Niveles bandit

Michele Benequen Feliciano

Septiembre16/2020

Bandit Level 0 → Level 1

Level Goal

The password for the next level is stored in a file called readme located in the home directory. Use this password to log into bandit1 using SSH. Whenever you find a password for a level, use SSH (on port 2220) to log into that level and continue the game.

Commands you may need to solve this level

ls, cd, cat, file, du, find

```
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme

bandit0@bandit:~$ boJ9jbbUNNfktd78OOpsqOltutMc3MY1
```

Bandit Level 1 → Level 2

Level Goal

The password for the next level is stored in a file called - located in the home directory

Commands you may need to solve this level

ls, cd, cat, file, du, find

```
bandit1@bandit:~$ ls -al
```

```
bandit1@bandit:~$ cat ./-
```

```
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
```

Bandit Level 2 → Level 3

Level Goal

The password for the next level is stored in a file called spaces in this filename located in the home directory

Commands you may need to solve this level

ls, cd, cat, file, du, find

```
bandit2@bandit:~$ ls
```

```
spaces in this filename
```

```
bandit2@bandit:~$ cat spaces\ in\ this\ filename
```

```
UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK
```

Bandit Level 3 → Level 4

Level Goal

The password for the next level is stored in a hidden file in the inhere directory.

Commands you may need to solve this level

ls, cd, cat, file, du, find

```
bandit3@bandit:~$ ls inhere/

bandit3@bandit:~$ ls -al inhere/

total 12

drwxr-xr-x 2 root    root    4096 Oct 16 14:00 .

drwxr-xr-x 3 root    root    4096 Oct 16 14:00 ..

-rw-r----- 1 bandit4 bandit3   33 Oct 16 14:00 .hidden


bandit3@bandit:~$ cat inhere/.hidden

pIwrPrtPN36QITSp3EQaw936yaFoFgAB
```

Bandit Level 4 → Level 5

Level Goal

The password for the next level is stored in the only human-readable file in the inhere directory. Tip: if your terminal is messed up, try the “reset” command.

Commands you may need to solve this level

ls, cd, cat, file, du, find

```
bandit4@bandit:~$ ls -Ral

./inhere:

total 48

drwxr-xr-x 2 root    root    4096 Oct 16 14:00 .

drwxr-xr-x 3 root    root    4096 Oct 16 14:00 ..

-rw-r----- 1 bandit5 bandit4   33 Oct 16 14:00 -file00

-rw-r----- 1 bandit5 bandit4   33 Oct 16 14:00 -file01

-rw-r----- 1 bandit5 bandit4   33 Oct 16 14:00 -file02

-rw-r----- 1 bandit5 bandit4   33 Oct 16 14:00 -file03

-rw-r----- 1 bandit5 bandit4   33 Oct 16 14:00 -file04

-rw-r----- 1 bandit5 bandit4   33 Oct 16 14:00 -file05

-rw-r----- 1 bandit5 bandit4   33 Oct 16 14:00 -file06
```

```
-rw-r----- 1 bandit5 bandit4   33 Oct 16 14:00 -file07

-rw-r----- 1 bandit5 bandit4   33 Oct 16 14:00 -file08

-rw-r----- 1 bandit5 bandit4   33 Oct 16 14:00 -file09
```

```
bandit4@bandit:~$ strings inhere/-file*

w$N?c

ZP*E

koReBOKuIDDepwhWk7jZC0RTdopnAYKh
```

Bandit Level 5 → Level 6

Level Goal

The password for the next level is stored in a file somewhere under the inhere directory and has all of the following properties:

- **human-readable**
- **1033 bytes in size**
- **not executable**

Commands you may need to solve this level

ls, cd, cat, file, du, find

```
find . -type f -size 1033c ! -executable -exec file {} + | grep ASCII
```

```
cat inhere/maybehere07/.file2
```

```
DXjZPULLxYr17uwoI01bNLQbtFemEgo7
```

Bandit Level 6 → Level 7

Level Goal

The password for the next level is stored somewhere on the server and has all of the following properties:

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

Commands you may need to solve this level

ls, cd, cat, file, du, find, grep

```
NzkIM486T9FUKB811soho09
```

```
bandit6@bandit:~$ find / -type f -user bandit7 -group bandit6 -size 33c ! -executable -exec file {} + | grep ASCII
```

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

HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs
```

Bandit Level 7 → Level 8

Level Goal

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

Commands you may need to solve this level

grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd

```
grep -Rni "millionth"

data.txt:96950:millionth	cvX2JJa4CFALtqS87jk27qwqGhBM9plV
```

Bandit Level 8 → Level 9

Level Goal

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

Commands you may need to solve this level

grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd

```
sort data.txt | uniq -u
```

```
UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR
```

Bandit Level 9 → Level 10

Level Goal

The password for the next level is stored in the file data.txt in one of the few human-readable strings, preceded by several ‘=’ characters.

Commands you may need to solve this level

grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd

```
strings data.txt |grep "==.*"
```

```
2========== the
```

```
========== password
```

```
========== isa
```

========== truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk

Bandit Level 10 → Level 11

Level Goal

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

Commands you may need to solve this level

grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd

base64 -d data.txt

The password is IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR

Bandit Level 11 → Level 12

Level Goal

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

Commands you may need to solve this level

grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd

```
tr '[A-Za-z]' '[N-ZA-Mn-za-m]' < data.txt
```

```
5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu
```

Bandit Level 12 → Level 13

Level Goal

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 may be useful to create a directory under /tmp in which you can work using mkdir. For example: mkdir /tmp/myname123. Then copy the datafile using cp, and rename it using mv (read the manpages!)

Commands you may need to solve this level

grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd, mkdir, cp, mv, file

```
mkdir /tmp/AGS_11_12
```

```
cp data.txt /tmp/AGS_11_12/data.txt
```

```
cd /tmp/AGS_11_12
```

```
xxd -r data.txt data.out
```

```
file data.out
```

```
mv data.out data.gz
gzip -d data.gz

file data
bzip2 -d data

file data.out
mv data.out data.gz
gzip -d data.gz

file data
tar -xf data

file data5.bin
tar -xf data5.bin

file data6.bin
bzip2 -d data6.bin

file data6.bin.out
tar -xf data6.bin.out
```

file data8.bin

mv data8.bin data8.gz

gzip -d data8.gz

cat data8

8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL

Bandit Level 13 → Level 14

Level Goal

The password for the next level is stored in /etc/bandit_pass/bandit14 and can only be read by user bandit14. For this level, you don't get the next password, but you get a private SSH key that can be used to log into the next level. Note: localhost is a hostname that refers to the machine you are working on

Commands you may need to solve this level

ssh, telnet, nc, openssl, s_client, nmap

ssh bandit14@localhost -i sshkey.private

cat /etc/bandit_pass/bandit14

4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e

Bandit Level 14 → Level 15

Level Goal

The password for the next level can be retrieved by submitting the password of the current level to port 30000 on localhost.

Commands you may need to solve this level

ssh, telnet, nc, openssl, s_client, nmap

```
echo "4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e" |nc 127.0.0.1 30000
```

```
Correct!
```

```
BfMYroe26WYalil77FoDi9qh59eK5xNr
```

Bandit Level 15 → Level 16

Level Goal

The password for the next level can be retrieved by submitting the password of the current level to port 30001 on localhost using SSL encryption.

Helpful note: Getting “HEARTBEATING” and “Read R BLOCK”? Use -ign_eof and read the “CONNECTED COMMANDS” section in the manpage. Next to ‘R’ and ‘Q’, the ‘B’ command also works in this version of that command…

Commands you may need to solve this level

ssh, telnet, nc, openssl, s_client, nmap

```
openssl s_client -connect 127.0.0.1:30001
```

[Input the password of the current lvl]

```
cluFn7wTiGryunymYOu4RcffSxQluehd
```

Bandit Level 16 → Level 17

Level Goal

The credentials for the next level can be retrieved by submitting the password of the current level to a port on localhost in the range 31000 to 32000. First find out which of these ports have a server listening on them. Then find out which of those speak SSL and which don't. There is only 1 server that will give the next credentials, the others will simply send back to you whatever you send to it.

Commands you may need to solve this level

ssh, telnet, nc, openssl, s_client, nmap

```
cat /etc/bandit_pass/bandit16
```

Bandit Level 17 → Level 18

Level Goal

There are 2 files in the homedirectory: passwords.old and passwords.new. The password for the next level is in passwords.new and is the only line that has been changed between passwords.old and passwords.new

NOTE: if you have solved this level and see ‘Byebye!’ when trying to log into bandit18, this is related to the next level, bandit19

Commands you may need to solve this level

cat, grep, ls, diff

```
diff passwords.old passwords.new

42c42

< hlbSBPAWJmL6WFDb06gpTx1pPButblOA

---

> kfBf3eYk5BPBRzwjqutbbfE887SVc5Yd
```

```
Pass: kfBf3eYk5BPBRzwjqutbbfE887SVc5Yd
```

Bandit Level 18 → Level 19

Level Goal

The password for the next level is stored in a file readme in the homedirectory. Unfortunately, someone has modified .bashrc to log you out when you log in with SSH.

Commands you may need to solve this level

ssh, ls, cat

```
ssh -t bandit18@bandit.labs.overthewire.org /bin/sh
```

```
cat readme
```

```
IueksS7Ubh8G3DCwVzrTd8rAVOwq3M5x
```

Bandit Level 19 → Level 20

Level Goal

To gain access to the next level, you should use the setuid binary in the homedirectory. Execute it without arguments to find out how to use it. The password for this level can be found in the usual place (/etc/bandit_pass), after you have used the setuid binary.

```
./bandit20-do cat /etc/bandit_pass/bandit20
```

```
GbKksEFF4yrVs6il55v6gwY5aVje5f0j
```

Bandit Level 20 → Level 21

Level Goal

There is a setuid binary in the homedirectory that does the following: it makes a connection to localhost on the port you specify as a commandline argument. It then reads a line of text from the connection and compares it to the password in the previous level (bandit20). If the password is correct, it will transmit the password for the next level (bandit21).

NOTE: Try connecting to your own network daemon to see if it works as you think

Commands you may need to solve this level

ssh, nc, cat, bash, screen, tmux, Unix 'job control' (bg, fg, jobs, &, CTRL-Z, …)

```
# Start server on port 31555

echo "GbKksEFF4yrVs6il55v6gwY5aVje5f0j" |nc -lvp 31555&



# Run the SU program

./suconnect 31555

connect to [127.0.0.1] from localhost [127.0.0.1] 51966

Read: GbKksEFF4yrVs6il55v6gwY5aVje5f0j

Password matches, sending next password
```

gE269g2h3mw3pwgrj0Ha9Uoqen1c9DGr

Bandit Level 21 → Level 22

Level Goal

A program is running automatically at regular intervals from cron, the time-based job scheduler. Look in /etc/cron.d/ for the configuration and see what command is being executed.

Commands you may need to solve this level

cron, crontab, crontab(5) (use “man 5 crontab” to access this)

```
bandit21@bandit:~$ cat /etc/cron.d/*
```

```
@reboot bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
```

```
* * * * * bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
```

Bandit Level 22 → Level 23

Level Goal

A program is running automatically at regular intervals from cron, the time-based job scheduler. Look in /etc/cron.d/ for the configuration and see what command is being executed.

NOTE: Looking at shell scripts written by other people is a very useful skill. The script for this level is intentionally made easy to

read. If you are having problems understanding what it does, try executing it to see the debug information it prints.

Commands you may need to solve this level

cron, crontab, crontab(5) (use “man 5 crontab” to access this)

```
export myname=bandit23
```

```
echo I am user $myname | md5sum | cut -d ' ' -f 1
```

```
8ca319486bfbbc3663ea0fbe81326349
```

```
cat /tmp/8ca319486bfbbc3663ea0fbe81326349
```

```
jc1udXuA1tiHqjIsL8yaapX5XIAI6i0n
```

Bandit Level 23 → Level 24

Level Goal

A program is running automatically at regular intervals from cron, the time-based job scheduler. Look in /etc/cron.d/ for the configuration and see what command is being executed.

NOTE: This level requires you to create your own first shell-script. This is a very big step and you should be proud of yourself when you beat this level!

NOTE 2: Keep in mind that your shell script is removed once executed, so you may want to keep a copy around…

Commands you may need to solve this level

cron, crontab, crontab(5) (use “man 5 crontab” to access this)

```
#!/bin/bash
```

```
cat /etc/bandit_pass/bandit24 > /tmp/unpredictable_name231321
```

Bandit Level 24 → Level 25

Level Goal

A daemon is listening on port 30002 and will give you the password for bandit25 if given the password for bandit24 and a secret numeric 4-digit pincode. There is no way to retrieve the pincode except by going through all of the 10000 combinations, called brute-forcing.

```
#coding: utf-8
```

```
import socket
```

```
pin=0
```

```
passwd='UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ '
```

```
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
```

```
s.connect(('localhost', 30002))
```

```
s.recv(1024)

while True:

  print 'pin: ' + str(pin)

  s.sendall(passwd + str(pin) + '\n')

  data = s.recv(1024)

  if "Correct!" in data:

    print data

  else:

    print "No"

  pin += 1


cat > /tmp/notpossible_named_231414.py

chmod +x /tmp/notpossible_named_231414.py



python /tmp/notpossible_named_231414.py > /tmp/result_3132
```

pass: uNG9O58gUE7snukf3bvZ0rxhtnjzSGzG

Bandit Level 25 → Level 26

Level Goal

Logging in to bandit26 from bandit25 should be fairly easy… The shell for user bandit26 is not /bin/bash, but something else. Find out what it is, how it works and how to break out of it.

Commands you may need to solve this level

ssh, cat, more, vi, ls, id, pwd

ssh bandit26@localhost -i bandit26.sshkey

=> Log out immedialtly

cat /etc/passwd|grep bandit26

bandit26:x:11026:11026:bandit level 26:/home/bandit26:/usr/bin/showtext

cat /usr/bin/showtext

#!/bin/sh

export TERM=linux

more ~/text.txt

exit 0

1- run vim (type: v)

2- edit the file that contain the passwd

(type: e /etc/bandit_pass/bandit26)

5czgV9L3Xx8JPOyRbXh6lQbmIOWvPT6Z

Bandit Level 26 → Level 27

Level Goal

Good job getting a shell! Now hurry and grab the password for bandit27!

Commands you may need to solve this level

ls

v

:set shell=/bin/bash

:shell

./bandit27-do cat /etc/bandit_pass/bandit27

3ba3118a22e93127a4ed485be72ef5ea

Bandit Level 27 → Level 28

Level Goal

There is a git repository at ssh://bandit27-git@localhost/home/bandit27-git/repo. The password for the user bandit27-git is the same as for the user bandit27.

Clone the repository and find the password for the next level.

Commands you may need to solve this level

git

mkdir /tmp/lvl27

cd /tmp/lvl27

git clone ssh://bandit27-git@localhost/home/bandit27-git/repo

cat repo/README

The password to the next level is: 0ef186ac70e04ea33b4c1853d2526fa2

Bandit Level 28 → Level 29

Level Goal

There is a git repository at ssh://bandit28-git@localhost/home/bandit28-git/repo. The password for the user bandit28-git is the same as for the user bandit28.

Clone the repository and find the password for the next level.

Commands you may need to solve this level

git

mkdir /tmp/lvl28

git clone ssh://bandit28-git@localhost/home/bandit28-git/repo

cat repo/README.md

Bandit Notes

Some notes for level29 of bandit.

credentials

- username: bandit29

- password: xxxxxxxxxx

git log -p README.md

bbc96594b4e001778eee9975372716b2

Bandit Level 29 → Level 30

Level Goal

There is a git repository at ssh://bandit29-git@localhost/home/bandit29-git/repo. The password for the user bandit29-git is the same as for the user bandit29.

Clone the repository and find the password for the next level.

Commands you may need to solve this level

git

```
mkdir -p /tmp/AGS_Solv/lvl29

cd /tmp/AGS_Solv/lvl29

git clone ssh://bandit29-git@localhost/home/bandit29-git/repo
```

```
cat repo/README.md

# Bandit Notes

Some notes for bandit30 of bandit.


## credentials


- username: bandit30

- password: <no passwords in production!>
```

Bandit Level 30 → Level 31

Level Goal

There is a git repository at ssh://bandit30-git@localhost/home/bandit30-git/repo. The

password for the user bandit30-git is the same as for the user bandit30.

Clone the repository and find the password for the next level.

Commands you may need to solve this level

git

mkdir -p /tmp/AGS_Solv_lvl30

cd /tmp/AGS_Solv_lvl30

git clone ssh://bandit30-git@localhost/home/bandit30-git/repo

cat repo/README.md

=> Nothing

cat packed-refs

 # pack-refs with: peeled fully-peeled

3aa4c239f729b07deb99a52f125893e162daac9e refs/remotes/origin/master

f17132340e8ee6c159e0a4a6bc6f80e1da3b1aea refs/tags/secret

=> Means that something isn't tracked anymore

git show f17132340e8ee6c159e0a4a6bc6f80e1da3b1aea

47e603bb428404d265f59c42920d81e5

Booom a password !

Bandit Level 31 → Level 32

Level Goal

There is a git repository at ssh://bandit31-git@localhost/home/bandit31-git/repo. The password for the user bandit31-git is the same as for the user bandit31.

Clone the repository and find the password for the next level.

Commands you may need to solve this level

git

```
mkdir -p /tmp/AGS_Solv_lvl31
```

```
cd /tmp/AGS_Solv_lvl31
```

```
git clone ssh://bandit31-git@localhost/home/bandit31-git/repo
```

```
cat README.md
```

This time your task is to push a file to the remote repository.

Details:

File name: key.txt

Content: 'May I come in?'

Branch: master

```
git branch

* master

echo "May I come in?" > key.txt

git add key.txt

git add -f key.txt

git commit -m "Updated"

git push
```

Bandit Level 32 → Level 33

After all this git stuff its time for another escape. Good luck!

Commands you may need to solve this level

sh, man

We can try and invoke a command that doesn't involve letters. Let's try and invoke bash by typing in $0

cat /etc/bandit_pass/bandit33

c9c3199ddf4121b10cf581a98d51caee

Bandit Level 33 → Level 34

At this moment, level 34 does not exist yet.