로컬 LAN환경에서의 스니핑(Sniffing) 탐지 및 관리도구 구현

김기욱*, 김창수*, 정신일**
*부경대학교 전자계산학과
*부경대학교 정보통신공학과

The Implementation of Sniffing Detector and Management Tool in Loacal LAN

Ki-Uk Kim*, Chang-Soo Kim*, Jung-Sin Il**
*Department of Computer Science, Pukyong Naitonal Unversity
**Department of Telecommunication Engineering, Pukyong Naitonal Unversity
E-mail : kimkiuk@mail1.pknu.ac.kr

요 약

최근 인터넷 사용의 증가와 더불어 네트워크 기반의 해킹피해가 증가하고 있다. 해킹을 탐지하기 위한 많은 연구가 진행중이고 여러 가지 탐지 도구들이 개발되어 있다. 본 연구에서는 이러한 해킹 기법 중에서 로컬 LAN환경에서 모든 네트워크 트래픽을 분석하여 불법적으로 정보를 수집하는 스니핑 탐지 및 관리 도구를 개발하였다. 스니핑 관리 및 탐지도구는 두 가지의 모듈로 구성되어 있다. 즉 스니핑 탐지모듈과 스니핑 관리지 모듈이다. 스니핑 탐지 탐지 도구는 임의의 host로부터의 침입을 발견한다. 그리고 스니핑 관리 도구에서는 스니퍼에 대한 정보를 웹 브라우저 상에 보여준다.

ABSTRACT

In these days, there are explosive growths of Internet users. But the damages of hacking are on the increase lately too. Currently, many researches for detection of hacking are studying, and there are many hacking detection tools. In this thesis, We designed and implemented Sniffing detection and Management Tool, Which can search an invasion by sniffing in Local LAN envirment. The Implementation of Sniffing Detector and Management Tool are composed of two modules. In other words, They are Sniffing Detector Tool and Sniffing Management Tool. The Sniffing Detector Tool discovers implementation of the Sniffing from optional host to Sniffing Detector host. And The Sniffing Management Tool displays information of Sniffer on Web_Browser.

Ⅰ. 서 론

최근 인터넷의 이용이 급증하고 있다. 그 사용 영역도 과거 학술적 목적이나 정보검색에서 나아가 제품에 대한 광고나 판매 등 상업적 용도로 그 사용 영역이 점차 확대되고 있는 추세이다. 인터넷의 사용이 활발해지면서 해킹의 피해 사례도 증가하고 있다. 2001년 3월의 통계자료[1]를 보면 전체적인 국내 해킹 피해 접수 건수가 395건으로 지속적으로 증가하였으며, 특히 일반 기업의 해킹 사고도 80건(62.0%)로 크게 증가하고 있는 추세이다. 해킹기법[2]도 해킹 툴을 사용하는 방법 외에 개인 사용자 계정 도용, 스팸 메일 관련 공격, 버퍼 오버플로우 공격, DOS(Denial of Service)공격 등 점점 다양해지고 있다.

본 논문에서는 이러한 해킹 공격 기법들 중 스니핑을 이용한 해킹 공격을 탐지하여 관리자 모드로 공격자의 정보를 알려주는 스니핑 탐지 및 관리도구를 구현하였다.

II. 본 론

1.네트워크의 동작 원리

1.1 TCP/IP

1.1.1 TCP (Transation Control Protocol)

TCP[3]는 IP 상위 layer의 서비스를 제공한다. TCP에서는 정보의 손실, 훼손 및 중복을 방지하기 위해서 승인과 체크섬을 사용한다. 또한 패킷의 순서 보장을 위해서 순서 번호(sequence number)를 관리하며 이 외에도 여러 응용 프로그램들이 동시에 TCP에서 제공하는 서비스를 받기 위해서 다중 채널(multiplexing)을 지원한다. TCP 패킷의 헤더[4]를 살펴보면 먼저 source port와 destination port는 TCP의 연결 및 서비스 종류를 구분하기 위해 사용된다. sequence number 필드는 전송하는 세그먼트의 순서를 나타내는 번호를 담게 되며 다음의 승인 번호와 함께 연결 설정시 중요한 역할을 하게 된다. 그리고 code bit 필드는 6개의 비트로 이루어지며 각기 URG, ACK, PSH, RST, SYN, FIN이 있다. URG는 급한 데이터임을 표시할 때 사용되며, RST와 FIN은 연결을 종료할 때, 그리고 SYN은 연결을 시작할 때 사용된다.

1.1.2 IP (Internet Protocol)

IP[5]는 비연결 및 비신뢰성 데이터 전송을 위한 프로토콜이다. 인터넷에서 가장 널리 사용되는 프로토콜로서 목적지까지 패킷을 전달하는 것이 주된 목적이며 일반적으로 이야기하는 IP 주소는 이 프로토콜에서 사용되는 것이다. IP 프로토콜의 기능은 크게 두 가지로 나눌 수 있다. 첫째는 목적지 IP까지의 길을 찾는 라우팅(routing) 기능이고, 두번째는 네트워크에서 전달할 수 있는 최대 패킷 크기에 맞게 패킷을 나누거나 합치는 기능이다. IP 프로토콜을 사용하여 데이터를 전송할 때는 전송 패킷에 IP 헤더가 붙여지는데 IP 헤더의 destination IP로 각 패킷은 독립적으로 목적지까지 전송된다. IP의 주된 목적은 패킷에 대한 라우팅 기능으로 data변조나 오류 등의 문제는 체크하지 않는다. 이런 IP layer의 단점을 이용한 공격 방법이 스누핑에 의한 해킹공격이다.

1.2 이더넷 주소와 IP주소

이더넷 주소는 LAN 카드의 물리적인 주소를 의미하고 IP 주소는 일반적인 인터넷 주소를 의미합니다. 인터넷의 모든 컴퓨터는 IP 주소를 가지고 있으며 IP 주소를 가지고 있기 때문에 각각의 컴퓨터들이 구분되는 것이다. 그리고 이 IP 주소에 의해 어떤 사람이 어떤 컴퓨터에 접속했는지 알 수 있다. 하나의 컴퓨터는 IP주소와 이더넷 카드가 가지고 있는 물리적 주소인 이더넷 주소를 모두 가지며 실제적으로 인터넷에서 통신을 할 경우 IP주소로 패킷이 전달되는 것이 아니라 이더넷 주소로 패킷이 전송된다.

2. 스니핑(Sniffing) 기법

스니핑[6]은 Ethernet LAN환경에서 모든 네트워크 트래픽을 분석하여 불법적으로 정보를 수집하는 공격기법으로 이러한 스니핑 공격은 웹호스팅, 인터넷 데이터센터(IDC)등과 같이 여러 업체가 같은 네트워크를 공유하는 환경에서는 매우 위협적인 공격이 될 수 있다.

2.1 스니핑의 원리

LAN의 호스트를 구별하기 위한 방법으로 이더넷 인터페이스는 MAC(Media Access Control) 주소를 갖게 되며, 모든 이더넷 인터페이스의 MAC 주소는 서로 다른 값을 갖는다. 따라서 로컬 네트워크상에서 각각의 호스트는 유일하게 구별될 수 있다. 이더넷에서 패킷의 전송과정을 살펴보면 같은 임의의 컴퓨터에서 전송된 패킷은 같은 LAN 상의 모든 컴퓨터에 broadcasting된다. 따라서 같은 네트워크내의 컴퓨터는 다른 컴퓨터로 전송되는 모든 트래픽을 볼 수 있다. 하지만 같은 LAN 상의 임의의 컴퓨터가 이더넷을 지나는 모든 트래픽을 받아들이면 관계없는 트래픽까지 처리해야 하므로 효율적이지 못하고 네트워크의 성능도 저하될 수 있다. 그래서 이더넷 인터페이스(LAN 카드)는 자신의 MAC 주소를 갖지 않는 트래픽을 무시하는 필터링 기능을 가지고 있다. 이 필터링에 의해 자신의 MAC address를 가진 트래픽만을 보도록 한다.

이더넷 인터페이스에서 네트워크 상의 모든 패킷을 볼 수 있도록 하는 기능을 설정할 수도 있는데 이를 "promiscuous mode"라 한다. 스니퍼는 이더넷 인터페이스를 이러한 "promiscuous mode"[7]로 설정하여 로컬 네트워크를 지나는 모든 트래픽을 도청할 수 있게 된다.

3. Sniffing 탐지 및 관리도구의 구현

본 논문에서 구현한 스니핑 탐지 및 관리도구는 스니핑을 탐지하는 모듈과 탐지된 결과를 웹의 브라우저에 출력하는 관리자 모듈로 구성이 되어 있다. 그리고 본 논문의 관리자 모듈은 KISA[8](한국정보보호센터)의 침입탐지 시스템 등급 규정에 기반하여 개발하였다.

3.1 시스템 구현 환경

- ▶ O/S : 리눅스[9], Windows 98
- ▶ 컴파일러 : gcc, jdk2.0
- ▶ 라이브러리 : libnet-1.0.1b (패킷 생성 기능)
  libpcap-0.5 (패킷 캡쳐 기능)
- ▶ 웹서버 : apache 1.3.12

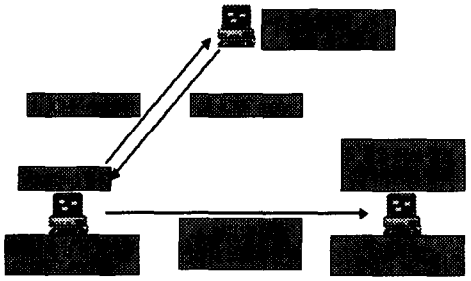
3.2 Sniffing 탐지 및 구현도구의 전체 구성

스니핑 탐지 및 관리도구는 스니핑을 탐지하는 탐지모듈과 탐지된 결과를 웹상의 브라우저에 보여주는 관리자 모듈로 구성되어 있다.

우선 탐지 시스템에서 스니핑 침입자로 예상되

는 host에 ICMP request패킷을 전송한다. 만약 스니핑 실행 host라면 자신의 MAC 주소와 일치하지 않은 ICMP request패킷이라도 promiscuous mode로 동작하기 때문에 ICMP reply 패킷을 스니핑 시스템으로 전송한다. 스니핑 탐지시스템은 수신된 ICMP reply패킷을 분석하여 침입 host에 대한 침입 정보를 알아낸다. 스니핑 탐지 시스템에서 알아낸 정보는 콘솔모드의 문자셋이기 때문에 사용자가 침입 host에 대한 침입 정보를 파악하기가 힘들다. 따라서 탐지 시스템에서 분석된 내용을 스니핑 관리자 시스템으로 전송하면 스니핑 관리자 시스템은 탐지 시스템에서 수신된 data를 사용자가 보기 쉬운 형태로 재조합한다.

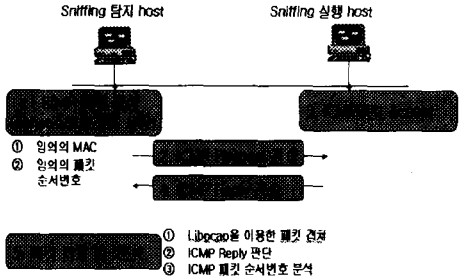
[그림 1]은 스니핑 탐지 및 관리도구의 전체 구성도이다.



[그림 60] 스니핑 탐지 및 관리 도구의 전체 시스템 흐름도

3.3 스니핑 탐지 시스템

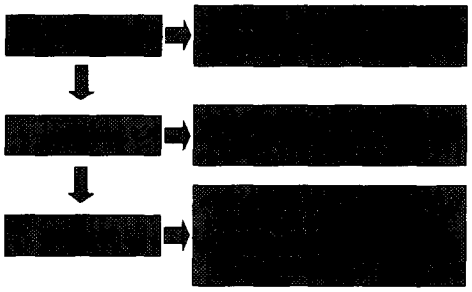
스니핑 탐지 시스템에서는 libnet라이브러리를 이용하여 실제 거짓 패킷을 만들고 libpcap라이브러리를 이용하여 캡처된 패킷을 분석함으로써 침입을 탐지한다.



[그림 61] 스니핑 탐지 시스템 모듈 흐름도

스니핑 탐지 시스템 모듈 흐름도는 [그림 2]와 같다. 위의 그림을 살펴보면 우선 스니핑 탐지 host에서 같은 LAN상에 도달할 수 없는 임의의 MAC 주소와 패킷 sequence number로 거짓 패킷을 생성한다. 이렇게 생성된 패킷을 ICMP request를 이용하여 스니핑이 의심되는 host에 송신한다. 만약 ICMP request패킷을 송신한 host가 스니퍼로서 promiscuous mode로 동작하고 있다면 자신의 MAC 주소와 같지 않은 ICMP request 패킷을 받아들이고 이에 대한 응답으로 ICMP reply신호를 스니핑 탐지 host에 보낸다. 스니핑 탐지 host는 libpcap라이브러리를 이용하여 ICMP reply패킷을 캡처하고 분석하여 분석된 패킷의 sequence number가 ICMP request의 sequence와 같은지 비교한 후 같다면 수신된 패킷은 스니퍼가 보낸 패킷이다. 위의 과정으로 스니핑 탐지 시스템은 침입을 탐지한다.

[그림 3]은 스니핑 탐지 시스템의 주요 모듈이다.

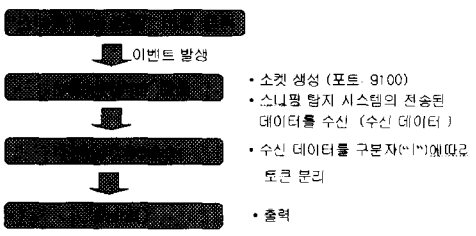


[그림 62] 스니핑 탐지 시스템 모듈

main함수에서는 libpcap라이브러리[9]를 이용하여 자신의 이더넷 장치를 promiscuous mode설정한 후 외부로부터 수신되는 패킷을 캡처할 준비한다. send_icmp은 libnet라이브러리를 이용하여 거짓 패킷을 생성하는 부분으로 이 함수에서 임의의 sequence number를 ICMP패킷에 삽입하여 스니핑이 의심되는 host로 전송한다. print_pkt함수는 침입 host로부터 전송된 ICMP reply패킷을 분석하여 수신된 패킷이 침입 host로부터 전송된 패킷이 침입 host에서 수신된 패킷인지 여부를 확인하여 맞다면 ICMP reply를 통해 수신된 침입정보를 UDP소켓으로 관리자 시스템으로 전송된다.[10]

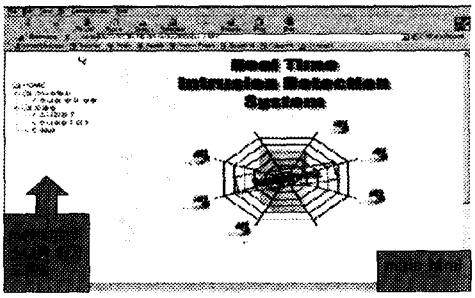
3.4 스니핑 관리자 시스템

스니핑 관리자 시스템은 자바 애플릿으로 구현하여 출력정보를 웹 브라우저상에 나타나도록 구현하였다. 그리고 이는 KISA의 침입 탐지 시스템 보안등급 규정에 기반하여 구현하였다. [그림 4]는 스니핑 관리자 모듈의 흐름도 이다.



[그림 63] 스니핑 관리자 모듈

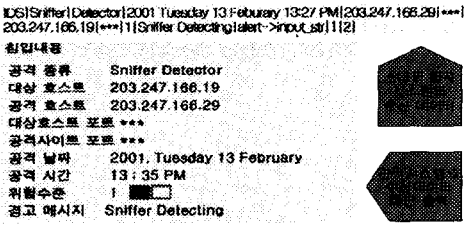
탐지 시스템에서 전송된 침입자에 대한 침입정보가 관리자 시스템으로 전송되면 관리자 시스템에 msgListener 이벤트를 발생시킨다. 이 함수에서 UDP소켓을 열어 탐지 시스템으로 부터의 스니퍼에 대한 정보를 수신하고 StringTokenizer함수로 수신 데이터의 토큰을 분리하여 브라우저상에 스니퍼의 IP, 침입날짜, 침입시간등을 출력한다.



[그림 64] 스니핑 관리자 시스템의 초기화면

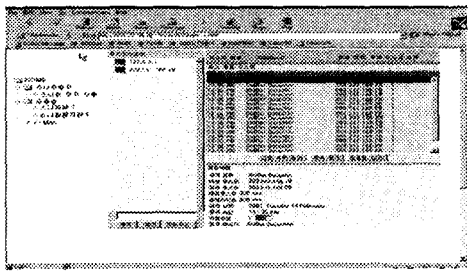
3.5 스니핑 탐지 및 구현도구의 실행 결과

[그림 6]은 스니핑 탐지 시스템의 결과와 스니핑 관리자 시스템의 출력 결과를 비교한 것이다.



[그림 65] 스니핑 탐지 시스템과 관리자 시스템의 출력 결과 비교

[그림 6]에서처럼 스니핑 관리자 시스템에서 ICMP reply패킷을 분석한 토큰 형태의 침입날짜, 침입시간, 침입자의 IP, 침입당한 IP등의 정보를 관리자 시스템으로 전송하여 브라우저상에 보기쉽게 나타낸다.



[그림 66] 스니핑 관리자 시스템의 출력 결과

III . 결론 및 향후과제

본 논문에서는 다양한 해킹 기법들 중 스니핑을 이용한 해킹을 탐지하여 침입자에 대한 침입정보를 브라우저에 나타내는 스니퍼 탐지 및 관리도구를 개발하였다. 스니핑을 탐지하는 도구들이 몇몇 있지만 본 논문에서는 libnet, libpcap라이브러리를 직접 사용하여 침입을 탐지하는 기능을 구현하였고 KISA(한국정보보호센터)의 침입탐지 시스템 등급 규정에 기반한 웹상의 관리자 시스템 기능까지 구현하였다.

스니핑 탐지 및 관리도구는 IDS(침입탐지시스템)의 일부 기능으로 추가가 가능하며 Cron에 등록하여 주기적으로 침입을 탐지할 수 있도록 활용할 수 있다.

본 논문에서는 유선환경에서 스니핑을 탐지하는 기능만을 구현하였지만 최근 무선 인터넷의 성장과 무선인터넷의 활용도가 커짐에 따라 향후 무선 환경에서의 침입 탐지 시스템을 개발할 예정이다.

참고문헌

[1] [해킹 피해 사례 통계자료] http://www.cyber118.or.kr

[2] [해킹기법] exploit017 "리얼해킹" 파워북 2001.1.6

[3] [TCP] 김화종 "컴퓨터 네트워크 프로그래밍" 홍릉과학 출판사 2000.1.27

[4] [TCP 헤더] Doyle, Jeff "Routing TCP-IP, Volume II (CCIE Professional Development series) (1st Edition)" HARDCOVER Cisco Press April - 2001

[5] [IP] W.Ricard stevens TCP/IP Illustrated Volume1 ADDISON-WESLEY

[6] [스니핑] Dr x "The Complete Hacker's Handbook" Carlton Books, Ltd. September - 2000

[7] [promiscuous mode] http://www.certcc.or.kr/paper/tr2000/2000-07/tr2000-07.htm#1

[8] [KISA 침입탐지 시스템 등급 규정] http://www.kisa.or.kr/

[9] [libpcap라이브러리] Stevens, W. Richard "Unix Network Programming" Prentice-Hall 1997.7

[10] [리눅스] Mann, Scott "LINUX TCP-IP Network Administration (1st Edition)" Prentice Hall PTR August - 2001