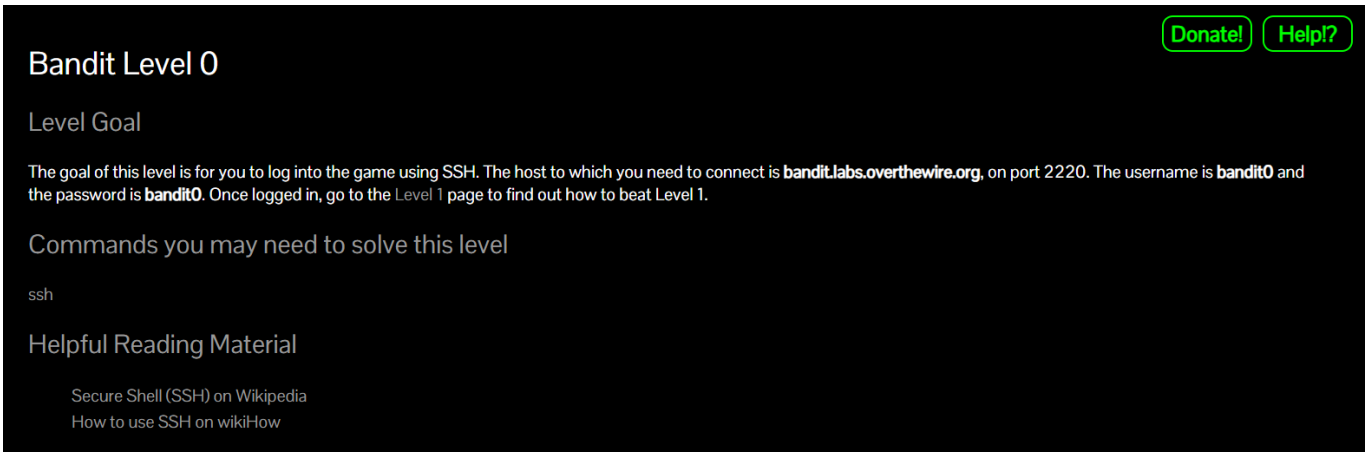
Overthewire - writeups CTF

- **Challenge:** Bandit Level 0 -> 33
- **Category:** Linux
- **Difficulty:** Easy
- **Source**: Overthewire

Note: Xin chào các bạn, đây là `writeup` đầu tiên mình viết khi mình bắt đầu với `CTF` và đặc biệt là `Pwnable`. Trong bài viết này, mình xin chia sẻ với mọi người về hướng tiếp cận và cách giải của mình về 34 level `bandit` ở trên OverTheWire. Các thử thách của bandit chủ yếu xoay quanh các lệnh linux cơ bản, thường hay sử dụng và quan trọng là nó sẽ giúp chúng ta thực hành các vấn đề liên quan về CTF. Vì là bài writeup đầu tiên mình viết nên mong mọi người góp ý.

Level 0

Level này yêu cầu mình sử dụng `ssh` để kết nối vào server `bandit.labs.overthewire.org` với port `2220`, username và password là `bandit0`.



Solution

Để kết nối vào server với cổng port 2220 ta sẽ sử dụng thêm option `-p 2220` (-p tức là port).

```
ssh bandit0@bandit.labs.overthewire.org -p 2220
```

Sau đó màn hình sẽ hiện ra yêu cầu nhập pass và khi đó ta chỉ cần nhập pass `bandit0` là được.

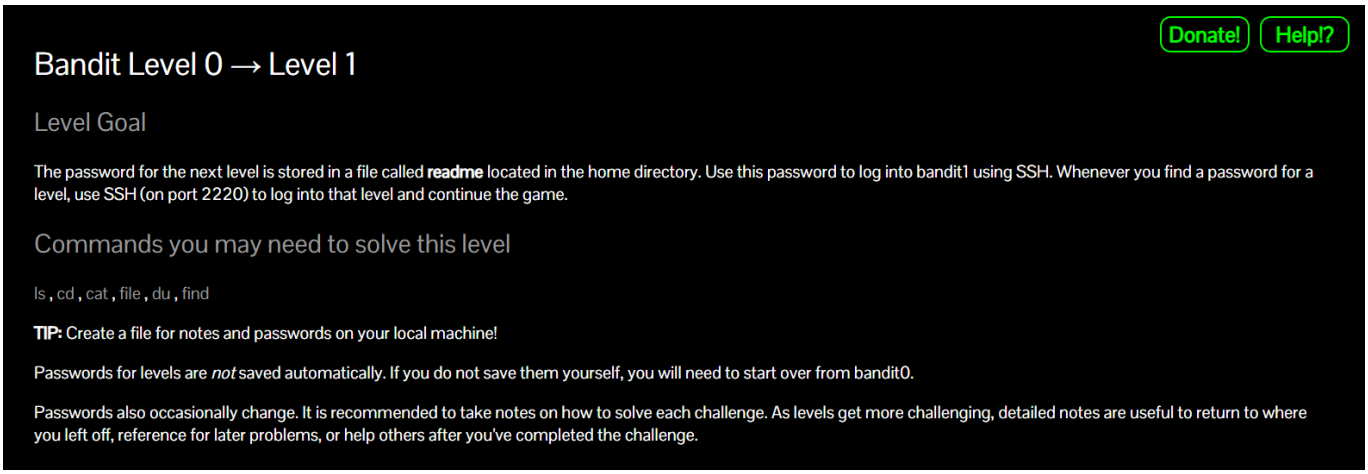
```
--[ Tools ]--

 For your convenience we have installed a few useful tools which you can find
 in the following locations:

    * gef (https://github.com/hugsy/gef) in /opt/gef/
    * pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
    * gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
    * pwntools (https://github.com/Gallopsled/pwntools)
    * radare2 (http://www.radare.org/)

--[ More information ]--

  For more information regarding individual wargames, visit
  http://www.overthewire.org/wargames/

  For support, questions or comments, contact us on discord or IRC.

  Enjoy your stay!

bandit0@bandit:~$
```

References

- Secure Shell (SSH) on Wikipedia
- How to use SSH on wikiHow

Level 0 -> level 1

Yeh, sau khi kết nối được vào server thì nó bảo có 1 file có tên là `readme` ngay tại thư mục `home` chứa password cho level tiếp theo. Và tương tự như vậy, dù ở bất cứ level nào, bạn cần tìm password được giấu ở đâu đó, sau đó `ssh` để kết nối tới level tiếp theo.



Solution

Trước khi giải quyết level này ta cần tìm hiểu về 1 số lệnh sau:

- `ls`: dùng để xem các file hiện có trong folder
- `cd`: dùng để di chuyển tới các folder cụ thể
- `cat`: dùng để xem nội dung của file
- `file`: dùng để xem kiểu file
- `du`: dùng để xem dung lượng file và folder
- `find`: dùng để tìm kiếm file và folder

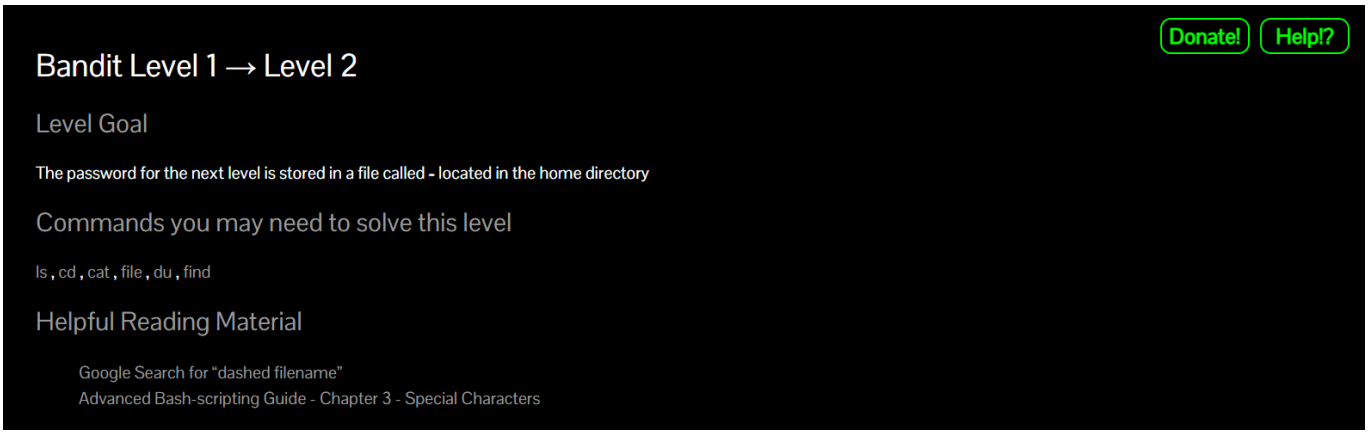
```
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
Congratulations on your first steps into the bandit game!!
Please make sure you have read the rules at https://overthewire.org/rules/
If you are following a course, workshop, walkthrough or other educational activity,
please inform the instructor 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:~$
```

Với 1 số lệnh trên, đầu tiên mình đã thử dùng `ls` để xem ở trong folder hiện tại có những file gì thì bất giờ file `readme` có ngay ở đây, và sau đó mình dùng `cat` để in ra nội dung của file `readme` đó.

Password cho level tiếp theo được hiện ra. (`ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If`)

Level 1 -> level 2

Level này yêu cầu ta mở file có tên là '`-`' được lưu trong folder `home`.



Solution

Đối với level này mình sẽ sử dụng lệnh `cat` để in password được lưu trong file '`-`' (dashed filename). Tuy nhiên, nếu mình sử dụng `cat -` như thông thường, thì nó sẽ không in ra gì cả vì nó sẽ hiểu một cách đặc biệt là lệnh đọc dữ liệu từ bàn phím (stdin) . Vậy nên nếu muốn in ra nội dung của file '`-`' ta cần chỉ rõ đường dẫn của file '`-`'.

Cụ thể: `cat ./-`

```
  For more information regarding individual wargames, visit
  http://www.overthewire.org/wargames/

  For support, questions or comments, contact us on discord or IRC.

  Enjoy your stay!

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

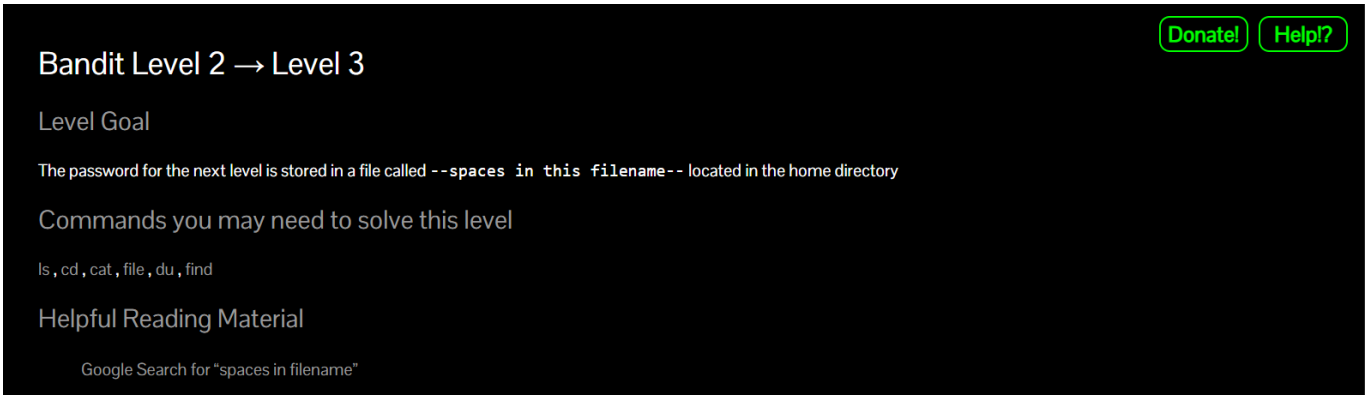
Password cho level tiếp theo được hiện ra. (`263JGJPfgU6LtdEvgfWU1XP5yac29mFx`)

References

- Google Search for "dashed filename"
- Advanced Bash-scripting Guide - Chapter 3 - Special Characters

Level 2 -> level 3

Level này yêu cầu ta mở file có tên là `--spaces in this filename--` được lưu trong folder `home`.



Solution

Đối với level này mình sẽ sử dụng `cat` để in password được lưu trong file `--spaces in this filename--` nhưng ta không thể truy cập folder hoặc file có khoảng cách 1 cách bình thường như vậy mà phải chỉ rõ đường dẫn file và thêm ký tự '`\`' vào trước mỗi khoảng cách.
Cụ thể: `cat ./--spaces\ in\ this\ filename--`

Ngoài ra, có 1 cách khác là mình có thể thêm 2 dấu nháy đơn(hoặc kép) vào 2 đầu của đường dẫn file đó.
Cụ thể: `cat './--spaces in this filename--`

```
bandit2@bandit:~$ ls
--spaces in this filename--
bandit2@bandit:~$ cat ./--spaces\ in\ this\ filename--
MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx
bandit2@bandit:~$ cat './--spaces in this filename--'
MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx
bandit2@bandit:~$
```

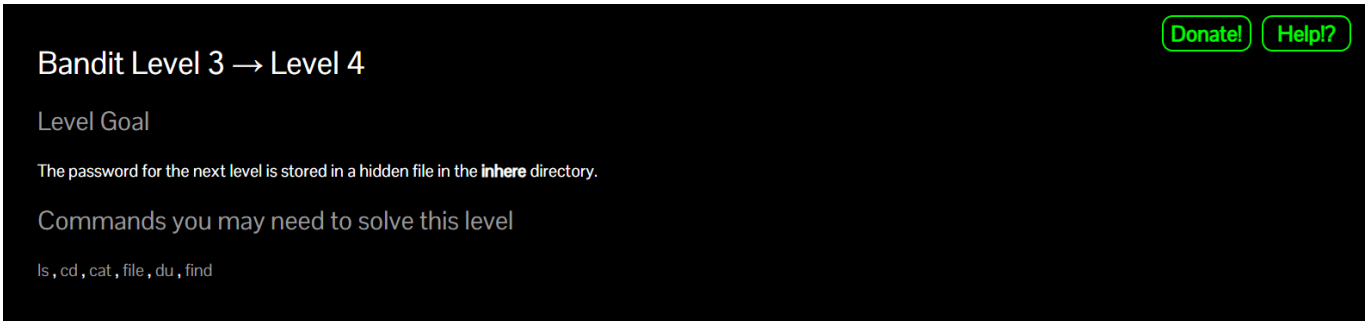
Password cho level tiếp theo được hiện ra. (`MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx`)

References

- Google Search for “spaces in filename”
- Dealing With Spaces in Filenames in Linux

Level 3 -> level 4

Level này yêu cầu ta mở hidden file được giấu trong folder `inhere` để lấy được password cho level tiếp theo.



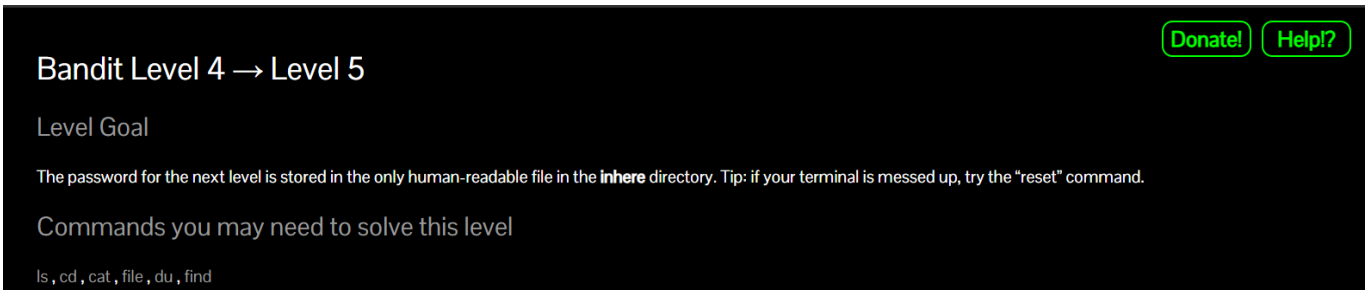
Solution

Đối với level này mình sẽ sử dụng `ls` để xem các file có trong folder `inhere` tuy nhiên, nếu chỉ sử dụng `ls` bình thường mà không truyền vào options nào thì nó sẽ không hiện đầy đủ các file (không hiện hidden file). Vì vậy, sau khi tìm hiểu thì mình thấy để hiện đầy đủ các file có trong 1 folder thì ta phải thêm option `-a` (all) vào.
Cụ thể: `ls -a inhere`

Password cho level tiếp theo được hiện ra. (`2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ`)

Level 4 -> level 5

Level này yêu cầu ta mở file duy nhất có thể đọc trong số các file ở trong folder `inhere` để có thể lấy được password cho level tiếp.



Solution

Như theo mô tả đề bài ta có thể thấy, chỉ có duy nhất 1 file có thể đọc. Vì vậy, ta sử dụng lệnh `file` để có thể in ra thông tin về file đó. Và đặc biệt hơn, trong bài này có tận 10 file khác nhau nên cách tốt nhất để in ra các thông tin của các file trong cùng 1 lần ta có thể truyền vào đường dẫn như sau.
Cụ thể: `file ./inhere/*`
`*` trong trường hợp này có ý nghĩa là nó sẽ bao gồm tất cả các file có ở trong folder `inhere`.

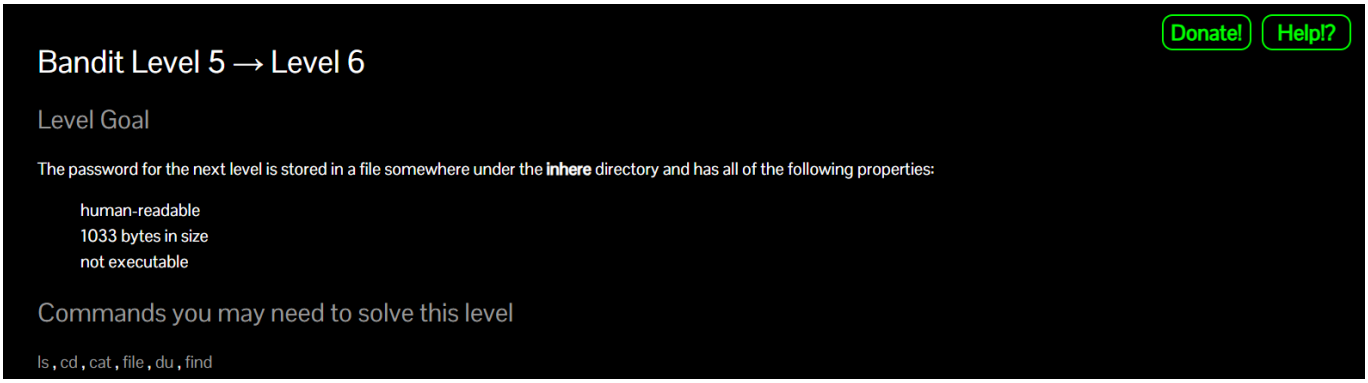
```
bandit4@bandit:~$ ls
inhere
bandit4@bandit:~$ file ./inhere/*
./inhere/-file00: data
./inhere/-file01: data
./inhere/-file02: data
./inhere/-file03: data
./inhere/-file04: data
./inhere/-file05: data
./inhere/-file06: data
./inhere/-file07: ASCII text
./inhere/-file08: data
./inhere/-file09: data
bandit4@bandit:~$ cat ./inhere/-file07
4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw
bandit4@bandit:~$
```

Password cho level tiếp theo được hiện ra. (`4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw`)

Level 5 -> level 6

Level này yêu cầu ta cần tìm password được lưu trong 1 file và được lưu dưới 1 folder. Ngoài ra, ta được cung cấp thêm thông tin là file đó có các thông tin về file như:

- human-readable (File đó có thể đọc)
- 1033 bytes in size (File có kích thước 1033byte)
- not executable (File đó không thể thực thi)



Solution

Dựa trên các thông tin mà file đó cung cấp, ta có thể brute-force để tìm file có đầy đủ các thông tin đó=)). Hoặc cách để tìm cách tốt hơn thì ta có thể lọc ra các file có các thông tin đó.

1. `human-readable`: ta có thể sử dụng lệnh `file` in ra thông tin các file sau đó kết hợp sử dụng lệnh `grep` để lọc ra các file có dạng dữ liệu là `ASCII text`.

Cụ thể: `file */* | grep "ASCII text"`

```
bandit5@bandit:~/inhere$ file */* |grep "ASCII text"
maybehere00/-file1:       ASCII text, with very long lines (1038)
maybehere00/-file2:       ASCII text, with very long lines (9387)
maybehere00/spaces file1: ASCII text, with very long lines (6117)
maybehere00/spaces file2: ASCII text, with very long lines (6849)
maybehere01/-file1:       ASCII text, with very long lines (6027)
maybehere01/-file2:       ASCII text
maybehere01/spaces file1: ASCII text, with very long lines (4138)
maybehere01/spaces file2: ASCII text, with very long lines (4542)
maybehere02/-file1:       ASCII text, with very long lines (3800)
maybehere02/spaces file1: ASCII text, with very long lines (6745)
maybehere02/spaces file2: ASCII text, with very long lines (8487)
maybehere03/-file1:       ASCII text, with very long lines (314)
maybehere03/-file2:       ASCII text, with very long lines (6594)
maybehere03/spaces file1: ASCII text, with very long lines (2189)
maybehere03/spaces file2: ASCII text, with very long lines (3384)
maybehere04/-file1:       ASCII text, with very long lines (4409)
maybehere04/-file2:       ASCII text, with very long lines (2618)
maybehere04/spaces file1: ASCII text, with very long lines (5531)
maybehere04/spaces file2: ASCII text, with very long lines (2490)
maybehere05/-file1:       ASCII text, with very long lines (2345)
maybehere05/-file2:       ASCII text, with very long lines (5958)
maybehere05/spaces file1: ASCII text, with very long lines (879)
maybehere05/spaces file2: ASCII text, with very long lines (2419)
maybehere06/-file1:       ASCII text, with very long lines (5730)
maybehere06/-file2:       ASCII text, with very long lines (1075)
```

2. `1033 bytes in size`: ta có thể sử dụng lệnh `find` để tìm các file với option `-size 1033c`. (1033c tức là 1033bytes)

   Cụ thể: `find . -size 1033c`

```
bandit5@bandit:~/inhere$ find -size 1033c
./maybehere07/.file2
bandit5@bandit:~/inhere$
```

3. `not executable`: ta có thể sử dụng lệnh `find` để tìm các file với option `-executable`. (File không thể thực thi)

   Cụ thể: `find . -executable`

```
bandit5@bandit:~/inhere$ find ! -executable
./maybehere18/-file2
./maybehere18/spaces file2
./maybehere18/.file2
./maybehere05/-file2
./maybehere05/spaces file2
./maybehere05/.file2
./maybehere08/-file2
./maybehere08/spaces file2
./maybehere08/.file2
./maybehere13/-file2
./maybehere13/spaces file2
./maybehere13/.file2
./maybehere16/-file2
./maybehere16/spaces file2
./maybehere16/.file2
./maybehere14/-file2
./maybehere14/spaces file2
./maybehere14/.file2
./maybehere07/-file2
./maybehere07/spaces file2
./maybehere07/.file2
./maybehere00/-file2
```

Như vậy, đối với 2 thông tin `human-readable` và `not executable` thì có rất nhiều file có thông tin đó, tuy nhiên đối với thông tin `1033 bytes in size` thì chỉ có duy nhất 1 file là `./maybehere07/.file2`. Vì vậy ta có thể chọn thông tin này để tìm kiếm file đó là cách tốt nhất.

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

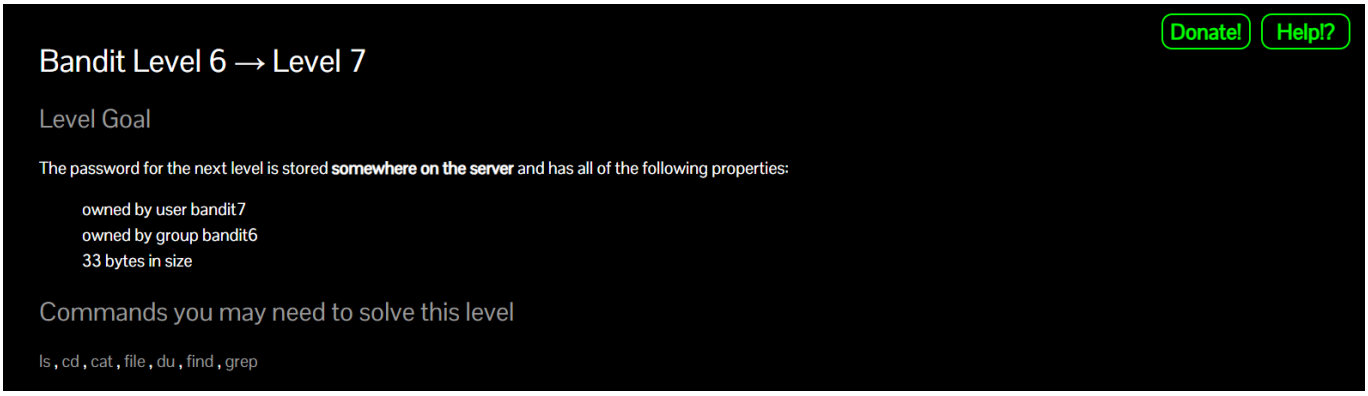
```
bandit5@bandit:~/inhere$
```

Password cho level tiếp theo được hiện ra. (`HWasnPhtq9AVKe0dmk45nxy20cvUa6EG`)

Level 6 -> level 7

Level này yêu cầu ta cần tìm password được giấu trong 1 file, và file được lưu ở đâu đó trong server. Và file đó có các thông tin như sau:

- owned by user bandit7 (thuộc sở hữu của người dùng bandit7)
- owned by group bandit6 (thuộc sở hữu của nhóm bandit6)
- 33 bytes in size: file có kích thước là 33 bytes



Solution

Như ta có thể thấy ở trên ta đã được cung cấp 3 thông tin về user, group và size. Vì thế, mình đã sử dụng lệnh `find` để tìm file có đầy đủ các thông tin đó.
Cụ thể: `find -user bandit7 -group bandit6 -size 33c`

- option -user: tìm theo người dùng sở hữu
- option -group: tìm theo nhóm sở hữu
- option -size: tìm theo kích thước

```
bandit6@bandit:/$ find -user bandit7 -group bandit6 -size 33c
find: ‘./sys/kernel/tracing/osnoise’: Permission denied
find: ‘./sys/kernel/tracing/hwlat_detector’: Permission denied
find: ‘./sys/kernel/tracing/instances’: Permission denied
find: ‘./sys/kernel/tracing/trace_stat’: Permission denied
find: ‘./sys/kernel/tracing/per_cpu’: Permission denied
find: ‘./sys/kernel/tracing/options’: Permission denied
find: ‘./sys/kernel/tracing/rv’: Permission denied
find: ‘./sys/kernel/debug’: Permission denied
find: ‘./sys/fs/pstore’: Permission denied
find: ‘./sys/fs/bpf’: Permission denied
find: ‘./root’: Permission denied
find: ‘./boot/lost+found’: Permission denied
find: ‘./boot/efi’: Permission denied
find: ‘./run/udisks2’: Permission denied
find: ‘./run/chrony’: Permission denied
find: ‘./run/user/5008’: Permission denied
find: ‘./run/user/5007’: Permission denied
find: ‘./run/user/5006’: Permission denied
find: ‘./run/user/5005’: Permission denied
find: ‘./run/user/5023’: Permission denied
find: ‘./run/user/5012’: Permission denied
find: ‘./run/user/5009’: Permission denied
find: ‘./run/user/11027’: Permission denied
find: ‘./run/user/11011’: Permission denied
find: ‘./run/user/11008’: Permission denied
find: ‘./run/user/14007’: Permission denied
find: ‘./run/user/14006’: Permission denied
find: ‘./run/user/14005’: Permission denied
find: ‘./run/user/14004’: Permission denied
find: ‘./run/user/14002’: Permission denied
find: ‘./run/user/15005’: Permission denied
find: ‘./run/user/11001’: Permission denied
find: ‘./run/user/11020’: Permission denied
find: ‘./run/user/13007’: Permission denied
find: ‘./run/user/13006’: Permission denied
find: ‘./run/user/13003’: Permission denied
find: ‘./run/user/13001’: Permission denied
find: ‘./run/user/13000’: Permission denied
```

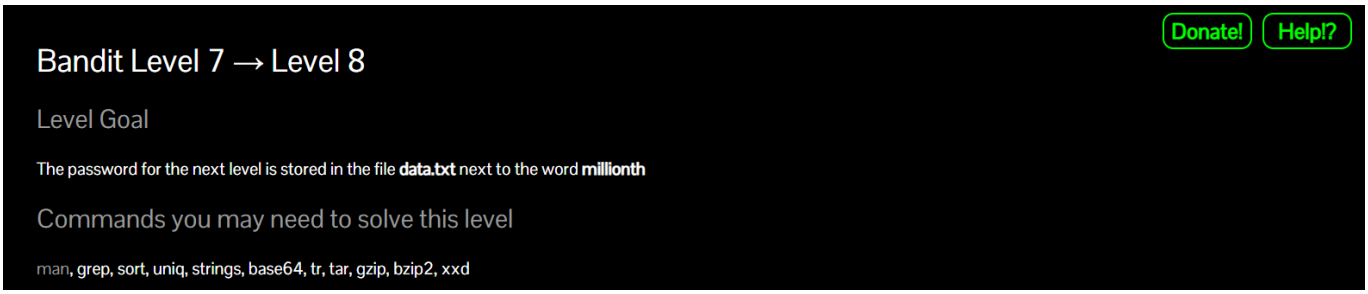
Ta có thể thấy ở trong hình, nó vẫn cho ra rất nhiều file có những thông tin đó. Sau đó, mình đã thử dụng `grep` để lọc thử xem thì khi mình thử truyền keyword là `bandit7` thì thật may mắn nó cho ra kết quả là 1 file có tên như vậy (`./var/lib/dpkg/info/bandit7.password`). Và mình thử `cat` ra xem thì thực sự có password được lưu ở trong đó.

```
find: ‘./var/lib/ubuntu-advantage/apt-esm/var/lib/apt/lists/partial’: Permission denied
find: ‘./var/lib/amazon’: Permission denied
find: ‘./var/lib/polkit-1’: Permission denied
find: ‘./var/spool/bandit24’: Permission denied
find: ‘./var/spool/rsyslog’: Permission denied
find: ‘./var/spool/cron/crontabs’: Permission denied
./var/lib/dpkg/info/bandit7.password
find: ‘./var/cache/pollinate’: Permission denied
find: ‘./var/cache/private’: Permission denied
find: ‘./var/cache/apt/archives/partial’: Permission denied
find: ‘./var/cache/ldconfig’: Permission denied
find: ‘./var/cache/apparmor/0fb44ac6.0’: Permission denied
find: ‘./var/cache/apparmor/208b6430.0’: Permission denied
find: ‘./var/crash’: Permission denied
find: ‘./var/tmp’: Permission denied
find: ‘./proc/tty/driver’: Permission denied
find: ‘./proc/596251/task/596251/fd/6’: No such file or directory
find: ‘./proc/596251/task/596251/fdinfo/6’: No such file or directory
find: ‘./proc/596251/fd/5’: No such file or directory
find: ‘./proc/596251/fdinfo/5’: No such file or directory
find: ‘./snap’: Permission denied
find: ‘./tmp’: Permission denied
find: ‘./etc/credstore’: Permission denied
find: ‘./etc/credstore.encrypted’: Permission denied
find: ‘./etc/sudoers.d’: Permission denied
find: ‘./etc/ssl/private’: Permission denied
find: ‘./etc/xinetd.d’: Permission denied
find: ‘./etc/stunnel’: Permission denied
find: ‘./etc/polkit-1/rules.d’: Permission denied
find: ‘./etc/multipath’: Permission denied
find: ‘./home/bandit31-git’: Permission denied
find: ‘./home/bandit5/inhere’: Permission denied
find: ‘./home/leviathan4/.trash’: Permission denied
find: ‘./home/bandit30-git’: Permission denied
find: ‘./home/bandit27-git’: Permission denied
find: ‘./home/leviathan0/.backup’: Permission denied
find: ‘./home/drifter6/data’: Permission denied
find: ‘./home/ubuntu’: Permission denied
find: ‘./home/bandit28-git’: Permission denied
find: ‘./home/bandit29-git’: Permission denied
find: ‘./home/drifter8/chroot’: Permission denied
bandit6@bandit:/$ cat ./var/lib/dpkg/info/bandit7.password
morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj
bandit6@bandit:/$
```

Password cho level tiếp theo được hiện ra. (`morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj`)

Level 7 -> level 8

Level này yêu cầu ta cần tìm password được giấu trong file `data.txt`. Và password được lưu bên cạnh từ `millonth`.

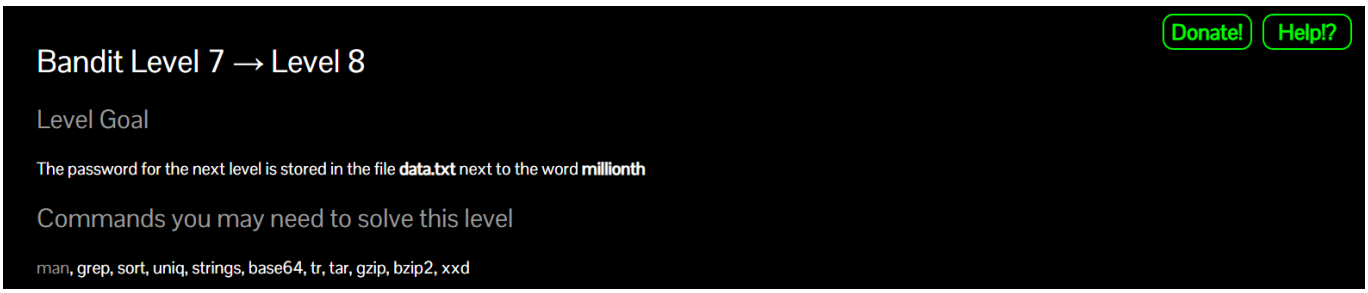


Solution

Trước khi giải quyết level này ta cần tìm hiểu về 1 số lệnh sau:

- `man`: dùng để xem hướng dẫn sử dụng 1 lệnh nào đó.
- `grep`: dùng để tìm kiếm 1 chuỗi các ký tự trong 1 output hoặc 1 file nào đó.
- `sort`: dùng để sắp xếp các dòng trong 1 file văn bản hoặc 1 output nào đó.
- `uniq`: dùng để loại bỏ các dòng trùng lặp trong 1 file văn bản hoặc 1 output nào đó.
- `strings`: dùng để in ra các chuỗi ký tự có thể in được từ 1 file nhị phân.
- `base64`: dùng để mã hóa hoặc giải mã dữ liệu theo chuẩn base64.
- `tr`: dùng để dịch hoặc xóa các ký tự.
- `tar`: dùng để nén và giải nén các file.
- `gzip`: dùng để nén và giải nén các file theo định dạng gzip.
- `bzip2`: dùng để nén và giải nén các file theo định dạng bzip2.
- `xxd`: dùng để tạo ra 1 bản hex dump hoặc chuyển đổi giữa hex dump và binary.

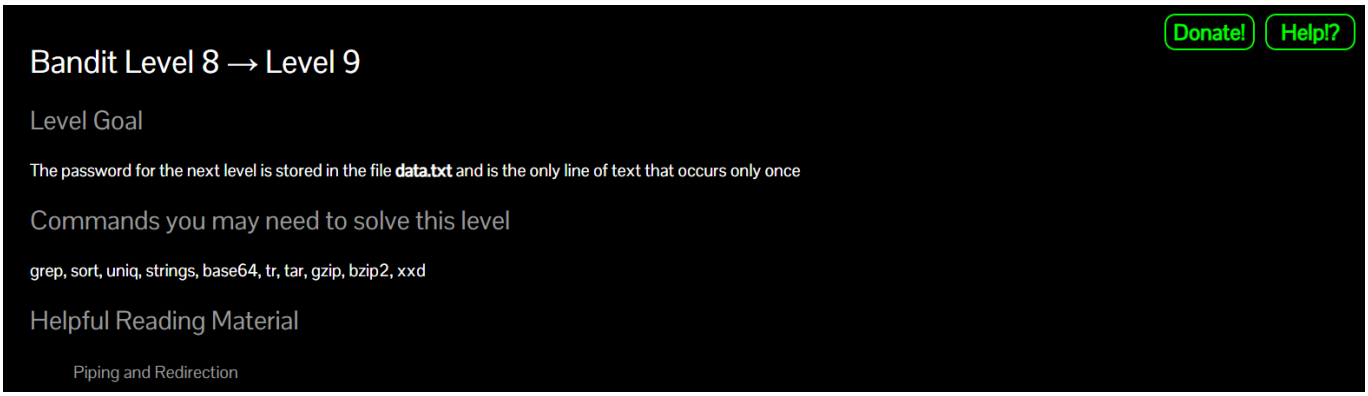
Đối với level này, đầu tiên mình sẽ sử dụng lệnh `cat` để in ra nội dung của file `data.txt` sau đó kết hợp sử dụng `grep` để tìm từ `millionth` vì password nằm ở bên cạnh từ này.
Cụ thể: `cat data.txt | grep "millionth"`



Password cho level tiếp theo được hiện ra. (`dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc`)

Level 8 -> level 9

Level này yêu cầu ta cần tìm password được giấu trong file `data.txt`. Và password là dòng chỉ xuất hiện 1 lần duy nhất trong file đó.



Solution

Đối với level này, mình sẽ sử dụng lệnh `sort` để sắp xếp các dòng trong file `data.txt`, sau đó mình sẽ kết hợp sử dụng lệnh `uniq` để loại bỏ các dòng trùng lặp, tuy nhiên mình sẽ sử dụng thêm option `-u` để nó chỉ giữ lại các dòng duy nhất.

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

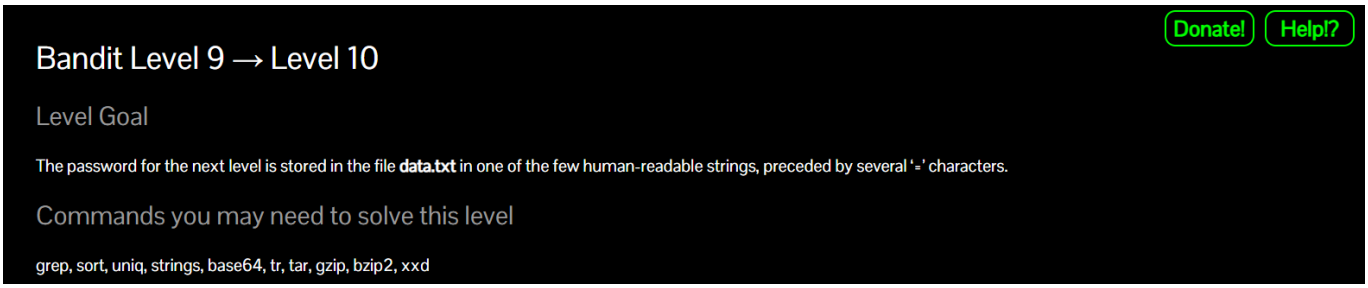
Password cho level tiếp theo được hiện ra. (`4CKMh1JI91bUIZZPXDqGanal4xvAg0JM`)

References

- Piping and Redirection

Level 9 -> level 10

Level này yêu cầu ta cần tìm password được giấu trong file `data.txt`. Và password là 1 trong các từ có thể đọc được và theo sau 1 vài ký tự `=` trong file đó.



Solution

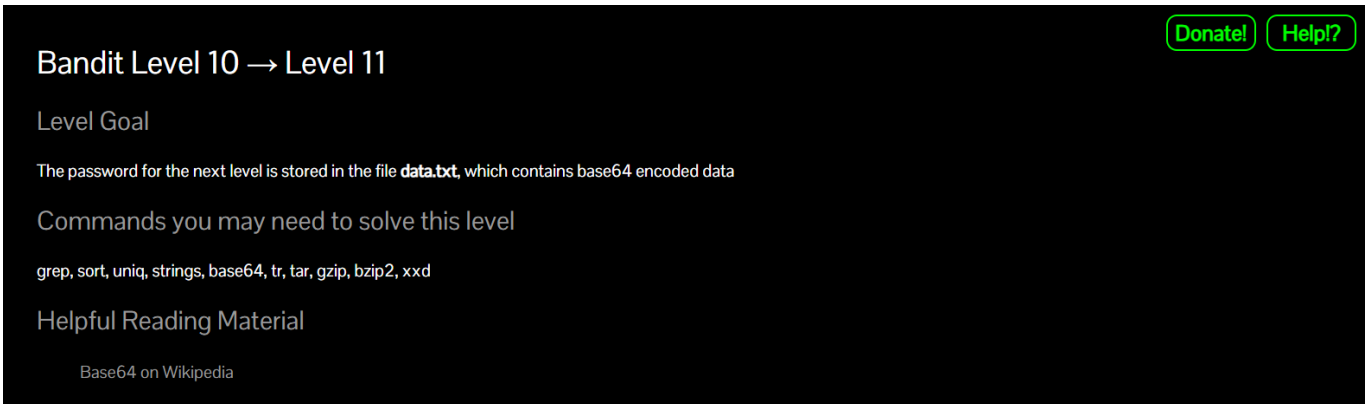
Đối với level này, mình sẽ sử dụng lệnh `strings` để in ra các chuỗi ký tự có thể đọc được từ file `data.txt` và kết hợp sử dụng lệnh `grep` để lọc những dòng có chữa ký tự `=`.

```
bandit9@bandit:~$ strings data.txt | grep '='
========== the
S=s*$u
[=u~]/
hW\=
=}y2|
=RiaT
1j=\
========== password
f=+n
Q========== is%
="K@
n7X=
F<'=
!=v5~6
>u`9J========== FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey
Fb=G
bandit9@bandit:~$
```

Password cho level tiếp theo được hiện ra. (`FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey`)

Level 10 -> level 11

Level này yêu cầu ta cần tìm password được giấu trong file `data.txt`. Tuy nhiên, data của file này đã được mã hóa base64.



Solution

Đối với level này, mình sẽ sử dụng lệnh `base64` để giải mã data trong file `data.txt` với option `-d` (decode).

Cụ thể: `base -d data.txt`

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

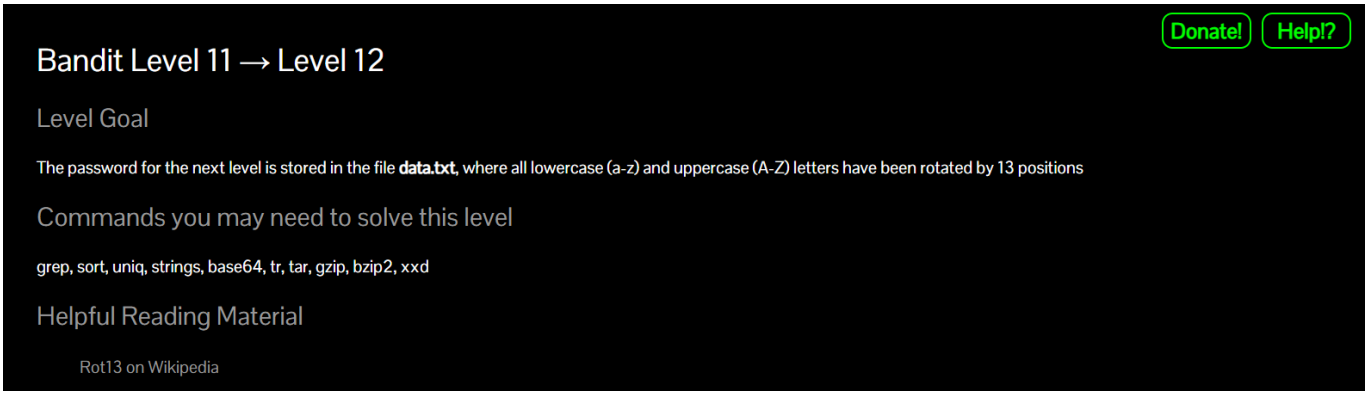
Password cho level tiếp theo được hiện ra. (`dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr`)

References

- Base64 on Wikipedia

Level 11 -> level 12

Level này yêu cầu ta cần tìm password được giấu trong file `data.txt`. Tuy nhiên, các kí tự in thường và in hoa của file nãy đã được dịch chuyển 13 vị trí.



Solution

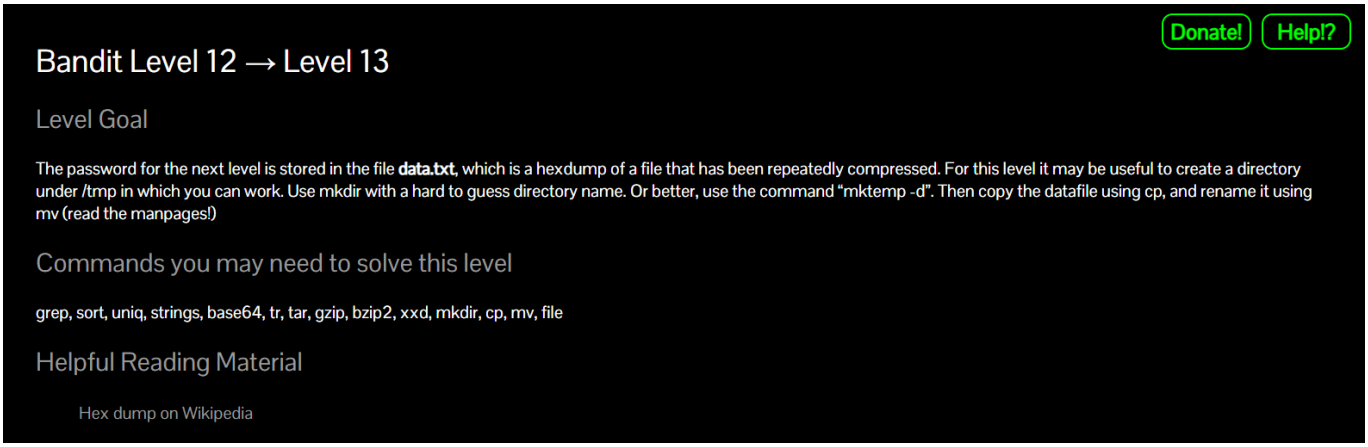
Đối với level này, mình sẽ sử dụng lệnh `tr` để dịch chuyển các kí tự in hoa và in thường sang 13 kí tự nữa để quay lại vị trí ban đầu. (Vì có tổng cộng 26 kí tự)

Cụ thể: `tr 'A-Za-z' 'N-ZA-z < data.txt`

Password cho level tiếp theo được hiện ra. (`7x16WNeHIi5YkIhWsfFIqoognUTyj9Q4`)

Level 12 -> level 13

Level này yêu cầu ta cần tìm password được giấu trong file `data.txt`. Tuy nhiên, file này là 1 file hex dump và được nén nhiều lần.



Solution

Trước khi giải quyết level này ta cần tìm hiểu về 1 số lệnh sau:

- `cp`: dùng để copy file hoặc folder
- `mv`: dùng để di chuyển hoặc đổi tên file hoặc folder
- `mkdir`: dùng để tạo folder Đối với level này, mình sẽ sử dụng lệnh `xxd` để chuyển đổi file hex dump sang dạng binary với option `-r` (reverse). Và sau đó mình sẽ sử dụng lệnh `file` để xem thông tin phù hợp về file đó. Sau đó mình sẽ đổi tên file phù hợp và thực hiện giải nén nhiều lần.

Cụ thể: `xxd -r data.txt data`

```
bandit12@bandit:~$ ls
data.txt
bandit12@bandit:~$ mkdir /tmp/ngocsinh
bandit12@bandit:~$ cp data.txt /tmp/ngocsinh
bandit12@bandit:~$ cd /tmp/ngocsinh
bandit12@bandit:/tmp/ngocsinh$ xxd -r data.txt data
bandit12@bandit:/tmp/ngocsinh$ file data
data: gzip compressed data, was "data2.bin", last modified: Fri Aug 15 13:15:53 2025, max compression, from Unix, original size modulo 2^32 584
bandit12@bandit:/tmp/ngocsinh$ mv data data.gz
bandit12@bandit:/tmp/ngocsinh$ gzip -d data.gz
bandit12@bandit:/tmp/ngocsinh$ ls
data  data.txt
bandit12@bandit:/tmp/ngocsinh$ file data
data: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/ngocsinh$ mv data data.bz2
bandit12@bandit:/tmp/ngocsinh$ bzip2 -d data.bz2
bandit12@bandit:/tmp/ngocsinh$ ls
data  data.txt
bandit12@bandit:/tmp/ngocsinh$ file data
data: gzip compressed data, was "data4.bin", last modified: Fri Aug 15 13:15:53 2025, max compression, from Unix, original size modulo 2^32 20480
bandit12@bandit:/tmp/ngocsinh$ mv data data.gz
bandit12@bandit:/tmp/ngocsinh$ gzip -d data.gz
bandit12@bandit:/tmp/ngocsinh$ ls
data  data.txt
bandit12@bandit:/tmp/ngocsinh$ file data
data: POSIX tar archive (GNU)
bandit12@bandit:/tmp/ngocsinh$ tar -xf data
bandit12@bandit:/tmp/ngocsinh$ ls
data  data5.bin  data.txt
bandit12@bandit:/tmp/ngocsinh$ tar -xf data5.bin
bandit12@bandit:/tmp/ngocsinh$ ls
data  data5.bin  data6.bin  data.txt
bandit12@bandit:/tmp/ngocsinh$ tar -xf data6.bin
bandit12@bandit:/tmp/ngocsinh$ ls
data  data5.bin  data6.bin  data8.bin  data.txt
bandit12@bandit:/tmp/ngocsinh$ tar -xf data8.bin
bandit12@bandit:/tmp/ngocsinh$ ls
data  data5.bin  data6.bin  data8.bin  data.txt
bandit12@bandit:/tmp/ngocsinh$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Fri Aug 15 13:15:53 2025, max compression, from Unix, original size modulo 2^32 49
bandit12@bandit:/tmp/ngocsinh$ mv data8.bin data.gz
bandit12@bandit:/tmp/ngocsinh$ gzip -d data.gz
gzip: data already exists; do you wish to overwrite (y or n)? y
bandit12@bandit:/tmp/ngocsinh$ ls
data  data5.bin  data6.bin  data.txt
bandit12@bandit:/tmp/ngocsinh$ file data
data: ASCII text
bandit12@bandit:/tmp/ngocsinh$ cat data
The password is FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn
bandit12@bandit:/tmp/ngocsinh$
```

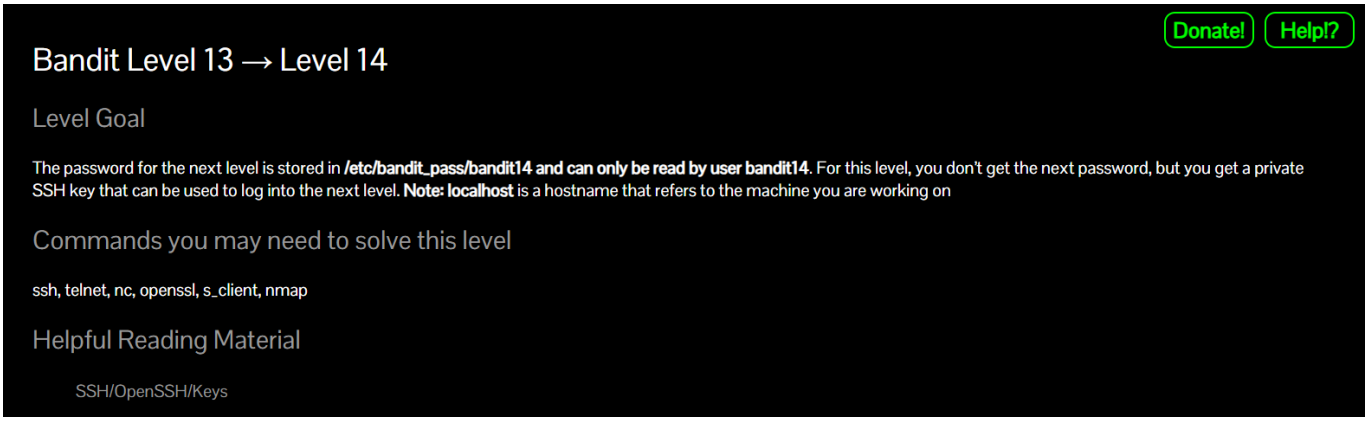
Password cho level tiếp theo được hiện ra. (`FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn`)

References

- Hex Dump on Wikipedia

Level 13 -> level 14

Level này chứa password cho level tiếp theo, tuy nhiên password chỉ đọc được bởi user bandit14. Nhưng ta lại được cung cấp 1 private SSH key dùng để kết nối vào level tiếp theo.



Solution

Trước khi giải quyết level này ta cần tìm hiểu về 1 số lệnh sau:

- `ssh`: dùng để kết nối bảo mật vào server
- `telnet`: dùng để kết nối không bảo mật vào server
- `nc`: công cụ tạo server, gửi/nhận dữ liệu qua TCP/UDP,...
- `openssl`: dùng để mã hóa, giải mã dữ liệu, tạo và kiểm tra các kết nối SSL/TLS
- `s_client`: lệnh con của `openssl` dùng để kết nối vào server SSL/TLS
- `nmap`: dùng để scan mạng như tìm host, tìm port, ...

Đối với level này, mình sẽ sử dụng lệnh `ssh` để kết nối vào level tiếp theo (level 14), và mình sẽ sử dụng thêm option `-i` để truyền vào path của `sshkey.private`.

Cụ thể: `ssh bandit14@bandit.labs.overthewire.org -p 2220 -i sshkey.private`

```
bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ ssh bandit14@bandit.labs.overthewire.org -p 2220 -i sshkey.private
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

Và thế là mình đã kết nối được tới level tiếp theo.

```
--[ More information ]--

  For more information regarding individual wargames, visit
  http://www.overthewire.org/wargames/

  For support, questions or comments, contact us on discord or IRC.

  Enjoy your stay!

bandit14@bandit:~$
```

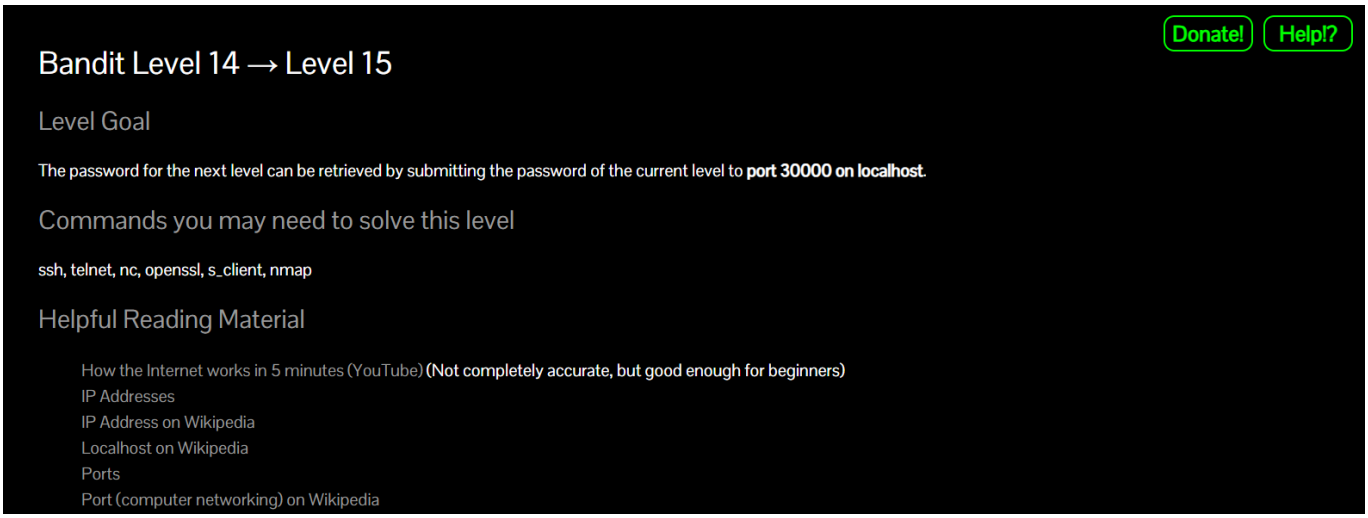
Password cho level tiếp theo được hiện ra. (`MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS`).
Note: Được lấy khi kết nối vào level tiếp theo.

References

- SSH/OpenSSH/Keys

Level 14 -> level 15

Level này yêu cầu ta kết nối giao thức với localhost và port 30000, sau đó gửi password của level hiện tại để nhận được password của level tiếp theo.



Solution

Đối với level này, mình sẽ sử dụng lệnh `telnet` để kết nối vào localhost với port `30000`.

Cụ thể: `telnet localhost 30000`

Sau đó mình sẽ nhập password của level hiện tại, được lưu ở path `/etc/bandit_pass/bandit14`.

```
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS
bandit14@bandit:~$ telnet localhost 30000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS
Correct!
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo

Connection closed by foreign host.
bandit14@bandit:~$
```

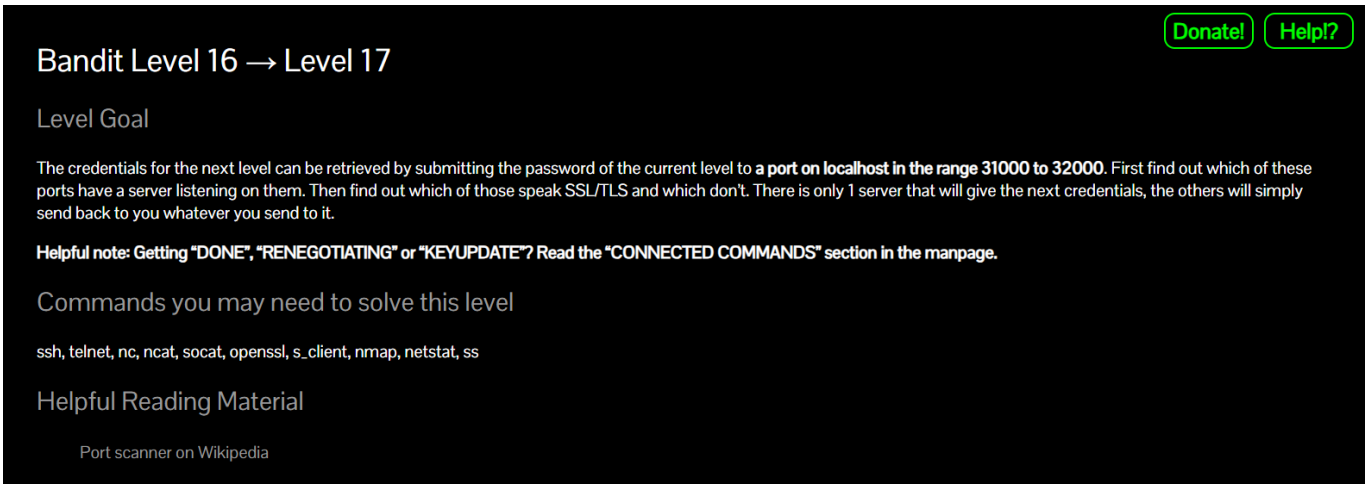
Password cho level tiếp theo được hiện ra. (`8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo`)

References

- How the Internet works in 5 minutes (YouTube)
- IP Addresses
- IP Address on Wikipedia
- Localhost on Wikipedia
- Ports
- Port (computer networking) on Wikipedia

Level 15 -> level 16

Level này yêu cầu ta kết nối giao thức với localhost và port 30001 kết hợp sử dụng mã hóa SSL/TLS.



Solution

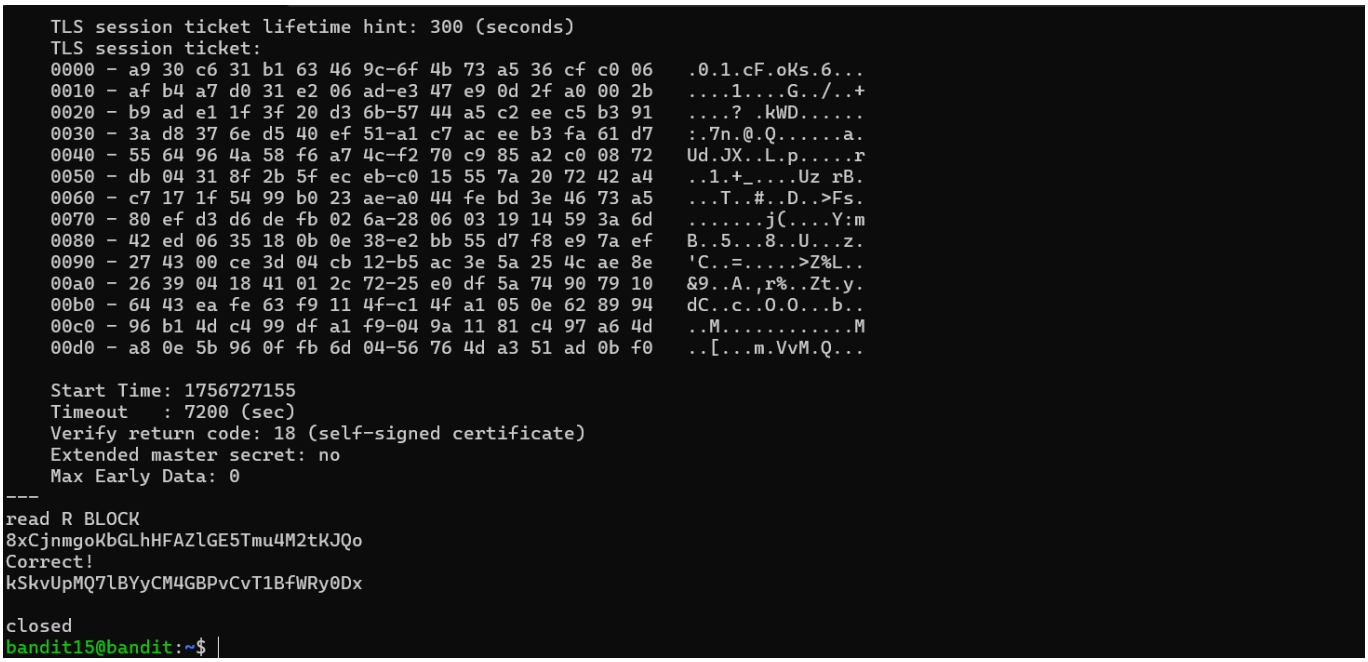
Trước khi giải quyết level này ta cần tìm hiểu về 1 số lệnh sau:

- `ncat`:dùng để đọc và ghi dữ liệu qua mạng bằng TCP/UDP.
- `socat`:dùng để chuyển tiếp dữ liệu giữa 2 địa chỉ mạng hoặc file.
- `netstat`:dùng để hiển thị các kết nối mạng, bảng định tuyến, thống kê giao diện, v.v.
- `ss`:dùng để hiển thị các socket đang hoạt động.

Đối với level này, mình sẽ sử dụng lệnh `openssl s_client` để kết nối vào localhost với port `30001`.

Cụ thể: `openssl s_client -connect localhost:30001`

Sau đó mình sẽ nhập password của level hiện tại, được lưu ở path `/etc/bandit_pass/bandit15`.



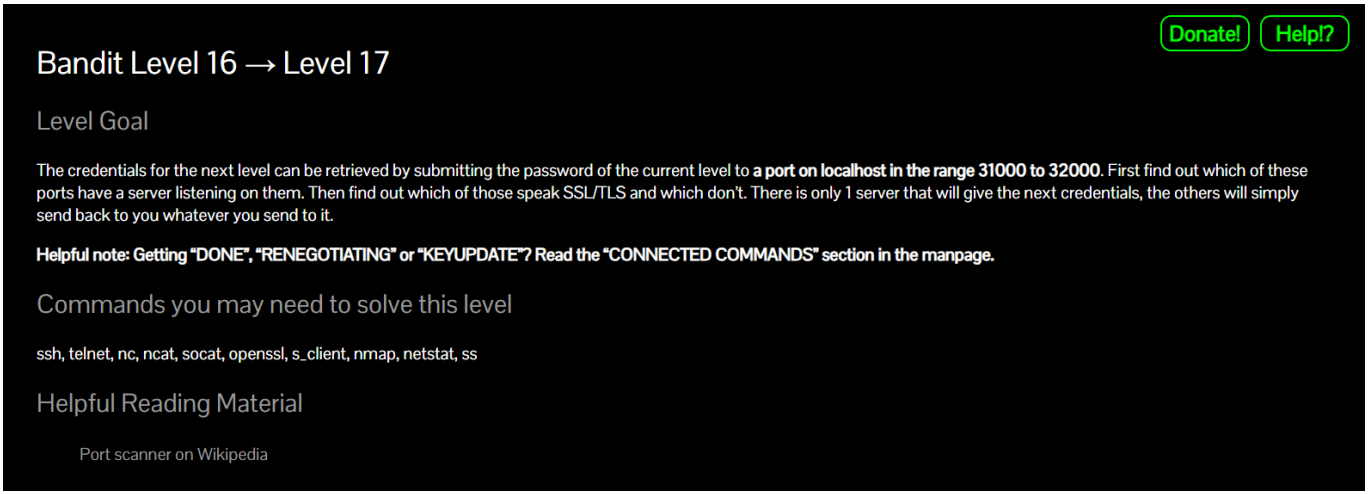
Password cho level tiếp theo được hiện ra. (`kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx`)

References

- Secure Socket Layer/Transport Layer Security on Wikipedia
- OpenSSL Cookbook - Testing with OpenSSL

Level 16 -> level 17

Level này yêu cầu ta kết nối vào localhost và 1 port nào đó nằm trong phạm vi từ 31000 đến 32000 và có SSL/TLS. Trong số các port đó, có duy nhất 1 port là cung cấp cho chúng ta thông tin về level tiếp theo, còn các port còn lại khi ta nhập password của level này thì nó sẽ in lại password đấy.



Solution

Đối với level này, đầu tiên mình sẽ sử dụng lệnh `nmap` để scan các port đang hoạt động. Và mình sẽ sử dụng thêm option `-p 31000-32000` để scan port trong phạm vi 31000-32000 kết hợp với option `-sV` để xem đầy đủ thông tin hơn về port đó(Ví dụ như chứa giao thức gì).

Cụ thể: `nmap -sV -p 31000-32000 localhost`

```
bandit16@bandit:~$ nmap -p 31000-32000 -sV localhost
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-01 12:48 UTC
Debugging Decreased to 0.
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00016s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE     VERSION
31046/tcp open  echo
31518/tcp open  ssl/echo
31691/tcp open  echo
31790/tcp open  ssl/unknown
31960/tcp open  echo
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.c
gi?new-service :
SF-Port31790-TCP:V=7.94SVN%T=SSL%I=7%D=9/1%Time=68B59630%P=x86_64-pc-linux
SF:-gnu%r(GenericLines,32,"Wrong!\x20Please\x20enter\x20the\x20correct\x20
SF:current\x20password\.\n")%r(GetRequest,32,"Wrong!\x20Please\x20enter\x2
SF:0the\x20correct\x20current\x20password\.\n")%r(HTTPOptions,32,"Wrong!\x
SF:20Please\x20enter\x20the\x20correct\x20current\x20password\.\n")%r(RTSP
SF:Request,32,"Wrong!\x20Please\x20enter\x20the\x20correct\x20current\x20p
SF:assword\.\n")%r(Help,32,"Wrong!\x20Please\x20enter\x20the\x20correct\x2
SF:0current\x20password\.\n")%r(FourOhFourRequest,32,"Wrong!\x20Please\x20
SF:enter\x20the\x20correct\x20current\x20password\.\n")%r(LPDString,32,"Wr
SF:ong!\x20Please\x20enter\x20the\x20correct\x20current\x20password\.\n")%
SF:r(SIPOptions,32,"Wrong!\x20Please\x20enter\x20the\x20correct\x20current
SF:\x20password\.\n");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 163.81 seconds
bandit16@bandit:~$
```

Như ta thấy, ta đã scan ra 5 port trong phạm vi 31000-32000 và có 2 port có SSL là 31518 và 31790. Vì vậy mình sẽ thử kết nối lần lượt vào 2 cổng port này để xem thử.

```
bandit16@bandit:~$ ncat --ssl localhost 31790
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMlOJf7+BrJObArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl87ORiO+rW4LCDCNd2lUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW3OekePQAzL0VUYbW
JGTi65CxbCnzc/w4+mqQyvmzpWtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XFOJuaQIDAQABAoIBABagpxpM1aoLWfvD
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNuDE6SFthOar69jp5RlLwD1NhPx3iBl
J9nOM8OJ0VToum43UOS8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52yOQ9qOkwFTEQpjtF4uNtJom+asvlpmS8A
vLY9r60wYSvmZhNqBUrj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOmama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRhORT
8c8hAuRBb2G82so8vUHk/fur85OEfc9TncnCY2crpoqsghifKLxrLgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyc9P2jGRNtMSkCgYEAypHd
HCctNi/FwjulhttFx/rHYKhLidZDFYeiE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enCIvGCSx+X3l5SiWg0A
R57hJglezIiVjv3aGwHwvlZvtszK6zV6oXFAu0ECgYAbjo46T4hyP5tJi93V5HDi
Ttiek7xRVxUl+iU7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFMLy9FL2m9oQWCg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB3OhYimtiG2Cg5JCqIZFHxD6MjEGOiu
L8ktHMPvodBwNsSBULpG0QKBgBAplTfC1HOnWiMGOU3KPwYWt0O6CdTkmJOmL8Ni
blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU
YOdjHdSOoKvDQNWu6ucyLRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyzRqaM
77pBAoGAMmjmIJdjp+Ez8duyn3ieo36yrttF5NSsJLAbxFpdlc1gvtGCWW+9Cq0b
dxviW8+TFVEBl1O4f7HVm6EpTscdDxU+bCXWkfjuRb7Dy9GOtt9JPsX8MBTakzh3
vBgsyi/sN3RqRBcGU40fOoZyfAMT8s1m/uYv52O6IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----
```

Sau khi thử kết nối lần lượt cả 2 port thì port thứ 2 cho ra khóa RSA cho level tiếp theo và mình sẽ ssh để kết nối vào level tiếp theo.

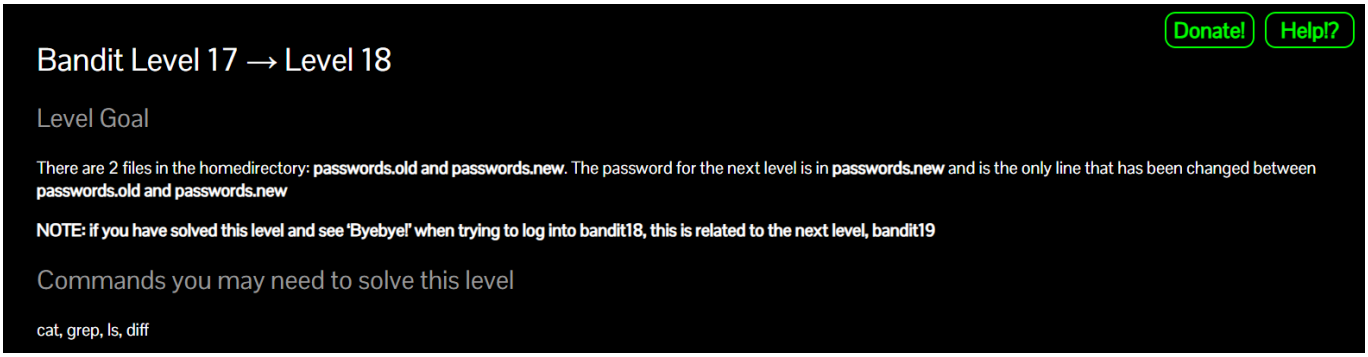
Password cho level tiếp theo. (`EReVavePLFHtFlFsjn3hyzMlvSuSAcRD`)
Note: được cập nhật khi kết nối vào level tiếp theo.

References

- Port scanner on Wikipedia

Level 17 -> level 18

Level này cho ta 2 file đó là `password.new` và `password.old`. Trong 2 file này sẽ có duy nhất 1 dòng có nội dung khác nhau và đó là password cho level tiếp theo.



Solution

Đối với level này, mình sẽ sử dụng lệnh `diff` (viết tắt của different) để so sánh 2 file `password.new` và `password.old`.

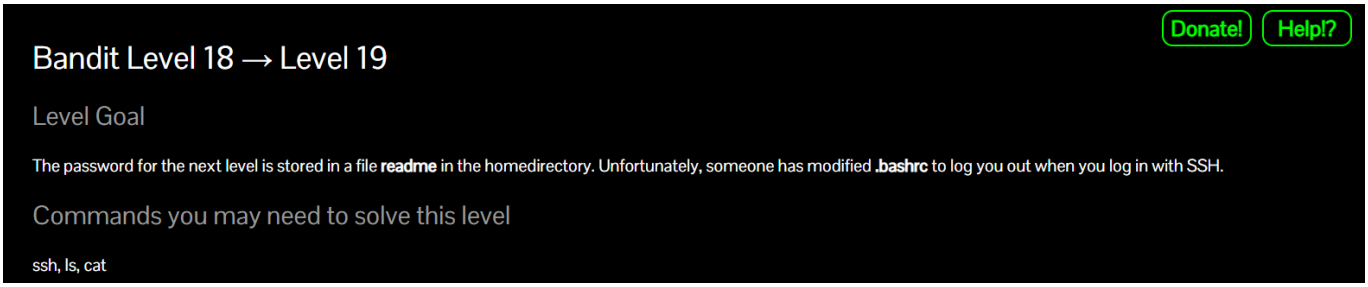
Cụ thể: `diff password.new password.old`

```
bandit17@bandit:~$ ls
passwords.new  passwords.old
bandit17@bandit:~$ diff passwords.new passwords.old
42c42
< x2gLTTjFwMOhQ8oWNbMN362QKxfRqGlO
---
> CgmS55GVlEKTgx8xpW8HuWnHlBKP924b
bandit17@bandit:~$
```

Password cho level tiếp theo được hiện ra. (`x2gLTTjFwMOhQ8oWNbMN362QKxfRqGlO`)

Level 18 -> level 19

Level này yêu cầu đọc file readme để có thể lấy được password cho level tiếp theo. Tuy nhiên, khi ta kết nối vào level này thì không may file `.bashrc` bị lỗi và không thể kết nối vào trong và remote được.



Solution

Đối với level này, theo mình tìm hiểu thì ta có thể thực hiện lệnh trực tiếp khi chúng ta thực hiện ssh.

Cụ thể: `ssh bandit18@bandit.labs.overthewire.org -p 2220 cat readme`

```
(pwnvenv) ngocsinh@Sinh:/mnt/d/ctf/CTF-Writeups/Overthewire$ ssh bandit18@bandit.labs.overthewire.org -p 2220 cat readme
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


                      This is an OverTheWire game server.
            More information on http://www.overthewire.org/wargames

backend: gibson-1
bandit18@bandit.labs.overthewire.org's password:
cGWpMaKXVwDUNgPAVJbWYuGHVn9zl3j8
(pwnvenv) ngocsinh@Sinh:/mnt/d/ctf/CTF-Writeups/Overthewire$
```

Password cho level tiếp theo được hiện ra. (`cGWpMaKXVwDUNgPAVJbWYuGHVn9zl3j8`)

Ngoài ra, vì khi ta ssh vào thì mặc định nó sẽ sử dụng `pseudo terminal`, nên ta có thể sử dụng option `-T` để ép nó không dùng pseudo terminal. Và ta sẽ được sử dụng command như bình thường.

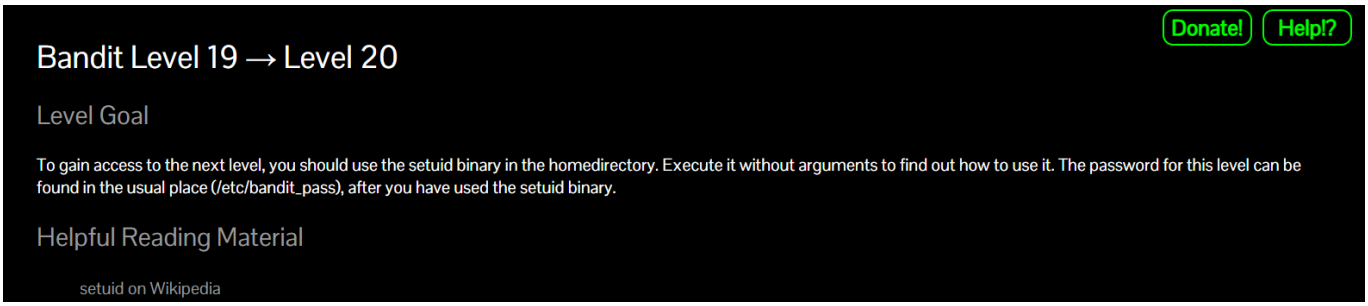
```
(pwnvenv) ngocsinh@Sinh:/mnt/d/ctf/CTF-Writeups/Overthewire$ ssh bandit18@bandit.labs.overthewire.org -p 2220 -T
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


                      This is an OverTheWire game server.
            More information on http://www.overthewire.org/wargames

backend: gibson-1
bandit18@bandit.labs.overthewire.org's password:
ls
readme
cat readme
cGWpMaKXVwDUNgPAVJbWYuGHVn9zl3j8
```

References

- ssh linux manual page

Level 19 -> level 20

Level này cho ta 1 file có tên là `bandit20-do`, file này có dạng setuid và ta được truyền `argument` vào để thực hiện lệnh.



Solution

Đối với level này, đơn giản mình chỉ cần truyền lệnh để thực hiện vào argument khi thực hiện file `bandit20-do`.

Cụ thể: `./bandit20-do cat /etc/bandit_pass/bandit20`

```
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO
bandit19@bandit:~$
```

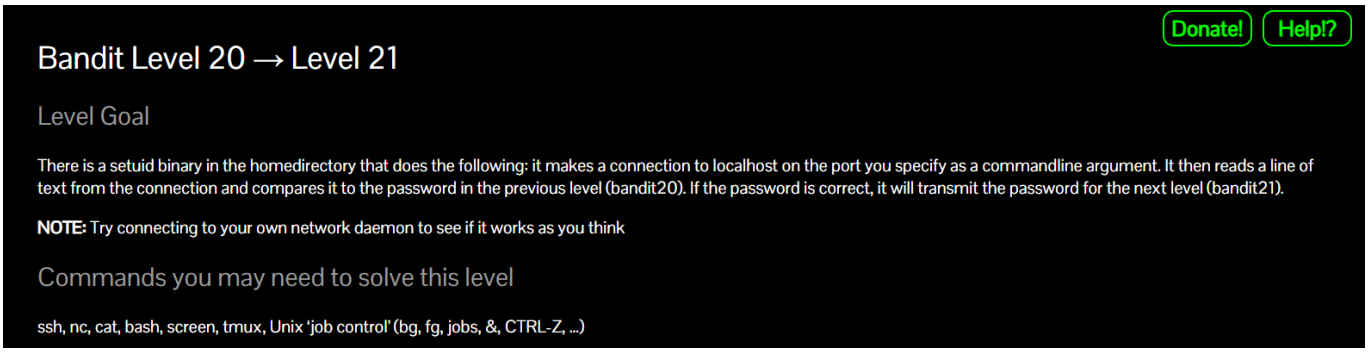
Password cho level tiếp theo được hiện ra. (`0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO`)

References

- setuid on Wikipedia

Level 20 -> level 21

Level này cho mình 1 file có dạng `setuid`, file đó nó kết nối tới localhost với port(argument) có thể lắng nghe. Khi nhập đúng password của level hiện tại nó sẽ gửi password của level tiếp theo.



Solution

Trước khi giải quyết level này ta cần tìm hiểu về 1 số lệnh sau:

- `bash`: dùng để thực thi các lệnh shell
- `screen`: dùng để quản lý nhiều phiên terminal trong 1 terminal duy nhất
- `tmux`: dùng để quản lý nhiều phiên terminal trong 1 terminal duy nhất (tương tự như screen nhưng hiện đại hơn)
- `unix`: dùng để quản lý các job, các tác vụ.

Đối với level này, mình sẽ sử dụng lệnh `nc` với option `-l` để mở 1 port với localhost có thể nghe. Sau đó mình sẽ truyền arugment vào cho file setuid đó khi thực thi. Và cuối cùng là nhập password của level này để nhận được password của level tiếp theo.

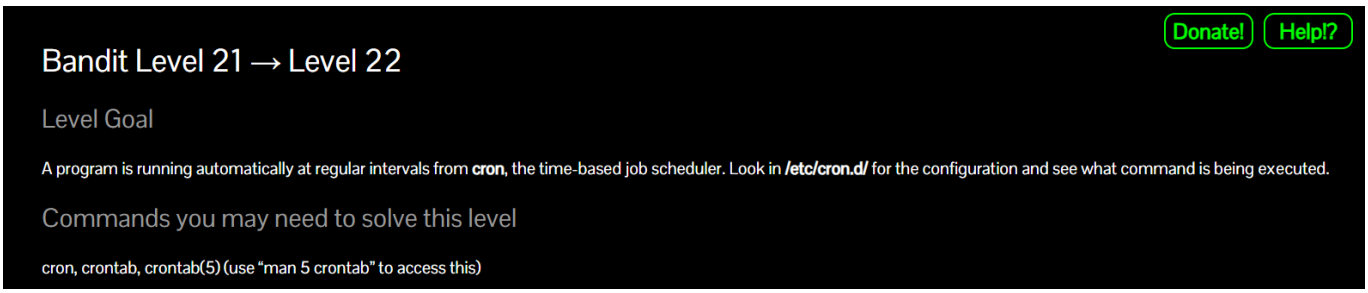
Cụ thể: `echo -n '0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO' | nc -l localhost 2007 &`

```
bandit20@bandit:~$ echo -n '0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO' | nc -l localhost 2007 &
[4] 1473541
bandit20@bandit:~$ ./suconnect 2007
Read: 0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO
Password matches, sending next password
EeoULMCra2q0dSkYj561DX7s1CpBuOBt
[4]   Done                    echo -n '0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO' | nc -l localhost 2007
bandit20@bandit:~$
```

Password cho level tiếp theo được hiện ra. (`EeoULMCra2q0dSkYj561DX7s1CpBuOBt`)

Level 21 -> level 22

Level này yêu cầu ta xem thử trong `/etc/cron.d` có lệnh nào đang được thực thi.



Solution

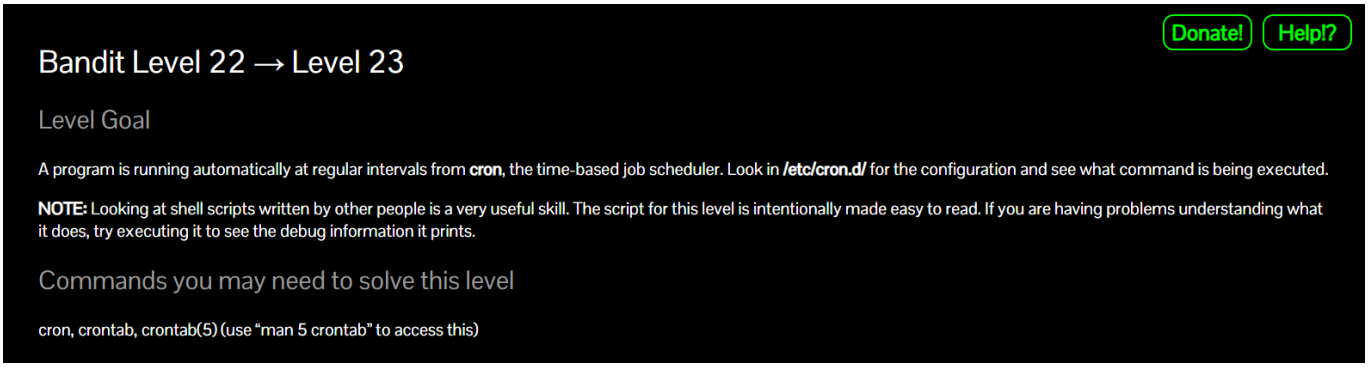
Đối với level này, đầu tiên mình sẽ xem thử trong `etc/cron.d` có những gì, và mình thấy có nhiều file cron và để ý thấy có file `cronjob_bandit22`. Khi mình xem thử bên trong thì có thấy cron này đang thực thi `/usr/bin/cronjob_bandit22.sh`. Và mình lại xem thử bên trong file shell đó thì thấy nó lấy password của level tiếp theo được lưu trong `/etc/bandit_pass/bandit22` và truyền vào file `/tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv` và `chmod 644` tức là file đó mình có thể đọc được. Và mình chỉ cần đọc file đó là có thể xem được password cho level tiếp theo.

```
bandit21@bandit:~$ cd /etc/cron.d
bandit21@bandit:/etc/cron.d$ ls
behemoth4_cleanup  cronjob_bandit22  cronjob_bandit24  leviathan5_cleanup    otw-tmp-dir
clean_tmp          cronjob_bandit23  e2scrub_all       manpage3_resetpw_job  sysstat
bandit21@bandit:/etc/cron.d$ cat cronjob_bandit22
@reboot bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
* * * * * bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
bandit21@bandit:/etc/cron.d$ cat /usr/bin/cronjob_bandit22.sh
#!/bin/bash
chmod 644 /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv
cat /etc/bandit_pass/bandit22 > /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv
bandit21@bandit:/etc/cron.d$ cat /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv
tRae0UfB9v0UzbCdn9cY0gQnds9GF58Q
bandit21@bandit:/etc/cron.d$
```

Password cho level tiếp theo được hiện ra. (`tRae0UfB9v0UzbCdn9cY0gQnds9GF58Q`)

Level 22 -> level 23

Tương tự level trước, level này yêu cầu ta xem thử trong `/etc/cron.d` có lệnh nào đang được thực thi.



Solution

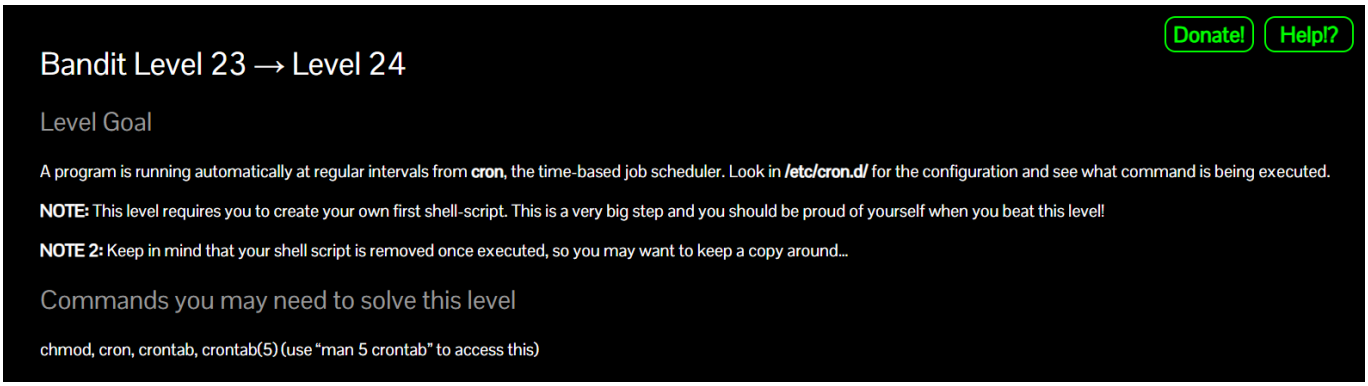
Đối với level này, đầu tiên mình sẽ xem thử trong `etc/cron.d` có những gì, và mình thấy có nhiều file cron và để ý thấy có file `cronjob_bandit23`. Khi mình xem thử bên trong thì có thấy cron này đang thực thi `/usr/bin/cronjob_bandit23.sh`. Và mình lại xem thử bên trong file shell đó thì thấy nó lấy password của level tiếp theo được lưu trong `/etc/bandit_pass/$myname` và truyền vào file `/tmp/$mytarget`. Ta thấy `myname=$(whoami)` mà whoami trong trường hợp này là `bandit23`. Còn `mytarget=$(echo I am user $myname | md5sum | cut -d ' ' -f 1)` mà ta đã biết được myname rồi nên mình sẽ thay myname thành bandit23 để lấy mã `md5sum`. Sau đó chỉ cần in ra `/tmp/$mytarget` với mytarget thay bằng md5sum đó.

```
bandit22@bandit:~$ cd /etc/cron.d
bandit22@bandit:/etc/cron.d$ ls
behemoth4_cleanup  cronjob_bandit22  cronjob_bandit24  leviathan5_cleanup    otw-tmp-dir
clean_tmp          cronjob_bandit23  e2scrub_all       manpage3_resetpw_job  sysstat
bandit22@bandit:/etc/cron.d$ cat cronjob_bandit23
@reboot bandit23 /usr/bin/cronjob_bandit23.sh  &> /dev/null
* * * * * bandit23 /usr/bin/cronjob_bandit23.sh  &> /dev/null
bandit22@bandit:/etc/cron.d$ cat  /usr/bin/cronjob_bandit23.sh
#!/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
bandit22@bandit:/etc/cron.d$ echo I am user bandit23 | md5sum | cut -d ' ' -f 1)
-bash: syntax error near unexpected token `)'
bandit22@bandit:/etc/cron.d$ echo I am user bandit23 | md5sum | cut -d ' ' -f 1
8ca319486bfbbc3663ea0fbe81326349
bandit22@bandit:/etc/cron.d$ cat /tmp/8ca319486bfbbc3663ea0fbe81326349
0Zf11ioIjMVN551jX3CmStKLYqjk54Ga
bandit22@bandit:/etc/cron.d$
```

Password cho level tiếp theo được hiện ra. (`0Zf11ioIjMVN551jX3CmStKLYqjk54Ga`)

Level 23 -> level 24

Tương tự như 2 level trước:), level này tiếp tục yêu cầu ta xem thử trong `/etc/cron.d` có lệnh nào đang được thực thi.



Solution

Đối với level này, đầu tiên mình sẽ xem thử trong `etc/cron.d` có những gì, và mình thấy có nhiều file cron và để ý thấy có file `cronjob_bandit24`. Khi mình xem thử bên trong thì có thấy cron này đang thực thi `/usr/bin/cronjob_bandit24.sh`. Và mình lại xem thử bên trong file shell đó thì thấy nó sẽ lần lượt duyệt qua các file có trong `/var/spool/$myname/foo`, sau đó thực thi file đó và xóa file đó. Vì vậy mình sẽ tạo 1 shell lưu ở trong path đó và sẽ đọc password ở ```bandit_pass/bandit24``.

```
bandit23@bandit:~$ cd /etc/cron.d
bandit23@bandit:/etc/cron.d$ ls
behemoth4_cleanup  cronjob_bandit22  cronjob_bandit24  leviathan5_cleanup    otw-tmp-dir
clean_tmp          cronjob_bandit23  e2scrub_all       manpage3_resetpw_job  sysstat
bandit23@bandit:/etc/cron.d$ cat cronjob_bandit24
@reboot bandit24 /usr/bin/cronjob_bandit24.sh &> /dev/null
* * * * * bandit24 /usr/bin/cronjob_bandit24.sh &> /dev/null
bandit23@bandit:/etc/cron.d$ cat /usr/bin/cronjob_bandit24.sh
#!/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

bandit23@bandit:/etc/cron.d$
```

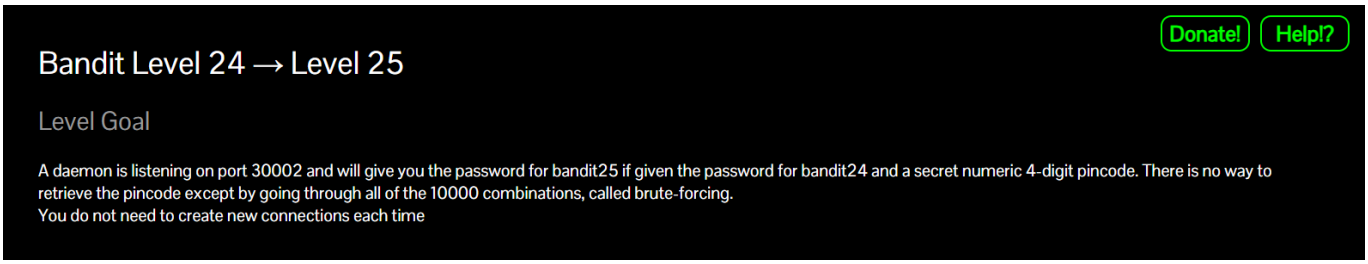
Tạo script

```
bandit23@bandit:~$ mktemp -d
/tmp/tmp.lIDdMBizE4
bandit23@bandit:~$ cd /tmp/tmp.lIDdMBizE4
bandit23@bandit:/tmp/tmp.lIDdMBizE4$ touch pw.txt
bandit23@bandit:/tmp/tmp.lIDdMBizE4$ nano script.sh
Unable to create directory /home/bandit23/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

bandit23@bandit:/tmp/tmp.lIDdMBizE4$ nano script.sh
Unable to create directory /home/bandit23/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

bandit23@bandit:/tmp/tmp.lIDdMBizE4$ chmod 777 tmp/tmp.lIDdMBizE4
chmod: cannot access 'tmp/tmp.lIDdMBizE4': No such file or directory
bandit23@bandit:/tmp/tmp.lIDdMBizE4$ chmod /tmp/tmp.lIDdMBizE4
chmod: missing operand after ‘/tmp/tmp.lIDdMBizE4’
Try 'chmod --help' for more information.
bandit23@bandit:/tmp/tmp.lIDdMBizE4$ chmod 777 /tmp/tmp.lIDdMBizE4
bandit23@bandit:/tmp/tmp.lIDdMBizE4$ chmod 777 script.sh
bandit23@bandit:/tmp/tmp.lIDdMBizE4$ chmod 777 pw.txt
bandit23@bandit:/tmp/tmp.lIDdMBizE4$ cp script.sh /var/spool/bandit24/foo/
bandit23@bandit:/tmp/tmp.lIDdMBizE4$ cat pw.txt
gb8KRRCsshuZXI0tUuR6ypOFjiZbf3G8
bandit23@bandit:/tmp/tmp.lIDdMBizE4$
```

Password cho level tiếp theo được hiện ra. (`gb8KRRCsshuZXI0tUuR6ypOFjiZbf3G8`)

Level 24 -> level 25

Level yêu cầu mình kết nối với `localhost` và port `30002`. Sau đó, nhập password của level này kèm với mã pincode gồm 4 chữ số.



Bandit Level 24 → Level 25

Level Goal

A daemon is listening on port 30002 and will give you the password for bandit25 if given the password for bandit24 and a secret numeric 4-digit pincode. There is no way to retrieve the pincode except by going through all of the 10000 combinations, called brute-forcing.
You do not need to create new connections each time

Solution

Đối với level này, mình sẽ tạo 1 script shell sau đó brute-force từ 0000-9999. Cụ thể hơn, mình sẽ sử dụng lệnh `nc` kèm option `-N` để khi truyền đầu vào thì sẽ đóng socket cả đọc và ghi.

Cụ thể: `echo gb8KRRCsshuZXI0tUuR6ypOFjiZbf3G8 1234 | nc localhost 30002 -N`

```
bandit24@bandit:~$ mktemp -d
/tmp/tmp.Qm5dfxYH6a
bandit24@bandit:~$ cd /tmp/tmp.Qm5dfxYH6a
bandit24@bandit:/tmp/tmp.Qm5dfxYH6a$ nano  shell.sh
Unable to create directory /home/bandit24/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

bandit24@bandit:/tmp/tmp.Qm5dfxYH6a$ touch pass.txt
bandit24@bandit:/tmp/tmp.Qm5dfxYH6a$ cat shell.sh
#!/bin/bash
for i in {0..9999}
do
   output=$(printf "gb8KRRCsshuZXI0tUuR6ypOFjiZbf3G8 %04d\n" "$i" | nc localhost 30002 -N)
   if ! echo "$output" | grep "Wrong"; then
       echo $output
       echo $i > pass.txt
       break
   fi
   echo $output
done
bandit24@bandit:/tmp/tmp.Qm5dfxYH6a$ chmod 777 shell.sh
bandit24@bandit:/tmp/tmp.Qm5dfxYH6a$ chmod 777 pass.txt
bandit24@bandit:/tmp/tmp.Qm5dfxYH6a$ ./shell.sh
```

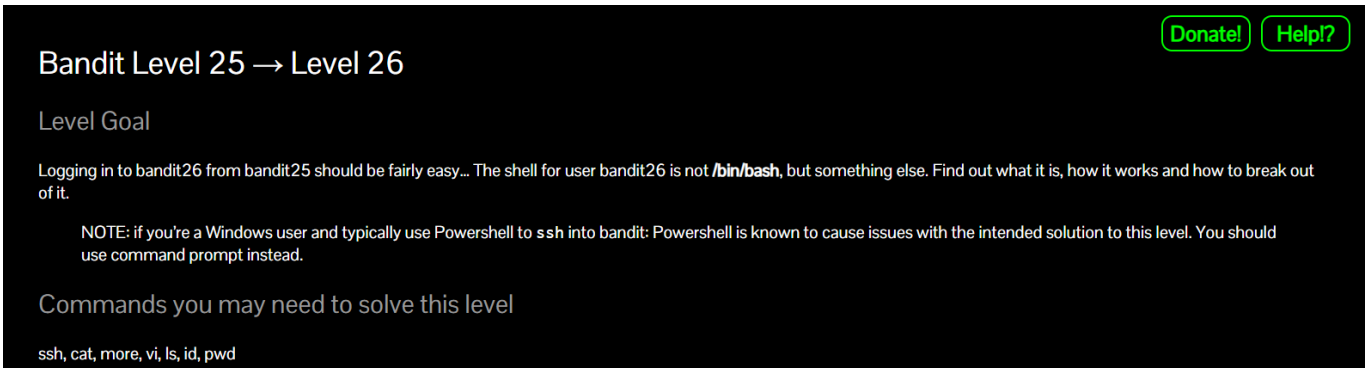
Thực hiện để lấy password cho level kế tiếp khi nhận được password được lưu ở file `pass.txt`.

```
le line, separated by a space. Wrong! Please enter the correct current password and pincode. Try again.
Wrong! Please enter the correct current password and pincode. Try again.
I am the pincode checker for user bandit25. Please enter the password for user bandit24 and the secret pincode on a sing
le line, separated by a space. Wrong! Please enter the correct current password and pincode. Try again.
Wrong! Please enter the correct current password and pincode. Try again.
I am the pincode checker for user bandit25. Please enter the password for user bandit24 and the secret pincode on a sing
le line, separated by a space. Wrong! Please enter the correct current password and pincode. Try again.
Wrong! Please enter the correct current password and pincode. Try again.
I am the pincode checker for user bandit25. Please enter the password for user bandit24 and the secret pincode on a sing
le line, separated by a space. Wrong! Please enter the correct current password and pincode. Try again.
Wrong! Please enter the correct current password and pincode. Try again.
I am the pincode checker for user bandit25. Please enter the password for user bandit24 and the secret pincode on a sing
le line, separated by a space. Wrong! Please enter the correct current password and pincode. Try again.
Wrong! Please enter the correct current password and pincode. Try again.
I am the pincode checker for user bandit25. Please enter the password for user bandit24 and the secret pincode on a sing
le line, separated by a space. Wrong! Please enter the correct current password and pincode. Try again.
Wrong! Please enter the correct current password and pincode. Try again.
I am the pincode checker for user bandit25. Please enter the password for user bandit24 and the secret pincode on a sing
le line, separated by a space. Wrong! Please enter the correct current password and pincode. Try again.
I am the pincode checker for user bandit25. Please enter the password for user bandit24 and the secret pincode on a sing
le line, separated by a space. Correct! The password of user bandit25 is iCi86ttT4KSNe1armKiwbQNmB3YJP3q4
bandit24@bandit:/tmp/tmp.Qm5dfxYH6a$ cat pass.txt
9162
bandit24@bandit:/tmp/tmp.Qm5dfxYH6a$ echo gb8KRRCsshuZXI0tUuR6ypOFjiZbf3G8 9162 | nc localhost 30002 -N
I am the pincode checker for user bandit25. Please enter the password for user bandit24 and the secret pincode on a sing
le line, separated by a space.
Correct!
The password of user bandit25 is iCi86ttT4KSNe1armKiwbQNmB3YJP3q4

bandit24@bandit:/tmp/tmp.Qm5dfxYH6a$
```

Password cho level tiếp theo được hiện ra. (`iCi86ttT4KSNe1armKiwbQNmB3YJP3q4`)

Level 25 -> level 26

Level này yêu cầu mình kết nối tới level tiếp theo, tuy nhiên level tiếp theo shell không sử dụng `/bin/bash` mà là một thứ gì đó.



Solution

Trước khi giải quyết level này ta cần tìm hiểu về 1 số lệnh sau:

- `more`: dùng để xem nội dung của file từng trang một.
- `vi`: dùng để chỉnh sửa file văn bản.
- `id`: dùng để in ra thông tin về người dùng hiện tại.
- `pwd`: dùng để in ra đường dẫn thư mục hiện tại.

Đối với level này, vì level tiếp không phải là /bin/bash nên đầu tiên mình sẽ xem thử level tiếp theo dùng shell gì. Mình sẽ sử dụng. Theo như mình tìm hiểu thì thông tin về user như UID, GID,.. và đặc biệt là shell mặc định sẽ được lưu ở trong file `/etc/passwd`. Và vì thế, mình sẽ `cat` và `grep` để tìm user `bandit26` để xem shell mặc định khi đăng nhập vào user đó là gì. Và sau đó in ra shell đó.

```
vortex12:x:5012:5012:vortex level 12:/home/vortex12:/bin/bash
vortex13:x:5013:5013:vortex level 13:/home/vortex13:/bin/bash
vortex14:x:5014:5014:vortex level 14:/home/vortex14:/bin/bash
vortex15:x:5015:5015:vortex level 15:/home/vortex15:/bin/bash
vortex16:x:5016:5016:vortex level 16:/home/vortex16:/bin/bash
vortex17:x:5017:5017:vortex level 17:/home/vortex17:/bin/bash
vortex18:x:5018:5018:vortex level 18:/home/vortex18:/bin/bash
vortex19:x:5019:5019:vortex level 19:/home/vortex19:/bin/bash
vortex2:x:5002:5002:vortex level 2:/home/vortex2:/bin/bash
vortex20:x:5020:5020:vortex level 20:/home/vortex20:/bin/bash
vortex21:x:5021:5021:vortex level 21:/home/vortex21:/bin/bash
vortex22:x:5022:5022:vortex level 22:/home/vortex22:/bin/bash
vortex23:x:5023:5023:vortex level 23:/home/vortex23:/bin/bash
vortex24:x:5024:5024:vortex level 24:/home/vortex24:/bin/bash
vortex25:x:5025:5025:vortex level 25:/home/vortex25:/bin/bash
vortex3:x:5003:5003:vortex level 3:/home/vortex3:/bin/bash
vortex4:x:5004:5004:vortex level 4:/home/vortex4:/bin/bash
vortex5:x:5005:5005:vortex level 5:/home/vortex5:/bin/bash
vortex6:x:5006:5006:vortex level 6:/home/vortex6:/bin/bash
vortex7:x:5007:5007:vortex level 7:/home/vortex7:/bin/bash
vortex8:x:5008:5008:vortex level 8:/home/vortex8:/bin/bash
vortex9:x:5009:5009:vortex level 9:/home/vortex9:/bin/bash
bandit25@bandit:~$ cat /etc/passwd | grep bandit26
bandit26:x:11026:11026:bandit level 26:/home/bandit26:/usr/bin/showtext
bandit25@bandit:~$ cat /usr/bin/showtext
#!/bin/sh

export TERM=linux

exec more ~/text.txt
exit 0
bandit25@bandit:~$
```

Như hình ở trên ta có thể thấy, sau khi đăng nhập nó sẽ tự động sử dụng lệnh `more` để xem nội dung của file `text.txt`, và sau đó exit. Và mình sẽ đăng nhập vào thử.

```
--[ Tools ]--

 For your convenience we have installed a few useful tools which you can find
 in the following locations:

    * gef (https://github.com/hugsy/gef) in /opt/gef/
    * pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
    * gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
    * pwntools (https://github.com/Gallopsled/pwntools)
    * radare2 (http://www.radare.org/)

--[ More information ]--

  For more information regarding individual wargames, visit
  http://www.overthewire.org/wargames/

  For support, questions or comments, contact us on discord or IRC.

  Enjoy your stay!

  _                     _ _ _   ___   __
 | |                   | (_) | |__ \ / /
 | |__   __ _ _ __   __| |_| |_   ) / /_
 | '_ \ / _` | '_ \ / _` | | __| / / '_ \
 | |_) | (_| | | | | (_| | | |_ / /| (_) |
 |_.__/ \__,_|_| |_|\__,_|_|\__|____\___/
Connection to localhost closed.
```

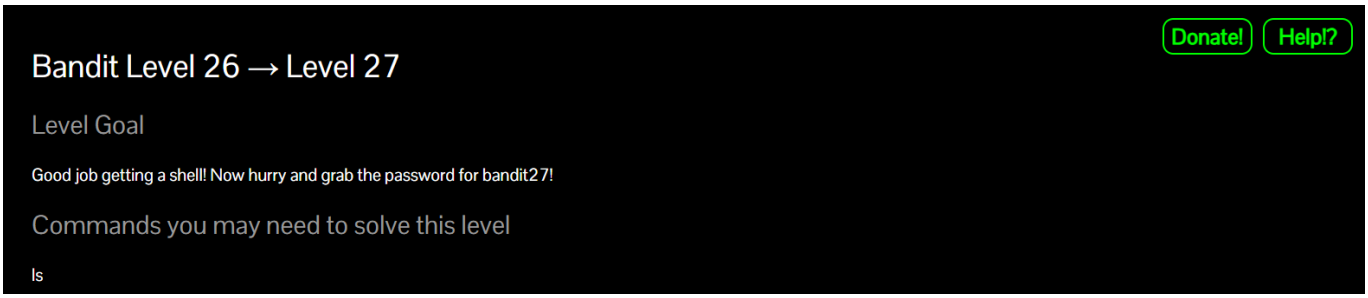
Sau khi đọc xong, nó exit luôn vì nội dung của nó quá ngắn. Vì vậy, sau khi tìm hiểu mình sẽ thử thu nhỏ khung hình lại nó chiếu nội dung file ít hơn. Sau đó mình sẽ sử dụng `v` để vào `vim`, và tiếp theo là set shell

bằng /bin/bash và chuyển sang shell `bash` với lệnh `:!bash`. Sau đó chiếm quyền và in ra password của level tiếp theo.

Password cho level tiếp theo được hiện ra. (`s0773xxkk0MXfdqOfPRVr9L3jJBUOgCZ`)

Level 26 -> level 27

Level yêu cầu mình kết nối tới level tiếp theo tương tự như level 20. (SUID)



Solution

Sau khi kết nối được tới level này và chuyển qua được shell bash. Mình check thấy có phải SUID `bandit27_do` với argument truyền vào là để thực thi 1 lệnh (tương tự level 20). Vì vậy mình cũng sẽ thực hiện tương tự như level 20 là truyền vào path của file lưu password cho level tiếp theo (`/etc/bandit_pass/bandit27`).

Password cho level tiếp theo được hiện ra. (`upsNCc7vzaRDx6oZC6GiR6ERwe1MowGB`)

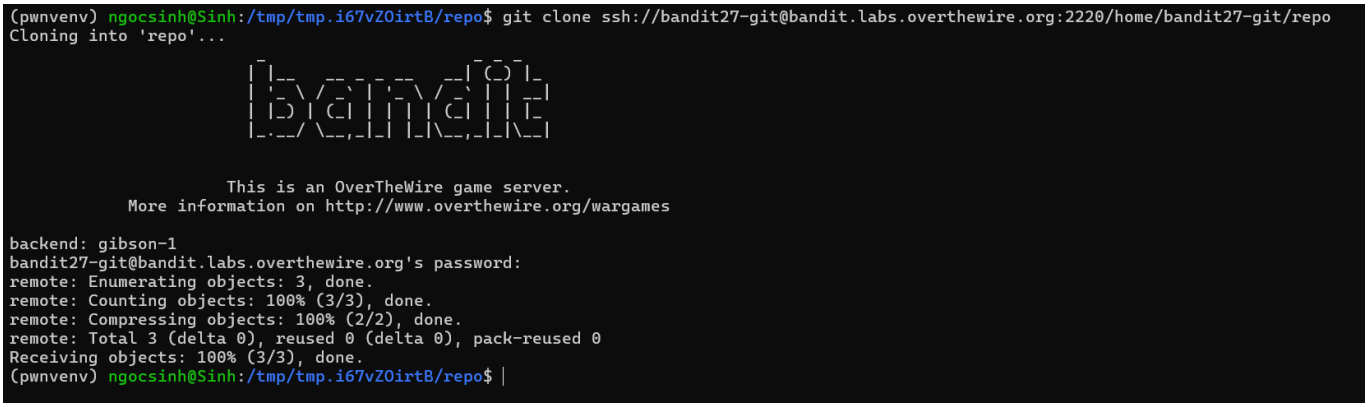
Level 27 -> level 28

Level này yêu cầu mình clone repo (`ssh://bandit27-git@localhost/home/bandit27-git/repo` và port `2220`) xuống và tìm password của level tiếp theo được lưu trong đó.

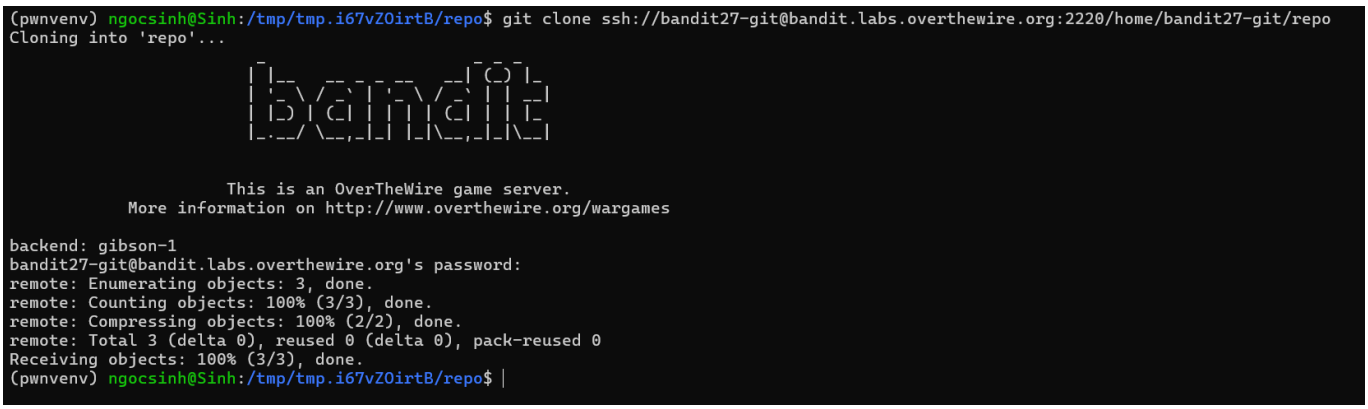
Solution

Đối với level này, mình sử dụng lệnh `git clone` với argument là repo theo yêu cầu.

Cụ thể: `git clone ssh://bandit27-git@bandit.labs.overthewire.org:2220/home/bandit27-git/repo`.



Sao đó mình check thử repo thì thấy password được lưu trong `README`.



Password cho level tiếp theo được hiện ra. (`Yz9IpL0sBcCeuG7m9uQFt8ZNpS4HZRcN`)

Level 28 -> level 29

Tương tự như level trước, level yêu clone repo (`ssh://bandit28-git@localhost/home/bandit28-git/repo` và port `2220`) xuống và tìm password cho level tiếp theo.

Solution

Đối với level này, mình sẽ sử dụng `git clone` để clone repo xuống như level trước đó và sau đó tìm password. Tuy nhiên khi `cat` ra file `README.md` thì phần password chỉ có toàn chữ cái `x`. Sau khi tìm hiểu thì mấy thấy có lệnh git log để xem lịch sử sửa đổi của các lần commit. Và đúng như vậy trước đó password vẫn còn nguyên vẹn nhưng sau đó đã bị fix. Vì vậy mình đã sử dụng lệnh `git checkout` để chuyển lại lần commit đó để xem nội dung file lúc đó. Và sau đó lấy được password.

```
(pwnvenv) ngocsinh@Sinh:/mnt/d/CTF/CTF-Writeups/Overthewire/repo$ ls
README.md
(pwnvenv) ngocsinh@Sinh:/mnt/d/CTF/CTF-Writeups/Overthewire/repo$ cat README.md
# Bandit Notes
Some notes for level29 of bandit.

## credentials

- username: bandit29
- password: xxxxxxxxxx

(pwnvenv) ngocsinh@Sinh:/mnt/d/CTF/CTF-Writeups/Overthewire/repo$ git log
commit 710c14a2e43cfd97041924403e00efb00b3a956e (HEAD -> master, origin/master, origin/HEAD)
Author: Morla Porla <morla@overthewire.org>
Date:   Fri Aug 15 13:16:10 2025 +0000

    fix info leak

commit 68314e012fbaa192abfc9b78ac369c82b75fab8f
Author: Morla Porla <morla@overthewire.org>
Date:   Fri Aug 15 13:16:10 2025 +0000

    add missing data

commit a158f9a82c29a16dcea4744458a5ccf692a385cd4
Author: Ben Dover <noone@overthewire.org>
Date:   Fri Aug 15 13:16:10 2025 +0000

    initial commit of README.md
(pwnvenv) ngocsinh@Sinh:/mnt/d/CTF/CTF-Writeups/Overthewire/repo$
```

Chuyển sang lần commit với id đó.

```
(pwnvenv) ngocsinh@Sinh:/mnt/d/CTF/CTF-Writeups/Overthewire/repo$ git checkout 68314e012fbaa192abfc9b78ac369c82b75fab8f
Note: switching to '68314e012fbaa192abfc9b78ac369c82b75fab8f'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to false

HEAD is now at 68314e0 add missing data
(pwnvenv) ngocsinh@Sinh:/mnt/d/CTF/CTF-Writeups/Overthewire/repo$ cat README.md
# Bandit Notes
Some notes for level29 of bandit.

## credentials

- username: bandit29
- password: 4pT1t5DENaYuqnqvadYs1oE4QLCdjmJ7

(pwnvenv) ngocsinh@Sinh:/mnt/d/CTF/CTF-Writeups/Overthewire/repo$
```

Password cho level tiếp theo được hiện ra. (`4pT1t5DENaYuqnqvadYs1oE4QLCdjmJ7`)

Level 29 -> level 30

Tương tự như level trước, level yêu clone repo (`ssh://bandit29-git@localhost/home/bandit29-git/repo` và port `2220`) xuống và tìm password cho level tiếp theo.

Solution

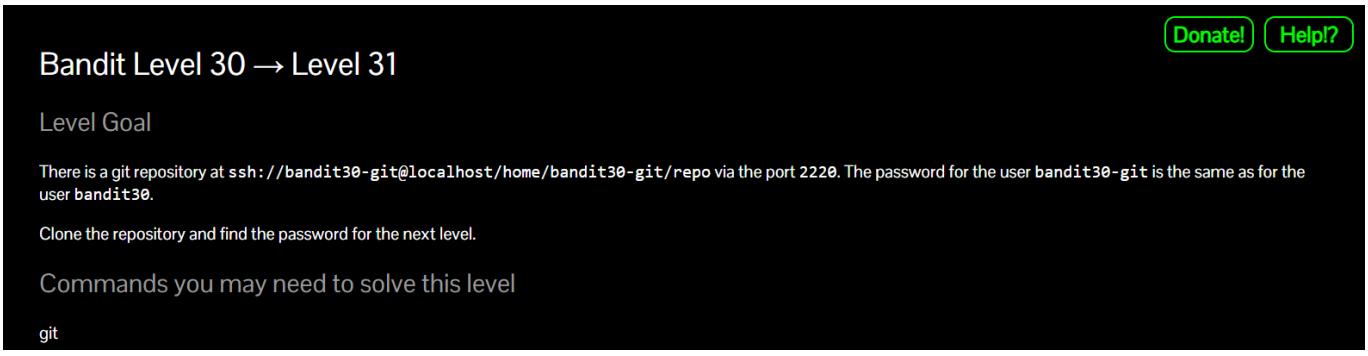
Đối với level này, mình sẽ sử dụng `git clone` để clone repo xuống như level trước đó và sau đó tìm password. Tuy nhiên khi `cat` ra file `README.md` thì phần password đã bị giấu nhưng tương tự như bài trước, ngoài `git log` để xem các lịch sử commit thì chúng ta còn có `git branch` để xem các nhánh khác có trong repo (thêm option `-a` để xem tất cả các nhánh có trong repo). Sau đó mình đã chuyển sang branch `dev` và file `README.md` đã hiện password cho level tiếp theo.

```
(pwnvenv) ngocsinh@Sinh:/tmp/tmp.sBCPJAlnmO/repo$ ls
README.md
(pwnvenv) ngocsinh@Sinh:/tmp/tmp.sBCPJAlnmO/repo$ cat README.md
# Bandit Notes
Some notes for bandit30 of bandit.

## credentials

- username: bandit30
- password: <no passwords in production!>

(pwnvenv) ngocsinh@Sinh:/tmp/tmp.sBCPJAlnmO/repo$ git branch -a
  dev
* master
  remotes/origin/HEAD -> origin/master
  remotes/origin/dev
  remotes/origin/master
  remotes/origin/sploits-dev
(pwnvenv) ngocsinh@Sinh:/tmp/tmp.sBCPJAlnmO/repo$ git checkout dev
Switched to branch 'dev'
Your branch is up to date with 'origin/dev'.
(pwnvenv) ngocsinh@Sinh:/tmp/tmp.sBCPJAlnmO/repo$ cat README.md
# Bandit Notes
Some notes for bandit30 of bandit.

## credentials

- username: bandit30
- password: qp30ex3VLz5MDG1n91YowTv4Q8l7CDZL

(pwnvenv) ngocsinh@Sinh:/tmp/tmp.sBCPJAlnmO/repo$
```

Password cho level tiếp theo được hiện ra. (`qp30ex3VLz5MDG1n91YowTv4Q8l7CDZL`)

Level 30 -> level 31

Tương tự như level trước, level yêu clone repo (`ssh://bandit30-git@localhost/home/bandit30-git/repo` và port `2220`) xuống và tìm password cho level tiếp theo.



Solution

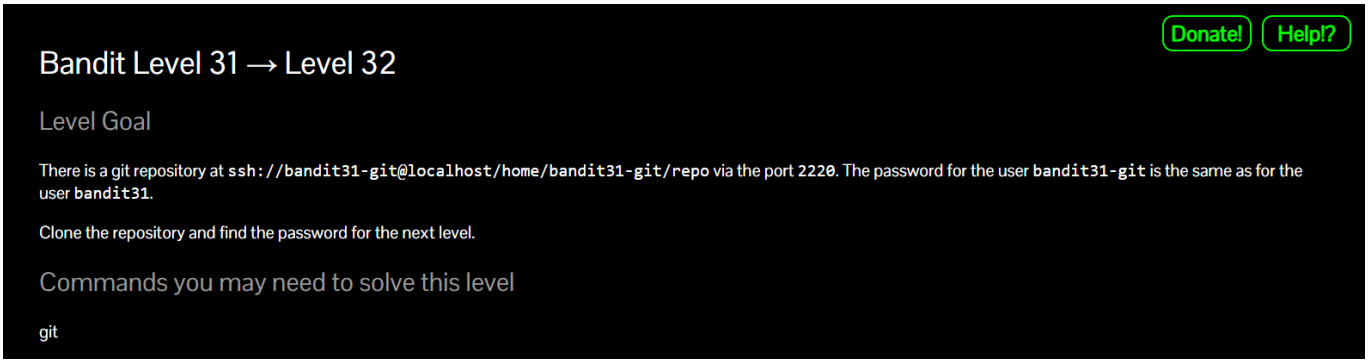
Đối với level này, mình sẽ sử dụng `git clone` để clone repo xuống như level trước đó và sau đó tìm password. Tuy nhiên khi `cat` ra file `README.md` thì phần password đã bị giấu nhưng tương tự như bài trước, ngoài `git log` và `git branch` ra chúng ta còn có `git tag` để xem các tag của các commit được đánh dấu. Vì vậy mình sẽ sử dụng git tag để xem các commit được đánh dấu và dùng `git show` để xem chi tiết về commit đó.

```
(pwnvenv) ngocsinh@Sinh:/tmp/tmp.sBCPJAlnmO/repo$ ls
README.md
(pwnvenv) ngocsinh@Sinh:/tmp/tmp.sBCPJAlnmO/repo$ cat README.md
just an epmty file... muahaha
(pwnvenv) ngocsinh@Sinh:/tmp/tmp.sBCPJAlnmO/repo$ git tag
secret
(pwnvenv) ngocsinh@Sinh:/tmp/tmp.sBCPJAlnmO/repo$ git show secret
fb5S2xb7bRyFmAvQYQGEqsbhVyJqhnDy
(pwnvenv) ngocsinh@Sinh:/tmp/tmp.sBCPJAlnmO/repo$
```

Password cho level tiếp theo được hiện ra. (`fb5S2xb7bRyFmAvQYQGEqsbhVyJqhnDy`)

Level 31 -> level 32

Tương tự như level trước, level yêu clone repo (`ssh://bandit31-git@localhost/home/bandit31-git/repo` và port `2220`) xuống và tìm password cho level tiếp theo.



Solution

Đối với level này, mình sẽ sử dụng `git clone` để clone repo xuống như level trước đó và sau đó tìm password. Tuy nhiên khi `cat` ra file `README.md` nội dung của file bảo là mình tạo 1 file `key.txt` với content là `May I come in?` sau đó push lên server. Vì vậy mình sẽ tạo file tương ứng đó và sử dụng:

- `git add`: để thêm file vào các file cần push
- `git commit`: để lưu lại các thay đổi
- `git push`: để đẩy các commit lên server

```
(pwnvenv) ngocsinh@Sinh:/tmp/tmp.Asv5wjZBUr$ ls
repo
(pwnvenv) ngocsinh@Sinh:/tmp/tmp.Asv5wjZBUr$ cd repo
(pwnvenv) ngocsinh@Sinh:/tmp/tmp.Asv5wjZBUr/repo$ ls
README.md
(pwnvenv) ngocsinh@Sinh:/tmp/tmp.Asv5wjZBUr/repo$ cat README.md
This time your task is to push a file to the remote repository.

Details:
    File name: key.txt
    Content: 'May I come in?'
    Branch: master

(pwnvenv) ngocsinh@Sinh:/tmp/tmp.Asv5wjZBUr/repo$ echo 'May I come in?' > key.txt
```

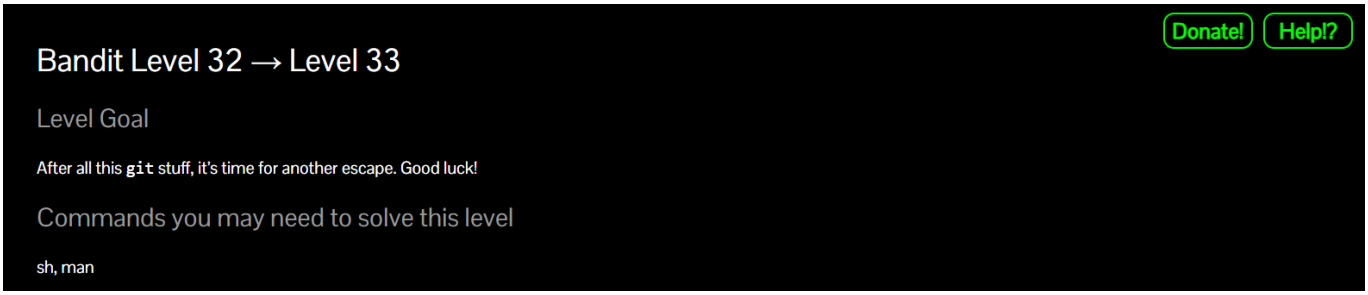
Push file lên server.

```
(pwnvenv) ngocsinh@Sinh:/tmp/tmp.Asv5wjZBUr/repo$ git add -f key.txt
(pwnvenv) ngocsinh@Sinh:/tmp/tmp.Asv5wjZBUr/repo$ git commit -m "Add key.txt file"
[master 0f45735] Add key.txt file
 1 file changed, 1 insertion(+)
 create mode 100644 key.txt
(pwnvenv) ngocsinh@Sinh:/tmp/tmp.Asv5wjZBUr/repo$ git push
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


                      This is an OverTheWire game server.
            More information on http://www.overthewire.org/wargames

backend: gibson-1
bandit31-git@bandit.labs.overthewire.org's password:
Enumerating objects: 4, done.
Counting objects: 100% (4/4), done.
Delta compression using up to 4 threads
Compressing objects: 100% (2/2), done.
Writing objects: 100% (3/3), 335 bytes | 335.00 KiB/s, done.
Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
remote: ### Attempting to validate files... ####
remote:
remote: .oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.oOo.
remote:
remote: Well done! Here is the password for the next level:
remote: 3O9RfhqyAlVBEZpVb6LYStshZoqoSx5K
```

Password cho level tiếp theo được hiện ra. (`3O9RfhqyAlVBEZpVb6LYStshZoqoSx5K`)

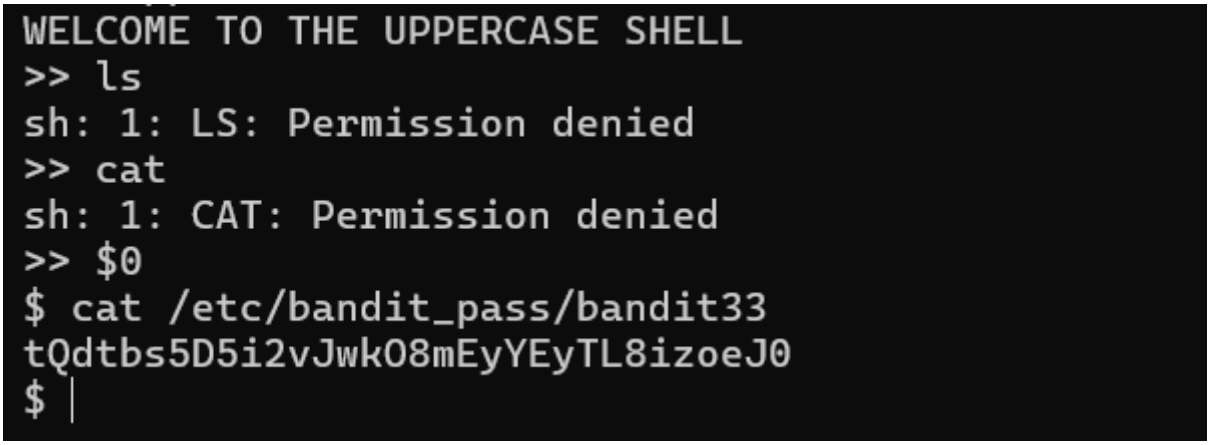
Level 32 -> level 33

Level yêu cầu mình tìm password cho level tiếp theo. Tuy nhiên trong level hiện tại, khi chúng ta connect vào thì nó sẽ tự động khởi chạy uppershell.



Solution

Đối với level này, vì khi chúng ta thực hiện lệnh nào đó thì nó sẽ tự động uppercase shell đó lên vì vậy nó sẽ không thực hiện được và báo lỗi. Vì vậy, sau khi tìm hiểu và thử thì mình thấy chúng ta có `$0` sẽ lưu shell mà hiện tại chúng ta đang dùng. Nên mình sẽ khởi chạy lại shell đó và thực hiện cat password của level tiếp theo.



Password cho level tiếp theo được hiện ra. (`tQdtbs5D5i2vJwkO8mEyYEyTL8izoeJ0`)