Write Up OverTheWire Bandit Level 0-10

Mutiara Setya Rini

Daftar Isi

Level 0	
Level 0 -> Level 1	2
Level 1 -> Level 2	3
Level 2 -> Level 3	4
Level 3 -> Level 4	5
Level 4 -> Level 5	6
Level 5 -> Level 6	8
Level 6 -> Level 7	10
Level 7 -> Level 8	12
Level 8 -> Level 9	14
Level 9 -> Level 10	15
Level 10 -> Level 11	16

Level 0

Diberikan problem sebagai berikut.

The goal of this level is for you to log into the game using SSH. The host to which you need to connect is bandit.labs.overthewire.org, on port 2220. The username is bandit0 and the password is bandit0. Once logged in, go to the Level 1 page to find out how to beat Level 1.



Log in ke SSH dan connect dengan bandit0@bandit.labs.overthewire.org dengan port 2220 dengan command: ssh bandit0@bandit.labs.overthewire.org -p 2220

Level 0-> Level 1

Diberikan problem sebagai berikut.

The password for the next level is stored in a file called readme located in the home directory. Use this password to log into bandit1 using SSH. Whenever you find a password for a level, use SSH (on port 2220) to log into that level and continue the game.

```
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
Congratulations on your first steps into the bandit game!!
Please make sure you have read the rules at https://overthewire.org/rules/
If you are following a course, workshop, walkthrough or other educational activity,
please inform the instructor about the rules as well and encourage them to
contribute to the OverTheWire community so we can keep these games free!
The password you are looking for is: ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If
bandit0@bandit:~$
```

Membuka list file di dalam directory dengan command ls. Di dalam directory terlihat hanya ada file readme. File readme tersebut kemudian dibuka dengan command cat readme. Password untuk level selanjutnya terdapat di dalam file readme.

Log out dari lab bandit untuk melanjutkan ke level selanjutnya.

Level 1-> Level 2

Diberikan problem sebagai berikut.

The password for the next level is stored in a file called - located in the home directory

Log in SSH ke dalam bandit1@bandit.labs.overthewire.org dengan port 2220 dan dengan password sesuai yang telah didapatkan dalam level sebelumnya.

```
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat ./-
263JGJPfgU6LtdEvgfWU1XP5yac29mFx
```

Melihat file yang terdapat dalam directory dengan menggunakan command ls. Terlihat bahwa hanya terdapat satu file dalam directory tersebut, yaitu file -. Kemudian file - bisa dibuka dengan command cat ./- karena sebenarnya dash (-) merupakan suatu reserved symbol di dalam terminal jadi tidak bisa dibuka/dilihat hanya dengan command cat saja.

Level 2-> Level 3

Diberikan problem sebagai berikut.

The password for the next level is stored in a file called spaces in this filename located in the home directory



Login ke dalam ssh dan connect ke bandit lab dengan port 2220 dan dengan password yang telah ditemukan dalam level sebelumnya.

Lihat file yang ada di dalam directory dengan menggunakan command ls. Dalam directory hanya ditemukan satu file, yaitu 'spaces in this filename'. Karena nama file mengandung spasi maka isi dalam file dapat dilihat dengan menggunakan command cat "spaces in this filename". Password berhasil ditemukan dalam file tersebut.

Setelah password ditemukan, logout dari ssh bandit2.

Level 3-> Level 4

Diberikan problem sebagai berikut.

The password for the next level is stored in a hidden file in the inhere directory.

Login ke dalam ssh dan connect ke bandit lab dengan port 2220 dan dengan password yang telah ditemukan dalam level sebelumnya.

```
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cat inhere
cat: inhere: Is a directory
bandit3@bandit:~$ cd inhere
```

Lihat file/directory yang ada di dalam directory utama dengan menggunakan command ls. Kemudian masuk dalam directory inhere dengan perintah cd inhere.

```
bandit3@bandit:~/inhere$ ls -la
total 12
drwxr-xr-x 2 root root 4096 Sep 19 07:08 .
drwxr-xr-x 3 root root 4096 Sep 19 07:08 ..
-rw-r 1 bandit4 bandit3 33 Sep 19 07:08 ... Hiding-From-You
bandit3@bandit:~/inhere$ cat ... Hiding-From-You
2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
bandit3@bandit:~/inhere$
```

Lihat isi dari directory inhere secara detail dengan command ls —la yang bisa digunakan untuk melihat file yang bersifat hidden atau file yang namanya didahului dengan titik. Sebenarnya menggunakan command ls —a saja cukup untuk mencari hidden file, tetapi akan lebih baik dan lebih detail jika dilengkapi dengan command ls —la. Dari isi directory, dapat dilihat bahwa terdapat file probable yang bernama ...Hiding-From-You. Kemudian lihat isi dari file tersebut dengan menggunakan perintah cat. Password berhasil didapatkan.

Setelah password didapatkan, logout dari ssh bandit3.

Level 4-> Level 5

Diberikan problem sebagai berikut.

The password for the next level is stored in the only human-readable file in the inhere directory. Tip: if your terminal is messed up, try the "reset" command.



Login ke dalam ssh dan connect ke bandit lab dengan port 2220 dan dengan password yang telah ditemukan dalam level sebelumnya.

```
bandit4@bandit:~$ ls
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls
-file00 -file01 -file02 -file03 -file04 -file05 -file06 -file07 -file08 -file09
bandit4@bandit:~/inhere$ file ./*
./-file00: data
./-file01: data
 /-file02: data
./-file03: data
./-file04: data
 /-file05: data
./-file06: data
./-file07: ASCII text
./-file08: data
./-file09: data
bandit4@bandit:~/inhere$ cat ./-file07
4oQYVPkxZ00E005pTW81FB8j8lxXGUQw
```

Lihat isi dari directory menggunakan command ls. Kemudian masuk ke dalam directory inhere dengan command cd inhere dan melihat isi dari directory tersebut. Karena clue dalam soal adalah password disimpan dalam bentuk human readable file maka file dapat dicari menggunakan command file ./* dan didapatkan file ./-file07 yang berbentuk ASCII. Kemudian lihat isi dari file tersebut dengan command cat. Password berhasil ditemukan.

Logout dari ssh bandit4 untuk melanjutkan ke level berikutnya.

Level 5-> Level 6

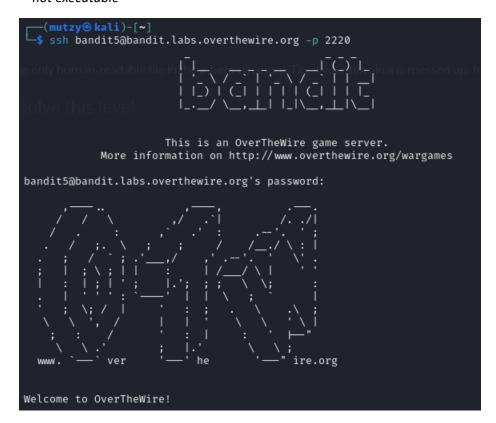
Diberikan problem sebagai berikut.

The password for the next level is stored in a file somewhere under the inhere directory and has all of the following properties:

human-readable

1033 bytes in size

not executable



Login ke dalam ssh dan connect ke bandit lab dengan port 2220 dan dengan password yang telah ditemukan dalam level sebelumnya.

```
bandit5@bandit:~$ find inhere -type f -size 1033c ! -executable
inhere/maybehere07/.file2
bandit5@bandit:-$ cat inhere/maybehere07/.file2
HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
bandit5@bandit:~$ bandit5@bandit:~$
```

Cari file sesuai kriteria spesifik yang sudah dicantumkan dalam soal, yaitu human-readable, 1033 bytes in size, not executable menggunakan command find inhere -type f -size 1033c ! -executable

inhere dalam command tersebut merupakan directory tempat file yang akan dicari, -type f berarti mencari file atau bukan berupa folder, -size 1033c berarti mencari file yang ukurannya 1033 bytes (c dalam 1033c merupakan bytes), dan! -executable berarti tidak mencari atau sedang mengecualikan file yang executable atau file yang bisa dieksekusi. Dari command tersebut didapatkan bahwa file yang dimaksud berada di path inhere/maybehere07/.file2. Kemudian lihat isi dari file tersebut menggunakan command cat. Password untuk level selanjutnya berhasil didapatkan.

Setelah password didapatkan, logout dari ssh bandit5 untuk melanjutkan ke level berikutnya.

Level 6-> Level 7

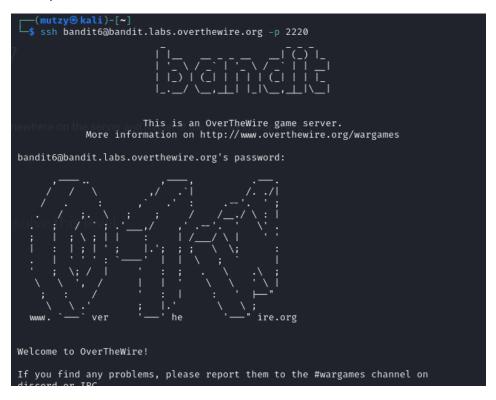
Diberikan problem sebagai berikut.

The password for the next level is stored somewhere on the server and has all of the following properties:

owned by user bandit7

owned by group bandit6

33 bytes in size



Login ke dalam ssh dan connect ke bandit lab dengan port 2220 dan dengan password yang telah ditemukan dalam level sebelumnya.

```
andit:~$ find / -type f -user bandit7 -group bandit6 -size 33c
find: '/drifter/drifter14_src/axTLS': Permission denied
find: '/root': Permission denied
find: '/snap': Permission denied
find: '/tmp': Permission denied
find: '/tmp': Permission denied
find: '/proc/tty/driver': Permission denied
find: '/proc/2794150/task/2794150/fdinfo/6': No such file or directory
 find: '/proc/2794150/fdinfo/5': No such file or directory
find: /proc/2794130/Td.hindy 3. No such lite of
find: '/home/bandit31-git': Permission denied
find: '/home/bandit5/inhere': Permission denied
find: '/home/bandit3/o-git': Permission denied
find: '/home/bandit30-git': Permission denied
find: '/home/bandit30-git': Permission denied
find: '/home/drifter8/chroot': Permission denied
find: '/home/bandit29-git': Permission denied
find: '/home/bandit28-git': Permission denied
find: '/home/bandit28-git': Permission denied
find: '/home/bandit27-git': Permission denied
find: '/lost+found': Permission denied
find: '/etc/polkit-1/rules.d': Permission denied
find: '/etc/polkit-1/rules.d': Permission denied
find: '/etc/multipath': Permission denied
find: '/etc/mattipath': Permission denied find: '/etc/xinetd.d': Permission denied
 find: '/etc/credstore.encrypted': Permission denied
find: '/etc/ssl/private': Permission denied
find: '/etc/sudoers.d': Permission denied
find: '/etc/credstore': Permission denied
find: '/dev/shm': Permission denied
find: '/dev/mqueue': Permission denied
find: '/var/log/amazon': Permission denied
 find: '/var/log/unattended-upgrades': Permission denied
find: '/var/log/chrony': Permission denied
find: '/var/log/private': Permission denied
find: '/var/tmp': Permission denied
find: '/var/tmp': Permission denied
find: '/var/spool/cron/crontabs': Permission denied
find: '/var/spool/cron/crontabs': Permission denied
find: '/var/spool/bandit24': Permission denied
find: '/var/spool/rsyslog': Permission denied
find: '/var/cache/ldconfig': Permission denied
find: '/var/cache/apt/archives/partial': Permission denied
find: '/var/cache/pollinate': Permission denied find: '/var/cache/private': Permission denied
find: '/var/cache/apparmor/2425d902.0': Permission denied find: '/var/cache/apparmor/baad73a1.0': Permission denied find: '/var/lib/polkit-1': Permission denied
             '/var/lib/amazon': Permission denied
 /var/lib/dpkg/info/bandit7.password
/var/lib/aps/lm/o/damit/.jassword
find: '/var/lib/apt/lists/partial': Permission denied
find: '/var/lib/chrony': Permission denied
find: '/var/lib/snapd/void': Permission denied
find: '/var/lib/snapd/cookie': Permission denied
find: '/var/lib/private': Permission denied
              '/var/lib/ubuntu-advantage/apt-esm/var/lib/apt/lists/partial': Permission denied
              '/var/lib/update-notifier/package-data-downloads/partial': Permission denied
```

Dari clue yang ada di dalam soal, kita dapat mencoba mencari file dengan command find / -type f - user bandit7 -group bandit6 -size 33c dan ternyata ditemukan banyak sekali line yang berisi permission denied. Karena kita tidak mungkin untuk mencari password dengan membaca satu per satu line tersebut, maka kita bisa menambahkan command menjadi find / -type f -user bandit7 -group bandit6 -size 33c 2>/dev/null.

```
bandit6@bandit:~$ find / -type f -user bandit7 -group bandit6 -size 33c 2>/dev/null
/var/lib/dpkg/info/bandit7.password
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj
bandit6@bandit:~$
```

Slash (/) dalam command ini berfungsi untuk mencari file mulai dari root, -type f untuk mencari jenis file, -user bandit7 untuk mencari file yang dimiliki oleh user bandit7, -group bandit6 berarti mencari file yang dimiliki oleh user yang berada dalam group bandit6, size 33c berarti bahwa file yang dicari memiliki ukuran 33 bytes, dan 2>/dev/null berarti bahwa kita mengecualikan semua file yang error (2> merupakan standar error atau stderr) kemudian dimasukkan ke dalam dev/null yang merupakan 'tempat pembuangan di linux'. Password berhasil ditemukan dengan menggunakan command tersebut.

Logout dari ssh bandit6 untuk melanjutkan ke level berikutnya.

Level 7-> Level 8

Diberikan problem sebagai berikut.

The password for the next level is stored in the file data.txt next to the word millionth



Login ke dalam ssh dan connect ke bandit lab dengan port 2220 dan dengan password yang telah ditemukan dalam level sebelumnya.

```
bandit7@bandit:~$ ls
data.txt
bandit7@bandit:~$ cat data.txt
               MBLQ2×4SPU4Y6XIscWooXopjdSntWOhY
momentary
vicuña 6nKKKgzHbJvPFsEFQgzd2wqJWcv8TGGQ
               ZhOy86fNIP8sWsOLLYiHrtjRsrpu1bND
equities
various Eg1ZcmYmpvkXS10Vu04areb2hhT9Pkft
redefinition's vPzYXGDGwByIVBRIKQDRHn5xgoekZKME
Allison 4JPUMGRznD4JAyy1SX2Cf5zAwEhT7AP7
compels 8XgWaEyaUVmm1FLZksXE6vRBAKfm7xGB
misstep 0p0wfzDrUfyAbU6V5MVGlrvDKjmc6a0Z
coagulating
               Ff0C46bf0MzwOojIDTWJAq9059WdKSdw
Onega's YiR7TkXXHKpt0Oqs2EtFzRSXu8XGCqQA
checkmate
                XjaNSCEGpEdkJIMfCnwWGJuRQ6fUIoUq
Lyndon 7m6zWzaFwemeBJ7jKzX01REfc9QtC9SQ
                j1kdDmGHBGtcor81a2lIZzVd9ulFtifz
archivist
Jerri's 2fCe8FdpTJFt4gtanwmG7a8A1AYlEpDQ
underarms
                ZSucs304S5mq2TONuDqpN5gwz7HsbCOQ
scrooge SYI06iTGl1SdxwJV21kH4fty0AAer8Rv
Elnora i1GGmWJChr5PUq8N8s9nt6nhYvoUtoRu
salver uZf07mMWSaF4hLwFmGKIKt0grSeTIPjy
                rgsv70D3SHSx60IfJTpI4p60BApa0sEI
hemorrhaged
fount's U4XHsnP97Bg0I3v027KBrpwtMvR9qF1I
               OOgaDupjr2RbwoOA98oN4jzlYq2Q1Rwc
autograph's
tranquillizes
                5ncuXd3UAIy3S0QRnVS8s3Sp7iEb0hrX
edgiest OJtPY7WKKVMFSkTHwYTUnWoZzRIQ76Ii
       C8GP1U4YQzLz6wdWbKsWBexSS361WShV
inconvenience's kJM03FuxWnwIyXy0Q3CgUjMM4RKPnyGc
hurled fYt4KTyYNxGpjSagdMXaggeaF1lj5TP1
strollers
               Gf1nIaOalC8w7MfeHQbFSRbmBdvK6MLk
Lincoln's
               HoRRZZXAEt2v03wM51A4sfCukDlHLlMy
               Qi4hcuzmfLfi79r0r1WqtE99n0Cxih5c
showerier
       ZoXDgeBUXPiKQIquLtWwqM1ZI8jzdkzF
Head
               mQGJw2ifm0p6Y6jPBPtLr679JY3gz0Mc
Mormonism's
riming fUq82ZhW36YYujQ0RhvzvxWEBH1E7ffM
eviscerating
                55uIcXOb4z4JJ8nOrVsqIm2GUF4Swhom
```

Melihat isi dari directory dengan command Is dan hanya ditemukan file data.txt. Namun saat dibuka, file data.txt ternyata memiliki banyak sekali line yang tidak mungkin dibaca satu per satu untuk menemukan passwordnya.

```
bandit7@bandit:~$ grep "millionth" data.txt
millionth dfwvzFQi4mU0wfNbF0e9RoWskMLg7eEc
bandit7@bandit:~$
```

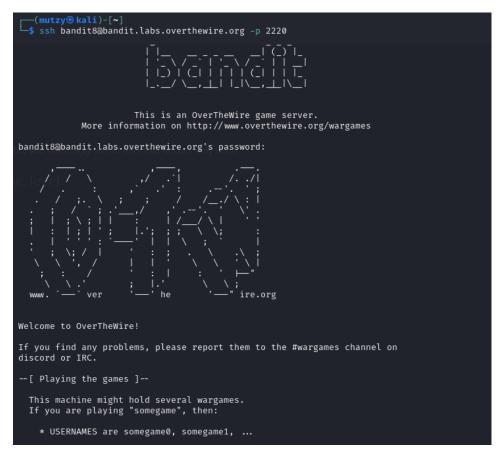
Hal ini bisa diatasi dengan menggunakan command grep untuk menemukan pattern teks/string yang dicari. Dalam problem ini dapat menggunakan command grep "millionth" data.txt untuk mencari password yang berada di sebelah string millionth. Dengan demikian password berhasil ditemukan.

Setelah password ditemukan, logout dari ssh bandit7 untuk melanjutkan ke level berikutnya.

Level 8-> Level 9

Diberikan problem sebagai berikut.

The password for the next level is stored in the file data.txt and is the only line of text that occurs only once



Login ke dalam ssh dan connect ke bandit lab dengan port 2220 dan dengan password yang telah ditemukan dalam level sebelumnya.

```
bandit8@bandit:~$ ls
data.txt
bandit8@bandit:~$ sort data.txt | uniq -u
4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
bandit8@bandit:~$
```

Di dalam soal telah diberitahu bahwa password disimpan di dalam file data.txt dan password berada di dalam line yang tidak ada duplikasinya. Dengan clue ini kita bisa mencari password dengan menggunakan command sort data.txt | uniq -u.

sort data.txt berarti isi dalam file data.txt diurutkan, kemudian uniq -u berarti menampilkan line yang muncul sekali. Dengan command tersebut, password berhasil ditemukan.

Logout dari ssh bandit8 untuk melanjutkan ke level berikutnya.

Level 9-> Level 10

Diberikan problem sebagai berikut.

The password for the next level is stored in the file data.txt in one of the few human-readable strings, preceded by several '=' characters.

Login ke dalam ssh dan connect ke bandit lab dengan port 2220 dan dengan password yang telah ditemukan dalam level sebelumnya.

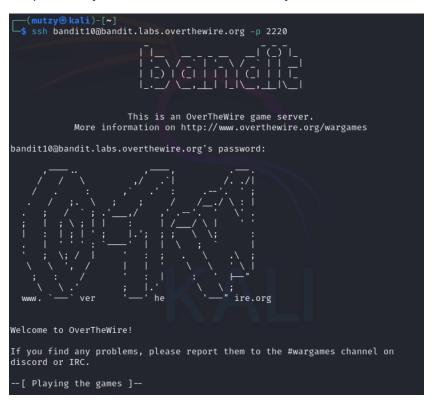
Sesuai dengan clue yang telah dicantumkan dalam problem, password diletakkan dalam file data.txt dan di dalam sebuah human readable strings yang dilalui dengan beberapa tanda '='. Dari clue tersebut, kita bisa mencari password dengan command strings data.txt | grep "====".strings data.txt berarti kita ingin menemukan seluruh string yang ada di dalam data.txt dan grep "===" berarti kita hanya ingin mencari atau memfilter suatu string yang memiliki tanda "===" di dalamnya. Password berhasil ditemukan.

Setelah password ditemukan, logout dari ssh bandit9 untuk melanjutkan ke level berikutnya.

Level 10-> Level 11

Diberikan problem sebagai berikut.

The password for the next level is stored in the file data.txt, which contains base64 encoded data



Login ke dalam ssh dan connect ke bandit lab dengan port 2220 dan dengan password yang telah ditemukan dalam level sebelumnya.

```
bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ cat data.txt | base64 -d
The password is dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr
bandit10@bandit:~$
```

Untuk mencari password di dalam file data.txt yang mengandung data encoded base64, kita bisa melakukannya dengan command cat data.txt | base64 -d.

cat data.txt berfungsi untuk melihat isi dari file data.txt dan base64 —d digunakan untuk decode teks base64 menjadi kembali ke bentuk aslinya.

Verifikasi password:



Bandit11 dapat terbuka dengan password yang didapatkan dalam bandit10, hal ini berarti password benar/valid.