

BÁO CÁO BÀI TẬP

Môn học: An toàn mạng máy tính

Kỳ báo cáo: Buổi 01 (Session 01)

Tên chủ đề: Dò quét và bắt gói tin trong mạng

GV: Nghi Hoàng Khoa

Ngày báo cáo: 19/10/2022

Nhóm: 07 (nếu không có xoá phần này)

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT101.N11.ANTN

STT	Họ và tên	MSSV	Email
1	Võ Anh Kiệt	20520605	20520605@gm.uit.edu.vn
2	Nguyễn Bảo Phương	20520704	20520704@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá
1	35 câu hỏi Bandit	100%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

1. 35 câu hỏi Bandit

BANDIT

Level 0:

Bật VPN mới chạy được.

Kết nối ssh với username, remote và port được chỉ định:

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

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

Level 0:

Thử dùng lệnh ls để liệt kê các file trong thư mục:

```
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL
```

Ta được chuỗi sau:

NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL

Level 1:

Dùng chuỗi lấy được từ file readme để làm password vào level 1.

Thử dùng lệnh “ls” thì được file “-“

```
bandit1@bandit:~$ ls
-
```

Tùy ý ta search “dashed filename” và có 2 cách để mở file có dấu “-“ là dùng “cat < -“ hoặc “cat ./-“

Ký tự “-“ chuyển hướng tới stdin/stdout nên muốn mở những file có kí tự “-“ ở đầu thì phải chỉ định đầu đủ vị chỉ của tệp như là ./-

```
bandit1@bandit:~$ cat ./
rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi
```

Ta được flag vào level 1 là:

rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi

Level 2:

Để đọc file có dấu cách trong tên, ta có thể để tên file trong ngoặc đơn hoặc thêm “\” vào trước mỗi dấu cách trong tên file.

```
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat spaces\ in\ this\ filename
aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG
```

Ta được flag cho level 2:

aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG

Level 3:

Sau khi vào thư mục “inhere” nhưng xài lệnh “ls” không xuất hiện file nào. Ta thử dùng “ls -a” để liệt kê ra cả những file ẩn và được file .hidden.

```
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$
```

Flag để vào level 3:

2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe

Level 4:

Sau khi vào level 4 thì vào thư mục inhere

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

Cách 1: cat từng file để xem nội dung

```
bandit4@bandit:~/inhere$ cat ./-file00
♦♦Q♦6
    ♦♦V♦♦♦gH♦b♦♦♦v♦♦Q♦e♦bandit4@bandit:~/inhere$ cat ./-file01
    ♦♦q$`8♦♦&[S♦]`S♦♦♦IE♦♦♦♦♦2;bandit4@bandit:~/inhere$ cat ./-file02
    ♦♦G)=I♦♦O♦
        $`S♦&♦♦♦♦♦/v♦♦♦%♦bandit4@bandit:~/inhere$ cat ./-file03
    ♦♦♦&♦♦♦l♦♦♦r♦♦QEd8♦tQ♦e♦♦Obandit4@bandit:~/inhere$ cat ./-file04

    ♦♦♦gXW♦Diz♦;♦B♦♦♦m♦z♦♦♦♦♦♦bandit4@bandit:~/inhere$ cat ./-file05
    ♦♦!♦>E♦+♦♦♦♦ "♦K♦bg
        ♦♦♦♦
    ♦♦I♦=4bandit4@bandit:~/inhere$ cat ./-file06
    ^♦f♦♦♦♦♦s♦_♦c♦$!C♦♦j♦?迟♦Mt♦bandit4@bandit:~/inhere$ cat ./-file07
    lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR
    bandit4@bandit:~/inhere$ |
```

Cách 2: cat /* để xem tất cả các file

```
bandit4@bandit:~/inhere$ cat /*
♦♦Q♦6
    ♦♦V♦♦♦gH♦b♦♦♦v♦♦Q♦e♦`8♦♦G[S♦]`S♦♦♦IE♦♦♦♦♦2;♦G)=I♦♦O♦
        $`S♦&♦♦♦♦♦/v♦♦♦%♦♦♦♦♦l♦♦♦r♦♦QEd8♦tQ♦e♦♦O
    ♦♦♦gXW♦Diz♦;♦B♦♦♦m♦z♦♦♦♦♦♦!♦>E♦+♦♦♦♦
    ♦♦K♦bg
        ♦♦♦♦
    ♦♦I♦=4^♦f♦♦♦♦♦s♦_♦c♦$!C♦♦j♦?迟♦Mt♦lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR
    ^♦B♦e♦_♦p♦1_♦NDF♦♦z#Z#Z♦#i
    \♦(♦)_,16♦♦♦e♦^PT4"♦:♦♦♦-`qbandit4@bandit:~/inhere$ cat -file00-file00
```

Vậy flag cho level 4:

lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR

Level 5:

Vào thư mục inhere

Với các tiêu chuẩn:

human-readable

1033 bytes in size

not executable

Vậy để thực hiện ta sẽ dùng lệnh: find . -type f -size 1033c -exec cat {} \;

trong đó find . là tìm kiếm tất cả

-type f là loại file

-size 1033c với 1033 size in byte

```
bandit5@bandit:~/inhere$ find . -type f -size 1033c -exec cat {} \;
P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU
```

Vậy ta có được đoạn flag: P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU

Level 6:

Đầu tiên ta thực hiện lệnh find / -user bandit7 -group bandit6 -size 33c

trong đó file / là tìm tất cả các file

-user bandit7 là được sở hữu bởi user bandit 7

-group bandit6 là được sở hữu bởi group 6

-size 33c là kích cỡ 33 byte

```
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c
find: '/var/tmp/shujuaa29': Permission denied
find: '/var/tmp/systemd-private-a83ff8463b764265be181d909810e8a-systemd-resolved.service-G8gzCb': Permission denied
find: '/var/tmp/systemd-private-a83ff8463b764265be181d909810e8a-ModemManager.service-rsclW': Permission denied
find: '/var/tmp/systemd-private-a83ff8463b764265be181d909810e8a-systemd-logind.service-bunSGY': Permission denied
find: '/var/tmp/systemd-private-a83ff8463b764265be181d909810e8a-chrony.service-d20XSp': Permission denied
find: '/var/snap/lnx/common/lxd': Permission denied
find: '/var/lib/amazon': Permission denied
find: '/var/lib/chrony': Permission denied
find: '/var/lib/private': Permission denied
find: '/var/lib/udisks2': Permission denied
find: '/var/lib/snappy/void': Permission denied
find: '/var/lib/snappy/cookie': Permission denied
find: '/var/lib/ubuntu Advantage/package-data-downloads/partial': Permission denied
find: '/var/lib/apt/lists/partial': Permission denied
/var/lib/dpkg/info/bandit7.password
find: '/var/lib/polkit-1': Permission denied
find: '/var/cache/pollinate': Permission denied
find: '/var/cache/private': Permission denied
find: '/var/cache/dconfig': Permission denied
find: '/var/cache/apt/archives/partial': Permission denied
find: '/var/cache/apparmor/c47abf7.0': Permission denied
find: '/var/cache/apparmor/e10c1cf9.0': Permission denied
find: '/var/log/amazon': Permission denied
find: '/var/log/chrony': Permission denied
find: '/var/log/private': Permission denied
find: '/var/log/unattended-upgrades': Permission denied
find: '/var/spool/cron/crontabs': Permission denied
find: '/var/spool/rsyslog': Permission denied
find: '/var/spool/bandit24': Permission denied
find: '/tmp': Permission denied
find: '/boot/efi': Permission denied
find: '/proc/tty/driver': Permission denied
find: '/proc/552286/task/552286/fd/6': No such file or directory
find: '/proc/552286/task/552286/fdinfo/6': No such file or directory
find: '/proc/552286/fd/5': No such file or directory
find: '/proc/552286/fdinfo/5': No such file or directory
find: '/run/chrony': Permission denied
find: '/run/udisks2': Permission denied
```

Quan sát thấy được là hầu hết các file đều bị denied và có một file duy nhất không bị, ta sẽ cat file đó bằng lệnh cat /var/lib/dpkg/info/bandit7.password

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

Ta có thể thấy được password: z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S

Level 7:

Ở level này khá đơn giản, đề yêu cầu tìm file data.txt với từ khóa millionth vậy ta chỉ cần thực hiện lệnh cat data.txt | grep millionth

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

Ta có thể thấy được password: TESKZC0XvTetK0S9xNwm25STk5iWrBvP

Level 8:

Đầu tiên ta sẽ cat file data.txt

The screenshot shows a terminal window titled 'bandit8@bandit:~'. The command 'cat data.txt' has been run, resulting in a massive amount of text. The text is mostly illegible due to its length, but some recognizable words and characters are scattered throughout, such as 'TESKZC0XvTetK0S9xNwm25STk5iWrBvP' which is part of the password. The terminal window is set against a dark background with white text.

Thấy được rất nhiều các dòng là định dạng của password nhưng chỉ có một dòng đúng, và theo đề bài thì dòng này chỉ xuất hiện 1 lần

Như vậy để kiểm tra dòng đó ta cần thực hiện lệnh cat data.txt | sort | uniq -u

Trong đó cat data.txt là hiện dữ liệu trong file data

sort là sắp xếp lại

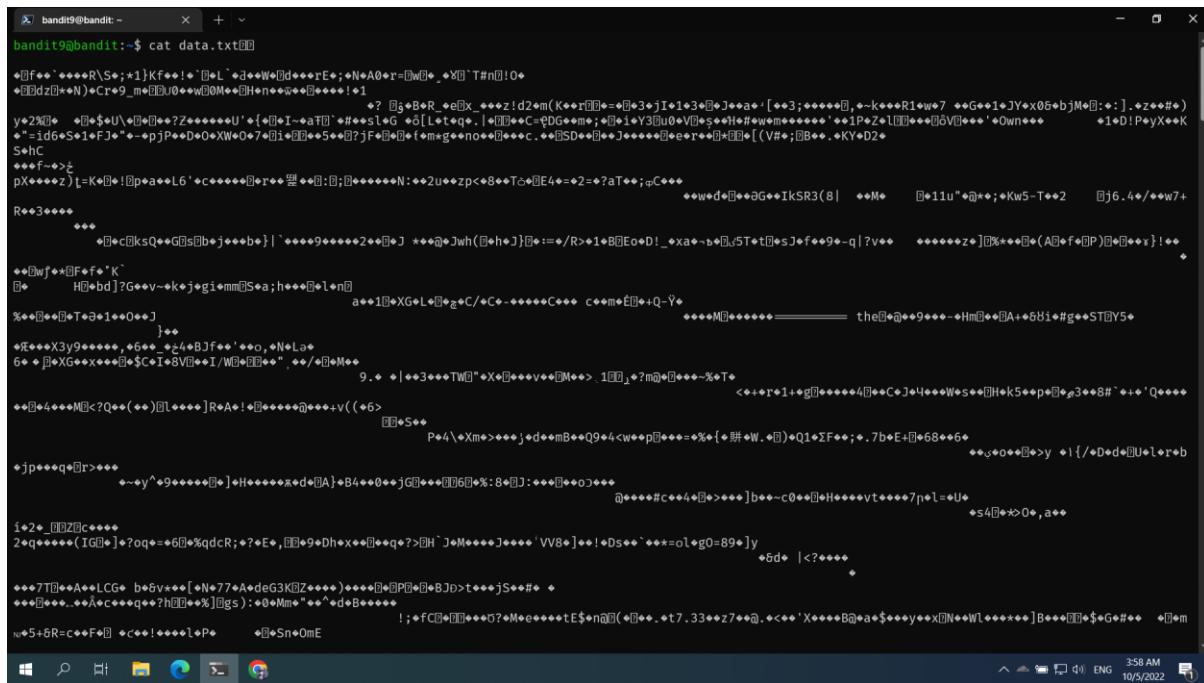
uniq -u là thể hiện việc dòng này không lặp lại hay chỉ xuất hiện 1 lần

```
bandit8@bandit:~$ cat data.txt | sort | uniq -u
EN632PlfYiZbn3PhVK3XOGSlNInNE00t
```

Vậy password là: EN632PlfYiZbn3PhVK3XOGSlNInNE00t

Level 9:

Đầu tiên ta sẽ cat data.txt để xem



```

bandit9@bandit:~$ cat data.txt
<...>

```

có thể thấy nó đang ở dạng ký tự đặc biệt và gần như không đọc được

như vậy để có thể đọc được thì ta sẽ cần đến lệnh strings data.txt

và theo đê bài ta biết được thêm là trong chuỗi password có chứa dấu = vậy nên ta sẽ thực hiện lệnh strings data.txt | grep =

```
bandit9@bandit:~$ strings data.txt | grep =
=id6
===== the
g0=89
5+&R=
V>%=
bu===== password
iwAw=
M'j=_ 
4iu===== is
b~=P
ED=Fpe
,=fX
x=f+
O=6pF
=do%
:26=
===== G7w8LIIi6J3kTb8A7j9LgrywtEUlyyp6s
=@dZ
u-;=
=#U?
2BEK=q
@!6=
```

Vậy password là: G7w8LIIi6J3kTb8A7j9LgrywtEUlyyp6s

Level 10:

Đầu tiên ta sẽ cat data.txt để xem

```
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIDZ6UGV6aUxkJSS05kTllGTmI2blZDS3pwaGxYSEJNCg==
```

Ta thấy được dữ liệu file data đang ở dạng base 64

vậy ta cần decode base64 để xem với lệnh: cat data.txt | base64 -d với base 64 -d là decode base64

```
bandit10@bandit:~$ cat data.txt | base64 -d
The password is 6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM
```

vậy password là: 6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM

Level 11:

Đầu tiên ta sẽ cat data.txt để xem

```
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf WIA0OSFzMjXXBC0KoSKBbJ8puQm5lIEi
```

Có thể thấy đây có thể là 1 dạng của ceasar cipher và theo đề bài đây là dạng đặc biệt ROT13 vì vậy có thể chuyển đổi với câu lệnh cat data.txt | tr "A-Za-z" "N-ZA-Mn-za-m" trong đó tr là đổi từ với bộ ký tự từ A tới Z cả in hoa và in thường sao cho đổi từ N tới Z sang A tới M và tương tự.

```
bandit11@bandit:~$ cat data.txt | tr "A-Za-z" "N-ZA-Mn-za-m"
The password is JVNBBSmZwKKOP0XbFXOoW8chDz5yVRv
```

vậy password là: JVNBBSmZwKKOP0XbFXOoW8chDz5yVRv

Level 12:

Đầu tiên ta sẽ cat data.txt để xem

```
bandit12@bandit:~$ cat data.txt
00000000: 1f8b 0808 7151 1063 0203 6461 7461 322e ....qQ.c..data2.
00000010: 6269 6e00 013f 02c0 fd42 5a68 3931 4159 bin..?..BZh91AY
00000020: 2653 595d ed11 a800 001b ffff d8ff fde7 65Y)..... .
00000030: dff7 ffff ffccf efcf7 7e7f dd39 3f7f .....~..?.
00000040: fafb ffbb cfbbf 3eff a9fb bf7f b001 3b1b ..>.....;
00000050: 6d20 0f50 0034 0680 0000 34c2 01ea 0d34 m..P.4....4....4
00000060: 0000 1900 1a32 1a68 d000 0000 0034 0000 ....2.h....4..
00000070: 000d 0069 91ea 0c5d 5100 0068 00c8 000d ...i...mQ..h...
00000080: 0323 4340 3d40 0f0d 1a68 01a3 4c83 401a ,#C@=@...h..L.@.
00000090: 687a 4034 0340 1a00 3468 0188 c868 3400 hz@4..@..4h..n4.
000000a0: 00c8 d01a 5874 d323 40d3 d206 81a1 a680 .....ht.#@. ....
000000b0: d0c8 0190 d034 0340 d000 c800 01a6 991a .....4..@. ....
000000c0: 0019 3400 d000 0006 800c 4d1a 0189 a001 ..4.....M. ....
000000d0: fc18 2890 6086 162a 8035 6a6b 3d5c 1382 ..(....*5j@\....
000000e0: 0a38 e6dd 214b 6f4a 3984 0192 256e e084 .8...1ko.9 ...%n..
000000f0: ed6b ad67 3318 b07a 005d 0e21 dbdb1 fb84 .k.g3..z.j.l. ....
00000100: 770f 055f 0044 3086 8230 d579 2881 afef w.._D0..0.y( ...
00000110: 531e 3071 f859 eeaee 01aa 1040 75cd 3c5b S..q.Y.....@u<[
00000120: f24a 16b8 34e7 43db 9e73 56a1 3d3d fd90 ..J..4.C..SV.=..
00000130: 6bc3 47a5 4c73 af13 a324 5731 b90e 2063 k.G.Ls...$W1... c
00000140: 45ef fe11 842e 03f9 b063 8f4c fb41 0a32 E.....c.L.A.2
00000150: 8fdb 7cea 82a0 ee91 4e05 c610 088e a2da I.....N. ....
00000160: 7536 2c72 1701 c248 ab7 1fef 30f8 147c u6,r...Hz ...0..
00000170: 0359 539c 5a21 4e94 6a33 9d18 6120 42a0 .YS.Z!N.j3 a B.
00000180: 6471 a01e 42a4 da3b 6ea5 5e7e edc3 f973 dq..B.;n.^.....s
00000190: 2ec7 5009 a7e8 10le a3ac b344 f2bb d9e6 ..P.....D.....
000001a0: 7bd7 c5fb 18bb 92ac 9fe8 aefa 673c dae0 {.....g<..
000001b0: 0cdb 0440 4869 1bd0 7d84 e1e5 85c2 1a60 ...@Hi...}.....
000001c0: 701c c9a5 50ca adf7 bba9 226f f175 1ec2 p...P....."0.u..
000001d0: 90de 557f ed09 5c3b 1886 84dc f110 24e7 ..U...;.....$.
000001e0: 871b 6148 f224 fb71 c3d1 1096 4a48 48a2 ..@H..$.q.....JHH.
000001f0: 99e6 647b 4f3b ac19 3be6 1cb9 24c3 ce48 ..d10;..; $..H
00000200: 829b 0182 07ef fbee df1f 40d4 f65a c7fb .....@.oz..
00000210: 5412 78a9 43dd 2198 d456 3c1f e161 2bf T.x.C..!..Vc..a+.
00000220: e682 f066 70e2 67bb ec48 d418 3e6a 0eef7 n..fp,g..H..>j..
00000230: 868a 1ddc e7b0 11ee 8b2a 8c53 0009 37f9 .....*,S..7.
00000240: 1017 0029 485a ec30 cb90 45bb 93ff 1772 ...)Hz.0..E....r
00000250: 4538 5090 5ded 11a8 e965 cb22 3f02 0000 E8P.]....e.^ ...
```

theo đề bài ta cần tạo 1 folder trong tmp và sau đó copy file data vào file data.txt.dump ở đó, sau đó chúng ta sẽ vào đường dẫn vừa tạo và sử dụng xxd để hexdump và ghi vào file data.txt

Sau đó sử dụng lệnh file data.txt để xem thông tin, có thể thấy có thêm 1 file data2.bin

```
bandit12@bandit:~$ cp data.txt /tmp/nhom7/data.txt.dump
bandit12@bandit:~$ cd /tmp/nhom7/
bandit12@bandit:/tmp/nhom7$ ls -a
. .. data.txt.dump
bandit12@bandit:/tmp/nhom7$ cat data.txt.dump | xxd -r > data.txt
bandit12@bandit:/tmp/nhom7$ ls -la
total 336
drwxrwxr-x    2 bandit12 bandit12  4096 Oct  5 04:26 .
drwxrwx-wt 4210 root      root     327680 Oct  5 04:25 ..
-rw-rw-r--    1 bandit12 bandit12   608 Oct  5 04:26 data.txt
-rw-r-----  1 bandit12 bandit12  2584 Oct  5 04:22 data.txt.dump
```

```
bandit12@bandit:/tmp/nhom7$ file data.txt
data.txt: gzip compressed data, was "data2.bin", last modified: Thu Sep 1 06:30:09 2022, max compression, from Unix, original size modulo 2^32 575
```

ta sẽ gunzip để phục hồi file data.txt

```
bandit12@bandit:/tmp/nhom7$ gunzip data.txt
gzip: data.txt: unknown suffix -- ignored
```

nhưng để gunzip thì ta cần phải có file có đuôi (suffix) là gz để gunzip, ta sẽ move data.txt vào data.txt.gz và sau đó gunzip trở lại, sau khi hoàn thành ta sẽ sử dụng lệnh file data.txt để check lại thông tin

```
bandit12@bandit:/tmp/nhom7$ mv data.txt data.txt.gz
bandit12@bandit:/tmp/nhom7$ gunzip data.txt.gz
bandit12@bandit:/tmp/nhom7$ ls -la
total 336
drwxrwxr-x    2 bandit12 bandit12  4096 Oct  5 04:27 .
drwxrwx-wt 4210 root      root     327680 Oct  5 04:27 ..
-rw-rw-r--    1 bandit12 bandit12   575 Oct  5 04:26 data.txt
-rw-r-----  1 bandit12 bandit12  2584 Oct  5 04:22 data.txt.dump
bandit12@bandit:/tmp/nhom7$ file data.txt
data.txt: bzip2 compressed data, block size = 900k
```

Ở đây ta vẫn chưa thấy được file sau khi thực hiện việc kiểm tra file bằng lệnh file data.txt vậy nên ta sẽ tiếp tục sử dụng bzip2 -d data.txt để tiếp tục giải nén

```
bandit12@bandit:/tmp/nhom7$ bzip2 -d data.txt
bzip2: Can't guess original name for data.txt -- using data.txt.out
bandit12@bandit:/tmp/nhom7$ file data.txt.out
data.txt.out: gzip compressed data, was "data4.bin", last modified: Thu Sep 1 06:30:09 2022, max compression, from Unix, original size modulo 2^32 20480
```

Vẫn chưa thấy nên ta tiếp tục, move data.txt.out vào data.txt.gz và tiếp tục giải nén

```
bandit12@bandit:/tmp/nhom7$ mv data.txt.out data.txt.gz
bandit12@bandit:/tmp/nhom7$ gunzip data.txt.gz
bandit12@bandit:/tmp/nhom7$ file data.txt
data.txt: POSIX tar archive (GNU)
```

Ở đây ta thấy được báo là POSIX tar archive, vậy nên ta cần giải nén bằng tar với lệnh tar -xvf data.txt, giải nén xong ta tiếp tục check file vừa được giải nén (data5.bin) thì thấy được đó là tar archive thì ta tiếp tục giải nén tương tự như vậy để được data6.bin.

Sau đó check file data6.bin và thấy được ta có thể giải nén bằng bzip2 và thấy được file data6.bin.out là tar archive và tiếp tục giải nén để có được data8.bin.

Kiểm tra data8.bin thì ta cần phải move data8.bin vào data.txt.gz và giải nén ra.

Cuối cùng ta được file data.txt ở dạng ASCII, ta sử dụng cat data.txt để xem

```
bandit12@bandit:/tmp/nhom7$ tar -xvf data.txt
data5.bin
bandit12@bandit:/tmp/nhom7$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/nhom7$ tar -xvf data5.bin
data6.bin
bandit12@bandit:/tmp/nhom7$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/nhom7$ bzip2 -d data6.bin
bzip2: Can't guess original name for data6.bin -- using data6.bin.out
bandit12@bandit:/tmp/nhom7$ file data6.bin.out
data6.bin.out: POSIX tar archive (GNU)
bandit12@bandit:/tmp/nhom7$ tar -xvf data6.bin.out
data8.bin
bandit12@bandit:/tmp/nhom7$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Thu Sep 1 06:30:09 2022, max compression, from Unix, original size modulo 2^32 49
bandit12@bandit:/tmp/nhom7$ mv data8.bin data.txt.gz
bandit12@bandit:/tmp/nhom7$ gunzip data.txt.gz
gzip: data.txt already exists; do you wish to overwrite (y or n)? y
bandit12@bandit:/tmp/nhom7$ file data.txt
data.txt: ASCII text
bandit12@bandit:/tmp/nhom7$ cat data.txt
The password is wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw
bandit12@bandit:/tmp/nhom7$
```

Vậy password là: wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw

Level 13:

Đầu tiên ta sẽ liệt kê tất cả các file và cat file key ra để xem, thì ta thấy được file private key và ta sẽ lưu file này vào máy local của cá nhân

```
bandit13@bandit:~$ ls -la
total 24
drwxr-xr-x  2 root      root      4096 Sep  1 06:30 .
drwxr-xr-x 49 root      root      4096 Sep  1 06:30 ..
-rw-r--r--  1 root      root      220 Jan  6 2022 .bash_logout
-rw-r--r--  1 root      root      3771 Jan  6 2022 .bashrc
-rw-r--r--  1 root      root      807 Jan  6 2022 .profile
-rw-r----- 1 bandit14 bandit13 1679 Sep  1 06:30 sshkey.private
bandit13@bandit:~$ cat sshkey.private
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAXkkOE83W2cOT7IWfc9aPaaQmQDdgzuXCv+ppZHa++buSkN+
gg0tcr7Fw8NLGa5+Uzec2rEg0WmeevB13AIoYp0MZYETq46t+jk9puNwZwIt9XgB
ZufGtZEwBbFWw/vVNLwOXBe4UWStGRWzgPpEeSv5Tb1VjLZIBdGphTIK22Amz6Zb
ThMsIMnyJafEwJ/T8PQO3myS91vUHEuoOMAz0UID4kN0MEZ3+XahyK0HJVq68KsV
ObefXG1vvA3GAJ29kxJaqvRfgYnqZryWN7w3CHjNU4c/2Jkp+n8L0SnxNA+WYA7
jiPyTF0is8uzMLYQ4l1Lzh/8/MpvhCQF8r22dwIDAQABoIBAQC6dWBjhxE0zjeA
J3j/RWmap9M5zfJ/wb2bfidNpwbB8rsJ4sZIDZQ7XuIh4LfgyoAQSS+bBw3RXvzE
pvJt3SmU8hIDuLsCjL1VnBY5pY7Bju8g8aR/3FyjyNAqx/TLfzLLYf0u7i9Jet67
xAh0tONG/u8FB5I3LAI2Vp60viwdWeC4n0xCthldpuPKNLA8rmMMVRTKQ+7T2VS
nXmwYckKUcUgzoVSpinZaS0zUDypdpy2+tRH3Mqa5kqN1YKjvF8RC47wo0YCktsD
o3FFpGNFec9Taa3Msy+DfQQhHKZFKIL3bJDONTmrVvtYK40/yeU4aZ/HA2DQzwhe
ol1AfiEhAoGBAOnVjosBkm7sblk+n4IEwPxs8s0mhPnTDUy5WGrpScrX0msVIBUF
laL3ZGLx3xCIwtCnEucB9DvN2HZkupc/h6hTKUYLqXuyLD8njTrbRhLgbC9QrKrS
M1F2fSTxVqPtZdLDMwjNR04xHA/fKh8bXXyTMqOHNJTHHNhbh3McduRjAoGBANKU
1hqfnw7+aXncJ9bjysr1ZWbqOE5Nd8AFgfwaKuGTTVX2NsUQnCMWdOp+wFak40JH
PKWkJNdBG+ex0H9JNQsTK3X5PBMAS8AfX0GrKeuwKWA6erytVTqj0fLYcdp5+z9s
8DtVCxDuVsM+i4X8UqIG0lvGbtKEVokHPFXP1q/dAoGAcHg5YX7WEehCgCYTzp0+
xysX8ScM2qS6xuZ3MqUWAXUWkh7NGZvhe0sGy9i0dANzwKw7mUUUViaCMR/t54W1
GC83sOs3D7n5Mj8x3Nd08xFit7dT9a245TvaeYQ7KgmqpSg/SCKCw4c3eiLava+J
3btnJeSIU+8ZXq9XjPRpKwUCgYA7z6Li0QKxNeXH3qHXcnHok855maUj5fJNpPbY
idkyZ8ySF8GlcFsky8Yw6fWCqfG3zDrohJ5l9JmEsBh7SadkwsZhvecQcS9t4vby
9/8X4js0P8ibfcKS4nBP+dT81kkkg5Z5MohXBORA7VWx+ACohcDEkprsQ+w32xeD
qT1EvQKBgQDKm8ws2ByvSUVs9GjTilCajFqLJ0eVYzRPaY6f++Gv/UVfAPV4c+S0
kAWpXbv5tbkkzbS0eaLPTKgLzavXtQoTtKwrjpolHKIHUz6Wu+n4abfAIRFubOdN
/+aLoRQ0yBDRbdXMsZN/jvY44eM+xRLdRVyMmdPtP8belRi2E2aEzA=
-----END RSA PRIVATE KEY-----
```

Sau khi đã tải về xong ta sẽ cấp quyền 400 bằng lệnh chmod cho file, và sau đó đăng nhập level 14 bằng file key ta đã tải về

```
bandit13@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
PS C:\Users\ACER> scp -P 2220 bandit13@bandit.labs.overthewire.org:sshkey.private .
[Progress Bar]
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

bandit13@bandit.labs.overthewire.org's password:
sshkey.private
PS C:\Users\ACER> chmod 400 sshkey.private
PS C:\Users\ACER> ssh -i sshkey.private bandit14@bandit.labs.overthewire.org -p 2220
100% 1679    7.0KB/s   00:00
```

```

bandit14@bandit:~$ --[ Tips ]--
This machine has a 64bit processor and many security-features enabled
by default, although ASLR has been switched off. The following
compiler flags might be interesting:

-m32          compile for 32bit
-fno-stack-protector    disable ProPolice
-Wl,-z,nowro      disable nrof

In addition, the execstack tool can be used to flag the stack as
executable on ELF binaries.

Finally, network-access is limited for most levels by a local
firewall.

--[ 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/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ 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:~$ |

```

Level 14:

Với level này ta sẽ sử dụng netcat để check localhost 30000, nhưng lẽ thời gian sẽ lâu nên ta có thể kết hợp giữa sử dụng netcat và cat /etc/bandit_pass/bandit14 để đồng thời check password thay vì đợi quá lâu

```

bandit14@bandit:~$ cat /etc/bandit_pass/bandit14 | nc localhost 30000
Correct!
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt

```

Vậy password là: jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt

Level 15:

Với level này ta sẽ sử dụng openssl để check localhost 30001, nhưng lẽ thời gian sẽ lâu nên ta có thể kết hợp giữa sử dụng netcat và cat /etc/bandit_pass/bandit15 để đồng thời check password thay vì đợi quá lâu

```
bandit15@bandit:~$ cat /etc/bandit_pass/bandit15 | openssl s_client -connect localhost:30001 -quiet
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  5 06:11:59 2022 GMT
verify return:1
depth=0 CN = localhost
notAfter=Oct  5 06:11:59 2022 GMT
verify return:1
Correct!
JQttfApK4SeyHwDlI9SXGR50qcloAil1
```

Vậy password là: JQttfApK4SeyHwDlI9SXGR50qclOAill

Level 16:

```
[kali㉿kali)-[~]
$ whatis nmap
nmap (1)           - Network exploration tool and security / port scanner
```

Trước tiên ta quét các port 31000-32000 với nmap để tìm ra cổng đang lắng nghe:
“nmap -A -p 31000-32000 localhost”

Công 31790 đang lắng nghe:

```
bandit16@bandit:~$ nmap -p31000-32000 localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-05 15:05 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00010s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
31046/tcp  open  unknown
31518/tcp  open  unknown
31691/tcp  open  unknown
31790/tcp  open  unknown
31960/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
```

Sau đó ta thấy private key được cung cấp như bên dưới sau khi sử dụng lệnh openssl s_client -connect localhost:31790, nhưng lẽ thời gian sẽ lâu nên ta có thể kết hợp giữa sử dụng netcat và cat /etc/bandit_pass/bandit16 để đồng thời check password thay vì đợi quá lâu

```
PowerShell * bandit16@bandit: ~ * + *
Start Time: 1665044388
Timeout : 7200 (sec)
Verify return code: 10 (certificate has expired)
Extended master secret: no
Max Early Data: 0
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SudyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMlOJf7+BrJObArnxd9Y7YT2bRPQ
Ja61Lzb58Yw3rF1870R1o+rW4LCDnd2vUe/6L2wyuKn0KsD5tBjEkQTu
DSt2mCN4rhAL+JFr56o4T6z8WWAW18BR6yGrMq70/kALHYw30kePQAzLoVUWb
JGT165CxbCnz/c+w+mqyvnzpwvThMAzTzAzQxNdkR2MBGySxDLrjg0LNW6sK7wNx
x0Vztz/bz1kPjfkU1JHs+9EbVNj+D1XF0JuQIDAQABAoIBAbagpxpMiaoLWfvD
Khcj10ncc0b+a0E1iaFYQw1k7fw+2+pNuNDE65Fth0ar69jp5RLlw1nhpx3iBl
J9nOM80J0VToums3UOSBYxF8WwhXr1yGnc1sskbpwXOUdc9uXa+UEszH2P29oyd
d8WEry0gPxunRpjlMxkAtWWhpMuve050vk9Tl5wbu9albssgTcXkmOnPw9nC
YNW6DP2lbcBrvgT9yCNL6c-ZKuFd52y0Q9qOkwTEQpjf4uHtJom+asv1pmS8A
vLY9r60wSvmZhnQBurj7lyctXMIu1kkd4w7f77k+DjHoAxyxcUp1DGL51s0mana
+TOWwgEcYEABJtPxP0GRj+1QkX262jM3dE1kza8ky5moIwlqYdsx8NhgRhORT
8CHaurBb2682s08vUHK/fur850Ef9TrnCv2crpoqsgfhfKLxrLgtT+qdpfzrx
Satldt8GFQ85yA/hnwM2Kx3NaesDm75Lsm-tBdAiyc9P2jGRNTMSkCgYeAyphd
HCCn1/Fwju1httFx/rYKhliZDFYe1e/v45bn4yFm8x7R/b0i7Kaszx-Exdyt
SghatdcG0Knyw1bpJvysavhZpaJMjdJ6ctFhVaBajm/enClvCsX-X3L551wg0A
R57hglzei1iVjv3aGhwvLztszk62v6oXFu0ECgAbj046T4hyP5Ji193VSH0i
TtieK7RVxu1-iu7rWkgAXFpMLFteQsrPj/LemxE5eTDAMFLy9FL2M9poQWcg
R8dwSk8r9FGLs-9akcv5PI/WEKlwgx1nB30H9YlmtiG2Cg53CaIZFHxD6MjEG0iu
L8ktMPvdbWnsSBULp600KBgBap1TfC1Hnw1mGO3KpwYw7t006cdtKmJ0n8Ni
blh9e1yZ9FsGxsgrRBXrsqXuz7tsQagHxbdlq/Z3Q7YfzOKU4ZxEnabyxNvWku
YodJhsOoKvDQNWu6cyLRAWfu1SexW9a/9p7ftpxm07SgywmfLF2MIAEwyzRqaM
77pBaogGAMmj2Jdjp+Ez8duyn3i36gyrtFSNSsJLAbxfpd1c1gvTGCMW+9cq9b
dxvW8-TFVEB1104FHVm6EpTsccdxu+bCXWkfjukRb7DyG0t9JPsx8MBTakzh3
vbgysi/sN3RqRbcGU40f0o2yfAMT8s1m/uYv52061geuz/ujbjY=
-----END RSA PRIVATE KEY-----
```

Ta thấy private key, sau đó copy lại và lưu vào file bandit17.rsa để làm pass lên level 17

-----BEGIN RSA PRIVATE KEY-----

MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57S
UdyJ

imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMlOJf7+BrJObArnxd9Y7YT2bRP
Q

Ja6Lzb558YW3FZl87ORiO+rW4LCDCNd2lUvLE/GL2GWyuKN0K5iCd5TbtJzEk
QTu

DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW3OekePQAzL0
VUYbW

JGTi65CxbCnzc/w4+mqQyvmzpWtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK
7wNX

x0YVztz/zbIkPjfku1jHS+9EbVNj+D1XFOJuaQIDAQABAoIBABagpxpM1aoLWf
vD

KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNuDE6SFthOar69jp5RLwD1NhPx3iBl

J9nOM8OJ0VToum43UOS8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P
29ovd

d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9
nC

YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52yOQ9qOkwFTEQpjF4uNtJom+asvlpm
S8A

vLY9r60wYSvmZhNqBURj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOm
ama

+TOWWgECgYEAE8JtPxP0GRJ+IQkX262jM3dElkza8ky5moIwUqYdsx0NxHgRR
hORT

8c8hAuRBb2G82so8vUHk/fur85OEfc9TncnCY2crpoqsgdifKLxrLgtT+qDpfZnx

SatLdt8GfQ85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyc9P2jGRNtMSkCgYEAy
pHd

HCctNi/FwjulhttFx/rHYKhLidZDFYeIE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt

SghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enCIvGCSx+X3l5SiWg0A

R57hJglezIiVjv3aGwHwvlZvtszK6zV6oXFau0ECgYAbjo46T4hyP5tJi93V5HDi

TtieK7xRVxUl+iU7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFMLy9FL2m9oQ
WCg

R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB3OhYimtiG2Cg5JCqIZFHxD6MjEG
Oiu

L8ktHMPvodBwNsSBULpG0QKBgBAplTfC1HOnWiMGOU3KPwYWt0O6CdTk
mJ0mL8Ni

blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWk
U

Y0djHdSOoKvDQNWy6ucyLRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyz
RqaM

77pBAoGAMmjmlJdjp+Ez8duyn3ieo36yrttF5NSsJLAbxFpd1c1gvtGCWW+9Cq0b
dxviW8+TFVEBl1O4f7HVm6EpTscdDxU+bCXWkfjuRb7Dy9G0tt9JPsX8MBTakz
h3

vBgsyi/sN3RqRBcGU40fOoZyfAMT8s1m/uYv52O6IgeuZ/ujbjY=

-----END RSA PRIVATE KEY-----

```
PS C:\Users\ACER> echo "-----BEGIN RSA PRIVATE KEY-----"
>> MIIeogIBAAKCAQEAvmOkuifmMg6HL2YPI0jon6iWfbp7c3jx34YkYWqUH57SUdyJ
>> imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMl0Jf7+BrJ0bArnxd9Y7YT2bRPQ
>> Ja6Lzb558YW3Fz1870Ri0+rW4LCDNd2lUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
>> DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW30ekePQAzL0VUYbw
>> JGTi65CxbCnzc/w4+mqQyvmpWtMAzJTzAzQxNbkr2MBGySxDLrjg0LWN6sK7wNX
>> x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XFOJuaQIDAQABoIBABagpxpM1aoLWfvD
>> KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNuDE6SFth0ar69jp5RlLwD1NhPx3iBl
>> J9n0M80J0VToum43UOS8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd
>> d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCxkMQnPw9nC
>> YNN6DDP21bcBrvgT9YCNL6C+ZKufD52y0Q9q0kwFTEQpjF4uNtJom+asvlpms8A
>> vLY9r60wYSvmZhNqBURj7lyCtXMIu1kkd4w7F77k+DjHoAXycxUp1DGL51s0mama
>> +TOWwgECgYE8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRhORT
>> 8c8hAuRBb2G82so8vUhk/fur850Efc9TncnCY2crpoqsgifKLxrLgtT+qDpfZnx
>> SatLdt8GfQ85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyc9P2jGRNtMSkCgYEAYpHd
>> HCctNi/FwjulhttFx/rHYKhLidZDFYeie/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
>> SghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enCIvGCSx+X3l5SiWg0A
>> R57hJglezIiVjv3aGwHwvlZvtszK6zV6oXFau0ECgYAbjo46T4hyP5tJi93V5HDi
>> TtieK7xRVxUl+iU7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFLy9FL2m9oQWCg
>> R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB30hYimtiG2Cg5JCqIZFHxD6MjEG0iu
>> L8ktHMPvodBwNsSBULpG0QKBgBAplTfC1HOnWiMGOU3KPwYWt0O6CdTkmJ0mL8Ni
>> blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU
>> Y0djHdSOoKvDQNWy6ucyLRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyzRqaM
>> 77pBAoGAMmjmlJdjp+Ez8duyn3ieo36yrttF5NSsJLAbxFpd1c1gvtGCWW+9Cq0b
>> dxviW8+TFVEBl1O4f7HVm6EpTscdDxU+bCXWkfjuRb7Dy9G0tt9JPsX8MBTakzh3
>> vBgsyi/sN3RqRBcGU40fOoZyfAMT8s1m/uYv52O6IgeuZ/ujbjY=
>> -----END RSA PRIVATE KEY-----" > bandit17.rsa|
```

Cấp quyền 400 cho private key

```
PS C:\Users\ACER> chmod 400 bandit17.rsa  
PS C:\Users\ACER> |
```

Sau đó ta dùng private key đó để đăng nhập level 17

Level 17:

Ở level này ta sẽ check list xem có gì, ta thấy được tồn tại 2 file pass mới và cũ, và theo đề pass là sự khác biệt giữa file mới và file cũ và đáp án nằm ở file mới.

```
bandit17@bandit:~$ ls  
passwords.new  passwords.old
```

Ta sẽ sử dụng lệnh diff để check:

```
bandit17@bandit:~$ diff passwords.old passwords.new
42c42
< 09wUIyMU4YhOzl1Lzxoz0voIBzZ2TUAf
—
> hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg
```

Vậy password là: hga5tuoCLF6ffZUpnagiMN8ssu9LFrdg

Level 18:

Tiếp theo ta đăng nhập vào level 18, thì lập tức ta bị đăng xuất ra ngay.

```

PS C:\Users\ACER> ssh 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:

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

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/.

Windows Taskbar icons and system status bar are visible at the bottom.
```

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

Trong đê sẽ cat readme đi cùng với câu lệnh và ta sẽ get được password:

```

PS C:\Users\ACER> ssh bandit18@bandit.labs.overthewire.org -p 2220 "cat readme"
[|_|_ \ /_,-,-,-\ /[-]|
 [ |_)| (|-| | | | | |
 [_._-/ \_,_|_|_| \_,_|_|_|

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

bandit18@bandit.labs.overthewire.org's password:
awhqeNnAbc1naukrpqDYcF95h7HoMTrC
PS C:\Users\ACER>
```

Vậy password là: awhqeNnAbc1naukrpqDYcF95h7HoMTrC

Level 19:

Ở level này ta sẽ list các file ra xem, ta thấy được file bandit20-do ta sẽ thực thi xem như thế nào. Sau khi chạy ta thấy cần đăng sau nó thêm 1 lệnh nữa thì nó mới có thể chạy được.

```
bandit19@bandit:~$ ls
bandit20-do
bandit19@bandit:~$ ./bandit20-do
Run a command as another user.
Example: ./bandit20-do id
```

Vậy ta sẽ thêm lệnh cat password phía sau để thực hiện show password

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

Vậy password là: VxCazJaVykJ6W36BkBU0mJTCM8rR95XT

Level 20:

Ở level này ta sẽ mở 2 level 1 bên nghe và 1 bên gọi và một bên nghe terminal 1 bên nghe sẽ set up netcat để nhận password

```
bandit20@bandit:~$ ls
suconnect
bandit20@bandit:~$ nc -lp 31337 < /etc/bandit_pass/bandit20
NvEJF7oVjkddltPSrdKEFollh9V1IBcq
```

terminal 2 bên gửi sẽ gửi data lên để bên nhận có thể nhận được password

```
bandit20@bandit:~$ ./suconnect 31337
Read: VxCazJaVykJ6W36BkBU0mJTCM8rR95XT
Password matches, sending next password
```

Vậy password là: NvEJF7oVjkddltPSrdKEFollh9V1IBcq

Level 21:

Trong level này, ta sẽ list file /etc/cron.d

Sau đó ta thấy file cronjob cho level 22 ta sẽ thử cat file đó ra xem.

Ta thấy được việc reboot được đẩy vào cronjob_bandit22.sh, ta sẽ tiếp tục cat ra xem tiếp.

Và tiếp thấy được việc cấp quyền chmod cho một file trong tmp với nhiều ký tự lạ và ta tiếp tục cat tiếp ra xem và ta get được mật khẩu

```

bandit21@bandit:~$ ls -la /etc/cron.d
total 48
drwxr-xr-x  2 root root 4096 Sep  1 06:30 .
drwxr-xr-x 110 root root 4096 Sep  8 12:09 ..
-rw-r--r--  1 root root   62 Sep  1 06:30 cronjob_bandit15_root
-rw-r--r--  1 root root   62 Sep  1 06:30 cronjob_bandit17_root
-rw-r--r--  1 root root  120 Sep  1 06:30 cronjob_bandit22
-rw-r--r--  1 root root  122 Sep  1 06:30 cronjob_bandit23
-rw-r--r--  1 root root  120 Sep  1 06:30 cronjob_bandit24
-rw-r--r--  1 root root   62 Sep  1 06:30 cronjob_bandit25_root
-rw-r--r--  1 root root  201 Jan  8 2022 e2scrub_all
-rwx----- 1 root root   52 Sep  1 06:30 otw-tmp-dir
-rw-r--r--  1 root root  102 Mar 23 2022 .placeholder
-rw-r--r--  1 root root  396 Feb  2 2021 sysstat
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:~$ ls -la /usr/bin/cronjob_bandit22.sh
-rwxr-x--- 1 bandit22 bandit21 130 Sep  1 06:30 /usr/bin/cronjob_bandit22.sh
bandit21@bandit:~$ cat /usr/bin/cronjob_bandit22.sh
#!/bin/bash
chmod 644 /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv
cat /etc/bandit_pass/bandit22 > /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv
bandit21@bandit:~$ cat /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv
WdDozAdTM2z9DiFEQ2mGlwngMfj4EZff
bandit21@bandit:~$ |

```

Vậy mật khẩu là: WdDozAdTM2z9DiFEQ2mGlwngMfj4EZff

Level 22:

Ở level này, ta sẽ tiếp tục list file /etc/cron.d, file cronjob và file cronjob_bandit23.sh, ta thấy được là họ tạo ra 1 file với myname và băm theo md5sum sau đó copy vào lưu target.

Vậy để có được ta sẽ băm câu “I am user bandit23” với md5sum, sau đó ta sẽ cat file với tên mới vừa được tạo ra. Vậy là ta sẽ có được kết quả

```

bandit22@bandit:~$ ls -la /etc/cron.d/
total 48
drwxr-xr-x  2 root root 4096 Sep  1 06:30 .
drwxr-xr-x 110 root root 4096 Sep  8 12:09 ..
-rw-r--r--  1 root root   62 Sep  1 06:30 cronjob_bandit15_root
-rw-r--r--  1 root root   62 Sep  1 06:30 cronjob_bandit17_root
-rw-r--r--  1 root root  120 Sep  1 06:30 cronjob_bandit22
-rw-r--r--  1 root root  122 Sep  1 06:30 cronjob_bandit23
-rw-r--r--  1 root root  120 Sep  1 06:30 cronjob_bandit24
-rw-r--r--  1 root root   62 Sep  1 06:30 cronjob_bandit25_root
-rw-r--r--  1 root root 201 Jan  8 2022 e2scrub_all
-rwx----- 1 root root   52 Sep  1 06:30 otw-tmp-dir
-rw-r--r--  1 root root 102 Mar 23 2022 .placeholder
-rw-r--r--  1 root root  396 Feb  2 2021 sysstat
bandit22@bandit:~$ cat /etc/cron.d/cronjob_bandit23
@reboot bandit23 /usr/bin/cronjob_bandit23.sh &> /dev/null
* * * * * bandit23 /usr/bin/cronjob_bandit23.sh &> /dev/null
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:~$ echo "I am user bandit23" | md5sum
8ca319486bfBBC3663ea0fbe81326349 -
bandit22@bandit:~$ cat /tmp/8ca319486bfBBC3663ea0fbe81326349
QYw0Y2aiA672PsMmh9puTQuhoz8SyR2G
bandit22@bandit:~$ |

```

Vậy password là: QYw0Y2aiA672PsMmh9puTQuhoz8SyR2G

Level 23:

Ở level này, ta sẽ tiếp tục list file /etc/cron.d, file cronjob và file cronjob_bandit24.sh ta có thể thấy được đoạn code.

```

bandit23@bandit:~$ ls -la /etc/cron.d/
total 48
drwxr-xr-x  2 root root 4096 Sep  1 06:30 .
drwxr-xr-x 110 root root 4096 Sep  8 12:09 ..
-rw-r--r--  1 root root   62 Sep  1 06:30 cronjob_bandit15_root
-rw-r--r--  1 root root   62 Sep  1 06:30 cronjob_bandit17_root
-rw-r--r--  1 root root  120 Sep  1 06:30 cronjob_bandit22
-rw-r--r--  1 root root  122 Sep  1 06:30 cronjob_bandit23
-rw-r--r--  1 root root  120 Sep  1 06:30 cronjob_bandit24
-rw-r--r--  1 root root   62 Sep  1 06:30 cronjob_bandit25_root
-rw-r--r--  1 root root 201 Jan  8 2022 e2scrub_all
-rwx-----  1 root root   52 Sep  1 06:30 otw-tmp-dir
-rw-r--r--  1 root root 102 Mar 23 2022 .placeholder
-rw-r--r--  1 root root 396 Feb  2 2021 sysstat
bandit23@bandit:~$ cat /etc/cron.d/cronjob_bandit24
@reboot bandit24 /usr/bin/cronjob_bandit24.sh &> /dev/null
* * * * * bandit24 /usr/bin/cronjob_bandit24.sh &> /dev/null
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

```

Trong cronjob_bandit24.sh ta thấy script sẽ thực thi và xóa tất cả các file trong thư mục /var/spool/\$myname/foo (trong TH này đang chạy với user là bandit24 nên \$myname là bandit24).

Ở hàm if thứ 2 thì ta thấy nó sẽ thực thi script nếu chủ của file là bandit23.

Nên để lấy được pass của level 24, ta cần quăng 1 file có chủ sở hữu của file là bandit23 và quăng file này vào /var/spool/bandit24/foo

Hiện tại ta đang là user bandit23 nên chúng ta cần tạo 1 file ở thư mục tmp, và dùng bản sao của nó để quăng vào /var/spool/bandit24/foo. Lý do dùng bản sao là để đề phòng có thứ gì sai làm trong quá trình này.

Nhớ cấp quyền +rwx cho bandit24_pass.sh, 777 cho /tmp/nhom07, +rwx cho lv24

```

bandit23@bandit:~$ mkdir /tmp/nhom07
bandit23@bandit:~$ cd /tmp/nhom07
bandit23@bandit:/tmp/nhom07$ touch bandit24_pass.sh
bandit23@bandit:/tmp/nhom07$ nano bandit24_pass.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/nhom07$ chmod +rx bandit24_pass.sh
bandit23@bandit:/tmp/nhom07$ chmod 777 /tmp/nhom07
bandit23@bandit:/tmp/nhom07$ touch lv24
bandit23@bandit:/tmp/nhom07$ chmod +rwx lv24
bandit23@bandit:/tmp/nhom07$ ls -la
total 1960
drwxrwxrwx 2 bandit23 bandit23    4096 Oct  7 11:31 .
drwxrwxrwt 1 root     root      1990656 Oct  7 11:31 ..
-rwxrwxr-x 1 bandit23 bandit23     61 Oct  7 11:30 bandit24_pass.sh
-rwxrwxr-x 1 bandit23 bandit23      0 Oct  7 11:31 lv24

```

Chuyển thư mục tới var/spool/bandit24/foo

cp bandit24_pass.sh /var/spool/bandit24/foo/bandit24.sh

Vậy ta có password là: VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar

Level 24:

Dùng lệnh nc để kết nối tới port 30002 của localhost.

```

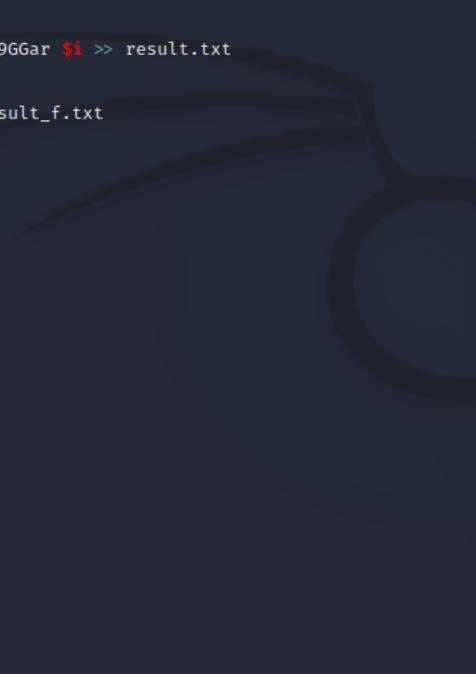
bandit24@bandit:~$ nc localhost 30002
I am the pincode checker for user bandit25. Please enter the password for user bandit24 and the secret pincode
on a single line, separated by a space.
nc localhost 30002
Wrong! Please enter the correct current password. Try again.
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar
Fail! You did not supply enough data. Try again.
Timeout. Exiting.

```

Theo đề bài, sau khi kết nối tới 30002, ta phải dùng password của user bandit24 và một mã pin gồm 4 chữ số để lấy được password của bandit25. Và không có cách nào lấy được mã pin này ngoại trừ việc thử 10000 tổ hợp các số từ 0000-9999.

Ta viết một script để brute-forcing: Ta dùng vòng lặp từ 0000 tới 9999, với mỗi vòng lặp cho password của bandit24 và 1 số từ 0000 tới 9999 vào file result, kết nối tới cổng 30002 và cho file result vào, sau đó xuất kết quả vào file result_f.txt.

Ta nên tạo 1 thư mục trong tmp và tạo file trong đó. Vì ta không có quyền tạo file ở thư mục gốc.



A screenshot of a terminal window titled "bandit24@bandit: /tmp/nhom07_bandit25". The terminal shows a script named "bruteforce_bandit25.sh" being edited in nano. The script contains the following code:

```

GNU nano 6.2
#!/bin/bash

for i in {0000..9999}
do
    echo VAFGXJ1PBSsPSnvsjI8p759leLZ9GGar $i >> result.txt
done

cat result.txt | nc localhost 30002 > result_f.txt

```

The terminal window has a dark background and light-colored text. At the bottom, there is a menu bar with options like File, Actions, Edit, View, Help, and a status bar showing "bruteforce_bandit25 *". Below the terminal is a file dialog box with the title "File Name to Write: bruteforce_bandit25.sh". The dialog includes standard file operations like Help (^G), Cancel (^C), DOS Format (M-D), Mac Format (M-M), Append (M-A), Prepend (M-P), Backup File (M-B), and Browse (^T).

Tạo thư mục trong tmp

mkdir /tmp/nhom07_bandit25

cd /tmp/nhom07_bandit25

Tạo file bruteforce_bandit25 và viết script với trình soạn thảo văn bản nano

nano bruteforce_bandit25.sh

Cấp quyền thực thi cho file bruteforce_bandit25.sh

chmod +x bruteforce_bandit25

Chạy file và tìm kiếm kết quả đúng

./bruteforce_bandit25

ls

cat result_f.txt | grep -v "Try again"

```

bandit24@bandit:/tmp/nhom07$ mkdir /tmp/nhom07_bandit25
bandit24@bandit:/tmp/nhom07$ cd
bandit24@bandit:$ cd /tmp/nhom07_bandit25
bandit24@bandit:/tmp/nhom07_bandit25$ nano bruteforce_bandit25.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/nhom07_bandit25$ cat bruteforce_bandit25.sh
#!/bin/bash

for i in {0000..9999}
do
    echo VAFGXJ1PBSsPSnvsjI8p759leLZ9GGar $i >> result.txt
done

cat result.txt | nc localhost 30002 > result_f.txt
bandit24@bandit:/tmp/nhom07_bandit25$ chmod +x bruteforce_bandit25.sh
bandit24@bandit:/tmp/nhom07_bandit25$ ./bruteforce_bandit25.sh
bandit24@bandit:/tmp/nhom07_bandit25$ ls
bruteforce_bandit25.sh  result_f.txt  result.txt
bandit24@bandit:/tmp/nhom07_bandit25$ cat result_f.txt | grep -v "Try again"
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 p7TaowMYrmu23Ol8hiZh9UvD0O9hpx8d
Exiting.

```

Miscellaneous:
 -S, --no-messages
 -v, --invert-match
 -V, --version
 --help
 Output control:
 -m, --max-count=NUM
 -b, --byte-offset
 -n, --line-number
 --line-buffered
 -H, --with-filename
 -h, --no-filename
 --label=LABEL
 -o, --only-matching
 -q, --quiet, --silent
 --binary-files=TYPE
 -a, --text
 -I
 -d, --directories=ACTION
 -D, --devices=ACTION
 -r, --recursive
 -R, --dereference-recur
 --include=GLOB

Vậy ta có password là: p7TaowMYrmu23Ol8hiZh9UvD0O9hpx8d

Level 25:

Trước tiên ta check thử shell của bandit26 xem có gì khác lạ.

```

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

```

recursive, '-' otherwise.
 Exit status is 0 if any line
 if any error occurs and -1
 Report bugs to: bug-grep@
 GNU grep home page: <<http://>
 General help using GNU so

Ta thấy nó có gì đó liên quan tới showtext và lệnh more cùng với file text.txt.

Chạy thử lệnh ls thì ta thấy có file bandit6.sshkey. Thủ dùng file này để đăng nhập vào bandit26 với lệnh “ssh bandit26@localhost -i bandit6.sshkey -p 2220” thì connection tự đóng.

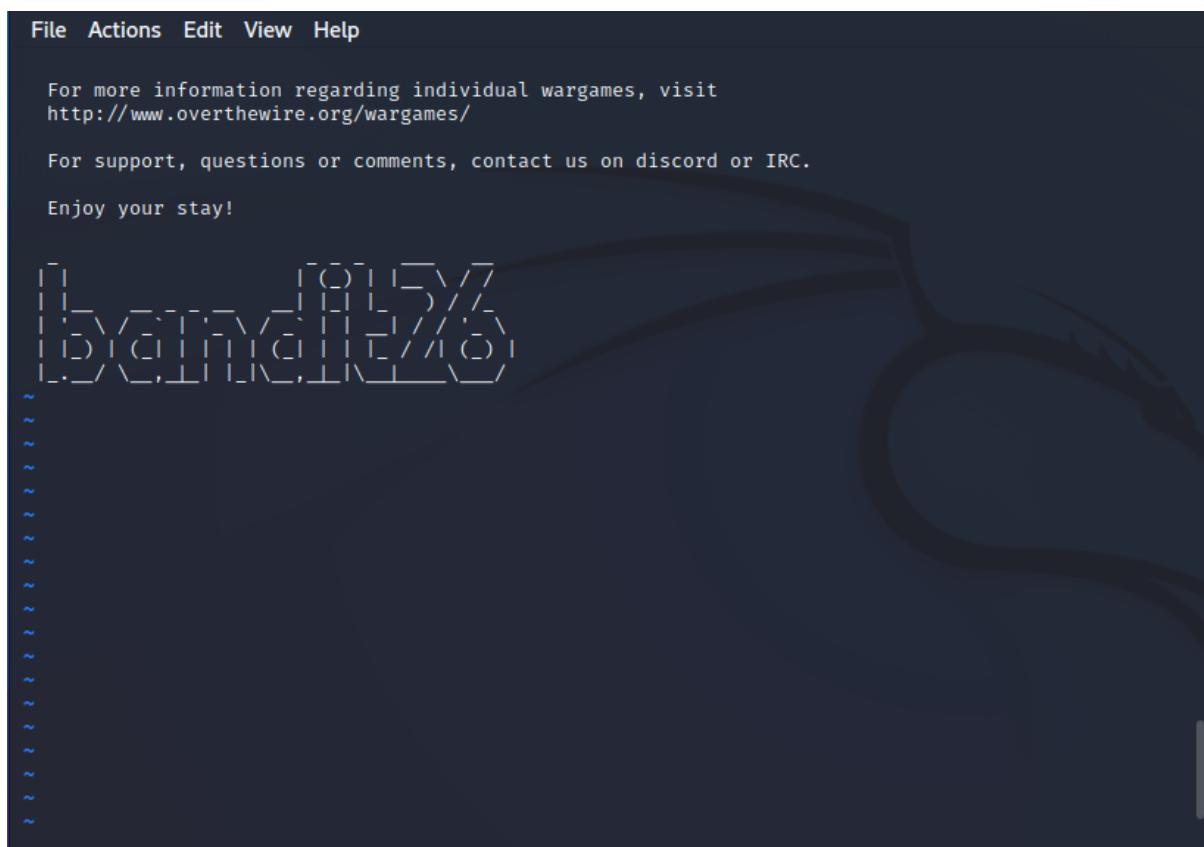
Ta dùng lệnh “cat /etc/passwd | grep “bandit26”

```

bandit25@bandit:~$ ls
bandit26.sshkey

```

```
bandit25@bandit:~$ ssh bandit26@localhost -i bandit26.sshkey -p2220
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhAAM/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/bandit25/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit25/.ssh/known_hosts).
```



Ta không được gì ngoài các ký tự ghép thành chữ bandit26

Xem lại thì đê có gợi ý lệnh more, sau khi tìm hiểu thì lệnh more là một lệnh cho phép hiển thị các file trong chế độ tương tác, More chỉ xuất hiện khi nội dung của file quá lớn để hiển thị trong terminal.

Ta thử thu nhỏ lại màn hình thì thấy xuất hiện chữ More.

Nhập v để vào vim.

Sau đó, để set up lại shell, ta dùng lệnh:

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

```
bandit26@bandit:~$ cat /etc/bandit_pass/bandit26
c7GvcKlw9mC7aUQaPx7nwFstuAIBw1o1
```

Vậy ta có password là: c7GvcKlw9mC7aUQaPx7nwFstuAIBw1o1

Level 26:

Cần shell từ level 26 để làm.

Chạy bandit27-do để biết chức năng của nó

“Run a command as another user”

Vậy ta chạy script này với command “cat /etc/bandit_pass/bandit27” để lấy pass của level 27

pass lv 27: YnQpBuifNMas1hcUFk70ZmqkhUU2EuaS

Level 27:

Để dùng lệnh git clone để clone repository về. Lưu ý ta tạo thư mục trong tmp để clone file về đó. Vì ta có quyền clone file về ở thư mục gốc

```
git clone ssh://bandit27-git@localhost:2220/home/bandit27-git/repo
```

Dùng lệnh ls để biết ta vừa clone gì về

Chuyển tới thư mục repo và mở thư mục README và nhận được password

```
bandit27@bandit:/tmp/nhom07_27$ ls
bandit27@bandit:/tmp/nhom07_27$ 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:C2ihUBV7ihnViwUXRb4RrEcLfXC5CXlhAAM/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).

[REDACTED]

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), 286 bytes | 286.00 KiB/s, done.
bandit27@bandit:/tmp/nhom07_27$ ls
repo
bandit27@bandit:/tmp/nhom07_27$ cd repo
bandit27@bandit:/tmp/nhom07_27/repo$ ls
README
bandit27@bandit:/tmp/nhom07_27/repo$ cat README
The password to the next level is: AVanL161y9rsbcJIsFHuw35rjaOM19nR
```

Vậy ta có password là: AVanL161y9rsbcJIsFHuw35rjaOM19nR

Level 28:

Tạo thư mục nhom07_28 và cd tới nó.

Dùng lệnh git clone để clone repository về.

```
git clone ssh://bandit28-git@localhost:2220/home/bandit28-git/repo
```

Ta tiếp tục tới thư mục repo và đọc file README giống như level trước thì thấy được username bandit 29 và password của nó đã bị che

```
bandit28@bandit:/tmp/nhom07_28(repo$ cat README.md
# Bandit Notes
Some notes for level29 of bandit.

## credentials

- username: bandit29
- password: xxxxxxxxxxxx
```

Dùng lệnh git log để xem lại các lịch sử commit, giám sát sự thay đổi

```
bandit28@bandit:/tmp/nhom07_28/repo$ git log
commit 43032edb2fb868dea2ceda9cb3882b2c33609ec (HEAD -> master, origin/master, origin/HEAD)
Author: Morla Porla <morla@overthewire.org>
Date:   Thu Sep 1 06:30:25 2022 +0000

    fix info leak

commit bdf3099fb1fb05faa29e80ea79d9db1e29d6c9b9
Author: Morla Porla <morla@overthewire.org>
Date:   Thu Sep 1 06:30:25 2022 +0000

    add missing data

commit 43d032b360b700e881e490fbbd2eee9eccd7919e
Author: Ben Dover <noone@overthewire.org>
Date:   Thu Sep 1 06:30:24 2022 +0000

    initial commit of README.md
```

Ta thấy được ở commit id 43032ed có ghi chú là “fix info leak”, ta thử xem thông tin cụ thể commit này với lệnh

```
git show <id commit>
```

```
bandit28@bandit:/tmp/nhmo07_28/repo$ git show 43032edb2fb868dea2ceda9cb3882b2c336c09ec
commit 43032edb2fb868dea2ceda9cb3882b2c336c09ec (HEAD → master, origin/master, origin/HEAD)
Author: Morla Porla <morla@overthewire.org>
Date:   Thu Sep 1 06:30:25 2022 +0000

    fix info leak

diff --git a/README.md b/README.md
index b302105 .. 5c6457b 100644
--- a/README.md
+++ b/README.md
@@ -4,5 +4,5 @@ Some notes for level29 of bandit.
## credentials

- username: bandit29
-- password: tQKvmcwNYcFS6vmPHIUSI3ShmsrQZK8S
+- password: xxxxxxxxxxxx
```

Vậy ta có password là: tOKymcwNYcFS6ymPHIUSI3ShmsrOZK8S

Level 29:

Tạo thư mục nhóm 07 29 trong tmp và cd tới nó.

Dùng lệnh git clone để clone repository về.

```
git clone ssh://bandit29-git@localhost:2220/home/bandit29-git/repo
```

```
bandit29@bandit:~$ mkdir /tmp/nhom07_29
bandit29@bandit:~$ cd /tmp/nhom07_29
bandit29@bandit:/tmp/nhom07_29$ 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).

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



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.
```

Giống như những level trước, ta chạy lệnh cd repo và cat README.md thì được

```

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).

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.
bandit29@bandit:/tmp/nhom07_29$ ls
repo
bandit29@bandit:/tmp/nhom07_29$ cd repo
bandit29@bandit:/tmp/nhom07_29/repo$ ls
README.md
bandit29@bandit:/tmp/nhom07_29/repo$ cat README.md
# Bandit Notes
Some notes for bandit30 of bandit.

## credentials

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

```

Ta dùng lệnh git branch -a để xem tất cả các nhánh

```

bandit29@bandit:/tmp/nhom07_29/repo$ git branch -a
* master
  remotes/origin/HEAD → origin/master
  remotes/origin/dev
  remotes/origin/master
  remotes/origin/splights-dev

```

Sau đó, ta có thể đi tới các nhánh khác để tìm password với lệnh

git checkout <branch name>

Ta tới nhánh dev, dùng lệnh ls để liệt kê file thì được folder code và file README.md. Ta đọc file README.md thì được password của bandit 30.

```

bandit29@bandit:/tmp/nhom07_29/repo$ git checkout dev
Branch 'dev' set up to track remote branch 'dev' from 'origin'.
Switched to a new branch 'dev'
bandit29@bandit:/tmp/nhom07_29/repo$ ls
code README.md
bandit29@bandit:/tmp/nhom07_29/repo$ cat README.md
# Bandit Notes
Some notes for bandit30 of bandit.

## credentials

- username: bandit30
- password: xbhV3HpNGlTIdnjUrdAlPzc2L6y9EOnS

```

Vậy ta có password là: xbhV3HpNGlTIdnjUrdAlPzc2L6y9EOnS

Level 30:

Tạo thư mục trong tmp và di chuyển vào trong nó để clone repo về:

```
mkdir /tmp/nhom07_30
```

```
cd /tmp/nhom07_30
```

Sau đó lặp lại các bước như những level trước và đọc file README.md thì ta thấy file này không cho ta thêm thông tin gì.

Sau khi thử nhiều cách, mình dùng lệnh git tag để xem lại các tag thì thấy được tag secret.

```
bandit30@bandit:/tmp/nhom07_30/repo$ git tag  
secret
```

Dùng lệnh git show để xem tag thì ta được password

```
bandit30@bandit:/tmp/nhom07_30/repo$ git show secret  
OfffzGDLzhAlerFJ2cAiz1D41JW1Mhmt
```

Level 31:

Tạo thư mục trong tmp và di chuyển vào trong nó để clone repo về:

```
mkdir /tmp/nhom07_31
```

```
cd /tmp/nhom07_31
```

Sau đó lặp lại các bước như những level trước và đọc file README.md thì ta được gợi ý tạo file “key.txt” và push file này lên remote repository

```
bandit31@bandit:~$ mkdir /tmp/nhom07_31
bandit31@bandit:~$ cd /tmp/nhom07_31
bandit31@bandit:/tmp/nhom07_31$ 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: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/bandit31/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit31/.ssh/known_hosts).

[REDACTED]

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: Total 4 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (4/4), done.
bandit31@bandit:/tmp/nhom07_31$ ls
repo
bandit31@bandit:/tmp/nhom07_31$ cd repo
bandit31@bandit:/tmp/nhom07_31/repo$ ls
README.md
bandit31@bandit:/tmp/nhom07_31/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
```

Dùng lệnh nano key.txt để tạo file và thêm nội dung “May I come in?” vào trong file.

```
bandit31@bandit:/tmp/nhom07_31/repo$ nano key.txt
Unable to create directory /home/bandit31/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

bandit31@bandit:/tmp/nhom07_31/repo$ cat key.txt
May I come in?
```

Ta thêm file vào repo

```
git add -f key.txt
```

```
bandit31@bandit:/tmp/nhom07_31/repo$ git add -f key.txt
```

Cuối cùng, ta commit file và đẩy file lên remote repository

```
git commit -m <nội dung muốn commit>
```

git push origin

Vậy ta có password là: rmCBvG56y58BXzv98yZGdO7ATVL5dW8y

Level 32:

Sau khi login vào level 32, ta thử các lệnh đơn giản như ls thì không thấy chạy được. Chú ý kỹ hơn thì thấy lệnh của ta đã bị in hoa. Nhập biến \$0 để shell quay lại bình thường.

```
WELCOME TO THE UPPERCASE SHELL  
-> ls  
sh: 1: LS: not found
```

Chạy thử lệnh ls -al thì thấy nó bình thường thật, ta thử cat /etc/bandit_pass/bandit33 thì ra được password thật.

```
>> $0
$ ls
uppershell
$ ls -al
total 36
drwxr-xr-x  2 root      root      4096 Sep  1 06:30 .
drwxr-xr-x  49 root      root      4096 Sep  1 06:30 ..
-rw-r--r--  1 root      root      220 Jan  6 2022 .bash_logout
-rw-r--r--  1 root      root     3771 Jan  6 2022 .bashrc
-rw-r--r--  1 root      root      807 Jan  6 2022 .profile
-rwsr-x---  1 bandit33 bandit33 15124 Sep  1 06:30 uppershell
$ cat /etc/bandit_pass/bandit33
odHo63fHiFqcWWJG9rlilDtPm45KzUky
```

Vậy ta có password là: odHo63fHiFqcWWJG9rLiLDtPm45KzUKy

Level 33:

Đây là thử thách cuối cùng, ta chạy ls và cat README.md và kết thúc chuỗi thử thách bandit này.

```
bandit33@bandit:~$ ls
README.txt
bandit33@bandit:~$ cat README.txt
Congratulations on solving the last level of this game!

At this moment, there are no more levels to play in this game. However, we are constantly working
on new levels and will most likely expand this game with more levels soon.
Keep an eye out for an announcement on our usual communication channels!
In the meantime, you could play some of our other wargames.

If you have an idea for an awesome new level, please let us know!
```

Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hành theo hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File **.PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng **Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)** – cỡ **chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.**
- Đặt tên theo định dạng: [Mã lớp]-SessionX_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành/Tên Cá nhân đã đăng ký với GV).

Ví dụ: [NT101.K11.ANTT]-Session1_Group3.

- Nếu báo cáo có nhiều file, nén tất cả file vào file **.ZIP** với cùng tên file báo cáo.
- **Không đặt tên đúng định dạng – yêu cầu, sẽ KHÔNG chấm điểm.**
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá: Sinh viên hiểu và tự thực hiện. Khuyến khích:

- Chuẩn bị tốt.
- Có nội dung mở rộng, ứng dụng trong kịch bản/câu hỏi phức tạp hơn, có đóng góp xây dựng.

Bài sao chép, trẽ, ... sẽ được xử lý tùy mức độ vi phạm.

HẾT