U-04 (상)

1. 점검 내용

- 시스템의 사용자 계정 정보가 저장된 파일에 사용자 계정 패스워드가 암호화되어 저장 되어 있는지 점검

---

2. 점검 목적

- 일부 오래된 시스템의 경우 /etc/passwd 파일에 패스워드가 평문으로 저장 되므로 사용자 계정 패스워드가 암호화되어 저장되어 있는지 점검하여 비인가자의 패스워드 파일 접근 시에도 사용자 계정 패스워드가 안전하게 관리 되고 있는지 확인하기 위한 목적

---

3. 취약 판단 기준

- 쉐도우 패스워드를 사용하지 않고, 패스워드를 암호화하여 저장하지 않는 경우 취약하다고 판단

---

4. 점검 방법

4.1. /etc/shadow 파일 내 패스워드 암호화 존재 확인

```
hee:$6$ZTGDxLwxwsF22eSS$Daw7bdltW5uL4jSeug.HLt3CexLN4YSv.oAvFd3RxcO9Cb4uayVJdNO8V92/
rzajC8gGiyMkkUfpIccdzI01k/:19932:0:99999:7:::
```

- hee : 사용자 이름
- (SHA-512 알고리즘)암호화 된 패스워드 6ZTGDxLwxwsF22eSS$Daw7bdltW5uL4jSeug.HLt3CexLN4YSv.oAvFd3RxcO9Cb4uayVJdNO8V92/rzajC8gGiyMkkUfpIccdzI01k/
- 19932 : 마지막 패스워드 변경일 (1970년 1월 1일부터 패스워드가 마지막으로 변경된 날까지의 일수)
- 0 : 최소 일수 (패스워드를 변경할 수 있는 최소 일수 : 현재 얼마든지 패스워드 변경 가능)
- 99999 : 최대 일수 (패스워드를 변경해야 하는 최대 일수 : 패스워드 만료 없음)
- 7 : 경고 일수 (패스워드가 만료되기 전 경고하는 일수)
- () : 만료일 (계정이 만료되는 날짜)
- () : 예약 필드 (파일 구조의 유연성을 보장하기 위해 존재)

4.2. /etc/passwd 패일 내 두 번째 필드가 X로 표시되는지 확인

```
hee:x:1000:1000:hee:/home/hee:/bin/bash
```

---

5. 보안 조치

패스워드 암호화 저장·관리 설정을 하도록 조치한다

```
sudo pwconv
```

- /etc/passwd 파일에 있는 사용자 계정의 패스워드가 /etc/shadow 파일로 옮겨지고 암호화 된다