U-18

- 분류 : 파일 및 디렉터리 관리
- 위험도 : 상

---

1. 점검 내용

- 허용할 호스트에 대한 접속 IP 주소 제한 및 포트 제한 설정 여부 점검

---

2. 점검 목적

- 허용한 호스트만 서비스를 사용하게 하여 서비스 취약점을 이용한 외부자 공격을 방지하기 위한 목적

---

3. 보안 위협

- 허용할 호스트에 대한 IP 및 포트제한이 적용되지 않은 경우, Telnet, FTP같 은 보안에 취약한 네트워크 서비스를 통하여 불법적인 접근 및 시스템 침해 사고가 발생할 수 있다

---

4. 참고

- 접속 IP 및 포트제한 애플리케이션 종류 예시
- TCP Wrapper: 네트워크 서비스에 관련한 트래픽을 제어하고 모니터링 할 수 있는 UNIX 기반의 방화벽 툴
- IPFilter: 유닉스 계열에서 사용하는 공개형 방화벽 프로그램으로써 Packet Filter로 시스템 및 네트워크 보안에 아주 강력한 기능을 보유한 프로그램
- IPtables: 리눅스 커널 방화벽이 제공하는 테이블들과 그것을 저장하는 체인, 규칙들을 구성할 수 있게 해주는 응용프로그램

---

5. 취약 판단 기준

- 접속을 허용할 특정 호스트에 대한 IP 주소 및 포트 제한을 설정하지 않은 경우 취약하다고 판단

---

6. 점검 방법

6.1. TCP Wrapper 설정 점검

```
cat /etc/hosts.allow #파일에서 허용된 호스트 확인
cat /etc/hosts.deny
```

6.2. IPtables 설정 점검

```
sudo iptables -L -n -v
```

---

7. 조치 방법

7.1. TCP Wrapper를 사용하여 접근 허용 IP 등록

```
echo "ALL: 192.168.1.100" | sudo tee -a /etc/hosts.allow
```

이 명령어는 `192.168.1.100` IP 주소를 모든 서비스에 대해 허용한다
필요한 서비스에 대해서만 허용하고 싶다면 `ALL` 대신 서비스 이름을 입력한다
예를 들어, `sshd: 192.168.1.100` 는 SSH 서비스에 대해서만 `192.168.1.100` 을 허용한다