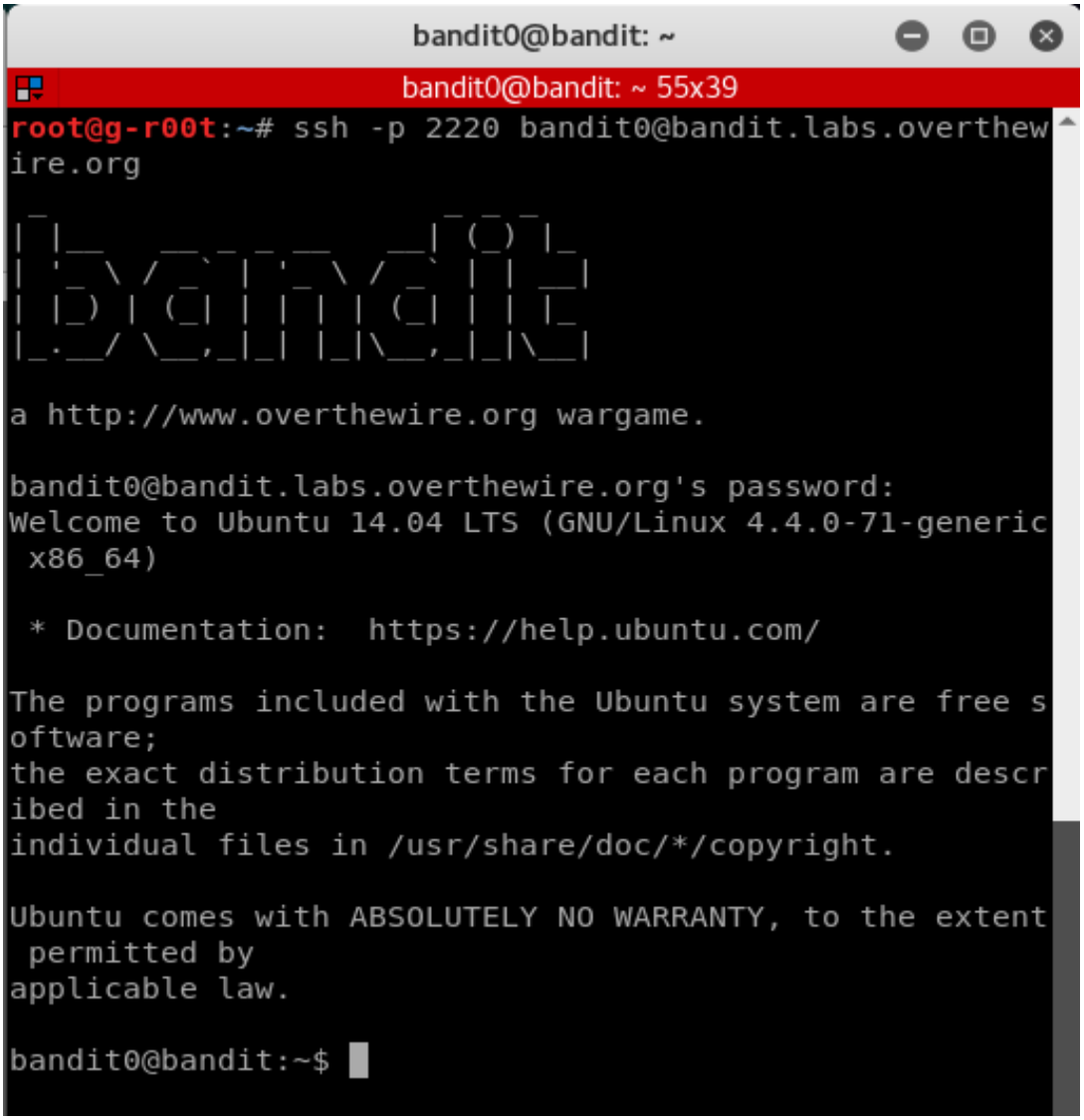
OverTheWire: BANDIT WRITEUP:

URL: http://overthewire.org/wargames/bandit/
START DATE: 14th/08/2017
AUTHOR: PETER NUMI
Email: kamandepeter.pk@gmail.com
PHONE: +254 707 897 394

Level 0:

using SSH to log into the bandit.labs.overthewire.org port number 2220 username: bandit0 password: bandit0

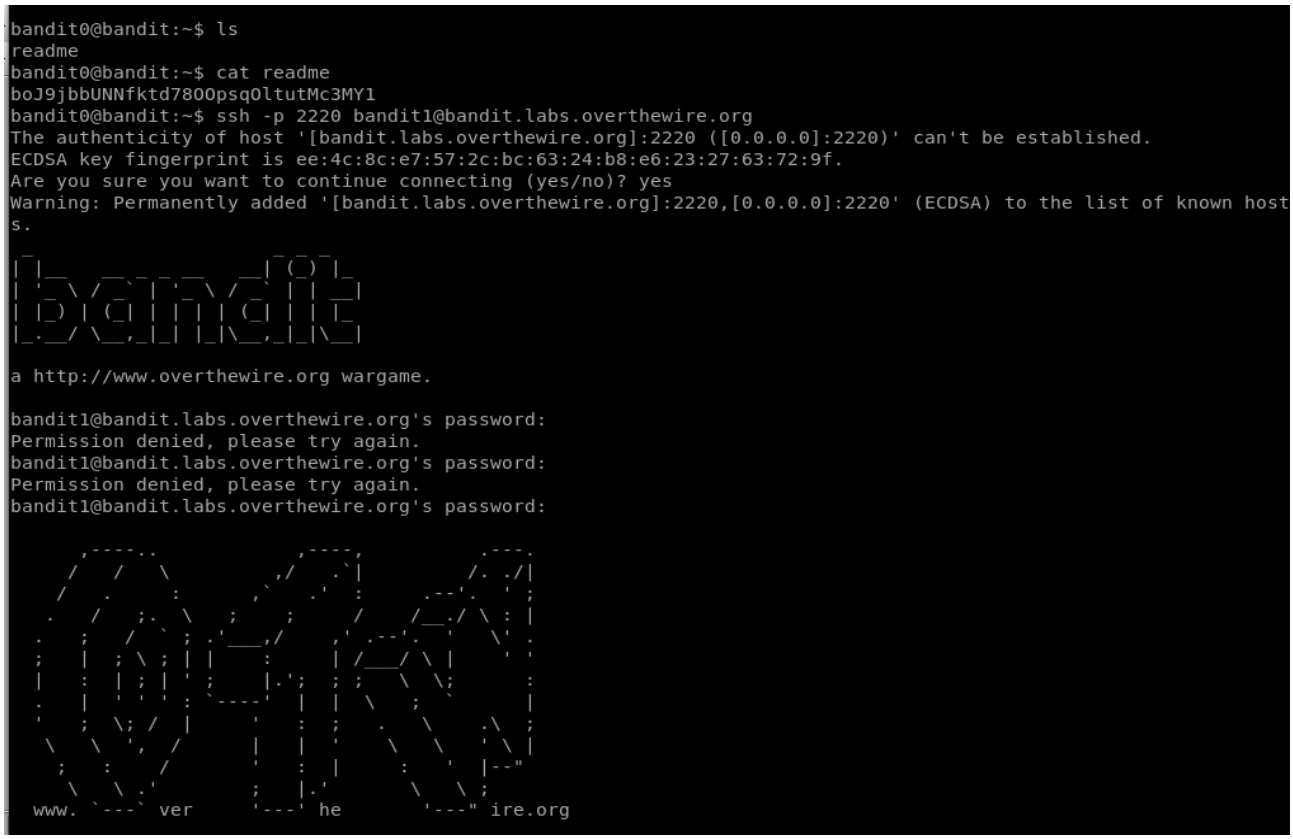
#ssh -p 2220 bandit0@bandit.labs.overthewire.org



Level 0 to Level 1:

On the home directory their was a file known as readme that contained the password to log into the next level.

#ls
#cat readme
 # ssh -p 2220 bandit1@bandit.labs.overthewire.org



Level 1 to Level 2:

The password for the next level is stored in a file name known as dashed file (-) on the home directory.

#ls -l
#ls
#cat ./-
#ssh -p 2220 bandit2@bandit.labs.overthewire.org

```
bandit1@bandit:~$ ls -l
total 4
-rw-r----- 1 bandit2 bandit1 33 Jun 15 11:40 -
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat -
^Z
[1]+  Stopped                 cat -
bandit1@bandit:~$ cat /-
cat: /-: No such file or directory
bandit1@bandit:~$ cat ./-
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
bandit1@bandit:~$ ssh -p 2220 bandit2@bandit.labs.overt
hewire.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.or
g]:2220,[0.0.0.0]:2220' (ECDSA) to the list of known ho
sts.
 _                     _ _ _
| |__   __ _ _ __   __| (_) |_
| '_ \ / _` | '_ \ / _` | | __|
| |_) | (_| | | | | (_| | | |_
|_.__/ \__,_|_| |_|\__,_|_|\__|

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

bandit2@bandit.labs.overthewire.org's password:
```

Level 2 to Level 3:

The password for the next level is stored in a file known as spaces in this filename on the home directory.

#ls -l
#ls
#cat spaces\ in\ this\ filename
#ssh -p 2220 bandit3@bandit.labs.overthewire.org

```
bandit2@bandit:~$ ls -l
total 4
-rw-r----- 1 bandit3 bandit2 33 Jun 15 11:41 spaces in
this filename
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat spaces\ in\ this\ filename
UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK
bandit2@bandit:~$ ssh -p 2220 bandit3@bandit.labs.overt
hewire.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.or
g]:2220,[0.0.0.0]:2220' (ECDSA) to the list of known ho
sts.
 _                     _ _ _
| |__   __ _ _ __   __| (_) |_
| '_ \ / _` | '_ \ / _` | | __|
| |_) | (_| | | | | (_| | | |_
|_.__/ \__,_|_| |_|\__,_|_|\__|

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

bandit3@bandit.labs.overthewire.org's password:
```

Level 3 to Level 4:

The password for the next level is stored in hidden file known as hidden in a directory known as inhere on the home directory.

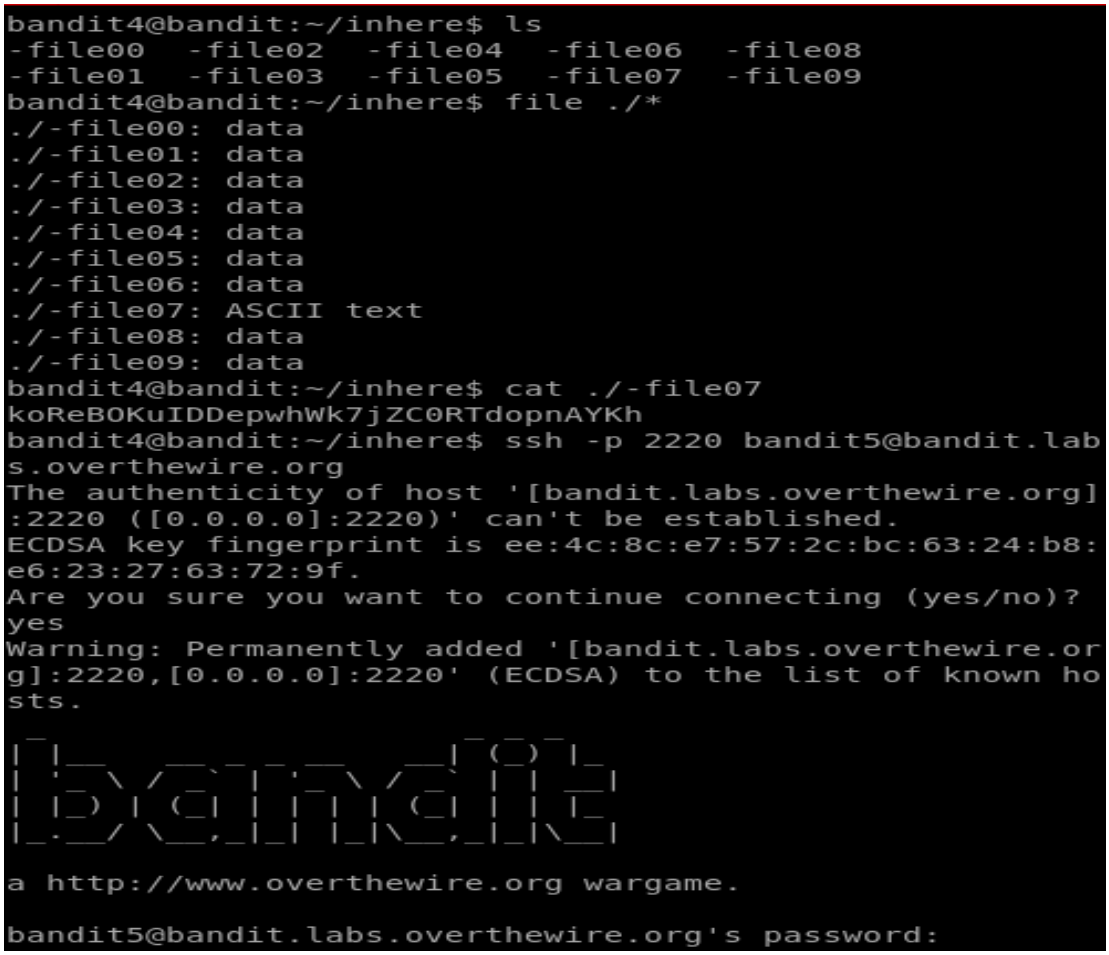
#ls
#cd inhere/
#ll – to show the hidden files
#cat .hidden
#ssh -p 2220 bandit4@bandit.labs.overthewire.org

```
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere/
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ ls -l
total 0
bandit3@bandit:~/inhere$ ll
total 12
drwxr-xr-x 2 root    root    4096 Jun 15 11:41 ./
drwxr-xr-x 4 bandit3 bandit3 4096 Aug 15 01:43 ../
-rw-r----- 1 bandit4 bandit3   33 Jun 15 11:41 .hidden
bandit3@bandit:~/inhere$ cat .hidden
pIwrPrtPN36QITSp3EQaw936yaFoFgAB
bandit3@bandit:~/inhere$ ssh -p 2220 bandit4@bandit.lab
s.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.or
g]:2220,[0.0.0.0]:2220' (ECDSA) to the list of known ho
sts.
 _                     _ _ _
| |__   __ _ _ __   __| (_) |_
| '_ \ / _` | '_ \ / _` | | __|
| |_) | (_| | | | | (_| | | |_
|_.__/ \__,_|_| |_|\__,_|_|\__|

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

bandit4@bandit.labs.overthewire.org's password:
```

Level 4 to Level 5:

The password for the next level is stored in the only human-readable file in the directory known as inhere on the home directory.

#ls
#cd inhere/
#ls
#file ./*
#cat ./-file07
#ssh -p 2220 bandit5@bandit.labs.overthewire.org



Level 5 to Level 6:

The password for the next level is in a file located in a directory known as inhere at the home directory.

The file has the following properties:

human-readable
1033 bytes in size
not executable

#ls
#cd inhere/
#ls
#find . -size 1033c ! -executable
#cat ./maybehere07/.file2
#ssh -p 2220 bandit6@bandit.labs.overthewire.org

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

```
          bandit5@bandit:~/inhere$ ssh -p 2220 bandit6@
s.overthewire.org
                         _ _ _
 _ |__   __ _ _ __   __| (_) |_
| '_ \ / _` | '_ \ / _` | | __|
| |_) | (_| | | | | (_| | | |_
|_.__/ \__,_|_| |_|\__,_|_|\__|

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

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

Level 6 to Level 7:

The password for the next level is stored somwhere on the server and has the following properties:

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

#find / -user bandit7 -group bandit6 -size 33c -type f 2>/dev/null
#cat /var/lib/dpkg/info/bandit7.password
#ssh -p 2220 bandit7@bandit.labs.overthewire.org

```
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -
size 33c -type f 2>/dev/null
/var/lib/dpkg/info/bandit7.password
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.passwo
rd
HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs
bandit6@bandit:~$ ssh -p 2220 bandit7@bandit.labs.overt
hewire.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.or
g]:2220,[0.0.0.0]:2220' (ECDSA) to the list of known ho
sts.
 _                         _ _ _
| |__   __ _ _ __   __| (_) |_
| '_ \ / _` | '_ \ / _` | | __|
| |_) | (_| | | | | (_| | | |_
|_.__/ \__,_|_| |_|\__,_|_|\__|

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

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

Level 7 to Level 8:

The password for the next level is stored in the file data.text next to the word millionth.

#ls
#grep “millionth” data.txt
#ssh -p 2220 bandit8@bandit.labs.overthewire.org

```
bandit7@bandit:~$ ls
data.txt
bandit7@bandit:~$ grep "millionth" data.txt
millionth       cvX2JJa4CFALtqS87jk27qwqGhBM9plV
bandit7@bandit:~$ ssh -p 2220 bandit8@bandit.labs.overt
hewire.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.or
g]:2220,[0.0.0.0]:2220' (ECDSA) to the list of known ho
sts.
 _                     _ _ _
| |__   __ _ _ __   __| (_) |_
| '_ \ / _` | '_ \ / _` | | __|
| |_) | (_| | | | | (_| | | |_
|_.__/ \__,_|_| |_|\__,_|_|\__|

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

bandit8@bandit.labs.overthewire.org's password:
```

Level 8 to Level 9:

The password for the next level is stored in the file data.txt and is the only line that occurs only once.

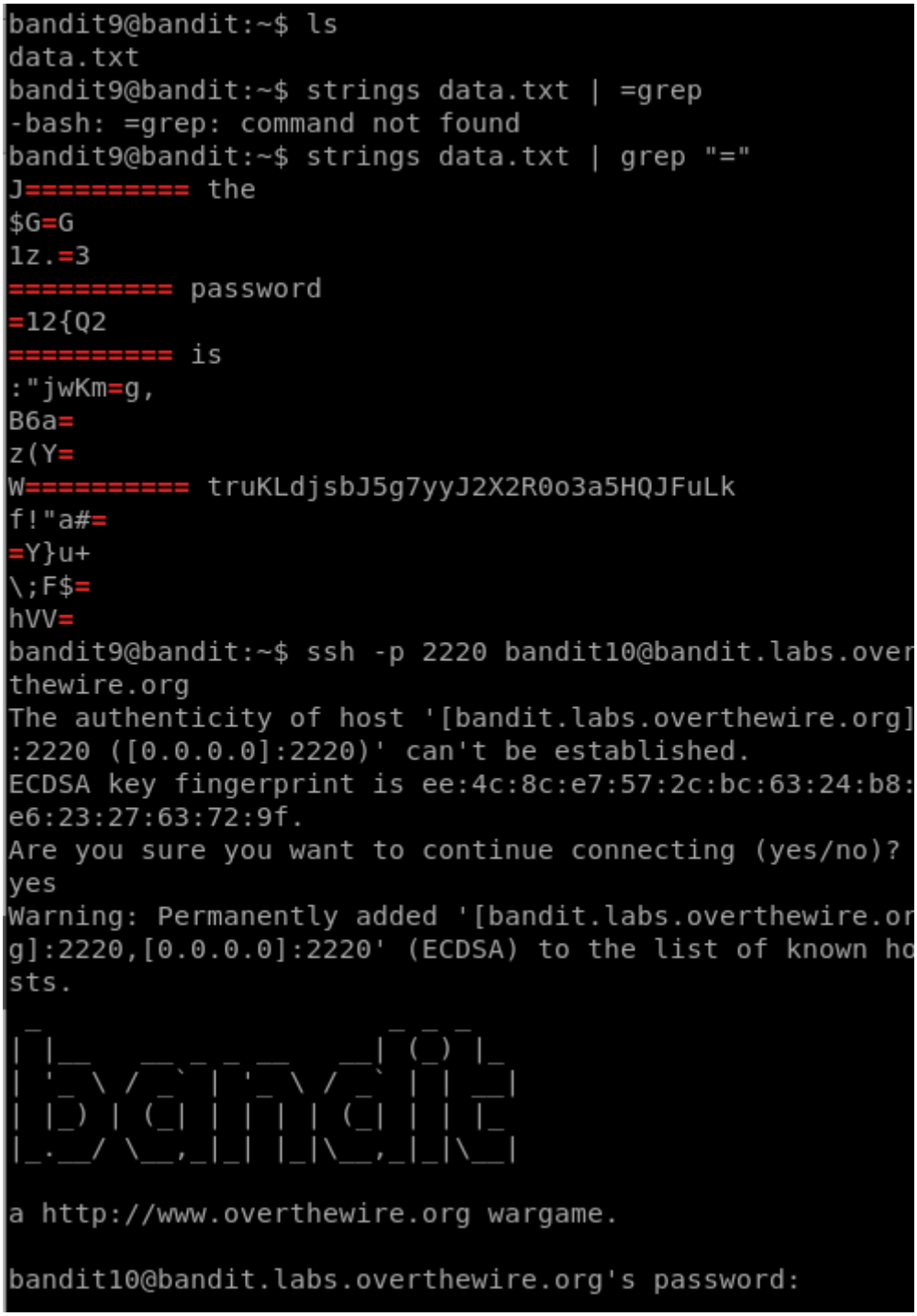
#cat data.txt | sort | uniq -u
#ssh -p 2220 bandit9@bandit.labs.overthewire.org

```
bandit8@bandit:~$ ls
data.txt
bandit8@bandit:~$ cat data.txt | sort | uniq -u
UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR
bandit8@bandit:~$ ssh -p 2220 bandit9@bandit.labs.overt
hewire.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.or
g]:2220,[0.0.0.0]:2220' (ECDSA) to the list of known ho
sts.
 _                     _ _ _
| |__   __ _ _ __   __| (_) |_
| '_ \ / _` | '_ \ / _` | | __|
| |_) | (_| | | | | (_| | | |_
|_.__/ \__,_|_| |_|\__,_|_|\__|

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

bandit9@bandit.labs.overthewire.org's password:
```

Level 9 to Level 10:

The password for the next level is stored in the file data.txt in one of the few human-readable strings, beginning with several '=' characters.

#ls
#strings data.txt | grep "="
#ssh -p 2220 bandit10@bandit.labs.overthewire.org



Level 10 to Level 11:

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

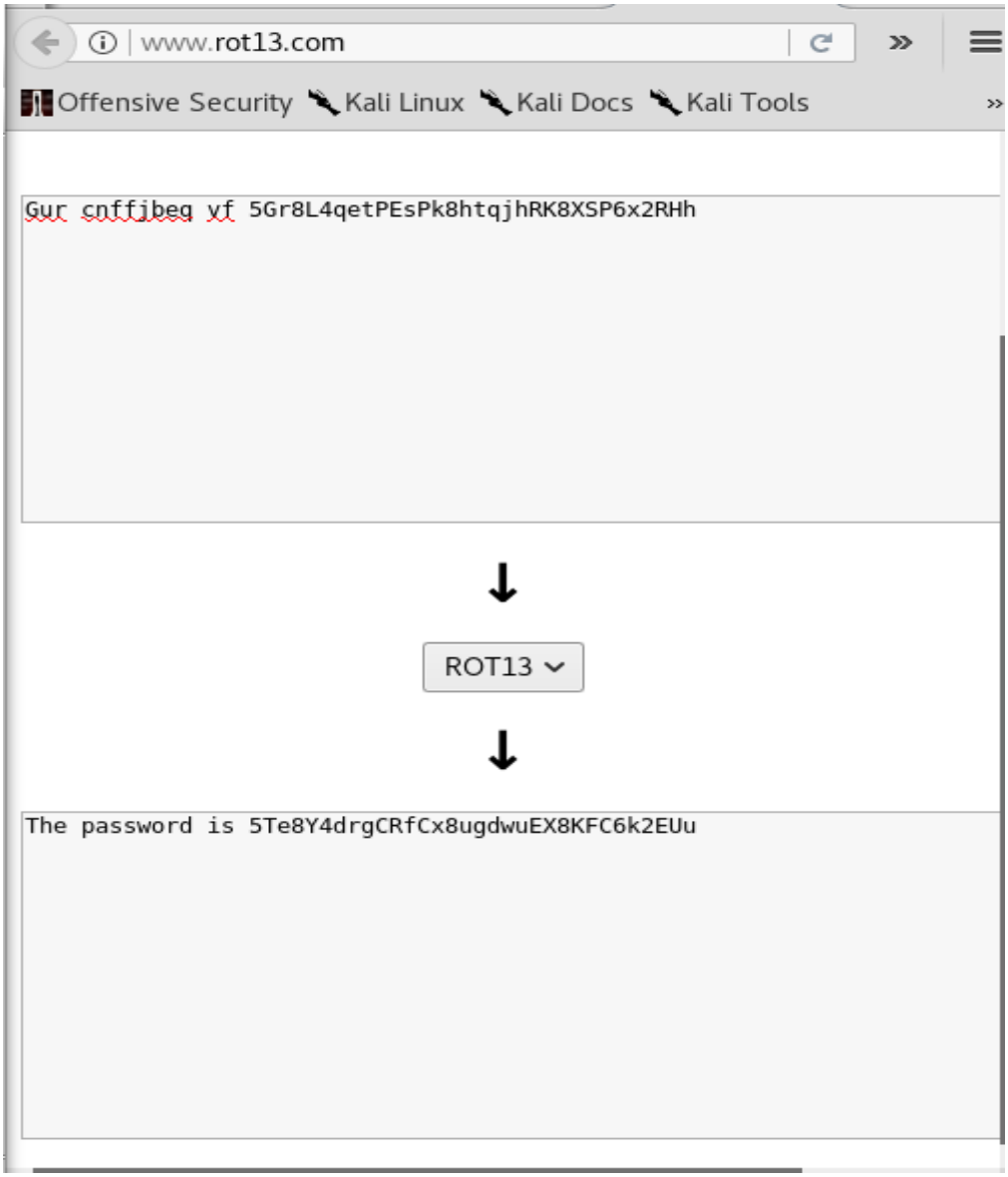
#ls
#cat data.txt
#echo
VGhlIHBhc3N3b3JkIGlzIElGdWt3S0dzRlc4TU9xM0lSRnFyeEUxaHhUTkViVVBSCg== | base64 –decode
#ssh -p 2220 bandit11@bandit.labs.overthewire.org

```
bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIElGdWt3S0dzRlc4TU9xM0lSRnFyeEUxaHh
UTkViVVBSCg==
bandit10@bandit:~$ echo VGhlIHBhc3N3b3JkIGlzIElGdWt3S0d
zRlc4TU9xM0lSRnFyeEUxaHhUTkViVVBSCg==
VGhlIHBhc3N3b3JkIGlzIElGdWt3S0dzRlc4TU9xM0lSRnFyeEUxaHh
UTkViVVBSCg==
bandit10@bandit:~$ echo VGhlIHBhc3N3b3JkIGlzIElGdWt3S0d
zRlc4TU9xM0lSRnFyeEUxaHhUTkViVVBSCg== | base64 --decode
The password is IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR
bandit10@bandit:~$ ssh -p 2220 bandit11@bandit.labs.ove
rthewire.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.or
g]:2220,[0.0.0.0]:2220' (ECDSA) to the list of known ho
sts.
                         _ _ _
| |__   __ _ _ __   __| (_) |_
| '_ \ / _` | '_ \ / _` | | __|
| |_) | (_| | | | | (_| | | |_
|_.__/ \__,_|_| |_|\__,_|_|\__|

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

bandit11@bandit.labs.overthewire.org's password:
```

Level 11 to Level 12:

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

#ls
#cat data.txt
 # use the provided data from cat to get the password from the following decrypter site tool : www.rot13.com
#ssh -p 2220 bandit12@bandit.labs.overthewire.org




```
bandit11@bandit:~$ ls
data.txt
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf 5Gr8L4qetPEsPk8htqjhRK8XSP6x2RHh
bandit11@bandit:~$ ssh -p 2220 bandit12@bandit.labs.ove
rthewire.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.or
g]:2220,[0.0.0.0]:2220' (ECDSA) to the list of known ho
sts.
 _                     _ _ _
| |__   __ _ _ __   __| (_) |_
| '_ \ / _` | '_ \ / _` | | __|
| |_) | (_| | | | | (_| | | |_
|_.__/ \__,_|_| |_|\__,_|_|\__|

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

bandit12@bandit.labs.overthewire.org's password:
```