리눅스 서버 보안

계정 관리

root 계정 원격 접속 제한

내용설명	• root 계정으로 직접 로그인하도록 허용하면 불법적인 침입자의 목표가 될 수 있음 • root 계정의 원격 접속을 제한하여야 함
보안정책	원격 접속 서비스를 사용하지 않거나, 사용 시 root 직접 접속을 차단하도록 설정

- 보안 정책 설정
  - “/etc/securetty” 파일에서 pts/0 ~ pts/x 설정 제거 또는, 주석 처리
  - “/etc/pam.d/login” 파일 수정

    (수정 전) #auth required /lib/security/pam_securetty.so

    (수정 후) auth required /lib/security/pam_securetty.so
  - “/etc/securetty” 파일 내 *pts/x 관련 설정이 존재하는 경우 PAM 모듈 설정과 관계없이 root 계정 접속을 허용하므로 반드시 "securetty" 파일에서 pts/x 관련 설정 제거 필요

계정 관리

패스워드 복잡성 설정

내용설명	패스워드 복잡성을 높이면 비인가자에 의해 발생하는 공격 발생률을 낮출 수 있음
보안정책	계정과 유사하지 않은 8자 이상의 영문, 숫자, 특수문자의 조합으로 암호 설정

- 보안 정책 설정
  - /etc/shadow 파일 내 설정된 패스워드 점검
  - 패스워드 관리 방법
    - 영문, 숫자, 특수문자를 조합하여 계정명과 상이한 8자 이상의 패스워드 설정

      (문자 종류 2종류 이상을 조합하여 최소 10자리 이상 또는, 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성)
    - 시스템마다 상이한 패스워드 사용
    - 패스워드를 기록해 놓을 경우 변형하여 기록
    - 가급적 자주 패스워드 변경

계정 관리

계정 잠금 임계값 설정

내용설명	• Brute Force 또는 Password Guessing Attack 발생 시 암호입력 실패 횟수를 제한 • 패스워드 자동공격을 차단하고 공격 시간을 지체시켜 패스워드 유출 위험을 줄임
보안정책	계정 잠금 임계값을 “5” 이하로 설정

- 보안 정책 설정
  - “/etc/pam.d/system-auth” 파일 수정 및 신규 삽입

    auth required /lib/security/pam_tally.so deny=5 unlock_time=120 no_magic_root

    account required /lib/security/pam_tally.so no_magic_root reset

계정 관리

패스워드 파일 보호

내용설명	• “/etc/shadow”파일에 암호화된 패스워드가 저장 • 지정 파일은 특별 권한이 있는 사용자들만 읽을 수 있도록 제한함
보안정책	패스워드 암호화 저장 • 관리 설정 적용

- 보안 정책 설정
  - # pwconv --> 쉐도우 패스워드 정책 적용 방법
  - # pwunconv --> 일반 패스워드 정책 적용 방법

계정 관리

root 이외의 UID(User Identification)가 '0' 금지

내용설명	• root(UID=0)와 동일한 UID를 가진 계정 존재 시 root 권한으로 시스템 접근 가능 • root의 UID를 가진 계정이 존재하지 않도록 확인 • 사용자 간 UID 중복 시에도 권한 중복으로 인한 사용자 감사 추적이 어려운 문제 발생 • 계정 UID 확인 필요
보안정책	• UID가 0인 계정 존재 시 변경 할 UID 확인 후 다른 UID로 변경 • 불필요 시 삭제 • 계정이 사용 중이면 명령어로 조치가 안 되므로 /etc/passwd 파일 설정 변경

- 보안 정책 설정
  - usermod 명령으로 UID가 0인 일반 계정의 UID를 500 이상으로 수정

    (예) test 계정의 UID를 501로 바꿀 경우

    #usermod –u 501 test

계정 관리

동일한 UID 금지

내용설명	• 중복된 UID가 존재할 경우 시스템에서 동일한 사용자로 인식하여 문제가 발생 • 공격자에 의한 개인정보 및 관련 데이터 유출 발생 시에도 감사 추적이 어렵게 됨
보안정책	• 동일한 UID로 설정된 사용자 계정의 UID를 서로 다른 값으로 변경

- 보안 정책 설정
  - usermod 명령으로 동일한 UID로 설정된 사용자 계정의 UID 변경

    #usermod -u <변경할 UID 값> <user_name>

계정 관리

root 계정 su 제한

내용설명	• 사용자가 su 명령을 사용하여 root 권한을 획득할 수 있음 • su 명령어 사용이 허용된 사용자만 root 계정으로 접속을 허용 함
보안정책	일반 사용자의 su 명령 사용 제한 1. Group 생성(생성할 그룹 요청, 일반적으로 wheel 사용) 2. su 명령어의 그룹 요청, 그룹으로 변경 3. su 명령어의 권한 변경(4750) 4. su 명령어 사용이 필요한 계정을 새로 생성한 그룹에 추가(추가할 계정 요청) • PAM(Pluggable Authentication Module)을 이용한 설정 가능

계정 관리

root 계정 su 제한

- **보안 정책 설정**
  - wheel group 생성(wheel 그룹이 존재하지 않는 경우)

    #groupadd wheel
  - su 명령어 그룹 변경

    #chgrp wheel /usr/bin/su
  - wheel 그룹에 su 명령 허용 계정 등록

    #usermod –G wheel <user_name>

    또는, 직접 /etc/group 파일을 수정하여 필요한 계정 등록

    wheel:x:10: -> wheel:x:10:root,admin

계정 관리

패스워드 최소 길이 설정

내용설명	• 패스워드 최소 길이가 설정되어 있지 않거나, 짧게 설정되어 있을 경우 패스워드가 쉽게 유출 • 패스워드 최소 길이 설정이 되어있는지 점검 함
보안정책	패스워드 정책 설정파일을 수정하여 패스워드 최소 길이를 8자 이상으로 설정

- 보안 정책 설정
  - “/etc/login.defs” 파일 수정 및 신규 삽입

    (수정 전) PASS_MIN_LAN 6

    (수정 후) PASS_MIN_LAN 8

계정 관리

패스워드 최대 사용기간 설정

내용설명	• 패스워드 최대 사용기간을 설정하지 않은 경우 일정 기간 경과 후에도 유출된 패스워드로 접속 가능 • 악의적인 사용자로부터 계속적인 접속을 차단하기 위해서는 패스워드 사용기간 제한
보안정책	• 패스워드 정책 설정파일을 수정하여 패스워드 최대 사용기간을 90일(12주) 로 설정

- 보안 정책 설정
  - "/etc/login.defs" 파일 수정 및 신규 삽입

    (수정 전) PASS_MAX_DAYS 99999

    (수정 후) PASS_MAX_DAYS 90 (단위: 일)

계정 관리

패스워드 최소 사용기간 설정

내용설명	•패스워드 최소 사용기간을 설정하지 않은 경우 사용자에게 익숙한 패스워드로 변경이 가능 •패스워드를 재사용함으로써 패스워드의 정기적인 변경은 무의미해질 수 있음 •이전 암호를 그대로 재사용하는 것을 방지하기 위해 최근 암호 기억 설정을 함께 적용하여 패스워드를 보호함
보안정책	• 패스워드 정책 설정파일을 수정하여 패스워드 최소 사용기간을 1일(1주)로 설정

- 보안 정책 설정
  - “/etc/login.defs” 파일 수정 및 신규 삽입

    (수정 전) PASS_MIN_DAYS

    (수정 후) PASS_MIN_DAYS 1 (단위: 일)

계정 관리

불필요한 계정 제거

내용설명	• OS나 Package 설치 시 Default로 생성되는 계정은 Default 패스워드를 사용하는 경우가 많기 때문에 패스워드 추측공격에 악용될 수 있음 • Default 계정은 삭제 • 관리되지 않는 불필요한 계정으로 인해 시스템 접속이 가능하므로 사용하지 않는 계정, 불필요한 계정, 의심스러운 계정은 제거 • 특히 장기간 패스워드가 변경되지 않는 미사용 계정은 패스워드 추측공격이 가능하며 해당 계정 정보의 유출 여부 확인이 어려움
보안정책	• 현재 등록된 계정 현황 확인 후 불필요한 계정 삭제

- 보안 정책 설정
  - 서버에 등록된 불필요한 사용자 계정 확인
  - userdel 명령으로 불필요한 사용자 계정 삭제

    #userdel <user_name>

계정 관리

관리자 그룹에 최소한의 계정 포함

내용설명	• 시스템을 관리하는 root 계정이 속한 그룹은 시스템 운영 파일에 대한 접근 권한이 부여되어 있으므로 최소한의 계정만 등록되어 있어야 함 • 해당 그룹 관리가 이루어지지 않으면 허가되지 않은 일반 사용자가 관리자의 권한으로 시스템에 접근하여 파일 수정 및 변경 등의 악의적인 작업으로 인해 시스템 운영에 피해를 줄 수 있음
보안정책	• 현재 등록된 계정 현황 확인 후 불필요한 계정 삭제

- 보안 정책 설정
  - “/etc/group” 파일의 root 그룹에 등록된 불필요한 계정 삭제
  - 예) root 그룹에 등록된 불필요한 test 계정 삭제

    (수정 전) root:x:0:root,test

    (수정 후) root:x:0:root

계정 관리

계정이 존재하지 않는 GID 금지

내용설명	• 미흡한 계정 그룹 관리로 인해 구성원이 없는 그룹이 존재할 경우 해당 그룹 소유의 파일이 비인가자에게 노출될 위험이 있음 • 계정이 존재하지 않는 GID(Group Identification) 설정을 관리자와 검토 후 제거하여야 함
보안정책	• 구성원이 존재하지 않는 그룹이 있을 경우 관리자와 검토하여 제거

- 보안 정책 설정
  - ➢ 구성원이 없거나, 더 이상 사용하지 않는 그룹명 삭제

```
#groupdel <group_name>
```

계정 관리

사용자 shell 점검

내용설명	• 로그인이 필요 없는 계정을 이용해 시스템에 접근하여 사용자의 명령어를 해석하고 악용할 가능성이 있음 • /bin/false 쉘(Shell)을 부여해 로그인을 금지함
보안정책	• 로그인이 필요하지 않은 계정에 대해 /bin/false(nologin) 쉘 부여

- 보안 정책 설정
  - "/etc/passwd"파일의 로그인 쉘 부분인 계정 맨 마지막에 /bin/false(nologin) 부여 및 변경

    (수정 전) daemon:x:1:1::/:/sbin/ksh

    (수정 후) daemon:x:1:1::/:/bin/false 또는, daemon:x:1:1::/:/sbin/nologin

계정 관리

Session Timeout 설정

내용설명	• 계정이 접속된 상태로 방치될 경우 권한이 없는 사용자에게 중요시스템이 노출되어 악의적인 목적으로 사용될 수 있음 • 일정 시간 이후 어떠한 이벤트가 발생하지 않으면 연결을 종료 설정 필요
보안정책	• 600초(10분) 동안 입력이 없을 경우 접속된 Session을 끊도록 설정

- 보안 정책 설정
  - sh, ksh, bash 사용하는 경우 : "/etc/profile(.profile)"파일 수정 및 추가

    TIMEOUT=600 (단위:초)

    export TMOUT
  - csh 사용하는 경우 : "/etc/csh.login" 또는 "/etc/csh.cshrc"파일 수정 및 추가

    set autologout=10 (단위: 분)

파일 및 디렉터리 관리

root 홈, 패스 디렉터리 권한 및 패스 설정

내용설명	• 잘못된 PATH 우선순위 등이 침해사고에 이용될 수 있음 • “.”(현재디렉터리) 또는 비인가자가 불법적으로 생성한 디렉터리를 우선으로 가르키지 않도록 설정
보안정책	• root 계정의 환경변수 설정파일과 “/etc/profile”등에서 PATH 환경변수에 포함되어 있는 현재 디렉터리를 나타내는 “.”을 PATH 환경변수의 마지막으로 이동 • “/etc/profile”, root계정의 환경변수 파일, 일반계정의 환경변수 파일을 순차적으로 확인

- 보안 정책 설정
  - root 계정의 설정파일(~/.profile 과 /etc/profile)을 수정

    (수정 전) PATH=.:$PATH:$HOME/bin

    (수정 후) PATH=$PATH:$HOME/bin

파일 및 디렉터리 관리

파일 및 디렉터리 소유자 설정

내용설명	• 소유자가 존재하지 않는 파일 및 디렉터리는 현재 권한이 없는 자의 소유였거나, 관리 소홀로 인해 생긴 파일일 가능성이 있음 • 중요 파일 및 디렉터리일 경우 문제가 발생할 수 있으므로 관리가 필요함
보안정책	• 소유자가 존재하지 않는 파일 및 디렉터리 삭제 또는, 소유자 변경

- 보안 정책 설정
  - 소유자가 존재하지 않는 파일이나 디렉터리가 불필요한 경우 rm 명령으로 삭제

    #rm <file_name>

    #rm <directory_name>
  - 필요한 경우 chown 명령으로 소유자 및 그룹 변경

    #chown <user_name> <file_name>

파일 및 디렉터리 관리

/etc/passwd 파일 소유자 및 권한 설정

내용설명	• 관리자 이외의 사용자가 “/etc/passwd”파일에 접근 시 root 권한 획득이 가능하므로 해당 파일의 접근을 제한하여야 함
보안정책	• “/etc/passwd” 파일의 소유자 및 권한 변경(소유자 root, 권한 644)

- 보안 정책 설정
  - “/etc/passwd” 파일의 소유자 및 권한 변경 (소유자 root, 권한 644)

```
#chown root /etc/passwd
#chmod 644 /etc/passwd
```

파일 및 디렉터리 관리

/etc/shadow 파일 소유자 및 권한 설정

내용설명	• “/etc/shadow” 파일은 root 계정을 제외한 모든 사용자의 접근을 제한 • 해당 파일에 대한 관리가 이루어지지 않을 경우 ID 및 패스워드 정보가 외부로 노출될 수 있는 위험이 존재
보안정책	• “/etc/shadow” 파일의 소유자 및 권한 변경(소유자 root, 권한 400)

- 보안 정책 설정
  - “/etc/shadow” 파일의 소유자 및 권한 변경 (소유자 root, 권한 644)

```
#chown root /etc/shadow

#chmod 400 /etc/shadow
```

파일 및 디렉터리 관리

/etc/hosts 파일 소유자 및 권한 설정

내용설명	• “/etc/hosts” 파일은 IP 주소와 호스트네임을 매핑하는데 사용되는 파일 • 파일의 접근권한 설정이 잘못 설정되어 있을 경우 악의적인 시스템을 신뢰하게 됨 • “/etc/hosts”파일에 대한 접근권한을 제한하고 있는지 점검함
보안정책	• “/etc/hosts” 파일의 소유자 및 권한 변경(소유자 root, 권한 600)

- 보안 정책 설정
  - “/etc/hosts” 파일의 소유자 및 권한 변경 (소유자 root, 권한 600)

```
#chown root /etc/hosts

#chmod 600 /etc/hosts
```

파일 및 디렉터리 관리

/etc/(x)inetd.conf 파일 소유자 및 권한 설정

내용설명	• inetd.conf(xinetd.d)의 접근권한이 잘못 설정될 경우 비인가자가 악의적인 프로그램을 등록하고 root권한으로 서비스를 실행시켜 기존 서비스에 영향을 줄 수 있음
보안정책	• "/etc/inetd.conf" 파일의 소유자 및 권한 변경(소유자 root, 권한 600)

- 보안 정책 설정
  - "/etc/inetd.conf" 파일의 소유자 및 권한 변경 (소유자 root, 권한 600)

    #chown root /etc/inetd.conf(xinetd.conf)

    #chmod 600 /etc/inetd.conf(xinetd.conf)
  - "/etc/xinetd.d/" 하위 디렉터리에 취약한 파일도 동일한 방법으로 조치

파일 및 디렉터리 관리

/etc/syslog.conf 파일 소유자 및 권한 설정

내용설명	• "/etc/syslog.conf" 파일은 시스템 운영 중 발생하는 주요 로그 기록을 설정하는 파일 • 만약 해당 파일의 접근 권한이 적절하지 않을 경우 시스템 로그가 정상적으로 기록되지 않아 침입자의 흔적 또는 시스템 오류 사항을 정확히 분석할 수 없음 • 일반 사용자는 해당 파일을 변경할 수 없도록 설정해야 함
보안정책	• "/etc/syslog.conf" 파일의 소유자 및 권한 변경(소유자 root, 권한 644)

- 보안 정책 설정
  - "/etc/syslog.conf" 파일의 소유자 및 권한 변경 (소유자 root, 권한 644)

```
#chown root /etc/syslog.conf
#chmod 644 /etc/syslog.conf
```

파일 및 디렉터리 관리

/etc/services 파일 소유자 및 권한 설정

내용설명	• 파일 /etc/services은 서비스를 관리하기 위해 사용 • 일반 사용자에 의해 접근 및 변경이 가능하면, 정상적인 서비스를 제한하거나 허용되지 않은 서비스를 악의적으로 실행시켜 침해사고를 발생시킬 수 있음 • 소유자 권한 설정을 통해 접근을 제한하여야 함.
보안정책	• "/etc/services" 파일의 소유자 및 권한 변경(소유자 root, 권한 644)

- 보안 정책 설정
  - "/etc/services" 파일의 소유자 및 권한 변경 (소유자 root, 권한 644)

```
#chown root /etc/services
#chmod 644 /etc/services
```

파일 및 디렉터리 관리

SUID, SGID, Sticky bit 설정파일 점검

내용설명	• SUID와 SGID가 설정된 파일은 특정 명령어를 실행하여 root 권한 획득 및 정상서비스 장애를 발생시킬 수 있음 • 로컬 공격에 많이 이용되므로 보안상 철저한 관리가 필요 • root 소유의 SUID 파일의 경우에는 필요한 파일을 제외하고 SUID, SGID 속성을 제거 • 잘못 설정되어 보안 위협이 되고 있는지 주기적인 진단 및 관리를 하여야 함
보안정책	• 불필요한 SUID, SGID 파일을 제거하고 애플리케이션에서 생성한 파일이나 사용자가 임의로 생성한 파일 등 의심스럽거나 특이한 파일 발견 시 SUID 제거

파일 및 디렉터리 관리

사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정

내용설명	• 환경변수 파일의 접근권한 설정이 잘못되어 있을 경우 비인가자가 다양한 방법으로 사용자 환경을 변경하여 침해사고를 일으킬 수 있음 • 홈 디렉터리 내의 환경변수 파일에 대한 접근 권한의 적정성을 점검
보안정책	• 환경변수 파일의 권한 중 타 사용자 쓰기 권한 제거 등 • (“.profile”, “.kshrc”, “.cshrc”, “.bashrc”, “.bash_prof ile”, “.login", “.exrc”, “.netrc”)

- 보안 정책 설정
  - 소유자 변경 방법

    #chown <user_name> <file_name>
  - 일반 사용자 쓰기 권한 제거 방법

    #chmod o-w <file_name>

파일 및 디렉터리 관리

World writable 파일 점검

내용설명	• 모든 사용자가 접근 및 수정할 수 있는 권한으로 설정된 파일이 존재할 경우 일반사용자로 인해 주요 파일 정보가 노출되거나 시스템 장애를 유발할 수 있음 • 만약 의도적으로 변경된 스크립트 파일을 root가 확인하지 않고 실행시켰을 경우 시스템 권한 노출을 비롯해 다양한 보안 위험이 초래될 수 있음
보안정책	• world writable 파일 존재 여부를 확인하고 불필요한 경우 제거

- 보안 정책 설정
  - 일반 사용자 쓰기 권한 제거 방법

    #chmod o-w <file_name>
  - 파일 삭제 방법

    #rm -rf <world-writable 파일명>

/dev에 존재하지 않는 device 파일 점검

내용설명	• 디바이스가 존재하지 않거나 이름이 잘못 입력된 경우 시스템은 /dev 디렉터리에 계속해서 파일을 생성하여 에러를 발생 • 실제 존재하지 않는 디바이스를 찾아 제거함으로써 root 파일 시스템 손상 및 다운 등의 문제를 방지하여야 함
보안정책	• major, minor, number 를 가지지 않는 device파일 제거

- 보안 정책 설정
  - dev에 존재하지 않는 device 파일 점검

    #find /dev -type f -exec ls -l {} \;

  - major, minor, number를 가지지 않는 device일 경우 삭제

파일 및 디렉터리 관리

접속 IP 및 포트 제한

내용설명	• TCP Wrapper를 이용하여 제한된 IP 주소에서만 접속할 수 있도록 설정하여야 함
보안정책	• /etc/hosts.deny 파일에 ALL Deny 설정 후 /etc/hosts.allow 파일에 접근 허용 IP 등록

- 보안 정책 설정
  - “/etc/hosts.deny” 파일 수정 및 신규삽입 (해당 파일이 없을 경우 새로 생성)

    (수정 전) 설정 없음

    (수정 후) ALL:ALL
  - “/etc/hosts.allow” 파일 수정 및 신규삽입 (해당 파일이 없을 경우 새로 생성)

    (수정 전) 설정 없음

    (수정 후) sshd : 192.168.0.148, 192.168.0.6(다른 서비스도 동일한 방식으로 설정)

파일 및 디렉터리 관리

UMASK 설정 관리

내용설명	•시스템 내에서 사용자가 새로 생성하는 파일의 접근권한은 UMASK 값에 따라 정해짐 •계정의 Start Profile에 UMASK 명령을 추가하면, 사용자가 로그인 한 후에도 변경된 UMASK 값을 적용 받게 됨 •잘못 설정된 UMASK 값은 잘못된 권한의 파일을 생성
보안정책	•설정파일에 UMASKK 값을 “027” 또는 “022”로 설정

- 보안 정책 설정
  - “/etc/profile” 파일 수정 및 신규 삽입

```
umask 022
export umask
```

파일 및 디렉터리 관리

홈 디렉터리 소유자 및 권한 설정

내용설명	•사용자 홈 디렉터리 내 설정파일이 비인가자에 의해 변조되면 정상적인 사용자 서비스가 제한됨 •홈 디렉터리의 소유자 외 일반 사용자들이 해당 홈 디렉터리를 수정할 수 없도록 제한하고 있는지 점검하여 정상적인 사용자 환경 구성 및 서비스 제공 유무를 확인함
보안정책	• 사용자별 홈 디렉터리 소유주를 해당 계정으로 변경하고 타사용자의 쓰기 권한 제거 • (“/etc/passwd” 파일에서 홈 디렉터리 확인, 진단 보고서에 조치할 홈 디렉터리 확인)

- 보안 정책 설정
  - “/etc/passwd” 파일 소유자 및 권한 변경

    #chown <user_name> <user_home_directory>

    #chmod o-w <user_home_directory>

파일 및 디렉터리 관리

홈 디렉터리로 지정한 디렉터리 존재 관리

내용설명	• 홈 디렉터리의 부재로 보안상 문제가 발생될 수 있음
보안정책	• 홈 디렉터리가 존재하지 않는 계정에 홈 디렉터리 설정 또는, 계정 삭제

- 보안 정책 설정
  - 홈 디렉터리가 없는 사용자 계정 삭제

    #userdel <user_name>
  - 홈 디렉터리가 없는 사용자 계정에 홈 디렉터리 지정

    #vi /etc/passwd

    #test:x:501:501::/home/test:/bin/bash (/home/test=홈 디렉터리)

    #test:x:501:501::/data:/bin/bash (홈 디렉터리 수정 /home/test -> /data)

파일 및 디렉터리 관리

숨겨진 파일 및 디렉터리 검색 및 제거

내용설명	• [.]으로 시작하는 숨겨진 파일 존재 여부 확인 후 불법적이거나 의심스러운 파일을 삭제
보안정책	• ls -al 명령어로 숨겨진 파일 존재 파악 후 불법적이거나 의심스러운 파일을 삭제함

- 보안 정책 설정
  - 숨겨진 파일 목록에서 불필요한 파일 삭제
  - 마지막으로 변경된 시간에 따라. 최근 작업한 파일 확인 시 [-t] 플래그 사용