Dreamhack-abcdefg-who(level1)

👉 **[함께실습] abcdefg-who에서 실습하는 문제입니다.**

드림이는 서버를 운영하고 있습니다.

어느 날 드림이의 패스워드가 유출된 이후로, 서버가 조금 달라졌음을 알게 되었습니다.

플래그를 찾아보세요!

Access Info

- id: `dream`
- pw: `hack1234`

사용 툴 - WSL

리눅스 포렌식 - https://isc9511.tistory.com/177#google_vignette

- Live Forensic → SSH로 접속하여 분석 (리눅스 명령어 사용 가능)
  - 이때, ID/PW 아는 경우에만 분석 가능

1. 파일 다운로드 후 압축 제거 → 서버 접속 방법 안내 (SSH)

2. WSL 을 통해 SSH 서버 접속

```
wwszah@wwwesh:~$ ssh dream@host8.dreamhack.games -p 23603
The authenticity of host '[host8.dreamhack.games]:23603 ([158.247.232.53]:23603)' 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 '[host8.dreamhack.games]:23603' (ED25519) to the list of known hosts.
dream@host8.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.
```

3. `cat /etc/passwd | grep -v nologin` 명령어를 통해 모두 frank 라는 사용자의 홈 디렉토리에 있는 .bash.sh 가 로그인 시 실행되는 것을 확인

```
cat /etc/passwd | grep -v nologin
root:x:0:0:root:/root:/bin/bash
sync:x:4:65534:sync:/bin:/bin/sync
alice:x:1000:1000::/home/alice:/home/frank/.bash.sh
bob:x:1001:1001::/home/bob:/home/frank/.bash.sh
charlie:x:1002:1002::/home/charlie:/home/frank/.bash.sh
dream:x:1003:1003::/home/dream:/home/frank/.bash.sh
eavan:x:1004:1004::/home/eavan:/home/frank/.bash.sh
frank:x:1005:1005::/home/frank:/home/frank/.bash.sh
george:x:1006:1006::/home/george:/home/frank/.bash.sh
```

4. frank 의 홈 디렉토리 파일 확인 → 다른 사용자에게는 없는 secret_log 파일 존재

```
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   687 Jul 25 16:06 .secret_log
```

5. `cat .secret_log` 명령어를 통해 파일을 읽으려고 했으나, 권한 거부

```
cat .secret_log
cat: .secret_log: Permission denied
```

6. 해당 서버 → dream 이므로 sudo 권한 상승을 통해 해당 파일에 접근 가능

```
DH{MY_n3w_keYl0g9er_g0OD}
```

👉🏻 DH{MY_n3w_keYl0g9er_g0OD}