

BÁO CÁO THỰC HÀNH

Môn học: An Ninh Mạng

Kỳ báo cáo: Bandit

Tên chủ đề: **Bài tập Bandit**

GVHD: Nghi Hoàng Khoa

Nhóm: 08

1. THÔNG TIN CHUNG:

Lớp: NT140.011.ANTN

STT	Họ và tên	MSSV	Email
1	Lưu Gia Huy	21520916	21520916@gm.uit.edu.vn
2	Nguyễn Vũ Anh Duy	21520211	21520211@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá
1	Hoàn thành toàn bộ 34 level	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

🚩 Level 0:

```
bandit0@bandit:~$ pwd
/home/bandit0
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL
bandit0@bandit:~$
```

Password: NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL

🚩 Level 1:

Trong Linux thì “-” được để liên kết đến STDIN, STDOUT. Do đó để đọc file có tên là “-” ta cần phải dùng đường dẫn tương đối của file hoặc đường dẫn tuyệt đối để tránh sự nhầm lẫn:

```
bandit1@bandit:~$ ls -la
total 24
-rw-r----- 1 bandit2 bandit1 33 Oct 5 06:19 -
drwxr-xr-x 2 root root 4096 Oct 5 06:19 .
drwxr-xr-x 70 root root 4096 Oct 5 06:20 ..
-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
bandit1@bandit:~$ cat ./-
rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi
bandit1@bandit:~$
```

Password: rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi

🚩 Level 2:

```
bandit2@bandit:~$ ls -la
total 24
drwxr-xr-x 2 root root 4096 Oct 5 06:19 .
drwxr-xr-x 70 root root 4096 Oct 5 06:20 ..
-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 bandit3 bandit2 33 Oct 5 06:19 spaces in this filename
bandit2@bandit:~$ cat spaces\ in\ this\ filename
aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG
```

Để đọc được file mà tên file có dấu cách ta sẽ dùng dấu \ ở trước mỗi dấu cách là có thể cat như bình thường

Password: aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG

🚩 Level 3:

```
bandit3@bandit:~$ ls -la
total 24
drwxr-xr-x  3 root root 4096 Oct  5 06:19 .
drwxr-xr-x 70 root root 4096 Oct  5 06:20 ..
-rw-r--r--  1 root root  220 Jan  6 2022 .bash_logout
-rw-r--r--  1 root root 3771 Jan  6 2022 .bashrc
drwxr-xr-x  2 root root 4096 Oct  5 06:19 inhere
-rw-r--r--  1 root root  807 Jan  6 2022 .profile
bandit3@bandit:~$ cd inhere/
bandit3@bandit:~/inhere$ ls -la
total 12
drwxr-xr-x 2 root root 4096 Oct  5 06:19 .
drwxr-xr-x 3 root root 4096 Oct  5 06:19 ..
-rw-r----- 1 bandit4 bandit3  33 Oct  5 06:19 .hidden
bandit3@bandit:~/inhere$ cat .hidden
2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe
bandit3@bandit:~/inhere$
```

Option **-a** của lệnh **ls** cho phép list các file ẩn

Password: 2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe

🚩 Level 4:

```
bandit4@bandit:~$ ls -la
total 24
drwxr-xr-x  3 root root 4096 Oct  5 06:19 .
drwxr-xr-x 70 root root 4096 Oct  5 06:20 ..
-rw-r--r--  1 root root  220 Jan  6 2022 .bash_logout
-rw-r--r--  1 root root 3771 Jan  6 2022 .bashrc
drwxr-xr-x  2 root root 4096 Oct  5 06:19 inhere
-rw-r--r--  1 root root  807 Jan  6 2022 .profile
bandit4@bandit:~$ cd inhere/ ; ls
-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
lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR
bandit4@bandit:~/inhere$
```

Lệnh **find . -type f | xargs file** sẽ tiến hành tìm các file trong thư mục hiện tại và các thư mục con của nó, ứng với mỗi file sẽ trích xuất kiểu dữ liệu của file đó.

Sau khi tìm được file có kiểu dữ liệu là **ASCII text** thì ta **cat** lấy password

Password: lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR

Level 5:

```
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ find ./inhere/ -type f -size 1033c ! -executable | xargs f
ile | grep 'ASCII\|UTF-8'
./inhere/maybeh ere07/.file2: ASCII text, with very long lines (1000)
bandit5@bandit:~$ cat ./inhere/maybeh ere07/.file2
P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU
```

Gần như lv4 tuy nhiên có thêm 2 option là **-size 1033c** và **! -executable** tức là có size chính xác là **1033 bytes** và không có quyền thực thi

Password: P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU

Level 6:

```
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c 2>/dev/null
/var/lib/dpkg/info/bandit7.password
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S
bandit6@bandit:~$
```

Lệnh trên để tìm các file bắt đầu từ thư mục gốc, tìm file mà người sở hữu là **user bandit7**, thuộc **group bandit6** và có size chính xác là **33 bytes**

Password: z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S

Level 7:

```
Formica mo0dVnMSPCo9WdHItXLHMeD0w6SqbMvF
dankness's      Y0dD93vvBemBnw7xH0XNKUwPKEfpe7H7
threaten        p0aRPotuhqaf7d9lM0chKcHSM5xQ23qU
monastic        HmNt0zjzjVBHmoKRMH2CMARixJtnt5X3
flank's 234YYMFvjRGfWFZeVlijZAoSaDJSZR3m
demarcates      42GyLcNN2VyYVQAzLk6lH1KoPF7gU60v
biceps's       InBCsYpHT8o1atjygiRFnVE2ExoyirYv
bandit7@bandit:~$ ^C
bandit7@bandit:~$ cat data.txt | grep millionth
millionth      TESKZC0XvTetK0S9xNwm25STk5iWrBvP
bandit7@bandit:~$
```

Password: TESKZC0XvTetK0S9xNwm25STk5iWrBvP

Level 8:

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

Lấy dữ liệu của file **data.txt**, sau đó tiến hành **sort**, theo bảng chữ cái, tiếp theo dùng **uniq -u** để chỉ lấy các dòng duy nhất (**unique**)

Password: EN632PlfYiZbn3PhVK3XOGSlNInNE00t

Level 9:

```
bandit9@bandit:~$ ls
data.txt
bandit9@bandit:~$ strings data.txt | grep =
=2""L(
x]T===== theG)"
===== passwordk^
Y=xW
t%=q
===== is
4=}D3
{1\=
FC&=z
=Y!m
$/2`=Y
4_Q=\
MO=(
?=|J
WX=DA
{TbJ;=l
[=lI
===== G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s
>8=6
=r=_
=uea
zl=4
bandit9@bandit:~$
```

Lệnh **strings** dùng để trích xuất ra các chuỗi có trong file, **grep** để lấy theo yêu cầu đề bài, password đứng sau kí tự "="

Password: G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s

Level 10:

```
bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ cat data.txt
VGhLIHBhc3N3b3JkIGlzIDZ6UGV6aUxkUjJSS05kTl1GTmI2b1ZDS3pwaGxYSEJNCg==
bandit10@bandit:~$ base64 -d data.txt
The password is 6zPezilDR2RKNDNYFNb6nVCKzphlXHBM
bandit10@bandit:~$
```

base64 option **-d** là **decode**

Password: 6zPezILdR2RKNdNYFNb6nVCKzphlXHBM

Level 11:

```
bandit11@bandit:~$ ls
data.txt
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf WIA0OSFzMjXXBC0KoSKBbJ8puQm5lIEi
bandit11@bandit:~$ cat data.txt | tr 'a-zA-Z' 'n-za-mN-ZA-M'
The password is JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv
bandit11@bandit:~$
```

Lệnh `tr 'a-zA-Z' 'n-za-mN-ZA-M'` sẽ thực hiện thay thế các kí tự **a-z** sẽ thay bằng **n-za-m** tương tự cho các chữ in hoa

Password: JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv

Level 12:

```
bandit12@bandit:~$ mkdir /tmp/Hjn4
bandit12@bandit:~$ cp data.txt /tmp/Hjn4/
bandit12@bandit:~$ ls /tmp/Hjn4
data.txt
bandit12@bandit:~$ cd /tmp/Hjn4
```

```

bandit12@bandit: /tmp/Hjn4  ×  +  v
bandit12@bandit:/tmp/Hjn4$ xxd -r data.txt > data
bandit12@bandit:/tmp/Hjn4$ file data
data: gzip compressed data, was "data2.bin", last modified: Thu Oct  5 06:19:20
ompression, from Unix, original size modulo 2^32 573
bandit12@bandit:/tmp/Hjn4$ mv data data.gz
bandit12@bandit:/tmp/Hjn4$ gunzip data.gz
bandit12@bandit:/tmp/Hjn4$ ls
data  data.txt
bandit12@bandit:/tmp/Hjn4$ file data
data: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/Hjn4$ bunzip2 data
bunzip2: Can't guess original name for data -- using data.out
bandit12@bandit:/tmp/Hjn4$ ls
data.out  data.txt
bandit12@bandit:/tmp/Hjn4$ file data.out
data.out: gzip compressed data, was "data4.bin", last modified: Thu Oct  5 06:19
ax compression, from Unix, original size modulo 2^32 20480
bandit12@bandit:/tmp/Hjn4$ mv data.out data.out.gz
bandit12@bandit:/tmp/Hjn4$ gunzip data.out.gz
bandit12@bandit:/tmp/Hjn4$ file data.out
data.out: POSIX tar archive (GNU)
bandit12@bandit:/tmp/Hjn4$ tar -xvf data.out
data5.bin
bandit12@bandit:/tmp/Hjn4$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/Hjn4$ tar -xvf data5.bin
data6.bin
bandit12@bandit:/tmp/Hjn4$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/Hjn4$ bunzip2 data6.bin
bunzip2: Can't guess original name for data6.bin -- using data6.bin.out
bandit12@bandit:/tmp/Hjn4$ file data6.bin.out
data6.bin.out: POSIX tar archive (GNU)
bandit12@bandit:/tmp/Hjn4$ tar -xvf data6.bin.out
data8.bin
bandit12@bandit:/tmp/Hjn4$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Thu Oct  5 06:1
max compression, from Unix, original size modulo 2^32 49
bandit12@bandit:/tmp/Hjn4$ gunzip data8.bin
gzip: data8.bin: unknown suffix -- ignored
bandit12@bandit:/tmp/Hjn4$ mv data8.bin data8.gz
bandit12@bandit:/tmp/Hjn4$ gunzip data8.gz
bandit12@bandit:/tmp/Hjn4$ ls
data5.bin  data6.bin.out  data8  data.out  data.txt
bandit12@bandit:/tmp/Hjn4$ file data8
data8: ASCII text
bandit12@bandit:/tmp/Hjn4$ cat data8
The password is wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw
bandit12@bandit:/tmp/Hjn4$

```

Đầu tiên sẽ giải mã file dump với **xxd -r**

Sau đấy ứng với file được nén bằng gì ta sẽ giải nén tương ứng như thế. Tuy nhiên với file type là **gzip** thì phải có đuôi là **gz**

File **gzip** sẽ được giải nén bằng lệnh **gunzip <tên file>**

File **bzip2** sẽ được giải nén bằng lệnh **bunzip2 <tên file>**

File **tar** sẽ được giải nén bằng lệnh **tar -xvf <tên file>**

Password: wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw

Level 13:

```
bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ cat sshkey.private
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAXkkOE83W2cOT7IwhFc9aPaaQmQDdgzuXCv+ppZHa++buSkN+
gg0tcr7Fw8NLGa5+Uzec2rEg0WmeevB13AIoYp0MZyETq46t+jk9puNwZwIt9XgB
ZufGtZEwWbFwW/vVLNwOXBe4UWStGRWzgPpEeSv5Tb1VjLZIBdGphTIK22Amz6Zb
ThMsiMnyJafEwJ/T8PQ03mys91vUHEuo0MAzoUID4kN0MEZ3+XahyK0HJVq68KsV
ObefXG1vvA3GAJ29kxJaqrRfgYnqZryWN7w3CHjNU4c/2Jkp+n8L0SnxANA+WYA7
jiPyTF0is8uzMLYQ4l1Lzh/8/MpvhCQF8r22dwIDAQABAoIBAQC6dWBjhyE0zjeA
J3j/RWmap9M5zfJ/wb2bfidNpwbB8rsJ4sZIDZQ7XuIh4LfgygoAQSS+bBw3RXvzE
pvJt3SmU8hIDuLScjL1VnBY5py7Bju8g8aR/3FyjyNAqx/TLfzLLYf0u7i9Jet67
xAh0t0NG/u8FB5I3LAI2Vp60viwvdWeC4n0xCthldpuPKNLA8rmMMVRTKQ+7T2VS
nXmwYckKUCUgzoVSpinZa50zUDypdp2+trH3MQa5kqN1YKjvF8RC47wo0YCKtsD
o3FFpGNFec9Taa3Msy+DfQqHhKZFKIL3bJDONTmrVvtYK40/yeU4aZ/HA2DQzwhe
ol1AfiEhAoGBA0Nvj0sBkm7sblK+n4IEwPxs8s0mhPnTDUy5WGrpSCrX0msVIBUf
laL3ZGLx3xCiwtCnEucB9DvN2HZkupc/h6hTKUYLqXuyLD8njTrbRhLgbC9QrKrS
M1F2fSTxVqPtZDlDMwjNR04xHA/fKh8bXXyTMq0HNJTHHnbh3McdURjAoGBANkU
1hqfnw7+aXncJ9bjysr1ZWbqOE5Nd8AFgfwaKuGTTVX2NsUQnCMWd0p+wFak40JH
PKWkJnDBG+ex0H9JNqSTK3X5PBMA58AfX0GrKeuwKWA6erytVTqj0fLYcdp5+z9s
8DtVCxduVsM+i4X8UqIG0lvGbtKEVokHPFXP1q/dAoGACg5YX7WEehCgCYTzp0+
xysX8ScM2qS6xuZ3MqUWAXUWkh7NGZvhe0sGy9iOdANzwKw7mUUFVlaCMR/t54W1
GC83s0s3D7n5Mj8x3Nd08xFit7dT9a245TvaoYQ7KgmqpSg/ScKCw4c3eILava+J
3btnJeSIU+8ZXq9XjPRpKwUCgYA7z6Li0QKxNeXH3qHXcnHok855maUj5fJNpPbY
iDkyZ8ySF8GlcFsky8Yw6fWCqfG3zDrohJ5l9JmEsBh7SadkwsZhvecQcS9t4vby
9/8X4js0P8ibfckS4nBP+dT81kkkg5Z5MohXBORA7VMx+ACohcDEkprSQ+w32xeD
qT1EvQKBgQDKm8ws2ByvSUVs9GjTilCajFqLJ0eVYZRPaY6f++Gv/UVfAPV4c+S0
kAWpXbv5tbkzbs0eaLPTKgZavXtQoTtKwrjpolHKIHUz6Wu+n4abfAIRFub0dN
/+aLoRQ0yBDRbdXMsZN/jvY44eM+xRLdRVyMmdPtP8belRi2E2aEZA==
-----END RSA PRIVATE KEY-----
bandit13@bandit:~$
```



```
--[ 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/)

--[ 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:~$ whoami
bandit14
bandit14@bandit:~$
```

Ta cần phải **chmod 400** vì:

File không được bảo mật tốt, bị truy cập bởi nhiều bên, nên nó không được tin tưởng để sử dụng.

```
> ~ /bandit
chmod 777 sshkey.private

> ~ /bandit
ssh -i sshkey.private bandit14@bandit.labs.overthewire.org -p 2220

      [B] [A] [N] [D] [I] [T]
      [I] [N] [C] [I] [T]
      [I] [N] [C] [I] [T]

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

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@                WARNING: UNPROTECTED PRIVATE KEY FILE!                @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0777 for 'sshkey.private' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "sshkey.private": bad permissions
bandit14@bandit.labs.overthewire.org's password:
```

🚩 Level 14:

```
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14 | nc localhost 30000
Correct!
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnnt
bandit14@bandit:~$
```

Password: jN2kgmIXJ6fShzhT2avhotn4Zcka6tnnt

Level 15:

```
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 18 14:12:44 2023 GMT
verify return:1
depth=0 CN = localhost
notAfter=Oct 18 14:12:44 2023 GMT
verify return:1
Correct!
JQtTfApK4SeyHwDlI9SXGR50qcl0Ail1
```

Password: JQtTfApK4SeyHwDlI9SXGR50qcl0Ail1

Level 16:

```
bandit16@bandit:~$ nmap -A -p 31000-32000 localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-19 17:17 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00014s 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
| Not valid before: 2023-10-18T14:11:44
|_ Not valid after: 2023-10-18T14:12:44
31691/tcp  open  echo
31790/tcp  open  ssl/unknown
| fingerprint-strings:
|_  FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, Help, Kerberos, LDAPSearchReq, LPDString, RTSPRequest,
|_  Wrong! Please enter the correct current password
|_  ssl-cert: Subject: commonName=localhost
| Subject Alternative Name: DNS:localhost
| Not valid before: 2023-10-18T14:11:43
|_ Not valid after: 2023-10-18T14:12:43
31960/tcp  open  echo
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint:
SF-Port31790-TCP:V=7.80%T=SSL%I=7%D=10/19%Time=653164C7%P=x86_64-pc-linux-
SF:gnu%r(GenericLines,31,"Wrong!\x20Please\x20enter\x20the\x20correct\x20c
SF:urrent\x20password\n")%r(GetRequest,31,"Wrong!\x20Please\x20enter\x20th
SF:e\x20correct\x20current\x20password\n")%r(HTTPOptions,31,"Wrong!\x20Ple
SF:ase\x20enter\x20the\x20correct\x20password\n")%r(RTSPRequest
SF:,31,"Wrong!\x20Please\x20enter\x20the\x20correct\x20current\x20password
SF:\n")%r(Help,31,"Wrong!\x20Please\x20enter\x20the\x20correct\x20current\
SF:x20password\n")%r(SSLSessionReq,31,"Wrong!\x20Please\x20enter\x20the\x2
SF:0correct\x20current\x20password\n")%r(TerminalServerCookie,31,"Wrong!\x
SF:20Please\x20enter\x20the\x20correct\x20current\x20password\n")%r(TLSSes
SF:sionReq,31,"Wrong!\x20Please\x20enter\x20the\x20correct\x20current\x20p
SF:assword\n")%r(Kerberos,31,"Wrong!\x20Please\x20enter\x20the\x20correct\
SF:x20current\x20password\n")%r(FourOhFourRequest,31,"Wrong!\x20Please\x20
SF:enter\x20the\x20correct\x20current\x20password\n")%r(LPDString,31,"Wron
SF:g!\x20Please\x20enter\x20the\x20correct\x20current\x20password\n")%r(LD
SF:APSearchReq,31,"Wrong!\x20Please\x20enter\x20the\x20correct\x20current\
SF:x20password\n")%r(SIPOptions,31,"Wrong!\x20Please\x20enter\x20the\x20co
SF:rrect\x20current\x20password\n");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 99.00 seconds
bandit16@bandit:~$
```

Dùng nmap để quét port. Nhận thấy port **31790** khả nghi

```
bandit16@bandit:~$ cat /etc/bandit_pass/bandit16 | openssl s_client -connect localhost:31790 -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 18 14:12:43 2023 GMT
verify return:1
depth=0 CN = localhost
notAfter=Oct 18 14:12:43 2023 GMT
verify return:1
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIIEgIBAAKCAQEAvM0kuifmMg6HL2YPI0jon6iWfbp7c3jx34YkYwqUH57SudyJ
imZzeyGC0gtZPGUjUSxiJSWI/oTqexh+cAMTSMLOJf7+BrJ0bArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl870RiO+rW4LCDCNd2lUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rHAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW30ekePQAZL0VUYbW
JGTi65CxbCnzc/w4+mqQvmzpWtMAzJTzAzQxNbK2MBGySxDLrjg0LWN6sK7wnX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XF0JuaQIDAQABAoIBABagpxpM1aoLWfvD
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNUDE6SFth0ar69jp5RLlWd1NhPx3iBl
J9nOM80JV0Toum43UOS8YxF8WwhXriYGnc1sskbwpX0UDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmXkAtWnhpMvfe0050vk9TL5wqbu9ALbssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKuFD52yOQ9q0kwFTEQpjtf4uNtJom+asvLpmS8A
vLY9r60wYSvmZhNqBUrj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51s0mama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIka8ky5moIwUqYdsx0NxHgRRh0RT
8c8hAuRBb2G82so8vUHK/fur850Efc9TncCY2crpoqsgghifKLxrLgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyC9P2jGRNtMSkCgYEAypHd
HCctNi/FwjulhttFx/rHYKhLidZDFYeiE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0Knyw1bpJVusavPzpaJMjdJ6tcFhVABAjm7enCIvGCSx+X3l5SiWg0A
R57hJglezIiVjv3aGwHwvLZvtszK6zV6oXFAu0ECgYAbjo46T4hyP5tJi93V5Hdi
TtieK7xRVxUL+iu7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFMLy9FL2m9oQWCg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwGxinB30hYimtiG2Cg5JCqIZFHxD6MjEG0iu
L8ktHMPvodBwNsSBULpG0QKBgBAPLTfC1H0nWiMGOU3KPwYwT006CdTkmJomL8Ni
blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdlQ/ZJQ7Yfz0KU4ZxEnabvXnvWkU
Y0djHdS0oKvDQNWu6ucyLRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyzRqaM
77pBAoGAMmjMIJdjp+Ez8duyn3ieo36yrftF5NSsJLABxFpdlc1gvtGCWW+9Cq0b
dxviW8+TFVEBl104f7HVM6EpTscdXU+bCXWkfjuRb7Dy9G0tt9JPsx8MBTakzh3
vBgysi/sN3RqRBcGU40f0oZyFAMT8s1m/uYv5206IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----

bandit16@bandit:~$
```

Gửi nó password của user hiện tại và ta có được thứ ta cần


```
> ~ /bandit
chmod 700 sshkey.private

> ~ /bandit
vi sshkey.private

> ~ /bandit
cat sshkey.private
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvM0kuiFmMg6HL2YPI0jon6iWfbp7c3jx34YkYwQH57SudyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMl0Jf7+BrJObArnx9Y7YT2bRPQ
Ja6Lzb558YW3FZl870RiO+rW4LDCNd2LuvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rHAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW30ekePQAZL0VUYbW
JGTi65CxbCnzc/w4+mqQyvzpwTMAZJTzAzQXNbkR2MBGySxDLrjg0LWN6sK7wNX
x0YVvtz/zbIkPjfkU1jHS+9EbVNj+D1XF0JuaQIDAQABaoIBABagpxpM1aoLWfVd
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNUDE6SFthOar69jp5RLLwD1NhPx3iB1
J9nOM80J0VToum43UOS8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52y0Q9q0kwFTEQpjtf4uNtJom+asvLpmS8A
vLY9r60wYSvmZhNqBURj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51s0mama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRhORT
8c8hAuRBb2G82so8vUHK/fur850Efc9TncnCY2cprpoqsgHfKLxrLgtT+qDpfZnx
SatLdt8GfQ85yA7hnWwJ2Mx3NaeSDm75Lsm+tBbAiyC9P2jGRNTMSKcgYEAypHd
HCctNi/FwjuLhttFx/rHYKhLidZDFYeIE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enCivGCSx+X3L5SiWg0A
R57hJglezIiVjv3aGwHwvLZvtszK6zV6oXFAu0ECgYAbjo46T4hyP5tJi93V5Hdi
TtieK7xRVxUL+iU7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFMLy9FL2m9oQWCg
R8VdwsK8r9FGLS+9aKcV5PI/WEKlwgXinB30hYimtiG2Cg5JCqIZFHxD6MjEG0iu
L8ktHMPvodBwNsSBULpG0QKBgBAPLTFc1H0nWlMGOU3KPwYwt006CdTkmJ0mL8Ni
blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU
Y0djHdS0oKvDQNWu6ucyLRAWFuISexw9a/9p7ftpxm0TSgyvmfLF2MIAEwyzRqaM
77pBAoGAMmjmIJdjp+Ez8duyn3ieo36yrttF5NSsJLABxPpdlc1gvtGCWW+9Cq0b
dxviW8+TFVEB1104f7Hvm6EpTscdDxU+bCXWkfjuRb7Dy9Gott9JPsX8MBTakzh3
vBgsyi/sN3RqRBcGU40f0oZyFAMT8s1m/uYv5206IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----
```

Level 17:

```
bandit17@bandit:~$ ls
passwords.new passwords.old
bandit17@bandit:~$ diff passwords.old passwords.new
42c42
< p6ggwdNHncmCNxuAt0KtKVq185ZU7AW
---
> hga5tuuCLF6fFzUpnagiMN8ssu9LFRdg
bandit17@bandit:~$
```

Password: hga5tuuCLF6fFzUpnagiMN8ssu9LFRdg

Level 18:


```
bandit21@bandit:~$ cd /etc/cron.d
bandit21@bandit:/etc/cron.d$ ls -la
total 56
drwxr-xr-x  2 root root  4096 Oct  5 06:20 .
drwxr-xr-x 106 root root 12288 Oct  5 06:20 ..
-rw-r--r--  1 root root   62 Oct  5 06:19 cronjob_bandit15_root
-rw-r--r--  1 root root   62 Oct  5 06:19 cronjob_bandit17_root
-rw-r--r--  1 root root  120 Oct  5 06:19 cronjob_bandit22
-rw-r--r--  1 root root  122 Oct  5 06:19 cronjob_bandit23
-rw-r--r--  1 root root  120 Oct  5 06:19 cronjob_bandit24
-rw-r--r--  1 root root   62 Oct  5 06:19 cronjob_bandit25_root
-rw-r--r--  1 root root  201 Jan  8 2022 e2scrub_all
-rwx-----  1 root root   52 Oct  5 06:20 otw-tmp-dlr
-rw-r--r--  1 root root  102 Mar 23 2022 .placeholder
-rw-r--r--  1 root root  396 Feb  2 2021 sysstat
bandit21@bandit:/etc/cron.d$ cat cronjob_bandit22
@reboot bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
* * * * * bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
bandit21@bandit:/etc/cron.d$ cat /usr/bin/cronjob_bandit22.sh
#!/bin/bash
chmod 644 /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv
cat /etc/bandit_pass/bandit22 > /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv
bandit21@bandit:/etc/cron.d$ cat /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv
WdDozAdTM2z9DiFEQ2mGlnwMfj4EZff
bandit21@bandit:/etc/cron.d$
```

Ở đây đọc file `/usr/bin/cronjob_bandit22.sh` ta thấy password cần tìm được ghi vào file khác ở thư mục `/tmp`, ta chỉ cần cat file đó là lấy được **password**

Password: WdDozAdTM2z9DiFEQ2mGlnwMfj4EZff

Level 22:

```
bandit22@bandit:~$ cd /etc/cron.d
bandit22@bandit:/etc/cron.d$ ls -la
total 56
drwxr-xr-x  2 root root  4096 Oct  5 06:20 .
drwxr-xr-x 106 root root 12288 Oct  5 06:20 ..
-rw-r--r--  1 root root   62 Oct  5 06:19 cronjob_bandit15_root
-rw-r--r--  1 root root   62 Oct  5 06:19 cronjob_bandit17_root
-rw-r--r--  1 root root  120 Oct  5 06:19 cronjob_bandit22
-rw-r--r--  1 root root  122 Oct  5 06:19 cronjob_bandit23
-rw-r--r--  1 root root  120 Oct  5 06:19 cronjob_bandit24
-rw-r--r--  1 root root   62 Oct  5 06:19 cronjob_bandit25_root
-rw-r--r--  1 root root  201 Jan  8 2022 e2scrub_all
-rwx-----  1 root root   52 Oct  5 06:20 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:/etc/cron.d$ cat cronjob_bandit23
@reboot bandit23 /usr/bin/cronjob_bandit23.sh &> /dev/null
* * * * * bandit23 /usr/bin/cronjob_bandit23.sh &> /dev/null
bandit22@bandit:/etc/cron.d$ cat /usr/bin/cronjob_bandit23.sh
#!/bin/bash

myname=$(whoami)
mytarget=$(echo I am user $myname | md5sum | cut -d ' ' -f 1)

echo "Copying passwordfile /etc/bandit_pass/$myname to /tmp/$mytarget"

cat /etc/bandit_pass/$myname > /tmp/$mytarget
bandit22@bandit:/etc/cron.d$ echo I am user bandit23 | md5sum | cut -d ' ' -f 1
8ca319486bfbbc3663ea0fbe81326349
bandit22@bandit:/etc/cron.d$ cat /tmp/8ca319486bfbbc3663ea0fbe81326349
QYw0Y2aiA672PsMmh9puTQuhoz8SyR2G
bandit22@bandit:/etc/cron.d$
```

Ta thấy là ở đây password mình cần lấy được ghi vào 1 file, tên file này được tính bằng cách **md5sum** 1 chuỗi string như hình. Do đó ta chỉ cần làm tương tự để có được mã **md5sum**, và thực hiện cat file đó ở thư mục **/tmp**

Password: QYw0Y2aiA672PsMmh9puTQuhoz8SyR2G

Level 23:

```
bandit23@bandit:~$ cd /etc/cron.d
bandit23@bandit:/etc/cron.d$ ls -la
total 56
drwxr-xr-x  2 root root  4096 Oct  5 06:20 .
drwxr-xr-x 106 root root 12288 Oct  5 06:20 ..
-rw-r--r--  1 root root    62 Oct  5 06:19 cronjob_bandit15_root
-rw-r--r--  1 root root    62 Oct  5 06:19 cronjob_bandit17_root
-rw-r--r--  1 root root   120 Oct  5 06:19 cronjob_bandit22
-rw-r--r--  1 root root   122 Oct  5 06:19 cronjob_bandit23
-rw-r--r--  1 root root   120 Oct  5 06:19 cronjob_bandit24
-rw-r--r--  1 root root    62 Oct  5 06:19 cronjob_bandit25_root
-rw-r--r--  1 root root   201 Jan  8 2022 e2scrub_all
-rwx-----  1 root root    52 Oct  5 06:20 otw-tmp-dlr
-rw-r--r--  1 root root   102 Mar 23 2022 .placeholder
-rw-r--r--  1 root root   396 Feb  2 2021 sysstat
bandit23@bandit:/etc/cron.d$ 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:/etc/cron.d$ cat /usr/bin/cronjob_bandit24.sh
#!/bin/bash

myname=$(whoami)

cd /var/spool/$myname/foo
echo "Executing and deleting all scripts in /var/spool/$myname/foo:"
for i in * .*;
do
    if [ "$i" != "." -a "$i" != ".." ];
    then
        echo "Handling $i"
        owner="$(stat -f "%U" "$i")"
        if [ "$owner" = "bandit23" ]; then
            timeout -s 9 60 ./$i
        fi
        rm -f ./$i
    fi
done

bandit23@bandit:/etc/cron.d$ mkdir /tmp/Hjn4
bandit23@bandit:/etc/cron.d$ touch /tmp/Hjn4/passwd.txt
bandit23@bandit:/etc/cron.d$ touch /tmp/Hjn4/script-get-passwd.sh
bandit23@bandit:/etc/cron.d$ chmod 777 /tmp/Hjn4/passwd.txt
bandit23@bandit:/etc/cron.d$ chmod 777 /tmp/Hjn4/script-get-passwd.sh
bandit23@bandit:/etc/cron.d$ echo "#! /bin/bash" > /tmp/Hjn4/script-get-passwd.sh
bandit23@bandit:/etc/cron.d$ echo "cat /etc/bandit_pass/bandit24 > /tmp/Hjn4/passwd.txt" >> /tmp/Hjn4/script-get-passwd.sh
bandit23@bandit:/etc/cron.d$ cp /tmp/Hjn4/script-get-passwd.sh /var/spool/bandit24/foo/script-get-passwd.sh
bandit23@bandit:/etc/cron.d$ cat /tmp/Hjn4/passwd.txt
VAfGXJ1PBSSpSnvsjI8p759leLZ9GGar
bandit23@bandit:/etc/cron.d$
```

Đọc code trong file **cronjob_bandit24** ta nhận thấy là file **/usr/bin/cronjob_bandit24.sh** sẽ được thực thi mỗi phút.

Script này sẽ tiến hành xóa các file trong thư mục **/var/spool/bandit24/foo**. Tuy nhiên nếu chủ sở hữu file đó là **bandit23** thì nó sẽ đợi 60s, rồi thực thi file đó.

Do đó để lấy được password, ta sẽ cần đưa vào thư mục **/var/spool/bandit24/foo** 1 file do ta tạo ra hiện đang là user **bandit23**. Do là file này sẽ thực thi nên là ta cần set quyền cho nó, để suôn sẻ mọi thứ thì ta cứ set full quyền 777 cho các file.

Thì file ta tạo ra để đẩy vào thư mục **/var/spool/bandit24/foo** có sẽ thực hiện **cat /etc/bandit_pass/bandit24** và ghi vào file **passwd.txt**

Đợi tầm 60s, cat lại file **passwd.txt**

Password: VAfGXJ1PBSSpSnvsjI8p759leLZ9GGar

Level 24:

```
bandit24@bandit:~$ cd /tmp
bandit24@bandit:/tmp$ mkdir bf_lv24
bandit24@bandit:/tmp$ cd bf_lv24
bandit24@bandit:/tmp/bf_lv24$ vi bf.sh
bandit24@bandit:/tmp/bf_lv24$ chmod +x bf.sh
bandit24@bandit:/tmp/bf_lv24$ ./bf.sh
Trying combination 0000
Trying combination 0001
Trying combination 0002
Trying combination 0003
Trying combination 0004
Trying combination 0005
Trying combination 0006
```

```
17
18 #!/bin/bash
19
20 for i in {0000..9999}
21 do
22     echo "Trying combination $i"
23     response=$(echo "VAfGXJ1PBSSsPSnvsjI8p759leLZ9GGar $i" | timeout 0.6s nc localhost 30002)
24     echo "$response" >> /tmp/bf_lv24/result.txt
25 done
26
```

Kết quả:

```
bandit24@bandit:/tmp/bf_lv24$ cat result.txt | sort | uniq -u
Correct!
Exiting.
The password of user bandit25 is p7TaowMYrmu230l8hiZh9UvD009hpx8d
bandit24@bandit:/tmp/bf_lv24$
```

Password: p7TaowMYrmu230l8hiZh9UvD009hpx8d

Level 25:

```
bandit25@bandit:~$ ls
bandit26.sshkey
bandit25@bandit:~$ pwd
/home/bandit25
bandit25@bandit:~$ cat bandit26.sshkey
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEApis2AuoooEqeYWamtWx2k5z9uU1Afl2F8VyXQqbv/LTrIwdW
pTfaeRHXzr0Y0a50e3GB/+W2+PREif+bPZLzTY1XFwpk+DiHk1kmL0moEW8HJuT9
/5XbnpjSzn0eEafFax20copjrzVqdBJQerkj0puv3UXY07AskgyD5XepwGALJOG
xZsMq1oZQ0W29aBtFykuGie2bxroRjuAPrYM4o3MMmtlNE5fC4G9Ihq0eq73MDi
1ze6d2jIGce873qxn308BA2qhRPJNEbnPev5gI+5tU+UxebW8KLbk0EhoXB953Ix
3lg0IrT9Y6sKRjsMSFmC6WN/07ovu8QzGqxdyWIDAQABAoIBAAXoETtVT9GtpHW
qlaKHgYtLE01t0F0hInWyolyZgL4inuRRva3CivVEWK6TcnDyILNL4MfcerehwGi
il4fQFvLR7E6UFcopvhJiSJHicvPQ9FfNFR3dYcNOQ/IFvE73bEqMwSISpWlel6w
eDjF3C7jHaS1s9PJWfN982aublL/yLbJP+ou3ifdljS7QzjWZA8NRlMwmBGPIh
Yq8weR3jIVQl3ndEYx07Cr/wXXebZWlP6CPZb67rBy0jg+366mxQbDZiWZYEaUME
zY5izFclr/kkj4s7NTRkC76Yx+rTNP5+BX+JT+rgz5aoQq8ghMw43NYwxjXym/MX
c8X8g0ECgYEA1crBUAR1gSkM+5mGjjoFLJKrFP+IhUHFh25qGI4Dcxxh1f3M53le
wF1rkp5S3JnHRFm9IW3gM1JoF0PQxI5aXHRGHphwPeKnsQ/xQBRWCEypqTme9amJV
tD3aDhKpIhYxkNxpQl5gDCat6tdFSxqPaNfdfsfaA0XlKGrQESUjIBcCgYEAxvmI
2R0J5BxalM4Iyg9hUpjZin8TW2ULH76pojFG6/KBD1NcnW3fu0ZUU790wAu7Qbbu
i7pieeqCqSYcZsmkh0vbdx54A6NNCR2btcsil6pD0e1jdsGdXISDRHFb9QxjZCj
6xzWMNvb5n1yUb9w9nFN1PZzATfUsOV+FY8CbG0CgYEAIfkTLwfhqZyLk2huTSWm
pzB0ltWfDpJ22MNqVzR3h3d+shLeJVjPzIe9396rF8KGdNsWslWpnJMKDjgZsz
JQBmMc6UMYRARVP1dIKANN4eY0FSHFEEbHcqXLho0mXOUTXe37DWfZza5V90ifY3
JquBd8uUptW1Ue41H4t/ErsCgYEArc5FYtF1QXIlfcDz3oUGz16itUZpgzlb71nd
1cbTm8EupCwR5I1j+IEQU+JTUQyI1nwWcnKwZI+5kBbKNUU/mLsRyY/UXYxEZh
ibrNklm94373kV1US/0DLZUDCQba7jz9Yp/C3dT/RlwoIw5mP3UxQCizFspNK0Se
euPeaxUCgYEAntklXwBbokgdDup/u/3ms5Lb/bm22zD0Cg2HrLWQCqKEkKKA06R5
/Wwyqhp/wTL8VXjxWo+W+DmewGdPHGQQ5FFdqqpuQpGUQ24YZS8m66v5ANBwd76t
IZdtFSHXS2S5CADTwniUS5mX1H09L5gUkk+h0cH5JnPtsMCAUM+BRY=
-----END RSA PRIVATE KEY-----
bandit25@bandit:~$ pwd
/home/bandit25
bandit25@bandit:~$
logout
Connection to bandit.labs.overthewire.org closed.

[~] > ~ 4m 13s 04:24:39 PM
scp -P 2220 bandit25@bandit.labs.overthewire.org:/home/bandit25/bandit26.sshkey /home/hjn4/bandit26.sshkey

[~] > ~ 16s 04:25:42 PM

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

bandit25@bandit.labs.overthewire.org's password:
bandit26.sshkey 100% 1679 6.2KB/s 00:00
```

Ta thấy code file sshkey, nên tiến hành copy về máy mình, và thực hiện ssh với file key đó

```
ssh -i bandit26.sshkey bandit26@bandit.labs.overthewire.org -p 2220
```



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

bandit26

www. ver he " ire.org

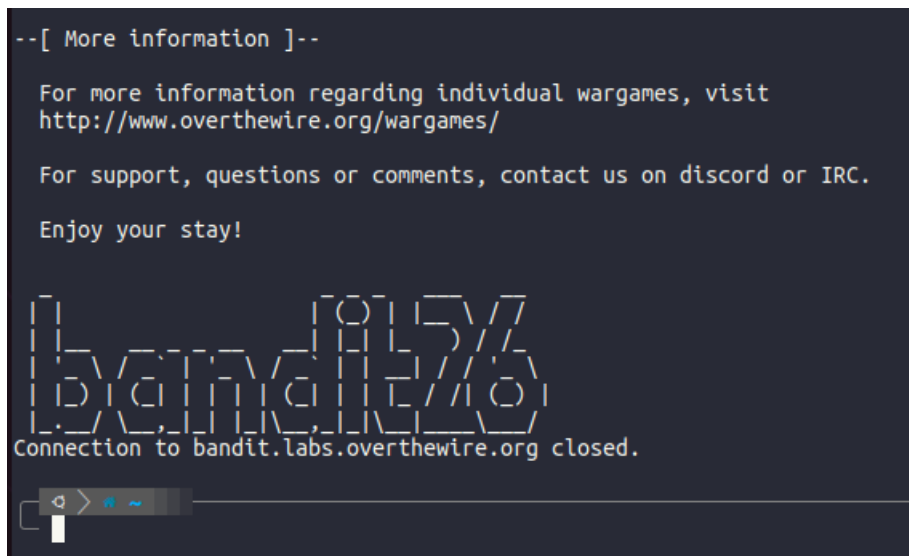
Welcome to OverTheWire!

```
--[ 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.

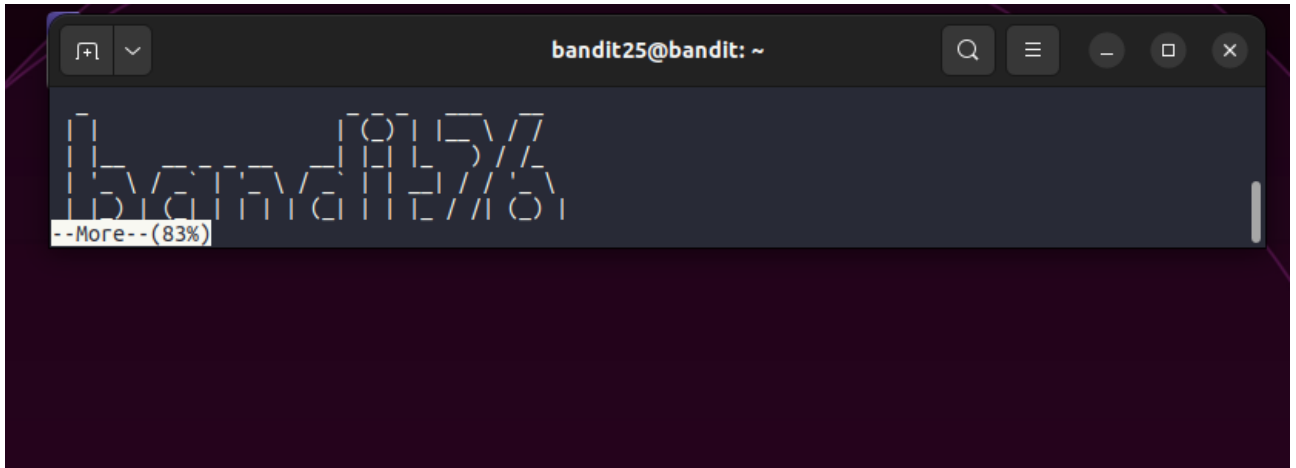
Enjoy your stay!



bandit26

Connection to bandit.labs.overthewire.org closed.

Tuy nhiên thì chưa có gì đã bị closed

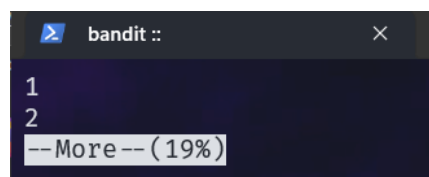


Ta thấy **more** có 1 cơ chế là giúp cho việc đọc dữ liệu dễ dàng hơn, ví dụ:

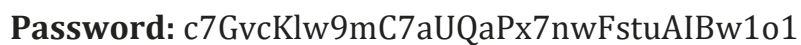
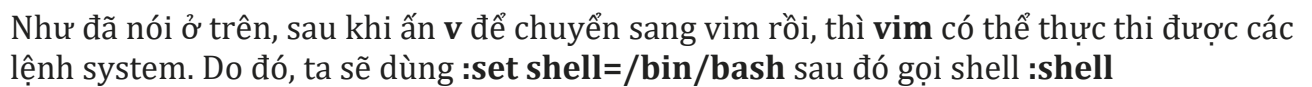
Đây là ví dụ về **more** và **cat** thì ở terminal đủ to để hiển thị dữ liệu sẽ trông như này



Tuy nhiên chỉ cần thu nhỏ terminal thì:



Khi đang ở chế độ này ta có thể ấn **v** để có thể chuyển sang **vim**



```

|||               |O| | \ \
| \_ / \_ / \_ / \_ / | | | \ \
|O| |O| | | | | |O| | \_ / \_ /
:shell
bandit26@bandit:~$ ls
bandit27-do  text.txt
bandit26@bandit:~$ ./bandit27-do
Run a command as another user.
Example: ./bandit27-do id
bandit26@bandit:~$ ./bandit27-do cat /etc/bandit_pass/bandit27
YnQpBuifNMas1hcUFk70ZmqkhUU2EuaS

```

Ta vẫn dùng shell của lv25. Ta thấy có file thực thi **bandit27-do** ta thực thi thử thì thấy nó bảo là dùng lệnh này như người dùng khác. Do đó ta sẽ dùng để cat password như trên.

Password: YnQpBuifNMas1hcUFk70ZmqkhUU2EuaS

Level 27:

```
bandit27@bandit: /tmp/Hjn4/repo
bandit27@bandit:/tmp$ mkdir Hjn4 ; cd Hjn4
bandit27@bandit:/tmp/Hjn4$ 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: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/bandit27/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit27/.ssh/known_hosts).

  _ _ _ _ _
 | b | a | n | d | i | t |
 | _ | _ | _ | _ | _ |
  _ _ _ _ _

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/Hjn4$ ls
repo
bandit27@bandit:/tmp/Hjn4$ cd repo/ ; ls
README
bandit27@bandit:/tmp/Hjn4/repo$ cat README
The password to the next level is: AVanL161y9rsbcJIsFHuw35rjaOM19nR
bandit27@bandit:/tmp/Hjn4/repo$
```

Đơn giản là clone repo về và read file README.md

Password: AVanL161y9rsbcJIsFHuw35rjaOM19nR

Level 28:


```
bandit28@bandit:/tmp/bandit28/repo$ git log
commit 14f754b3ba6531a2b89df6ccae6446e8969a41f3 (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/bandit28/repo$ git show 14f754b3ba6531a2b89df6ccae6446e8969a41f3
commit 14f754b3ba6531a2b89df6ccae6446e8969a41f3 (HEAD -> master, origin/master, origin/HEAD)
Author: Morla Porla <morla@overthewire.org>
Date: Thu Oct 5 06:19:41 2023 +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

bandit28@bandit:/tmp/bandit28/repo$
```

Ta dùng **git log** để xem log các commits

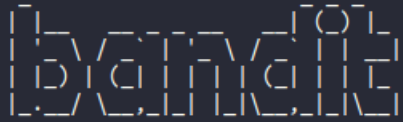
Ta thấy là có 1 commit với nội dung “fix info leak”.

Dùng **git show <id commit>** thế là ta có được password

Password: tQKvmcwNYcFS6vmPHIUSI3ShmsrQZK8S

 **Level 29:**

```
bandit29@bandit:~$ mkdir /tmp/bandit29 ; cd /tmp/bandit29
bandit29@bandit:/tmp/bandit29$ 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/ureryLY.
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/bandit29$ ls
repo
bandit29@bandit:/tmp/bandit29$ cd repo
bandit29@bandit:/tmp/bandit29/repo$ ls
README.md
bandit29@bandit:/tmp/bandit29/repo$ cat README.md
# Bandit Notes
Some notes for bandit30 of bandit.

## credentials

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

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

## credentials

- username: bandit30
- password: xbhV3HpNGlTIdnjUrdAlPzc2L6y9EOnS
bandit29@bandit:/tmp/bandit29/repo$
```

Ở đây ta dùng **git branch -a** để show ra các branch hiện có

Dùng **git checkout dev** để nhảy sang nhánh **dev** để kiểm tra thử

Đọc file **README.md** và ta có được password

Password: xbhV3HpNGlTIdnjUrdAlPzc2L6y9EOOnS

🚩 Level 30:

```
bandit30@bandit:~$ mkdir /tmp/bandit30 ; cd /tmp/bandit30
bandit30@bandit:/tmp/bandit30$ git clone ssh://bandit30-git@localhost:2220/home/bandit30-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/bandit30/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit30/.ssh/known_hosts).

[ _ _ _ _ _ ]
[ _ _ _ _ _ ]
[ _ _ _ _ _ ]
[ _ _ _ _ _ ]
[ _ _ _ _ _ ]

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

bandit30-git@localhost's password:
remote: Enumerating objects: 4, done.
remote: Counting objects: 100% (4/4), done.
remote: Total 4 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (4/4), done.
bandit30@bandit:/tmp/bandit30$ ls
repo
bandit30@bandit:/tmp/bandit30$ cd repo/
bandit30@bandit:/tmp/bandit30/repo$ ls
README.md
bandit30@bandit:/tmp/bandit30/repo$ cat README.md
just an empty file... muahaha
bandit30@bandit:/tmp/bandit30/repo$ git tag
secret
bandit30@bandit:/tmp/bandit30/repo$ git show secret
OoffzGDLzhAlerFJ2cAiz1D41JW1Mhmt
bandit30@bandit:/tmp/bandit30/repo$
```

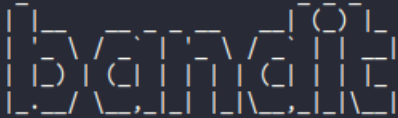
Ở đây thì tag được dùng để đánh dấu các commit, dễ dàng cho việc tìm kiếm sau này. Để check các tag, dùng **git tag**.

Ta thấy có tag **secret**, dùng **git show tag** ta có được password

Password: OoffzGDLzhAlerFJ2cAiz1D41JW1Mhmt

🚩 Level 31:

```
bandit31@bandit:~$ mkdir /tmp/bandit31 ; cd /tmp/bandit31
bandit31@bandit:/tmp/bandit31$ 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).
```



```

      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/bandit31$ cd repo/ ; ls
README.md
bandit31@bandit:/tmp/bandit31/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

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



```
bandit31@bandit:/tmp/bandit31/repo$ cat key.txt
May I come in?
bandit31@bandit:/tmp/bandit31/repo$ git add -f key.txt
bandit31@bandit:/tmp/bandit31/repo$ git commit -m "hjn4"
[master 7130b33] hjn4
1 file changed, 1 insertion(+)
create mode 100644 key.txt
bandit31@bandit:/tmp/bandit31/repo$ git push origin master
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).

      _ _ _ _ _
     | | | | | |
    | | | | |
   | | | | |
  | | | | |
 | | | | |
|_|_|_|_|_|

      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), 318 bytes | 318.00 KiB/s, done.
Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
remote: ### Attempting to validate files... ###
remote:
remote: .o0o.o0o.o0o.o0o.o0o.o0o.o0o.o0o.o0o.o0o.
remote:
remote: Well done! Here is the password for the next level:
remote: rmCBvG56y58BXzv98yZGdO7ATVL5dW8y
remote:
remote: .o0o.o0o.o0o.o0o.o0o.o0o.o0o.o0o.o0o.o0o.
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/repo$
```

Ở đây đơn giản là tạo file key.txt với content như yêu cầu, add, commit và push

Password: rmCBvG56y58BXzv98yZGdO7ATVL5dW8y

🚩 Level 32:


```
WELCOME TO THE UPPERCASE SHELL
>> clear
sh: 1: CLEAR: Permission denied
>> ls
sh: 1: LS: Permission denied
>> $0
$ whoami
bandit33
$ ls -la
total 36
drwxr-xr-x  2 root    root    4096 Oct  5 06:19 .
drwxr-xr-x 70 root    root    4096 Oct  5 06:20 ..
-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 bandit32 15128 Oct  5 06:19 uppershell
$ cat /etc/bandit_pass/bandit33
odHo63fHiFqcWWJG9rLiLDtPm45KzUKy
$
```

- Ta có thể thấy các lệnh thông thường sẽ bị in hoa lên, do đây không còn là shell thông thường nữa.
- Do đó để trở lại cái shell /bin/bash hay zsh như thông thường thì thay vì gõ **zsh** sẽ bị in hoa thành **ZSH**, ta có thể gõ **\$0**
- **\$0** là biến chứa tên của shell.

```
echo $0
zsh
```

- Do đó khi ta gõ **\$0** thì tức đang gọi đến shell trong trường hợp này là **sh**

Password: odHo63fHiFqcWWJG9rLiLDtPm45KzUKy

🚩 Level 33:

```
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!
bandit33@bandit:~$
```

The end! Love your challs

HẾT