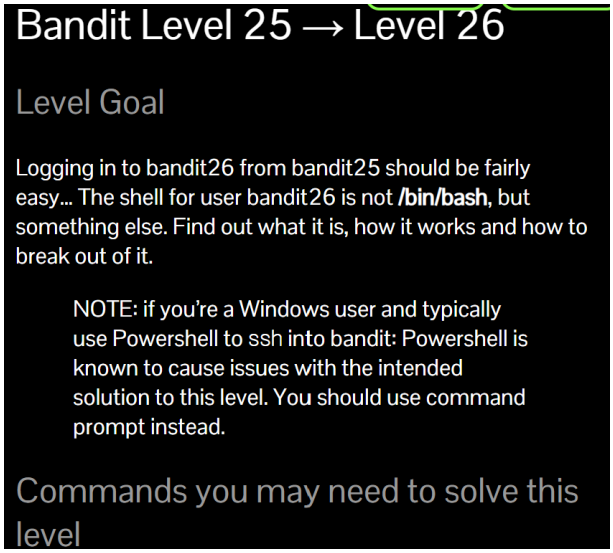
7회차 - 20. 케로로

Bandit 레벨 25 ~ 27 라이트업

정보보호학부 2024111262 조현서

Lv. 25 → 26



Bandit 25에서 bandit 26으로 로그인하는 것은 쉬울 수도 있다고 한다. Bandit26의 shell 은 /bin/bash 가 아니라고 한다.

```
bandit25@bandit:~$ ls -al
total 32
drwxr-xr-x  2 root     root     4096 Mar  6 13:56 .
drwxr-xr-x 41 root     root     4096 Oct 16  2018 ..
-rw-r-----  1 bandit25 bandit25   33 Mar  6 13:56 .bandit24.password
-r--------  1 bandit25 bandit25 1679 Oct 16  2018 bandit26.sshkey
-rw-r--r--  1 root     root      220 May 15  2017 .bash_logout
-rw-r--r--  1 root     root     3526 May 15  2017 .bashrc
-rw-r-----  1 bandit25 bandit25    4 Mar  6 13:56 .pin
-rw-r--r--  1 root     root      675 May 15  2017 .profile
bandit25@bandit:~$ file bandit26.sshkey
bandit26.sshkey: PEM RSA private key
bandit25@bandit:~$
```

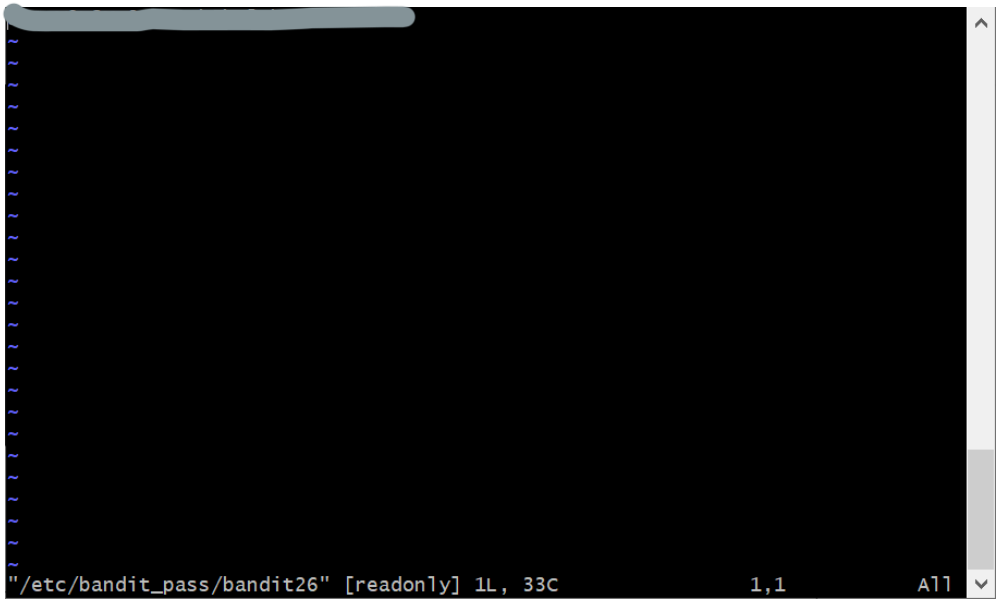
홈 디렉토리를 살펴보니, bandit26.sshkey라는 파일이 있었다. 이 파일은 RSA private key 가 있는 파일이고, 이 파일로 bandit26 계정으로 접속하면, bandit26 문자열을 출력하고 연결이 바로 끊져진다.

```
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

more ~/text.txt
exit 0
bandit25@bandit:~$
```

그래서 사용자들의 간단한 정보가 들어있는 /etc/passwd를 열어보았다. 열어보니, /usr/bin/showtext 라는 게 뜨는데, 이는 로그인할 때 처음 실행하게 될 프로그램인 것처럼 보인다. 이 /usr/bin/showtext 프로그램을 열어보니, more ~/text.txt 라는 줄이 있다. 이는 한 페이지씩 출력하게 하는 명령어인데, 이를 활용하여 풀어보려고 한다.

위와 같이 터미널 화면을 줄이고, 다시 bandit26에 접속하게 되면 한 페이지가 다 안

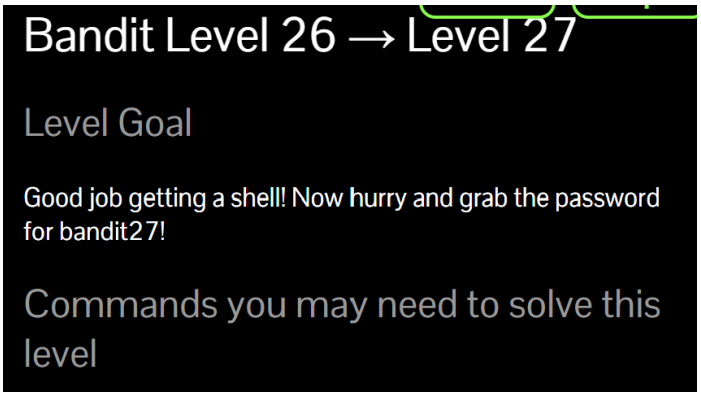
들어오게 된다. 여기서 여러 명령어를 실행할 수 있는데, v를 입력하게 되면 vi 에디터가 실행되는 것을 확인할 수 있다.



그 상태에서 :e /etc/bandit_pass/bandit26 를 입력하여, /etc/bandit_pass/bandit26이라는 파일을 열거나 편집할 수 있게 한다. 파일을 열어보니, 비밀번호를 확인할 수 있었다. 비밀번호는 "**s0773xxkk0MXfdqOfPRVr9L3jJBU0gCZ**"이다.

Lv.25 → 26 해결

Lv. 26 → 27



해석해보니, shell 얻은 거 잘했어! 이제 빨리 27로 가자라는 말만 있다.

```
bandit26@bandit:~$ ls -al
total 36
drwxr-xr-x  3 root     root     4096 Oct 16  2018 .
drwxr-xr-x 41 root     root     4096 Oct 16  2018 ..
-rwsr-x---  1 bandit27 bandit26 7296 Oct 16  2018 bandit27-do
-rw-r--r--  1 root     root      220 May 15  2017 .bash_logout
-rw-r--r--  1 root     root     3526 May 15  2017 .bashrc
-rw-r--r--  1 root     root      675 May 15  2017 .profile
drwxr-xr-x  2 root     root     4096 Oct 16  2018 .ssh
-rw-r-----  1 bandit26 bandit26  258 Oct 16  2018 text.txt
bandit26@bandit:~$ ./bandit27-do
Run a command as another user.
  Example: ./bandit27-do id
bandit26@bandit:~$ ./bandit27-do id
uid=11026(bandit26) gid=11026(bandit26) euid=11027(bandit27) groups=11026(bandit26)
bandit26@bandit:~$
```

Bandit26의 홈 디렉토리를 살펴보니, 일반적인 권한 설정과 다르게, x 부분에 s 라고 쓰여있는 setuid가 걸린 파일을 발견하였다. 이 파일을 실행시켜 보니, euid에 bandit27이라고 쓰여있다. 이전에 풀었던 문제와 유사해보였다.

```
bandit26@bandit:~$ ./bandit27-do cat /etc/bandit_pass/bandit27
[redacted]
bandit26@bandit:~$
```

해당 파일을 실행시켜 일시적으로 bandit27의 권한을 얻었는데 그 권한으로 bandit27의 패스워드를 불러왔다.

```
bandit26@bandit:~$ ssh bandit27@localhost
```

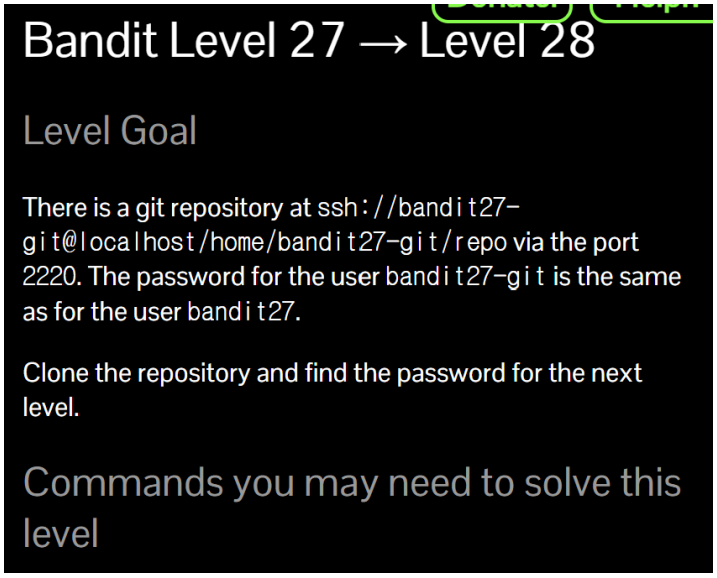
```
bandit27@bandit:~$ id
uid=11027(bandit27) gid=11027(bandit27) groups=11027(bandit27)
bandit27@bandit:~$
```

비밀번호는

"**upsNCc7vzaRDx6oZC6GiR6ERwe1MowGB**" 이다.

Lv.26→ 27 해결

Lv. 27 → 28



해석해보니, ssh://bandit27-git@localhost/home/bandit27-git/repo에 git 저장소가 있다고 한다. 사용자 bandit27-git의 암호는 사용자 bandit27과 동일하다고 한다. 저장소를 복제하고 다음 단계의 암호를 찾으라고 한다.

```
bandit27@bandit:~$ ls -al
total 20
drwxr-xr-x  2 root root 4096 Oct 16  2018 .
drwxr-xr-x 41 root root 4096 Oct 16  2018 ..
-rw-r--r--  1 root root  220 May 15  2017 .bash_logout
-rw-r--r--  1 root root 3526 May 15  2017 .bashrc
-rw-r--r--  1 root root  675 May 15  2017 .profile
bandit27@bandit:~$
```

홈 디렉토리를 살펴보니까 문제 풀이에 필요한 단서가 딱히 없어 보인다. 문제에서는 저장소를 복제하라고 했는데, 현재 디렉토리에는 bandit27의 권한이 없어서 /tmp에서 작업을 해보려고 한다.

```
bandit27@bandit:~$ cd /tmp
bandit27@bandit:/tmp$ mkdir ./mybandit27
bandit27@bandit:/tmp$ cd ./mybandit27
bandit27@bandit:/tmp/mybandit27$ ls -al
total 305924
drwxr-sr-x 2 bandit27 root      4096 Mar  9 08:12 .
drwxrws-wt 1 root     root 313204736 Mar  9 08:12 ..
bandit27@bandit:/tmp/mybandit27$
```

```
bandit27@bandit:/tmp/mybandit27$ git clone ssh://bandit27-git@localhost/home/bandit27-git/repo
Cloning into 'repo'...
Could not create directory '/home/bandit27/.ssh'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:98UL0ZWr85496EtCRkKlo20X30PnyPSB5tB5RPbhczc.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/bandit27/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit27-git@localhost's password:
remote: Counting objects: 3, done.
remote: Compressing objects: 100% (2/2), done.
remote: Total 3 (delta 0), reused 0 (delta 0)
Receiving objects: 100% (3/3), done.
bandit27@bandit:/tmp/mybandit27$
bandit27@bandit:/tmp/mybandit27$
```

Git clone 명령어를 작성하여 저장소를 복제하였다.

```
bandit27@bandit:/tmp/mybandit27$ ls -al
total 305928
drwxr-sr-x 3 bandit27 root      4096 Mar  9 08:17 .
drwxrws-wt 1 root     root 313204736 Mar  9 08:20 ..
drwxr-sr-x 3 bandit27 root      4096 Mar  9 08:17 repo
bandit27@bandit:/tmp/mybandit27$ cd repo
bandit27@bandit:/tmp/mybandit27/repo$ ls -al
total 16
drwxr-sr-x 3 bandit27 root 4096 Mar  9 08:17 .
drwxr-sr-x 3 bandit27 root 4096 Mar  9 08:17 ..
drwxr-sr-x 8 bandit27 root 4096 Mar  9 08:17 .git
-rw-r--r-- 1 bandit27 root   68 Mar  9 08:17 README
bandit27@bandit:/tmp/mybandit27/repo$ file README
README: ASCII text
bandit27@bandit:/tmp/mybandit27/repo$ cat README
The password to the next level is: [redacted]
bandit27@bandit:/tmp/mybandit27/repo$
```

Repo 디렉토리에 있는 readme를 읽으면 손쉽게 패스워드를 알 수 있다. 다음 단계의 비밀번호는 "**Yz9IpL0sBcCeuG7m9uQFt8ZNpS4HZRcN**"이다.

```
bandit27@bandit:/tmp/mybandit27/repo$ ssh bandit28@localhost
```

```
bandit28@bandit:~$ id
uid=11028(bandit28) gid=11028(bandit28) groups=11028(bandit28)
bandit28@bandit:~$
```

Lv.27 → 28 해결