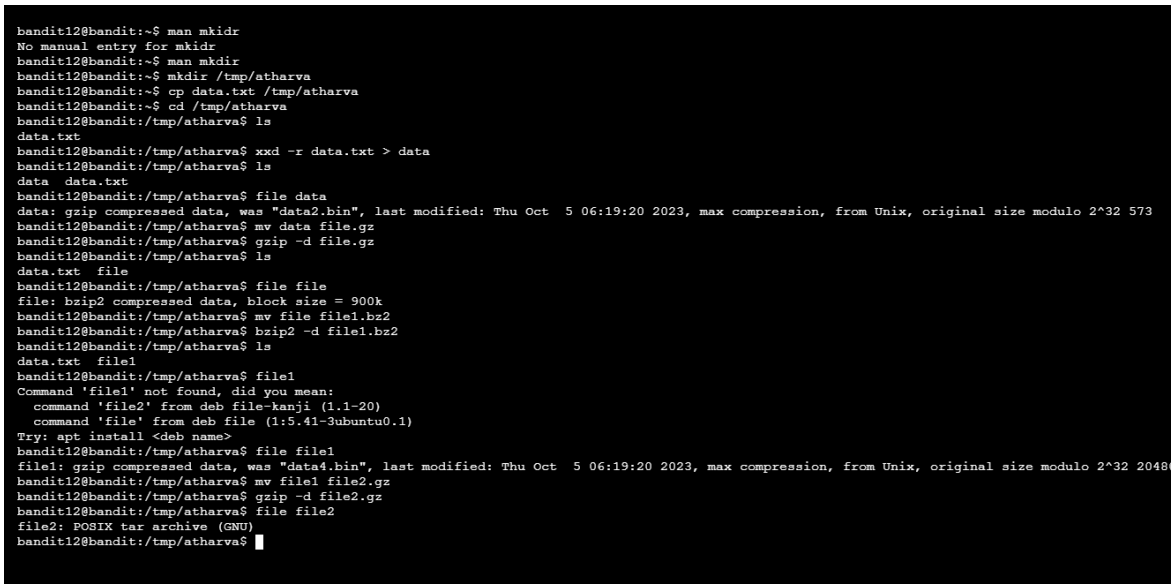
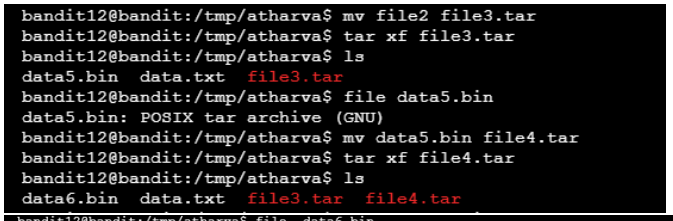
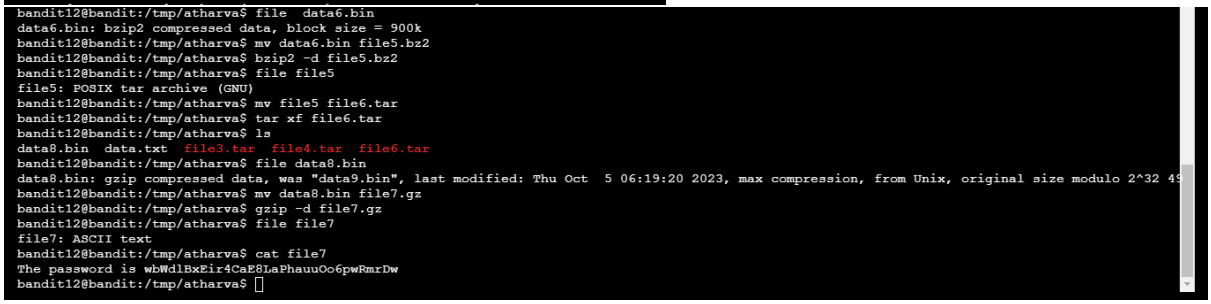
WRITEUP [Bandit Lv12-21]

Lv 12->13

Application used: ssheasy.com







In this, we had to first make our own folder using mkdir command and copy data.txt file over there to get the password, since data.txt is compressed a lot we decompressed it from it's gzip and bzip2 types using gzip -d/ bzip2 -d commands and extracted .tar files until we got the filetype as ASCII from where we received our password as "wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw"

Exit to logout of current bandwit12 and login to bandwit13 using this password

BANDWIT 13->14

In this level we get into bandit13 and see the file sshkey.private in it, since pass is visible to only bandit14 users we login to bandit14 using this key, ssh -i helps to read the private key as an identification command through which we can login to bandit14

In bandit14 in order to get the password we have to use cat command with the file where password is stored and we get

“fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq”

Lvl 14->15

```
bandit14@bandit:~$ man nc
bandit14@bandit:~$ nc localhost 30000
fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq
Wrong! Please enter the correct current password
fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq
bandit14@bandit:~$ nc localhost 30000
fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq
Correct!
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt
```

In this, we learn the nc command, [netcat helps in port scanning TCP and UDP connections etc], we have to switch to port 30000 and paste password of bandit14 there to retrieve password of bandit15

using nc we switch to port 30000 and then paste the password of bandit14 successfully getting password of bandit15 which is

“jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt”

Lvl 15->16

```
   command 'sn' from deb mono-devel (6.8.0.105+dfsg-3.2)
   command 'msb' from deb mysql-sandbox (3.2.05-1)
   command 'mhn' from deb mailutils-mh (1:3.14-1)
   command 'mhn' from deb nmh (1.7.1-11)
   command 'mon' from deb mon (1.3.6-2)
   command 'mvn' from deb maven (3.6.3-5)
   command 'mln' from deb mmv (1.01b-19build1)
Try: apt install <deb name>
bandit15@bandit:~$ man ncat
bandit15@bandit:~$ man ncat | grep ssl
                --ssl                   Connect or listen with SSL
                --ssl-cert              Specify SSL certificate file (PEM) for listening
                --ssl-key               Specify SSL private key (PEM) for listening
                --ssl-verify            Verify trust and domain name of certificates
                --ssl-trustfile         PEM file containing trusted SSL certificates
                --ssl-ciphers           Cipherlist containing SSL ciphers to use
                --ssl-alpn              ALPN protocol list to use.
       --ssl (Use SSL)
       --ssl-verify (Verify server certificates)
           In client mode, --ssl-verify is like --ssl except that it also requires verification of the server certificate. Ncat comes with a
           certificates; these will also be used if available. Use --ssl-trustfile to give a custom list. Use -v one or more times to get
       --ssl-cert certfile.pem (Specify SSL certificate)
           (in connect mode). Use it in combination with --ssl-key.
       --ssl-key keyfile.pem (Specify SSL private key)
           This option gives the location of the PEM-encoded private key file that goes with the certificate named with --ssl-cert.
       --ssl-trustfile cert.pem (List trusted certificates)
           combined with --ssl-verify. The argument to this option is the name of a PEM file containing trusted certificates. Typically, the
       --ssl-ciphers cipherlist (Specify SSL ciphersuites)
       --ssl-alpn ALPN list (Specify ALPN protocol list)
           http://www.openssl.org
bandit15@bandit:~$ ncat --ssl localhost 30001
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt
Correct!
JQttfApK4SeyHwDlI9SXGR50qclOAil1
```

Honestly, this one was hardest for me specifically because of ssl encryption thing had to google out ways to solve such problem just to know that instead of nc we can use ncat which is net concatenate which is similar to nc command

using “ncat –ssl localhost 30001” found out using the man command of the function we can switch to port 30001 and type the password of bandit15 to access password for bandit16 which is

“JQttfApK4SeyHwDlI9SXGR50qclOAil1”

Lvl 16->17

```
bandit16@bandit:~$ man nmap
bandit16@bandit:~$ nmap localhost -p 31000-32000
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-27 20:29 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00010s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
31046/tcp open  unknown
31518/tcp open  unknown
31691/tcp open  unknown
31790/tcp open  unknown
31960/tcp open  unknown
```

```
bandit16@bandit:~$ ncat localhost --ssl 31790
JQttfApK4SeyHwDlI9SXGR50qclOAil1
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
SghaTdcG0Knywlbp JVyusavPzpaJMjdJ6tcFhVAbAjm7enCIvGCSx+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-----
```

Using hit and trial, we find the port in which we can get the credential, in this case we got it in form of a private key

Using the private key we can login to bandit17 and in case you need the password we can extract it from there itself

password bandit17 after logging in using private key using

cat /etc/bandit_pass/bandit17 is:

“VwOSWtCA7lRKkTfbr2IDh6awj9RNZM5e”

```
bandit17@bandit:~$ cat /etc/bandit_pass/bandit17
VwOSWtCA7lRKkTfbr2IDh6awj9RNZM5e
bandit17@bandit:~$
```

Lvl 17->18

```
bandit17@bandit:~$ man diff
bandit17@bandit:~$ diff passwords.old passwords.new
42c42
< p6ggwdNHncnmCNxuAt0KtKVq185ZU7AW
---
> hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg
bandit17@bandit:~$
```

In this lvl given 2 files passwords.old and passwords.new we will use diff command in order to retrieve them

the passwords we obtain are

“p6ggwdNHncnmCNxuAt0KtKVq185ZU7AW”

“hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg”

NOTE: Can’t login using either password after this step

Lvl 18->19

[Since I was not able to retrieve the pass for bandit18 I can’t continue just now till the task specified I’ll do it as soon as possible and update it on github]