OverTheWire Bandit

WRITE-UP

PERTEMUAN 2

Muhamad Rizki Maulana

Dokumen ini berisi dokumentasi penyelesaian OverTheWire Bandit sebagai bagian dari pembelajaran Penetration Testing Fundamental.

Tantangan ini melatih:

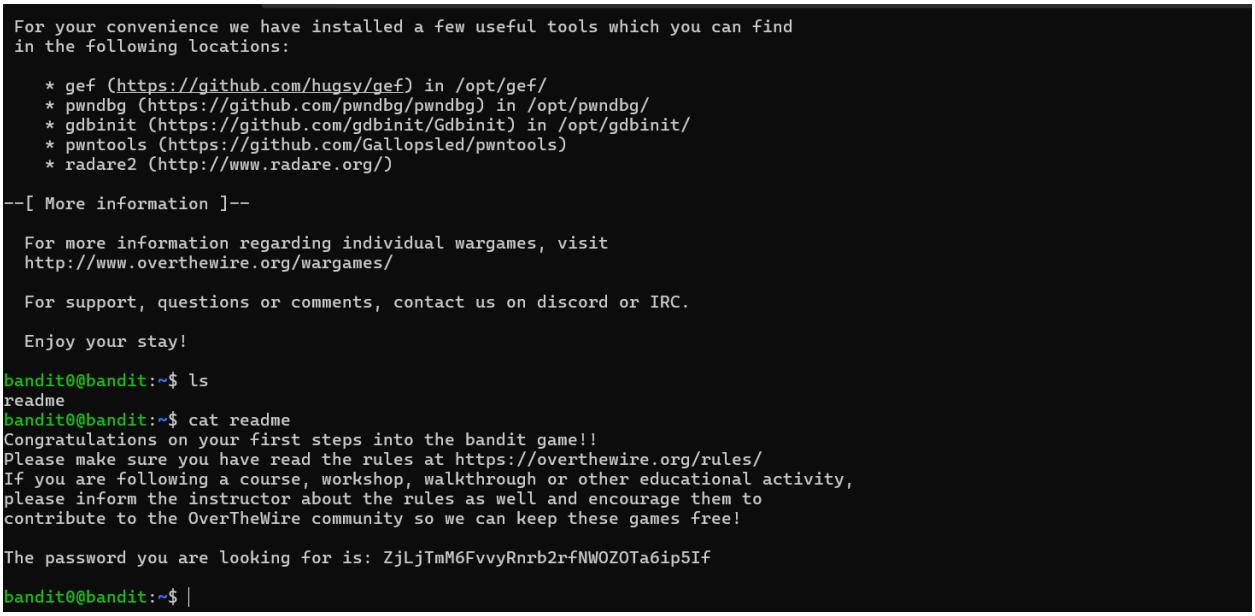
- File handling
- Permission analysis
- Encoding & decoding
- Compression analysis
- Networking dan SSL communication

Langkah-langkah:

1. Level 0 – 1

Tujuan: Login pertama ke server menggunakan SSH dan membaca file readme.

Command: ssh bandit0@bandit.labs.overthewire.org -p 2202, ls, dan cat readme.



Setelah membaca file readme, muncul password yang digunakan untuk login ke level berikutnya.

2. Level 1 – 2

Tujuan: Membaca file Bernama “-“

Command: ls dan cat ./-

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

Isi file tersebut menampilkan password untuk masuk ke level 2

3. Level 2 – 3

Tujuan: membaca file dengan nama yang memiliki spasi

Command: ls dan cat – "--spaces in this filename--"

```
bandit2@bandit:~$ ls
--spaces in this filename--
```

```
bandit2@bandit:~$ cat -- "--spaces in this filename--"
MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx
```

File terebut berisi password untuk level 3

4. Level 3 – 4

Tujuan Menemukan hidden file di dalam folder

Command: cd inhere, ls -a, dan cat …Hiding-From-You

```
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ ls -a
.  ..  ...Hiding-From-You
```

```
bandit3@bandit:~/inhere$ cat ...Hiding-From-You
2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
```

Isi file hidden tersebut adalah password untuk level 4.

5. Level 4 – 5

Menemukan file readable di antara beberapa file binary

Command: cd inhere, file *, dan cat <file_yang_bertipe_ASCII>

```
bandit4@bandit:~$ ls
inhere
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls -a
.  ..  -file00  -file01  -file02  -file03  -file04  -file05  -file06  -file07  -file08  -file09
bandit4@bandit:~/inhere$ cat ./-file07
4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw
```

File ASCII tersebut berisi password untuk level 5

6. Level 5 – 6

Tujuan: mencari file dengan ukuran 10300 bytes dan bukan executable

Command: find . -type f -size 1033c ! -executable dan cat <file>

```
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls - a
ls: cannot access '-': No such file or directory
ls: cannot access 'a': No such file or directory
bandit5@bandit:~/inhere$ ls -a
.           maybehere01  maybehere04  maybehere07  maybehere10  maybehere13  maybehere16  maybehere19
..          maybehere02  maybehere05  maybehere08  maybehere11  maybehere14  maybehere17
maybehere00  maybehere03  maybehere06  maybehere09  maybehere12  maybehere15  maybehere18
bandit5@bandit:~/inhere$ find . -type f -size 1033c ! -executable
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
```

File yang ditemukan berisi password untuk level 6

7. Level 6 – 7

Tujuan: mencari file berdasarkan owner dan group tertentu

Command: find . -type f -size 1033c ! -executable, cat <file_ditemukan>.

```
bandit6@bandit:~$ ls
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
```

Isi file tersebut adalah password untuk level 7

8. Level 7 – 8

Tujuan: mencari password dalam file data.txt berdasarkan keyword tertentu

Command: grep millionth data.txt

```
bandit7@bandit:~$ ls
data.txt
bandit7@bandit:~$ grep millionth data.txt
millionth       dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
bandit7@bandit:~$
```

Baris yang ditemukan berisi password untuk level 8

9. Level 8 – 9

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

Baris unik tersebut adalah password untuk level 9

10. Level 9 – 10

Tujuan: Mencari string readable dalam file binary

Command: strings data.txt | grep =

```
bandit9@bandit:~$ ls
data.txt
bandit9@bandit:~$ strings data.txt
{7(b
FB`=
F`qYJ
%I"r
~5m~
iy\3
L^G^
@shLq
tC5!
G       2)
lHQS
5@8Y;)$X
c\5D=
7r}Q
TN#,p
b5A5
o 3`
hvSB
========== the
(V_g
{"%z
yzJq
%x"R
```

11. Level 10 – 11

Tujuan: decode file yang dienkripsi menggunakan base64

Command: base64 -d data.txt

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

String yang ditemukan merupakan password untuk level 10

12. Level 11 – 12

Tujuan decode hasil yang menggunaka ROT13 cipher.

Command: cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'

```
bandit11@bandit:~$ ls
data.txt
bandit11@bandit:~$ cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'
The password is 7x16WNeHIi5YkIhWsfFIqoognUTyj9Q4
```

Hasil decoding merupakan password untuk level 12

13. Level 12 – 13

Tujuan: extract file dengan multiple compression layer

Command: xxd -r data.txt > file, file file, gunzip, bunzip2, tar -xf

```
bandit12@bandit:~$ ls
data.txt
bandit12@bandit:~$ mkdir /tmp/aquaa
bandit12@bandit:~$ cd /tmp/aquaa
bandit12@bandit:/tmp/aquaa$ cp ~/data.txt .
bandit12@bandit:/tmp/aquaa$ ls
data.txt
bandit12@bandit:/tmp/aquaa$ xxd -r data.txt > file
bandit12@bandit:/tmp/aquaa$ xxd -r data.txt > file
bandit12@bandit:/tmp/aquaa$ file file
file: gzip compressed data, was "data2.bin", last modified: Tue Oct 14 09:26:00 2025, max compression, from Unix, origin
al size modulo 2^32 572
bandit12@bandit:/tmp/aquaa$ mv file file.gz
bandit12@bandit:/tmp/aquaa$ gunzip file.gz
bandit12@bandit:/tmp/aquaa$ file file
file: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/aquaa$ mv file file.bz2
bandit12@bandit:/tmp/aquaa$ bunzip2 file.bz2
bandit12@bandit:/tmp/aquaa$ file file
file: gzip compressed data, was "data4.bin", last modified: Tue Oct 14 09:26:00 2025, max compression, from Unix, origin
al size modulo 2^32 20480
bandit12@bandit:/tmp/aquaa$ file file
file: gzip compressed data, was "data4.bin", last modified: Tue Oct 14 09:26:00 2025, max compression, from Unix, origin
al size modulo 2^32 20480
bandit12@bandit:/tmp/aquaa$ mv file file.gz
bandit12@bandit:/tmp/aquaa$ gunzip file.gz
bandit12@bandit:/tmp/aquaa$ file file
file: POSIX tar archive (GNU)
```

```
bandit12@bandit:/tmp/aquaa$ mv data6 data6.gz
bandit12@bandit:/tmp/aquaa$ gunzip data6.gz

gzip: data6.gz: not in gzip format
bandit12@bandit:/tmp/aquaa$ tar -xf data6
tar: data6: Cannot open: No such file or directory
tar: Error is not recoverable: exiting now
bandit12@bandit:/tmp/aquaa$ ls
data5.bin  data6.gz  data.txt  file
bandit12@bandit:/tmp/aquaa$ mv data6.gz data6
bandit12@bandit:/tmp/aquaa$ file data6
data6: POSIX tar archive (GNU)
bandit12@bandit:/tmp/aquaa$ ls
data5.bin  data6  data.txt  file
bandit12@bandit:/tmp/aquaa$ tar -xf data6
bandit12@bandit:/tmp/aquaa$ ls
data5.bin  data6  data8.bin  data.txt  file
bandit12@bandit:/tmp/aquaa$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Tue Oct 14 09:26:00 2025, max compression, from Unix,
riginal size modulo 2^32 49
bandit12@bandit:/tmp/aquaa$ mv data8.bin data8.gz
bandit12@bandit:/tmp/aquaa$ gunzip data8.gz
bandit12@bandit:/tmp/aquaa$ ls
data5.bin  data6  data8  data.txt  file
bandit12@bandit:/tmp/aquaa$ file data8
data8: ASCII text
```

```
bandit12@bandit:/tmp/aquaa$ cat data8
The password is FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn
```

Ulangi proses extract sesuai tipe file sampai datap ASCII text dan file akhir berisi password untuk ke level 13

14. Level 13 – 14

Tujuan: login menggunakan SSH private key

Command: ssh -i sshkey.private bandit14@bandit.labs.overthewire.org -p 2220

```
bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ cat sshkey .private
cat: sshkey: No such file or directory
cat: .private: No such file or directory
bandit13@bandit:~$ cat sshkey.private
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAxkkOE83W2cOT7IWhFc9aPaaQmQDdgzuXCv+ppZHa++buSkN+
gg0tcr7Fw8NLGa5+Uzec2rEg0WmeevB13AIoYp0MZyETq46t+jk9puNwZwIt9XgB
ZufGtZEwWbFWw/vVLNwOXBe4UWStGRWzgPpEeSv5Tb1VjLZIBdGphTIK22Amz6Zb
ThMsiMnyJafEwJ/T8PQO3myS91vUHEuoOMAzoUID4kN0MEZ3+XahyK0HJVq68KsV
ObefXG1vvA3GAJ29kxJaqvRfgYnqZryWN7w3CHjNU4c/2Jkp+n8L0SnxaNA+WYA7
jiPyTF0is8uzMlYQ4l1Lzh/8/MpvhCQF8r22dwIDAQABAoIBAQC6dWBjhyEOzjeA
J3j/RWmap9M5zfJ/wb2bfidNpwbB8rsJ4sZIDZQ7XuIh4LfygoAQSS+bBw3RXvzE
pvJt3SmU8hIDuLsCjL1VnBY5pY7Bju8g8aR/3FyjyNAqx/TLfzlLYfOu7i9Jet67
xAh0tONG/u8FB5I3LAI2Vp6OviwvdWeC4nOxCthldpuPkNLA8rmMMVRTKQ+7T2VS
nXmwYckKUcUgzoVSpiNZaS0zUDypdpy2+tRH3MQa5kqN1YKjvF8RC47woOYCktsD
o3FFpGNFec9Taa3Msy+DfQQhHKZFKIL3bJDONtmrVvtYK40/yeU4aZ/HA2DQzwhe
ol1AfiEhAoGBAOnVjosBkm7sblK+n4IEwPxs8sOmhPnTDUy5WGrpSCrXOmsVIBUf
laL3ZGLx3xCIwtCnEucB9DvN2HZkupc/h6hTKUYLqXuyLD8njTrbRhLgbC9QrKrS
M1F2fSTxVqPtZDlDMwjNR04xHA/fKh8bXXyTMqOHNJTHHNhbh3McdURjAoGBANkU
1hqfnw7+aXncJ9bjysr1ZWbqOE5Nd8AFgfwaKuGTTVX2NsUQnCMWdOp+wFak40JH
PKWkJNdBG+ex0H9JNQsTK3X5PBMAS8AfX0GrKeuwKWA6erytVTqjOfLYcdp5+z9s
8DtVCxDuVsM+i4X8UqIGOlvGbtKEVokHPFXP1q/dAoGAcHg5YX7WEehCgCYTzpO+
xysX8ScM2qS6xuZ3MqUWAxUWkh7NGZvhe0sGy9iOdANzwKw7mUUFViaCMR/t54W1
GC83sOs3D7n5Mj8x3NdO8xFit7dT9a245TvaoYQ7KgmqpSg/ScKCw4c3eiLava+J
3btnJeSIU+8ZXq9XjPRpKwUCgYA7z6LiOQKxNeXH3qHXcnHok855maUj5fJNpPbY
iDkyZ8ySF8GlcFsky8Yw6fWCqfG3zDrohJ5l9JmEsBh7SadkwsZhvecQcS9t4vby
9/8X4jS0P8ibfcKS4nBP+dT81kkkg5Z5MohXBORA7VWx+ACohcDEkprsQ+w32xeD
qT1EvQKBgQDKm8ws2ByvSUVs9GjTilCajFqLJ0eVYzRPaY6f++Gv/UVfAPV4c+S0
```

Berhasil login ke 14 dan mendapatkan password level 14

15. Level 14 – 15

Tujuan: mengirim password ke service melalui TCP

Command: cat /etc/bandit_pass/bandit14, nc localhost 30000

```
bandit15@bandit:~$ ls
bandit15@bandit:~$ cat /etc/bandit_pass/bandit15
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo
bandit15@bandit:~$ openssl s_client -connect localhost:30001
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 CN = SnakeOil
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN = SnakeOil
verify return:1
---
Certificate chain
 0 s:CN = SnakeOil
   i:CN = SnakeOil
   a:PKEY: rsaEncryption, 4096 (bit); sigalg: RSA-SHA256
   v:NotBefore: Jun 10 03:59:50 2024 GMT; NotAfter: Jun  8 03:59:50 2034 GMT
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIFBzCCAu+gAwIBAgIUBLz7DBxA0IfojaL/WaJzE6Sbz7cwDQYJKoZIhvcNAQEL
BQAwEzERMA8GA1UEAwwIU25ha2VPaWwwHhcNMjQwNjEwMDM1OTUwWhcNMzQwNjA4
```

Server merespon dengan password untuk level 15.