Level 20 -> Level 21

The goal of this level is to use the setuid binary in the homedirectory. It makes a connection to localhost on the port you specify as a command line argument. It then reads a line of text from the connection and compares it to the password in the previous level (bandit20). If the password is correct, it will transmit the password for the next level (bandit21).

Use **ls -la** to find out all the files and their permissions, user, etc. The red mark indicates that the file has elevated its permissions.

We will execute the setuid binary without any argument so that we can get to know about how to use it. For execution we will use command: **./suconnect**

The given file will connect to the TCP port on localhost. It will take the password of previous level and if it is correct it will return us the password of this level.

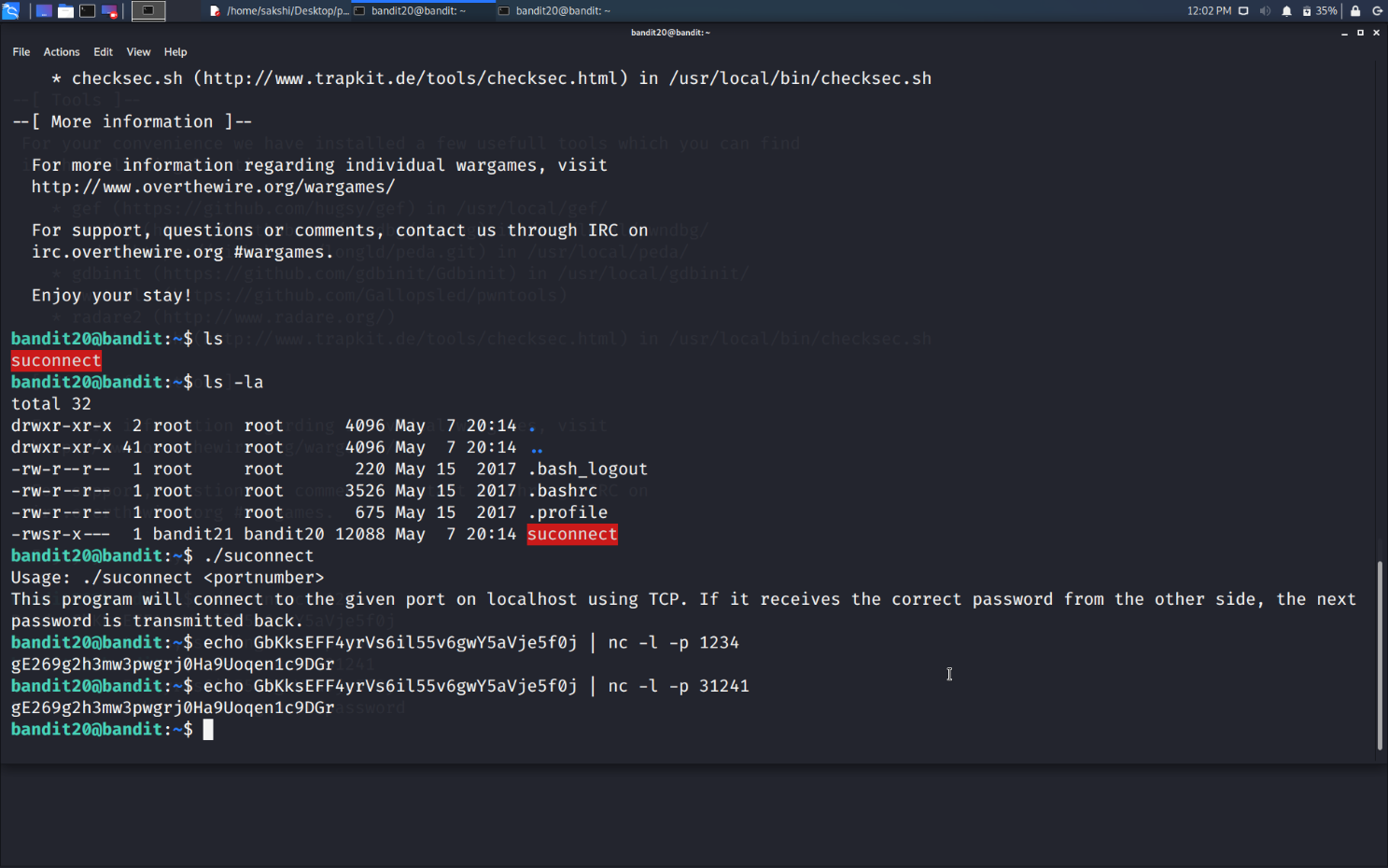
So, we will use **Netcat(nc)** to make an arbitrary port listening. Netcat can function as a server, by listening for inbound connections on arbitrary ports and doing the same reading and writing.

**Steps to follow:-**

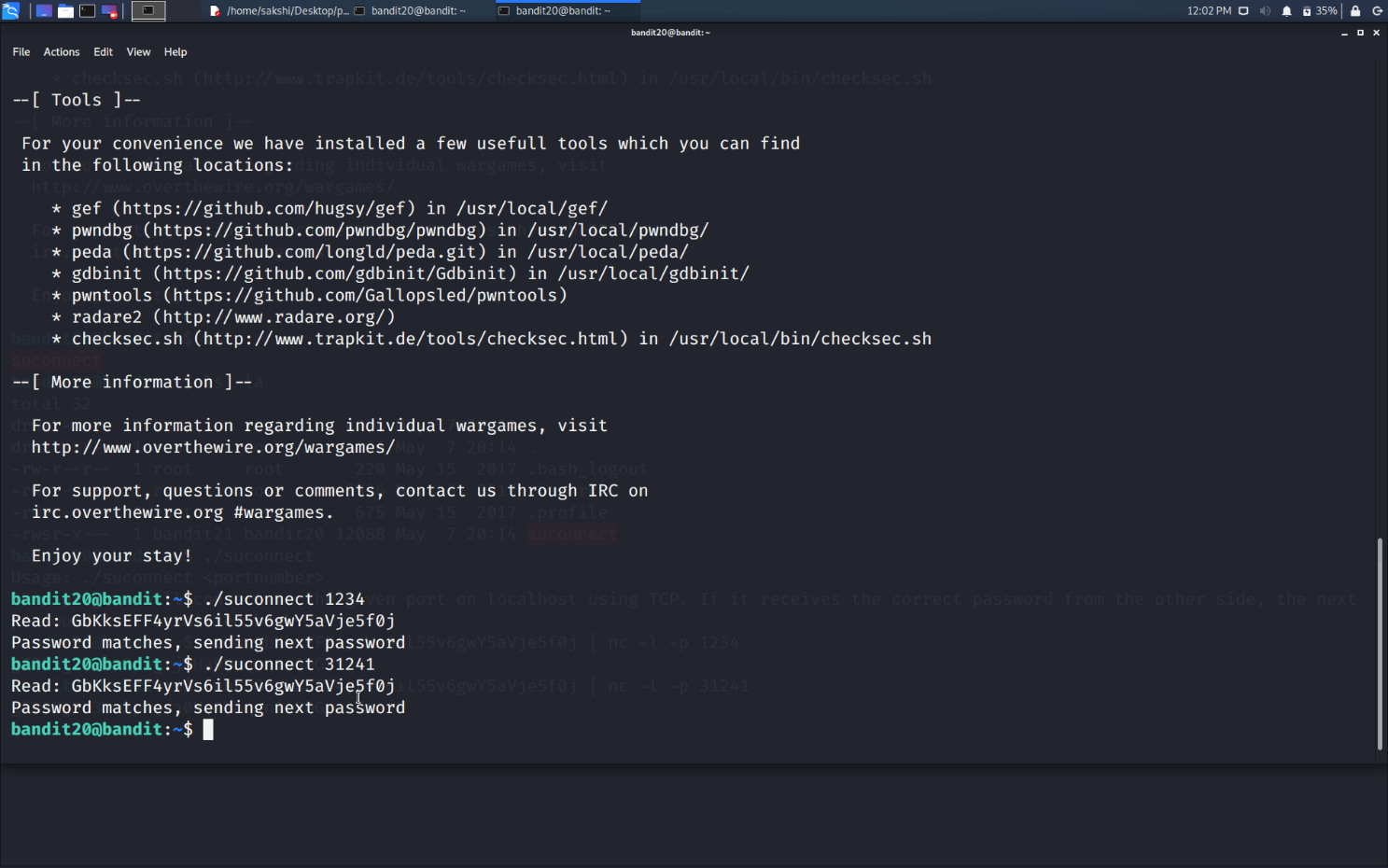
* Open to terminals.
* In Terminal 1 we will use **nc -l -p <arbitrary\_port\_number>** to make a listening port and use **echo** command to submit the password of previous level.
* After completing above two steps, In terminal 2 execute setuid binary with the port number as an argument i.e. **./suconnect < arbitrary\_port\_number >**
* After the execution of commands the password will be sent to the terminal 1 from terminal 2.

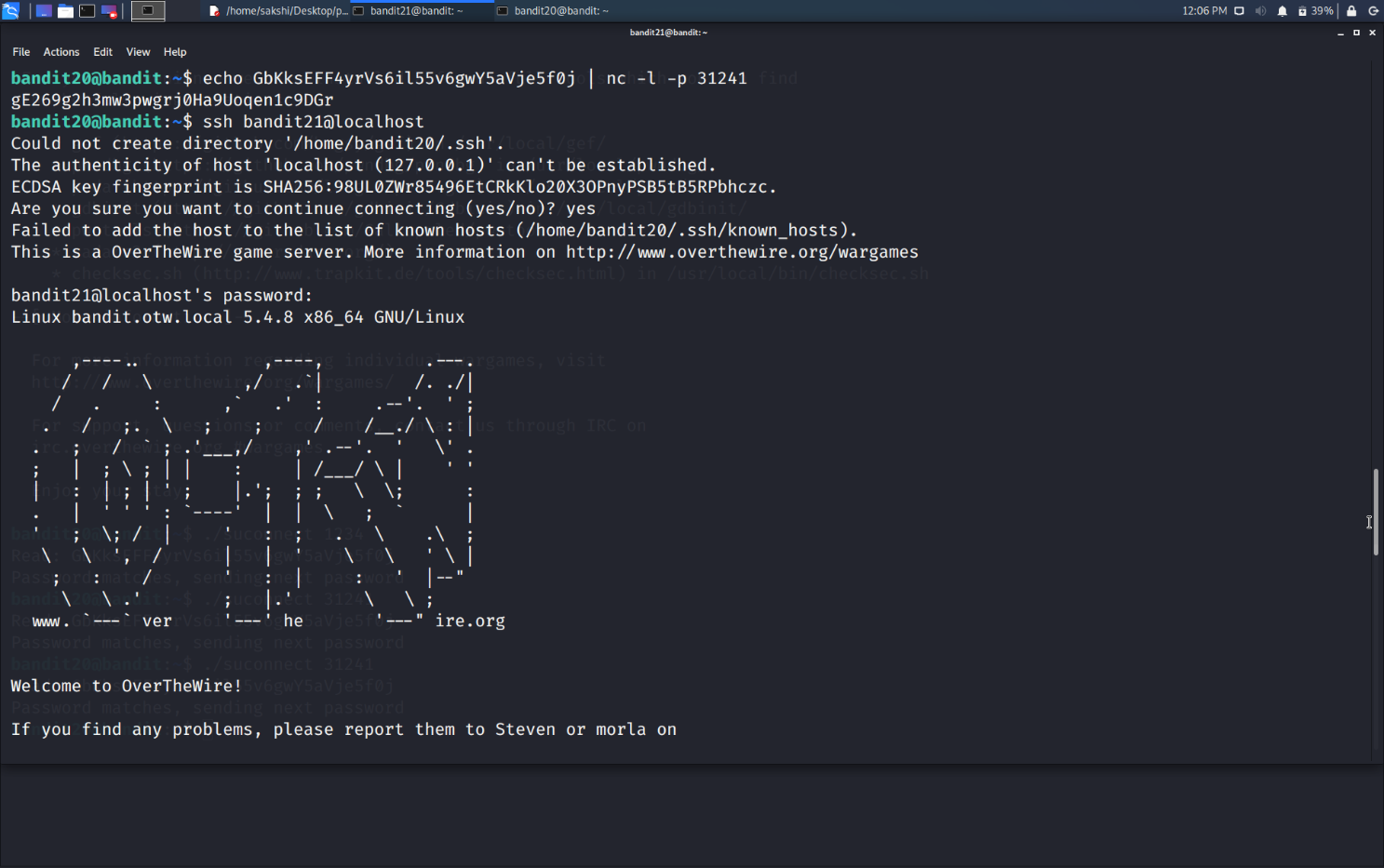
I used two different ports :- 1234 and 31241 to do this task.

**Terminal 1:-**

****

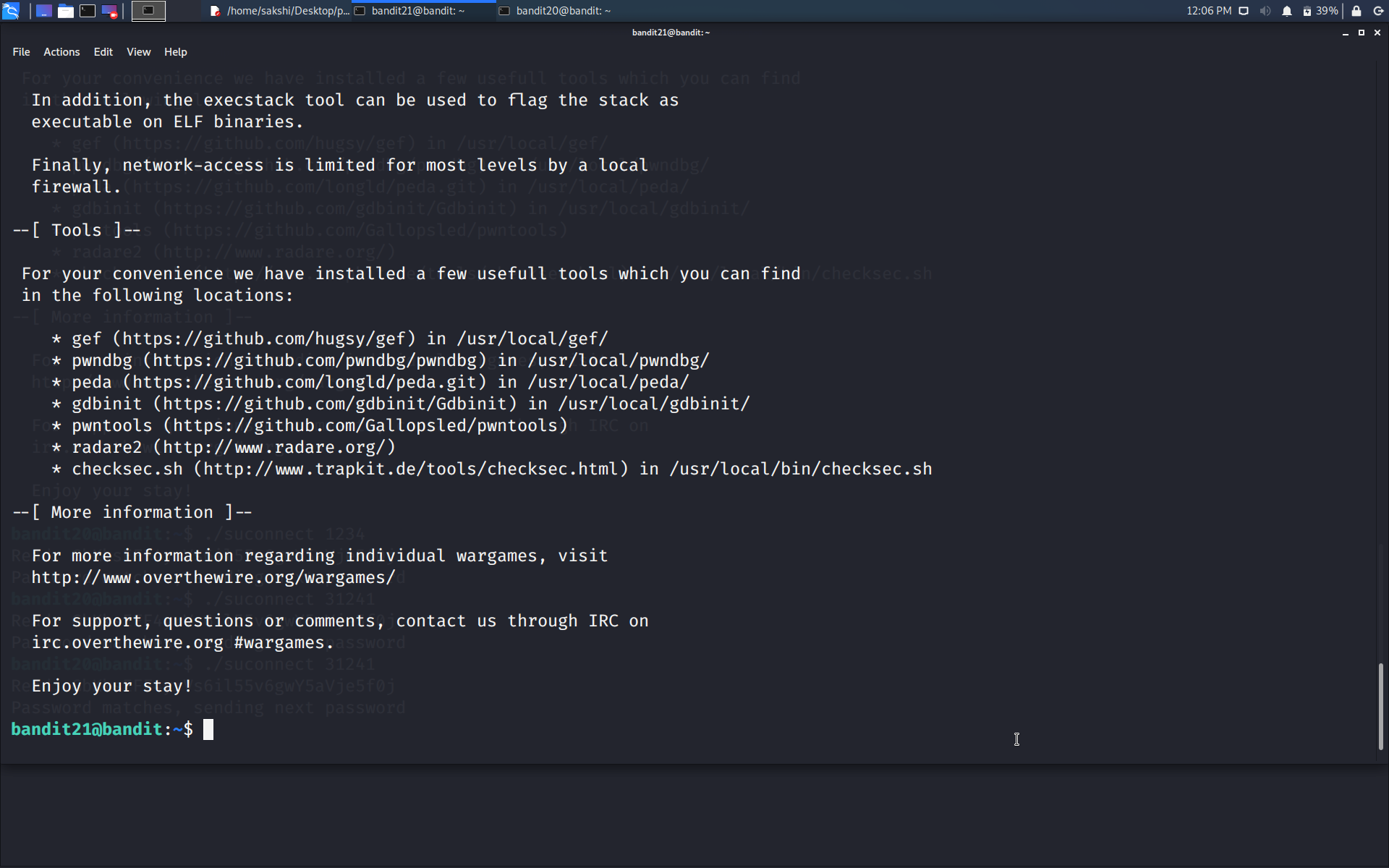
**Terminal 2:-**

****



Use the command **ssh bandit21@localhost** to connect to the level 21.

Enter the password and hit enter.



Successfully passed level 21.…