Proxy Server를 통한 IP Spoofing 공격과 방어 연구

이보만* · 박대우*

*호서대학교 벤처전문대학원 IT응용기술학과

A Study of IP Spoofing Attack and Defense Through Proxy Server

Bo-Man Lee* · Dea-Woo Park*

*Dept. of Information Technology, Hoseo Graduate School of Venture

E-mail : *bomans@nate.com · *prof1@paran.com

요 약

해외로부터의 Hacking의 특징은 추적 기법을 동원 하더라도 공격자 Real IP 주소를 찾을 수 없기 때문에 수사에 어려움이 큰 것이 현실이다. 이는 공격자가 Proxy Server를 여러 번 거치면서 자신의 IP 주소를 숨기는 IP Spoofing 기법을 사용하기 때문이다. 본 논문에서는 공격자들이 어떻게 IP Spoofing 기법을 이용하고, Proxy Server를 응용하여 공격을 시도하는지를 연구한다. 또한 Proxy Server를 통한 IP Spoofing 공격 및 방어하는 방법과 IP 역추적 방법을 제안하여 본 연구의 자료가 국제적인 Hacking과 보안방어 기술 발전에 기여 할 것이다.

ABSTRACT

The characteristics of International Hacking is that because even if with tracing techniques, nobody can find Real IP address of the attacker so it is true that Great difficulty in the investigation. so that an attacker goes through the Proxy Server Many times and they use techniques of IP Spoofing to hide their IP address. In this paper, study How attackers use IP Spoofing Technique and the application of Proxy Server. In addition, to Propose IP Spoofing attacks through the Proxy Server attack and defend methods also IP traceback methods so this study materials will contribute to the development of International Hacking and Security Protection Technology.

키워드

IP Spoofing, Proxy Server, International hacking, International security

Ⅰ. 서 론

2000년 이후 중국으로부터 Hacking공격이 이루어지면서 각 국가에서는 Hacking 방어의 필요성이 증대되고 있다. 특히 한국은 인터넷 인프라가 발달하여 주요 공격의 대상이 되고, 한국의 Proxy Server[1] 를 공격의 연결 통로로 이용하여 피해가 발생하고 있다.

중국에서 해커가 한국의 중소 게임업체와 대형 게임업체의 서버를 다운을 시켜서 서비스를 하지 못하게 하는 공격을 발생시키며[2][3], 상납금을 요구하였다. 또한 미국의 기업인 구글(Google)의 중국 지사에서 Hacking이 발생하여 공격자를 추적한 결과, 중국정부가 Hacking에 개입한 것으로 밝혀져, 중국 구글 검색 서비스를 하지 않는[4] 등 국제적인 공격과 피해가 계속하여 발생되고 있다.

이와 같은 국제적인 Hacking에 대한 정보보안의 필요성이 증대되고, 공격 후에 피해에 따른 책임소재를 판단하기위한 증거로 IP 역추적[5] 과 공격자의 색출에 꼭 필요한 패킷[6] 분석과 로그기록[7] 등 증거자료에 관한 연구가 필요하다.

따라서 본 논문에서는 해커가 자신의 IP 주소를 숨기기기 위해 사용하는 IP Spoofing[8] 기법을 연구하며, 또한 Proxy Server를 여러 번 거치면서 공격을 하는 공격을 패킷 분석과 로그기록 등 증거자료에 대하여 분석하고, 이를 방어하고 추적하는 기법을 연구하여 국제 정보보안 기술 발전에 기여 할 것이다.

Ⅱ. 관련 연구

2.1. IP Spoofing

공격자가 그림 1처럼 IP 주소를 바꾸어 다른 것처럼 보이도록 하는 방법이 IP Spoofing이다.

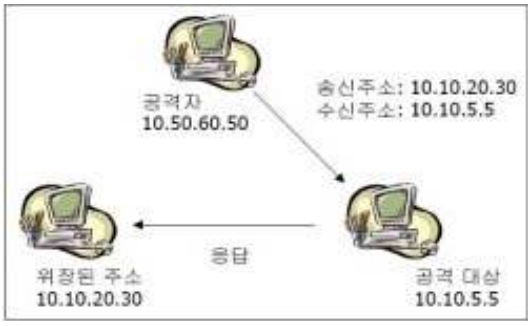

그림 1. IP Spoofing 의 공격 방법

공격대상은 그 패킷을 받게 되지만 공격자의 주소가 아닌 수취인으로 기재된 IP 주소로 회신을 한다. 그러므로 공격자는 패킷을 위장된 주소로 컴퓨터에 보낼 수 있다. 하지만 어떤 패킷도 되돌려 받지 않는다. 단방향 공격 (one-way-attack)이라고도 한다.

만약 공격자가 그림 2처럼 피해자의 시스템과 위장한 주소를 가진 시스템 사이의 경로 안에 들어가 있다면 회신을 받을 수도 있다. 따라서 공격자는 공격의 진행 상태를 확인할 수 있다.

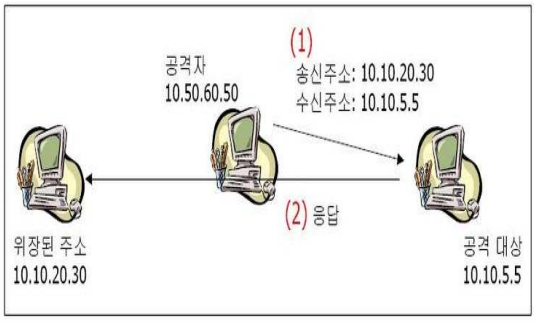

그림 2. 상태 확인이 가능한 IP Spoofing

2.2. Proxy Server

Proxy Server는 클라이언트와 서버 사이에서 데이터를 중계하는 역할을 하는 가상 서버이다. Proxy Server의 기능에는 방화벽[9] 기능이 있다. 인터넷 동시 접속자가 많을 때, 음란사이트 등 유해 사이트를 차단할 때, 내부 사용자 IP주소를 사설 IP주소로 설정하여 보안을 강화할 때, 해커 등 외부의 침입을 방지하고자 할 때 사용하며, 인터넷을 사용할 때 보안이나 규제가 필요한 기업이나 학교 등에서 사용하고 있다. 또한 캐시기능이 있어 네트워크의 트래픽을 줄이고, 데이터의 전송 시간을 향상 시킨다.

현재 주로 사용되고 있는 Proxy 소프트웨어로는 Squid, 탑프래시, 보라매, MS Proxy, 인터폴, 웹빌더, 스푼 등이 있다.

2.3. IP 역추적

1) TCP 연결[10] 역추적(TCP connection traceback) 연결 역추적(connection traceback)이라고 하며, 해커가 우회공격을 시도하는 경우, 해커의 실제 위치를 추적하는 기술로서 TCP연결을 기반으로 우회 공격을 시도하는 해커의 실제 위치를 실시간으로 추적하는 기법이다.

2) IP 패킷 역추적(IP packet traceback)

패킷 역추적(packet traceback)이라고 하며 IP주소가 변경된 패킷의 실제 송신지를 추적하는 기술로서 IP주소가 변경된 패킷을 송신하는 시스템을 찾는 기술이다.

Ⅲ. Proxy Server를 사용한 IP Spoofing 공격

3.1. Proxy Server를 사용한 공격 환경 분석

일반적 사용자는 Proxy Server를 사용하더라도 한곳의 Proxy Server 만을 사용하게 된다. 하지만 해커는 2개 이상의 Proxy Server를 사용하게 된다. 보통 Proxy Server는 사용자에게 전송을 원하는 목적지의 주소 등을 받는데, 이곳에 또 다른 Proxy Server를 적는 형식으로 계속해서 Proxy Server를 이어줌으로서 여러 개의 Proxy Server를 사용할 수 있다.

해커들이 서로 다른 나라의 Proxy Server들을 사용함으로서 차후 추적 및 수사에 어려움을 줄 수 있게 된다. 또한 경유 Proxy Server를 미리 Hacking 하여 로그기록을 고의적으로 삭제해 버릴 경우, 사실상 추적이 어렵게 된다.

3.2. Proxy Server를 사용한 IP Spoofing 공격

3.2.1. 공격 환경

실제 해커의 공격은 Proxy Server를 2~3번 이상 사용하지만 실험에서는 Proxy Server를 2번 사용하여 간소화 하였다. 다음은 공격실험을 위한 Proxy Server를 사용한 IP Spoofing 공격을 위한 시스템의 사양이다.

- CPU : Intel(R) Core(TM) i3 CPU 530
- RAM : 4 GB
- OS : Microsoft Windows 7 - 32bit
- HDD : 500 GB
- 가상 OS software : VMware
- 네트워크 환경: NAT(Network Address Translation) 기반의 가상 네트워크

■ Proxy Server 1, 2(가상 컴퓨터)
- CPU : 원 시스템과 공유
- RAM : 512 MB (원 시스템에서 분할)
- OS : Microsoft Windows XP - 32bit
- HDD : 50 GB (원 시스템에서 분할)
- Proxy Server Program: Squid-2.7 STABLE 8

■ A (가상 컴퓨터)
- CPU : 원 시스템과 공유
- RAM : 256 MB (원 시스템에서 분할)
- OS : Microsoft Windows XP - 32bit
- HDD : 15 GB (원 시스템에서 분할)

■ B (가상 컴퓨터)
- CPU : 원 시스템과 공유
- RAM : 256 MB (원 시스템에서 분할)
- OS : Microsoft Windows XP - 32bit
- HDD : 15 GB (원 시스템에서 분할)

■ C (가상 컴퓨터)
- CPU : 원 시스템과 공유
- RAM : 256 MB (원 시스템에서 분할)
- OS : Microsoft Windows XP - 32bit
- HDD : 15 GB (원 시스템에서 분할)

3.2.2. 공격과정

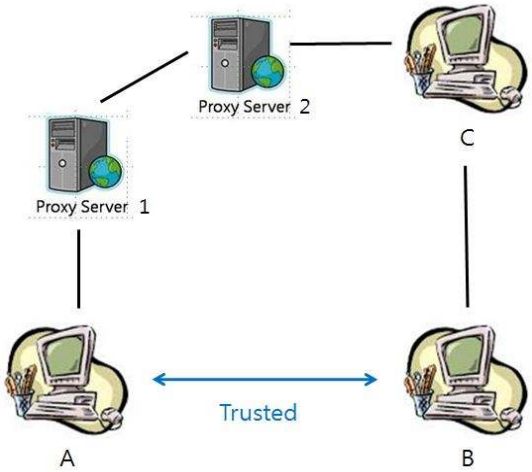

그림 3. 공격 실험 네트워크 구성도

그림 3처럼 C의 패킷은 Proxy Server 1과 2를 통해 A로 보내지게 되며, A와 B는 상호 신뢰된 관계 즉 내부 호스트 관계이다.

C는 A로 자신의 IP주소를 위장하여 SYN를 보내 접속 요청을 한다. 요청에 대한 응답으로 A가 C에 대한 ACK와 함께 자신의 SYN을 전송하지만 C가 이에 대해 ACK를 보내지 않으면 A는 자신이 보낸 ACK에 대한 C의 응답을 기다리게 된다. 이 과정을 연속적으로 반복하면 A는 외부의 접속요청에 응답할 수 없는 오버플로우 상태가 된다.

C는 자신의 IP주소를 A로 가장한 후 B에 접속 요청(SYN)을 보낸다. B는 수신된 SYN 패킷이 A에서 온 것으로 인식, A에게 ACK와 새로운 SYN를 보내지만 이미 A는 외부와 통신 불능상태이므로 응답을 할 수 없게 된다.

C는 자신의 IP 주소를 A주소로 위장하여 B가 A로 보낸 SYN/ ACK에 대한 ACK를 B에 보낸다. 결국 C와 B 불법적 접속이 이루어지고, B와 A는 연결되어 있는 것으로 착각한다.

이후 이미 맺어진 신뢰관계를 사용하여 B 시스템을 자유롭게 사용할 수 있게 된다.

Ⅳ. Proxy Server를 응용한 IP Spoofing 공격에 대한 방어와 역추적 분석

4.1. IP Spoofing 공격 분석 및 방어

IP Spoofing 공격은 신뢰관계를 사용한 공격이기 때문에 그림 4처럼 신뢰관계를 만들어 주는 서비스를 중지 시키고, 관련 파일을 삭제함으로써 신뢰관계를 사용하지 않는 것이 방법이다.

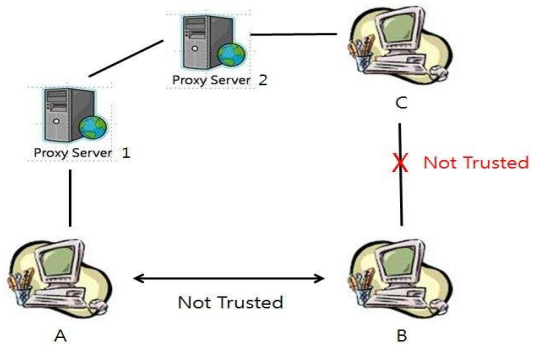

그림 4. 신뢰관계 해제를 통한 방어

또한 그림 5처럼 외부에서 들어오는 패킷 중에서 출발지 IP주소(Source IP Address)에 내부망 IP주소를 가지고 있는 패킷을 라우터 등에서 패킷 필터링을 사용하여 막아낼 수 있다.

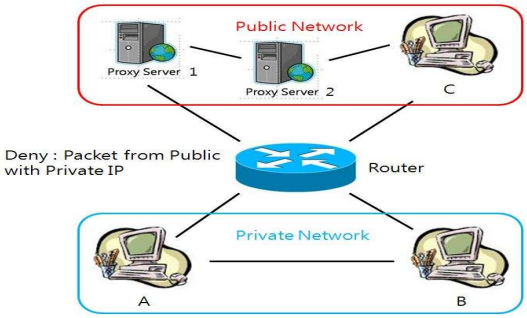

그림 5. 외부 패킷 필터링을 이용한 방어

내부 네트워크에서 발생하는 모든 트래픽을 암호화 하여 변경이 불가능하게 하여 방어 할 수

있다. 다른 내부 사용자에 의한 공격을 막기 위해서는 각 시스템에서 TCPwrapper, ssh 등을 설치해서 운영하고, rsh, rlogin 등과 같이 패스워드의 인증 과정이 없는 서비스를 사용하지 않는다.

4.2. Proxy Server를 통한 공격의 IP 역추적

IP역추적을 위해서는 Proxy Server를 이용한 공격을 당한 시스템의 로그 기록을 검사하여 첫 번째 Proxy Server의 IP 주소를 탐색하여 파악된 Proxy Server의 로그 기록을 다시 검사하여 공격자를 찾게 된다.

또한 그림 6처럼 공격에 사용된 Proxy Server가 둘 이상이라면, 첫 번째 Proxy Server 에서의 로그 기록에 남은 IP 주소는 공격에 사용된 두 번째 Proxy Server가 된다. 이를 공격에 사용된 Proxy Server 개수만큼 반복하면 공격자의 실제 IP 주소를 찾을 수 있다.

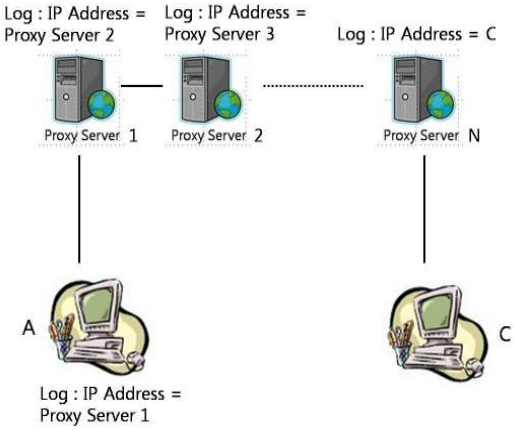

그림 6. 2개 이상 Proxy Server 공격의 추적

Ⅴ. 결 론

Hacking의 공격과 피해가 지속됨에 따라 국제 Hacking에 대한 보안의 필요성이 증대되면서 공격에 사용되는 IP Spoofing 과 Proxy Server 이용 공격이 알려지기 시작하였고, 공격에 따른 분석 및 방어 연구와 로그 분석 및 패킷 분석, IP 역추적 기법에 대한 연구가 진행되고 있다.

본 논문에서는 해커가 공격에 사용하는 Proxy Server와 IP Spoofing 공격을 연구하여 Hacking에 대한 공격을 실험 하였고, IP Spoofing 공격분석에 따른 방어 방법과 Proxy Server의 IP 역추적 방법을 연구하여 정보보안 기술 발전에 기여하였다.

향후 연구로는 다수의 해외와 국내 Proxy Server를 이용한 공격에 대해 효율적 IP 역추적과 포렌식 자료 생성에 관한 연구가 필요하다.

참고문헌

[1] 오영선, 이현태, “H.323을 지원하는 Application Proxy Server의 설계”, 한국해양정보통신학회학술대회논문집, 제 4권 제 2호, pp. 296-301, 2000. 10.

[2] 네이버뉴스, “중국 거주 해커에 영세 게임업체들 `벌벌'”, http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=105&oid=001&aid=0001790385, 2007. 10.

[3] 네이버뉴스, “중국연계 해커조직 유명 게임사이트 Hacking”, http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=102&oid=034&aid=0000296667, 2006. 6.

[4] 보안뉴스, “구글(Google) 사태와 전망”, http://www.boannews.com/media/view.asp?idx=19882&kind=1, 2010. 3.

[5] 김재동, 채철주, 이재광, “IP 역추적 기술을 이용한 능동형 보안 시스템”, 한국해양정보통신학회논문지, 제 11권 제 5호, pp.933-939, 2007. 5.

[6] 차영환, “관심 대상모니터링 네트워크에서의 중복된 감지-보고 패킷들의 발생 억제에 관한 연구”, 한국해양정보통신학회논문지, 제 13권 제 9호, pp.1955-1963, 2009. 9.

[7] 천준호, 신동규, 장근원, 전문석, "DDoS 공격에 대한 방화벽 로그 기록 취약점 분석", 정보보호학회논문지, 제 17권 제 6호, pp. 143-148, 2007. 12.

[8] V. Shyamaladevi, Dr. R.S.D Wahidabanu, “Analyze and Determine the IP Spoofing Attacks Using Stackpath Identification Marking and Filtering Mechanism”, International Journal of Recent Trends in Engineering, 제 1권, 제 1호, 2009. 5.

[9] 윤여웅, 이상호, "게이트웨이형 웹 애플리케이션 방화벽 보호프로파일에 관한 연구", 정보과학학회지, 제 25권 제 5호, pp.44-52, 2007. 5.

[10] Huang G, Miao L, Zhang D -F, Zhou Z -Y, "Analysis and verif TCP connection management protocol based on model checking ", Computer Engineering and Design, Vol. 30, no. 10, pp.2381-2386. 28 May 2009.