

BÀI TẬP BANDIT

Level 0

Sử dụng lệnh ssh để kết nối với server bandit theo cú pháp

- `$ ssh <username>@<remote> -p <port number>`

Khi kết nối, ta sử dụng mật khẩu “bandit0” đã cho trước để đăng nhập vào

Level 0 → 1

Sử dụng lệnh ls để kiểm tất cả các file và folder có trên máy

Dùng lệnh cat để đọc nội dung file

```
bandit0@bandit:~$ ls  
readme  
bandit0@bandit:~$ cat readme  
NH2SXQwcBdpmTEzi3bvBHMM9H66vVxjL
```

Kết quả sau khi lấy được flag và chuyển sang level 1

Level 1 → 2

Sử dụng lệnh ls để kiểm tất cả các file và folder trên máy

Vì file này có tên là dấu “-“ đặc biệt nên không thể dùng lệnh cat lên thẳng tên file để đọc, cần thêm “./” trước file

```
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat -
^Z
[1]+  Stopped                  cat -
bandit1@bandit:~$ cat ./-
rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi
bandit1@bandit:~$ exit
```

Kết quả sau khi lấy được flag và chuyển sang level 2

Level 2 → 3

Sử dụng lệnh ls để kiểm tất cả các file và folder trên máy

Vì file này có dấu cách trong tên nên không thể cứ thế cat mà phải đưa vào trong ngoặc kép hoặc thêm dấu “ ` ” trước mỗi dấu cách trong tên file

```
bandit2@bandit:~$ ls  
spaces in this filename  
bandit2@bandit:~$ cat ./space-in-this-filename  
cat: ./space-in-this-filename: No such file or directory  
bandit2@bandit:~$ cat spaces\ in\ this\ filename  
aBZ0W5EmUfAf7kHTQe0wd8bauFJ2lAiG  
bandit2@bandit:~$ cat "spaces in this filename"  
aBZ0W5EmUfAf7kHTQe0wd8bauFJ2lAiG  
bandit2@bandit:~$
```

Kết quả sau khi lấy được flag và chuyển sang level 3

```
bandit2@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.

└─(kali㉿kali)-[~]
$ ssh bandit3@bandit.labs.overthewire.org -p 2220
[██████████] [██████████] [██████████] [██████████]

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

bandit3@bandit.labs.overthewire.org's password:
[██████████] [██████████] [██████████] [██████████]

www.verheire.org
```

Level 3 → 4

Sử dụng lệnh ls để kiểm tất cả các file và folder trên máy

Sử dụng lệnh cd để đi vào thư mục /inhere

Vì file ẩn nên sử dụng ls –a để kiểm toàn bộ file

```
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ ls -a
. .. .hidden
bandit3@bandit:~/inhere$ cat .hidden
2EW7BBSr6aMMoJ2HjW067dm8EgX26xNe
bandit3@bandit:~/inhere$ cd
bandit3@bandit:~$ exit
logout
```

Kết quả sau khi lấy được flag và chuyển sang level 4

```
bandit3@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.

└─(kali㉿kali)-[~]
$ ssh bandit4@bandit.labs.overthewire.org -p 2220
[██████████] [██████████] [██████████] [██████████]

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

bandit4@bandit.labs.overthewire.org's password:
```



Level 4 → 5

Sử dụng lệnh ls -a để kiểm toàn bộ tất cả các file và folder trên máy

Dùng lệnh cd để di chuyển vào thư mục /inhere

Sử dụng lệnh ls -a để kiểm toàn bộ tất cả các file và folder trong thư mục /inhere

Để tìm file có dạng đọc được, ta dùng lệnh find và xargs (–type f là để giới hạn tìm kiếm file)

Dùng lệnh cat để đọc file duy nhất người đọc được

```
bandit4@bandit:~$ ls -a
. .. .bash_logout .bashrc inhere .profile
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls -a
. -file00 -file02 -file04 -file06 -file08
.. -file01 -file03 -file05 -file07 -file09
bandit4@bandit:~/inhere$ find . -type f | xargs file
./-file01: data
./-file02: data
./-file08: data
./-file06: data
./-file00: data
./-file04: data
./-file05: data
./-file07: ASCII text
./-file03: data
./-file09: data
bandit4@bandit:~/inhere$ cat -file07
cat: invalid option -- 'f'
Try 'cat --help' for more information.
bandit4@bandit:~/inhere$ cat ./-file07
lrIWWI6bB37kxfiCQZqUd0IYfr6eEeqR
```

Kết quả sau khi lấy được flag và chuyển sang level 5

```
bandit4@bandit:~/inhere$ exit
logout
Connection to bandit.labs.overthewire.org closed.

└─[kali㉿kali]─[~]
$ ssh bandit5@bandit.labs.overthewire.org -p 2220
[██████████] [██████████] [██████████]
[██████████] [██████████] [██████████]
[██████████] [██████████] [██████████]

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

bandit5@bandit.labs.overthewire.org's password:
[██████████] [██████████] [██████████]
[██████████] [██████████] [██████████]
[██████████] [██████████] [██████████]

http://www.overthewire.org/wargames
```

Level 5 → 6

Sử dụng lệnh ls -a để kiểm toàn bộ tất cả các file và folder trên máy

Dùng lệnh cd để di chuyển vào thư mục /inhere

Sử dụng lệnh ls -a để kiểm toàn bộ tất cả các file và folder trong thư mục /inhere

Để tìm file có dạng đọc được, ta dùng lệnh find và điều kiện executable (-type f là để giới hạn tìm kiếm file, -size 1033c là năng 1033 byte)

Dùng lệnh cat để đọc file tìm được

```
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls -a
.          maybehere02  maybehere06  maybehere10  maybehere14  maybehere18
..         maybehere03  maybehere07  maybehere11  maybehere15  maybehere19
maybehere00  maybehere04  maybehere08  maybehere12  maybehere16
maybehere01  maybehere05  maybehere09  maybehere13  maybehere17
bandit5@bandit:~/inhere$ find . -type f -size 1033c ! -execut
find: unknown predicate `~execute'
bandit5@bandit:~/inhere$ find . -type f -size 1033c ! -execu
find: unknown predicate `~execu'
bandit5@bandit:~/inhere$ find . -type f -size 1033c ! -executable
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU
```

Kết quả sau khi lấy được flag và chuyển sang level 6

Level 6 → 7

Sử dụng lệnh ls -a để kiểm toàn bộ tất cả các file và folder trên máy

Dùng lệnh cd để di chuyển vào thư mục /inhere

Sử dụng lệnh ls -a để kiểm toàn bộ tất cả các file và folder trong thư mục /inhere

Để tìm file có dạng đọc được, ta dùng lệnh find (-type f là để giới hạn tìm kiếm file, -user bandit7 là giới hạn người dùng tên bandit7, -group bandit6 là giới hạn nhóm sở hữu tên bandit6 và -size 33c là tìm file nồng độ 33 byte)

```
bandit6@bandit:~$ ls -a
. .. .bash_logout .bashrc .profile
bandit6@bandit:~$ find / -type f -user bandit7 -group bandit6 -size 33c
find: '/etc/ssl/private': Permission denied
find: '/etc/polkit-1/localauthority': Permission denied
find: '/etc/sudoers.d': Permission denied
find: '/etc/multipath': Permission denied
find: '/root': Permission denied
find: '/boot/efi': Permission denied
```

File duy nhất phù hợp

```
denied
find: '/var/lib/amazon': Permission denied
/var/lib/dpkg/info/bandit7.password
find: '/var/log': Permission denied
find: '/var/cache/private': Permission denied
```

Dùng lệnh cat để đọc file tìm thấy

```
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S
bandit6@bandit:~$
```

Kết quả sau khi lấy được flag và chuyển sang level 7

Level 7 → 8

Sử dụng lệnh ls -a để kiểm toàn bộ tất cả các file và folder trên máy

Ta thấy có file data.txt có thể đọc

Cat file thấy nó chứa rất nhiều string có thể chứa mật khẩu

```
bandit7@bandit:~$ ls -a
. .. .bash_logout .bashrc data.txt .profile
bandit7@bandit:~$ cat data.txt
gallop hu3ZhCrGRvfa05jsY6ttvApzVCA2Hjvs
Aurelia's ikl4F3cK5m6Cl6HAxva6zUAVJhI2Cvc6
stoicism JiW9ts44udf20bJHe8H5dS1c99Muwz42
```

Sử dụng lệnh strings để đọc các string trong data.txt và grep để tìm cụm từ “millionth”

```
bandit7@bandit:~$ strings data.txt | grep "millionth"
millionth      TESKZC0XvTetK0S9xNwm25STk5iWrBvP
```

Kết quả sau khi lấy được flag và chuyển sang level 8

```
bandit7@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.

└─(kali㉿kali)-[~]
└─$ ssh bandit8@bandit.labs.overthewire.org -p 2220
[REDACTED]

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

bandit8@bandit.labs.overthewire.org's password:
[REDACTED]
```

Level 8 → 9

Sử dụng lệnh ls -a để kiểm toàn bộ tất cả các file và folder trên máy

Ta thấy có file data.txt có thể đọc

Cat file thấy nó chứa rất nhiều string có thể chứa mật khẩu

```
bandit8@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  data.txt  .profile
bandit8@bandit:~$ cat data.txt
kjIuqjobFBhKw9Mmfj2wAniWbXB2VxSfv
5Y76FifuxKStZi4CVovF2uPhgLrZnLzG
AiYd84l00VTA4gqJPX7f6DH8eG3zwq1W
```

Sử dụng lệnh strings để đọc các string trong data.txt và uniq -c để đếm số string lặp trong file

```
qloQnuijJULtNwvInPelooyLoLyPLvuagSK  
bandit8@bandit:~$ sort data.txt | uniq -c  
 10 18DyjwhN856SsMx8bNrFSvr6rJxNQKhE  
 10 1iyGemEgn3qU00FcAJyGPH0iewqZyp1y  
 10 2CQ5DQRdte9Ft8YpMHqCwQcN18k9lCI  
 10 365RauAVsFlxktPMpoLtIf1uxijU1TfV  
 10 4K2MoVHd1gXfoOdDjvlaRxFNZwmI4A4C  
 10 52p0CnGhAvm4m3fPKqz9mTxVDeVYCvnG  
 10 5Y76FifuxKStZi4CVovF2uPhgLrZnLzG  
 10 7A4l2BI3lPJgNdWAMyXAGlfB8uvCQLX0  
 10 8cxarYi5VoKRj3lzo2baLOJaMgUtzoRH  
 10 97Qwmy18JE8aGIud1stpTsOrOtUMHeGI  
 10 9d8exmGtSsGcU1gz6HmgTfSxmnmI4FB0
```

Ta tìm được string duy nhất không lặp

```
10 eJZcdtHKg9jLpvP9Kv31Fj1opqlA1A9k  
1 EN632PlfYiZbn3PhVK3XOGSLNInNE00t  
10 eNdwlpf6iBeQ3o11iHefoHd9GYKDThFQ
```

Kết quả sau khi lấy được flag và chuyển sang level 9

Level 9 → 10

Sử dụng lệnh ls -a để kiểm toàn bộ tất cả các file và folder trên máy

Ta thấy có file data.txt có thể đọc

Cat file thấy nó chứa các string không thể đọc

Sử dụng lệnh strings để đọc các string trong data.txt và grep để tìm dấu “=” và tìm được một chuỗi string phù hợp yêu cầu đề bài

```
◆bandit9@bandit:~$ strings data.txt | grep "="
=2""L(
x]T_____ theG)"
_____ passwordk^
Y=xW
t%oq
_____ is
4=D3
{1\o
FC&z
=Y!m
      $/2`)=Y
4_Qo\
MOo(
?-|J
WXDA
{TbJ; oI
[=lI
_____ G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s
>8o6
=r_o_
=u ea
zlo4
```

Kết quả sau khi lấy được flag và chuyển sang level 10

Level 10 → 11

Sử dụng lệnh ls -a để kiểm toàn bộ tất cả các file và folder trên máy

Ta thấy có file data.txt có thể đọc

Cat file thấy nó chứa string đã được encode base64

Sử dụng lệnh strings để đọc các string trong data.txt và –decode để decode đoạn string được flag cho bandit11

```
bandit10@bandit:~$ ls -a
. .. .bash_logout .bashrc data.txt .profile
bandit10@bandit:~$ strings data.txt | base64 --decode
The password is 6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM
bandit10@bandit:~$
```

Kết quả sau khi lấy được flag và chuyển sang level 11

Level 11 → 12

Sử dụng lệnh ls -a để kiểm toàn bộ tất cả các file và folder trên máy

Ta thấy có file data.txt có thể đọc

Cat file thấy nó chứa string đã được encode rot13

Sử dụng lệnh strings để đọc các string trong data.txt và tr để decode đoạn string được flag cho bandit11

```
bandit11@bandit:~$ ls -a
. .. .bash_logout .bashrc data.txt .profile
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf WIA0OSFzMjXXBC0KoSKBbJ8puQm5lIEi
bandit11@bandit:~$ strings data.txt | rot13
Command 'rot13' not found, but can be installed with:
apt install bsdgames # version 2.17-29, or
apt install hxtools # version 20211204-1
Ask your administrator to install one of them.
bandit11@bandit:~$ strings data.txt | tr '[a-z][A-Z]' '[n-zA-m][N-ZA-M]'
The password is JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv
bandit11@bandit:~$
```

Kết quả sau khi lấy được flag và chuyển sang level 12

```
[kali㉿kali)-[~] $ ssh bandit12@bandit.labs.overthewire.org -p 22
```

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

bandit12@bandit.labs.overthewire.org's password:

Level 12 → 13

Sử dụng lệnh ls -a để kiểm toàn bộ tất cả các file và folder trên máy

Cat file data.txt ta thấy nó là một file hex dump

```
bandit12@bandit:~$ ls -a
. .. .bash_logout .bashrc data.txt .profile
bandit12@bandit:~$ cat data.txt
00000000: 1f8b 0808 6855 1e65 0203 6461 7461 322e ....hU.e..data2.
00000010: 6269 6e00 013d 02c2 fd42 5a68 3931 4159 bin..= ... BZh91AY
00000020: 2653 5948 1b32 0200 0019 ffff faee cff7 &SYH.2.....
00000030: f6ff e4f7 bfbc ffff bffd ff9 39ff 7ffb .....9 ...
00000040: bd31 eeff b9fb fbbb b9bf f77f b001 3b2c .1.....;;
00000050: d100 0d03 d200 6868 0d00 0069 a00d 0340 .....hh...i...@
00000060: 1a68 00d0 0d01 a1a0 0001 a680 0003 46d4 .h.....F.
00000070: 6434 3234 611a 340d 07a4 c351 068f 5000 d424a.4....Q..P.
00000080: 069a 0680 0000 0006 8006 8da4 681a 6868 .....h.hh
00000090: 0d06 8d00 6834 3400 d07a 9a00 01a0 0341 .....h44..z....A
000000a0: ea1e a190 da40 3d10 ca68 3468 6800 00c8 .....@=..h4hh...
000000b0: 1a1a 1b50 0683 d434 d069 a0d0 3100 d000 ... P ... 4.i..1...
000000c0: 001e a680 00d0 1a00 d0d0 6864 d0c4 d0d0 .....hd...
000000d0: 000c 8641 7440 0108 032e 86b4 4cf0 22bb ...At@.....L.".
000000e0: 6682 2b7e b3e2 e98d aa74 dacc 0284 330d f.+~....t....3.
000000f0: bbb2 9494 d332 d933 642a 3538 d27e 09ce .....2.3d*58.~..
00000100: 53da 185a 505e aada 6c75 59a2 b342 0572 S..ZP^..luY..B.r
00000110: 249a 4600 5021 25b0 1973 c18a 6881 1bef $.F.P!%..s..h...
00000120: 3f9b 1429 5b1d 3d87 68b5 804f 1d28 42fa ?..)[.=.h..O.(B.
00000130: 16c2 3241 98fb 8229 e274 5a63 fe92 3aca ..2A...).tZc...:.
00000140: 70c3 a329 d21f 41e0 5a10 08cb 888f 30df p..) ..A.Z.....0.
```

Tạo thư mục mới /tmp/21521386

```
bandit12@bandit:~$ mkdir /tmp/21521386
```

Copy file data.txt vào thư mục vừa tạo

```
bandit12@bandit:~$ cp data.txt /tmp/21521386
```

CD để di chuyển đến vị trí thư mục mới vừa tạo

```
bandit12@bandit:/tmp$ cd /tmp/21521386
bandit12@bandit:/tmp/21521386$ ls -a
. .. data.txt
bandit12@bandit:/tmp/21521386$ cat data.txt
00000000: 1f8b 0808 6855 1e65 0203 6461 7461 322e ....hU.e..data2.
00000010: 6269 6e00 013d 02c2 fd42 5a68 3931 4159 bin..= ...BZh91AY
00000020: 2653 5948 1b32 0200 0019 ffff faee cff7 &SYH.2.....
00000030: f6ff e4f7 bfbc ffff bff7 ffb9 39ff 7ffb .....9...
00000040: bd31 eeff b9fb fbbb b9bf f77f b001 3b2c .1.....;;
00000050: d100 0d03 d200 6868 0d00 0069 a00d 0340 .....hh...i...@
00000060: 1a68 00d0 0d01 a1a0 0001 a680 0003 46d4 .h.....F.
00000070: 6434 3234 611a 340d 07a4 c351 068f 5000 d424a.4....Q..P.
00000080: 069a 0680 0000 0006 8006 8da4 681a 6868 .....h.hh
```

Vì file data.txt là 1 hex dump nên ta cần reverse nó bằng lệnh xxd -r và đưa nó vào file mới data

```
bandit12@bandit:/tmp/21521386$ xxd -r data.txt > data
bandit12@bandit:/tmp/21521386$ ls -a
. .. data data.txt
```

Dùng lệnh file để xác định các dạng nén file đã sử dụng

Có 3 dạng nén trong bandit12 đó là gzip, bzip2 và hệ thống archive tar

1. Gzip:

```
:/tmp/21521386$ file data
data: gzip compressed data, was "data2.bin", last modified: Thu Oct  5 06:19:20 2023, max compression, from U
nix, original size modulo 2^32 573
bandit12@bandit:/tmp/21521386$ gunzip data
gzip: data: unknown suffix -- ignored
bandit12@bandit:/tmp/21521386$ gzip -d data
gzip: data: unknown suffix -- ignored
bandit12@bandit:/tmp/21521386$ mv data data2.gz
bandit12@bandit:/tmp/21521386$ ls -a
. .. data2.gz data.txt
bandit12@bandit:/tmp/21521386$ gzip -d data2.gz
bandit12@bandit:/tmp/21521386$ file data2
data2: bzip2 compressed data, block size = 900k
```

2. Bzip2:

```
bandit12@bandit:/tmp/21521386$ ls -a
. .. data2.gz data.txt
bandit12@bandit:/tmp/21521386$ gzip -d data2.gz
bandit12@bandit:/tmp/21521386$ file data2
data2: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/21521386$ mv data2.gz data3.bz2
mv: cannot stat 'data2.gz': No such file or directory
bandit12@bandit:/tmp/21521386$ ls -a
. .. data2 data.txt
bandit12@bandit:/tmp/21521386$ mv data2 data3.bz2
bandit12@bandit:/tmp/21521386$ file data3
data3: cannot open `data3' (No such file or directory)
bandit12@bandit:/tmp/21521386$ ls -a
. .. data3.bz2 data.txt
```

3. Tar:

```
bandit12@bandit:/tmp/21521386$ ls -a
. .. data4.gz data.txt
bandit12@bandit:/tmp/21521386$ gzip -d data4.gz
bandit12@bandit:/tmp/21521386$ file data4
data4: POSIX tar archive (GNU)
bandit12@bandit:/tmp/21521386$ mv data4 data5.tar
bandit12@bandit:/tmp/21521386$ tar data5.
data5.b data5.F data5.H data5.J data5.L data5.N data5.P data5.T data5.w data5.Z
data5.B data5.g data5.i data5.k data5.m data5.o data5.R data5.U data5.W
data5.C data5.G data5.I data5.K data5.M data5.O data5.s data5.v data5.X
data5.f data5.h data5.j data5.l data5.n data5.p data5.S data5.V data5.z
bandit12@bandit:/tmp/21521386$ tar data5.tar
tar: You may not specify more than one '-Acdtrux', '--delete' or '--test-label' option
Try 'tar --help' or 'tar --usage' for more information.
bandit12@bandit:/tmp/21521386$ tar xf data5.tar
bandit12@bandit:/tmp/21521386$ ls -a
. .. data5.bin data5.tar data.txt
```

Sau khi giải nén lần lượt ta cuối cùng tìm được file ASCII text có thể đọc được

Dùng lệnh cat đọc ta có được flag cho bandit 13

```
bandit12@bandit:/tmp/21521386$ ls -a
. .. data8.tar data9 data.txt
bandit12@bandit:/tmp/21521386$ file data9
data9: ASCII text
bandit12@bandit:/tmp/21521386$ cat data9
The password is wbWdlBxEir4CaE8LaPhauu0o6pwRmrDw
bandit12@bandit:/tmp/21521386$
```

Level 13→14

The password for the next level is stored in **/etc/bandit_pass/bandit14** and can only be read by user **bandit14**. For this level, you don't get the next password, but you get a private SSH key that can be used to log into the next level. Note: **localhost** is a hostname that refers to the machine you are working on

Ở level này thì ta phải lấy file flag (sshkey.private) để log in ở level kế tiếp.
Sao đó tìm flag ở level đó

```

bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ ls -a
. .. .bash_logout .bashrc .profile sshkey.private
bandit13@bandit:~$ ssh -i sshkey.private bandit14@localhost -p 2220
kex_exchange_identification: read: Connection reset by peer
Connection reset by 127.0.0.1 port 2220
bandit13@bandit:~$ ssh -i sshkey.private bandit14@localhost -p 2220
The authenticity of host '[localhost]: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
Could not create directory '/home/bandit13/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit13/.ssh/known_hosts).

```



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

!!! You are trying to log into this SSH server with a password on port 2220 from localhost.
!!! Connecting from localhost is blocked to conserve resources.
!!! Please log out and log in again.



Welcome to OverTheWire!
If you find any problems, please report them to the #wargames channel on discord or IRC.

The password for the next level can be retrieved by submitting the password of the current level to port 30000 on localhost.

```

bandit14@bandit:~$ ls
bandit14@bandit:~$ ls -a
. .. .bash_logout .bashrc .profile .ssh
bandit14@bandit:~$ cat etc/bandit_pass/bandit14
cat: etc/bandit_pass/bandit14: No such file or directory
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq
bandit14@bandit:~$ 

```

fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq

Level 14→15

Tiến hành dùng lệnh ‘nc’ để gửi password đã lấy được ở level trước đến cổng 30000 localhost để lấy password mới

```
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
fGrHPx402xGC7U7rXKDaxiWFT0iF0ENq
bandit14@bandit:~$ telnet localhost 30000
Trying 127.0.0.1 ...
Connected to localhost.
Escape character is '^]'.
fGrHPx402xGC7U7rXKDaxiWFT0iF0ENq
Correct!
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt
Connection closed by foreign host.
bandit14@bandit:~$
```

jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt

Level 15→16

The password for the next level can be retrieved by submitting the password of the current level to **port 30001 on localhost** using SSL encryption.

Helpful note: Getting “HEARTBEATING” and “Read R BLOCK”? Use `-ign_eof` and read the “CONNECTED COMMANDS” section in the manpage. Next to ‘R’ and ‘Q’, the ‘B’ command also works in this version of that command...

Tiến hành kết nối đến localhost với mã hoá ssl và gửi password

```

ASK your administrator to install one of them.
bandit15@bandit:~$ openssl s_client -connect localhost:30001 -sign_eof
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 CN = localhost
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN = localhost
verify error:num=10:certificate has expired
notAfter=Oct 25 02:04:01 2023 GMT
verify return:1
depth=0 CN = localhost
notAfter=Oct 25 02:04:01 2023 GMT
verify return:1
_____
Certificate chain
  0 s:CN = localhost
    i:CN = localhost
      a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA1
      v:NotBefore: Oct 25 02:03:01 2023 GMT; NotAfter: Oct 25 02:04:01 2023 GMT
_____
Server certificate
-----BEGIN CERTIFICATE-----
MIIDCzCCA0gAwIBAgIEDEsf0TANBgqhkiG9w0BAQUFADUaMRiwEAYDVQQDAls
b2NhbGhvC3QwhcNMjMxMDI1MDiWzMzAwhcNMjMxMDI1MDiWnDAwJyAUMRiwEAYD
VQQDAlsb2NhbGhvC3QwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCs
eD5l3b7r1DuonDce5udeAdjZe35y4eMjH2MCYTJFFix+K+jFEjdP4cTL1G0keg
nIU+i0f135t0Xivu5CWi9+fSGAW3U3MX44WOW+ryxspc6BTtI7I1UPjprfIQ8
Cq/y/6kgjhoZythofKvUc4ceMiUvmxTu8MqakwfaRZ0j5jlQdH+wFPD4PNodydb+
a51dm0DBj1HTnoHncp+r1uKE6AalbIXHc6cRN67L4zmqJPGaHTLjDyLAUnk91eg
Cbsv2mqTBd18Yhg508vDRdgDhTayflrWkh+78PE2A306uVMB0g+Gyypmh+6j8mKDo
n2bsnZHku3TTCrnz/VdAgMBAAGjZTBjMBQGA1UdEQNMAuCCWxvY2saG9zdDBL
Bg1ghkgBvhvCAQ0EPHY80XV0b21hdGljYWxsseBnZW5lcmF0ZWogYnkgTmNhdC4g
U2VLIGh0dBz0i8vbm1cc5vcmcvbmNhC8uMA0GCSqGSIb3DQEBBQUAA4IBAQBz
mRRbjrh6D7HhhnI4DyNyRpBgieZaw8kNYVes/uTvgeM+SwlkTp3pfnXBk7p-7of
/AGPerxFnf6gouYZ5bnhxpUeh3kaQT70D6Ie5Qwp0A16QAKf+Gs/8zhnwlEAC0D
5E+0WiRdeQ+Y/klhRD7cT81nexXTcthEGC2CLcpNpFacsIRg+34+oUqbxCQqu6iq
ftfBAcn3uAjta/Sb/Z37cDppfYnHyutat0k302qjQyjuAC3GCbLEK0pMTsWe1Md
fKa0DeU8lf1l57ekex81ud70fN2G70U9uYgbHuXrn+S6lzWZ3ub7Pgr837e0mGjy3
S7e28Y7URlho+nUJ4wqJ
-----END CERTIFICATE-----
subject=CN = localhost
issuer=CN = localhost
_____
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: RSA-PSS
Server Temp Key: X25519, 253 bits
_____
SSL handshake has read 1339 bytes and written 373 bytes

```

```

Start Time: 1698241227
Timeout   : 7200 (sec)
Verify return code: 10 (certificate has expired)
Extended master secret: no
Max Early Data: 0
_____
read R BLOCK
jN2kgmIXJ6fShzhT2avhotn4Zcka6tn
Correct!
JQtffApK4SeyHwDli9SXGR50qc1OAi11
closed
bandit15@bandit:~$
```

JQtffApK4SeyHwDli9SXGR50qc1OAi11

Level 16→17

The credentials for the next level can be retrieved by submitting the password of the current level to a port on localhost in the range 31000 to 32000. First find out which of these ports have a server listening on them. Then find out which of those speak SSL and which don't. There is only 1 server that will give the next credentials, the others will simply send back to you whatever you send to it.

Ta cần tìm ra xem cổng nào trong đoạn 31000 đến 32000 sẽ trả về thứ chúng ta cần, là credentials cho level tiếp theo.

Tiến hành scan các port để cho

Thấy có tổng cộng 5 port đang mở, tiến hành gửi từng port để xem port nào gửi về thứ ta cần

```
bandit16@bandit:~$ nmap -p 1-200 192.168.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-25 13:43 UTC
Stats: 0:00:08 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:15 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 93.25% done; ETC: 13:43 (0:00:00 remaining)
Nmap scan report for 192.168.0.1
Host is up (0.000069s latency).
All 200 scanned ports on 192.168.0.1 are closed

Nmap done: 1 IP address (1 host up) scanned in 15.81 seconds
```

```
bandit16@bandit:~$ nmap -A localhost -p 31000-32000
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-25 13:43 UTC
Stats: 0:00:21 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Stats: 0:00:26 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Stats: 0:00:31 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Stats: 0:00:32 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Verbosity Increased to 1.
Stats: 0:00:36 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Stats: 0:01:13 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 80.00% done; ETC: 13:45 (0:00:18 remaining)
Stats: 0:01:28 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 80.00% done; ETC: 13:45 (0:00:22 remaining)
Stats: 0:01:33 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 80.00% done; ETC: 13:45 (0:00:23 remaining)
Stats: 0:01:38 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 100.00% done; ETC: 13:45 (0:00:00 remaining)
Completed Service scan at 13:45, 97.87s elapsed (5 services on 1 host)
NSE: Script scanning 127.0.0.1.
Initiating NSE at 13:45
Completed NSE at 13:45, 0.03s elapsed
Initiating NSE at 13:45
Completed NSE at 13:45, 0.06s elapsed
Initiating NSE at 13:45
Completed NSE at 13:45, 0.00s elapsed
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00020s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE      VERSION
31046/tcp open  echo
31518/tcp open  ssl/echo
| ssl-cert: Subject: commonName=localhost
| Subject Alternative Name: DNS:localhost
| Issuer: commonName=localhost
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2023-10-25T02:03:02
| Not valid after:  2023-10-25T02:04:02
| MD5:  9289 b4b4 1eb6 496c 792f 0763 ec52 30b7
| SHA-1: 5e2a 0439 8a13 ea3b afd0 32b5 98ba 951f f267 c69a
31691/tcp open  echo
31790/tcp open  ssl/unknown
| fingerprint-strings:
|   FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, Help, Kerberos, LDAPSearchReq, LPDString, RTSPRequest, SIPOption
s, SSLSessionReq, TLS SessionReq, TerminalServerCookie:
|_    Wrong! Please enter the correct current password
| ssl-cert: Subject: commonName=localhost
```

Cổng 31790 là cổng ta cần

```

bandit16@bandit:~$ openssl s_client -connect localhost:31790
CONNECTED(0x0000003)
Can't use SSL_get_servername
depth=0 CN = localhost
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN = localhost
verify error:num=10:certificate has expired
notAfter=Oct 25 02:04:02 2023 GMT
verify return:1
depth=0 CN = localhost
notAfter=Oct 25 02:04:02 2023 GMT
verify return:1
-----
Certificate chain
  0 s:CN = localhost
    i:CN = localhost
      a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA1
      v:NotBefore: Oct 25 02:03:02 2023 GMT; NotAfter: Oct 25 02:04:02 2023 GMT
-----
Server certificate
-----BEGIN CERTIFICATE-----
MIIDCzCCAfOgAwIBAgIEToxavzANBgkqhkiG9w0BAQUFADAUMRIwEAYDVQQDDA
lsb2NhbGhvC3QwHhCNMjMxMDI1MDIwMzAyWhcNMjMxMDI1MDIwNDayWjAUMRIwEAYD
VQQDAalsb2NhbGhvC3QwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQ
qXTA7Km5+fqnjYTP9evn938SDGkt35e3sj1QVeFwe0jqMrkJAcL6PeeW7+7G/E/p
c1SzimkIry3kuTg573ujldZynqju9dhrapWBi48vPyAl8fluQOrUssszW3jMS1t
K8sUtgtu3nBE+hlgyPicUjBNLN7fTm5P2Xrmqk9BVz66J6u3u0v9QhBiS1Rrg
/qlx8/IbuCeJSuh9gAlusQg68fbIfzDlrCx7sk50+1LaMktAJATgU4TnYnx8zECQ
Y2JBqx/KGMA07/tckWLAKpPkeJ1Xyufi02+kvh0/4Wm1Qybs4GPZe1Tvu5CcpsNc
c4RPBStn50fBvfYrmpmAgaGjZTBjMBQGA1UdEQQNMaUCCWxvY2FsaG9zdDBL
BglghkgBhvCAQDEPhy8QXV0b21hdGljYWxseBnZW5lcmF0ZWQgYnkgTmNhC4g
U2VlIGH0dBz0i8vbmlhcC5vcmcvbmNhC8uMA0GCSqGSIb3DQEBBQUAA4IBAQ
sBhPOIDeJ9xiBzWP16jAUZQECltFy39YCibeku78CJHsCiit/xsiSY/86xJDQpK6
i2506cjaraMN/IFwpSVb329hNGFJid1MTWHnhVZTDYOUJS6Ax9EsRkqXuTOinbr
f2TSp5HISMu/shqrPovU2pKSJam8B8xeKelpQ2wfRWcJ+hLNgEIolxUV8rxwmFh
fZ0jelSC7ylqcwKN6eSayLefU0+HjBI/d1dUkj5/k/lmvwbrMPw5A2mpdetmVPl
gRASSgxD4t/5Xd6by3JrWNQLYlNsddBg4Kpke5deSrsUHPN1nfG1PErxPuXNkbIz
+d/Uw1BFemjiuPcs4ja
-----END CERTIFICATE-----
subject=CN = localhost

```

```

[LS session ticket:
0000 - 2d f7 b9 0f 1b 33 66 df-ff 5d 6e ad 42 4d e6 68
0010 - 6d 70 1a d7 37 4a 90 a6-da c2 b8 20 9b 90 63 e1
0020 - 10 a2 7e 0c f5 df 31 80-ba ed 1f 27 81 53 ec b1
0030 - 09 dd 8c 8b 91 e4 8b 74-6f aa 5e 5f c8 1d f1 2b
0040 - 2f 61 09 1c 5a 7e 7a dd-b9 97 79 2e 40 0d 07 da
0050 - e0 42 b2 6a aa 9f 44 a7-c6 de fa 4b f8 65 5e ed
0060 - a6 23 a9 62 05 c5 ff e3-90 4d 94 8e e1 35 e6 86
0070 - 85 b3 74 d8 44 20 1e 65-e3 53 a4 b1 07 0b 07 23
0080 - d0 2d cb 7b d6 13 a9 1a-fc b5 9e b2 6f e6 f4 25
0090 - fa 61 51 e9 41 66 34 d3-8f 87 14 be d8 51 22 d5
00a0 - 4c db 67 2a 5a d3 02 c3-fd 55 30 da 55 d7 43 47
00b0 - 39 4d 29 81 5c a3 d8 d2-1b bb 15 38 9e bd f4 74
00c0 - 9f 04 ed 2b d8 e6 df 2e-a1 0d cd 9c 95 64 93 c8

Start Time: 1698242684
Timeout : 7200 (sec)
Verify return code: 10 (certificate has expired)
Extended master secret: no
Max Early Data: 0

read R BLOCK
JQttfApK4SeyHwDli9SXGR50qclOAi1
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOj0n6iWfbp7c3jx34YkYWqUH57SuDyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMLOf7+BrJ0bArnxoY7Y7T2bRPQ
Ja6Lzb558YW3FzL870Ri0+rW4LCDNd2lUVLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAl+JFr56o4T6z8WWAW18BR6yGrMq7Q/KALHYW30ekePQAzL0VUYBW
JGTi65CxbCnzC/w4+mqQyvmpWtMAzJtzAzQxNbkr2MBGySxDLrjg0LWN6sK7wNX
x0YYzxt/zbIkPjfkU1jHS+9EbVnj+D1XFOjuaQIDAQABAoIBAgpxpM1aoLWfvD
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNuDE6SFth0ar69jp5RllwD1NhPx3iBl
J9nOM80J0VToum43UOS8YxF8WwhXr1yGnc1sskbwpX0UDc9uX4+UESZH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqb9A1blssgTcCKMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52y009q0kwFTEOpjtF4uNTjom+asvlpms8A
vLY9r60wYSvmZhNqBURj7lyCtXMIu1kkd4w7F77k+Djh0AXyxcUp1DGL51s0mama
+TOWwgECgYEa8JtPxP0GRj+I0kx262jM3dElkza8ky5moIwQYdsx0NxHgRRhORT
8c8hAuRBb2G82so8vUhk/fur805Ef9TncnCY2crpoqshifKLxrLgtT+qDpfZnx
SatLdt8Gf085yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyc9P2jGRNtMSkcgYEayphd
HCctNi/FwjulhttFx/rHYKhLidZDFYeIE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0KnywlbpJVyusaavPzpaJMjdJ6tcFhVabAjm7enCivGCSx+x3l5SiWg0A
R57hJglezIiVjv3aGwHwvlZvtsK6zV6oXFau0EcgyAbjo46T4hyP5tJi93V5HDi
TtieK7xRVxUl+iU7rWkGAXFpMLFteQEsRz7PJ/LemmEY5eTDAFLMy9FL2m9oQWCg
R8VdwSk8r9FGls+9aKcV5PI/WEKlwgXinB30hYimtiG2Cg5JCqIZFhxD6MjEG0iu
L8ktHMPvodBwNsSBULpG0QKBgBapltfc1HonW1MGOU3KpwYwt006Cd7kmJ0mL8Ni
bh9elyZ9FsGxsgrTRBXRsqtXuz7wtsQAgLhxndlq/ZJQ7YfzOKU4ZxEnabvXnvWkU
Y0djHsOokvDQNWWu6ucyLRWFu1SeXw9a/9p7ftpxm@TsgyvmlfLF2MIAEwyzRqaM
77pBAoGMmjmiJdjP+Ez8duyn3ieo36yrttF5NsSjLAbxFpdIcgvtxCwW+9Cq0b
dxviW8+TFEBL104f7Vm6EpTscdDxu+bCXWkfjiuRb7Dy9Gott9JPsX8MBTakzh3
vBgsyi/sn3RqrBcGU40f0ooZyfAMT8s1m/uYv5206IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----
```

closed
bandit16@bandit:~\$

Sau đó copy key được trả về và làm tương tự như level 14 để tìm flag

```

File Actions Edit View Help
└──(danghuy㉿kali)-[~]
    $ vim key

└──(danghuy㉿kali)-[~]
    $ chmod 400 key

└──(danghuy㉿kali)-[~]
    $ ssh -i key bandit17@bandit.labs.overthewire.org -p 2220
ssh: Could not resolve hostname -: Name or service not known

└──(danghuy㉿kali)-[~]
    $ ssh -i key bandit17@bandit.labs.overthewire.org -p 2220
    kex_exchange_identification: Connection closed by remote host
Connection closed by 51.20.13.48 port 2220

└──(danghuy㉿kali)-[~]
    $ ssh -i key bandit17@bandit.labs.overthewire.org -p 2220
    [REDACTED]

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

    [REDACTED]
    www. ver he ire.org

Welcome to OverTheWire!
If you find any problems, please report them to the #wargames channel on
discord or IRC.

--[ Playing the games ]--

This machine might hold several wargames.
If you are playing "somegame", then:

* USERNAMES are somegame0, somegame1, ...
* Most LEVELS are stored in /somegame/.
```

Level 17→18

There are 2 files in the homedirectory: **passwords.old** and **passwords.new**. The password for the next level is in **passwords.new** and is the only line that has been changed between **passwords.old** and **passwords.new**

NOTE: if you have solved this level and see 'Byebyel' when trying to log into bandit18, this is related to the next level, bandit19

Sử dụng ‘diff’ để kiểm tra hai tệp

```
bandit17@bandit:~$ ls
passwords.new  passwords.old
bandit17@bandit:~$ diff passwords.old passwords.new
42c42
< p6ggwdNHncnmCNxuAt0KtKVq185ZU7AW
> hga5tuuCLF6fFzUpnagiMN8ssu9LFrdf
bandit17@bandit:~$ ^C
bandit17@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.

└─(danghuy㉿kali)-[~]
└─$
```

hga5tuuCLF6fFzUpnagiMN8ssu9LFrdf

Level 18→19

The password for the next level is stored in a file **readme** in the homedirectory. Unfortunately, someone has modified **.bashrc** to log you out when you log in with SSH.

Đầu tiên ta log in theo cách thông thường thì nó bị đóng ngay lập tức. Lí do là SSH thông thường sử dụng pseudo-terminal. Để không bị văng ra ngay lúc kết nối, thử tìm cách không dùng pseudo-terminal.

```
(danghuy㉿kali)-[~]
$ ssh bandit18@bandit.labs.overthewire.org -p 2220
[=] [=] [=] [=] [=] [=] [=]
[=] [D][C][I][T][C][I][E]
[=] [/]\_,\_,\_,\_,\_,\_,\_
[=]

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

bandit18@bandit.labs.overthewire.org's password:
[=] [=] [=] [=] [=] [=] [=]
[=] [D][C][I][T][C][I][E]
[=] [/]\_,\_,\_,\_,\_,\_,\_
[=]

www. ver he ire.org
```

Trang SSHOpen Linux Manual có đề cập dùng option -T có thể loại bỏ đc pseudo-terminal

```
* 1881:2 ~ http://www.1881:2.org/7/
--[ 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!

Byebye !
Connection to bandit.labs.overthewire.org closed.

(danghuy㉿kali)-[~]
$
```

```
(danghuy㉿kali)-[~]
$ ssh -T bandit18@bandit.labs.overthewire.org -p 2220
kex_exchange_identification: Connection closed by remote host
Connection closed by 51.20.13.48 port 2220

(danghuy㉿kali)-[~]
$ ssh -T bandit18@bandit.labs.overthewire.org -p 2220
[=|_ _ \ /_ _ | | _ \ /_ _ | | _ \ | _ |
 | | | | | | | | | | | | | | | | | |
 | . _ / \ _ , | _ | | | | | | | | | |
[=|_ _ \ /_ _ | | _ \ /_ _ | | _ \ | _ |

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

bandit18@bandit.labs.overthewire.org's password:
hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg
-bash: line 1: hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg: command not found
ls
readme
cat readme
awhqfNnAbc1naukrpqDYcF95h7HoMTrC
exit

(danghuy㉿kali)-[~]
$
```

awhqfNnAbc1naukrpqDYcF95h7HoMTrC

Level 19 → 20:

Ở level này, em được cung cấp sẵn một tệp setuid binary để thực thi:

```
bandit19@bandit:~$ ls  
bandit20-do
```

Em đã sử dụng tệp này để thực thi việc mở file password cho level 20, với câu lệnh “./bandit20-do cat /etc/bandit_pass/bandit20”, và kết quả nhận được như sau:

```
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20  
VxCazJaVykJ6W36BkBU0mJTCM8rR95XT
```

Kết quả đó là password cho level tiếp theo.

Level 20 → 21:

Tệp setuid binary được cung cấp sẵn để thực thi:

```
bandit20@bandit:~$ ls  
suconnect
```

Bởi vì tệp trên sẽ kết nối tới localhost với port được chỉ định, sau đây sẽ đọc một dòng text từ kết nối đó, cuối cùng là so sánh với password ở level trước đó. Vì thế để thực hiện được việc này thì em sẽ tạo thêm 1 terminal mới và kết nối đến level này, sau đó sẽ sử dụng lệnh “nc -lvp 2003” để tạo lắng nghe ở port 2003:

```
bandit20@bandit:~$ nc -lvp 2003  
Listening on 0.0.0.0 2003
```

Ở terminal cũ thì em sẽ sử dụng tệp được cung cấp sẵn và chạy để kết nối đến port 2003 vừa được mở để lắng nghe này:

```
bandit20@bandit:~$ ./suconnect 2003
```

Sau khi chạy xong thì ở terminal mới sẽ thông báo sau:

```
bandit20@bandit:~$ nc -lvp 2003  
Listening on 0.0.0.0 2003  
Connection received on localhost 51036
```

Bởi vì đã nhận được kết nối, thê nên em sẽ đưa password ở level trước vào để suconnect đọc được và so sánh, kết quả nhận được ở terminal chạy suconnect:

```
bandit20@bandit:~$ ./suconnect 2003  
Read: VxCazJaVykI6W36BkBU0mJTCM8rR95XT  
Password matches, sending next password  
bandit20@bandit:~$
```

Bởi vì đã khớp password nên suconnect đã gửi password của level tiếp theo đến port 2003, và kết quả password nhận được ở bên terminal mới như sau:

```
bandit20@bandit:~$ nc -lvp 2003
Listening on 0.0.0.0 2003
Connection received on localhost 51036
VxCazJaVykJ6W36BkBU0mJTCM8rR95XT
NvEJF7oVjkddltPSrdKEFollh9V1IBcq
bandit20@bandit:~$
```

Level 21 → 22:

Như yêu cầu của đề bài, em sẽ truy cập vào đường dẫn /etc/cron.d/ để xem câu lệnh đang được thực thi là gì:

```
bandit21@bandit:~$ ls /etc/cron.d/
cronjob_bandit15_root  cronjob_bandit22  cronjob_bandit24      e2scrub_all  sysstat
cronjob_bandit17_root  cronjob_bandit23  cronjob_bandit25_root  otw-tmp-dir
bandit21@bandit:~$
```

Với kết quả trả về trên, và hiện tại đang ở level 21 -> 22 nên em nghĩ password cần tìm khả năng cao là sẽ ở trong cronjob_bandit22, mở lên xem cronjob_bandit22:

```
bandit21@bandit:~$ cat /etc/cron.d/cronjob_bandit22
@reboot bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
* * * * * bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
bandit21@bandit:~$
```

Thông qua kết quả trên có thể thấy rằng script đang được thực thi chính là /usr/bin/cronjob_bandit22.sh, tiếp đến là theo đường dẫn đó để mở xem có gì:

```
bandit21@bandit:~$ cat /usr/bin/cronjob_bandit22.sh
#!/bin/bash
chmod 644 /tmp/t706lds9S0RqQh9aMcZ6ShpAoZKF7fgv
cat /etc-bandit_pass/bandit22 > /tmp/t706lds9S0RqQh9aMcZ6ShpAoZKF7fgv
bandit21@bandit:~$
```

Qua đó có thể thấy password của level kế tiếp được đưa vào trong file /tmp/t706lds9S0RqQh9aMcZ6ShpAoZKF7fgv, nên phải mở file này để lấy password:

```
bandit21@bandit:~$ cat /tmp/t706lds9S0RqQh9aMcZ6ShpAoZKF7fgv  
WdDozAdTM2z9DiFEQ2mGlwngMfj4EZff  
bandit21@bandit:~$
```

Level 22 → 23:

Qua đọc đề, có thể thấy chắc chắn cũng giống như ở level trước thì script đang được thực thi chính là /usr/bin/cronjob_bandit23.sh, therefore em sẽ truy cập vào script này:

```
bandit22@bandit:~$ 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:~$
```

Kết quả trên cho thấy, tóm lại nôm na sẽ là tùy vào myname là gì thì mytarget sẽ trả về đó, sau đó file password theo myname sẽ được đưa vào file mytarget tương ứng với myname trên. Vì là đang ở level 22 -> 23 nên chắc chắn myname ở đây sẽ là bandit23.

Tiếp đến em sẽ thay myname thành bandit23 vào câu lệnh “echo I am user \$myname | md5sum | cut -d ' ' -f 1” để tìm ra mytarget:

```
bandit22@bandit:~$ echo I am user bandit23 | md5sum | cut -d ' ' -f 1  
8ca319486bfbb3663ea0fbe81326349  
bandit22@bandit:~$
```

Dùng kết quả trên để tìm ra password cho level tiếp theo:

```
bandit22@bandit:~$ cat /tmp/8ca319486bfbb3663ea0fbe81326349  
QYw0Y2aiA672PsMmh9puTQuhoz8SyR2G  
bandit22@bandit:~$
```

Level 23→24:

Vẫn như những bài trên, tiếp tục xem script /usr/bin/cronjob_bandit24.sh:

```
bandit23@bandit:~$ 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
```

Qua đoạn code nhận được có thể thấy rằng nó lần lượt lặp qua từng tệp rồi thực thi và xóa, các tệp nằm trong thư mục /var/spool/\$myname/foo.

Để có thể lấy được password cho level tiếp theo thì em sẽ vào trong thư mục /var/spool/bandit24/foo để đưa password vào file txt của mình, với dòng lệnh shell-script sau:

```
bandit23@bandit:/var/spool/bandit24/foo$ echo "cat /etc/bandit_pass/bandit24 > /tmp/pass.txt" > nghia.sh
```

Sau khi đưa dòng lệnh “cat /etc/bandit_pass/bandit24 > /tmp/pass.txt” vào file script thì sẽ cấp quyền cho nó như sau:

```
bandit23@bandit:/var/spool/bandit24/foo$ chmod 777 nghia.sh
bandit23@bandit:/var/spool/bandit24/foo$
```

Thực thi lệnh ls để kiểm tra file còn tồn tại hay không:

```
bandit23@bandit:/var/spool/bandit24/foo$ ls nghia.sh
ls: cannot access 'nghia.sh': No such file or directory
```

Thấy file không tồn tại, vậy thì file đã tự động được thực thi và xóa đi, lúc này em sẽ vào file txt để lấy password:

```
bandit23@bandit:/var/spool/bandit24/foo$ cat /tmp/pass.txt
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar
bandit23@bandit:/var/spool/bandit24/foo$
```

Level 24→25:

Ở level này thì yêu cầu cung cấp cho nó password của level trước và thêm vào đó là mã pin 4 số, và cách duy nhất để có mã pin này là brute force, để làm được điều này thì sẽ cần phải tạo một thư mục rỗng mới:

```
bandit24@bandit:~$ cd /tmp  
bandit24@bandit:/tmp$ mkdir bandit24_tmp  
bandit24@bandit:/tmp$ cd bandit24_tmp  
bandit24@bandit:/tmp/bandit24_tmp$
```

Ở đây, em sẽ tạo ra một file script để brute force mã pin:

```
#!/bin/bash  
  
for i in {0000 .. 9999}  
do  
    echo "VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar $i"  
done
```

Tiếp đến là cấp quyền cho nó:

```
bandit24@bandit:/tmp/bandit24_tmp$ nano brute.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/bandit24_tmp$ chmod u+x brute.sh
```

Cuối cùng là sẽ thực hiện kết nối mạng tới localhost ở port 30002, cùng với đó là lọc đi các kết quả trả về sai, chỉ giữ đúng 1 kết quả trả về đúng duy nhất:

```
bandit24@bandit:/tmp/bandit24_tmp$ ./brute.sh | nc localhost 30002 | grep -v "Wrong"
```

Đợi một lúc để cho quá trình brute force được thành công, và kết quả nhận được như sau:

```
I am the pincode checker for user bandit25. Please enter the password for user bandit24 and the  
secret pincode on a single line, separated by a space.  
Correct!  
The password of user bandit25 is p7TaowMYrmu230l8hiZh9UvD009hpx8d  
  
Exiting.  
bandit24@bandit:/tmp/bandit24_tmp$
```

Level 25 → 26

Kiểm tra lệnh ls ta thấy có file bandit26.sshkey

```
bandit25@bandit:~$ ls -l
total 4
-r----- 1 bandit25 bandit25 1679 Oct  5 06:19 bandit26.sshkey
bandit25@bandit:~$ █
```

Đưa passwd từ file passwd ta thấy có file tên showtext

```
-r----- 1 bandit25 bandit25 1679 Oct  5 06:19 bandit26.sshkey
bandit25@bandit:~$ cat /etc/passwd | grep bandit26.sshkey
bandit25@bandit:~$ cat /etc/passwd | grep bandit26
bandit26:x:11026:11026:bandit level 26:/home/bandit26:/usr/bin/showtext
bandit25@bandit:~$ █
```

Kiểm tra showtext

```
bandit25.x.11026.11026.bandit level 26:/home/bandit25:/usr/bin/showtext
bandit25@bandit:~$ cat /usr/bin/showtext
#!/bin/sh

export TERM=linux

exec more ~/text.txt
exit 0
```

Có thẻ hiệu đơn giản như thẻ này :

Nếu bạn chạy showtext trong terminal, nó sẽ hiển thị nội dung của tệp văn bản text.txt bằng trình more, và khi bạn thoát khỏi trình more, shell script sẽ kết thúc với mã thoát là 0.

Như vậy nếu như script không hiện ra được hết thì shell sẽ không kết thúc, ta sẽ khai thác chỗ này của bài.

Sử dụng lệnh ssh

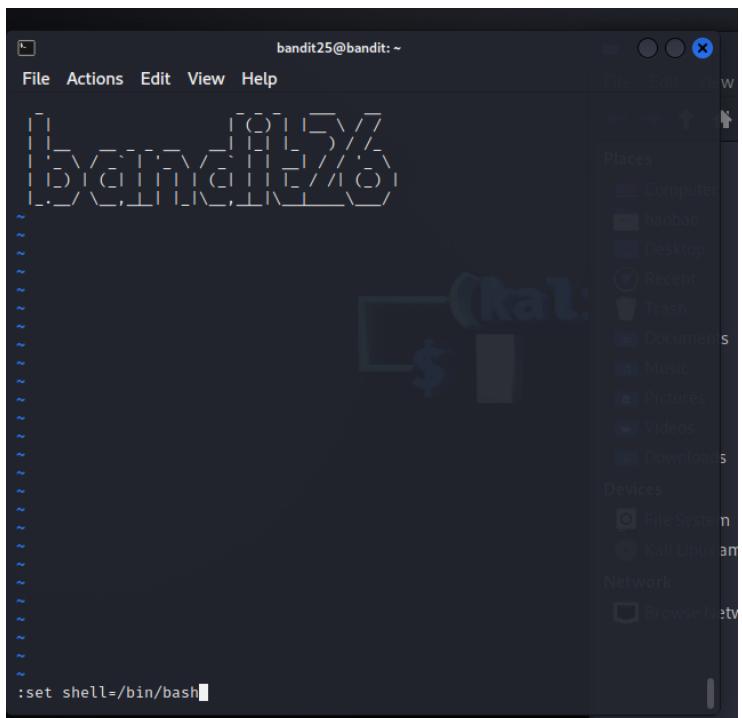
```
... skipping 1 line
| |_) | (_| | + + + |_) + + + |_ / /| |_
| |
|_| ._| / \_,_| + |_|\_ \_,_| + |\_ \_ \_ \_
/
Connection to localhost closed.
bandit25@bandit:~$ ssh bandit26@localhost -i bandit26.sshkey -p 2220
```

```
bandit25@bandit:~
```

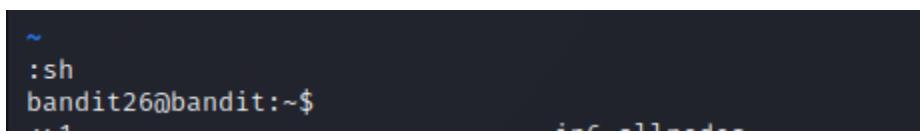
File Actions Edit View Help

```
-- More -- (81%)
```

⇒ Vì không hiện được toàn bộ text nên bây giờ chúng ta đang kẹt ở vị trí này Nhấn v để trình soạn thảo vi của vim, và nhập lệnh vào

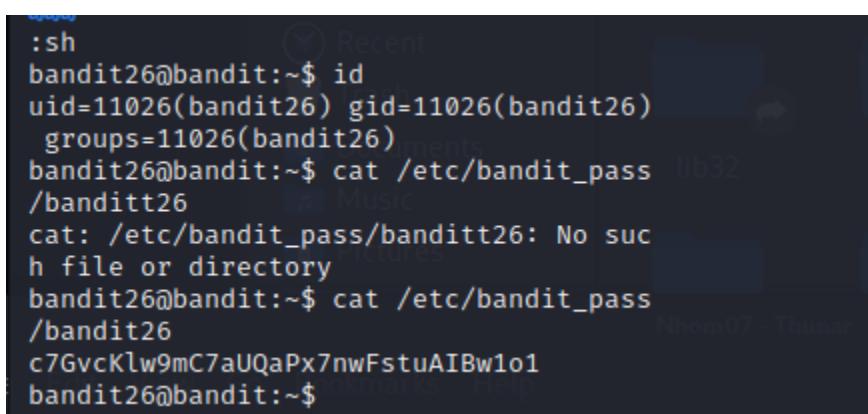


```
:set shell=/bin/bash
```



```
:sh  
bandit26@bandit:~$
```

Vậy là ta đã vào được bandit26



```
:sh  
bandit26@bandit:~$ id  
uid=11026(bandit26) gid=11026(bandit26)  
groups=11026(bandit26)  
bandit26@bandit:~$ cat /etc/bandit_pass  
/banditt26  
cat: /etc/bandit_pass/banditt26: No suc  
h file or directory  
bandit26@bandit:~$ cat /etc/bandit_pass  
/bandit26  
c7GvcKlw9mC7aUQaPx7nwFstuAIBw1o1  
bandit26@bandit:~$
```

⇒ Vậy là có được passwd từ bài 25

Level 26→27

Dùng lệnh ls ta thấy

```
bandit26@bandit:~$ ls  
bandit27-do  text.txt  
bandit26@bandit:~$ ./bandit27-do  
Run a command as another user.  
Example: ./bandit27-do id
```

Sử dụng bandit27-do để lấy pass từ file mật khẩu

```
bandit27-do: cannot open `bandit27-do' (No such file or directory)  
bandit26@bandit:~$ file bandit27-do  
bandit27-do: setuid ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV),  
dynamically linked, interpreter /lib/ld-linux.so.2, BuildID[sha1]=037b97b430734c  
79085a8720c90070e346ca378e, for GNU/Linux 3.2.0, not stripped  
bandit26@bandit:~$ ./bandit27-do cat /etc/bandit_pass/bandit27  
YnQpBuifNMas1hcUFk70ZmqkhUU2EuaS  
bandit26@bandit:~$ Connection to localhost closed.
```

Vậy là đã có pass từ bài 26

password26-27: YnQpBuifNMas1hcUFk70ZmqkhUU2EuaS

Level 27→28

Ta clone kho lưu trữ về với lệnh sau

```
and the repository exists.  
bandit27@bandit:/tmp/dean2$ git clone ssh://bandit27-git@localhost:2220/home/bandit27-git/repo  
Cloning into 'repo'...  
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.  
ED25519 key fingerprint is SHA256:C2iHUBV7ihmV1wUXR04RrEcLFXC5CXlhmAAM/urerLY.  
This key is not known by any other names  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Could not create directory '/home/bandit27/.ssh' (Permission denied).  
Failed to add the host to the list of known hosts (/home/bandit27/.ssh/known_hosts).  
  
This is an OverTheWire game server.  
More information on http://www.overthewire.org/wargames  
  
bandit27-git@localhost's password:  
remote: Enumerating objects: 3, done.  
remote: Counting objects: 100% (3/3), done.  
remote: Compressing objects: 100% (2/2), done.  
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 0  
Receiving objects: 100% (3/3), done.  
bandit27@bandit:/tmp/dean2$ ls  
pass.txt  repo  
bandit27@bandit:/tmp/dean2$ cd repo  
bandit27@bandit:/tmp/dean2/repo$ ls  
README  
bandit27@bandit:/tmp/dean2/repo$ cat README  
The password to the next level is: AVanL161y9rsbcJIsFHuw35rjaOM19nR  
bandit27@bandit:/tmp/dean2/repo$
```

Mật khẩu để download là mật khẩu sau khi pass level 26

Sau đó tìm ra mật khẩu được để trong file README

AVanL161y9rsbcJIsFHuw35rjaOM19nR

Level 28→29

Ta tiếp tục clone kho lưu trữ về với các lệnh sau

```
bandit28@bandit:~$ git clone ssh://bandit28-git@localhost:2220/home/bandit28-git/repo
fatal: could not create work tree dir 'repo': Permission denied
bandit28@bandit:~$ mkdir /tmp/danghuy
bandit28@bandit:~$ cd /tmp/danghuy
bandit28@bandit:/tmp/danghuy$ echo "AVanL161y9rsbcJIsFHuw35rja0M19nR" > pass.txt
bandit28@bandit:/tmp/danghuy$ git clone ssh://bandit28-git@localhost:2220/home/bandit28-git/repo
Cloning into 'repo' ...
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnViwUXRb4RrEcIxFc5CXlhmAAM/urerLY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit28/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit28/.ssh/known_hosts).

This is an OverTheWire game server.  

More information on http://www.overthewire.org/wargames  

bandit28-git@localhost's password:  

remote: Enumerating objects: 9, done.  

remote: Counting objects: 100% (9/9), done.  

remote: Compressing objects: 100% (6/6), done.  

remote: Total 9 (delta 2), reused 0 (delta 0), pack-reused 0  

Receiving objects: 100% (9/9), done.  

Resolving deltas: 100% (2/2), done.
```

Đọc file README.md thấy nội dung sau

```
bandit28@bandit:/tmp/danghuy$ ls
pass.txt  repo
bandit28@bandit:/tmp/danghuy$ cd repo
bandit28@bandit:/tmp/danghuy/repo$ ls
README.md
bandit28@bandit:/tmp/danghuy/repo$ cat README.md
# Bandit Notes
Some notes for level29 of bandit.

## credentials

- username: bandit29
- password: xxxxxxxxxxxx
```

Ta kiểm tra git log để xem lịch sử của các commit trong dự án Git và thấy có kiểm tra lịch sử một commit có thông điệp commit là "add missing data"

```

bandit28@bandit:/tmp/danghuy/repo$ git log
commit 14f754b3da6531a2b89df6ccae6446e8969a41f3 (HEAD → master, origin/master, origin/HEAD)
Author: Morla Porla <morla@overthewire.org>
Date:   Thu Oct 5 06:19:41 2023 +0000

    fix info leak

commit f08b9cc63fa1a4602fb065257633c2dae6e5651b
Author: Morla Porla <morla@overthewire.org>
Date:   Thu Oct 5 06:19:41 2023 +0000

    add missing data

commit a645bcc508c63f081234911d2f631f87cf469258
Author: Ben Dover <noone@overthewire.org>
Date:   Thu Oct 5 06:19:41 2023 +0000

    initial commit of README.md
bandit28@bandit:/tmp/danghuy/repo$ git checkout f08b9cc63fa1a4602fb065257633c2dae6e5651b
Note: switching to 'f08b9cc63fa1a4602fb065257633c2dae6e5651b'.

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 f08b9cc add missing data

```

Sau đó ta vào lại file README.md và đọc lại mật khẩu

```

HEAD is now at f08b9cc add missing data
bandit28@bandit:/tmp/danghuy/repo$ ls
README.md
bandit28@bandit:/tmp/danghuy/repo$ cat README.md
# Bandit Notes
Some notes for level29 of bandit.

## credentials

- username: bandit29
- password: tQKvmcwNYcFS6vmPHIUSI3ShmsrQZK8S

```

tQKvmcwNYcFS6vmPHIUSI3ShmsrQZK8S

Level 29→30

Với các bước clone git về tương tự như sau

```

and the repository exists.
bandit29@bandit:/tmp/bandit29_certa$ git clone ssh://bandit29-git@localhost:2220/home/bandit29-git/repo
Cloning into 'repo' ...
The authenticity of host '[localhost]: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
Could not create directory '/home/bandit29/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit29/.ssh/known_hosts).

Kali Linux...          [  ] / - - - \ / [ ( ) ] 
[  ] | ( [ ] | [ ] | ( [ ] | [ ] | [ ] )
[ . ] / \ [ ] , [ ] [ ] \ [ ] , [ ] [ ] 

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

bandit29-git@localhost's password:
remote: Enumerating objects: 16, done.
remote: Counting objects: 100% (16/16), done.
remote: Compressing objects: 100% (11/11), done.
remote: Total 16 (delta 2), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (16/16), done.
Resolving deltas: 100% (2/2), done.

```

Ta tiếp tục check mật khẩu trong file README.md

```

Receiving deltas: 100% (2/2) done.
bandit29@bandit:/tmp/bandit29_certa$ ls
repo
bandit29@bandit:/tmp/bandit29_certa$ cd repo
bandit29@bandit:/tmp/bandit29_certa/repo$ ls
README.md
bandit29@bandit:/tmp/bandit29_certa/repo$ cat README.md
# Bandit Notes
Some notes for bandit30 of bandit.

## credentials

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

```

Ta tiếp tục kiểm tra git log

```

bandit29@bandit:/tmp/bandit29_certa/repo$ git log
commit 4364630b3b27c92aff7b36de7bb6ed2d30b60f88 (HEAD → master, origin/master, origin/HEAD)
Author: Ben Dover <noone@overthewire.org>
Date:   Thu Oct 5 06:19:43 2023 +0000

    fix username

commit fca34ddb7d1ff1f78df36538252aea650b0b040d
Author: Ben Dover <noone@overthewire.org>
Date:   Thu Oct 5 06:19:43 2023 +0000

    initial commit of README.md

```

Ta check out chuyên qua commit với thông điệp “initial commit of README.md”

```

bandit29@bandit:/tmp/bandit29_certa/repo$ git checkout fca34ddb7d1ff1f78df36538252aea650b0b040d
Note: switching to 'fca34ddb7d1ff1f78df36538252aea650b0b040d'.

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 fca34dd initial commit of README.md
bandit29@bandit:/tmp/bandit29_certa/repo$ ls
README.md
bandit29@bandit:/tmp/bandit29_certa/repo$ cat README.md
# Bandit Notes
Some notes for bandit30 of bandit.

## credentials

- username: bandit29
- password: <no passwords in production!>

```

Ta sử dụng git branch -a để liệt kê tất cả các nhánh (branch) có sẵn trong dự án Git, bao gồm cả các nhánh cục bộ (local) và các nhánh từ xa (remote)

Và sau đó đọc file README.md

```

bandit29@bandit:/tmp/bandit29_certa/repo$ git branch -a
* (HEAD detached at fca34dd)
  master
  remotes/origin/HEAD → origin/master
  remotes/origin/dev
  remotes/origin/master
  remotes/origin/splights-dev
bandit29@bandit:/tmp/bandit29_certa/repo$ git checkout remotes/origin/dev
Previous HEAD position was fca34dd initial commit of README.md
HEAD is now at 1d160de add data needed for development
bandit29@bandit:/tmp/bandit29_certa/repo$ ls
code README.md
bandit29@bandit:/tmp/bandit29_certa/repo$ cat README.md
# Bandit Notes
Some notes for bandit30 of bandit.

## credentials

- username: bandit30
- password: xbhV3HpNGlTIdnjUrdAlPzc2L6y9EOnS

```

xbhV3HpNGlTIdnjUrdAlPzc2L6y9EOnS

Level 30→31

Với các bước clone git về tương tự như sau

Ta tiếp tục kiểm tra git log và các nhánh của Git

```
bandit30@bandit:/tmp/bandit30_ce/repo$ git log
commit d39631d73f786269b895ae9a7b14760cbf40a99f (HEAD -> master, origin/master, origin/HEAD)
Author: Ben Dover <noone@overthewire.org>
Date:   Thu Oct 5 06:19:45 2023 +0000

    initial commit of README.md
bandit30@bandit:/tmp/bandit30_ce/repo$ git branch -a
* master
  remotes/origin/HEAD -> origin/master
  remotes/origin/master
```

Ta sử dụng git tag để quản lý và xem danh sách các tags trong dự án được sử dụng để đánh dấu các phiên bản hoặc các điểm quan trọng khác trong lịch sử của mã nguồn. Tags thường dùng để dễ dàng xác định và truy cập các phiên bản cụ thể trong mã nguồn mà không cần phải nhớ commit hash.

Sau đó ta tiến hành lấy mật khẩu

OoffzGDIzhAlerFJ2cAiz1D41JW1Mhmt

Level 31→32

Với các bước clone git về tương tự như sau

```
bandit31@bandit:~$ mkdir /tmp/bandit31_cer  
bandit31@bandit:~$ cd /tmp/bandit31_cer
```

```
bandit31@bandit:~/tmp$ git clone ssh://bandit31-git@localhost:2220/home/bandit31-git/repo
Cloning into 'repo'...
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7jhNV1wUXRb4RrEcLfxC5CXlhmAAM/urerLY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit31/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit31/.ssh/known_hosts).

[ _ ] _ \ / _ - _ - _ \ / _ ( ) _ [
| | | ) | ( | | | | | ( | | | |
|_ . _ / \ _ , _ | | | \ _ , _ | \ _ |

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

bandit31-git@localhost's password:
remote: Enumerating objects: 4, done.
remote: Counting objects: 100% (4/4), done.
remote: Compressing objects: 100% (3/3), done.
remote: Writing objects: 100% (4/4), done.
remote: Total 4 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (4/4), done.
```

Ta đọc file để kiểm password

```
receiving objects, 100% (7/7), done.
bandit31@bandit:/tmp/bandit31_cer$ ls
repo
bandit31@bandit:/tmp/bandit31_cer$ cat repo
cat: repo: Is a directory
bandit31@bandit:/tmp/bandit31_cer$ cd repo
bandit31@bandit:/tmp/bandit31_cer/repo$ ls
README.md
bandit31@bandit:/tmp/bandit31_cer/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
```

Theo yêu cầu ta phải push file lên repository nên ta thực hiện các bước sau

```
bandit31@bandit:/tmp/bandit31_cer/repo$ nano key.txt
Unable to create directory '/home/bandit31/.local/share/nano/': No such file or director
It is required for saving/loading search history or cursor positions.

bandit31@bandit:/tmp/bandit31_cer/repo$ ls -a
. .. .git .gitignore key.txt README.md
bandit31@bandit:/tmp/bandit31_cer/repo$ cat .gitignore
*.txt
bandit31@bandit:/tmp/bandit31_cer/repo$ git add -f key.txt
bandit31@bandit:/tmp/bandit31_cer/repo$ git commit -m"key.txt"
[master 75d0c56] key.txt
 1 file changed, 1 insertion(+)
 create mode 100644 key.txt
bandit31@bandit:/tmp/bandit31_cer/repo$ git push -u origin master
The authenticity of host '[localhost]:2220 ([127.0.0.1]:220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihBV7ihnV1wUXRb4RrEcLfxC5CxLhmAAM/urerLY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit31/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit31/.ssh/known_hosts).

[ _ \ _ / _ - _ \ _ / _ [ _ ( ) _ ] _ ]
[ _ ] [ _ ] [ _ ] [ _ ] [ _ ] [ _ ]
[ _ - / _ \ _ , _ \ _ \ _ , _ \ _ \ _ ]
```

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

```
bandit31-git@localhost's password:
Enumerating objects: 4, done.
Counting objects: 100% (4/4), done.
Delta compression using up to 2 threads
Compressing objects: 100% (2/2), done.
Writing objects: 100% (3/3), 322 bytes | 322.00 KiB/s, done.
Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
remote: ### Attempting to validate files ... ####
remote:
remote: .00.00.00.00.00.00.00.00.00.00.00.00.00.00.
remote:
remote: Well done! Here is the password for the next level:
remote: rmCBvG56y58BXzv98yZGd07ATVL5dW8y
remote:
remote: .00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.
remote:
To ssh://localhost:2220/home/bandit31-git/repo
 ! [remote rejected] master → master (pre-receive hook declined)
error: failed to push some refs to 'ssh://localhost:2220/home/bandit31-git/repo'
bandit31@bandit:/tmp/bandit31_cer/repo$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

rmCBvG56y58BXzv98yZGdO7ATVL5dW8y

Level 32→33

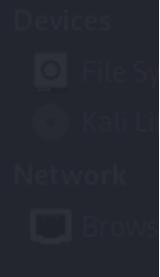
Sau khi vào ta bandit lv32 ta được

```
Enjoy your stay!  
WELCOME TO THE UPPERCASE SHELL  
>> [REDACTED]  
  
>> exit  
sh: 1: EXIT: Permission denied  
>> sudo pwd  
sh: 1: SUDO: Permission denied  
>> shele  
sh: 1: SHELE: Permission denied  
>> $0  
$ [REDACTED]
```

Có vẻ như chúng ta đang ở uppercase Shell

Ta có thể thấy với bất cứ lệnh nào nhập vào thì chương trình mặc định variable của ta là 1 và từ chối quyền truy cập, có vẻ như cần phải thoát ra khỏi upper shell, và đến bourne shell, do đó nhập vào \$0

```
sh: 1: SHELE: Permission denied
>> $0
$ pwd
/home/bandit32
$ export Bao=/bin/bash
$ echo $Bao
/bin/bash
$ $Bao
bandit33@bandit:~$
```



Ở đây ta tạo 1 biến môi trường là Bao để sau gọi đến bash

Lấy mật khẩu để đến level33

```
/bin/bash
$ $Bao
bandit33@bandit:~$ cat /etc/bandit_pass/bandit32
cat: /etc/bandit_pass/bandit32: Permission denied
bandit33@bandit:~$ cat /etc/bandit_pass/bandit33
odHo63fHiFqcWWJG9rLiLDtPm45KzUKy
```

odHo63fHiFqcWWJG9rLiLDtPm45KzUKy