NFR을 이용한 네트워크 침입 탐지

최선철*, 차현철**
* 동산 여자 전산 고등학교, ** 동양대학교 컴퓨터 공학부
(qna@dreamwiz.com, hccha@phenix.dyu.ac.kr)

A Detection Method for Network Intrusion using the NFR

Seon-Cheol Choi, Hyun-Chul Cha
Dongsan Women's Computer High school,
School of Computer Engineering, Dongyang University

Abstract

In this paper, we have illustrated implementations and there results of network attacks and detections. We consider two attacks, smurf attack and network mapping attack, which are one of the typical intrusions using the ICMP. The NFR™ is used to capture all of our interesting packets within the network traffic. We implement the smurf and network mapping attacks with the UNIX raw socket, and build the NFR's backend for it's detection. The N-Code programming is used to build the backend. The implementing results show the possibility of preventing illegal intruding to network systems.

I. 서론

침입(intrusion)이란 네트워크를 통한 데이터의 전송에 관련하여 비 인가된 사용자가 자원의 무결성(integrity), 기밀성(confidentiality), 가용성(availability)을 저해하는 일련의 행동들을 말하며, 침입 탐지(intrusion detection)란 컴퓨터 시스템에 대한 침입을 식별하고 격리시키기 위한 시도를 의미하는 보안(security) 기술을 말한다[1]. 또한, 침입 탐지 시스템(IDS; Intrusion Detection System)은 컴퓨터와 네트워크 시스템에서 이러한 침입 행위를 탐지하는 시스템을 말하며, IDS는 호스트 기반(H-IDS; host-based IDS) IDS와 네트워크 기반 IDS(N-IDS; Network-based IDS)로 분류할 수 있다. H-IDS는 운영체제에 의해 생성되는 로그(log)를 감사자료로 삼는데 비해 N-IDS는 네트워크상의 실제 패킷들의 내용을 검사하여 이를 감사자료로 사용한다[2,3]. 네트워크에 대한 비중과 중요성이 날로 증가하고 있는 오늘날, N-IDS를 연구하고 개발하는 것이 현재의 추세이며, 이러한 종류의 IDS로는 NFR, NSM, DIDS, EMERALD, NetSTAT 등이 있다[4,5].

본 논문에서는 여러 가지 네트워크 침입 중 ICMP를 이용한 공격의 종류와 특징들을 알아보고, 로우 소켓(raw socket)을 사용하여 침입 프로그램을 구현하였으며, N-Code 프로그래밍을 통해 NFR™ backend를 만들어 이의 탐지를 구현하여 봄으로써 해킹침해 예방의 가능성을 모색하여 보고자 한다.

논문의 구성은 다음과 같다. 1장의 서론에 이어 2장에서는 ICMP를 이용하는 네트워크 침입과 그 특징들을 살펴본 후 공격과 탐지 프로그램의 구현에 대해 설명한다. 3장에서는 구현된 프로그램들을

실제 네트워크 환경에서 실시한 테스트와 테스트 결과를 기술하였으며, 마지막으로 4장에서는 결론과 향후 연구 과제를 다루었다.

II. ICMP를 사용하는 공격과 탐지

2.1 ICMP 공격의 종류와 특징

현재, 인터넷의 표준 프로토콜로 사용되고 있는 TCP/IP는 패킷 인증 과정이 없고 전송되는 패킷의 내용이 중간에서 읽혀질 수 있는 등의 문제점을 가지고 있어 많은 공격의 대상이 되고 있다. 이들 공격들은 사용되는 프로토콜에 따라 분류해 보면 IP 공격, TCP 공격, UDP 공격, ICMP 공격, SMTP 공격 등으로 나누어 볼 수 있다[2]. 이 중 특히, ICMP 공격은 패킷 전송 중 에러가 발생하였을 때 발신지 호스트에게 이 상황을 보고하여 발신지에서 이에 대한 적절한 처리를 할 수 있게 하는 기법을 제공하는 프로토콜인 ICMP를 이용하는 공격을 말한다[6,7]. ICMP 공격의 구체적 종류로는 smurf 공격, ping-of-death 공격, 백 도어(back-door)의 취약성을 이용한 Loki 공격 등이 있으며, 실제 공격을 수행하기 전에 네트워크에 속한 호스트들의 상태와 취약점을 파악하기 위해 사용되는 network mapping도 ICMP 공격의 한 형태이다[8,9]. 본 논문에서는 이 중 network mapping과 smurf 공격을 연구 대상으로 한다.

Network mapping 공격은 일반적으로 공격자가 단일 혹은 소수의 broadcast echo request를 네트워크 상에 전송하고 이 요구에 대한 echo reply들로 작동 중인 호스트들을 확인하는 특징이 있다. 이 때, echo reply를 보내오는 호스트는 작동 중의 상태이며 따라서 공격의 대상이 될 수 있는 것이다. 소수의 지연된 broadcast echo request가 목표 시스템에 어떤 문제를 야기 시키는 것은 않지만 실제 공격의 전조로서 흔히 이용된다.

Smurf 공격은 서비스 거부 공격의 한 가지 형태이며 공격의 매개 역할을 하는 네트워크(intermediary network)와 공격 목표 시스템 쌍방에 극도의 트래픽 혼잡을 유발하는 영향을 미치게 된다. 공격자는 IP 근원지(source) 주소를 목표 시스템의 IP 주소로 위장한 브로드캐스트 echo request를 매개 네트워크에 보내는 것으로 공격을 시작하며 시간 지연 없이 반복하여 보냄으로써 매개 네트워크상의 여러 시스템들은 엄청난 echo request에 응답하느라 자원을 소비하게 하고, 목표시스템의 경우 궁극적으로 echo replies에 의해 가용 자원의 고갈을 맞도록 한다. 이 때, smurf 공격은 특정 네트워크를 향한 많은 broadcast ICMP echo request 패킷들이 짧은 기간 내에 발생하는 반면, network mapping 공격은 소수의 broadcast ICMP echo request 패킷들이 비교적 긴 시간에 발생하는 특징을 가진다. 이러한 network mapping과 smurf 공격의 원리는 다음의 그림 1과 같다. 그림 1에서 공격자가 보낸 broadcast echo request에 대한 reply들이 공격자 자신에게 돌아오는 경우는 network mapping 공격이 되며 공격 목표 호스트에게로 보내질 경우가 smurf 공격이 된다.

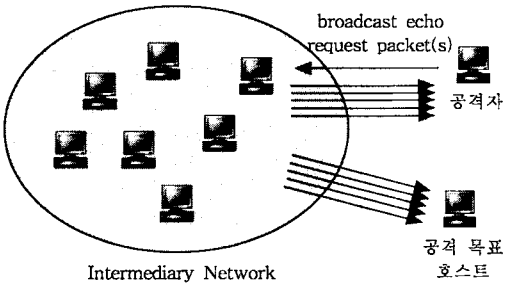


그림 1. Network mapping 공격과 smurf 공격

이들 두 가지 ICMP 공격의 탐지는 브로드캐스트 주소를 갖는 ICMP echo request 패킷을 찾는, 즉, IP 헤더의 10번째 바이트인 protocol 필드가 1(ICMP)이고 17-20번째 바이트인 목적지 주소(destination address)필드가 255(broadcast)이며 ICMP 헤더의 첫 번째 필드인 TYPE 필드가 8(echo request)인 패킷을 찾아내는 것으로 가능하다.

2.2 공격 프로그램의 구현

Network mapping 및 smurf 공격을 UNIX 상에서 C 언어를 사용하여 구현하였다. 특히, smurf 공격의 경우 근원지 IP 주소를 공격자가 아닌 목표 호스트로 위장할 수 있어야 하므로 로우 소켓을 사용하여 IP 헤더의 값들을 직접 선택할 수 있도록 하였다. 또한, 명령어 라인 상에서 전송할 패킷의 개수를 직접 입력하고 프로그램은 사용자가 원하는 개수만큼의 패킷을 전송할 수 있도록 구현하였다 [10,11].

2.3 탐지 프로그램의 구현

NFR사에서 개발한 NFR™은 네트워크 상에 송수신 중인 패킷을 수집하고 프로토콜을 해석하여 감사자료로 사용하는 구조로, N-Code라는 강력한 스크립트 언어를 사용하여 어떠한 종류의 가상 사건이라도 규정할 수 있도록 해주어 사용자 사건 설정에 보다 유연하다는 장점을 지니고 있다. NFR에서는 모니터링을 원하는 트래픽의 패턴을 N-Code 스크립트 언어를 사용하여 backend를 작성하여야 하며 서로 관련 있는 유사한 backend들을 모아 package를 구성하여야 한다. 하나의 backend는 설명(description) 파일, 환경(configuration) 파일, 필터(filter)와 record N-Code 파일 등 3개의 파일로 구성된다[12].

본 연구에서 구현한 backend의 이름은 icmp_csc로 명명하였으며, 이 backend를 구성하는 설명 파일, 환경 파일, 대상필터 파일의 이름은 각각 icmp_csc.desc와 icmp_csc.cfg 및 icmp_csc.nfr로 하였다. 설명 파일인, icmp_csc.desc는 해당 backend에 관련된 설명을 기술한 것으로 backend의 실행과는 직접적인 관련이 없으며, 생략도 가능하다. 환경 파일인 icmp_csc.cfg는 NFR의 초기 실행 시 이 backend가 실행될 것 인지의 여부, GUI화면에 나타낼 backend의 이름, 히스토그램 및 리스트 두 가지 방식 중 채택될 레코딩 방식, 질의 항목, 수집된 자료를 저장할 저장 장치상의 패스 등을 지정하여야 하며, 본 backend에서는 두 가지 기록방식 중 리스트방식을 채택하였다. 필터 파일인 icmp_csc.nfr은 네트워크 트래픽 중에서 필요한 정보를 걸러내고 기록하는 역할을 담당하며 NFR 내에서 직접 컴파일 되고 실행된다. 이 필터 파일에서는 icmp_csc backend가 기록할 패킷이 IP 헤더의 TYPE 필드가 1인 ICMP 패킷 중에서 ICMP 패킷의 TYPE이 0(혹은 8)이고 CODE 필드가 0인 echo

reply(request) 패킷을 선택한 후, 해당 패킷의 검출 시각과 발신지 IP주소, 도착지 IP 주소, ICMP 패킷의 TYPE, CODE 필드의 값 등을 기록하도록 하였다.

III. 실험 및 결과

3.1 실험 환경

본 논문에서 구현한 ICMP 공격 및 탐지의 실험은 10Base-T방식의 Fast Ethernet 근거리 통신망으로 연결된 세 대의 호스트 상에서 수행되었다. 실험에 사용된 호스트들의 환경은 표 1과 같다.

표 1. 실험 호스트 환경

구분 \ 호스트	공격 호스트	목표 호스트	탐지 호스트
도메인 명	ice.dyu.ac.kr	netlab.dyu.ac.kr	netopia.dyu.ac.kr
IP 주소	192.168.5.24	192.168.5.171	192.168.5.37
플랫폼	Sun Sparc Station 5	Pentium PC	Sun Sparc Ultra 1
OS	Sun Solaris 2.5.1	Excel Linux 6.2	Sun Solaris 2.6
주/보조 기억장치	32M / 1.05GB	64M / 10GB	128M / 2.16GB

3.2 실험 결과 및 분석

ICMP 공격을 구현한 프로그램인 icmp_attack으로 2개의 echo request 메시지를 192.168.5.* 네트워크상의 브로드캐스트 주소로 발송한 모습은 그림 2와 같다. 이 때, 공격 호스트 ice의 실제 IP 주소인 192.168.5.24를 192.168.5.171(netlab)로 위장하였다.

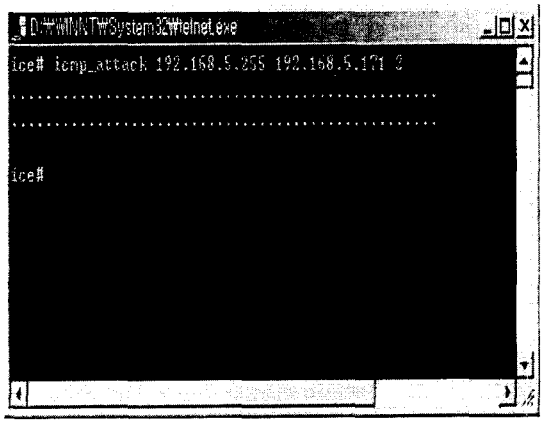


그림 2. 공격 프로그램의 실행 예

탐지 호스트인 netopia에서 실행된 NFR 상의 icmp_csc backend로 필터링 한 ICMP 패킷들 중 브로드캐스트 주소로 발송된 echo request 패킷만을 검출한 결과는 그림 3과 같다. 그림 2의 공격 프

로그램이 두 개의 브로드캐스트 echo request 패킷을 전송하였으며 전송된 패킷이 backend에 의해 탐지될 수 있음을 보여준다.

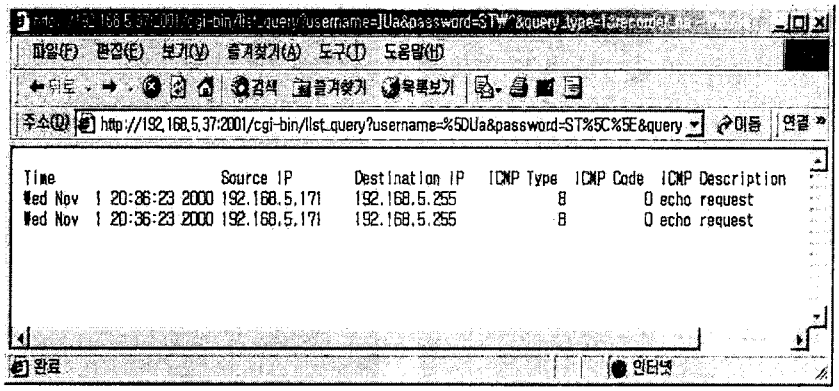
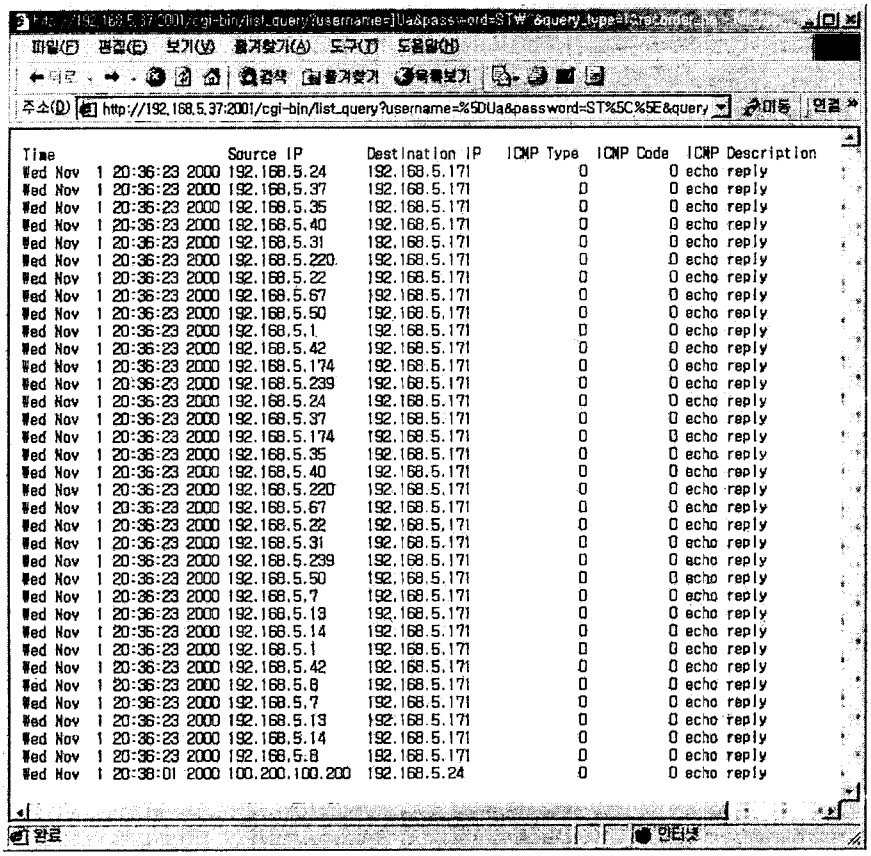


그림 3. 브로드캐스트 주소로 발송된 ICMP 패킷의 탐지

이러한 공격의 영향을 알아보기 위해 되돌아오는 모든 ICMP echo reply 패킷들을 검출하여 보았다. 그림 4는 공격의 결과로 192.168.5.* 네트워크 내에 속한 호스트들에 의해 생성된 echo reply들을 보여주며 17개의 호스트들로부터 각각 2개의 echo reply가 응답되어 모두 34개의 echo reply 패킷들이 생성되었음을 보여준다.



Time	Source IP	Destination IP	ICMP Type	ICMP Code	ICMP Description
Wed Nov 1 20:36:23 2000	192.168.5.24	192.168.5.171	0	0	echo reply
Wed Nov 1 20:36:23 2000	192.168.5.37	192.168.5.171	0	0	echo reply
Wed Nov 1 20:36:23 2000	192.168.5.35	192.168.5.171	0	0	echo reply
Wed Nov 1 20:36:23 2000	192.168.5.40	192.168.5.171	0	0	echo reply
Wed Nov 1 20:36:23 2000	192.168.5.31	192.168.5.171	0	0	echo reply
Wed Nov 1 20:36:23 2000	192.168.5.220	192.168.5.171	0	0	echo reply
Wed Nov 1 20:36:23 2000	192.168.5.22	192.168.5.171	0	0	echo reply
Wed Nov 1 20:36:23 2000	192.168.5.67	192.168.5.171	0	0	echo reply
Wed Nov 1 20:36:23 2000	192.168.5.50	192.168.5.171	0	0	echo reply
Wed Nov 1 20:36:23 2000	192.168.5.1	192.168.5.171	0	0	echo reply
Wed Nov 1 20:36:23 2000	192.168.5.42	192.168.5.171	0	0	echo reply
Wed Nov 1 20:36:23 2000	192.168.5.174	192.168.5.171	0	0	echo reply
Wed Nov 1 20:36:23 2000	192.168.5.239	192.168.5.171	0	0	echo reply
Wed Nov 1 20:36:23 2000	192.168.5.24	192.168.5.171	0	0	echo reply
Wed Nov 1 20:36:23 2000	192.168.5.37	192.168.5.171	0	0	echo reply
Wed Nov 1 20:36:23 2000	192.168.5.174	192.168.5.171	0	0	echo reply
Wed Nov 1 20:36:23 2000	192.168.5.35	192.168.5.171	0	0	echo reply
Wed Nov 1 20:36:23 2000	192.168.5.40	192.168.5.171	0	0	echo reply
Wed Nov 1 20:36:23 2000	192.168.5.220	192.168.5.171	0	0	echo reply
Wed Nov 1 20:36:23 2000	192.168.5.67	192.168.5.171	0	0	echo reply
Wed Nov 1 20:36:23 2000	192.168.5.22	192.168.5.171	0	0	echo reply
Wed Nov 1 20:36:23 2000	192.168.5.31	192.168.5.171	0	0	echo reply
Wed Nov 1 20:36:23 2000	192.168.5.239	192.168.5.171	0	0	echo reply
Wed Nov 1 20:36:23 2000	192.168.5.50	192.168.5.171	0	0	echo reply
Wed Nov 1 20:36:23 2000	192.168.5.7	192.168.5.171	0	0	echo reply
Wed Nov 1 20:36:23 2000	192.168.5.13	192.168.5.171	0	0	echo reply
Wed Nov 1 20:36:23 2000	192.168.5.14	192.168.5.171	0	0	echo reply
Wed Nov 1 20:36:23 2000	192.168.5.1	192.168.5.171	0	0	echo reply
Wed Nov 1 20:36:23 2000	192.168.5.42	192.168.5.171	0	0	echo reply
Wed Nov 1 20:36:23 2000	192.168.5.8	192.168.5.171	0	0	echo reply
Wed Nov 1 20:36:23 2000	192.168.5.7	192.168.5.171	0	0	echo reply
Wed Nov 1 20:36:23 2000	192.168.5.13	192.168.5.171	0	0	echo reply
Wed Nov 1 20:36:23 2000	192.168.5.14	192.168.5.171	0	0	echo reply
Wed Nov 1 20:36:23 2000	192.168.5.8	192.168.5.171	0	0	echo reply
Wed Nov 1 20:36:01 2000	100.200.100.200	192.168.5.24	0	0	echo reply

그림 4. 공격 결과 나타나는 echo reply 패킷들

IV. 결론

우리 생활에 커다란 변화를 가져다주는 정보화 혁명은 네트워크를 통한 정보 접근의 용이성 등을 특징으로 하고 있으며, 해킹침해에 대응하기 위한 침입탐지는 네트워크 보안의 중요한 한 요소가 된다.

본 연구에서는 근래 많이 시도되고 있는 서비스 거부 공격의 하나인 ICMP를 사용하는 침입의 전형적 패턴인 network mapping 및 smurf 공격과 이를 탐지하는 IDS를 구현하여 보았다. 브로드캐스트 주소로 발송된 ICMP의 echo request는 목표 네트워크상의 많은 호스트들로 하여금 echo reply 패킷을 생성케 하였고 이들은 NFR에서 모두 탐지될 수 있었다. N-Code를 사용하여 작성한 backend는 정의된 침입 패킷을 네트워크 상에서 정확히 탐지해냈으며, 해킹침해 예방의 가능성을 확인시켜 주었다.

본 연구의 향후 연구과제는 공격 패킷이 탐지되었을 때 사용자에게 자동으로 이를 알려주는 경고 기능의 구현이며, 더불어 ICMP 공격의 또 다른 종류인 ping-of-death 공격과 Loki 공격의 실행 및 이의 탐지 구현이다.

참고문헌

[1] 정진욱, "초고속정보통신기반 구축에 따른 시스템 및 네트워크 시큐리티", *정보과학회지*, 14권 3호, pp.38-49, 1996.

[2] 이철원 외 5인, "국내·외 정보보호관련 연구 동향", *정보과학회지*, 15권 4호, pp. 6-13, Mar., 1997.

[3] 임휘성, "윈도우시스템에 대한 원격 서비스거부공격과 대책", *http://www.certcc.or.kr/concert/cs9802/03/index.htm*

[4] 김병구·정태명, "침입탐지 기술의 현황과 전망", *정보과학회지*, 18권 1호, pp. 29-39, Jan., 2000.

[5] 강일련, "차세대 보안솔루션 IDS", *http://icop.wellnet.co.kr/ids/*

[6] Duglas E. Comer, *Computer Networks and Internets*, Prentice-Hall International, Inc., 1997.

[7] 박창민, "pc통신상에서의 정보 보호", *http://member.barn.co.kr/bitbob/unix/part1/hacking/pc.html*

[8] 이상렬, "해킹 공격 & 대응 ", *http://www.secuinfo.com/worldwide/hack/hack2_6.asp?enter=hack*

[9] Vici Irwin, "Advanced Intrusion Detection and Packet Filtering", *Cisco Systems Inc.*, 1999.

[10] Mixter , "A brief programming tutorial in C for raw sockets", *http://mixter.warrior2k.com/rawip.txt*

[11] 박성호(역), "BeeJ's Guide to Network Programming", *http://home.hanmir.com/~wmagic/해킹/네트워크프로그래밍.html*

[12] Marcus J. Ranum, "NFR Documentation" *http://www.nfr.com/nfr/*