12장 웹 침해사고 조사

박 종 혁 교수

UCS Lab

Tel: 02-970-6702

Email: jhpark1@seoultech.ac.kr

개요

- 학습 목표
  - 최근 침해사고는 대부분 웹 서비스를 통해 발생하고 있고, 이는 웹 해킹(Web Hacking)이라는 명칭으로 불리며 그 위험성이 커지고 있다.
  - 웹 해킹에 대한 정확한 사고 조사를 위한 방안을 알아본다.

- 학습 내용
  - 웹 침해사고의 특징
  - 사고 분석 절차
  - 사고 조사의 상세 내용

목 차

웹 침해사고의 특징

- 조사자는 웹 서비스의 기본적 구조와 원리에 대해 이해하고 있어야 함

- 조사자는 사고 발생시 피해 유형에 따라 원인 파악, 사고조사 범위를 한정 짓고, 정확하고 효율적인 사고 조사를 수행

- 기존의 포렌식 기술과 해킹 기술을 기본적으로 이해하고 있어야 정확한 공격 경로와 피해 범위를 파악할 수 있음

웹 침해사고의 특징 – 웹 서비스의 이해

- 웹 서비스
  - 사용자(웹 브라우저) + 서버(웹 서버/ 웹 어플리케이션 서버) + 데이터베이스 시스템
  - 웹 브라우저 ex)인터넷 익스플로러(IE)
  - 웹 서버 ex)IIS, 아파치(Apache)
  - 웹 애플리케이션(DB시스템을 연동하여 운영) ex)Tomcat
  - 웹 서버, 웹 애플리케이션 서버는 서비스의 규모, 구성, 부하 분산 등에 따라 동일한 서버 또는 별도의 서버에 존재
  - 데이터베이스 시스템은 일반적으로 개별 시스템에 구성, 규모에 따라 웹 서버 등과 함께 단일 시스템에 구성

웹 침해사고의 특징 – 웹 침해사고의 위험성

- 웹 침해사고는 단순히 개별 시스템 하나에서만 발생하는 것 아니라 전체 네트워크 신뢰에 큰 영향을 미침

- 조사자 입장에서 피해 규모, 공격자 추적 어려움

웹 침해사고의 특징 – 웹 침해사고의 위험성

- 피해 규모의 확산
  - 일반적 네트워크 구조에서 웹 서버, 웹 애플리케이션 서버는 DMZ에 존재
  - 공격자가 시스템 계정을 획득하면 데이터베이스까지 모두 장악 가능, 내부 사용자들이 신뢰할 수 있는 웹 어플리케이션을 수정하여 악성 코드를 내부 사용자 PC에 심을 수 있음

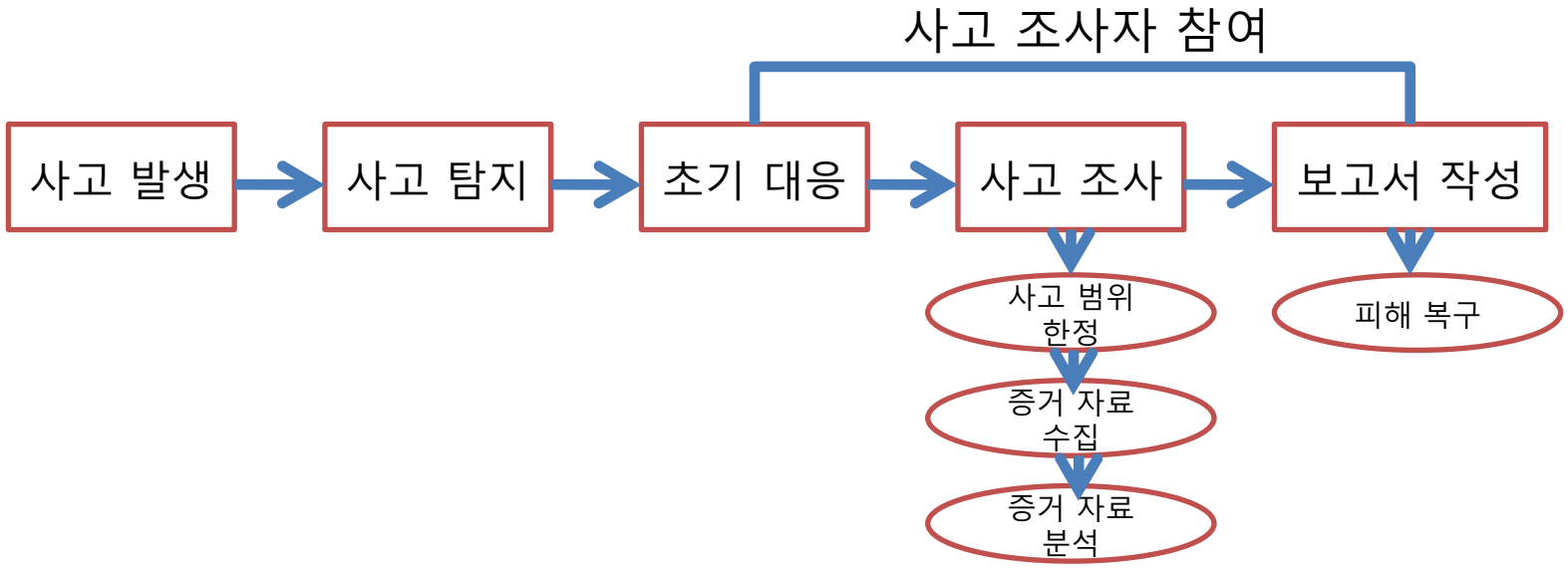
웹 침해사고의 특징 – 웹 침해사고의 위험성

- 탐지 및 추적의 어려움

  - 일반으로 침해가 발생한 시점과 탐지하는 시점 사이에 시간차가 존재하므로 이미 중요한 증거자료들이 훼손된 이후이기 때문에 사고분석이 어려움

  - 첫째, 공격자에 의해 증거자료가 변조 또는 삭제
  - 둘째, 로그가 존재하지 않거나 있다고 하더라도 방대한 분량으로 인해 분석이 쉽지 않음
  - 셋째, 공격자가 프록시 등을 통해 IP숨겼을 경우 추격의 어려움

웹 침해사고 분석 절차



- 사고 발생은 공격자가 정보 시스템에 실제적으로 악의적인 의도를 가지고 침해를 실시한 시점
- 사고 분석 절차의 시발점인 사고 탐지 단계와 시간차가 발생
- 사고 조사자가 실제적으로 참여하여 침해사고 분석하는 시점은 초기대응, 사고 조사, 보고서 작성 단계

웹 침해사고 분석 절차 – 사고 탐지

- 공격자의 침해 사실이 발견되는 단계
- 일반적으로 침해 사실이 많은 시간이 지난 후 발견
- 현재 대응책
  - 침입탐지시스템(IDS), 침입차단시스템(IPS), 웹 애플리케이션 방화벽 (Web Application Firewall; WAF)
  - 제한적인 탐지 및 차단만 가능, 근본적으로 웹 애플리케이션의 보안 수준이 개발자의 성숙도 차이, 보안 인지 여부, 실수 등으로 인해 최적화 되 있지 못함

웹 침해사고 분석 절차 – 초기 대응

- 발견된 이상현상에 대한 정보를 수집, 침해 사고 여부 파악 단계
- 증상 조사, 증거 보존, 관련자에게 연락 및 비상 대응팀 소집
- 사고 조사 전까지 지속적으로 상태 모니터링 및 최소한의 대응으로 증거의 훼손 최소화, 피해상황 파악
- 침해 사고로 판단 할 수 있는 근거
  - 악성파일 발견, 홈페이지 변조, 고객의 피해신고, 시스템/네트워크 이상현상 <증거의 무결성 훼손 주의>

웹 침해사고 분석 절차 – 사고 조사

- 사고 조사자가 본격적으로 투입되어 사고의 범위를 구분, 증거자료 수집, 분석하는 가장 핵심적인 단계

- 효율적인 사고 분석, 사고 조사 계획 수립 위해 필요한 정보 및 자원을 수집하여 사고 조사 범위를 한정

- 불만족스러운 결과 도출 시 조사 범위 확대 및 증거 자료를 확대하여 추가적인 조사를 실시

웹 침해사고 분석 절차 – 보고서 작성

- 사고 조사 단계의 마지막 단계
- 모든 과정, 분석 결과를 문서화
- 보고서 내용은 육하원칙을 기본으로 시간과 증거를 바탕으로 객관적으로 기술

조사 범위 규정

- 조사에서 가장 먼저 이루어져야 하는 중요한 단계
- 사고 발생시 일반적으로 자원, 시간 등의 제약사항이 존재
- 정확한 사고 조사 범위 선정 위해
  - 조사자의 경험, 사고와 관련하여 수집된 다양한 정보 필요
  - 다음과 같은 자원을 이용

조사 범위 규정 – 초기 대응에서 수집된 정보

- 사고의 인지 시점, 피해 현상, 이와 관련 초기 대응을 어떤 식으로 실시했는지 알 수 있는 자료

- 이를 바탕으로 사고 조사자는 사고의 성격, 피해 정도, 필요한 정보/증거 자료 파악

조사 범위 규정 – 네트워크 구성도

- 사고 조사에 있어서 필수적 정보

- 네트워크 관련 시스템의 물리적 위치, 연계되어 있는 시스템 파악하여 피해 규모와 침입 경로, 침입 시나리오 등 파악

조사 범위 규정 – 정보시스템 관리자/개발자와의 인터뷰

- 사고 조사에 있어 매우 좋은 협력자가 될 수 있는 반면 사고의 성격에 따라 조사 대상이 될 수 있으므로 인터뷰 시 정보의 수집, 공유에 주의

- 보고서에 실리지 않은 내용이나 궁금 사항에 대해 정보 수집 가능, 사고 조사의 시간을 단축 시켜줌

조사 범위 규정 – 정보시스템 관리자/개발자와의 인터뷰

- 정보 수집 완료 후 조사 범위 한정 짓고 공격자가 침해를 한 경로에 대한 시나리오 세울 수 있음

- 시스템에 대한 접근 경로가 나열된 후에는 해당 시나리오에 대해 기술의 난이도/발생 가능성에 따라 우선순위 정함

증거 자료 수집

- 사고 조사 범위에 포함되는 정보시스템에서 증거 자료를 수집하는 단계

- 분석에 포함되는 장비
  - 방화벽, IDS/IPS 등 보안 장비, WS(Web Server)/ WAS(Web Application Server)/ DBMS(Database Management System)

구분	설명
설정 파일	방화벽 정책과, WS, WAS, DBMS등 사고 당시 설정 파일
상태 정보	시스템의 네트워크 상태 정보, OS정보, WS, WAS, DBMS정보
시스템 로그	MS Windows의 이벤트, Unix/Linux 운영체제의 로그파일(WS, WAS, DBMS 등)
웹 트래픽 로그	IDS/IPS등 보안장비 로그, WS, WAS, DBMS의 로그파일
파일	사고 당시 웹 애플리케이션 파일, 발견된 백도어 파일 등
메모리 덤프	사고 시스템의 메모리 덤프(공격의 유형에 따라 공격자는 파일이 아닌 메모리 상주 형태의 백도어를 숨겨둘 수 있다.)

증거 자료 수집

- 웹 침해사고 분석 정식 절차는 네트워크 차단 후 휘발성 데이터 수집, 디스크 이미징을 통한 증거자료 수집

- 로그 파일, 웹 애플리케이션 파일만으로 조사하는 경우도 있음

- 운영 중 시스템에서 수집할 경우 사고 시스템의 증거자료 훼손 주의, **CMA** 시간 훼손 막기 위해서는 화면 스크린샷을 미리 찍어 증거를 확보

증거 자료 분석

- 수집된 증거 자료를 분석하는 단계
- 전문적 조사자의 지식, 경험 요구
- 증거자료를 기반으로 분석
- 해당 행위로 인해 초래되는 피해 규모 파악하는 과정

증거 자료 분석 – 침해 행위 분석

- 수집한 설정, 로그파일, 메모리 덤프 등 대상으로 침해 행위를 찾아 내는 일련의 과정

- 초기 대응에서 수집한 정보를 신뢰하기 보다는 참고용으로만 이용하고 직접적으로 확인하는 것이 중요

증거 자료 분석 – 침해 행위 분석

- 네트워크 분석
  - 방화벽 설정, 네트워크 구성, 조사 대상 시스템의 네트워크 설정, 운영체제 정보, WS/WAS/DMBS 정보 등 바탕으로 사고 발생 시점의 현황을 파악

- 시스템 분석
  - 조사 시스템의 운영체제와 어떤 서비스를 기반으로 웹 서비스, 연동 서비스 운영 중인지 파악 및 파악된 운영체제/ 서버의 종류에 따라 최근 발표된 취약점 정보 유무 파악

증거 자료 분석 – 침해 행위 분석

- 웹 애플리케이션 분석
  - 조사 대상 서비스가 작성된 프로그래밍 언어, 알려진 웹 애플리케이션을 사용하는지 자체 개발 웹 애플리케이션을 사용하는지 파악
  - 알려진 웹 애플리케이션일 경우 알려진 취약점 유무 조사
  - 웹 애플리케이션의 기능, 구현 등을 파악하여 악용 가능한 기능이나 취약 부분 존재 유무 파악

증거 자료 분석 – 침해 행위 분석

- 로그 파일 분석
  - 웹 서비스 활용도 높을수록 디스크 공간의 문제로 인해 로그파일이 존재하지 않거나, 양이 너무 방대하여 분석에 어려움
  - 최근 POST 메소드 방식으로 공격하므로 파일분석에 어려움
  - 수작업으로 로그분석 시
    - 공격에 사용되는 특정 문자열이나 공격에 악용 되었을 것으로 추정되는 애플리케이션의 요청을 추적

증거 자료 분석 – 침해 행위 분석

- 로그 파일 분석
  - 초기단계에서 악성코드 발견 되었을 경우 로그 파일에서 해당 파일명을 문자열로 하여 공격에 가담한 IP들을 찾아낼 수 있음
    - 도출된 IP를 대상으로 접속한 일자를 추적하여 최초 공격 시점 및 악성코드 업로드 된 시점 파악
    - 시간적 흐름에 따라 분석함으로 공격자의 행동패턴 분석
    - 공격자의 시스템 파악 가능

증거 자료 분석 – 침해 행위 분석

- 악성 파일 분석
  - 공격자가 가장 먼저 서버측에 업로드하는 악성파일은 웹 애플리케이션 형태의 백도어
  - 웹 로그 분석 또는 웹 디렉터리를 조사하여 백도어 탐색 및 기능, 실행내역 파악
  - 웹 침해사고에서 일반적으로 사용되는 악성파일은 웹쉘(WebShell)
    - 서버를 운영하는 시스템의 계정 권한 획득, 정보 획득이 주목적
  - 악성파일이 제공하는 기능
    - 시스템 명령어 실행, 임의파일 업/다운로드, DB클라이언트, 시스템 정보 확인, 파일 및 디렉터리 조작(수정/삭제/생성)
    - 레지스트리 조작, 익스플로잇 실행, 네트워크 포트 스캐닝, 리버스 커넥션(Reverse Connection, 침해 서버에서 공격자의 PC로 접속을 시도)

증거 자료 분석 – 침해 행위 분석

- 악성 파일 분석
  - 백 도어 탐지 방법 : 파일 목록 검사 / 파일 내부 패턴 검사
    - 파일 목록 검사
      - 파일의 생성시간, 변경일자 등 확인
      - 업로드 디렉터리 등 위치에 비정상적으로 존재하는 웹 실행 파일 확인 하여 백도어 탐색
    - 파일 내부 패턴 검사
      - 소스 파일에서 웹 백도어에서 자주 사용되는 주요 함수와 이미 알려진 웹 백도어의 패턴 검사
      - 시스템 수준의 백도어 : 백신, Chkrootkot, Tripwire등 도구로 탐색

개발언어	일반적 패턴
PHP	•명령어 실행 위해 passthru(), system() 등 함수 사용 •패턴 매칭 우회 위해 eval(), base64_decode() 등 함수 사용
ASP	•명령어 실행 위해 Wscript.Shell, Shell.Application 객체 사용 •패턴 매칭 우회 위한 코딩 수행 (VBScript.Encode)
JSP	•명령어 실행 위해 Runtime.getRuntime 객체 사용 •패턴 매칭 우회 위해 JavaScript 이용 문자열 치환, 분할

증거 자료 분석 – 피해 규모 파악

- 공격자가 어느 정도 까지 권한을 획득 했으며, 어떤 정보에 접근했는지 알아내는 것이 침해사고 분석의 핵심

- 피해를 정확하게 파악하기 위해서
  - 로그 파일 분석, 악성 파일 분석 통해 공격자의 행위를 시간 순으로 파악
  - 공격자가 시스템 권한 또는 관리자 권한 획득 여부 파악
  - 내수 시스템으로 침투 여부 파악
  - 획득한 권한으로 접근한 정보 파악

Q & A