Bandit을 통해 배운 내용으로 **picoCTF**풀기

목차

-주요한 밴딧 문제 풀이와 명령어

-picoCTF를 통한 복습

Cat ./-

Level1. 상대경로

```
bandit1@bandit:~$ cat ./-
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
bandit1@bandit:~$
```

Cat

Level2. 파일이름공백

```
bandit2@bandit:~$ cat "spaces in this filename"
UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK
bandit2@bandit:~$
```

```
bandit2@bandit:~$ cat spaces\ in\ this\ filename
UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK
bandit2@bandit:~$
```

file

Level4. 메타문자*

```
bandit4@bandit:~/inhere$ file ./*
./-file00: data
./-file01: data
./-file02: data
./-file03: data
./-file04: data
./-file05: data
./-file06: data
./-file07: ASCII text
./-file08: data
./-file09: data
bandit4@bandit:~/inhere$ cat ./-file07
koReBOKuIDDepwhWk7jZC0RTdopnAYKh
bandit4@bandit:~/inhere$
```

비슷한 ?도 설명추가필

find

Level5. size,숨김파일

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

```
bandit5@bandit:~/inhere/maybehere07$ cat .file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7
```

find

Level6. redirection

```
find: '/var/spool/bandit24': Permission denied
find: '/var/spool/cron/crontabs': Permission denied
find: '/var/spool/rsyslog': Permission denied
find: '/var/tmp': Permission denied
find: '/var/lib/apt/lists/partia[redacted] Permission denied
find: '/var/lib/polkit-1': Permission denied
/var/lib/dpkg/info/bandit7.password
find: '/var/log': Permission denied
find: '/var/cache/apt/archives/partial': Permission denied
find: '/var/cache/ldconfig': Permission denied
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c^C
bandit6@bandit:~$ ^C
bandit6@bandit:~$ ^C
bandit6@bandit:~$ ^C
bandit6@bandit:~$ cd /var/lib/dpkg/info/bandit7.password
-bash: cd: /var/lib/dpkg/info/bandit7.password: Not a directory
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs
```

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

grep

Level7.

```
unbolting       ZT3DWRG5Xxpk5gP5kIZEFX9xbSP38ZEA
medley's        3q5mIH78Z6GcYtaNoMV5H2CSBnWEtGVc
modicums        0XeHP6ftqaz3bnaMJ1PVj1AAm6AH9PmP
wardrobes       RQDRMHxUcj9nRnXRlwvL7RjJRXInNEon
foolisher       r0OI3S1rFXs34imOe19mw0iOhnR6jy4e
assessor        PNQVYrR7lvhBBABXWKuulWFljHpxLtKi
phalanx's       3pXGFxqDqZ03MpyvJxUzasOAJQozUv7m
Jimmy's yqCF9lL9Xmtqmpf2kFfw2EDopM4sII5X
hoof    LgoZ6ChOfRyGYhNQP07Zm3UO3SEeaq4z
cellular        5OeOj4qcncuYsZ2yblP0EFXjfzhdoNBQ
annotations     AbhvqJmHuJ9C8lzalUwUjkIdfINE13z2
starved HrMrGnXJUsYmlOwSC453dah2vZmU26NH
router's        YG3JEBoJakBltrlkmrM3xTHWlY3Y97L9
contaminant's   3jAyfygEovAUAyqSdrQ2KQPHQNjyL1QV
spermicide's    k7jelY3TAXdlO6MJE8fw20qQpiUjbzXy
intaglio's      WpDQUcOYT7Szx3pAmYNIESUBQWhEu3h2
herringboning   IQx3N6pUQh5AhWW8U5e92DVuGCUA5DaL
Volkswagen's    mjVcavl0qTrUDmqC3dBrFgWXVCX9Q8hk
quarterback     WdH0nWNPBbGUiKfA8GDxNwsYfp3Ke3VV
encampments     7idPfiatkvHK7bILqSKwP4DsWBcuvlAi
```

```
bandit7@bandit:~$ grep millionth
^Z
[4]+  Stopped                 grep millionth
bandit7@bandit:~$ grep -r "millionth"
data.txt:millionth      cvX2JJa4CFALtqS87jk27qwqGhBM9plV
```

Sort,uniq

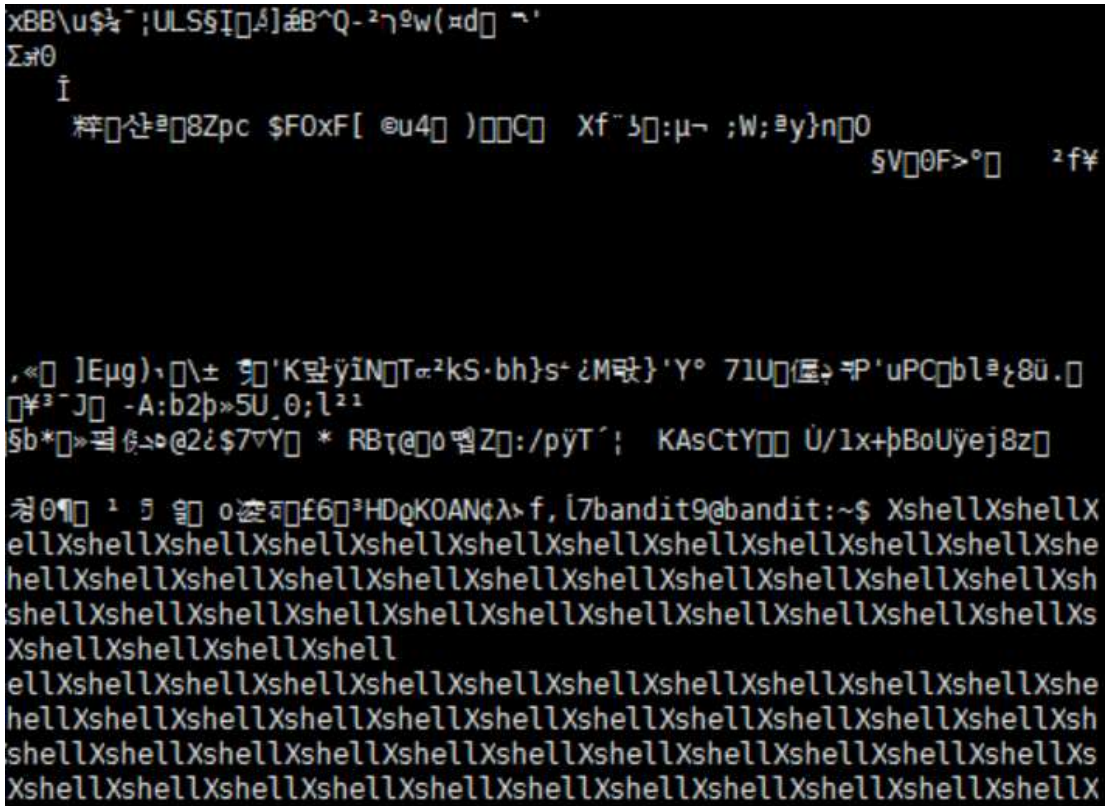
Level8. 파이프라인

```
mpgNGRH628hTQxajScbagkxaPKklUhjn
VkBAEWyIibVkeURZV5mowiGg6i3m7Be0
UJiCNvDNfgb3fcCj8PjjnAXHqUM63Uyj
VkBAEWyIibVkeURZV5mowiGg6i3m7Be0
w4zUWFGTUrAAh8lNkS8gH3WK2zowBEkA
aR2QhaBoDMncvJqPWkvLXMzEx9meBIbX
TThRArdF2ZEXM047TIYkyPPLtvzzLcDf
v9zaxkVAOdIOlITZY2uoCtBlfX2gmly9
Ef509iQpb5gQJsjz5dMXLxpeAfkbLOrw
07KC3ukwX7kswl8Le9ebb3H3sOoNTsR2
```

```
bandit8@bandit:~$ cat data.txt | sort | uniq -u
UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR
```

grep

Level9.바이너리파일



strings

strings, |, grep

```
alpaca@ubuntu:~/Downloads$ strings strings | grep "pico"
picoCTF{sTrIngS_sAVeS_Time_d3ffa29c}
alpaca@ubuntu:~/Downloads$
```

pipe

nc, |, grep

```
alpaca@ubuntu:~/Downloads$ nc 2018shell.picoctf.com 44310 | grep "pico"
picoCTF{almost_like_mario_a13e5b27}
```

Aca-shell-A

rm, whoami, cp

```
Sweet! We have gotten access into the system but we aren't root.
It's some sort of restricted shell! I can't see what you are typing
but I can see your output. I'll be here to help you along.
If you need help, type "echo 'Help Me!'" and I'll see what I can do
There is not much time left!
~/$ ls
blackmail
executables
passwords
photos
secret
~/$ echo 'Help me!'
```

```
Srmabatoge them! Get rid of all their intel files!
~/secretrm intel_1
Nice! Once they are all gone, I think I can drop you a file of an exploit!
Just type "echo 'Drop it in!' " and we can give it a whirl!
~/secret$ echo 'Drop it in!'
Drop it in!
I placed a file in the executables folder as it looks like the only place we can
 execute from!
Run the script I wrote to have a little more impact on the system!
```

```
Now that you can look at files, can you enter any?
~/$ ls
blackmail
executables
passwords
photos
secret
~/$ cd secret
Now we are cookin'! Take a look around there and tell me what you find!
```

```
Looking through the text above, I think I have found the password. I am just hav
ing trouble with a username.
Oh drats! They are onto us! We could get kicked out soon!
Quick! Print the username to the screen so we can close are backdoor and log int
o the account directly!
You have to find another way other than echo!
~/executables$ whoami
l33th4x0r
Perfect! One second!
Okay, I think I have got what we are looking for. I just need to to copy the fil
e to a place we can read.
Try copying the file called TopSecret in tmp directory into the passwords folder
.
```

```
~/$ cp /tmp/TopSecret passwords
Server shutdown in 10 seconds...
Quick! go read the file before we lose our connection!
~/$ cd passwords
~/passwords$ ls
TopSecret
~/passwords$ cat TopSecret
Major General John M. Schofield's graduation address to
1879 at West Point is as follows: The discipline which
ree country reliable in battle is not to be gained by h
ent.On the contrary, such treatment is far more likely
n army.It is possible to impart instruction and give co
nd such a tone of voice as to inspire in the soldier no
```

```
picoCTF{CrUsHeD_It_dddcec58}
```

grep

Level7.

```
unbolting       ZT3DWRG5Xxpk5gP5kIZEFX9xbSP38ZEA
medley's        3q5mIH78Z6GcYtaNoMV5H2CSBnWEtGVc
modicums        0XeHP6ftqaz3bnaMJ1PVj1AAm6AH9PmP
wardrobes       RQDRMHxUcj9nRnXRlwvL7RjJRXInNEon
foolisher       r0OI3S1rFXs34imOe19mw0iOhnR6jy4e
assessor        PNQVYrR7lvhBBABXWKuulWFljHpxLtKi
phalanx's       3pXGFxqDqZ03MpyvJxUzasOAJQozUv7m
Jimmy's yqCF9lL9Xmtqmpf2kFfw2EDopM4sII5X
hoof    LgoZ6ChOfRyGYhNQP07Zm3UO3SEeaq4z
cellular        5OeOj4qcncuYsZ2yblP0EFXjfzhdoNBQ
annotations     AbhvqJmHuJ9C8lzalUwUjkIdfINE13z2
starved HrMrGnXJUsYmlOwSC453dah2vZmU26NH
router's        YG3JEBoJakBltrlkmrM3xTHWlY3Y97L9
contaminant's   3jAyfygEovAUAyqSdrQ2KQPHQNjyL1QV
spermicide's    k7jelY3TAXdlO6MJE8fw20qQpiUjbzXy
intaglio's      WpDQUcOYT7Szx3pAmYNIESUBQWhEu3h2
herringboning   IQx3N6pUQh5AhWW8U5e92DVuGCUA5DaL
Volkswagen's    mjVcavl0qTrUDmqC3dBrFgWXVCX9Q8hk
quarterback     WdH0nWNPBbGUiKfA8GDxNwsYfp3Ke3VV
encampments     7idPfiatkvHK7bILqSKwP4DsWBcuvlAi
```

```
bandit7@bandit:~$ grep millionth
^Z
[4]+  Stopped                 grep millionth
bandit7@bandit:~$ grep -r "millionth"
data.txt:millionth      cvX2JJa4CFALtqS87jk27qwqGhBM9plV
```

grep

Level7.

```
unbolting       ZT3DWRG5Xxpk5gP5kIZEFX9xbSP38ZEA
medley's        3q5mIH78Z6GcYtaNoMV5H2CSBnWEtGVc
modicums        0XeHP6ftqaz3bnaMJ1PVj1AAm6AH9PmP
wardrobes       RQDRMHxUcj9nRnXRlwvL7RjJRXInNEon
foolisher       r0OI3S1rFXs34imOe19mw0iOhnR6jy4e
assessor        PNQVYrR7lvhBBABXWKuulWFljHpxLtKi
phalanx's       3pXGFxqDqZ03MpyvJxUzasOAJQozUv7m
Jimmy's yqCF9lL9Xmtqmpf2kFfw2EDopM4sII5X
hoof    LgoZ6ChOfRyGYhNQP07Zm3UO3SEeaq4z
cellular        5OeOj4qcncuYsZ2yblP0EFXjfzhdoNBQ
annotations     AbhvqJmHuJ9C8lzalUwUjkIdfINE13z2
starved HrMrGnXJUsYmlOwSC453dah2vZmU26NH
router's        YG3JEBoJakBltrlkmrM3xTHWlY3Y97L9
contaminant's   3jAyfygEovAUAyqSdrQ2KQPHQNjyL1QV
spermicide's    k7jelY3TAXdlO6MJE8fw20qQpiUjbzXy
intaglio's      WpDQUcOYT7Szx3pAmYNIESUBQWhEu3h2
herringboning   IQx3N6pUQh5AhWW8U5e92DVuGCUA5DaL
Volkswagen's    mjVcavl0qTrUDmqC3dBrFgWXVCX9Q8hk
quarterback     WdH0nWNPBbGUiKfA8GDxNwsYfp3Ke3VV
encampments     7idPfiatkvHK7bILqSKwP4DsWBcuvlAi
```

```
bandit7@bandit:~$ grep millionth
^Z
[4]+  Stopped                 grep millionth
bandit7@bandit:~$ grep -r "millionth"
data.txt:millionth      cvX2JJa4CFALtqS87jk27qwqGhBM9plV
```

감사합니다