Bandit notes:

Level 0:  ssh bandit0@bandit.labs.overthewire.org -p 2220
Password bandit0 (provided)
Apparently only tries port 22 if not specified with -p flag

Level 0→1: ls → cat readme → ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If

Level 1→2: cat ./- (in order to deal with weird named file) → 263JGJPfgU6LtdEvgfWU1XP5yac29mFx

Level 2→3: cat “spaces in this filename” → MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx

Level 3→4: cd inhere → ls -a → cat ./…Hiding-From-You → 2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ

Level 4→5: cd inhere → for i in $(seq 0 9); do     echo $(file ./-file0${i}); done → -fil07 is ASCII → cat ./-file07 → 4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw

Level 5→6: make temp directory with cd $(mktemp -d) with file path /tmp/tmp.DwOPO1aw4k (randomly generated) → then run ls -laR inhere > /tmp/tmp.DwOPO1aw4k/allfiles.txt → now find what is the right size: cat allfiles.txt | grep "1033" > sized.txt → looks like only one option: .file2 in maybehere07 → HWasnPhtq9AVKe0dmk45nxy20cvUa6EG

Level 6→7: use the find command: find / -type f -user bandit7 -group bandit6 -size 33c → look through the output, find what isn’t permission denied, and see /var/lib/dpkg/info/bandit7.password → morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj

Level 7→8: cat data.txt | grep "millionth" → dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc

Level 8→9: sort data.txt | uniq -c → look for what only appears once: 4CKMh1JI91bUIZZPXDqGanal4xvAg0JM

Level 9→10: look for human readable strings with “strings” command and then search for where a “=” shows up → strings data.txt | grep ".=" → FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey

Level 10→11: base64 -d data.txt → dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr

Level 11→12: cat data.txt | tr '[A-Za-z]' '[N-ZA-Mn-za-m]' → everything is shifted over 13 characters, so here we are mapping the first 13 characters (A-M) to (N-Z) and then the next 13 (N-Z) to (A-M), both for upper and lower → 7x16WNeHIi5YkIhWsfFIqoognUTyj9Q4

Level 12→13: make tmp directory and copy data.txt into it and rename it data_dump → see header of data_dump (1f8b08) which is gzip, so add .gz extension to the output of reversing the hexdump → undo hexdump with xxd -r data_dump > undumped.gz → undumped starts with BZ which is bzip2 (so add extension) → bzip2 -d undumped.bz2 → now can see that there is a data file in there (data4.bin) so use tar to extract (add .tar extension): tar -xf undumped.tar → find data5.bin as output → it seems to have data6.bin in it so extract again and get data6.bin → data6.bin doesn't seem to have any file names showing up in it, but it doesn't have either of the gzip or bzip2 headers, so try tar again → now we have data8.bin → xxd data8.bin has header 1f8b08 so use gzip one more time on that → FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn

Level 13→14: find a file called ssh.private key and I made a copy of this key on my computer


-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAxkkOE83W2cOT7IWhFc9aPaaQmQDdgzuXCv+ppZHa++buSkN+
gg0tcr7Fw8NLGa5+Uzec2rEg0WmeevB13AIoYp0MZyETq46t+jk9puNwZwIt9XgB
ZufGtZEwWbFWw/vVLNwOXBe4UWStGRWzgPpEeSv5Tb1VjLZIBdGphTIK22Amz6Zb
ThMsiMnyJafEwJ/T8PQO3myS91vUHEuoOMAzoUID4kN0MEZ3+XahyK0HJVq68KsV
ObefXG1vvA3GAJ29kxJaqvRfgYnqZryWN7w3CHjNU4c/2Jkp+n8L0SnxaNA+WYA7
jiPyTF0is8uzMlYQ4l1Lzh/8/MpvhCQF8r22dwIDAQABAoIBAQC6dWBjhyEOzjeA
J3j/RWmap9M5zfJ/wb2bfidNpwbB8rsJ4sZIDZQ7XuIh4LfygoAQSS+bBw3RXvzE
pvJt3SmU8hIDuLsCjL1VnBY5pY7Bju8g8aR/3FyjyNAqx/TLfzlLYfOu7i9Jet67
xAh0tONG/u8FB5I3LAI2Vp6OviwvdWeC4nOxCthldpuPKNLA8rmMMVRTKQ+7T2VS
nXmwYckKUcUgzoVSpiNZaS0zUDypdpy2+tRH3MQa5kqN1YKjvF8RC47woOYCktsD
o3FFpGNFec9Taa3Msy+DfQQhHKZFKIL3bJDONtmrVvtYK40/yeU4aZ/HA2DQzwhe
ol1AfiEhAoGBAOnVjosBkm7sblK+n4IEwPxs8sOmhPnTDUy5WGrpSCrXOmsVIBUf
laL3ZGLx3xCIwtCnEucB9DvN2HZkupc/h6hTKUYLqXuyLD8njTrbRhLgbC9QrKrS
M1F2fSTxVqPtZDlDMwjNR04xHA/fKh8bXXyTMqOHNJTHHNhbh3McdURjAoGBANkU
1hqfnw7+aXncJ9bjysr1ZWbqOE5Nd8AFgfwaKuGTTVX2NsUQnCMWdOp+wFak40JH
PKWkJNdBG+ex0H9JNQsTK3X5PBMAS8AfX0GrKeuwKWA6erytVTqjOfLYcdp5+z9s
8DtVCxDuVsM+i4X8UqIGOlvGbtKEVokHPFXP1q/dAoGAcHg5YX7WEehCgCYTzpO+
xysX8ScM2qS6xuZ3MqUWAxUWkh7NGZvhe0sGy9iOdANzwKw7mUUFViaCMR/t54W1
GC83sOs3D7n5Mj8x3NdO8xFit7dT9a245TvaoYQ7KgmqpSg/ScKCw4c3eiLava+J
3btnJeSIU+8ZXq9XjPRpKwUCgYA7z6LiOQKxNeXH3qHXcnHok855maUj5fJNpPbY
iDkyZ8ySF8GlcFsky8Yw6fWCqfG3zDrohJ5l9JmEsBh7SadkwsZhvecQcS9t4vby
9/8X4jS0P8ibfcKS4nBP+dT81kkkg5Z5MohXBORA7VWx+ACohcDEkprsQ+w32xeD
qT1EvQKBgQDKm8ws2ByvSUVs9GjTilCajFqLJ0eVYzRPaY6f++Gv/UVfAPV4c+S0
kAWpXbv5tbkkzbS0eaLPTKgLzavXtQoTtKwrjpolHKIHUz6Wu+n4abfAIRFubOdN
/+aLoRQ0yBDRbdXMsZN/jvY44eM+xRLdRVyMmdPtP8belRi2E2aEzA==
-----END RSA PRIVATE KEY-----


Then I tried to ssh into bandit14 with the private key: ssh -i Downloads/banditprivatekey14.txt bandit14@bandit.labs.overthewire.org -p 2220 → but it said the permissions were too open and didn't work → so I changed the permissions so that only I can read it: chmod 600 Downloads/banditprivatekey.txt → and then tried the ssh command again and got in

Level 14→15: found an .ssh folder and in it a file called authorizedkeys which is the following:
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDGSQ4TzdbZw5PshaEVz1o9ppCZAN2DO5cK/6mlkdr75u5KQ36CDS1yvsXDw0sZrn5TN5zasSDRaZ568HXcAihinQxnIROrjq36OT2m43BnAi31eAFm58a1kTBZsVbD+9Us3A5cF7hRZK0ZFbOA+kR5K/lNvVWMtkgF0amFMgrbYCbPpltOEyyIyfIlp8TAn9Pw9A7ebJL3W9QcS6g4wDOhQgPiQ3QwRnf5dqHIrQclWrrwqxU5t59cbW+8DcYAnb2TElqq9F+BiepmvJY3vDcIeM1Thz/YmSn6fwvRKfFo0D5ZgDuOI/JMXSKzy7MyVhDiXUvOH/z8ym+EJAXyvbZ3 rudy@localhost

But that doesn't look like the standard keys. Last level it said that bandit14 had its password in the **/etc/bandit_pass/bandit14** file:
MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS → now want to use this password to connect to localhost → nc can be used to connect to a host and port which is what we want, with this `nc [<options>] <host> <port>` command structure → so run nc localhost 30000 and enter the password, and get 8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo

Level 15→16: using openssl (command structure looks like:  openssl s_client -connect host:port) to run openssl s_client -connect localhost:30001 → then enter the password above → kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx

Level 16→17: use nmap to look through ports (`nmap -p80-443 localhost`, eg) → so run nmap -p31000-32000 localhost

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-20 16:02 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00017s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
31046/tcp open  unknown
31518/tcp open  unknown
31691/tcp open  unknown
31790/tcp open  unknown
31960/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```