

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: `ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5lf`

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 ...
ممکن نستخدم الدابل كوتشين او السكيب كراكتز

commend: `cat "spaces in this filename" or cat spaces\ in\ this\ filename`

password: `MNk8KNH3Usiio41PRUEoDFPqfxLPISmx`

Level 3:Level 4

الباسورد موجود في دايريكتوري اسمه `inhere` ف الاول بنستخدم `cd` 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: `2WmrDFRmJlq3IPxneAaMGhap0pFhF3NJ`

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 باستخدام **find** ودا بيحدد لي اي هو نوع كل فايل **commend**

(علشان اجيب الفايلز الموجودة في الدايريكتوري واحد نوعهم) **commend:file ./***

cat ./-file07

password:4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw

Level 5:Level 6

الباسورد هنا موجود في **inhere directory** بس له مواصفات معينة 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

ه يظهر الفايل الي فيه الباسورد

commend:at /var/lib/dpkg/info/bandit7.password

password:morbNTDkSW6jllUc0ymOdMaLnOIFVAaj

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:FGUW5iILVJrxX9kMYMmlN4MgbpfMiqey
```

Level 10:Level 11

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

```
commend: cat data.txt
```

```
output:VGhllHBhc3N3b3JkIGlzlGR0UjE3M2ZaS2lwUIJzREZTR3NnMlJXbnBOVmozcvJyCg==
```

ازاي بقت نفاك 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 7x16WNeHli5YklhWsfFlqoognUTyj9Q4
```

Level 12:Level 13

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

```
commends:mkdir /tmp/emann
```

```
cd /tmp/emann
```

ناخد كوبي من data.txt للدايركتوري 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 اضبط اكثر 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

commands:mv data8.bin data8.gz

gzip -d data8.gz

file data8

output:data8: ASCII text

commands:cat data8

output:The password is FO5dwFsc0cbaliH0h8J2eUks2vdTDwAn

الحمد لله والله

Level 13:Level 14

مفیش باسورد هنا ولكن هندخل ع السيرفر ب privatekey

commands:cat sshkey.private

طلع انه private key

ssh -i sshkey.private -p 2220 bandit14@localhost

كدە دخلنا ع bandit 14

commands:cat /etc/bandit_pass/bandit14

password:MU4VWeTyJk8ROof1qqmcBPALh7IDCPvS

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

commands:nc localhost 30000

MU4VWeTyJk8ROof1qqmcBPALh7IDCPvS

رد السيرفر:Correct!

8xCjnmgoKbGLhHFAZIGE5Tmu4M2tKJQo

Level 15:Level 16

هنا عاوزني ابعت واستقبل من السيرفر بس بطريقة secure اكثر عن طريق SSL|TLS

port 30001 علي encryption

commands: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 داا
commend:mkdir /tmp/moo

cd /tmp/moo

nano no

ندخل علي bandit17

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

بس هيجيلي permission 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

> x2gLTTjFwMOhQ8oWNbMN362QKxfRqGIO

Level 18:Level 19

هنا لما احي 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:cGWpMaKXVwDUNgPAVJbWYyUGHVn9zl3j8

Level 19:Level 20

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

commend:./bandit20-do

bandit 20 بصلاحيات

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

password:0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO

Level 20:Level 21

هنا برده 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

