TAG : OTW

Nome : Thomaz Veloso Rebelo da Silva
Data : 15/03/2020

WRITE-UP BANDIT OVER THE WIRE
ASSUMA QUE TODOS OS LVLS SE CONECTAM COM
ssh bandit0@bandit.labs.overthewire.org -p 2220 onde 0 será o nome de cada lvl

LVL 0-

Um “ls” para checar os arquivos e um “cat” para ler o “readme”
passwd: boJ9jbbUNNfktd78OOpsqOltutMc3MY1

LVL 1-

Um “ls” para checar os arquivos e um “cat” para ler o “-”(use cat ./-)
passwd:CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9

LVL 2-

Um “ls” para checar os arquivos e um “cat” para ler o “spaces in this filename”(use TAB para auto complet)
passwd:UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK

LVL 3-

Um “ls -lah” para checar os arquivos ,”cd inhere,“ls -lah” para checar os arquivo e um “cat” para ler o “.hidden”
passwd:pIwrPrtPN36QITSp3EQaw936yaFoFgAB

LVL 4-

Um “ls -lah” para checar os arquivos ,”cd inhere,“ls -lah” para checar os arquivo e um “cat” para ler o “-file07”(use ./para ler)
passwd:koReBOKuIDDepwhWk7jZC0RTdopnAYKh
Testei todos os arquivos até achar o -file07 dando clear um após o outro

LVL 5-

Um “ls -lah” para checar os arquivos,”cd inhere,“ls -lah” para checar os arquivo,temos muitas pastas e dentro delas muitos arquivos um brute force é ossivel mas muito complicado mas temos o tamanho do arquivo logo podemos usar “find -size 1033c” com isso temos “./maybehere07/.file2” dando “cat ./maybehere07/.file2”
passwd:DXjZPULLxYr17uwoI01bNLQbtFemEgo7

LVL 6-

Se dermos “ls -lah” temos apenas arquivos inúteis damos “cd ..” até o / e usamos o “find” de novo só que agora com o user logo temos “find -user bandit7 -group bandit6 -size 33c” temos um arquivo sem permission denied que é “/var/lib/dpkg/info/bandit7.password” dando um cat nele “cat /var/lib/dpkg/info/bandit7.password”

passwd:HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs

LVL 7-

Um “ls -lah” para checar os arquivos, temos um data.txt com a dica que temos no enunciado usamos o “grep”,cat data.txt | grep "millionth"

passwd:cvX2JJa4CFALtqS87jk27qwqGhBM9plV

LVL 8-

Um “ls -lah” para checar os arquivos, temos um data.txt com a dica que temos no enunciado usamos o sort e uniq ficando assim “cat data.txt | sort | uniq -u”(sort para organizar e uniq para printar a única linha)

passwd:UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR

LVL 9-

Um “ls -lah” para checar os arquivos, temos um data.txt com a dica que temos no enunciado usamos “strings” com “grep” ficando assim “strings data.txt | grep "="”

passwd:truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk

LVL 10-

Um “ls -lah” para checar os arquivos, temos um data.txt com a dica que temos no enunciado usamos “cat data.txt” e pegamos o código em base64 e usamos um decode online(podemos usar o decode so proprio linux mas eu fiz assim)

passwd:IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR

LVL 11-

Um “ls -lah” para checar os arquivos, temos um data.txt com a dica que temos no enunciado usamos “cat data.txt” e pegamos o código em caesar cipher com 13 de rotação e usamos um decode online(não sei se daria pra fazer direto do terminal(deve ter mas eu não sei mesmo))

passwd:5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu

LVL 12-

Não consegui fazer,petendo terminar ainda esse ano o bandit.