

***UNIVERSIDAD POLITECNICA DE QUINTANA ROO.*** ***Asignatura:*** *Sistemas Operativos.*  ***Tarea:*** *Actividad #993.* ***Grupo y Grado:*** *27BV* ***Carrera:*** *Ingeniería en Software* ***Alumno:*** *Juan Alberto Kuyoc Santiago.*

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

Level 0 -> 1 cat ~/readme

//NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL

exit

Level 1 -> 2 ssh bandit1@bandit.labs.overthewire.org -p 2220

//NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL

ls -alps cat ./-

//rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi

exit

Level 2 -> 3 ssh bandit2@bandit.labs.overthewire.org -p 2220 //rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi ls -alps cat spaces\ in\ this\ filename

//aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG

exit

Level 3 -> 4 ssh bandit3@bandit.labs.overthewire.org -p 2220

//Contraseña LVL2 -> 3 = aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG ls -alps cd inhere

//inhere/ ls -al cat .hidden

//2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe

exit

Level 4 -> 5 ssh bandit4@bandit.labs.overthewire.org -p 2220

//2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe

ls -alps cd inhere

ls

find . -type f | xargs file cat ./-file07

//lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR

exit

Level 5 -> 6

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

//lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR

ls

cd inhere

find . -type f -size 1033c ! -executable // ./maybehere07/.file2 cat ./maybehere07/.file2

//P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU

exit

Level 6 -> 7 ssh bandit6@bandit.labs.overthewire.org -p 2220 //P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU find / -type f -user bandit7 -group bandit6 -size 33c cat /var/lib/dpkg/info/bandit7.password //z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S

exit

Level 7 -> 8

ssh bandit7@bandit.labs.overthewire.org -p 2220 //z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S ls -alps cat data.txt whatsis strings strings data.txt | grep "millionth"

//TESKZC0XvTetK0S9xNwm25STk5iWrBvP

exit

Level 8 -> 9

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

//TESKZC0XvTetK0S9xNwm25STk5iWrBvP

ls cat data.txt sort data.txt man uniq

sort data.txt | uniq -c //EN632PlfYiZbn3PhVK3XOGSlNInNE00t

exit

Level 9 -> 10 ssh bandit9@bandit.labs.overthewire.org -p 2220 //EN632PlfYiZbn3PhVK3XOGSlNInNE00t strings data.txt | grep "=" //G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s

exit

Level 10 -> 11 ssh bandit10@bandit.labs.overthewire.org -p 2220 //G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s cat data.txt base64 -d data.txt

//6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM

exit

Level 11 -> 12 ssh bandit11@bandit.labs.overthewire.org -p 2220

//6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM

cat data.txt

Respuesta de consola -> https://gchq.github.io/CyberChef/ -> ROT13

//JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv

exit

Level 12 -> 13

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

//JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv

cat data.txt man xxd

mkdir /tmp/joshua cp data.txt /tmp/joshua cd /tmp/joshua ls

xxd -r data.txt > data

ls 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.gz gzip -d file.gz ls file file mv file file.tar tar xf file.tar ls file data5.bin rm file.tar rm data.txt

ls file file 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 ls file data8.bin mv data8.bin data.gz gzip -d data.gz ls file data cat data

//wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw

exit

Level 13 -> 14 -> 15 ssh bandit13@bandit.labs.overthewire.org -p 2220

//wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw ls

ssh -i sshkey.private bandit14@localhost (si no funciona añade "-p 2220" al final) cat /etc/bandit\_pass/bandit14 nc localhost 30000 cat /etc/bandi\_pass/bandit14 nc localhost 30000

exit exit

Level 15 -> 16 ssh bandit15@bandit.labs.overthewire.org -p 2220 cat /etc/bandit\_pass/bandit15 ncat --ssl localhost 30001 (pones la posible contraseña)

exit

Level 16 -> 17 ssh bandit16@bandit.labs.overthewire.org -p 2220 //JQttfApK4SeyHwDlI9SXGR50qclOAil1 cat /etc/bandit\_pass/bandit16 nmap localhost -p 31000-32000 nc localhost 31790 ncat --ssl localhost 31790 mkdir /tmp/random\_sshkey cd /tmp/random\_sshkey

touch private.key vim private.key hmod 400 private.key

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

Level 17 -> 18 man diff diff passwords.old passwords.new exit

Level 18 -> 19 ssh bandit18@bandit.labs.overthewire.org -p 2220 man ssh man ssh | grep terminal

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

/bin/sh

//kfBf3eYk5BPBRzwjqutbbfE887SVc5Yd cat readme exit

Level 19 -> 20 ssh bandit19@bandit.labs.overthewire.org -p 2220

//IueksS7Ubh8G3DCwVzrTd8rAVOwq3M5x

./bandit20-do

./bandit20-do id

./bandit20-do ls

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

Level 20 -> 21 ssh bandit20@bandit.labs.overthewire.org -p 2220 //GbKksEFF4yrVs6il55v6gwY5aVje5f0j echo "GbKksEFF4yrVs6il55v6gwY5aVje5f0j" | netcat jobs ./suconnect 1234

exit

Level 21 -> 22 ssh bandit21@bandit.labs.overthewire.org -p 2220 //gE269g2h3mw3pwgrj0Ha9Uoqen1c9DGr vim /etc/cron.d/ ls /etc/cron.d/ cat /etc/cron.d/cronjob\_bandit22.sh cat /tmp/t706lds950RqQh9aMcz65hpAoZKF7fgv

exit

Level 22 -> 23 ssh bandit22@bandit.labs.overthewire.org -p 2220 //Yk7owGAcWjwMVRwrTesJEwB7WVOiILLI cat /etc/cron.d/cronjob\_bandit23 cat /usr/bin/cronjob\_bandit23.sh whoami $myname myname=banit23 md5sum man md5sum echo I am user $myname | md5sum | cut -d ' ' -f 1 cat /tmp/8ca319486bfbbc3663ea0fbe81326349 exit

Level 23 -> 24 ssh bandit23@bandit.labs.overthewire.org -p 2220 //jc1udXuA1tiHqjIsL8yaapX5XIAI6i0n ls /etc/cron.d/ cat /etc/cron.d/cronjob\_bandit24 cat /usr/bin/cronjob\_bandit24.sh mkdir /tmp/rand cd /tmp/rand mkdir rand cd rand vim test.sh chmod 777 test.sh vim test.sh

chmod 777 pass

cp test.sh /var/spool/bandit24/ cat pass cat test.sh cat pass

exit

Level 24 -> 25 ssh bandit24@bandit.labs.overthewire.org -p 2220 //UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ netcat localhost 30002 $ for i in {1..10} exit

Level 25 -> 26 ssh bandit25@bandit.labs.overthewire.org -p 2220

//uNG9O58gUE7snukf3bvZ0rxhtnjzSGzG

ls

ssh -i bandit26.sshkey bandit26@localhost cat /etc/passwd cat /usr/bin/showtext more .bashrc ssh bandit26@localhost -i bandit26.sshkey :set shell=/bin/bash

:shell

whoami

cat /etc/bandit\_pass/bandit26

Level 26 -> 27

//5czgV9L3Xx8JPOyRbXh6lQbmIOWvPT6Z

./bandit27-do

./bandit27-do cat /etc/bandit:pass/bandit27 exit

\*vuelve a bandit25\*

exit

Level 27 -> 28

~$ cd /tmp/

/tmp$ mkdir git\_level27

/tmp$ cd git\_level27 /tmp/git\_level27$ git clone ssh://bandit27-git@localhost/home/bandit27-git/repo

$ls -l

$cd repo

$ls -la

$cat README

Level 28 -> 29 ssh bandit28@bandit.labs.overthewire.org -p 2220 //0ef186ac70e04ea33b4c1853d2526fa2 pass=0ef186ac70e04ea33b4c1853d2526fa2 mkdir /tmp/git\_level28 cd /tmp/git\_level28 git clone ssh://bandit28-git@localhost/home/banit28-git/repo ls -la

cd repo

ls -la

cat README.md

git log git branch git chackout 186a1038cc54d1358d42d468cdc8e3cc28a93fcb cat README.md

exit

Level 29 -> 30 ssh bandit29@bandit.labs.overthewire.org -p 2220 //bbc96594b4e001778eee9975372716b2 cd /tmp/

/tmp$ mkdir git\_level29

/tmp$ cd git\_level29 /tmp/git\_level29$ git clone ssh://bandit29-git@localhost/home/banit29-git repo ls -la cd repo/ ls -la

cat READDEME.md

git branch -a git checkout remotes/origin/dev ls -la

cat READEME.md

exit

Level 30 -> 31 ssh bandit30@bandit.labs.overthewire.org -p 2220 //5b90576bedb2cc04c86a9e924ce42faf cd /tmp/ /tmp$ mkdir git\_level30

/tmp$ cd git\_level30 /tmp/git\_level30$ git clone ssh://bandit30-git@localhost/home/banit30-git repo ls -la cd repo/ ls -la

cat READDEME.md

git branch -a git tag git show secret

exit

Level 31 -> 32 ssh bandit31@bandit.labs.overthewire.org -p 2220 //47e603bb428404d265f59c42920d81e5 cd /tmp/ /tmp$ mkdir git\_level31

/tmp$ cd git\_level31 /tmp/git\_level29$ git clone ssh://bandit31-git@localhost/home/banit31-git repo ls -la cd repo/ ls -la

cat READDEME.md echo "May I come in?" > key.txt

ls -la rm .gitignore ls -la git add.

git commit -m "Added ke.txt" git push origin master exit

Level 32 -> 33 ssh bandit32@bandit.labs.overthewire.org -p 2220

//56a9bf19c63d650ce78e6ec0354ee45e

>>ls

>>pwd

>>cd

>>$shell

>>$EUID >>$0 export SHELL=/bin/bash echo $SHELL

/bin/bash

$SHELL

cat /etc/bandit\_pass/bandit33