목차

Last update: 2022/01/11 08:19	파일 및 디렉터리 관리	https://atl.kr/dokuwiki/doku.php/%ED%8C%8C%EC%9D%BC_%EB%B0%8F_%EB%94%94%EB%A0%89%ED%84%B0%EB%A6%AC_%EA%B4%80%EB%A6%AC?rev=1641889148

root 홈, 패스 디렉터리 권한 및 패스 설정

/etc/profile, ~/.bash_profile 파일 내에 PATH 변수 내에 “ . ”, “ :: “ 이 맨 앞에 존재하는 경우 변경

```
(수정 전) PATH=.:$PATH:$HOME/bin
(수정 후) PATH=$PATH:$HOME/bin:.
```

파일 및 디렉터리 소유자 설정

소유자가 존재하지 않는 파일 및 디렉터리를 삭제 및 관리

```
#find / -nouser -print
```

/etc/passwd 파일 소유자 및 권한 설정

/etc/passwd 권한 확인 후

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

/etc/shadow 파일 소유자 및 권한 설정

/etc/shadow 권한 확인 후

```
#chmod 400 /etc/shadow
#chown root /etc/shadow
```

/etc/hosts 파일 소유자 및 권한 설정

/etc/hosts 파일 소유자 권한 확인 후

```
#chmod 600 /etc/hosts
#chown root /etc/hosts
```

/etc/(x)inetd.conf 파일 소유자 및 권한 설정

/etc/xinetd.conf 파일 및 /etc/xinetd.d/ 하위 모든 파일의 소유자 및 권한 확인

```
#chown root /etc/xinetd.conf
#chmod 600 /etc/xinetd.conf
```

※ /etc/xinetd.d/ 하위 디렉터리에 취약한 파일도 위와 동일한 방법으로 조치

/etc/syslog.conf 파일 소유자 및 권한 설정

CentOS6 이상

```
#chown root /etc/rsyslog.conf
#chmod 640 /etc/rsyslog.conf
```

/etc/services 파일 소유자 및 권한 설정

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

SUID, SGID, Sticky bit 설정 파일 점검

Step 1) 제거 방법

```
#chmod -s <file_name>
```

Step 2) 주기적인 감사 방법

```
#find / -xdev -user root -type f \( -perm -04000 -o -perm -02000 \)  -exec
```

```
ls –al {} \;
```

Step 3) 반드시 사용이 필요한 경우 특정 그룹에서만 사용하도록 제한하는 방법 일반 사용자의 Setuid 사용을 제한함 (임의의 그룹만 가능)

```
#/usr/bin/chgrp <group_name> <setuid_file_name>
#/usr/bin/chmod 4750 <setuid_file_name>
```

사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정

※ 환경변수 파일 종류: .profile, .kshrc, .cshrc, .bashrc, .bash_profile, .login, .exrc, .netrc 등

```
#ls -l .bash_profile
일반 사용자 쓰기 권한 제거
#chmod o-w .bash_profile
```

world writable 파일 점검

world writable 파일: 파일의 내용을 소유자나 그룹 외 모든 사용자에 대해 쓰기가 허용된 파일 (예 : rwxrwxrwx root root <파일명 >)

```
#find / -type f -perm -2 -exec ls -l {} \;
일반 사용자 쓰기 권한 제거
#chmod o-w <file name>
```

/dev에 존재하지 않는 device 파일 점검

```
#find /dev -type f -exec ls -l {} \;
major, minor number를 가지지 않는 device일 경우 삭제
```

$HOME/.rhosts, hosts.equiv 사용 금지

```
ls -al /etc/hosts.equiv 소유자 및 권한 확인
#chown root /etc/hosts.equiv
#chmod 600 /etc/hosts.equiv
```

/etc/hosts.equiv 및 $HOME/.rhosts 파일에서 +를 제거하고 허용 호스트 및 계정 등록

```
 #cat /etc/hosts.equiv (or $HOME/.rhosts)
```

접속 IP 및 포트 제한

Step 1) vi 편집기를 이용하여 /etc/hosts.deny 파일 열기 (해당 파일이 없을 경우 새로 생성)

Step 2) 아래와 같이 수정 또는, 신규 삽입 (ALL Deny 설정)

```
(수정 전) 설정 없음
(수정 후) ALL:ALL
```

Step 3) vi 편집기를 이용하여 /etc/hosts.allow 파일 열기 (해당 파일이 없을 경우 생성)

```
(수정 전) 설정 없음
(수정 후) sshd : 192.168.0.148, 192.168.0.6
```

(다른 서비스도 동일한 방식으로 설정) < TCP Wrapper 접근제어 가능 서비스 >

```
SYSTAT, FINGER, FTP, TELNET, RLOGIN, RSH, TALK, EXEC, TFTP, SSH
```

< TCP Wrapper는 다음 두 파일에 의해 접근이 제어됨 > /etc/hosts.deny – > 시스템 접근을 제한할 IP 설정 /etc/hosts.allow – > 시스템 접근을 허용핼IP 설정

```
위의 두파일이 존재하지 않은 시 --> 모든 접근 허용
```

RHEL 8이상

RHEL/CentOS 8 버전에서는 /etc/hosts.allow 나 /etc/hosts.deny 파일이 확인 되지 않으며 파일을 생성 후 기존 과 같이 허용이나 차단에 대한 룰을 입력 하여도 적용이 되지 않습니다.

즉, 8 버전에서는 sshd 패키지에 libwrap 라이브러리 참조를 제거 한 것이라고 볼 수 있으며 그래서 8 버전부터는 /etc/hosts.deny 등을 통해 차단이 아닌 OS 방화벽인 firewalls를 통해 차단을 수행 해

야 합니다.

```
특정 IP만 허용
#firewall-cmd --permanent --add-source=10.10.10.10
특정 IP만 제거
#firewall-cmd --permanent --remove-source=10.10.10.10
IP대역 허용
#firewall-cmd --permanent --add-source=10.10.10.0/24
서비스 포트 허용
#firewall-cmd --permanent --add-port=80/tcp
서비스 포트 범위 허용
#firewall-cmd --permanent --add-port=1000-2000/tcp
방화벽 적용
#firewall-cmd --reload
```

참고자료 https://access.redhat.com/solutions/3935901

hosts.lpd 파일 소유자 및 권한 설정

```
Step 1) hosts.lpd 파일 삭제
 #rm –rf /etc/hosts.lpd
Step 2) 파일의 퍼미션 변경 (hosts.lpd 파일이 필요시)
 #chmod 600 /etc/hosts.lpd
Step 3) 소유자를 root로 변경 (hosts.lpd 파일이 필요시)
 #chown root /etc/hosts.lpd
```

UMASK 설정 관리

umask 확인 수정이 필요할 경우 /etc/profile 파일 내 다음과 같이 수정

```
umask 022
export umask
```

홈디렉토리 소유자 및 권한 설정

/etc/passwd 파일의 소유자 및 권한 변경

```
#chown <user_name> <user_home_directory>
#chmod o-w <user_home_directory>
```

홈디렉토리로 지정한 디렉토리의 존재 관리

/etc/passwd 파일에 설정된 홈디렉터리가 존재하지 않는 경우, 해당 계정으로 로그인시 홈디렉터리가 루트 디렉터리(/)로 할당되어 접근이 가능함

```
Step 1) 홈 디렉터리가 없는 사용자 계정 삭제
 #userdel <user_name>
Step 2) 홈 디렉터리가 없는 사용자 계정에 홈 디렉터리 지정
 #vi /etc/passwd
 #test:x:501:501::/:/bin/bash (홈 디렉터리가 /로 설정 된 경우)
 #test:x:501:501::/home/test:/bin/bash (홈 디렉터리 수정 / -> /home/test)
```

숨겨진 파일 및 디렉토리 검색 및 제거

```
특정 디렉터리 내 불필요한 파일 점검
#ls -al [디렉터리명]
전체 숨김 디렉터리 및 숨김 파일 점검
#find / -type f –name ".*" (파일 점검)
#find / -type d -name ".*" (디렉터리 점검)
```

Step 1) 숨겨진 파일 목록에서 불필요한 파일 삭제 Step 2) 마지막으로 변경된 시간에 따라, 최근 작업한 파일 확인 시 -t 옵션으로 수정 시간 순 정렬 확인