	Apache 보안 설정 팁 httpd.apache.org/docs/1.3/misc/security_tips.html (Version 1.3) httpd.apache.org/docs/2.0/misc/security_tips.html (Version 2.0) httpd.apache.org/docs/2.2/misc/security_tips.html (Version 2.2) Apache 보안 모듈 사용 mod_security : www.modsecurity.org (참고서적) Apache Security O' relly Book www.apachesecurity.net/download/apachesecurity-ch02.pdf www.thinkingstone.com/talks/Apache_Web_Platform_Security.pdf	

라우터 장비 보안 설정(Cisco 장비 기준)

항목	상세설명	체크
보안 패치	**1. 라우터 IOS는 최신 버전이거나 또는 최신 보안 업데이트하였는가?** (주요 네트워크 장비의 경우 가용성 때문에 오히려 최신버전의 IOS가 장애를 일으킬 수도 있어 운영자들이 업데이트를 꺼려하는 경향이 있으나, Critical한 보안 문제를 내포하는 버전의 경우 반드시 긴급패치를 해야 함)	

운영	1. 적절한 배너를 사용하고 있는가? (Banner)
	`Router(config)# banner exec ^C`
	2. 로그인 시간을 제어하고 있는가?
	`Router(config)# line con 0`
	`Router(config-line)# exec-timeout 15 0`
	`Router(config)# line vty 0 4`
	`Router(config-line)# exec-timeout 10 0`
	3. NTP를 통한 시간 동기화를 하고 있는가?
	`Router(config)# ntp update-calendar`
	`Router(config)# ntp server xxx.xxx.xxx.xxx`
	4. 설정 파일은 주기적으로 백업하고 있는가?
	5. 원격접근시 SSH를 사용하고 있는가?
	`Router(config)# line vty 0 4`
	`Router(config-line)# transport input ssh`
	6. 적절한 DNS 서버가 명시되어 있는가?
	`Router(config)# ip domain-lookup`
	`Router(config)# ip name-server xxx.xxx.xxx.xxx`
	또는
	`Router(config)# no ip domain-lookup`
	7. 일반 사용자 모드와 특권 모드의 패스워드가 다르게 지정되어 있는가?	

8. 라우팅 프로토콜 사용시 AS간 또는 피어 라우터에 MD5 인증을 적절히 구현하였는가?

(프로토콜별 예제)

BGP	router bgp 100 neighbor external-peers peer-group neighbor xxx.xxx.xxx.xxx remote-as 200 neighbor xxx.xxx.xxx.xxx peer-group external-peers neighbor yyy.yyy.yyy.yyy remote-as 300 neighbor yyy.yyy.yyy.yyy peer-group external-peers neighbor xxx.xxx.xxx.xxx password xxxxxxxxxx neighbor xxx.xxx.xxx.xxx password xxxxxxxxxx
OSPF	interface Ethernet0 ip address xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy ip ospf message-digest-key 10 md5 xxxxxxxxxx router ospf 10 network xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy area 0 area 0 authentication message-digest
EIGRP	interface Ethernet0 ip address xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy ip authentication mode eigrp 1 md5 ip authentication key-chain eigrp 1 mypassword . key chain xxxxxxxxxxx key 12345 key-string abcdefg accept-lifetime infinite . router eigrp 1 network zzz.zzz.zzz.zzz no auto-summary

9. 주요 지점 네트워크 장비에서는 비공인 IP(RFC1918)를 필터링하여 IP Spoofing에 대응하고 있는가?

로깅

1. 라우터 장비 접속 로깅을 하고 있는가?

① 인증서버가 있다면, aaa logging을 적용하고 로그를 남기고 있는가?

② 로그에 timestamp를 남기고 있는가?

③ ACL 위반 패킷들을 로깅하고 있는가?

```
Router(config)# access-list 3 deny any log
Router(config)# access-list 101 deny any log
```

〈참고 : Logging 방식〉

○ Buffered Logging : 로그를 라우터 장비에 버퍼크기만큼 남김

```
Router(config)# logging on
Router(config)# logging buffered [size] debugging
Router(config)# service timestamp log date msec local show-timezone
```

ㅇ Syslog Logging : 로그를 원격 호스트에 514/udp를 통해 전달

```
Router(config)# logging on
Router(config)# logging host xxx.xxx.xxx.xxx
Router(config)# logging console critical
Router(config)# logging trap informational
Router(config)# logging facility local7
```

〈참고 : Logging Level〉

로깅레벨	보안수준	설명
Emergencies	0	
Alerts	1	즉각적인 조치 필요
Critical	2	치명적인 수준
Errors	3	에러 수준
Warnings	4	경고 수준
Notifications	5	보통이지만 알림 수준
Informational	6	정보 수준
Debugging	7	디버깅 메시지

2. 로그파일은 주기적으로 백업하고 있는가?

불필요 서비스 제거

1. 불필요한 AUX 라인이 제거되었는가?

```
Router(config)# line aux 0
Router(config-line)# transport input none
Router(config-line)# no exec
Router(config-line)# no password
```

2. 불필요한 서비스는 중단하였는가?

```
Router(config)# no service udp-small-servers          (echo, discard,
Router(config)# no service tcp-small-servers          daytime 등 중지)
Router(config)# no service finger                     (fingerd 중지)
Router(config)# no service tftp                       (tftp 서비스 중지)
Router(config)# no service pad                        (X.25 중지)
Router(config)# no ip bootp server                    (booting server 중지)
Router(config)# no service config                     (네트워크를 통해
Router(config)# no boot network                       config 파일을
Router(config)# no boot system                        읽어오는 설정중지)
Router(config)# no boot host
Router(config)# no ip source-route                    (IP Spoofing 대응)
Router(config)# no ip http server                     (웹서비스 중지)
Router(config-if)# no ip redirects                    (라우팅테이블변경악용)
Router(config-if)# no ip unreachables                 (스캐닝공격대응)
Router(config-if)# no ip directed-broadcast           (Smurf Attack 대응)
Router(config-if)# no ip proxy-arp                    (ARP 서비스 중지)
Router(config-if)# no ip mask-relay                   (netmask요청응답중지)
```

3. FTP, RCP, RSH 등과 관련된 다음 라인들이 존재하지 않는가?

```
ftp-server enable
ip rcmd rcp-enable
ip rcmd rsh-enable
transport input rlogin telnet
```

안전한 설정 (show running-config)

1. 라우터 안전한 패스워드를 사용하고 있는가?

[Console 접속시(물리적인 접근 필요)]

```
Router(config)# line con 0
Router(config-line)# password xxxxxx
Router(config-line)# service password-encryption
```

[Virtual Terminal 접속 시 (Telnet 등을 통한 원격접근 시)]

```
Router(config)# enable secret xxxxxx
```

➔ enable secret0이 가장 우선이지만 같은 패스워드를 쓰지 않도록 주의

```
Router(config)# line vty 0 4
Router(config-line)# transport input none
Router(config-line)# no exec
Router(config-line)# exec-timeout 0 1
```

➔ 원격접속 자체가 필요없는 소규모 사업장인 경우 telnet listener 다운

〈참고 : Password 저장방식〉
ㅇType0 : Config 파일에 누구나 읽을 수 있는 평문으로 저장
service password-encryption 명령어로 Type7 암호화 가능
ㅇType5 : MD5의 해시함수를 사용하여 복호화가 불가능, 가장 안전함
ㅇType7 : Vigenere Algorithm을 사용하여 암호화하나 역함수 존재

2. 접근통제(ACL)를 하고 있는가?

ㅇ 유의사항 및 예제
- access-list 룰을 원격접속에 적용시 access-class 사용
  ➔ access-class [ACL#] {in|out}
- access-list 룰을 특정 인터페이스에 적용시 access-group 사용
  ➔ access-group [ACL#] {in|out}
- access-list는 중복설정 불가
- 해당 룰의 마지막에는 항상 “deny any any” 가 추가됨
- access-list의 룰의 여러 개일 때 특정라인만 삭제/변경 불가

```
Router(config)# access-list 10 permit host xxx.xxx.xxx.xxx
Router(config)# access-list 10 permit host yyy.yyy.yyy.yyy
Router(config)# access-list 10 deny any log
Router(config)# access-list 100 deny tcp any any eq 135
Router(config)# access-list 100 deny ip host x.x.x.x host y.y.y.y
Router(config)# access-list 100 permit tcp any any
Router(config)# line vty 0 4
Router(config-line)# access-class 10 in
Router(config-line)# exit
Router(config)# int s0
Router(config-if)# ip access-group 100 in
Router(config)# access-list 100 deny ip zz.zz.zz.zz yy.yy.yy.yy any log
```

〈참고 : Access-List 유형과 사용법〉
ㅇstandard access-list : 패킷의 소스IP로만 허용/차단 (1~99)
➔ access-list [ACL#] {permit|deny} {src IP wildcard|any}
ㅇextended access-list : 소스IP, 목적지IP, Port, Protocol 등으로 확장하여 허용/차단 (100~199)
➔ access-list [ACL#] {permit|deny} [ip|tcp|udp|icmp] {src IP wildcard|any|host} {dst IP wildcard|any|host}

3. SNMP(Simple Network Management Protocol) 접근제한을 하고 있는가?

① Community String은 쉽게 추측할 수 없는 문자열로 설정했는가?
② SNMP RO(Read Only)와 RW(Read Write) 문자열을 다르게 설정했는가?
③ 암호화가 지원되는 상위 SNMP(v3)를 사용하고 있는가?

➔ snmp-server community [string] {ro|rw} [ACL#]

```
Router(config)# access-list 10 permit host 7.7.7.5
Router(config)# snmp-sever community xxxxxx RO 10
```

4. 사용자 계정을 통해 인증을 하고 있는가?

```
Router(config)# username xxxxxxx password 7 xxxxxxxxxxx
```

5. 인증서버가 있다면 적절히 구성되었는가? (AAA 서버)

① 인증서버를 이용하여 원격접근시 구성을 적절히 하고 있는가?

```
Router(config)# aaa new-model
Router(config)# aaa authentication login [list-name] tacacs+ local
.
Router(config)# tacacs-server host x.x.x.x
Router(config)# tacacs-server key xxxxxxx
Router(config)# line vty 0 4
Router(config)# login authentication [list-name]
```

② 인증서버를 이용하여 SSH,SCH 구성을 적절히 하고 있는가?

```
Router(config)# aaa new-model
Router(config)# aaa authentication login default group tacacs+
Router(config)# aaa authorization exec default group tacacs+
.
Router(config)# ip ssh time-out 120
Router(config)# ip ssh authentication-retries 3
Router(config)# ip scp server enable
```

참고 사이트	Cisco Router 공식 IOS 사이트 www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_category_home.html www.cisco.com/warp/public/732/updatesw.shtml 참고사이트 www.windowsecurity.com/whitepapers/Cisco_Router_Security_Overview.html

PC 보안 체크리스트(Windows XP 기준)

항목	상세설명	체크
보안 패치	**1. 현재 사용하는 운영체제 버전에 대하여 최신보안패치를 하였는가?** Internet Explorer → **도구** → Windows Update 사이트 **2. 서비스팩이 설치되어 있는가?** **3. 자동 업데이트를 사용하고 있는가?** 시작 → 설정 → 제어판 → 보안센터 → 자동업데이트를 사용함으로 설정	
주요 Tool	**1. 바이러스 백신을 설치하고 최신 버전의 엔진으로 업데이트하였는가?** **2. 윈도우에서 기본적으로 제공하고 있는 개인 방화벽을 사용하고 있는가?** 시작 → 설정 → 제어판 → 네트워크 연결 → 로컬영역 연결 속성 → 고급 탭 → 윈도우 방화벽 사용 → 예외 탭에서 예외 프로그램 / 포트 추가 **3. 스파이웨어/애드웨어 제거 프로그램을 설치하고 최신 업데이트하였는가?** 4. 기타 무상/상용 침입차단시스템 또는 개인 방화벽이 있는가? 5. 사용하고 있는 소프트웨어(오피스 등)는 주기적으로 업데이트하고 있는가? 6. 사내 전용 PC보안 프로그램으로 통제하고 있는가? (존재시)	
불필요 요소 제거	**1. 불필요한 공유를 중지하였는가?** ① 시작 → 설정 → 제어판 → 관리도구 → 컴퓨터 관리 → 시스템 도구 → 공유폴더 → 공유 → 불필요한 공유 폴더 중지 ② 시작 → 실행 → cmd.exe C:₩ net share [공유폴더명] /delete ③ 시작 → 실행 → regedit.exe (레지스트리 편집) KEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩lanmanserver ₩parameters (키 생성하기) Value Name : AutoShareWks Type : REG_DWORD Value : 0 **2. 널세션을 제거하였는가? (IPC$)** 시작 → 실행 → secpol.msc → 로컬보안정책 → 보안옵션 → 네트워크 액세스 : SAM계정과 공유의 익명열거 허용안함을 사용함 설정 3. 드라이브 전체를 공유하거나 공유폴더 설정이 잘못되어 있지는 않은가? 4. 불필요한 서비스를 제거하였는가? SMTP, FTP , World Wide Web Publishing, NNTP, IIS ADMIN MSSQLServer / MySQL 등 DB서버, Telnet, Terminal Services, Messenger Service, SNMP Service, SNMP Trap Service 등	
안전한 설정	**1. 웹브라우저의 보안 설정을 하였는가?** ① Internet Explorer → 도구 → 인터넷 옵션 → 보안 → 보통이상 설정 ② Internet Explorer → 도구 → 인터넷 옵션 → 내용 → 자동완성 비활성화 **2. 불필요한 ActiveX가 존재하는가?** C:₩windows₩Downloaded Program Files	

	3. ActiveX 컨트롤에 대해 서명되지 않은 플러그인은 통제하고 있는가? Internet Explorer → 도구 → 인터넷 옵션 → 보안 → 사용자 지정 수준 → ActiveX 컨트롤 및 플러그인 관련설정 서명 안 된 ActiveX 컨트롤 다운로드 : 사용안함 안전하지 않는 것으로 표시된 ActiveX 컨트롤 초기화 및 스크립트 : 사용안함 ActiveX 컨트롤에 대해 자동으로 확인 : 사용안함 4. 메신저를 사용하는 경우 자동로그인이나 자동저장기능을 해제하였는가? 5. 주요메시지나 파일은 암호화하여 전송하는가? 6. 웹메일을 사용하는 경우 보안접속 기능을 사용하여 로그인하는가? **7. P2P 프로그램으로 출처를 알 수 없는 파일을 받았거나, 웹에서 다운로드받은 프로그램을 실행하기 전 백신프로그램으로 해당 파일을 검사하고 있는가?** **8. 메일 클라이언트에서 '사용할 IE' 보안영역을 제한된 사이트로 한정했는가?** **9. 공유 폴더 설정시 Everyone 그룹을 제거하고 특정 사용자에게 읽기/쓰기 권한을 명확히 주고 있는가?** 10. 원격지원이 불가능하도록 설정되어 있는가? 내컴퓨터 → 속성 → 원격 → 원격지원 요청/사용자 원격연결 체크박스 해제 11. 관리자 계정 administrator를 다른 이름으로 바꾸었는가?	
관리	**1. CMOS 또는 로그온시 패스워드를 설정하였는가?** **2. 8자 이상의 길이로 영문자, 숫자, 특수문자 등이 혼용된 비밀번호를 쓰고 있으며 주기적으로 변경하는가?** **3. 불필요한 사용자 계정을 삭제했는가?** 시작 → 제어판 → 관리도구 → 컴퓨터 관리 → 시스템 도구 → 로컬 사용자 및 그룹 → 사용자 → Guest 등 불필요한 계정 사용 안 함 4. 화면 보호기의 암호를 설정하였는가? 바탕화면 오른쪽 마우스 버튼 → 등록정보 → 디스플레이 등록정보 → 화면보호기 → 암호사용 → 변경 5. NTFS 파일 시스템을 사용하고 사용자별로 접근통제를 하는가? C:₩ convert drive_letter: /fs:ntfs **6. 출처가 불분명한 이메일이나 수상한 첨부파일이 있는 경우 확인하지 않고 바로 삭제하고 있는가?** **7. 웹사이트 방문시 보안경고 창이 뜰 경우 신뢰할 수 있는 기관에 대해서만 프로그램 설치에 동의하는가?** **8. 주요 데이터는 주기적으로 별도의 저장장치에 백업하고 있는가?** **9. 금융 거래용 공인인증서는 USB와 같은 별도 저장장치에 보관하고 있는가?** 10. 사용하지 않을 때 PC를 인터넷에 연결하여 켜놓지는 않는가? 11. 침해사고가 발생했을 시 대응방법과 신고절차를 숙지하고 있는가?	
참고 사이트	[FAT->NTFS 변경] technet.microsoft.com/en-us/library/bb456984.aspx www.microsoft.com/protect/yourself/home/office.mspx	

▌유닉스(UNIX) 보안 체크리스트

항목	상세설명	체크
보안 패치	**1. 현재 사용하는 운영체제 버전에 대하여 최신 Patch를 적용하였는가?** **2. 보안 업데이트 주기를 설정하고, 정기적으로 수행하고 있는가?** **3. 사용하고 있는 소프트웨어는 최신 버전으로 유지하고 있는가?** **4. 특히 SUID, SEUID가 설정된 파일 중에서 버퍼 오버 플로우 등 공개된 취약점을 내포하고 있는 파일들은 최신 Patch를 적용하였는가?** 〈참고 : Overflow 취약성이 많이 공개된 서비스들〉 RPC, SNMP, NFS, X Window, BIND, OpenSSH, OpenSSL 의 낮은 버전	
주요 Tool	**1. TCP Wrapper를 사용하여 접속제한을 하고 있는가?** ① /etc/hosts.deny 파일 내용을 "ALL:ALL"로 구성하여 불필요한 호스트로부터의 서비스 접근통제를 하고 있는가? ② /etc/hosts.allow 파일에서 인가된 관리자에게만 권한이 허용되어 있는가? ③ 각 설정 파일은 일반 사용자가 읽을 수 없도록 600 권한을 주었는가? ④ /etc/inetd.conf 내의 모든 TCP 서비스를 wrapping 하고 있는가? 2. Iptables와 같은 방화벽(방화벽을 따로 사용하지 않을 경우)에서 Inbound Traffic에 대한 접근통제(INPUT, OUTPUT, FORWARD)를 하고 있는가? **3. Tripwire 등 무결성 검사 소프트웨어를 정기적으로 수행하여 시스템상 변경 여부를 정기적으로 확인하고 있는가?** 4. John the Ripper 등의 도구를 이용하여 패스워드 점검을 정기적으로 수행하는가? (암호가 없는 계정, 추측 가능한 암호 사용 등) 5. nmap 등의 포트 스캐닝 도구를 이용하여 로컬시스템에서 불필요한 포트에 대한 점검을 정기적으로 수행하는가? **6. 평문으로 전송하는 Telnet, ftp 대신 OpenSSH와 같은 공개툴을 이용하여 암호화된 통신을 하고 있는가?** **7. Cron 등 정기적으로 수행할 수 있는 도구을 이용하여 주요 보안 리포트를 정기적으로 관리자에게 리포팅하는가?** 8. chkrookit 등과 같은 백도어 설치 탐지 툴을 이용하여 주기적으로 시스템 내 백도어 존재 유무를 점검하고 있는가?	
불필요 요소 제거	**1. 반드시 필요한 소프트웨어만 설치되었는가?** **2. 불필요한 계정은 삭제되었는가?** 3. /etc/hosts 파일에 불필요한 시스템이 포함되어 있지는 않은가? **4. 보안상 취약한 setuid, seteuid, setgid가 제거되었는가?** # find / -type f ₩(-perm -04000 -o -perm -02000 ₩) -exec ls -lg {} ₩; 5. 소유자가 없거나 그룹 아이디가 없는 파일이 존재하지 않는가? # find / -type f -nouser -o -nogroup -print 6. 누구나 변경할 수 있는 민감한 파일(World-Writable)은 존재하지 않는가? # find / -type f -perm -2 -print **7. NFS를 사용하여 불필요하거나 민감한 디렉토리가 마운트되지 않았는가?** # showmount -e	

8. Cron 데몬에 불필요하게 자원을 낭비하는 사용자/프로세스는 제거되었는가?
9. DoS 공격에 취약한 네트워크 서비스와 불필요한 서비스가 제거되었는가?

tcpmux	1/tcp	unrpc	111/tcp
echo	7/tcp	etbios-ns	137/tcp
echo	7/udp	etbios-ns	137/udp
discard	9/tcp	etbios-dgm	138/tcp
discard	9/udp	etbios-dgm	138/udp
systat	11/tcp	etbios-ssn	139/tcp
daytime	13/tcp	etbios-ssn	139/udp
daytime	13/udp	map	143/tcp
netstat	15/tcp	nmp	161/udp
chargen	19/tcp	nmp-trap	162/udp
chargen	19/udp	dmcp	177/udp
ftp	21/tcp	xec	512/tcp
ssh	22/tcp	iff	512/udp
telnet	23/tcp	login	513/tcp
smtp	25/tcp	who	513/udp
domain (DNS)	53/tcp	shell	514/tcp
domain (DNS)	53/udp	syslog	514/udp
bootps	67/tcp	printer	515/tcp
bootps	67/udp	talk	517/udp
bootpc	68/tcp	ntalk	518/udp
bootpc	68/udp	route	520/udp
tftp	69/udp	klogind	543/tcp
finger	79/tcp	socks	1080/tcp
http	80/tcp	nfs	2049/tcp
pop2	109/tcp	nfs	2049/udp
pop3	110/tcp	X11	6000+n/tcp

안전한 설정

1. /etc/passwd 파일은 적절히 구성되었는가?

① 사용자 패스워드는 암호화되어 /etc/shadow에 존재하는가?
② UID가 0인(루트 권한) 사용자가 존재하는가?
③ GID가 0인(루트 권한) 사용자가 존재하는가?
④ 추측하기 쉬운 패스워드를 사용하는 사용자가 존재하는가?
⑤ 벤더 기본 계정(daemon, bin, adm, lp, uucp 등)에 shell이 부여되어 있는가?
⑥ 패스워드 에이징(Aging,일정기간 이상이면 변경 또는 잠금) 정책이 있는가?

- /etc/default/passwd
  ➔ MAXWEEKS, MINWEEKS, PASSLENGTH 설정

〈참고〉
/etc/shadow 파일 필드 내용
[(1)아이디 : (2)암호화된 패스워드:최근 패스워드 변경일 : (3)패스워드를 변경해야 하는 최소일수 : (4)변경한 패스워드를 사용할 수 있는 최대일수 : (5)패스워드를 변경하도록 강제하는 경고일수 : (6)패스워드가 만기된 후 실제 사용중지까지 일수 : (7)사용중지날짜]

2. 원격 접속시 루트로 로그인할 수 없도록 통제되어 있는가?

① /etc/securetty (HP-UX) : CONSOLE
/etc/default/login (Solaris) : CONSOLE=/dev/console

② 파일 권한은 600으로 설정하였는가?

3. /etc/inetd.conf 은 적절히 구성되었는가?

① 소유자는 root이고 파일 권한은 600으로 설정하였는가?

② r 시리즈 명령어 (rlogin, rsh, rexec)는 사용하지 않고 있는가?
만일 사용하고 있다면, 접근통제를 철저하게 하고 있는가?

③ ttdb, cmsd, tftp 등 보안에 취약한 데몬은 제거되었는가?

4. /etc/hosts.equiv, $HOME/.rhosts 파일이 존재한다면, 적절히 구성되었는가?

① "+","+ +" 설정(임의의 사용자과 권한 획득가능 상태)이 금지되었는가?

② 사용하지 않는다면, /dev/null로 링크되어 있는가?

③ 일반 사용자들이 자신의 홈디렉토리에서 생성할 수 없도록 통제하는가?

④ 소유자는 root이며, 파일 권한은 600으로 설정하였는가?

5. 일정시간이 지난 후 자동 로그아웃하는 session timeout이 설정되었는가?
(예제) /etc/system ➔ set swip:tcpidletimeout=100
/etc/default/login ➔ TIMEOUT=300

6. 서버 접근시(telnet, ssh, ftp 등) IP별 접근 제한을 설정하였는가?

7. 비로그인 데몬은 root가 아닌 nobody 권한으로 동작하고 있는가?

8. 시스템 환경변수 PATH에 현재 디렉토리를 의미하는 . 이 제거되었는가?

9. 파일/디렉토리 권한은 다음과 같이 설정되어 있는가?

파일/디렉토리	권한 (소유자)
사용자 홈디렉토리, 히스토리 파일, /boot 로그인시 환경설정 파일 등	700 (사용자)
cron.allow, cron.deny, at.allow, at.deny initd.d 디렉토리, rc.d 디렉토리	755 이하
/var/log 내 각종 로그파일 (wtmp, dmesg, xferlog, messages,lastlog 등) /etc/services, /etc/motd, /etc/syslog.conf	644 (Root)
/etc, /bin, /sbin,, /usr/bin, /usr/sbin. 등	741 (Root)
/tmp, /var/tmp	1777 (Root)

10. /etc/profile의 umask가 027로 설정되어 있는가?
〈참고〉

권한	umask	권한 통제
744	022	Group, Others 쓰기 권한
741	026	Group 쓰기 권한, Others 읽기/쓰기 권한
740	027	Group 쓰기 권한, Others 읽기/쓰기/실행 권한
700	077	Group, Others 읽기/쓰기/실행 권한

11. 일반 사용자가 로컬 시스템에서 리소스 사용을 제한하고 있는가?
(생성 가능한 최대 프로세스 개수, 최대 메모리 크기 등)

12. 네트워크 서비스의 경우 배너 설정을 하여 버전 정보를 숨기고 있는가?
/etc/default/telnetd, /etc/default/ftpd ➔ BANNER=" banner_information"

13. 보안에 관련된 적절한 커널 튜닝을 하였는가?

① Smurf 공격 대응
ndd -set /dev/ip ip_forward_directed_broadcasts 0

	② SYN Flooding 공격 대응 # ndd -set /dev/tcp tcp_conn_req_max_q0 512 ③ IP Forwarding 공격 대응 # ndd -set /dev/ip ip_forwarding 0 ④ Source Routing 공격 대응 # ndd -set /dev/ip ip_ip_forward_src_routed 0 14. /dev 에 디바이스 이외의 파일이 존재하는가? # find /dev -type f -exec ls -l {} ₩; 15. 일반 사용자가 스택 상에서 프로그램 실행 방지를 위한 설정이 존재하는가? /etc/system ➔ set noexec_user_stack=1, set noexec_user_stack_log=1 16. 일반 사용자가 주요 시스템 명령어(su, last, ifconfig, gcc 등)을 사용하지 못하도록 접근 권한을 설정하였는가?	
관리	**1. 적절한 패스워드 정책이 존재하는가?** ① 주요 패스워드 변경은 ○○일, 그 외는 ○○일마다 변경하는가? ② 최소 ○자 이상 길이로 영문자, 숫자, 특수문자를 혼용하여 사용하는가? ③ 안전한 패스워드를 사용하기 위해 패스워드 조합 툴을 실행하는가? ④ ○회 로그인 실패시 로그인 계정을 잠그도록 하는가? ⑤ 사용자의 패스워드를 저장시켜 놓지 않고 있는가? ⑥ 기본 계정이 기본 패스워드를 갖지 않도록 하는가? **2. BIOS와 부트 매니저(존재시)에 패스워드를 사용하고 있는가?** 3. 주요 파일들은 백업하고 복구하는 절차를 따르고 있는가? (일별, 주별, 월별) (예제) # ufsdump 0uf /dev/rmt/0 /home # ufsrestore xvf /dev/rmt/0 /home 4. 비정상적인 로그인 접속을 로깅하고 있는가? (예제) /etc/default/login ➔ RETRIES=5 5. 주기적으로 로그를 분석하고 있는가? 6. 침해사고가 발생했을 시 대응방법과 신고절차를 숙지하고 있는가?	
참고 사이트	1. UNIX 관련 공식 패치 및 보안 홈페이지 [Sun Solaris] ftp://sunsolve1.sun.com/pub/patches/ http://sunsolve.sun.com/show.do?target=patchpage [HP-UX] http://www4.itrc.hp.com/service/patch/mainPage.do [IRIX] http://www.sgi.com/support/security/ http://www.sgi.com/support/security/advisories.html [BSD/OS] http://www.bsdi.com/services/support/patches/ http://www.bsdi.com/services/support/ [FreeBSD] ftp://ftp.freebsd.org/pub/FreeBSD/releases/ http://www.freebsd.org/security/	

	[NetBSD] http://www.netbsd.org/support/security/ [OpenBSD] ftp://ftp.openbsd.org/pub/OpenBSD/patches/ http://openbsd.org/errata.html 2. CERT.org UNIX 체크리스트 http://www.cert.org/tech_tips/usc20_full.html 3. Useful Tools : http://sectools.org/ [Portsentry] http://sourceforge.net/projects/sentrytools/ [tcpdump] http://www.tcpdump.org/ [tcp wrapper] ftp://ftp.porcupine.org/pub/security/ [Tripwire] http://www.tripwire.com/ [lsof] http://freshmeat.net/projects/lsof/ [openssh] http://www.openssh.com/ [nessus] http://www.nessus.org/ [nmap] http://insecure.org/ [iptables] http://security.maruhn.com/ [SAINT] http://www.saintcorporation.com [SARA] http://www-arc.com/sara/ [john the ripper] http://www.openwall.com/john/ [Ethreal] http://www.ethereal.com/ [antisniff] http://www.securitysoftwaretech.com/antisniff/ [snort] http://www.snort.org/	

▌리눅스(Linux) 보안 체크리스트(배포판에 종속되지 않는 일반적인 리눅스 환경)

항목	상세설명	체크
보안 패치	**1. 현재 사용하는 리눅스 배포판의 커널 패치를 적용하였는가?** **2. 사용하고 있는 공개 소프트웨어는 최신 버전으로 유지하고 있는가?** **3. SUID, SEUID가 설정된 파일 중에서 특히 버퍼 오버 플로우 등 공개된 취약점을 내포하고 있는 파일들은 최신 패치를 적용하였는가?** 〈참고 : Overflow 취약성이 많이 공개된 서비스들〉 RPC, SNMP, NFS, X Window, BIND, OpenSSH, OpenSSL 의 낮은 버전	
주요 Tool	**1. TCP Wrapper를 사용하여 접속제한을 하고 있는가?** ① /etc/hosts.deny 파일 내용을 "ALL:ALL"로 구성하여 불필요한 호스트로부터의 서비스 접근통제를 하고 있는가? ② /etc/hosts.allow 파일에서 인가된 관리자에게만 권한이 허용되어 있는가? ③ 각 설정 파일은 일반 사용자가 읽을 수 없도록 600 권한을 주었는가?	

```
service telnet
{
        flags         = REUSE NAMEINARGS
        protocol      = tcp
        socket_type = stream
        wait          = no
        user          = telnetd
        server        = /usr/sbin/tcpd
        server_args = /usr/sbin/in.telnetd
}
```

2. Iptables와 같은 방화벽(방화벽을 따로 사용하지 않을 경우)에서 Inbound Traffic에 대한 접근통제(INPUT, OUTPUT, FORWARD)를 하고 있는가?
3. **Tripwire 등 무결성 검사 소프트웨어를 정기적으로 수행하여 시스템상 변경 여부를 정기적으로 확인하고 있는가?**
4. John the Ripper 등의 도구를 이용하여 패스워드 점검을 정기적으로 수행하는가? (암호가 없는 계정, 추측 가능한 암호 사용 등)
5. Nessus, nmap 등의 공개 스캐닝 도구를 이용하여 로컬시스템의 취약점과 불필요한 포트에 대한 점검을 정기적으로 수행하는가?
6. **평문으로 전송하는 Telnet, ftp 대신 OpenSSH, OpenVPN과 같은 공개툴을 이용하여 암호화된 통신을 하고 있는가?**
7. **Cron, At 등 정기적으로 수행할 수 있는 도구을 이용하여 주요 보안 리포트를 정기적으로 관리자에게 리포팅하는가?**
8. PORTSENTRY와 같은 공개 침입탐지 및 방어 툴을 사용하고 있는가?
9. chkrookit 등과 같은 백도어 설치 탐지 툴을 이용하여 주기적으로 시스템 내 백도어 존재 유무를 점검하고 있는가?
10. **PAM, ulimit 등을 활용하여 일반 사용자에게 리소스 제한을 하고 있는가?**
    ① 사용 가능한 메모리를 제한하고 있는가?
    ② 생성할 수 있는 프로세스를 제한하고 있는가?
    ③ 로그인 동시접속을 제한하고 있는가?
    ④ Core 파일을 생성하지 않고 있는가?
    /etc/pam.d/login ➔ session required /lib/security/pam_limits.so
    /etc/security/limits.conf ➔ core, rss, nproc, maxlogins 설정

불필요 요소 제거

1. **/etc/rc.d/init.d 내 불필요한 서비스가 중지되었는가?**
   (예제) # chkconfig –list | grep 3:on
   # ls -l /etc/rc.d/rc3.d/S*

   〈참고 – 꼭 필요한지 확인해야 할 서비스〉
   apmd, xntpd, portmap, sound, netfs, rstatd, rusersd, rwhod, rwalld, named, bootparamd, squid, yppasswdd, ypservd, dhcpd, atd, pcmcia, snmpd, ,routed, lpd, mars-new, nfs, amd, gated, sendmail, httpd, ypbind, xfs, innd, linuxconf

2. **불필요한 계정은 삭제되었는가?**
3. /etc/hosts 파일에 불필요한 시스템이 포함되어 있지는 않은가?
4. **보안상 취약한 suid, sgid가 제거되었는가?**

find / -type f ₩(-perm -04000 -o -perm -02000 ₩) -exec ls -lg {} ₩;
(예제) # chmod u-s /usr/bin/chage

5. 소유자가 없거나 그룹 아이디가 없는 파일이 존재하지 않는가?
find / -type f -nouser -o -nogroup -print

6. 누구나 변경할 수 있는 민감한 파일(World-Writable)은 존재하지 않는가?
find / -type f -perm -2 -print

7. NFS를 사용하여 불필요하거나 민감한 디렉토리가 마운트되지 않았는가?
showmount -e

8. Cron 데몬에 불필요하게 자원을 낭비하는 사용자/프로세스는 제거되었는가?

9. 불필요한 포트가 오픈되어 리스닝하고 있는가? # netstat -a

안전한 설정

1. /etc/passwd 파일은 적절히 구성되었는가?

① 사용자 패스워드는 암호화되어 /etc/shadow에 존재하는가?
② UID 또는 GID가 0인(루트 권한) 사용자가 존재하는가?
③ 추측하기 쉬운 패스워드를 사용하는 사용자가 존재하는가?
④ 벤더 기본 계정(daemon, bin, adm, lp, uucp 등)에 shell이 부여되어 있는가?
⑤ 패스워드 에이징(Aging,일정기간 이상이면 변경 또는 잠금) 정책이 있는가?
- /etc/login.defs
➔ PASS_MIN_DAYS, PASS_MAX_DAYS, PASS_MIN_LEN, PASS_WARN_AGE

〈참고〉
/etc/shadow 파일 필드 내용
[(1)아이디 : (2)암호화된 패스워드 (3)최근 패스워드 변경일 : (4)패스워드를 변경해야 하는 최소일수 : (5)변경한 패스워드를 사용할 수 있는 최대일수 : (6)패스워드를 변경하도록 강제하는 경고일수 : (7)패스워드가 만기된 후 실제 사용중지까지 일수 : (8)사용중지날짜]

2. 원격 접속시 루트로 로그인할 수 없도록 통제되어 있는가?

① /etc/securetty : console
② 파일 권한은 600으로 설정하였는가?

3. /etc/xinetd.conf 은 적절히 구성되었는가?

① 파일 권한은 600으로 설정하였는가?
② r 시리즈 명령어 (rlogin, rsh, rexec)는 사용하지 않고 있는가?
③ /etc/xinetd.d 내 보안에 취약한 데몬은 제거되었는가?

4. 파일/디렉토리 권한은 다음과 같이 설정되어 있고 정기적으로 점검하는가?

파일/디렉토리	권한 (소유자)
사용자 홈디렉토리, 히스토리 파일 로그인시 환경설정 파일 등	700 (사용자)
Cron 데몬의 cron.allow, cron.deny, at.allow, at.deny Initd.d 디렉토리, Rc.d 디렉토리	755 이하
/var/log 내 각종 로그파일 (wtmp, dmesg, xferlog, messages,lastlog 등) /etc/services, /etc/aliases, /etc/motd, /var/log/wtmp, /var/run/utmp, /etc/syslog.conf, /etc/fstab, /etc/passwd, /etc/group	644 (Root)
/etc, /bin, /sbin,, /usr/bin, /usr/sbin. 등	741 (Root)
/tmp, /var/tmp	1777 (Root)

5. /etc/profile의 umask가 027로 설정되어 있는가?
〈참고〉

권한	umask	권한 통제
744	022	Group, Others 쓰기 권한
741	026	Group 쓰기 권한, Others 읽기/쓰기 권한
740	027	Group 쓰기 권한, Others 읽기/쓰기/실행 권한
700	077	Group, Others 읽기/쓰기/실행 권한

6. /etc/hosts.equiv, $HOME/.rhosts 파일이 존재한다면, 적절히 구성되었는가?
① "+","+ +" 설정(임의의 사용자과 권한 획득가능 상태)이 금지되었는가?
② 사용하지 않는다면, /dev/null로 링크되어 있는가?
(예제) # ln -s /dev/null /etc/hosts.equiv
ln -s /dev/null /.rhosts
③ 일반 사용자들이 자신의 홈디렉토리에서 생성할 수 없도록 통제하는가?

7. 서버 접근시(telnet, ssh, ftp 등) IP별 접근 제한을 설정하였는가?

8. 비로그인 데몬은 root가 아닌 nobody 권한으로 동작하고 있는가?

9. 시스템 환경변수 PATH에 현재 디렉토리를 의미하는 . 이 제거되었는가?
 # echo $PATH

10. 일정시간이 지난 후 자동 로그아웃하는 session timeout이 설정되었는가?
(예제) /etc/default/login ➔ TIMEOUT=300

11. 일반 사용자가 로컬 시스템에서 리소스 사용을 제한하고 있는가?
(생성 가능한 최대 프로세스 개수, 최대 메모리 크기 등)

12. 네트워크 서비스의 경우 배너 설정을 하여 버전 정보를 숨기고 있는가?

13. 보안에 관련된 적절한 커널 튜닝을 하였는가?
① Smurf 공격 대응
sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1
② SYN Flooding 공격 대응
sysctl -w net.ipv4.tcp_max_syn_backlog=1280 (백로그 큐 증가)
sysctl -w net.ipv4.tcp_syncookies=1 (공격시 로깅 메시지 출력)
③ ICMP Redirect 비허용 (임의의 라우팅 테이블 변경 방지)
sysctl -w net.ipv4.conf.eth0.accept_redirects=0
sysctl -w net.ipv4.conf.lo.accept_redirects=0
sysctl -w net.ipv4.conf.default.accept_redirects=0
sysctl -w net.ipv4.conf.all.accept_redirects=0
④ Source Route 패킷 비허용
sysctl -w net.ipv4.conf.eth0.accept_source_route=0
sysctl -w net.ipv4.conf.lo.accept_source_route=0
sysctl -w net.ipv4.conf.default.accept_source_route=0
sysctl -w net.ipv4.conf.all.accept_source_route=0
⑤ Proxy ARP 미설정
sysctl -w net.ipv4.conf.eth0.proxy_arp=0
sysctl -w net.ipv4.conf.lo.proxy_arp=0
sysctl -w net.ipv4.conf.default.proxy_arp=0
sysctl -w net.ipv4.conf.all.proxy_arp=0

	14. /dev 에 디바이스 이외의 파일이 존재하는가? (예제) # find /dev -type f -exec ls -l {} ₩; 15. 일반 사용자가 스택 상에서 프로그램 실행 방지를 위한 설정이 존재하는가? (예제) /etc/system ➔ set noexec_user_stack=1 16. 일반 사용자는 제한적인 쉘을 사용하고 있는가? **17. 일반 사용자가 주요 시스템 명령어(su, last, ifconfig, gcc 등)을 사용하지 못하도록 접근 권한을 설정하였는가?**	
관리	**1. 적절한 패스워드 정책이 존재하는가?** ① 주요 패스워드 변경은 OO일, 그 외는 OO일마다 변경하는가? ② 최소 O자 이상 길이로 영문자, 숫자, 특수문자를 혼용하여 사용하는가? ③ 안전한 패스워드를 사용하기 위해 패스워드 조합 툴을 실행하는가? ④ O회 로그인 실패시 로그인 계정을 잠그도록 하는가? ⑤ 사용자의 패스워드를 저장시켜 놓지 않고 있는가? ⑥ 기본 계정이 기본 패스워드를 갖지 않도록 하는가? **2. BIOS와 부트 매니저(존재시)에 패스워드를 사용하고 있는가?** **3. SUDO를 사용하여 루트 권한을 제한하고 있는가?** **4. Root만이 Cron에 접근하도록 설정되었는가?** **5. 로컬/원격 시스템 접근시 적절한 배너가 설정되었는가?** /etc/motd, /etc/issue, /etc/issue.net 4. 주요 파일들은 백업하고 복구하는 절차를 따르고 있는가? (일별, 주별, 월별) 5. 비정상적인 로그인 접속을 로깅하고 있는가? (예제) /etc/default/login ➔ RETRIES=5 5. 주기적으로 로그(messages, secure, maillog 등)를 분석하고 있는가? 6. 침해사고가 발생했을 시 대응방법과 신고절차를 숙지하고 있는가?	
참고 사이트	1. 리눅스 배포판 공식 보안 홈페이지 Calera http://www.calderasystems.com/support/security/ Debian http://www.debian.org/security/ Mandrake http://www.linux-mandrake.com/en/security/ Redhat http://www.redhat.com/security/ Slackware http://www.sastk.org/ SuSe http://www.suse.com/us/support/security/index.html Turbo http://www.turbolinux.com/cgi-bin/security/index.cgi?mode=all Gentoo http://www.gentoo.org/security/en/index.xml Selinux http://www.nsa.gov/selinuX/ 2. 국내 리눅스 포털 http://www.superuser.co.kr 3. Useful Tools : http://sectools.org/ [Portsentry] http://sourceforge.net/projects/sentrytools/ [tcpdump] http://www.tcpdump.org/ [tcp wrapper] ftp://ftp.porcupine.org/pub/security/ [Tripwire] http://www.tripwire.com/ [lsof] http://freshmeat.net/projects/lsof/ [openssh] http://www.openssh.com/	

	[nessus] http://www.nessus.org/ [nmap] http://insecure.org/ [iptables] http://security.maruhn.com/ [SAINT] http://www.saintcorporation.com [SARA] http://www-arc.com/sara/ [john the ripper] http://www.openwall.com/john/ [Ethreal] http://www.ethereal.com/ [antisniff] http://www.securitysoftwaretech.com/antisniff/ [snort] http://www.snort.org/ [lids] http://www.lids.org/ 4. X window 보안 http://www.stanford.edu/services/securecomputing/x-window/	

Windows 2000 Server 보안 체크리스트

항목	상세설명	체크
보안 패치	**1. 현재 사용하는 운영체제 버전에 대하여 주기적으로 업데이트하고 있는가?** Internet Explorer → 도구 → Windows Update 사이트 **2. 서비스팩이 설치되어 있는가?** **3. 자동 업데이트를 사용하고 있는가?**	
주요 Tool	1. 바이러스 백신을 설치하였는가? 2. 윈도우에서 기본적으로 제공하고 있는 개인 방화벽을 사용하고 있는가? 시작 → 설정 → 제어판 → 네트워크 연결 → 로컬영역 연결 속성 → 고급 탭 → 윈도우 방화벽 사용 → 예외 탭에서 예외 프로그램 / 포트 추가 3. 스파이웨어 제거 프로그램을 주기적으로 실행하는가? 4. 기타 무상/상용 침입차단시스템 또는 개인 방화벽이 있는가?	
불필요 요소 제거	**1. 불필요한 [숨김] 공유를 중지하였는가?** ① 시작 → 설정 → 제어판 → 관리도구 → 컴퓨터 관리 → 시스템 도구 → 공유폴더 → 공유 → 불필요한 공유 폴더 중지 ② 시작 → 실행 → cmd.exe C:₩ net share [공유폴더명] /delete ③ 시작 → 실행 → regedit.exe (레지스트리 편집) HKLM₩SYSTEM₩CurrentControlSet₩Services₩lanmanserver₩ Value Name : AutoShareWks Type : REG_DWORD Value : 0 **2. 널세션을 제거하였는가? (IPC$, 레지스트리 편집)** HKLM₩SYSTEM₩CurrentControlSet₩Control₩LSA Value Name: RestrictAnonymous	

	Data Type: REG_DWORD Value: 1 3. 익명(Anonymous)의 네트워크 공유는 제한되었는가? 3. 불필요한 자동 시작 서비스는 제거되었는가? 시작 → 실행 → services.msc 4. 프린터 공유 권한이 있다면, 일반 사용자에게 불필요한 권한이 제거되었는가? 5. 넷미팅을 통한 원격 데스크탑 공유가 해제되었는가? 6. 불필요한 컴포넌트가 설치되어 있지 않은가?	
안전한 설정	**1. 관리자로 자동 로그인되는 기능을 해제하였는가?** HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩Winlogon Value Name: AutoAdminLogon Data Type: REG_SZ Value Data: 0 2. 로그온 캐시 사용을 해제하였는가? HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩Winlogon Value Name: CachedLogonsCount Data Type: REG_SZ Value Data: 2 이하 3. 레지스트리에 익명 접근을 통제하고 있는가? HKLM₩System₩CurrentControlSet₩Control₩SecurePipeServers₩Winreg Administrators : all 4. 로컬로 로그온시 경고 메시지가 출력되는가? 5. 스크린 세이버가 패스워드로 보호되어 있는가? 6. CMOS 패스워드는 설정되어 있는가? **7. 공유 폴더 설정시 특정 사용자에게 읽기/쓰기 권한을 명확히 주고 있는가?**	
관리	**1. 시스템 접근시 경고문을 사용하고 있는가?** HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩Winlogon Value Name: LegalNoticeCaption Data Type: REG_SZ Value Data: "경고문" **2. 불필요한 사용자 계정을 삭제했는가?** 시작 → 제어판 → 관리도구 → 컴퓨터 관리 → 시스템 도구 → 로컬 사용자 및 그룹 → 사용자 → Guest 등 불필요한 계정 사용 안 함 **3. 패스워드 정책설정이 적절하게 구성되었는가?** ① 사용자 패스워드는 최소 0 이상을 강제하는가? ② 패스워드는 0일 이후 만기되고 있는가? ③ 0회 잘못된 시도에 로그아웃되고 ○분 후 초기화되는가? ④ 복잡도를 만족하는 패스워드를 사용하도록 강제하는가? 4. NTFS 파일 시스템을 사용하고 있는가?	

5. 사용자 권한이 적절히 할당되어 있는가?

사용자 권한	도메인 컨트롤러	멤버 서버
네트워크에서 액세스 가능	Administrators Authenticated Users Enterprise Domain Controllers	Administrators Users
백업파일과 디렉토리	Administrators Backup Operators	Administrators Backup Operators
바이패스 순환 체킹	Authenticated Users	Users
시스템 시간 변경	Administrators	Administrators
페이지 파일 생성	Administrators	Administrators
토큰 객체 생성	(None)	(None)
글로벌 객체 생성	SERVICE, Administrators	SERVICE, Administrators
공유 객체 생성	(None)	(None)
프로그램 디버깅	Administrators	Administrators
네트워크에서 액세스 제한	Guests	Guests
로컬에서 로그온 제한	Guests	Guests
컴퓨터와 사용자 계정에 트러스트 위임 가능	Administrators	(None)
원격 시스템에서 강제종료	Administrators	Administrators
쿼터 증가	Administrators	Administrators
스케줄링 우선순위 변경	Administrators	Administrators
장치 드라이버 로딩	Administrators	Administrators
로컬에서 로그온 가능	Administrators Backup Operators	Administrators Backup Operators
감사 및 보안 로그 관리	Auditor's Group (Exchange Enterprise Servers Group)	Auditor's Group (Exchange Enterprise Servers Group on Exchange server)
펌웨어 환경변수 수정	Administrators	Administrators
파일 및 디렉토리 복구	Administrators Backup Operators	Administrators Backup Operators
시스템 종료	Administrators	Administrators
디렉토리 서비스 데이터 동기화	Not checked (Checked in AD STIG Checklist)	N/A

6. 도메인 컨트롤러 사용시 적절한 커버러스 정책이 반영되었는가?
   ① 사용자 로그온 제한이 설정되어 있는가?
   ② 서비스 티켓 최대 시간(Service Ticket Lifetime)이 설정되어 있는가?
   ③ 사용자 티켓 최대 시간(User Ticket Lifetime)이 설정되어 있는가?
   ④ 사용자 티켓 갱신시간 (User Ticket Renewal Lifetime)이 설정되어 있는가?
   ⑤ 시간 동기화 (Clock Synchronization)이 설정되어 있는가?

7. 이벤트 로깅을 적절히 설정하고 주기적으로 분석하고 있는가?

%SystemRoot%₩System32₩CONFIG₩AppEvent.evt

%SystemRoot%₩System32₩CONFIG₩SecEvent.evt

	%SystemRoot%₩System32₩CONFIG₩SysEvent.evt ① 시스템/보안/응용프로그램의 최대 로그사이즈가 설정되었는가? ② 네트워크를 통한 이벤트 로그 접근이 제한되었는가? ③ 보안 이벤트를 ○개월 이상 보존하고 있는가? **8. 이벤트 감사권한를 적절히 설정하고 주기적으로 검사하고 있는가?** 9. 침해사고가 발생했을 시 대응방법과 신고절차를 숙지하고 있는가?	
참고 사이트	[Security Templates] http://support.microsoft.com/kb/321679 [Win2K Server] www.microsoft.com/technet/archive/security/chklist/w2ksvrcl.mspx	

DB 보안 체크리스트

<table>
<tr><th>항목</th><th>상세설명</th><th>체크</th></tr>
<tr><td>보안 패치</td><td>1. 사용하고 있는 DB는 최신 버전의 보안 업데이트를 적용하였는가?
2. 보안 업데이트 주기를 설정하고, 정기적으로 수행하고 있는가?</td><td></td></tr>
<tr><td>불필요 요소 제거</td><td>1. 데이터베이스 디폴트 계정(아이디, 패스워드)을 변경 또는 제거하였는가?
〈참고〉
<table>
<tr><th>오라클 기본 계정</th><th>MS SQL 기본 계정</th></tr>
<tr><td>scott/tiger
system/manager
dbsnmp/dbsnmp
tracesvr/trace
sys/change_on_install
sapr3/sap
demo/demo
outln/outln
mtssys/mtssys
ordsys/ordsys
ordplugins/ordplugins
mdsys/ddsys
ctxsys/ctxsys
adams/wood
blake/paper
jones/steel
clark/cloth
auroraorbunauthenticated/invalid
wksys/wksys
olapsys/manager
olapdba/olapdx
LBACSYS/LBACSYS
olapsvr/instance</td><td>sa / null
probe / null
MySQL 기본 계정
root / null
null / null
mysql / null
Sybase 기본계정
sa / sa</td></tr>
</table>
2. 데이터베이스 초기 설치시 꼭 필요한 Product만 설치하였는가?
3. 시스템 권한 및 오브젝트 권한은 Public으로부터 제거되었는가?</td><td></td></tr>
</table>