
서버 취약점 분석·평가 보고서

UNIX & WINDOWS 취약점진단 결과보고서

2022. 06. 02

점검자 : 류규원
학번 : 18501013

전체목차

1. 수행 개요	1
1.1. 목적	1
1.2. 수행범위	1
1.3. 진단일정	1
1.4. 수행절차	1
1.5. 진단대상	2
1.6. 취약점진단 항목	2
1.6.1. 서버 취약점 진단 항목(UNIX)	2
1.6.2. 서버 취약점 진단 항목(WINDOWS)	3
1.7. 평가기준	4
1.7.1. 보안수준 산출 방법	4
1.7.2. 평가 등급 기준	5
2. 진단결과 요약 및 분석	6
2.1. 총평 및 개선방안	6
2.2. 진단 결과 요약	8
2.2.1. 서버 보안수준	8
2.2.2. 서버 영역 별 보안수준	9
2.2.3. 서버 위험도 등급별 취약점 현황	10
3. 상세 진단 결과	11

표 목차

[표 1-1] 진단일정	1
[표 1-2] 상세 수행 절차	1
[표 1-3] 진단대상	2
[표 1-4] 서버 취약점 진단 항목(UNIX)	3
[표 1-5] 서버 취약점 진단 항목(WINDOWS)	3
[표 1-6] 위험도 등급 기준	4
[표 1-7] 진단 결과 기준	4
[표 1-8] 취약점 분석 평가 등급 기준	5
[표 2-1] 서버 진단결과	6
[표 2-2] Unix 서버 취약 항목 결과	6
[표 2-3] WINDOWS 서버 취약 항목 결과	7

그림 목차

[그림 1-1] 수행 절차	1
[그림 2-1] 서버 평균 보안수준	8
[그림 2-2] 서버 영역별 평균 보안수준(Unix)	9
[그림 2-3] 서버 영역별 평균 보안수준(Windows)	9
[그림 2-4] 서버 위험도 등급별 취약점 현황(Unix)	10
[그림 2-5] 서버 위험도 등급별 취약점 현황(Windows)	10

1. 수행 개요

1.1. 목적

UNIX 및 WINDOWS 시스템에 대한 기술 취약점진단을 수행하여 발생할 수 있는 취약점을 도출하고, 주요 정보통신 기반시설 취약점 분석·평가 기준에서 요구하는 기술적 사항에 대한 분석 후 대응방안을 수립하는데 목적이 있음

1.2. 수행범위

보안성 강화를 위해 주요 영역별 항목을 점검하여 취약점을 도출하고 분석하여 보호대책 방안을 제시함

1.3. 진단일정

구분	내역	일정	비고
대상 및 일정 협의	진단대상 및 일정 상세 협의		
취약점 진단	취약점 진단 수행		
결과 분석	결과 분석 및 대응방안 마련		
보고서	진단 결과 보고서 작성		

[표 1-1] 진단일정

1.4. 수행절차

취약점진단은 다음과 같은 절차에 의해 수행됨



[그림 1-1] 수행 절차

단계	내용	비고
대상선택	<ul style="list-style-type: none"> ✓ 취약점 진단 대상 선정 ✓ 취약점 진단을 위한 일정 협의 	
정보수집	<ul style="list-style-type: none"> ✓ 시스템 현황 및 용도 파악 ✓ OOOO 요구사항 및 진단 제약사항 파악 ✓ 체크리스트 검토 및 확정 	
취약점 진단	<ul style="list-style-type: none"> ✓ 취약점 체크리스트를 이용한 수작업 실시 	
진단결과 분석	<ul style="list-style-type: none"> ✓ 진단 결과에 대한 문제점 및 원인 분석/평가 	
대응방안 마련	<ul style="list-style-type: none"> ✓ 발견된 취약점에 대한 대응방안 수립 	
보고서 작성	<ul style="list-style-type: none"> ✓ 취약점 진단 보고서 작성 	

[표 1-2] 상세 수행 절차

1.5. 진단대상

진단대상	세부대상	전체 대수	비고
서버	UNIX	1대	
	WINDOWS	1대	
총계		2대	

[표 1-3] 진단대상

1.6. 취약점진단 항목

1.6.1. 서버 취약점 진단 항목(UNIX)

구분	항목		위험도
계정 및 패스워드 관리	U-1	로그인 설정	H
	U-2	root 이외의 UID가 '0' 금지	H
	U-3	불필요 계정 존재 여부 (Default 계정)	L
	U-4	shell 제한(서버보안 구축)	L
	U-5	passwd 파일 권한 설정	H
	U-6	group 파일 권한 설정	H
	U-7	shadow 파일 권한 설정	H
	U-8	패스워드 최소 길이 제한 설정	M
	U-9	패스워드의 최대 사용기간 설정	M
	U-10	취약한 패스워드 존재여부	M
접근제어	U-11	일반 사용자의 su 명령어 제한	H
	U-12	일반 사용자의 su 명령어 제한	H
	U-13	root 계정 ftp 접속제한	H
	U-14	익명 FTP(AnonymousFTP)를 제한	H
	U-15	세션 타임아웃을 설정	L
	U-16	r-commands 제한	H
	U-17	NFS(Network File System)공유 관련 취약점을 제거여부	H
시스템 보안	U-18	Crontab 관련 파일에 대한 접근 제한	H
	U-19	PATH 환경 변수 설정	H
	U-20	UMASK 설정	H

구분	항목		위험도
서비스 보안	U-21	hosts 파일의 권한 설정	H
	U-22	inetd.conf 파일의 권한 설정	H
	U-23	hosts.equiv 파일의 권한 설정	H
	U-24	서비스 파일권한 설정	H
	U-25	기타 서비스 설정	M
	U-26	서비스 Banner 관리	L
	U-27	SNMP 서비스 설정	H
로그관리 및 보안패치	U-28	syslog 기록 설정	M
	U-29	su 로그를 기록 설정	H
	U-30	보안패치	H

[표 1-4] 서버 취약점 진단 항목(UNIX)

1.6.2. 서버 취약점 진단 항목(WINDOWS)

구분	항목		위험도
계정 관리	W-1	관리자 그룹에 최소한의 사용자 포함	H
	W-2	Guest 계정 비활성화	H
	W-3	패스워드 복잡도 설정	M
	W-4	계정 잠금 임계값 설정	H
	W-5	패스워드 최소 길이 설정	M
	W-6	패스워드 최소 사용기간 설정	M
	W-7	패스워드 최대 사용기간 설정	M

[표 1-5] 서버 취약점 진단 항목(WINDOWS)

1.7. 평가기준

1.7.1. 보안수준 산출 방법

각 진단 대상에 대한 보안 수준을 산출하기 위해 위험도를 등급으로 구분하고 그에 대한 가중치를 설정함

위험도 등급	기준	가중치
H (High)	<ul style="list-style-type: none"> 해당 취약점으로 인해 관리자 권한의 획득이 가능한 취약점 해당 취약점으로 인해 데이터 변조 및 서비스 가용성에 큰 영향을 줄 수 있는 취약점 시스템 접근에 대한 중요 정보를 제공하는 취약점 	10
M (Medium)	<ul style="list-style-type: none"> 인가된 사용자에 의한 허가되지 않은 작업을 허용하거나 비인가자의 정보 수집으로 인해 시스템에 접근하거나 피해를 줄 수 있는 취약점 감사(Audit)를 위해 반드시 필요한 항목 	8
L (Low)	<ul style="list-style-type: none"> 해당 취약점으로 인해 시스템에 영향을 주지는 않으나 시스템에 대한 일부 정보를 수집할 수 있는 취약점 해당 취약점으로 인해 시스템에 영향을 주지는 않으나 관리 목적상 중요한 취약점 	6

[표 1-6] 위험도 등급 기준

※ 위험도 등급 기준은 “주요정보통신기반 취약점 분석평가 기준” (미래창조과학부고시 제2013-37호)에 근거함

각 개별 항목에 대한 진단결과를 총 세 가지로 분류하고 이에 대해 점수를 부여함

결과값	기준	점수
취약점 제거(X)	✓ 해당 취약점이 존재하지 않아 안전한 상태	0
취약점 발견(O)	✓ 해당 취약점이 존재하여 취약한 상태	1
해당없음(N/A)	✓ 진단이 불필요하거나 해당 사항이 없는 상태	결과제외

[표 1-7] 진단 결과 기준

각 진단 대상에 대한 보안 수준은 각 진단 항목에 따라 자산별로 취약점 점수를 구하고, 이를 합한 값을 100점 기준으로 환산하여 보안수준을 아래와 같이 연산 후 산정함

$$\text{보안수준} = \frac{(\text{모든 취약점이 식별되었을 경우의 점수 합}) - (\text{식별된 취약점들의 점수 합})}{\text{모든 취약점이 식별되었을 경우의 점수 합}} \times 100$$

※ 진단 결과 기준은 미래창조과학부고시 제2013-37호 “주요정보통신기반 취약점 분석평가 기준”의 취약점 분석평가 점수 산출식 예시에 근거함

1.7.2. 평가 등급 기준

각 평가 등급 기준은 아래의 예시를 참조하여 산정함

등급	점수	비고
취약	0~50점	점검항목/점검 분야의 취약도가 매우 높아 위협에 노출될 경우 매우 심각한 피해를 초래
미흡	51~65점	점검항목/점검 분야의 취약도가 높아 위협에 노출될 경우 심각한 피해를 초래
보통	66~80점	점검항목/점검 분야의 취약도가 존재하며 위협에 노출될 경우 피해를 초래
양호	81~90점	점검항목/점검 분야의 취약도가 존재하나 위협에 노출될 경우 일부 피해를 초래
우수	91~100점	점검항목/점검 분야의 취약도가 존재하나 위협에 노출될 경우 피해가 거의 없거나 사소한 피해를 초래

[표 1-8] 취약점 분석 평가 등급 기준

2. 진단결과 요약 및 분석

2.1. 총평 및 개선방안

진단대상	진단 수	점수	평가등급
UNIX	30개	44점	취약
WINDOWS	7개	32점	취약
총계(평균)	37개	38점	취약

[표 2-1] 서버 진단결과

UNIX 서버와 WINDOWS 서버에 대한 취약점 진단 결과 UNIX 서버는 44점으로 평가등급기준 '취약' 등급을, WINDOWS 서버는 32점으로 평가등급기준 '취약' 등급으로 분석됨

UNIX 서버에서 발견된 취약점은 다음과 같음

구분	항목 코드	취약점 주요내용
계정 및 패스워드 관리 (6개 항목)	U-1	로그인 설정 미흡
	U-2	root 이외의 UID가 0인 계정설정 미흡
	U-3	불필요 계정 존재 여부 (Default 계정) 설정 미흡
	U-8	패스워드 최소 길이 제한 설정 미흡
	U-9	패스워드 최소 사용기간 설정 미흡
	U-10	취약한 패스워드 존재
접근제어 (5개 항목)	U-11	일반 사용자의 su 명령어 설정 미흡
	U-12	root 계정 Telnet 제한 설정 미흡
	U-13	root 계정 ftp 접속제한 설정 미흡
	U-14	익명 FTP(AnonymousFTP)를 제한 설정 미흡
	U-15	세션 타임아웃을 설정 미흡
서비스보안 (1개 항목)	U-25	기타서비스설정
로그관리 및 보안패치 (2개 항목)	U-29	su 로그를 기록 설정
	U-30	보안패치

[표 2-2] Unix 서버 취약 항목 결과

WINDOWS 서버에서 발견된 취약점은 다음과 같음

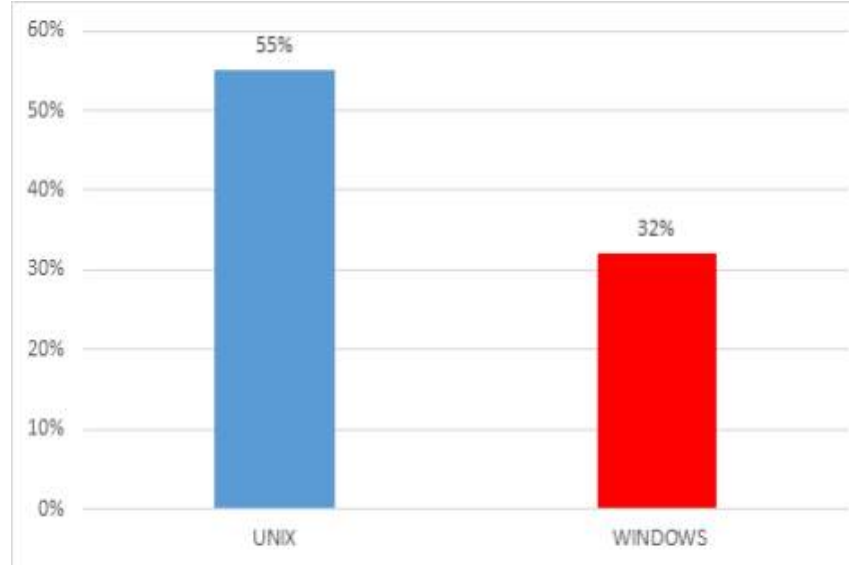
구분	항목 코드	취약점 주요내용
계정관리 (5개 항목)	W-3	패스워드 복잡도 설정 미흡
	W-4	계정 잠금 임계값 설정 미흡
	W-5	패스워드 최소 길이 설정 미흡
	W-6	패스워드 최소 사용기간 설정 미흡
	W-7	패스워드 최대 사용기간 설정 미흡

[표 2-3] WINDOWS 서버 취약 항목 결과

2.2. 진단 결과 요약

2.2.1. 서버 보안수준

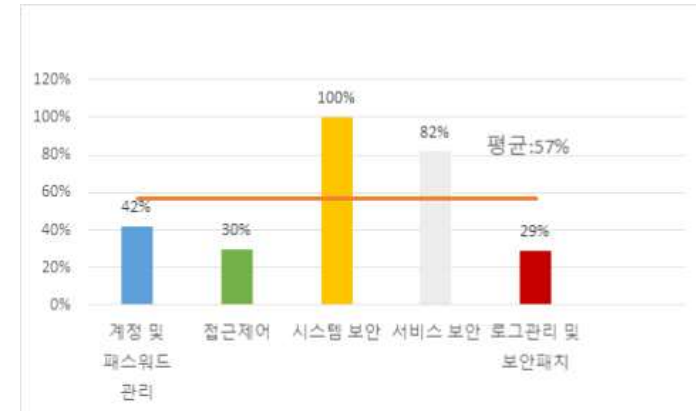
01대의 UNIX 서버, 01대의 WINDOWS 서버에 대한 취약점 진단 결과 UNIX 서버와 WINDOWS 서버의 보안 수준은 각각 **44점**, **32점**으로 모두 평가등급 기준 **"취약"**의 보안수준으로 분석·평가됨



[그림 2-1] 서버 평균 보안수준

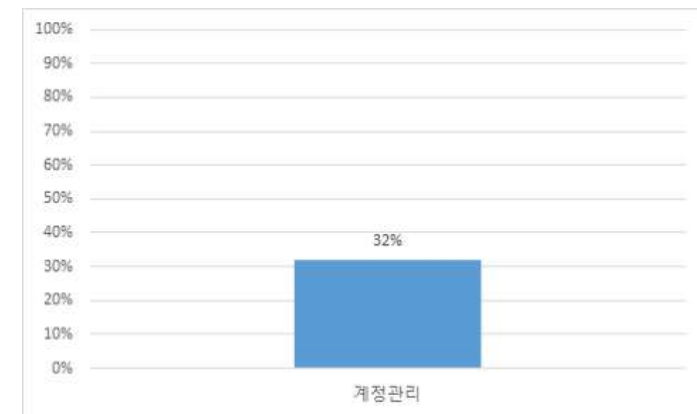
2.2.2. 서버 영역 별 보안수준

UNIX 서버의 영역별 보안수준은 시스템보안(100%), 서비스보안(82%)로 **"우수"**, **"양호"**로 평가되었으며 계정 및 패스워드 관리(42%), 접근제어(30%), 로그 및 패치 관리(29%) 영역은 영역별 평균 점수보다 낮은 점수로 분석·평가됨



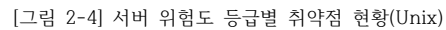
[그림 2-2] 서버 영역별 평균 보안수준(Unix)

Windows 계정관리(32%) 은 **"취약"**로 평가되었음



[그림 2-3] 서버 영역별 평균 보안수준(Windows)

UNIX 서버 위험도 등급별 취약점 현황을 분석한 결과 H(high) 38%, M(Midium) 40% L(Low) 50%로 분석·평가됨



A bar chart comparing the percentage of correct answers for two categories, '양호' (Good) and '취약' (Weak), between two groups, H (blue bars) and M (orange bars). The y-axis represents the percentage from 0% to 100% in 10% increments. For the '양호' category, group H has 32% correct answers and group M has 100%. For the '취약' category, group H has 68% correct answers and group M has 0%.

Category	H (%)	M (%)
양호	32%	100%
취약	68%	0%

- 10 -

3.1 UNIX 서버

- 11 -

[계정 및 패스워드 관리] 1.2.root 이외의 UID가 0인 계정 존재여부 -(위험도 : 상)		
정보시스템 현황	문제점	점검기준
<pre> root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin sync:x:5:0:sync:/sbin:/bin/sync shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt mail:x:8:12:mail:/var/spool/mail:/sbin/nologin operator:x:11:0:operator:/root:/sbin/nologin games:x:12:100:games:/usr/games:/sbin/nologin ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin nobody:x:99:99:Nobody:/:/sbin/nologin system-network:x:192:192:system Network Management:/:/sbin/nologin dbus:x:81:81:system message bus:/:/sbin/nologin polkitd:x:999:998:User for polkitd:/:/sbin/nologin libstoragemgmt:x:998:995:daemon account for libstoragemgmt:/var/run/lsm:/sbin/ login colord:x:997:994:User for colord:/var/lib/colord:/sbin/nologin rpc:x:32:32:rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin sane:x:996:993:SANE scanner daemon user:/usr/share/sane:/sbin/nologin gluster:x:995:992:GlusterFS daemons:/run/gluster:/sbin/nologin sasauth:x:994:76:Sasauthd user:/run/sasauthd:/sbin/nologin </pre>	<p>passwd파일을 점검한 결과 UID '0' 계정은 root 이외에 user01도 존재하여 취약함</p>	취약
조치 현황	개선사항	점검기준
<pre> sssd:x:990:984:User for sssd:/:/sbin/nologin usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin geoclue:x:989:983:User for geoclue:/var/lib/geoclue:/sbin/nologin ntp:x:38:38:/:etc/ntp:/sbin/nologin gdm:x:42:42:/:/var/lib/gdm:/sbin/nologin rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin gnome-initial-setup:x:988:982:/:run/gnome-initial-setup:/sbin/nologin sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin postfix:x:89:89:/var/spool/postfix:/sbin/nologin tcpdump:x:72:72:/:/sbin/nologin admin:x:1000:1000:centos7:/home/admin:/bin/bash user01:x:501:501:/home/user01:/bin/bash user02:x:502:502:/home/user02:/bin/bash user03:x:503:503:/home/user03:/bin/bash </pre>	<p>UID가 '0' 인 user01계정에 대한 UID인 '501' 변경 조치함.</p>	양호/취약

[계정 및 패스워드 관리] 1.3. 불필요 계정 존재 여부 (Default 계정) -(위험도 : 하)		
정보시스템 현황	문제점	점검기준
<pre> lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin mail:x:8:12:mail:/var/spool/mail:/sbin/nologin </pre>	<p>passwd파일 확인결과 시스템에서 사용하지 않는 lp,uucp,mail,news 계정이 존재하여 취약함.</p>	취약
조치 현황	개선사항	점검기준
<pre> root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin sync:x:5:0:sync:/sbin:/bin/sync shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt operator:x:11:0:operator:/root:/sbin/nologin games:x:12:100:games:/usr/games:/sbin/nologin ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin nobody:x:99:99:Nobody:/:/sbin/nologin system-network:x:192:192:system Network Management:/:/sbin/nologin dbus:x:81:81:system message bus:/:/sbin/nologin polkitd:x:999:998:User for polkitd:/:/sbin/nologin libstoragemgmt:x:998:995:daemon account for libstoragemgmt:/var/run/ login colord:x:997:994:User for colord:/var/lib/colord:/sbin/nologin </pre>	<p>불필요한 계정인 lp, news, uucp, mail 계정을 userdel명령어를 이용하여 삭제조치함 -userdel 명령어를 이용하여 삭제조치후 /etc/passwd 파일에서 삭제 여부를 확인함.</p>	양호

[계정 및 패스워드 관리]		
1.4. shell 제한(서버보안 구축) -(위험도 : 하)		
정보시스템 현황	문제점	점검기준
daemon:x:2:2:daemon:/sbin:/sbin/nologin bin:x:1:1:bin:/bin:/sbin/nologin nobody:x:99:99:Nobody:/:/sbin/nologin operator:x:11:0:operator:/root:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin	nologin이 조치되어 있어 양호함	양호
조치 현황	개선사항	점검기준

[계정 및 패스워드 관리]		
1.5. passwd 파일 권한 설정 -(위험도 : 상)		
정보시스템 현황	문제점	점검기준
-rw-r--r--. 1 root root 2344 Apr 7 20:51 passwd	/etc/passwd파일의 접근권한을 점검한 결과 644로 설정되어있어 정보통신 기반시설 취약점진단기 준인 644이하임으로 양호함 (다만 기관에서 설치한 시큐어 os 에서 passwd파일의 접근을 차단 하고 있음) 직접 보여줄시- 취약하나 시큐어 os 확인 결과 passwd 파일을 원 천적을 접근하지 못하도록 600으 로 양호함	양호
조치 현황	개선사항	점검기준

[계정 및 패스워드 관리]		
1.6. group 파일 권한 설정 -(위험도 : 상)		
정보시스템 현황	문제점	점검기준
<pre>-rw-r--r--. 1 root root 1011 Apr 7 20:51 /etc/group</pre>	<p>/etc/groups파일의 접근권한을 점검한 결과 644로 설정되어있어 정보통신 기반시설 취약점진단기준인 644이하임으로 양호함</p>	양호
조치 현황	개선사항	점검기준

[계정 및 패스워드 관리]		
1.7. shadow 파일 권한 설정 -(위험도 : 상)		
정보시스템 현황	문제점	점검기준
<pre>[root@localhost etc]# ls -al shadow -----. 1 root root 1194 Apr 7 20:51 shadow</pre>	<p>/etc/shadow파일의 접근권한을 점검한 결과 모두 접근 권한이 허용되지 않음으로 양호함</p>	양호
조치 현황	개선사항	점검기준

[계정 및 패스워드 관리]		
1.8. 패스워드 최소 길이 제한 설정 -(위험도 : 중)		
정보시스템 현황	문제점	점검기준
PASS_MAX_DAYS 99999 PASS_MIN_DAYS 0 PASS_MIN_LEN 5 PASS_WARN_AGE 7	/etc/login.defs 파일의 “PASS_MIN_LEN” 최소길이 가 5로 되어있어 취약함 또한 기존 USER들의 경우 패스워 드 최소 길이가 기존 설정값(5) 에 따라 생성되어 패스워드 변경 필요	취약
조치 현황	개선사항	점검기준
PASS_MAX_DAYS 99999 PASS_MIN_DAYS 0 PASS_MIN_LEN 8 PASS_WARN_AGE 7	/etc/login.defs 파일의 “PASS_MIN_LEN” 옵션을 8 로 변경하여 조취하였음 서비스를 재기동을 해야한다.	양호

[계정 및 패스워드 관리]		
1.9. 패스워드의 최대 사용기간 설정 -(위험도 : 중)		
정보시스템 현황	문제점	점검기준
PASS_MAX_DAYS 99999 PASS_MIN_DAYS 0 PASS_MIN_LEN 8 PASS_WARN_AGE 7	/etc/shadow파일의 PASS_MAX_DAYS 점검한 결과 “99999” 로 설정이 되어 있어 취약함	취약
조치 현황	개선사항	점검기준
PASS_MAX_DAYS 90 PASS_MIN_DAYS 0 PASS_MIN_LEN 8 PASS_WARN_AGE 7	/etc/login.defs 파일의 PASS_MAX_DAYS을 “90” 으로 변경하여 조치함	양호

[계정 및 패스워드 관리]		
1.10. 취약한 패스워드 존재여부 -(위험도 : 중)		
정보시스템 현황	문제점	점검기준
<pre>[root@localhost etc]# ls -al shadow -----. 1 root root 1194 Apr 7 20:51 shadow</pre>	<p>/etc/login.defs 파일의 "PASS_MIN_LEN" 최소길이가 5로 되어있어 취약함 사용자들의 패스워드가 취약점점검기준에 만족하지 못함</p> <p>또한 기존 USER들의 경우 패스워드 최소 길이가 기존 설정값(5)에 따라 생성되어 패스워드 변경 필요</p>	양호
조치 현황	개선사항	점검기준

[접근제어]		
2.1 일반 사용자의 su 명령어 제한 -(위험도 : 상)		
정보시스템 현황	문제점	점검기준
<pre>#auth required pam_wheel.so use_uid auth substack system-auth auth include postlogin</pre> <pre>[root@localhost etc]# ls -al /bin/su -rwsr-xr-x. 1 root root 32128 Sep 30 2020 /bin/su</pre>	<p>/etc/pam.d/su 파일의 "auth required pam_wheel.so use_uid" 설정값이 주석처리 되어 있어 취약함</p> <p>/bin/su 파일의 퍼미션이 4750 이하이기 때문에 양호함.</p>	취약
조치 현황	개선사항	점검기준
<pre>#auth required pam_wheel.so use_uid auth substack system-auth auth include postlogin</pre>	<p>/etc/pam.d/su 파일의 "auth required pam_wheel.so use_uid" 설정값이 주석처리를 제거하여 조치함</p>	양호

[접근제어] 2.2 root 계정 Telnet 제한 -(위험도 : 상)		
정보시스템 현황	문제점	점검기준
<pre>telnet 23/tcp telnet 23/udp</pre>	/etc/services 파일의 'telnet' 설정되어있어 취약함	취약
조치 현황	개선사항	점검기준
<pre>#telnet 23/tcp #telnet 23/udp</pre>	/etc/services 파일의 'telnet' 설정값을 주석처리하 여 조치하였음.	양호

[접근제어] 2.3 root 계정 ftp 접속제한 -(위험도 : 상)		
정보시스템 현황	문제점	점검기준
<pre># 21 is registered to ftp, but also used by fsp ftp 21/tcp ftp 21/udp fsp fspd</pre>	/etc/services 파일의 'ftp' 설정되어있어 취약함	취약
조치 현황	개선사항	점검기준
<pre>#ftp 21/tcp #ftp 21/udp fsp fspd</pre>	/etc/services 파일의 'ftp' 설정값을 주석처리하여 조치하였음.	양호

[접근제어] 2.4 익명 FTP(AnonymousFTP)를 제한 -(위험도 : 상)		
정보시스템 현황	문제점	점검기준
<pre>games:x:12:100:games:/usr/games:/sbin/nologin ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin</pre>	/etc/passwd 파일의 'ftp' 계정이 존재하여 취약함	취약
조치 현황	개선사항	점검기준
<pre>adm:x:3:4:adm:/var/adm:/sbin/nologin sync:x:5:0:sync:/sbin:/bin/sync shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt operator:x:11:0:operator:/root:/sbin/nologin games:x:12:100:games:/usr/games:/sbin/nologin ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin</pre>	userdel ftp 명령어를 사용하여 ftp계정을 제거하여 조치하였음.	양호

[접근제어] 2.5 세션 타임아웃을 설정 -(위험도 : 하)		
정보시스템 현황	문제점	점검기준
<pre>else umask 022 fi for i in /etc/profile.d/*.sh /etc/profile.d/sh.local ; do if [-r "\$i"]; then if ["\${-#*i}" != "\$-"]; then else "\$i" >/dev/null fi fi done unset i unset -f nathminne</pre>	/etc/profile 파일의 타임아웃 설정이 되어있지않아 취약함	취약
조치 현황	개선사항	점검기준
<pre>TIMEOUT=300</pre>	/etc/profile 파일의 타임아웃 설정 "TIMEOUT=300"을 해주어 조치함.	양호

[접근제어] 2.6 r-commands 제한 -(위험도 : 상)		
정보시스템 현황	문제점	점검기준
<pre>[admin@localhost xinetd.d]\$ ls [admin@localhost xinetd.d]\$ █</pre>	<pre>/etc/xinetd.d/rlogin 존재하지 않아 양호함.</pre>	양호
조치 현황	개선사항	점검기준

[접근제어] 2.7 NFS(Network File System)공유 관련 취약점을 제거여부 -(위험도 : 상)		
정보시스템 현황	문제점	점검기준
<pre>[admin@localhost etc]\$ cat /etc/exports [admin@localhost etc]\$ █</pre>	<pre>/etc/exprots 파일 확인결과 아 무런 설정이 되어있지않아 양호 함.</pre>	양호
조치 현황	개선사항	점검기준

[시스템 보안]		
3.1 Crontab 관련 파일에 대한 접근 제한 -(위험도 : 상)		
정보시스템 현황	문제점	점검기준
<pre> else umask 022 fi for i in /etc/profile.d/*.sh /etc/profile.d/sh.local ; do if [-r "\$i"]; then if ["\${-#*i}" != "\$-"]; then else "\$i" >/dev/null fi fi done unset i unset -f nathmunne </pre>	<p>/etc/crontab 권한을 살펴본 결과 other의 권한이 write 권한이 부여되어 있지 않아 양호함</p>	양호
조치 현황	개선사항	점검기준

[시스템 보안]		
3.2 PATH 환경 변수 설정 -(위험도 : 상)		
정보시스템 현황	문제점	점검기준
<pre> /usr/local/bin:/usr/local/sbin:/usr/bin:/usr /sbin:/bin:/sbin:/home/admin/.local/bin:/home admin/bin </pre>	<p>"echo #PATH"의 값을 살펴본 결과 ‘.’ 등의 길이 포함되어있지 않아 양호함.</p>	양호
조치 현황	개선사항	점검기준

[시스템 보안] 3.3 UMASK 설정 -(위험도 : 상)		
정보시스템 현황	문제점	점검기준
<pre>[root@localhost etc]# umask 0022</pre>	<p>셸에서 umask을 확인결과 umask값이 022로 설정되어있어 양호함.</p>	양호
조치 현황	개선사항	점검기준

[시스템 보안] 3.4 hosts 파일의 권한 설정 -(위험도 : 상)		
정보시스템 현황	문제점	점검기준
<pre>[root@localhost etc]# ls -al hosts -rw-r--r--. 1 root root 158 Jun 7 2013 hosts</pre>	<p>/etc/hosts의 other의 접근 권한을 확인한 결과 접근권한이 부여되어있지 않아 양호함.</p>	양호
조치 현황	개선사항	점검기준

[시스템 보안] 3.5 inetd.conf 파일의 권한 설정 -(위험도 : 상)		
정보시스템 현황	문제점	점검기준
<pre>[root@localhost etc]# ls -al hosts -rw-r--r--. 1 root root 158 Jun 7 2013 hosts</pre>	/etc/hosts의 other의 접근 권한을 확인한 결과 접근권한이 부여되어있지 않아 양호함.	양호
조치 현황	개선사항	점검기준

[시스템 보안] 3.6 hosts.equiv 파일의 권한 설정 -(위험도 : 상)		
정보시스템 현황	문제점	점검기준
<pre>[root@localhost etc]# ls -al hosts -rw-r--r--. 1 root root 158 Jun 7 2013 hosts</pre>	파일이 존재하지않아 N/A	N/A
조치 현황	개선사항	점검기준

[서비스 보안] 4.1 서비스 파일권한 설정 -(위험도 : 상)		
정보시스템 현황	문제점	점검기준
<pre>[root@localhost etc]# ls -al hosts -rw-r--r--. 1 root root 158 Jun 7 2013 hosts</pre>	/etc/services의 other의 write 권한을 확인한결과 write 권한이 부여되어있지 않아 양호함.	양호
조치 현황	개선사항	점검기준

[서비스 보안] 4.2 기타 서비스 설정 -(위험도 : 중)		
정보시스템 현황	문제점	점검기준
<pre>echo 7/tcp echo 7/udp discard 9/tcp discard 9/udp</pre>	/etc/service 파일에서 불필요한 서비스 확인결과, echo, discard 이확인 되므로 취약함.	취약
조치 현황	개선사항	점검기준
<pre>#echo 7/tcp #echo 7/udp #discard 9/tcp #discard 9/udp</pre>	/etc/service 파일에서 echo등 불필요한 포트를 disable처리해 양호함.	양호

[서비스 보안] 4.3 서비스 Banner 관리 -(위험도 : 하)		
정보시스템 현황	문제점	점검기준
<pre>[admin@localhost etc]\$ cat issue \S Kernel \r on an \m</pre>	<p>/etc/issue 점검결과 (시스템정보가 노출되어 취약)아무정보가 없어 양호</p> <p>telnet, ftp, smtp 서비스는 제공하지 않아 양호함</p>	양호
조치 현황	개선사항	점검기준

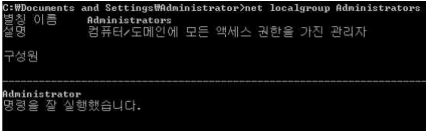

[서비스 보안] 4.4 SNMP 서비스 설정 -(위험도 : 상)		
정보시스템 현황	문제점	점검기준
<pre>[admin@localhost etc]\$ ps -ef grep snmp admin 11931 2836 0 21:39 pts/0 00:00:00 grep --color=auto s nmp [admin@localhost etc]\$</pre>	<p>프로세스 확인결과 SNMP가 서비스 되고 있지 않아 양호함.</p>	양호
조치 현황	개선사항	점검기준

[로그관리 및 보안패치]		
5.1 syslog 기록 설정 -(위험도 : 중)		
정보시스템 현황	문제점	점검기준
<pre># The authpriv file has restricted access. authpriv.* /var/log/secure # Log all the mail messages in one place. mail.* -/var/log/maillog # Log cron stuff cron.* /var/log/cron # Everybody gets emergency messages *.emerg :omusrmsg:* # Save news errors of level crit and higher in a special file. uucp,news.crit /var/log/spooler # Save boot messages also to boot.log local7.* /var/log/boot.log</pre>	<p>etc/syslog.conf 파일확인결과 시스템 보안 수준을 고려한 로그 를 남기고 있어 양호함.</p>	양호
조치 현황	개선사항	점검기준

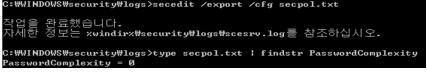
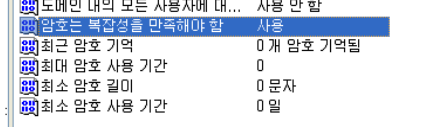
[로그관리 및 보안패치]		
5.2 su 로그를 기록 설정 -(위험도 : 상)		
정보시스템 현황	문제점	점검기준
<pre># Log anything (except mail) of level info or higher. # Don't log private authentication messages! *.info;mail.none;authpriv.none;cron.none /var/log/messages # The authpriv file has restricted access. authpriv.* /var/log/secure # Log all the mail messages in one place. mail.* -/var/log/maillog</pre>	<p>/etc/syslog.conf 파일 확인 결 과 su 로그가 설정되지 않아 취약 함.</p>	취약
조치 현황	개선사항	점검기준
<pre># Log all the mail messages in one place. mail.* -/var/log/maillog authpriv.info /var/log/sulog</pre>	<p>etc/syslog.conf 파일에서 su 로그를 남길 수 있도록 설정해주 어 조치함.</p>	양호

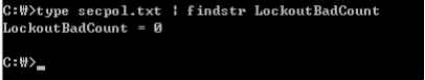
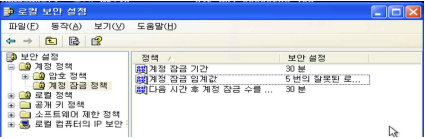
[로그관리 및 보안패치]		
5.3 보안패치 -(위험도 : 상)		
정보시스템 현황	문제점	점검기준
유지보수 일지----	<p>시스템 유지보수 업체를 통해서 정기적으로 보안패치를 수행하고 있어 양호함</p> <p>-----</p> <p>유지보수가 안되어 있는 시스템 응용프로그램의 영향 보안패치 불가능</p>	취약
조치 현황	개선사항	점검기준

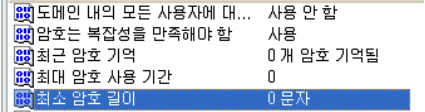
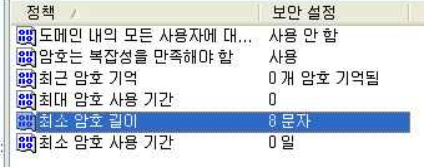
3.2 Windows 서버


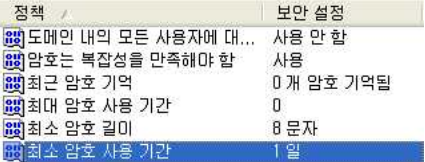
[계정관리]		
1.1 관리자 그룹에 최소한의 사용자 포함 -(위험도 : 상)		
정보시스템 현황	문제점	점검기준
	대상시스템의 Administrators 그룹의 존재하는 계정이 1개로 양호함.	양호
조치 현황	개선사항	점검기준
	불필요한 계정을 삭제조치함.	

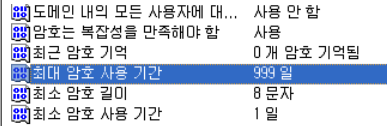

[계정관리]		
1.2 Guest 계정 비활성화-(위험도 : 상)		
정보시스템 현황	문제점	점검기준
	<p>명령프롬프트에서 “net user” 명령어를 사용하여 확인한결과 비활성화 되어있어 양호함.</p>	양호
조치 현황	개선사항	점검기준

[계정관리]		
1.3 패스워드 복잡도 설정-(위험도 : 중)		
정보시스템 현황	문제점	점검기준
	<p>대상시스템의 패스워드 복잡도를 점검한 결과 설정값이 “0” 으로 되어있어 취약함.</p>	취약
조치 현황	개선사항	점검기준
	<p>대상시스템의 패스워드 복잡도 설정값을 1로 설정하여 조치함.</p>	

[계정관리]		
1.4 계정 잠금 임계값 설정-(위험도 : 상)		
정보시스템 현황	문제점	점검기준
 <pre>C:\W>type secpol.txt findstr LockoutBadCount LockoutBadCount = 0 C:\W></pre>	<p>계정잠금 임계값이 “0” 으로 설정되어있어 brute force, Dictionary attack에 위협이 있으므로 취약함</p>	취약
조치 현황	개선사항	점검기준
	<p>대상시스템의 계정잠금 임계값을 “5” 로 설정하여 조치함.</p>	

[계정관리]		
1.5 패스워드 최소 길이 설정-(위험도 : 중)		
정보시스템 현황	문제점	점검기준
	<p>대상시스템의 패스워드 최소길이 가 설정되어있지 않아 취약함</p>	취약
조치 현황	개선사항	점검기준
	<p>대상시스템의 패스워드 최소길이 설정을 8자리로 설정하여 조치함.</p>	

[계정관리]		
1.6 패스워드 최소 사용기간 설정-(위험도 : 중)		
정보시스템 현황	문제점	점검기준
	<p>최소암호기한이 0으로 설정되어 있어서 패스워드 변경없이 지속 사용가능하므로 취약함.</p>	취약
조치 현황	개선사항	점검기준
	<p>패스워드 최소사용기간을 1로 설정하여 조치함.</p>	

[계정관리]		
1.7 패스워드 최대 사용기간 설정-(위험도 : 중)		
정보시스템 현황	문제점	점검기준
	<p>패스워드 최대 사용기간이 60일 이상으로 설정되어 취약함</p>	취약
조치 현황	개선사항	점검기준
	<p>패스워드 최대사용기간 설정을 60일로 설정하여 조치함.</p>	