서버 필수 보안수칙 (Linux용)

※ 본 가이드에서는 일반적인 설정법을 명시하고 있으나 각 서버들의 특성을 모두 반영할 순 없기에 절대적이지 않습니다. 가이드에 없는 내용은 장비 벤더사 혹은 유지보수 업체 담당자들과 협의하여 조치하시기 바랍니다.

■ 인증 강화

1. **현재 패스워드 복잡도 체크 및 기준 미달 시 재설정**
   - 패스워드는 영문 + 숫자 + 특수문자 조합하여 8자리 이상 설정
2. **패스워드 보안 설정 (3종 세트)**
   - 복잡도 / 최대 사용기간 / 최소 사용기간 설정
3. **로그인 실패 임계값 도달 시 일정시간 잠금**
   - 예: 로그인 10회 연속 실패시 해당 계정 10분간 잠금

■ 접근 통제

1. **서버의 외부 인터넷 오픈 최소화**
   - 부득이한 경우 출발지 IP를 지정 (혹은 학교에서 제공하는 VPN 사용)
2. **SSH 등 원격제어 서비스 사용시 포트 변경**
   - 기본 포트가 아닌 추측하기 어려운 임의의 포트로 설정
3. **서버 자체 방화벽 설치 및 운영**
   - 가급적 원격 접속을 금하고, 반드시 접속해야 할 경우는 IP 등으로 접근통제 처리
4. **root 계정 원격 접속 제한**

■ 기본 보안

1. **OS는 최신 버전을 사용하고 최신 업데이트를 적용하여 사용**
2. **서버 전용 백신 설치**
3. **불필요한 계정 삭제**
4. **세션 타임 아웃 설정**

관련 문의 : 정보통신팀 031-290-5217/5224, security@skku.edu

1 현재 패스워드 복잡도 체크 및 기준 미달 시 재설정

- 패스워드는 영문 + 숫자 + 특수문자 조합하여 8자리 이상 설정

패스워드는 영문 + 숫자 + 특수문자 조합하여 8자리 이상으로 구성해야 하며, 현재 사용중인 패스워드가 이 기준에 해당하지 않을 때는 반드시 변경해 주시기 바랍니다.
passwd 명령어를 이용하여 현재 로그인 된 계정의 패스워드를 변경할 수 있습니다.

※ root 계정은 'passwd 〈USER〉' 명령어를 통해 다른 사용자의 패스워드 변경 가능
(예 : passwd user1)

```
[root@RHEL6 ~]# passwd
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

실제 교내외에서 확인되고 있는 취약한 패스워드 리스트입니다. 아래의 패스워드와 같은 혹은 동일한 수준의 패스워드를 사용하고 있다면 지금 즉시 변경 바랍니다.

Password
123
1234
123456
123123
123qwe
1234qwer
1234qwer!
789
korea1
korea2
korea3
qwe123
qwer1234
qwer1234!
root
test
useruser

② 패스워드 보안 설정 (3종 세트)

- 복잡도 / 최대 사용기간 / 최소 사용기간 설정

패스워드가 유추 가능하도록 설정되어 있을 경우, 무차별 대입 공격, 사전 대입 공격 등에 취약하므로 패스워드 구성 시 복잡도는 영문 + 숫자 + 특수문자 조합하여 8자리 이상으로 구성될 수 있게끔 강제하는 설정이 필요합니다.

< 패스워드 복잡도 설정 체크 >

▶ LINUX - RHEL5 버전 패스워드 복잡성 설정 확인

→ PAM 모듈을 통한 설정 확인('pam_cracklib.so' 모듈이 존재하는 라인에

```
# /etc/pam.d/system-auth 또는 # /etc/pam.d/password-auth
password requisite pam_cracklib.so try_first_pass retry=3 type= minlen=5
```

▶ LINUX - RHEL7 버전 패스워드 복잡성 설정 확인

→ /etc/security/pwquality.conf 설정 확인

```
# /etc/security/pwquality.conf
minlen = 5
#lcredit=1
#ucredit=1
#dcredit=1
#ocredit=1
```

< 패스워드 복잡도 설정 >

▶ **LINUX - RHEL5 버전 패스워드 복잡성 설정**

→ PAM 모듈을 통한 설정 방법('pam_cracklib.so' 모듈이 존재하는 라인에 비밀번호 관리정책 설정)

```
# vi /etc/pam.d/system-auth 또는 # vi /etc/pam.d/password-auth
password requisite pam_cracklib.so try_first_pass retry=3 minlen=8 dcredit=-1 ucredit=0 lcredit=-1 ocredit=-1
```

▶ **LINUX - RHEL7 버전 패스워드 복잡성 설정**

→ /etc/security/pwquality.conf 설정 방법

```
# vi /etc/security/pwquality.conf
minlen=8
lcredit=-1
ucredit=-1
dcredit=-1
ocredit=-1
```

권장 값	기 능	설 명
lcredit=-1	최소 소문자 요구	소문자 최소 1자 이상 요구
ucredit=-1	최소 대문자 요구	최소 대문자 1자 이상 요구
dcredit=-1	최소 숫자 요구	최소 숫자 1자 이상 요구
ocredit=-1	최소 특수문자 요구	최소 특수문자 1자 이상 요구
minlen=8	최소 패스워드 길이 설정	최소 8자리 이상 설정
difok=N	기존 패스워드와 비교	기본값 10(50%)

② 패스워드 보안 설정 (3종 세트)

- 복잡도 / 최대 사용기간 / 최소 사용기간 설정

패스워드의 최대 사용기간 설정으로 주기적인 변경을 유도, 패스워드 유출에 따른 위험을 감소시킬 수 있습니다. PASS_MAX_DAYS으로 설정 가능하며 권장값은 '180'(6개월) 입니다.

< 패스워드 최대 사용기간 설정 체크 >

▶ '/etc/login.defs' 파일의 'PASS_MAX_DAYS' 설정이 '90' 이하로 설정되어 있는지 확인한다.
'lgoin.defs' 파일의 설정은 설정 이후 신규 생성되는 계정에 대해서는 적용되지만, 설정 전에 생성된 기존 계정에는 적용되지 않는다.

```
# cat etc/login.defs
PASS_MAX_DAYS 99999
PASS_MIN_DAYS  0
PASS_MIN_LEN  5
PASS_WARN_AGE  7
```

< 패스워드 최대 사용기간 설정 >

▶ '/etc/login.defs' 파일의 'PASS_MAX_DAYS' 설정을 '90' 이하로 변경한다. 주석처리가 되어 있으면 주석을 삭제하고, 'PASS_MAX_DAYS' 설정이 존재하지 않으면 새로 입력한다.

```
# vi etc/login.defs
PASS_MAX_DAYS 90
PASS_MIN_DAYS  0
PASS_MIN_LEN  5
PASS_WARN_AGE  7
```

▶ 'chage' 명령어를 이용하여 비밀번호 최대 사용기간을 변경한다.
(단, 0 이하로 설정되어 있는 것은 무제한을 설정이므로 유의해야 한다.)

```
# chage –M 90 [사용자명]

변경사항 확인
# chage –l [사용자명]
Last password change : Jan 21, 2016
Password expires: Jan 31, 2016
Password inactive  : never
Account expires : never
Minimum number of days between password change   : 0
Maximum number of days between password change   : 90
Number of days of warning before password expires  : 1
```

※ 시스템 계정의 경우 기간 만료로 인해 장애가 발생할 수 있어 담당자와 협의 후 적용할 것을 권고한다.

② 패스워드 보안 설정 (3종 세트)

- 복잡도 / 최대 사용기간 / 최소 사용기간 설정

패스워드의 최소 사용기간 설정으로 사용자가 익숙한 패스워드로의 즉시적인 재설정을 막아 그로 인한 보안성 저하를 방지할 수 있습니다. PASS_MIN_DAYS으로 설정 가능하며 권장값은 '1'(1일) 입니다.

< 패스워드 최소 사용기간 설정 체크 >

▶ '/etc/login.defs' 파일 내 'PASS_MIN_DAYS' 설정 확인

```
# cat etc/login.defs
.....
PASS_MIN_DAYS  0
```

< 패스워드 최소 사용기간 설정 >

▶ '/etc/login.defs' 파일 내 'PASS_MIN_DAYS' 설정 수정 또는 추가

```
# vi etc/login.defs
PASS_MIN_DAYS  1
```

※ /etc/login.defs 파일의 설정은 설정 이후 신규 생성되는 계정에 대해서는 적용되지만, 설정 전에 생성된 기존 계정에는 적용되지 않음

③ 로그인 실패 임계값 도달 시 일정시간 잠금

- 예: 로그인 10회 연속 실패시 해당 계정 10분간 잠금

로그인 실패 임계값 도달 시 일정시간 잠금으로 무차별 대입 공격 등을 방어할 수 있습니다.
deny와 unlock_time으로 설정 가능하며 권장값은 '10'(10회) / '600'(10분) 입니다.

▶ RHEL 5 버전 이하일 경우, "/etc/pam.d/system-auth" 파일 변경

※ pam 모듈 설정 변경 시 각 구문의 위치에 따라 정책이 달라지므로 반드시 순서를 고려하여 설정

```
# vi /etc/pam.d/system-auth
        auth    required        pam_env.so      ...①
(추가)  auth    required        pam_tally.so deny=3 ...②

        account     required        pam_unix.so ...③
(추가)  account     required        pam_tally.so ...④
```

▶ RHEL 6 버전 이상일 경우, "/etc/pam.d/system-auth" 및 "/etc/pam.d/password-auth" 변경

※ pam 모듈 설정 변경 시 각 구문의 위치에 따라 정책이 달라지므로 반드시 순서를 고려하여 설정

```
# vi /etc/pam.d/system-auth 및 # vi /etc/pam.d/password-auth
        auth        required        pam_env.so ...①
(추가)  auth        required        pam_faillock.so preauth audit deny=3 unlock_time=600 ...②
        auth        sufficient      pam_unix.so try_first_pass nullok ...③
(추가)  auth        [default=die]   pam_faillock.so authfail audit deny=3 unlock_time=600 ...④
        auth        required        pam_deny.so

        account     required        pam_unix.so ...⑤
(추가)  account     required        pam_faillock.so ...⑥
```

※ 아래의 순서를 준수하지 않거나 일부 항목만 설정할 경우, 모든 계정(root 포함)의 로그인이 불가 또는 계정 잠금 정책 설정이 적용되지 않을 수 있음

① pam_env.so 아래 설정	[auth required pam_faillock.so preauth audit deny=3 unlock_time=600]
③ pam_unix.so 아래 설정	auth [default=die] pam_faillock.so authfail audit deny=3 unlock_time=600
⑤ pam_unix.so 아래 설정	account required pam_faillock.so

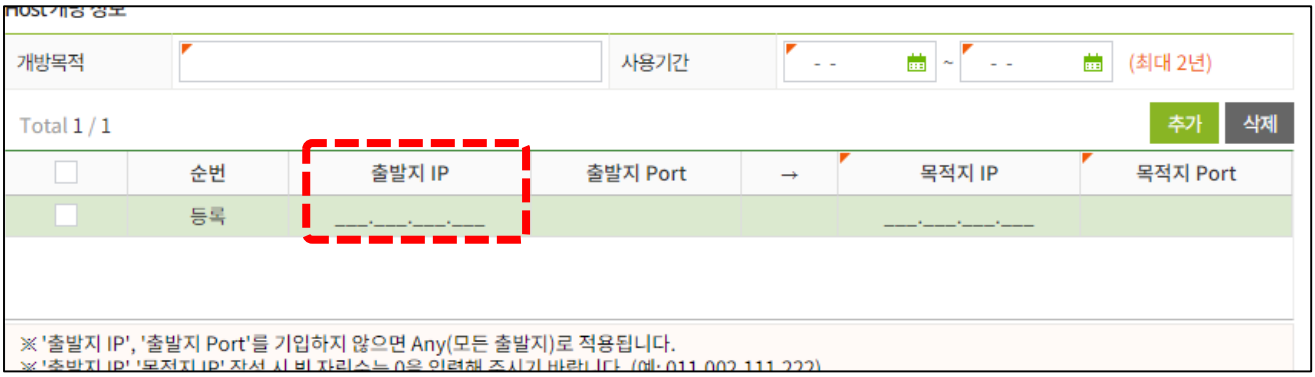
옵 션	
deny	**로그인 실패 시 계정 잠금 임계값 지정**
unlock_time	**계정이 잠겼을 경우 잠금이 해제되는 소요시간(단위 초)**
reset	로그인 성공 시 이전 로그인 실패 횟수 초기화 (선택사항)
even_deny_root	root 계정에 대한 계정 잠금 임계값 적용 (선택사항)
no_magic_root	root에게는 패스워드 잠금 설정을 적용하지 않음

※ 조치 후 로그인 계정이 차단되었을 경우 계정과 연계되어 있는 프로그램 서비스에 영향을 줄 수 있으므로 차단된 계정과 연계된 프로그램들의 서비스 작동 여부 확인 후 적용

① 서버의 외부 인터넷 오픈 최소화

- 부득이한 경우 출발지 IP를 지정 (혹은 학교에서 제공하는 VPN 사용)

외부 인터넷에 오픈 된 서비스가 많을수록 위험은 증가합니다.
가급적 외부 인터넷 오픈을 최소화하고, 부득이한 경우는 출발지 IP를 지정(혹은 학교에서 제공하는 VPN 사용)해서 사용하시기 바랍니다.



〈 인터넷 오픈 메뉴 (GLS / 정보광장) 〉

② SSH 등 원격제어 서비스 사용시 포트 변경

- 기본 포트가 아닌 추측하기 어려운 임의의 포트로 설정

원격제어 서비스는 기본 포트번호를 변경해서 사용하며, (교내에서도 공격이 가능하기 때문에) 외부 인터넷 오픈 여부와 상관없이 적용 합니다. 랜덤한 번호일수록 보안에 유리합니다.

```
  GNU nano 2.3.1                File: /etc/ssh/sshd_config

#       $OpenBSD: sshd_config,v 1.100 2016/08/15 12:32:04 naddy Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin

#Port 22
Port 34627
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none
```

③ 서버 자체 방화벽 설치 및 운영

- 가급적 원격 접속을 금하고, 반드시 접속해야 할 경우는 IP 등으로 접근통제 처리

학교의 메인 방화벽이 있지만, 각각의 서버들을 모두 철저히 보호하긴 어렵습니다. 각 서버가 운영되는 환경과 여건이 모두 다른 만큼, 각 서버는 자체 방화벽을 활용하여 자신의 서비스를 보다 안전하게 지키는 방법을 강구해야 합니다.

리눅스용 방화벽은 여러가지가 있습니다.

가장 널리 이용되는 어플리케이션에 대해서 소개해 드리니, 각 서버에 설치 가능한 방화벽을 선택하여 설치 후, 허용 호스트에 대한 접속 IP 주소 제한 및 포트 제한 설정을 하시기 바랍니다. 허용 호스트는 최소한으로 설정하는 것이 좋습니다.

아래 명령어들 역시 가장 기본적인 것이니만큼 참고만 하시고, 보다 자세한 내용은 각 방화벽의 정보를 검색하여 확인하시기 바랍니다.

〈 서버 자체 방화벽 종류 예시 〉

※ **firewalld** : (Centos 기준) 7 버전 이후에 사용되는 방화벽 어플리케이션. 네트워크 인터페이스에 기초한 Zone을 통해 설정을 적용

※ **iptables** : (Centos 기준) 6 버전 이전에 사용되던 방화벽 어플리케이션. INPUT, OUTPUT, FORWARD 같은 체인을 이용해 설정을 적용

< 서버 자체 방화벽 설치 여부 확인 >

- **firewalld**

```
# firewall-cmd --state
running 실행 중
not running 실행 중이지 않은 경우

# service firewalld status 또는 systemctl status firewalld
active (exited) 실행 중인 경우
inactive (dead) 실행 중이지 않은 경우
```

- **iptables**

```
# service iptables status 또는 systemctl status iptables
active (exited) 실행 중인 경우
inactive (dead) 실행 중이지 않은 경우
```

③ 서버 자체 방화벽 설치 및 운영

- 가급적 원격 접속을 금하고, 반드시 접속해야 할 경우는 IP 등으로 접근통제 처리

< 서버 자체 방화벽 설정 >

▶ firewalld

firewall-cmd --list-all
사용 가능한 모든 서비스/포트 리스트 확인

firewall-cmd –parmanent –add-port=80/tcp
특정 port(http) 서비스 방화벽 Any 오픈하기

firewall-cmd –parmanent –remove-port=80/tcp
특정 port(http) 서비스 방화벽 Any 오픈 제거(=차단) 하기

firewall-cmd --parmanent --add-source=193.190.111.111/32
특정 IP 접속 허용

firewall-cmd –permanent –remove-source=193.190.111.111/32
특정 IP 차단

firewall-cmd --permanent --add-source=193.190.111.111/32 --add-port=22/tcp
특정 IP에서 특정 port(ssh) 접속 허용

firewall-cmd --reload
설정한 정책을 적용

▶ iptables

iptables --list
현재 작성된 정책 리스트 확인

iptables -A INPUT -p tcp --dport 80 -j ACCEPT
특정 port(http) 서비스 방화벽 Any 오픈하기

iptables -A INPUT -s 193.190.111.111 -j ACCEPT
특정 IP 접속 허용

iptables -A INPUT -s 193.190.111.111 -j DROP
특정 IP 차단

iptables –A INPUT –p tcp –s 193.190.111.111 –dport 22 –j ACCEPT
iptables –A INPUT –p tcp –s –dport 22 –j DROP
특정 IP에서 특정 port(ssh) 접속 허용

service iptables firewall-cmd --reload
설정한 정책을 적용

4 root 계정 원격 접속 제한

root 계정은 시스템 관리자가 사용하는 특별 계정으로서 사용자 계정을 생성하거나 소프트웨어를 설치하고 환경 및 설정을 변경할 수 있는 Super User의 모든 권한을 갖기 때문에 보안에 특히 유의해야 합니다. 이를 외부의 비인가자가 획득할 수 없도록 원격 접속을 제한하여 사용하시기 바랍니다.

< root 계정 원격 접속 가능여부 체크 >

▶ "/etc/securetty" 파일에서 *pts/0 ~ pts/x 설정 확인

```
# cat /etc/securetty
  console
  vc/1
  vc/2
  pts/0
  pts/1
```

▶ Telnet 설정 확인

```
# cat /etc/pam.d/login
    #auth required /lib/security/pam_securetty.so
```

▶ SSH 설정 (sshd_config) 확인

설정파일 위치 : /etc/sshd_config, /etc/ssh/sshd_config, /usr/local/etc/sshd_config, /usr/local/sshd/etc/sshd_config, /usr/local/ssh/etc/sshd_config, /etc/opt/ssh/sshd_config

```
# cat /etc/sshd_config
    PermitRootLogin yes
```

▶ SSH의 경우 설정 값에 따른 root 원격접속 제한은 아래와 같다.

설정 값	root 원격접속 가능	양호/취약
PermitRootLogin=yes	O	취약
#PermitRootLogin=no	O	취약
해당 설정 없음	O	취약
PermitRootLogin=no	X	양호

※ PermitRootLogin=Without-passwd의 경우 원격에서 키 없이 root 직접 접속이 불가능하나, 키 값이 탈취될 경우 root 접속이 가능하므로 권고하지 않음
※ 기본 값은 "PermitRootLogin=yes"이며 주석일 경우 root 원격접속 가능

4 root 계정 원격 접속 제한

< root 계정 원격 접속 제한 설정 >

▶ **"/etc/securetty" 파일에서 *pts/0 ~ pts/x 설정 제거 또는 주석 처리**

→ Telnet 접속 시 root 접근 제한 설정 파일 "/etc/securetty" 파일 내 pts/x 관련 설정이 존재하는 경우 PAM 모듈 설정과 관계없이 root 계정 접속을 허용하므로 반드시 "/etc/securetty" 파일에서 pts/x 관련 설정 제거 필요

※ ***pts/0 ~ pts/x 설정*** : tty(terminal-teletype) : 서버와 연결된 모니터, 키보드 등을 통해 사용자가 콘솔로 직접 로그인함
※ pts(pseudo-terminal, 가상터미널) : Telnet, SSH, 터미널 등을 이용하여 접속함

▶ **"/etc/pam.d/login" 파일 수정**

```
# vi /etc/pam.d/login
    (수정 전) #auth required /lib/security/pam_securetty.so
    (수정 후) auth required /lib/security/pam_securetty.so
```

▶ **vi 편집기를 이용하여 "/etc/ssh/sshd_config" 파일을 연 후 아래와 같이 주석 제거 또는 신규 삽입**

```
# vi /etc/ssh/sshd_config
    (수정 전) #PermitRootLogin Yes
    (수정 후) PermitRootLogin No
```

1 OS는 최신 버전을 사용하고 최신 업데이트를 적용하여 사용

구버전의 OS는 그 자체로 많은 취약점들이 노출되어 있기 때문에 신경써서 적용한 많은 보안조치들이 무색해질 수 있습니다. OS는 최신 버전을 사용해 주시기 바라며 또한 주기적인 업데이트를 통하여 알려진 취약점에 대한 조치를 적용해야 합니다.

cat /etc/*release* // 리눅스 배포판 정보 확인
cat /etc/issue // 리눅스 배포판 정보 확인
uname -a // 리눅스 커널 정보 확인

```
[root@demo ~]# cat /etc/*release*
CentOS Linux release 7.6.1810 (Core)
Derived from Red Hat Enterprise Linux 7.6 (Source)
NAME="CentOS Linux"
VERSION="7 (Core)"
ID="centos"
ID_LIKE="rhel fedora"
VERSION_ID="7"
PRETTY_NAME="CentOS Linux 7 (Core)"
ANSI_COLOR="0;31"
CPE_NAME="cpe:/o:centos:centos:7"
HOME_URL="https://www.centos.org/"
BUG_REPORT_URL="https://bugs.centos.org/"

CENTOS_MANTISBT_PROJECT="CentOS-7"
CENTOS_MANTISBT_PROJECT_VERSION="7"
REDHAT_SUPPORT_PRODUCT="centos"
REDHAT_SUPPORT_PRODUCT_VERSION="7"

CentOS Linux release 7.6.1810 (Core)
CentOS Linux release 7.6.1810 (Core)
cpe:/o:centos:centos:7
```

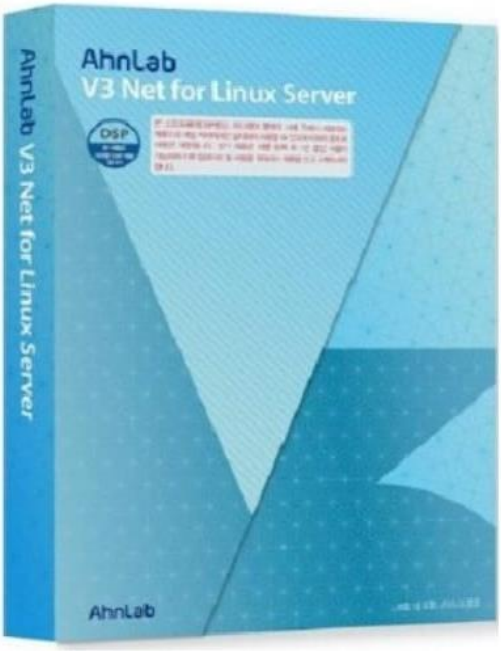
```
vagrant@ubuntu1804:~$ cat /etc/issue
Ubuntu 18.04.1 LTS \n \l

vagrant@ubuntu1804:~$
```

```
[root@localhost ~]# uname -a
Linux localhost.localdomain 4.18.0-147.el8.x86_64 #1 SMP Wed
2019 x86_64 x86_64 x86_64 GNU/Linux
[root@localhost ~]#
```

② 서버 전용 백신 설치

이제는 Linux도 악성코드로부터 안전지대라고 할 수 없습니다. 이에 학교에서는 서버 전용 백신(유료 버전, 리눅스용 / 윈도우 서버용 각각)을 구성원들이 자유롭게 이용할 수 있도록 배포하고 있습니다. 학교 보안포털(https://security.skku.edu)에서 다운로드하여 설치하시면 악성코드 대응에 큰 도움이 될 수 있습니다.



악성코드 대응	
악성코드검사	실시간 검사
	파일 검사(모든 파일)
	예약 검사
엔진 업데이트	자동 업데이트
	예약 업데이트
환경설정	모든 파일 검사
	감염되기 쉬운 파일 검사
	압축 파일 검사
	치료 방법 선택
	치료 전 검역소로 보내기

https://security.skku.edu 〉자료실 〉보안S/W 〉〉 '백신 프로그램(서버용)'

백신 프로그램(서버용)

윈도우 서버용 백신(AhnLab V3 Net for Windows Server 9.0)

리눅스/유닉스용 백신(AhnLab V3 Net for UNIX/LINUX) / 간단 메뉴얼

본 백신들은 성균관대학교의 구성원들에 한하여 교내에서만 사용토록 라이선스가 제한되어 있습니다.
(이를 어기고 무단으로 사용할 경우, 민/형사상의 책임이 발생할 수 있습니다.)

▣ 문의

설치 및 사용 관련 : (031) 290-5224

정책 관련 : (031)290-5228, 5217 / jh.jung@skku.edu, security@skku.edu

3 불필요한 계정 삭제

시스템에 불필요한 계정이 존재하는 경우, 해커의 타겟이 되어 도용되기 쉽습니다. 주기적으로 불필요 계정의 존재여부를 체크해 주시기 바랍니다.

< 불필요 계정 존재여부 확인 >

▶ **현재 등록된 계정 현황 내 불필요한 계정이 존재하는지 확인**

```
# cat /etc/passwd
 daemon:x:1:1::/:/bin/bash
 uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
 operator:x:11:0:operator:/root:/sbin/nologin
```

< 불필요 계정 삭제 조치 >

▶ 현재 등록된 계정 현황 확인 후 불필요한 계정 삭제 또는 /sbin/nologin, /bin/false 쉘 부여

→ 불필요한 사용자 계정 삭제

```
# userdel <사용자명>
```

→ 사용하지 않는 계정에 /sbin/nologin, /bin/false 쉘 부여

```
# vi /etc/passwd
    daemon:x:1:1::/:/bin/false
```

※ 시스템 계정 상세 설명

계정	설 명
adm	시스템 관리자를 위한 별도의 계정
lp	프린터를 사용할 수 있는 계정
shutdown, halt	시스템 종료 및 재부팅에 사용하는 계정으로 오직 root 만이 시스템을 제어할 수 있도록 조치
news	news 서비스를 사용할 수 있는 계정
uucp	다른 유닉스 시스템들 간에 파일을 복사하고, 다른 시스템 상에서 실행될 명령어들을 전송하는 서비스에 사용하는 계정으로 해당 서비스 사용하지 않을 경우 조치
operator	시스템 백업 등과 같이 특수한 목적으로 할당된 계정으로 다수의 사용자가 시스템을 관리할 때 이용할 계정
games	X-windows에서 사용할 수 있는 게임 및 유틸리티 계정
gopher	웹의 성장으로 거의 존재하지 않는 서비스
nscd	네임 서비스에 대한 캐시를 관리하는 데몬
nobody	Web과 관련이 많고, minor하지만 /etc/inetd.conf를 보면 nobody user로 실행이 되는 network daemon이 존재, 예를 들어 tftp를 사용 중일 경우 삭제 불가

※ OS Default 계정들은 제거 시 OS패치 등 서버에 영향이 있을 가능성이 있으므로 쉘 제한
※ 일반적인 경우 서비스 영향은 없으나 취약점 조치 시 서버 운영 담당자와 협의하여 영향도 검토 후 적용
※ 조치 후 시스템에서 계정과 관련하여 작동되는 서비스들의 정상 작동 여부 확인

4 세션 타임아웃 설정

세션 타임아웃을 설정하여 불필요한 위험의 발생 가능성을 낮출 수 있습니다.

< 세션 타임아웃 설정 여부 확인 >

▶ 환경 파일의 설정 값 확인

→ sh(bourne shell), ksh(korn shell), bash(bourne again shell)을 사용하는 경우

```
# cat /etc/profile(.profile)
 #TMOUT=0 (단위 : 초)
```

→ csh(c shell), tcsh(tenex c shell)을 사용하는 경우

```
# cat /etc/csh.login 또는 # cat /etc/.login
#set autologout=0 (단위 : 분)
```

< 세션 타임아웃 설정 >

▶ root 로 모니터링 할 경우 /.profile, /.bash_profile 등에 600초 이상 입력

→ sh(born shell), ksh(korn shell), bash(born again shell)을 사용하는 경우

```
# vi /etc/profile(.profile)
  TMOUT=600 (단위: 초)
  export TMOUT
```

→ csh 을 사용하는 경우

```
# vi /etc/csh.login 또는 # vi /etc/csh.cshrc
  set autologout=10 (단위: 분)
```

※ 일반적인 경우 서비스 영향은 없으나 취약점 조치 시 서버 운영 담당자와 협의하여 영향도 검토 후 적용
※ 모니터링 용도 등 예외적으로 사용이 필요할 경우 **해당 계정의 환경변수 파일**에만 **별도의 세션 타임아웃 시간을 설정**
※ 세션 타임아웃 설정은 **계정별, 특정 쉘별**로 별도로 설정이 가능하며, 아래의 환경파일에 적용할 수 있음
- 적용 우선순위 : 계정별 홈디렉터리의 환경 파일(1순위) > 시스템 환경파일(2순위)

Shell	환경 파일
bash(Bourne Again shell)	/etc/profile $HOME/.profile $HOME/.bash_profile $HOME/.bash_login $HOME/.bash_logout $HOME/.bashrc
sh (Bourne shell) ksh (Korn shell)	/etc/profile $HOME/.profile
csh (C shell) tcsh (TENEX C shell)	/etc/.login /etc/csh.cshrc /etc/csh.login $HOME/.cshrc $HOME/.login $HOME/.logout $HOME/.tcshrc (tcsh만 해당)