**Overthewire-Bandit**

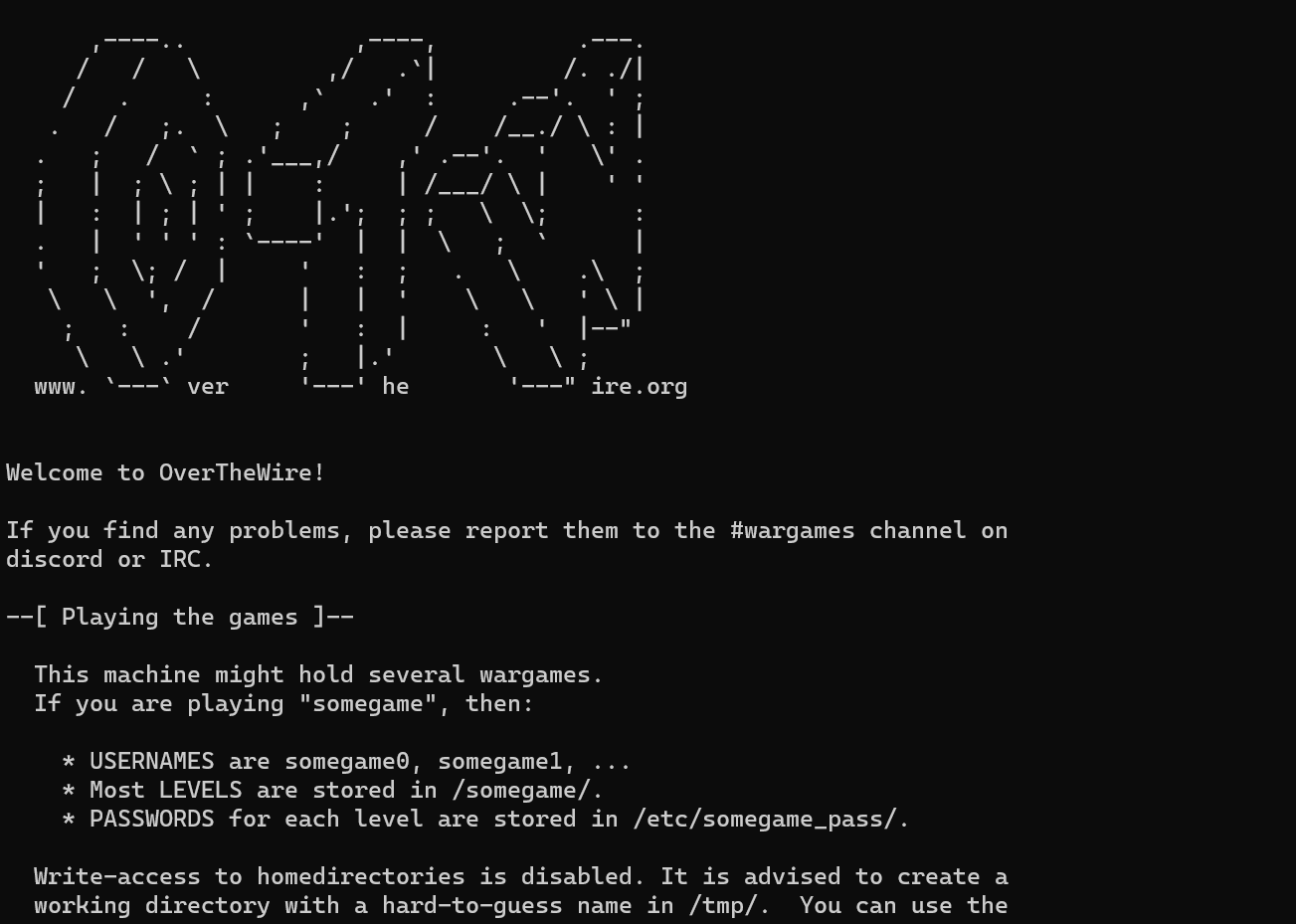
Name: Meeti

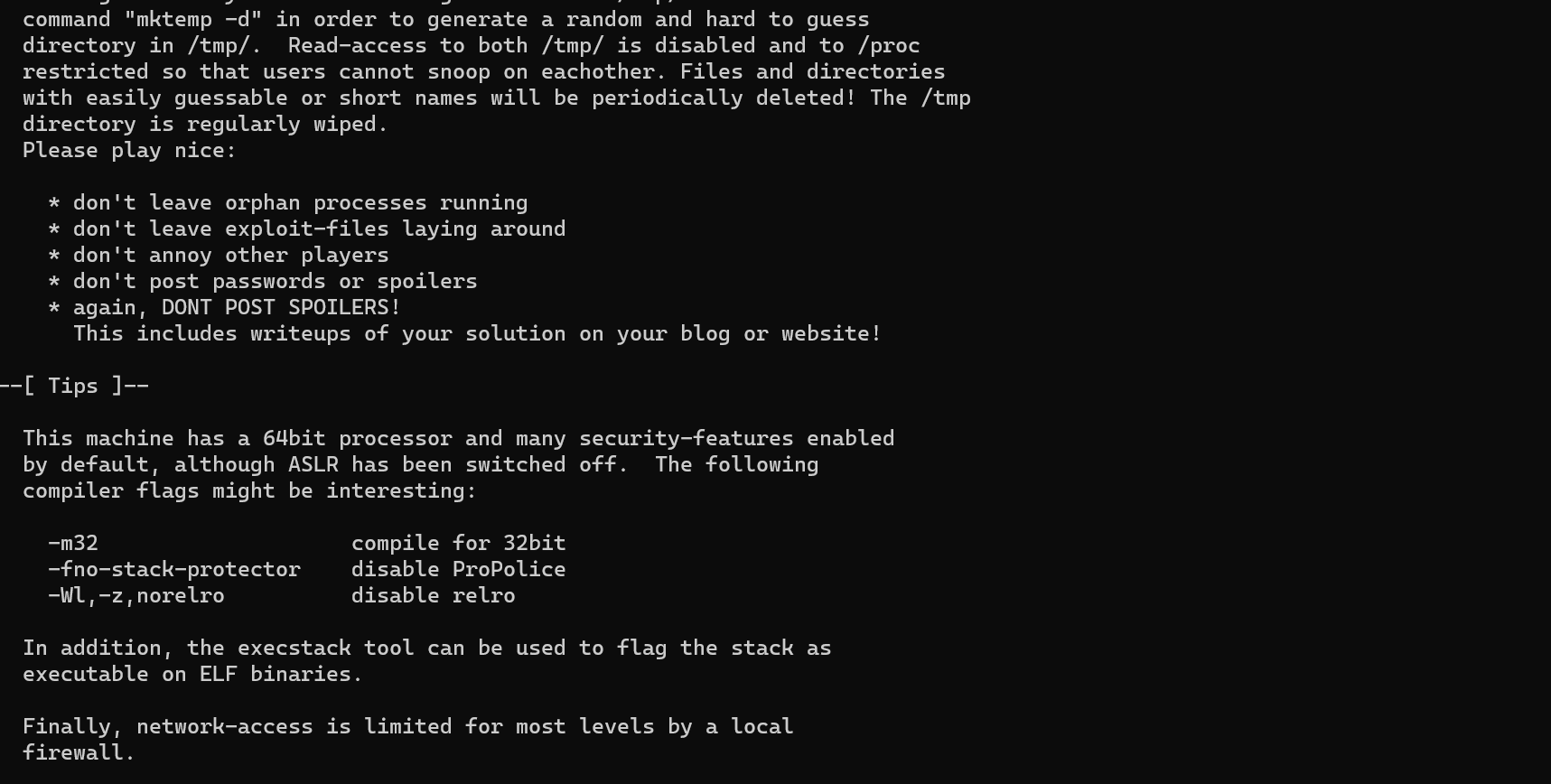
Levels: 13-20

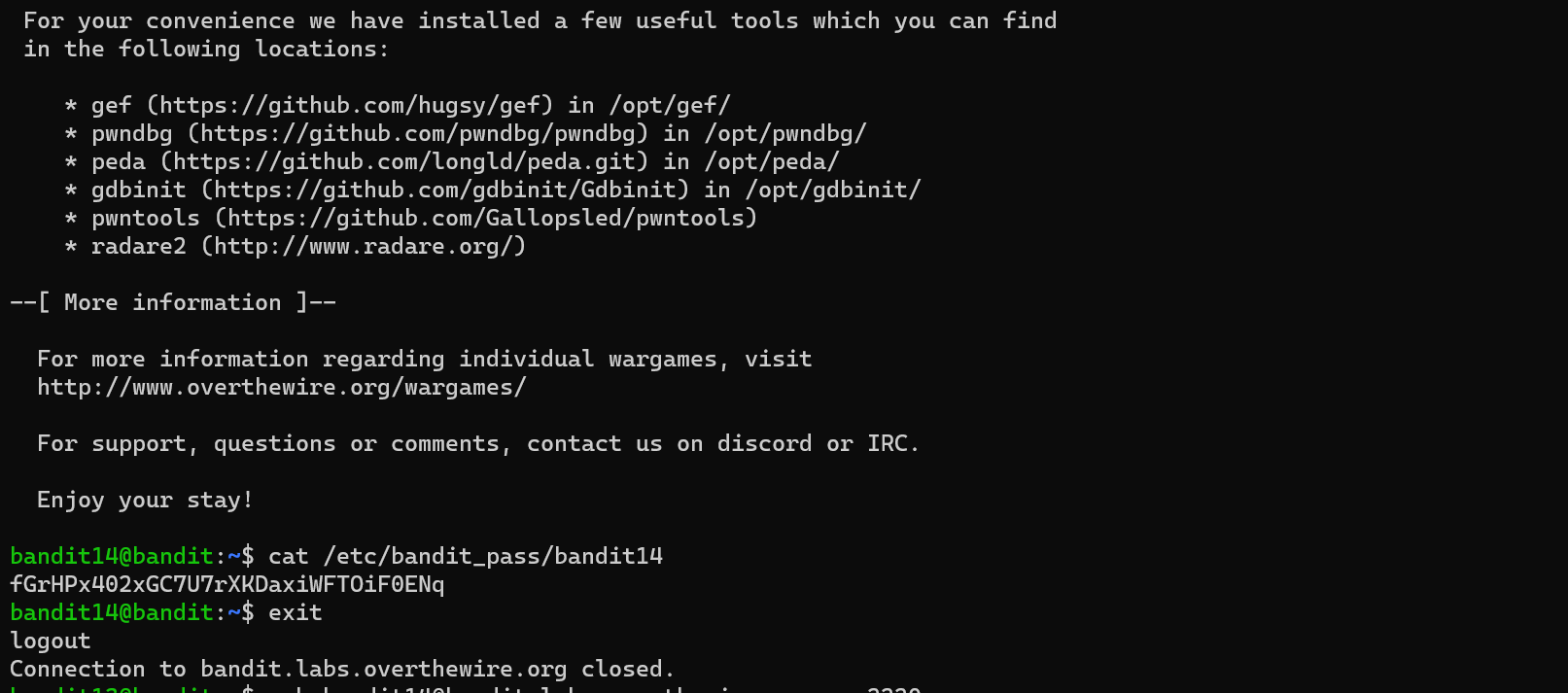
Bandit level 13-14

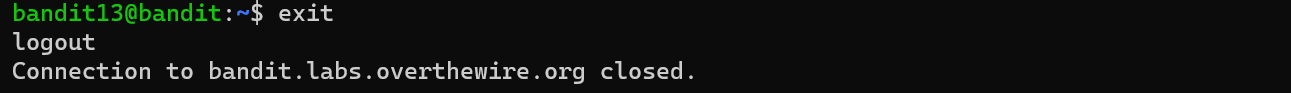
1. Browsed the helpful reading material.
2. Checked the ssh command in the manual.
3. ssh: program to login to a remote machine and execute commands there.
4. -i: this selects a file from which the identity for public key authentication is read.

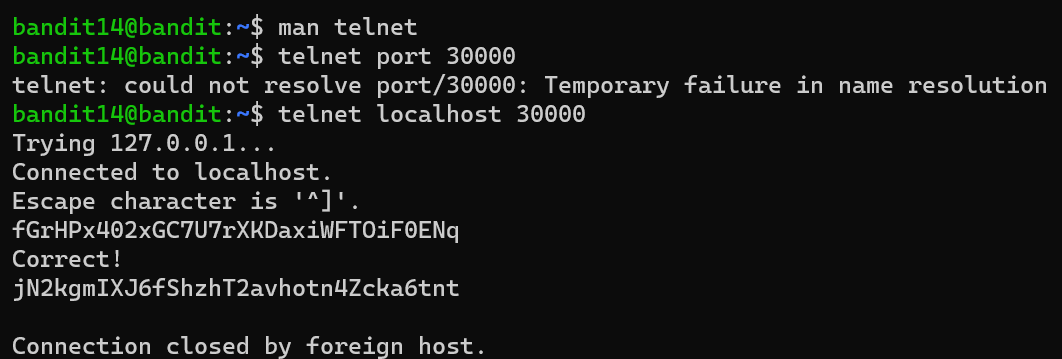






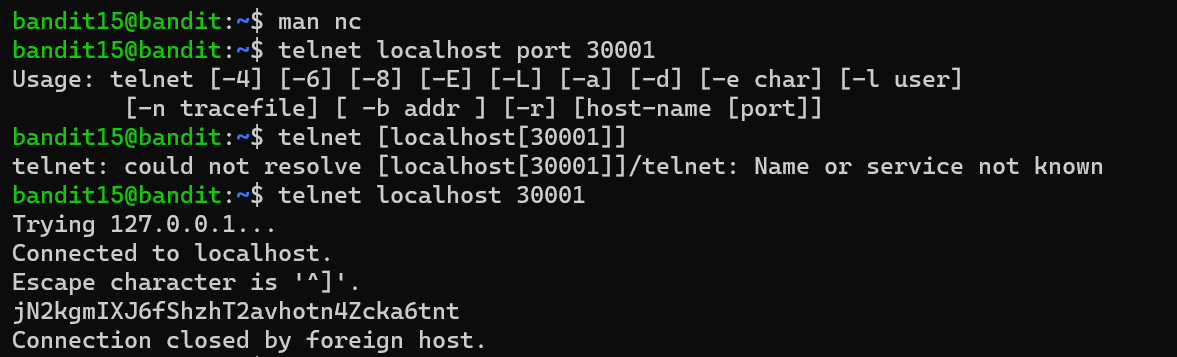


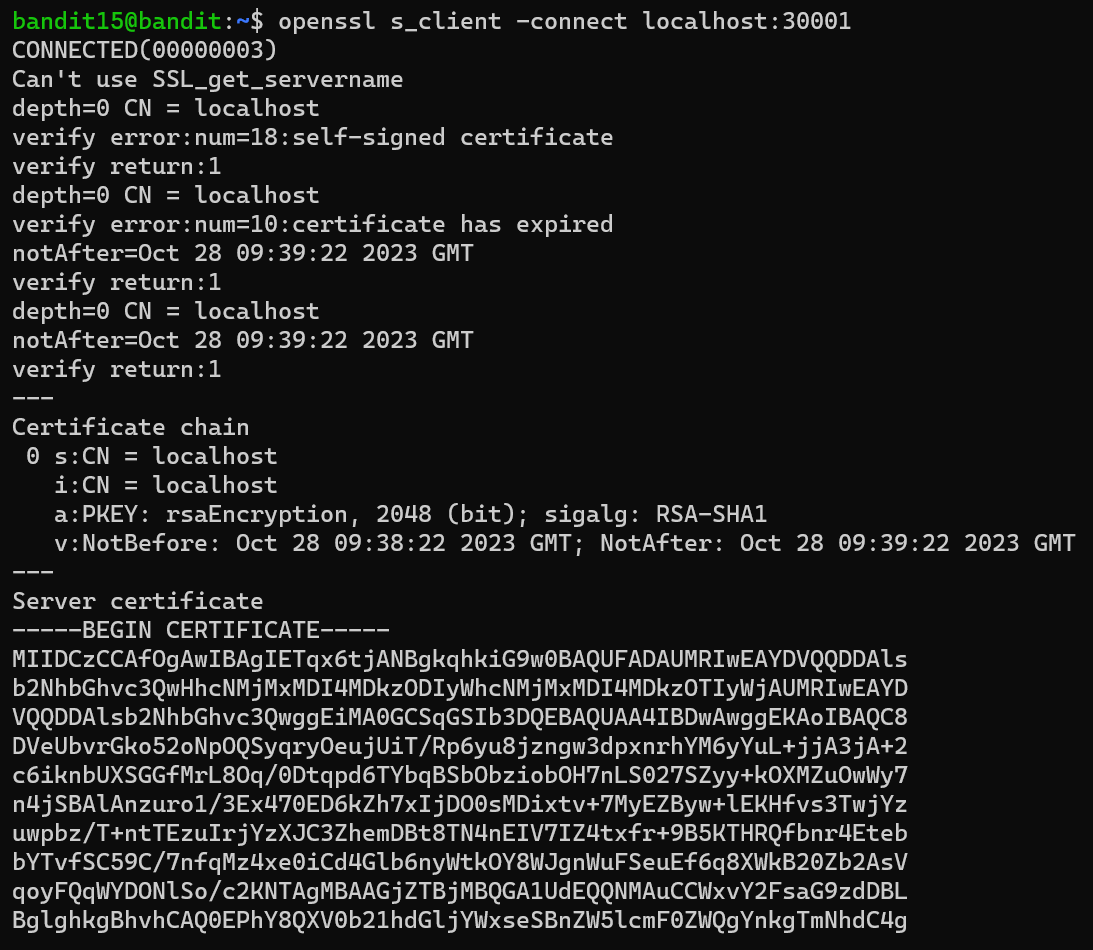
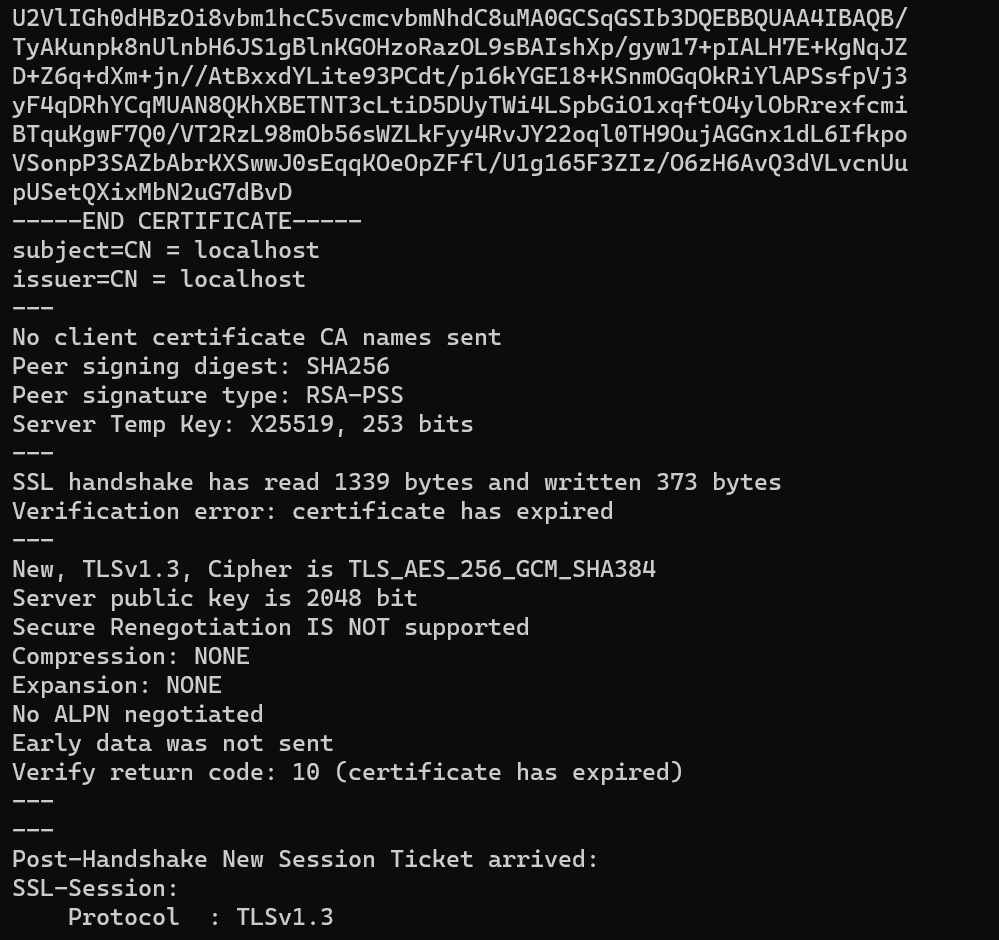
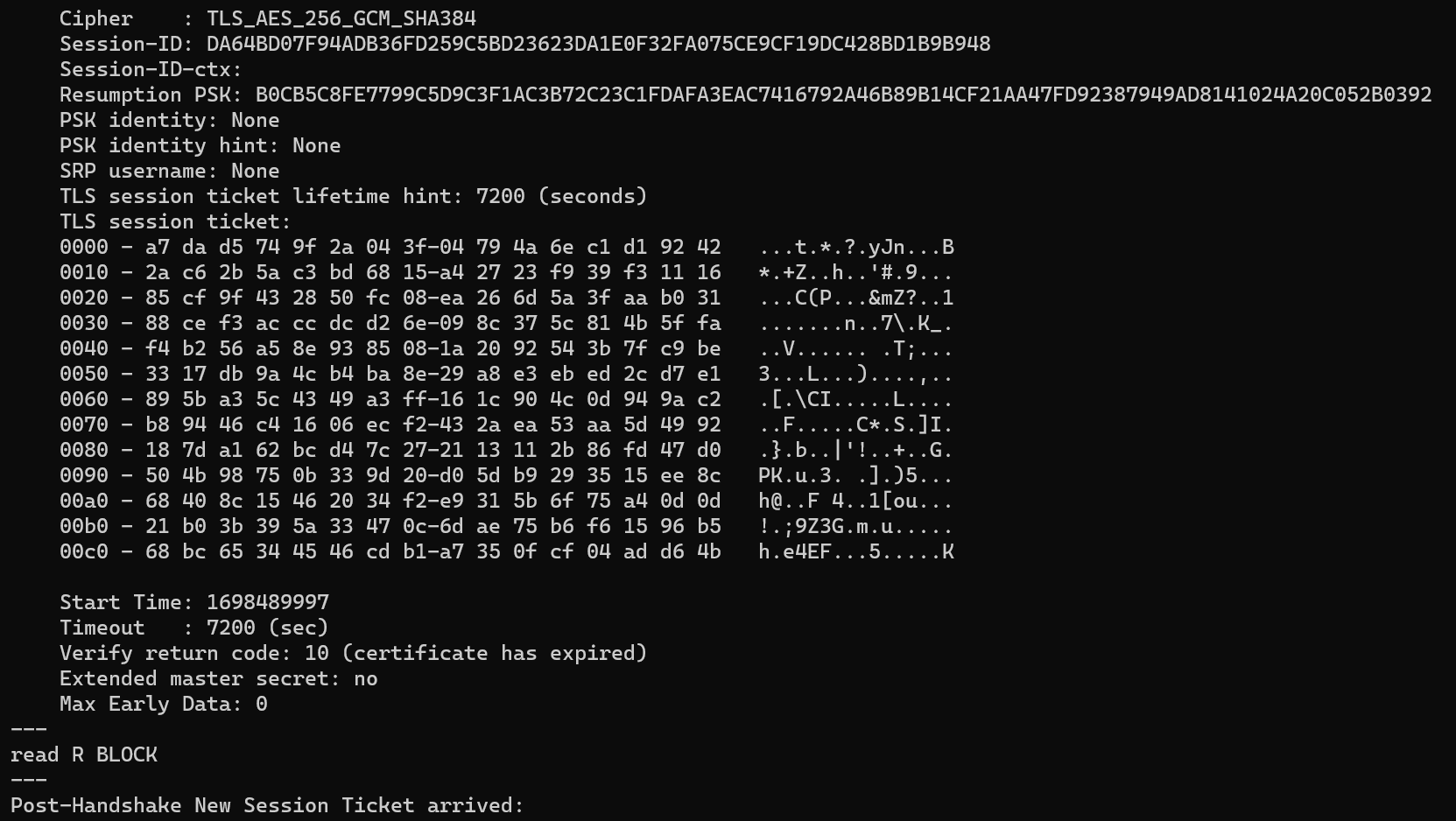
Bandit level 14-15

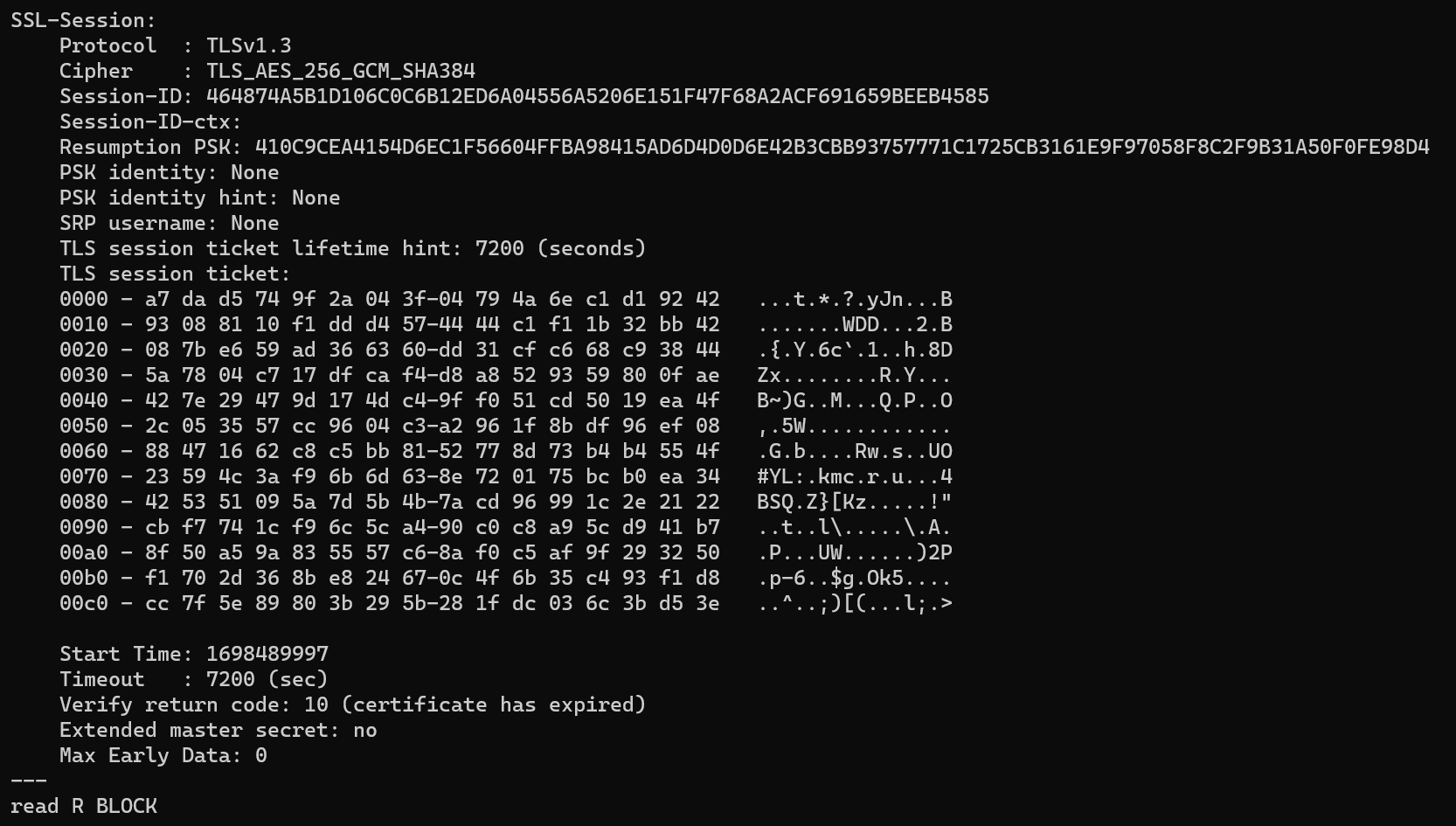
1. Checked manual for telnet.
2. telnet: network protocol that is used to connect to remote systems over a TCP/IP network. 

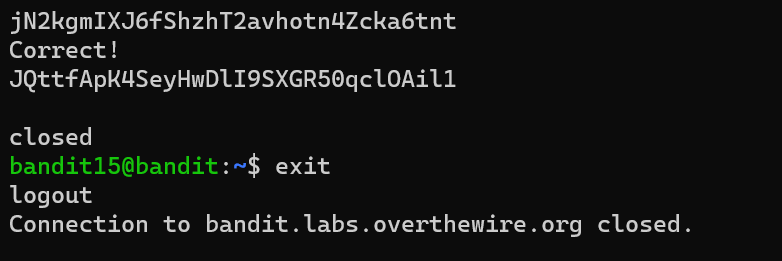
Bandit 15-16

Openssl s\_client: implements a generic SSL/TLS client which connects to a remote host using SSL/TLS







Bandit 16-17

Browsed through the helpful reading material.

<https://www.linuxjournal.com/article/4234>

Found that nmap (network mapper) is the most powerful network probing tool.

Checked nmap in the manual.

nmap: an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts

Scanned ports 31000 to 32000 using nmap -p31000-32000 localhost

This showed the ports with a server listing on them.

Checked each port one by one by connecting via openssl s\_client

Port 31790 spoke ssl and returned a private rsa key on entering the password.

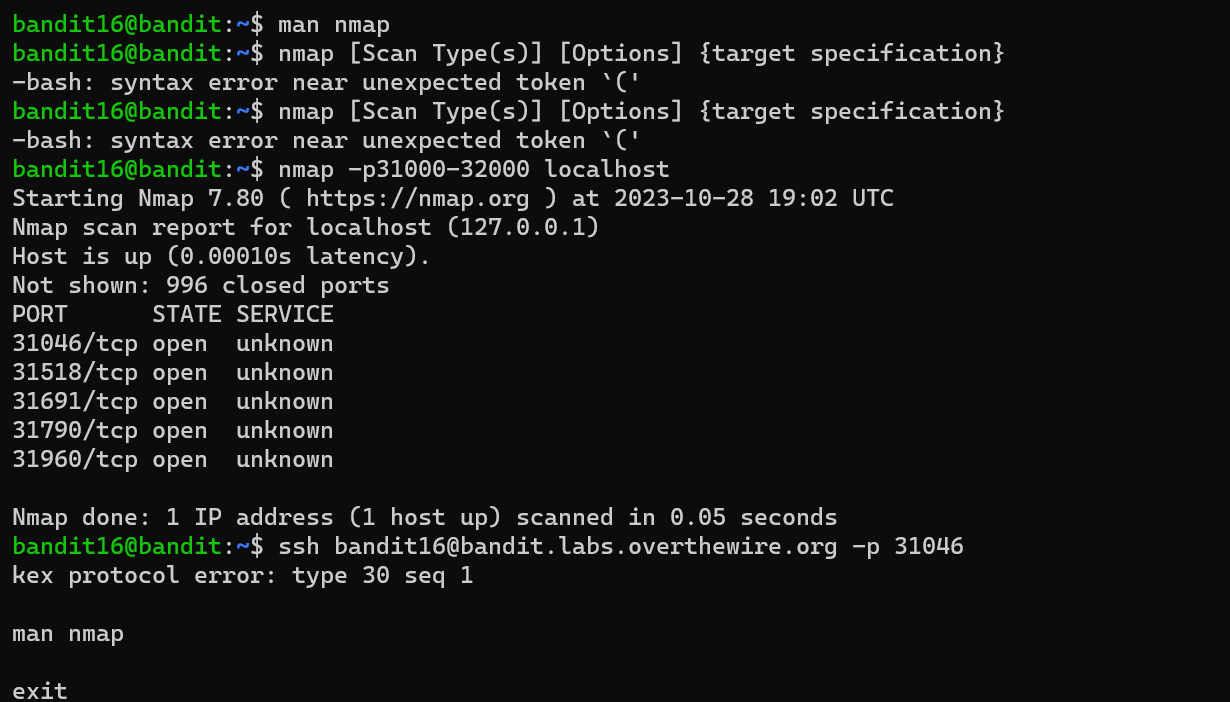
GNU nano is a small and friendly text editor.

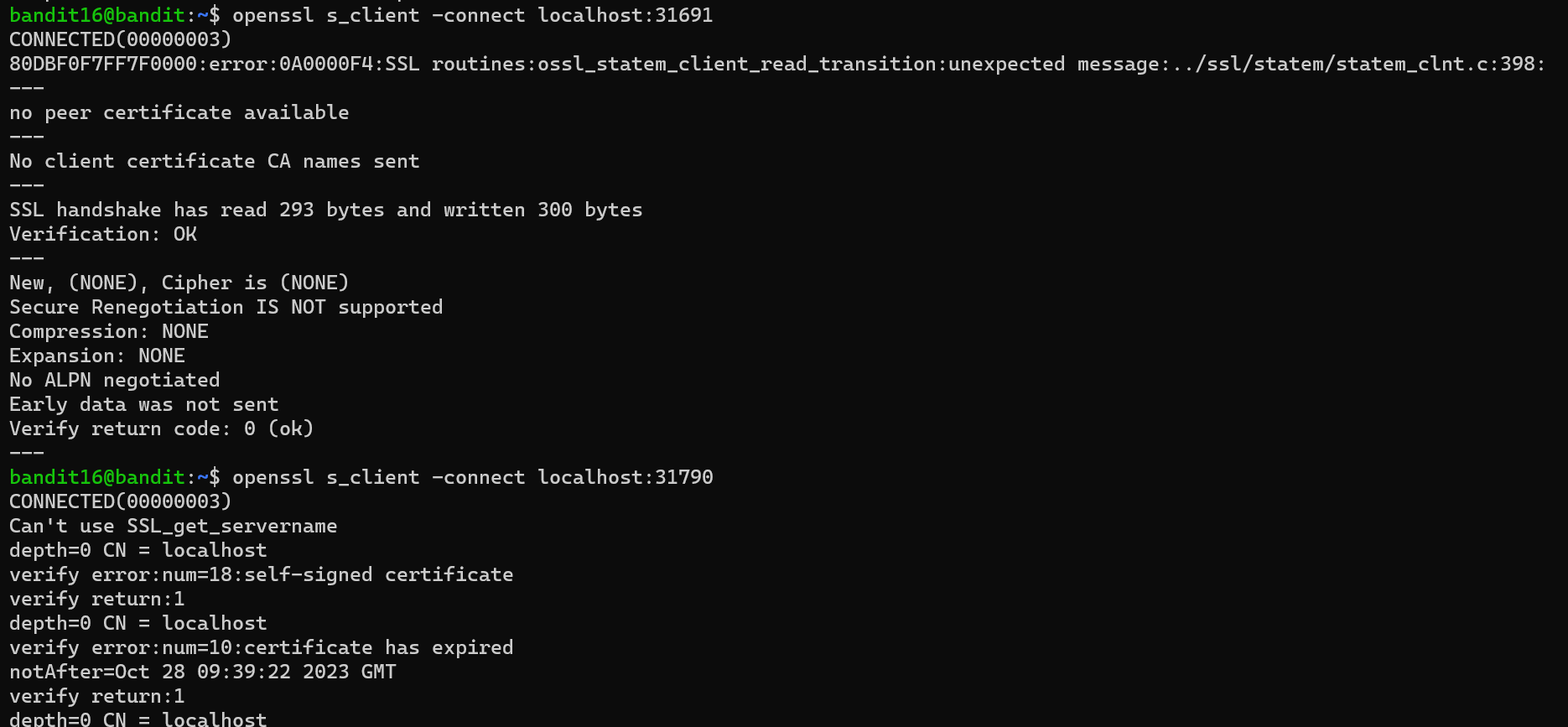
chmod changes the file mode bits of each given file according to mode

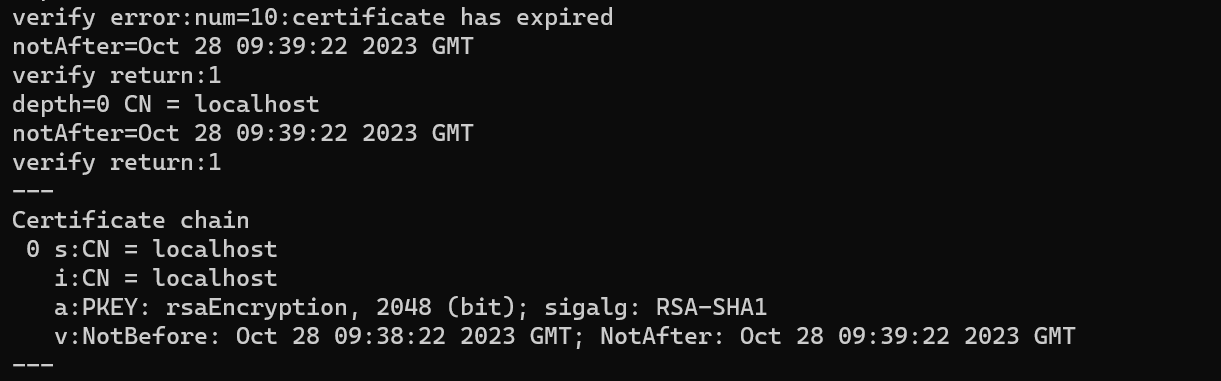
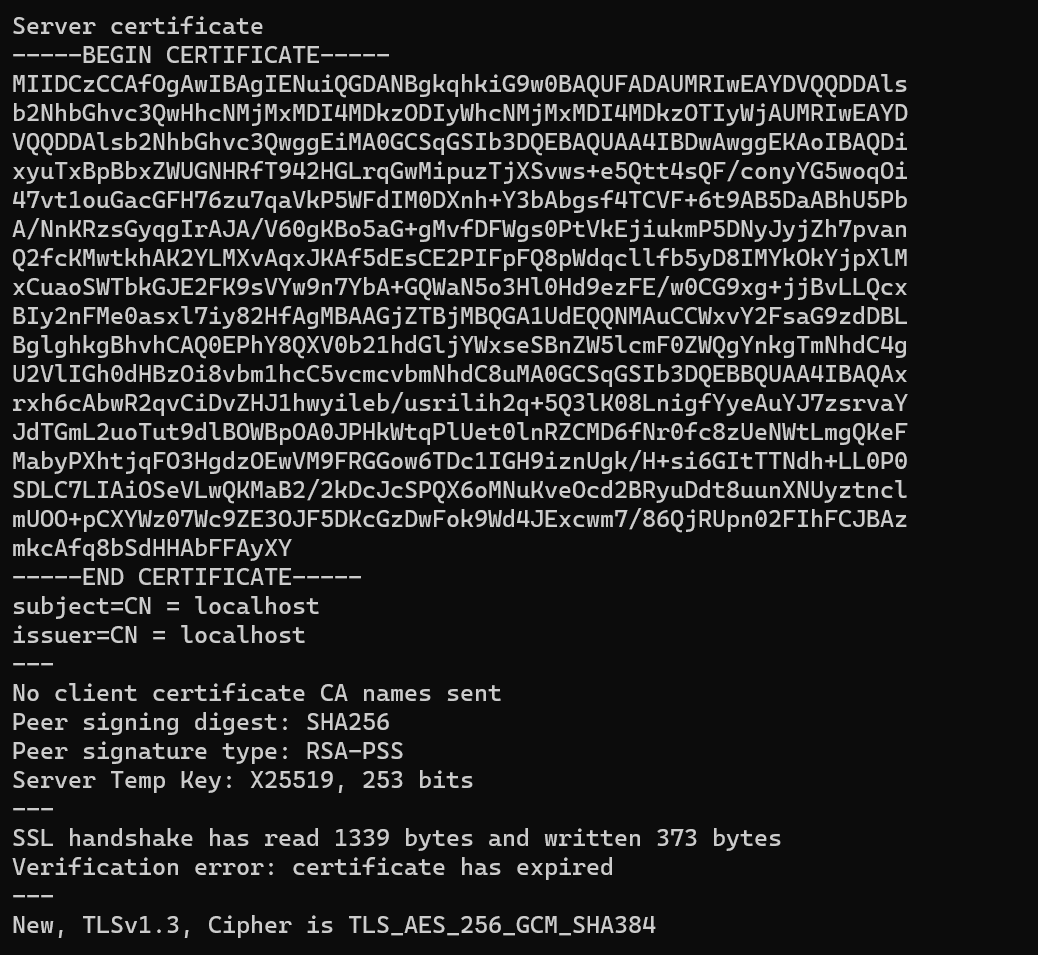
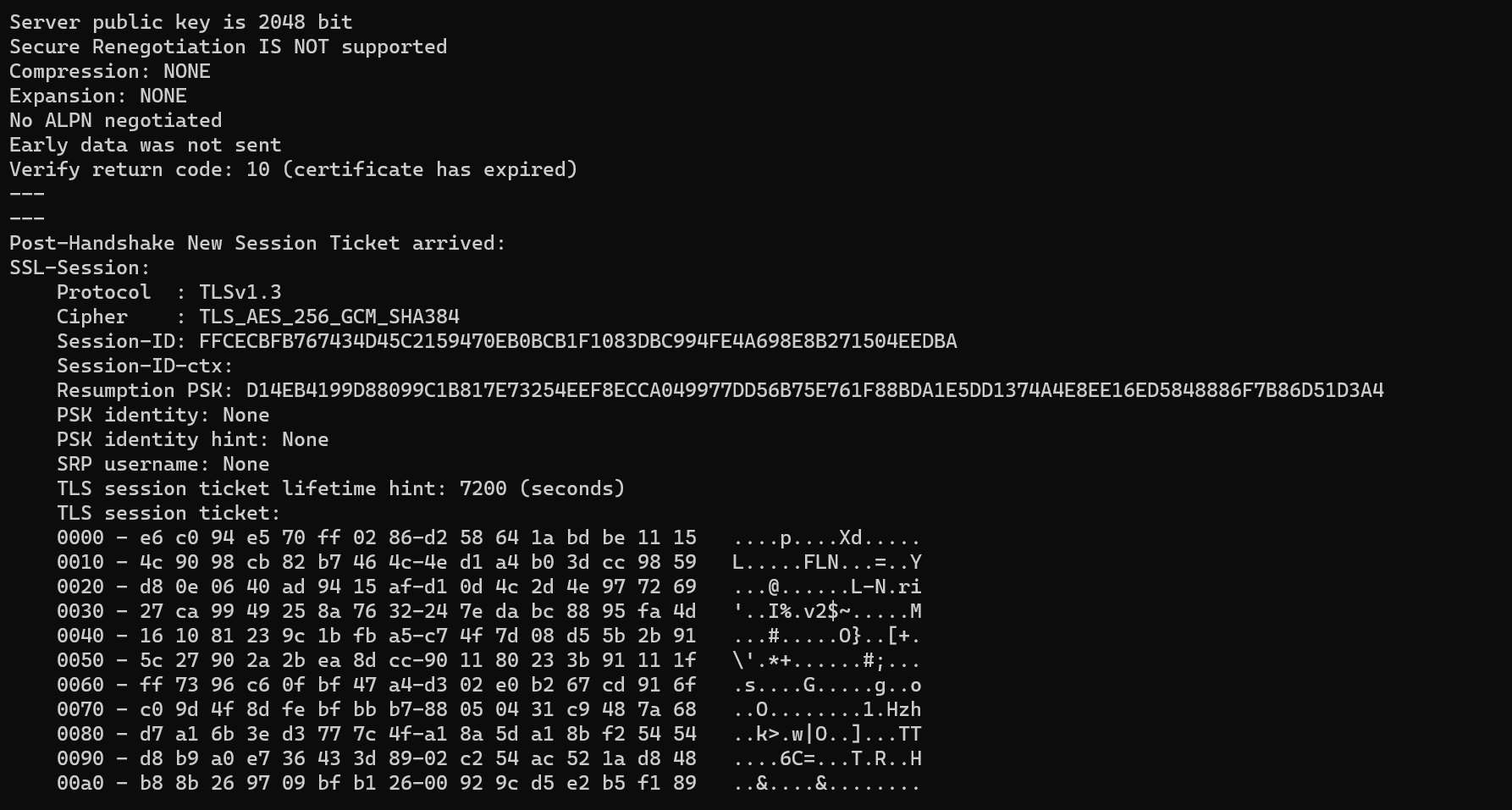
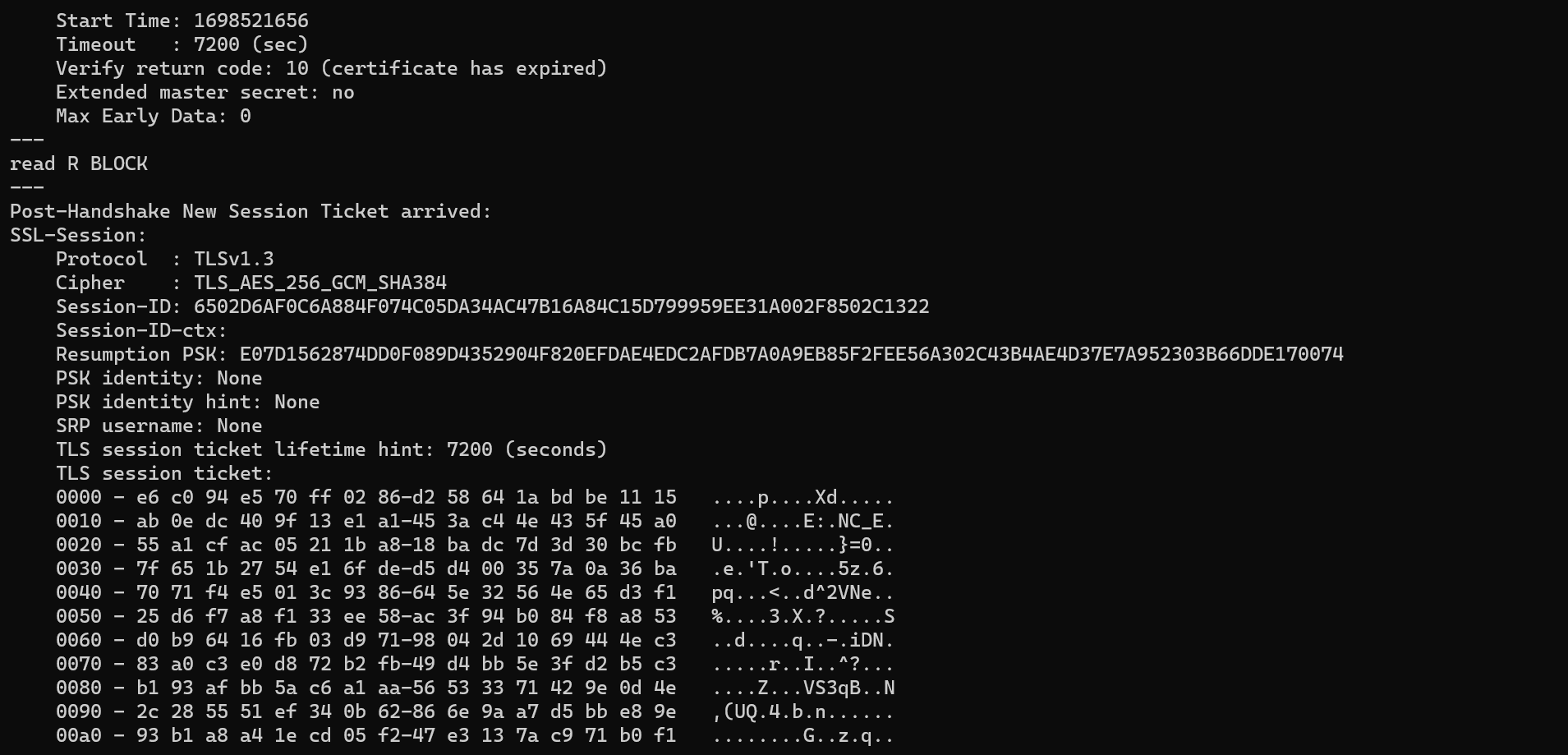
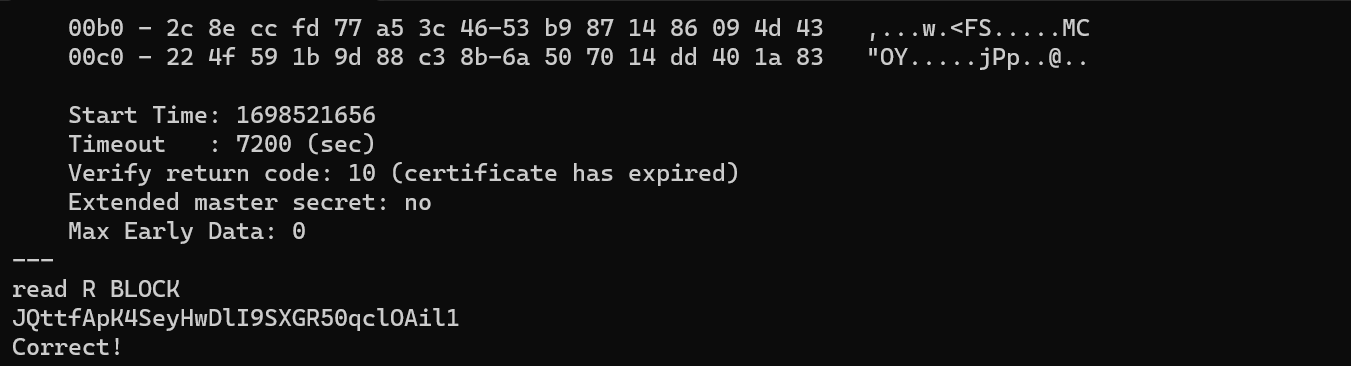
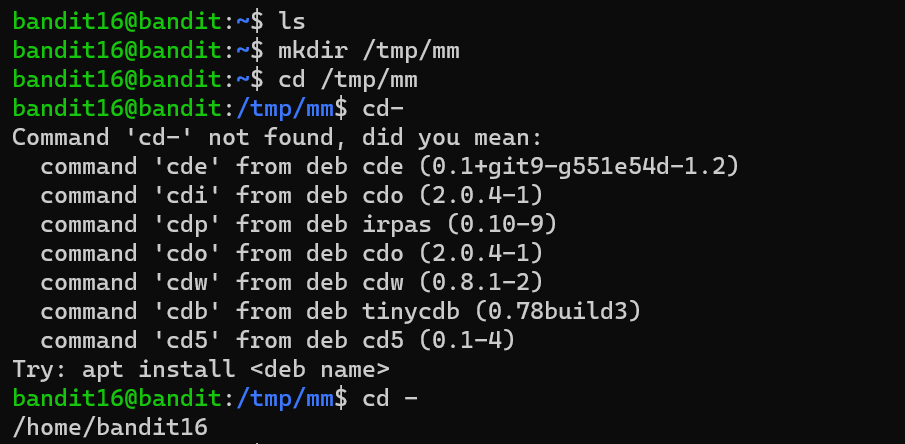
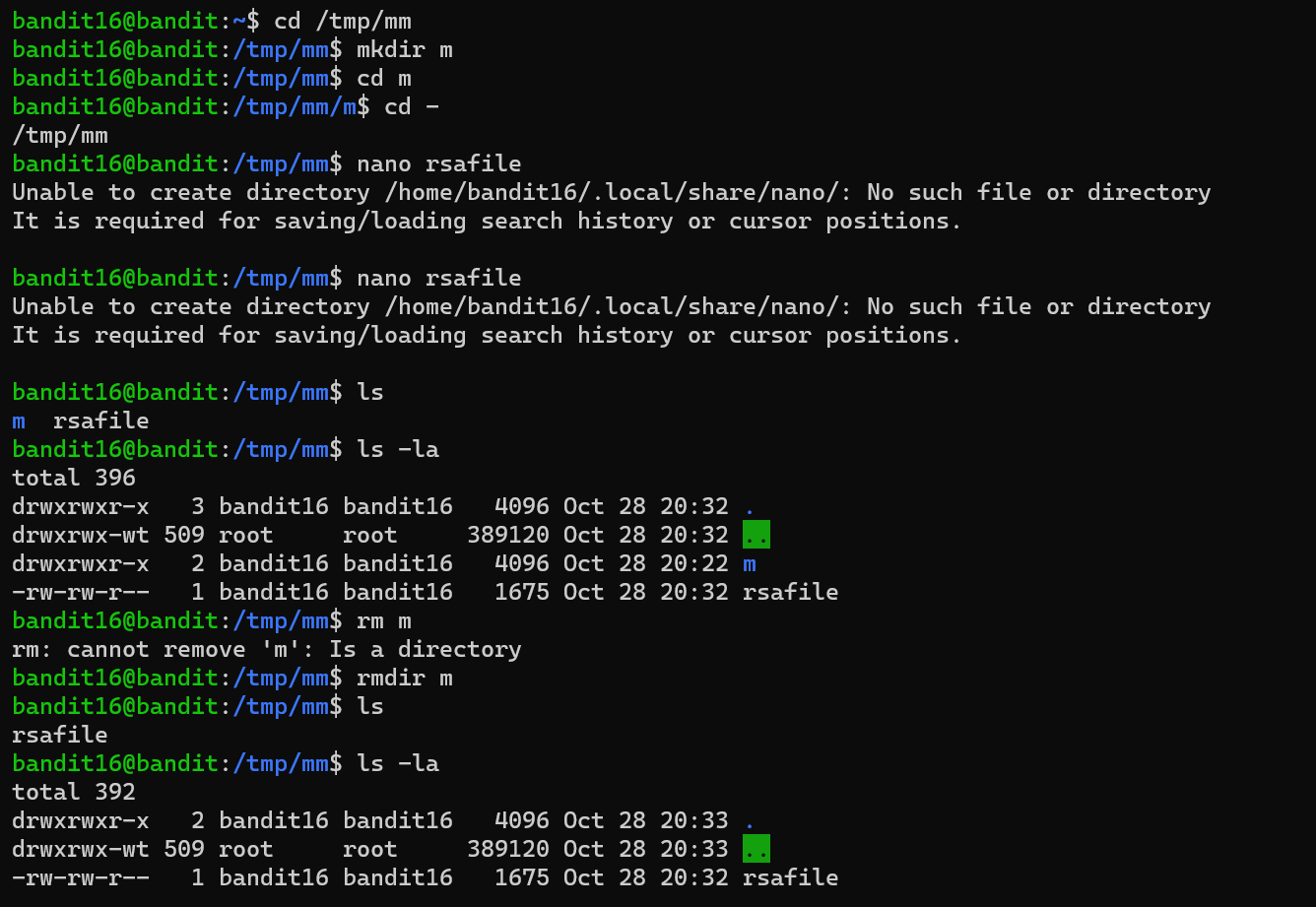
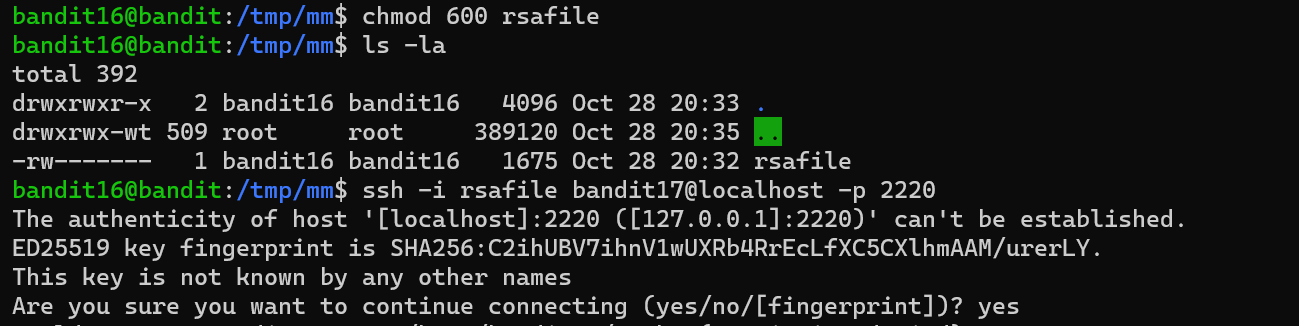
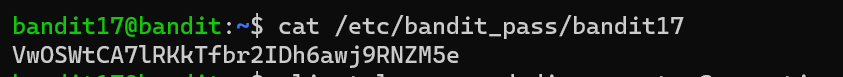
6=4+2: read and write

ssh -i: Selects a file from which the identity (private key) for public

key authentication is read.



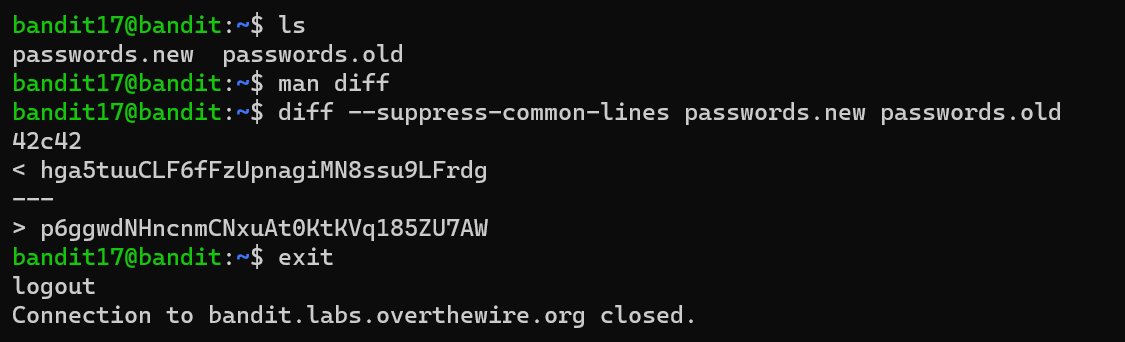


Bandit 17-18

diff - compare files line by line

--suppress-common-lines: removes the common lines.



Bandit 18-19

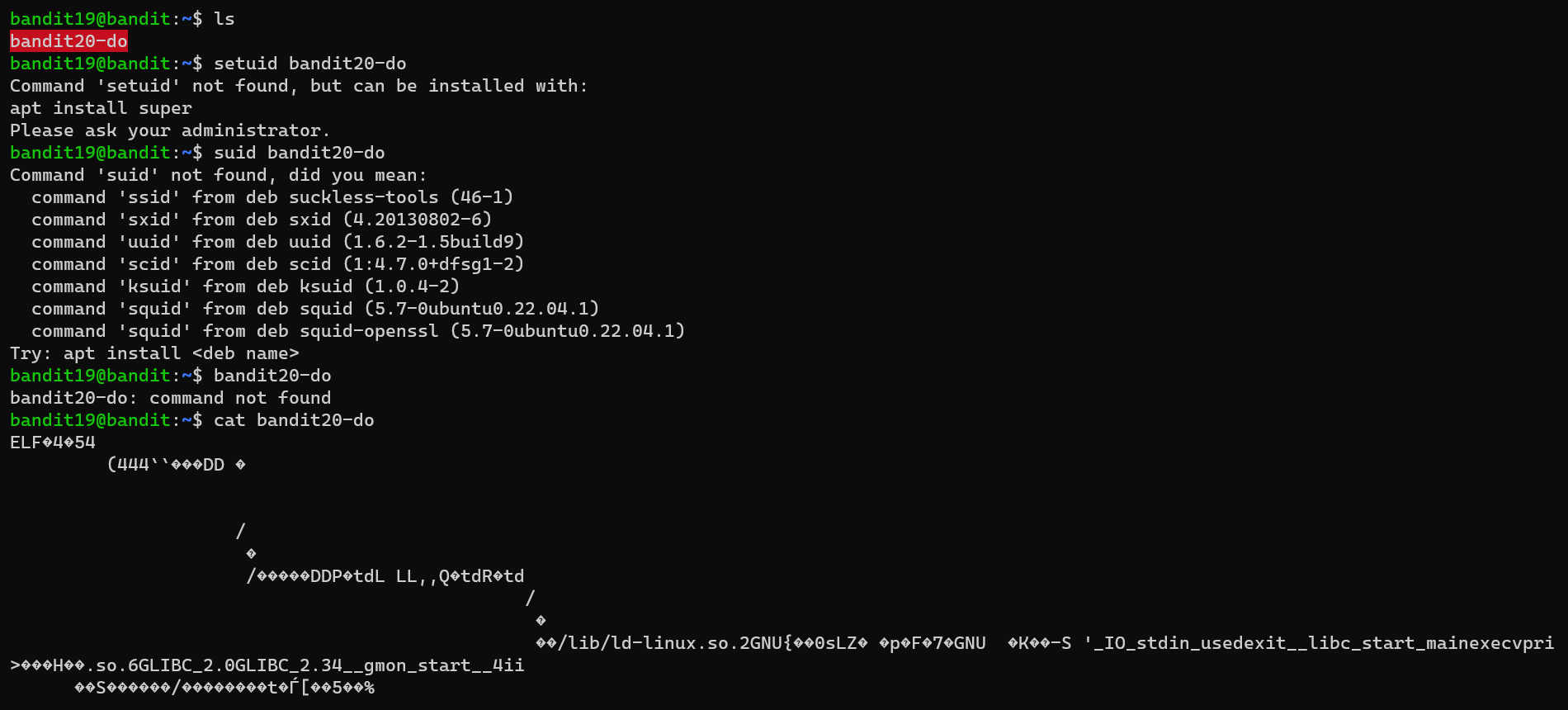
Cat readme: Concatenates the readme file to obtain password.

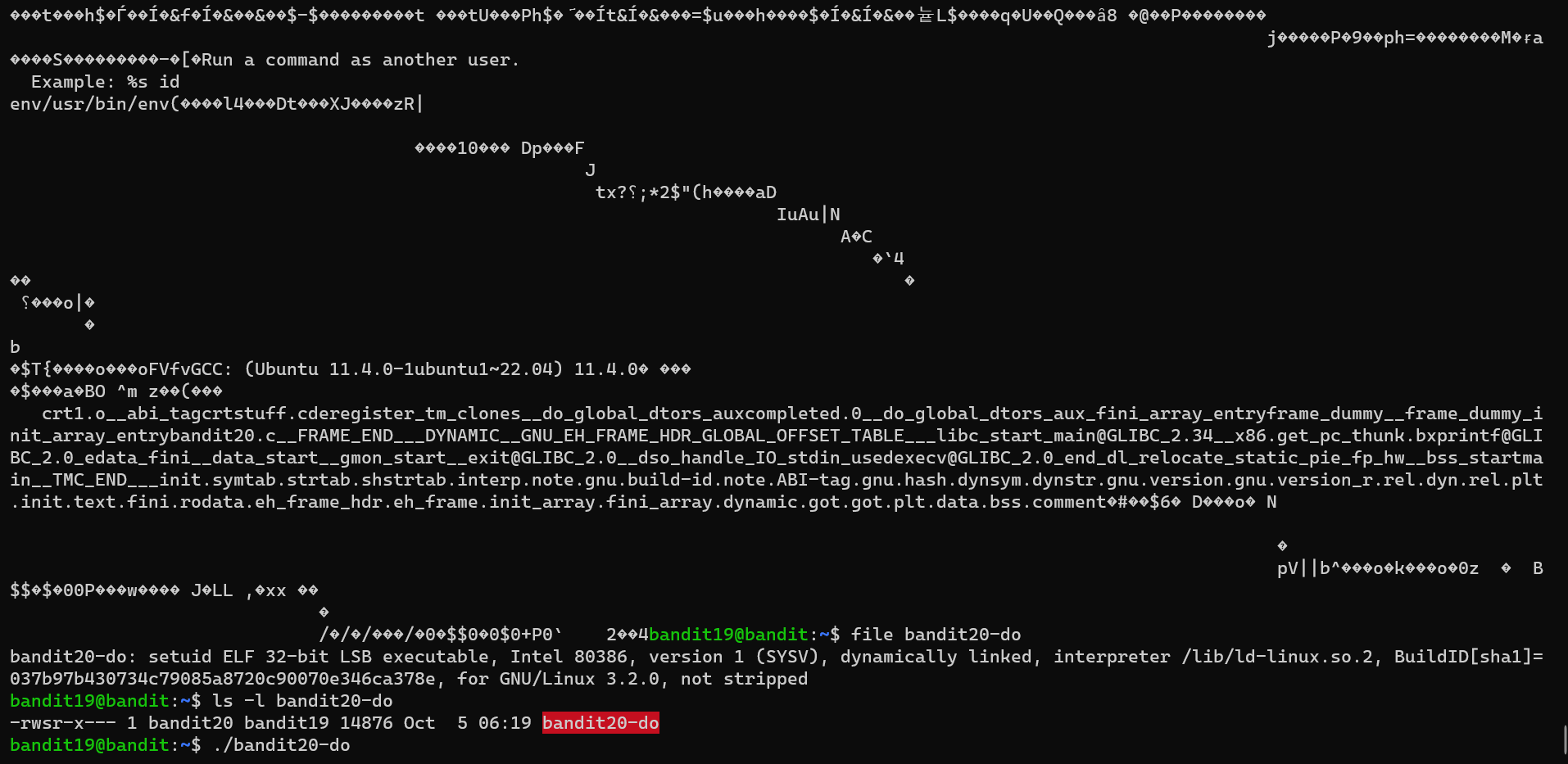


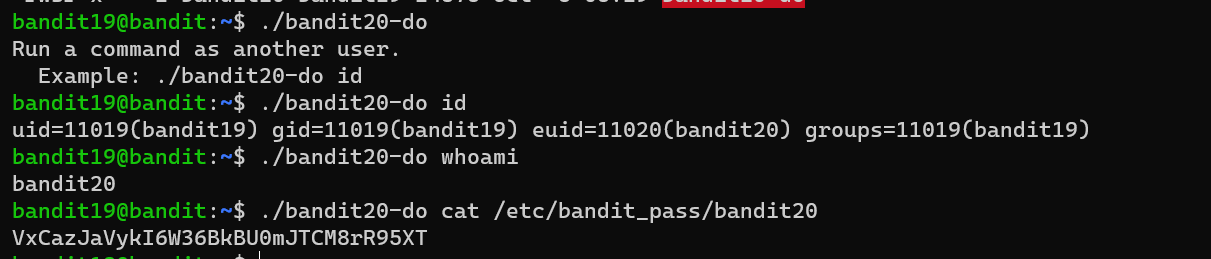
Bandit 19-20

 ./ is a relative path to something in the current directory. The dot is the current directory and the slash is a path delimiter

Whoami: Checks the current id.







Bandit 20-21

nc(netcat) is a simple unix utility which reads and writes data across network connections, using TCP or UDP pro- tocol. It is designed to be a reliable "back-end" tool that can be used directly or easily driven by other programs and scripts. At the same time, it is a fea- ture-rich network debugging and exploration tool, since it can create almost any kind of connection you would need and has several interesting built-in capabilities.

-lvp:

-l: Specify source address to use

-v: verbose

-p: port

