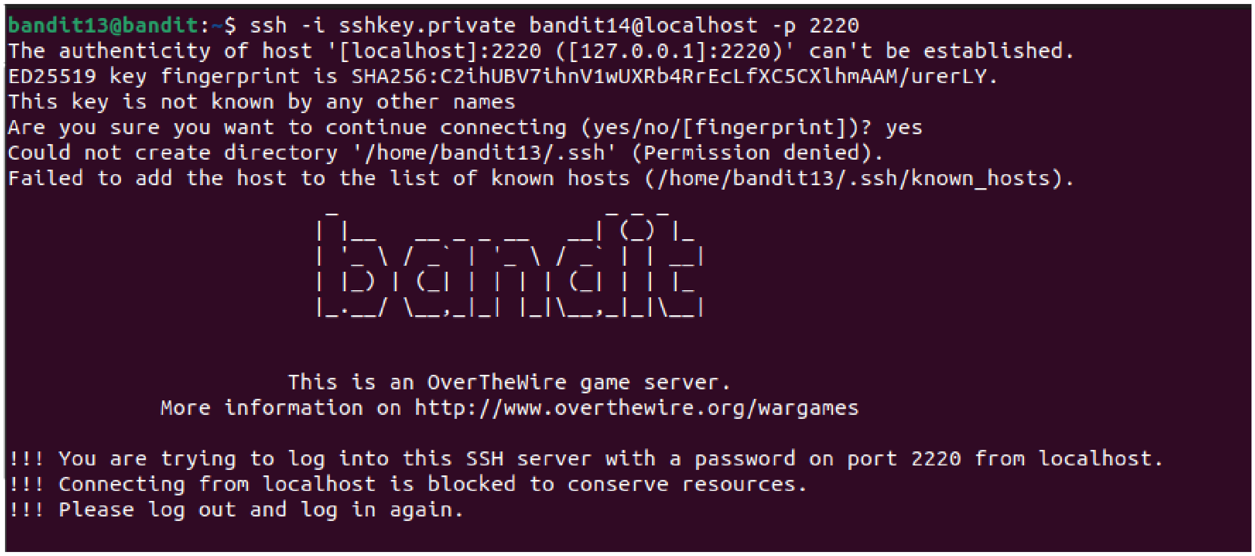
Level 14:



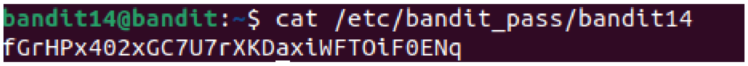
```
mak@MAK:~$ ssh bandit13@bandit.labs.overthewire.org -p 2220
```



```
bandit13@bandit:~$ ls
sshkey.private
```



```
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.
```

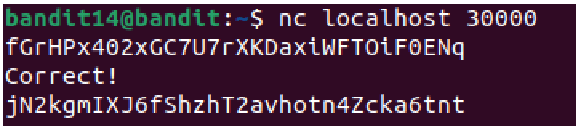


```
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq
```

Password: wbwdlBxEir4CaE8LaPhauu006pwRmrDw

Level 15:

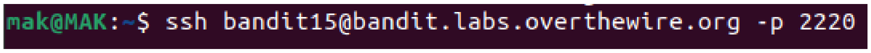
While being on the bandit14



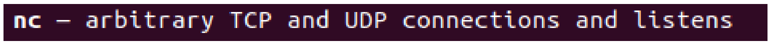
```
bandit14@bandit:~$ nc localhost 30000
fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq
Correct!
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt
```

Password: fGrHPx402xGC7U7rXKDaxLWFTOLFOENG

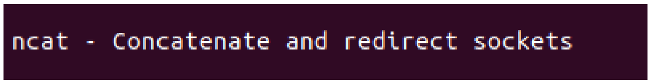
Level 16:



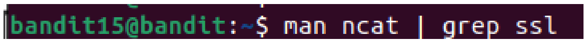
```
mak@MAK:~$ ssh bandit15@bandit.labs.overthewire.org -p 2220
```



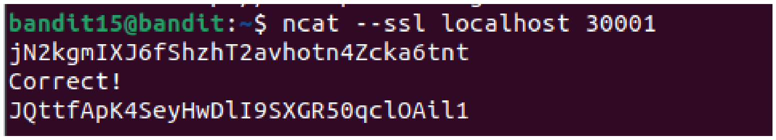
```
nc — arbitrary TCP and UDP connections and listens
```



```
ncat - Concatenate and redirect sockets
```



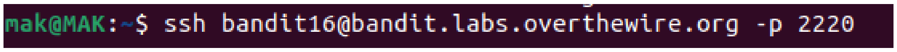
```
bandit15@bandit:~$ man ncat | grep ssl
```



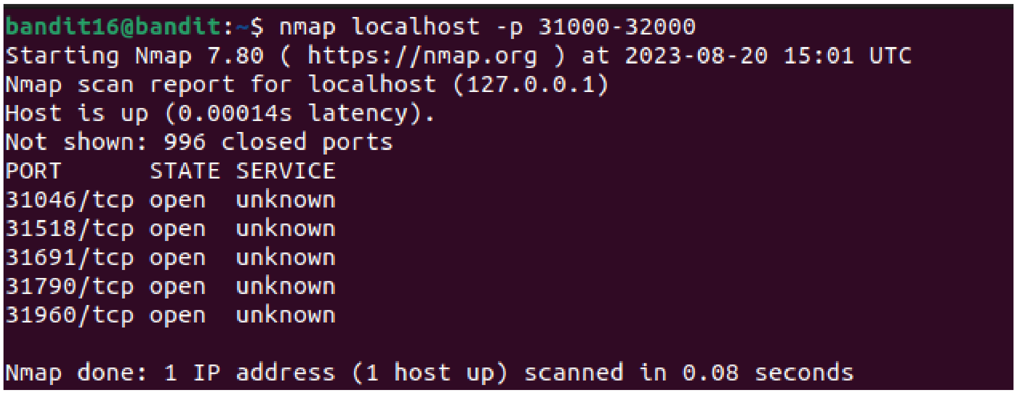
```
bandit15@bandit:~$ ncat --ssl localhost 30001
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt
Correct!
JQttfApK4SeyHwDlI9SXGR50qclOAil1
```

Password: jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt

Level 17:

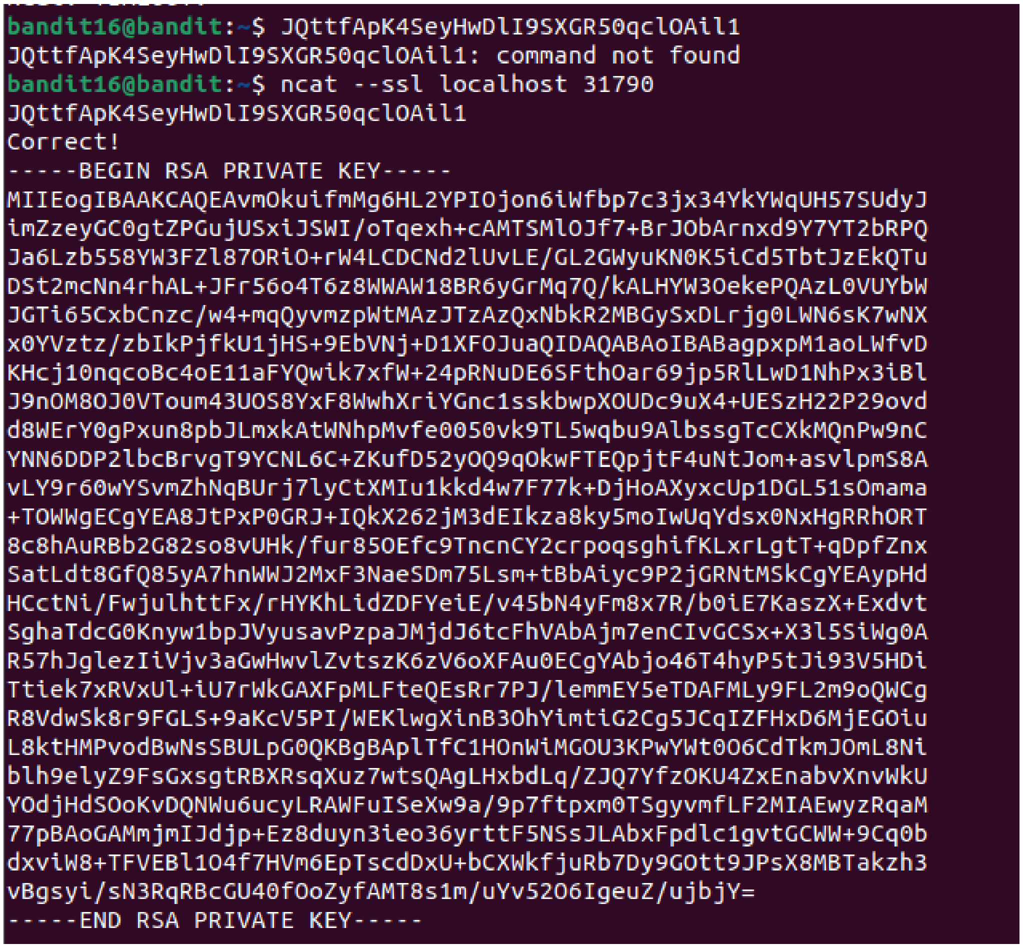


```
mak@MAK:~$ ssh bandit16@bandit.labs.overthewire.org -p 2220
```



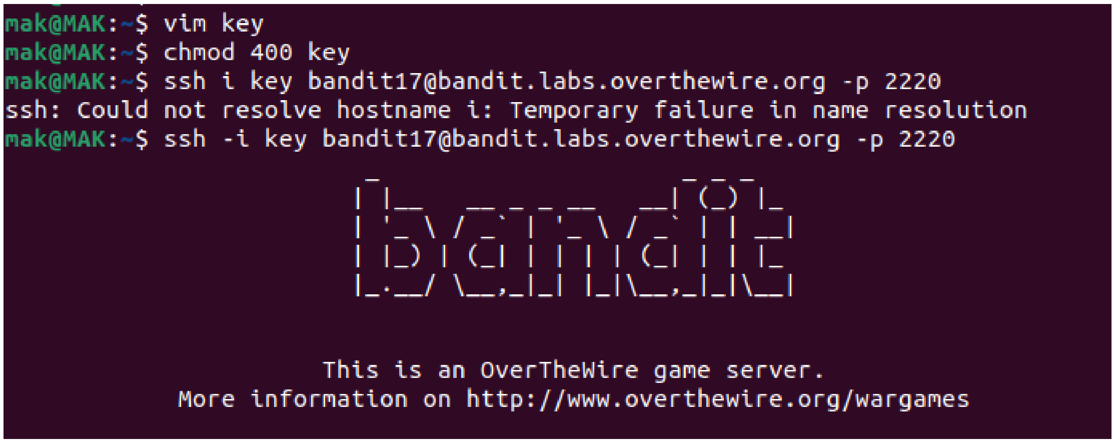
```
bandit16@bandit:~$ nmap localhost -p 31000-32000
Starting Nmap 7.80 ( https://nmap.org ) at 2023-08-20 15:01 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00014s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
31046/tcp open  unknown
31518/tcp open  unknown
31691/tcp open  unknown
31790/tcp open  unknown
31960/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

Then, trial and error. Got it right on the fourth one.



```
bandit16@bandit:~$ JQttfApK4SeyHwDlI9SXGR50qclOAil1
JQttfApK4SeyHwDlI9SXGR50qclOAil1: command not found
bandit16@bandit:~$ ncat --ssl localhost 31790
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-----
```

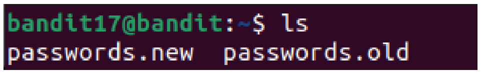
Copy this private key and then paste it in the vim editor. Name it key and then provide appropriate permissions. Then move on to the next level.



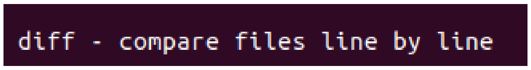
```
mak@MAK:~$ vim key
mak@MAK:~$ chmod 400 key
mak@MAK:~$ ssh i key bandit17@bandit.labs.overthewire.org -p 2220
ssh: Could not resolve hostname i: Temporary failure in name resolution
mak@MAK:~$ ssh -i key bandit17@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

Password: JQttfAPK4SeyHwDl19SXGR50qcl0Ail1

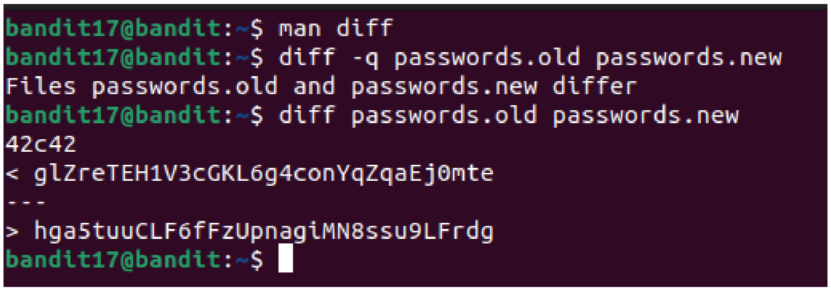
Level 18:



```
bandit17@bandit:~$ ls
passwords.new  passwords.old
```



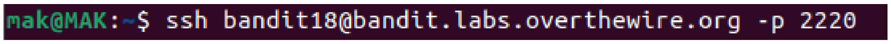
```
diff - compare files line by line
```



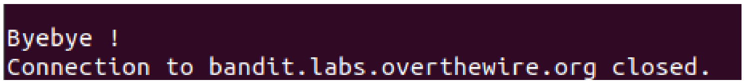
```
bandit17@bandit:~$ man diff
bandit17@bandit:~$ diff -q passwords.old passwords.new
Files passwords.old and passwords.new differ
bandit17@bandit:~$ diff passwords.old passwords.new
42c42
< glZreTEH1V3cGKL6g4conYqZqaEj0mte
---
> hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg
bandit17@bandit:~$ 
```

Password: glZreTEH1V3cGKL6g4conYqZqaEj0mte

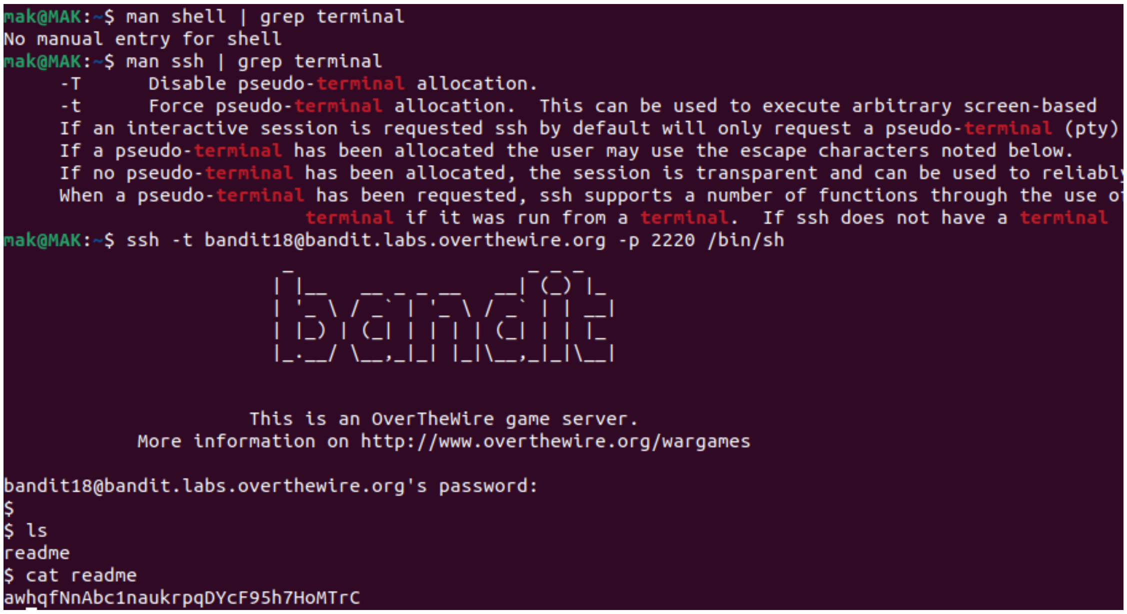
Level 19:



```
mak@MAK:~$ ssh bandit18@bandit.labs.overthewire.org -p 2220
```



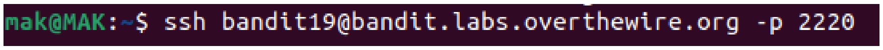
```
Byebye !
Connection to bandit.labs.overthewire.org closed.
```



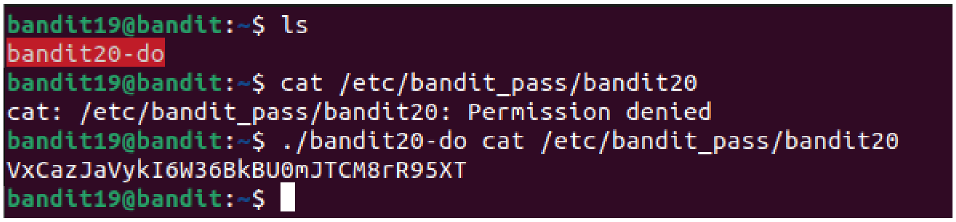
```
mak@MAK:~$ man shell | grep terminal
No manual entry for shell
mak@MAK:~$ man ssh | grep terminal
     -T      Disable pseudo-terminal allocation.
     -t      Force pseudo-terminal allocation.  This can be used to execute arbitrary screen-based
     If an interactive session is requested ssh by default will only request a pseudo-terminal (pty)
     If a pseudo-terminal has been allocated the user may use the escape characters noted below.
     If no pseudo-terminal has been allocated, the session is transparent and can be used to reliabl
     When a pseudo-terminal has been requested, ssh supports a number of functions through the use o
                           terminal if it was run from a terminal.  If ssh does not have a terminal
mak@MAK:~$ ssh -t bandit18@bandit.labs.overthewire.org -p 2220 /bin/sh
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit18@bandit.labs.overthewire.org's password:
$
$ ls
readme
$ cat readme
awhqfNnAbc1naukrpqDYcF95h7HoMTrC
```

Password: hgastuuCLF6fFzUpnagiMN8ssu9LFrdg

Level 20:



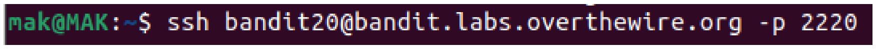
```
mak@MAK:~$ ssh bandit19@bandit.labs.overthewire.org -p 2220
```



```
bandit19@bandit:~$ ls
bandit20-do
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:~$
```

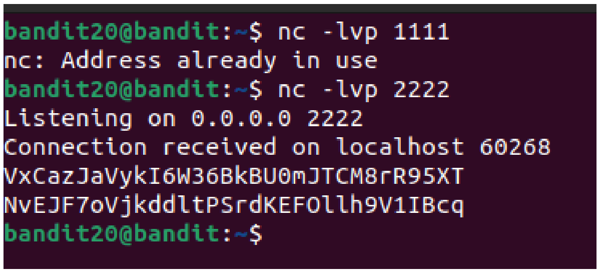
Password: awhqfNnAbc1naukrpqDYCF95h7HOMTrC

Level 21:



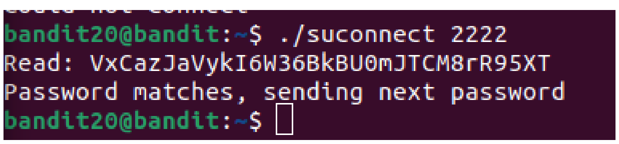
```
mak@MAK:~$ ssh bandit20@bandit.labs.overthewire.org -p 2220
```

The 2nd Terminal:



```
bandit20@bandit:~$ nc -lvp 1111
nc: Address already in use
bandit20@bandit:~$ nc -lvp 2222
Listening on 0.0.0.0 2222
Connection received on localhost 60268
VxCazJaVykI6W36BkBU0mJTCM8rR95XT
NvEJF7oVjkddltPSrdKEFOllh9V1IBcq
bandit20@bandit:~$
```

1st Terminal:

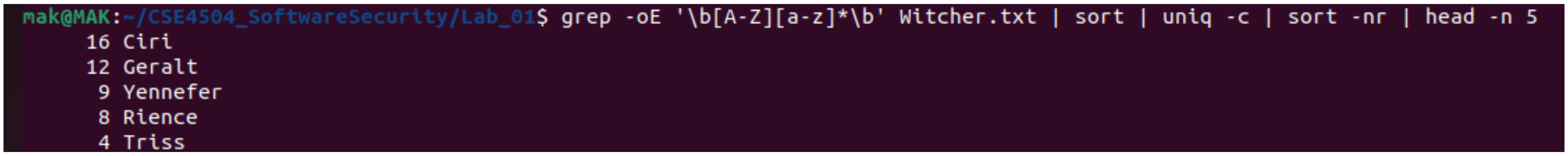


```
bandit20@bandit:~$ ./suconnect 2222
Read: VxCazJaVykI6W36BkBU0mJTCM8rR95XT
Password matches, sending next password
bandit20@bandit:~$
```

Password: VxCazJavykI6W36BKBU0mJTCM8rR95XT

Task 1:

Find the most frequent 5 capitalized words with their frequencies. You can only use pipes and redirections in the terminal. You can use multiple commands.



```
mak@MAK:~/CSE4504_SoftwareSecurity/Lab_01$ grep -oE '\b[A-Z][a-z]*\b' Witcher.txt | sort | uniq -c | sort -nr | head -n 5
     16 Ciri
     12 Geralt
      9 Yennefer
      8 Rience
      4 Triss
```

grep -oE '\b[A-Z][a-z]*\b' filename.txt | sort | uniq -c | sort -nr | head -n 5