ACM RECRUITMENT:

DEVIKA K ANIL (AM.EN.U4EAC24022)

OVERTHEWIRE BANDIT

LEVEL 0: bandit0

Command:

Ssh: used to securely connect to a remote server.

Ssh bandit)@bandit.labs.overthewire.org -p 220

LEVEL 0-1: ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If

Commands:

ls :

lists all the files

cat readme:

reads and displays file contents of file readme

LEVEL 1-2: 263JGJPfgU6LtdEvgfWU1XP5yac29mFx

Commands :

ssh bandit1@bandit.labs.overthewire.org -p 2220

ls : found the file named "-"

cat ./- : opened the file named "-" in the directory and found the password

LEVEL 2-3: MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx

Commands :

ssh bandit2@bandit.labs.overthewire.org -p 2220

ls : found the file named "spaces in this filename" in the directory

cat spaces\ in\ this\ filename\ : opened the file named "spaces in this filename" in the directory and found the password

LEVEL 3-4: 2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ

Commands :

ssh bandit3@bandit.labs.overthewire.org -p 2220

ls: found the directory named "inhere"

cd inhere: opened the directory named "inhere"

ls -a: found the hidden file named "...Hiding-From-You"

cat ...Hiding-From-You : opened the file named "...Hiding-From-You" and found the password.

LEVEL 4-5: 4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw

Commands :

ssh bandit4@bandit.labs.overthewire.org -p 2220

ls: found the directory named "inhere"

cd inhere: opened the directory named "inhere"

file ./* :found the files inside inhere which contained ASCII text

cat ./-file07 : opened the file named "-file07" and found the password

LEVEL 5-6: HWasnPhtq9AVKe0dmk45nxy20cvUa6EG

Commands :

ssh bandit5@bandit.labs.overthewire.org -p 2220

Ls: found the directory named "inhere" in the directory

Cd inhere/: opened the directory named "inhere"

Find . -type f -size 1033c ! -executable : found the file inside maybehere07 directory in inhere

Cat ./maybehere07/.file2 : opened the file named ".file2" and found the password

LEVEL 6-7: morbNTDkSW6jIlUc0ymOdMaInOlFVAaj

Commands ：

ssh bandit6@bandit.labs.overthewire.org -p 2220

Find / -type f -user bandit7 -group bandit6 -size 33c ：found the specified file

Cat /var/lib/dpkg/info/bandit7.password : opened the file and found the password for next server

LEVEL 7-8: dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc

Commands :

ssh bandit7@bandit.labs.overthewire.org -p 2220

Ls : found the file data.txt

Cat data.txt

Strings data.txt | grep “millionth” : Using grep command found the password

LEVEL 8-9: 4CKMh1JI91bUIZZPXDqGanal4xvAg0JM

Commands :

ssh bandit8@bandit.labs.overthewire.org -p 2220

ls: found file data.txt

Cat data.txt: found contents of data.txt

Sort data.txt | uniq -c : found the password

LEVEL 9-10: FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey

Commands :

ssh bandit9@bandit.labs.overthewire.org -p 2220

ls: found file data.txt

Strings data.txt | grep “=” : Using grep,strings commands and found the password

LEVEL 10-11: dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr

Commands :

ssh bandit10@bandit.labs.overthewire.org -p 2220

ls: found data.txt

Cat data.txt | base64 -d data.txt : Using grep commands and found the password

LEVEL 11-12: 7x16WNeHIi5YkIhWsfFIqoognUTyj9Q4

Commands :

ssh bandit11@bandit.labs.overthewire.org -p 2220

ls: found file data.txt

Cat data.txt : found encrypted password

Decoded password using cyberchef

LEVEL 12-13: FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn

Commands:

ssh bandit12@bandit.labs.overthewire.org -p 2220

Ls : found file data.txt

Mkdir /tmp/acm : created temp directory

Cp data.txt /tmp/acm : copied data.txt to temp file

Cd /tmp/acm

Xxd -r data.txt > data : converted the hexdump back into its original binary format
Using file and extracting commands on repeat to get ASCII text file

File data

Mv data file.gz

Gzip -d file.gz

ls

File file

Mv file file.bz2

Bzip2 -d file.bz2

Ls

File file

Mv file file.tar

Tar xf file.tar

Ls

File data5.bin

Rm file.tar

Rm data.txt

Ls

File data5.bin

Mv data5.bin data.tar

Tar xf data.tar

Ls

File data6.bin

Mv data6.bin data.bz2

Bzip2 -d data.bz2

Ls

File data

Mv data data.tar

Ls

Tar xf data.tar

File data8.bin

Mv data8.bin data.gz

Ls

File data

Cat data: opened the final ouput file after extraction to get password

LEVEL 13-14: MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS

Commands :

ssh bandit13@bandit.labs.overthewire.org -p 2220

Ls : found file sshkey.private

Ssh -I sshkey.private bandit14@localhost -p 2220 : Connected to the server using ssh server

Cat /etc/bandit_pass/bandit14 : opened the file and got the password for next level

LEVEL 14-15: 8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo

Commands :

ssh bandit14@bandit.labs.overthewire.org -p 2220

Nc localhost 30000: connected to the localhost at port 30000 and entered the password and found the password

LEVEL 15-16: kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx

Commands :

ssh bandit15@bandit.labs.overthewire.org -p 2220

openssl s_client -connect localhost:30001 : connected to the localhost at port 30001 and entered the password and found the password for next level

LEVEL 16-17: EReVavePLFHtFlFsjn3hyzMlvSuSAcRD

Commands :

ssh bandit16@bandit.labs.overthewire.org -p 2220

Nmap localhost -p 31000-32000 : found the ports that are open

--ssl localhost:31790 : connected to the localhost at port 31790 and entered the password and found the password.

LEVEL 17-18: x2gLTTjFwMOhQ8oWNbMN362QKxfRqGlO

Commands :

ssh -i bandit16 bandit17@bandit.labs.overthewire.org -p 2220

Ls -la

Cat /etc/bandit_pass/bandit17 : found password for next level

LEVEL 18-19: cGWpMaKXVwDUNgPAVJbWYuGHVn9zl3j8

Commands :

Ssh -t bandit18@bandit.labs.overthewire.org -p 2220

ls

Cat readme: opens file readme and gets password for consequent level

LEVEL 19-20: 0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbY0

Commands :

ssh bandit19@bandit.labs.overthewire.org -p 2220

ls -l :lists binary files

./bandit20-do: executes binary file

./bandit20-do ls : lists files inside

./bandit20-do cat /etc/bandit_pass/bandit20 : Opening the file containing password using the binary file and found the password for next level