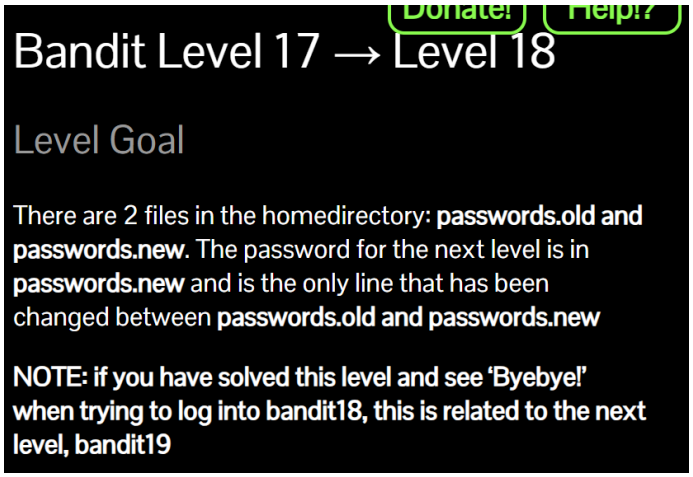
5회차 - 20. 케로로

Bandit 레벨 17 ~ 20 라이트업

정보보호학부 2024111262 조현서

Lv. 17 → 18



홈디렉토리에 passwords.old와 passwords.new 총 두 개의 파일이 있다고 한다. passwords.old와 passwords.new 중 한 줄의 내용이 바꼈는데 그 바뀐 게 password라고 한다. 만약 이 레벨을 풀고 bandit18로 접속하려고 할 때 Byebye! 본다면 다음 그 다음 bandit19와 관련이 있다고 한다.

```
bandit17@bandit:~$ ls -al
total 36
drwxr-xr-x  3 root     root     4096 Jan 11 19:18 .
drwxr-xr-x 70 root     root     4096 Jan 11 19:19 ..
-rw-r-----  1 bandit17 bandit17   33 Jan 11 19:18 .bandit16.password
-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-----  1 bandit18 bandit17 3300 Jan 11 19:18 passwords.new
-rw-r-----  1 bandit18 bandit17 3300 Jan 11 19:18 passwords.old
-rw-r--r--  1 root     root      807 Jan  6  2022 .profile
drwxr-xr-x  2 root     root     4096 Jan 11 19:18 .ssh
bandit17@bandit:~$ file passwords.old
passwords.old: ASCII text
bandit17@bandit:~$ file passwords.new
passwords.new: ASCII text
```

ls -al을 해보면 문제에서 말했듯이 passwords.old, passwords.new가 있는 걸 볼 수 있다. 둘 다 ASCII text이기 때문에 cat으로 출력해보려고 한다.

```
bandit17@bandit:~$ cat passwords.old
T2EKnlGM58236UTzM4BWH7gvpuh7Lr9o
x5SNiYaBDbuvnMsCaCGy1lmz2VAISLSH
JE5YLIiRqiT9zdiHy3lcGYZbuXZX6KOg
pKUpVHvaRf6rCn62H2Xf9xJqVszYidZH
riOYKjlMmtbzpV8EgWvHtcdoNplo2wue
Bdxj9x3jRfLbvZKIopfNvSAbQ4PqwNhB
dsBabeLrESMdD101d0paFNWgznyNdLm5
8sUsKKHRhm0MnnaNWvxYpu3d05vIc98o
umfCzH42IcitzUmFNiHB4a3IV5nxev0z
KI5OxX6tnuptS5XRKqtpuGn2sIZBvPcT
o17igJBBHexf9ehE0JL34NCG70lI8vWL
2EbK93KhwZEYRjX0dJkGAVLA6USLi5Dq
gDVHD7jTMGesoLzoxrjSklfucJn3cmzT
EPPQUeeXgHYZqYZ1j1hw7TrNPg5LzcAz
E0VFLxyvDgXx5H0ZOpl8DUTAMev52Nfc
LhVL3jHRn4EWi8H0mERqyU1j1qiu6HWj
lq5xc6fee4qpO3WYzkac3rIodbXFRaCc
QzsAgmKBkFW0svO66HOp8z5DiwADpeij
JLLt60lEV4Xx9u42qLTHhBmxQDoyZhh6
GVNbdpkJST7iYnwr3gY0XzXnrZlxQhdu
xHrZuqp1C27kbcvnSsXFmJqfIRupIpFx
```

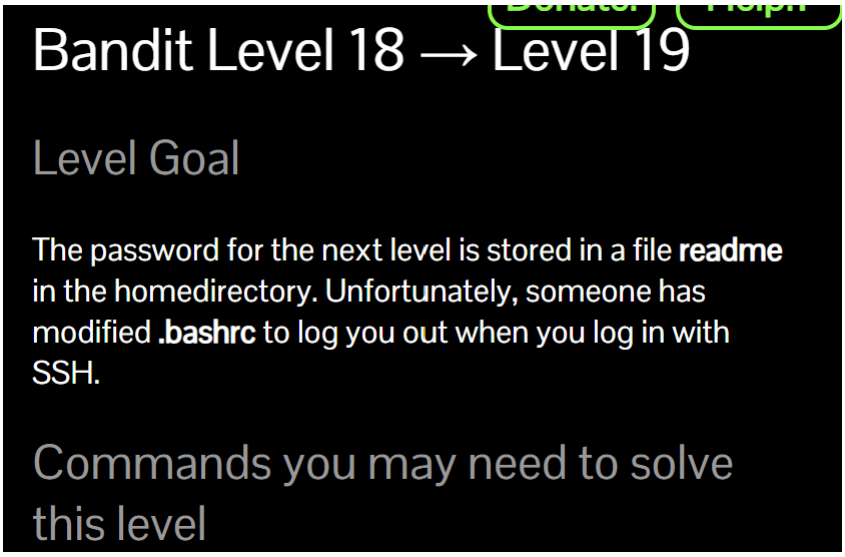
cat으로 출력해보았지만 old와 new 파일의 비교는 어려워 보인다. diff 명령어를 사용해보려고 한다. Diff는 differences의 줄임말로 두 파일 사이의 내용을 비교하는 명령어라고 한다.

```
bandit17@bandit:~$ diff passwords.old passwords.new
42c42
```

42c42가 뭔지 모르겠어서 서치해보니, 이는 42번째 줄에서 다른 내용이 나왔다라는 뜻이라고 한다. 그 후, 비밀번호처럼 문자열이 출력되었다.
비밀번호는 "**MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS**"이다.

Lv.17 → 18해결

Lv. 18 → 19

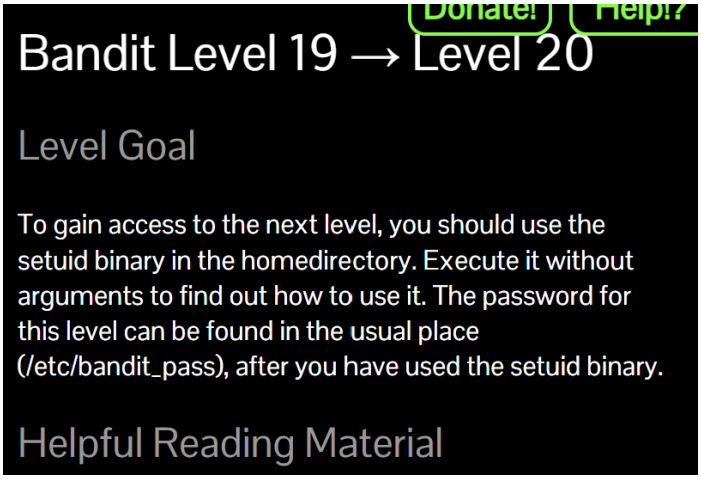


다음 단계로 가기 위한 password는 홈디렉토리에 있는 readme라는 파일에 있다. .bashrc를 수정해서 접속하려고 하면 바로 내보낸다고 하는 것 같다.
실제로 접속해보니 Byebye가 뜨면서 접속이 종료되었다.

어떻게 할지 전혀 감이 안 와서 다른 사람들의 풀이들을 참고해보니,
맨처음에 접속할 때, ssh 뒤에 사용할 명령어를 붙이면 바로 실행할 수 있다고 한다.
그래서, ssh bandit18@bandit. labs.overthewire.org -p 2220 "cat readme" 를 입력해보니, 비밀번호가
"**cGWpMaKXVwDUNgPAVJbWYuGHVn9zl3j8**"로 출력되었다.

Lv.18→ 19해결

Lv. 19 → 20



다음 단계로 가기 위해서 우리는 홈 디렉토리에 있는 setuid binary를 사용해야 한다고 한다. 인자 없이 실행해서 어떻게 사용하는지 알아내라고 한다. password는 저번처럼 /etc/bandit_pass있다고 한다.

```
bandit19@bandit:~$ file bandit20-do
bandit20-do: setuid ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dy
namically linked, interpreter /lib/ld-linux.so.2, BuildID[sha1]=c148b21f7eb7e816
998f07490c8007567e51953f, for GNU/Linux 3.2.0, not stripped
```

ls -al을 해보면 bandit20-do 파일을 볼 수 있다. file 명령어를 사용해보니까 setuid ELF 파일이라고 한다. 이를 실행시켜보면 run a command as another user. 이라고 뜨고 사용 예시를 보여주는데, 그 예시대로

```
bandit19@bandit:~$ ./bandit20-do id
uid=11019(bandit19) gid=11019(bandit19) euid=11020(bandit20) groups=11019(bandit
19)
bandit19@bandit:~$ id
uid=11019(bandit19) gid=11019(bandit19) groups=11019(bandit19)
```

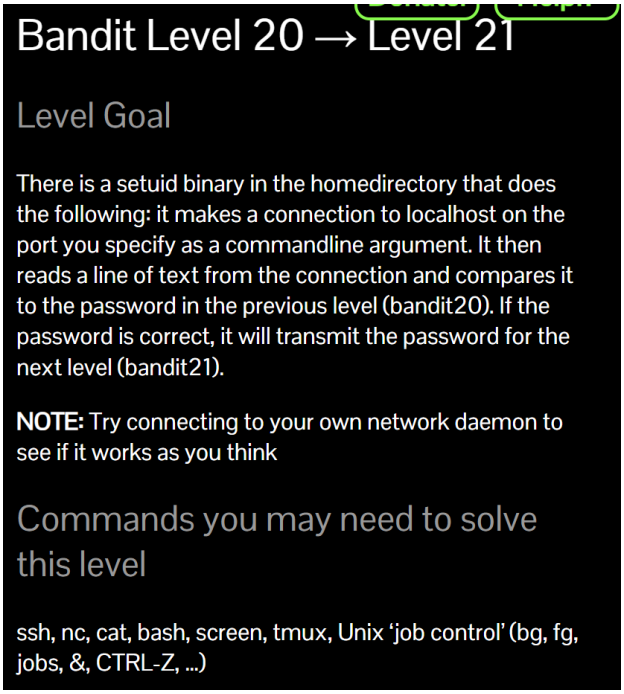
./ 이는 지난번과 유사하지만 SSL/TLS 암호화 방식이 사용된다는 점에서 차이점이 있다. Openssl 명령어를 사용해서 연결한 후, 현재 레벨의 비밀번호를 전송해보려고 한다. "openssl s_client -connect localhost:30001" 를 입력하니,

```
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
VxCazJaVykI6W36BkBU0mJTCM8rR95XT
```

다음 단계의 비밀번호를 출력시킬 수 있었다.
다음 단계의 비밀번호는 "0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO"이다.

Lv.19 → 20 해결

Lv. 20 → 21



홈 디렉토리에 setuid binary가 있는데 이건 커맨드라인 인자로 특정시킨 로컬호스트의 포트로 연결하게 해주는 그런 파일이라고 한다. bandit20의 password와 비교해서 일치한다면 다음 단계로 가능 password를 전송해준다고 한다.

Ls-al을 해보면 suconnect라는 ELF 파일이 있다.

```
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
VxCazJaVykI6W36BkBU0mJTCM8rR95XT
bandit20@bandit:~$ ./suconnect
Usage: ./suconnect <portnumber>
This program will connect to the given port on localhost using TCP. If it receiv
es the correct password from the other side, the next password is transmitted ba
ck.
```

해당 파일을 실행시켜보면, 사용법과 거기에 대한 설명이 뜬다. tcp를 사용하여 localhost의 지정된 포트에 전송시켜야 한다고 한다. 사용방법은 ./suconnect [포트번호] 라고 한다. 이에 따라

```
bandit20@bandit:~$ ./suconnect 3333
Read: GbKksEFF4yrVs6il55v6gwY5aVje5f0j
Password matches, sending next password
bandit20@bandit:~$
```

```
bandit20@bandit:~$ nc -l -p 3333
```

서로 다른 터미널을 사용하여
3333번 포트를 열어주고 bandit20의 패스워드를 보내보았다.
다음 단계의 비밀번호는 "**EeoULMCra2q0dSkYj561DX7s1CpBuOBt**"이다.

Lv.20 → 21 해결