Active Directory를 이용한 PC 감사 및 포렌식

이유빈*, 이성원**, 조태남***
*우석대학교 정보보안학과
**(주)아이제론
***우석대학교 IT전자융합공학과
e-mail : lyb2696@gmail.com*, forensic@izerone.co.kr**, tncho@ws.ac.kr***

PC Audit and Forensics using Active Directory

Yu-Bin Lee*, Seong-Won Lee**, Taenam Cho***
*Dept. of Information Security, Woosuk University
**Ltd. Izerone
***Dept. of IT and Electronics Engineering, Woosuk University

요 약

Active Directory(AD)는 윈도우즈 환경 하에서 LDAP 디렉터리 서비스나 Keberos 기반의 컴퓨터 인증 등을 제공한다. 본 논문에서는 AD의 감사 기능을 이용하여 여러 컴퓨터들을 하나의 서버에서 로그를 관리하고 감사할 수 있는 2가지 방안을 제시한다. 이러한 로그를 이용하여 특정 컴퓨터에 대한 디지털 포렌식에 활용할 수 있을 것이다.

1. 서론

디지털 포렌식은 각종 사건의 경위를 조사하고 증거를 포착하는 기술로서 활용되고 있다. 본 논문에서는 PC를 통하여 이루어질 수 있는 각종 불법적 파일의 공유와 삭제 등을 효율적으로 감사하고 추적할 수 있는 방법에 대해 연구하였다. 윈도우즈에서 제공하는 Active Directory와 감사기능을 사용하여 서버가 여러 컴퓨터들의 로그를 백업하고 필요시 이를 활용하여 불법적 행위를 추적할 수 있는 방법을 제시하고 실험하였다. 첫 번째는 실시간 모니터링 방법이며 두 번째는 관심 대상인 주요 이벤트들만 선별적으로 서버에 자동으로 보고하는 방법이다.

2. 시스템 구성

시스템은 1대의 Active Directory 서버와[1] 1대의 클라이언트로 구성하였다. 여러 대의 클라이언트를 하나의 서버에 연결할 수 있지만, 본 연구에서는 간략한 기능 테스트를 위하여 1대의 클라이언트만 사용하였다. 서버에는 Windows Server 2016을 설치하였으며, 클라이언트 PC에는 Windows 10 Pro를 설치하였다.

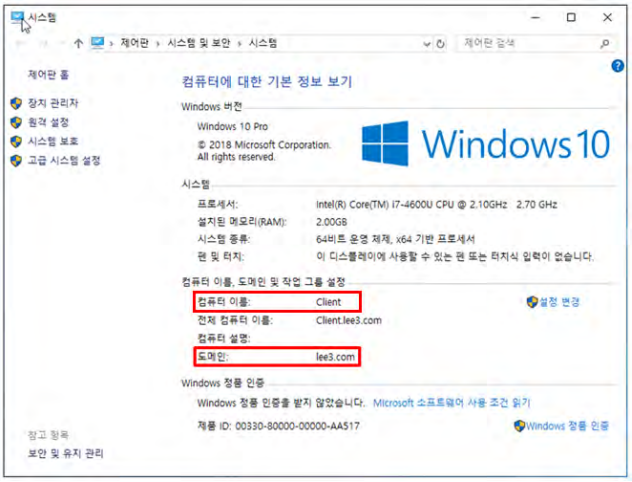
3. 실시간 모니터링

3.1 실험 환경 설정

이 방법은 서버에서 실시간으로 클라이언트의 로그를 열람할 수 있도록 하는 방법이다. 클라이언트의 Test 폴더나 하위폴더 및 파일 접근에 대한 읽기/쓰기/사제 로그를 열람할 수 있도록 실험할 것이다. 이를 위한 서버와 클라이언트를 설정방법은 다음과 같다.

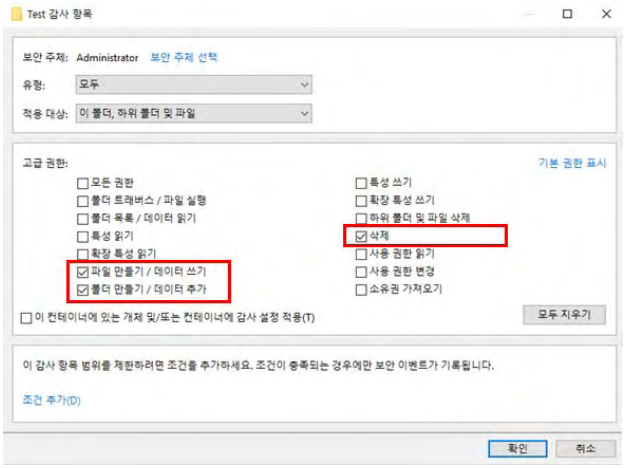
(1) 클라이언트

① 서버에 설치된 AD 도메인 서비스에 가입한다. (그림 1)과 같이 본 실험에서의 서비스 도메인은 “lee3.com”이며, 클라이언트의 이름은 “client”이다.



(그림 1) 클리이언트의 AD 가입

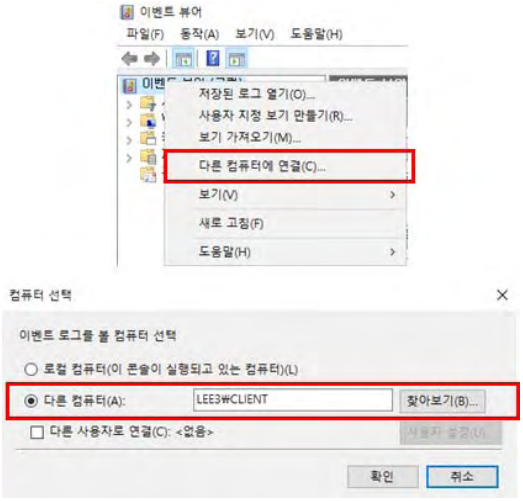
② Test 폴더를 생성하여 감사 설정 추가한다[2]. 본 실험에서는 (그림 2)와 같이 “삭제”, “파일만들기/데이터쓰기”, “폴더만들기/데이터추가”를 감사 대상으로 설정하였다.



(그림 2) Test 폴더에 대한 감사 설정

(2) 서버

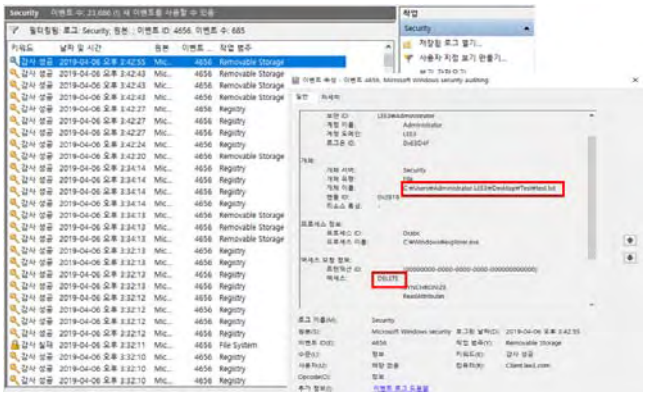
이벤트 로그를 실행하고 (그림 3)과 같이 이벤트 뷰어에서 “다른 컴퓨터에 연결”에서 클라이언트 “client”를 선택한다.



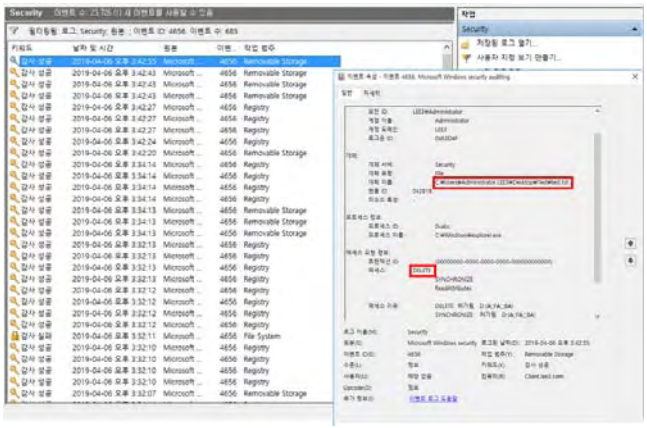
(그림 3) 클라이언트 등록

3.2 실험 결과

클라이언트에 생성한 Test 폴더 안에 폴더 또는 파일을 생성, 수정, 삭제하여 로그를 발생시켰다. (그림 4)는 이벤트 id가 4656(감사 대상으로 설정한 객체에 대한 접근 이벤트)인[3] 이벤트 로그를 검색한 화면이며, 특히 한 예로서 “test.txt”를 삭제한 이벤트에 대한 로그를 보여주고 있다. (그림 5)와 같이 서버에서 검색한 로그로서 클라이언트와 동일한 것을 볼 수 있으며 Test 폴더에 있는 “test.txt” 파일을 삭제한 로그도 동일함을 확인할 수 있다.



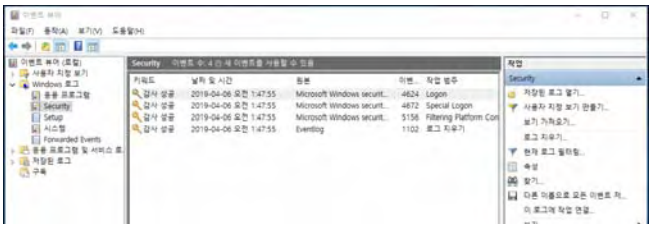
(그림 4) id=4656에 대한 클라이언트 로그



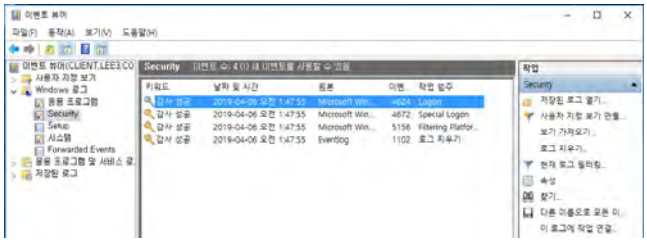
(그림 5) id=4656에 대한 서버 로그

3.3 제한 사항

이 방법은 서버에서 실시간으로 클라이언트의 로그를 모니터링하는 방법으로서 서버에 로그가 백업되지는 않는다. 따라서 PC가 켜져 있고 온라인으로 연결되어 있어야 하며, (그림 6)과 같이 클라이언트에서 로그를 삭제하면 (그림 7)과 같이 서버에서도 삭제한 로그를 볼 수 없다는 것이다. 또한 이 기능을 위해서는 클라이언트의 방화벽을 중지시켜야 한다는 보안상의 제약점을 안고 있다.



(그림 6) 로그가 삭제된 클라이언트 화면



(그림 7) 로그가 삭제된 서버 화면

4. 주요 이벤트 백업

4.1 시스템 설정

이 방법에서는 실시간 모니터링 방법의 제한점을 보완하여 감사대상이 되는 이벤트가 발생하면 해당 이벤트만 서버로 전송하여 서버에 저장함으로써, 오프라인 검색이 가능하며 클라이언트에서 삭제하더라도 서버에서 확인이 가능하도록 하는 방법이다.

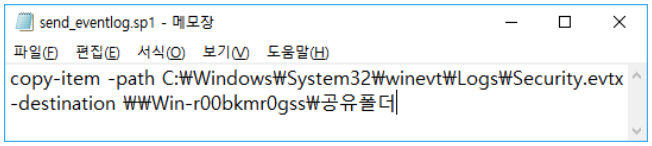
(1) 서버

백업하고자 하는 로그를 저장할 공유폴더를 생성한다. 본 실험에서는 "\Win-r00bkmr0gss\공유폴더"이다.

(2) 클라이언트

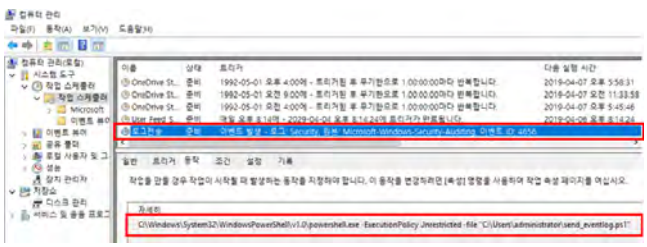
① 실시간 모니터링 방법에서 (그림 2)와 같이 감사 항목을 설정하여 저장한다.

② 클라이언트에서는 "copy-item" 명령어를 사용하여 서버로 보낼 로그인 "Security.evtx"를 서버의 공유폴더로 전송하도록 쉘 프로그램을 작성한다. 본 실험에서는 (그림 8)과 같이 send_eventlog.sp1으로 저장하였다.



(그림 8) 서버로 로그를 전송하는 쉘 프로그램

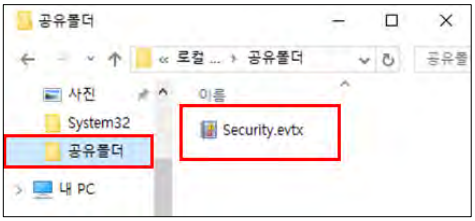
③ (그림 9)와 같이 id가 4656인 이벤트가 발생하면 Powershell.exe를 작동시켜서 send_eventlog.sp1을 수행하도록 스케줄러를 작성하여 등록한다.



(그림 9) 스케줄러 등록

4.2 실험 결과

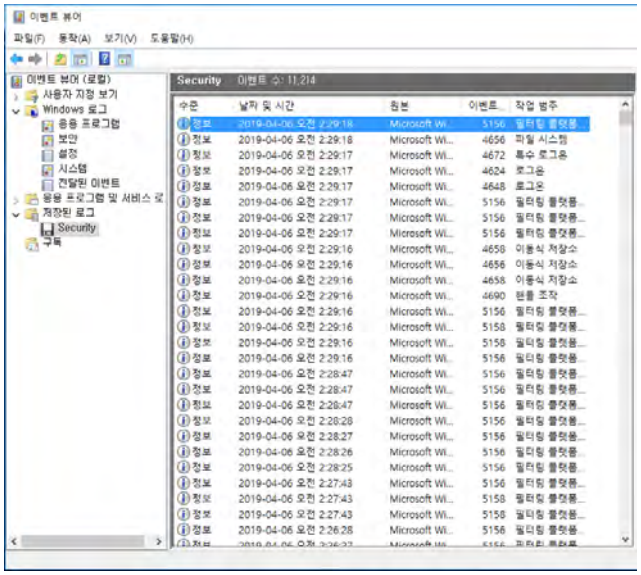
실시간 모니터링에서와 같이 클라이언트에서 Test 폴더에 파일을 생성/삭제 등으로 접근하였을 때, (그림 9)와 같이 서버로 전송되어 설정된 공유폴더에 Security.evtx가 저장되는 것을 확인할 수 있다.



(그림 10) 서버에 저장된 Security 이벤트 로그

이 방법에서는 실시간 모니터링 방법과 달리 서버에 로그의 백업본이 저장되기 때문에, (그림 11)과 같이 클라이언트에서 로그를 삭제하더라도 (그림 12)와 같이 서버에서는 저장된 로그를 통하여 열람할 수 있다. 또한 클라이언트가 온라인 상태가 아닐 경우에도 열람이 가능하다.

(그림 11) 클라이언트에서 로그 삭제한 화면



(그림 12) 서버에서 확인한 로그

4.3 제한 사항

실시간 모니터링 방법의 제한점을 해결하기는 하였으

나, 이 방법에서도 개선해야할 제한사항이 존재한다. 첫째, 이 실험의 목적은 클라이언트에서 발생한 로그가 실수나 고의에 의해 삭제되는 경우에도 서버에서 이를 감사하고 디지털 포렌식을 수행할 수 있도록 하기 위한 것이다. 그런데 서버로 로그를 보내는 쉘 프로그램이 클라이언트에서 동작하기 때문에 악의적인 클라이언트에 의해 조작될 수 있다. 둘째, 서버로 보내는 로그가 동일한 이름으로 저장되기 때문에 이전 로그에 덮어쓰기가 된다는 점이다.

5. 결론 및 향후 연구

본 연구에서는 마이크로소프트에서 클라이언트들의 디렉터리 서비스나 인증을 위해 제공하는 Active Directory를 이용하여, 클라이언트의 주요 이벤트를 감사하고 로그를 백업하여 실수나 악의적으로 클라이언트의 로그가 삭제되더라도 추적할 수 있는 방법을 연구하였다.

향후에는 4.3에서 기술한 제한 사항을 보완하기 위한 방법을 연구할 것이다. 즉, 쉘 프로그램을 클라이언트가 아니라 서버에서 구동되도록 하여, 클라이언트가 악의적으로 조작하지 못하도록 하는 방법을 연구한다. 또한 지속적인 로그 전송으로 덮어쓰기가 되지 않도록 기존 로그에 추가하도록 하거나, 파일명을 달리하면서 구분될 수 있도록 하며, 백업의 기간 설정 등에 대해 연구할 예정이다.

ACKNOWLEDGMENT

본 연구는 한국연구재단의 연구 지원 (NRF-2017R1D1A3B03032637)에 의한 것입니다.

6. 참고 문헌

[1] Jordan Krause (김도균 역), "Windows Server 2016 쿡북", 에이콘, 2018.

[2] 파일 또는 폴더에 기본 감사 정책 적용, https://docs.microsoft.com/ko-kr/windows/security/threat-protection/auditing/apply-a-basic-audit-policy-on-a-file-or-folder, MicroSoft.

[3] Windows 8 and Windows Server 2012 Security Event Details, https://www.microsoft.com/en-us/download/confirmation.aspx?id=35753, Microsoft.