Бандит

Для начала перешел на сервер введя нужные данные

```
C:\Users\lenovo>ssh bandit0bandit.labs.overthewire.org -p 2220
ssh: Could not resolve hostname bandit0bandit.labs.overthewire.org: \335\362\356\362 \365\356\361
42\345\361\362\345\355.

C:\Users\lenovo>ssh bandit0@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

backend: gibson-1
bandit0@bandit.labs.overthewire.org's password:
Permission denied, please try again.
bandit0@bandit.labs.overthewire.org's password:
```

Чтобы перейти на следующего ввел

```
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
```

И получил пароль

1) ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If

Ввел и перешел на следующий уровень

```
bandit1@bandit:~$
```

Использую подсказки на сайте продолжаем далее

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

2) 263JGJPfgU6LtdEvgfWU1XP5yac29mFx

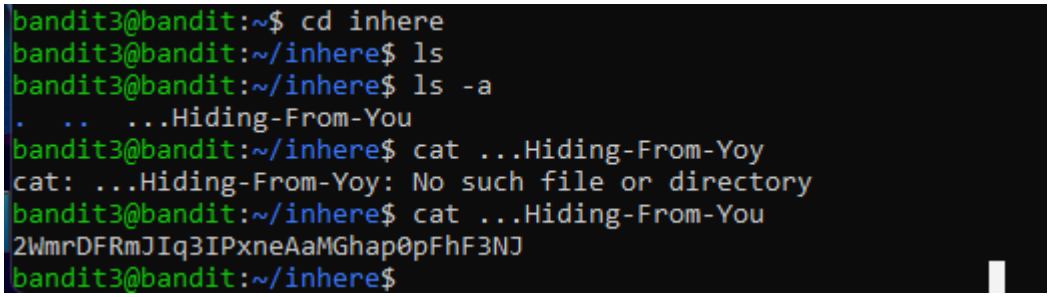
Следующий пароль

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

3) MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx

Тут начинается работа с директорией inhere

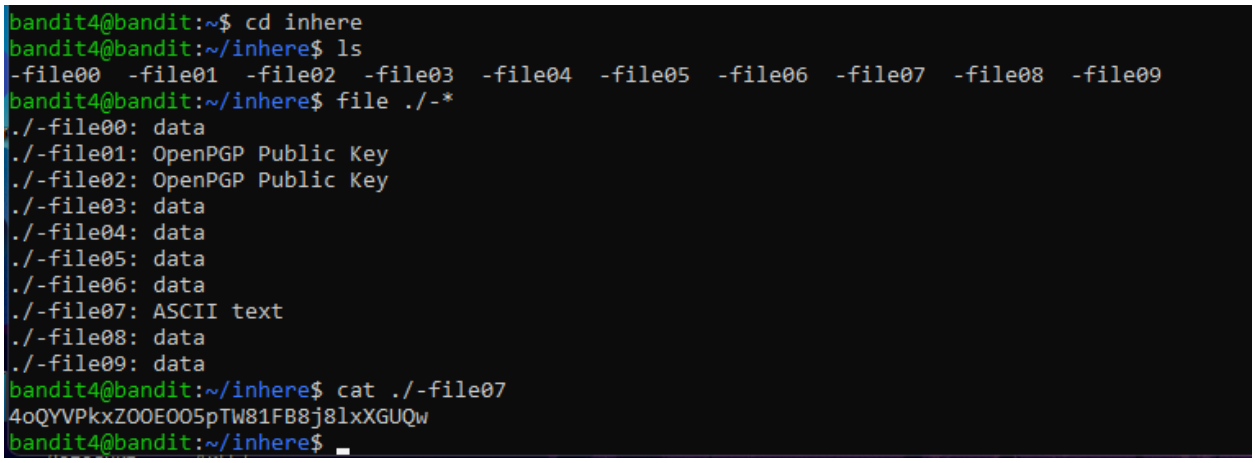
-a – включает содержимое начинающееся с .



4) 2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ

В той же директории ищем следующий пароль.

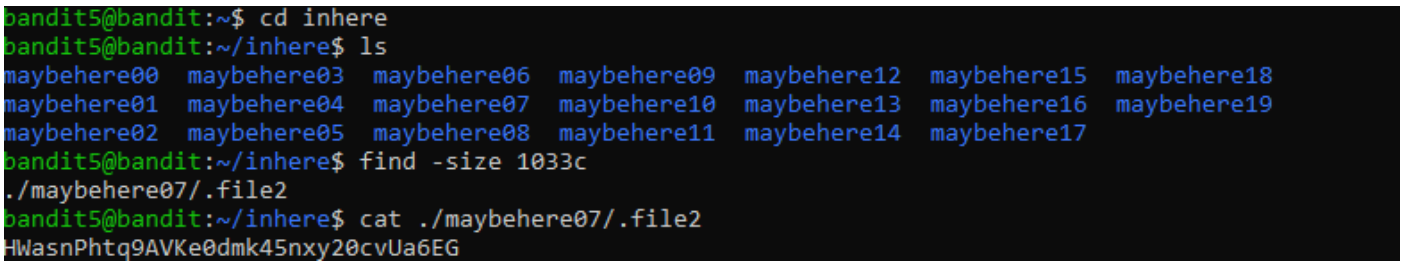
Для работы с этим использую file для получения типа файла, а * использую так как файлы начинаются с –
* - сколько угодно любых знаков



5) 4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw

Теперь работа с размером 1033

Для этого использую find –cize 1033c



6) HWasnPhtq9AVKe0dmk45nxy20cvUa6EG

Теперь ищу файл на сервере, который принадлежит пользователю bandit7, группе bandit6 и весит 33 байта

Вспоминаю и юзаю –user –group

```
bandit6@bandit:~$ cd /
bandit6@bandit:/$ find -user bandit7 -group bandit6 -size 33c
find: ‘./proc/tty/driver’: Permission denied
find: ‘./proc/1/task/1/fd’: Permission denied
find: ‘./proc/1/task/1/fdinfo’: Permission denied
find: ‘./proc/1/task/1/ns’: Permission denied
find: ‘./proc/1/fd’: Permission denied
find: ‘./proc/1/map_files’: Permission denied
find: ‘./proc/1/fdinfo’: Permission denied
find: ‘./proc/1/ns’: Permission denied
find: ‘./proc/2/task/2/fd’: Permission denied
find: ‘./proc/2/task/2/fdinfo’: Permission denied
find: ‘./proc/2/task/2/ns’: Permission denied
find: ‘./proc/2/fd’: Permission denied
find: ‘./proc/2/map_files’: Permission denied
find: ‘./proc/2/fdinfo’: Permission denied
find: ‘./proc/2/ns’: Permission denied
find: ‘./proc/17/task/17/fd/6’: No such file or directory
find: ‘./proc/17/task/17/fdinfo/6’: No such file or directory
find: ‘./proc/17/fd/5’: No such file or directory
find: ‘./proc/17/fdinfo/5’: No such file or directory
```

Ищу единсвенный файл с доступом

```
find: ‘./var/lib/private’: Permission denied
find: ‘./var/lib/ubuntu-advantage/apt-esm/var/lib/apt/lists/partial’:
./var/lib/dpkg/info/bandit7.password
find: ‘./var/lib/amazon’: Permission denied
find: ‘./var/crash’: Permission denied
```

```
bandit6@bandit:/$ cat ./var/lib/dpkg/info/bandit7.password
morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj
bandit6@bandit:/$
```

7) morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj

Теперь поиск по файлу data.txt и найти напротив слова millionth

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

8) dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc

Sort – для сортировки по требованию

Uniq – уникальыне строки с –u (тоолько строки выходящие 1 раз)

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

9) 4CKMh1JI91bUIZZPXDqGanal4xvAg0JM

Далее Паролей там ооооооочень много поэтому юзаю strings для последовательности меньше 4

-10 – кол-во неприрывных символов в строке

```
bandit9@bandit:~$ strings -10 data.txt
========== the
========== password
f\Z'========== is
========== FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey
```

10) FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey

Base64 – декодинг и кодинг данных base64

-d – декодировать

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

11) dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr

Использую tr для передвижения (замены) букв на 13 пунктов

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

12) 7x16WNeHIi5YkIhWsfFIqoognUTyj9Q4