**[포렌식을 위한 네트워크 패킷**

**분석 및 데이터 복원]**

**(제안서)**

2016년 03월

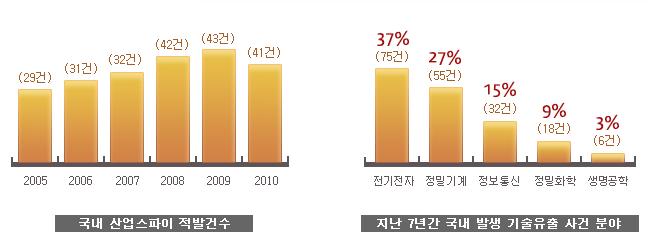
호서대학교 공과대학 정보보호학과

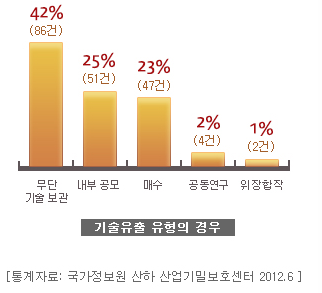
|  |  |  |
| --- | --- | --- |
| **제 출 문** | | |
| **과 제 명** | 포렌식을 위한 네트워크 패킷  분석 및 데이터 복원 | |
| **참여학생** | 학 번 | 성 명 |
| 20111748 | 위푸름 |
| 20123381 | 유진영 |
| 20122343 | 김수진 |
|  |  |
| **수행기간** | 2016.03.01 ~ 2016.00.00 | |
| 본 보고서를 호서대학교 정보보호학과  정보보호 프로젝트 제안서로 제출합니다.    2016년 3월 14일  **호서대학교 정보보호학과 학과장 귀하** | | |

프로젝트의 필요성

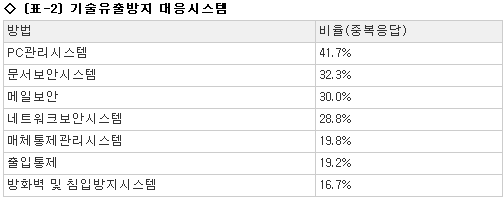
21세기에 접어들면서 국내를 비롯한 해외에서 인터넷기술의 급속한 발달로 인하여 업무, 교육, 의료 등 다양한 부분에서 온라인을 이용한 업무처리 형태로 진화해왔다. 하지만 기술이 발전되면서 편리함이 증가한 만큼 해당 기술을 악용하는 무리들도 나타나기 시작하면서 서로의 이윤을 목적으로 공격하는 부류와 막는 부류로 하나의 전장이 되어버렸다. 특히 근래에 들어서는 디지털 포렌식(Digital Forensic)이라는 분야가 나옴으로써 디지털상의 자료(메시지 내용, 이메일, 로그 등)들도 법정에서 증거로 효력이 입증되면서부터 국가적인 차원에서 해당 분야에 대한 관심이 증가 하고 있다.

****특히 최근 국내외에서 기업내부의 기밀정보를 유출하는 경우가 빈번하게 발생하고 있다. 유출사항으로는 아래의 [표-1]와 같이 데이터 유출 다음으로 이메일 및 메신저를 통한 유출이 많음을 확인할 수 있다. 이러한 유출은 기업의 막대한 손실을 불러오며 나아가 핵심기술의 경우에는 국가적 손실까지 불러올 수 있는 위험성이 존재한다.



하지만 현실은 기업의 담당자는 물론 일반 직원들은 보안에 대한 인식이 저조할 뿐 아니라 중소기업의 경우 교육이 기업내의 보안교육이 제대로 이루어지지 않은 경우가 대부분이며 이에 지속적으로 문제점이 발생하였다. 기업들의 유출방지 대응방안으로는 아래 [표-2]와 같이 가장 많이 적용된 시스템도 50%가 넘지 않는 상태이며, 그 중에서도 메일 보안 및 네트워크보안시스템의 경우는 저조한 상태를 보여주고 있다.

그러나 기술유출방지를 위해 인프라가 구축이 되어있고, 각종 보안프로그램이 설치되어 있어도 많은 사내규정과 승인절차에 사용자가 불편함을 느껴 설치하였다가 삭제하거나 설치하지 않는 경우도 없지 않다. 또한 기업의 기밀을 빼돌리는 경쟁사의 산업스파이의 경우 사내 기밀문서를 유출할 확률도 높으며, 이에 대한 대처가 필요하다.

****

프로젝트 목표 및 내용

프로젝트의 추진 전략 및 방법

1) 개발 환경

OS: window 10

사용 언어: python, c, css, javascript, html

사용 프로그램: VMware, github, sourceinsight, sublime text

2) 역할 분담

|  |  |
| --- | --- |
| 위푸름 | UI·UX 디자인 및 PPT제작, front-end 개발 |
| 유진영 | Back-end 개발 |
| 김수진 | front-end 개발 |

3) 세부 일정

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 자료조사 | All | 3/2 | 3 | 3/4 |
| 제안서 작성 | All | 3/5 | 7 | 3/11 |
| 제안서 PPT 작성 | 위푸름 | 3/11 | 3 | 3/13 |
| 제안서 발표 | 김수진 | 3/14 | 1 | 3/14 |
| 기존 프로그램 분석 | 유진영 | 3/16 | 3 | 3/18 |
| 모듈 별 프로그램 설계 | 유진영 | 3/19 | 4 | 3/22 |
| 모듈 별 기술조사 | 유진영 | 3/23 | 4 | 3/26 |
| Front-end 기술 조사 | 김수진, 위푸름 | 3/16 | 7 | 3/22 |
| Front-end UI 디자인 | 위푸름 | 3/23 | 3 | 3/25 |
| Front-end UX 디자인 | 위푸름 | 3/26 | 3 | 3/28 |
| 핵심 모듈 개발 | 유진영 | 3/27 | 14 | 4/11 |
| Front-end 개발 | 김수진, 위푸름 | 3/23 | 21 | 4/12 |
| Front-end 1차 테스트 | All | 4/13 | 8 | 4/20 |
| Back-end 1차 테스트 | All | 4/13 | 8 | 4/20 |
| 중간 PPT 작성 | 위푸름 | 4/21 | 4 | 4/24 |
| 중간 발표 | 위푸름 | 4/25 | 1 | 4/25 |
| 검토 및 개선 | All | 4/26 | 5 | 4/30 |
| Front/Back-end 연동 | All | 5/1 | 2 | 5/2 |
| 프로젝트 2차 테스트 | All | 5/3 | 10 | 5/12 |
| 통합 테스트 | All | 5/13 | 22 | 6/3 |
| 최종 보고서 작성 | All | 6/4 | 7 | 6/10 |
| 최종 PPT 작성 | 위푸름 | 6/9 | 4 | 6/12 |
| 최종 발표 | 유진영 | 6/13 | 1 | 6/13 |

프로젝트 결과의 활용 방안 및 기대효과

회사 안에서 사용하는 전자통신 수단이 다양해지고, 스마트폰 · 소셜 네트워크 서비스(SNS) ·

웹하드 사용의 증가에 따라 기업 기밀유출 가능성이 높아지므로 기업 감사에도 보다 높은 기술이 요구되고 있다. 기업의 보안담당자 혹은 감사원은 의심되는 이용자에 대한 색출과 이용자가 한 행위(파일 전송, 메일전송 등)를 파악하기 위하여 기업 내에 있는 보안관제부서에 해당 이용자의 행위에 대한 네트워크 패킷을 요구하여 분석을 실시할 수 있다.

따라서 회사 내규 등에 임직원 프라이버시 침해가 아닌 기업 리스크 관리를 위한 모니터링의 취지를 명확히 밝히고 임직원 동의서를 받은 후 네트워크 패킷 분석을 통한 모니터링으로 비정상 네트워크 트래픽 탐지, 인터넷 사용내역, 접근 사이트 내용, 이메일 수신 및 발신 기록 등 다양한 분야에서 내부통제 강화 용도로 활용 된다.

IPS와 방화벽의 경우 보통 시그니쳐 기반으로 탐지하여 공격의 유무 판단을 위주로 수행을 한다면 본 프로젝트의 프로그램은 그 행위에 대하여 더 나아가 패킷 심층분석을 통해 외부로 빠져나가는 파일에 대한 실질적인 정보습득과 복원을 수행한다. 이러한 과정에서 유출된 문서의 최종 목적지 추적 및 파일 복원을 통한 해당 유출자에 대한 징계 근거자료로 제출될 수 있다.

네트워크 패킷 분석을 통한 데이터 복원 기술은 패킷들을 파일 및 프로토콜 정보를 이용하여 원래의 파일의 형태로 복원하기 위한 기술이다. 이 기술을 이용하여 프로토콜의 트래픽을 분석할 수 있으며, 파일이 아닌 다양한 제어 패킷들도 수집/복원되고, 이런 정보들을 통해서 비인가 사설 FTP서버 접속 탐지, 특정 프로토콜을 이용한 비인가 서비스 이용 탐지 등과 같은 보안사고를 예방할 수 있다.