U-53 (하)

1. 점검 내용

- 로그인이 불필요한 계정 (admin, sys, daemon..등)에 쉘 부여 여부 점검

---

2. 점검 목적

- 로그인이 불필요한 계정에 쉘 설정을 제거하여 로그인이 필요하지 않은 계정을 통한 시스템 명령어를 실행하지 못하게 하기 위한 목적

---

3. 취약 판단 기준

- 로그인이 필요하지 않은 계정에 /bin/false(/sbin/nologin) 쉘이 부여되지 않은 경우 취약하다고 판단

3.1. /bin/false 쉘

- 아무 작업도 하지 않고 즉시 종료되는 명령어
- 이 쉘을 사용자 계정에 할당 시 사용자가 로그인을 시도 할 때 아무 작업도 수행되지 않고 즉시 로그아웃 된다
- 주로 시스템 계정이나 로그인이 필요하지 않은 계정에 사용된다

3.2. /sbin/nologin 쉘

- 로그인을 차단하며 사용자가 로그인을 시도할 때 "This account is currently not available." 메세지 출력
- 시스템 계정이나 로그인이 필요하지 않은 계정에 사용되며 로그인 시도 시 명확한 메시지 제공한다

---

4. 점검 방법

4.1. /etc/passwd 파일 확인

```
cat /etc/passwd
```

4.2. 불필요한 계정 필터링

```
grep -E
"^daemon|^bin|^sys|^adm|^listen|^nobody|^nobody4|^noaccess|^diag|^operator|^games|^g
opher" /etc/passwd | grep -v "admin"
```

4.3. /bin/false 또는 /sbin/nologin 쉘이 부여된 경우 확인

```
awk -F: '($7 == "/bin/false" || $7 == "/sbin/nologin") {print $1, $7}' /etc/passwd
```

---

5. 보안 조치 방법

- 위 명령어를 통해 출력 된 계정이 있다면, 이 계정들은 적절한 쉘이 설정되지 않은 상태이다

적절한 쉘이 설정되지 않았다 : 로그인 불가능 쉘이 설정되어 있지 않은 경우 해당 계정을 사용하여 시스템에 접근하거나 명령어를 실행할 수 있는 위험이 존재

- 쉘을 `/bin/false` 또는 `/sbin/nologin`으로 변경해야 한다

```
sudo usermod -s /bin/false 사용자아이디
sudo usermod -s /sbin/nologin 사용자아이디
```