

SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

Information System Security Audit & Control

**4th Year 2nd Semester 2016**

Name: Piumal Dinuka W.

SLIIT ID: IT13087234

Practical Session: WEEK DAY

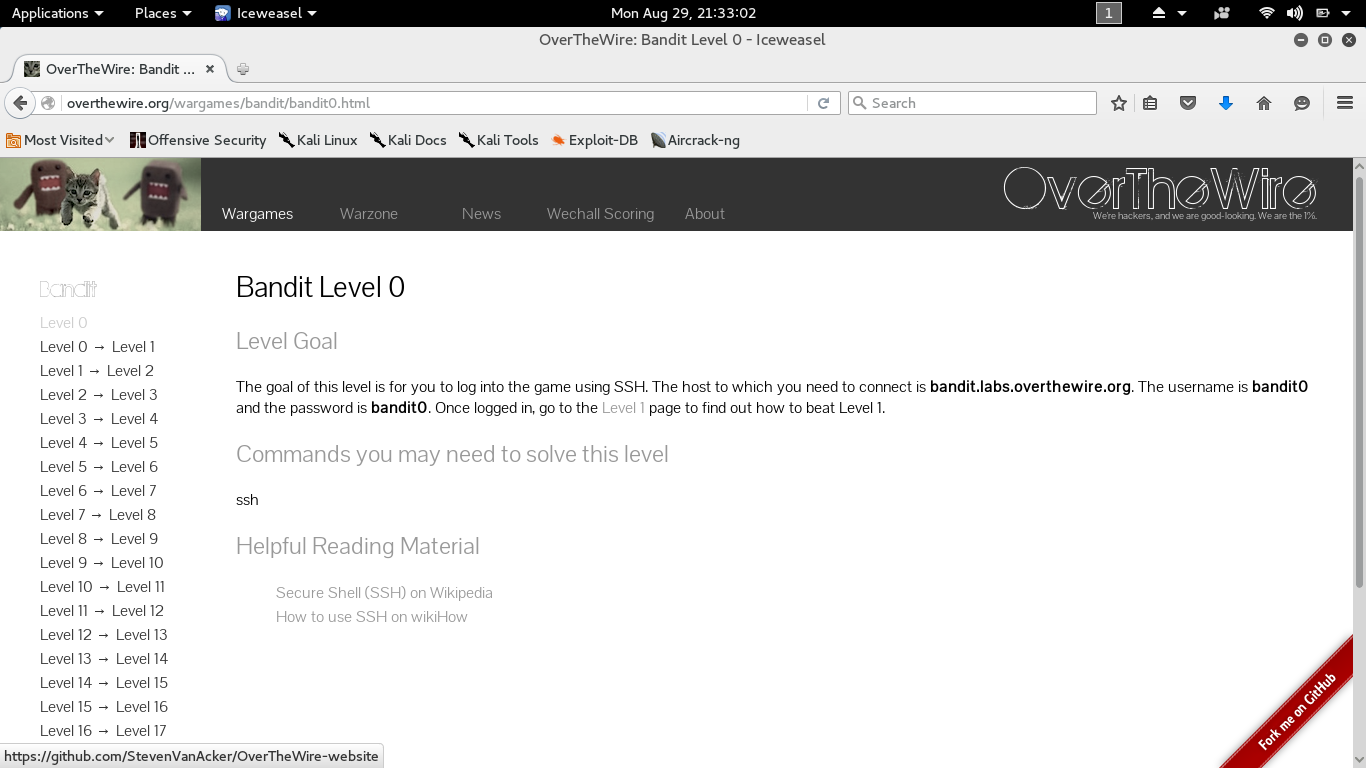
Practical Number: Lab 4 – Overthewire.org / Bandit lab

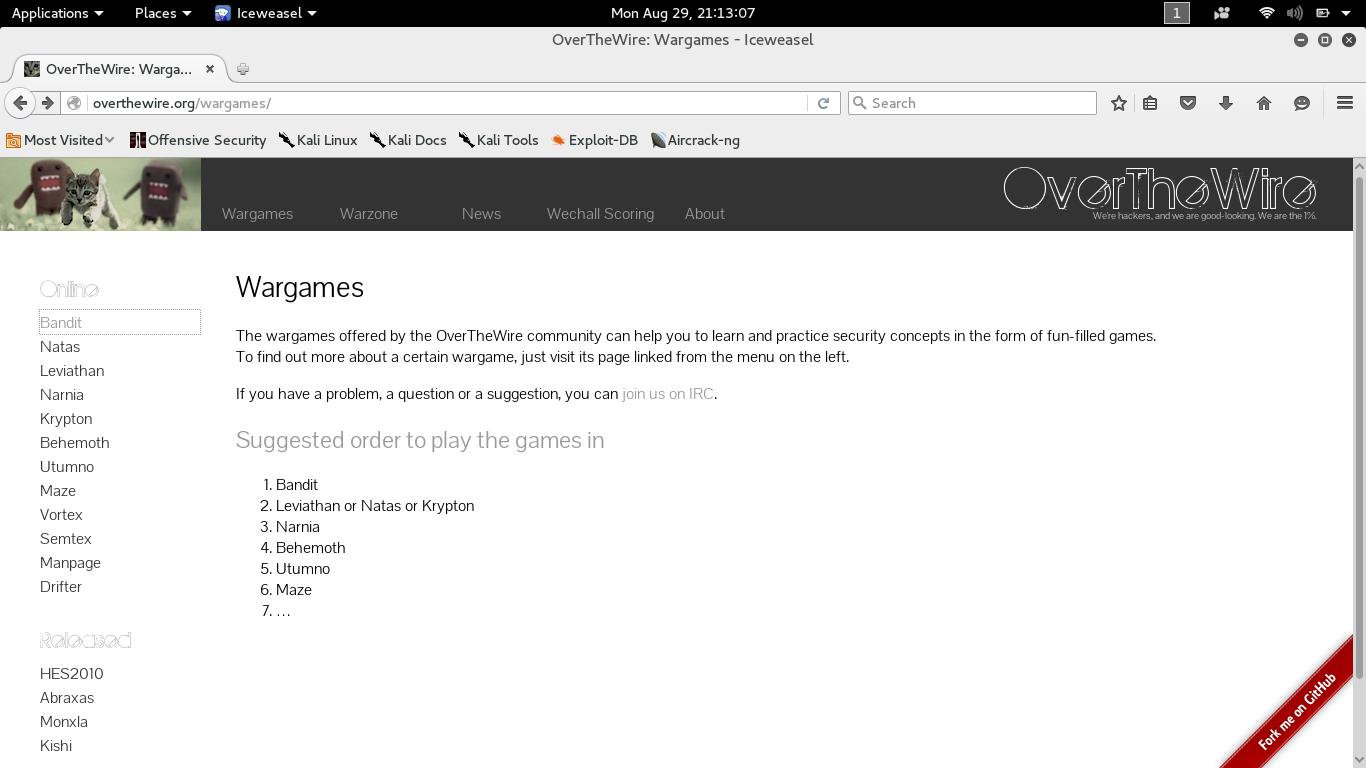
Date of Submission: - 9//2016

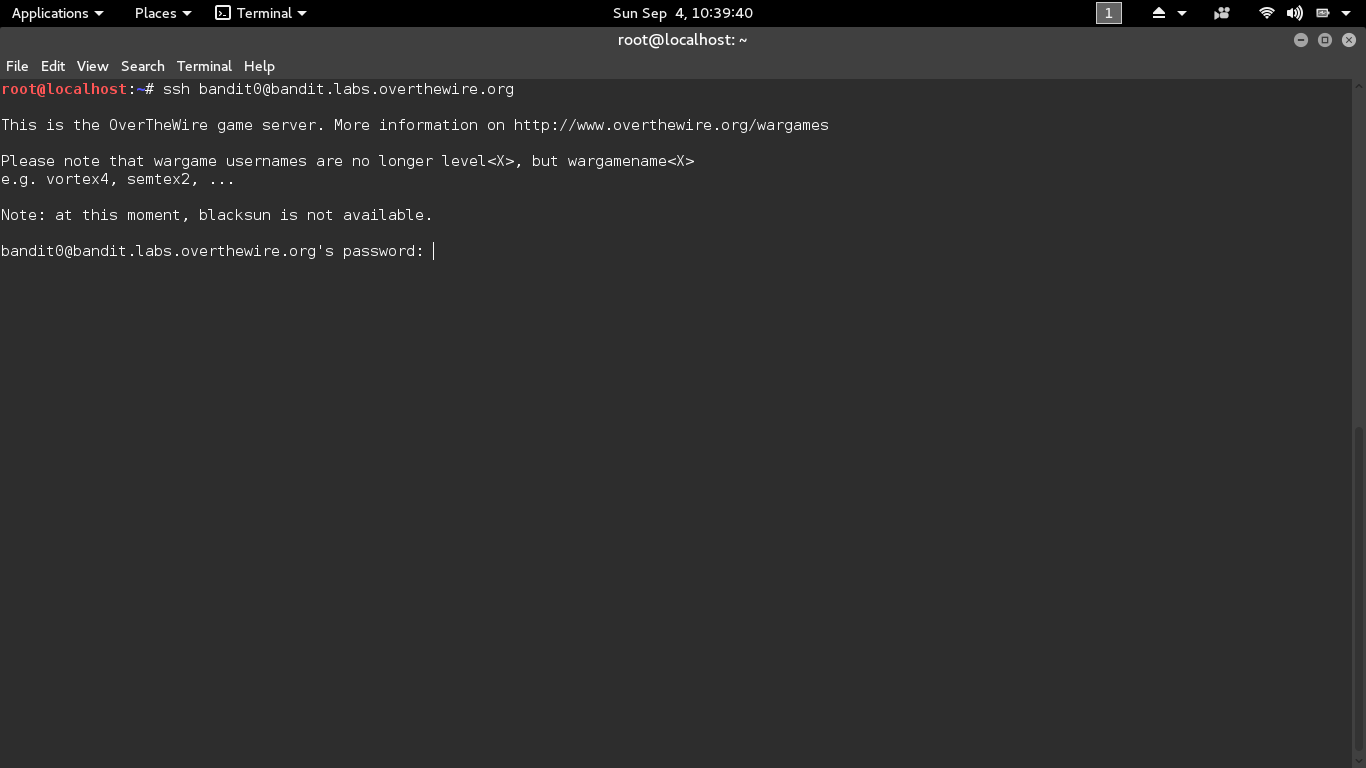
Date of Evaluation : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

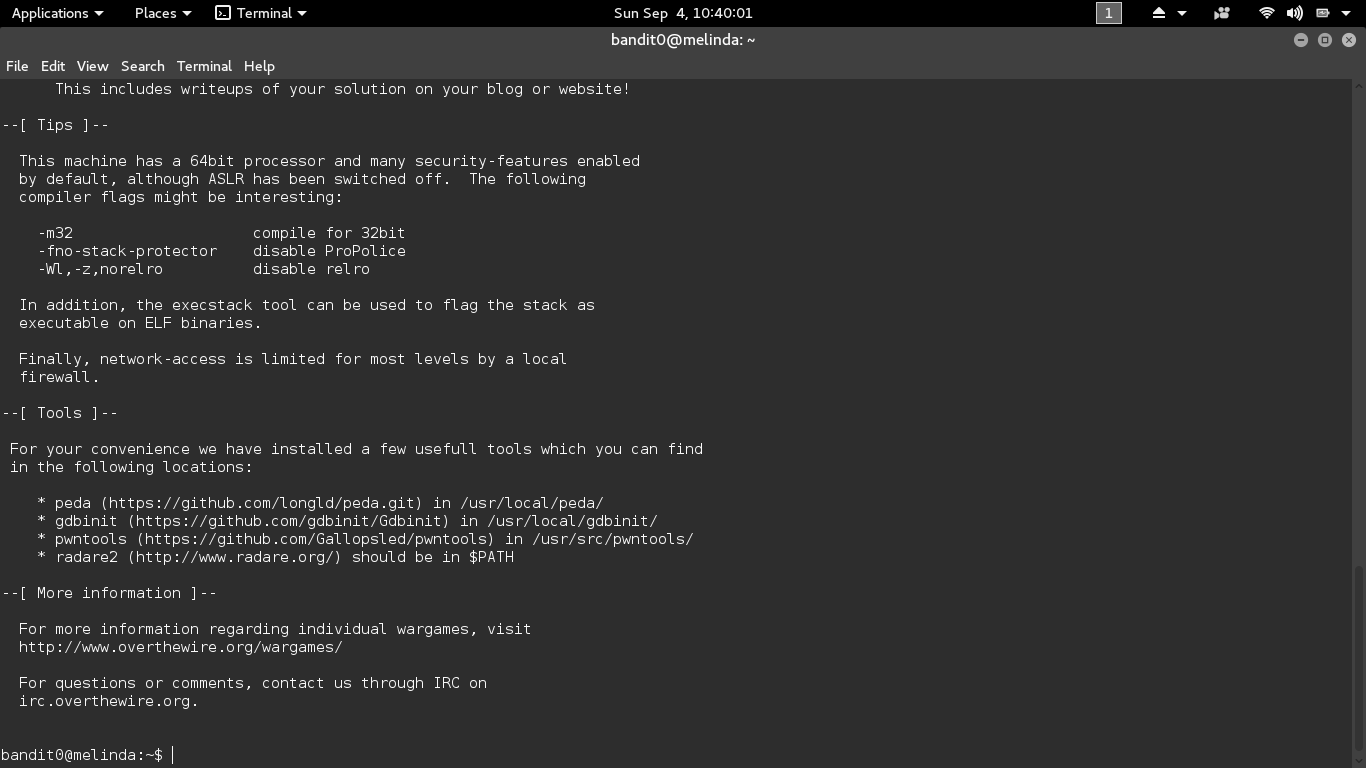
Evaluators Signature : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Level 0

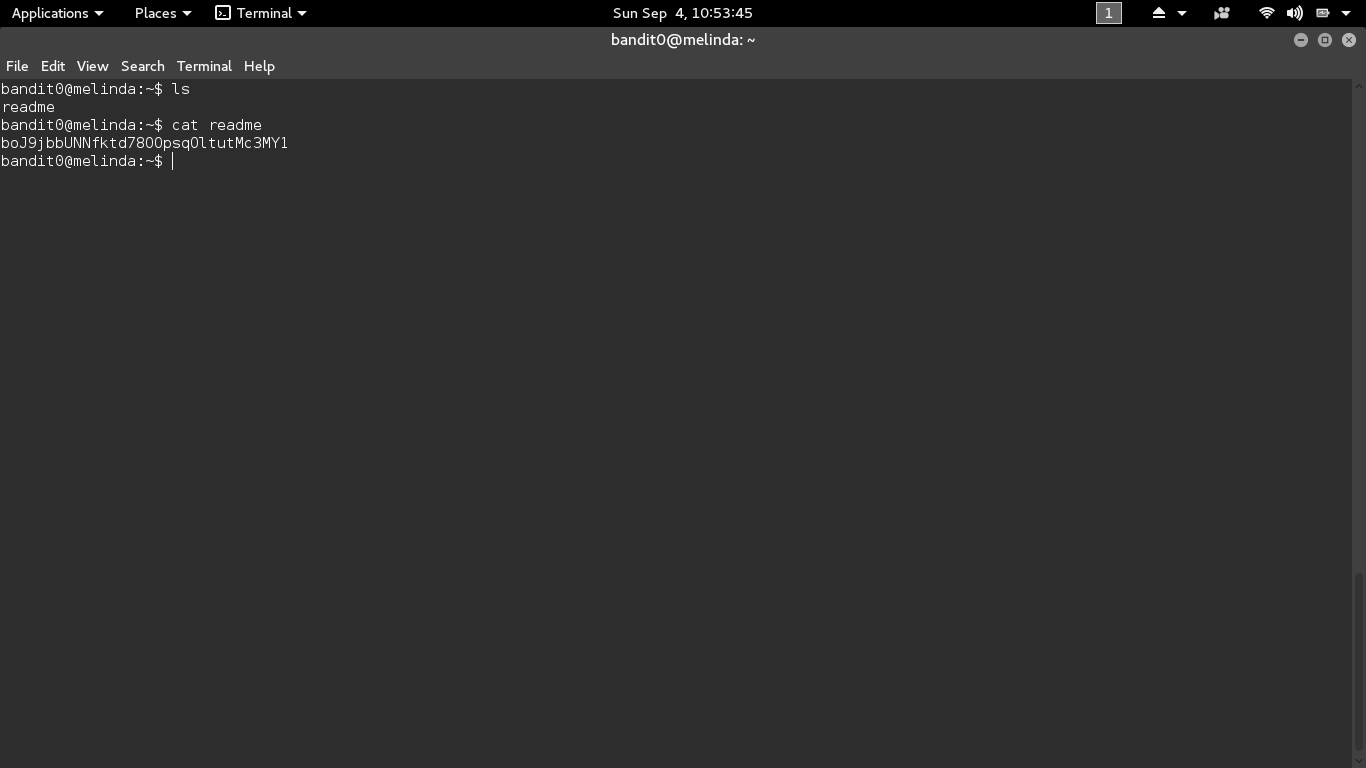


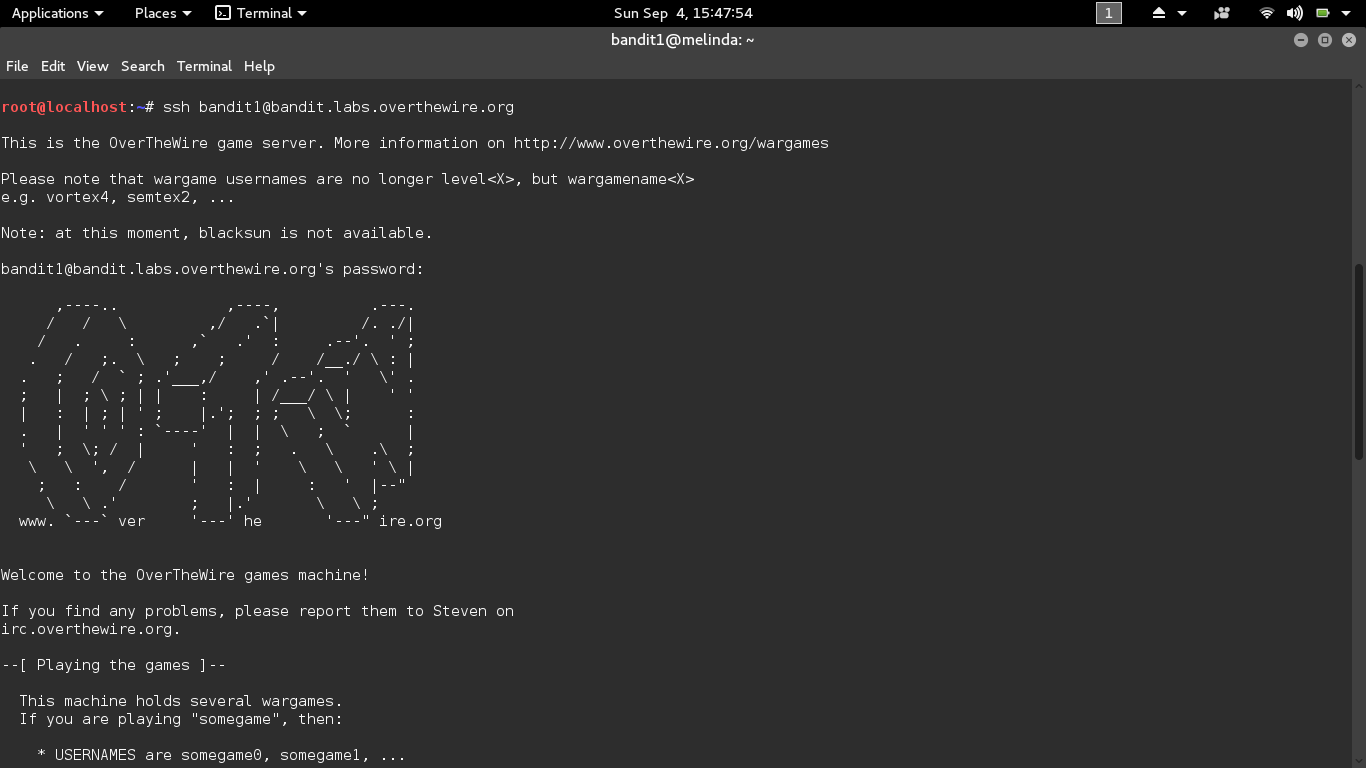


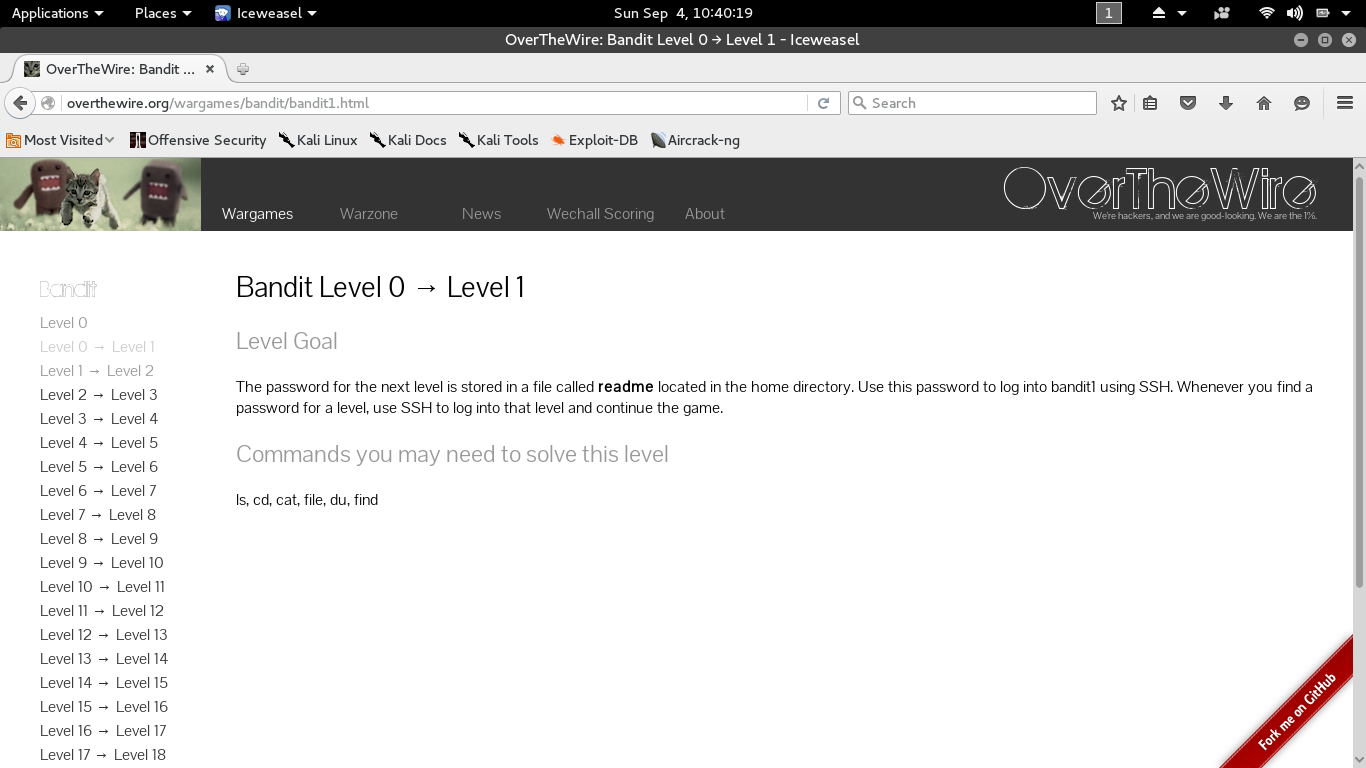
 Login to Site Using Linux Terminal



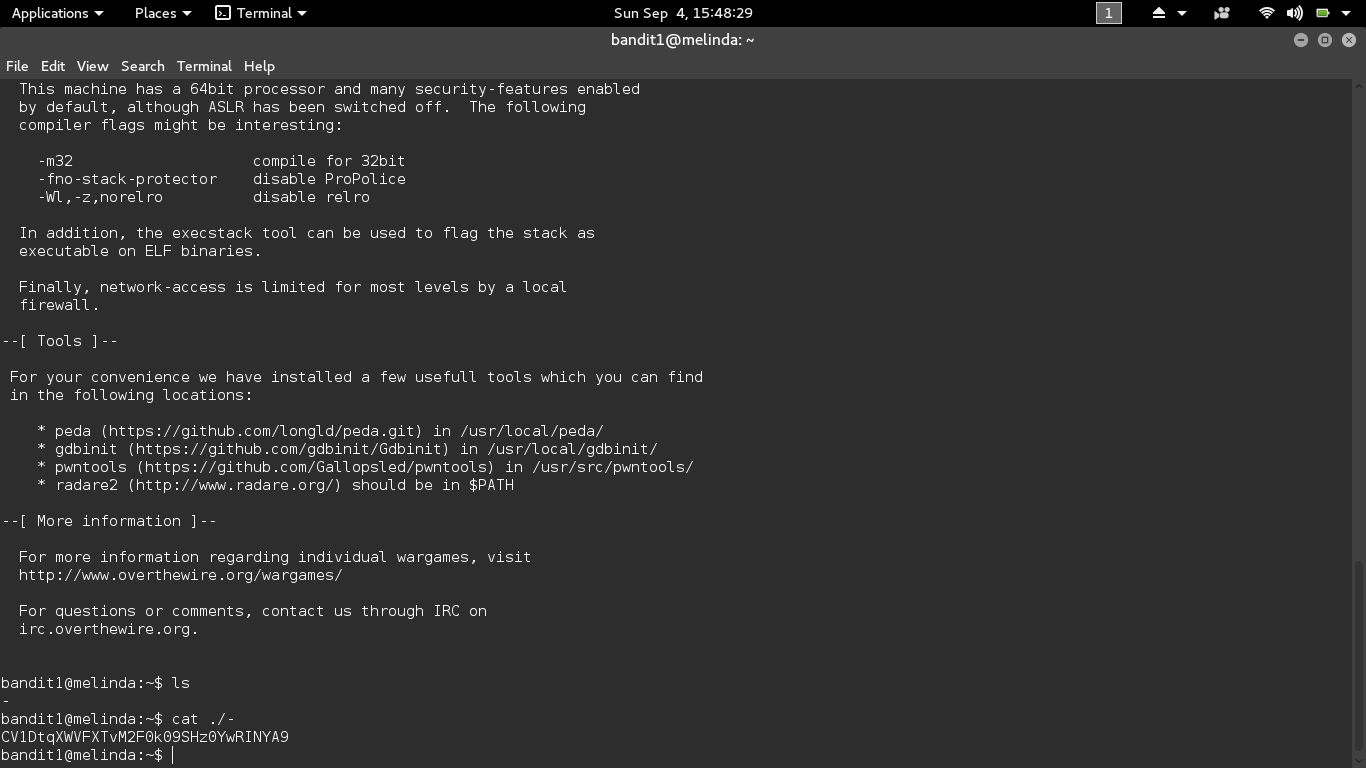
Bandit 0 Password



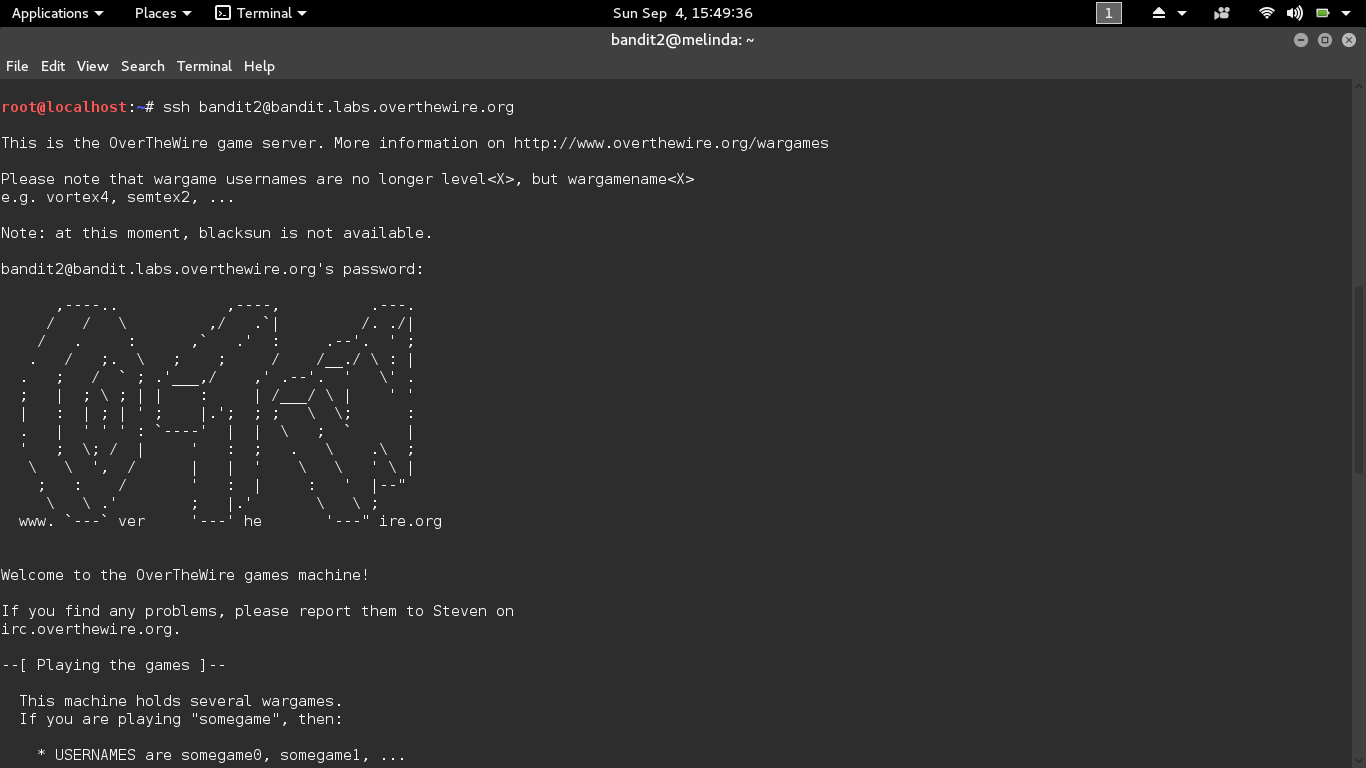
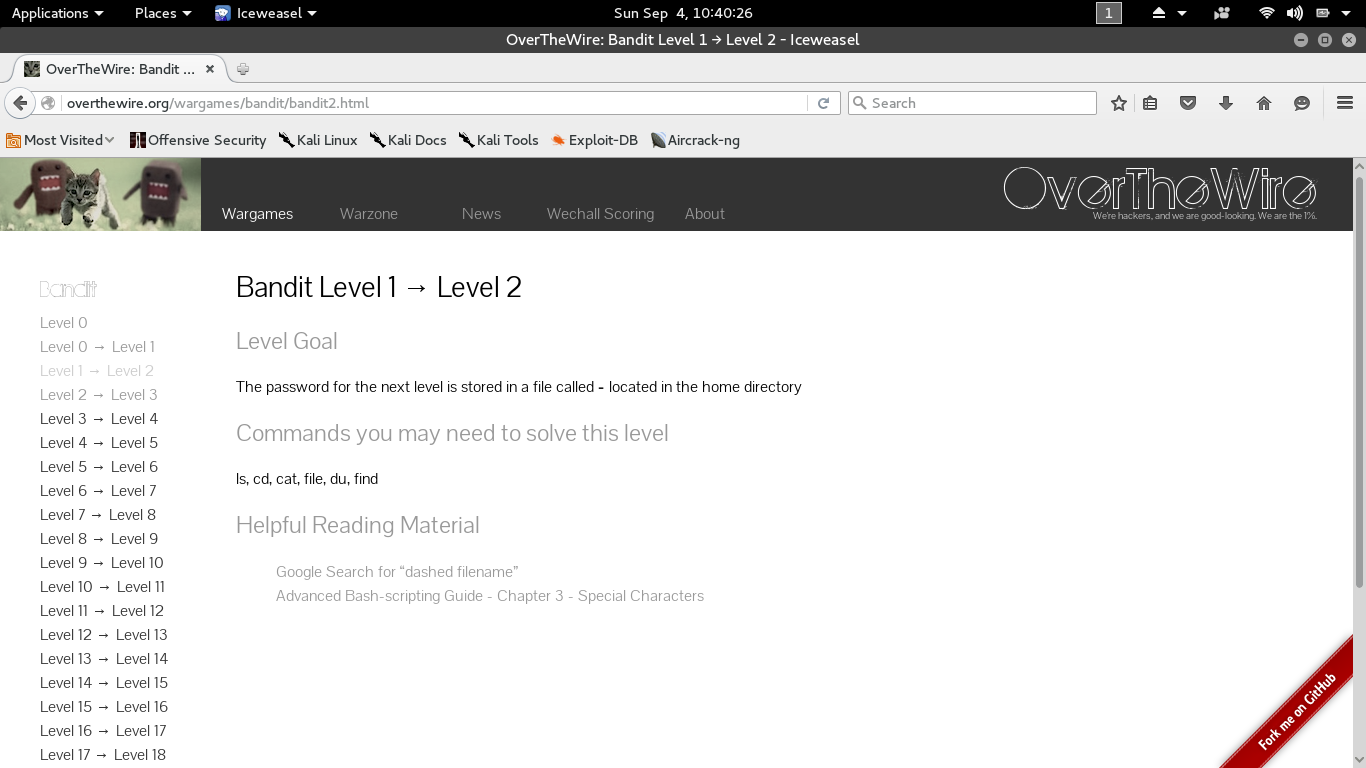
Level 0 → Level 1



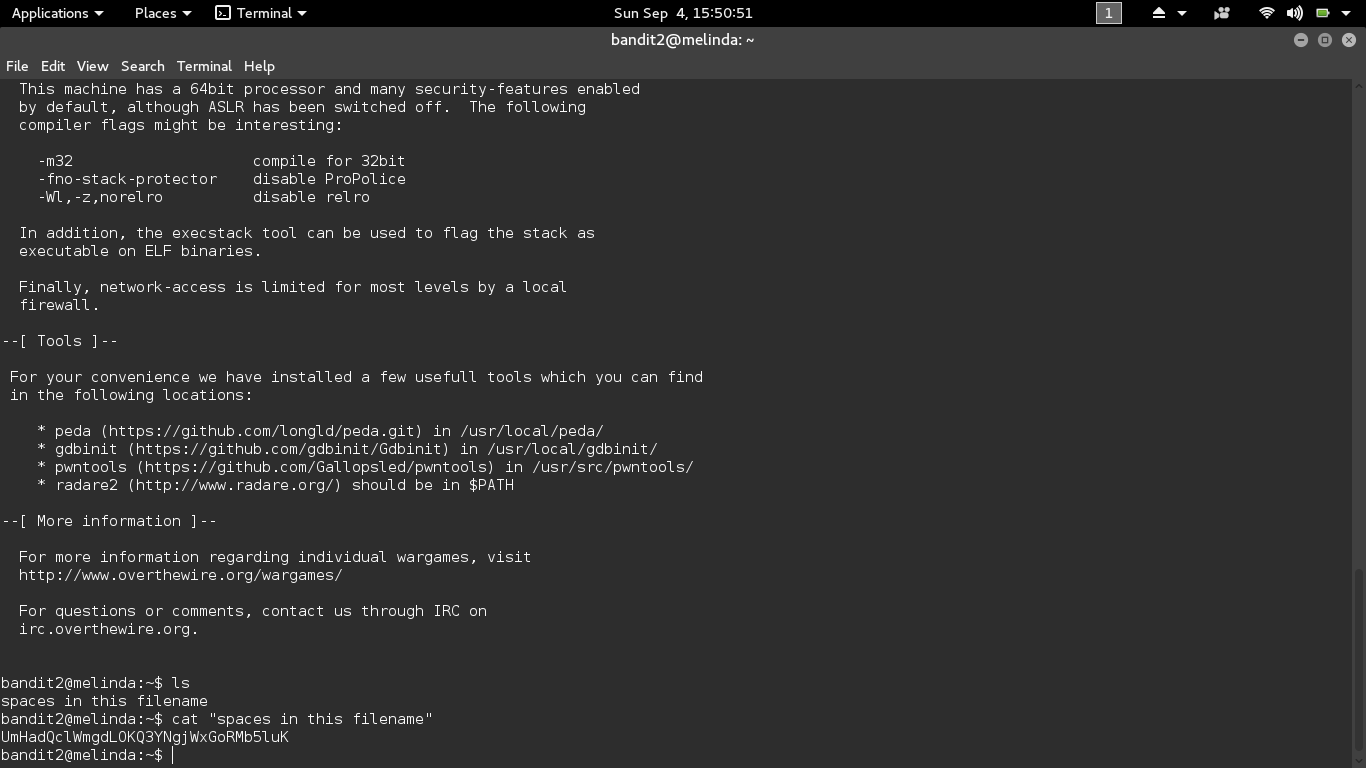
Bandit 1 Password



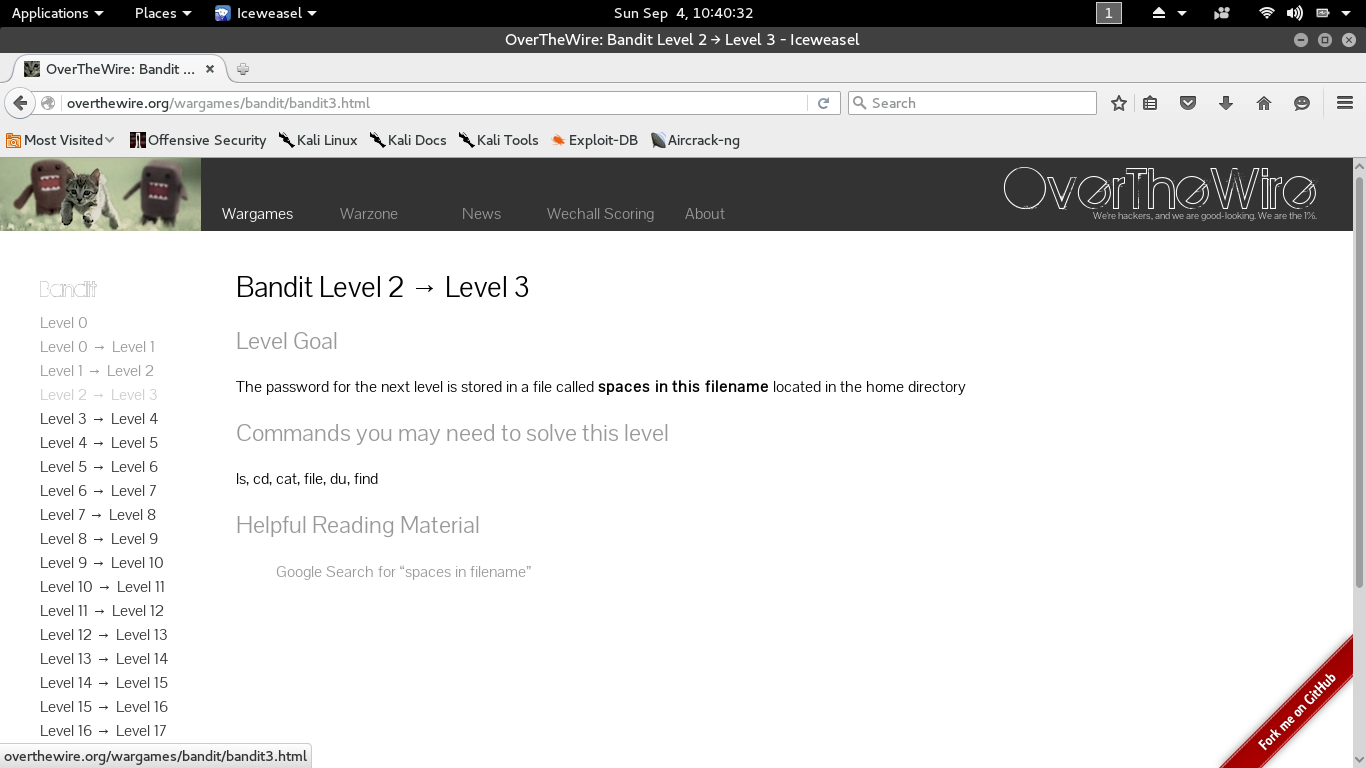
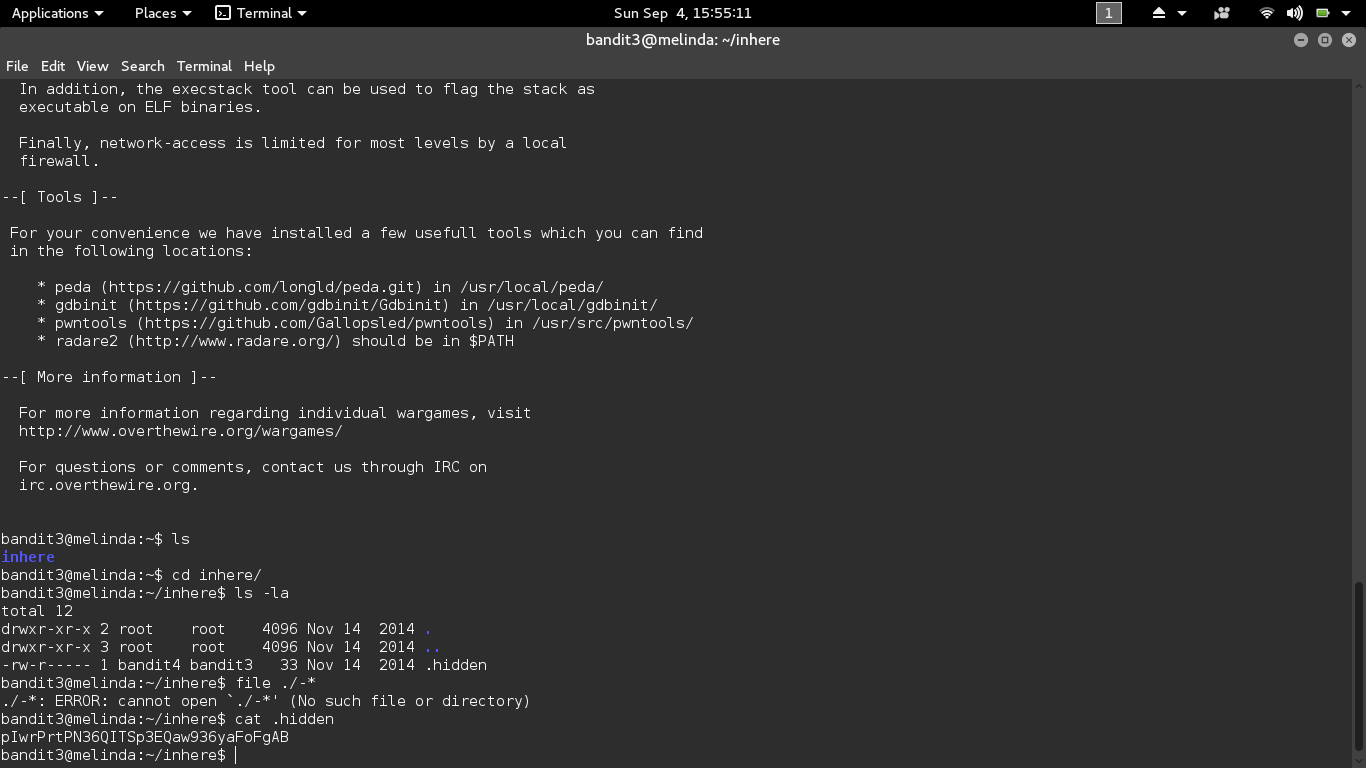
Level 1 → Level 2



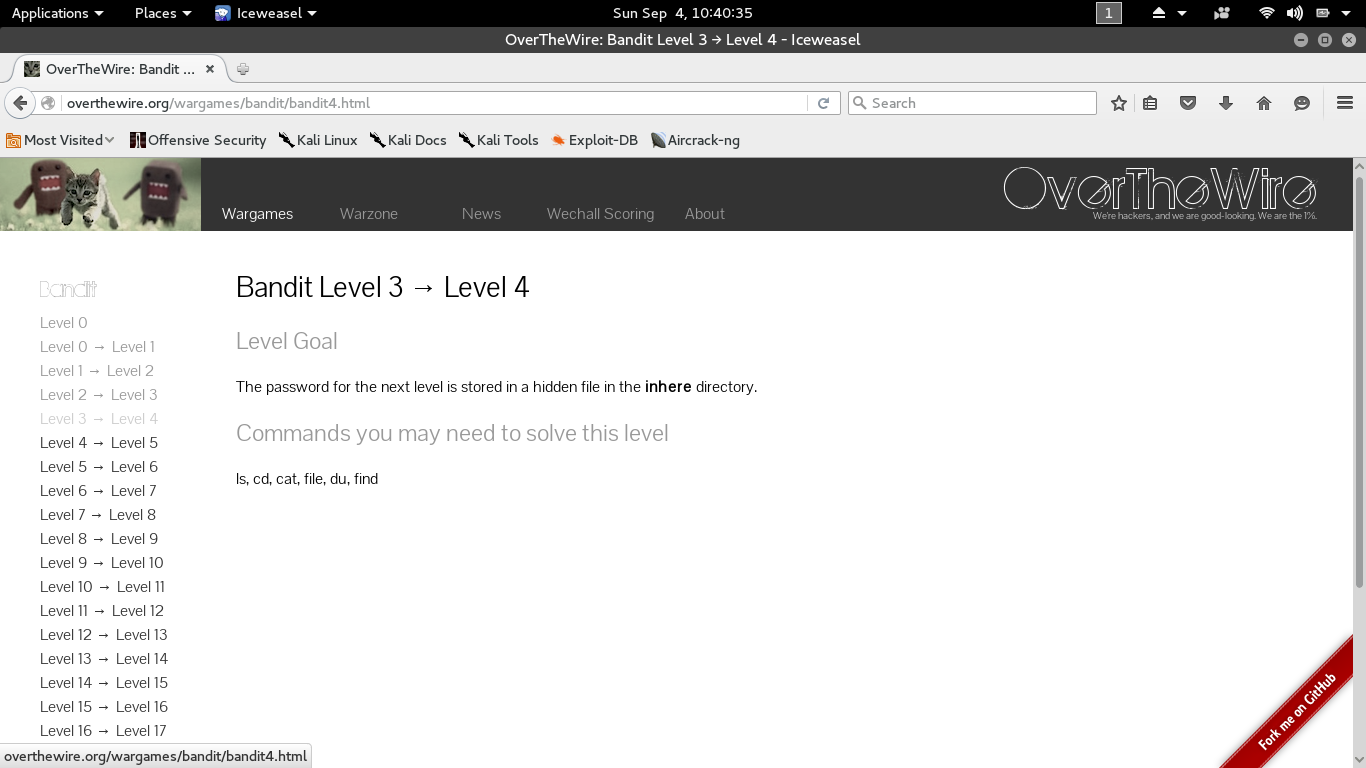
Bandit 2 Password



Level 2 → Level 3



Level 3 → Level 4

The file we need is in a hidden file in the inhere directory.

bandit3@melinda:~$ ls

inhere

bandit3@melinda:~$ cd inhere

bandit3@melinda:~/inhere$ ls -la

total 12

drwxr-xr-x 2 root    root    4096 2012-05-10 23:51 .

drwxr-xr-x 3 root    root    4096 2012-05-10 23:51 ..

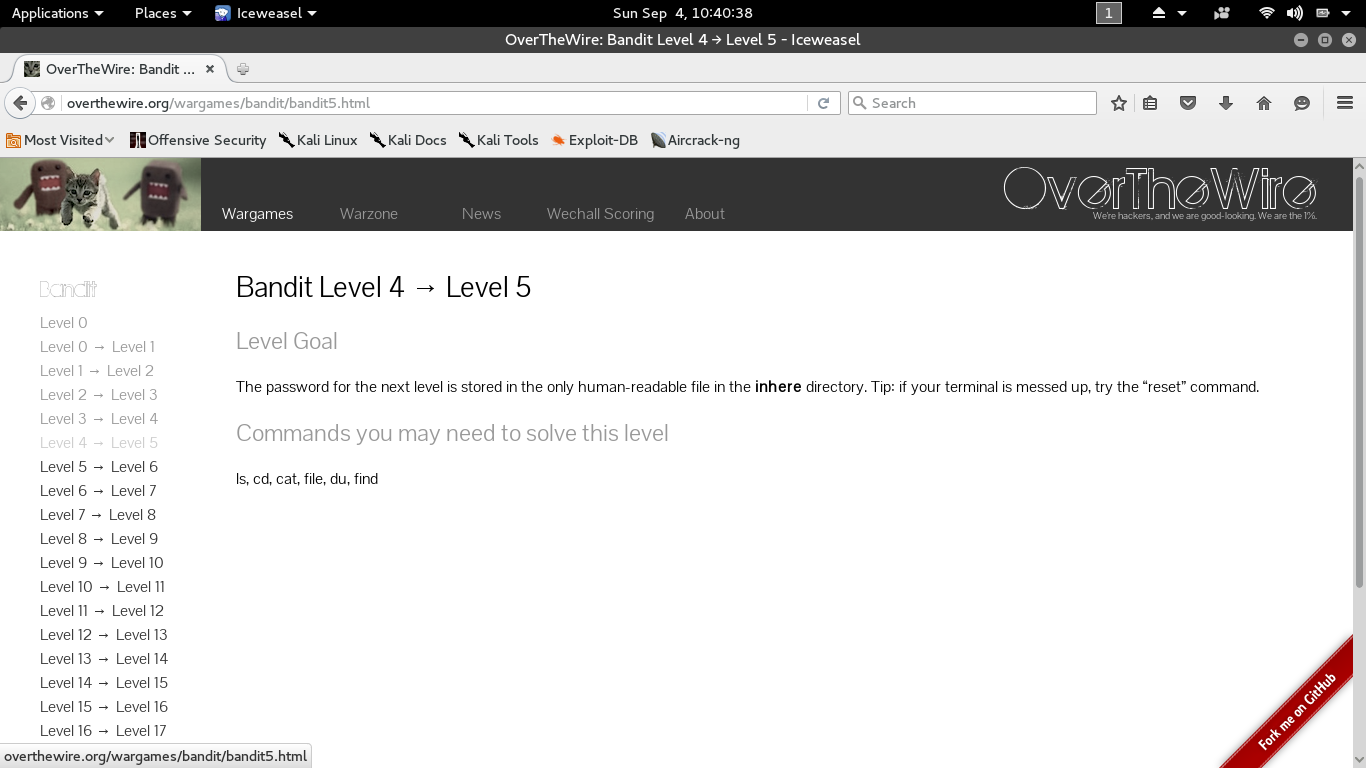
-rw-r----- 1 bandit4 bandit3   33 2012-05-10 23:51 .hidden

bandit3@melinda:~/inhere$ cat .hidden

pIwrPrtPN36QITSp3EQaw936yaFoFgAB

Level 4 → Level 5

The password is somewhere in the inhere directory and is the only human readable file in the directory



bandit4@melinda:~$ ls

inhere

bandit4@melinda:~$ cd inhere

bandit4@melinda:~/inhere$ ls -la

total 48

drwxr-xr-x 2 root    root    4096 2012-05-10 23:51 .

drwxr-xr-x 3 root    root    4096 2012-05-10 23:51 ..

-rw-r----- 1 bandit5 bandit4   33 2012-05-10 23:51 -file00

-rw-r----- 1 bandit5 bandit4   33 2012-05-10 23:51 -file01

-rw-r----- 1 bandit5 bandit4   33 2012-05-10 23:51 -file02

-rw-r----- 1 bandit5 bandit4   33 2012-05-10 23:51 -file03

-rw-r----- 1 bandit5 bandit4   33 2012-05-10 23:51 -file04

-rw-r----- 1 bandit5 bandit4   33 2012-05-10 23:51 -file05

-rw-r----- 1 bandit5 bandit4   33 2012-05-10 23:51 -file06

-rw-r----- 1 bandit5 bandit4   33 2012-05-10 23:51 -file07

-rw-r----- 1 bandit5 bandit4   33 2012-05-10 23:51 -file08

-rw-r----- 1 bandit5 bandit4   33 2012-05-10 23:51 -file09

bandit4@melinda:~/inhere$ file ./-\*

./-file00: data

./-file01: data

./-file02: data

./-file03: data

./-file04: data

./-file05: data

./-file06: data

./-file07: ASCII text

./-file08: data

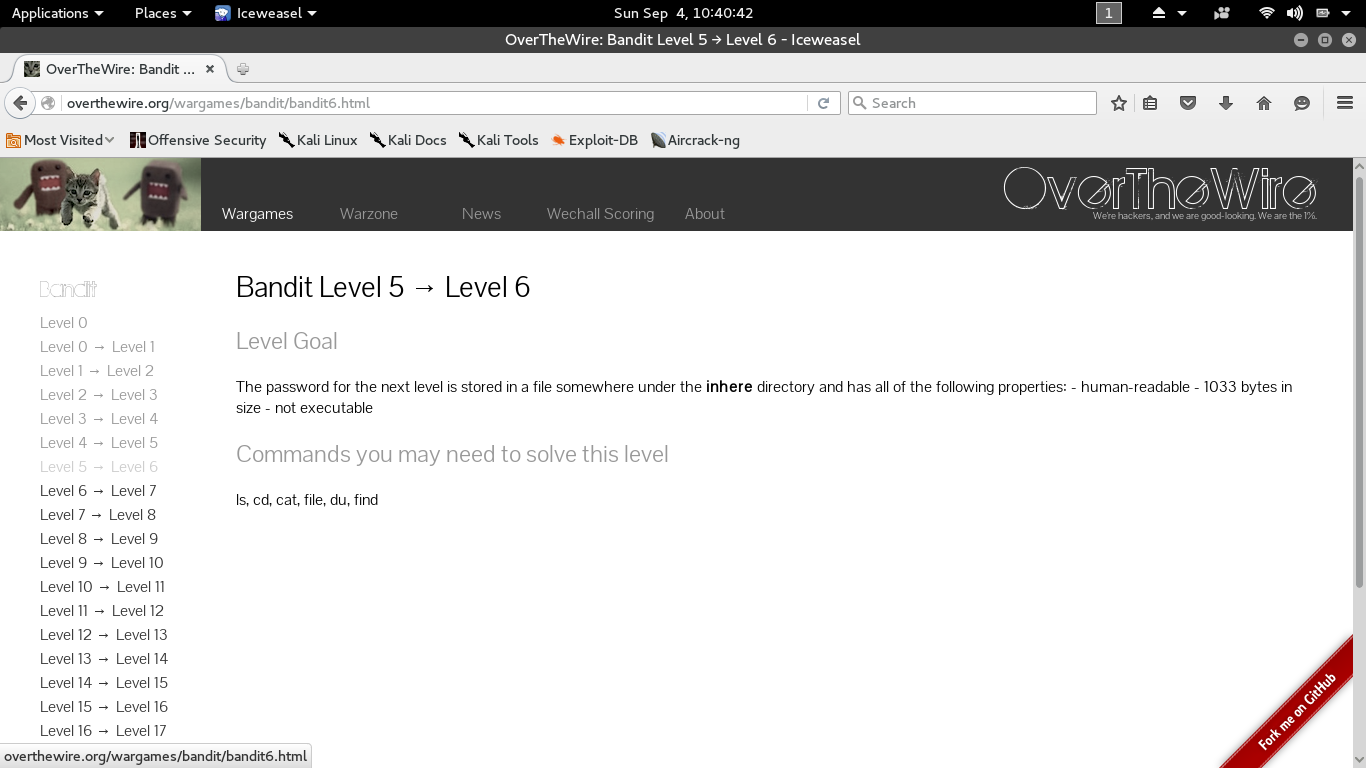
./-file09: data

bandit4@melinda:~/inhere$ cat ./-file07

koReBOKuIDDepwhWk7jZC0RTdopnAYKh

Level 5 → Level 6

This is similar to the previous, except have some more file attributes to look for. As well as more files to look through.



bandit5@melinda:~$ ls

inhere

bandit5@melinda:~$ cd inhere

bandit5@melinda:~/inhere$ ls -la

total 88

drwxr-x--- 22 root bandit5 4096 2012-05-10 23:51 .

drwxr-xr-x  3 root root    4096 2012-05-10 23:51 ..

drwxr-x---  2 root bandit5 4096 2012-05-10 23:51 maybehere00

drwxr-x---  2 root bandit5 4096 2012-05-10 23:51 maybehere01

drwxr-x---  2 root bandit5 4096 2012-05-10 23:51 maybehere02

drwxr-x---  2 root bandit5 4096 2012-05-10 23:51 maybehere03

drwxr-x---  2 root bandit5 4096 2012-05-10 23:51 maybehere04

drwxr-x---  2 root bandit5 4096 2012-05-10 23:51 maybehere05

drwxr-x---  2 root bandit5 4096 2012-05-10 23:51 maybehere06

drwxr-x---  2 root bandit5 4096 2012-05-10 23:51 maybehere07

drwxr-x---  2 root bandit5 4096 2012-05-10 23:51 maybehere08

drwxr-x---  2 root bandit5 4096 2012-05-10 23:51 maybehere09

drwxr-x---  2 root bandit5 4096 2012-05-10 23:51 maybehere10

drwxr-x---  2 root bandit5 4096 2012-05-10 23:51 maybehere11

drwxr-x---  2 root bandit5 4096 2012-05-10 23:51 maybehere12

drwxr-x---  2 root bandit5 4096 2012-05-10 23:51 maybehere13

drwxr-x---  2 root bandit5 4096 2012-05-10 23:51 maybehere14

drwxr-x---  2 root bandit5 4096 2012-05-10 23:51 maybehere15

drwxr-x---  2 root bandit5 4096 2012-05-10 23:51 maybehere16

drwxr-x---  2 root bandit5 4096 2012-05-10 23:51 maybehere17

drwxr-x---  2 root bandit5 4096 2012-05-10 23:51 maybehere18

drwxr-x---  2 root bandit5 4096 2012-05-10 23:51 maybehere19

bandit5@melinda:~/inhere$ find ./ -size 1033c

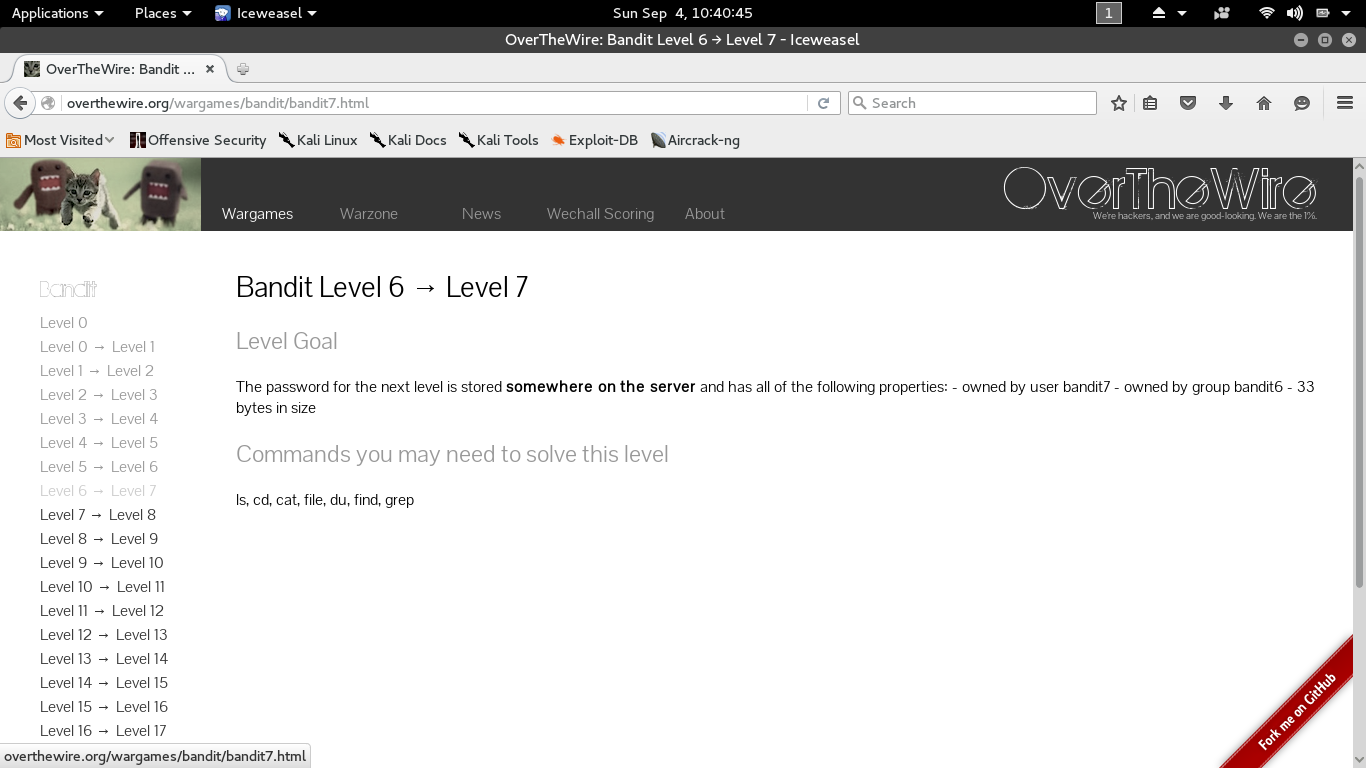
./maybehere07/.file2

bandit5@melinda:~/inhere$ cat ./maybehere07/.file2

DXjZPULLxYr17uwoI01bNLQbtFemEgo7

Level 6 → Level 7

The file can be anywhere on the server, but we are given it’s attributes. This is a job for find. The command attached to the end gets rid of garbage returns and allows viewing of our password file amongst several others with the same attributes.



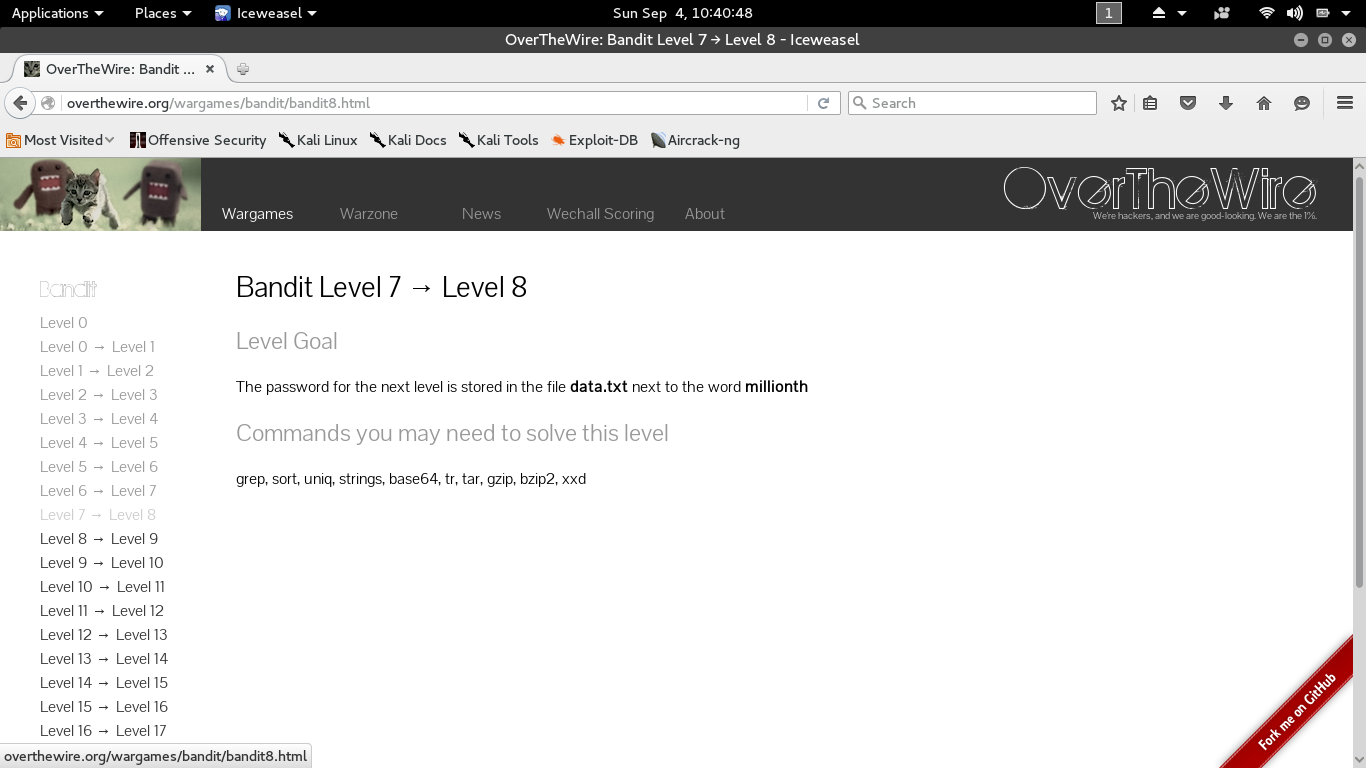
bandit6@melinda:~$ find / -user bandit7 -group bandit6 -size 33c 2>/dev/null /var/lib/dpkg/info/bandit7.password

bandit6@melinda:~$ cat /var/lib/dpkg/info/bandit7.password

HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs

Level 7 → Level 8

The password for the next level is stored in the file data.txt next to the word millionth. can pipe cat to grep for this.



bandit7@melinda:~$ ls

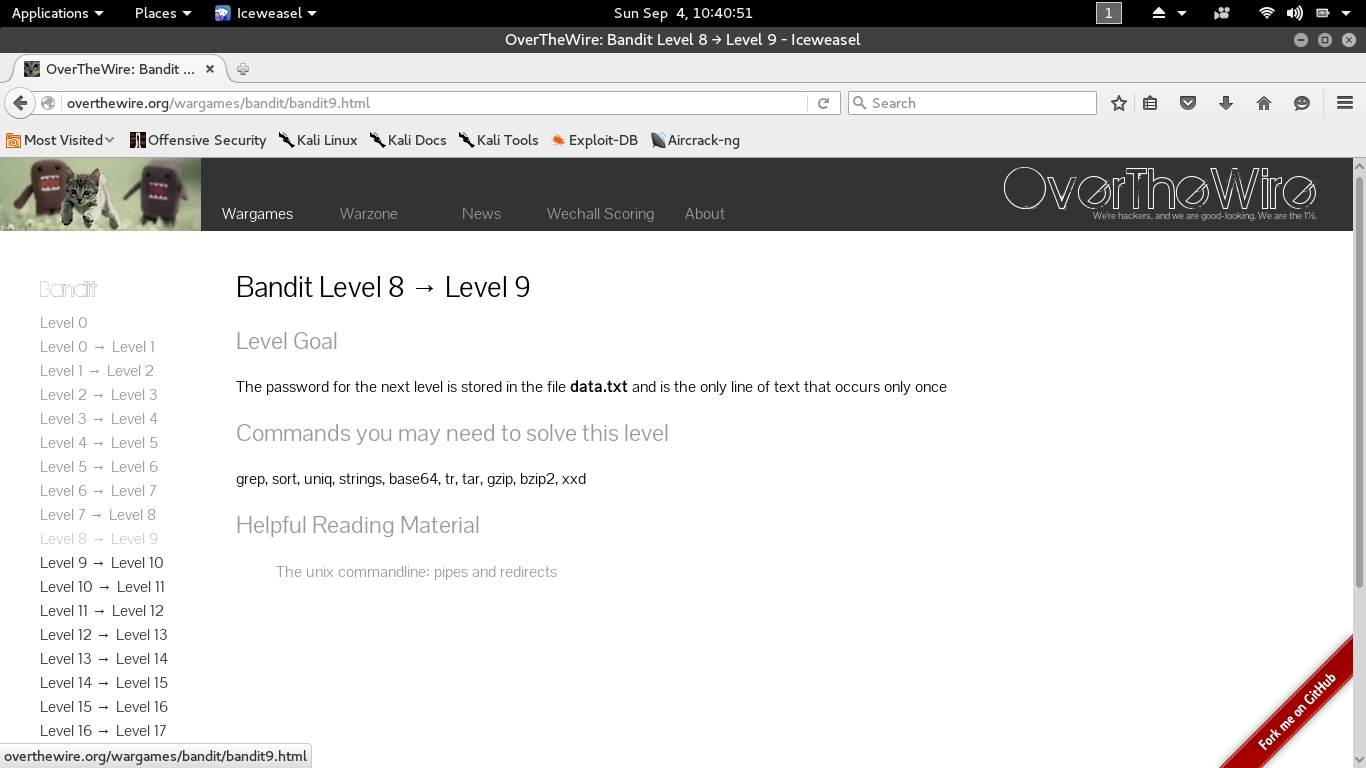
data.txt

bandit7@melinda:~$ cat data.txt | grep millionth

millionth       cvX2JJa4CFALtqS87jk27qwqGhBM9plV

Level 8 → Level 9

Need to find a unique line among many. Can pipe a few commands together to do this.



bandit8@melinda:~$ ls

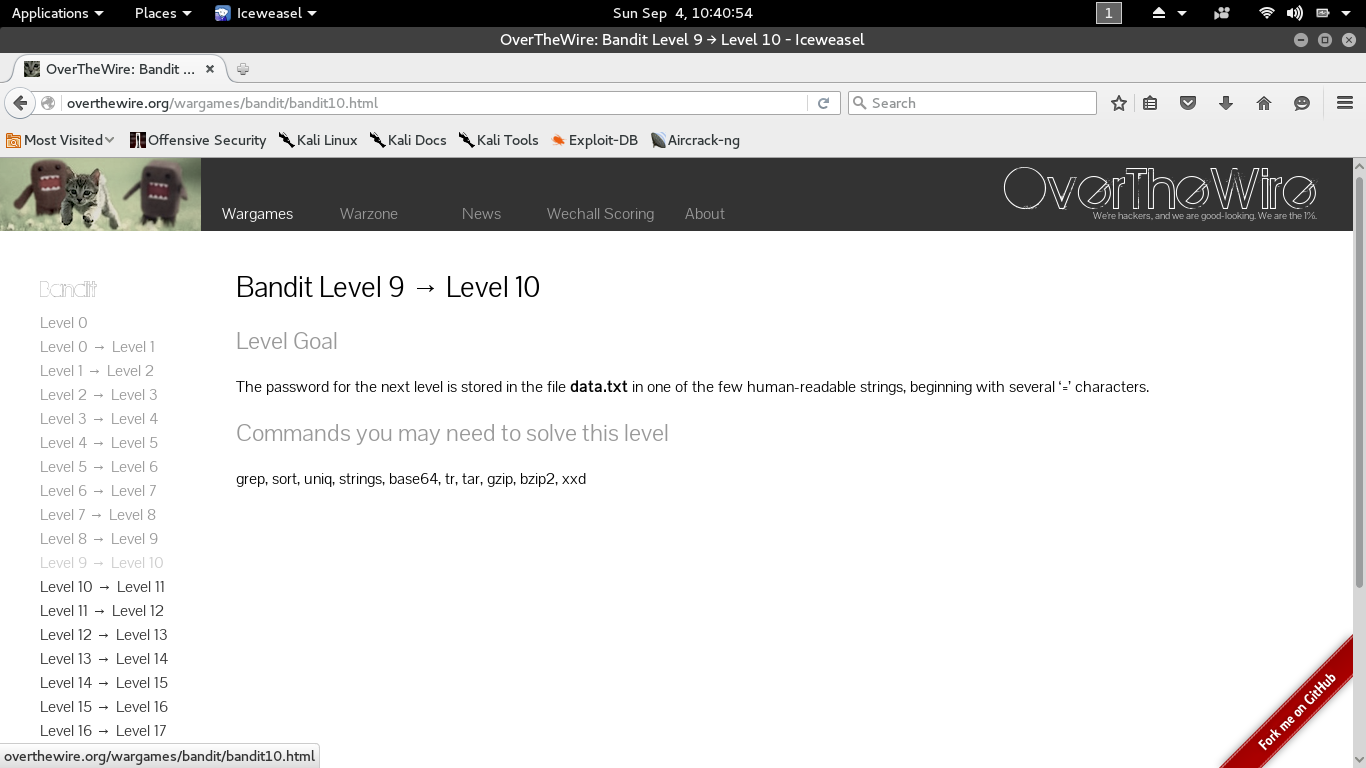
data.txt

bandit8@melinda:~$ cat data.txt | sort | uniq -u

UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR

Level 9 → Level 10

The password for the next level is stored in the file data.txt among of few lines of human-readable strings starting with ‘=’ characters.



bandit9@melinda:~$ ls

data.txt

bandit9@melinda:~$ strings data.txt | grep '='

========== the

R=ev2,

NF=!^

M5Q=

========== password

TuI@=

========== iss

c       =$

w=RO

eD=p

jR=JlB

G========== truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk

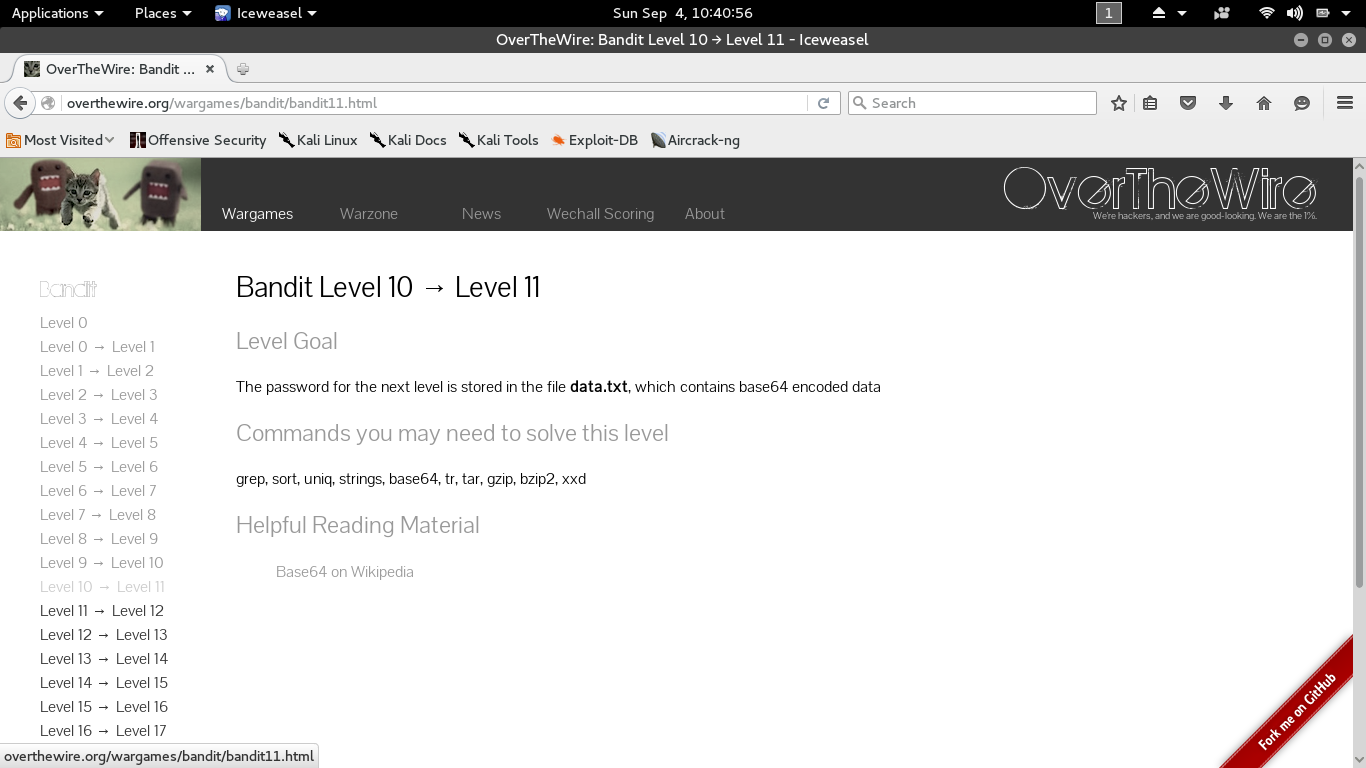
:=\*1p

KA=%

Password is - truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk

Level 10 → Level 11

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



bandit10@melinda:~$ ls

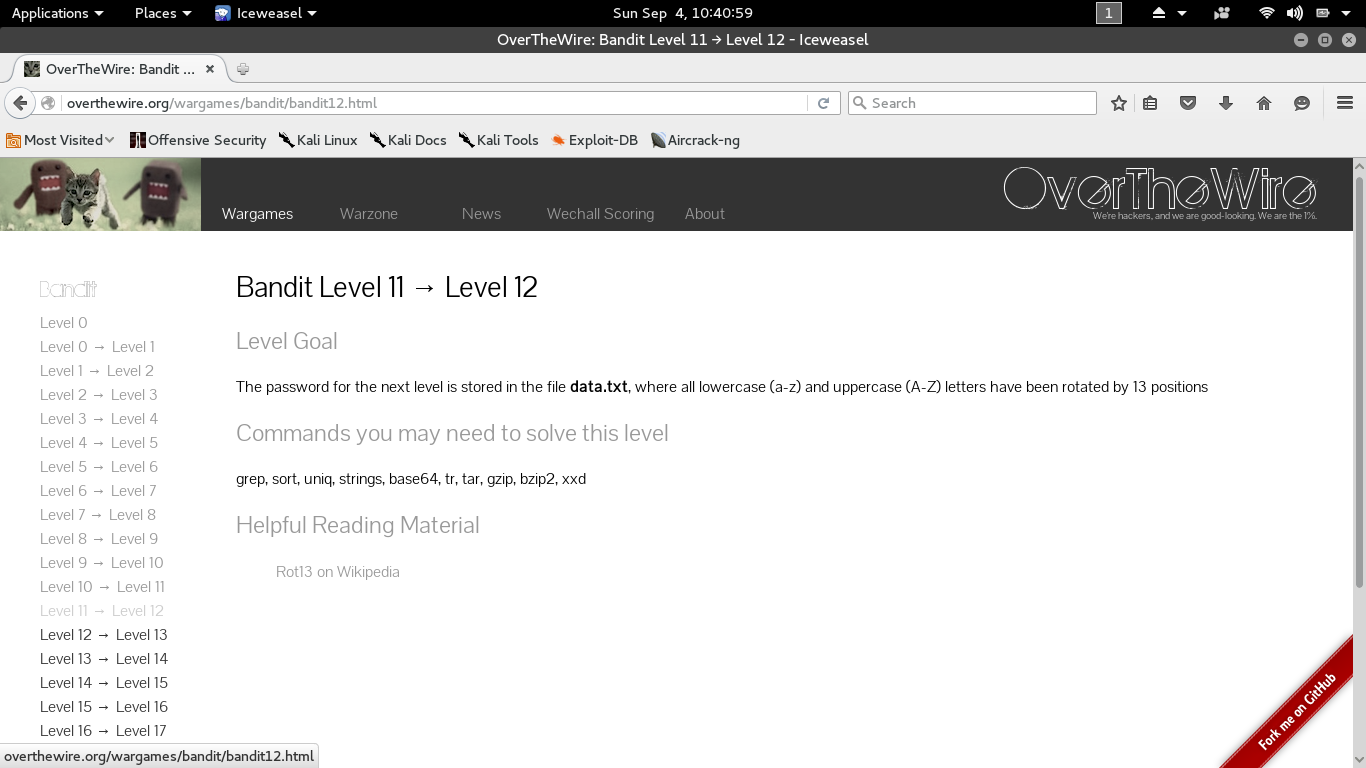
data.txt

bandit10@melinda:~$ base64 -d data.txt

The password is IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR

Level 11 → Level 12

The password is encoded using simple rot13 encryption. There are many options to solve this including using various scripting languages and simply using an online rot13 decoder. Let’s try a solution in our shell.



bandit11@melinda:~$ ls

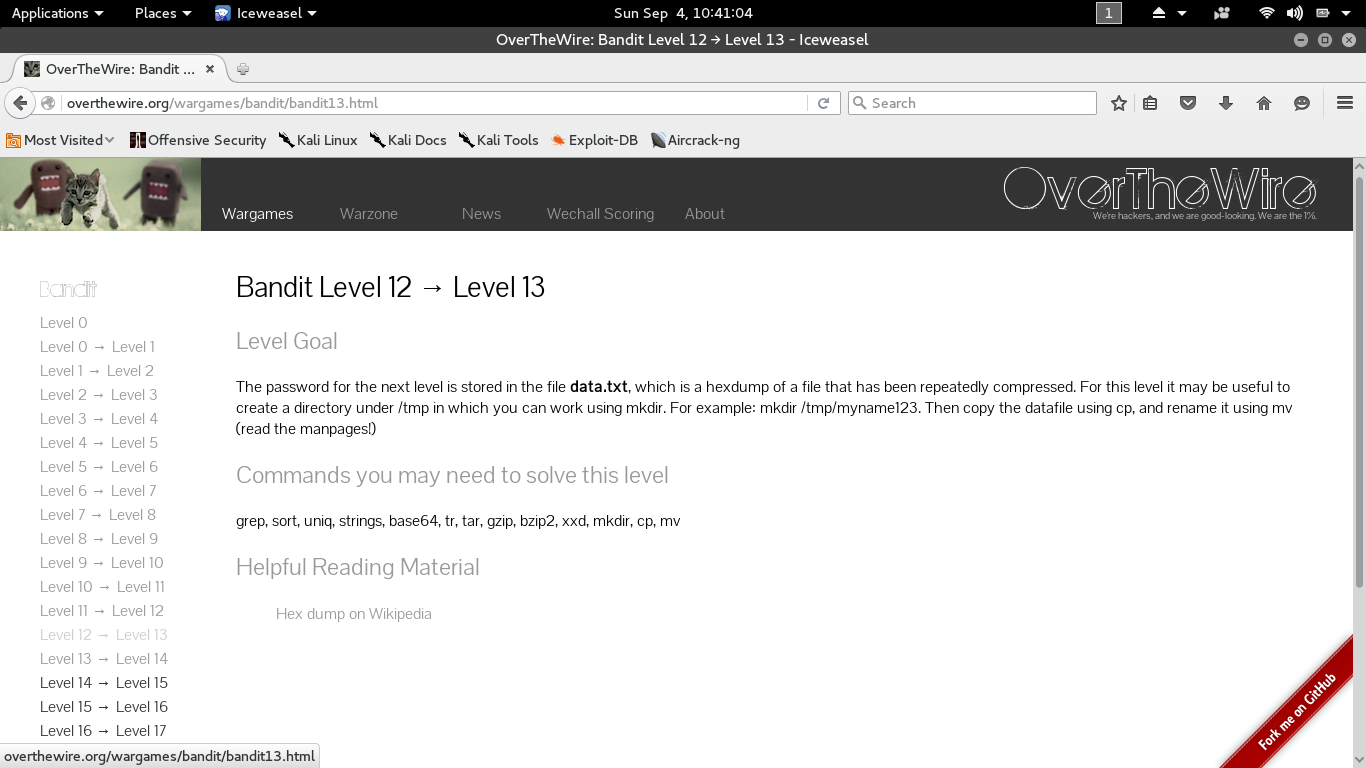
data.txt

bandit11@melinda:~$ cat data.txt | tr a-zA-Z n-za-mN-ZA-M

The password is 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu

Level 12 → Level 13

The password for the next level is stored in the file data.txt, which is a hexdump of a file that has been repeatedly compressed. For this level it is necessary to create a directory under /tmp in which you can work using mkdir. We need to decompress and check the file over and over again until we get the right format.



bandit12@melinda:~$ ls

data.txt

bandit12@melinda:~$ file data.txt

data.txt: ASCII text

bandit12@melinda:~$ mkdir /tmp/stw

bandit12@melinda:~$ cd /tmp/stw

bandit12@melinda:/tmp/stw$ xxd -r ~/data.txt > data.txt

bandit12@melinda:/tmp/stw$ file data.txt

data.txt: gzip compressed data, was "data2.bin", from Unix, last modified: Thu May 10 23:52:05 2012, max compression

bandit12@melinda:/tmp/stw$ zcat data.txt > dataNew

bandit12@melinda:/tmp/stw$ ls

dataNew  data.txt

bandit12@melinda:/tmp/stw$ file dataNew

dataNew: bzip2 compressed data, block size = 900k

bandit12@melinda:/tmp/stw$ bzip2 -d dataNew

bzip2: Can't guess original name for dataNew -- using dataNew.out

bandit12@melinda:/tmp/stw$ ls

dataNew.out  data.txt

bandit12@melinda:/tmp/stw$ file dataNew.out

dataNew.out: gzip compressed data, was "data4.bin", from Unix, last modified: Thu May 10 23:52:05 2012, max compression

bandit12@melinda:/tmp/stw$ zcat dataNew.out > evenNewer

bandit12@melinda:/tmp/stw$ ls

dataNew.out  data.txt  evenNewer

bandit12@melinda:/tmp/stw$ file evenNewer

evenNewer: POSIX tar archive (GNU)

bandit12@melinda:/tmp/stw$ tar -xvf evenNewer

data5.bin

bandit12@melinda:/tmp/stw$ file data5.bin

data5.bin: POSIX tar archive (GNU)

bandit12@melinda:/tmp/stw$ tar -xvf data5.bin

data6.bin

bandit12@melinda:/tmp/stw$ file data6.bin

data6.bin: bzip2 compressed data, block size = 900k

bandit12@melinda:/tmp/stw$ bzip2 -d data6.bin

bzip2: Can't guess original name for data6.bin -- using data6.bin.out

bandit12@melinda:/tmp/stw$ ls

data5.bin  data6.bin.out  dataNew.out  data.txt  evenNewer

bandit12@melinda:/tmp/stw$ file data6.bin.out

data6.bin.out: POSIX tar archive (GNU)

bandit12@melinda:/tmp/stw$ tar -xvf data6.bin.out

data8.bin

bandit12@melinda:/tmp/stw$ file data8.bin

data8.bin: gzip compressed data, was "data9.bin", from Unix, last modified: Thu May 10 23:52:05 2012, max compression

bandit12@melinda:/tmp/stw$ zcat data8.bin > lost

bandit12@melinda:/tmp/stw$ ls

data5.bin  data6.bin.out  data8.bin  dataNew.out  data.txt  evenNewer  lost

bandit12@melinda:/tmp/stw$ file lost

lost: ASCII English text

bandit12@melinda:/tmp/stw$ cat lost

The password is <strong>8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL</strong>