Confidentia
l

인프라진단 수행계획서

2023. 07. 26.

SK shieldus

Confidentiality Agreements

본 보고서는 시스템 정보와 관련한 비공개 사항이 포함되어 있으므로, 열람권한은 우선적으로 정보보안 책임자로 제한되며, 이외의 열람자격은 정보보안 책임자가 허락한 최소한의 인원으로 제한하여 주시기 바랍니다.

본 보고서는 양사간의 사전 협의 없이 어떠한 목적으로도 외부로 유출되거나 무단 복제, 무단 사용될 수 없으며, 기밀성을 유지한다는 전제하에 사용이 엄격 하게 제한됩니다.

본 보고서는 인포섹㈜에서 작성을 하였으며, 정보보호 서약에 대한 사항을 준수 합니다.

- 목 차 -

1.개요

1.1.목적

본 인프라 진단은 **"JM COMPANY"**에서 운영 중인 주요 정보시스템에 대하여 인터넷을 통해 접근하여 악용할 수 있는 취약성이 존재하는지 또는 내부 직원이나 내부망에 거점을 확보한 자가 악용할 수 있는 취약성이 존재하는지를 점검하고, 발견된 취약성에 대한 대응책을 수립하여 안전하고 신뢰할 수 있는 정보시스템 구축 및 운영을 위한 기반을 마련 및 보안 수준 향상을 위한 방법을 제시하고자 합니다.

1.2.진단방법

정보시스템 관리/운영 부문과 기술적 부문에 대한 취약성을 진단하고 관리자 인터뷰를 통해 대상 시스템을 점검합니다.

○ 인프라 장비 담당자 인터뷰 수행을 통한 현황 파악 및 분석 수행

1.3.진단일정

인프라 취약점진단 수행 일정은 사전준비 및 공조체계 마련, 서버 취약점 점검, 점검결과 분석, 보고서 작성의 4단계로 수행하며, 세부 일정은 다음과 같습니다.

구분	내용	일정
사전준비	대상협의 및 환경분석	2023.07.26 이전
취약점점검	취약점 점검 수행(자동/수동)	2023.07.26 ~ 2023.07.31
결과분석 / 보고서	결과분석 및 보고서 작성	2023.07.31
결과보고서 제출	최종 결과보고서 제출	2023.08.31 (종료)

[표 1 – 진단일정]

1.4.진단대상

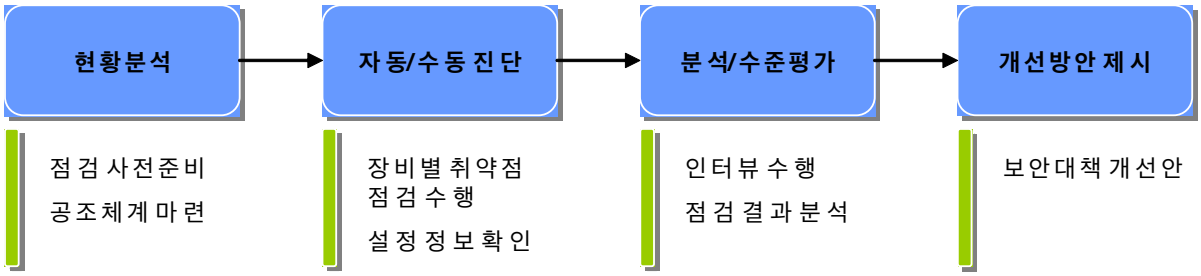
인프라진단 대상의 상세 내역은 다음과 같습니다.

No	구분	호스트명	IP Address	OS 버전
1	OS	EC2AMAZ-V2J5JME	10.0.4.23	Window Server 2019
2	OS	ip-10-0-0-11	10.0.0.11	Ubuntu 22.04
3	WEB	EC2AMAZ-V2J5JME	10.0.4.23	Apache2
4	WAS	ip-10-0-0-11	10.0.0.11	Tomcat 9.0.1
5	DBMS	rm1-rds.cxg7zmjbycvd.us-east-2.rds.amazonaws.com	10.0.8.15	Oracle 19c

[표 2 – 인프라ws 진단대상]

1.5.진단절차

인프라 진단 수행 절차는 아래 그림과 같이 “현황 분석”, “자동/수동 진단”, “분석/수준평가”, “개선방안 제시”를 수행하여 최종 취약점 분석 보고서를 작성합니다.



[그림 1 – 취약성 진단 수행 절차]

1. 현황 분석
원활한 진단을 수행하기 위하여 실제 진단 전에 입수된 자료와 담당자 인터뷰 등을 통해 대상 웹서버에 대한 정보(IP, Hostname, Service, WAS 정보, 웹 구조, 네트워크 Config 등)를 수집하며 전반적인 보안 현황을 파악합니다.

2. 자동/수동 진단
실제 장비의 취약점을 진단하는 단계로 자동화 진단도구를 이용한 서버 점검(인포섹 자체 점검 도구 사용) 및 네트워크 Config 점검을 수행합니다.

3. 분석/수준 평가
진단 단계에서 식별된 취약점을 분석하여 문제점을 도출하고, 현재 취약점의 보안 수준을 평가하여 각 장비의 취약점이 미칠 수 있는 위험을 분석 평가합니다.

4. 개선방안 제시
분석 평가된 취약점에 따른 개선방안을 도출하여 이에 따른 보안 가이드를 제시합니다.

1.6.진단항목

Windows 진단항목은 “SK쉴더스 보안 가이드 라인_Windows 2019(2022.03)”을 기반으로 계정관리 8개 항목, 파일 시스템 5개 항목, 네트워크 서비스 4개 항목, 주요 응용 설정 3개 항목, 시스템 보안 설정 16개 항목, 바이러스 진단 2개 항목, 레지스트리 보안 설정 6개 항목, 보안패치 2개 항목, 이슈 취약점 1개, 총 47개 항목으로 구성되어 있으며 상세 진단항목은 다음과 같습니다.

구분	NO.	대상항목
1. 계정 관리	1	로컬 계정 사용 설정
	2	계정 잠금 정책 설정
	3	암호 정책 설정
	4	취약한 패스워드 점검
	5	사용자 계정 컨트롤(User Account Control) 설정
	6	익명 SID/이름 변환 허용 정책
	7	콘솔 로그온 시 로컬 계정에서 빈 암호 사용 제한 정책 점검
	8	관리자 그룹에 최소한의 사용자 포함
2. 파일 시스템	1	CMD.EXE 파일 권한 설정
	2	사용자 홈 디렉터리 접근 제한
	3	공유 폴더 설정
	4	SAM(Security Account Manager) 파일 권한 설정
	5	파일 및 디렉터리 보호
3. 네트워크 서비스	1	불필요한 서비스 제거
	2	터미널 서비스 암호화 수준 설정
	3	NetBIOS 서비스 보안 설정
	4	터미널 서비스 Time Out 설정
4. 주요 응용 설정	1	Telnet 서비스 보안 설정
	2	DNS(Domain Name Service) 보안 설정
	3	SNMP(Simple Network Management Protocol) 서비스 보안 설정
5. 시스템 보안 설정	1	원격 로그파일 접근 진단
	2	화면 보호기 설정
	3	이벤트 뷰어 설정
	4	로그인 시 경고 메시지 표시 설정
	5	마지막 로그온 사용자 계정 숨김
	6	로그온 하지 않은 사용자 시스템 종료 방지
	7	로컬 감사 정책 설정
	8	가상 메모리 페이지 파일 삭제 설정
	9	Lan Manager 인증 수준

구분	NO.	대상항목
	10	Everyone 사용 권한을 익명 사용자에게 적용 안함
	11	이동식 미디어 포맷 및 꺼내기 admin만 허용
	12	세션 연결 끊기 전 유휴 시간 설정
	13	예약된 작업 의심스런 명령어나 파일 점검
	14	원격 시스템 종료 권한 설정
	15	보안 감사를 로그 할 수 없는 경우 즉시 시스템 종료 방지
	16	보안 채널 데이터 디지털 암호화 또는 서명 설정
6. 바이러스 진단	1	백신 프로그램 설치
	2	최신 엔진 업데이트
7. 레지스트리 보안 설정	1	SAM(Security Account Manager) 보안 감사 설정
	2	Null Session 설정
	3	Remote Registry Service 설정
	4	RDS(Remote Data Service) 제거
	5	AutoLogon 제한 설정
	6	DOS 공격에 대한 방어 레지스트리 설정
8. 보안패치	1	최신 서비스 팩 적용
	2	최신 HOT FIX 적용
9. 이슈 취약점	1	OpenSSL 취약점

[표 3– Windows 진단항목]

Unix 계열 진단항목은 “SK쉴더스 보안 가이드 라인_LINUX(2022.03)”을 기반으로 계정 관리 12개 항목, 파일 시스템 23개 항목, 네트워크 서비스 10개 항목, 로그관리 3개 항목, 주요 응용 설정 6개 항목, 시스템 보안 설정 3개 항목, 보안패치 1개 항목, 총 58개 항목으로 구성되어 있으며 상세 진단 항목은 다음과 같습니다.

구분	NO.	대상항목
1. 계정 관리	1	로그인 설정
	2	Default 계정 삭제
	3	일반계정 root 권한 관리
	4	/etc/passwd 파일 권한
	5	/etc/group 파일 권한 설정
	6	/etc/shadow 파일 권한 설정
	7	패스워드 사용 규칙 적용

구분	NO.	대상항목
	8	취약한 패스워드 점검
	9	로그인이 불필요한 계정 shell 제한
	10	SU(Select User) 사용 제한
	11	계정이 존재하지 않는 GID 금지
	12	동일한 UID 금지
2. 파일 시스템	1	사용자 UMASK(User MASK) 설정
	2	SUID(Set User-ID), SGID(Set Group-ID) 설정
	3	/etc/(x)inetd.conf 파일 권한 설정
	4	.history 파일 권한 설정
	5	Crontab 파일 권한 설정 및 관리
	6	/etc/profile 파일 권한 설정
	7	/etc/hosts 파일 권한 설정
	8	/etc/issue 파일 권한 설정
	9	사용자 홈 디렉터리 및 파일 관리
	10	중요 디렉터리 파일 권한 설정
	11	PATH 환경변수 설정
	12	FTP(File Transfer Protocol) 접근제어 파일 권한 설정
	13	Root 원격 접근제어 파일 권한 설정
	14	NFS(Network File System) 접근제어 파일 권한 설정
	15	/etc/services 파일 권한 설정
	16	부팅 스크립트 파일 권한 설정
	17	/etc/hosts.allow, /etc/hosts.deny 설정
	18	기타 중요 파일 권한 설정
	19	At 파일 소유자 및 권한 설정
	20	Hosts.lpd 파일 소유자 및 권한 설정
	21	/etc/(r)syslog.conf 파일 소유자 및 권한 설정
	22	World writable 파일 점검
	23	/dev에 존재하지 않는 device 파일 점검
	1	RPC(Remote Procedure Call) 서비스 제한
	2	NFS(Network File System) 제한

구분	NO.	대상항목
3. 네트워크 서비스	3	Automountd 서비스 제거
	4	NIS(Network Information Service) 제한
	5	'r' commands 서비스 제거
	6	불필요한 서비스 제거
	7	서비스 Banner 관리
	8	Session timeout 설정
	9	root의 계정 telnet, ssh 접근 제한
	10	DNS 보안 버전 패치
4. 로그 관리	1	(x)inetd Services 로그 설정
	2	시스템 로그 설정
	3	로그 저장 주기
5. 주요 응용 설정	1	FTP(File Transfer Protocol) 서비스 사용자 제한
	2	SNMP(Simple Network Management Protocol) 서비스 설정
	3	SMTP(Simple Mail Transfer Protocol) 서비스 설정
	4	DNS(Domain Name Service) 보안 설정
	5	SWAT(Samba Web Administration Tool) 보안 설정
	6	x-server 접속 제한 설정
6. 시스템 보안 설정	1	/etc/system 파일 보안 설정
	2	Kernel 파라메터 설정
	3	ISN(Initial Sequence Number) 파라메터 설정
7. 로그 관리	1	보안 패치 적용

[표 4 – Unix 진단항목]

Apache 계열 진단항목은 "SK쉴더스 보안 가이드 라인_Apache(2022.03)"을 기반으로 설정 14개 항목, 솔루션 취약점 3개 항목, 보안패치 1개 항목, 총 18개 항목으로 구성되어 있으며 상세 진단항목은 다음과 같습니다.

구분	NO.	대상항목
	1	데몬 관리
	2	관리서버 디렉터리 권한 설정
	3	설정파일 권한 설정
	4	디렉터리 검색 기능 제거

구분	NO.	대상항목
1. 설정	5	로그 디렉터리/파일 권한 설정
	6	로그 포맷 설정
	7	로그 저장 주기
	8	헤더 정보 노출 방지
	9	HTTP Method 제한
	10	에러 메시지 관리
	11	FollowSymLinks 옵션 비활성화
	12	MultiViews 옵션 비활성화
	13	상위 디렉터리 접근 금지 설정
	14	웹 서비스 영역 분리 설정
2. 솔루션 취약점	1	불필요한 파일 삭제
	2	기본 문서명 사용 제한
	3	SSL v3.0 POODLE 취약점
3. 보안 패치	1	보안 패치 적용

[표 5 – Apache 진단항목]

Tomcat 계열 진단항목은 “SK쉴더스 보안 가이드 라인_Tomcat(2022.03)”을 기반으로 설정 11개 항목, 솔루션 취약점 4개 항목, 보안패치 1개 항목, 접근 제어 4개 항목, 총 20개 항목으로 구성되어 있으며 상세 진단항목은 다음과 같습니다.

구분	NO.	대상항목
1. 설정	1	데몬 관리
	2	관리서버 디렉터리 권한 설정
	3	설정 파일 권한 설정
	4	로그 디렉터리/파일 권한 설정
	5	로그 포맷 설정
	6	로그 저장 주기
	7	HTTP Method 제한
	8	디렉터리 검색 기능 제거
	9	Session Timeout 설정
	10	헤더 정보 노출 방지
	11	에러 메시지 관리

구분	NO.	대상항목
2. 솔루션 취약점	1	불필요한 파일 사제
	2	프로세스 관리 기능 삭제
	3	SSL v3.0 POODLE 취약점
	4	Apache Commons-Collection 라이브러리 취약점
3. 보안 패치	1	보안 패치 적용
4. 접근 제어	1	관리자 콘솔 접근통제
	2	관리자 default 계정명 변경
	3	관리자 패스워드 암호 정책
	4	패스워드 파일 권한 설정

[표 6 – Tomcat 진단항목]

Oracle 계열 진단항목은 “SK쉴더스 보안 가이드 라인_Oracle(2022.03)”을 기반으로 계정 관리 6개 항목, 권한 관리 9개 항목, DBMS 보안설정 6개 항목, 환경 파일 점검 8개 항목, 보안패치 1개 항목, 보안 감사 설정 2개 항목, 네트워크 접근 제어 2개 항목, 총 34개 항목으로 구성되어 있으며 상세 진단항목은 다음과 같습니다.

구분	NO.	대상항목
1. 계정 관리	1	불필요한 계정 확인
	2	무제한 로그인 시도 차단
	3	패스워드 주기적 변경
	4	패스워드 복잡도 설정
	5	취약한 패스워드 사용 점검
	6	OS DBA 그룹 멤버 확인
2. 관한 관리	1	개발 및 운영 시스템 분리 사용
	2	Public에 대한 권한 제한
	3	SYS.LINK$ 테이블 접근 제한
	4	SYSDBA 권한 제한
	5	DBA 권한 제한
	6	with grant option 사용 제한
	7	with admin option 사용 제한
	8	SYSDBA 로그인 제한
	9	CREATE ANY DIRECTORY 권한 제한
	1	백업 관리

구분	NO.	대상항목
3. DBMS 보안설정	2	PL/SQL Package의 Public Role 점검
	3	Listener 보안 설정 여부
	4	DB 접속 IP 통제
	5	로그 저장 주기
	6	세션 IDLE_TIMEOUT 설정
4. 환경 파일 점검	1	SQL*PLUS 명령 히스토리 검사
	2	Initialization 파일 접근 권한 설정
	3	Oracle Password 파일 접근 권한 설정
	4	AlertLog 파일 접근 제한
	5	Trace Log 파일 접근 제한
	6	컨트롤, redo 로그파일, 데이터 파일 접근 제한
	7	$TNS_ADMIN 파일 접근 제한
	8	감사 로그 파일 접근 제한
5. 보안 패치	1	보안 패치 적용
6. 보안 감사 설정	1	SYS 감사 수행 설정
	2	Audit Trail 기록 설정
7. 네트워크 접근 제어	1	DATA DICTIONARY 접근 제한
	2	원격 OS 인증 방식 설정

[표 7 – Oracle 진단항목]

1.7.진단 평가 기준

보안 등급	A (안전)	B (양호)	C (보통)	D (취약)	E (위험)
보안수준 점수(%)	85 이상~ 100 미만	70 이상~ 85 미만	55 이상~ 70 미만	40 이상~ 55 미만	0 이상~ 40 미만
해커공격 대응수준	고급해커 120시간 공격에 대응	고급해커 48시간 공격에 대응	중급해커 120시간 공격에 대응	초급해커 120시간 공격에 대응	초급해커 48시간 공격에 대응

[표 8 – 보안 평가등급(TCSEC)]

※ 평가등급 (TCSEC): 미 국방성 (DoD)의 컴퓨터시스템 보안등급 기준인 TCSEC (Trusted Computer System Evaluation Criteria) 의 개념에 기반하며, 기술적 영역에 대한 기업의 보안환경을 분석하여 그 수준을 진단하고 등급을 평가하는 기준. 기술적 보안에 대해 A ~ E 5 단계 등급과 100점 만점의 보안수준 점수로서 평가

2.진단결과

2.1.수행 산출물

인프라 보안진단을 통하여 제공되는 산출물은 다음과 같습니다.

No	작업 산출물	제출시기	비 고
1	인프라진단 수행계획서	진단 수행 전	본 문서
2	인프라진단 결과보고서	진단 수행 후	서버 취약점 분석평가 결과

[표 9– 수행 산출물]

2.2.수행 후의 조치사항

1) 작업 수행완료 후 특권 획득 표시 및 기타 흔적들의 삭제(예: /upload/infosec.jsp)
2) 대상 시스템의 정상작동 확인

2.3.협조 및 유의사항

서버 취약점 진단의 효율 및 정확성을 보장하기 위하여 다음 사항에 대한 지원을 요청합니다.

1) 대상 서버 중 내부망에 위치한 서버 취약점 진단을 위한 점검용 node 및 IP Address 부여
2) 서버 취약점 진단을 위한 대상 서버의 Administrator 또는 root 계정 확보 요청
3) 서버 별 실무담당자 연락처 요청 (ex. 시스템 담당, 응용 담당, 유지 보수 담당자 등)
4) 진단 컨설턴트가 사용할 수 있는 Remote 또는 Local Network Segment 환경의 제공
5) 진단 스크립트 업로드를 위한 FTP, 터미널 서비스 오픈 요청