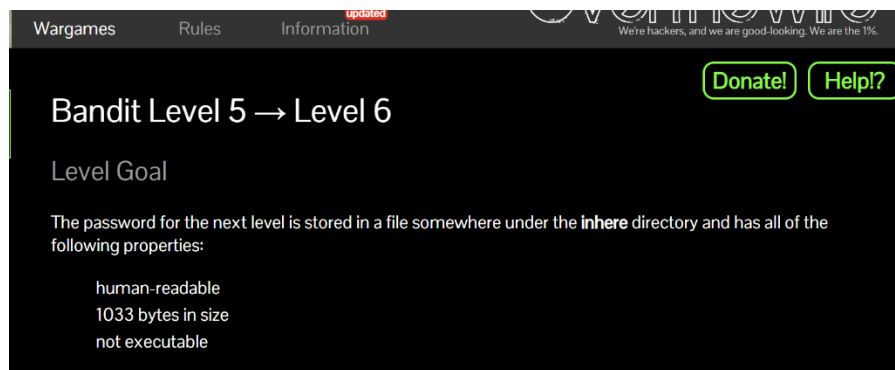


2회차 - 20. 케로로

Bandit 레벨 5 ~ 8 라이트업

정보보호학부 2024111262 조현서

Lv. 5 → 6



다음 레벨의 비밀번호는 `inhere` 디렉토리 어딘 가에 저장되어 있으며, 사람이 읽을 수 있고, 크기가 1033바이트이고, 실행할 수 없는 파일이라고 한다.

```
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls
maybehere00 maybehere02 maybehere04 maybehere06 maybehere08 maybehere10 maybehere12 maybehere14 maybehere16 maybehere18
maybehere01 maybehere03 maybehere05 maybehere07 maybehere09 maybehere11 maybehere13 maybehere15 maybehere17 maybehere19
bandit5@bandit:~/inhere$ find . -size 1033c
./maybehere07/.file2
```

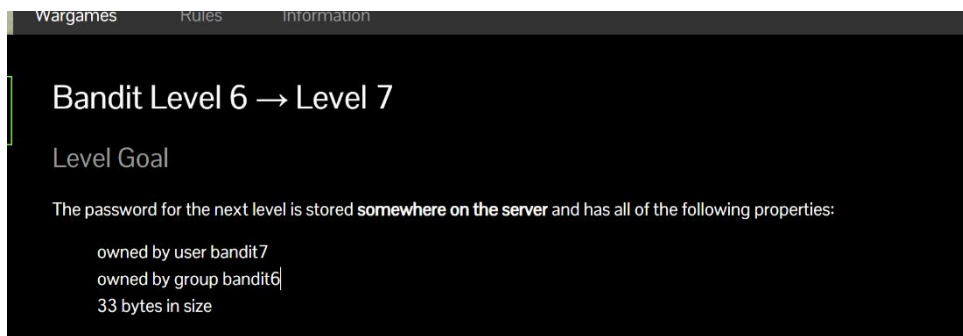
일단 “cd”를 통해, `inhere`로 이동한 후, “ls” 명령어를 입력하니, 많은 디렉토리가 나열되었다. 이 디렉토리를 하나하나 뒤져볼 수는 없기에, 명령어 “`find . -size 1033c`”를 통해, 파일 크기가 1033바이트인 파일을 출력하게끔 하였다. 해당 크기인 파일이 `maybehere07` 디렉토리에 있는 `file2` 라는 파일이라는 것을 알 수 있었다.

```
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
```

해당 파일을 "cat" 명령어를 통해 출력하니, 출력된 비밀번호는 "HWasnPhtq9AVKe0dmk45nxy20cvUa6EG" 이다.

Lv.5 → 6 해결

Lv. 6 → 7



다음 레벨의 비밀번호는 서버 어딘가에 저장되어 있고, 사용자는 bandit7이고, 그룹은 bandit6이고, 크기는 33바이트인 파일에 저장되어 있는 것으로 유추된다.

```
bandit6@bandit:~$ find / -size 33c -user bandit7 -group bandit6
find: '/drifter/drifter14_src/axTLS': Permission denied
find: '/root': Permission denied
find: '/snap': Permission denied
find: '/tmp': Permission denied
find: '/proc/tty/driver': Permission denied
find: '/proc/3633790/task/3633790/fd/6': No such file or directory
find: '/proc/3633790/task/3633790/fdinfo/6': No such file or directory
find: '/proc/3633790/fd/5': No such file or directory
find: '/proc/3633790/fdinfo/5': No such file or directory
find: '/home/bandit31-git': Permission denied
find: '/home/ubuntu': Permission denied
find: '/home/bandit5/inhere': Permission denied
find: '/home/bandit30-git': Permission denied
find: '/home/drifter8/chroot': Permission denied
find: '/home/drifter6/data': Permission denied
find: '/home/bandit29-git': Permission denied
find: '/home/bandit28-git': Permission denied
find: '/home/bandit27-git': Permission denied
find: '/lost+found': Permission denied
find: '/etc/polkit-1/rules.d': Permission denied
find: '/etc/multipath': Permission denied
find: '/etc/stunnel': Permission denied
find: '/etc/xinetd.d': Permission denied
find: '/etc/credstore.encrypted': Permission denied
find: '/etc/ssl/private': Permission denied
find: '/etc/sudoers.d': Permission denied
find: '/etc/credstore': Permission denied
find: '/dev/shm': Permission denied
find: '/dev/mqueue': Permission denied
find: '/var/log/amazon': Permission denied
find: '/var/log/unattended-upgrades': Permission denied
find: '/var/log/chrony': Permission denied
find: '/var/log/private': Permission denied
find: '/var/tmp': Permission denied
find: '/var/spool/cron/crontabs': Permission denied
find: '/var/spool/bandit24': Permission denied
find: '/var/spool/rsyslog': Permission denied
find: '/var/cache/ldconfig': Permission denied
find: '/var/cache/apt/archives/partial': Permission denied
```

서버 어딘가에 있다고 하였으니, 최상위 경로인 "/" 에서 find 명령어를 활용해 찾아보 고자 했다. "find / -size 33c -user bandit7 -group bandit6" 명령어를 입력해, 해당 속성을 만족하는 파일을 찾고자 하였다. 그 결과 수 많은 파일들이 출력되었다.

```

find: /var/lib/dpkg/info: Permission denied
bandit6@bandit:~$ find / -size 33c -user bandit7 -group bandit6 2> /dev/null
/var/lib/dpkg/info/bandit7.password
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
morbNTDkSW6jIlUc0ymOdMaLnOIFVAaj
bandit6@bandit:~$

```

이들을 보니, 대부분이 Permission Denied 된 것들이 많다. 그래서 "2> /dev/null" 을 추가적으로 입력하여, 에러난 결과를 모두 걸러지게끔 하였다. 그러더니, bandit7.password 라는 파일 하나를 발견하였다. 이를 cat 명령어로 출력하니, 비밀번호는 "morbNTDkSW6jIlUc0ymOdMaLnOIFVAaj"이다.

Lv.6 → 7 해결

Lv. 7 → 8

Bandit Level 7 → Level 8

Level Goal

The password for the next level is stored in the file **data.txt** next to the word **millionth**

Commands you may need to solve this level

man, grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd

다음 레벨의 비밀번호는 data.txt 파일에 저장되어 있으며, 단어 "millionth" 옆에 있다고 한다.

```

bandit7@bandit:~$ cat data.txt

```

```

mallard's      MTKvAaiubyq3Ie88Ulua0HY7ZgFZ4zed
barometric     sV8kzJtlqpjJn6boaaa4gtFGB6GuwhvJ
tracers 2ZITFahgp9og6GNRSOXLt46Qit3PuNvP
outflanks      YqKPcc2DzEHNqjN2I5DxyM2p06zbev bq
triumphing     gUzNHvBcDAYvRnG2a8m8Rt5q8bw776Pa
aspect's       xdoF0oK7LWNkM6eeIBwYQazCC35Zm0VM
distribute     jvQId40mRNK9w5bNSKXWG0cPn0tRlFDq
humiliation    bNtphrnEeCKgPKkAeio0uGzVKuj9Bz8h
crowds  lcLZWfW9Y1H9ijvCM1Hx2R6zvJqHgsMt
refurnishes    hFF11AaZoViObnrtdAA0TcRg9fWV3h6U
Hindi's gEPWTgmaR0cPV9Q5B69JrkqxeUDIePRj
perfumeries    RFR7ZFHI0WfyBBcQDe1G7rpHo4iGKkmV
recomence      uqAu36x9lViN0sJpqjePhp5Ty2XocPKB
complaint      Ch3MnrWSfvaR6lrPT4ZN4FbXIVbRTuUw
telekinetics's u00d6SmlsJvqbbpD2wX1urojDvGKnvna
sutured S3S5Bz1ZIALg9pWuvAez3eif9TpZ3g4T
mechanic       bmiYfQiKgQxohljoFhLGFAPGrKSfkem4
unluckiest     OXKwX7Zdo8lB82TexwVwt22GAhULh65A
obsession      SLiXncgs0tGAZnpJePzln10Jo3DELTHB
footman's      zet6GehCCq4kLxSJZS36Y6ES5ngq0n65
Filippo's      FB8VvtGT14D4hcaZr2uIKYMuY4qvEQx

```

Cat 명령어로 data.txt 파일을 불러오면, 엄청 많은 내용들이 쏟아진다. 해당 파일 내용을 출력할 때, 필터링이 필요할 거 같아서, "grep" 이라는 명령어를 활용하려고 한다.

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

비밀번호가 millionth라는 단어 옆에 있다고 하였으니, "cat data.txt | grep millionth" 명령어를 입력해보았다. 다음 단계의 비밀번호는 "**dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc**"이다.

Lv.7 → 8 해결

Lv. 8 → 9

Bandit Level 7 → Level 8

Level Goal

The password for the next level is stored in the file **data.txt** next to the word **millionth**

Commands you may need to solve this level

man, grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd

다음 레벨의 비밀번호는 data.txt 파일에 저장되어 있으며, 단 한 번만 등장하는 텍스트 줄에 있다고 한다.

```
bandit8@bandit:~$ cat data.txt

7qHmEo1FEbzthgyNpKc38YofXjYKZv18
RpRE5maDwMQTa8oJt7vVNqff7ElrjLTq
zokSjnkcdJ1hdGEBE4feukfCtFmv82ZZ
omBfCRI91Zm06GI0RLngq05AMwe8Ndqo
35l6mr3f6TvLJyDwU6aUgJX07cLhr6t9
iGmmKP7APsDfPxrZjCL7eDpGEWR3ot3q
4P8FsHcdr7d5WKnpTaaXY5Ss1KICd2gL
5hYz0028e1Q2TrtPVz5GZbpMzZNjebhh
IkJadTScIdBQY9a4KVjBEHyXKubCxSLx
HloFLs5IpuFLuVJugBxKEipr5Qa0bJmk
qeI18Iw0qI0fe3fGMr6tTPpL6SbPMjk3
s8SnoFuk0jR1CTdQ7pctd67nakJWN2Vc
omBfCRI91Zm06GI0RLngq05AMwe8Ndqo
WVQJq1JYFGgtR69JgWxUAKPb0RaKc90J
```

Cat 명령어로 data.txt 파일을 출력해보니, 알 수 없는 수 많은 문자열들이 출력되었다. 이 중에서 단 한 번만 등장하는 텍스트 줄에 비밀번호가 있다고 하니, data.txt의 중복을 제거하는 작업이 필요해 보인다. 중복을 제거하기 위해서, "uniq"를 사용하려고 한다. 이는 파일 내용이 중복되면 제거한다고 한다. 이 uniq의 옵션인 "-c"를 활용하여, 몇 번 중복되었는지도 출력해 주게끔 하려고 한다. 단, 이 uniq는 이어진 중복만 제거하기 때문에 추가적인 명령이 더 필요해 보인다. 그리고, "sort" 명령어를 활용하여, 파일을 오름차순으로 정렬해주려고 한다.

```
bandit8@bandit:~$ cat data.txt | sort | uniq -c
10 0BKVRLEJQcpNx8wnSPxDLFnFKlQafKK6
10 0eJPctF8gK96ykGBBaKydHJgxSpTLJtz
10 0kJ7XHD4gVtNsZIpqyP1V45sfz90BLFo
10 0lPovKhpHZebxji0gdjtGcd5GWiZnNBj
10 0REUHKk0yMq0OweI6NK9ZqIpE5dVlWWM
10 1jfUH1m4XCjr7eWaeLeGdaNSxFXRTx0L
10 1VKPEkd0bCtIRwMFVQfY7InuLwOFyDsn
10 2u8fvAzvnaFlvQG3iPt4Wc1TFhPcGxhH
10 35L6mr3f6TVLJyDwU6aUgJX07cLhr6t9
10 3FIgaJXBlaQA1TMVGo1gxRDSiACNyvvJ
10 3nNA31e0gfURQKNHVIhGkMNLqLw4yyLN
1 4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
10 4P8F5HcdR7d5WKnPTAaXY5SsLKICd2gL
10 5EmwMKZHwF6Lwq5jHuaDlffJBhbcX0b
10 5hYz0028e1Q2TrtPVz5GZbpMzZNjebhh
10 5I2jWpqjtVp576xXI2TLh1UCyXJtGQ78
10 6Boy6esAjn1xCyn8uI6KZ7VD7zysDM8i
10 7cP8ssLElERHXq0Jc9T84bxsmJBjNXk2
10 7qHnEo1FEbzthgyNpKc38YofXjYKZv18
10 8FctUQlFXsJnNeyiDY5KfE3vRy6sZFEEJ
10 8pePxslMzXqA2mi87wFjxd44qDRdrPiw
10 9jfkBkGp40LjMu1iH9cce4bUo9y8nd0j
10 9PqZLdu143n5djN9mL1MCanrmHERUv7k
10 9Tar2wcD3Urge6s2yp18CAE8zX1poUwV
10 A4MlxXbxP5t0RE87qkmAdwWPJ03Aw6r0
10 aFStfHbnQdPWqyRHEzhqe91Wch408xHJ
10 aMKlTMrptUxxTypChocCTrqYRkR2gT8h
10 AOz67fZdaabu2Q0yatGKX1dXNUIuyU0D
10 BIA2jxKMFnitEvp0WmsM0oDAwj4WSUa
10 BmwX4bYhJXyImwt4AVHr7wFyLYCn4IIIs
10 BooZo7QXA1Tft7d6zbVkgJlGoJzuBTXS
```

"cat data.txt | sort | uniq -c"을 입력하니, 다른 문자열들은 다 10번 중복되는데, 유일하게 한 번만 출력된 문자열을 확인할 수 있었다. 다음 단계 비밀번호는 "4CKMh1JI91bUIZZPXDqGanal4xvAg0JM"이다

Lv.8 → 9 해결