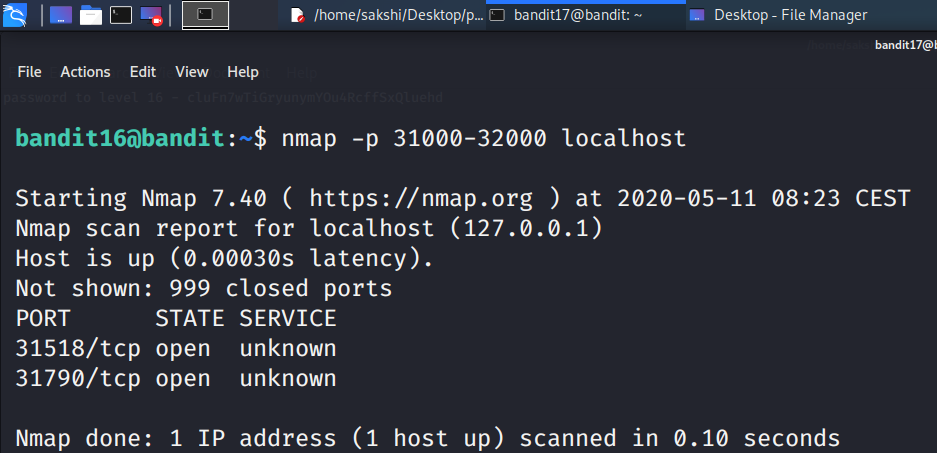
Level 16 -> Level 17

The goal of this level is to submit the password of the current level to **port on localhost in the range 31000 to 32000** and get the password to the next level.

First, we need to find out which of these ports have a server listening on them. We will use **nmap port scan** to find out the listening ports in the range 31000-32000.



Only two ports 31518 and 31790 are open

Then, we need to 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.

We will check at both the ports one by one by connecting to the port using **openssl s\_client command** and by submitting password of current level.

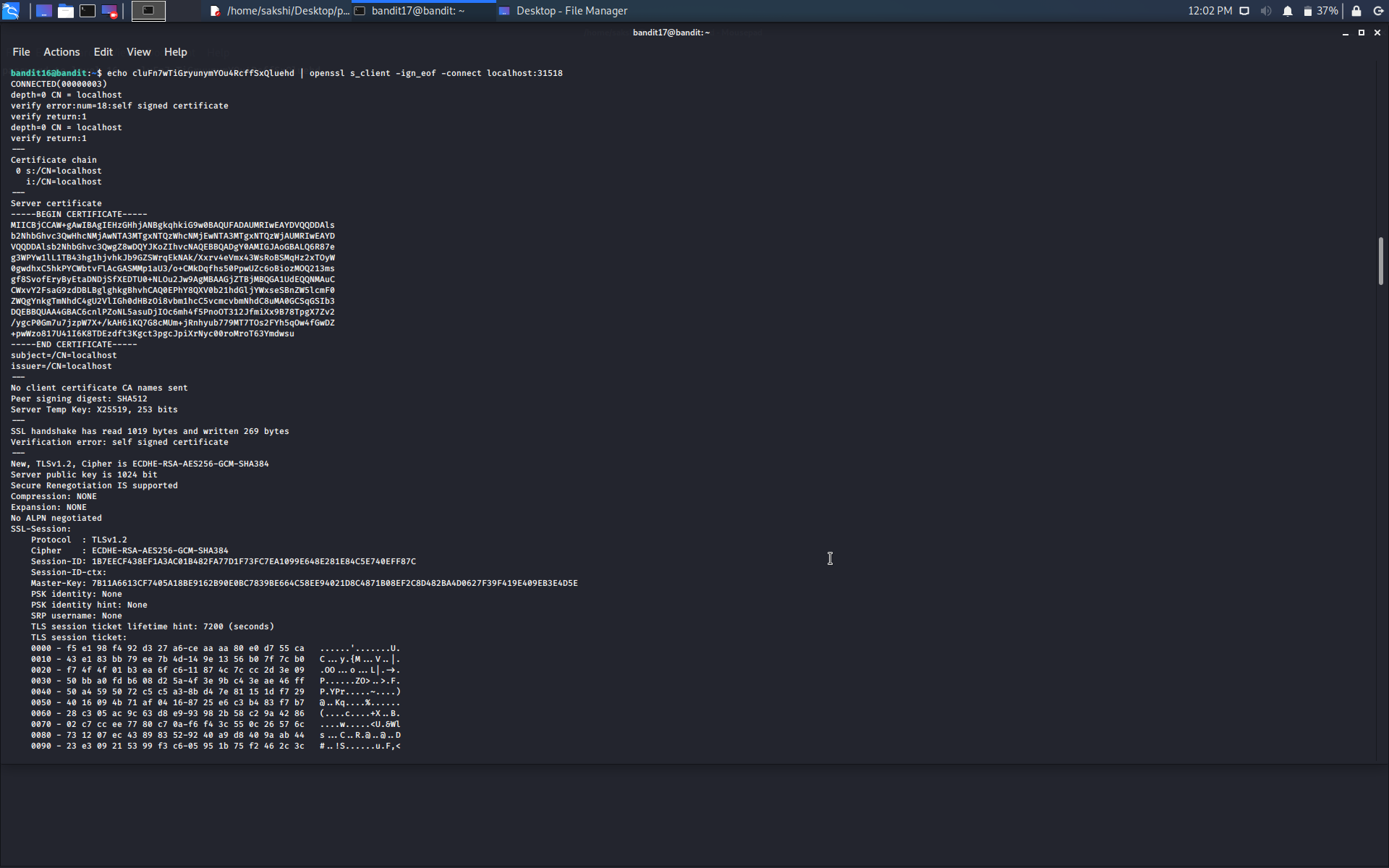
Get the password of the current level by using the command **cat /etc/bandit\_pass/bandit15**

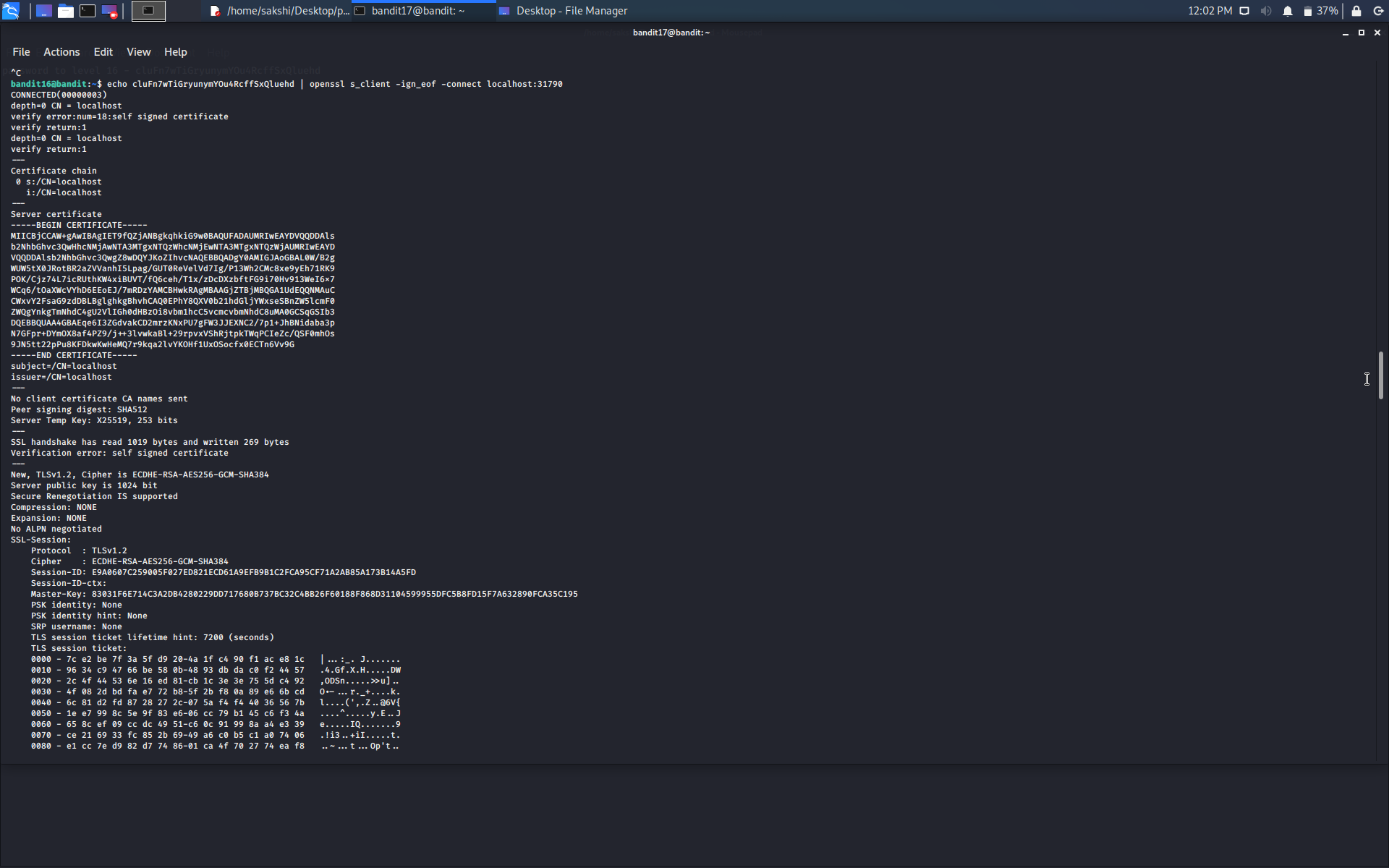
We can use the command as **echo password\_of\_current\_level | openssl s\_client -ign\_eof -connect localhost:31518** to connect to port 31518.

* We are connected to the port 31518 but no password or key is found at this post.
* Using ctrl+c keys we will come out of this and check on the other port i.e. 31790.

We will connect to this by using same command i.e.

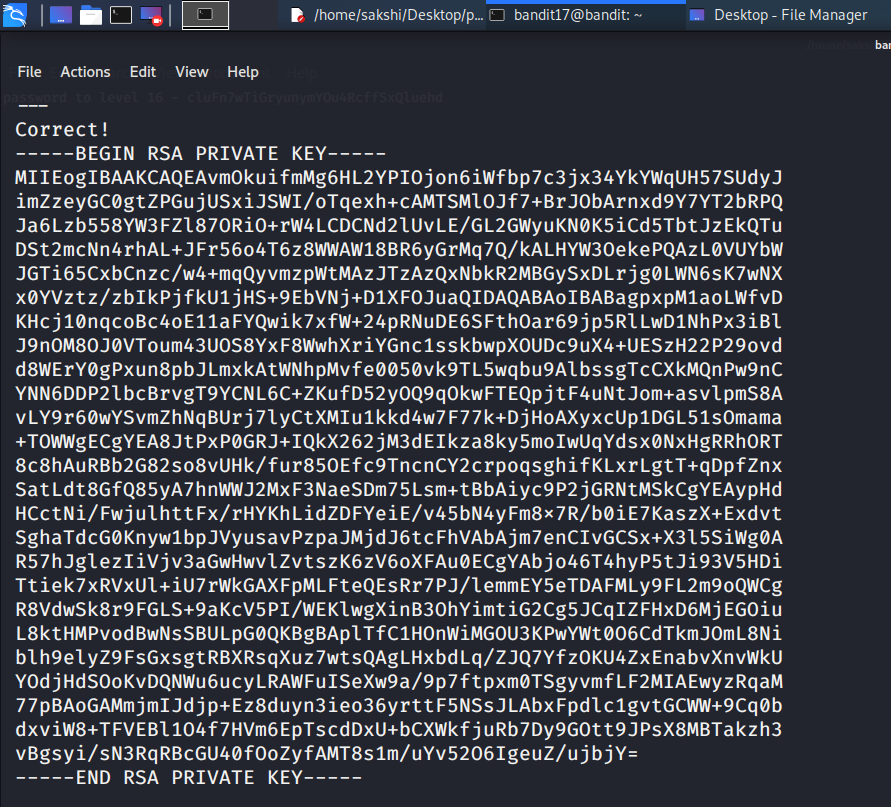
**echo password\_of\_current\_level | openssl s\_client -ign\_eof -connect localhost:31790**





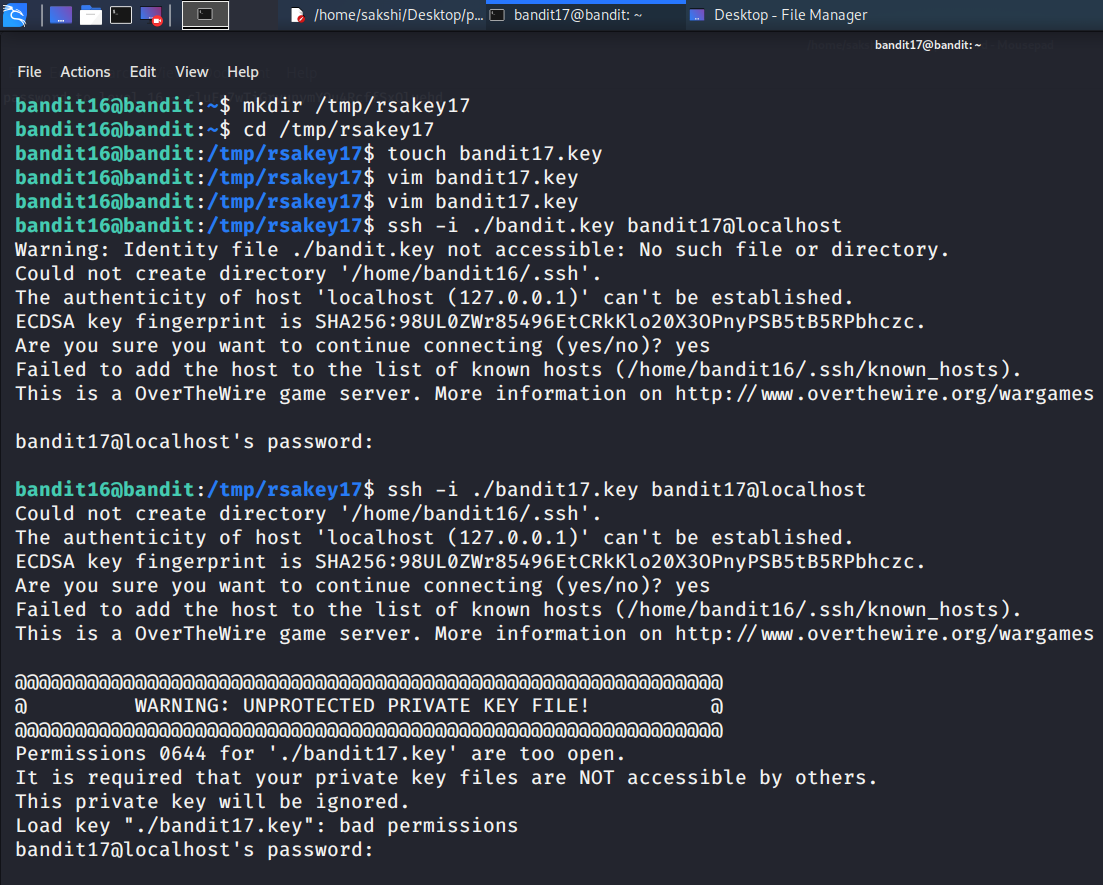
RSA private key is found at this port which will be used by us to connect to the next level.

The key looks like:-

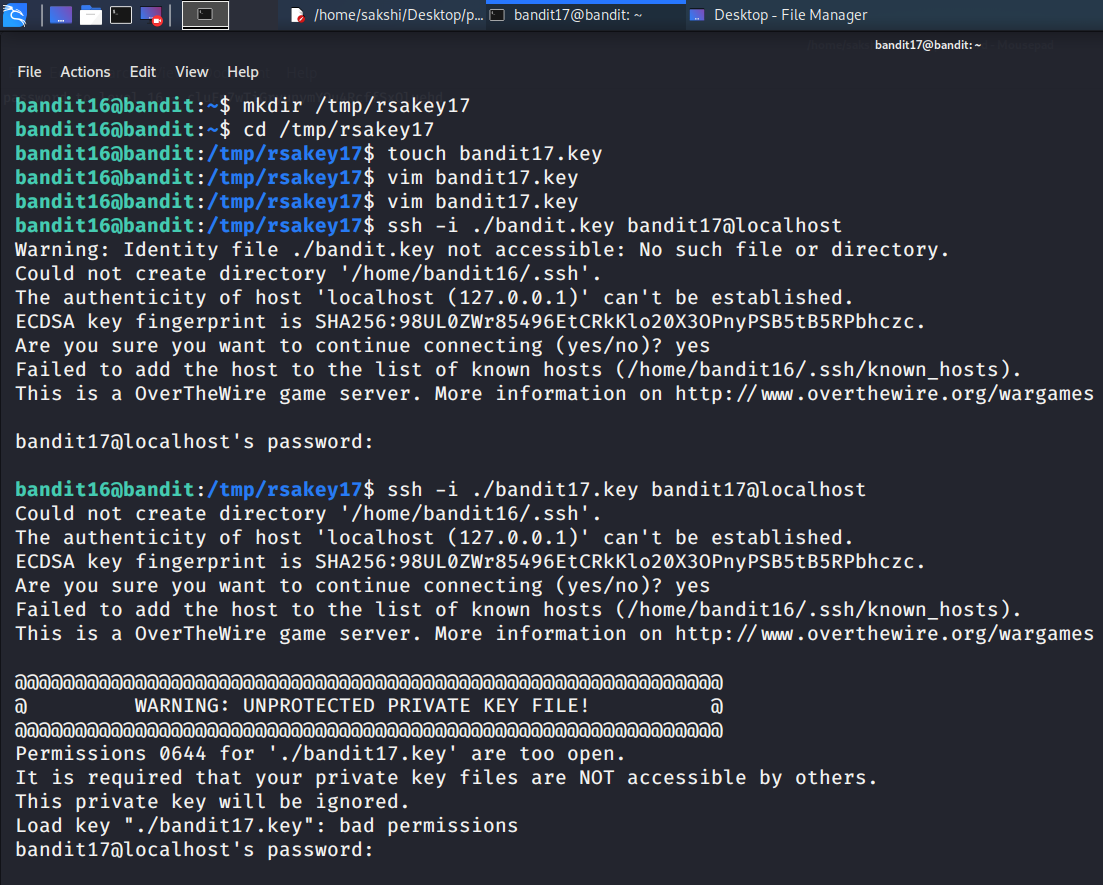


Steps that can be followed now –

* Make a directory in /tmp directory with any name. I made it as **mkdir /tmp/rsakey17.**
* Enter into the newly created directory using **cd command.**
* Make a file using **touch command** with any name. I made it as **touch bandit17.key**.
* Open the newly created file using **vim command.** File will open as a text editor. Press **i** to enable insert mode copy the RAS key and paste in this editor. Press **esc key and then type :wq** to quit the editor.

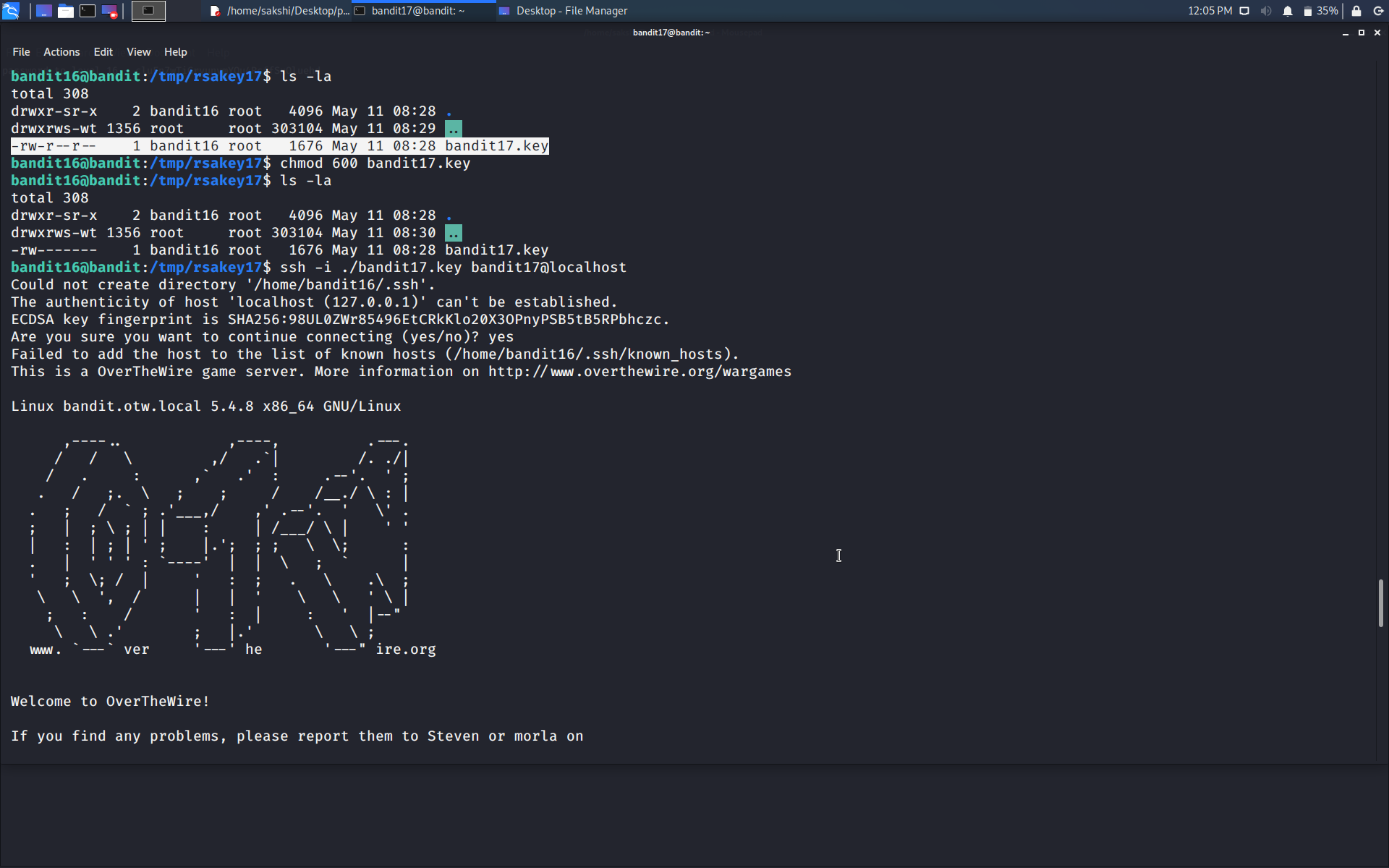


* Use command **ssh -I ./bandit17.key bandit17@localhost** to insert the key and login to the next level.
* OOPS!!!! A warning flashed that the file bandit17.key that we created for saving our rsa key is not protected. It has permission 0644 which are too open.



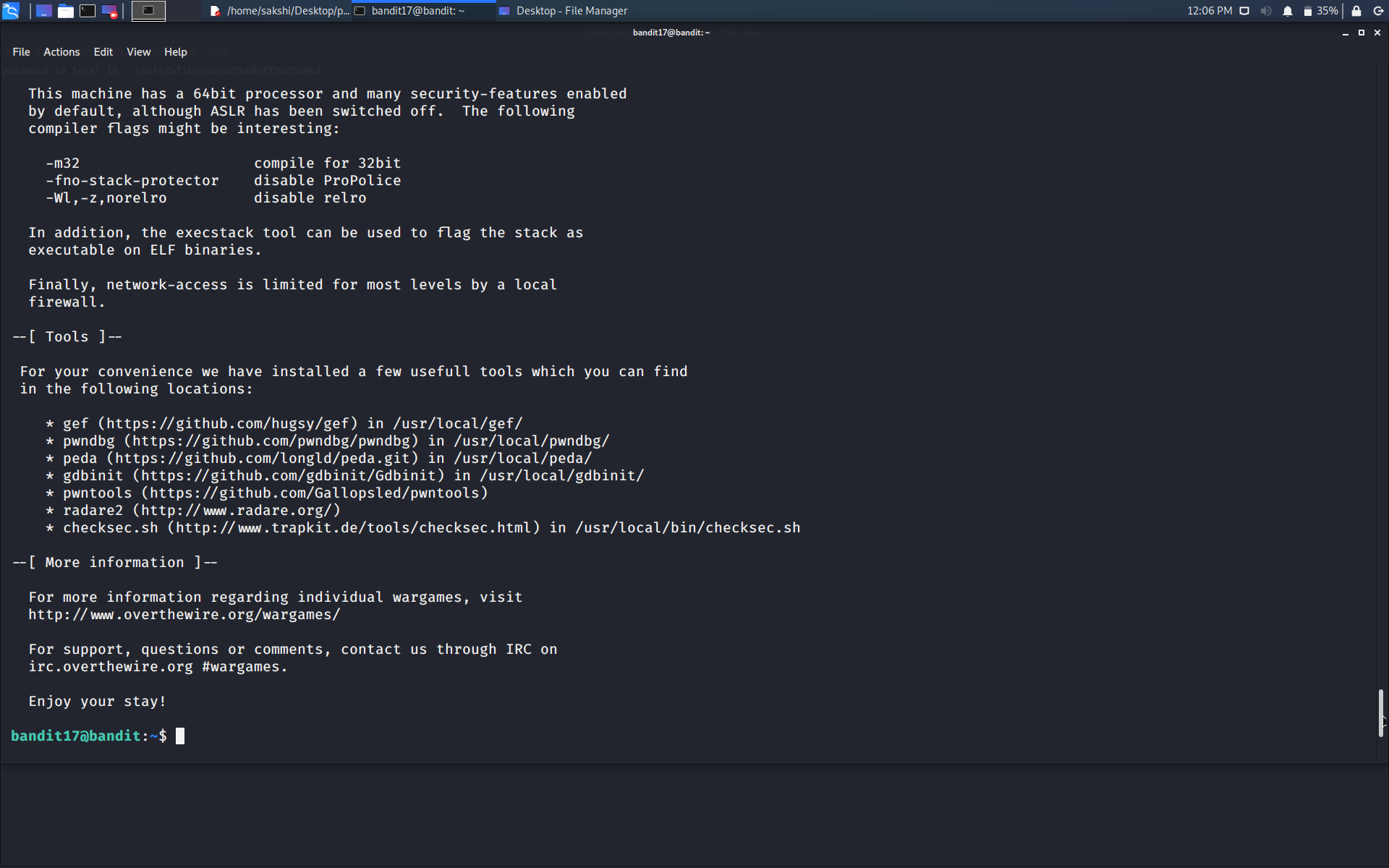
* Check the permissions of the file using command **ls -la. (permissions are– 644 -rw-r—r--)**
* Change the permissions using the command **chmod 600 bandit17.key** where 600

are new permssions .i.e **-rw-------**



* Now again, use command **ssh -I ./bandit17.key bandit17@localhost** to insert the key and login to the next level.

This time we are successful in logging in…….



Successfully passed level 17.…