관리자를 위한 리눅스 서버 시스템 모니터링 및 제어 솔루션 구현

Implementation of Linux Server System Monitoring and Control Solution for Administrator

장 성 원*, 박 찬 홍*, 박 상 주*, 성 현 경*
상지대학교 컴퓨터정보공학부*

Sung-Won Jang*, Chan-Hong Park*,
Sang-Ju Park*, Hyeon-Kyeong Seong*
School of Computer Information and Communication Eng. Sangji University

요약

리눅스 서버는 웹, FTP, SSH등 여러 가지 서비스를 제공한다. 이러한 서비스를 받는 사용자들이 이것을 이용하여 해킹을 시도하고 있다. 그렇기 때문에 서버 보안에 대한 대책이 필요하다. 본 논문에서는 다중의 리눅스 서버의 대한 각 종 서비스 로그를 분석하여 리눅스 기반이 아닌 윈도우즈 기반에서 다중 리눅스 서버 시스템을 모니터링 및 제어할 수 있는 솔루션을 개발하였다.

I. 서론

리눅스 서버를 이용하여 웹, FTP, SSH등 여러 가지 서비스를 사용자들은 제공받을 수 있다. 또한 이러한 서비스를 받는 사용자들이 서비스 본래의 순기능을 사용하지 않고 역기능을 사용하려는 불특정 다수가 존재할 수 있기 때문에 해킹의 우려가 커질 수 있다. 그렇기 때문에 서버 보안에 대한 대책이 필요하며 그 중 각 종 서비스에 대한 로그를 분석하여 그에 맞게 대응하는 방법이 있을 수 있다.[1-3] 하지만 이러한 대응 방법은 관리자 입장에서 1대의 서버가 아닌 N대의 리눅스 서버를 관리하고 그에 대한 로그를 분석해야 한다면 이는 텍스트 기반으로 복잡하게 나열된 서비스 로그를 분석하고 그에 맞게 대응하는 것은 시간적으로 비효율적이다.[4] 이러한 N대의 리눅스 서버의 로그를 쉽게 분석하고 관리자에게 분석 정보를 시각적으로 보여줌으로써 한 눈에 알아볼 수 있게 되면서 그에 대한 시스템 제어를 할 수 있는 대응 방법이 필요하게 된 것이다. 현재 윈도우즈 서버로 관리하는 곳이 많기 때문에 N개의 리눅스 서버를 리눅스 서버로 통합 제어하지 않고 윈도우즈 기반의 서버에서 관리할 수 있도록 할 것이다.[5]

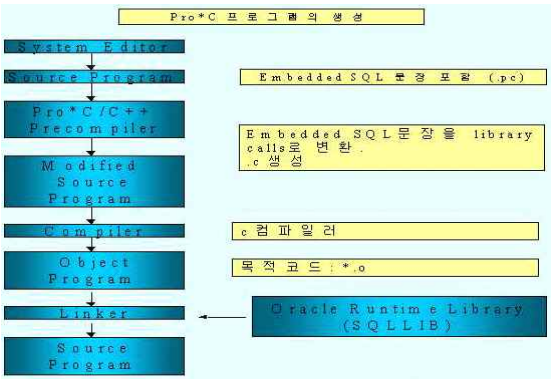
Ⅱ. 관련연구

2.1 Linux Log File

HTTP, FTP, SSH의 3가지 서비스를 대상으로 프로그램이 동작하므로 이것을 바탕으로 4가지 로그파일을 분석한다. 분석할 대상의 첫 번째 로그파일은 /var/log/wtmp 파일이다, 이 파일은 ssh(Secure Shell) 접속 성공의 관련된 정보를 추출할 수 있다. 이 파일은 2진 형태로 이루어져 있기 때문에 파일 자체로는 분석이 불가능 하며 last 명령어를 통해서 정보를 확인할 수 있다.

2.2 Pro*C/C++

Pro*C/C++를 이용하기 위해서는 SQL 문장이 삽입된 C 프로그램을 (.pc) 작성하고 이 프로그램 소스파일을 Pro*C/C++로 먼저 처리하면 삽입된 SQL 문장들이 C 코드로 재 생성되어 (.c) 새로운 소스파일이 나온다. 이것을 가지고 통상적인 C프로그램처럼 컴파일 해주고 링킹하는 과정을 거치면 오라클과 연동할 수 있는 실행 가능한 프로그램이 되는 것이다. 일반적으로 오라클 9i버전인 경우에는 설치과정을 그대로 진행할 경우 Pro*C/C++가 같이 설치된다.



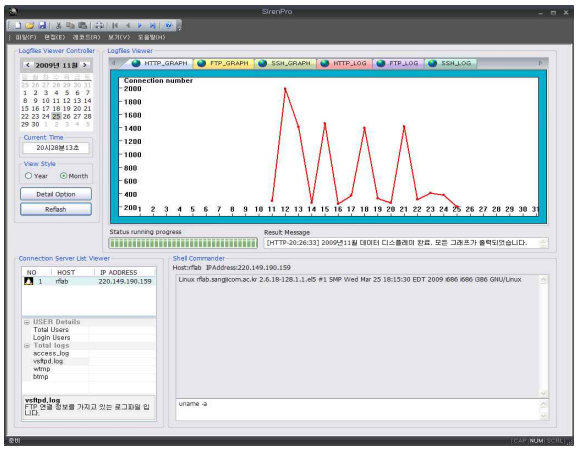
▶▶ 그림 1. Embedded SQL Program의 생성

Ⅲ. 모니터링 및 제어 솔루션 구현

표 1. 개발 환경 및 개발 도구 모음

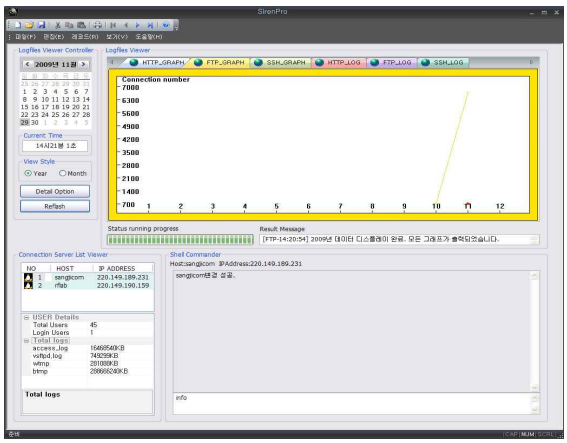
	server	client
Operating System	Windows XP SP3	CentOS 5.2
Development Tool	Microsoft Visual Studio 2008 v9.0.30729.1 SP	Pro*C/C++ Release 10.2.0.1.0
DBMS	Oracle 10g	Oracle 10g

그림2는 구현된 서버 어플리케이션이다. 현재 RFLab 리눅스 서버가 마운팅되어 HTTP 서비스에 대한 11월의 전체 접속량을 보여주고 있다. 또한 쉘커멘더를 통해서 RFLab서버에게 쉘 명령어를 보냄으로써 제어가 가능한 것을 알 수가 있다.



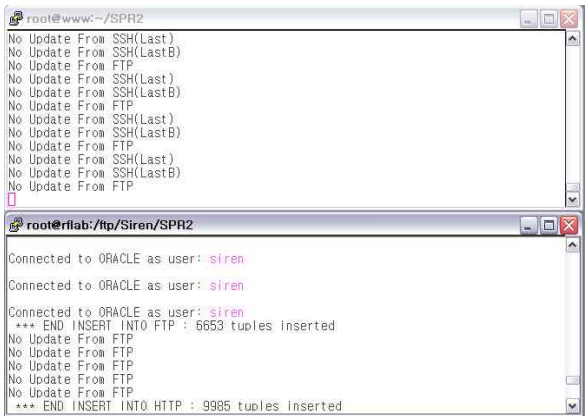
▶▶ 그림 2. RFLab서버의 11월 HTTP 접속 정보화면

또한 본 어플리케이션은 다중의 리눅스 서버 접속도 가능하기 때문에 아래의 그림3와 같이 Sangjicom서버와 RFLab서버의 2009년 FTP접속에 대한 그래프를 나타내고 있으며 Sangjicom서버로 1대1 쉘 접속을 통하여 그 서버 시스템의 정보를 Property창에 출력하고 있다.



▶▶ 그림 3. Sangjicom서버와 RFLab서버의 2009년 FTP 접속 정보화면

클라이언트 어플리케이션은 텍스트기반으로 구성되어 있으며 최초 실행시 서버에 마운팅되며 데이터베이스 자동로그인 후 업데이트를 수행하고 있다. 업데이트는 1초당 한번씩 로그를 체크하여 전송하며 현재 상태를 텍스트로 화면에 출력한다.



▶▶ 그림 4. RFLab서버와 Sangjicom서버의 클라이언트 어플레케이션이 실행되는 화면

Ⅴ. 결론 및 향후 연구 방향

본 논문에서 구현된 어플리케이션을 통해서 관리자는 다중의 리눅스 서버에서 제공되는 HTTP, FTP, SSH 서비스에 대한 접속량을 그래프 및 테이블로 보여준다. 또한 관리자는 그 결과를 통해서 쉘 명령어를 이용해 각각의 리눅스 서버에 보안 정책 및 시스템을 제어할 수가 있다. 그렇기 때문에 기존의 텍스트형식의 로그파일을 분석하고 시스템을 제어하는 방식보다 시간적으로 더 높은 효율성을 보장한다. 또한 브로드캐스트 메시지 전송으로 인하여 멀티 프로세싱이 가능하다. 하지만 이러한 기능은 윈도우즈 기반의 어플리케이션으로 구현되었기 때문에 리눅스 서버에서는 불가능하다. 그렇기 때문에 플랫폼에 독립적으로 수행될 수 있도록 JSP같은 웹프로그래밍언어를 사용하여 웹 상에서 볼 수 있도록 어플리케이션을 구현한다면 플랫폼에 대해 독립적으로 수행될 수 있을 것이다.

▮ 참 고 문 헌 ▮

[1] 김태용 저, CentOS 리눅스 구축관리실무, 슈퍼유저 코리아

[2] Stergios Spanosa, Apostolos Melionesb, George Stassinopoulosa "The internals of advanced interrupt handling techniques: Performance optimization of an embedded Linux network interface" Computer Communications Volume 31, Issue 14, 5 September 2008, Pages 3460–3468

[3] K. Salah, A. Kahtani "Performance evaluation comparison of Snort NIDS under Linux and Windows Server" Journal of Network and Computer Applications, Volume 33, Issue 1, January 2010, Pages 6–15

[4] http://otn.oracle.com 의 Pro*C/C++ Precompiler Programmer's Guide 참고