Level 15 -> Level 16

The goal of this level is to submit the password of the current level to **port 30001 on localhost** using SSL encryption and get the password to the next level.

Firstly we will 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:30001** to get the password of next level.

**echo** command in Linux is used to display line of text/string that are passed as an argument.

**OpenSSL** is a multi-platform, open source SSL/TLS toolkit. OpenSSL can be downloaded from <http://www.openssl.org/>. It is already present in Linux based systems.

The OpenSSL command line tool can be used for several purposes like creating certificates, viewing certificates and testing https services/connectivity etc.

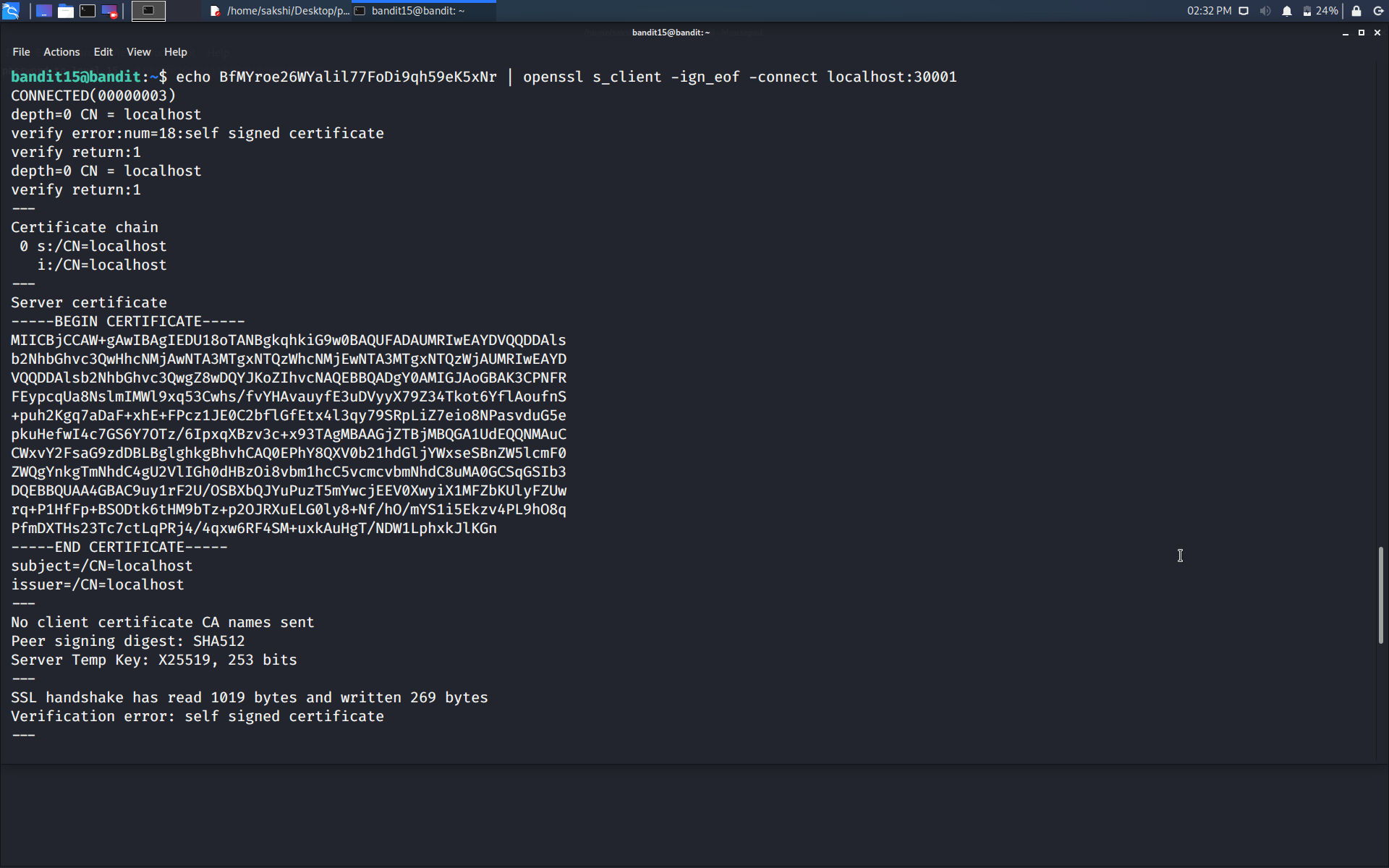
The following command can be used to test connectivity:

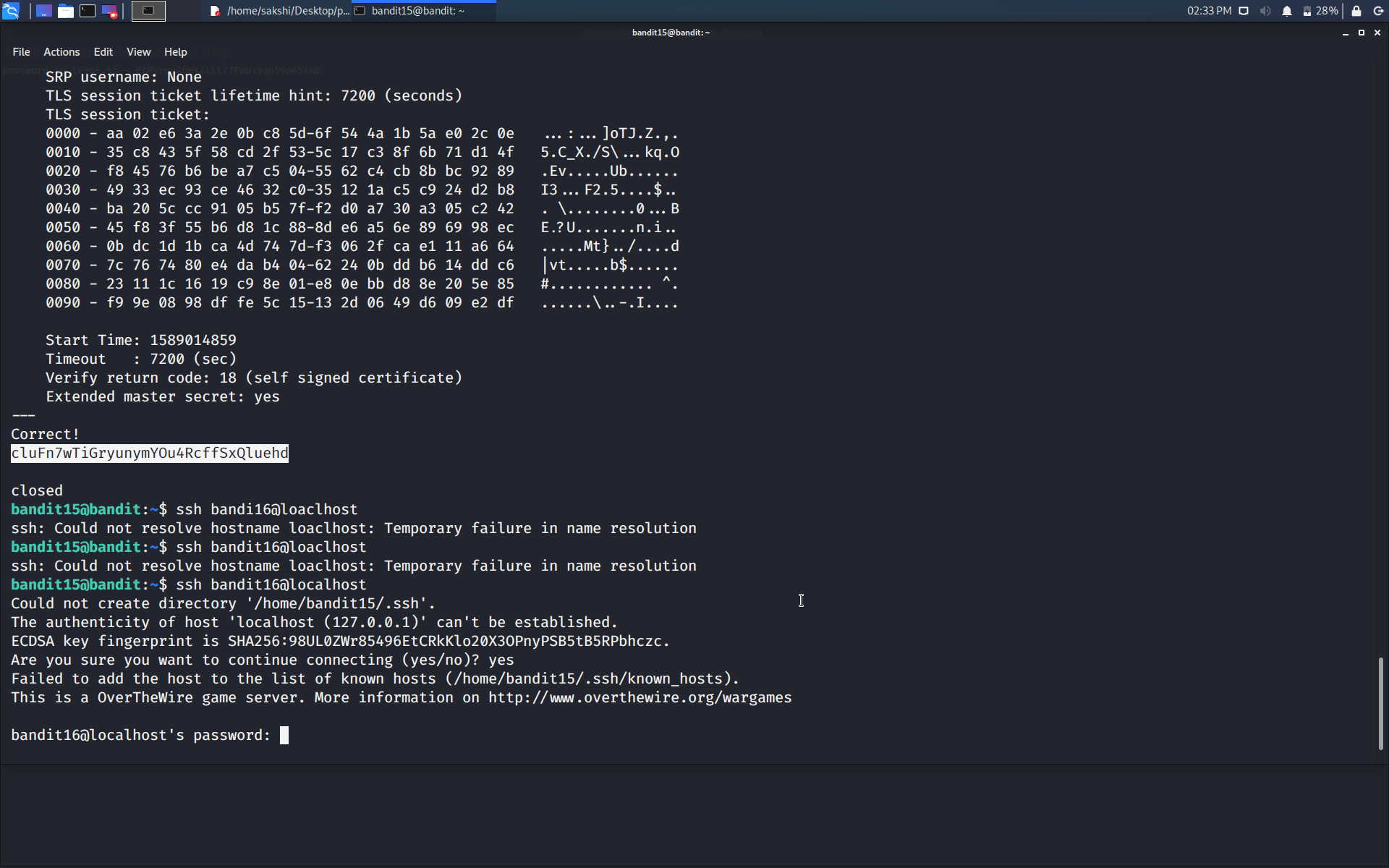
openssl s\_client -connect <hostname>:<port>

For example: openssl s\_client -connect [example.com](http://pingfederate.example.com/):443

**ign\_eof** does is it prevents the server from closing down the connection when the end of file is reached in our input

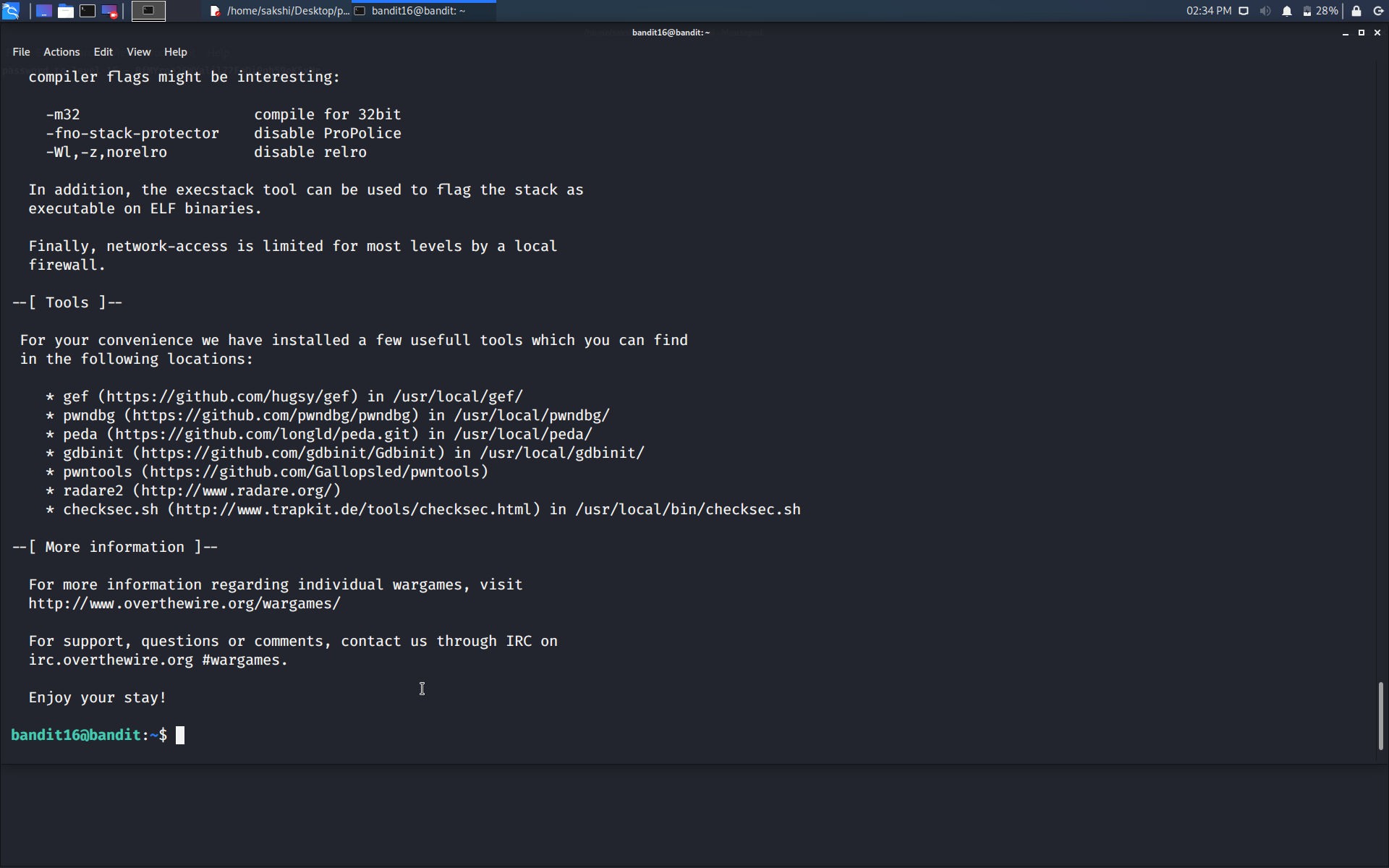
This is how we will get password to the next level.





Use the command **ssh bandit16@localhost** to connect to the level 16.

Enter the password and hit enter.



Successfully passed level 16.…