情 報 保 護 學 會 誌
第 16 卷 第 1 號, 2006. 2

전통적인 네트워크 해킹 기법과 기술적 대응방안

김 태 훈, 최 호 성, 김 성 은, 김 주 현

요 약

하나의 네트워크가 보안적으로 완전해지기 위해서는 외부 네트워크에 서비스를 제공하는 서버뿐만 아니라 내부적 사용을 위한 다수의 클라이언트에 대한 보안 취약점도 최소화 시켜야 한다. PC의 하드웨어적 성능 발전은 개인의 정보처리 능력을 획기적으로 향상시킨 순기능도 있는 반면 웜바이러스 감염과 같은 보안적 문제에 노출되었을 경우 전체 네트워크를 마비시킬 수 있는 치명적인 위협요소가 되는 역기능도 있다. 본고는 PC를 대상으로 하는 전통적인 네트워크 해킹기법과 이에 대한 대응 솔루션을 분석하여 보다 효율적인 방법으로 네트워크의 보안성을 증대 시킬 수 있는 기술적 방안에 대해 기술한다.

Ⅰ. 서 론

IPv4를 기반으로 이루어진 현재의 인터넷 네트워크는 1985년 로버트 모리스의 논문에서도 언급되었듯이 구조적 결함을 가지고 있다. 즉, TCP/IP 패킷의 헤더 정보는 Checksum 값만 재 계산할 경우 손쉽게 변조가 가능하다. 흔히 IP Spoofing 공격으로 알려진 해킹 기법은 이러한 구조적 취약점을 이용하여 출발지 주소를 변조하는 기법을 말하는 것이다. 만일, A라는 클라이언트와 서버 B가 서로 신뢰관계이고 서버 B에 직접적인 접근이 사실상 어려운 해커 C는 서버 B에 접속하기 위하여 A의 IP주소로 위장하여 접속할 수 있다. TCP 프로토콜의 경우 Session단위의 접속이 이루어지기 때문에 TCP Sequence Number Guessing Attack 기법이 병행된다.

또한 Packet Sniffing 공격은 네트워크에 돌아다니는 패킷을 무차별적으로 수신하여 분석함으로써 타 시스템의 트래픽을 분석하고 정보를 유출하는 형태의 해킹 기법이다. 그러나 Packet Sniffing 공격기법은 악의적인 목적 이외에 네트워크 트래픽 분석도구 및 IDS와 같은 보안장비에서도 활용되는 기술이다. 보안적 목적을 이루기 위해 필요에 따라 모든 트래픽을 모니터링 해야 할 수도 있기 때문이다.

이러한 전통적인 공격 기법들은 최근 감소하는 추세지만 (인터넷침해사고지원대응센터 2005년 통계 기준) 절대적인 수치면에서는 아직도 높은 수치를 유지하고 있다. 이는 공격기법에 있어 보다 전문성을 요구하고 실제로 성공시키기 어려운 부분이 많기 때문이다. 또한, 이러한 공격방식의 주된 목표는 대상 시스템에 불법적으로 침입하여 정보를 직접적으로 수집/조작/변조하기 위한 것일 가능성이 높다. 이는 단 한 건이 발생하더라도 매우 큰 정보유출 사고로 직결 되는 것이므로 심각성이 매우 크다.

전체 사용 운영체제의 90%이상을 점유하고 있는 Microsoft사의 Windows 운영체제 역시 이러한 문제로부터 자유로울 수 없으며 웜 바이러스를 비롯한 다양한 악성코드로 인한 추가적인 문제까지 고려하여야 하는 상황이다. 표 1에서 보는 바와 같이 인터넷침해사고대응지원센터에서 집계한 통계자료에 의하면 최근 6개월간 국내에서 발생하고 있는 해킹피해 중 Windows 운영체제가 가장 많은 피해 건수를 일으키고 있다.

이러한 문제의 가장 큰 원인은 PC의 정보 유출 사고를 유발시키는 웜바이러스 및 기타 악성 코드가 전통적인 네트워크 해킹 기법을 적절히 이용하여 동작하기 때문이다. 대부분의 웜바이러스들은 자신을 복제하기 위해서 Buffer Overflow와 같은 시스템 해킹 기법 및 Network Scan/Spoofing 공격을 함께 병행

* (주)싸이웍스 ({thkim, chs, hyunni}@syworks.com)

하고 있다. 결과적으로 로컬 네트워크에 존재하는 모든 Windows 운영체제 기반 PC들은 잠재적으로 내부의 보안적 위협요소로 돌변할 수 있다. 더 큰 문제는 이러한 문제에 대한 표준화된 대응 체계가 부족하다는 것이다.

본고에서는 Windows 운영체제 기반 PC로 인한 네트워크 보안 문제를 해결하기 위해 일반적인 솔루션에 대해 살펴보고, 각각의 구조적 접근방법에 따른 기술적 특징을 분석하여 적절한 대응방안 및 향후 발전 방향에 대해 기술한다.

(표 1) 2005년도 하반기 운영체제별 해킹피해 건수

운영체제	2005년						합계
	7월	8월	9월	10월	11월	12월	
Windows	1,089	778	378	509	366	675	3,795
Linux	520	1,690	384	226	274	62	3,156
Solaris	0	15	2	5	22	1	45
기 타	6	8	109	7	5	1	136
합 계	1,615	2,491	873	747	667	739	7,132

II. 전통적인 네트워크 해킹기법

PC를 활용하여 내부 사용자가 보안 문제를 일으키는 경우보다는 사용자 자신도 모르는 사이 감염된 웜바이러스 및 악성 코드로 인해 네트워크 해킹을 시도할 수도 있다. 이는 전통적인 네트워크 해킹기법을 이용한 웜바이러스의 동작 원리를 분석함으로써 문제점을 파악할 수 있다.

2.1 Network Scan 공격

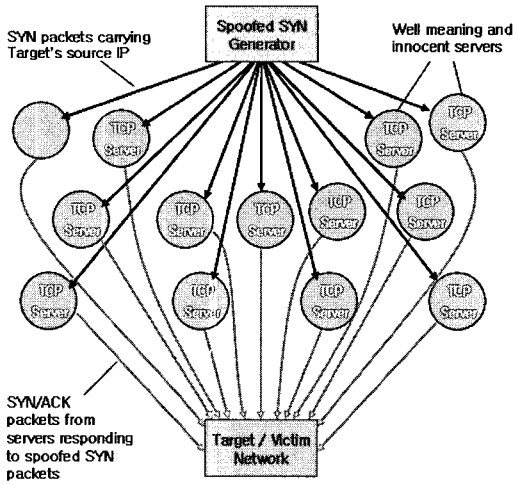
Networks Scan은 공격에 앞서 공격에 필요한 정보를 수집하는 일련의 과정을 통칭하여 말할 수 있다. 가령, 목적 시스템의 정보를 유출하려는 악의적 사용자는 대상 시스템이 외부 네트워크와 인터페이스 하는 IP주소 및 port번호와 같은 정보를 추출하여야 한다. 만일, 이러한 부분에 대해서 사전 정보가 없을 경우 공격자는 기본 정보 수집을 위한 Network Scan 공격을 시작한다. 이 스캔 공격의 결과를 근거로 접근가능 정보를 얻게 되고, 해당 정보(port번호)를 통한 보안적 취약점이나 결함을 활용하여 관리자 권한을 얻게 된다. 이 때, 해당 port로 관리자의 권한을 얻을 수 있는지 검사하기 위한 코드를 전송하여 결과를 얻는 것도 스캔 공격이라고 할 수 있을 것이다. 대부분의 웜 바이러스는 자신을 복제하기 위해서 로컬 및 주변 네트워크 전체에 대해서 스캔 공격을 실시한다. 이 과정에서 일반적인 스캔 공격과의 차이점은 특정 포트에 대해서만 접근 가능 유무를 검사하며 경우에 따라 포트 검사를 하지 않는 대신 ICMP Echo request만을 전송하기도 한다. 이러한 스캔은 한 호스트에 집중된 스캔 트래픽을 유발하는 것이 아니라, 하나의 스캔 정보를 다수의 시스템에 무작위로 전송한다는 특징이 있다. 이러한 동작원리로 인한 가장 큰 문제점은 불필요한 내부 트래픽이 증가한다는 것이다. 기존의 보안솔루션들을 활용하여 탐지 및 일부 제어가 가능하지만 다수의 시스템에서 동시다발적으로 발생하는 경우 기존의 보안솔루션으로는 문제를 궁극적으로 해결할 수 없다. 더욱이 최근 PC의 하드웨어 성능은 저가형 서버보다 우수하기 때문에 단 시간에 전체 네트워크를 마비시키는 결과를 초래한다. 대표적 사례로는 지난 2003년 1월 25일의 인터넷 대란을 들 수가 있다.

2.2 IP Spoofing 공격

IP Spoofing 공격은 서버가 동일한 네트워크 환경 또는 Netmask를 가진 클라이언트에게만 다양한 서비스를 하고, 그렇지 않은 클라이언트에게는 서비스를 제한하도록 설계되어 있을 경우, 해커가 외부망에서 서버에 침투함에 있어서 내부 클라이언트인 것처럼 IP를 속여서 서버에 접근하거나, 일반적인 DoS공격에서 추적을 피하기 위해서 사용되는 공격 기법이다.

IP Spoofing 공격의 최초 등장배경은 복잡한 사용자 인증체계를 우회하여 비인가자가 특정 자원이나 정보에 접근하기 위한 것이었으나, 최근에는 서비스거부(Denial of Service, DoS), 분산서비스거부(Distributed Denial of Service) 공격에 활용되고 있다.

웜바이러스와 같은 악성 코드에 감염된 PC의 사용자가 별도의 대응시스템을 구비하지 않았을 경우, 대부분 감염 사실조차 인지하지 못하기 때문에 특별한 외적 증상이 어느 정도 발생하여야 문제를 해결하려 할 것이며 관련 지식이 없는 사용자는 문제를 방치한 채 PC를 사용하게 되어 더 큰 문제를 야기할 수 있다. 만일, 악성 코드가 스스로를 복제하는 것 이외의 코드를 수행할 경우, 개인정보의 유출이나 외부 공격을 위한 경로로 활용될 수도 있다. 그림 1에서 보는 바와 같이 웜바이러스와 같은 악성 코드에 감염된 PC는 다른 해커에 의하여 일시에 특정 서버나 네트워크 장비를 공격하는 PC로 돌변할 가능성이 매우 크다.



〔그림 1〕 IP Spoofing 기법을 이용한 DR-DoS 공격

또한 Land 공격과 같이 비정상적인 트래픽이나 출발지 IP주소가 변조된 공격 패킷을 대상 시스템에 대량으로 전송함으로써 정상적인 운영이 불가능하도록 할 수 있으며, 일부 웜바이러스들은 이러한 DDoS 공격 방법을 활용하여 의도적으로 특정 시스템을 공격하기도 한다. 이 경우 최초 웜바이러스 감염 시에는 그 이상 동작을 하지 않으나 특정 패킷을 수신하거나 정해진 시간이 되면 공격을 시작하기 때문에 그 피해 범위는 더욱 증가하게 된다.

2.3 Packet Sniffing 공격

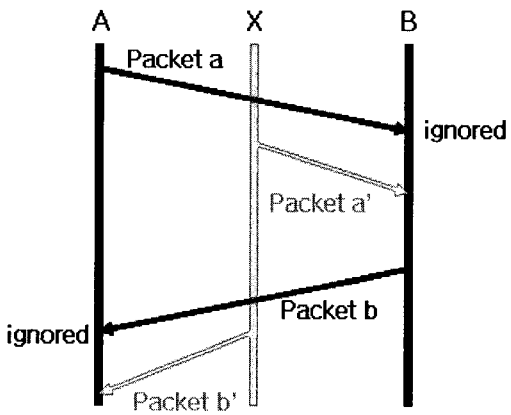
Packet Sniffing 공격은 사전적인 의미와 같이 네트워크상에서 자신이 아닌 다른 상대방들의 패킷 교환을 엿듣는 것을 의미한다. 간단히 말하면 네트워크 트래픽을 도청(Eavesdropping)하는 과정을 스니핑이라고 할 수 있다. 이러한 스니핑을 할 수 있도록 하는 도구를 스니퍼(Sniffer)라고 하며 스니퍼를 설치하는 과정은 전화기 도청 장치를 설치하는 과정과 유사하다.

TCP/IP 프로토콜은 학술적인 용도로 인터넷이 시작되기 이전부터 설계된 프로토콜이기 때문에 보안은 크게 고려하지 않고 시작되었다. 대표적으로 패킷에 대한 암호화, 인증 등을 고려하지 않았기 때문에 데이터 통신의 보안의 기본 요소 중 기밀성, 무결성 등을 보장할 수 없었다. 특히 스니핑은 보안의 기본 요소 중 기밀성을 해치는 공격 방법이다.

그러나 패킷 스니핑 공격은 무작위로 패킷을 수집하고 거기서 정보를 읽어 들이는 공격방법이기 때문에 정보 유출을 목적으로 한 것으로 한정 지을 수 있다. 따라서 네트워크 전체에 대한 안정성 확보라는 측면에서 보면 위협적인 요소는 아니다. 다만, 이로 인한 개인 정보나 특정 서비스에 접근할 수 있는 사용자 계정 정보 유출 사고가 발생할 수 있다. 스위치 허브에서는 이러한 스니핑 공격이 일반적으로 불가능하지만 ARP Spoofing 공격으로 스위치 허브의 정보를 조작한다면 스니핑 공격이 가능해질 수 있다.

2.4 Connection Hijacking 공격

TCP/IP의 Session은 서버와 클라이언트 통신에서 서로 인증을 확인하고, Data를 순차적으로 송·수신하기 위해 항상 Sequence Number를 증가 시키면서 통신을 하는데, 이 Sequence Number를 알게 되면 Server에 별 다른 인증 절차 없이 통신을 할 수 있는 프로토콜의 취약점을 이용하여 공격자가 이를 도용하는 해킹 기법이다. 실시간으로 Sequence Number를 알아내기 위해 먼저 SYN Flooding 또는 ACK Storm 공격기법을 이용하기도 한다.



〔그림 2〕 TCP Connection Hijacking

Ⅲ. 기존 대응 솔루션의 문제점

3.1 네트워크 내·외부 접점에서의 보안 솔루션

외부에서 내부로 이어지는 공격의 경우 방화벽을 통해서 서비스 거부가 되는 현상을 차단할 수 있다. 여기서 언급된 차단이라 함은 TCP Session이 비정상적으로 완료되지 못하는 SYN Flooding 공격의 차단을 의미한다. 또한, 서버의 오동작이나 과부하로 이어질 수 있는 공격 트래픽의 차단을 추가적으로 포

함시킬 수 있을 것이다. 최근 기존의 방화벽을 대체하고 있는 침입방지시스템(Intrusion Prevention Systems, IPS) 역시 이에 대한 대응를 충분히 해줄 수 있으며 오히려 더욱 발전된 메커니즘을 제공한다. 그러나 이러한 솔루션들은 비정상이라고 판단되지 않는 트래픽 유입으로 발생하는 서비스 거부 공격에 대해서는 사실상 대안이 없다고 할 수 있다. 특히, Outbound되는 공격의 경우 더욱 그러하다. 악성 코드를 탐지 및 차단 할 수 있다고 하더라도 내부에서 내부로 이어지는 그 어떤 공격에 대해서도 아무런 대책이 없으며 처리가 불가능하다. 대형 네트워크의 경우 내부에서 관리되는 각각의 네트워크 세그먼트 단위에서 이를 처리할 수 있다. 결과적으로 PC 자체에서 이런 문제를 해결하는 방법이 최선이라고 할 수 있다.

3.2 보안패치와 바이러스 백신 솔루션

웜바이러스나 악성코드에 PC가 자체적으로 대응하기 위해서는 악성코드에 감염되지 않는 것이 최우선이다. 이를 위해서는 보안적 결함이 있는 요소를 제거하고 백신을 설치해야 하는 조건이 갖추어져야 한다. 그러나 이러한 대응 방식은 수동적 조치에 해당한다. 보안적 결함이 알려지고 그로 인한 피해가 발생한 후에 이를 보완할 수 있으며 조치가 가능하다. 따라서, Zero-day 동안에는 아무런 대응도 할 수 없게 된다.

3.3 PC기반의 방화벽/IPS 솔루션

PC기반의 방화벽이나 IPS를 운영함으로 보다 능동적으로 대응할 수 있다. 그러나 이 역시도 한계가 있다. PC자체가 외부에 공격을 수행하는 경우에 대한 대책이 부족하다. 또한, 사용자의 네트워크 접근을 위한 정상적인 프로세스를 통한 공격에 대해서 아무런 제약을 주지 않는다.

3.4 Network Access Control 솔루션

네트워크 접근 제어 솔루션은 허가된 사용자나 PC만이 네트워크에 접속할 수 있도록 제어하여 네트워크의 안정성을 확보하는 방법이다. 보안적으로 안전하지 않을 수 있는 시스템이 무단으로 내부 네트워크를 사용하지 못하도록 할 수 있기 때문에 어느 정도의 네트워크 보안 문제를 해결할 수는 있으나 일단 접근이 허용된 이후에 대해서는 아무런 조치가 불가능하므로 취약점을 갖고 있다.

Ⅳ. 기술적 대응 방안

앞서 설명한 기존 보안솔루션들의 장단점을 고려하여 이상적인 대응 솔루션으로서 호스트 기반의 유해트래픽 제어 솔루션을 살펴 보도록 한다. 호스트 기반의 유해트래픽 제어 기술은 PC에서 비정상적인 트래픽이나 전체 네트워크에 위협을 줄 수 있는 과도한 트래픽 생성을 차단하는 기술이다. 이 기술은 네트워크 세그먼트 단위가 아닌 호스트 단위의 트래픽 제어에 해당되므로 가장 이상적인 방법이라고 할 수 있다. 몇몇 시스템의 문제 때문에 전체 네트워크를 차단할 필요가 없기 때문에 웜 바이러스와 같은 악성코드로 인해 발생하는 피해를 PC 하나로 끝낼 수 있다. 그러나 구현하기가 어려울 뿐만 아니라 안정성 및 다양한 기술적 문제 요소들이 존재하며 단순한 방화벽 기능 뿐만 아니라 QoS(Quality of Service) 기능을 동시에 갖추어야 한다.

4.1 Packet Filtering PC 방화벽 기능

패킷 필터링 방식의 PC 방화벽은 기존의 네트워크 방화벽과 달리 PC내부의 접근을 통제하는 방법에 있어서 차이가 있다. 최근 가장 많이 사용하고 있는 특정 프로세스 단위의 접근을 제어하는 방식보다는 패킷을 직접 필터링 할 수 있는 방식이 더욱 바람직하다. 이를 기반으로 포트단위 접근제어가 가능하여야 하고, 기존에 알려진 비정상 공격 트래픽을 차단할 수 있어야 한다. 여기서 언급한 공격 트래픽은 Outbound되는 공격 트래픽을 말하는 것으로서 IP Spoofing공격을 포함하는 전통적인 네트워크 공격을 말하는 것이다. 즉, 보호의 대상이 되는 클라이언트 자신 조차도 신뢰할 수 없는 것으로 간주할 수 있어야 한다.

4.2 QoS 기능

QoS 기능 또한 IP프로토콜을 기반으로 하고 있는 모든 프로토콜들에 대해서 강제로 대역폭이나 세션 수 등을 제한할 수 있어야 한다. 악성코드로 인해 발생하는 트래픽 폭주현상은 정상적인 패킷의 형태를 가지고 있지만 단위 시간동안 발생시키는 세션의 수가 기하급수적으로 늘어나는 특징을 가지고 있다. 여기에는 세션이라는 단위로 말할 수 있는 TCP/IP 프로토콜뿐만 아니라 ICMP Echo, UDP/IP, Broadcast 트래픽이 모두 포함되어야 한다.

이 두 가지의 기능을 적절히 조합할 경우, PC자체

의 보안적인 문제를 해결하는 것과 동시에 PC가 네트워크 자원을 불필요하게 소모시키거나 네트워크의 안정성을 저해시키는 문제를 해결할 수 있다.

V. 결 론

전통적인 네트워크 공격방법을 활용하는 악성코드의 동작 및 확산을 차단하기 위해서는 결국 문제의 주체가 되는 호스트의 트래픽을 직접 제어하는 방법이 가장 효과적이다. 물론, 악성코드에 감염되지 않는 것이 가장 이상적인 것이라 할 수 있겠으나, Zero-day가 날로 늘어가는 최근의 추세를 감안하면 이 역시 빠른 대응이 이루어지기 힘들다. IPv6 기반의 유비쿼터스 시대가 도래할 경우, 작금의 문제는 더욱 커질 수 밖에 없다. 따라서 향후 개발되는 다양한 플랫폼에서는 이러한 문제를 해결할 수 있는 근본적인 대안을 제시하여야 할 것이다.

특히, PC 및 네트워크에 관한 전문 지식이 부족한 사용자 일수록 보안적인 부분을 등한시 하므로 일련의 모든 보안정책을 사용자가 쉽게 이해하고, 설정 할 수 있도록 자동화 되어야 할 필요성도 있으며, 지속적인 학습과 보안 규칙에 따른 표준화된 관리체계 구축이 절실히 요구된다.

참 고 문 헌

[1] RFC 2990, "Next Steps for the IP QoS Architecture", Nov. 2000

[2] RFC 4301, "Security Architecture for the Internet Protocol", Dec. 2005

[3] RFC 1180, "TCP/IP tutorial", Jan. 1991

[4] Joel Scambray, Stuart McClure, "Hacking Windows 2000 Exposed: Network Security Secrets & Solutions", McGraw-Hill, Nov. 2001

[5] George Kurtz, "Hacking Exposed Linux, 2nd Edition", McGraw-Hill, Dec. 2002

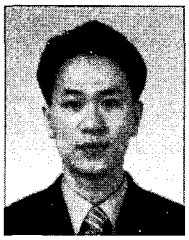
[6] 김상철, "Abnormal IP Packets", 인터넷침해사고대응지원센터 기술문서, May 2002

[7] http://monkey.org/~dugsong/dsniff/

〈著 者 紹 介〉

김 태 훈 (Tae-Hoon Kim)

2003년 2월 : 동국대학교 공과대학 컴퓨터공학과 공학사
1998년 ~ 현재 : (주)싸이웍스 대표이사
관심분야 : PC보안, 유해정보차단

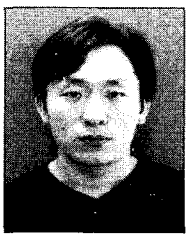


최 호 성 (Ho-Sung Choi)

1998년 2월 : 동양공업전문대학 전기과 졸업
2001년 11월 : 정보통신부장관 표창 수상
2002년 8월 ~ 2003년 12월 : 비트캠프 C/S & Security과정 보안강사
2004년 2월 : 가남출판사 "Windows MFC 정복" 저술.
1999년 1월 ~ 현재 : (주)싸이웍스 기술이사
관심분야 : 윈도우 시스템 보안, 네트워크 보안, PC 보안

김 성 은 (Sung-Eun Kim)

1997년 2월 : 명지대학교 공과대학 컴퓨터공학과 공학사
1997~1999년 8월 : (주)씨엔지 시스템 개발팀
1999년 9월 ~ 현재 : (주)싸이웍스 연구개발팀
관심분야 : PC보안, Client/Server 프로그래밍, 커널모드 드라이버



김 주 현 (Joohyun Kim)

2002년 2월 : 명지대학교 공과대학 기계공학과 공학사
2004년 ~ 현재 : (주)싸이웍스 연구원
관심분야 : Network 보안, Unix/Linux 시스템 보안