침해사고 조치 가이드

2012. 10.

KrCERT/CC
인터넷침해사고대응지원센터

KISA 한국인터넷진흥원
Korea Internet & Security Agency

가이드 요약

□ 가이드 목적

o 해킹사고 원인 분석 및 조치 시 참고자료

o 사고 예방을 위한 서비스 보안 강화 시 참고자료

□ 가이드 내용

o 사고가 발생한 경우 사고 유형별 점검 사항과 특이사항 발생에 따른 조치방법 안내

사고 유형	점검 사항
공통	· 계정 / 로그파일 / 웹쉘 / 백도어 / 루트킷
웹변조	· 웹페이지 / HTTP 메소드 / 웹로그
악성코드 경유지/유포지	· 웹페이지 / 접속IP
봇넷 C&C	· 네트워크 연결
해킹 경유지	· 네트워크 연결 / 설치 프로그램

o 시스템 보안 강화를 위해 서비스 별 조치방법 안내

서비스	조치 방안
웹 서버	· OS에 대한 최신 패치 적용 · 웹 서버 전용 호스트로 구성 · 서버에 대한 접근 제어 · DMZ 영역에 위치 · 강력한 관리자 계정 패스워드 사용 · 파일 접근권한 설정 · 웹 프로세스의 권한 제한 · 로그파일의 보호 · 웹 서비스 영역의 분리 · 설정파일 백업 · Inbound 트래픽 제한
네트워크	· 원격 접근 제한 · 불필요한 서비스 중단 · 로그관리
DB	· 시스템 보안패치 적용 · 원격으로부터의 접속 차단 · 사용자별 접속권한 설정
어플리케이션	· 웹 취약점 점검 수행 · 휘슬 설치 및 주기적인 검사 수행 · 캐슬 설치 및 운영

< 목 차 >

Ⅰ. 침해사고 개요 ····· 4

Ⅱ. 사고 유형별 시스템 점검항목 및 조치 방안 ····· 6

공통 ····· 6

웹변조 ····· 7

악성코드 경유지/유포지 ····· 8

봇넷 C&C ····· 9

해킹 경유지 ····· 9

Ⅲ. 웹 서버 취약점 조치 방안 ····· 11

Ⅳ. 네트워크 취약점 조치 방안 ····· 14

Ⅴ. DB 취약점 조치 방안 ····· 16

Ⅵ. 어플리케이션 취약점 조치 방안 ····· 19

[별첨1] WHISTL, Rootkit Hunter, Check Rootkit 사용법 ····· 28

[별첨2] 주요 용어 정리 ····· 30

I. 침해사고 개요

침해사고 정의

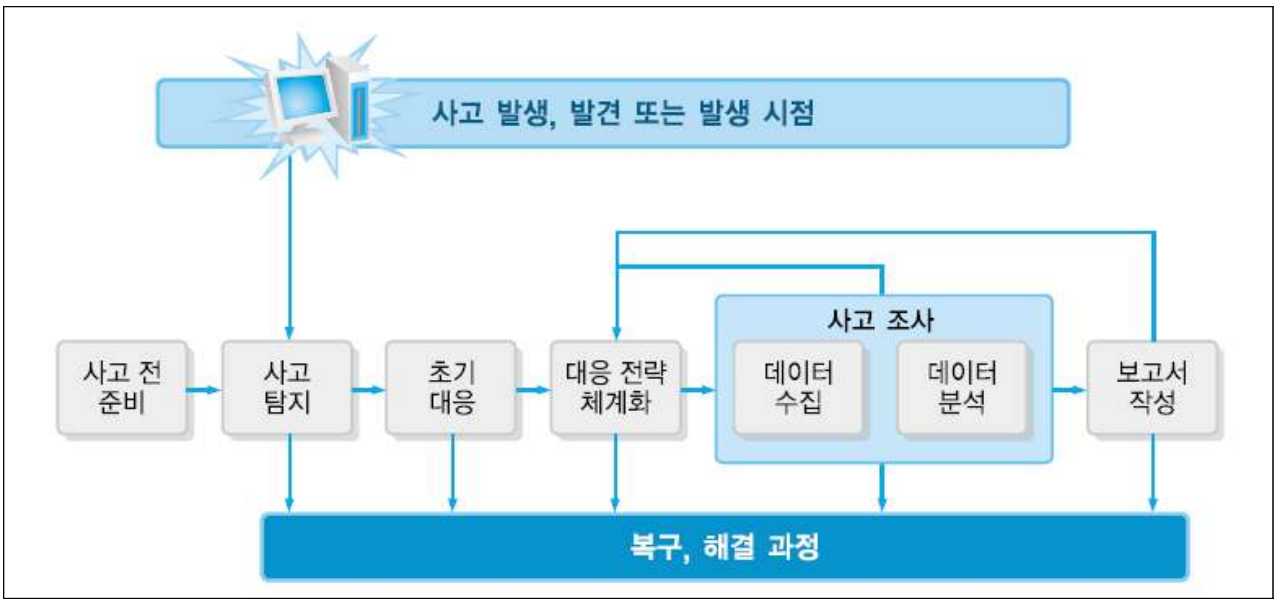
<정보통신망 이용촉진 및 정보보호 등에 관한 법률 제2조 1항 7조>

"침해사고"란 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태를 말한다.

❍ 침해사고 유형

- 바이러스, 트로이잔, 웜, 백도어, 악성코드 등의 공격
- 비인가된 시스템 접근 및 파일 접근
- 네트워크 정보 수집을 포함한 비인가된 네트워크 정보 접근
- 네트워크 서비스의 취약점을 이용하여 서비스를 무단 이용하는 비인가된 서비스 이용
- 네트워크 및 시스템의 정상적인 서비스를 마비 또는 파괴시키는 서비스 방해

❍ 침해사고 대응 7단계



- **(1단계: 사고 전 준비)** 사고가 발생하기 전 침해사고 대응팀과 조직적인 대응을 준비
- **(2단계: 사고 탐지)** 정보보호 및 네트워크 장비에 의한 이상 징후 탐지. 관리자에 의한 침해사고의 식별
- **(3단계: 초기 대응)** 초기 조사 수행, 사고 정황에 대한 기본적인 세부사항 기록, 사고대응팀 신고 및 소집, 침해사고 관련 부서에 통지
- **(4단계: 대응 전략 체계화)** 최적의 전략을 결정하고 관리자 승인을 획득, 초기 조사 결과를 참고하여 소송이 필요한 사항인지를 결정하여 사고 조사 과정에 수사기관 공조 여부를 판단
- **(5단계: 사고조사)** 데이터 수집 및 분석을 통하여 수행. 언제, 누가, 어떻게 사고가 일어났는지, 피해 확산 및 사고 재발을 어떻게 방지할 것인지를 결정
- **(6단계: 보고서 작성)** 의사 결정자가 이해할 수 있는 형태로 사고에 대한 정확한 보고서를 작성
- **(7단계: 해결)** 차기 유사 공격을 식별 및 예방하기 위한 보안 정책의 수립, 절차 변경, 사건의 기록, 장기 보안 정책 수립, 기술 수정 계획 수립 등을 결정

<각 단계별 세부 내용은 침해사고 분석절차 안내서 참고>

http://www.kisa.or.kr/jsp/common/down.jsp?folder=uploadfile&filename=%EC%A0%9C2010-8%ED%98%B8-%EC%B9%A8%ED%95%B4%EC%82%AC%EA%B3%A0_%EB%B6%84%EC%84%9D_%EC%A0%88%EC%B0%A8%28%EB%82%B4%EC%A7%80%29%EC%B5%9C%EC%A2%85%28fin%29.pdf

II. 사고 유형별 시스템 점검항목 및 조치 방안

<한국인터넷진흥원에 분석을 요청할 경우 유의사항>

- 침해사고 관련 파일(악성코드, 프로세스)등을 제거하지 않은 상태에서 분석요청
- 불가피하게 제거해야 할 경우 악성파일은 경로와 MAC time(생성·접근·수정 시간)을 확보하고, 프로세스는 해당 프로세스와 관련된 디렉토리 또는 파일 경로와 MAC time을 확보해야 함(**악성파일 백업 필수**)

※ 리눅스의 경우 stat 명령문과 lsof 명령문 활용

사고 유형 - 공통

❍ 시스템 점검 사항

사고유형	점검항목	점검 내용	비고
공통	계정	· 사용하지 않는 계정 및 숨겨진 계정 확인 ☞ Windows : [관리도구]->[컴퓨터 관리]->[로컬사용자 및 그룹]->[사용자] 정보 확인 ☞ Linux : /etc/passwd 확인	· $ 문자가 포함된 계정 확인 · 패스워드 미설정 계정 확인 · /bin/bash 점검
	로그파일	· 이벤트 로그 및 시스템 로그 변조 유무 확인 ☞ Windows : [관리도구]->[컴퓨터 관리]->[이벤트뷰어] 확인 ☞ Linux : /var/log/secure, message 등 확인 · 웹로그 경로 및 변조 유무 확인 ☞ [관리도구]->[인터넷정보서비스(IIS)관리]에서 웹로그 경로 확인 ☞ Linux : /usr/local/apache/logs 확인	· 웹로그 생성/수정 시간 확인
	웹쉘	· 확장자별 웹쉘 Signature 점검 ☞ asp, aspx, asa, cer, cdx, php, jsp, html, htm, jpg, jpeg, gif, bmp, png	· 휘슬(WHISTL) 사용 ※ www.krcert.or.kr 신청 ※ 사용법 : 붙임1 참조
	백도어	· 네트워크 상태 확인 ☞ nmap -sV *서버IP* · 비정상 포트 및 외부연결 확인 ☞ Windows : netstat, TCPView 등 사용 ☞ Linux : netstat -nlp, lsof -i	· 6666, 6667 등 의심 Port 확인 · 의심 Port를 사용하는 프로세스 확인
	루트킷	· 숨겨진 프로세스 및 비정상 프로세스 확인 · 변조된 파일 및 시스템 명령어 확인 ☞ Windows : IceSword, GMER 등 사용 ☞ Linux : Rootkit Hunter, Check Rootkit 등 사용	· Rootkit Hunter 업데이트 필수 ☞ rkhunter --update ※ 사용법 : 붙임1 참조

❍ 특이사항 발생에 따른 조치 방안

- 사용하지 않는 계정과 숨겨진 계정 삭제
- 웹쉘 발견 시 업로드된 경로를 파악하여 해당 취약점 제거
- 루트킷의 경우 일부 시스템 명령어만 변조된 경우는 무결성이 보장된 명령어로 교체 가능하나 다수의 라이브러리들이 변조되었을 경우는 시스템 재설치 필요
- 백도어 포트가 발견될 경우 해당 port에 대한 차단정책을 적용하고 백도어 서비스와 관련된 파일을 확인하여 삭제(차단정책 적용을 위해 서버내 방화벽(iptables, hosts.allow/deny 활용 가능)
- 서버내 바이너리 변조를 통한 백도어 증상 확인 시 관련된 바이너리 제거 및 재설치

※ 리눅스 바이너리 변조 여부 확인 : rpm -Va 활용 가능

사고 유형 – 웹변조

❍ 시스템 점검사항

사고유형	점검항목	점검 내용	비고
웹사이트 변조	웹페이지 확인	· 공통 : index.html, main.html, default.html, index.php, main.php · Windows : index.asp, main.asp, default.asp	· 기타 메인페이지로 설정된 파일 확인
	HTTP 메소드	· Windows : WebDAV 활성화 확인 ☞ [관리도구]->[인터넷정보서비스(IIS)관리]->[웹서비스 확장] 허용 여부 확인 · Linux : Apache 웹서버의 httpd.conf 확인 ☞ <Directory/>에서 MOVE 또는 PUT 메소드 allow 설정 여부 확인	· Windows : [사용금지]로 설정 · Linux : deny로 설정
	웹로그 분석	· MOVE, PUT 메소드 공격 여부 확인 ☞ grep MOVE 웹로그 | grep -v 404	· Linux : grep 기본 제공 · Windows : grep.exe 사용

❍ 특이사항 발생에 따른 조치 방안

- 윈도우 IIS 웹서버의 WebDAV가 활성화 되어 있을 경우 사용 중지

- 리눅스 아파치 웹서버의 설정파일에서 사용하지 않는 HTTP 메소드에 대해 허용 금지
- IIS 웹서버 또는 아파치 웹서버의 설정이 변경되었을 경우 관리자 계정 변경 필수
- 웹페이지 내용이 변경되었을 경우 휘슬을 통해 웹쉘 감염여부를 확인하고 발견될 경우 삭제 조치
- 웹쉘이 발견될 경우 웹 접속로그를 통해 웹쉘에 접근한 IP를 확인하고 방화벽을 통해 접근 제한 정책 적용

사고 유형 - 악성코드 경유지 / 유포지

❍ 시스템 점검사항

사고유형	점검항목	점검 내용	비고
악성코드 유포지/경유지	웹페이지 확인	· 악성코드 유포 페이지 확인 ☞ x.html 등과 같은 의심 페이지 점검 · 악성코드 유포지 URL 삽입 페이지 검출 ☞ grep -r *"유포지 URL"* 웹페이지Path · 웹페이지 생성 및 수정 시간 확인	· KISA에서 보급중인 휘슬 설치 권장 ※ www.krcert.or.kr 신청
	접속 IP 확인	· 악성코드 유포/경유 페이지 접속 IP 추출 ☞ grep "유포/경유 페이지 Path" 웹로그 Path ※ 추출된 IP는 악성코드에 감염된 좀비 PC를 확보하는데 매우 중요	

❍ 특이사항 발생에 따른 조치 방안

- 악성코드 유포 페이지에 대한 파일 생성 및 수정시간 확인
- 유포 페이지 생성 시점 기준으로 웹 접속로그 및 시스템 로그를 분석하여 또 다른 침해여부 확인
- 휘슬을 통해 웹쉘 감염여부를 확인하고 발견될 경우 삭제 조치
- 웹쉘이 발견될 경우 웹 접속로그를 통해 웹쉘에 접근한 IP를 확인하고 방화벽을 통해 접근 제한 정책 적용

사고 유형 - 봇넷 C&C

❍ 시스템 점검사항

사고유형	점검항목	점검 내용	비고
봇넷 C&C	네트워크 연결	· 외부 네트워크 연결 확인 ☞ Windows - netetat -na를 통해 확인 후 의심 Port (6667, 6668 등과 같은 IRC Port)에 연결된 IP를 확인 ☞ Linux : netstat -na 또는 lsof -i - Windows와 동일하게 확인 · 네트워크 트래픽 분석 ☞ Windows : Wireshark를 사용하여 패킷 분석 ☞ Linux : TCPDump를 사용하여 패킷 분석	

❍ 특이사항 발생에 따른 조치 방안

- 외부 네트워크와 연결된 백도어 포트 발견 시 방화벽을 통해 해당 포트로의 접근 제한 정책 적용
- 백도어 포트 서비스를 실행중인 파일 확인 및 삭제

사고 유형 - 해킹 경유지

❍ 시스템 점검사항

사고유형	점검항목	점검 내용	비고
해킹 경유지	네트워크	· 공통 : Nmap, netstat 사용하여 의심 Port 확인 ☞ nmap -sV *서버IP* ☞ 1723, 4444, 38317 등 의심 Port 확인 · Windows : RRAS 서비스 설정 확인 ☞ [컴퓨터 관리]->[서비스 및 응용프로그램]->[서비스]의 Routing and Remote Access 서비스 시작유형(사용안함) 확인 · Linux : PPTP 서비스 실행 확인 ☞ ps -ef 명령 실행 후 pptpd 프로세스 확인	· RRAS 및 PPTP 프로세스는 VPN 서비스
	설치 프로그램 확인	· Windows : CCProxy, RealVNC 등 설치 확인 ☞ [제어판]->[프로그램 추가/제거]에서 설치 여부 확인 · Linux : Rootkit Hunter, Check Rootkit 검사를 통해 악성 프로그램 설치 여부 확인	· Rootkit Hunter 업데이트 필수 ☞ rkhunter --update ※ 설치는 붙임 참고

❍ 특이사항 발생에 따른 조치 방안

- 윈도우 서버의 RRAS 서비스가 실행중일 경우 해당 서비스 중지
- 윈도우 서버의 이벤트 로그를 통해 RRAS 서비스를 실행시킨 이력 및 IP를 확인하고 해당 IP에 대한 접근 제한 정책 적용
- 리눅스 서버의 PPTP 서비스가 실행중일 경우 해당 프로세스 중지
- 리눅스 서버의 시스템 로그를 통해 PPTP 서비스를 실행시킨 이력 및 IP를 확인하고 해당 IP에 대한 접근 제한 정책 적용

III. 웹 서버 취약점 조치 방안

<상세한 조치 방안은 웹서버 구축 보안점검 안내서 참고>

http://www.kisa.or.kr/jsp/common/down.jsp?folder=uploadfile&filename=%EC%A0%9C2010-9%ED%98%B8-%EC%9B%B9%EC%84%9C%EB%B2%84_%EA%B5%AC%EC%B6%95_%EB%B3%B4%EC%95%88%EC%A0%90%EA%B2%80_%EC%95%88%EB%82%B4%EC%84%9C.pdf

※ 취약점 점검 체크리스트 제공

❍ OS에 대한 최신 패치 적용

- OS 벤더사이트나 보안 취약점 정보 사이트를 주기적으로 방문하여 현재 사용하고 있는 OS에 대한 최신 취약점 정보획득 및 패치
- 정기적으로 취약점 점검 도구와 보안 체크리스트를 사용하여 호스트 OS의 보안 취약점 점검

❍ 웹 서버 전용 호스트로 구성

- 웹 서비스 운영에 필요한 최소한의 프로그램들만 남겨두고 불필요한 서비스들은 반드시 제거
- 시스템 사용을 목적으로 하는 일반 사용자 계정은 모두 삭제하거나 최소한의 권한만 할당
- 오직 관리자만이 로그인 가능하도록 설정

❍ 서버에 대한 접근 제어

- 관리목적의 웹 서버 접근은 콘솔 접근만을 허용
- 위 사항이 불가능할 경우 관리자가 사용하는 PC의 IP만 접근이 가능하도록 접근제어 수행

❍ DMZ 영역에 위치

- 웹 서버를 방화벽에 의해서 보호 받도록 하고, 웹 서버가 침해당하더라도 웹 서버를 경유해서 내부 네트워크로의 침입은 불가능하도록 구성

❍ 강력한 관리자 계정 패스워드 사용

- 관리자 계정 패스워드는 유추가 불가능하고 패스워드 크랙으로도 쉽게 알아낼 수 없는 강력한 패스워드 사용
- 패스워드 길이는 최소 8자 이상을 사용하고, 이름이나 계정명으로 유추할 수 없도록 구성
- 또한, 사전에 없는 단어를 사용하고 기호문자를 최소 한 개이상 포함

❍ 파일 접근권한 설정

- 관리자 계정이 아닌 일반 사용자 계정으로 관리자 계정이 사용하는 파일들을 변경할 수 없도록 구성

❍ 웹 프로세스의 권한 제한

- 시스템 전체적인 관점에서 웹 프로세스가 웹 서비스 운영에 필요한 최소한의 권한만을 갖도록 제한
- 웹 서버 관리시에는 일반적으로 사용되는 nobody 권한으로 웹 프로세스가 동작하도록 구성

❍ 로그 파일의 보호

- 침입 혹은 침입시도 등 보안 문제점 파악을 위해 로그 파일이 노출, 변조 혹은 삭제되지 않도록 불필요한 접근으로부터 보호
- 불필요한 접근으로부터 보호하기 위해 로그파일을 별도의 서버에 백업하여 관리하는 것이 필요
- 로그파일은 최소 3개월 이상의 로그를 확보하는 것이 필요

❍ 웹 서비스 영역의 분리

- 웹 서비스 영역과 시스템(OS)영역을 분리시켜서 웹 서비스의 침해가 시스템 영역으로 확장될 가능성을 최소화
- 웹 서버의 루트 디렉토리와 OS의 루트 디렉토리를 다르게 지정

❍ 설정파일 백업

- 초기 설정 파일을 백업 받아서 보관해 두고, 변경이 있을 때마다 설정 파일을 백업함으로써 해킹사고 발생 시 빠르게 복구

❍ Inbound 트래픽 제한

- 공개용 침입차단시스템을 이용하여 트래픽을 제한

※ 리눅스 커널에서는 iptables 또는 ipchains 침입차단 시스템이 기본으로 제공됨

- 전체 서비스(포트)에 대해 차단 설정 후 고객이 필요로 하는 서비스(포트)에 대해 선별적으로 접속 제한을 해제

※ 필요 서비스(포트) 예 : FTP(21), SSH(22), SMTP(25), DNS(53), SSL(443)등

- 필요할 경우 아래와 같이 iptables를 사용하여 특정 포트에 대한 Inbound 트래픽을 제한

※ iptables는 테이블 형식으로 관리되며, 먼저 등록된 것이 효력을 발생하기 때문에 허용하는 정책이 거부하는 정책보다 먼저 위치해야 함

```
iptables -A INPUT -p TCP --dport 22  -s ip앞 세자리.0/24 -j ACCEPT
iptables -A INPUT -p TCP --dport 22  -s 192.168.0.0/24 -j ACCEPT
iptables -A INPUT -p TCP --dport 22 -j DROP
 → ssh 포트에 대해 특정 ip군과 사설ip만 허용하고 나머지는 Drop
```

IV. 네트워크 취약점 조치 방안

<상세한 조치 방안은 웹서버 구축 보안점검 안내서 참고>

http://www.kisa.or.kr/jsp/common/down.jsp?folder=uploadfile&filename=%EC%A0%9C2010-9%ED%98%B8-%EC%9B%B9%EC%84%9C%EB%B2%84_%EA%B5%AC%EC%B6%95_%EB%B3%B4%EC%95%88%EC%A0%90%EA%B2%80_%EC%95%88%EB%82%B4%EC%84%9C.pdf

❍ 네트워크 장비의 원격 접근 제한 설정

- 허용된 ip 외에는 telnet이나 ssh를 통해 네트워크 장비에 원격 접속할 수 없도록 제한

❍ SNMP 접근 제한 설정

- 패스워드 역할을 하는 community 문자열의 default 값(public)을 추측하기 어렵고 의미없는 문자열로 변경
- 네트워크 장비에서 ACL(access-list) 기능을 이용하여 SNMP에 대한 접근 제한

❍ 불필요한 서비스 중단

- 네트워크 장비를 처음 설치하거나 IOS등을 업그레이드 한 후에는 사용하지 않거나 보안상 불필요한 서비스를 반드시 중지

❍ 설정을 통한 로그인시간 제한

- 로그인 한 후 일정 시간동안 아무런 명령어를 입력하지 않으면 자동으로 접속을 종료하도록 설정

❍ 로그 관리

- 시스템 자체적으로 제공하는 로그와, access-list와 같은 특정한 룰에 매칭되는 로그를 남기도록 설정

V. DB 취약점 조치 방안

<상세한 조치 방안은 웹서버 구축 보안점검 안내서 참고>

http://www.kisa.or.kr/jsp/common/down.jsp?folder=uploadfile&filename=%EC%A0%9C2010-9%ED%98%B8-%EC%9B%B9%EC%84%9C%EB%B2%84_%EA%B5%AC%EC%B6%95_%EB%B3%B4%EC%95%88%EC%A0%90%EA%B2%80_%EC%95%88%EB%82%B4%EC%84%9C.pdf

DB 구분 - My SQL

❍ DB 시스템 보안패치 적용

- My-SQL이 동작하는 시스템에 대한 기본적인 보안패치 적용

❍ DBMS 계정 확인

- My-SQL 디폴트 설치 시 설정되지 않은 채 비어있는 데이터베이스 관리자 패스워드 변경

※ My-SQL의 관리자인 root는 기본 설치 시 비밀번호가 NULL로 설정됨

- My-SQL 설치 시 기본적으로 생성되어 있는 'test' 계정 삭제

❍ 원격으로 부터의 접속 차단

- My-SQL이 디폴트로 리스닝하는 3306/tcp 포트를 차단함으로써 데

이터베이스가 로컬로 설치된 PHP 어플리케이션에 의해서만 사용되도록 설정

- 데이터 백업 등의 이유로 데이터베이스로 원격에서 접속해야 하는 경우 SSH 프로토콜 사용

❍ 데이터베이스내의 사용자별 접속/권한 설정 확인

- DB 생성 후 사용자 접근 권한 설정 시 일반 사용자에게는 최소한의 권한만을 부여

❍ 데이터 디렉토리 보호

- My-SQL 데몬을 mysql이라는 시스템 계정으로 구동할 경우, mysql 디렉토리 이하에 대한 읽기, 쓰기 권한을 제한함으로써 데이터 파일 및 로그파일 보호

DB 구분 - MS SQL

❍ DB 시스템 보안패치 적용

- MS에서 제공되는 서비스 팩과 수시로 발표되는 보안패치 설치

❍ 인증 및 계정관리 확인

- 윈도우 인증모드 사용을 통해, SQL 사용 권한이 없는 도메인 사용자 또는 윈도우 사용자로부터 윈도우 비밀번호 정책을 사용하여 보안 강화
- 게스트 계정 비활성화
- sysadmin은 데이터베이스에 대한 완전한 관리 권한을 필요로 하는 사용자를 위해 만들어진 역할이므로, 이 역할에 인증되지 않은 사용자는 삭제

❍ 외부로부터의 SQL Server 포트 접속 차단

- SQL Server의 디폴트 포트인 1433/tcp, 1434/tcp를 임의의 다른 포트로 설정하여 운영

❍ 확장 프로시저 제거

- 서버의 유지관리를 위해 제공하는 확장 프로시저 중 공격에 자주 이용되고 있는 특정 프로시저(xp_cmdshell) 제거

VI. 어플리케이션 취약점 조치 방안

상세한 조치 방안은 홈페이지 개발보안 안내서 참고

http://www.kisa.or.kr/jsp/common/down.jsp?folder=uploadfile&filename=%EC%A0%9C2010-11%ED%98%B8-%ED%99%88%ED%8E%98%EC%9D%B4%EC%A7%80_%EA%B0%9C%EB%B0%9C_%EB%B3%B4%EC%95%88_%EC%95%88%EB%82%B4%EC%84%9C.pdf

❍ 웹 취약점 점검 서비스 수행(http://www.krcert.or.kr)

- 원격으로 웹 공격에 대한 취약점 점검 수행, 점검 결과 제공

❍ 휘슬 설치 및 주기적인 검사 수행(http://www.krcert.or.kr)

- 공격자에 의해 생성된 웹쉘 및 악성코드 은닉 사이트 탐지 가능

❍ 캐슬 설치 및 운영(http://www.krcert.or.kr)

- 홈페이지 보안성 강화를 위한 웹방화벽 기능 제공

❍ 접근통제 취약점에 대한 조치

설명 – /admin, /admin_login 등과 같이 보편적으로 사용되는 관리자 페이지 주소를 입력하여 해당페이지로 접근이 가능한 취약점
· 관리자 페이지를 유추하기 어려운 주소로 변경하고 관리자 호스트 IP만 접근 가능하도록 설정

❍ 부적절한 파라미터 취약점에 대한 조치

설명 – URL, 쿼리 문자열, HTTP 헤더, 쿠키, HTML 폼 인자, HTML hidden 필드 등의 HTTP 요청을 변조하여 웹사이트의 보안 메커니즘을 우회하는 취약점
· 모든 입력 값에 대해 중앙에서 집중적으로 처리하는 하나의 컴포넌트나 라이브러리를 사용하여 모든 인자에 대해 사용전에 입력 값 검증을 수행하도록 구성

❍ Cookie Injection 취약점에 대한 조치

설명 – 쿠키 값 변조를 통해 다른 사용자로의 위장 및 권한상승을 수행할 수 있는 취약점
· Client Side Session 방식인 Cookie는 구조상 다양한 취약점에 노출될 수 있으므로 웹서버에서 제공되는 Sever Side Session을 사용 · SSL과 같은 기술을 사용하여 로그인 트랜잭션 전체를 암호화

❍ SQL Injection(악의적인 명령어 주입) 취약점에 대한 조치

설명 – 데이터베이스 접근을 위해 사용되는 SQL Query문을 비정상적으로 조작하여 사용자 인증 우회, DB에 저장된 데이터 열람, DB의 시스템 명령어를 이용하여 시스템 조작 등의 행위를 할 수 있는 취약점
· 데이터베이스와 연동하는 스크립트의 모든 파라미터를 점검하여 사용자의 입력 값이 SQL injection을 일으키지 않도록 수정 ※ 사용자 입력값 및 URL 인자값에 대해 특수문자(‘, “, ', ;, :, %, Space, --, +, <, >, (,), #, & 등)와 SQL 구문(Insert, Select 등)이 포함되어 있는지 검사 후 허용되지 않은 문자열이나 문자가 포함된 경우에는 에러로 처리 · SQL 서버의 에러 메시지를 사용자에게 보여주지 않도록 설정 · 웹 어플리케이션이 사용하는 데이터베이스 사용자의 권한을 제한하여 일반 사용자 권한으로는 모든 system stored procedures에 접근하지 못하도록 설정함으로써

SQL Injection 취약점을 이용하여 데이터베이스 전체에 대한 제어권을 얻거나 데이터베이스를 운용중인 서버에 접근이 불가능하도록 수정

· php.ini 설정 중 magic_quotes_gpc 값을 On으로 설정

❍ XSS(크로스사이트 스크립팅) 취약점에 대한 조치

설명 – 자바스크립트처럼 클라이언트 측에서 실행되는 언어로 작성된 악성 스크립트 코드를 웹 페이지, 웹 게시판 또는 이메일에 포함시켜 사용자에게 전달하면, 해당 웹 페이지나 이메일을 사용자가 클릭하거나 읽을 경우 악성 스크립트 코드가 웹 브라우저에서 실행되는 취약점

· 사용자로부터 입력받는 모든 값을 서버에서 검증 후 입력 받도록 수정

· 스크립트 문장에 존재할 수 있는 아래와 같은 특수 문자를 다른 문자로 변환하도록 소스를 수정

※ 특수 문자 치환 예

<	→	&lt
>	→	&gt
(	→	&#40
)	→	&#41
#	→	&#35
&	→	&#38

· 특수 문자 변환을 위해서는 Server Side 언어별로 아래와 같은 함수 이용 가능

※ ASP : Server.HTMLEncode( )
PHP : htmlspecialchars( ) 또는 strip_tags( ) 또는 strip_replace( )

❍ 버퍼 오버플로우 취약점에 대한 조치

설명 – 지정된 버퍼의 크기보다 큰 데이터를 저장함으로써 실행 시 오류를 발생시키는 취약점

· 서버 제품군과 라이브러리의 경우, 사용하고 있는 제품군에 대한 최신 버그 리포트를 지속적으로 참고하여 최신 패치를 적용

· 자체 제작한 어플리케이션의 경우 HTTP 요청을 통해 사용자의 입력을 받아들이는 모든 코드를 검토하여 입력 값에 대해 적절한 크기를 점검하는지 확인

❍ CSRF(스크립트 요청 참조) 취약점에 대한 조치

설명 – 공격자가 사용자의 Cookie 값이나 Session 정보를 의도한 사이트로 보내거나 특정한 동작을 유발하는 스크립트를 글에 삽입하여 사용자가 게시물 등

을 클릭할 경우 공격자가 원하는 동작이 실행되게 하는 취약점
· 헤더, 쿠키, 질의문, 폼 필드, 숨겨진 필드등과 같은 모든 파라미터들을 엄격한 규칙에 의해서 검증하여 HTML을 사용할 경우 태그 내에 html, ?, & 등이 포함되지 않도록 수정

❍ RFI(Remote File Inclusion) 취약점에 대한 조치

설명 – URL이나 파일시스템 참조 등 외부 객체 참조를 사용하는 어플리케이션에서 입력파일 또는 입력 외부객체를 검증하지 않을 때 발생하는 취약점

· PHP 환경설정 파일 수정

※ PHP 4.x 이하 버전 : 'allow_url_fopen' 항목을 'off'로 변경
PHP 5.x 이하 버전 : 'allow_url_fopen' 항목과 'allow_url_include' 항목을 'off'로 변경

· 외부 사이트의 소스 실행이 반드시 필요한 홈페이지에 대해서는 선별적으로 해당 기능을 허용

```
<VirtualHost www.abc.co.kr>
        ServerAdmin webmaster@abc.co.kr
        DocumentRoot /home/abc/public_html
        ServerName www.abc.co.kr
        php_admin_flag allow_url_fopen On ←추가
</VirtualHost>
```

❍ 파일 업로드 취약점에 대한 조치

설명 – 공격자가 조작한 Server Side Script 파일을 게시판 등에 업로드하고, 업로드된 파일이 서버상에 저장된 경로를 유추한 후 이 경로를 통해 Server Side Script 파일을 실행하여 쉘을 획득하거나 권한을 탈취하는 취약점

· Upload 파일을 위한 전용 디렉토리를 별도 생성하여 httpd.conf와 같은 웹 서버 데몬 설정파일에서 실행 설정을 제거함으로써, Server Side Script가 Upload되더라도 웹 엔진이 실행하지 않게 환경을 설정

※IIS보안 설정
설정 -> 제어판 -> 관리도구 -> 인터넷 서비스 관리자 선택 -> 해당 Upload 폴더에 오른쪽 클릭을 하고 등록 정보 -> 디렉토리 -> 실행권한을 '없음'으로 설정

※Apache 설정
Apache 설정 파일인 httpd.conf의 해당 디렉토리에 대한 문서 타입을 컨트롤하기 위해 Directory 세션의 AllowOverride 지시자에서 FileInfo 또는 All 추가

```
<Directory "/usr/local/apache">
    AllowOverride FileInfo(또는 All) ...
    ...
```

```
</Directory>
```

파일 업로드 디렉토리에 .htaccess 파일을 만들고 AddType 지시자를 이용, 현재 서버에서 운영되는 Server Side Script 확장자를 text/html로 MIME Type을 재조정하여 업로드 된 Server Side Script가 실행되지 않도록 설정

```
<.htaccess>
  <FilesMatch "\.(ph|inc|lib)">
    Order allow, deny
    Deny from all
  </FilesMatch>
  AddType text/html .html .htm .php .php3 .php4 .phtml .phps .in .cgi .pl .shtml .jsp
```

설정 후 데몬 재시작

※ 모든 확장자를 제한하고 허용하는 일부 확장자만 업로드 되도록 제한
확장자 검사 우회(ex. shell.gif.jsp, shell.jpg.jsp)를 막기 위해 뒤에서부터 검사하도록 수정

❍ 파일 다운로드 취약점에 대한 조치

설명 – 웹 어플리케이션에서 상대경로를 사용할 수 있도록 설정되어 있는 경우, 상대경로 표시 문자열인 "../"를 통해 허가되지 않은 상위경로로 이동하여 시스템 주요 파일, 소스코드 등 중요자료의 열람이 가능한 취약점
· 파일 다운로드 시 파일명을 직접 URL에서 사용하거나 입력받지 않도록 하며, 게시판 이름과 게시물 번호를 이용하여 서버 측에서 데이터베이스 재검색을 통하여 해당 파일을 다운로드 할 수 있도록 수정 · 다운로드 위치는 지정된 데이터 저장소를 지정하여 사용하고, 데이터 저장소 상위 디렉토리로 이동되지 않도록 설정 · PHP를 사용하는 경우 php.ini에서 magic_quotes_gpc를 On으로 설정하여 ".\./"와 같은 역 슬래시 문자에 대응할 수 있도록 설정

❍ 부적절한 파라미터 취약점에 대한 조치

설명 – 웹 어플리케이션에서 상대경로를 사용할 수 있도록 설정되어 있는 경우, 상대경로 표시 문자열인 "../"를 통해 허가되지 않은 상위경로로 이동하여 시스템 주요 파일, 소스코드 등 중요자료의 열람이 가능한 취약점
· 파일 다운로드 시 파일명을 직접 URL에서 사용하거나 입력받지 않도록 하며, 게시판 이름과 게시물 번호를 이용하여 서버 측에서 데이터베이스 재검색을 통하여 해당 파일을 다운로드 할 수 있도록 수정 · 다운로드 위치는 지정된 데이터 저장소를 지정하여 사용하고, 데이터 저장소 상위 디렉토리로 이동되지 않도록 설정

❍ 백업 파일 노출 취약점에 대한 조치

설명 – 관리자가 홈페이지 상에서 작은 수정을 위해 기존 홈페이지 파일의 원본을 특정 확장자를 사용하여 저장할 수 있는데, 이러한 특정 확장자의 파일들이 서버에서 적절하게 처리되지 못할 경우 소스가 유출 될 수 있는 취약점

· 백업파일이 웹 서버에 존재하는 것은 소스 노출이나 DB정보 노출 등의 문제가 발생할 수 있으므로 웹 서버상의 불필요한 백업 파일들은 모두 삭제

· 홈페이지 서비스와 관련없는 디렉토리(백업디렉토리 등)는 일반 사용자 접근이 불가능하도록 권한 설정

```
<Files ~ "\.bak$">
  Order allow,deny
  Deny from all
</Files>
```

❍ 디렉토리 리스팅 취약점에 대한 조치

설명 – 웹 서버에는 현재 브라우징 하는 디렉토리의 모든 파일들을 사용자에게 보여 줄 수 있는 디렉토리 인덱스 기능이 존재하는데, 이런 설정이 활성화되어 있는 경우 공격자가 웹 어플리케이션의 구조를 파악할 수 있는 기회를 제공하게 되는 취약점

· 아파치 웹서버 : httpd.conf 파일에서 DocumentRoot 항목을 아래와 같이 수정

```
...
<Directory "/usr/local/www">
  Options Indexes ← 제거한다
</Directory>
...
```

· IIS 웹서버 : IIS 관리메뉴의 기본웹사이트 등록정보에서 홈 디렉토리 검색부분 체크 해제

❍ 설정파일 및 환경변수 노출 취약점에 대한 조치

설명 – 웹 어플리케이션을 설정하기 위해 위치하는 파일들은 시스템이나 DB에 관련한 많은 정보를 포함하고 있는데, 이런 파일들이 공격자에게 노출될 경우 공격자에게 시스템의 많은 정보를 제공하게 되는 취약점

· 홈페이지 서비스와 관련없는 파일은 일반 사용자 접근이 불가능하도록 권한 설정

❍ 부적절한 HTTP Method 사용 취약점에 대한 조치

설명 - 원격 사용자가 DocumentRoot 디렉토리에 파일을 업로드하거나 수정하는 등의 행위를 하는 것을 제한해야 하는데, 이러한 제한이 적절히 이루어지지 않을 경우 홈페이지가 변조되거나 침해를 입을 수 있는 취약점

· PUT, DELETE Method는 제한된 사용자만 가능하도록 하거나 아무도 사용하지 못하도록 아래와 같이 설정

```
...
<Directory "/home/*/public_html">
  <Limit POST PUT DELETE>
  Require valid-user
  </Limit>
</Directory>
...
```

❍ 헤더 정보 노출 취약점에 대한 조치

설명 - 웹 서버에서는 응답 메시지의 헤더에 웹 서버 버전이나 응용 프로그램 버전 등을 전송하는데, 많은 정보들이 노출될 경우 알려진 취약점을 이용한 공격에 악용될 수 있는 취약점

· 아파치 웹 서버의 경우 httpd.conf 내용에 ServerTokens 지시자를 삽입하여 헤더에 의해 전송되는 정보를 최소화

❍ 오류 메시지 노출 취약점에 대한 조치

설명 - 오류 메시지가 공격자에게 무엇이 틀렸는지 알려주는 표시를 해주는 것으로 인해 공격자가 다양한 공격 방법을 시도할 수 있게 되는 취약점

· 별도의 오류 페이지를 제작하여 각각의 오류코드에 대해 제작된 하나의 오류 페이지로 Redirection 처리
· 아파치 웹 서버의 경우 httpd.conf 파일에서 아래와 같이 설정

```
ErrorDocument 404 /error_page.html
```

❍ 파일시스템 설정 오류 취약점에 대한 조치

설명 - 악성 프로그램을 /tmp, /dev/shm등의 파일시스템 관련 디렉토리에 업로드

하여 실행하는 형태로 공격에 악용될 수 있는 취약점
· /etc/fstab(파일시스템의 마운트 설정정보 파일) 내용을 아래와 같이 수정하여 해당 디렉토리의 실행권한을 제거(변경 후에는 mount 명령을 실행하여 적용해야 함) none on /dev/shm type tmpfs (rw,noexec) /dev/hda9 on /tmp type ext3 (rw,noexec,nosuid,nodev)

❍ 심볼릭 링크 취약점에 대한 조치

설명 – 웹 서버에서 심볼릭 링크를 이용해서 기존의 웹 문서 이외의 파일시스템에 접근하는 것이 가능한 취약점
· 아파치 웹서버 환경설정파일(httpd.conf)의 Options 지시자에서 심볼릭 링크를 가능하게 하는 옵션인 “FollowSymLinks"를 제거

❍ 최신 보안 패치 항상 유지

- 제로보드, 테크보드, 그누보드 등의 웹 어플리케이션에 대한 최신의 보안패치를 유지

[붙임1] WHISTL 및 Rootkit Hunter, Check Rootkit 사용법

1. WHISTL 설치 및 사용.

- 다운로드 : http://toolbox.krcert.or.kra ☞ 웹사이트 보안도구 ☞ 휘슬

```
o root 디렉토리에 .whistl 디렉토리 생성
 [root@linux root]# mkdir . /whistl

o whistl 압축해제 및 실행권한 설정
 [root@linux .whistl]# tar zxvf Whistl_Linux.tgz
 [root@linux .whistl]# chmod 755 whistl_kernel_2.6
 ※ kernel 2.4.x 의 경우 whistl_kernel_2.4에 실행권한(755) 부여

o 실행
 [root@linux .whistl]# ./whistl_kernel_2.6
```

2. Rootkit Hunter 설치 및 사용

- 다운로드 : http://www.rootkit.nl/projects/rootkit_hunter.html

```
o 압축해제
 [root@linux root]# tar zxvf rkhunter-1.3.8.tar.gz
 [root@linux root]# cd rkhunter-1.3.8

o 설치
 [root@linux rkhunter-1.3.8]# ./installer.sh --layout default —install

o 업데이트
[root@linux rkhunter-1.3.8]# rkhunter —update

o 실행
[root@linux rkhunter-1.3.8]# rkhunter -c
```

3. Check Rootkit 설치 및 사용

- 다운로드 : http://www.chkrootkit.org/download.htm

o 압축해제

```
[root@linux root]# tar zxvf chkrootkit.tar.gz
[root@linux root]# cd chkrootkit
```

o 설치

```
[root@linux chkrootkit]# make sense;
```

o 실행

```
[root@linux chkrootkit]# ./chkrootkit -q
```

※ -q 옵션 : rootkit에 감염된 파일(프로세스)만 출력

[붙임2] 주요 용어 정리

o 해킹(Hacking)

- 컴퓨터 또는 시스템의 정당한 접근권한 없이 또는 허용된 접근권한을 초과하여 정보통신시스템에 침입하는 행위 [망법 제48조 1항, 3항에 의한 정의]
- 예를 들어, 아이디, 비밀번호를 탈취 후 타인의 시스템에 접속 하여 정보를 유출하거나 S/W의 취약점을 악용하여 시스템 침입·파괴하는 행위
- 최근에는 악성코드 및 해킹도구를 복합적으로 활용하여 해킹하는 추세

o 악성코드(Malicious Code/program)

- 정당한 사유없이 정보통신시스템, 데이터 등을 훼손·멸실·변경 또는 그 운용을 방해할 수 있는 프로그램 [망법 제48조 2항에 의한 정의]
- 일반적으로는 정보유출, 시스템 파괴, 원격조종 등 악의적인 목적으로 이용하는 컴퓨터 프로그램을 총칭

o 홈페이지 변조(Defacement)

- 홈페이지의 화면을 변조시켜 다른 이미지가 보이도록 하는 침해사고 유형을 의미하며, 특정 기업이나 조직의 이미지, 신뢰성 등을 실추하려는 목적으로 많이 발생

o 권한상승

- 시스템 사용에 있어 제한없이 자유자재로 사용하기 위해 시스템에서 허용하는 권한을 상승시키는 행위를 의미
- 예를 들면, 해커가 일반 사용자 권한을 획득한 후 → 관리자 권한(Root)을 획득하여 시스템 사용권한을 상승

o 웹쉘(WebShell)

- 해커가 원격에서 웹서버를 조종할 수 있도록 제작한 웹서버용 악성코드
- 웹서버가 가지고 있는 취약점을 악용해 웹쉘을 업로드시켜 웹서버를 해킹하는데 이용하거나, 해킹한 웹서버를 관리하기 위한 목적으로 설치하기도 함

o 바이러스(Virus)

- 정상적인 실행파일에 달라붙어(기생) PC를 다운시키거나 파일을 파괴하는 등 컴퓨터의 운영을 방해하는 악성코드의 일종
- 감염대상이 되는 파일이나 프로그램이 있어야 하며, 자신을 복제하는 기능이 있음

※ 주로 '80~'90년대에 많이 발생했고, 플로피디스크 등을 통해 감염

o 웜(Worm)

- 다른 파일에 기생하지 않고 독립적으로 자신을 복제하여 확산함으로써 전파속도가 매우 빠른 특징을 가지는 악성코드 유형
- 주로 메일이나 네트워크 공유폴더 등을 통해 전파되어 시스템과 네트워크에 부하를 높이는 증상을 보임

o 트로이목마(Trojan)

- 컴퓨터에 숨어 있다가 사용자의 정보를 몰래 유출하는 악성코드의 일종
- 정상적인 파일(게임, 응용S/W 등)에 포함되어 함께 설치되는 경우가 많음

※ 그리스 신화 트로이목마에서 개념이 나옴

o 백도어(Backdoor)

- 해커가 이용자 몰래 컴퓨터에 접속하여 악의적인 행위를 하기 위해 설치해 놓은 출입통로 역할을 하는 악성코드

o 루트킷(Rootkit)

- 루트킷은 해커가 설치한 악성코드(트로이목마, 악성봇 등)가 백신이나 PC 사용자에게 발각되지 않도록 숨겨주는 역할을 함
- 대부분의 루트킷은 일반 프로그램이 동작하는 계층보다 더 하위계층, 즉 커널이라는 운영체제 핵심 부분에 숨어서 동작하여 탐지·분석이 어려움

o 유포지 사이트

- 악성코드를 직접적으로 유포하는 웹사이트

o 경유지 사이트

- 실제 악성코드를 유포하지 않으나 이용자 PC가 감염되도록 악성코드 유포지로 연결시켜주는 웹사이트
- 해커가 자신의 위치를 속이기 위해 다른 시스템을 경유하여 공격할 때의 경유한 사이트

o 명령제어서버(C&C, Command and Control)

- 해커가 각 봇(좀비PC)을 관리하고 명령을 내리기 위해 구축하는 서버로, 사용자PC 등이 봇에 감염되면 해당 C&C서버로 자동 접속됨
- C&C서버에 접속하면 봇넷의 일원이 되고 해커가 C&C서버에 내리는 명령을 받아 다양한 공격을 수행하게 됨