학내망 보안을 위한 정보보호 동아리의 역할과 사고대응에 관한 연구

황현욱*, 주필환*, 이재서*, 김민수*, 노봉남*

*전남대학교 정보보호협동, 정보보호119

A Study on University Information Security Club's Role and Incidence Response for Campus Security

Hyun-Uk Hwang*, Pill-Hwan Chu*, Jae-Seo Lee*, Min-Soo Kim*, Bong-Nam Noh*

*Information-Security119, Department of Information Security, Chonnam Univ.

요 약

최근 해커들의 수많은 공격의 근원지가 되고 있는 학내망의 보안은 많은 대학에 정보보호 관련 동아리가 활동하고 있음에도 불구하고 건전한 방향으로 활성화가 되지 못하고 있는 현실이다. 동아리의 효율적인 운영과 학내망 해킹사고 예방을 위해 정보보호 동아리 사고대응팀의 운영과 정보보호 활동은 필수적으로 요구된다. 본 논문에서는 침해사고 예방과 사고대응을 위해 전남대학교 학내망에서 정보보호 동아리인 정보보호119의 역할과 동아리 운영 방안모델을 제시하고, 학내망 침해사고 예방을 위해 학내망 중앙관리 침입탐지 시스템과 자동화 된 원격모의해킹시스템을 구현하였다.

Ⅰ. 서론

해킹 사고는 하루가 다르게 급속히 증가하고 있다[1]. 오늘 하루에도 학교의 수천대의 서버는 외부의 공격에 모두 노출되어 관리자도 알지 못한 채 크래커의 장난감이 되고, 또 다른 범죄도구의 하나가 되어 다른 서버를 공격하는데 이용되고 있다. 공격의 무분별한 난입의 큰 시발점을 교육망이 제공하고 있으며, 특히 다양한 종류의 OS와 수많은 서버를 제공하는 대학의 학내망은 외국의 크래커들의 즐거움을 증가시키고 있다.

하루가 다르게 발전하는 해킹기술은 조직의 규모나 목적에 상관없이 사고대응을 하기 위한 전담조직이나 인력을 요구하고 있다. 특히 다양한 구성원들이 광범위한 목적을 가지고 네트워크를 사용하고 있는 대학은 그 특성상 침해사고가 더욱 빈번하게 발생하고 있다. 현재 정보전산원에서는 교내 침해사고 발생 시 일차적으로 시스템운영실 보안담당자가 피해 시스템을 진단하고 침해사고로 판단될 경우 정보보호119팀에 해당 서버를 점검하도록 도움을 청하고 있지만 이는 일시적인 사고대응일 뿐이다. 이에 전남대학교는 정보보호119를 통해 침해사고 대응팀을 구축[2,3,4,5]하고 침해사고에 대해 보다 적극적으로 사전활동을 함으로써 교내 구성원의 정보를 보다 효율적으로 보호할 수 있도록 추진하였다.

본 논문에서는 현재 전남대학교 학내망을 정보보호 동아리와 유기적으로 연계하여 보안의 위험성에 대해 분석하고 CERT로서의 역할과, 전남대학교 정보보호119가 학내망 보안을 위해 구현한 연구내용을 소개하고자 한다. 본 논문의 2장에서 학내망 보안의 중요성에 대해 소개하고 그 문제점을 지적한 뒤, 3장에서 정보보호 동아리를 통한 cert 운영에 대해 설명하고, 4장에서는 현재 피해 시스템 분석대응을 위해 구현된 내용을 소개하며, 5장에서 결론과 향후 연구 계획에 대해 기술한다.

Ⅱ. 학내망 보안

1. 학내망 보안의 중요성

수많은 서버와 호스트가 존재하는 대학 내의 네트워크는 오래전부터 많은 문제점을 제기해 왔다. 과거에도 마찬가지였지만 미래에도 대학 내의 네트워크의 안전은 대학 내의 책임이지 정부의 기관이나 특정 외부인들의 도움으로는 해결해 나갈 수 없는 일이다.

대학은 큰 구성체이다. 그러기에 많은 정보보안에 따르는 위협들이 존재한다. 그 하나하나의 위협에서 분석과 진단은 시작된다. 여러 가지 위협 중에서 가장 큰 위협은 역시 사람에 의한 위협이다. 크래커들의 침입은 난무했고, 이를 관리하는 대학 구성원의 대처 또한 매우 미온적이다. 실제적으로 대학에 있어 보안적인 관점의 시스템 구축은 매우 힘든 상황이다. 서버관리에 있어서 절차와 규정, 응용업무에 있어서 논리상의 오류의 검정, 컴퓨터 처리시 실수에 따르는 응용업무 시스템 위협 등 여러 가지 문제를 해결하고 대처할 수 있는 제도적인 문제점이나 인력이 부족하다. 또한 투자비용의 부족함 때문에 대학의 모든 시설에 있어 보안의 관점을 이해시키고 적용시킨다는 것은 매우 힘든 일이다.

2. 학내망 보안의 문제점 제시

학내망 보안의 문제점으로는 여러 가지 원인을 들 수 있다. 먼저 대학 내 수많은 서버나 호스트가 보안이 취약한 환경으로 설치되고 방치되어 존재한다는 것이다. 두 번째로는 전문적인 지식을 가진 관리자의 부재이다. 이를 극복하기 위한 서버관리자나 학생들의 보안교육 부족과 정보보호 인식의 부족함은 오랫동안 보안의 취약성으로 방치된 문제 중의 하나이다. 침해사고가 발생했을 시 대응할 수 있는 인력부족 역시 어려운 현실중의 하나이다. 세 번째로는 대학이라는 조직의 특성상 광범위한 네트워크에 따른 보안 네트워크 구축이 어려울뿐더러 정보 전산원에서 수많은 서버의 보안을 책임져 줄 수 없다. 대학은 학생, 교수, 교직원등 다양한 구성원으로 이루어져 있으며 광범위하게 정보가 공유되므로 연구 자료의 유출과 해커들의 침입의 가능은 한층 더 높아진다. 결국 수많은 취약점과 보안 문제는 한순간에 해결할 수 없는 정도의 심각한 문제성임을 인식할 수 있다.

결국 예산, 인력 등의 모든 문제는 외부에서 해결할 수 없으며 결국은 대학자신의 힘으로 풀어나가야 할 숙제임을 던져주고 있는 것이다 .

Ⅲ. 정보보호 동아리 CERT 운영

1. 침해사고대응

그림 1은 전남대학교 학내망에서 정보보호 119 동아리가 학내망의 보안을 위해 cert으로서의 역할과 대응하기 위한 연구 과제들이다.

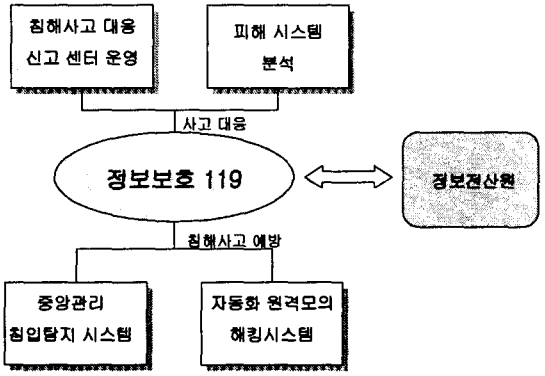

그림 1: 학내망 보안을 정보보호119의 역할 구조

1) 실질적인 침해사고 대응 및 분석, 피해 복구 기술 지원

침해사고 발생 시 침해 시스템에 대한 원인분석, 침해경로 분석, 침해사고재발방지 대책 등의 기술을 지원하여 침해사고에 적절히 대응할 수 있도록 한다.

2) 침해사고 처리 후 지원

위의 과정을 거쳐 처리된 시스템에 대하여 추후 일정 기간이 지난 뒤 재점검을 실시하여 시스템의 보안을 확고히 한다.

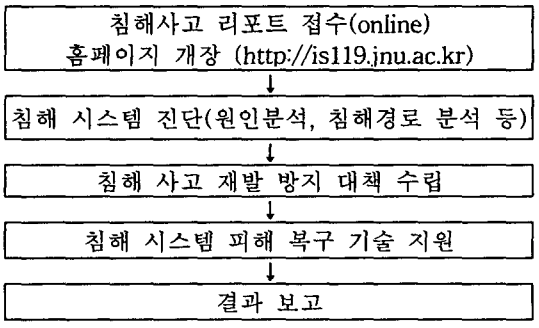

그림 2: 정보보호119 침해사고대처순서

2. 침해사고예방을 위한 기술지원

1) 학내망 시스템 분석 및 예방

학내망의 학교의 규모에 따라 거대한 네트워크를 형성하고 있다. 학내망의 효율적인 분석을 위해서는 초기 학내망에 산재되어 있는 전체 시스템의 규모와 상황을 파악해야 한다. 이 작업은 정보전산원에서도 특별한 시간과 인원이 투입되지 않는 이상 쉽지 않은 작업이다. 실제 정보보호119에서 전남대학교의 전체시스템을 파악하고 기본 취약점을 점검하는데 2달여의 시간이 소모되었다. 이러한 시스템 상황 파악 후 운영체제별로 또는 네트워크 클래스별로 권역을 나누어 정기적 또는 비정기적으로 시스템을 점검한 후 취약한 시스템에 대한 보안 경고 및 시스템 차원의 심각한 오류를 경고한다.

2) 보안 프로그램 소개, 패치 정보 제공, 운영체제별 보안 적용 기술 문서 제공

예방 차원에서 학내망을 점검한 후에는 추후 초보 관리자와 지속적인 보안 정보를 위해 공개된 보안프로그램의 설치, 유지 및 취약점에 따른 패치정보를 제공해주고, 각 운영체제별로 보안 설치 및 보안 관리에 대한 기술 문서를 제공하여 관리자 스스로도 따라 할수 있도록 지속 적인 관리를 하고 있다.

3) 학내망 모의해킹 실시

사전에 기존 발표 되었던 보안권고에 따라 OS 버전별 exploit을 DB화 시키고 그에 따르는 각 exploit별로 전체 호스트 대상으로 모의 해킹을 실시한다. 모의 해킹에 성공된 호스트에 관하여 보고서를 작성하여 관리자에게 연락을 취해 패치 정보, 대처 방법을 전달한다. 또한 새롭게 발표되는 보안 권고문에 주의를 귀울여 그때마다 전체 호스트 대상으로 취약점을 가지는 호스트 조사와 모의해킹을 실시한다.

3. 학내망 분석 결과 보고서 작성

보안적인 성격 때문에 시간이 흐른 후의 대응은 효과가 크지 않다. 따라서 수시보고서와 월 4회 이상의 주간 보고서를 통해 보안 문제를 제공하고 있다.

4. 침해사고 대응신고 센터운영

교내 구성원으로부터 학내망 서버 침해사고 신고를 받기 위해 정보전산원 홈페이지에 침해사고대응신고 센터를 개설하여 정보보호119에서 운영하고 있다. 그림 3에서 보는 것처럼 양식에 따라 정보보호119 침해사고대응신고 홈페이지에 개설운영중에 있으며, 교내 구성원으로부터 침해사고 신고 접수를 받은 시스템에 대해 침해사고 대응체제를 구축한다. 접수를 받으면 정보보호119의 분석 전문가가 해당 서버로 직접 방문하여 실시간 점검과 보안 방향을 제시하고 있다.

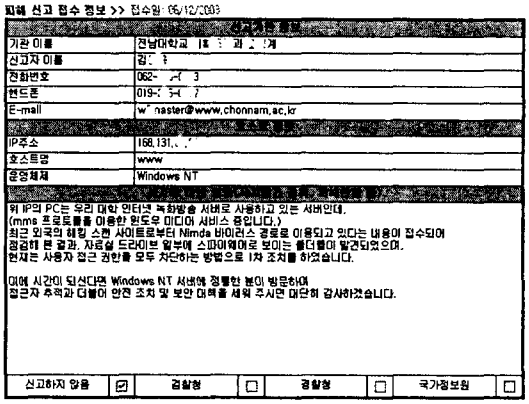

그림 3: 침해사고대응신고접수

Ⅳ. 학내망 보안을 위한 연구

1. 학내망 중앙관리 침입탐지 시스템

1) 목적

대학이라는 조직은 광범위한 네트워크망에 모두 보안 시설을 투자할 수 없다. 따라서 학내망 중앙관리 침입탐지 시스템을 통하여 공개도구인 네트워크 침입탐지 시스템인 snort를 통하여 모은 정보를 학내망 중앙관리 침입탐지 시스템으로 안전한 통신을 지원하고, 각 호스트의 다양한 이벤트를 수집/분석하여 네트워크의 위험을 파악할 수 있게된다. 정책에 위배되는 경우 이를 바로 관리서버에 통보하며, 보안사고 발생 후 사후 처리를 위한 보안 로그 분석이 가능하다. 단일 콘솔을 이용한 보안 관련 이벤트의 손쉬운 감시 및 경보를 제공하며 상이한 형태의 위협 및 공격을 정확히 파악하여, 지정된 침입의 유형에 따라 허위 경보를 줄이고 실재 보안 위협을 신속하게 포착하여 대응시간을 단축시킨다.

2) 동작 모델

중앙관리 침입탐지 시스템의 동작 모델은 그림4와 같다.

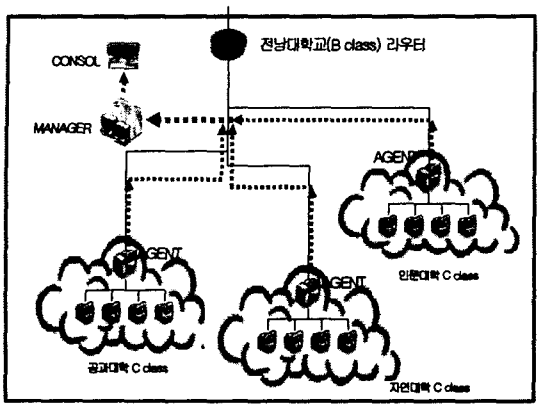

그림 4: 학내망 중앙관리 침입탐지 시스템

① 단일콘솔은 관리서버에서 분석된 로그를 다양한 검색과 분석을 통해 보안의 취약점이나 내부자료 유출과 같은 보안 사항을 검토할 수 있다.
② 관리 서버는 에이전트의 보안 정책을 설정하고 관리하며, 수집된 보안로그를 분석한다.
③ 보안 에이전트는 관리 서버에 의해 정해진 조직의 보안 정책을 적용하고, 보안 로그를 수집하여 보안 정책이 잘 적용될 수 있도록 한다.

3) 시스템 구조

본 시스템은 IDS 통합관리 시스템 형태로 학내망에 적용하여 개발하였으며, 국제표준(IDXP, IDMEF)을 준수하고 있다. 전체 시스템 구성도는 그림 5와 같다.

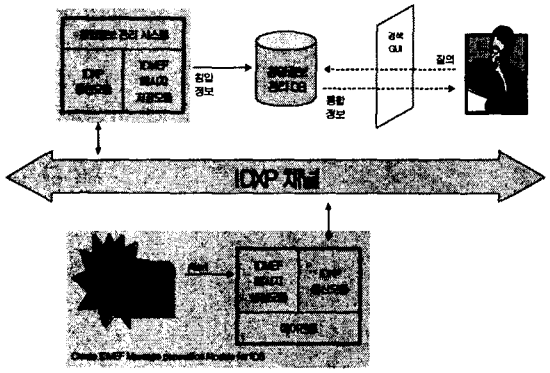

그림 5: 전체 시스템 구성도

침입정보 관리 프레임워크의 설계에 있어서 XML을 이용하여 침입정보 교환 메시지를 생성하고 저장하며 RoadRunner를 이용하여 침입정보를 교환, Correlation규칙을 통해 통합된 침입정보를 이용하여 분석이 가능하다. 그리고 시스템 관리자의 보안등급 설정으로 보안정책 기반의 보안관리 수행을 할 수 있도록 한다.

2. 자동화 된 원격모의해킹시스템 (ARHS: Automatic Remote Hacking System)

1) 목적

ARHS는 검사할 호스트의 각종 시스템 정보와 운영 서비스를 조사하여 잠재적인 보안 문제를 찾아냄으로써 규모가 큰 학내망에 맞게 개발하였다. Linux와 Solaris 두 가지 운영 체제에 대한 서비스를 제공하고 있으며 다른 운영 체제에 대한 점검도 쉽게 추가할 수 있도록 설계하였다.

보안 점검 과정은 모두 편리한 웹 인터페이스를 통해 이루어진다. 또한 암호화 기법을 사용하여 이러한 과정은 모두 안전하게 진행 할 수 있도록 설계하였다. 여기서 그치지 않고 실제 크래커들이 사용하는 각종 해킹 도구와 스크립트를 이용하여 실제 해킹을 통한 점검을 수행한다. 점검을 통해 얻은 결과를 바탕으로 그에 알맞은 대처 방안을 제공한다.

2) 구성도

검사할 대상 서버의 각종 데몬과 서비스를 조사하여 각 데몬의 정보뿐만 아니라 소프트웨어와 하드웨어 여러 시스템 정보를 얻어낸다. 현재 리눅스와 솔라리스 두 가지 운영 체제에 대한 서비스를 제공할 수 있으며 다른 운영 체제에 대한 점검도 얼마든지 쉽게 추가할 수 있도록 모듈화 시켜 설계하였다. ssh, ftp, sendmail, pop3, imap, finger, http, finger 등 주요 서비스들에 대한 정보를 바탕으로 이를 미리 수집된 데이터와 비교하여 잠재적인 보안 위협을 보고한다. 이러한 과정은 모두 편리한 웹 인터페이스를 통해 이루어지도록 한다. 또한 여기서 그치지 않고 실제 해커들이 사용하는 각종 해킹 도구와 스크립트들을 이용하여 단순한 정보 수집이 아닌 실제적인 점검을 수행한다. 이를 바탕으로 얻은 정확한 정보는 이에 대한 대처 요령과 함께 알아보기 쉽게 제공되므로 누구나 유용하게 이용할 수 있다. ARHS의 모의 공격 흐름도는 그림 6과 같다.

3) 기능

① 네트워 상태 체크

점검 대상 서버에서 점검 요청이 올 경우 호스트가 살아있는지 점검하여 잘못된 입력의 가능성과 네트워 상태를 먼저 진단한다.

② 모의 해킹 테스트

본 도구는 실제로 많은 해커들이 사용하고 있는

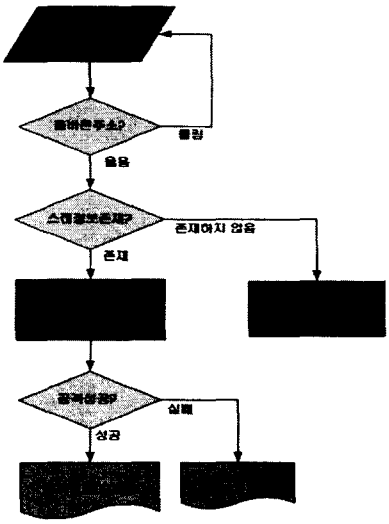

그림 6: ARHS 모의공격 흐름도

해킹 도구 및 스크립트를 수집하여 이를 활용하였다. 그런데 해킹 도구나 스크립트는 심각한 시스템 문제를 유발할 수 있다. 이를 보안하기 위해서 직접 해킹 도구를 실행하는 것이 아니라 이를 엔진에서 적절히 조작하여 실행함으로서 보안 점검 과정 중에 발생할 수 있는 위험을 최소화한다.

③ 웹 인터페이스의 제공

별도의 프로그램 없이 웹 브라우저를 통해 몇 가지 점검 사항에 대한 입력만으로 쉽게 점검을 받을 수 있게 구현한다.

④ 취약점에 대한 해결책 제공

보안 점걸 결과에 따라서 그에 적절한 대처 방안을 알려 준다.

⑤ 신속한 업데이트

본 도구는 중앙 서버가 점검 서비스를 제공하여 점검 대상 서버는 특별한 노력 없이 항상 최신의 정보를 바탕으로 점검 서비스를 받을 수 있도록 한다.

⑥ 모듈화

본 도구는 보안 점검 및 해킹 모듈의 추가를 용이하게 한다. 따라서 새로운 보안 취약점이나 해킹 코드가 발표될 경우 모듈의 추가만으로 이를 쉽게 활용할 수 있다.

4) 구현 결과

ARHS 시스템은 기능에 따른 모듈화에 중점을 두었다. 스캔이나 모의 공격에서 사용되어지는 모듈이나 취약점 형태는 새롭게 나오는 공격형태를 수집 정리하여 DB화 하고, 업데이트하고 있다. ARHS 시스템과 보안상의 해결을 위해 관리자와 와 도구의 인증방식은 RSA를 통한 공개키 인증방식을 통해 구현하였다. 마지막으로, 필요한 스캔형태, 공격형태 등에 대한 데이터를 자동 패치 할 수 있도록 기능을 추가하였다. ARHS의 결과 화면은 그림 7과 같다.

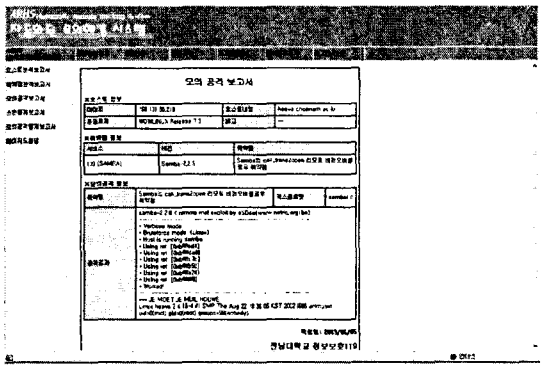

그림 7: ARHS 결과화면

V. 결론

학내망 보안은 꾸준히 노력을 요구하는 작업이다. 단순히 정보보호동아리의 활동만으로, 또는 학교의 일방적인 노력만으로도 되는 것은 아니다. 대학구성원의 조화가 이루어져 정책을 세우고 정보전산원을 통해 시행되며, 정보보호동아리의 감초같은 역할을 통한다면 충분히 가능하리라고 본다.

전남대학교 정보보호 동아리 정보보호119는 정보전산원과 연계한 cert을 통해 학내망 보안의 중심으로 자리잡고 있으며, 통합보안 관리시스템의 학내망 적용과, 자동화된 취약점 진단을 위한 테스트를 위해 ARHS 시스템을 설계 구현하였다. 추후 학내망의 안정화와 제도적인 장치를 제안하고, 학내망의 정확한 조사를 통해 DB화 하고, 학내망 내에서 각 호스트의 이상증후를 감지하고 추적하여 해당 호스트의 정확한 위치를 제공하는 연구를 진행 할 예정이다.

참고문헌

[1] "CERT/CC Overview Incident and Vulnerability Trends," http://www.cert.org
[2] Moria J. West Brown 외, Handbook for Computer Security Incident Response Team(CSIRTs), 1988
[3] 정현철, 하도윤, 박유리, "Cert 구축 및 운영 가이드," http://www.cert.co.kr
[4] 김명찬, "학내망 보안운영 사례"
[5] 오규철, "CERT 구축 및 운영"