Bandit Writeup

Glenn Fitzpatrick

What is Bandit?

Challenges

Bandit 0

Prompt: Login to bandit0 using the following credentials

Knowns

- Username: bandit0
- Password: bandit0
- Login: bandit.labs.overthewire.org
- Port: 2220

Solution

```
$ sshpass -f bandit0.pass ssh bandit.labs.overthewire.org -l bandit0 -p 2220
```

QED

Bandit 0 –> 1

Prompt: The password for bandit1 is in a file called readme

Knowns

- Filename: readme
- Location: Home Directory

Solution

```
$ cat readme
```

QED

Bandit 1 –> 2

Prompt: The password for bandit2 is in a file called "-"

Knowns

- Filename: "-"
- Location: Home Directory

Solution

```
$ cat ./-
```

QED

Bandit 2 –> 3

Prompt: The password for bandit3 is in a file called "spaces in this filename"

Knowns

- Filename: "spaces in this filename"
- Location: Home Directory

Solution

```
$ cat "spaces in this filename"
```

QED

Bandit 3 –> 4

Prompt: The password for bandit4 is in a hidden file in the “inhere” directory

Knowns

- File: Hidden file (Begins with .)
- Location: inhere

Solution

```
$ cd inhere
inhere $ ls -a
** There is a dot-file called .hidden **
inhere $ cat .hidden
```

QED

Bandit 4 –> 5

Prompt: The password for bandit5 is in the only human readable file in the “inhere” directory

Knowns

- Location: inhere
- Type: Human Readable

Solution

```
$ file inhere/*
** Only file07 is ASCII text **
$ cat inhere/-file07
```

QED

Bandit 5 –> 6

Prompt: The password for bandit6 is somewhere in the inhere directory and has some given charcteristics

Knowns

- Location: inhere
- Human-readable
- 1033 bytes in size
- not executable

Solution

```
$ find inhere/ -size 1033c
** There is only one file **
** Lucky guess because unlikely two files are exactly the same size **
$ cat inhere/maybehere07/.file2
```

QED

Bandit 6 –> 7

Prompt: The password for bandit7 is somewhere on the server and has the given characteristics

Knowns

- Owner User: bandit7
- Owner Group: bandit6
- Size: 33 bytes

Solution

```
$ find / -user bandit7 -group bandit6 -size 33c 2>/dev/null
** There is one file **
$ cat /var/lib/dpkg/info/bandit7.password
```

QED

Bandit 7 –> 8

Prompt: The password for bandit8 is in data.txt next to the word millionth

Knowns

- Filename: data.txt
- Location: next to "millionth"

Solution

```
$ cat data.txt | grep "millionth"
```

QED

Bandit 8 –> 9

Prompt: The password for bandit9 is in data.txt and is the only line that occurs once

Knowns

- Filename: data.txt
- Password only occurs once

Solution

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

QED

Bandit 9 –> 10

Prompt: The password for bandit10 is stored in data.txt and is one of the few human readable strings led by several "=" characters

Knowns

- Filename: data.txt
- Human readable part
- Led by many "=" characters

Solution

```
$ cat data.txt | strings | grep "==="
** It is the 4th line down **
```

QED

Bandit 10 –> 11

Prompt: The password for bandit11 is in data.txt which contains base64 encoded data

Knowns

- Filename: data.txt
- Encoding: base64

Solution

```
$ cat data.txt | base64 -d
```

QED

Bandit 11 –> 12

Prompt: The passsword for bandit12 is in data.txt which has been rotated by 13 letter positions

Knowns

- Filename: data.txt
- Encoding: Rot13

Solution

```
$ cat data.txt | tr [N-ZA-Mn-za-m] [A-Za-z]
```

QED

Bandit 12 –> 13

Prompt: The password for bandit13 is in data.txt which is a hexdump of a repeatedly compressed file

Knowns

- Filename: data.txt
- Encoding: hexdump and multiple compressions

Solution

```
$ mkdir /tmp/RandomName && cd /tmp/RandomName
/tmp/RandomName $ cp ~/data.txt .
/tmp/RandomName $ xxd -r data.txt > newData
/tmp/RandomName $ file newData
** It is gzip compressed **
/tmp/RandomName $ mv newData newData.gz && gunzip newData.gz
/tmp/RandomName $ file newData
** newData is now bzip2 compressed **
/tmp/RandomName $ mv newData newData.bz2 && bzip2 -d newData.bz2
/tmp/RandomName $ file newData
** It is gzip compressed, repeat gzip process **
/tmp/RandomName $ file newData
** newData is now a tar archive **
/tmp/RandomName $ mv newData newData.tar && tar -xvf newData.tar
** Gives out new file called data5.bin **
/tmp/RandomName $ file data5.bin
** It is another tar archive, repeat tar process **
```

```
** Gives out data6.bin **
/tmp/RandomName $ file data6.bin
** It is a bzip2 compressed file, repeat bzip2 processs **
/tmp/RandomName $ file data6.bin
** It is a tar archive, repeat tar process **
** Gives out file data8.bin **
/tmp/RandomName $ file data8.bin
** It is gzip compressed, repeat gzip process **
/tmp/RandomName $ file data8.bin
** It is now ascii text **
/tmp/RandomName $ cat data8.bin
```

QED

Bandit 13 –> 14

Prompt: The password can only be accessed by bandit14. Instead you get a private ssh key to log into bandit 14.

Knowns

- Filetype: ssh private key
- Host: localhost

Solution

```
$ ssh -i sshkey.private bandit14@localhost
** WE ARE NOW LOGGED IN AS BANDIT14 **
$ cat /etc/bandit_pass/bandit14
```

QED

Bandit 14 –> 15

Prompt: The password for bandit15 can be retrieved by submitting bandit14's password to port 30000 on localhost

Knowns

- Data: bandit14's password

Solution

```
$ cat /etc/bandit_pass/bandit14 | nc localhost 30000
```

QED

Bandit 15 –> 16

Prompt: The password for bandit16 can be retrieved by submitting bandit15's password to port 30001 on localhost using ssl encryption

Knowns

- Data: bandit15's password
- Encryption: SSL

Solution

```
$ cat /etc/bandit_pass/bandit15 | openssl s_client -connect localhost:30001 -ign_eof
```

QED

Bandit 16 –> 17

Prompt: The password for bandit17 can be retrieved by submitting bandit16's password to a port on localhost between 31000 and 32000. Only one has a server listening and is speaking ssl.

Knowns

- Port Range: 31000 - 32000
- Encryption: SSL

Solution

```
$ nmap localhost -p31000-32000
** There are 5 ports open, just brute force it **
$ cat /etc/bandit_pass/bandit16 | openssl s_client -connect localhost:<port> -ign_eof
** One of then gives you an RSA key to log in to bandit17 with **
```

QED

Bandit 17 –> 18

Prompt: The password for bandit18 is the only line that has been changed between two files in the home directory

Knowns

- Filenames: passwords.old, passwords.new

Solution

```
$ diff passwords.old passwords.new
```

QED

Bandit 18 –> 19

Prompt: The password for bandit19 is in the home directory, however the bashrc immediately logs you out when you log in

Knowns

- Filename: readme
- Location: home
- Tactics: Must use ssh execution

Solution

```
[Attack Computer] $ sshpass -f <password file> ssh bandit18@bandit.labs.overthewire.org -p 2220 cat readme
```

QED

Bandit 19 –> 20

Prompt: To gain access to bandit20, use the setuid binary in the home directory

Knowns

- SETUID
- Location: home

Solution

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

QED

Bandit 20 –> 21

Prompt: Use the setuid to transmit the password to bandit21

Knowns

- SETUID
  - Makes a connection to a specified port
  - Listens for usr input (bandit20 password)
  - Then transmit bandit21 password
- Location: home

Solution

```
[1] $ nc -lvp 8675
[2] $ ./suconnect 8675
[1] $ ** Paste bandit20 password **
```

QED

Bandit 21 –> 22

Prompt: A program is running from *cron*. Look at /etc/cron.d to figure it out

Knowns

- Cron job
- /etc/cron.d

Solution

```
$ vim /etc/cron.d
** Points to a file **
$ vim /usr/bin/cronjob_bandit22.sh
** Outputs the password to a file **
$ cat <file>
```

QED

Bandit 22 –> 23

Prompt: Look at another cronjob

Knowns

- Cron job
- /etc/cron.d

Solution

```
$ vim /etc/cron.d
** Points to a file **
$ vim /usr/bin/cronjob_bandit23.sh
** It's a script that hashes a phrase then copies the password to a file of that name in /tmp **
$ cat /tmp/<hash>
```

QED

Bandit 23 –> 24

Prompt: A program is running from cron. Look at what is being executed. You will need to write your bash script

Knowns

- Cron job
- /etc/cron.d

Solution

```
$ vim /etc/cron.d
** Points to a file **
$ vim /usr/bin/cronjob_bandit24.sh
** It's a script that runs all files in the /var/spool/bandit24 folder **
$ mkdir /tmp/RandomName
/tmp/RandomName $ vim runFile.sh
/tmp/RandomName $ chmod 777 runFile.sh
/tmp/RandomName $ cp runFile.sh /var/spool/bandit24
** Wait for a minute **
/tmp/RandomName $ cat pass.txt
```

QED

runFile.sh

```
#!/bin/bash

cat /etc/bandit_pass/bandit24 > /tmp/RandomName/pass.txt
```

Bandit 24 –> 25

Prompt: A daemon is listening on port 30002 and will return the password for bandit25 if it is given the password for bandit24 and a secret 4 digit pincode

Knowns

- Port: 30002
- Input: bandit24 password, 4 digit pin

Solution

```
$ mkdir /tmp/RandomName
$ cd /tmp/RandomName
/tmp/RandomName $ for i in {0000..9999};do echo <bandit24_pass> $i >> numFile.txt; done
/tmp/RandomName $ cat numFile.txt | nc localhost 30002
```

QED

Bandit 25 –> 26

Prompt: Log into bandit26 from bandit25. The shell isn't /bin/bash, figure it out

Knowns

- Shell: Not /bin/bash

Solution

```
** Try to log in from bandit25 **
** Open the terminal very small so that more is used **
** Then hit v and enter :r /etc/bandit_pass/bandit26 **
** Then hit space a few times **
```

QED
