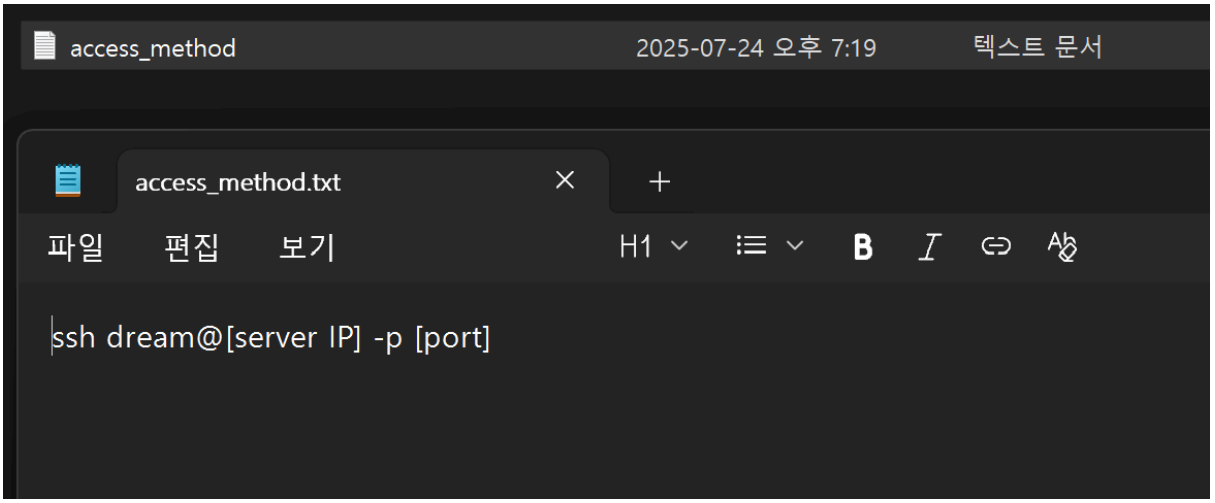
abcdefg-who

Description

드림이는 서버를 운영하고 있습니다.
어느 날 드림이의 패스워드가 유출된 이후로, 서버가 조금 달라졌음을 알게 되었습니다.
플래그를 찾아보세요!

Access Info
id: dream
pw: hack1234

1. access_method.txt



ssh dream@[server IP] -p [port] 라는 시큐어 쉘을 활용한 명령어가 하나 주어진다.

2. 서버 접속

```
kimyeeun0885@BOOK-O8SBKF5IKA: ~
kimyeeun0885@BOOK-O8SBKF5IKA:~$ ssh dream@host1.dreamhack.games -p 21588
The authenticity of host '[host1.dreamhack.games]:21588 ([139.99.121.66]:21588)' can't be established.
ED25519 key fingerprint is SHA256:4xa2IkANyzFDfR24xnJyqn9T/SxRggAa0rKZzlA4dzA.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[host1.dreamhack.games]:21588' (ED25519) to the list of known hosts.
dream@host1.dreamhack.games's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 4.19.234 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

ssh를 사용하는 서비스이므로 ssh와 주어진 id,pw로 서버에 접속했다.

```
pwd
/home/dream
ls -al
total 28
drwxr-xr-x 1 dream dream 4096 Jul 24 10:33 .
drwxr-xr-x 1 root  root  4096 Jun 11  2024 ..
-rw-r--r-- 1 dream dream  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 dream dream 3771 Feb 25  2020 .bashrc
drwx------ 2 dream dream 4096 Jul 24 10:33 .cache
-rw-r--r-- 1 dream dream  807 Feb 25  2020 .profile
```

제일 먼저 pwd 와 ls -al 로 확인해봤다.

```
ls /home
alice
bob
charlie
dream
eavan
frank
george
```

ls /home 으로 사용자 확인하였다.

```
ls -al /home/alice
total 24
drwxr-xr-x 2 alice alice 4096 Jun 11  2024 .
drwxr-xr-x 1 root  root  4096 Jun 11  2024 ..
-rw-r--r-- 1 alice alice  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 alice alice 3771 Feb 25  2020 .bashrc
-rw-r--r-- 1 alice alice  807 Feb 25  2020 .profile
ls -al /home/bob
total 24
drwxr-xr-x 2 bob  bob  4096 Jun 11  2024 .
drwxr-xr-x 1 root root 4096 Jun 11  2024 ..
-rw-r--r-- 1 bob  bob   220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 bob  bob  3771 Feb 25  2020 .bashrc
-rw-r--r-- 1 bob  bob   807 Feb 25  2020 .profile
ls -al /home/charlie
total 24
drwxr-xr-x 2 charlie charlie 4096 Jun 11  2024 .
drwxr-xr-x 1 root    root    4096 Jun 11  2024 ..
-rw-r--r-- 1 charlie charlie  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 charlie charlie 3771 Feb 25  2020 .bashrc
-rw-r--r-- 1 charlie charlie  807 Feb 25  2020 .profile
ls /al /home/eavan
ls: cannot access '/al': No such file or directory
/home/eavan:
ls -al /home/eavan
total 24
drwxr-xr-x 2 eavan eavan 4096 Jun 11  2024 .
drwxr-xr-x 1 root  root  4096 Jun 11  2024 ..
-rw-r--r-- 1 eavan eavan  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 eavan eavan 3771 Feb 25  2020 .bashrc
-rw-r--r-- 1 eavan eavan  807 Feb 25  2020 .profile
ls -al /home/frank
total 36
drwxr-xr-x 1 frank frank 4096 Jun 11  2024 .
drwxr-xr-x 1 root  root  4096 Jun 11  2024 ..
-rwxrwxrwx 1 root  root    60 Jun 11  2024 .bash.sh
-rw-r--r-- 1 frank frank  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 frank frank 3771 Feb 25  2020 .bashrc
-rw-r--r-- 1 frank frank  807 Feb 25  2020 .profile
--w--w--w- 1 root  root  1965 Jul 24 10:40 .secret_log
```

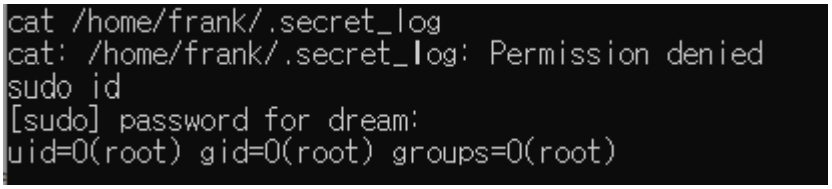
ls -al /home/사용자명

으로 내부에 존재하는 파일 확인 중 frank 에서 다른 사용자에게선 볼 수 없었던 secret_log 파일 발견

```
cat /home/frank/.bash.sh
#!/bin/bash
/bin/bash 2>&1 | tee -a /home/frank/.secret_log
```

하지만 secret_log에는 쓰기 권한만 있고 읽기 권한은 존재 X

→ cat /home/frank/.bash.sh 읽어봄 → .bash.sh 파일을 실행하면 새로운 bash 쉘이 열리고 그 안에서 실행되는 모든 명령어의 출력이 .secret_log에 저장된다는 걸 알 수 있음



우선 cat /home/frank/.secret_log 를 했을 때 현재 내 id가 dream 이기 때문에 역시나 읽을 수 없었다.

dream이의 서버이므로 sudo id 로 root로 권한 상승을 할 수 있었다.

다시 cat 명령어로 읽어보니 파일 내부에서 flag를 확인할 수 있었다.

FLAG

DH{MY_n3w_keYl0g9er_g0OD}