2002년 한국정보처리학회 춘계학술발표논문집 제9권 제1호

웹기반 실시간 스니핑 탐지 시스템의 설계 및 구현

석원홍* 강진석** 강홍식***
인제대학교 정보컴퓨터공학부
babootaeng@naver.com
comdol12@netian.com
hskang@nice.inje.ac.kr

Design and Implementation of a Web-based Real-Time Sniffing Detection System

Won-Hong Seok*, Jin-Suck Kang**, Heung-Seek Kang***
Dept of Information and Computer Engineering, Inje University

요약

최근 인터넷의 확산에 따라 여러 가지 침해사고 발생이 증가하고 있는 추세이다. 그 중에도 인터넷의 표준 프로토콜로 사용 중인 TCP/IP 의 전송방식이 암호화하지 않은 텍스트기반으로 이루어진 데이터이기에 간단한 스니핑 기법으로도 데이터 유출 및 절취가 가능하다. 동일 네트워크에 대형 시스템들이 몰려 있는 웹호스팅 업체나 IDC등에서는 더 유의해야 한다. 취약한 하나의 시스템만 관리자 권한을 획득하여 스니퍼를 돌린다면 전체 네트워크를 장악하게 되며, 외부 공격자뿐만 아니라 내부 공격자에게도 큰 취약점을 가지고 있다. 본 논문에서는 이러한 스니핑 공격을 원격지에서 실시간으로 탐지해냄으로서 스니핑 공격에 대처할 수 있도록 시스템을 구현하였다.

1. 서 론

인터넷의 발전으로 현대 사회에서 인터넷은 중요한 위치를 자리 잡고 있다. 현실적으로 개인이나 기업들은 인터넷을 통해 정보와 개인 정보들은 공유하고 있다.

특히, 전자 상거래의 확대로 인해 인터넷은 중요한 경제 활동의 중심지로 발돋움하고 있다. 이러한 현실에서 해커들이 즐겨 사용하는 해킹기법인 스니핑을 통해 개인 정보 유출이나 신용카드번호, 및 통장과 관련된 비밀번호 등이 외부로 빠져나가는 사례들은 전자상거래 발전에 큰 장애로 지적되고 있다. 따라서 본 논문에서는 작게는 개인 정보 유출을 막고 크게는 전자상거래의 투명성과 안전성을 확보하기 위한 차원에서 웹 상에서 실시간으로 스니핑을 전담하여 탐지할 수 있는 시스템을 설계하고 구현하였다.

본 논문의 전체 구성은 1장의 서론, 2장의 스니핑의 개념, 3장의 스니핑 탐지시스템 구현 4장 실험 및 결과 그리고 마지막 5장의 결론으로 구성되어 있다.

2. 스니핑 개념

2.1 스니핑 이란

스니퍼는 네트워크 상에서 오고가는 패킷을 엿보는 도청 장치다. 스니핑이란 이러한 스니퍼를 이용하여 네트워크상의 패킷을 도청하는 것을 말한다.

2.2 스니핑의 원리

일반적으로 호스트는 필터링 과정을 통해 자신을 목적지로 하는 패킷만 선택하여 받아들인다. 필터링 과정은 이더넷 인터페이스에서 이루어지는데, 이더넷 인터페이스를 promiscuous mode로 설정하게 되면 이더넷 인터페이스는 필터링을 하지 않고 모두 받아들이게 된다. 스니핑은 바로 이러한 원리를 역이용한 해킹 기법이다.

2.3 스니핑 탐지 기법

스니퍼는 네트워크 인터페이스를 promiscuous mode로 설정하여 네트워크를 도청하게 된다.
따라서 관리자는 호스트가 promiscuous mode로 설정되어 있는지 주기적으로 점검하여 스니퍼가 실행되고 있는 시스템을 탐지해야 한다.

a. 시스템 내부
이더넷이 promiscuous mode로 설정되어 있는지 시스템 내부에서 확인하는 방법은 다음과 같다.
$ifconfig -a|grep PROMISC

b. 시스템 외부

· Arp를 이용하는 방법 : IP는 맞지만 목적지 MAC address를 다르게 하여 Arp 요구를 보내는 방법으로, promiscuous mode가 아닌 경우에 패킷이 목적지까지 갈 수 없지만 promiscuous mode인 경우에는 응답을 하는 특징을 이용하여 검사하는 방법

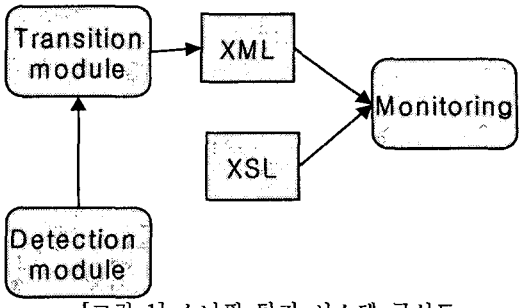
· DNS를 이용하는 방법 : 목적지 서버에 위조된 연결 요청을 보내어, 일반적인 스니핑 프로그램이 요청받은 시스템의 IP 주소를 Inverse DNS Lookup 한다는 특징을 이용하여 검사하는 방법

· Decoy 방법 : 관리자가 고의적으로 ID와 패스워드를 패킷에 흘려 공격자가 이 패스워드나 ID를 사용하게 함으로서 스니핑을 탐지해 내는 방법

· ping을 이용하는 방법 : 목적지에 ping을 보낼 때 목적지 IP는 맞지만 목적지 MAC address는 존재하지 않는 정보로 하여 ICMP Echo Packet을 보내어 응답이 오는지 검사하는 방법으로, promiscuous mode 인 경우 응답한다는 특징을 이용하여 검사하는 방법이다. 본 논문에서 구현하는 시스템은 이 방법을 사용한다.

3.스니핑 탐지 시스템 구현

본 3장에서는 구현하고자 하는 스니핑 탐지시스템을 모듈별로 기술한다.



[그림 1] 스니핑 탐지 시스템 구성도

[그림 1]은 스니핑 탐지 시스템의 구성도이며 이에 대한 상세 설명은 다음과 같다.
a. Detection 모듈

원격지 컴퓨터가 스니핑을 당하는지 탐지하는 역할을 한다. 스니핑을 탐지하는 기술 중에 하나인 ping을 이용한다.
목적지에 ping을 보낼 때, 목적지의 IP는 맞지만 목적지 MAC address는 존재하지 않는 것으로 하여 ICMP Echo Packet을 보낸 다음 응답이 오는지 검사하는 방법이다.대부분의 정상적인 시스템에서는 MAC address정보가 올바르지 않기 때문에 패킷을 무시 하지만 promiscuous mode가 설정된 시스템에서는 응답을 한다는 특징으로 검사하는 방법이다.

b. Transition 모듈

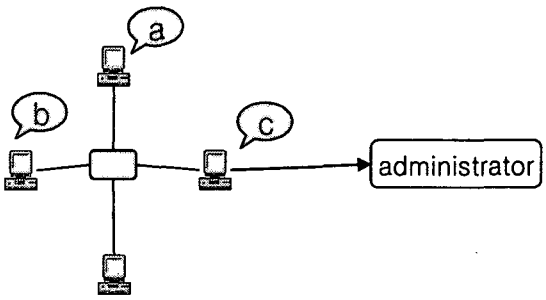
Detection 모듈에서는 스니핑 당하는 것으로 의심되는 컴퓨터를 발견하게 되면 로그파일을 남기게 된다. 이런 로그파일을 최근 차세대 웹 표준 문서 포맷인 XML(eXtensible Markup Language) 파일로 변환한다.

c. Monitoring
Transition 모듈에서 생성된 XML을 웹상으로 보여 주기 위해서는 XSL이 필요하다. XML 문서는 데이터를 분류 저장할 뿐이고, 그 데이터를 사용하여 문서를 작성하고 출력하는 것은 XSL(eXtensible Stylesheet Language)의 몫이다. XML과 XSL은 독립된 문서지만 서로 문서교환이 자유롭고, XML문서의 데이터를 XSL에서 사용자가 원하는 형식으로 자유롭게 출력할 수 있는 장점을 가지고 있다.

4. 실험 및 결과

본 장에서는 3장에서 구현한 스니핑 탐지 시스템을 실험하고 그 결과를 분석한다.

다음과 같이 테스트 환경을 구성한다.



[그림 2] 테스트 환경

a: 공격 당하는 컴퓨터

b: 공격자 컴퓨터(Hunt를 이용한다.)

c: 스니핑 탐지 시스템이 구현된 시스템

※ 구현 시스템 환경

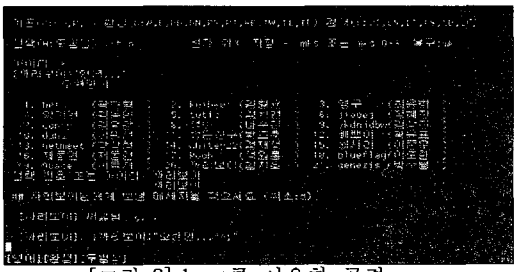
운영체제 : Red Hat 7.1 (Kernel 2.4.10)

컴파일 환경 : gcc-2.96, libpcap-0.6

웹 서버 : apache-1.3.22

실험에서의 공격 툴은 Hunt를 사용하였다. Hunt는 출력 결과가 쉬운 형태로 되어 있으며, 스푸핑 기능도 제공하고 또한 사용하기는 쉬운 공격 툴이다.

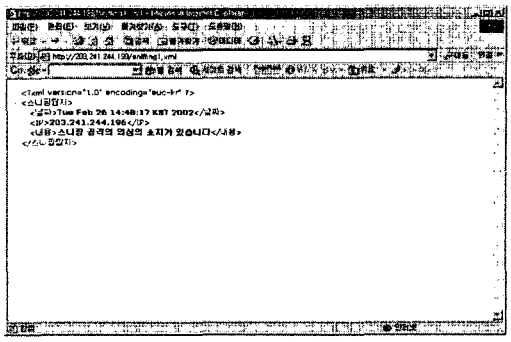
[그림 3]은 Hunt 이용하여 스니핑 공격을 하는 장면이다.



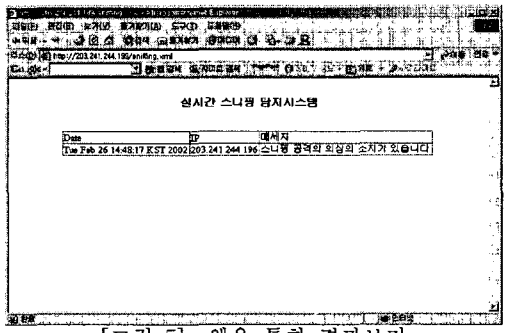
[그림 3] hunt를 이용한 공격

실시간 스니핑 탐지시스템에서 Detection 모듈이 스니핑 공격을 탐지하여 로그파일을 생성하게 되면, Transition 모듈이 XML파일을 생성하게 된다.

[그림 4]는 생성된 XML파일을 웹을 통해 살펴 본 것이다.



[그림 4] 생성된 XML파일



[그림 5] 웹을 통한 결과보기

[그림 5]와 같이 생성된 XML 파일은 관리자가 보기 쉽게 XSL과 결합하여 웹상으로 보여 주게 된다. 관리자는 Apache 파일인 http.conf를 통해서 지정된 IP를 통해서만 결과를 볼 수 있다.

본 장에서는 스니핑 탐지시스템이 어떻게 동작하는지를 실제 공격을 통해서 실험해 본 것이다. 공격은 스니핑 공격 툴인 Hunt를 사용하였다. 스니핑 공격을 탐지한 정보를 웹을 통해 살펴보았다.

5. 결론

인터넷 표준 프로토콜인 TCP/IP는 설계 당시에 데이터를 전혀 암호화하지 않게 설계되었다. 때문에, 네트워크 상에 데이터 유출 및 절취가 가능한 스니핑 해킹기법에 심각한 취약점을 가지고 있다.

이러한 이유로 스니핑 공격에 대한 문제 해결을 위해 많은 연구가 이루어지고 있다. 스니핑 공격에 대한 근본적인 해결 방법으로는 데이터를 암호화하는 것이다. 현재 SSH과 같은 암호 프로토콜을 이용하게 된다면 스니핑을 통해 데이터가 유출된다고 하더라도 암호화된 내용을 해석하지 못한다면 정보를 알

수 없게 된다. 이러한 문제 해결 방안이 나와 있으나 일관된 암호 프로토콜의 부재와 애플리케이션의 부재, 유저가 사용하기에 불편하다는 점 때문에 암호화된 네트워크를 구성하여 사용되는 데에는 어려움이 따른다. 따라서 본 논문에서는 스니핑 방지를 위한 대책으로, 내부 네트워크를 실시간으로 점검함로서 스니핑의 공격을 탐지하여 대처하는 시스템을 구현하였다.

앞으로의 과제는 스니핑을 탐지하는 기능뿐만 아니라 역추적 할 수 있는 방법을 연구하는 것이다.

참고문헌

[1]http://www.securitymap.net/sdm/docs/faq/스니핑-faq.html
[2]http://www.certcc.or.kr/paper/tr2000-07/tr2000-07.html
[3]http://www.securitypacketstorm.org
[4]http://www.cse.nau.edu/~mc8/Socket/Tutorials/section1.html
[5]Hunt http://lin.fsid.cvut.cz/~kra/index.html
[6]seninel http://www.subterranin.net/site
[7]libpcap http://www.tcpdump.org
[8]에릭 레이 저, 장은영 역 XML 시작하기 1999
[9]stevens 저, unix network programming volume 1
[10]stevens 저, TCP/IP Illustrated, Volume1