Bandit Level 16 - Level 17

The password for next level is stored on the localhost on a port from the range 31000 to 32000. Only one of these ports speak SSL/TLS and is listening.

We can use two different commands to achieve this. Lets check for listening ports.

```
bandit16@bandit:~$ nc -zv localhost 31000-32000
```

If we run the above, every single port from 31000 to 32000 will be listed. If it is listening it will say 'succeeded', else it way say 'connection refused'. We can either wade through the entire list to look for listening ports or pipe the results to a grep to only look for 'succeeded' connections.

```
bandit16@bandit:~$ nc -zv localhost 31000-32000 2>&1 | grep succeeded
Connection to localhost (127.0.0.1) 31046 port [tcp/*] succeeded!
Connection to localhost (127.0.0.1) 31518 port [tcp/*] succeeded!
Connection to localhost (127.0.0.1) 31691 port [tcp/*] succeeded!
Connection to localhost (127.0.0.1) 31790 port [tcp/*] succeeded!
Connection to localhost (127.0.0.1) 31960 port [tcp/*] succeeded!
```

So 5 ports are listening. The next step is to determine which port is SSL/TLS. We can use openssl to achieve this. We can use openssl to inspect each listening port.

```
openssl s_client localhost:31790
```

The only problem with this, is that its slow. Another way to achieve this is to run nmap.

```
bandit16@bandit:~$ nmap -sV localhost -p 31000-32000
```

After a minute or so, it outputs the following.

```
PORT      STATE SERVICE     VERSION
31046/tcp open  echo
31518/tcp open  ssl/echo
31691/tcp open  echo
31790/tcp open  ssl/unknown
31960/tcp open  echo
```

Since we are looking for SSL/TLS connection, port 31790 looks like it is the right answer.

So, lets use openssl to connect and submit level 16 password to hopefully retrieve level 17 password. We can pass the password straight to openssl.

```
bandit16@bandit:~$ echo "kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx" | openssl
s_client -quiet -connect localhost:31790
Can't use SSL_get_servername
depth=0 CN = SnakeOil
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN = SnakeOil
verify return:1
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMlOJf7+BrJObArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl87ORiO+rW4LCDCNd2lUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW3OekePQAzL0VUYbW
JGTi65CxbCnzc/w4+mqQyvmzpWtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XFOJuaQIDAQABAoIBABagpxpM1aoLWfvD
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNuDE6SFthOar69jp5RlLwD1NhPx3iBl
J9nOM8OJ0VToum43UOS8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52yOQ9qOkwFTEQpjtF4uNtJom+asvlpmS8A
vLY9r60wYSvmZhNqBUrj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOmama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRhORT
8c8hAuRBb2G82so8vUHk/fur85OEfc9TncnCY2crpoqsghifKLxrLgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyc9P2jGRNtMSkCgYEAypHd
HCctNi/FwjulhttFx/rHYKhLidZDFYeiE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enCIvGCSx+X3l5SiWg0A
R57hJglezIiVjv3aGwHwvlZvtszK6zV6oXFAu0ECgYAbjo46T4hyP5tJi93V5HDi
Ttiek7xRVxUl+iU7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFMLy9FL2m9oQWCg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB3OhYimtiG2Cg5JCqIZFHxD6MjEGOiu
L8ktHMPvodBwNsSBULpG0QKBgBAplTfC1HOnWiMGOU3KPwYWt0O6CdTkmJOmL8Ni
blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU
YOdjHdSOoKvDQNWu6ucyLRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyzRqaM
77pBAoGAMmjmIJdjp+Ez8duyn3ieo36yrttF5NSsJLAbxFpdlc1gvtGCWW+9Cq0b
dxviW8+TFVEBl1O4f7HVm6EpTscdDxU+bCXWkfjuRb7Dy9GOtt9JPsX8MBTakzh3
```

```
vBgsyi/sN3RqRBcGU40fOoZyfAMT8s1m/uYv52O6IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----
```

We are presented with a RSA key. Lets create a temp directory, create a file and paste the RSA key in there.

```
bandit16@bandit:~$ mktemp -d
/tmp/tmp.rvp6aole60
bandit16@bandit:~$ cd /tmp//tmp.rvp6aole60
bandit16@bandit:/tmp/tmp.rvp6aole60$ touch sshkey17.private
bandit16@bandit:/tmp/tmp.rvp6aole60$ nano
```

Next we need to change the permission for the sshkey17. Set permissions to user only access. We can use number notation to achieve this.

```
bandit16@bandit:/tmp/tmp.rvp6aole60$ chmod 700 sshkey17.private
```

Lets SSH into bandit17 with the newly created key with new persmissions.

```
bandit16@bandit:/tmp/tmp.rvp6aole60$ ssh -i sshkey17.private
bandit17@bandit.labs.overthewire.org -p 2220
```

Stay logged in to find password for next level