한국인터넷진흥원 침해사고 분석 절차 안내서

챕터 3. 침해사고 분석 기술

BoB7기 취약점분석 정성조

# 윈도우 사고분석

윈도우 사고분석에 있어 포렌식 측면에서 봤을 때 피해시스템에 영향을 주지 않고 필요한 정보를 얻어야 한다.

# 초기 분석

정확한 분석을 위해서는 휘발성 증거를 반드시 수집해야 한다.

* 시스템 시간 확인: 시간을 동기화시키고 date /T, time /T, uptime(부팅 시간) 명령어를 사용하여 시간을 확인한다.
* 시스템 정보: psinfo -h -s (설치된 핫픽스 및 소프트웨어 목록 정보) 명령어를 사용하여 시스템 정보를 확인한다.
* 프로세스 정보 확인: 실행 프로세스명, 프로세스 실행파일 위치, 커맨드 라인, 실행시간, 참조중인 DLL 및 파일 -> pslit 명령어를 통해 점검할 수 있다. ( 시스템 DLL, 자체 제작 DLL에 대한 자세한 점검이 필요함. listdlls는 DLL 정보를 상세하게 보여준다. ), 프로세스가 어떤 파일을 참조하는가에 대한 정보는 handle 프로그램을 이용하여 확인할 수 있다.
* 네트워크 정보 확인: netstat -an 명령어로 프로토콜 상태, IP 기반 네트워크 연결 정보, 포트를 확인할 수 있다. (ipconfig /all, netstat -an, fport, promiscdetect)
* 사용자/그룹 확인: net user(시스템에 존재하는 계정 정보 출력), net localgroup (시스템에 존재하는 그룹정보 출력)
* 공유, 로그인 정보 확인: net share(시스템 공유 정보 출력), net session(공유 자원에 접속한 컴퓨터 정보 출력), nbtstat -c(NBT에 연결된 세션 정보 출력), ntlast -f(원격접속 로그 정보 출력)

스크립트를 사용하여 로그 분석을 자동화하여 신속한 로그 수집이 필요하다.

* 자동화 도구: WFT(Windows Forensic Toolchest); 수집된 정보를 브라우저로 확인할 수 있음.

# 루트킷 점검

루트킷(RootKit): 악성 코드가 시스템에 탐지되는 것을 막는 도구

* 루트킷 기능: 사용자 모드와 커널 모드의 루트킷으로 구분된다. (사용자 모드: 특정 프로세스에 사용한 DLL 파일 교체, IAT 후킹 등), (커널 모드: 윈도우 Native API(ntdll.dll, Kernel32.dll, User32.dll 등)의 커널 드라이브와 Win32 응용 프로그램 조작)
* 루트킷 종류: Hacker Defender, FU, Vanquish, AFX rootkit, NT Rootkit
* 루트킷 탐지: 루트킷 탐지 프로그램 종류 및 기능 분석 표 이용, IceSword 도구 이용

# 상세분석

* 레지스트리 분석: 윈도우 레지스트리를 통해 설치된 소프트웨어 정보, 환결 설정, 임시 저장값 등을 분석할 수 있다.
* 시작 프로그램 레지스트리 분석(악성 프로그램 자동 실행 방지)
* 자동실행 점검: 내용이 비어 있는 서비스, 영문인 서비스, 이름이 다른 서비스, 경로가 다른 서비스 점검, Autoruns를 이용한 스케줄링 점검, 자동시작 폴더 점검,
* Winlogon Notification DLL – 이벤트 핸들러 코드를 작성하여 자동 실행하는 악성코드 작성 가능 – Autoruns의 Winlogon 기능을 통해 점검 가능
* 이벤트 로그분석: eventvwr.msc를 통한 이벤트 로그 확인
* MAC time 분석 (M:mtime(파일을 생성 및 최근 수정한 시간), A:atime(최근 파일을 읽거나 실행시킨 시간), C:ctime(파일 속성이 변경된 시간)) – 시간을 분석하여 악성코드가 실행한 파일, 생성한 파일 등을 분석해야 함.
* 침임 방법 분석(윈도우 취약점, 웹 어플리케이션 취약점, MS-SQL 취약점)
* 웹 서비스가 구동 중이었다면 로그 분석을 통해 공격 여부 및 방법을 확인할 수 있음. IIS Log(C:\WINNT\system32\LogFiles\W3SVCI)
* MBSA(Microsoft Baseline Security Analyzer) -> 보안 패치 상태, IIS, SQL 보안 상태 점검 가능
* 인터넷 임시파일 분석: 쿠키, 열어본 페이지, 임시 인터넷 파일, 객체 분석 -> indexview를 통해 확인할 수 있음.

# 해킹 프로그램 분석

* 분석환경 구성: 최소 2개 이상의 가상 서버 구동
* Snapshot 기능을 활용하여 리눅스(서비스 제공), 윈도우(피해 대상) 두 서버를 구축한다.
* 분석 방법: SysAnalyzer 도구 사용 -> 지정된 시간에 걸쳐 Snapshot을 비교할 수 있음 -> 실행 프로세스, 포트, 실행 DLL, 커널에 로드된 모듈, 변경/생성된 레지스트리 키 확인 가능
* 분석 방법:Malcode Analysis Pack -> fakeDNS: 외부망 차단, 내부망을 통해 악성코드 분석 가능, MailPot: 대량으로 발생되는 스팸 메일 확인 가능
* 모니터링 프로그램 활용

# 리눅스 사고 분석

사고 빈도는 낮아졌지만 리눅스 활용도는 낮아지지 않았음.

# 기본 정보 수집

* OS 종류, 커널 버전, 용도, 운영 중인 서비스, 네트워크 현황, 보안 패치 적용 현황, 보안 장비 운영 현황

# 휘발성 정보 수집

* 프로세스 확인: ps -ef, lsof(List Open File): 오픈된 파일 리스트 확인
* netstat -an: 포트 열림 상태, 수신지, 발신지 확인
* nmap -sT -p 1-65535: 1부터 65535번 포트까지 스텔스 스캔
* fuser: 현재 사용 중인 파일 또는 소켓이 사용하는 프로세스 확인
* who: 접속 중인 사용자 정보 확인

# 상세 분석

* /etc/paswd에서 uid=0 (root id) 확인
* utmp, wtmp: 현재, 과거에 로그인 했던 사용자 정보 로그
* messages: 명령어 로그
* access\_log: 웹 로그
* rpm -V fileutils: 명령어 무결성 검사
* strace -e trace=open (명령어): 변조된 파일의 위치, 명령의 변조 유무 확인
* find 명령을 통한 setuid, 숨김 파일 등 확인

# 네트워크 사고 분석

* 불법적인 자원 사용(호스트: 액세스 등, 네트워크: 회선 상태 등의 로그 확인)
* DoS: 패킷 로그 주로 확인
* 데이터 손상 및 변조: 액세스 로그, 패킷 로그 확인
* 정보 누설: 액세스 로그, 저장 장치 상태, 포트 로그 확인

# 프로토콜 개요

# IP 헤더

* Flag (0: 일반적, 1: 0이면 조각, 1이면 조각 허용 X, 2: 0이면 마지막 조각, 1이면 마지막이 아님)
* TTL: 전송 과정에서 통과할 수 있는 라우터의 개수
* Protocol: ICMP (1), TCP (6), UDP (17)

# TCP 헤더

* Source Port: 보내는 사람의 포트
* Destination Port 받는 사람의 포트
* Sequence Number: TCP 세그먼트 번호
* Acknowledgement Number: 받아야 하는 세그먼트 번호
* Control Bits: 패킷의 용도 표시

# 패킷 수집 및 디코드

* 공격의 종류에 따라 방화벽의 앞과 뒤, 네트워크 전체의 패킷을 수집한다.
* 버퍼나 파일로 저장하고, 크기는 24~32 MB로 설정하는 것이 좋다.
* MAC, IP, TCP/UDP 주소별 트래픽 통계를 관찰한다.
* 프로토콜 분석기를 통해 패킷을 디코드하여 분석한다. (ex) wireshark, fiddler,)

# 공격형 트래픽의 특징

* 특정 서버만을 공격
* 패킷 과부하 공격

# 데이터베이스 사고 분석

* MY-SQL, MS-SQL, Informix, Mongo DB, Maria DB 등

# MY-SQL( == MariaDB)

* 관리자 아이디가 기본 아이디인가?
* mysql -uroot -p: 루트로 mysql에 접속
* mysql -uadmin -p: 어드민으로 mysql에 접속
* 패스워드가 없는 계정이 존재하는가?
* select user, password from user; 유저이름, 패스워드 추출
* UPDATE user SET password=password(‘new-password’): 패스워드 설정
* WHERE user = ‘user\_name’;
* flush privileges;
* SET PASSWORD for user\_name=password(‘new\_pasword’)
* u username password new-password