해외에서 Proxy Server를 연동한 우회적인 공격기법 연구

이보만*, 박대우*

*호서대학교 벤처전문대학원 IT응용기술학과

A Study of Indirect Attack Method with Interlocked Proxy Server in Foreign Country

Boman Lee*, Dea-Woo Park*

*Dept. of IT Application Technology, Hoseo Graduate School of Venture

e-mail:bomans@nate.com, prof1@paran.com

요 약

Hacking 공격자에 대한 수사실무에서는 Proxy Server를 연동한 해외에서의 우회공격에 대한 기법과 기술을 알아야 MAC address 또는 Real IP에 대한 역추적이 가능하다. 즉 Proxy Server를 여러 번 거치면서 자신의 Real IP를 숨기고 ARP Spoofing 기법을 사용하여 MAC address를 속이기 때문이다. 본 논문에서는 해외에서의 해킹 공격자들이 어떻게 공격자의 Real IP를 숨기고, ARP Spoofing 기법을 응용하여 공격을 시도하는 기법과 기술을 연구한다. 또한 Proxy Server를 통한 우회공격에서 ARP Spoofing 공격을 보안하는 방법을 연구한다. 본 논문 연구가 해외로 부터의 Hacking과 방어를 위한 기술 발전에 기여 할 것 이다.

키워드

ARP 스푸핑(ARP Spoofing), 프록시 서버(Proxy Server), 맥 어드레스(MAC Address), 해외 해킹(International Hacking)

Ⅰ. 서 론

2000년대에 중국으로부터의 Hacking 공격[1]이 이슈가 되면서 각 국가에서는 해외로부터의 Hacking 공격 방어의 필요성이 증대되고 있다. 특히 한국은 인터넷[2] 인프라가 발달하여 주요 공격의 대상이 되고, Hacking 공격자들이 한국을 Proxy Server로 사용, 공격의 연결 통로로 이용하여 피해가 발생하고 있다.

중국에서 해커가 한국의 대형 게임업체[3]와 영세 게임업체[4]의 서버를 다운을 시켜서 서비스를 하지 못하게 하는 등의 공격을 하여, 기업에게 서비스를 하고 싶으면 상납금을 달라고 요구하는 일도 발생하였다. 또한 미국의 기업인 구글(Google)의 중국 지사에서 Hacking공격[5]이 발생하여 공격자를 추적한 결과, 중국정부가 Hacking 공격에 개입한 것으로 밝혀져, 구글이 중국 검색 서비스를 하지 않는 등 국제적인 공격과 피해가 계속하여 발생되고 있다.

이와 같은 국제적인 Hacking에 대한 정보보안의 필요성이 증대되고, 공격 후에 피해에 따른 책임소재를 판단하기위한 증거로 Real IP[6]등의 주소 역추적[7]과 공격자의 색출에 꼭 필요한 패킷[8]분석[9]과 로그기록 등 증거자료에 관한 연구와 방어가 필요하다.

따라서 본 논문에서는 해커가 자신의 MAC address를 숨기기기 위해 사용하는 ARP Spoofing[10] 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. 본 론

2.1 Proxy Server

Proxy Server는 원래 클라이언트와 서버 사이에서 데이터를 중계하는 역할을 하는 가상 서버이다. Proxy Server의 기능에는 방화벽 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 캐시 기능이 있어 네트워크의 트래픽을 줄이고, 데이터의 전송 시간을 향상 시킨다. 하지만 Hacking 공격자가 사용할 경우 공격자가 자신을 숨길 수 있는 방법이 되기도 한다. 현재 주로 사용되고 있는 Proxy 소프트웨어로는 Squid, 탑프래시, 보라매, MS Proxy, 인터폴, 웹빌더, 스푼 등이 있다.

2.2 ARP Spoofing

본론은 필요에 따라 3-4 개의 장으로 편집할 수 있습니다.

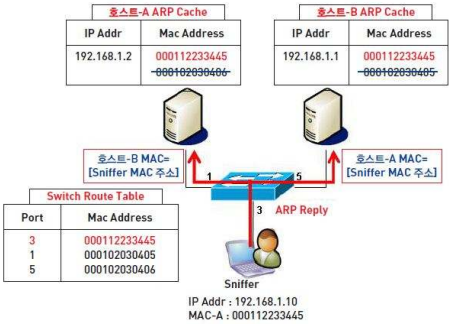

그림 1. ARP Spoofing 개념도

ARP Spoofing 공격은 그림1 과 같이 ARP protocol의 취약점을 이용한 공격으로 Hacking 공격자는 자신의 MAC address를 공격 대상 컴퓨터가 통신하고자 하는 컴퓨터의 MAC address중 하나로 속여 피해 시스템에 접근하여 중간에서 패킷을 가로채는 기법이다. 공격자는 패킷을 가져오는 것에 그치지 않고 얻은 패킷을 위조 및 변조하여 재전송하는 방법으로 Hacking 공격을 시도한다.

2.3 IP 역추적

IP 역추적의 방법에는 TCP 연결 역추적(TCP connection traceb ack)방법이 있다. 다른 말로는 연결 역추적(connection traceback)이라고도 하며, 해커가 우회공격을 시도하는 경우, 해커의 실제 위치를 추적하는 기술로서 TCP연결을 기반으로 우회 공격을 시도하는 해커의 실제 위치를 실시간으로 추적하는 기법이다. 다른 방법에는 IP 패킷 역추적(IP packet traceback)이 있는데, 다른 말로는 패킷 역추적(packet traceback)이라고 하며, IP주소가 변경된 패킷의 실제 송신지를 추적하는 기술로서 IP주소가 변경된 패킷을 송신하는 시스템을 찾는 기술이다.

Ⅲ. Proxy Server를 연동한 Hacking 공격

3.1 Proxy Server를 사용한 Hacking 공격 환경

실제 해커의 공격은 Proxy Server를 5회 이상 거쳐서 실행하지만 실험에서는 Proxy Server를 2번 사용하여 간소화 하였다. 네트워크 구성은 NAT(Network Address Translation)을 사용하며 네트워크의 복잡도를 줄이기 위하여 Proxy Server와 client들만을 사용하였다. Proxy Server와 client의 옵션으로는 통신하는 모든 패킷에 대한 IP와 MAC address에 대한 로그 기록을 저장하여 보관하도록 하였다. 또한 시스템 구성은 가상의 컴퓨터를 구성하고 CPU를 공유하여 사용한다. 다음의 표 1, 2, 3은 실험을 위한 Proxy Server를 사용한 Hacking 공격을 위한 시스템의 환경이다.

표 1. Main 환경

시스템	항목	값
Main	CPU	Intel Core i3
	RAM	4GB
	운영체제	Windows 7
	HDD	500GB
	가상 시스템 Software	VM ware
	가상 네트워크 환경	NAT

표 2. Proxy Server 1 ,2 환경

시스템	항목	값
Proxy Server 1	CPU	Intel Core i3
	RAM	512MB
	운영체제	Windows XP
	HDD	50GB
Proxy Server 2	CPU	Intel Core i3
	RAM	512MB
	운영체제	Windows XP
	HDD	50GB

표 3. Client A, B, C 환경

시스템	항목	값
Client A	CPU	Intel Core i3
	RAM	256GB
	운영체제	Windows XP
	HDD	20GB
Client B	CPU	Intel Core i3
	RAM	256GB
	운영체제	Windows XP
	HDD	20GB
Client C	CPU	Intel Core i3
	RAM	256GB
	운영체제	Windows XP
	HDD	20GB

3.2 Proxy Server를 사용한 Hacking 공격 분석

그림 2는 공격 실험 네트워크의 구성도이다. Hacking 공격자 A는 Proxy Server들을 사용하여 공격을 시도하는데, 일반적인 Proxy Server보다 탐지가 어려운 High anonymous Proxy Server를 찾아 공격에 사용한다.

먼저 Hacking 공격자인 A는 공격대상인 C의 통신 패킷을 체크하고 있다가, C가 ARP request를 보내면서 B가 누구인지를 묻는 메시지가 나오길 기다린다. C가 ARP request를 보내면, A는 B의 MAC address를 사용하여 ARP reply를 보내게 되고 ARP protocol의 특성 상 MAC address가 같기 때문에 C가 A를 B로 인식하게 되도록 한다. 따라서 C는 MAC address를 가지고 B로 패킷을 전송하지만, 실제로는 A로 패킷을 보내게 된다. 공격자 A는 B로 향하는 데이터를 가로채어 정보를 탈취 하거나, B에도 같은 방법으로 공격을 하여 B와 C의 통신을 모두 가로 챌 수 있다. 따라서 B와 C의 패킷들을 가로채면서 정상적인 통신을 하는 것처럼 착각하게 만들어 B와 C의 정상적인 패킷을 계속해서 가로채면서 정보를 얻을 수 있게 된다.

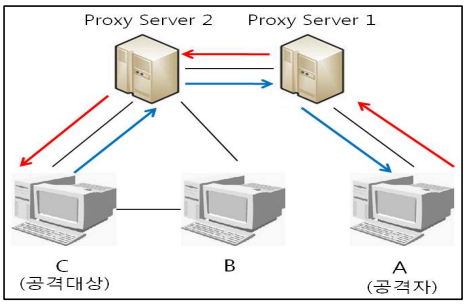

그림 2. Hacking 공격 시스템 구성도

Ⅳ. Proxy Server를 연동한 Hacking 공격에 대한 방어와 역추적 분석

4.1 Proxy Server를 연동한 Hacking 공격 방어

ARP Spoofing 공격은 ARP protocol의 취약점을 이용하여 공격을 시도하는 것이기 때문에 ARP protocol의 취약점을 보완하는 방법으로 ARP table 이 자동적으로 변경 되는 것을 막아줌으로서 위조, 변조 되는 것을 사전에 차단하는 것이 좋다. 그림 3처럼 ARP table을 Static으로 변경하여 적용하면 ARP table 이 자동적으로 바뀌지 않게 되어 방어가 가능하게 된다.

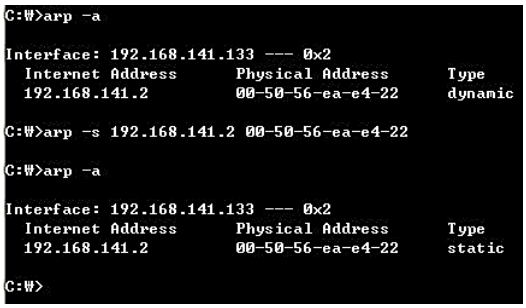

그림 3. ARP Table static 설정

또한 공격이 Proxy Server를 사용하여 외부에서 들어오는 패킷이기 때문에 외부에서 들어오는 패킷 중에서 MAC address가 내부의 MAC address인 경우 패킷을 스위치나 라우터 등에서 패킷 필터링을 사용하여 막아낼 수 있다.

4.2 Proxy Server를 사용한 Hacking 공격의 역추적

IP역추적을 위해서는 스위치와 라우터에 기록되어 있는 로그를 바탕으로 첫 번째 경로로 사용된 Proxy Server에 저장된 로그에서 IP와 MAC address를 분석하여 이전에 패킷이 지나온 두 번째 Proxy Server의 주소를 알아낸다. 두 번째 Proxy Server에서도 동일한 방법으로 IP와 MAC address를 분석하면 세 번째 Proxy Server를 찾아낼 수 있고, 이를 반복하다 보면 최종적으로 Hacking 공격자의 IP 또는 MAC address를 찾을 수 있게 된다.

V. 결 론

Hacking의 공격과 피해가 지속됨에 따라 국제 Hacking에 대한 보안의 필요성이 증대되면서 우회 공격에 사용되는 Proxy Server가 알려지기 시작하였고, Hacking 공격자의 공격 기법은 역추적이 불가능한 방법으로 발전하고 있다. 이에 Hacking 공격에 따른 분석 및 방어 연구와 로그 분석 및 패킷 분석, IP등의 주소 역추적 기법에 대한 연구가 계속되고 있다.

본 논문에서는 해커가 공격에 사용하는 Proxy Server를 연동한 공격을 연구하여 Hacking공격에 대한 분석을 하였고, ARP Spoofing 공격분석에 따른 방어 방법과 Proxy Server의 IP와 MAC address 역추적 방법을 연구하여 정보보안 기술 발전에 기여 하였다.

향후 연구로는 해외 Proxy Server를 이용한 공격에 대한 IP등의 주소 역추적 또는 취약점을 가진 다른 protocol 에 관한 연구가 필요하다.

참고문헌

[1] Hyung-Kyu Yang, Kang-Ho Lee, Jong-Ho Choi, "A Study on Personal Information Hacking Using Domestic Search Engines", Journal of Korea Society of Computer and Information Transaction, Vol 12, No 3, pp.195-201, July 2007.

[2] Jun-Pyo Lee, Chul-Yong Jo, Jong-Sun Lee, Tae-Young Kim, Chul-Hee Kwon , "Design of a Request Pattern based Video Proxy Server Management Technique for an Internet Streaming Service", Journal of Korea Society of Computer and Information Transaction, Vol.15, No.6, pp.57-64, June 2010.

[3] Naver News, "Chinese hacker organization hacked korean famous gaming sites," June 2006.

[4] Naver News, "hacker in China make korean Small game companies shake and tremble," October 2007.

[5] Security News, "Google situation and Prospect", March 2010.

[6] Woo-Seok Seo, Dea-Woo Park, Moon-Seog Jun, "A Study on the DDoS Defense Algorithm using CFC based on Attack Pattern Analysis of TCP/IP Layers", Journal of Korea Society of Digital Industry & Information Management Transaction, Vol.17, No.6, pp.143- 148, December 2007.

[7] Jae-Dong Kim, Chul-Ju Chae, Jae-Gwang Lee, "Active Security System using IP Traceback Technology", Journal of Korean Institute of Maritime Information and Communication Sciences Transaction, Vol.11, No.5, pp.933-939, May 2007.

[8] Yeong-Hwan Tscha, "On Suppressing the Occurrence of Redundant Sensing-Reproting Packets in Assets Monitoring Networks", Journal of Korean Institute of Maritime Information and Communication Sciences Transaction, Vol.13, No.9, pp.1955-1963, September 2009.

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

[10] 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, Vol,1, No,1, May 2009.