BANDIT WAR GAMES

Aniruddh Singh

Level 0 : ssh bandit0@bandit.labs.overthewire.org -p 2220

Level 0-1 :

Command : cat readme

Password : boJ9jbbUNNfktd78OOpsqOltutMc3MY1

Level 1-2 :

Command : cat ./-

Password : CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9

Level 2-3 :

Command : cat "spaces in this filename"

Password : UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK

Level 3-4 :

Command : cd inhere

ls -a

cat .hidden

Password : pIwrPrtPN36QITSp3EQaw936yaFoFgAB

Level 4-5 :

Command : cat ./-file07

Password : koReBOKuIDDepwhWk7jZC0RTdopnAYKh

Level 5-6 :

Command : find . -type f -exec ls -lk \{\} \; | grep 1033 //by which we can find in which directory

a file of size1033 bytes is present (which is .file2)

cd maybehere

ls -a

cat .file2

Password : DXjZPULLxYr17uwoI01bNLQbtFemEgo7

Level 6-7 :

Command : cd / //change to root directory

ls

find | grep bandit7

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

Password : HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs

Level 7-8 :

Command : cat data.txt | grep millionth

Password : cvX2JJa4CFALtqS87jk27qwqGhBM9plV

Level 8-9 :

Command : cat data.txt | sort -g | uniq -c | - sort -g

Password : UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR

Level 9-10 :

Command : strings data.txt | grep ==

Password : truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk

Level 10-11 :

Command : base64 -d data.txt

Password : IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR

Level 11-12 :

Command :

echo "Gur cnffjbeq vf 5Gr8L4qetPEsPk8htqjhRK8XSP6x2RHh" | tr '[a-z]' '[n-za-m]'

echo "Ghe password is 5Ge8L4drgPEfPx8ugdwuRK8XSP6k2RHu" | tr '[A-Z]' '[N-ZA-M]'

Password : 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu

Level 12-13 :

Command : mkdir /tmp/mynamesoumya

cp data.txt /tmp/mynamesoumya

cd /*tmp/*mynamesoumya

ls

xxd -r data.txt | strings //to reverse the hex

xxd -r data.txt nonhex.bin

zcat nonhex.bin | file - //opposite of gzip x zcat

//opposite to bzip2 x bzcat

zcat nonhex.bin | bzcat | zcat | tar -xO | tar -xO | bzcat | tar -xO | zcat

Password : 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL

Level 13-14 :

Command : ssh -i sshkey.private bandit14@localhost

Password : 4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e

Level 14-15 : instead of localhost I tried writing bandit14 but dint work

tried to know the local host name using hostnamectl ..dint work..

hostname game o/p

=> hostname = soumya virtual machine

hostnamectl = gives all details

Command : echo 4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e | nc localhost 30000

Password : BfMYroe26WYalil77FoDi9qh59eK5xNr

Level 15-16 : -quiet – connect //y

Command : echo BfMYroe26WYalil77FoDi9qh59eK5xNr | openssl s\_client -quiet -connect localhost:30001

Password : cluFn7wTiGryunymYOu4RcffSxQluehd

Level 16-17 :

Command : nmap localhost -p31000-32000 // Not shown: 999 closed ports

PORT STATE SERVICE

31518/tcp open unknown

31790/tcp open unknown

echo cluFn7wTiGryunymYOu4RcffSxQluehd | openssl s\_client -quiet -connect localhost:31518

echo cluFn7wTiGryunymYOu4RcffSxQluehd | openssl s\_client -quiet -connect localhost:31790

mkdir /*tmp/*sravan

nano sshkey.private

ssh -i /tmp/sravan/sshkey.private [bandit17@localhost](mailto:bandit17@localhost) //connecting to bandit 17 using private key

cd /etc

find . | grep bandit17

cd ./bandit\_pass

cat bandit17

Password : xLYVMN9WE5zQ5vHacb0sZEVqbrp7nBTn

Level 17-18 :

Command : diff passwords.old passwords.new

Password : kfBf3eYk5BPBRzwjqutbbfE887SVc5Yd

Level 18-19 :

Command : ssh -T bandit18@localhost

ls

readme

cat readme

Password : IueksS7Ubh8G3DCwVzrTd8rAVOwq3M5x

Level 19-20 :

Command : ./bandit20-do

./bandit20-do id

./bandit20-do cat /etc/bandit\_pass/bandit20

Password : GbKksEFF4yrVs6il55v6gwY5aVje5f0j

Level 20-21:

Command : echo GbKksEFF4yrVs6il55v6gwY5aVje5f0j | nc -l -p 1025

./suconnect 1025

Password : gE269g2h3mw3pwgrj0Ha9Uoqen1c9DGr

Level 21-22 :

Command : cd /etc/cron.d/

cat cronjob\_bandit22

cat /usr/bin/cronjob\_bandit22.sh

cat /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv

Password : Yk7owGAcWjwMVRwrTesJEwB7WVOiILLI

Level 22-23:

Command : *cd /etc/cron.d/*

*cat cronjob\_bandit23*

*cat /usr/bin/cronjob\_bandit23.sh*

*cd /usr/bin*

*./cronjob\_bandit23.sh //bandit22 is the default user change it to 23*

*echo mytarget=$(echo I am user bandit23 | md5sum | cut -d ' ' -f 1) //8ca319486bfbbc3663ea0fbe81326349*

*cat /tmp/$mytarget*

Password : jc1udXuA1tiHqjIsL8yaapX5XIAI6i0n

Level 23-24 :

Command : echo mytarget=$(echo I am user bandit24 | md5sum | cut -d ' ' -f 1)

mytarget=ee4ee1703b083edac9f8183e4ae70293

cat /tmp/ee4ee1703b083edac9f8183e4ae70293

Password : UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ

Level 24-25 :

Command :

cat forloop.sh

#!/bin/bash

passwd=UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ

for i in {0..9}{0..9}{0..9}{0..9}

do

echo $passwd $i >> result.txt

done

cat result.txt | nc localhost 30002

method 2:

cat testbandit25.sh

#!/bin/bash

for i in {1000..1500}

do

a="UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ $i"

echo $a

echo $a | nc localhost 30002 >> soumyatest.txt

echo "finished testing port $i"

done

Password : uNG9O58gUE7snukf3bvZ0rxhtnjzSGzG

///////////////////////////////////////////////////////////////////////////////////////////

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

awk '{print $11}' challenge4 | sort -g | uniq -c | sort -g

sed -i 's/number/---/g' admin1.txt

egrep "10.0.0.153|64.242.88.10" access\_log >> unixworkshop.txt^C

unrar e apache-access\_log.rar

wget "<https://bit.ly/1Fda7Cu>"

hostnamectl

systemctl status open-vm-tools.service