OVER THE WIRE BANDIT WARGAMES

Level 0:

ssh = the command is used to connect to the server, already mentioned in detail.

Level 1-8:

ls = this is used for checking files, and directories in the current directory.

cd = used for change directory.

cat = used to read every line of files in the current directory.

file = used to locate files in a directory.

du = used for checking the size of files.

find = used for searching types of files.

grep = used to search for lines that match a regular expression and print them.

Level 9-12:

sort = used for sorting all data in categories.

uniq = used after sort for reducing the repeats of data.

strings = are used for treating every specific character as the string to read it.

base64 = used to encode or decode the data by using -e for encoding and -d for decoding.

tr = used to translate characters from set to other.

Level 13-14:

mkdir = used for Creates directories.

Mv = used for Moves (renames) files and directories

Cp = used for Copies files and directories.

Level 15-17:

Telenet = used for communicating with another host using the TELNET protocol.

Openssl = used to connect as the client using the hostname localhost at a given port. (in parameters like s\_client)

nano = used to create private keys. (in bandit17)

chmod = used to change file permissions. Diff = used to find passwords.

level 0-1:

bandit0@bandit:~$ ls

readme

bandit0@bandit:~$ cat readme

boJ9jbbUNNfktd78OOpsqOltutMc3MY1

level 1-2:

bandit1@bandit:~$ ls

-

bandit1@bandit:~$ cat ./-

CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9

Level 2-3:

bandit2@bandit:~$ ls

spaces in this filename

bandit2@bandit:~$ cat "spaces in this filename"

UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK

Level 3-4:

bandit3@bandit:~$ ls

inhere

bandit3@bandit:~$ cd inhere

bandit3@bandit:~/inhere$ ls -al

total 12

drwxr-xr-x 2 root root 4096 Sep 28 14:04 .

drwxr-xr-x 4 bandit3 bandit3 4096 Oct 14 13:39 ..

-rw-r----- 1 bandit4 bandit3 33 Sep 28 14:04 .hidden

bandit3@bandit:~/inhere$ cat .hidden

pIwrPrtPN36QITSp3EQaw936yaFoFgAB

Level 4-5:

bandit4@bandit:~$ ls

inhere

bandit4@bandit:~$ cd inhere

bandit4@bandit:~/inhere$ ls -al

total 48

-file00 -file01 -file02 -file03 -file04

-file05 -file06 -file07 -file08 -file09

bandit4@bandit:~/inhere$ file ./-\*

./-file00: Non-ISO extended-ASCII text, with CR line terminators, with escape sequences

./-file01: data

./-file02: data

./-file03: data

./-file04: data

./-file05: data

./-file06: data

./-file07: ASCII text

./-file08: data

./-file09: data

bandit4@bandit:~/inhere$ cat ./-file07

koReBOKuIDDepwhWk7jZC0RTdopnAYKh

Level 5-6:

bandit5@bandit:~$ ls

inhere

bandit5@bandit:~$ cd inhere

bandit5@bandit:~/inhere$ ls

maybehere00 maybehere02 maybehere04 maybehere06 maybehere08 maybehere10 maybehere12 maybehere14 maybehere16 maybehere18

maybehere01 maybehere03 maybehere05 maybehere07 maybehere09 maybehere11 maybehere13 maybehere15 maybehere17 maybehere19

bandit5@bandit:~/inhere$ find -size 1033c -type f

./maybehere07/.file2

bandit5@bandit:~/inhere$ cat ./maybehere07/.file2

DXjZPULLxYr17uwoI01bNLQbtFemEgo7

Level 6-7:

bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c 2>/dev/null

/var/lib/dpkg/info/bandit7.password

cat /var/lib/dpkg/info/bandit7.password

HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs

Level 7-8:

bandit7@bandit:~$ ls

data.txt

bandit7@bandit:~$ grep “millionth” data.txt

millionth cvX2JJa4CFALtqS87jk27qwqGhBM9plV

Level 8-9:

bandit8@bandit:~$ ls

data.txt

bandit8@bandit:~$ cat data.txt | sort | uniq -u

UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR

Level 9-10:

bandit9@bandit:~$ ls

data.txt

bandit9@bandit:~$ strings data.txt | grep "="

|========== the

,]=NB

@k<=

"m=g

========== password

=r-3

========== is

mu=v.

<= V57

i=Hk>$B

========== truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk

S1N=

PbgQ=Zp

=M Q

x3X}=

Level 10-11:

bandit10@bandit:~$ ls

data.txt

bandit10@bandit:~$ cat data.txt | base64 --decode

The password is IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR

Level 11-12:

bandit11@bandit:~$ ls

data.txt

bandit11@bandit:~$ cat data.txt

Gur cnffjbeq vf 5Gr8L4qetPEsPk8htqjhRK8XSP6x2RHh

bandit11@bandit:~$ cat data.txt | tr '[A-Za-z]' '[N-ZA-Mn-za-m]'

The password is 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu

Level 12-13:

ommand-

cat data.txt

mkdir /tmp/pavan

cp data.txt /tmp/pavan

cd /tmp/pavan

ls

file data.txt

xxd -r data.txt data1

file data1

mv data1 data2.gz

gzip -d data2.gz

file data2

mv data2 data3.bz2

bzip2 -d data3.bz2

file data3

mv data3 data4.gz

gzip -d data4.gz

file data4

tar -xvf data4

file data5.bin

tar -xvf data5.bin

file data6.bin

mv data6.bin data7.bz2

bzip2 -d data7.bz2

file data7

tar -xvf data7

file data8.bin

mv data8.bin data9.gz

gzip -d data9.gz

file data9

cat data9

(I type commands only. The process was to clumsy to identify the things.)

Level 13-14:

bandit13@bandit:~$ ls

sshkey.private

bandit13@bandit:~$ ssh -i sshkey.private bandit14@localhost -p 2220

Are you sure you want to continue connecting (yes/no)? yes

bandit14@bandit:~$ cat /etc/bandit\_pass/bandit14

4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e

Level 14-15:

bandit14@bandit:~$ nc localhost 30000

4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e

Correct!

BfMYroe26WYalil77FoDi9qh59eK5xNr

Level 15-16:

bandit14@bandit:~$ openssl s\_client -ign\_eof -connect localhost:30001

...[SNIPPED]...

BfMYroe26WYalil77FoDi9qh59eK5xNr

Correct!

cluFn7wTiGryunymYOu4RcffSxQluehd

Level 16-17:

nmap -A localhost -p 31000-32000

openssl s\_client -connect localhost:31790

mkdir /tmp/gaurav\_ssh

cd /tmp/gaurav\_ssh

nano gaurav.private

chmod 600 gaurav.private

ssh bandit17@localhost -i gaurav.private

Level 17-18:

bandit17@bandit:~$ ls

ban ssh bandit18@localhost

bandit17@bandit:~$ diff passwords.new passwords.old

ssh bandit18@localhost

ssh -T bandit18@localhost

(use -t parameter to disable pseudo -tty allocation.)

Level 18-19:

ssh bandit18@bandit.labs.overthewire.org -p 2220 cat readme

bandit18@bandit.labs.overthewire.org's password:

IueksS7Ubh8G3DCwVzrTd8rAVOwq3M5x

Level 19-20:

bandit19@bandit:~$ ls

bandit20-do

bandit19@bandit:~$ ./bandit20-do cat /etc/bandit\_pass/bandit20

GbKksEFF4yrVs6il55v6gwY5aVje5f0j