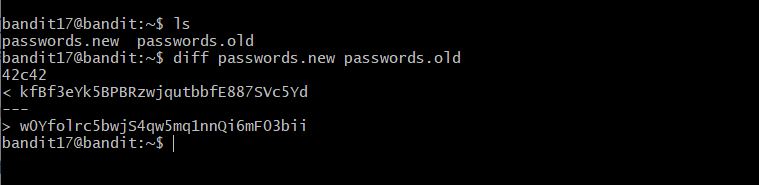
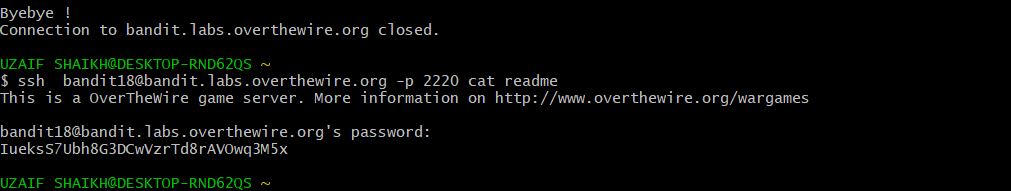
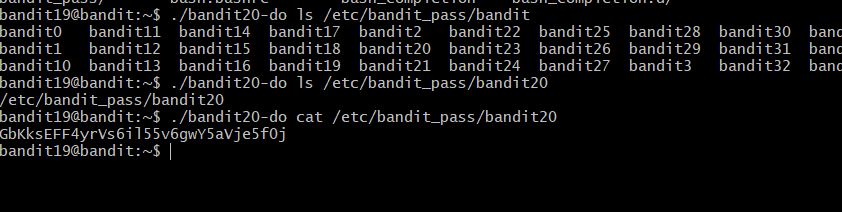
So continuing with Bandit18, for this level it said the file has been edited so I just had to use the diff command to find the difference between two password files and I got the pass for the next level.



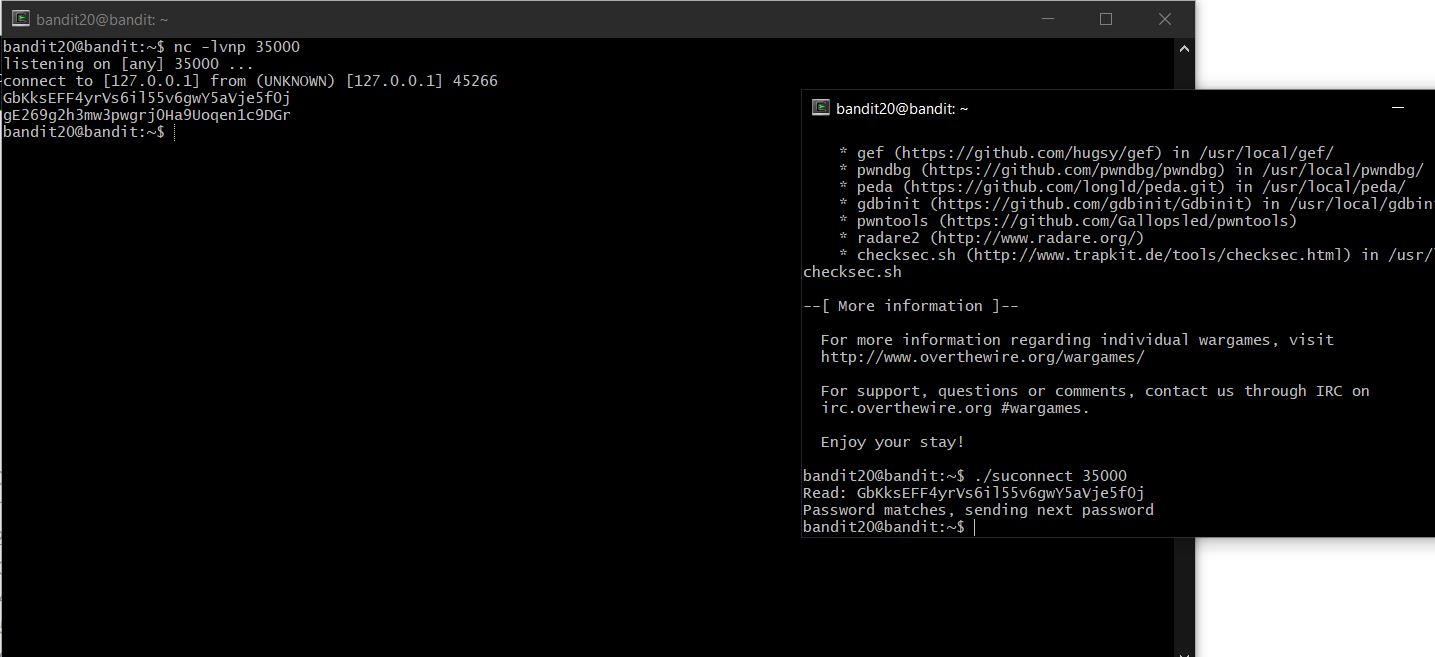
For this level, I was couldn't log in to bandit18 using ssh, so to get the password for the next level I just used the ssh to display the readme file on bandit18, and got the password for the next without going into bandit18.



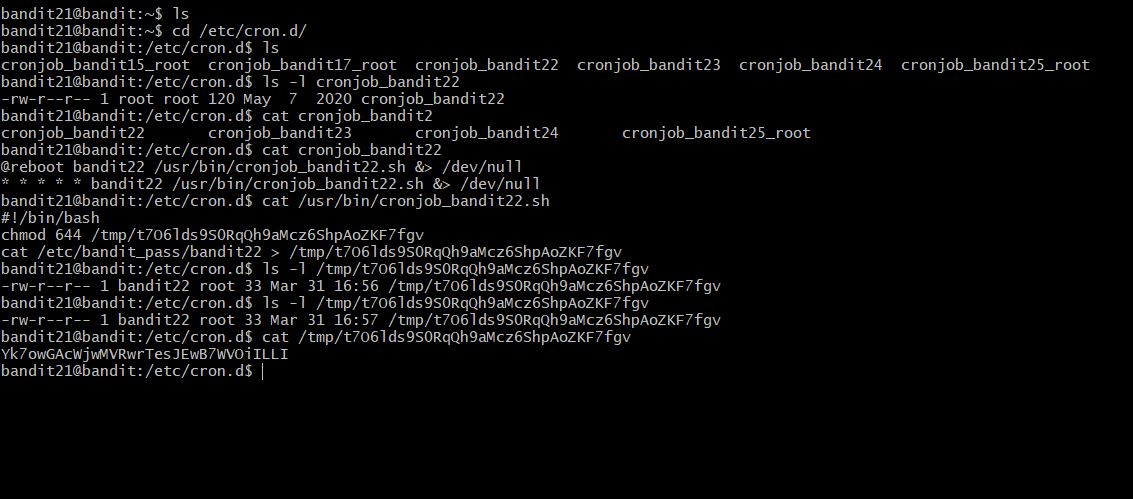
For this level, I had to use the executable file bandit20-do to get the password but the file needed an id as arg so I just cat the /etc/bandit\_pass/bandit20 and got the password.



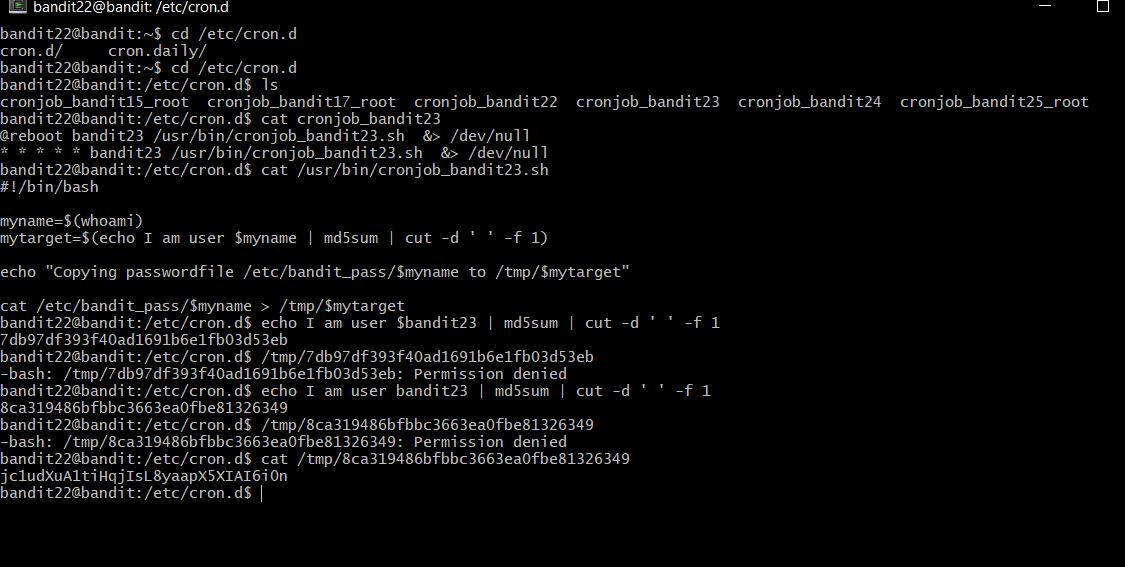
For this level, I just had to make localhost connect on a port to listening, as the executable file will only give the password of the next level if it is given the password for the current level, so I used netcat to make the connection and run the suconnect on the port and got the password.



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.

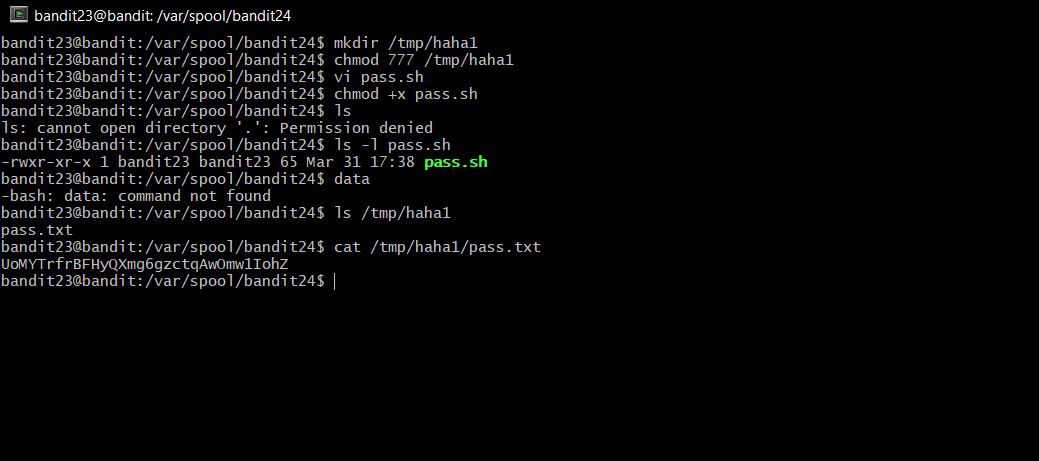


For this level, I followed the same path as the previous level and time the shell script used a md5sum to generate the name of the file so I just followed what was there in the script but replace the bandit22 with bandit23 and got the password for the level 23.

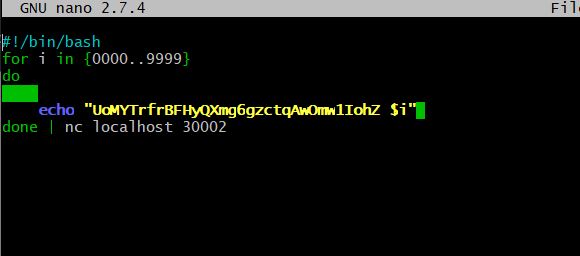


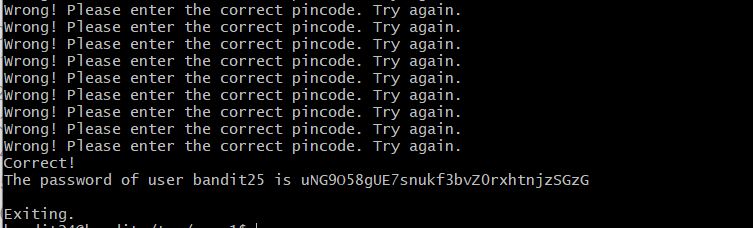
It took me a while to get the password for the next level, I looked at the script for bandit24 in dir /etc/cron.d at it goes to cd /var/spool/bandit24 and when it is executed it has the permission of bandit24 so I had to write a bash script which will copy the pass for bandit24, and after writing the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



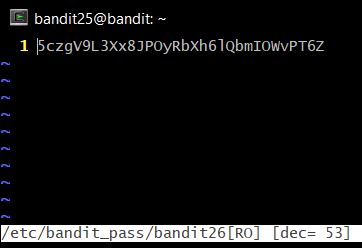


This level, was really fun, for this I had to guess the 4 digit pin with the password of the previous level so for this, I wrote a bash script that connects to port 30002 and sends the password and the pin in a loop from 0000 to 9999 and after running the script I got the pass for next level.



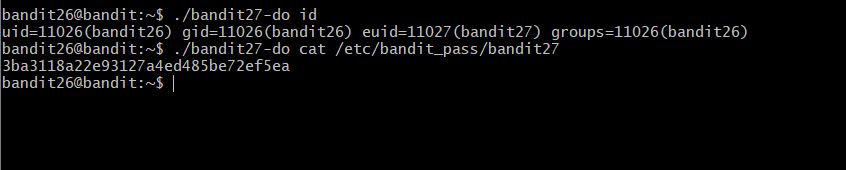


This level was really weird haha, I logged into bandit25 and there was an RSA key for bandit26 but went I tried to connect to it the connection was just closed, so I had to order the shell since it didn't use bin/bash, so I just made the terminal size smaller and the run ssh -i and types "!r /etc/bandit\_pass/bandit26" to get the password in vi and I got it.

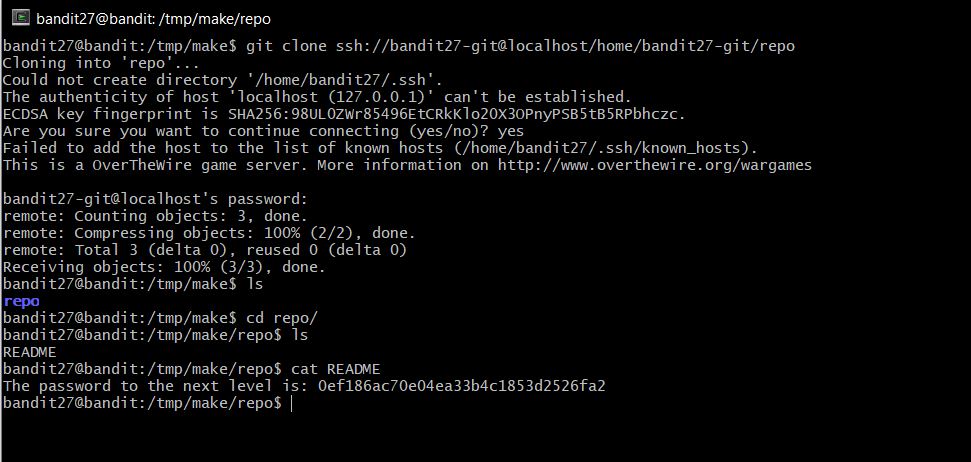


This level was really similar to the last level for this level I just had to do the same thing but instead of reading the password for bandit26 I just set the shell as /bin/bash using the command "!set shell=/bin/bash" after setting the shell I just had to type ":shell" to get the shell and BOOM I was into bandit26.

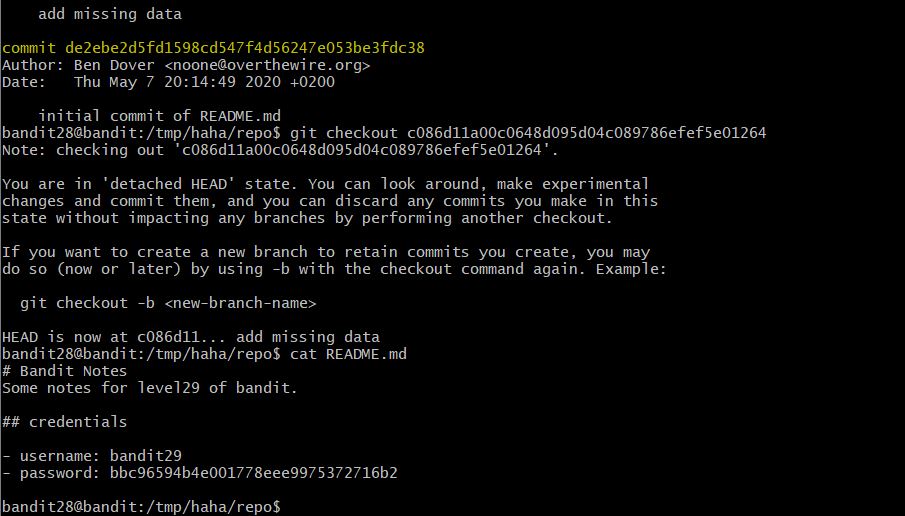
For this level, I just used the executable in the home for the id I used the password for bandit27, there was a level similar to this.



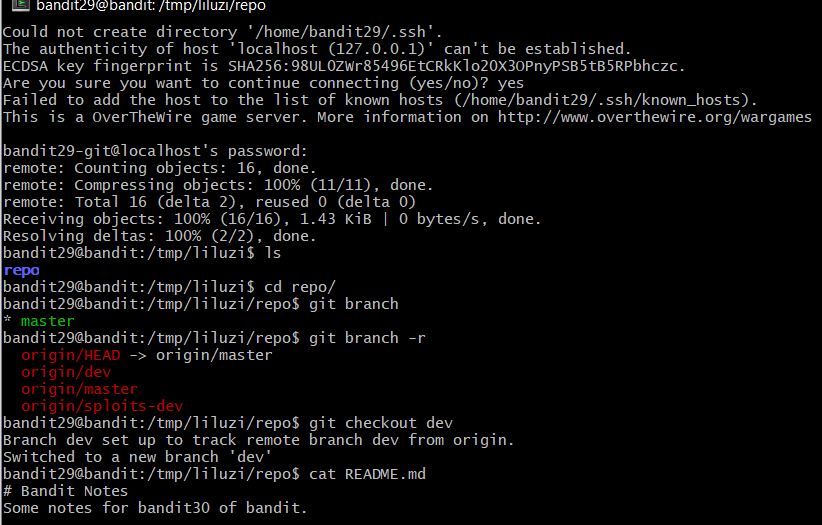
This level was pretty easy for me, cause I have done COMP1531 so I am familiar with git commands, I just had to git clone a repo and inside the repo, I got the password in the readme file.

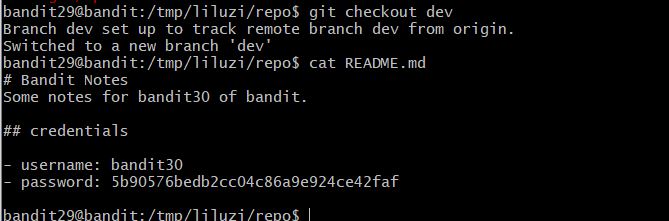


For this level, I just had to check the log history for the repo, and checkout to the last commit and found the password there.

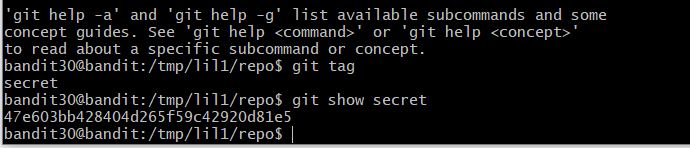


Even this level was super easy, I checked if there were multiple branches and after switching the branch I got the password in the branch dev.

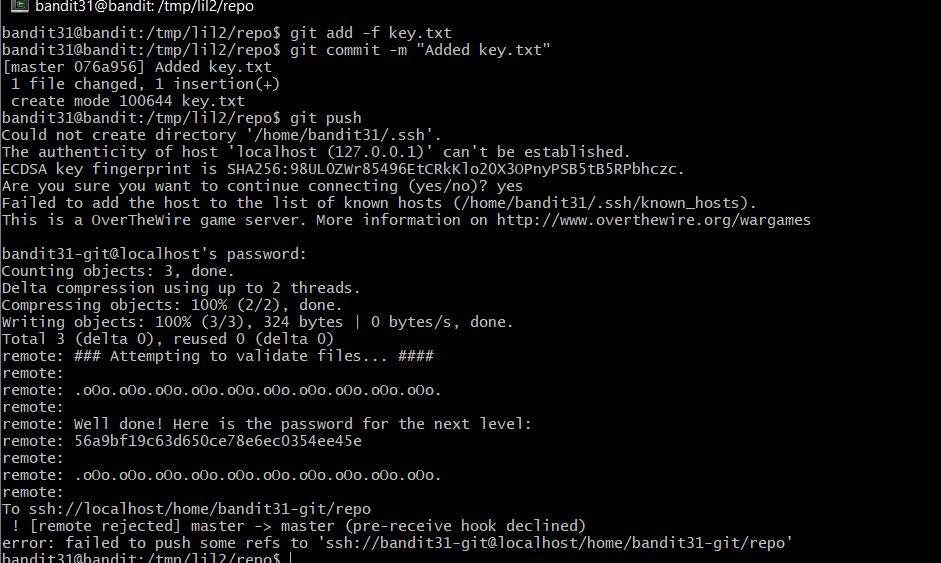




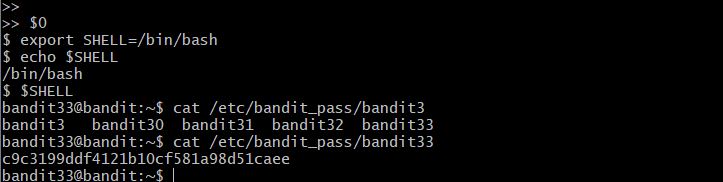
For this level, I just had to do a little bit of research on git and found the tag command and in the tag contain secret and using the command show secret gave away the password for the next level.



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



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.



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.