Level 0:

طالب مني اعمل connect مع السيرفر دا **bandit.labs.overthewire.org** **علي port 2220**
استخدمت ssh protocol علشان اوصل بالسيرفر
Command: ssh bandit0@bandit.labs.overthewire.org -p 2220
Password: bandit0

Level 0:Level 1

وعلشان نوصل لتاني level مفروض نوصل لفايل اسمه readme علشان نوصل للباسورد الي فيه فاستخدمنا

2- Commends:
ls -al
cat readme
password:ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If

Level 1:Level 2

هنا الباسورد موجود في فايل اسمه - طبعا لو عملنا cat - دا بالنسبة له standard input وهيستني مني ان ادخل input ودا طبعا الي مش انا عاوزاه انا عاوزة اعرض محتويات الفايل دا ف الحل ...
نستخدم ال redirection

commend : cat < -
password: 263JGJPfgU6LtdEvgfWU1XP5yac29mFx

Level 2:Level 3

المطلوب ان الباسورد موجود في فايل اسمه spaces in filename المشكله هنا انه معتبر ان كل كلمه
هنا دا اسم فايل لوحده مش دا كله مجرد اسم الفايل الحل ...
ممكن نستخدم الدابل كوتشين او السكيب كاراكتر

commend:cat "spaces in this filename" or cat spaces\ in\ this\ filename
password:MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx

Level 3:Level 4

الباسورد موجود في دايريكتوري اسمه inhere ف الاول بنستخدم cd commend علشان نوصل له وبعدين نبدا نعرض كل محتوياته ب ls -al علشان نظهر الملفات المخفية طبعا اي ملف مخفي في لينكس بيكون قبله .

commend:cat ...Hiding-From-You
password:2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ

Level 4:Level 5

هنا الباسورد موجود في فايل في دايريكتوري اسمه inhere وفي فايل واحد بس هو readable
علشان اقدر اجيب الفايل دا من ضمن باقي الفايلات الموجودة في الدايريكتوتي باستخدم find commend ودا بيحدد لي اي هو نوع كل فايل
commend:file ./*(علشان اجيب الفايلز الموجودة في الدايريكتوري واحدد نوعهم)
cat ./-file07
password:4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw

Level 5:Level 6

الباسورد هنا موجود في inhere directory بس له مواصفات معينه فنبحث عنه باستخدام :
commend:find -type f -size 1033c ! -executable
cat ./inhere/maybehere07/.file2
password: HWasnPhtq9AVKe0dmk45nxy20cvUa6EG

Level 6:Level 7

هنا بقا مطلوب اننا نجيب فايل ولكن ف السيرفر كله
commend:find / -type f -size 33c -user bandit7 -group bandit6

ولكن ظهرلنا ايرورز كتيرة ف بالتالي علشان نعرف نقرا نعمل redirection لل ايرورز دي
commend:find / -type f -size 33c -user bandit7 -group bandit6 2>/dev/null
هيظهر الفايل الي فيه الباسورد
commend:at /var/lib/dpkg/info/bandit7.password
password:morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj

Level 7:Level 8

هنا الباسورد موجود في data.txt وحددلي انه فيه كلمة millionth
commend:cat data.txt|grep millionth
password:dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc

Level 8:Level 9

محتاج ان اجيب السطر الوحيد الي مش متكرر

commend:sort data.txt|uniq -u

uniqبيحتاج ان الاسطر تكون مترتبة

password:4CKMh1JI91bUIZZPXDqGanal4xvAg0JM

Level 9:Level 10

عاوز الملفات المقروءة و فيها علامة يساوي

commend:strings data.txt|grep =

علشان اجيب الفايلات المقروءة استخدمنا strings commend

password:FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey

Level 10:Level 11

مطلوب مننا اننا نقرا محتويات فايل معموله encoded based 64 فنشوف اي الموجود ف الفايل دا

commend: cat data.txt

output:VGhlIHBhc3N3b3JkIGlzIGR0UjE3M2ZaS2lwUlJzREZTR3NnMlJXbnBOVmozcVJyCg==

ازاي بقت نفك التشفير دا

commend:base64 -d data.txt

output:The password is dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr

Level 11:Level 12

بردو الباسورد هنا متشفر باستخدام ROT 13 نشوف اي الموجود في الفايل

commend:cat data.txt

output:Gur cnffjbeq vf 7k16JArUVv5LxVuJfsSVdbbtaHGlw9D4

commend:echo Gur cnffjbeq vf 7k16JArUVv5LxVuJfsSVdbbtaHGlw9D4 |rot13

ouput:The password is 7x16WNeHIi5YkIhWsfFIqoognUTyj9Q4

Level 12:Level 13

الباسورد هنا موجود في data.txt والفايل دا عبارة عن hexadump تم ضغطه اكتر من مرة الاول نعمل دايركتوري نشتغل فيه

commends:mkdir /tmp/emann

cd /tmp/emann

ناخد كوبي من data.txt للدايريكتوري الي عملناه

commend:cp ~/data.txt /tmp/emann

دلوقتي نحول ال hexadump للملف الاصلي

commend:xxd -r data.txt > data

عاوزين نعرف دلوقتي اي نوع الملف دا بعد اما رجعناه لاصله

commend: file data
output:data: gzip compressed data, was "data2.bin", last modified: Thu Sep 19 07:08:15 2024, max compression, from Unix, original size modulo 2^32 574

طلع انه ملف مضغوط فنفك ضغطه

commend:mv data data.gz
gzip - d data.gz

ثم نشوف الملف تاني عبارة عن اي لانه اضغط اكتر من مرة

commend:file data
output:bzip2 compressed data, block size = 900k

نقعد نفك بقا الضغط

commends:mv data data.bz2
file data
bzip2 -d data.bz2
output:data: gzip compressed data, was "data4.bin", last modified: Thu Sep 19 07:08:15 2024, max compression, from Unix, original size modulo 2^32 20480
commends:mv data data.gz
gzip -d data.gz
file data
output:data: POSIX tar archive (GNU)
commends:tar -xvf data
output:data5.bin
commends:file data5.bin
output:data5.bin: POSIX tar archive (GNU)
commends:mv data5.bin data5.tar
tar -xvf data5.tar
output:data6.bin
commends:file data6.bin
output:data6.bin: bzip2 compressed data, block size = 900k
commends:mv data6.bin data6.bz2
bzip2 -d data6.bz2
file data6
output:data6: POSIX tar archive (GNU)
commends:mv data6 data6.tar
tar -xvf data6.tar
output:data8.bin
commends:file data8.bin

output:data8.bin: gzip compressed data, was "data9.bin", last modified: Thu Sep 19 07:08:15 2024, max compression, from Unix, original size modulo 2^32 49
commends:mv data8.bin data8.gz
gzip -d data8.gz
file data8
output:data8: ASCII text
commends:cat data8
output:The password is FO5dwFsc0cbaliH0h8J2eUks2vdTDwAn
الحمدلله والله

Level 13:Level 14

مفيش باسورد هنا ولكن هندخل ع السيرفر ب privatekey
commends:cat sshkey.private
طلع انه private key
ssh -i sshkey.privata -p 2220 bandit14@localhost
كدة دخلنا ع bandit 14
commends:cat /etc/bandit_pass/bandit14
password:MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS

Level 14:Level 15

مطلوب هنا ان ابعت الباسورد علي port 30000 علي local host و هيجيب لي الباسورد بتاع الليفل الجاي
هنستخدم هنا netcad ودي اداة بنستخدمها علشان نتصل بالسيرفر
commends:nc localhost 30000
MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS
رد السيرفر:Correct!
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo

Level 15:Level 16

هنا عاوزني ابعت واستقبل من السرفر بس بطريقة secure اكتر عن طريق SSL|TLS encryption علي port 30001
commends:openssl s_client -connect localhost:30001
وبعت الباسورد ورد السيرفر بCorrect!
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx

closed

Level 16:Level 17

الاول المطلوب اننا نشوف اي ال ports المفتوحة ما بين رينج 32000-31000

commend:nmap -sV -p 31000-32000 localhost

اما نشوف اي ال ports المفتوحة ومتوفرة ليها خدمة ال ssl

نعمل كونكت مع السيرفر

commend:openssl s_client -connect localhost : 31790

وندخله الباسورد وهيرد علينا ب privatekey فنعمل فايل نضيف فيه ال private key دا

commend:mkdir /tmp/moo

cd /tmp/moo

nano no

ندخل علي bandit17

commend:ssh -i no bandit17@localhost -p 2220

بس هيجيلي permession denied لان الفايل دا no له صلاحيات لباقي الجروبات وال other فلازم نغير صلاحياته لانه private key

commend: chmod 600 no

وبس كدة دخلنا علي bandit 17

Level 17:Level 18

عندنا 2 فايلز زي بعض بالظبط بس اختلاف سطر واحد ودا الي فيه باسورد الليفل الجاي

commends:diff passwords.old passwords.new

output:42c42

< ktfgBvpMzWKR5ENj26lbLGSblgUG9CzB

> x2gLTTjFwMOhQ8oWNbMN362QKxfRqGlO

Level 18:Level 19

هنا لما اجي ادخل بيخرجني تلقائي بسبب تعديل في .bashrc وعاوزين نوصل لفايل readme لانه الي فيه الباسورد ف الحل

commend:bandit18@bandit.labs.overthewire.org -p 2220 cat readme

password:cGWpMaKXVwDUNgPAVJbWYuGHVn9zl3j8

Level 19:Level 20

هنا بيقولنا ان موجود ف ال home directory setuid binary نشغله الاول علشان نشوف بيشتغل ازاي

commend:./bandit20-do

دا بيشتغل بصلاحيات bandit 20

./bandit20-do cat /etc/bandit_pass/bandit20 دا المسار الي فيه الباسورد

password:0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO

Level 20:Level 21

هنا بردو فيه setuid binary نشغله نشوف بيشتغل ازاي

output:Usage: ./suconnect <portnumber>
This program will connect to the given port on localhost using TCP. If it receives the correct password from the other side, the next password is transmitted back.

commend : nc -l -p 12345

و باسورد bandit20
في تيرمينال تانية

commend:./suconnect 12345

وهيرد عليا بباسورد bandit 21

password:EeoULMCra2q0dSkYj561DX7s1CpBuOBt

Level 21:Level 22

هنا هنتعامل مع ال cron job ودي هي مهمة بيتم تشغيلها تلقائيا علي فترات زمنية محددة نشوف محتويات /etc/cron.d/ زي ما قال

commend: ls -al /etc/cron.d/

هيظهر لنا الملفات المجدولة الي هي هتكون .cton

commend:cat /etc/cron.d/cronjob_bandit22

out put:@reboot bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
* * * * * bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null

دا معناه ان /usr/bin/cronjob_bandit22.sh يتم تشغيله تلقائيًا عند كل إعادة تشغيل وكل دقيقة فنشوف دا بيعمل اي

commend:cat /usr/bin/cronjob_bandit22.sh

output:#!/bin/bash
chmod 644 /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgvcat /etc/bandit_pass/bandit22 > /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv
دا معناه انه غير صلاحية الملف دا
tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgvc/ تبقي قراءة وكتابة لل owner
و قراءة فقط للباقي وان الملف دا محفوظ فيه باسورد bandit 22
/tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv
commend:cat /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv
output:tRae0UfB9v0UzbCdn9cY0gQnds9GF58Q

Level 22:Level 23

نفس فكرة ال cron job لحد لما نوصل لفايل ونشوف اي محتوياته
usr/bin/cronjob_bandit22.sh/

```
commend :cat usr/bin/cronjob_bandit22.sh/
output:#!/bin/bash

myname=$(whoami)
mytarget=$(echo I am user $myname | md5sum | cut -d '
' -f 1)

echo "Copying passwordfile /etc/bandit_pass/$myname
to /tmp/$mytarget"

cat /etc/bandit_pass/$myname > /tmp/$mytarget
```

ف الاخر ان باسورد الليفل الجاي هتكون ف **tmp/$mytarget/**

```
commends:echo I am user bandit23 | md5sum
output:8ca319486bfbbc3663ea0fbe81326349
commend:cat tmp/8ca319486bfbbc3663ea0fbe81326349
password:0Zf11ioIjMVN551jX3CmStKLYqjk54Ga
```

Level 23:Level 24

بردو **cron job** بردو نعمل نفس الخطوات لحد لما نوصل للفايل الي بيتنفذ كل شوية دا ونشوف فيه اي

commend: cat /usr/bin/cronjob_bandit24.sh
output:#!/bin/bash

```
myname=$(whoami)

cd /var/spool/$myname/foo
echo "Executing and deleting all scripts in
/var/spool/$myname/foo:"
for i in * .*;
do
   if [ "$i" != "." -a "$i" != ".." ];
   then
      echo "Handling $i"
      owner="$(stat --format "%U" ./$i)"
      if [ "${owner}" = "bandit23" ]; then
         timeout -s 9 60 ./$i
      fi
      rm -f ./$i
   fi
done
```

note:

انا مقدرتش افهم ال **cron job** بتاع **bandit 24** بيعمل اي لوحدي فسالت شات جي بي تي و هحاول ان شاء الله اذاكر الجزء دا واسرش عنه اكتر

الي فهمته بعد عنااء ان لو كتبت اسكريبت داخل **/var/spool/bandit24/** هيتنفذ بصلاحيات **bandit 24** ف محتاجين نكتب اسكريبت يطبع الباسورد من **etc/bandit_pass/bandit24/**

```
commends:mkdir /tmp/read
cd /tmp/read
 nano pass
```

وكتبنا في **pass**

cat /etc/bandit_pass/bandit24 > /tmp/password_bandit24

نغير صلاحيات السكريبت علشان يتنفذ

commends:chmod 777 /tmp/read

chmod 777 /tmp/read/pass

محتاجين ننقل السكريبت علشان يتنفذ تلقائي

commend:cp pass /var/spool/bandit24/foo

cat /tmp/password_bandit24

output:gb8KRRCsshuZXI0tUuR6ypOFjiZbf3G8

Level 23:Level 24

للاسف الي فهمته ان ف حله هكتب اسكريبت ودا مجربتوش قبل كدة ولا درسته و ضغط الميد تيرم حاليا ف باذن الله بعد الميد هتعلمه وهكمل حل باقي اللاباات هي فعلا مفيدة جدا جداا و استفادت كتير جدا التطبيق العملي غير حقيقي