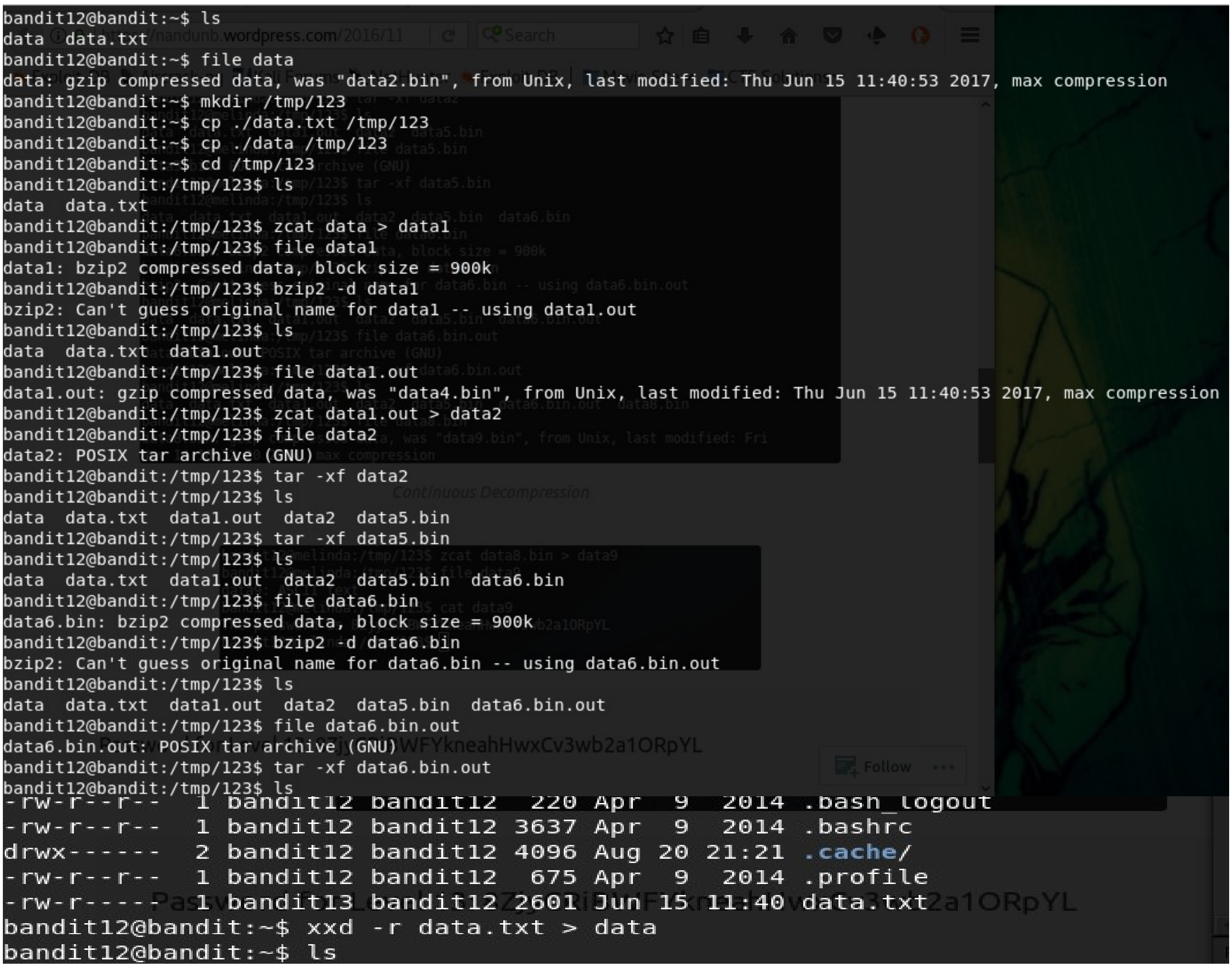
OverTheWire: BANDIT WRITEUP:

URL: http://overthewire.org/wargames/bandit/
START DATE: 21th/08/2017

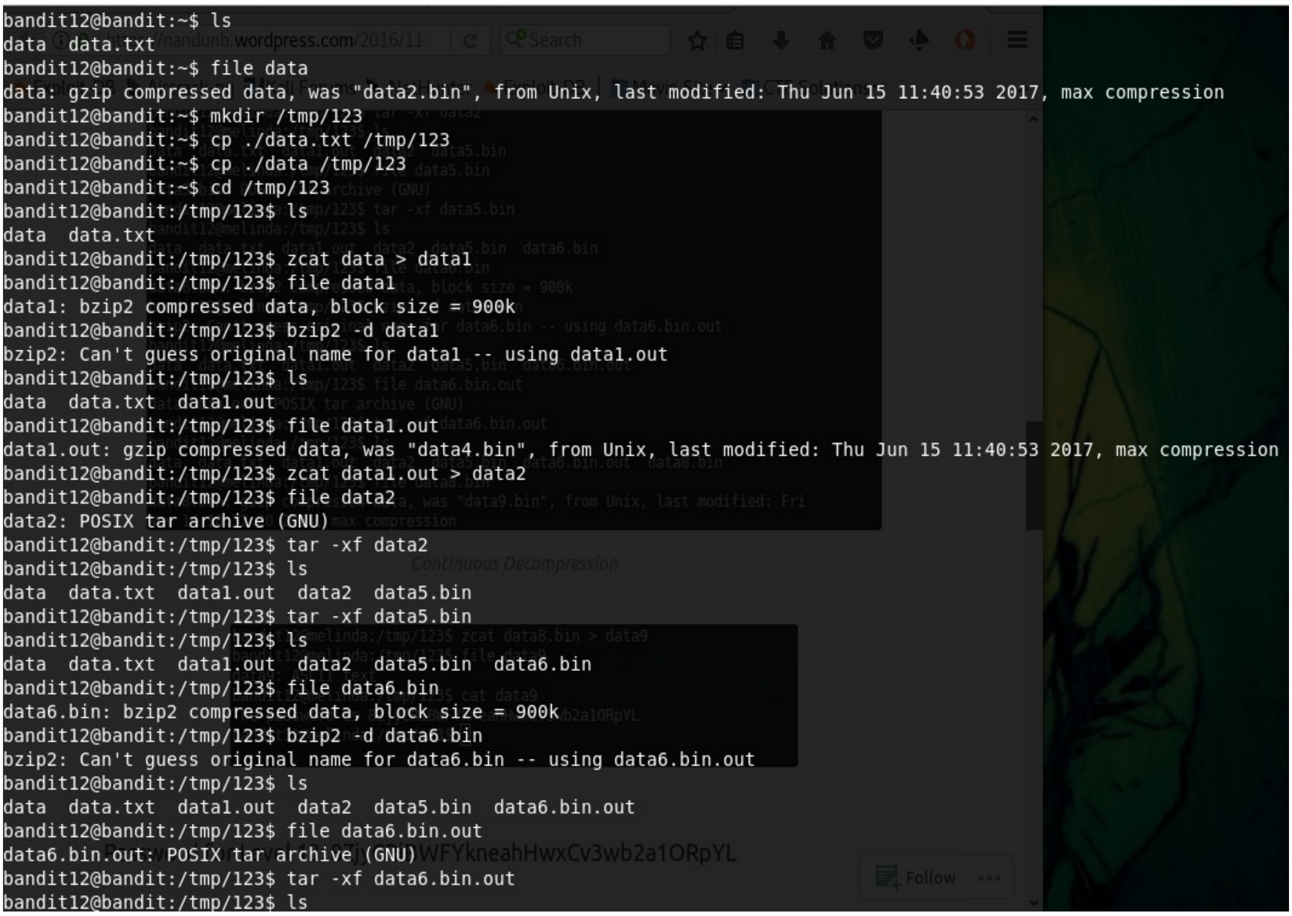
AUTHOR: PETER NUMI
Email: kamandepeter.pk@gmail.com
PHONE: +254 707 897 394

Level 12 to Level 13:

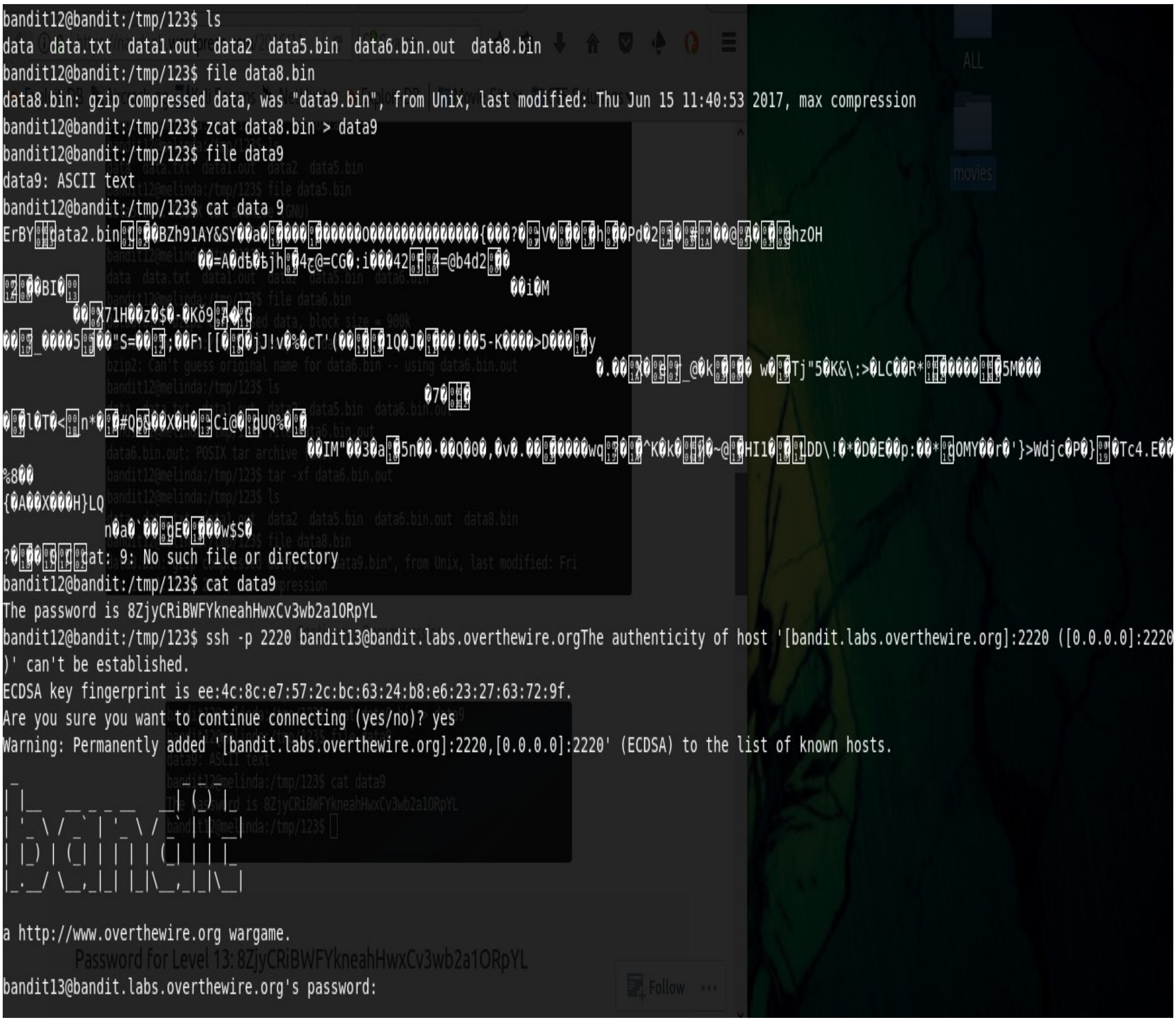
```
#ls
#xxd -r data.txt > data
#ls
#file data
#mkdir /tmp/123
#cp ./data.txt /tmp/123
#cp ./data /tmp/123
#cd /tmp/123
#ls
#zcat data > data1  compress or expand files
#file data1
#bzip2 -d data1 compresses single files
#ls
#file data1.out opens the data files
#zcat data1.out > data2
#file data2
#tar -xf data2
#data2  data5.bin
#tar -xf data5.bin uncompresses the data5.bin
#ls
#file data6.bin
#bzip2 -d data6.bin
#ls
#file data6.bin.out
#tar -xf data6.bin.out
#ls
#file data8.bin
#zcat data8.bin > data9
#file data9
#cat data9
#ssh -p 2220 bandit13@bandit.labs.overthewire.org
```



```
bandit12@bandit:~$ ls
data  data.txt
bandit12@bandit:~$ file data
data: gzip compressed data, was "data2.bin", from Unix, last modified: Thu Jun 15 11:40:53 2017, max compression
bandit12@bandit:~$ mkdir /tmp/123
bandit12@bandit:~$ cp ./data.txt /tmp/123
bandit12@bandit:~$ cp ./data /tmp/123
bandit12@bandit:~$ cd /tmp/123
bandit12@bandit:/tmp/123$ ls
data  data.txt
bandit12@bandit:/tmp/123$ zcat data > data1
bandit12@bandit:/tmp/123$ file data1
data1: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/123$ bzip2 -d data1
bzip2: Can't guess original name for data1 -- using data1.out
bandit12@bandit:/tmp/123$ ls
data  data.txt  data1.out
bandit12@bandit:/tmp/123$ file data1.out
data1.out: gzip compressed data, was "data4.bin", from Unix, last modified: Thu Jun 15 11:40:53 2017, max compression
bandit12@bandit:/tmp/123$ zcat data1.out > data2
bandit12@bandit:/tmp/123$ file data2
data2: POSIX tar archive (GNU)
bandit12@bandit:/tmp/123$ tar -xf data2
bandit12@bandit:/tmp/123$ ls
data  data.txt  data1.out  data2  data5.bin
bandit12@bandit:/tmp/123$ tar -xf data5.bin
bandit12@bandit:/tmp/123$ ls
data  data.txt  data1.out  data2  data5.bin  data6.bin
bandit12@bandit:/tmp/123$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/123$ bzip2 -d data6.bin
bzip2: Can't guess original name for data6.bin -- using data6.bin.out
bandit12@bandit:/tmp/123$ ls
data  data.txt  data1.out  data2  data5.bin  data6.bin.out
bandit12@bandit:/tmp/123$ file data6.bin.out
data6.bin.out: POSIX tar archive (GNU)
bandit12@bandit:/tmp/123$ tar -xf data6.bin.out
bandit12@bandit:/tmp/123$ ls
-rw-r--r--  1 bandit12 bandit12  220 Apr  9  2014 .bash_logout
-rw-r--r--  1 bandit12 bandit12 3637 Apr  9  2014 .bashrc
drwx------  2 bandit12 bandit12 4096 Aug 20 21:21 .cache/
-rw-r--r--  1 bandit12 bandit12  675 Apr  9  2014 .profile
-rw-r-----  1 bandit13 bandit12 2601 Jun 15 11:40 data.txt
bandit12@bandit:~$ xxd -r data.txt > data
bandit12@bandit:~$ ls
```



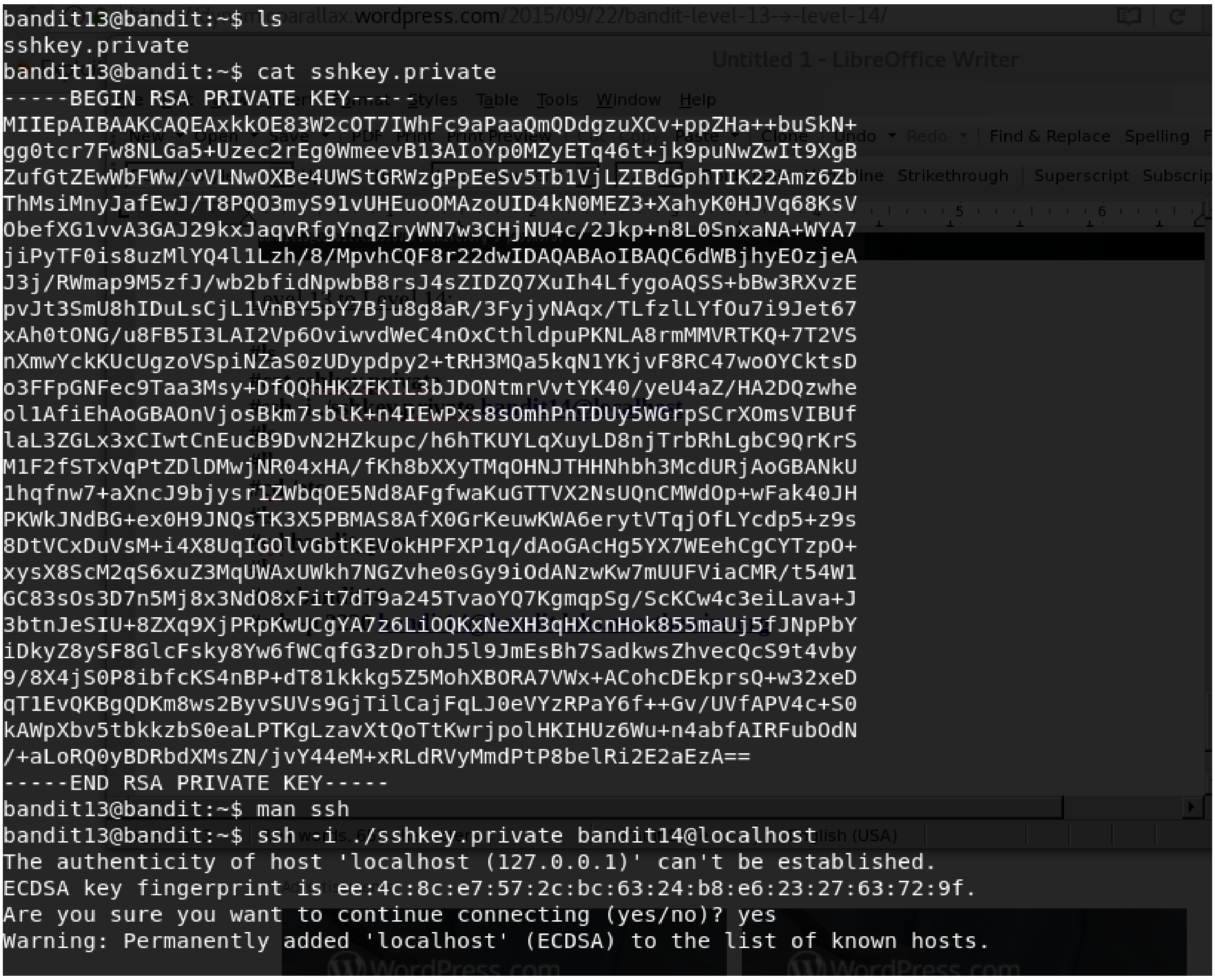
```
bandit12@bandit:~$ ls
data  data.txt
bandit12@bandit:~$ file data
data: gzip compressed data, was "data2.bin", from Unix, last modified: Thu Jun 15 11:40:53 2017, max compression
bandit12@bandit:~$ mkdir /tmp/123
bandit12@bandit:~$ cp ./data.txt /tmp/123
bandit12@bandit:~$ cp ./data /tmp/123
bandit12@bandit:~$ cd /tmp/123
bandit12@bandit:/tmp/123$ ls
data  data.txt
bandit12@bandit:/tmp/123$ zcat data > data1
bandit12@bandit:/tmp/123$ file data1
data1: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/123$ bzip2 -d data1
bzip2: Can't guess original name for data1 -- using data1.out
bandit12@bandit:/tmp/123$ ls
data  data.txt  data1.out
bandit12@bandit:/tmp/123$ file data1.out
data1.out: gzip compressed data, was "data4.bin", from Unix, last modified: Thu Jun 15 11:40:53 2017, max compression
bandit12@bandit:/tmp/123$ zcat data1.out > data2
bandit12@bandit:/tmp/123$ file data2
data2: POSIX tar archive (GNU)
bandit12@bandit:/tmp/123$ tar -xf data2
bandit12@bandit:/tmp/123$ ls
data  data.txt  data1.out  data2  data5.bin
bandit12@bandit:/tmp/123$ tar -xf data5.bin
bandit12@bandit:/tmp/123$ ls
data  data.txt  data1.out  data2  data5.bin  data6.bin
bandit12@bandit:/tmp/123$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/123$ bzip2 -d data6.bin
bzip2: Can't guess original name for data6.bin -- using data6.bin.out
bandit12@bandit:/tmp/123$ ls
data  data.txt  data1.out  data2  data5.bin  data6.bin.out
bandit12@bandit:/tmp/123$ file data6.bin.out
data6.bin.out: POSIX tar archive (GNU)
bandit12@bandit:/tmp/123$ tar -xf data6.bin.out
bandit12@bandit:/tmp/123$ ls
```



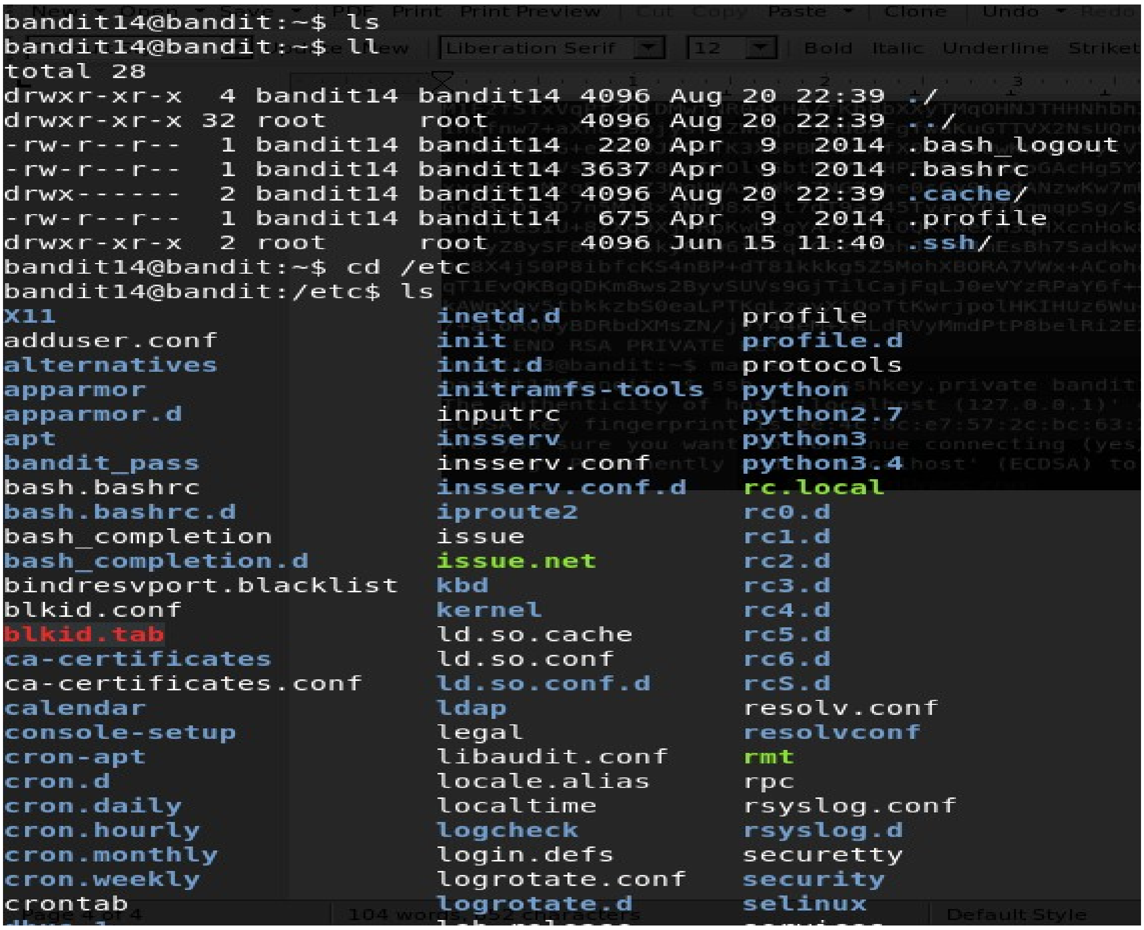
```
bandit12@bandit:/tmp/123$ ls
data  data.txt  data1.out  data2  data5.bin  data6.bin.out  data8.bin
bandit12@bandit:/tmp/123$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", from Unix, last modified: Thu Jun 15 11:40:53 2017, max compression
bandit12@bandit:/tmp/123$ zcat data8.bin > data9
bandit12@bandit:/tmp/123$ file data9
data9: ASCII text
bandit12@bandit:/tmp/123$ cat data 9
ErBY��data2.bin���BZh91AY&SY��a������������o��������������{���?��V����h��Pd�2��#���@����hzOH
                          ��=A�dƀ�ƀjh��4ꞔ@=CG�:i���42�F�4=@b4d2��
�2��BI��                                                       ��i�M
         ���71H��z�$�-�Kŏ9�A��G
���_����5���"S=���;��F[[���jJ!v�%�cT'(�����1Q�J����!��5-K����>D�����y
                                                                      �.�����_@�k���� w���Tj"5�K&\:>�LC��R*�������5M���
                                                       �7���
���l�T�<�n*���#Q�&��X�H��Ci@���UQ%���
                                            ��IM"��3�a��5n��·��Q��,�v�.���������wq������^K�k����~@��HI1����DD\!�*�D�E��p:��*��OMY��r�'}>Wdjc�P�}���Tc4.E��
%8��
{�A��X���H}LQ
             n�a�`����E�����w$S�
?��������at: 9: No such file or directory
bandit12@bandit:/tmp/123$ cat data9
The password is 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
bandit12@bandit:/tmp/123$ ssh -p 2220 bandit13@bandit.labs.overthewire.orgThe authenticity of host '[bandit.labs.overthewire.org]:2220 ([0.0.0.0]:2220
)' can't be established.
ECDSA key fingerprint is ee:4c:8c:e7:57:2c:bc:63:24:b8:e6:23:27:63:72:9f.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[bandit.labs.overthewire.org]:2220,[0.0.0.0]:2220' (ECDSA) to the list of known hosts.
 _                     _ _ _
| |__   __ _ _ __   __| (_) |_
| '_ \ / _` | '_ \ / _` | | __|
| |_) | (_| | | | | (_| | | |_
|_.__/ \__,_|_| |_|\__,_|_|\__|

a http://www.overthewire.org wargame.
        Password for Level 13: 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
bandit13@bandit.labs.overthewire.org's password:
```

Level 13 to Level 14:

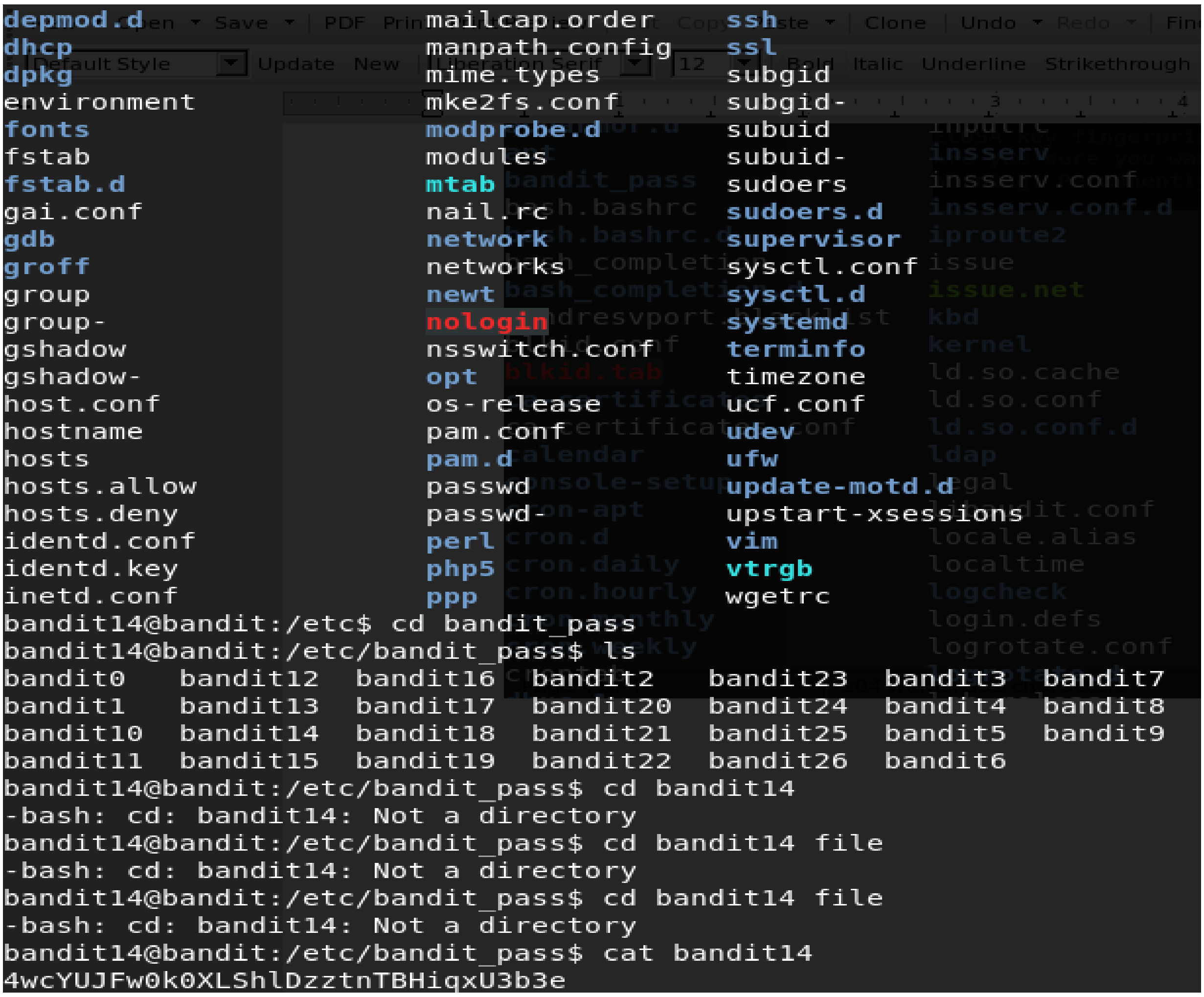
#ls
#cat sshkey.private
#ssh -i ./sshkey.private bandit14@localhost
#ls
#ll
#cd /etc
#ls
#cd bandit_pass
#ls
#cat bandit14
#ssh -p 2220 bandit14@bandit.labs.overthewire.org



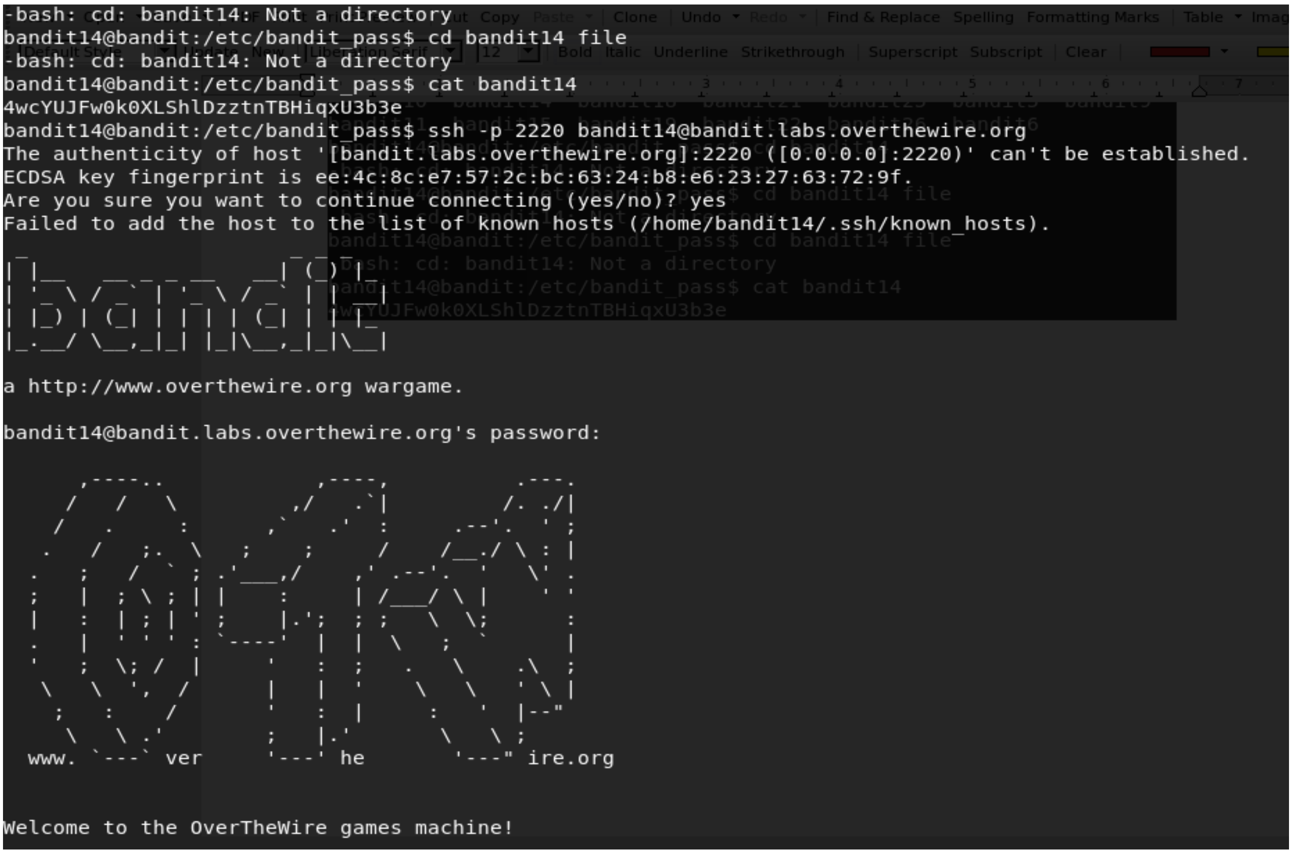
```
bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ cat sshkey.private
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAxkkOE83W2cOT7IWhFc9aPaaQmQDdgzuXCv+ppZHa++buSkN+
gg0tcr7Fw8NLGa5+Uzec2rEg0WmeevB13AIoYp0MZyETq46t+jk9puNwZwIt9XgB
ZufGtZEwWbFWw/vVLNwOXBe4UWStGRWzgPpEeSv5Tb1VjLZIBdGphTIK22Amz6Zb
ThMsiMnyJafEwJ/T8PQO3myS91vUHEuoOMAzoUID4kN0MEZ3+XahyK0HJVq68KsV
ObefXG1vvA3GAJ29kxJaqvRfgYnqZryWN7w3CHjNU4c/2Jkp+n8L0SnxaNA+WYA7
jiPyTF0is8uzMlYQ4l1Lzh/8/MpvhCQF8r22dwIDAQABAoIBAQC6dWBjhyEOzjeA
J3j/RWmap9M5zfJ/wb2bfidNpwbB8rsJ4sZIDZQ7XuIh4LfygoAQSS+bBw3RXvzE
pvJt3SmU8hIDuLsCjL1VnBY5pY7Bju8g8aR/3FyjyNAqx/TLfzlLYfOu7i9Jet67
xAh0tONG/u8FB5I3LAI2Vp6OviwvdWeC4nOxCthldpuPKNLA8rmMMVRTKQ+7T2VS
nXmwYckKUcUgzoVSpiNZaS0zUDypdpy2+tRH3MQa5kqN1YKjvF8RC47woOYCktsD
o3FFpGNFec9Taa3Msy+DfQQhHKZFKIL3bJDONtmrVvtYK40/yeU4aZ/HA2DQzwhe
ol1AfiEhAoGBAOnVjosBkm7sblK+n4IEwPxs8sOmhPnTDUy5WGrpSCrXOmsVIBUf
laL3ZGLx3xCIwtCnEucB9DvN2HZkupc/h6hTKUYLqXuyLD8njTrbRhLgbC9QrKrS
M1F2fSTxVqPtZDlDMwjNR04xHA/fKh8bXXyTMqOHNJTHHNhbh3McdURjAoGBANkU
1hqfnw7+aXncJ9bjysr1ZWbqOE5Nd8AFgfwaKuGTTVX2NsUQnCMWdOp+wFak40JH
PKWkJNdBG+ex0H9JNQsTK3X5PBMAS8AfX0GrKeuwKWA6erytVTqjOfLYcdp5+z9s
8DtVCxDuVsM+i4X8UqIGOlvGbtKEVokHPFXP1q/dAoGAcHg5YX7WEehCgCYTzpO+
xysX8ScM2qS6xuZ3MqUWAxUWkh7NGZvhe0sGy9iOdANzwKw7mUUFViaCMR/t54W1
GC83sOs3D7n5Mj8x3NdO8xFit7dT9a245TvaoYQ7KgmqpSg/ScKCw4c3eiLava+J
3btnJeSIU+8ZXq9XjPRpKwUCgYA7z6LiOQKxNeXH3qHXcnHok855maUj5fJNpPbY
iDkyZ8ySF8GlcFsky8Yw6fWCqfG3zDrohJ5l9JmEsBh7SadkwsZhvecQcS9t4vby
9/8X4jS0P8ibfcKS4nBP+dT81kkkg5Z5MohXBORA7VWx+ACohcDEkprsQ+w32xeD
qT1EvQKBgQDKm8ws2ByvSUVs9GjTilCajFqLJ0eVYzRPaY6f++Gv/UVfAPV4c+S0
kAWpXbv5tbkkzbS0eaLPTKgLzavXtQoTtKwrjpolHKIHUz6Wu+n4abfAIRFubOdN
/+aLoRQ0yBDRbdXMsZN/jvY44eM+xRLdRVyMmdPtP8belRi2E2aEzA==
-----END RSA PRIVATE KEY-----
bandit13@bandit:~$ man ssh
bandit13@bandit:~$ ssh -i ./sshkey.private bandit14@localhost
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is ee:4c:8c:e7:57:2c:bc:63:24:b8:e6:23:27:63:72:9f.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
```



```
bandit14@bandit:~$ ls
bandit14@bandit:~$ ll
total 28
drwxr-xr-x  4 bandit14 bandit14 4096 Aug 20 22:39 ./
drwxr-xr-x 32 root     root     4096 Aug 20 22:39 ../
-rw-r--r--  1 bandit14 bandit14  220 Apr  9  2014 .bash_logout
-rw-r--r--  1 bandit14 bandit14 3637 Apr  9  2014 .bashrc
drwx------  2 bandit14 bandit14 4096 Aug 20 22:39 .cache/
-rw-r--r--  1 bandit14 bandit14  675 Apr  9  2014 .profile
drwxr-xr-x  2 root     root     4096 Jun 15 11:40 .ssh/
bandit14@bandit:~$ cd /etc
bandit14@bandit:/etc$ ls
X11                      inetd.d           profile
adduser.conf             init              profile.d
alternatives             init.d            protocols
apparmor                 initramfs-tools   python
apparmor.d               inputrc           python2.7
apt                      insserv           python3
bandit_pass              insserv.conf      python3.4
bash.bashrc              insserv.conf.d    rc.local
bash.bashrc.d            iproute2          rc0.d
bash_completion          issue             rc1.d
bash_completion.d        issue.net         rc2.d
bindresvport.blacklist   kbd               rc3.d
blkid.conf               kernel            rc4.d
blkid.tab                ld.so.cache       rc5.d
ca-certificates          ld.so.conf        rc6.d
ca-certificates.conf     ld.so.conf.d      rcS.d
calendar                 ldap              resolv.conf
console-setup            legal             resolvconf
cron-apt                 libaudit.conf     rmt
cron.d                   locale.alias      rpc
cron.daily               localtime         rsyslog.conf
cron.hourly              logcheck          rsyslog.d
cron.monthly             login.defs        securetty
cron.weekly              logrotate.conf    security
crontab                  logrotate.d       selinux
```



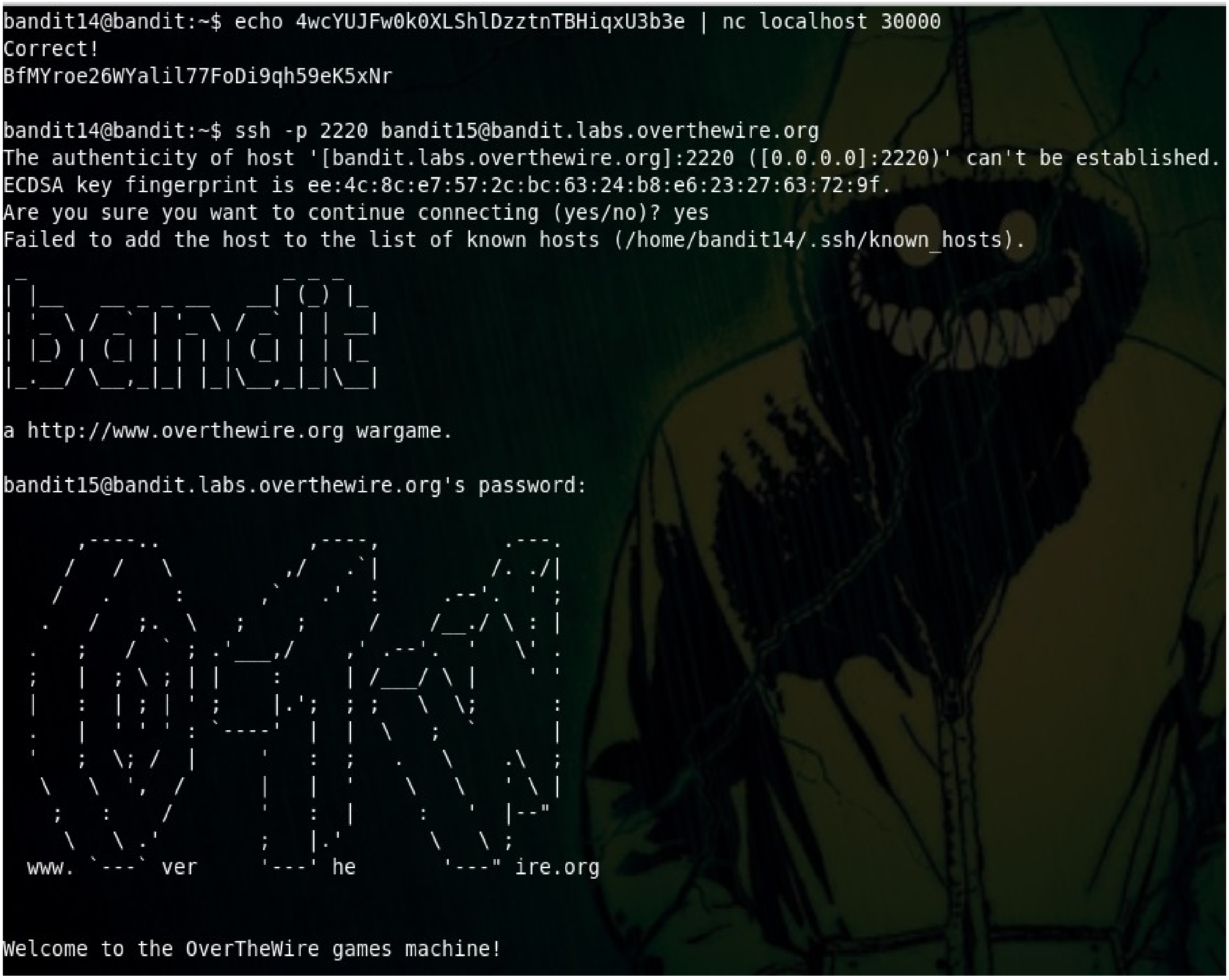
```
depmod.d          mailcap.order      ssh
dhcp              manpath.config     ssl
dpkg              mime.types         subgid
environment       mke2fs.conf        subgid-
fonts             modprobe.d         subuid
fstab             modules            subuid-
fstab.d           mtab               sudoers
gai.conf          nail.rc            sudoers.d
gdb               network            supervisor
groff             networks           sysctl.conf
group             newt               sysctl.d
group-            nologin            systemd
gshadow           nsswitch.conf      terminfo
gshadow-          opt                timezone
host.conf         os-release         ucf.conf
hostname          pam.conf           udev
hosts             pam.d              ufw
hosts.allow       passwd             update-motd.d
hosts.deny        passwd-            upstart-xsessions
identd.conf       perl               vim
identd.key        php5               vtrgb
inetd.conf        ppp                wgetrc
bandit14@bandit:/etc$ cd bandit_pass
bandit14@bandit:/etc/bandit_pass$ ls
bandit0   bandit12  bandit16  bandit2   bandit23  bandit3  bandit7
bandit1   bandit13  bandit17  bandit20  bandit24  bandit4  bandit8
bandit10  bandit14  bandit18  bandit21  bandit25  bandit5  bandit9
bandit11  bandit15  bandit19  bandit22  bandit26  bandit6
bandit14@bandit:/etc/bandit_pass$ cd bandit14
-bash: cd: bandit14: Not a directory
bandit14@bandit:/etc/bandit_pass$ cd bandit14 file
-bash: cd: bandit14: Not a directory
bandit14@bandit:/etc/bandit_pass$ cd bandit14 file
-bash: cd: bandit14: Not a directory
bandit14@bandit:/etc/bandit_pass$ cat bandit14
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
```



```
-bash: cd: bandit14: Not a directory
bandit14@bandit:/etc/bandit_pass$ cd bandit14 file
-bash: cd: bandit14: Not a directory
bandit14@bandit:/etc/bandit_pass$ cat bandit14
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
bandit14@bandit:/etc/bandit_pass$ ssh -p 2220 bandit14@bandit.labs.overthewire.org
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([0.0.0.0]:2220)' can't be established.
ECDSA key fingerprint is ee:4c:8c:e7:57:2c:bc:63:24:b8:e6:23:27:63:72:9f.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit14/.ssh/known_hosts).
 _                     _ _ _
| |__   __ _ _ __   __| (_) |_
| '_ \ / _` | '_ \ / _` | | __|
| |_) | (_| | | | | (_| | | |_
|_.__/ \__,_|_| |_|\__,_|_|\__|

a http://www.overthewire.org wargame.

bandit14@bandit.labs.overthewire.org's password:

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


Welcome to the OverTheWire games machine!
```

Level 14 to Level 15:

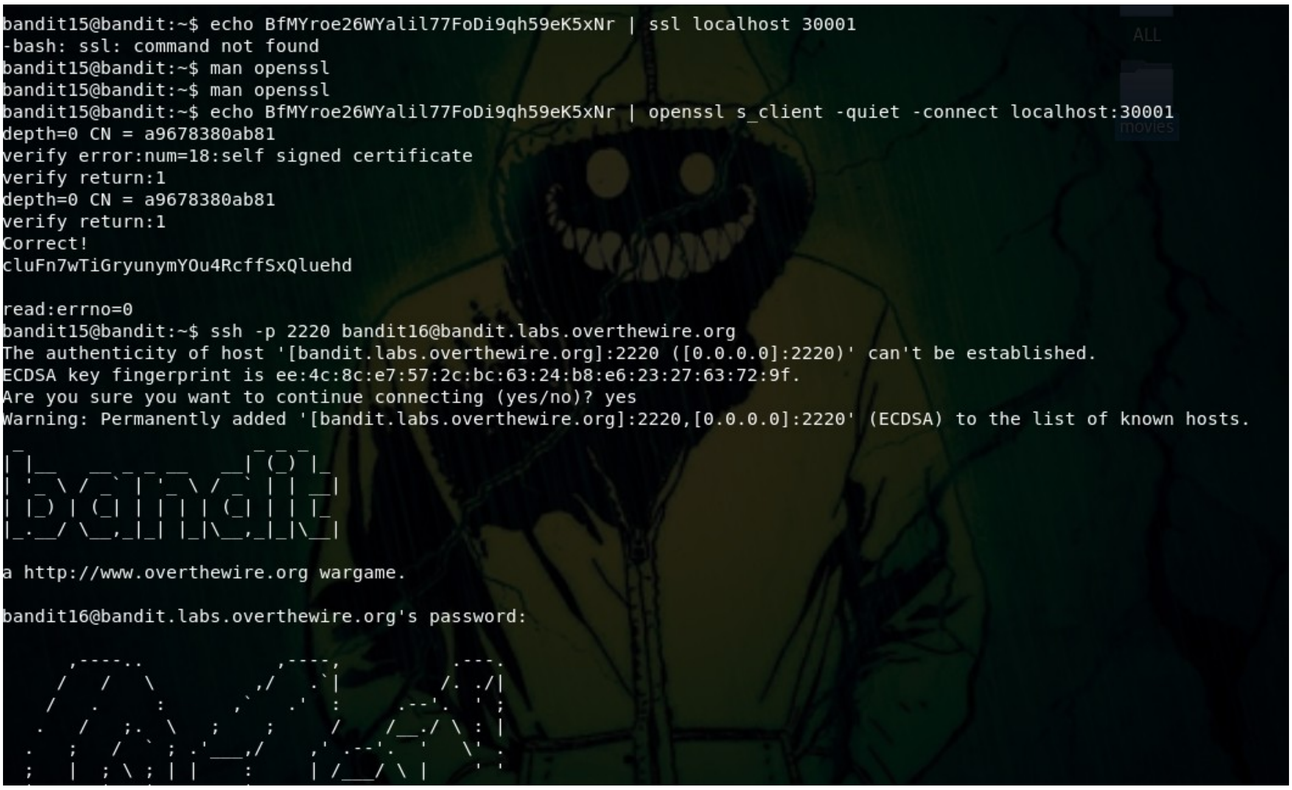
#echo 4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e | nc localhost 30000
#ssh -p 2220 bandit15@bandit.labs.overthewire.org



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

bandit14@bandit:~$ ssh -p 2220 bandit15@bandit.labs.overthewire.org
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([0.0.0.0]:2220)' can't be established.
ECDSA key fingerprint is ee:4c:8c:e7:57:2c:bc:63:24:b8:e6:23:27:63:72:9f.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit14/.ssh/known_hosts).
 _                     _ _ _
| |__   __ _ _ __   __| (_) |_
| '_ \ / _` | '_ \ / _` | | __|
| |_) | (_| | | | | (_| | | |_
|_.__/ \__,_|_| |_|\__,_|_|\__|

a http://www.overthewire.org wargame.

bandit15@bandit.labs.overthewire.org's password:

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


Welcome to the OverTheWire games machine!
```

Level 15 to Level 16:

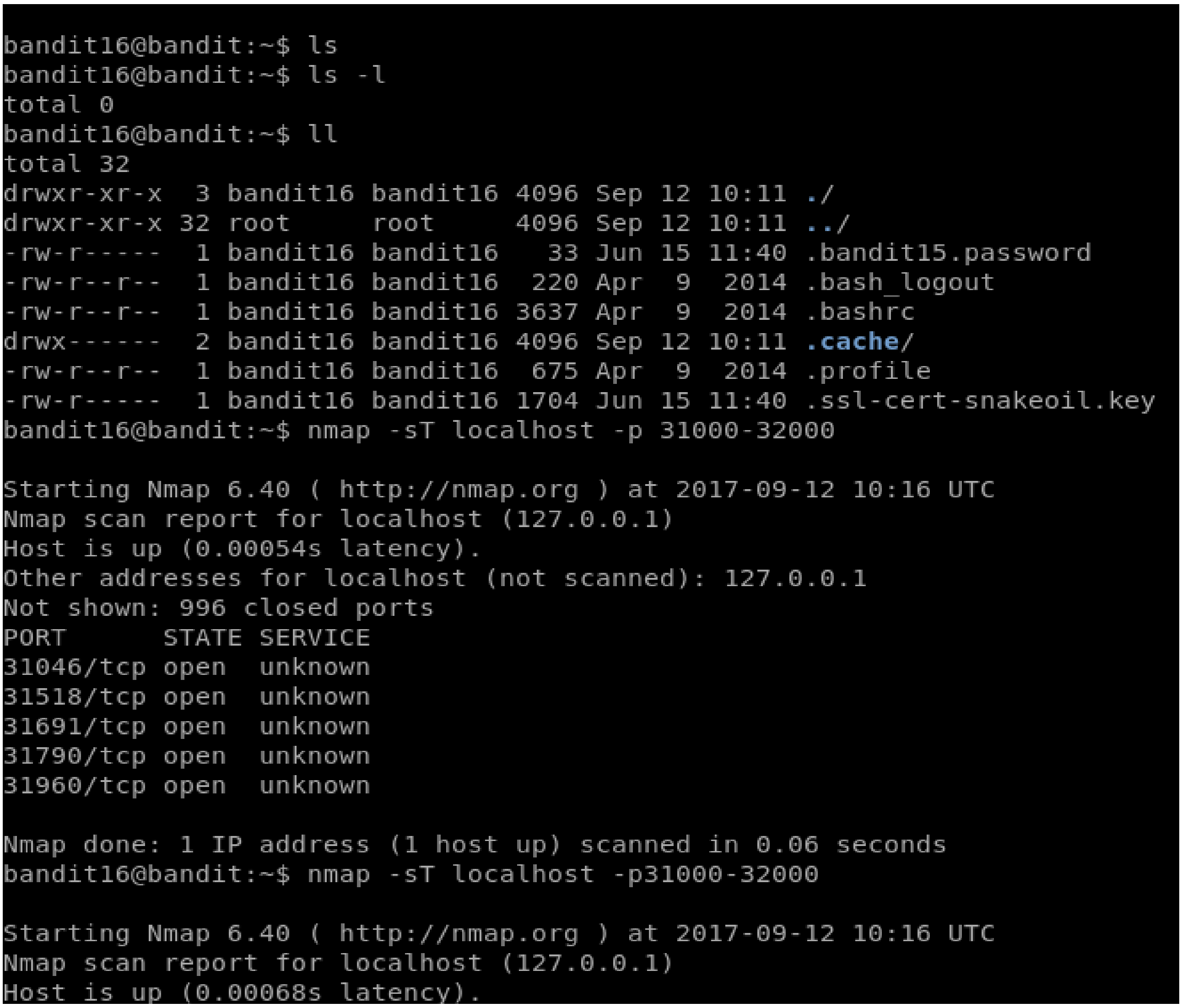
#echo BfMYroe26WYalil77FoDi9qh59eK5xNr | openssl s_client -quiet -connect localhost:30001
#ssh -p 2220 bandit16@bandit.labs.overthewire.org



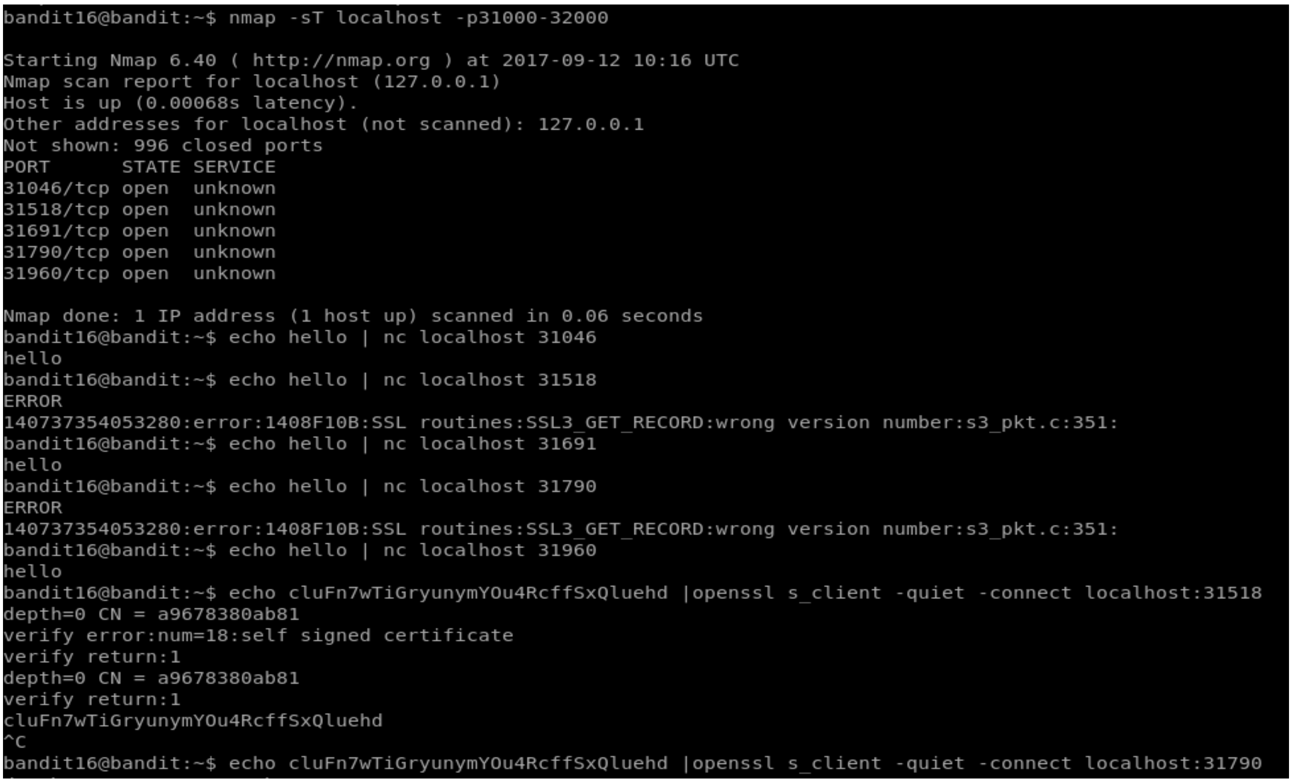
```
bandit15@bandit:~$ echo BfMYroe26WYalil77FoDi9qh59eK5xNr | ssl localhost 30001
-bash: ssl: command not found
bandit15@bandit:~$ man openssl
bandit15@bandit:~$ man openssl
bandit15@bandit:~$ echo BfMYroe26WYalil77FoDi9qh59eK5xNr | openssl s_client -quiet -connect localhost:30001
depth=0 CN = a9678380ab81
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = a9678380ab81
verify return:1
Correct!
cluFn7wTiGryunymYOu4RcffSxQluehd

read:errno=0
bandit15@bandit:~$ ssh -p 2220 bandit16@bandit.labs.overthewire.org
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([0.0.0.0]:2220)' can't be established.
ECDSA key fingerprint is ee:4c:8c:e7:57:2c:bc:63:24:b8:e6:23:27:63:72:9f.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[bandit.labs.overthewire.org]:2220,[0.0.0.0]:2220' (ECDSA) to the list of known hosts.
 _                     _ _ _
| |__   __ _ _ __   __| (_) |_
| '_ \ / _` | '_ \ / _` | | __|
| |_) | (_| | | | | (_| | | |_
|_.__/ \__,_|_| |_|\__,_|_|\__|

a http://www.overthewire.org wargame.

bandit16@bandit.labs.overthewire.org's password:

      ,----..            ,----,          .---.
     /   /   \         ,/   .`|         /. ./|
    /   .     :      ,`   .'  :     .--'.  ' ;
   .   /   ;.  \   ;    ;     /    /__./ \ : |
  .   ;   /  ` ; .'___,/    ,' .--'.  '   \' .
  ;   |  ; \ ; | |    :     |  /___/ \ |    ' '
```

Level 16 to Level 17:

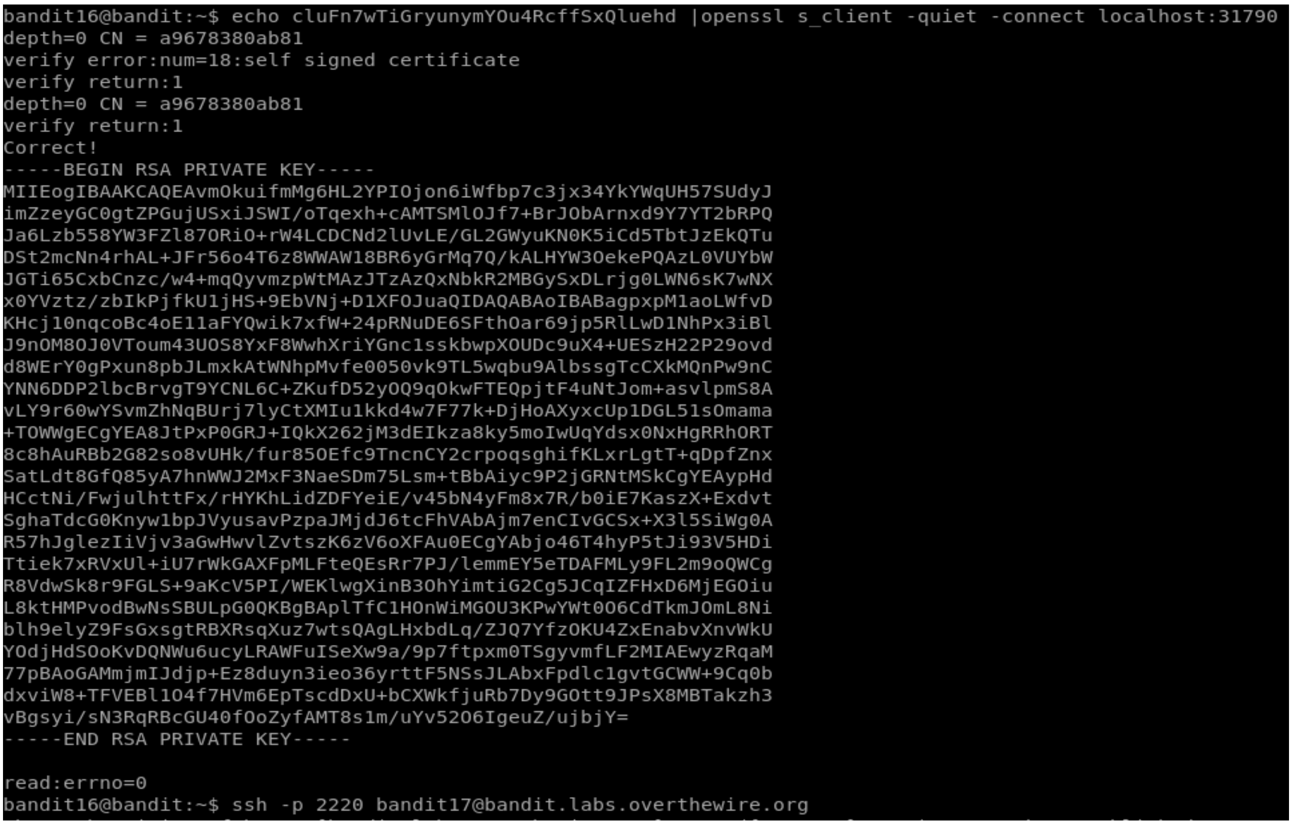
#nmap -sT localhost -p 31000-32000
#echo hello | nc localhost 31046
#echo hello | nc localhost 31518
#echo hello | nc localhost 31691
#echo hello | nc localhost 31790
#echo hello | nc localhost 31960
#echo cluFn7wTiGryunymYOu4RcffSxQluehd |openssl s_client -quiet -connect localhost:31518
#control + c to stop service seemed it had hunged
#echo cluFn7wTiGryunymYOu4RcffSxQluehd |openssl s_client -quiet -connect localhost:31790
#ssh -p 2220 bandit17@bandit.labs.overthewire.org
#control + c
#mkdir /*tmp*/peternumi
#ls
#cd *tmp/*peternumi
# touch sshkey.private
# vi sshkey.private
# a to append
# pasted the key
# ssh -i ./sshkey.private bandit17@localhost
#control + c
#chmod 600 sshkey.private
#ssh -i ./sshkey.private bandit17@localhost
#vi key.private
#chmod 600 key.private
#ls
#ssh -i ./key.private bandit17@localhost



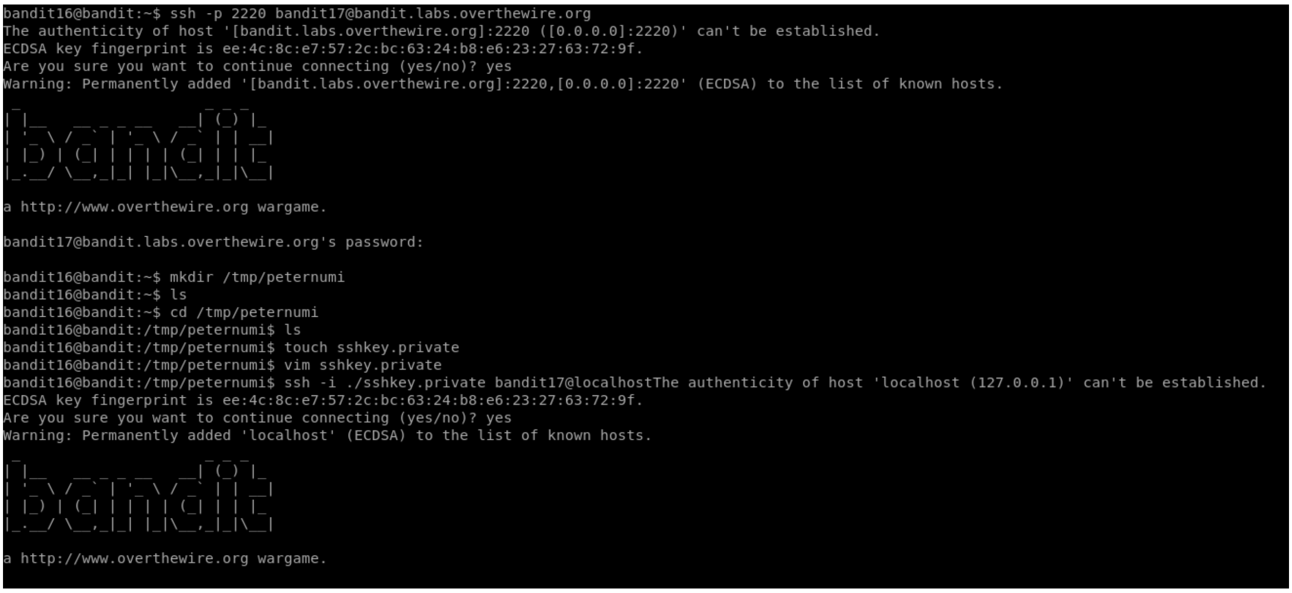
```
bandit16@bandit:~$ ls
bandit16@bandit:~$ ls -l
total 0
bandit16@bandit:~$ ll
total 32
drwxr-xr-x  3 bandit16 bandit16 4096 Sep 12 10:11 ./
drwxr-xr-x 32 root     root     4096 Sep 12 10:11 ../
-rw-r-----  1 bandit16 bandit16   33 Jun 15 11:40 .bandit15.password
-rw-r--r--  1 bandit16 bandit16  220 Apr  9  2014 .bash_logout
-rw-r--r--  1 bandit16 bandit16 3637 Apr  9  2014 .bashrc
drwx------  2 bandit16 bandit16 4096 Sep 12 10:11 .cache/
-rw-r--r--  1 bandit16 bandit16  675 Apr  9  2014 .profile
-rw-r-----  1 bandit16 bandit16 1704 Jun 15 11:40 .ssl-cert-snakeoil.key
bandit16@bandit:~$ nmap -sT localhost -p 31000-32000

Starting Nmap 6.40 ( http://nmap.org ) at 2017-09-12 10:16 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00054s latency).
Other addresses for localhost (not scanned): 127.0.0.1
Not shown: 996 closed ports
PORT      STATE SERVICE
31046/tcp open  unknown
31518/tcp open  unknown
31691/tcp open  unknown
31790/tcp open  unknown
31960/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
bandit16@bandit:~$ nmap -sT localhost -p31000-32000

Starting Nmap 6.40 ( http://nmap.org ) at 2017-09-12 10:16 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00068s latency).
```



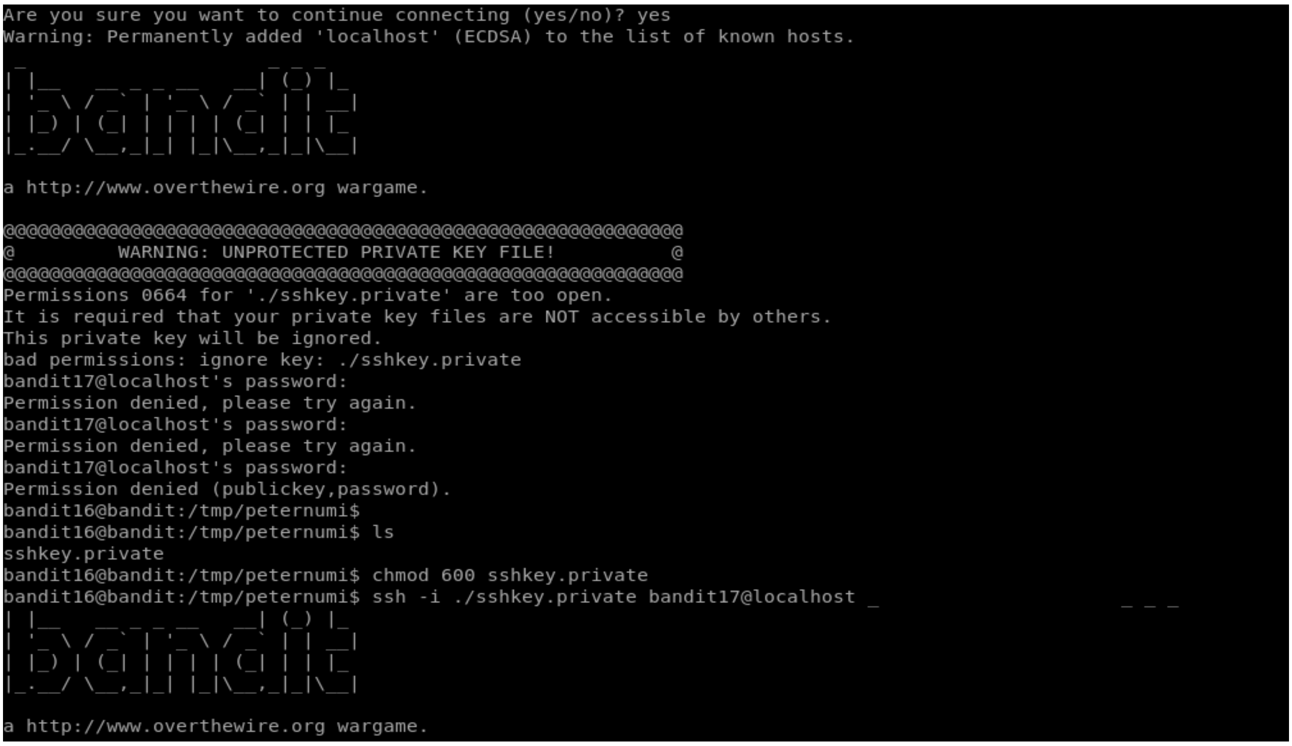
```
bandit16@bandit:~$ nmap -sT localhost -p31000-32000

Starting Nmap 6.40 ( http://nmap.org ) at 2017-09-12 10:16 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00068s latency).
Other addresses for localhost (not scanned): 127.0.0.1
Not shown: 996 closed ports
PORT      STATE SERVICE
31046/tcp open  unknown
31518/tcp open  unknown
31691/tcp open  unknown
31790/tcp open  unknown
31960/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
bandit16@bandit:~$ echo hello | nc localhost 31046
hello
bandit16@bandit:~$ echo hello | nc localhost 31518
ERROR
140737354053280:error:1408F10B:SSL routines:SSL3_GET_RECORD:wrong version number:s3_pkt.c:351:
bandit16@bandit:~$ echo hello | nc localhost 31691
hello
bandit16@bandit:~$ echo hello | nc localhost 31790
ERROR
140737354053280:error:1408F10B:SSL routines:SSL3_GET_RECORD:wrong version number:s3_pkt.c:351:
bandit16@bandit:~$ echo hello | nc localhost 31960
hello
bandit16@bandit:~$ echo cluFn7wTiGryunymYOu4RcffSxQluehd |openssl s_client -quiet -connect localhost:31518
depth=0 CN = a9678380ab81
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = a9678380ab81
verify return:1
cluFn7wTiGryunymYOu4RcffSxQluehd
^C
bandit16@bandit:~$ echo cluFn7wTiGryunymYOu4RcffSxQluehd |openssl s_client -quiet -connect localhost:31790
```



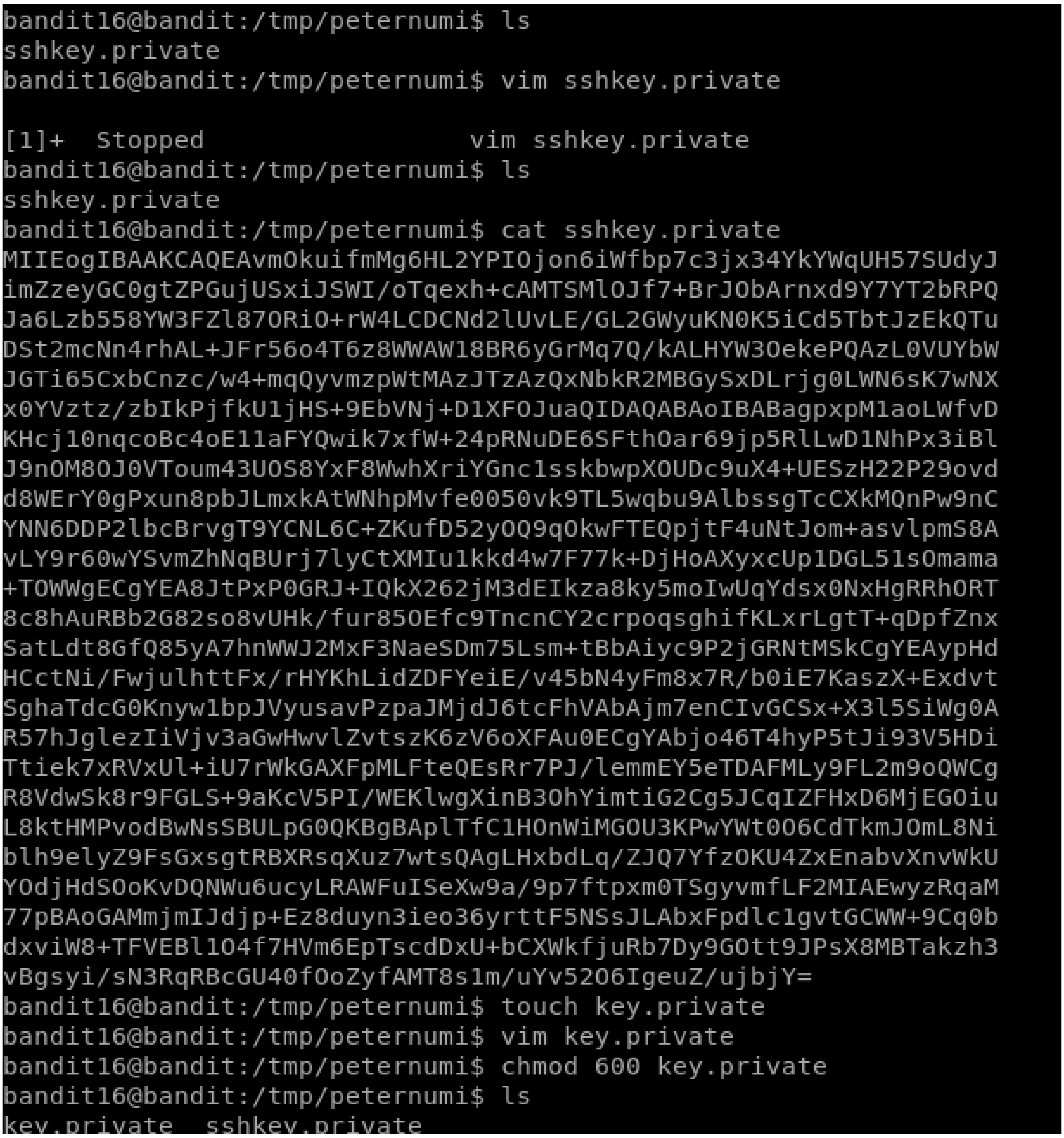
```
bandit16@bandit:~$ echo cluFn7wTiGryunymYOu4RcffSxQluehd |openssl s_client -quiet -connect localhost:31790
depth=0 CN = a9678380ab81
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = a9678380ab81
verify return:1
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ
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-----

read:errno=0
bandit16@bandit:~$ ssh -p 2220 bandit17@bandit.labs.overthewire.org
```



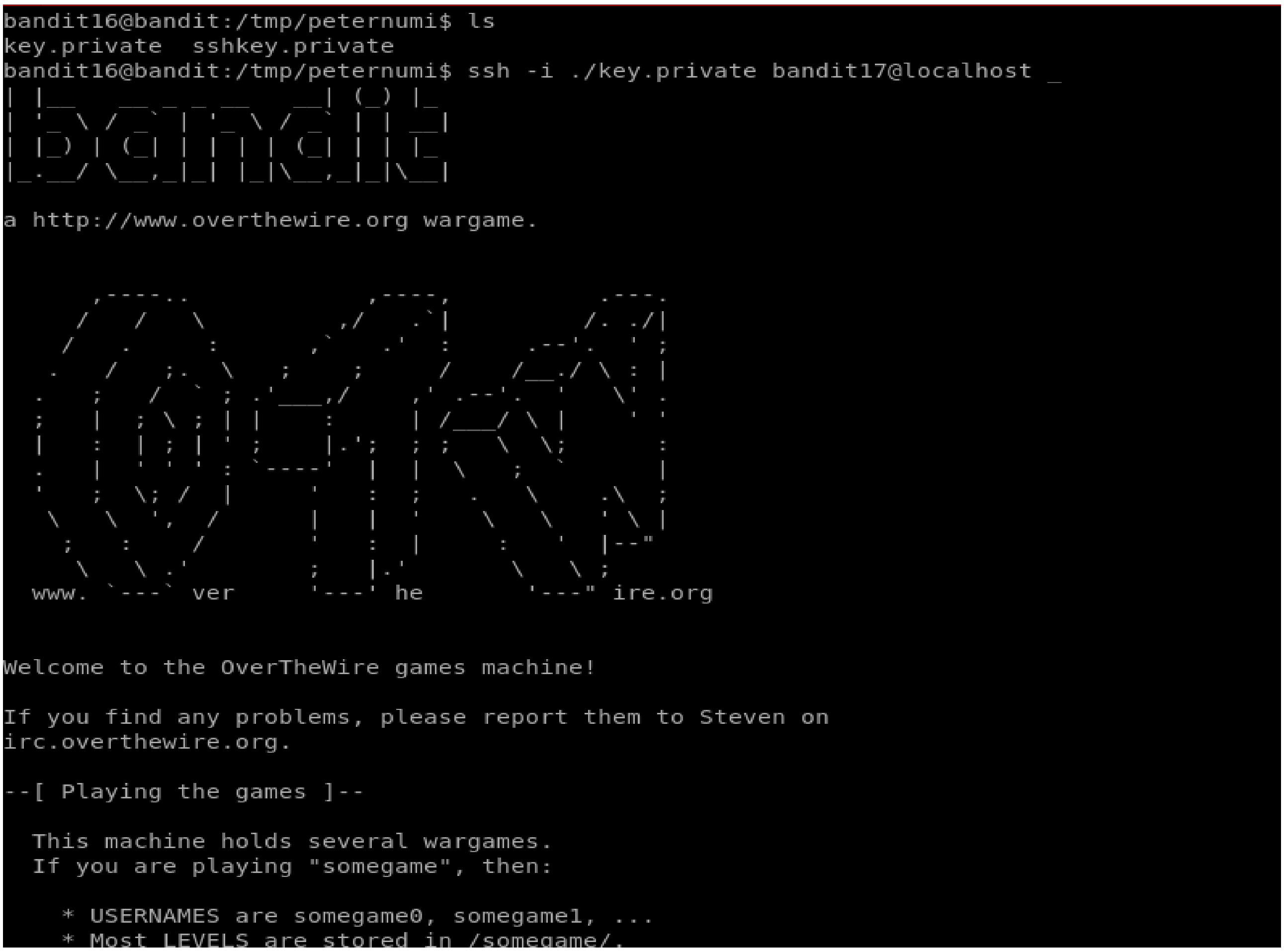
```
bandit16@bandit:~$ ssh -p 2220 bandit17@bandit.labs.overthewire.org
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([0.0.0.0]:2220)' can't be established.
ECDSA key fingerprint is ee:4c:8c:e7:57:2c:bc:63:24:b8:e6:23:27:63:72:9f.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[bandit.labs.overthewire.org]:2220,[0.0.0.0]:2220' (ECDSA) to the list of known hosts.
 _                     _ _ _
| |__   __ _ _ __   __| (_) |_
| '_ \ / _` | '_ \ / _` | | __|
| |_) | (_| | | | | (_| | | |_
|_.__/ \__,_|_| |_|\__,_|_|\__|

a http://www.overthewire.org wargame.

bandit17@bandit.labs.overthewire.org's password:

bandit16@bandit:~$ mkdir /tmp/peternumi
bandit16@bandit:~$ ls
bandit16@bandit:~$ cd /tmp/peternumi
bandit16@bandit:/tmp/peternumi$ ls
bandit16@bandit:/tmp/peternumi$ touch sshkey.private
bandit16@bandit:/tmp/peternumi$ vim sshkey.private
bandit16@bandit:/tmp/peternumi$ ssh -i ./sshkey.private bandit17@localhostThe authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is ee:4c:8c:e7:57:2c:bc:63:24:b8:e6:23:27:63:72:9f.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
 _                     _ _ _
| |__   __ _ _ __   __| (_) |_
| '_ \ / _` | '_ \ / _` | | __|
| |_) | (_| | | | | (_| | | |_
|_.__/ \__,_|_| |_|\__,_|_|\__|

a http://www.overthewire.org wargame.
```



```
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
 _                     _ _ _
| |__   __ _ _ __   __| (_) |_
| '_ \ / _` | '_ \ / _` | | __|
| |_) | (_| | | | | (_| | | |_
|_.__/ \__,_|_| |_|\__,_|_|\__|

a http://www.overthewire.org wargame.

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0664 for './sshkey.private' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
bad permissions: ignore key: ./sshkey.private
bandit17@localhost's password:
Permission denied, please try again.
bandit17@localhost's password:
Permission denied, please try again.
bandit17@localhost's password:
Permission denied (publickey,password).
bandit16@bandit:/tmp/peternumi$
bandit16@bandit:/tmp/peternumi$ ls
sshkey.private
bandit16@bandit:/tmp/peternumi$ chmod 600 sshkey.private
bandit16@bandit:/tmp/peternumi$ ssh -i ./sshkey.private bandit17@localhost _                     _ _ _
| |__   __ _ _ __   __| (_) |_
| '_ \ / _` | '_ \ / _` | | __|
| |_) | (_| | | | | (_| | | |_
|_.__/ \__,_|_| |_|\__,_|_|\__|

a http://www.overthewire.org wargame.
```



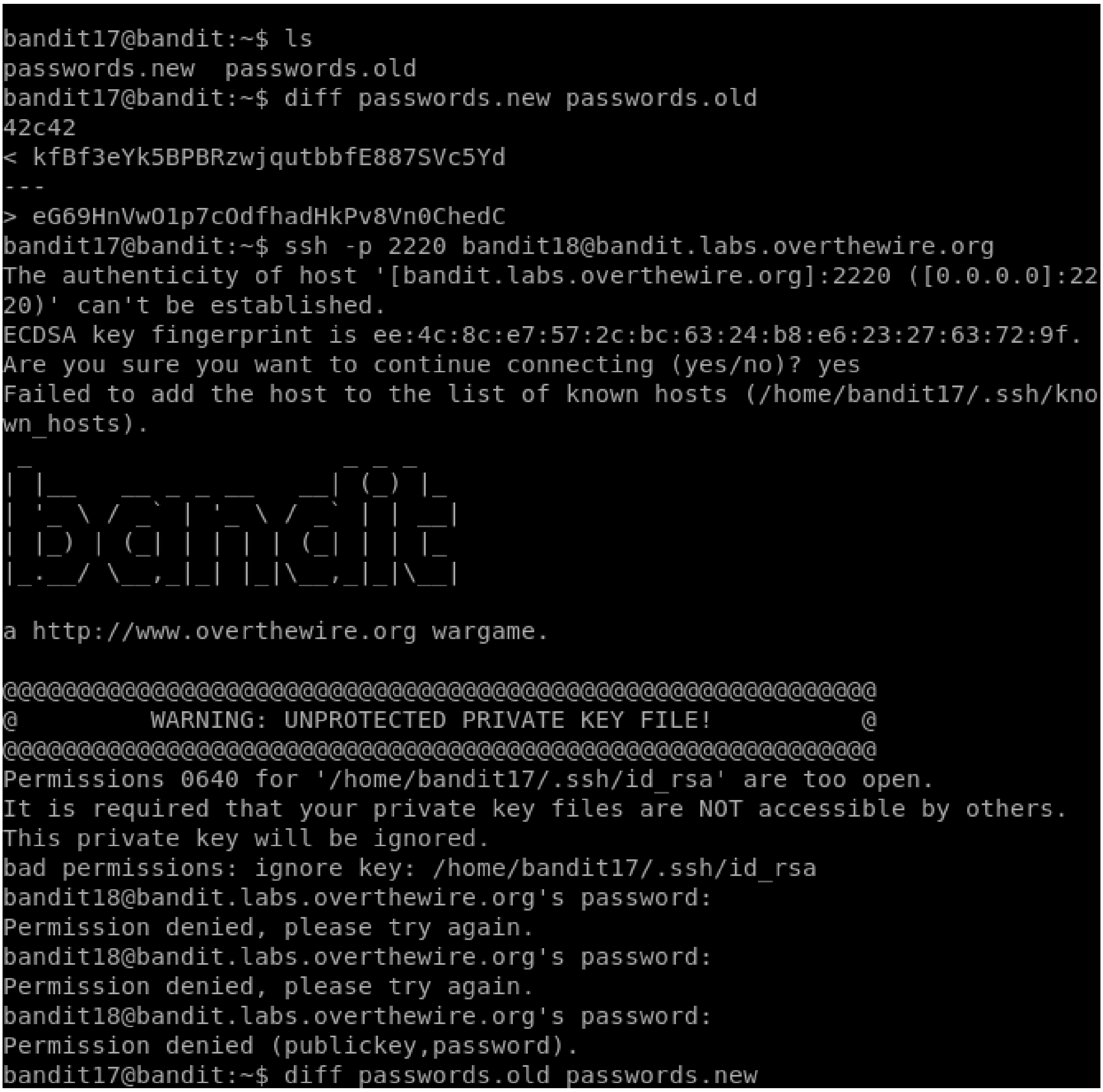
```
bandit16@bandit:/tmp/peternumi$ ls
sshkey.private
bandit16@bandit:/tmp/peternumi$ vim sshkey.private

[1]+  Stopped                 vim sshkey.private
bandit16@bandit:/tmp/peternumi$ ls
sshkey.private
bandit16@bandit:/tmp/peternumi$ cat sshkey.private
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=
bandit16@bandit:/tmp/peternumi$ touch key.private
bandit16@bandit:/tmp/peternumi$ vim key.private
bandit16@bandit:/tmp/peternumi$ chmod 600 key.private
bandit16@bandit:/tmp/peternumi$ ls
key.private  sshkey.private
```



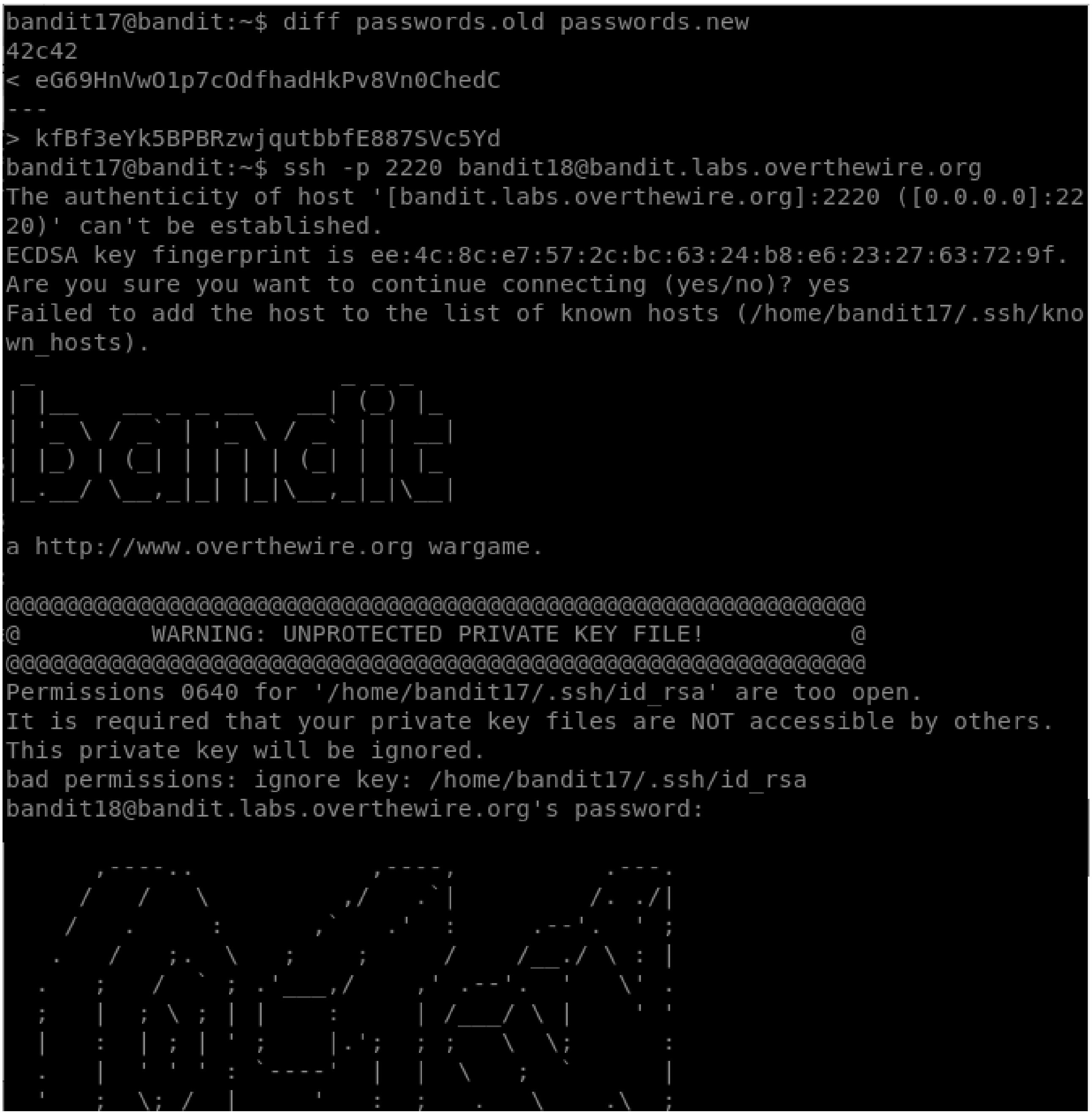
```
bandit16@bandit:/tmp/peternumi$ ls
key.private  sshkey.private
bandit16@bandit:/tmp/peternumi$ ssh -i ./key.private bandit17@localhost _
| |__   __ _ _ __   __| (_) |_
| '_ \ / _` | '_ \ / _` | | __|
| |_) | (_| | | | | (_| | | |_
|_.__/ \__,_|_| |_|\__,_|_|\__|

a http://www.overthewire.org wargame.


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


Welcome to the OverTheWire games machine!

If you find any problems, please report them to Steven on
irc.overthewire.org.

--[ Playing the games ]--

  This machine holds several wargames.
  If you are playing "somegame", then:

    * USERNAMES are somegame0, somegame1, ...
    * Most LEVELS are stored in /somegame/.
```

<u>Level 17 to Level 18:</u>

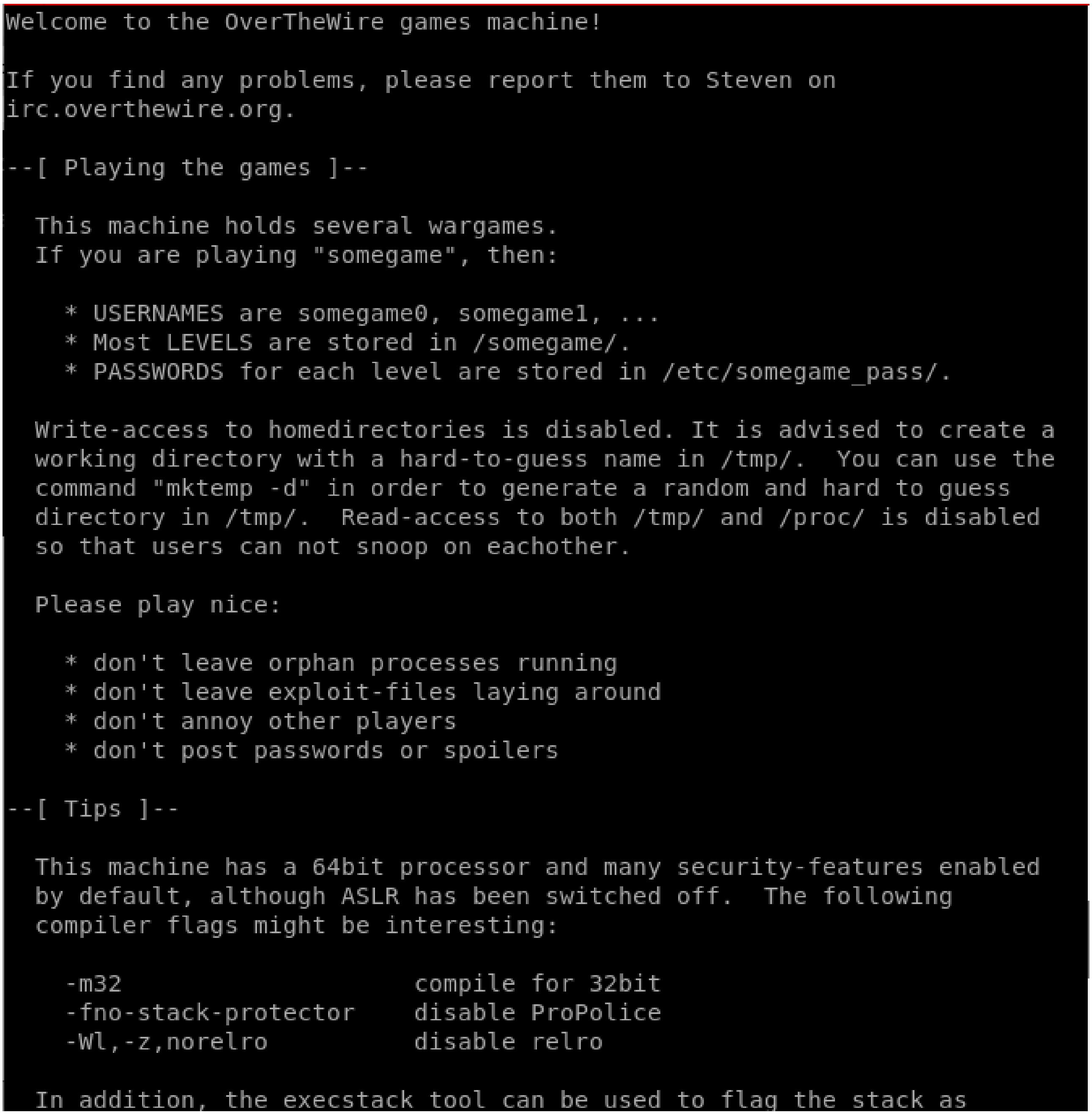
#ls
#man diff
#diff passwords.old passwords.new
#ssh -p 2220 bandit18@bandit.labs.overthewire.org



```
bandit17@bandit:~$ ls
passwords.new  passwords.old
bandit17@bandit:~$ diff passwords.new passwords.old
42c42
< kfBf3eYk5BPBRzwjqutbbfE887SVc5Yd
---
> eG69HnVwO1p7cOdfhadHkPv8Vn0ChedC
bandit17@bandit:~$ ssh -p 2220 bandit18@bandit.labs.overthewire.org
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([0.0.0.0]:22
20)' can't be established.
ECDSA key fingerprint is ee:4c:8c:e7:57:2c:bc:63:24:b8:e6:23:27:63:72:9f.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit17/.ssh/kno
wn_hosts).
 _                     _ _ _
| |__   __ _ _ __   __| (_) |_
| '_ \ / _` | '_ \ / _` | | __|
| |_) | (_| | | | | (_| | | |_
|_.__/ \__,_|_| |_|\__,_|_|\__|

a http://www.overthewire.org wargame.

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0640 for '/home/bandit17/.ssh/id_rsa' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
bad permissions: ignore key: /home/bandit17/.ssh/id_rsa
bandit18@bandit.labs.overthewire.org's password:
Permission denied, please try again.
bandit18@bandit.labs.overthewire.org's password:
Permission denied, please try again.
bandit18@bandit.labs.overthewire.org's password:
Permission denied (publickey,password).
bandit17@bandit:~$ diff passwords.old passwords.new
```

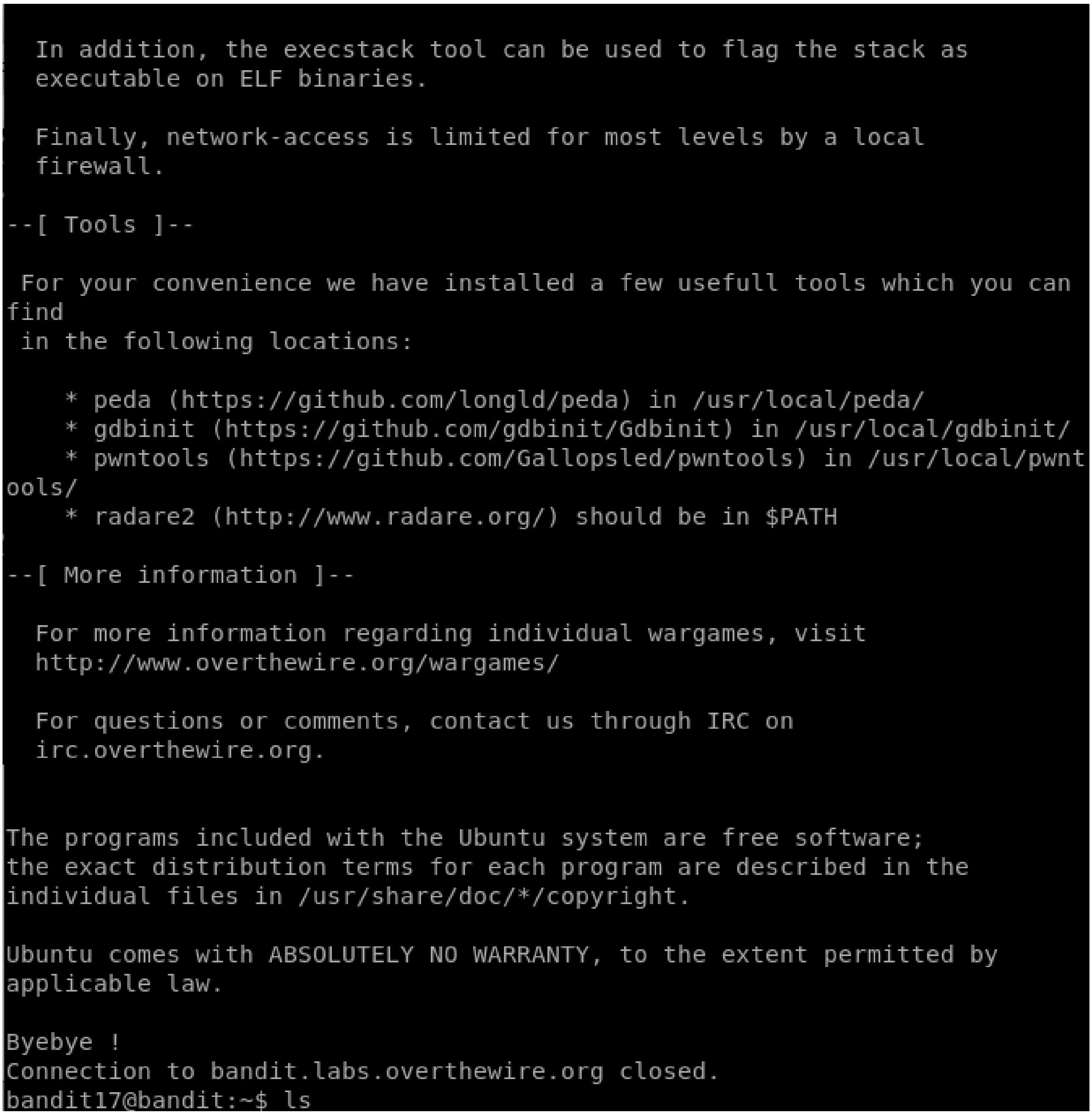


```
bandit17@bandit:~$ diff passwords.old passwords.new
42c42
< eG69HnVwO1p7cOdfhadHkPv8Vn0ChedC
---
> kfBf3eYk5BPBRzwjqutbbfE887SVc5Yd
bandit17@bandit:~$ ssh -p 2220 bandit18@bandit.labs.overthewire.org
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([0.0.0.0]:22
20)' can't be established.
ECDSA key fingerprint is ee:4c:8c:e7:57:2c:bc:63:24:b8:e6:23:27:63:72:9f.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit17/.ssh/kno
wn_hosts).
 _                     _ _ _
| |__   __ _ _ __   __| (_) |_
| '_ \ / _` | '_ \ / _` | | __|
| |_) | (_| | | | | (_| | | |_
|_.__/ \__,_|_| |_|\__,_|_|\__|

a http://www.overthewire.org wargame.

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0640 for '/home/bandit17/.ssh/id_rsa' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
bad permissions: ignore key: /home/bandit17/.ssh/id_rsa
bandit18@bandit.labs.overthewire.org's password:

      ,----..            ,----,          .---.
     /   /   \         ,/   .`|         /. ./|
    /   .     :      ,`   .'  :     .--'.  ' ;
   .   /   ;.  \   ;     ;      /    /__./ \ : |
  .   ;   /  ` ; .'___,/    ,' .--'.  '   \' .
  ;   |  ; \ ; | |    :     |  /___/ \ |    ' '
  |   :  | ; | ' ;    |.';  ;  ;   \  \;      :
  .   |  ' ' ' : `----'  |  |  \   ;  `      |
  '   ;  \; /  |      '   :  ;   .   \    .\  ;
```



```
Welcome to the OverTheWire games machine!

If you find any problems, please report them to Steven on
irc.overthewire.org.

--[ Playing the games ]--

  This machine holds several wargames.
  If you are playing "somegame", then:

    * USERNAMES are somegame0, somegame1, ...
    * Most LEVELS are stored in /somegame/.
    * PASSWORDS for each level are stored in /etc/somegame_pass/.

  Write-access to homedirectories is disabled. It is advised to create a
  working directory with a hard-to-guess name in /tmp/.  You can use the
  command "mktemp -d" in order to generate a random and hard to guess
  directory in /tmp/.  Read-access to both /tmp/ and /proc/ is disabled
  so that users can not snoop on eachother.

  Please play nice:

    * don't leave orphan processes running
    * don't leave exploit-files laying around
    * don't annoy other players
    * don't post passwords or spoilers

--[ Tips ]--

  This machine has a 64bit processor and many security-features enabled
  by default, although ASLR has been switched off.  The following
  compiler flags might be interesting:

    -m32                    compile for 32bit
    -fno-stack-protector    disable ProPolice
    -Wl,-z,norelro          disable relro

  In addition, the execstack tool can be used to flag the stack as
```

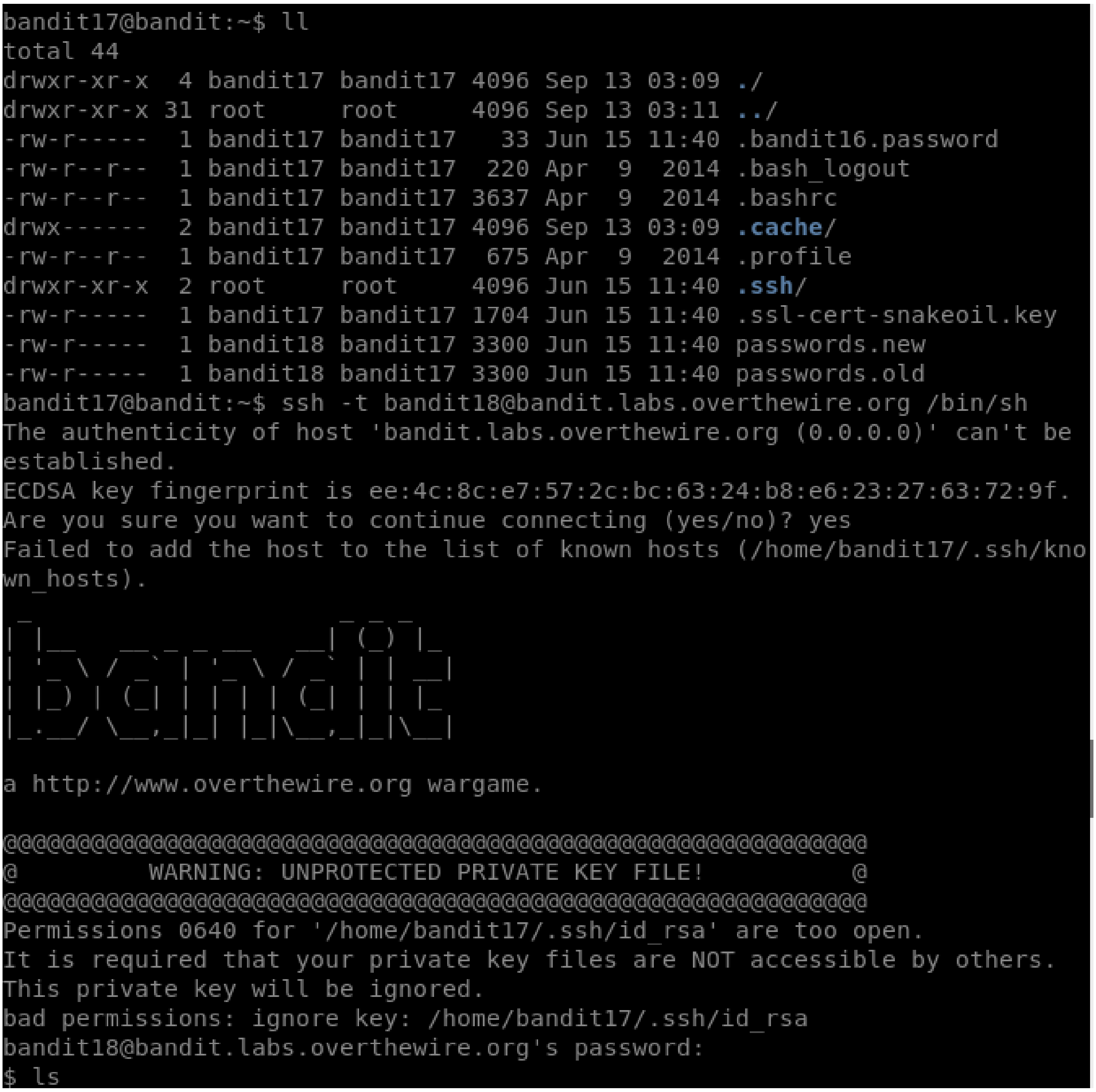
password: eG69HnVwO1p7cOdfhadHkPv8Vn0ChedC



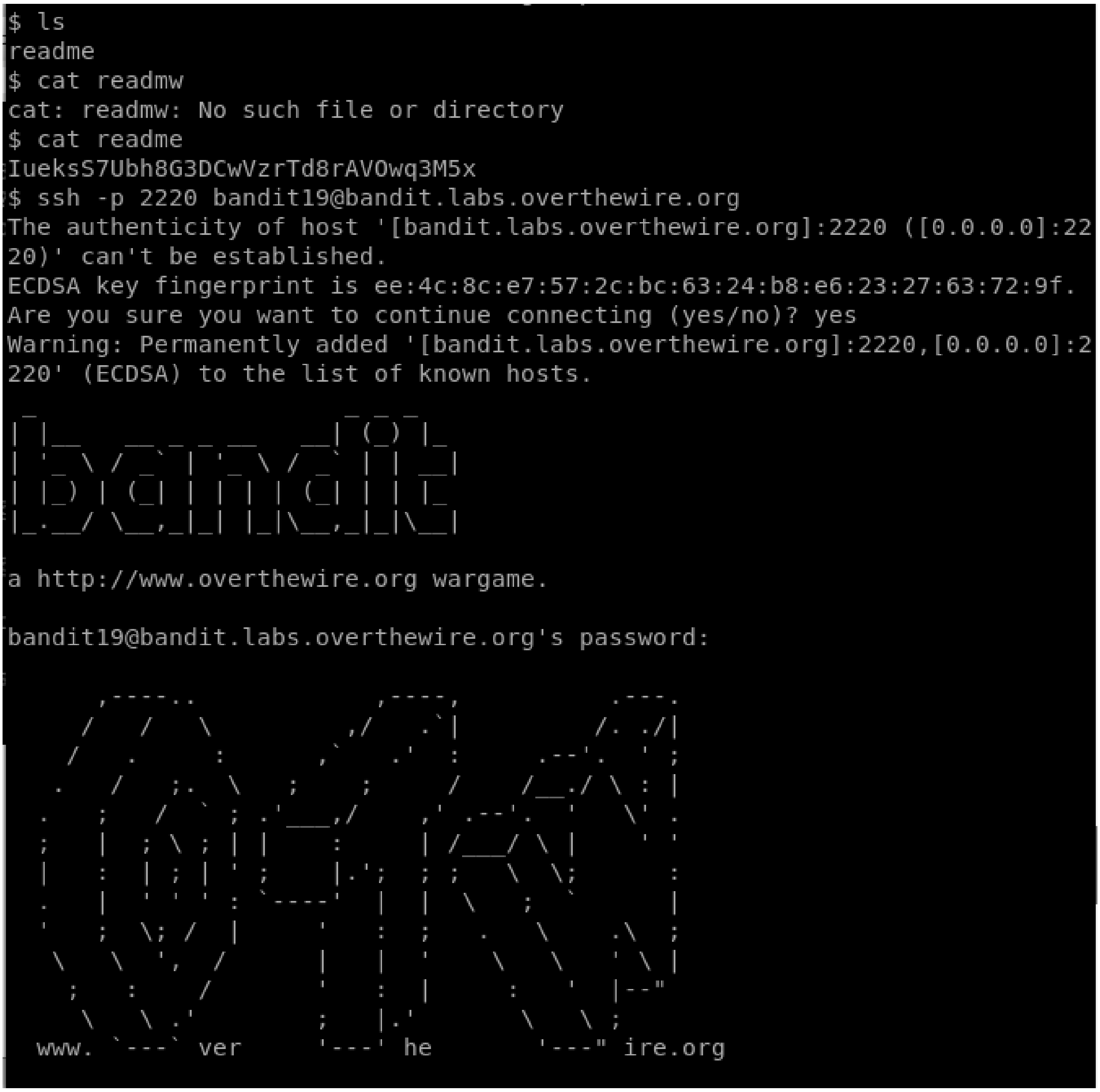
```
  In addition, the execstack tool can be used to flag the stack as
  executable on ELF binaries.

  Finally, network-access is limited for most levels by a local
  firewall.

--[ Tools ]--

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

    * peda (https://github.com/longld/peda) in /usr/local/peda/
    * gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
    * pwntools (https://github.com/Gallopsled/pwntools) in /usr/local/pwnt
ools/
    * radare2 (http://www.radare.org/) should be in $PATH

--[ 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.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Byebye !
Connection to bandit.labs.overthewire.org closed.
bandit17@bandit:~$ ls
```

Level 18 to Level 19:

#ll
#bandit -t bandit18@bandit.labs.overthewire.org /*bin*/sh
#ls
#cat readme
#ssh -p 2220 bandit19@bandit.labs.overthewire.org



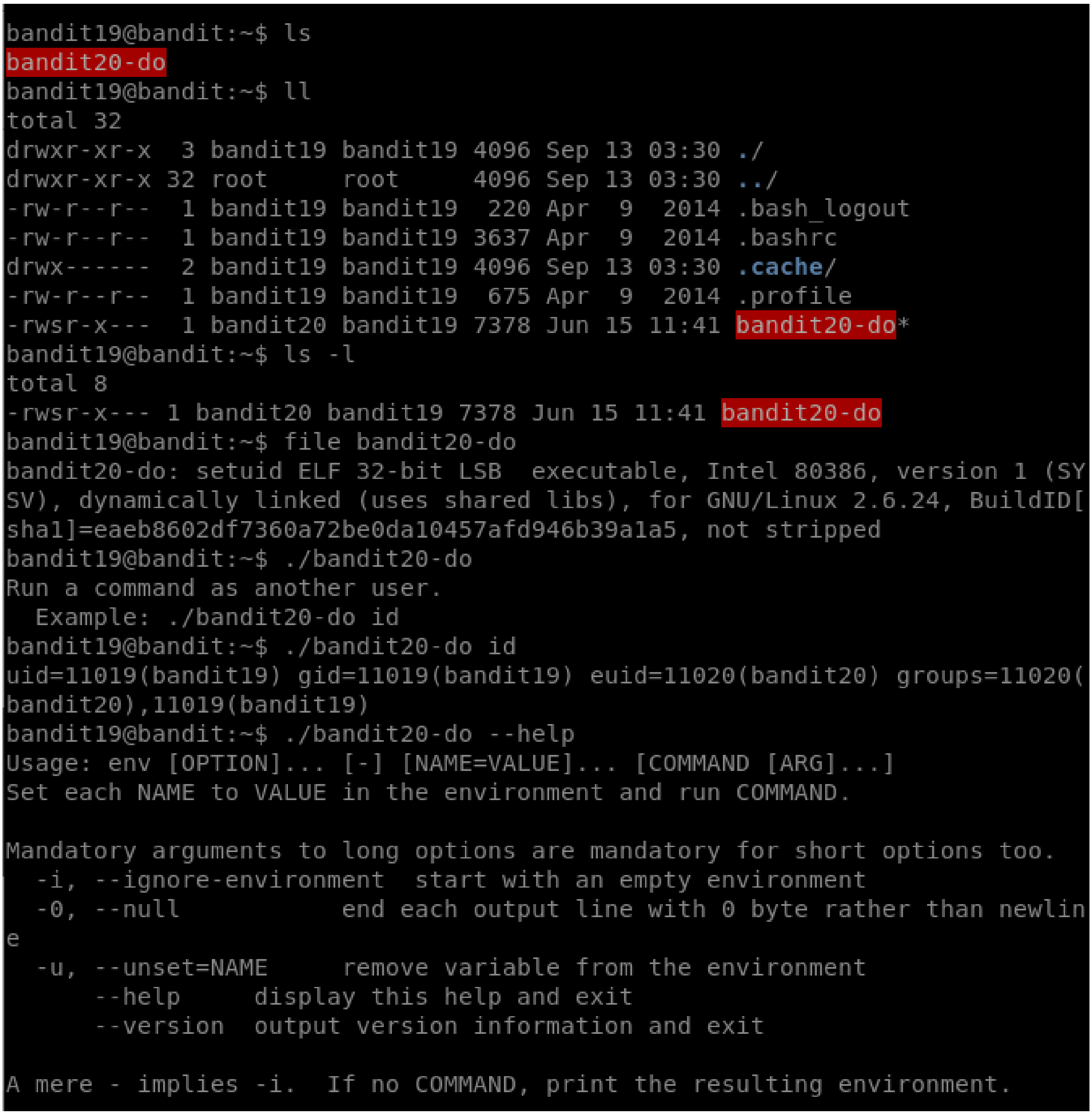
```
bandit17@bandit:~$ ll
total 44
drwxr-xr-x  4 bandit17 bandit17 4096 Sep 13 03:09 ./
drwxr-xr-x 31 root     root     4096 Sep 13 03:11 ../
-rw-r-----  1 bandit17 bandit17   33 Jun 15 11:40 .bandit16.password
-rw-r--r--  1 bandit17 bandit17  220 Apr  9  2014 .bash_logout
-rw-r--r--  1 bandit17 bandit17 3637 Apr  9  2014 .bashrc
drwx------  2 bandit17 bandit17 4096 Sep 13 03:09 .cache/
-rw-r--r--  1 bandit17 bandit17  675 Apr  9  2014 .profile
drwxr-xr-x  2 root     root     4096 Jun 15 11:40 .ssh/
-rw-r-----  1 bandit17 bandit17 1704 Jun 15 11:40 .ssl-cert-snakeoil.key
-rw-r-----  1 bandit18 bandit17 3300 Jun 15 11:40 passwords.new
-rw-r-----  1 bandit18 bandit17 3300 Jun 15 11:40 passwords.old
bandit17@bandit:~$ ssh -t bandit18@bandit.labs.overthewire.org /bin/sh
The authenticity of host 'bandit.labs.overthewire.org (0.0.0.0)' can't be
established.
ECDSA key fingerprint is ee:4c:8c:e7:57:2c:bc:63:24:b8:e6:23:27:63:72:9f.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit17/.ssh/kno
wn_hosts).
 _                     _ _ _
| |__   __ _ _ __   __| (_) |_
| '_ \ / _` | '_ \ / _` | | __|
| |_) | (_| | | | | (_| | | |_
|_.__/ \__,_|_| |_|\__,_|_|\__|

a http://www.overthewire.org wargame.

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0640 for '/home/bandit17/.ssh/id_rsa' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
bad permissions: ignore key: /home/bandit17/.ssh/id_rsa
bandit18@bandit.labs.overthewire.org's password:
$ ls
```



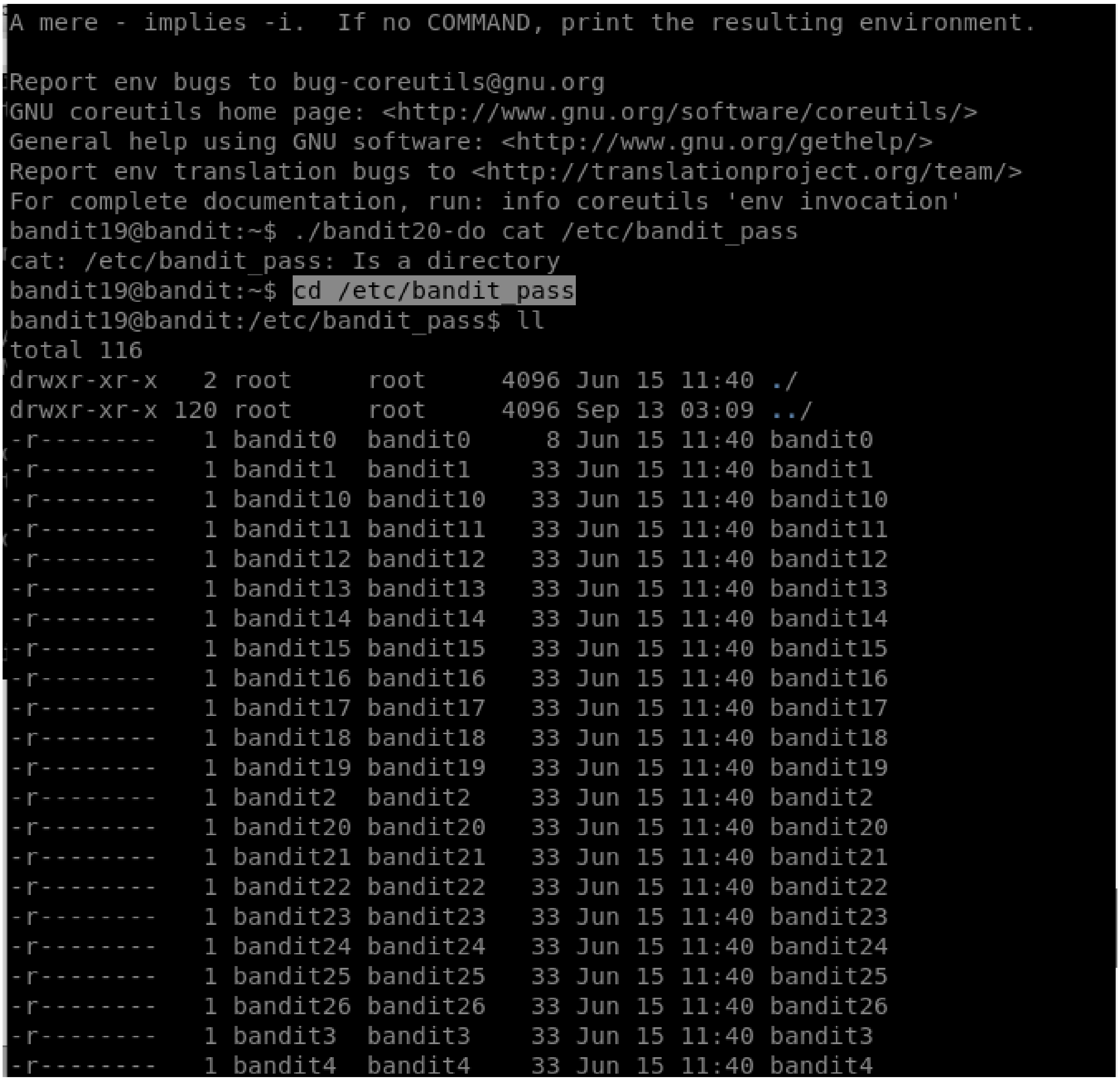
```
$ ls
readme
$ cat readmw
cat: readmw: No such file or directory
$ cat readme
IueksS7Ubh8G3DCwVzrTd8rAVOwq3M5x
$ ssh -p 2220 bandit19@bandit.labs.overthewire.org
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([0.0.0.0]:22
20)' can't be established.
ECDSA key fingerprint is ee:4c:8c:e7:57:2c:bc:63:24:b8:e6:23:27:63:72:9f.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[bandit.labs.overthewire.org]:2220,[0.0.0.0]:2
220' (ECDSA) to the list of known hosts.
 _                     _ _ _
| |__   __ _ _ __   __| (_) |_
| '_ \ / _` | '_ \ / _` | | __|
| |_) | (_| | | | | (_| | | |_
|_.__/ \__,_|_| |_|\__,_|_|\__|

a http://www.overthewire.org wargame.

bandit19@bandit.labs.overthewire.org's password:

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

Level 19 to Level 20:

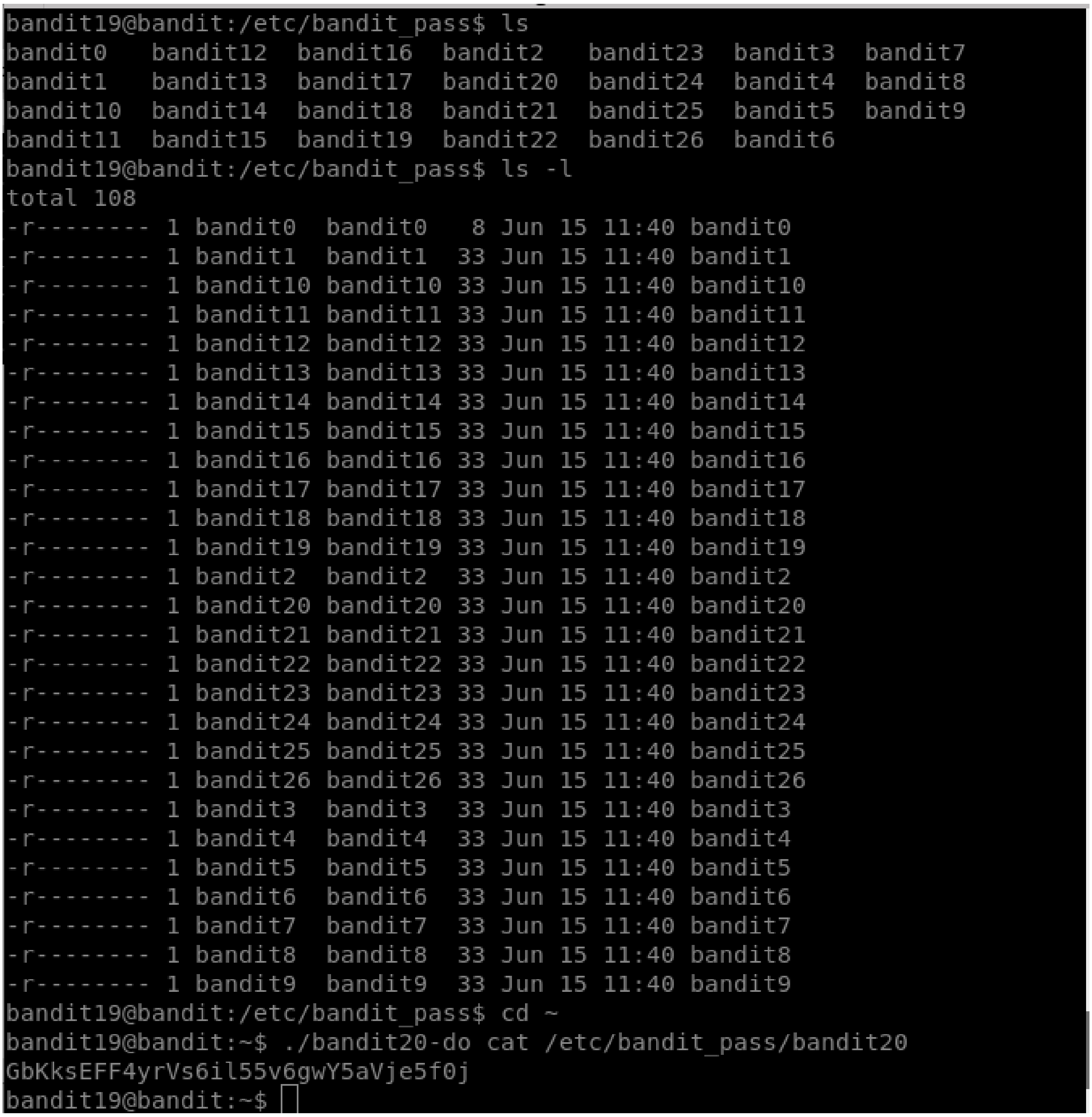
#ls
#file bandit20-do
#./bandit20-do
#./bandit20-do id
#./bandit20-do --help
#./bandit20-do cat /etc/bandit_pass
#cd /etc/bandit_pass
#ll
#ls -l
#ls
#cd ~
#cd /etc/bandit_pass cat /*etc*/bandit_pass/bandit20
#ssh -p 2220 bandit20@bandit.labs.overthewire.org



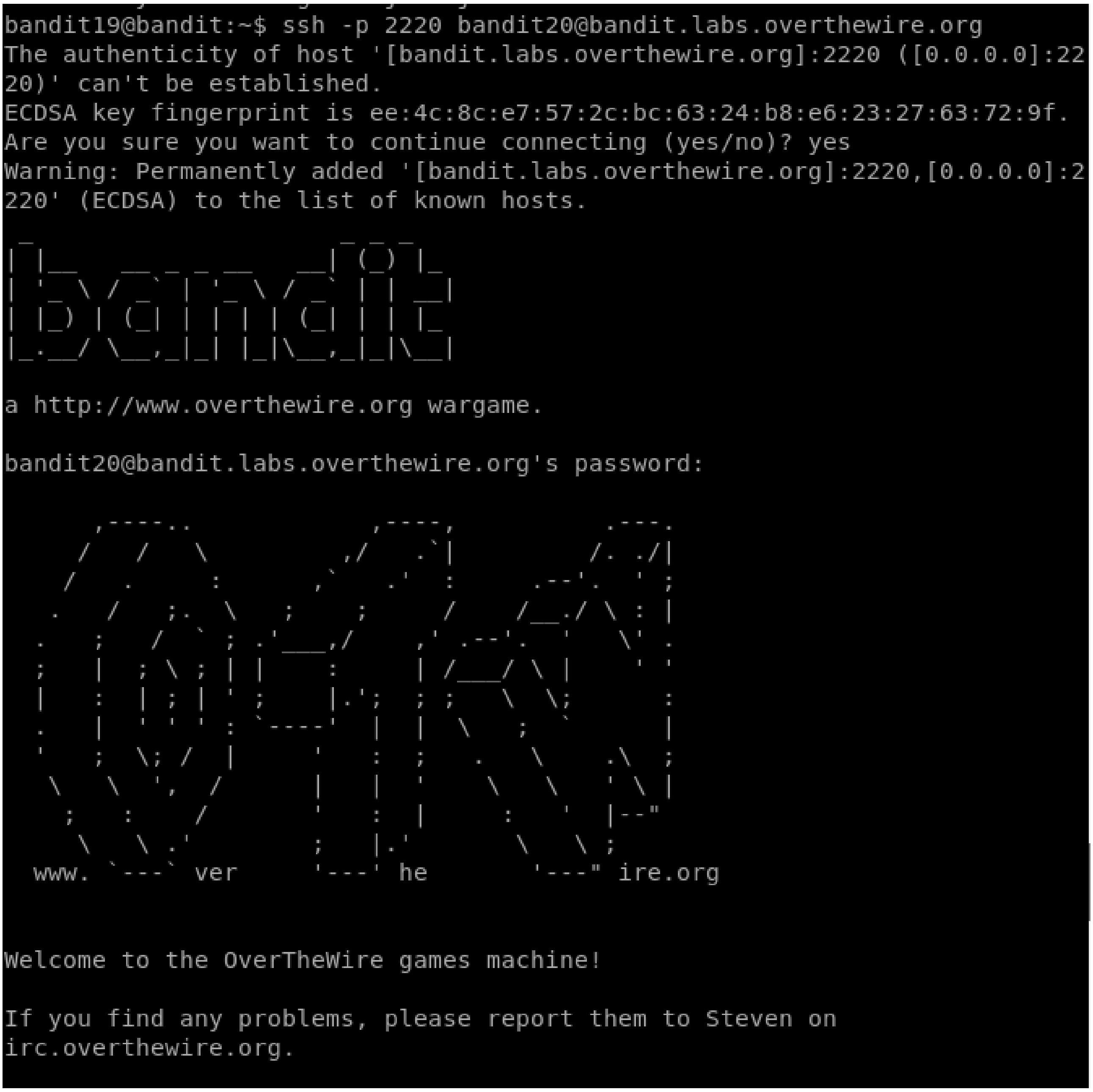
```
bandit19@bandit:~$ ls
bandit20-do
bandit19@bandit:~$ ll
total 32
drwxr-xr-x  3 bandit19 bandit19 4096 Sep 13 03:30 ./
drwxr-xr-x 32 root     root     4096 Sep 13 03:30 ../
-rw-r--r--  1 bandit19 bandit19  220 Apr  9  2014 .bash_logout
-rw-r--r--  1 bandit19 bandit19 3637 Apr  9  2014 .bashrc
drwx------  2 bandit19 bandit19 4096 Sep 13 03:30 .cache/
-rw-r--r--  1 bandit19 bandit19  675 Apr  9  2014 .profile
-rwsr-x---  1 bandit20 bandit19 7378 Jun 15 11:41 bandit20-do*
bandit19@bandit:~$ ls -l
total 8
-rwsr-x--- 1 bandit20 bandit19 7378 Jun 15 11:41 bandit20-do
bandit19@bandit:~$ file bandit20-do
bandit20-do: setuid ELF 32-bit LSB  executable, Intel 80386, version 1 (SY
SV), dynamically linked (uses shared libs), for GNU/Linux 2.6.24, BuildID[
sha1]=eaeb8602df7360a72be0da10457afd946b39a1a5, not stripped
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=11020(
bandit20),11019(bandit19)
bandit19@bandit:~$ ./bandit20-do --help
Usage: env [OPTION]... [-] [NAME=VALUE]... [COMMAND [ARG]...]
Set each NAME to VALUE in the environment and run COMMAND.

Mandatory arguments to long options are mandatory for short options too.
  -i, --ignore-environment  start with an empty environment
  -0, --null           end each output line with 0 byte rather than newlin
e
  -u, --unset=NAME     remove variable from the environment
      --help     display this help and exit
      --version  output version information and exit

A mere - implies -i.  If no COMMAND, print the resulting environment.
```



```
A mere - implies -i.  If no COMMAND, print the resulting environment.

Report env bugs to bug-coreutils@gnu.org
GNU coreutils home page: <http://www.gnu.org/software/coreutils/>
General help using GNU software: <http://www.gnu.org/gethelp/>
Report env translation bugs to <http://translationproject.org/team/>
For complete documentation, run: info coreutils 'env invocation'
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass
cat: /etc/bandit_pass: Is a directory
bandit19@bandit:~$ cd /etc/bandit_pass
bandit19@bandit:/etc/bandit_pass$ ll
total 116
drwxr-xr-x   2 root     root     4096 Jun 15 11:40 ./
drwxr-xr-x 120 root     root     4096 Sep 13 03:09 ../
-r--------   1 bandit0  bandit0     8 Jun 15 11:40 bandit0
-r--------   1 bandit1  bandit1    33 Jun 15 11:40 bandit1
-r--------   1 bandit10 bandit10   33 Jun 15 11:40 bandit10
-r--------   1 bandit11 bandit11   33 Jun 15 11:40 bandit11
-r--------   1 bandit12 bandit12   33 Jun 15 11:40 bandit12
-r--------   1 bandit13 bandit13   33 Jun 15 11:40 bandit13
-r--------   1 bandit14 bandit14   33 Jun 15 11:40 bandit14
-r--------   1 bandit15 bandit15   33 Jun 15 11:40 bandit15
-r--------   1 bandit16 bandit16   33 Jun 15 11:40 bandit16
-r--------   1 bandit17 bandit17   33 Jun 15 11:40 bandit17
-r--------   1 bandit18 bandit18   33 Jun 15 11:40 bandit18
-r--------   1 bandit19 bandit19   33 Jun 15 11:40 bandit19
-r--------   1 bandit2  bandit2    33 Jun 15 11:40 bandit2
-r--------   1 bandit20 bandit20   33 Jun 15 11:40 bandit20
-r--------   1 bandit21 bandit21   33 Jun 15 11:40 bandit21
-r--------   1 bandit22 bandit22   33 Jun 15 11:40 bandit22
-r--------   1 bandit23 bandit23   33 Jun 15 11:40 bandit23
-r--------   1 bandit24 bandit24   33 Jun 15 11:40 bandit24
-r--------   1 bandit25 bandit25   33 Jun 15 11:40 bandit25
-r--------   1 bandit26 bandit26   33 Jun 15 11:40 bandit26
-r--------   1 bandit3  bandit3    33 Jun 15 11:40 bandit3
-r--------   1 bandit4  bandit4    33 Jun 15 11:40 bandit4
```



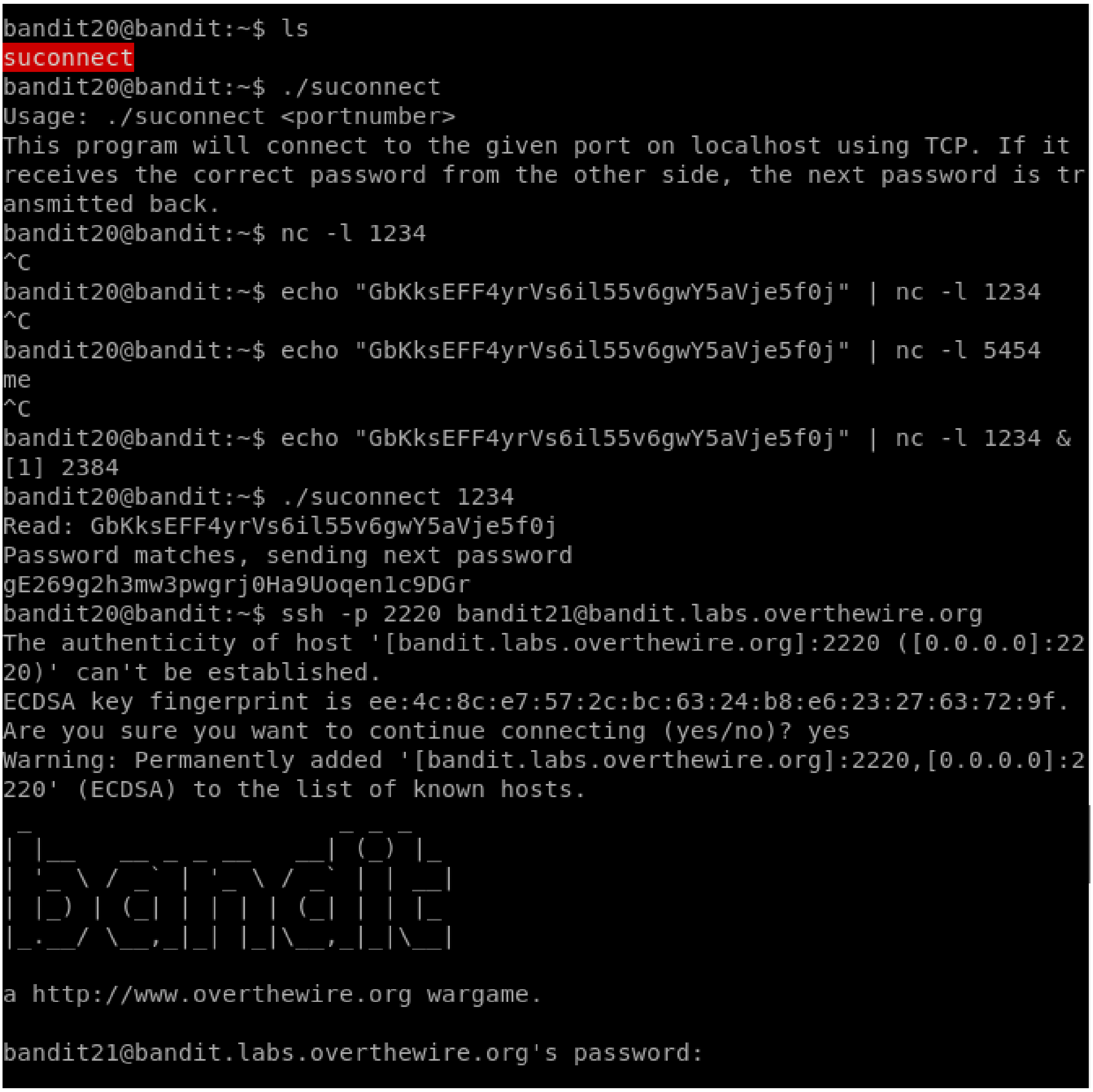
```
bandit19@bandit:/etc/bandit_pass$ ls
bandit0   bandit12  bandit16  bandit2   bandit23  bandit3  bandit7
bandit1   bandit13  bandit17  bandit20  bandit24  bandit4  bandit8
bandit10  bandit14  bandit18  bandit21  bandit25  bandit5  bandit9
bandit11  bandit15  bandit19  bandit22  bandit26  bandit6
bandit19@bandit:/etc/bandit_pass$ ls -l
total 108
-r-------- 1 bandit0  bandit0   8 Jun 15 11:40 bandit0
-r-------- 1 bandit1  bandit1  33 Jun 15 11:40 bandit1
-r-------- 1 bandit10 bandit10 33 Jun 15 11:40 bandit10
-r-------- 1 bandit11 bandit11 33 Jun 15 11:40 bandit11
-r-------- 1 bandit12 bandit12 33 Jun 15 11:40 bandit12
-r-------- 1 bandit13 bandit13 33 Jun 15 11:40 bandit13
-r-------- 1 bandit14 bandit14 33 Jun 15 11:40 bandit14
-r-------- 1 bandit15 bandit15 33 Jun 15 11:40 bandit15
-r-------- 1 bandit16 bandit16 33 Jun 15 11:40 bandit16
-r-------- 1 bandit17 bandit17 33 Jun 15 11:40 bandit17
-r-------- 1 bandit18 bandit18 33 Jun 15 11:40 bandit18
-r-------- 1 bandit19 bandit19 33 Jun 15 11:40 bandit19
-r-------- 1 bandit2  bandit2  33 Jun 15 11:40 bandit2
-r-------- 1 bandit20 bandit20 33 Jun 15 11:40 bandit20
-r-------- 1 bandit21 bandit21 33 Jun 15 11:40 bandit21
-r-------- 1 bandit22 bandit22 33 Jun 15 11:40 bandit22
-r-------- 1 bandit23 bandit23 33 Jun 15 11:40 bandit23
-r-------- 1 bandit24 bandit24 33 Jun 15 11:40 bandit24
-r-------- 1 bandit25 bandit25 33 Jun 15 11:40 bandit25
-r-------- 1 bandit26 bandit26 33 Jun 15 11:40 bandit26
-r-------- 1 bandit3  bandit3  33 Jun 15 11:40 bandit3
-r-------- 1 bandit4  bandit4  33 Jun 15 11:40 bandit4
-r-------- 1 bandit5  bandit5  33 Jun 15 11:40 bandit5
-r-------- 1 bandit6  bandit6  33 Jun 15 11:40 bandit6
-r-------- 1 bandit7  bandit7  33 Jun 15 11:40 bandit7
-r-------- 1 bandit8  bandit8  33 Jun 15 11:40 bandit8
-r-------- 1 bandit9  bandit9  33 Jun 15 11:40 bandit9
bandit19@bandit:/etc/bandit_pass$ cd ~
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
GbKksEFF4yrVs6il55v6gwY5aVje5f0j
bandit19@bandit:~$ 
```



```
bandit19@bandit:~$ ssh -p 2220 bandit20@bandit.labs.overthewire.org
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([0.0.0.0]:22
20)' can't be established.
ECDSA key fingerprint is ee:4c:8c:e7:57:2c:bc:63:24:b8:e6:23:27:63:72:9f.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[bandit.labs.overthewire.org]:2220,[0.0.0.0]:2
220' (ECDSA) to the list of known hosts.
 _                     _ _ _
| |__   __ _ _ __   __| (_) |_
| '_ \ / _` | '_ \ / _` | | __|
| |_) | (_| | | | | (_| | | |_
|_.__/ \__,_|_| |_|\__,_|_|\__|

a http://www.overthewire.org wargame.

bandit20@bandit.labs.overthewire.org's password:

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


Welcome to the OverTheWire games machine!

If you find any problems, please report them to Steven on
irc.overthewire.org.
```

Level 20 to Level 21:

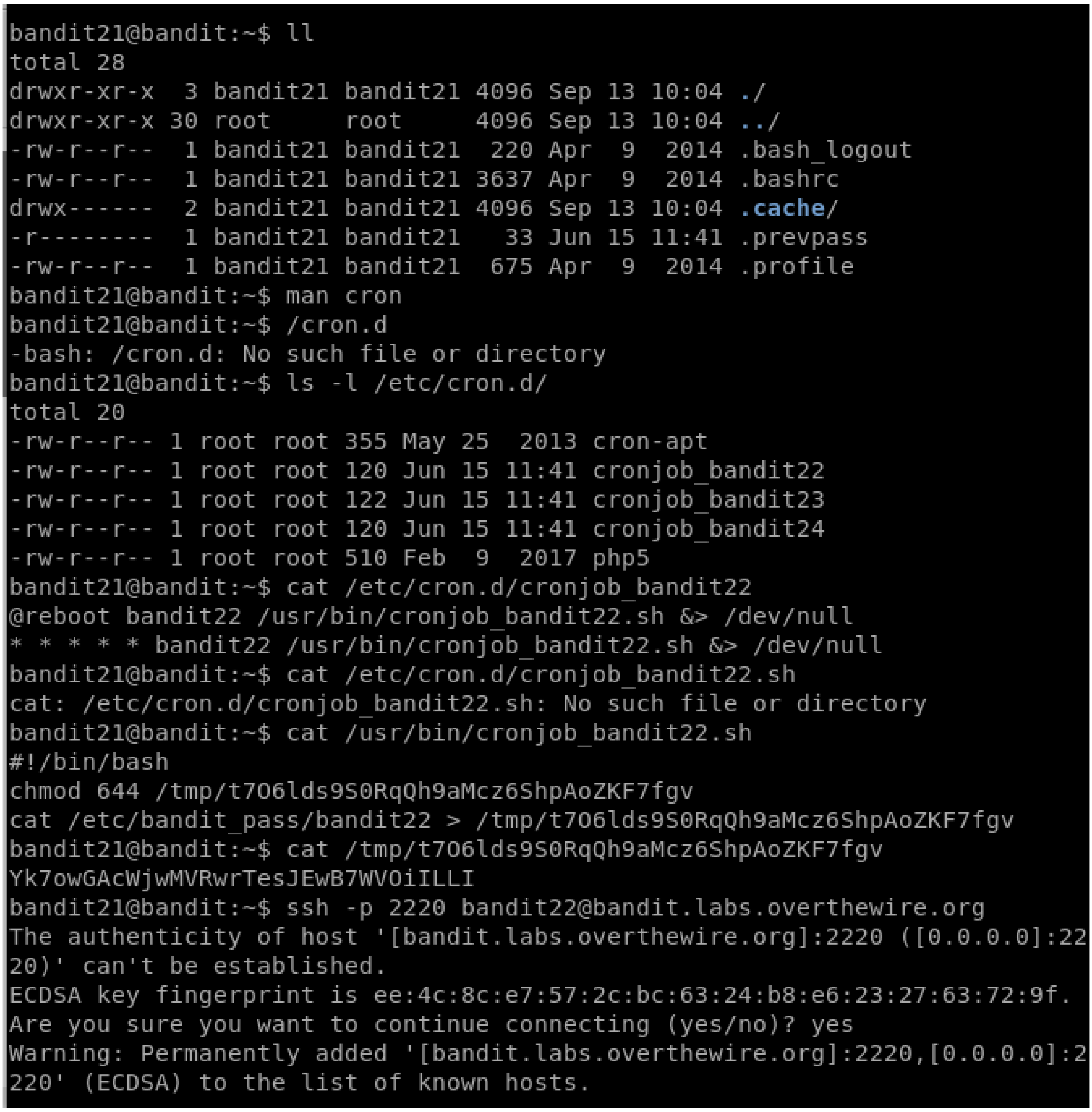
#ls
#./suconnect
#echo "GbKksEFF4yrVs6il55v6gwY5aVje5f0j" | nc -l 1234 &
#./suconnect 1234
#ssh -p 2220 bandit21@bandit.labs.overthewire.org



```
bandit20@bandit:~$ ls
suconnect
bandit20@bandit:~$ ./suconnect
Usage: ./suconnect <portnumber>
This program will connect to the given port on localhost using TCP. If it
receives the correct password from the other side, the next password is tr
ansmitted back.
bandit20@bandit:~$ nc -l 1234
^C
bandit20@bandit:~$ echo "GbKksEFF4yrVs6il55v6gwY5aVje5f0j" | nc -l 1234
^C
bandit20@bandit:~$ echo "GbKksEFF4yrVs6il55v6gwY5aVje5f0j" | nc -l 5454
me
^C
bandit20@bandit:~$ echo "GbKksEFF4yrVs6il55v6gwY5aVje5f0j" | nc -l 1234 &
[1] 2384
bandit20@bandit:~$ ./suconnect 1234
Read: GbKksEFF4yrVs6il55v6gwY5aVje5f0j
Password matches, sending next password
gE269g2h3mw3pwgrj0Ha9Uoqen1c9DGr
bandit20@bandit:~$ ssh -p 2220 bandit21@bandit.labs.overthewire.org
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([0.0.0.0]:22
20)' can't be established.
ECDSA key fingerprint is ee:4c:8c:e7:57:2c:bc:63:24:b8:e6:23:27:63:72:9f.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[bandit.labs.overthewire.org]:2220,[0.0.0.0]:2
220' (ECDSA) to the list of known hosts.
 _                     _ _ _
| |__   __ _ _ __   __| (_) |_
| '_ \ / _` | '_ \ / _` | | __|
| |_) | (_| | | | | (_| | | |_
|_.__/ \__,_|_| |_|\__,_|_|\__|

a http://www.overthewire.org wargame.

bandit21@bandit.labs.overthewire.org's password:
```

Level 21 to Level 22:

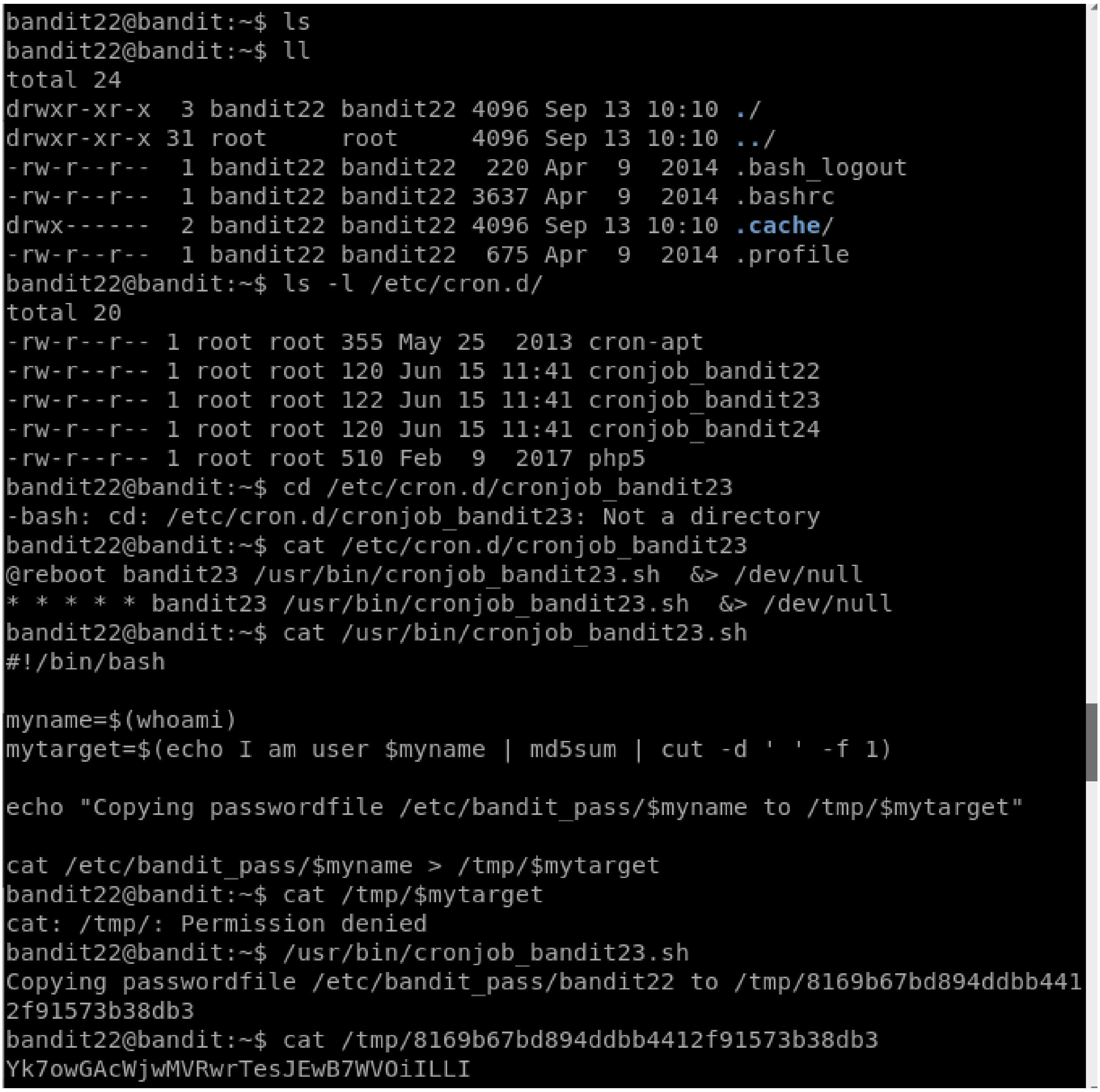
#ll
#ls -l ***/etc/cron.d/***
#cat /usr/bin/cronjob_bandit22.sh
#cat /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv
#ssh -p 2220 bandit22@bandit.labs.overthewire.org



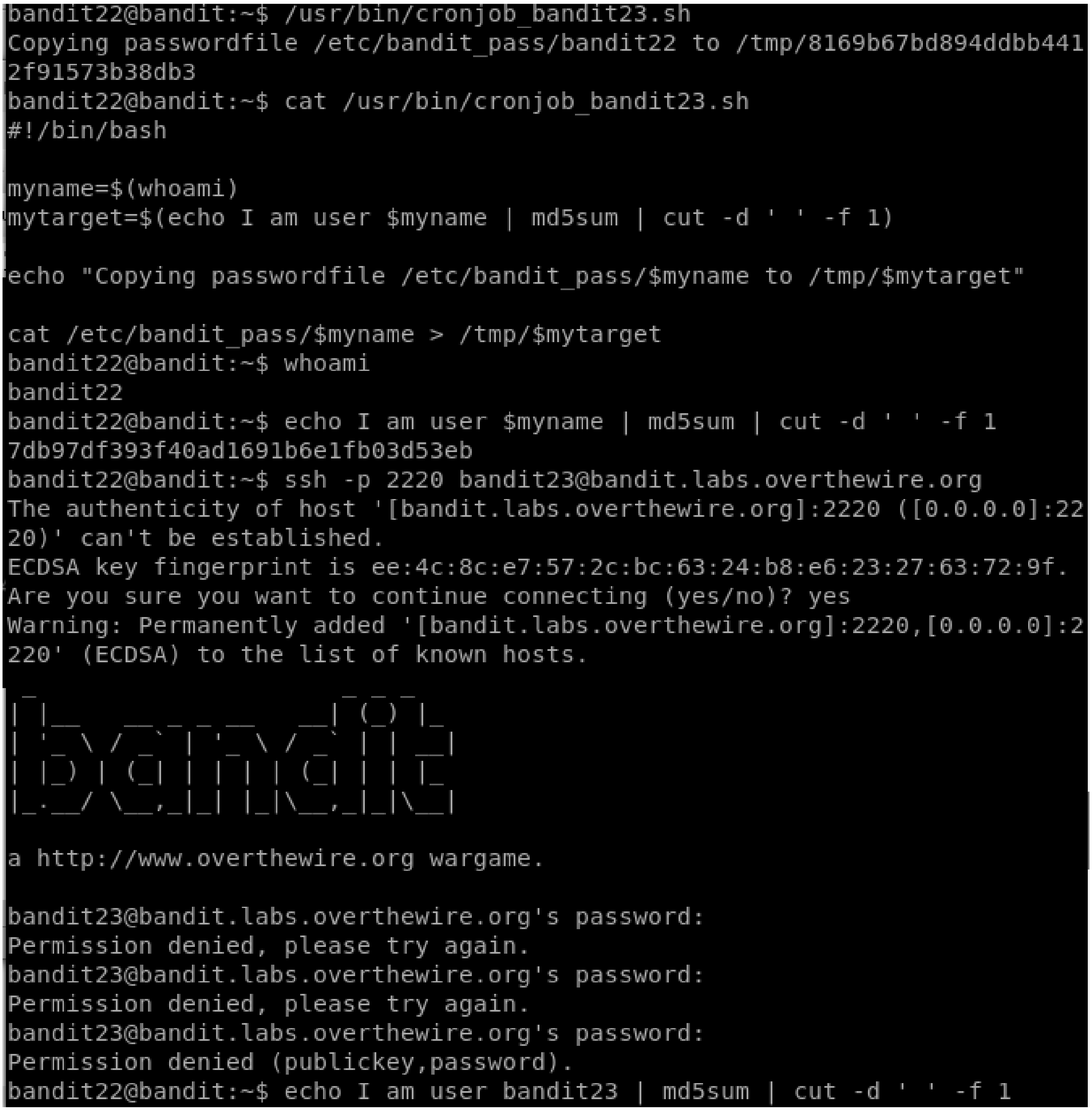
```
bandit21@bandit:~$ ll
total 28
drwxr-xr-x  3 bandit21 bandit21 4096 Sep 13 10:04 ./
drwxr-xr-x 30 root     root     4096 Sep 13 10:04 ../
-rw-r--r--  1 bandit21 bandit21  220 Apr  9  2014 .bash_logout
-rw-r--r--  1 bandit21 bandit21 3637 Apr  9  2014 .bashrc
drwx------  2 bandit21 bandit21 4096 Sep 13 10:04 .cache/
-r--------  1 bandit21 bandit21   33 Jun 15 11:41 .prevpass
-rw-r--r--  1 bandit21 bandit21  675 Apr  9  2014 .profile
bandit21@bandit:~$ man cron
bandit21@bandit:~$ /cron.d
-bash: /cron.d: No such file or directory
bandit21@bandit:~$ ls -l /etc/cron.d/
total 20
-rw-r--r-- 1 root root 355 May 25  2013 cron-apt
-rw-r--r-- 1 root root 120 Jun 15 11:41 cronjob_bandit22
-rw-r--r-- 1 root root 122 Jun 15 11:41 cronjob_bandit23
-rw-r--r-- 1 root root 120 Jun 15 11:41 cronjob_bandit24
-rw-r--r-- 1 root root 510 Feb  9  2017 php5
bandit21@bandit:~$ cat /etc/cron.d/cronjob_bandit22
@reboot bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
* * * * * bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
bandit21@bandit:~$ cat /etc/cron.d/cronjob_bandit22.sh
cat: /etc/cron.d/cronjob_bandit22.sh: No such file or directory
bandit21@bandit:~$ 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
bandit21@bandit:~$ ssh -p 2220 bandit22@bandit.labs.overthewire.org
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([0.0.0.0]:22
20)' can't be established.
ECDSA key fingerprint is ee:4c:8c:e7:57:2c:bc:63:24:b8:e6:23:27:63:72:9f.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[bandit.labs.overthewire.org]:2220,[0.0.0.0]:2
220' (ECDSA) to the list of known hosts.
```

Level 22 to Level 23:

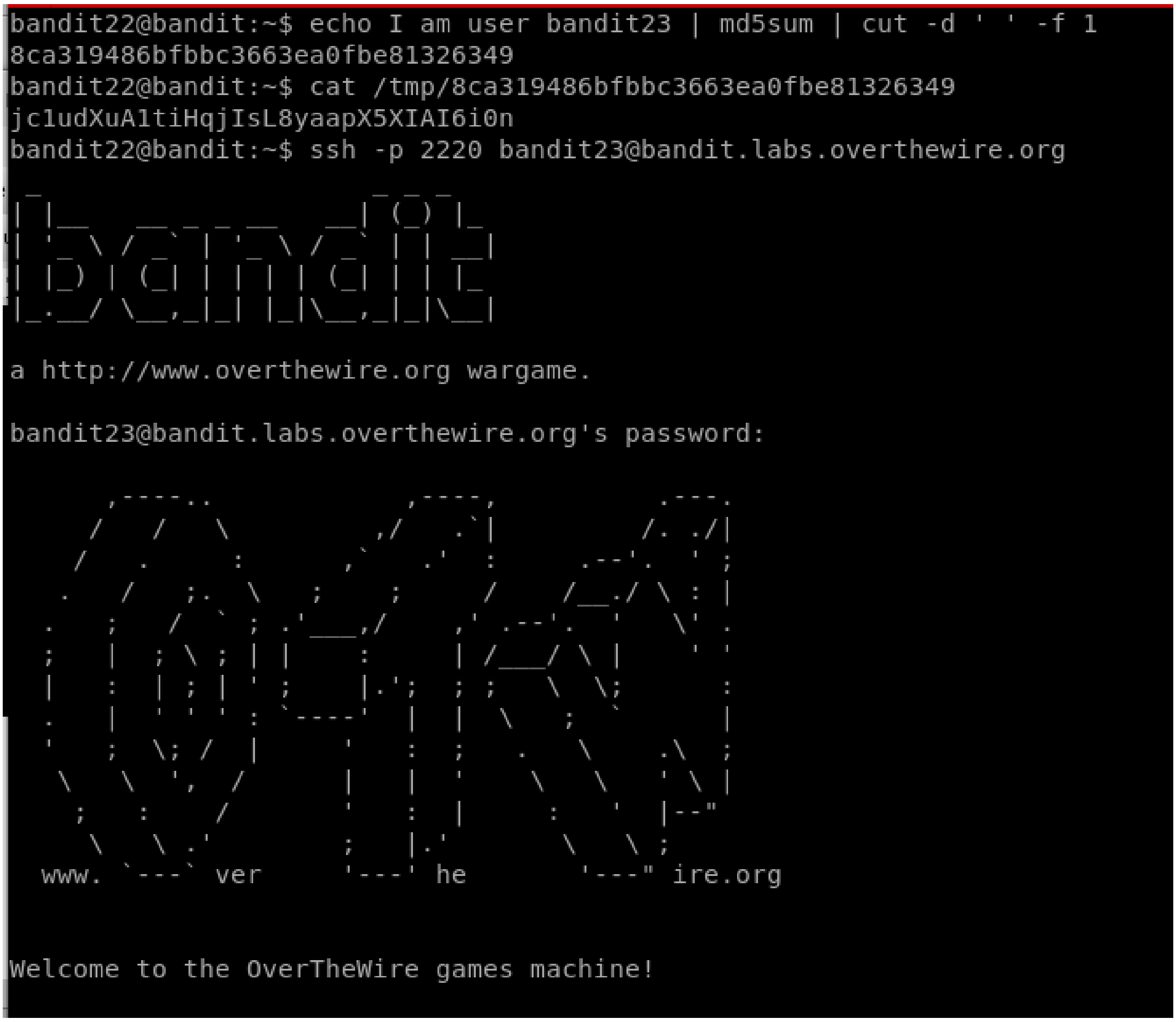
```
#ls
#ll
#ls -l /etc/cron.d/
#cat /etc/cron.d/cronjob_bandit23
#cat /usr/bin/cronjob_bandit23.sh
#cat /tmp/$mytarget
#/usr/bin/cronjob_bandit23.sh
#cat /tmp/8169b67bd894ddbb4412f91573b38db3
#/usr/bin/cronjob_bandit23.sh
#cat /usr/bin/cronjob_bandit23.sh
#echo I am user bandit23 | md5sum | cut -d ' ' -f 1
#cat /tmp/8ca319486bfbbc3663ea0fbe81326349
#ssh -p 2220 bandit23@bandit.labs.overthewire.org
```



```
bandit22@bandit:~$ ls
bandit22@bandit:~$ ll
total 24
drwxr-xr-x  3 bandit22 bandit22 4096 Sep 13 10:10 ./
drwxr-xr-x 31 root     root     4096 Sep 13 10:10 ../
-rw-r--r--  1 bandit22 bandit22  220 Apr  9  2014 .bash_logout
-rw-r--r--  1 bandit22 bandit22 3637 Apr  9  2014 .bashrc
drwx------  2 bandit22 bandit22 4096 Sep 13 10:10 .cache/
-rw-r--r--  1 bandit22 bandit22  675 Apr  9  2014 .profile
bandit22@bandit:~$ ls -l /etc/cron.d/
total 20
-rw-r--r-- 1 root root 355 May 25  2013 cron-apt
-rw-r--r-- 1 root root 120 Jun 15 11:41 cronjob_bandit22
-rw-r--r-- 1 root root 122 Jun 15 11:41 cronjob_bandit23
-rw-r--r-- 1 root root 120 Jun 15 11:41 cronjob_bandit24
-rw-r--r-- 1 root root 510 Feb  9  2017 php5
bandit22@bandit:~$ cd /etc/cron.d/cronjob_bandit23
-bash: cd: /etc/cron.d/cronjob_bandit23: Not a directory
bandit22@bandit:~$ cat /etc/cron.d/cronjob_bandit23
@reboot bandit23 /usr/bin/cronjob_bandit23.sh  &> /dev/null
* * * * * bandit23 /usr/bin/cronjob_bandit23.sh  &> /dev/null
bandit22@bandit:~$ cat /usr/bin/cronjob_bandit23.sh
#!/bin/bash

myname=$(whoami)
mytarget=$(echo I am user $myname | md5sum | cut -d ' ' -f 1)

echo "Copying passwordfile /etc/bandit_pass/$myname to /tmp/$mytarget"

cat /etc/bandit_pass/$myname > /tmp/$mytarget
bandit22@bandit:~$ cat /tmp/$mytarget
cat: /tmp/: Permission denied
bandit22@bandit:~$ /usr/bin/cronjob_bandit23.sh
Copying passwordfile /etc/bandit_pass/bandit22 to /tmp/8169b67bd894ddbb441
2f91573b38db3
bandit22@bandit:~$ cat /tmp/8169b67bd894ddbb4412f91573b38db3
Yk7owGAcWjwMVRwrTesJEwB7WVOiILLI
```



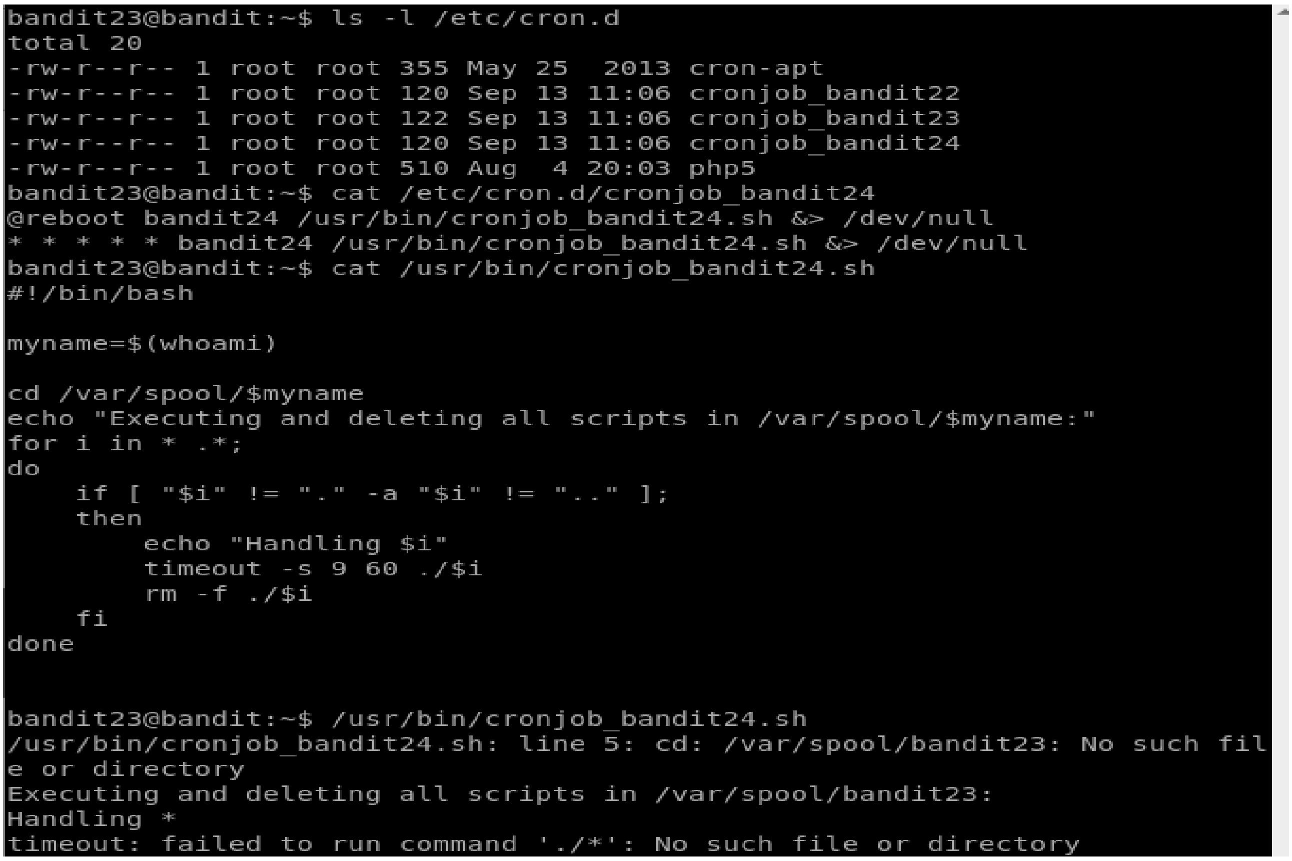
```
bandit22@bandit:~$ /usr/bin/cronjob_bandit23.sh
Copying passwordfile /etc/bandit_pass/bandit22 to /tmp/8169b67bd894ddbb441
2f91573b38db3
bandit22@bandit:~$ cat /usr/bin/cronjob_bandit23.sh
#!/bin/bash

myname=$(whoami)
mytarget=$(echo I am user $myname | md5sum | cut -d ' ' -f 1)

echo "Copying passwordfile /etc/bandit_pass/$myname to /tmp/$mytarget"

cat /etc/bandit_pass/$myname > /tmp/$mytarget
bandit22@bandit:~$ whoami
bandit22
bandit22@bandit:~$ echo I am user $myname | md5sum | cut -d ' ' -f 1
7db97df393f40ad1691b6e1fb03d53eb
bandit22@bandit:~$ ssh -p 2220 bandit23@bandit.labs.overthewire.org
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([0.0.0.0]:22
20)' can't be established.
ECDSA key fingerprint is ee:4c:8c:e7:57:2c:bc:63:24:b8:e6:23:27:63:72:9f.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[bandit.labs.overthewire.org]:2220,[0.0.0.0]:2
220' (ECDSA) to the list of known hosts.
 _                     _ _ _
| |__   __ _ _ __   __| (_) |_
| '_ \ / _` | '_ \ / _` | | __|
| |_) | (_| | | | | (_| | | |_
|_.__/ \__,_|_| |_|\__,_|_|\__|

a http://www.overthewire.org wargame.

bandit23@bandit.labs.overthewire.org's password:
Permission denied, please try again.
bandit23@bandit.labs.overthewire.org's password:
Permission denied, please try again.
bandit23@bandit.labs.overthewire.org's password:
Permission denied (publickey,password).
bandit22@bandit:~$ echo I am user bandit23 | md5sum | cut -d ' ' -f 1
```



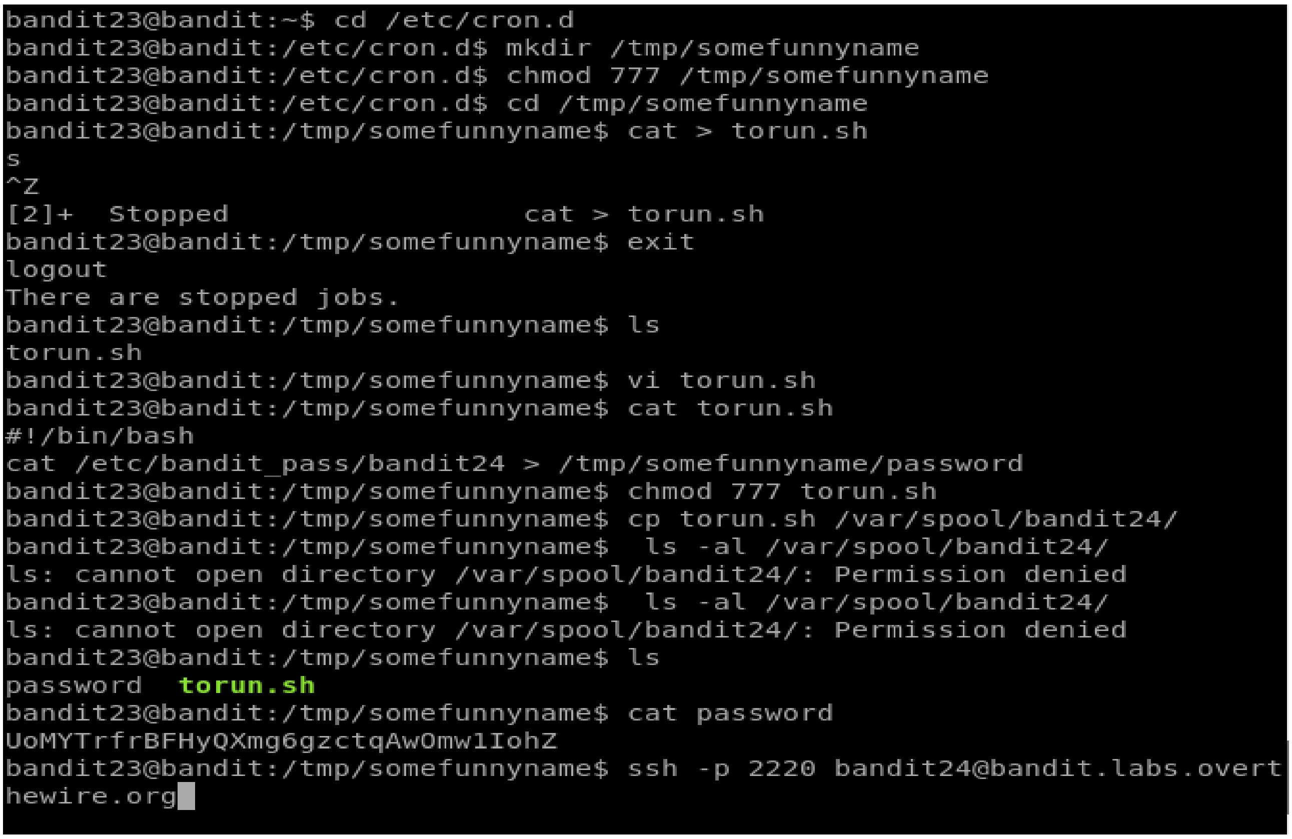
```
bandit22@bandit:~$ echo I am user bandit23 | md5sum | cut -d ' ' -f 1
8ca319486bfbbc3663ea0fbe81326349
bandit22@bandit:~$ cat /tmp/8ca319486bfbbc3663ea0fbe81326349
jc1udXuA1tiHqjIsL8yaapX5XIAI6i0n
bandit22@bandit:~$ ssh -p 2220 bandit23@bandit.labs.overthewire.org
 _                     _ _ _
| |__   __ _ _ __   __| (_) |_
| '_ \ / _` | '_ \ / _` | | __|
| |_) | (_| | | | | (_| | | |_
|_.__/ \__,_|_| |_|\__,_|_|\__|

a http://www.overthewire.org wargame.

bandit23@bandit.labs.overthewire.org's password:

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


Welcome to the OverTheWire games machine!
```

<u>Level 23 to Level 24:</u>

#ls -l /etc/cron.d/
#cat /etc/cron.d/cronjob_bandit24
#cat /usr/bin/cronjob_bandit24.sh
#/usr/bin/cronjob_bandit24.sh
#cd /etc/cron.d
#mkdir /tmp/somefunnyname
#chmod 777 /tmp/somefunnyname
#cd /tmp/somefunnyname
#vi torun.sh
>> the script <<
!/bin/bash
cat /etc/bandit_pass/bandit24 > /tmp/somefunnyname/password
>>the script<<
#chmod 777 torun.sh
#cp torun.sh /var/spool/bandit24
….. give it some minute for the script to run …..
#ls
#cat password
#ssh -p 2220 bandit24@bandit.labs.overthewire.org



```
bandit23@bandit:~$ ls -l /etc/cron.d
total 20
-rw-r--r-- 1 root root 355 May 25  2013 cron-apt
-rw-r--r-- 1 root root 120 Sep 13 11:06 cronjob_bandit22
-rw-r--r-- 1 root root 122 Sep 13 11:06 cronjob_bandit23
-rw-r--r-- 1 root root 120 Sep 13 11:06 cronjob_bandit24
-rw-r--r-- 1 root root 510 Aug  4 20:03 php5
bandit23@bandit:~$ cat /etc/cron.d/cronjob_bandit24
@reboot bandit24 /usr/bin/cronjob_bandit24.sh &> /dev/null
* * * * * bandit24 /usr/bin/cronjob_bandit24.sh &> /dev/null
bandit23@bandit:~$ 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 $i"
        timeout -s 9 60 ./$i
        rm -f ./$i
    fi
done


bandit23@bandit:~$ /usr/bin/cronjob_bandit24.sh
/usr/bin/cronjob_bandit24.sh: line 5: cd: /var/spool/bandit23: No such fil
e or directory
Executing and deleting all scripts in /var/spool/bandit23:
Handling *
timeout: failed to run command './*': No such file or directory
```

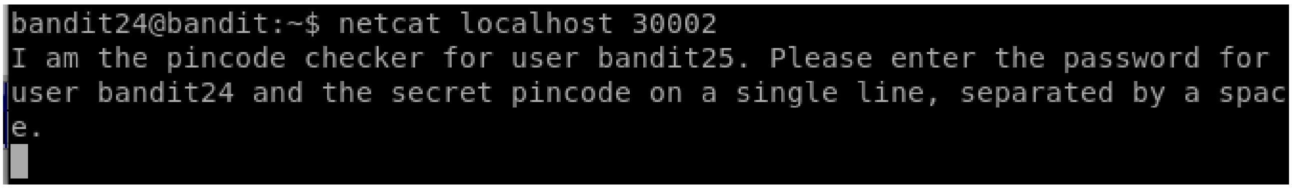


```
bandit23@bandit:~$ cd /etc/cron.d
bandit23@bandit:/etc/cron.d$ mkdir /tmp/somefunnyname
bandit23@bandit:/etc/cron.d$ chmod 777 /tmp/somefunnyname
bandit23@bandit:/etc/cron.d$ cd /tmp/somefunnyname
bandit23@bandit:/tmp/somefunnyname$ cat > torun.sh
s
^Z
[2]+  Stopped                 cat > torun.sh
bandit23@bandit:/tmp/somefunnyname$ exit
logout
There are stopped jobs.
bandit23@bandit:/tmp/somefunnyname$ ls
torun.sh
bandit23@bandit:/tmp/somefunnyname$ vi torun.sh
bandit23@bandit:/tmp/somefunnyname$ cat torun.sh
#!/bin/bash
cat /etc/bandit_pass/bandit24 > /tmp/somefunnyname/password
bandit23@bandit:/tmp/somefunnyname$ chmod 777 torun.sh
bandit23@bandit:/tmp/somefunnyname$ cp torun.sh /var/spool/bandit24/
bandit23@bandit:/tmp/somefunnyname$  ls -al /var/spool/bandit24/
ls: cannot open directory /var/spool/bandit24/: Permission denied
bandit23@bandit:/tmp/somefunnyname$  ls -al /var/spool/bandit24/
ls: cannot open directory /var/spool/bandit24/: Permission denied
bandit23@bandit:/tmp/somefunnyname$ ls
password  torun.sh
bandit23@bandit:/tmp/somefunnyname$ cat password
UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ
bandit23@bandit:/tmp/somefunnyname$ ssh -p 2220 bandit24@bandit.labs.overt
hewire.org
```

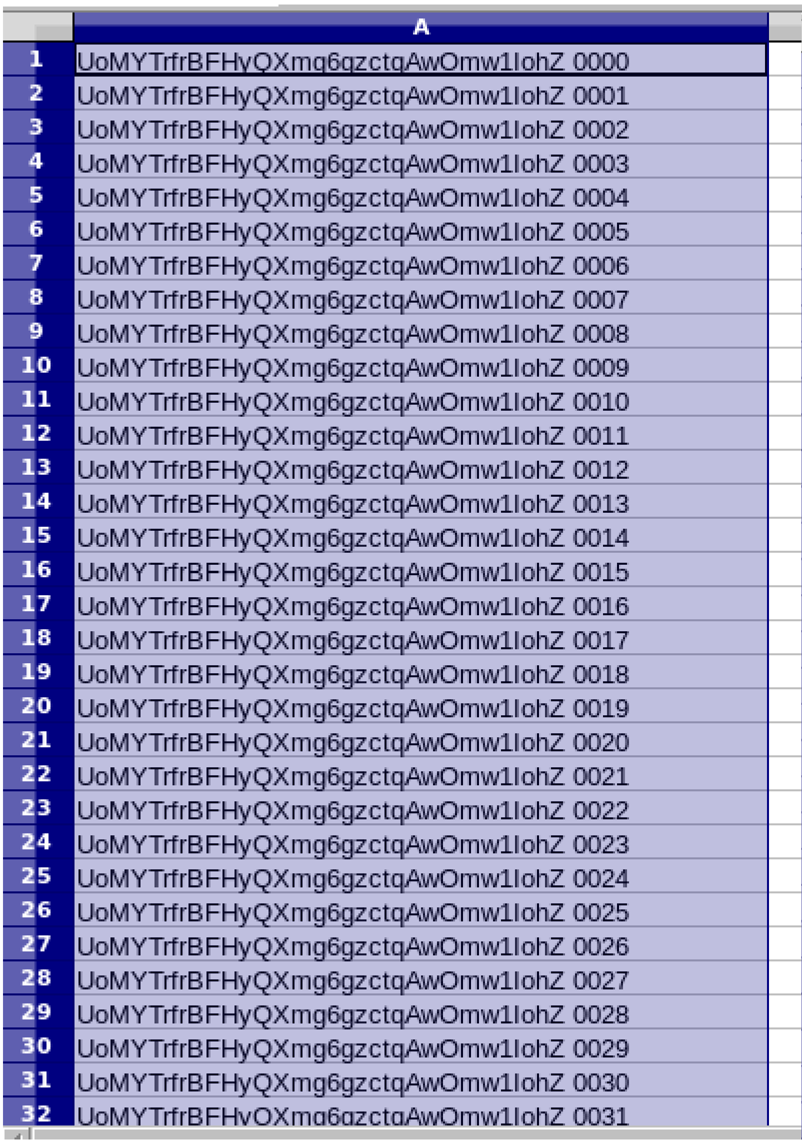
Level 24 to Level 25:

#netcat localhost 30002
So I was creative with my hack this time round for me, so I open LibreOffice Calc ..
Inputed the password for Level 24 space and the 4 digit pin 000>>
UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ *space* ***0000,*** *then allowed then scrolled downwards allowing it to self auto-generate for me the 4 digit password from 0000 to 9999 without repeating numbers ..*

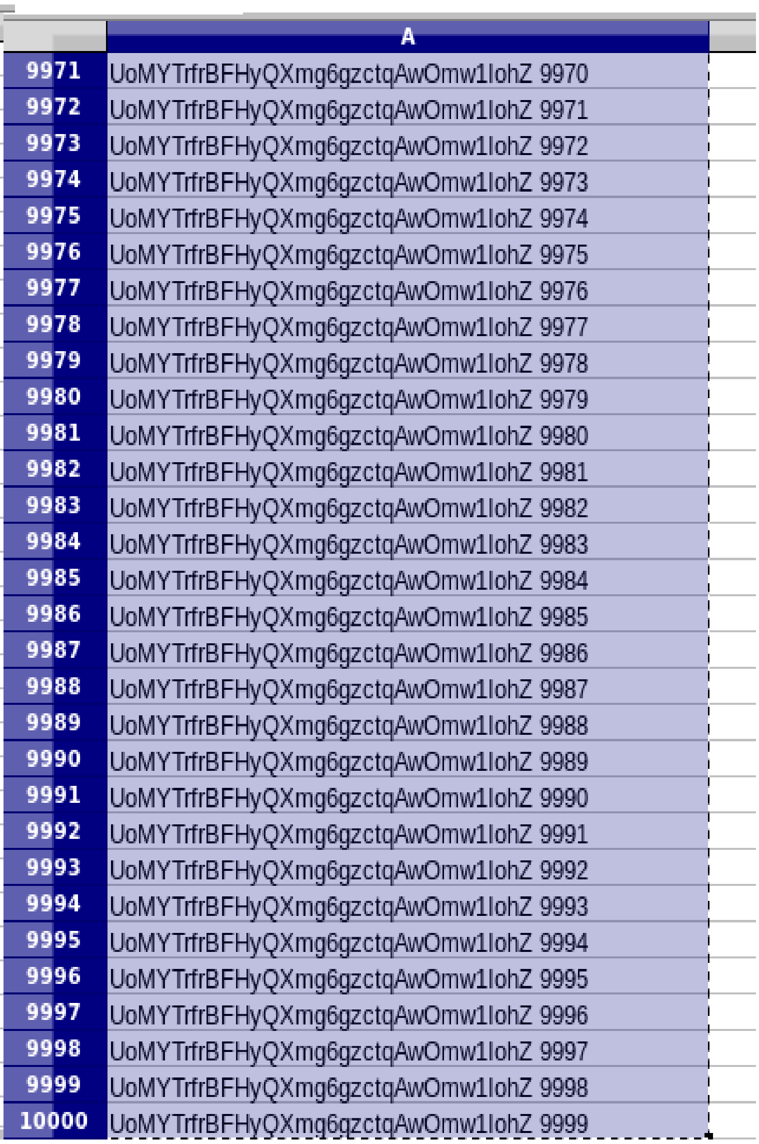
copied all … then .. pasted in the passwords.txt file
#touch passwords.txt
#vi passwords.txt
a button, for append pasted then escape button then :wq
#netcat localhost 30002 < passwords.txt
#ssh -p 2220 bandit25@bandit.labs.overthewire.org



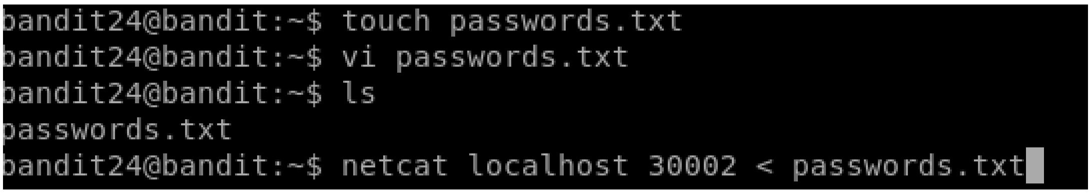
```
bandit24@bandit:~$ netcat localhost 30002
I am the pincode checker for user bandit25. Please enter the password for
user bandit24 and the secret pincode on a single line, separated by a spac
e.
```



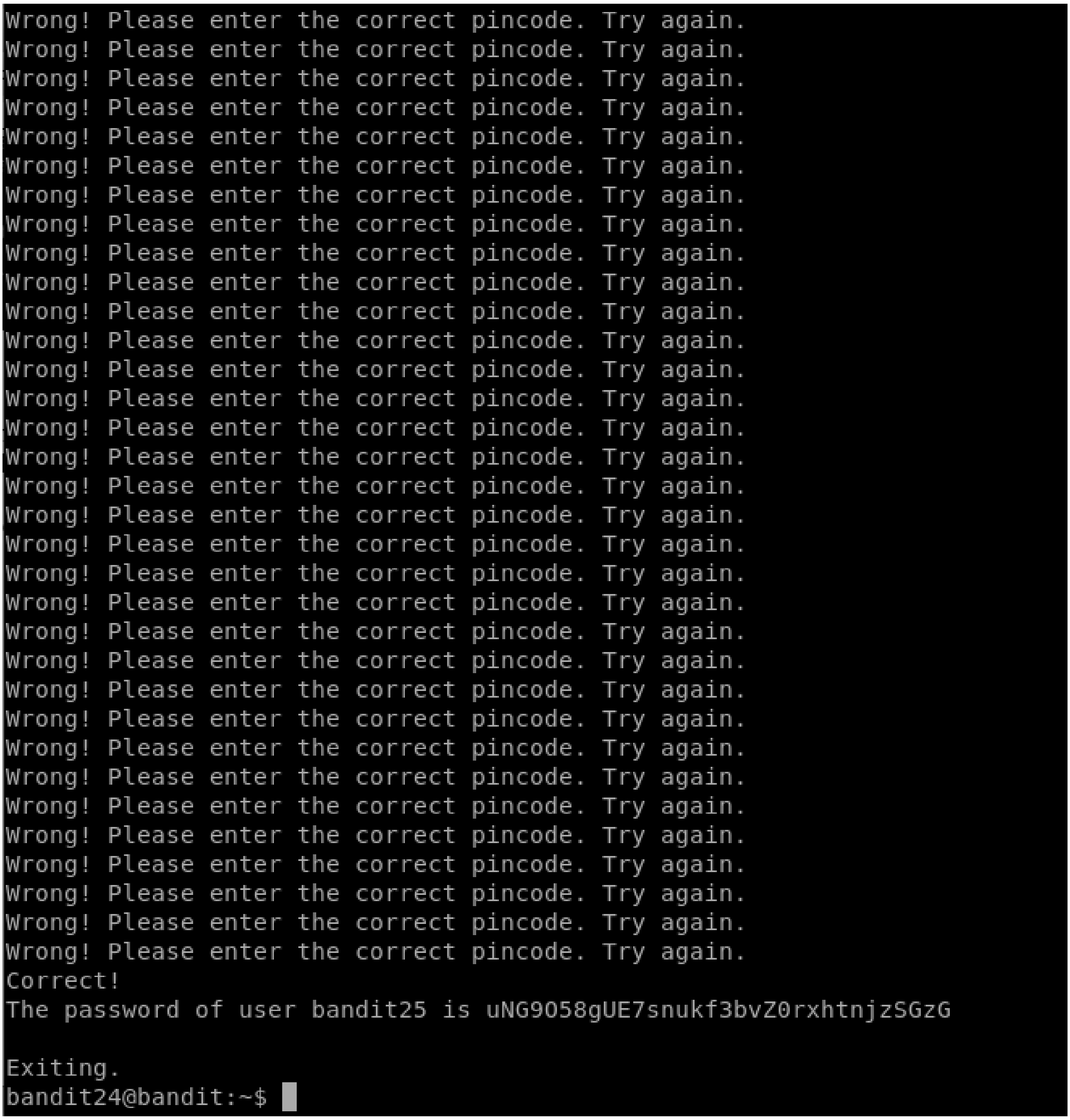
	A
1	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 0000
2	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 0001
3	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 0002
4	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 0003
5	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 0004
6	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 0005
7	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 0006
8	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 0007
9	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 0008
10	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 0009
11	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 0010
12	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 0011
13	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 0012
14	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 0013
15	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 0014
16	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 0015
17	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 0016
18	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 0017
19	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 0018
20	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 0019
21	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 0020
22	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 0021
23	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 0022
24	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 0023
25	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 0024
26	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 0025
27	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 0026
28	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 0027
29	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 0028
30	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 0029
31	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 0030
32	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 0031



	A
9971	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 9970
9972	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 9971
9973	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 9972
9974	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 9973
9975	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 9974
9976	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 9975
9977	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 9976
9978	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 9977
9979	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 9978
9980	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 9979
9981	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 9980
9982	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 9981
9983	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 9982
9984	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 9983
9985	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 9984
9986	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 9985
9987	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 9986
9988	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 9987
9989	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 9988
9990	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 9989
9991	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 9990
9992	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 9991
9993	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 9992
9994	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 9993
9995	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 9994
9996	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 9995
9997	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 9996
9998	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 9997
9999	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 9998
10000	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ 9999



```
bandit24@bandit:~$ touch passwords.txt
bandit24@bandit:~$ vi passwords.txt
bandit24@bandit:~$ ls
passwords.txt
bandit24@bandit:~$ netcat localhost 30002 < passwords.txt
```



```
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Correct!
The password of user bandit25 is uNG9O58gUE7snukf3bvZ0rxhtnjzSGzG

Exiting.
bandit24@bandit:~$
```

Level 25 to Level 26:

This level was a tricky one I had to seek the Internet to do some research…
so I thought one was to ssh directly using the bandit26.sshkey one finds in the home directory..
so I did an ls to list to files present on the directory I am at… then I did a pwd to view my current profile status…
Then I found this command “`cat /etc/passwd | grep bandit26`” that allows one to view the password on the following path and the grep to specify the specify file bandit26.
The output was …
bandit26:x:11026:11026:bandit level 26:/home/bandit26:/usr/bin/showtext
then I did a cat command on this path :/usr/bin/showtext
the output was a script ..

```
>>script<<
#!/bin/sh

more ~/text.txt
exit 0
>>script<<
```

so from here I noticed one had to reduce the terminal size to as small as possible, then ssh to localhost using the bandit26.sshkey, then type v so as to enable vi mode.. then after you have enabled vi mode type this command ; `:r /etc/bandit_pass/bandit26` so as to view the password.

#ls

#pwd

#cat *etc*passwd | grep bandit26

#cat /*usr*/bin/showtext

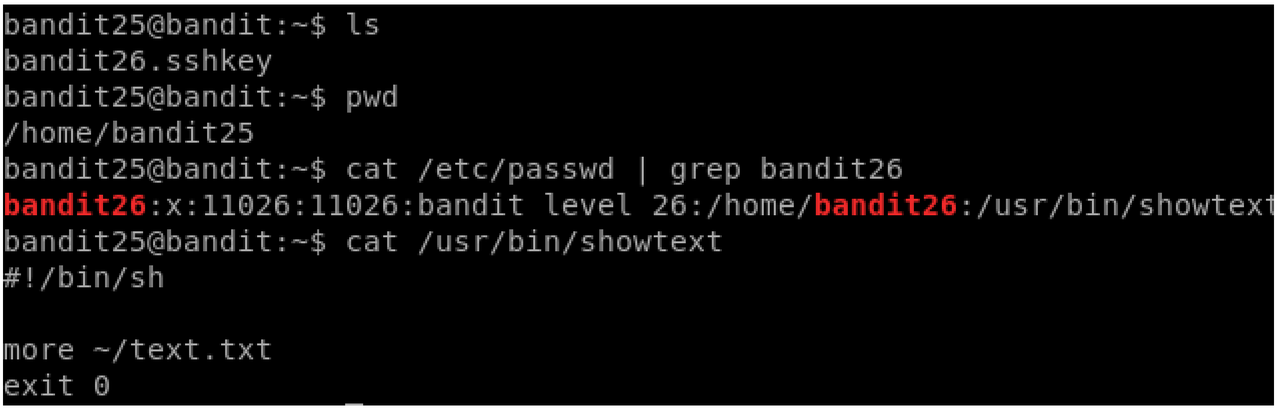
reduce screen size first .. then ssh...

#ssh -i bandit26.sshkey@localhost

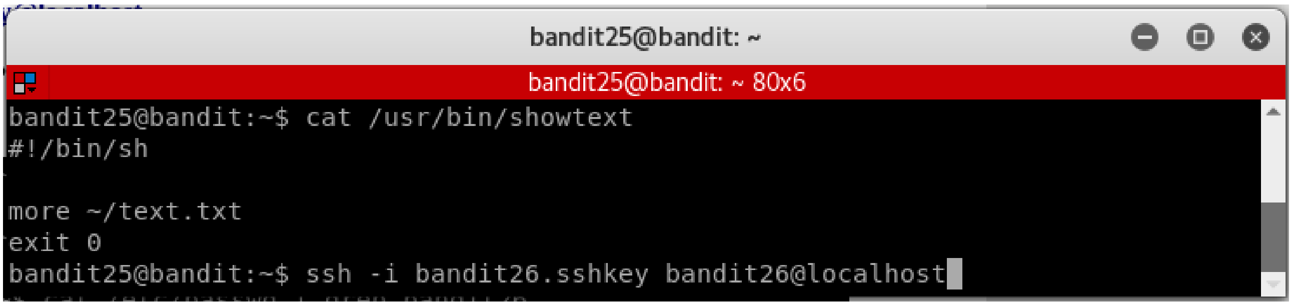
#v

#:r */etc/bandit26_pass?bandit26*

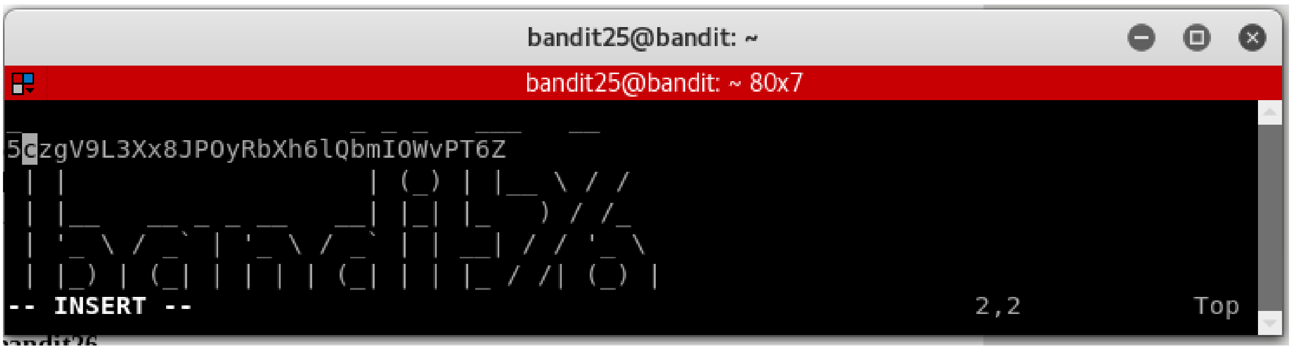
#ssh -p 2220 bandit26@bandit.labs.overthewire.org



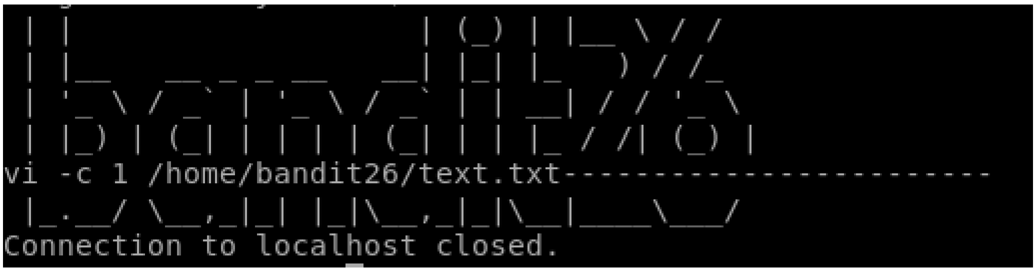
```
bandit25@bandit:~$ ls
bandit26.sshkey
bandit25@bandit:~$ pwd
/home/bandit25
bandit25@bandit:~$ cat /etc/passwd | grep bandit26
bandit26:x:11026:11026:bandit level 26:/home/bandit26:/usr/bin/showtext
bandit25@bandit:~$ cat /usr/bin/showtext
#!/bin/sh

more ~/text.txt
exit 0
```



```
bandit25@bandit:~$ cat /usr/bin/showtext
#!/bin/sh

more ~/text.txt
exit 0
bandit25@bandit:~$ ssh -i bandit26.sshkey bandit26@localhost
```

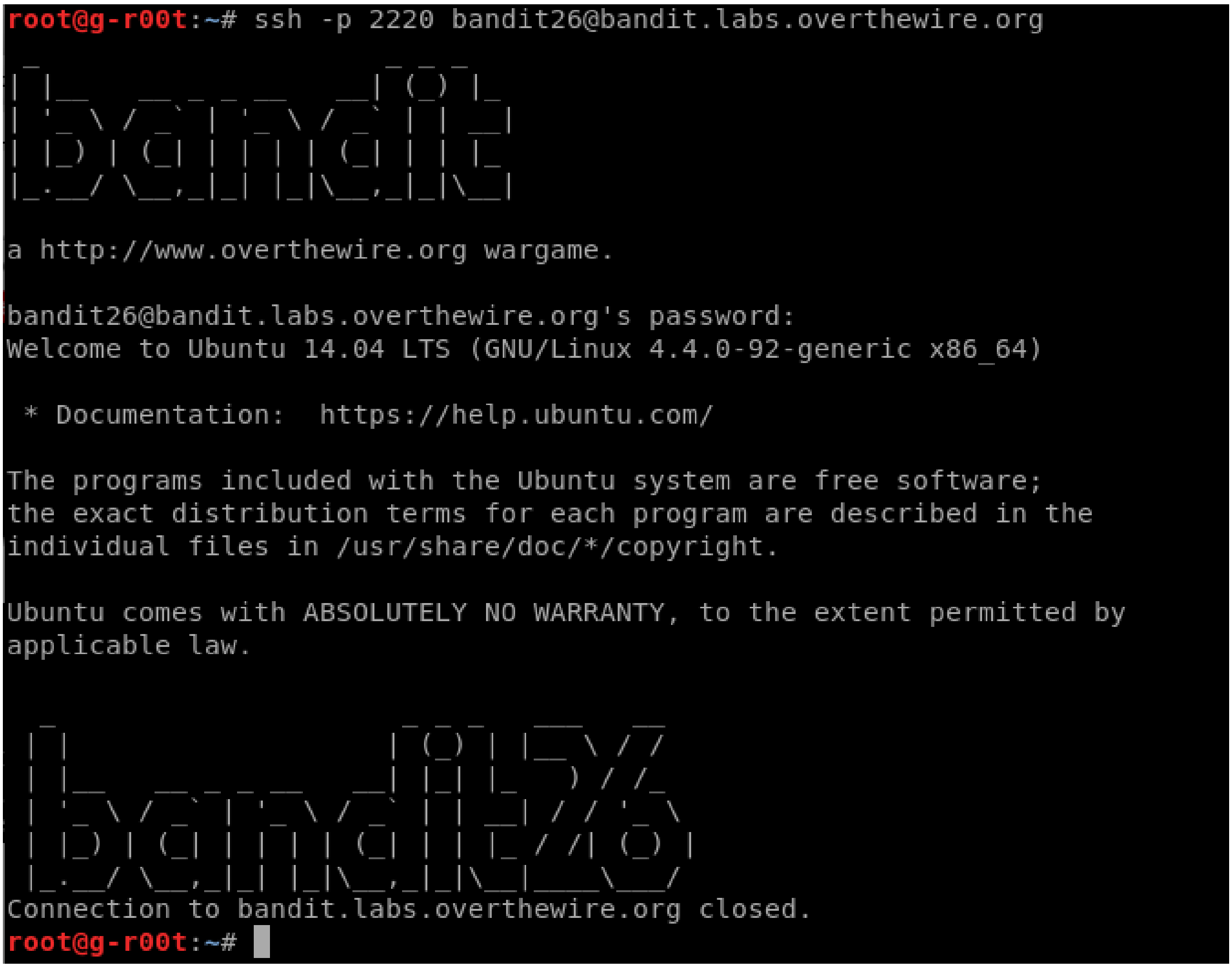


```
 _                     _ _ _   ___   __
5czgV9L3Xx8JPOyRbXh6lQbmIOWvPT6Z
 | |                   | (_) | |__ \ / /
 | |__   __ _ _ __   __| |_| |_   ) / /_
 | '_ \ / _` | '_ \ / _` | | __| / / '_ \
 | |_) | (_| | | | | (_| | | |_ / /| (_) |
-- INSERT --                                              2,2           Top
```



```
 | |                   | (_) | |__ \ / /
 | |__   __ _ _ __   __| |_| |_   ) / /_
 | '_ \ / _` | '_ \ / _` | | __| / / '_ \
 | |_) | (_| | | | | (_| | | |_ / /| (_) |
vi -c 1 /home/bandit26/text.txt-------------------------
 |_.__/ \__,_|_| |_|\__,_|_|\__|____\___/
Connection to localhost closed.
```

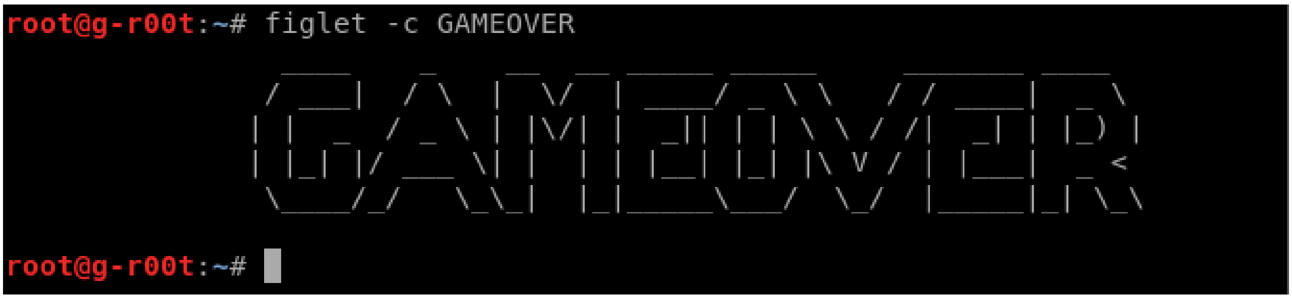
Level 26 to Level 27:



```
root@g-r00t:~# ssh -p 2220 bandit26@bandit.labs.overthewire.org
 _                     _ _ _
| |__   __ _ _ __   __| (_) |_
| '_ \ / _` | '_ \ / _` | | __|
| |_) | (_| | | | | (_| | | |_
|_.__/ \__,_|_| |_|\__,_|_|\__|

a http://www.overthewire.org wargame.

bandit26@bandit.labs.overthewire.org's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 4.4.0-92-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

  _                     _ _ _   ___   __
 | |                   | (_) | |__ \ / /
 | |__   __ _ _ __   __| |_| |_   ) / /_
 | '_ \ / _` | '_ \ / _` | | __| / / '_ \
 | |_) | (_| | | | | (_| | | |_ / /| (_) |
 |_.__/ \__,_|_| |_|\__,_|_|\__|____\___/
Connection to bandit.labs.overthewire.org closed.
root@g-r00t:~#
```

Bandit Level 26 → Level 27

At this moment, level 27 does not exist yet.



```
root@g-r00t:~# figlet -c GAMEOVER
                ____    _    __  __ _____ _____     _______ ____  
               / ___|  / \  |  \/  | ____/ _ \ \   / / ____|  _ \ 
              | |  _  / _ \ | |\/| |  _|| | | \ \ / /|  _| | |_) |
              | |_| |/ ___ \| |  | | |__| |_| |\ V / | |___|  _ < 
               \____/_/   \_\_|  |_|_____\___/  \_/  |_____|_| \_\

root@g-r00t:~# 
```