

So continuing with Bandit18, for this level it said the file has been edited so I just had to use the diff command to find the difference between two password files and I got the pass for the next level.

```
bandit17@bandit:~$ ls
passwords.new passwords.old
bandit17@bandit:~$ diff passwords.new passwords.old
42c42
< kFBf3eYk5BPBRzwjqtbbfE887SVc5Yd
---
> w0Yfo1rc5bwjS4qw5mq1nnQi6mF03bii
bandit17@bandit:~$ |
```

For this level, I was couldn't log in to bandit18 using ssh, so to get the password for the next level I just used the ssh to display the readme file on bandit18, and got the password for the next without going into bandit18.

```
Byebye !
Connection to bandit.labs.overthewire.org closed.
UZAIF SHAIKH@DESKTOP-RND62QS ~
$ ssh bandit18@bandit.labs.overthewire.org -p 2220 cat readme
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit18@bandit.labs.overthewire.org's password:
Iueks57Ubh8G3DCwVzrTd8rAV0wq3M5x
UZAIF SHAIKH@DESKTOP-RND62QS ~
```

For this level, I had to use the executable file bandit20-do to get the password but the file needed an id as arg so I just cat the /etc/bandit_pass/bandit20 and got the password.

```
bandit19@bandit:~$ ./bandit20-do ls /etc/bandit_pass/bandit
bandit0 bandit11 bandit14 bandit17 bandit2 bandit22 bandit25 bandit28 bandit30 band
bandit1 bandit12 bandit15 bandit18 bandit20 bandit23 bandit26 bandit29 bandit31 band
bandit10 bandit13 bandit16 bandit19 bandit21 bandit24 bandit27 bandit3 bandit32 band
bandit19@bandit:~$ ./bandit20-do ls /etc/bandit_pass/bandit20
/etc/bandit_pass/bandit20
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
GbKksEFF4yrVs6il55v6gwY5aVje5f0j
bandit19@bandit:~$ |
```

For this level, I just had to make localhost connect on a port to listening, as the executable file will only give the password of the next level if it is given the password for the current level, so I used netcat to make the connection and run the suconnect on the port and got the password.

```
bandit20@bandit:~$ nc -lvp 35000
listening on [any] 35000 ...
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 45266
GbKksEFF4yrVs6il55v6gWY5avje5f0j
gE269g2h3mw3pwrj0Ma9Uo9en1c9Dgr
bandit20@bandit:~$ |

bandit20@bandit:~$
* gef (https://github.com/hugsy/gef) in /usr/local/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /usr/local/pwndbg/
* peda (https://github.com/longld/peda.git) in /usr/local/peda/
* gdbinit (https://github.com/gdbinit/gdbinit) in /usr/local/gdbin
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)
* checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/
checksec.sh

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us through IRC on
irc.overthewire.org #wargames.

Enjoy your stay!

bandit20@bandit:~$ ./suconnect 35000
Read: GbKksEFF4yrVs6il55v6gWY5avje5f0j
Password matches, sending next password
bandit20@bandit:~$ |
```

For this level, the hint was to look into `/etc/cron.d` and there was a couple of files so I cat the `cronjob_bandit22` file and it points to a shell script looking at the shell script it shows the password is saved in a file in tmp dir so I just cat the address and got the password for it.

```
bandit21@bandit:~$ ls
bandit21@bandit:~$ cd /etc/cron.d/
bandit21@bandit:/etc/cron.d$ ls
cronjob_bandit15_root cronjob_bandit17_root cronjob_bandit22 cronjob_bandit23 cronjob_bandit24 cronjob_bandit25_root
bandit21@bandit:/etc/cron.d$ ls -l cronjob_bandit22
-rw-r--r-- 1 root root 120 May 7 2020 cronjob_bandit22
bandit21@bandit:/etc/cron.d$ cat cronjob_bandit22
cronjob_bandit22 cronjob_bandit23 cronjob_bandit24 cronjob_bandit25_root
bandit21@bandit:/etc/cron.d$ cat cronjob_bandit22
@reboot bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
* * * * * bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
bandit21@bandit:/etc/cron.d$ cat /usr/bin/cronjob_bandit22.sh
#!/bin/bash
chmod 644 /tmp/t7061ds9S0RqQh9aMcz6ShpAoZKF7fgv
cat /etc/bandit_pass/bandit22 > /tmp/t7061ds9S0RqQh9aMcz6ShpAoZKF7fgv
bandit21@bandit:/etc/cron.d$ ls -l /tmp/t7061ds9S0RqQh9aMcz6ShpAoZKF7fgv
-rw-r--r-- 1 bandit22 root 33 Mar 31 16:56 /tmp/t7061ds9S0RqQh9aMcz6ShpAoZKF7fgv
bandit21@bandit:/etc/cron.d$ ls -l /tmp/t7061ds9S0RqQh9aMcz6ShpAoZKF7fgv
-rw-r--r-- 1 bandit22 root 33 Mar 31 16:57 /tmp/t7061ds9S0RqQh9aMcz6ShpAoZKF7fgv
bandit21@bandit:/etc/cron.d$ cat /tmp/t7061ds9S0RqQh9aMcz6ShpAoZKF7fgv
Yk7owGAcwjwMVRwrTesJEwB7WVOiILLI
bandit21@bandit:/etc/cron.d$ |
```

For this level, I followed the same path as the previous level and time the shell script used a `md5sum` to generate the name of the file so I just followed what was there in the script but replace the `bandit22` with `bandit23` and got the password for the level 23.

```

bandit22@bandit: /etc/cron.d
bandit22@bandit:~$ cd /etc/cron.d
cron.d/      cron.daily/
bandit22@bandit:~$ cd /etc/cron.d
bandit22@bandit:/etc/cron.d$ ls
cronjob_bandit15_root cronjob_bandit17_root cronjob_bandit22 cronjob_bandit23 cronjob_bandit24 cronjob_bandit25_root
bandit22@bandit:/etc/cron.d$ cat cronjob_bandit23
@reboot bandit23 /usr/bin/cronjob_bandit23.sh &> /dev/null
* * * * * bandit23 /usr/bin/cronjob_bandit23.sh &> /dev/null
bandit22@bandit:/etc/cron.d$ cat /usr/bin/cronjob_bandit23.sh
#!/bin/bash

myname=$(whoami)
mytarget=$(echo I am user $myname | md5sum | cut -d ' ' -f 1)

echo "Copying passwordfile /etc/bandit_pass/$myname to /tmp/$mytarget"

cat /etc/bandit_pass/$myname > /tmp/$mytarget
bandit22@bandit:/etc/cron.d$ echo I am user $bandit23 | md5sum | cut -d ' ' -f 1
7db97df393f40ad1691b6e1fb03d53eb
bandit22@bandit:/etc/cron.d$ /tmp/7db97df393f40ad1691b6e1fb03d53eb
-bash: /tmp/7db97df393f40ad1691b6e1fb03d53eb: Permission denied
bandit22@bandit:/etc/cron.d$ echo I am user bandit23 | md5sum | cut -d ' ' -f 1
8ca319486bfbbc3663ea0fbe81326349
bandit22@bandit:/etc/cron.d$ /tmp/8ca319486bfbbc3663ea0fbe81326349
-bash: /tmp/8ca319486bfbbc3663ea0fbe81326349: Permission denied
bandit22@bandit:/etc/cron.d$ cat /tmp/8ca319486bfbbc3663ea0fbe81326349
jc1udXuA1tiHqjIsl8yaapX5XIAI6i0n
bandit22@bandit:/etc/cron.d$ |

```

It took me a while to get the password for the next level, I looked at the script for bandit24 in dir /etc/cron.d at it goes to cd /var/spool/bandit24 and when it is executed it has the permission of bandit24 so I had to write a bash script which will copy the pass for bandit24, and after writing the script I got the password for bandit24.

```

bandit23@bandit: /var/spool/bandit24
1 #!/bin/bash
2
3 cat /etc/bandit_pass/bandit24 > /tmp/haha1/pass.txt|
4
5
6
7
8
9
10
11
~
~
~
~
~
~

```

```

bandit23@bandit: /var/spool/bandit24
bandit23@bandit:/var/spool/bandit24$ mkdir /tmp/haha1
bandit23@bandit:/var/spool/bandit24$ chmod 777 /tmp/haha1
bandit23@bandit:/var/spool/bandit24$ vi pass.sh
bandit23@bandit:/var/spool/bandit24$ chmod +x pass.sh
bandit23@bandit:/var/spool/bandit24$ ls
ls: cannot open directory '.': Permission denied
bandit23@bandit:/var/spool/bandit24$ ls -l pass.sh
-rwxr-xr-x 1 bandit23 bandit23 65 Mar 31 17:38 pass.sh
bandit23@bandit:/var/spool/bandit24$ data
-bash: data: command not found
bandit23@bandit:/var/spool/bandit24$ ls /tmp/haha1
pass.txt
bandit23@bandit:/var/spool/bandit24$ cat /tmp/haha1/pass.txt
UoMYTrfrBFHyQXmg6gzctqAw0mw1IohZ
bandit23@bandit:/var/spool/bandit24$ |

```

This level, was really fun, for this I had to guess the 4 digit pin with the password of the previous level so for this, I wrote a bash script that connects to port 30002 and sends the password and the pin in a loop from 0000 to 9999 and after running the script I got the pass for next level.

```

GNU nano 2.7.4
#!/bin/bash
for i in {0000..9999}
do
    echo "UoMYTrfrBFHyQXmg6gzctqAw0mw1IohZ $i" | nc localhost 30002
done

```

```

Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Correct!
The password of user bandit25 is uNG9058gUE7snukf3bvZ0rxhtnjzSGzG
Exiting.

```

[illegible]

For this level, I just used the executable in the home for the id I used the password for bandit27, there was a level similar to this.

1000

This level was pretty easy for me, cause I have done COMP1531 so I am familiar with git commands, I just had to git clone a repo and inside the repo, I got the password in the readme file.

```
bandit27@bandit: /tmp/make/repo
bandit27@bandit:/tmp/make$ git clone ssh://bandit27-git@localhost/home/bandit27-git/repo
Cloning into 'repo'...
Could not create directory '/home/bandit27/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZWr85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit27/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit27-git@localhost's password:
remote: Counting objects: 3, done.
remote: Compressing objects: 100% (2/2), done.
remote: Total 3 (delta 0), reused 0 (delta 0)
Receiving objects: 100% (3/3), done.
bandit27@bandit:/tmp/make$ ls
repo
bandit27@bandit:/tmp/make$ cd repo/
bandit27@bandit:/tmp/make/repo$ ls
README
bandit27@bandit:/tmp/make/repo$ cat README
The password to the next level is: 0ef186ac70e04ea33b4c1853d2526fa2
bandit27@bandit:/tmp/make/repo$ |
```

For this level, I just had to check the log history for the repo, and checkout to the last commit and found the password there.

```
add missing data
commit de2ebe2d5fd1598cd547f4d56247e053be3fdc38
Author: Ben Dover <noone@overthewire.org>
Date: Thu May 7 20:14:49 2020 +0200

    initial commit of README.md
bandit28@bandit:/tmp/haha/repo$ git checkout c086d11a00c0648d095d04c089786efef5e01264
Note: checking out 'c086d11a00c0648d095d04c089786efef5e01264'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by performing another checkout.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -b with the checkout command again. Example:

    git checkout -b <new-branch-name>

HEAD is now at c086d11... add missing data
bandit28@bandit:/tmp/haha/repo$ cat README.md
# Bandit Notes
Some notes for level29 of bandit.

## credentials
- username: bandit29
- password: bbc96594b4e001778eee9975372716b2
bandit28@bandit:/tmp/haha/repo$
```

Even this level was super easy, I checked if there were multiple branches and after switching the branch I got the password in the branch dev.

```
bandit29@bandit: /tmp/liluzi/repo
Could not create directory '/home/bandit29/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0Zwr85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit29/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit29-git@localhost's password:
remote: Counting objects: 16, done.
remote: Compressing objects: 100% (11/11), done.
remote: Total 16 (delta 2), reused 0 (delta 0)
Receiving objects: 100% (16/16), 1.43 KiB | 0 bytes/s, done.
Resolving deltas: 100% (2/2), done.
bandit29@bandit:/tmp/liluzi$ ls
repo
bandit29@bandit:/tmp/liluzi$ cd repo/
bandit29@bandit:/tmp/liluzi/repo$ git branch
* master
bandit29@bandit:/tmp/liluzi/repo$ git branch -r
  origin/HEAD -> origin/master
  origin/dev
  origin/master
  origin/sploits-dev
bandit29@bandit:/tmp/liluzi/repo$ git checkout dev
Branch dev set up to track remote branch dev from origin.
Switched to a new branch 'dev'
bandit29@bandit:/tmp/liluzi/repo$ cat README.md
# Bandit Notes
Some notes for bandit30 of bandit.
```

```
bandit29@bandit:/tmp/liluzi/repo$ git checkout dev
Branch dev set up to track remote branch dev from origin.
Switched to a new branch 'dev'
bandit29@bandit:/tmp/liluzi/repo$ cat README.md
# Bandit Notes
Some notes for bandit30 of bandit.

## credentials

- username: bandit30
- password: 5b90576bedb2cc04c86a9e924ce42faf

bandit29@bandit:/tmp/liluzi/repo$ |
```

For this level, I just had to do a little bit of research on git and found the tag command and in the tag contain secret and using the command show secret gave away the password for the next level.

```
'git help -a' and 'git help -g' list available subcommands and some
concept guides. See 'git help <command>' or 'git help <concept>'
to read about a specific subcommand or concept.
bandit30@bandit:/tmp/lil1/repo$ git tag
secret
bandit30@bandit:/tmp/lil1/repo$ git show secret
47e603bb428404d265f59c42920d81e5
bandit30@bandit:/tmp/lil1/repo$ |
```

For this level, I need to push a file and after doing that I got the password for the next level.

```
bandit31@bandit:/tmp/lil2/repo
bandit31@bandit:/tmp/lil2/repo$ git add -f key.txt
bandit31@bandit:/tmp/lil2/repo$ git commit -m "Added key.txt"
[master 076a956] Added key.txt
1 file changed, 1 insertion(+)
create mode 100644 key.txt
bandit31@bandit:/tmp/lil2/repo$ git push
Could not create directory '/home/bandit31/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0Zwr85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit31/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit31-git@localhost's password:
Counting objects: 3, done.
Delta compression using up to 2 threads.
Compressing objects: 100% (2/2), done.
Writing objects: 100% (3/3), 324 bytes | 0 bytes/s, done.
Total 3 (delta 0), reused 0 (delta 0)
remote: ### Attempting to validate files... ####
remote:
remote: .oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.
remote:
remote: Well done! Here is the password for the next level:
remote: 56a9bf19c63d650ce78e6ec0354ee45e
remote:
remote: .oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.
remote:
To ssh://localhost/home/bandit31-git/repo
! [remote rejected] master -> master (pre-receive hook declined)
error: failed to push some refs to 'ssh://bandit31-git@localhost/home/bandit31-git/repo'
bandit31@bandit:/tmp/lil2/repo$ |
```

For this level, after logging into the ssh I went into the uppercase shell so, for this, I enable the bond shell with the command "\$0" and export the shell as /bin/bash and to get into the shell I used the command \$SHELL and I got able to enter the bandit33.

```
>>
>> $0
$ export SHELL=/bin/bash
$ echo $SHELL
/bin/bash
$ $SHELL
bandit33@bandit:~$ cat /etc/bandit_pass/bandit3
bandit3 bandit30 bandit31 bandit32 bandit33
bandit33@bandit:~$ cat /etc/bandit_pass/bandit33
c9c3199ddf4121b10cf581a98d51caee
bandit33@bandit:~$ |
```


Well, this was the end of the bandit levels it was really fun to do bandit, I learned a lot about some of the Linux commands, and this exercise helped me to understand the basic of shell scripting. And working with Nmap really help me to learn how somebody can exploit an open port.