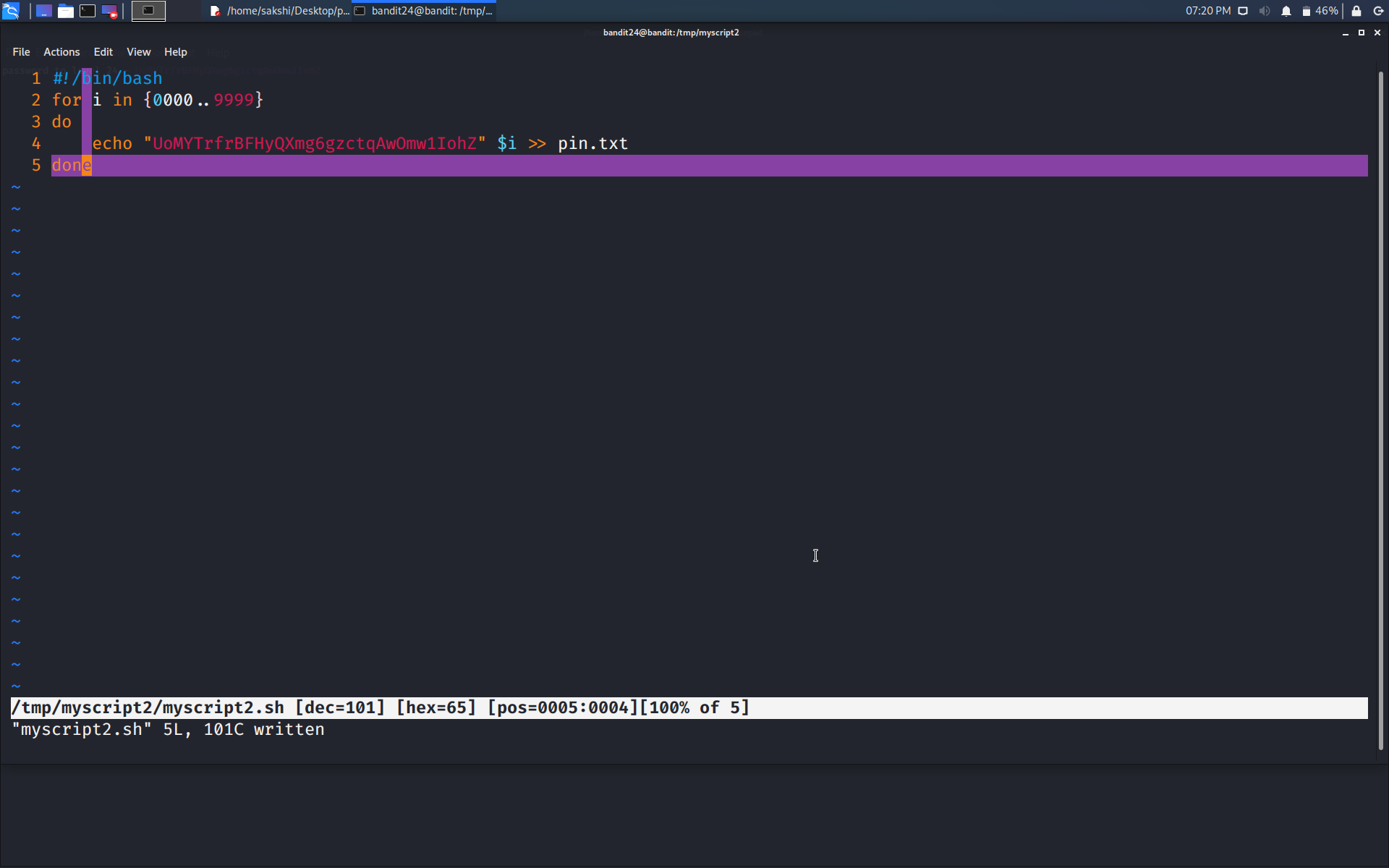
Level 24 -> Level 25

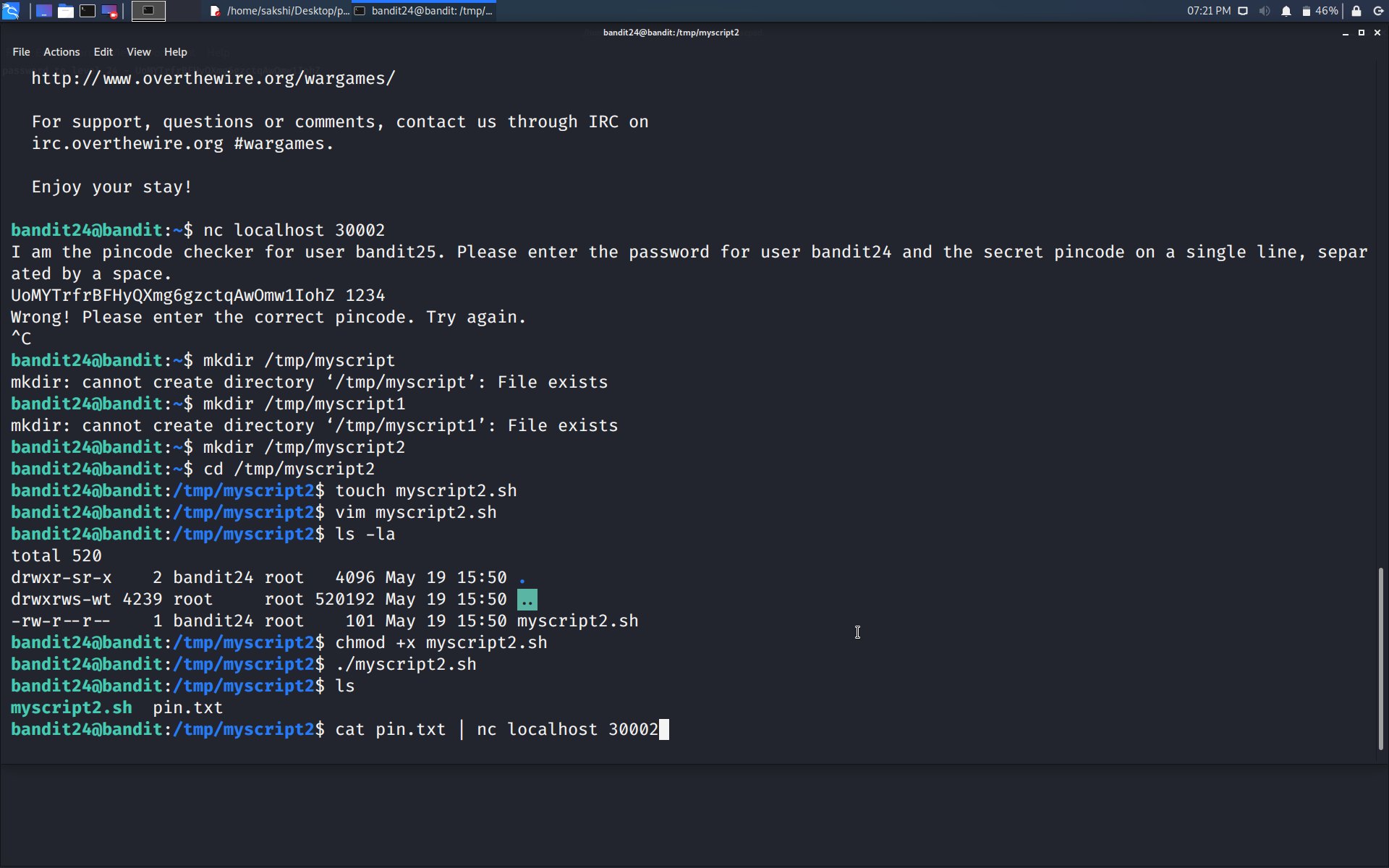
The main goal of this level is to get the four-digit pincode. A daemon is listening on port 30002 and will give us the password for bandit25 if given the password for bandit24 and a secret numeric 4-digit pincode. There is no way to retrieve the pincode except by going through all of the 10000 combinations, called brute-forcing.

**Steps to follow:**

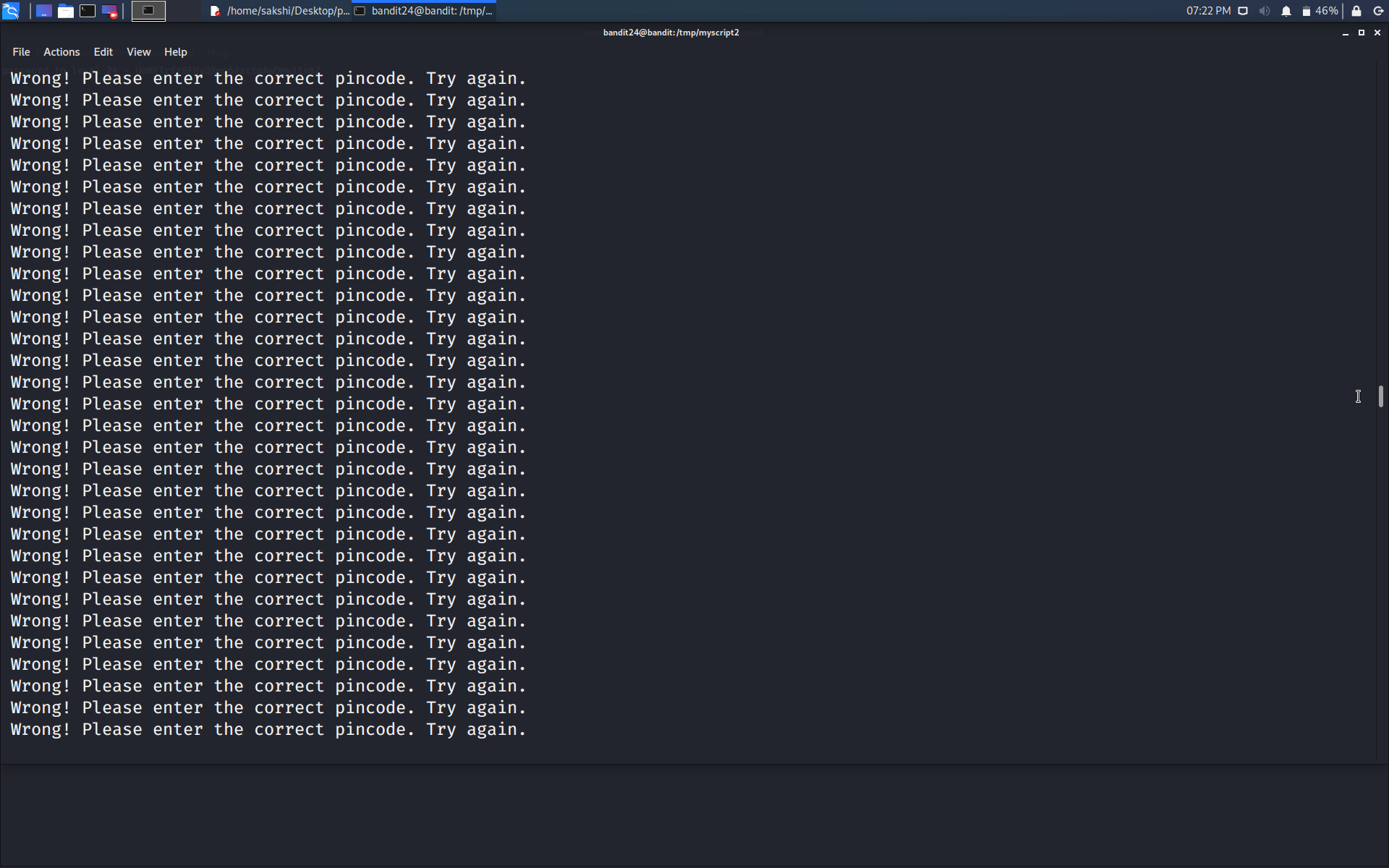
1. Using **nc localhost 30002** command we will connect to the port 30002. It displays a message that we need to submit the password of previous level including a four-digit pincode.
2. Hence, we need to write a script that will perform brute-force and check every possible pincode of four-digits.
3. The script I have written is as following:



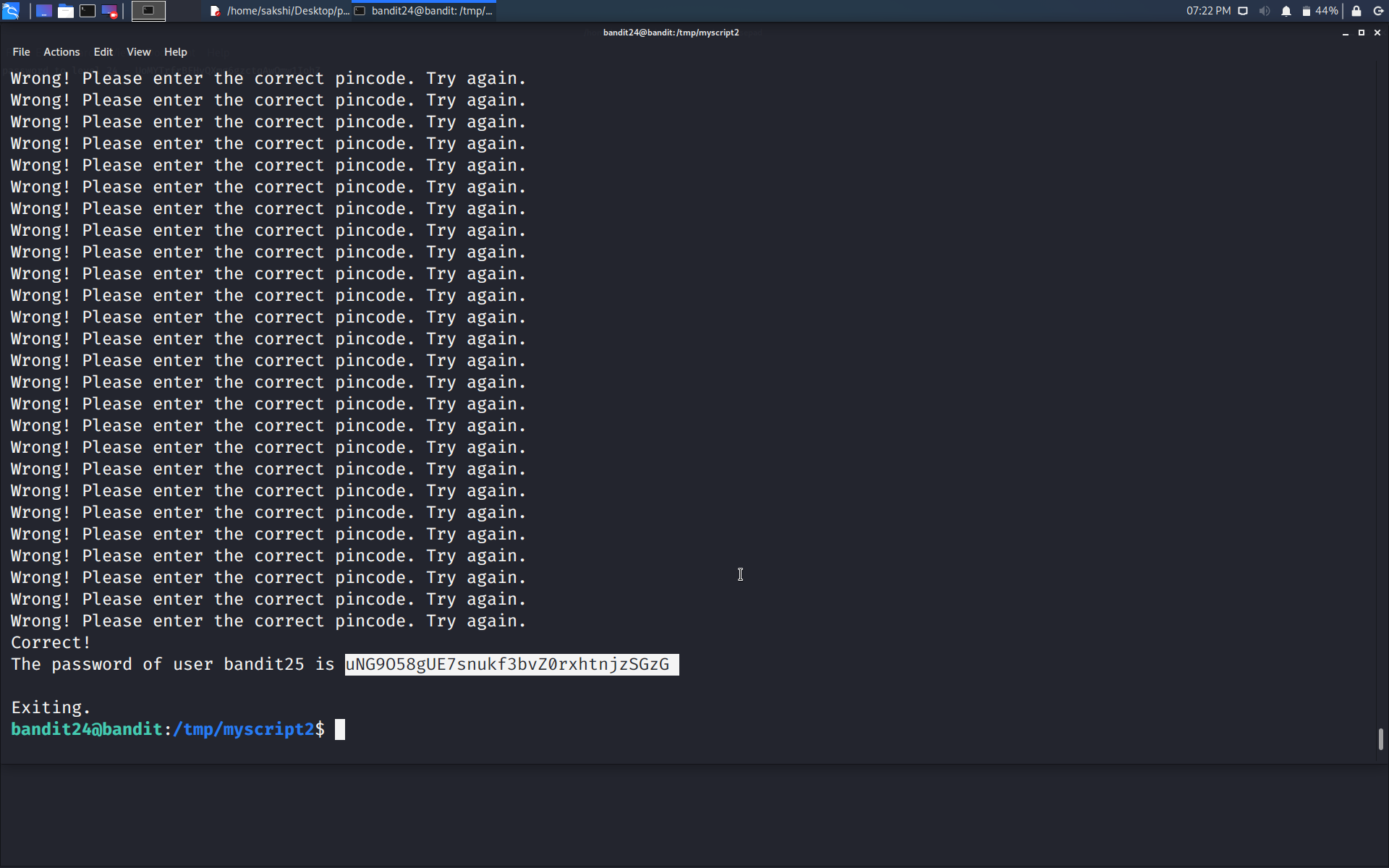
1. The above script will echo all password + pincode (where pincode starting from 0000 to 9999) in the file named pin.txt.



1. Now, we just need to do is cat pin.txt file to the port 30002 by using command **cat pin.txt | nc localhost 30002**.
2. The command wiil try every input and check for the match.

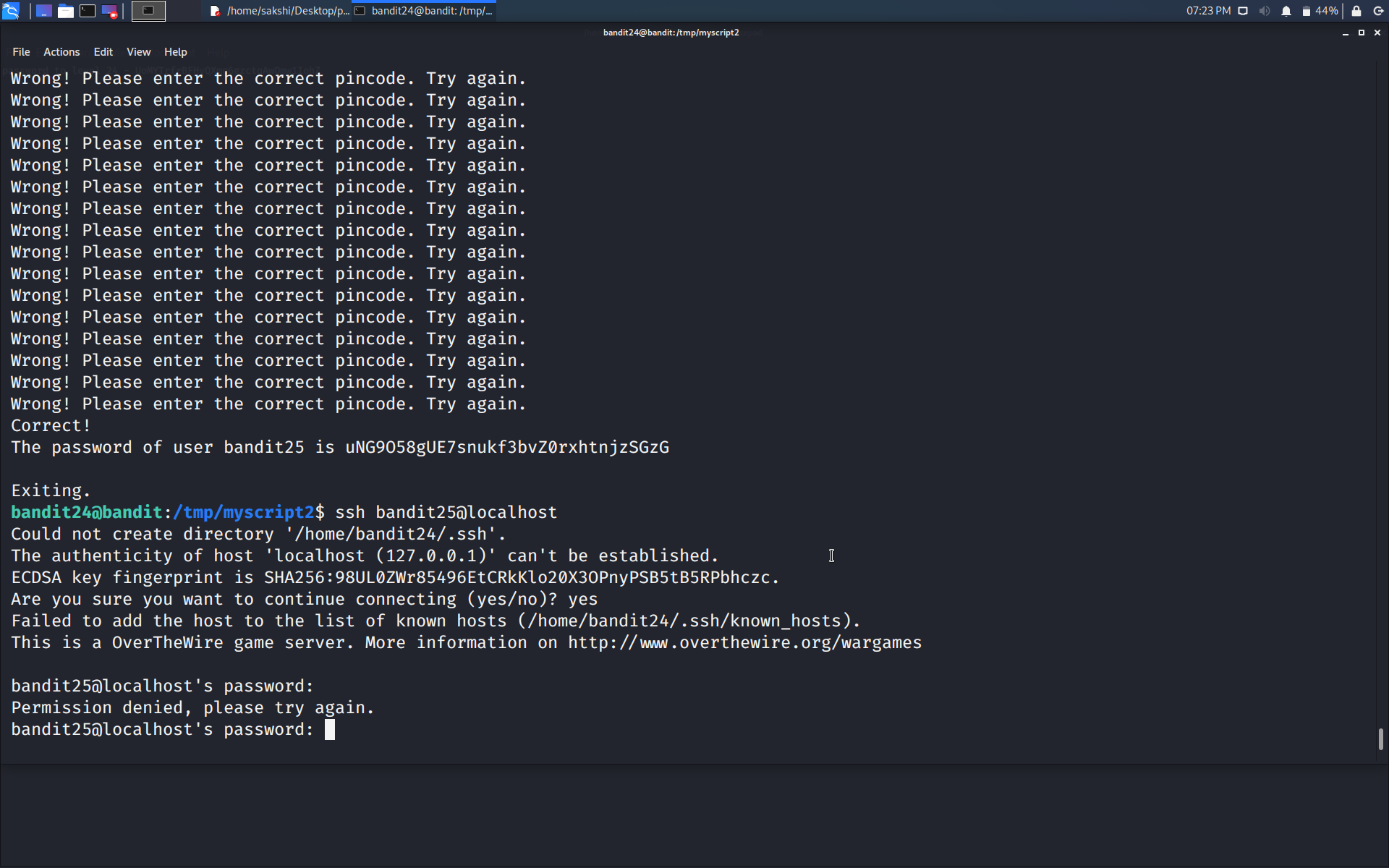


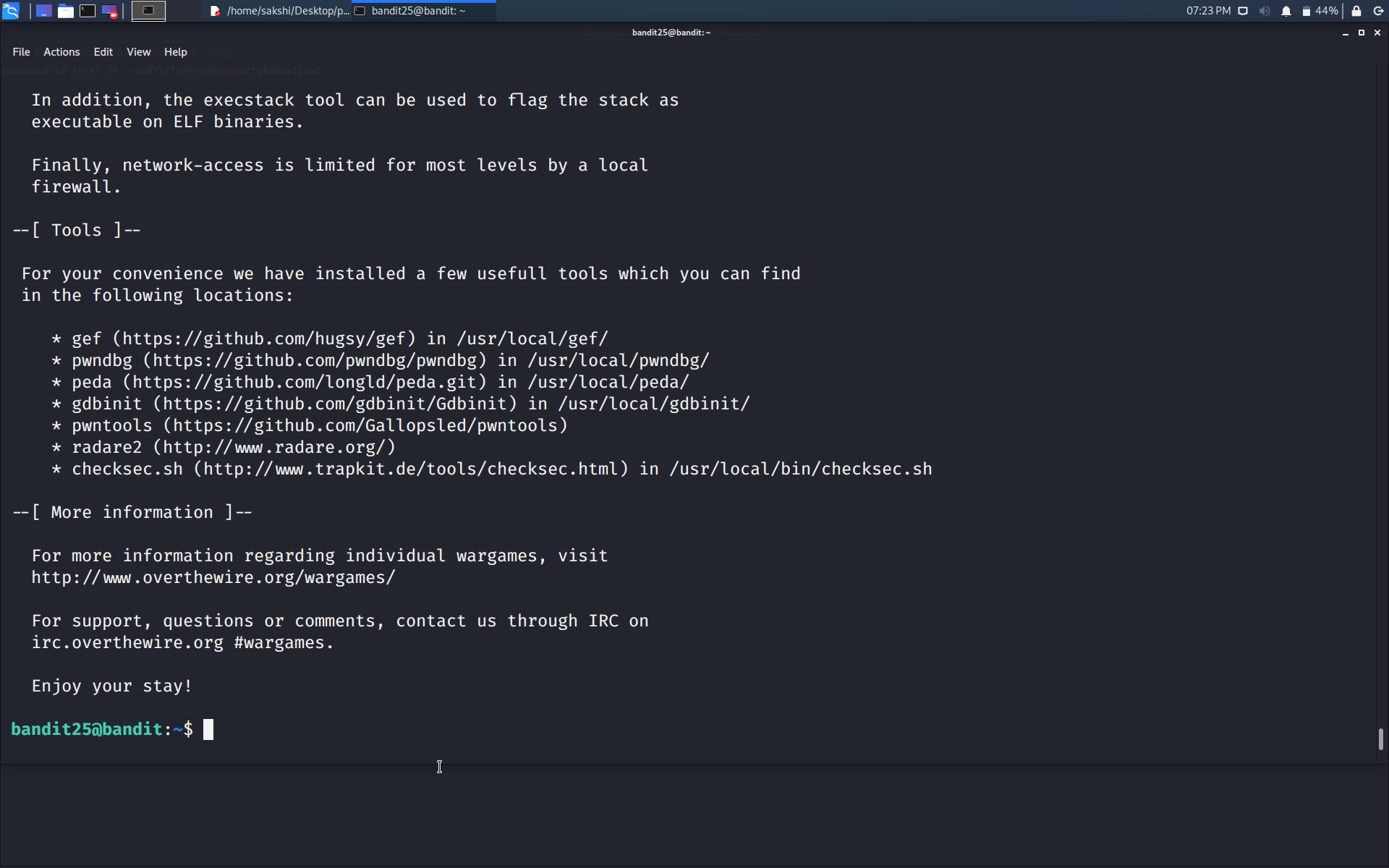
And yes!!!!! We got the password…



Use the command **ssh bandit25@localhost** to connect to the level 25.

Enter the password and hit enter.





Successfully passed level 25.…