- **BANDIT 12-13**

  Here, I learned the concept of hexdumps. A hexdump is used when data cannot be represented as a string and hence is not readable.

  Commands learnt: mkdir – used to create a new directory
  cp- used to copy data from the directory
  xxd – creates hexdumps , -r flag used reverts the hexdump
  gzip- command used to compress or decompress files
  bzip2 – another command to compress or decompress files
  tar- creates archive files

```
bandit12@bandit:~$ cat data.txt
00000000: 1f8b 0808 6855 1e65 0203 6461 7461 322e  ....hU.e..data2.
00000010: 6269 6e00 013d 02c2 fd42 5a68 3931 4159  bin..=...BZh91AY
00000020: 2653 5948 1b32 0200 0019 ffff faee cff7  &SYH.2..........
00000030: f6ff e4f7 bfbc ffff bff7 ffb9 39ff 7ffb  ............9...
00000040: bd31 eeff b9fb fbbb b9bf f77f b001 3b2c  .1.............;,
00000050: d100 0d03 d200 6868 0d00 0069 a00d 0340  ......hh...i...@
00000060: 1a68 00d0 0d01 a1a0 0001 a680 0003 46d4  .h............F.
00000070: 6434 3234 611a 340d 07a4 c351 068f 5000  d424a.4....Q..P.
00000080: 069a 0680 0000 0006 8006 8da4 681a 6868  ............h.hh
00000090: 0d06 8d00 6834 3400 d07a 9a00 01a0 0341  ....h44..z.....A
000000a0: ea1e a190 da40 3d10 ca68 3468 6800 00c8  .....@=..h4hh...
000000b0: 1a1a 1b50 0683 d434 d069 a0d0 3100 d000  ...P...4.i..1...
000000c0: 001e a680 00d0 1a00 d0d0 6864 d0c4 d0d0  ..........hd....
000000d0: 000c 8641 7440 0108 032e 86b4 4cf0 22bb  ...At@......L.".
bandit12@bandit:~$ cp data.txt /tmp/alif
bandit12@bandit:~$ cd /tmp/alif
bandit12@bandit:/tmp/alif$ ls
data.txt
bandit12@bandit:/tmp/alif$ xxd -r data.txt > data
bandit12@bandit:/tmp/alif$ ls
data  data.txt
bandit12@bandit:/tmp/alif$ file data
data: gzip compressed data, was "data2.bin", last modified: Thu Oct
bandit12@bandit:/tmp/alif$ mv data file.gz
bandit12@bandit:/tmp/alif$ gzip -d file.gz
bandit12@bandit:/tmp/alif$ ls
data.txt  file
bandit12@bandit:/tmp/alif$ file file
file: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/alif$ mv file file.bz2
bandit12@bandit:/tmp/alif$ bzip2 -d file.bz2
bandit12@bandit:/tmp/alif$ ls
data.txt  file
bandit12@bandit:/tmp/alif$ file file
file: gzip compressed data, was "data4.bin", last modified: Thu Oct
bandit12@bandit:/tmp/alif$ mv file file.gz
bandit12@bandit:/tmp/alif$ gzip -d file.gz
bandit12@bandit:/tmp/alif$ ls
data.txt  file
bandit12@bandit:/tmp/alif$ file file
file: POSIX tar archive (GNU)
bandit12@bandit:/tmp/alif$ mv file file.tar
bandit12@bandit:/tmp/alif$ tar xf file.tar
bandit12@bandit:/tmp/alif$ ls
data5.bin  data.txt  file.tar
bandit12@bandit:/tmp/alif$ file data5.bin
data5.bin: POSIX tar archive (GNU)
```

```
bandit12@bandit:/tmp/alif$ mv data5.bin data6.tar
bandit12@bandit:/tmp/alif$ tar -xf data6.tar
bandit12@bandit:/tmp/alif$ ls
data6.bin  data6.tar  data.txt
bandit12@bandit:/tmp/alif$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/alif$ mv data6.bin data7.bz
bandit12@bandit:/tmp/alif$ bzip2 -d data7.bz
bandit12@bandit:/tmp/alif$ ls
data6.tar  data7  data.txt
bandit12@bandit:/tmp/alif$ file data7
data7: POSIX tar archive (GNU)
bandit12@bandit:/tmp/alif$ mv data7 data8.tar
bandit12@bandit:/tmp/alif$ tar -xf data8.tar
bandit12@bandit:/tmp/alif$ ls
data6.tar  data8.bin  data8.tar  data.txt
bandit12@bandit:/tmp/alif$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last m
bandit12@bandit:/tmp/alif$ mv data8.bin data9.gz
bandit12@bandit:/tmp/alif$ gzip -d data9.gz
bandit12@bandit:/tmp/alif$ ls
data6.tar  data8.tar  data9  data.txt
bandit12@bandit:/tmp/alif$ file data9
data9: ASCII text
bandit12@bandit:/tmp/alif$ tmp/alif$ cat data9
-bash: tmp/alif$: No such file or directory
bandit12@bandit:/tmp/alif$
bandit12@bandit:/tmp/alif$ cat data9
The password is wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw
bandit12@bandit:/tmp/alif$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

- **BANDIT 13-14**

  The password for this level is stored in etc/bandit_pass/bandit14 and can only be logged in by bandit 14.

  In this level we don't directly get the password for the next level , instead a private ssh key which can be used to login to the next level.

  Commands learnt : whoami – helps to find out the current logged in user.

```
bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ head sshkey.private
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAxkkOE83W2cOT7IWhFc9aPaaQmQDdgzuXCv+ppZHa++buSkN+
ggOtcr7Fw8NLGa5+Uzec2rEgOWmeevB13AIoYpOMZyETq46t+jk9puNwZwIt9XgB
ZufGtZEwWbFWw/vVLNwOXBe4UWStGRWzgPpEeSv5Tb1VjLZIBdGphTIK22Amz6Zb
ThMsiMnyJafEwJ/T8PQO3myS91vUHEuoOMAzoUID4kNOMEZ3+XahyKOHJVq68KsV
ObefXG1vvA3GAJ29kxJaqvRfgYnqZryWN7w3CHjNU4c/2Jkp+n8LOSnxaNA+WYA7
jiPyTFOis8uzMlYQ4l1Lzh/8/MpvhCQF8r22dwIDAQABAoIBAQC6dWBjhyEOzjeA
J3j/RWmap9M5zfJ/wb2bfidNpwbB8rsJ4sZIDZQ7XuIh4LfygoAQSS+bBw3RXvzE
pvJt3SmU8hIDuLsCjL1VnBY5pY7Bju8g8aR/3FyjyNAqx/TLfzlLYfOu7i9Jet67
xAhOtONG/u8FB5I3LAI2Vp6OviwvdWeC4nOxCthldpuPKNLA8rmMMVRTKQ+7T2VS
bandit13@bandit:~$ whoami
bandit13
bandit13@bandit:~$ cat /etc/bandit_pass/bandit14
cat: /etc/bandit_pass/bandit14: Permission denied
bandit13@bandit:~$ ssh -i sshkey.private bandit14@localhost -p 2220
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit13/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit13/.ssh/known_hosts).
```

```
bandit14@bandit:~$ whoami
bandit14
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq
bandit14@bandit:~$ exit
logout
Connection to localhost closed.
bandit13@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

- **BANDIT 14-15**

```
bandit14@bandit:~$ ls
bandit14@bandit:~$ telnet localhost 30000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq
Correct!
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt

Connection closed by foreign host.
bandit14@bandit:~$ pc localost 30000
Command 'pc' not found, but can be installed with:
apt install fp-compiler-3.2.2
Please ask your administrator.
bandit14@bandit:~$ nc localhost 30000
fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq
Correct!
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt

exit
bandit14@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

The password for the next level can be retrieved by submitting the password of current level to port 30000 on localhost.

Commands learnt : nc (netcat) – allows to read and write data over a network connection.

- **BANDIT 15-16**

```
bandit15@bandit:~$ openssl s_client -connect localhost:30001
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 CN = localhost
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN = localhost
verify error:num=10:certificate has expired
notAfter=Oct 26 02:11:37 2023 GMT
verify return:1
depth=0 CN = localhost
notAfter=Oct 26 02:11:37 2023 GMT
verify return:1
---
Certificate chain
 0 s:CN = localhost
   i:CN = localhost
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA1
   v:NotBefore: Oct 26 02:10:37 2023 GMT; NotAfter: Oct 26 02:11:37 2023 GMT
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIDCzCCAfOgAwIBAgIEBv+T9TANBgkqhkiG9w0BAQUFADAUMRIwEAYDVQQDDAls
b2NhbGhvc3QwHhcNMjMxMDI2MDIxMDM3WhcNMjMxMDI2MDIxMTM3WjAUMRIwEAYD
VQQDDAlsb2NhbGhvc3QwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC2
read R BLOCK
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt
Correct!
JQttfApK4SeyHwDlI9SXGR50qclOAil1

closed
bandit15@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

The password for the next level can be retrieved by submitting the password of the current level to port 30001 on localhost using SSL encryption.
Since the task states that the password can be retrieved using SSL encryption, I connect to the localhost server with the OpenSSL client and send the password from this level. The server then sends back the password for the next level.

- **BANDIT 16-17**

```
bandit16@bandit:~$ nmap -sV -T4 -p 31000-32000 localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-27 17:07 UTC
Stats: 0:01:13 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 83.33% done; ETC: 17:09 (0:00:15 remaining)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00010s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE     VERSION
31046/tcp open  echo
31337/tcp open  tcpwrapped
31518/tcp open  ssl/echo
31691/tcp open  echo
31790/tcp open  ssl/unknown
31960/tcp open  echo
1 service unrecognized despite returning data. If you know the service/versi
SF-Port31790-TCP:V=7.80%T=SSL%I=7%D=10/27%Time=653BEE7D%P=x86_64-pc-linux-
SF:gnu%r(GenericLines,31,"Wrong!\x20Please\x20enter\x20the\x20correct\x20c
SF:urrent\x20password\n")%r(GetRequest,31,"Wrong!\x20Please\x20enter\x20th
SF:e\x20correct\x20current\x20password\n")%r(HTTPOptions,31,"Wrong!\x20Ple
SF:ase\x20enter\x20the\x20correct\x20current\x20password\n")%r(RTSPRequest
SF:,31,"Wrong!\x20Please\x20enter\x20the\x20correct\x20current\x20password
SF:\n")%r(Help,31,"Wrong!\x20Please\x20enter\x20the\x20correct\x20current\
SF:x20password\n")%r(SSLSessionReq,31,"Wrong!\x20Please\x20enter\x20the\x2
SF:0correct\x20current\x20password\n")%r(TerminalServerCookie,31,"Wrong!\x
SF:20Please\x20enter\x20the\x20correct\x20current\x20password\n")%r(TLSSes
SF:sionReq,31,"Wrong!\x20Please\x20enter\x20the\x20correct\x20current\x20p
SF:assword\n")%r(Kerberos,31,"Wrong!\x20Please\x20enter\x20the\x20correct\
SF:x20current\x20password\n")%r(FourOhFourRequest,31,"Wrong!\x20Please\x20
SF:enter\x20the\x20correct\x20current\x20password\n")%r(LPDString,31,"Wron
SF:g!\x20Please\x20enter\x20the\x20correct\x20current\x20password\n")%r(LD
SF:APSearchReq,31,"Wrong!\x20Please\x20enter\x20the\x20correct\x20current\
SF:x20password\n")%r(SIPOptions,31,"Wrong!\x20Please\x20enter\x20the\x20co
SF:rrect\x20current\x20password\n");

Service detection performed. Please report any incorrect results at https://
Nmap done: 1 IP address (1 host up) scanned in 98.58 seconds
```

```
    Start Time: 1698426729
    Timeout   : 7200 (sec)
    Verify return code: 10 (certificate has expired)
    Extended master secret: no
    Max Early Data: 0
---
read R BLOCK
JQttfApK4SeyHwDlI9SXGR50qclOAil1
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMlOJf7+BrJObArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl87ORiO+rW4LCDCNd2lUvLE/GL2GWyuKNOK5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW3OekeFQAzLOvUYbW
JGTi65CXbCnzc/w4+mqGyvmzpWtMAzJTzAzOxNbkR2MBGy5xDLrjpOLWN6sK7WNX
xOYVztz/zbIkPjfkU1jHS+9EbVNj+D1XFOJuaQIDAQABAoIBABagpxpM1aoLWfVD
KHcj1OnqcoBc4oE11aFYQwik7xfW+24pRNuDE6SFthOar69jp5RlLwD1NhPx3iBl
J9nOM8OJOVTourn43UOS8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd
d8WErYOgPxun8pbJLmxkAtWNhpMvfe0O5Ovk9TL5wqbu9A1bssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZkufD52yOQ9qOkwFTEQpjtF4uNtJom+asVlpmS8A
vLY9r6OwYSvmzhNqBUrjF7lYctXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOmama
+TOWWgECgYEA8JtPxPQGRJ+IQkX262jM3dEIkza8ky5moIwUqYdsxONxHgRRhORT
8c8hAuRBb2G82so8vUHk/fur85OEfc9TncnCY2crpoqsghifKLxrLgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyc9P2jGRNtMSkCgYEAypHd
HCctNi/FwjulhttFx/rHYKhLidZDFYeiE/v45bN4yFm8x7R/bOiE7KaszX+Exdvt
SghaTdcGOKnyw1bpJVyusaVPzpaJMjdJ6tcFhVAbAjm7enCIvGCSx+X3l5SiWgOA
R57hIJgleziiVjv3aGwHwvlZvtc2k62V6oXFAuOECgYAbjo46T4hyP5tJi93V5HDi
Ttiek7xRVxUl+iU7rWkGAXFpMLFteQESRr7PJ/lemmEY5eTDAFMLy9FL2m9oQWCg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB3OhYimtiG2Cg5JCqIZFHxD6MjEGOiu
L8ktHMPvodBwNsSBULpGOQKBgBAplTfC1HOnwiMGOU3KPwYWtOO6CdTkmJOmL8Ni
blh9elyZ9FsGxsgtRBXRsqXuZ7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU
YOdjHdSOoKvDQNWu6ucyLRAWFuISeXw9a/9p7ftpxmOTSgyVmfLF2MIAEwyzRqaM
77pBAoGAMmjmIJdjp+Ez8duyn31eo36yrttF5NSsjLAbxFpdlc1gvtGCWW+9CqOb
dXv1W8+TFVEBl1O4f7HVm6EpTscdDxU+bCXWkfjuRb7Dy9GOtt9JPsX8MBTakzh3
vBgsYi/sN3RqRBcGU4OfOoZyfAMT8s1m/uYV52O6IgeUz/ujbjY=
-----END RSA PRIVATE KEY-----

closed
bandit16@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

The credentials for the next level can be retrieved by submitting the password of the current level to a port on localhost in the range 31000 to 32000. Nmap is a network scanner. It can do Host Discovery, Port Scanning, Version Detection (Service Detection) and a lot more. The -sV flag lets us do a service/version detection scan.

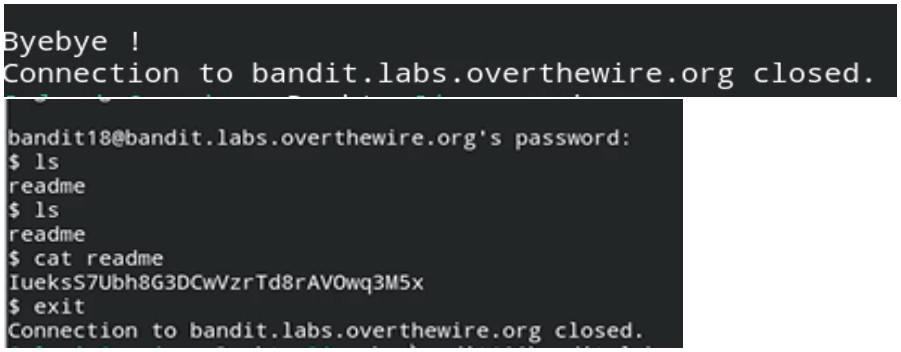
- **BANDIT 17-18**

```
bandit17@bandit:~$ man diff
bandit17@bandit:~$ diff passwords.old passwords.new
42c42
< hlbSBPAWJmL6WFDb06gpTx1pPButblOA
---
> kfBf3eYk5BPBRzwjqutbbfE887SVc5Yd
bandit17@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
[alexis@manjaro Desktop]$ ssh bandit18@bandit.labs.overthewire.org -p 2220
```

There are 2 files in the homedirectory: passwords.old and passwords.new. The password for the next level is in passwords.new and is the only line that has been changed between passwords.old and passwords.new. The diff command prints the

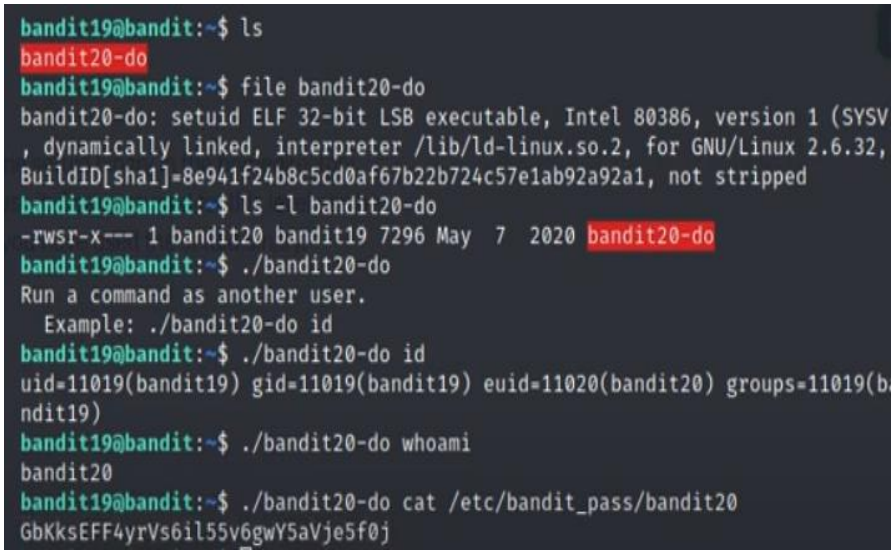
difference between two files. Since I wrote ‘passwords.new’ in second place, the new password is also printed in the second part.

- **BANDIT 18-19**



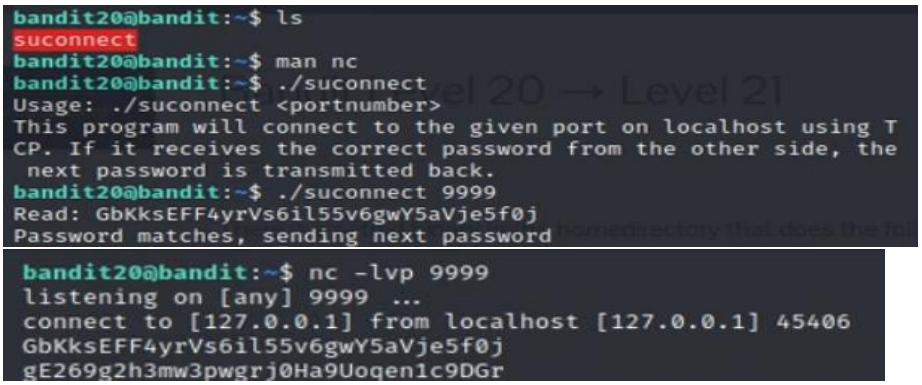
The password for the next level is stored in a file readme in the homedirectory. Unfortunately, someone has modified. bashrc to log you out when you log in with SSH. ‘.bashrc’ is a file that is run every time a terminal is loaded. This means it is also run when logging in through SSH because this also loads a terminal.

- **BANDIT 19-20**



In this case, the owner is badit20 and the group is bandit19, this with ‘-rwsr-x—’ means the user bandit19 can execute the binary, but the binary is executed as user bandit20. Executing the binary says it simply executes another command as another user (as already explained, this user is bandit20). This means we can access the bandit20 users password file, which can only be read by the user bandit20.

- **BANDIT 20-21**



Using 'netcat', we can create a connection in server mode - which listens for inbound connection. Running the setuid binary means it will connect to our netcat server, receive the password inputted through echo and sends back the next password.

- **BANDIT 21-22**

First, we look at what is in the '/etc/cron.d' folder. Specifically, for this level, I looked at the cronjob 'cronjob_bandit22'. This cronjob runs the /usr/bin/cronjob_bandit22.sh file as bandit22 user. The five stars indicate it is run every minute, every day. This file creates a file in the 'tmp' folder and gives read permission to everyone. Then it copies the input of the bandit22 password file into the newly created file.