1. 취약점 진단 및 모의해킹 개요

❖ 취약점 진단

- ◆ IT 운영환경에 대한 취약점 진단 및 보호대책을 수립하여 정보보호 수준 향상
- ◆ 웹 취약점 진단 및 소스코드 취약점 진단
- ◆ 서버 OS, DBMS, WEB, WAS, NETWORK, 보안장비 보안 취약점 진단
- ◆ 보호대책 및 개선과제 제시

❖ 모의해킹

- ◆ 실제 해킹과 동일한 형태의 공격을 통해 실제적인 보안 취약점 확인 및 제거 방안 제시
- ◆ 내/외부 시스템 모의해킹
- ◆ APT 진단(내부 정보 유출진단)
- ◆ 진단 대상 및 개선과제 제시

2. 취약점 진단 방법론

사전협의단계

1. SYSTEM 취약점 프로젝트 요청
2. 담당자 미팅 (유선/오프라인)
3. 진단 기준 선정 (기반시설/금취분평)
4. 진단 대상 선정 (OS, Middleware 등)
5. 진단 기간 선정 (진단 수 대비 인력)

정보수집단계

1. 진단 정보 요청
2. 오픈 포트 분석
3. 데몬 분석
4. 계정 분석
5. 진단 대상 최종 FIX

취약점 진단단계

1. 진단 수행
2. 보안 담당자 인터뷰
3. 시스템담당자 인터뷰

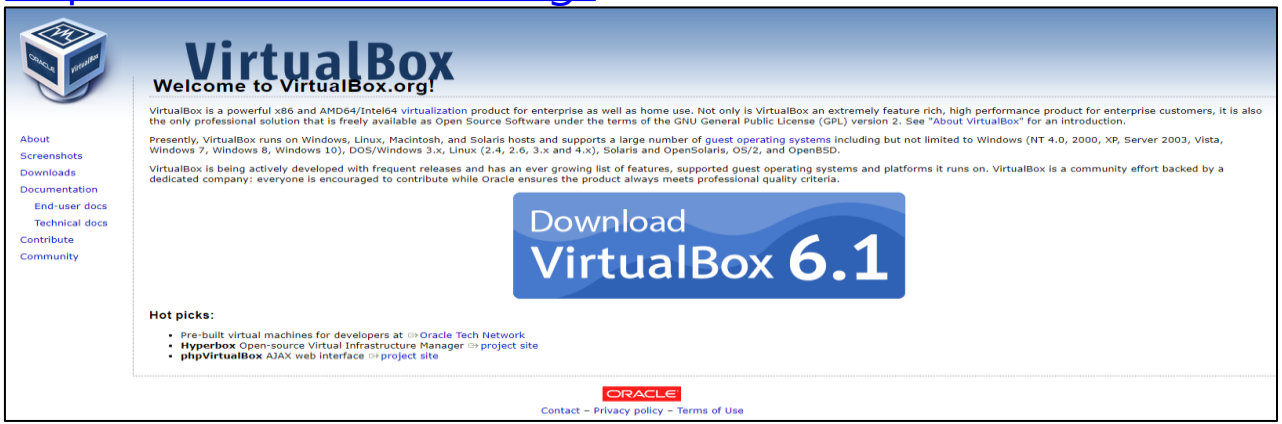
보고서 작성 및 프로젝트 종료 단계

1. 결과 보고서 작성
2. 결과 보고서 리뷰
3. 산출물 제출
4. 데이터 클렌징
5. 프로젝트 종료

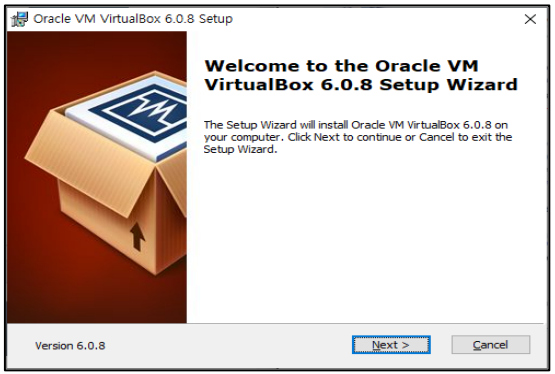
3. SYSTEM 환경분석

❖ VirtualBox 설치 (가상환경구성)

- ◆ https://www.virtualbox.org/ 접속



- ◆ 다운로드 및 설치

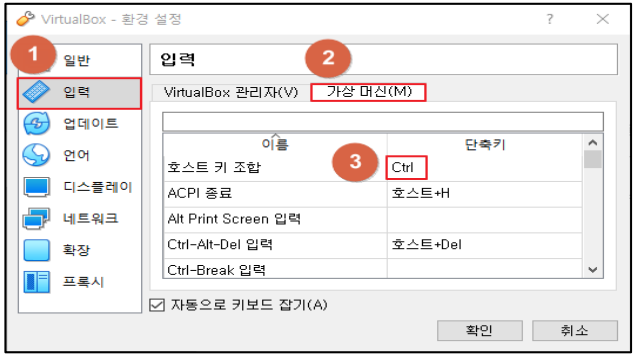


3. SYSTEM 환경분석

❖ VirtualBox 설정 (호스트 키 조합)

◆ 환경 설정 선택

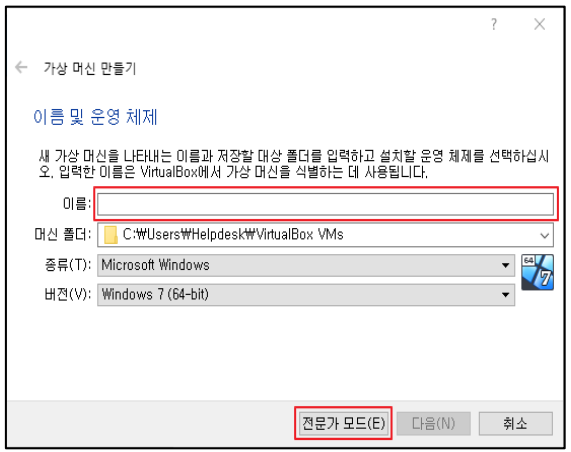
◆ 호스트 키 조합 단축키 설정

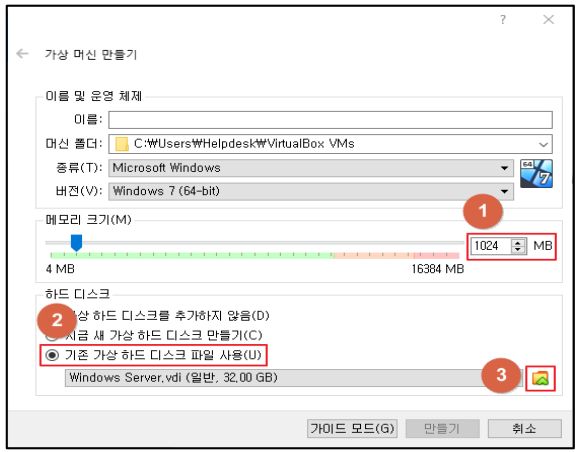


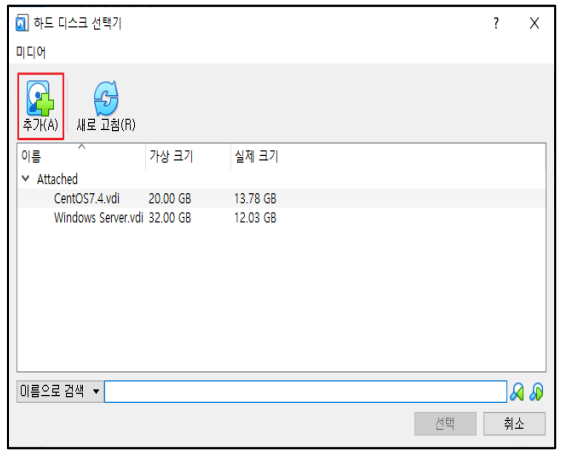
3. SYSTEM 환경분석

❖ VirtualBox 설정 (가상이미지 추가)

◆ 가상이미지 "새로 만들기" 메뉴를 통한 설정







3. SYSTEM 환경분석

❖ VirtualBox 설정 (가상이미지 구동)

- ◆ 가상이미지 구동 확인
- ◆ 현 사용중인 Local PC IP주소 확인
- ◆ Putty를 통한 가상 머신 SSH 접근

3. SYSTEM 환경분석

❖ 기본정보

◆ OS

- -

◆ DBMS

- -

◆ WEB Server

- -

◆ WAS

- -

3. SYSTEM 환경분석

❖ 포트분석 (예시)

```
[root@localhost ~]# netstat -tlnp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address  Foreign Address        State       PID/Program name
tcp        0      0 0.0.0.0:3306   0.0.0.0:*              LISTEN      2000/mysqld
tcp        0      0 0.0.0.0:111    0.0.0.0:*              LISTEN      1437/rpcbind
tcp        0      0 0.0.0.0:44209  0.0.0.0:*              LISTEN      1497/rpc.statd
tcp        0      0 0.0.0.0:22     0.0.0.0:*              LISTEN      1861/sshd
tcp        0      0 127.0.0.1:631  0.0.0.0:*              LISTEN      1538/cupsd
tcp        0      0 127.0.0.1:25   0.0.0.0:*              LISTEN      2102/master
```

Proto	Local Address	Well Known 여부	Foreign Address	Program name	비고
tcp	0.0.0.0:**22**	Y (ssh)	0.0.0.0:*	sshd	SSH 연결 Port
tcp	0.0.0.0:**3306**	Y (mysql)	0.0.0.0:*	mysqld	DBMS(mysql) 서비스 Port

3. SYSTEM 환경분석

❖ Daemon 분석 (예시)

```
[root@localhost ~]# ps -ef | grep "httpd₩|mysql₩|rpc*"
rpc        1437      1  0 Mar16 ?        00:00:00 rpcbind
rpcuser    1497      1  0 Mar16 ?        00:00:00 rpc.statd
root       1898      1  0 Mar16 ?        00:00:00 /bin/sh /usr/bin/mysqld_safe --datadir=/var/lib/mysql --
socket=/var/lib/mysql/mysql.sock --pid-file=/var/run/mysqld/mysqld.pid --basedir=/usr --user=mysql
mysql      2000   1898   0 Mar16 ?        00:01:58 /usr/libexec/mysqld --basedir=/usr --
datadir=/var/lib/mysql --user=mysql --log-error=/var/log/mysqld.log --pid-
file=/var/run/mysqld/mysqld.pid --socket=/var/lib/mysql/mysql.sock
apache    24342   2142   0 Mar21 ?        00:00:00 /usr/sbin/httpd
apache    24343   2142   0 Mar21 ?        00:00:00 /usr/sbin/httpd
```

RUSER	Daemon Command	목적	Daemon 경로	비고
root	mysqld_safe	mysql_safe 구동 확인	datadir=/var/lib/mysql	
mysql	mysqld	mysql 구동	datadir=/var/lib/mysql	

3. SYSTEM 환경분석

❖ 계정 분석 (예시)

```
[root@localhost ~]# cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
adiosl:x:500:500:adiosl:/home/adiosl:/bin/bash
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
cubrid:x:501:501::/home/cubrid:/bin/bash
```

Username	Account Info	Home directory	Command/shell	비고
root	관리자 계정	/root	/bin/bash	
mysql	mysql 구동 계정	/var/lib/mysql	/bin/bash	

3. SYSTEM 환경분석

❖ 분석 총평

- ◆ 기본 정보
  - -
- ◆ Port 정보
  - -
  - -
- ◆ Daemon 정보
  - -
  - -
- ◆ 계정 정보
  - -
  - -

4. ’21년 주요정보통신기반시설 Unix 항목 Review

분류	항목코드	점검항목	항목 중요도
1. 계정관리	U-01	root 계정 원격 접속 제한	상
	U-02	패스워드 복잡성 설정	상
	U-03	계정 잠금 임계값 설정	상
	U-04	패스워드 파일 보호	상
	U-44	root 이외의 UID가 '0' 금지	중
	U-45	root 계정 su 제한	하
	U-46	패스워드 최소 길이 설정	중
	U-47	패스워드 최대 사용 기간 설정	중
	U-48	패스워드 최소 사용기간 설정	중
	U-49	불필요한 계정 제거	하
	U-50	관리자 그룹에 최소한의 계정 포함	하
	U-51	계정이 존재하지 않는 GID 금지	하
	U-52	동일한 UID 금지	중
	U-53	사용자 shell 점검	하
	U-54	Session Timeout 설정	하
2. 파일 및 디렉터리 관리	U-05	root 홈, 패스 디렉터리 권한 및 패스 설정	상
	U-06	파일 및 디렉터리 소유자 설정	상
	U-07	/etc/passwd 파일 소유자 및 권한 설정	상
	U-08	/etc/shadow 파일 소유자 및 권한 설정	상
	U-09	/etc/hosts 파일 소유자 및 권한 설정	상
	U-10	/etc/(x)inetd.conf 파일 소유자 및 권한 설정	상
	U-11	/etc/syslog.conf 파일 소유자 및 권한 설정	상
	U-12	/etc/services 파일 소유자 및 권한 설정	상
	U-13	SUID,SGID,Stick bit 설정 파일 점검	상
	U-14	사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정	상
	U-15	world writable 파일 점검	상
	U-16	/dev에 존재하지 않는 device 파일 점검	상
	U-17	$HOME/.rhosts, hosts.equiv 사용 금지	상
	U-18	접속 IP 및 포트 제한	상
	U-55	hosts.lpd 파일 소유자 및 권한 설정	하
	U-56	UMASK 설정 관리	중
	U-57	홈디렉토리 소유자 및 권한 설정	중
	U-58	홈디렉토리로 지정한 디렉토리의 존재 관리	중
	U-59	숨겨진 파일 및 디렉토리 검색 및 제거	하

분류	항목코드	점검항목	항목 중요도
3. 서비스 관리	U-19	finger 서비스 비활성화	상
	U-20	Anonymous FTP 비활성화	상
	U-21	r 계열 서비스 비활성화	상
	U-22	cron 파일 소유자 및 권한설정	상
	U-23	Dos 공격에 취약한 서비스 비활성화	상
	U-24	NFS 서비스 비활성화	상
	U-25	NFS 접근 통제	상
	U-26	Utomountd 제거	상
	U-27	RPC 서비스 확인	상
	U-28	NIS , NIS+ 점검	상
	U-29	tftp, talk 서비스 비활성화	상
	U-30	Sendmail 버전 점검	상
	U-31	스팸 메일 릴레이 제한	상
	U-32	일반사용자의 Sendmail 실행 방지	상
	U-33	DNS 보안 버전 패치	상
	U-34	DNS Zone Transfer 설정	상
	U-35	웹서비스 디렉토리 리스팅 제거	상
	U-36	웹서비스 웹 프로세스 권한 제한	상
	U-37	웹서비스 상위 디렉토리 접근 금지	상
	U-38	웹서비스 불필요한 파일 제거	상
	U-39	웹서비스 링크 사용 금지	상
	U-40	웹서비스 파일 업로드 및 다운로드 제한	상
	U-41	웹서비스 웹 서비스 영역의 분리	상
	U-60	ssh 원격접속 허용	중
	U-61	ftp 서비스 확인	하
	U-62	ftp 계정 shell 제한	중
	U-63	Ftpusers 파일 소유자 및 권한 설정	하
	U-64	Ftpusers 파일 설정	중
	U-65	at 파일 소유자 및 권한 설정	중
	U-66	SNMP 서비스 구동 점검	중
	U-67	SNMP 서비스 커뮤니티스트링의 복잡성 설정	중
	U-68	로그온 시 경고 메시지 제공	하
	U-69	NFS 설정파일접근권한	중
	U-70	expn, vrfy 명령어 제한	중
	U-71	Apache 웹 서비스 정보 숨김	중
4. 패치 관리	U-42	최신 보안패치 및 벤더 권고사항 적용	상
5. 로그 관리	U-43	로그의 정기적 검토 및 보고	상
	U-72	정책에 따른 시스템 로깅 설정	하

4. ’21년 주요정보통신기반시설 Unix 항목 Review

❖ SYSTEM OS(Linux) 진단 항목 리뷰

1. 계정 관리

코드	항목명	중요도	항목 리뷰 내용
U-01	root 계정 원격 접속 제한	상	Unix 계열 서버를 원격으로 접근하는 방식은 크게 Telnet, SSH 방식이 존재합니다. Telnet과 SSH는 계정과 패스워드를 모두 입력해서 접근하는 방식은 모두 동일하지만 패킷 상에서의 암호화를 처리하는 부분이 크게 차이가 납니다. 해당 항목은 대상 서버에 접근할 경우 Telnet 사용은 지양해야 하며 만약 SSH 방식으로 접근할 시 “root” 계정으로의 직접적인 접근은 차단해야 합니다.
U-02	패스워드 복잡성 설정	상	"/etc/pam.d/system-Uth" 설정 파일 내 패스워드 복잡도가 “영문, 숫자, 특수문자”를 조합하여 최소 8자리 이상으로 설정되어 있는지 확인해야 합니다. 패스워드 복잡도의 기준은 각각의 회사마다 관리하고 있는 “정보보호정책” 및 “정보보호지침”에 의거해서 기준이 상이 할 수 있습니다.
U-03	계정 잠금 임계값 설정	상	"/etc/pam.d/system-Uth" 설정 파일 내 임계값이 5회, 잠금 시간이 60분(3600초)으로 설정되어 있는지 확인해야 합니다. 패스워드 복잡도의 기준은 각각의 회사마다 관리하고 있는 “정보보호정책” 및 “정보보호지침”에 의거해서 기준이 상이 할 수 있습니다.
U-04	패스워드 파일 보호	상	사용자 계정의 패스워드 암호화를 관장하는 대표적인 파일은 “shadow”로써 해당 파일의 존재 유무와 실제 모든 계정이 기록되어 있는 “passwd” 파일 내 로그인이 가능한 모든 사용자 계정이 암호화 되어 있는지 확인해야 합니다.
U-44	root 이외의 UID가 '0' 금지	중	UID는 User ID를 뜻하는 번호로써 “0”의 숫자를 부여 받은 계정은 최고관리자로 사용할 수 있습니다. Unix 계열 서버에서 기본적으로 UID가 “0”인 계정은 “root”가 유일 하여 시스템 계정 및 로그인이 가능한 모든 사용자 계정의 UID가 “0”을 사용하고 있는지 확인이 필요합니다.
U-45	root 계정 su 제한	하	Unix 계열 OS에서 로그인을 가장 안전하게 관리할 수 있는 방법은 하기와 같습니다. 1) “일반 사용자 계정”(UID 500 이상) 로그인 2) “/etc/group” 파일 내 “wheel” 그룹에 허용된 일반사용자 추가 3) “/bin/su” 파일에 타사용자 특수권한 제거

4. ’21년 주요정보통신기반시설 Unix 항목 Review

❖ SYSTEM OS(Linux) 진단 항목 리뷰

1. 계정 관리

코드	항목명	중요도	항목 리뷰 내용
U-46	패스워드 최소 길이 설정	중	"/etc/login.defs" 설정 파일 내 패스워드 길이가 8자리 이상으로 설정되어 있는지 확인해야 합니다. 패스워드 복잡도의 기준은 각각의 회사마다 관리하고 있는 “정보보호정책” 및 “정보보호지침”에 의거해서 기준이 상이 할 수 있습니다.
U-47	패스워드 최대 사용기간 설정	중	"/etc/login.defs" 설정 파일 내 패스워드 최대 사용기간이 90 이하로 설정되어 있는지 확인해야 합니다. 패스워드 복잡도의 기준은 각각의 회사마다 관리하고 있는 “정보보호정책” 및 “정보보호지침”에 의거해서 기준이 상이 할 수 있습니다.
U-48	패스워드 최소 사용기간 설정	중	"/etc/login.defs" 설정 파일 내 패스워드 최소 사용기간이 1 이상으로 설정되어 있는지 확인해야 합니다. 패스워드 복잡도의 기준은 각각의 회사마다 관리하고 있는 “정보보호정책” 및 “정보보호지침”에 의거해서 기준이 상이 할 수 있습니다.
U-49	불필요한 계정 제거	하	기본적으로 사용하지 말아야 할 DefUlt 계정은 “lp”, “uucp”, nuucp”이 존재하며 lp 로컬 프린터 계정, uucp와 nuucp 계정은 Unix 계열 간 파일 이동이 가능한 계정입니다. 추가로 시스템 및 일반 계정 중 로그인이 가능한 계정이 존재한다면 어떤 목적으로 사용하고 있는지 확인이 필요합니다. 계정 중 유추가 가능한 계정이나 사용하지 않는 계정이 존재하는지 확인이 필요합니다.
U-50	관리자 그룹에 최소한의 계정 포함	하	Unix 계열에서의 관리자 그룹은 “/etc/group” 설정파일 내 “root”로써 “root” 계정 외 타사용자가 포함되어 있는지 확인이 필요합니다.
U-51	계정이 존재하지 않는 GID 금지	하	Unix 계열에서는 사용자 계정을 생성하게 되면 기본적으로 그룹도 함께 생성 됩니다. 이번 항목에서는 불필요 계정이 삭제하였다면 그룹에서도 삭제가 되었는지 확인하는 항목입니다. Passwd 파일의 내용과 group 파일의 내용을 비교 분석하는 것이 필요합니다.

4. ’21년 주요정보통신기반시설 Unix 항목 Review

❖ SYSTEM OS(Linux) 진단 항목 리뷰

1. 계정 관리

코드	항목명	중요도	항목 리뷰 내용
U-52	동일한 UID 금지	중	사용자 계정 생성시 순차적 및 각각의 UID를 설정할 수 있습니다. 물론 계정 생성 이후에 UID를 변경하는 것도 가능합니다. 이번 항목에서는 시스템 및 로그인이 가능한 모든 사용자 계정의 UID가 중복된 값이 있는지 확인해야 합니다.
U-53	사용자 shell 점검	하	Unix 계열에서 “shell”은 사용자가 OS 내에 명령어 및 시스템을 호출할 때 사용하는 중간 인터페이스입니다. Unix OS에서 어떤 shell을 사용하느냐에 따라 sh, csh, bash 등으로 나뉠 수 있습니다. 이번 항목에서 사용자 shell 이라는 부분은 로그인을 할 수 있다 없다 두가지로 크게 분류해서 진단하시면 됩니다. 예시) /bin/false, /sbin/nologin : 로그인 불가 | /bin/bash : 로그인 가능
U-54	Session Timeout 설정	하	Unix 계열로의 원격 접근 후 shell을 실행하지 않고 대기상태에서의 시간이 길어질 경우 자동으로 연결이 끊어지도록 설정하는 부분으로 시스템 초기 구성시에는 적용되지 않는 설정입니다.

4. ’21년 주요정보통신기반시설 Unix 항목 Review

❖ SYSTEM OS(Linux) 진단 항목 리뷰

2. 파일 및 디렉토리 관리

코드	항목명	중요도	항목 리뷰 내용
U-05	root 홈, 패스 디렉토리 권한 및 패스 설정	상	OS에서 환경변수는 “시스템 환경변수”, “사용자 환경변수”로 구분되어 집니다. “시스템 환경변수”는 OS가 부팅되어 자동으로 실행해야하는 시스템 서비스를 구동합니다. “시스템 환경변수”는 운영 및 관리자가 서비스를 구현하는 과정에서 추가 Middleware 및 서비스를 구동해야하는 경우 추가로 작성하는 변수입니다. 이번 항목에서는 “시스템 환경변수” 전체 내용에서 맨 앞과, 중간에 “.”이 포함되어 있는지 확인해야 합니다.
U-06	파일 및 디렉토리 소유자 설정	상	삭제된 소유자의 UID와 동일한 사용자가 해당 파일, 디렉토리에 접근 가능하여 사용자 정보 등 중요 정보가 노출될 위험이 있습니다. 추가로 소유자가 존재하지 않는 파일 및 디렉토리를 삭제 및 관리하여 임의의 사용자에 의한 불법적 행위를 사전에 차단하기 위합입니다.
U-07	/etc/passwd 파일 소유자 및 권한 설정	상	관리자(root) 외 사용자가 "/etc/passwd" 파일의 변조가 가능할 경우 shell 변조, 사용자 추가/삭제, root 를 포함한 사용자 권한 획득 시도 등 악의적인 행위가 가능하며, /etc/passwd 파일 변경을 통한 비인가자의 권한 상승을 막기 위함입니다
U-08	/etc/shadow 파일 소유자 및 권한 설정	상	“/etc/shadow” 파일을 관리자만 제어할 수 있게 하여 비인가자들의 접근을 제한하도록 shadow 파일 소유자 및 권한을 관리해야 하며 해당 파일에 대한 권한 관리가 이루어지지 않을 시 ID 및 패스워드 정보가 외부로 노출될 수 있습니다.
U-09	/etc/hosts 파일 소유자 및 권한 설정	상	hosts 파일에 비인가자 쓰기 권한이 부여된 경우, 공격자는 hosts파일에 악의적인 시스템을 등록하여, 이를 통해 정상적인 DNS를 우회하여 악성사이트로의 접속을 유도하는 파밍(Pharming) 공격 등에 악용될 수 있으며, /etc/hosts 파일을 관리자만 제어할 수 있게 하여 비인가자들의 임의적인 파일 변조를 방지하기 위함입니다.
U-10	/etc/(x)inetd.conf 파일 소유자 및 권한 설정	상	(x)inetd.conf 파일에 비인가자의 쓰기 권한이 부여되어 있을 경우, 비인가자가 악의적인 프로그램을 등록하여 root 권한으로 불법적인 서비스를 실행할 수 있습니다. 이는 방지하기 위해서는 /etc/(x)inetd.conf 파일을 관리자만 제어할 수 있게 하여 비인가자들의 임의적인 파일 변조를 방지해야 합니다.

4. ’21년 주요정보통신기반시설 Unix 항목 Review

❖ SYSTEM OS(Linux) 진단 항목 리뷰

2. 파일 및 디렉토리 관리

코드	항목명	중요도	항목 리뷰 내용
U-11	/etc/syslog.conf 파일 소유자 및 권한 설정	상	services 파일의 접근 권한이 적절하지 않을 경우 비인가 사용자가 운영 포트번호를 변경하여 정상적인 서비스를 제한하거나, 허용되지 않은 포트를 오픈하여 악성 서비스를 의도적으로 실행할 수 있습니다. 이를 방지하기 위해서 /etc/services 파일을 관리자만 제어할 수 있게 해야 합니다.
U-12	/etc/services 파일 소유자 및 권한 설정	상	syslog.conf 파일의 접근권한이 적절하지 않을 경우, 임의적인 파일 변조로 인해 침입자의 흔적 또는 시스템 오류 사항을 분석하기 위해 반드시 필요한 시스템 로그가 정상적으로 기록 되지 않을 수 있습니다. 이를 방지하기 위해서 /etc/syslog.conf 파일의 권한 적절성을 점검하여 관리자 외 비인가자의 임의적인 syslog.conf 파일 변조를 방지해야 합니다.
U-13	SUID, SGID, Sticky bit 설정 및 권한 설정	상	SUID, SGID 파일의 접근권한이 적절하지 않을 경우 SUID, SGID 설정된 파일로 특정 명령어를 실행하여 root 권한 획득 및 정상 서비스 장애를 발생시킬 수 있습니다. 이를 방지하기 위해서 불필요한 SUID, SGID 설정을 제거해야 합니다. * SUID(Set User-ID) : 설정된 파일 실행 시, 특정 작업 수행을 위하여 일시적으로 파일 소유자의 권한을 얻게 됨. * SGID(Set Group-ID) : 설정된 파일 실행 시, 특정 작업 수행을 위하여 일시적으로 파일 소유 그룹의 권한을 얻게 됨.
U-14	사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정	상	홈 디렉토리 내의 사용자 파일 및 사용자별 시스템 시작파일 등과 같은 환경변수 파일의 접근권한 설정이 적절하지 않을 경우, 비인가자가 환경변수 파일을 변조하여 정상 사용중인 사용자의 서비스가 제한 될 수 있습니다. 이를 방지하기 위해 비인가자의 환경변수 조작을 통제해야 합니다.
U-15	world writable 파일 점검	상	시스템 파일과 같은 중요 파일에 world writable 설정이 될 경우, 악의적인 사용자가 해당 파일을 마음대로 파일을 덧붙이거나 지울 수 있게 되어 시스템의 무단 접근 및 시스템 장애를 유발할 수 있습니다. 이를 방지하기 위해 world writable 파일을 이용한 시스템 접근 및 악의적인 코드 실행 권한을 변경하거나 제거해야 합니다.
U-16	/dev에 존재하지 않는 device 파일 점검	상	공격자는 rootkit 설정파일들을 서버 관리자가 쉽게 발견하지 못하도록 /dev 에 device 파일인 것처럼 위장하는 수법을 많이 사용합니다. 이를 방지하기 위해서 실제 존재하지 않는 디바이스를 찾아 제거해야 합니다.

4. ’21년 주요정보통신기반시설 Unix 항목 Review

❖ SYSTEM OS(Linux) 진단 항목 리뷰

2. 파일 및 디렉토리 관리

코드	항목명	중요도	항목 리뷰 내용
U-17	$HOME/.rhosts, hosts.equiv 사용 금지	상	rlogin, rsh 등과 같은 'r'command의 보안 설정이 적용되지 않은 경우, 원격지의 공격자가 관리자 권한으로 목표 시스템 상의 임의의 명령을 수행시킬 수 있습니다. 이를 방지하기 위해 'r'command 사용을 통한 원격 접속은 인증 없이 관리자 원격 접속이 가능하므로 서비스 포트를 차단해야 합니다.
U-18	접속 IP 및 포트 제한	상	허용할 호스트에 대한 IP 및 포트제한이 적용되지 않은 경우, Telnet, FTP같은 보안에 취약한 네트워크 서비스를 통하여 불법적인 접근 및 시스템 침해사고가 발생할 수 있습니다. 이를 방지하기 위해 허용한 호스트만 서비스를 사용하게 해야 합니다.
U-55	hosts.lpd 파일 소유자 및 권한 설정	하	hosts.lpd 파일의 접근권한이 적절하지 않을 경우 비인가자가 /etc/hosts.lpd 파일을 수정하여 허용된 사용자의 서비스를 방해할 수 있으며, 호스트 정보를 획득 할 수 있습니다. 이를 방지하기 위해 비인가자의 임의적인 hosts.lpd 변조를 막기 위해 hosts.lpd 파일 삭제 또는 소유자 및 권한 관리를 해야 합니다.
U-56	UMASK 설정 관리	중	잘못된 UMASK 값으로 인해 시스템 내 신규 생성 파일에 대하여 과도한 권한이 부여될 수 있으며, 이로 인한 파일의 시스템 악용 우려가 있습니다. 이를 방지하기 위해 UMASK 값을 안전한 값으로 설정해야 합니다.
U-57	홈디렉토리 소유자 및 권한 설정	중	홈 디렉토리 내 설정파일 변조 시 정상적인 서비스 이용이 제한될 우려가 존재합니다. 이를 방지하기 위해 사용자 홈 디렉토리 소유자 및 권한 설정을 점검해야 합니다.
U-58	홈디렉토리로 지정한 디렉토리의 존재 관리	중	사용자에게 지정된 디렉토리가 아닌 곳이 홈 디렉토리로 설정될 경우 해당 디렉토리 내 명령어 사용이 가능하며 이에 따라 시스템 관리 및 보안상 문제가 발생할 수 있습니다. 이를 방지하기 위해 /home 이외 사용자의 홈 디렉토리 존재 여부를 점검해야 합니다.

4. ’21년 주요정보통신기반시설 Unix 항목 Review

❖ SYSTEM OS(Linux) 진단 항목 리뷰

2. 파일 및 디렉토리 관리

코드	항목명	중요도	항목 리뷰 내용
U-17	$HOME/.rhosts, hosts.equiv 사용 금지	상	rlogin, rsh 등과 같은 'r'command의 보안 설정이 적용되지 않은 경우, 원격지의 공격자가 관리자 권한으로 목표 시스템 상의 임의의 명령을 수행시킬 수 있습니다. 이를 방지하기 위해 'r'command 사용을 통한 원격 접속은 인증 없이 관리자 원격 접속이 가능하므로 서비스 포트를 차단해야 합니다.
U-18	접속 IP 및 포트 제한	상	허용할 호스트에 대한 IP 및 포트제한이 적용되지 않은 경우, Telnet, FTP같은 보안에 취약한 네트워크 서비스를 통하여 불법적인 접근 및 시스템 침해사고가 발생할 수 있습니다. 이를 방지하기 위해 허용한 호스트만 서비스를 사용하게 해야 합니다.
U-55	hosts.lpd 파일 소유자 및 권한 설정	하	hosts.lpd 파일의 접근권한이 적절하지 않을 경우 비인가자가 /etc/hosts.lpd 파일을 수정하여 허용된 사용자의 서비스를 방해할 수 있으며, 호스트 정보를 획득 할 수 있습니다. 이를 방지하기 위해 비인가자의 임의적인 hosts.lpd 변조를 막기 위해 hosts.lpd 파일 삭제 또는 소유자 및 권한 관리를 해야 합니다.
U-56	UMASK 설정 관리	중	잘못된 UMASK 값으로 인해 시스템 내 신규 생성 파일에 대하여 과도한 권한이 부여될 수 있으며, 이로 인한 파일의 시스템 악용 우려가 있습니다. 이를 방지하기 위해 UMASK 값을 안전한 값으로 설정해야 합니다.
U-57	홈디렉토리 소유자 및 권한 설정	중	홈 디렉토리 내 설정파일 변조 시 정상적인 서비스 이용이 제한될 우려가 존재합니다. 이를 방지하기 위해 사용자 홈 디렉토리 소유자 및 권한 설정을 점검해야 합니다.
U-58	홈디렉토리로 지정한 디렉토리의 존재 관리	중	사용자에게 지정된 디렉토리가 아닌 곳이 홈 디렉토리로 설정될 경우 해당 디렉토리 내 명령어 사용이 가능하며 이에 따라 시스템 관리 및 보안상 문제가 발생할 수 있습니다. 이를 방지하기 위해 /home 이외 사용자의 홈 디렉토리 존재 여부를 점검해야 합니다.
U-59	숨겨진 파일 및 디렉토리 검색 및 제거	하	숨겨진 파일 및 디렉토리 중 의심스러운 내용은 정상 사용자가 아닌 공격자에 의해 생성되었을 가능성이 높으므로 이를 발견하여 제거해야 합니다. 공격자는 숨겨진 파일 및 디렉토리를 통해 시스템 정보 습득, 파일 임의 변경 등을 할 수 있습니다.

4. ’21년 주요정보통신기반시설 Unix 항목 Review

❖ SYSTEM OS(Linux) 진단 항목 리뷰

3. 서비스 관리

코드	항목명	중요도	항목 리뷰 내용
U-19	finger 서비스 비활성화	상	Finger를 통해서 네트워크 외부에서 해당 시스템에 등록된 사용자 정보를 확인할 수 있어 비인가자에게 사용자 정보가 조회되는 것을 차단해야 합니다. * Finger(사용자정보 확인 서비스) : 옵션에 따라 시스템에 등록된 사용자뿐만 아니라 네트워크를 통하여 연결되어 있는 다른 시스템에 등록된 사용자들에 대한 자세한 정보를 보여줌
U-20	Anonymous FTP 비활성화	상	Anonymous FTP를 사용 시 anonymous 계정으로 로그인 후 디렉토리에 쓰기 권한이 설정되어 있다면 악의적인 사용자가 local exploit을 사용하여 시스템에 대한 공격을 가능하게 할 수 있습니다. 이를 방지하기 위해 실행중인 FTP 서비스에 익명 FTP 접속이 허용되고 있는지 확인하여 접속허용을 차단해야 합니다.
U-21	r 계열 서비스 비활성화	상	'r'command 사용을 통한 원격 접속은 NET Backup이나 다른 용도로 사용되기도 하나, 인증 없이 관리자 원격 접속이 가능하여 이에 대한 보안위협을 방지하고자 합니다.
U-22	cron 파일 소유자 및 권한설정	상	root 외 일반 사용자에게도 crontab 명령어를 사용할 수 있도록 할 경우, 고의 또는 실수로 불법적인 예약 파일 실행으로 시스템 피해를 일으킬 수 있습니다. 이를 방지하기 위해 비인가자가 allow, deny 파일에 접근할 수 없도록 설정하고 있는지 점검해야 합니다.
U-23	DoS 공격에 취약한 서비스 비활성화	상	시스템 보안성을 높이기 위해 취약점이 많이 발표된 echo, discard, daytime, chargen, ntp, snmp 등 서비스를 중지해야 합니다. 해당 서비스가 활성화되어 있는 경우 시스템 정보 유출 및 DoS 공격의 대상이 될 수 있습니다.
U-24	NFS 서비스 비활성화	상	비인가자가 NFS 서비스로 인가되지 않은 시스템이 NFS 시스템에 마운트하여 비인가된 시스템 접근 및 파일변조 등의 침해 행위 가능성이 존재합니다. NFS 서비스는 한 서버의 파일을 많은 서비스 서버들이 공유하여 사용할 때 많이 이용되는 서비스이지만 이를 이용한 침해사고 위험성이 높으므로 사용하지 않는 경우 중지해야 합니다.
U-25	NFS 접근 통제	상	NFS 접근제한 설정이 적절하지 않을 경우 비인가자가 인증절차 없이 해당 공유 시스템에 원격으로 마운트하여 중요 파일을 변조하거나 유출할 위험이 있습니다. 이를 방지하기 위해 NFS 접근권한이 없는 비인가자의 접근을 통제해야 합니다.

4. ’21년 주요정보통신기반시설 Unix 항목 Review

❖ SYSTEM OS(Linux) 진단 항목 리뷰

3. 서비스 관리

코드	항목명	중요도	항목 리뷰 내용
U-26	Utomountd 제거	상	파일 시스템의 마운트 옵션을 변경하여 root 권한을 획득할 수 있으며, 로컬 공격자가 Utomountd 프로세스 권한으로 임의의 명령을 실행할 수 있습니다. 로컬 공격자가 Utomountd 데몬에 RPC를 보낼 수 있는 취약점이 존재하기 때문에 해당 서비스가 실행중일 경우 서비스를 중지시켜야 합니다.
U-27	RPC 서비스 확인	상	다양한 취약성(버퍼 오버플로우, DoS, 원격실행 등)이 존재하는 RPC 서비스를 점검하여 해당 서비스를 비활성화 하도록 해야 합니다. 버퍼 오버플로우(Buffer Overflow), DoS, 원격실행 등의 취약성이 존재하는 RPC 서비스를 통해 비인가자의 root 권한 획득 및 침해사고 발생 위험이 있으므로 서비스를 중지하여야 합니다.
U-28	NIS , NIS+ 점검	상	NIS를 사용하는 경우 비인가자가 타시스템의 root 권한 획득이 가능합니다. 이를 방지하기 위해 안전하지 않은 NIS 서비스를 비활성화 하고 안전한 NIS+ 서비스를 활성화하여야 합니다.
U-29	tftp, talk 서비스 비활성화	상	사용하지 않는 서비스나 취약점이 발표된 서비스 운용 시 공격 시도가 가능하여 안전하지 않거나 불필요한 서비스를 제거해야 합니다.
U-30	Sendmail 버전 점검	상	취약점이 발견된 Sendmail 버전의 경우 버퍼 오버플로우(Buffer Overflow) 공격에 의한 시스템 권한 획득 및 주요 정보 요출 가능성이 있습니다. 이를 방지하기 위해 Sendmail 서비스 사용 목적 검토 및 취약점이 없는 버전의 사용 유무를 점검해야 합니다.
U-31	스팸 메일 릴레이 제한	상	SMTP 서버의 릴레이 기능을 제한하지 않는 경우, 악의적인 사용목적을 가진 사용자들이 스팸메일 서버로 사용하거나 DoS공격의 대상이 될 수 있습니다.

4. ’21년 주요정보통신기반시설 Unix 항목 Review

❖ SYSTEM OS(Linux) 진단 항목 리뷰

3. 서비스 관리

코드	항목명	중요도	항목 리뷰 내용
U-32	일반사용자의 Sendmail 실행 방지	상	일반사용자가 q 옵션을 이용해서 메일큐, Sendmail 설정을 보거나 메일큐를 강제적으로 drop 시킬 수 있어 악의적으로 SMTP 서버의 오류를 발생시킬 수 있습니다. 일반사용자의 q 옵션을 제한하여 Sendmail 설정 및 메일큐를 강제적으로 drop 시킬 수 없게 하여 비인가자에 의한 SMTP 서비스 오류를 방지해야 합니다.
U-33	DNS 보안 버전 패치	상	최신버전(2016.01 기준 9.10.3-P2) 이하의 버전에서는 서비스거부 공격, 버퍼 오버플로우(Buffer Overflow) 및 DNS 서버 원격 침입 등의 취약성이 존재합니다.
U-34	DNS Zone Transfer 설정	상	비인가자 Zone Transfer를 이용해 Zone 정보를 전송받아 호스트 정보, 시스템 정보, 네트워크 구성 형태 등의 많은 정보를 파악할 수 있습니다. 이를 방지하기 위해 허가되지 않는 사용자에게 Zone Transfer를 제한해야 합니다.
U-35	Apache 디렉토리 리스팅 제거	상	디렉토리 검색 기능이 활성화 되어 있을 경우, WEB 서버 구조 노출뿐만 아니라 백업 파일이나 소스파일, 공개되어서는 안되는 파일 등이 노출이 가능합니다. 이를 방지하기 위해 외부에서 디렉토리 내의 모든 파일에 대한 접근 및 열람을 제한해야 합니다.
U-36	Apache 웹 프로세스 권한 제한	상	웹 프로세스 취약점 공격으로 Apache 권한이 탈취 당할 경우 Apache 프로세스의 권한이 root이면 시스템 전체의 제어권을 탈취 당해 피해범위가 확산될 가능성이 있습니다. 이를 방지하기 위해 Apache 데몬을 root 권한으로 구동하지 않고 별도의 권한으로 서비스하도록 설정해야 합니다.
U-37	Apache 상위 디렉토리 접근 금지	상	상위 경로로 이동하는 것이 가능할 경우 접근하고자 하는 디렉토리의 하위 경로에 접속하여 상위 경로로 이동함으로써 악의적인 목적을 가진 사용자의 접근이 가능하게 됩니다. 이를 방지하기 위해 상위 경로 이동 명령으로 비인가자의 특정 디렉토리에 대한 접근 및 열람을 제한해야 합니다.

4. ’21년 주요정보통신기반시설 Unix 항목 Review

❖ SYSTEM OS(Linux) 진단 항목 리뷰

3. 서비스 관리

코드	항목명	중요도	항목 리뷰 내용
U-38	Apache 불필요한 파일 제거	상	Apache 설치 시 htdocs 디렉토리 내에 매뉴얼 파일은 시스템 관련정보를 노출하거나 해킹에 악용될 수 있습니다. 이를 방지하기 위해 Apache 설치 시 디폴트로 설치되는 불필요한 파일을 제거해야 합니다.
U-39	Apache 링크 사용 금지	상	시스템 자체의 root 디렉토리(/)에 링크를 걸게 되면 웹 서버 구동 사용자 권한(nobody)으로 모든 파일 시스템의 파일에 접근할 수 있게 되어 "/etc/passwd" 파일과 같은 민감한 파일을 누구나 열람할 수 있습니다. 이를 방지하기 위해 무분별한 심볼릭 링크, aliases 사용을 제한해야 합니다.
U-40	Apache 파일 업로드 및 다운로드 제한	상	악의적 목적을 가진 사용자가 반복 업로드 및 웹 쉘 공격 등으로 시스템 권한을 탈취하거나 대용량 파일의 반복 업로드로 서버자원을 고갈시키는 공격의 위험이 있습니다. 이를 방지하기 위해 파일 업로드 및 다운로드를 제한해야 하지만 불가피하게 필요시 용량 사이즈를 제한해야 합니다.
U-41	Apache 웹 서비스 영역의 분리	상	웹 서버의 루트 디렉토리와 OS의 루트 디렉토리를 다르게 지정하지 않았을 경우, 비인가자가 웹 서비스를 통해 해킹이 성공할 경우 시스템 영역까지 접근이 가능하여 피해가 확장될 수 있습니다. 이를 방지하기 위해 웹 서비스 영역과 시스템 영역을 분리시켜야 합니다.
U-60	ssh 원격접속 허용	중	원격 접속 시 Telnet, FTP 등은 암호화되지 않은 상태로 데이터를 전송하기 때문에 아이디/패스워드 및 중요 정보가 외부로 유출될 위험성이 있습니다. 이를 방지하기 위해 SSH 프로토콜을 사용해야 합니다.
U-61	ftp 서비스 확인	하	FTP 서비스는 아이디 및 패스워드가 암호화되지 않은 채로 전송되어 스니핑이 가능합니다. 이를 방지하기 위해 취약한 서비스인 FTP서비스를 가급적 제한해야 합니다.

4. ’21년 주요정보통신기반시설 Unix 항목 Review

❖ SYSTEM OS(Linux) 진단 항목 리뷰

3. 서비스 관리

코드	항목명	중요도	항목 리뷰 내용
U-62	ftp 계정 shell 제한	중	불필요한 기본 계정에 쉘(Shell)을 부여할 경우, 공격자에게 해당 계정이 노출되어 ftp 기본 계정으로 시스템 접근하여 공격이 가능합니다. 이를 방지하기 위해 FTP 서비스 설치 시 기본으로 생성되는 ftp 계정을 로그인이 필요하지 않은 계정으로 쉘을 제한해야 합니다.
U-63	ftpusers 파일 소유자 및 권한 설정	하	해당 파일에 대한 권한 관리가 이루어지지 않을 시 비인가자의 FTP 접근을 통해 계정을 등록하고 서버에 접속하여 침해사고가 발생할 수 있습니다. 이를 방지하기 위해 비인가자의 ftpusers 파일 수정을 제한하여 비인가자들의 ftp 접속을 차단해야 합니다.
U-64	ftpusers 파일 설정	중	FTP 서비스는 아이디 및 패스워드가 암호화되지 않은 채로 전송되어 스니핑에 의해서 아이디 및 패스워드가 노출될 수 있습니다. 이를 방지하기 위해 root의 FTP 직접 접속을 제한해야 합니다.
U-65	at 파일 소유자 및 권한 설정	중	해당 파일에 대한 권한 관리가 이루어지지 않을 시 공격자가 권한을 획득한 사용자 계정을 등록하여 불법적인 예약 파일 실행으로 시스템 피해가 발생할 수 있습니다. 이를 방지하기 위해 at.allow 파일과 at.deny 파일에 대한 접근제한이 필요합니다.
U-66	SNMP 서비스 구동 점검	중	SNMP 서비스로 인하여 시스템의 주요 정보 유출 및 정보의 불법 수정이 발생할 수 있습니다. 이를 방지하기 위해 SNMP 서비스를 중지해야 합니다.
U-67	SNMP 서비스 Community String의 복잡성 설정	중	Community String은 DefUlt로 public, private로 설정된 경우가 많으며, 이를 변경하지 않으면 이 String을 악용하여 환경설정 파일 열람 및 수정을 통한 공격, 간단한 정보수집에서부터 관리자 권한 획득 및 DoS 공격까지 다양한 형태의 공격이 가능합니다. 이를 방지하기 위해 Community String 기본 설정인 Public, Private를 유추하지 못하도록 설정해야 합니다.

4. ’21년 주요정보통신기반시설 Unix 항목 Review

❖ SYSTEM OS(Linux) 진단 항목 리뷰

3. 서비스 관리

코드	항목명	중요도	항목 리뷰 내용
U-68	로그온 시 경고 메시지 제공	하	로그인 배너가 설정되지 않을 경우 배너에 서버 OS 버전 및 서비스 버전이 공격자에게 노출될 수 있으며 공격자는 이러한 정보를 통하여 해당 OS 및 서비스의 취약점을 이용하여 공격을 시도할 수 있습니다. 이를 방지하기 위해 서버 접속 시 관계자만 접속해야 한다는 경고 메시지를 설정해야 합니다.
U-69	NFS 설정파일 접근권한	중	NFS 접근제어 설정파일에 대한 권한 관리가 이루어지지 않을 시 인가되지 않은 사용자를 등록하고 파일시스템을 마운트하여 불법적인 변조를 시도할 수 있습니다. 이를 방지하기 위해 NFS 접근 제어 파일의 소유자 및 파일 권한을 관리해야 합니다.
U-70	expn, vrfy 명령어 제한	중	VRFY, EXPN 명령어를 통하여 특정 사용자 계정의 존재유무를 알 수 있고, 사용자의 정보를 외부로 유출 할 수 있습니다. 이를 방지하기 위해 SMTP 서비스의 expn, vrfy 명령을 사용하지 못하게 옵션을 설정해야 합니다.
U-71	Apache 웹 서비스 정보 숨김	중	불필요한 정보가 노출될 경우 해당 정보를 이용하여 시스템의 취약점을 수집할 수 있습니다. 이를 방지하기 위해 HTTP 헤더, 에러페이지에서 웹 서버 버전 및 종류, OS 정보 등 웹 서버와 관련된 불필요한 정보가 노출되지 않도록 설정해야 합니다.

4. ’21년 주요정보통신기반시설 Unix 항목 Review

❖ SYSTEM OS(Linux) 진단 항목 리뷰

4. 패치 관리

코드	항목명	중요도	항목 리뷰 내용
U-42	최신 보안패치 및 벤더 권고사항 적용	상	최신 보안패치가 적용되지 않을 경우, 이미 알려진 취약점을 통하여 공격자에 의해 시스템 침해사고 발생 가능성이 존재합니다. 이를 방지하기 위해 주기적인 패치를 진행해야 합니다.

5. 로그 관리

코드	항목명	중요도	항목 리뷰 내용
U-43	로그의 정기적 검토 및 보고	상	로그의 검토 및 보고 절차가 없는 경우 외부 침입 시도에 대한 식별이 누락 될 수 있고, 침입 시도가 의심되는 사례 발견 시 관련 자료를 분석하여 해당 장비에 대한 접근을 차단하는 등의 추가 조치가 어려울 수 있습니다. 이를 방지하기 위해 정기적인 로그 점검을 진행해야 합니다.
U-72	정책에 따른 시스템 로깅 설정	하	로깅 설정이 되어 있지 않을 경우 원인 규명이 어려우며, 법적 대응을 위한 충분한 증거로 사용할 수 없습니다. 이를 방지하기 위해 로그 기록을 정책에 따라 보관하도록 설정해야 합니다.

5. 주요정보통신기반시설 Linux 진단

❖ SYSTEM OS(Linux) 진단 수행

▶ 결과보고서

항목분류	코드	항목명	중요도	결과 (양호/취약/인터뷰)	결과
계정 관리	AU-01	root 계정 원격 접속 제한	상	양호	[현황] - 취약점 요약 Comment [대응방안] - 취약일 경우에 대한 대응방안 요약 Comment
계정 관리	AU-02	패스워드 복잡성 설정	상	양호	
계정 관리	AU-03	계정 잠금 임계값 설정	상	양호	
계정 관리	AU-04	패스워드 파일 보호	상	양호	
파일 및 디렉토리 관리	AU-05	root 홈, 패스 디렉토리 권한 및 패스 설정	상	양호	
파일 및 디렉토리 관리	AU-06	파일 및 디렉토리 소유자 설정	상	양호	
파일 및 디렉토리 관리	AU-07	/etc/passwd 파일 소유자 및 권한 설정	상	양호	
파일 및 디렉토리 관리	AU-08	/etc/shadow 파일 소유자 및 권한 설정	상	양호	
파일 및 디렉토리 관리	AU-09	/etc/hosts 파일 소유자 및 권한 설정	상	양호	
파일 및 디렉토리 관리	AU-10	/etc/(x)inetd.conf 파일 소유자 및 권한 설정	상	양호	
파일 및 디렉토리 관리	AU-11	/etc/syslog.conf 파일 소유자 및 권한 설정	상	양호	
파일 및 디렉토리 관리	AU-12	/etc/services 파일 소유자 및 권한 설정	상	양호	

[Backup] ‘21년 주요정보통신기반시설 Windows 항목

분류	항목코드	점검항목	항목 중요도
1. 계정 관리	W-01	Administrator 계정 이름 바꾸기	상
	W-02	Guest 계정 상태	상
	W-03	불필요한 계정 제거	상
	W-04	계정 잠금 임계값 설정	상
	W-05	해독 가능한 암호화를 사용하여 암호 저장	상
	W-06	관리자 그룹에 최소한의 사용자 포함	상
	W-46	Everyone 사용 권한을 익명 사용자에게 적용	중
	W-47	계정 잠금 기간 설정	중
	W-48	패스워드 복잡성 설정	중
	W-49	패스워드 최소 암호 길이	중
	W-50	패스워드 최대 사용 기간	중
	W-51	패스워드 최소 사용 기간	중
	W-52	마지막 사용자 이름 표시 안함	중
	W-53	로컬 로그온 허용	중
	W-54	익명 SID/이름 변환 허용	중
	W-55	최근 암호 기억	중
	W-56	콘솔 로그온 시 로컬 계정에서 빈 암호 사용 제한	중
	W-57	원격터미널 접속 가능한 사용자 그룹 제한	중
2. 서비스 관리	W-07	공유 권한 및 사용자 그룹 설정	상
	W-08	하드디스크 기본 공유 제거	상
	W-09	불필요한 서비스 제거	상
	W-10	IIS 서비스 구동 점검	상
	W-11	IIS 디렉토리 리스팅 제거	상
	W-12	IIS CGI 실행 제한	상
	W-13	IIS 상위 디렉토리 접근 금지	상
	W-14	IIS 불필요한 파일 제거	상
	W-15	IIS 웹 프로세스 권한 제한	상
	W-16	IIS 링크 사용금지	상
	W-17	IIS 파일 업로드 및 다운로드 제한	상
	W-18	IIS DB 연결 취약점 점검	상
	W-19	IIS 가상 디렉토리 삭제	상
	W-20	IIS 데이터 파일 ACL 적용	상
	W-21	IIS 미사용 스크립트 매핑 제거	상
	W-22	IIS Exec 명령어 쉘 호출 진단	상
	W-23	IIS WebDAV 비활성화	상
	W-24	NetBIOS 바인딩 서비스 구동 점검	상
	W-25	FTP 서비스 구동 점검	상
	W-26	FTP 디렉토리 접근권한 설정	상
	W-27	Anonymouse FTP 금지	상
	W-28	FTP 접근 제어 설정	상
	W-29	DNS Zone Transfer 설정	상

분류	항목코드	점검항목	항목 중요도
2. 서비스 관리	W-30	RDS(RemoteDataServices)제거	상
	W-31	최신 서비스팩 적용	상
	W-58	터미널 서비스 암호화 수준 설정	중
	W-59	IIS 웹서비스 정보 숨김	중
	W-60	SNMP 서비스 구동 점검	중
	W-61	SNMP 서비스 커뮤니티스트링의 복잡성 설정	중
	W-62	SNMP Access control 설정	중
	W-63	DNS 서비스 구동 점검	중
	W-64	HTTP/FTP/SMTP 배너 차단	하
	W-65	Telnet 보안 설정	중
	W-66	불필요한 ODBC/OLE-DB 데이터 소스와 드라이브 제거	중
	W-67	원격터미널 접속 타임아웃 설정	중
	W-68	예약된 작업에 의심스러운 명령이 등록되어 있는지 점검	중
3. 패치 관리	W-32	최신 HOT FIX 적용	상
	W-33	백신 프로그램 업데이트	상
	W-69	정책에 따른 시스템 로깅 설정	중
4. 로그 관리	W-34	로그의 정기적 검토 및 보고	상
	W-35	원격으로 액세스할 수 있는 레지스트리 경로	상
	W-70	이벤트 로그 관리 설정	하
	W-71	원격에서 이벤트 로그 파일 접근 차단	중
5. 보안 관리	W-36	백신 프로그램 설치	상
	W-37	SAM 파일 접근 통제 설정	상
	W-38	화면보호기 설정	상
	W-39	로그온 하지 않고 시스템 종료 허용 해제	상
	W-40	원격 시스템에서 강제로 시스템 종료	상
	W-41	보안 감사를 로그할 수 없는 경우 즉시 시스템 종료 해제	상
	W-42	SAM 계정과 공유의 익명 열거 허용 안 함	상
	W-43	Utologon 기능 제어	상
	W-44	이동식 미디어 포맷 및 꺼내기 허용	상
	W-45	디스크볼륨 암호화 설정	상
	W-72	Dos 공격 방어 레지스트리 설정	중
	W-73	사용자가 프린터 드라이버를 설치할 수 없게 함	중
	W-74	세션 연결을 중단하기 전에 필요한 유휴시간	중
	W-75	경고 메시지 설정	하
	W-76	사용자별 홈 디렉터리 권한 설정	중
	W-77	LAN Manager 인증 수준	중
	W-78	보안 채널 데이터 디지털 암호화 또는 서명	중
	W-79	파일 및 디렉토리 보호	중
	W-80	컴퓨터 계정 암호 최대 사용 기간	중
	W-81	시작 프로그램 목록 분석	중
6. DB 관리	W-82	Windows 인증 모드 사용	중