보안공학연구논문지 *Journal of Security Engineering*
Vol.11, No.1 (2014), pp.115-122
http://dx.doi.org/10.14257/jse.2014.02.07

백도어를 이용한 닌자 게이트웨이 라우팅 기법에 관한 연구

박병호[1], 신대철[2], 나형두[3]

A Study on Ninja Gateway Routing Using Backdoor Method

Byungho Park[1], Daecheol Shin[2], Hyeng-doo Na[3]

요 약

국제 해커그룹 어나니머스는 북한 내부망인 광명을 해킹할 것 이라고 선언했는데, 북한 내부에서 사용하는 내부망인 광명은 인터넷과 연결되지 않은 단독 폐쇄망으로서 인터넷을 경유하여 해킹한다는 것은 매우 어렵기 때문이다. 어나니머스는 닌자게이트와 내부 협조자를 이용하여 해킹할 것이라고 선언하였는데 구체적인 닌자게이트에 대한 스펙은 알려지지 않았다. 본 연구에서는 새로운 기법을 적용한 실제 물리적으로 라우터간 연결되지 않은 인터넷 및 폐쇄네트워크 망에서의 연결방법에 대하여 기술하고자 한다. 이 연구의 결과로 비록 내부 폐쇄망일지라도 별도의 차단 대책이 필요한 것으로 사료된다.

핵심어 : 라우터, 어나니머스, 백도어, 닌자 게이트웨이

Abstract

Anonymous, International Hacker Group, declared to hack the Kwangmyung intranet of North Korea. This network used inside North Korea is not connected to the Internet so that its hacking is very difficult.

They announced that they would use the hacking method with the internal control coordinator and the Ninja gateway, but they did not give any specific information about it. In this study, we suggest a new approach to use a bottom-up and then connect between the closed network and the Internet without linking each router. The result of this study needs a separate isolating measure for a router hacking method even though it is a closed network.

Keywords : Router, Anonymous, Backdoor, Ninja Gateway

접수일(2013년12월27일), 심사의뢰일(2013년12월28일), 심사완료일(1차:2014년01월15일, 2차:2014년01월24일)
게재일(2014년02월28일)

[1]339-701 세종특별자치시 세종로 2639, 홍익대학교 컴퓨터정보통신공학과.
email: sunsonbob@hongik.ac.kr
[2]100-744 서울시 중구 세종대로 110, 서울시청 통합보안관제팀.
email: dcshin@seoul.go.kr
[3](교신저자)140-701 서울시 용산구 이태원로 22(용산동3가 1번지), 국방부 정보화기획관실.
email: nhd2036@mnd.go.kr

ISSN: 1738-7531 JSE

1. 서론

인터넷은 서버들을 연결하여 다양한 정보가 교류하는 네트워크망으로서 일반적인 전 세계인의 대다수가 접속하여 사용할 수 있는 공개망과 각국의 군사, 공안 및 행정망으로 이용하는 내부 인트라넷으로 사용되고 있다. 특히, 내부 폐쇄망인 국방망, 경찰망 및 행정망 등에 대하여 각국은 인터넷과 물리적으로 격리되어져있어 절대 안전하다고 생각하고 있다.

국제 해커그룹 어나니머스는 2013년 4월, 북한 관영 조선 중앙 통신이 운영하는 웹사이트에 침입하여 사이트 가입자의 개인 정보를 발표했다. 또한, 그들은 한국 전쟁의 출시를 기념하기 위해 2013년 6월 25일에 두 번째로 북한 인민망인 광명을 해킹할 것 이라고 선언했다[5,6]. 이것이 주목받는 이유는 북한은 매우 폐쇄적인 국가이기 때문에 일반 국민들은 인터넷을 사용할 수가 없고 특수한 계층에서만 매우 제한적으로 사용된다고 알려졌기 때문이다. 특히, 북한 내부에서 사용하는 인민망인 광명은 인터넷과 연결되지 않은 단독 폐쇄망으로서 인터넷을 경유하여 해킹한다는 것은 매우 어렵기 때문이었다. 어나니머스는 닌자게이트와 내부 협조자를 이용하여 해킹할 것이라고 선언하였는데 구체적인 닌자 게이트에 대한 스펙은 알려지지 않았다. 네트워크 장비를 이용한 해킹 기법은 다수 알려져 있으며, 최근인 2013년 10월에도 미 정부 US-CERT 발표 및 D-Link 라우터에는 백도어가 존재한다고 발표하였다[7]. D-Link의 문제는 사용자가 원격 관리 기능을 사용하는 경우 이 기능을 사용하여 공격하면 라우터의 설정이 변경되거나 오류가 발생할 우려가 있다고 한다. 기존 연구에서는 네트워크망에 연결된 인터넷 환경 하에서 주로 라우터 자체에 대한 백도어를 이용한 해킹방법의 가능성 등을 통하여 개략적인 가이드만 제시하였다[1-3],[8].

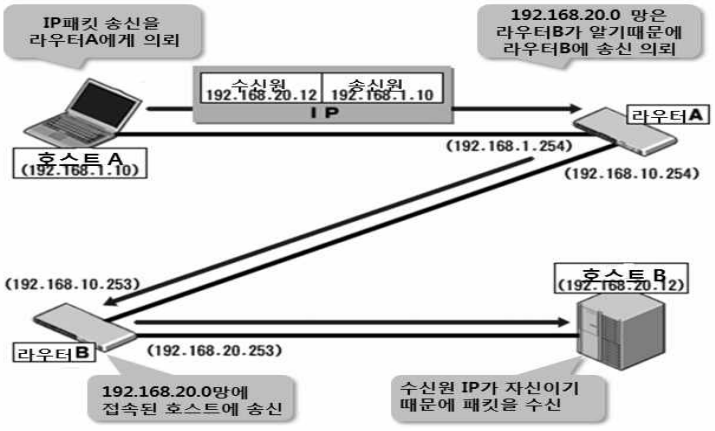
본 연구에서는 새로운 기법을 적용하여 실제 물리적으로 연결되지 않은 네트워크에서 백도어를 통한 라우터 해킹을 통하여 닌자게이트 기법을 기술하고자 하며, 이를 통해 별도로 운용되는 대표적 국가 폐쇄망인 국방망, 행정망 및 은행망 등 인트라넷 망에 대하여 안전하다고 방심해서는 안되며, 이를 위한 별도의 차단 대책이 필요할 것이다.

본 논문은 4개장으로 구성되어 2장에서는 라우팅에 대한 설명과 라우팅 기법에 대하여 설명하고, 3장에서는 본 연구의 핵심인 일반적인 네트워크 구성방법인 라우터와의 연결 없이 각각 폐쇄망에 대한 연결법에 대한 기법을 제시하며, 4장은 본 연구의 결론이다.

2. 관련 연구

라우터(Router)는 네트워크와 네트워크 간의 경로(Route)를 설정하고 가장 빠른 길로 트래픽을 연결해주는 네트워크 장치이자 최적경로를 설정해주는 장비로서 동일한 전송 프로토콜을 사용하는 분리된 네트워크를 연결하여 각 네트워크 계층을 서로 연결한다[9,10]. 이 장비는 패킷의 위치를 추출하여 그 위치에 대한 최상의 경로를 지정하고 이 경로를 따라 데이터 패킷을 다음 라우터 장

치로 전송시키는 장치이다. 그림 1은 일반적인 라우터의 역할을 묘사한 것이다.



[그림 1] 다수의 라우터를 이용한 네트워크 구성 예

[Fig.1] An example of Network Configuration Using Multi Router

라우터는 브리지가 가지는 기능에 추가하여 경로 배정표(Routing Table)에 따라 다른 네트워크 또는 자신의 네트워크 내의 노드를 결정한다. 스위치가 MAC 어드레스를 기반으로 패킷을 목적지로 전달하는 것처럼, 라우터의 내부에는 라우팅 소프트웨어 및 라우팅 테이블이 있는데, 주소 테이블에 해당하는 라우팅 테이블을 가지고 라우팅 서비스를 제공하며, 라우팅 소프트웨어는 수신 받은 데이터 그램의 목적지 주소를 조사하고, 이 주소에 대해 메모리에서 구축된 라우팅 테이블을 참조하여, 출력 포트 중 하나를 통해 데이터 그램을 적절하게 전송시킨다. 보다 정확하게 말하면, 라우터는 철저하게 라우팅 테이블에 의존해 라우팅을 한다. 따라서 라우터의 역할은 라우팅 테이블을 관리하는 것이 절반 이상의 비중을 차지하며, 이 라우팅 테이블을 어떻게 구성하고 관리하느냐에 따라 라우터의 원래 목적인 최적의 경로를 찾는 것이 가능해진다.

라우팅 테이블의 정보를 관리하는 방법은 크게 정적(static) 라우팅과 동적(dynamic) 라우팅으로 나눌 수 있다. 정적 라우팅은 관리자가 직접 라우터에 대해 접속하려는 특정 장소에 상대 라우터를 지정하는 방식이며, 동적 라우팅은 라우터가 자체적으로 라우터끼리의 접속 정보를 주고받아 라우팅 테이블이 자동 갱신되는 방법이다[11,12].

동적 라우팅이 당연히 편하고 효과적인 방법처럼 보이지만, 정적 라우팅도 라우터 자체의 부하가 적고 회선 대역폭의 효율이 좋다는 장점이 있다. 따라서 모뎀이나 브로드밴드 네트워크와 같이 필요할 때만 연결하는 환경에서는 라우팅 정보를 라우터끼리 주고받지 않는 정적 라우팅이 주로 이용된다. 본 연구에서는 정적 라우팅 기법을 활용하여 폐쇄망끼리의 연결시 사용을 설명한다.

그림 2는 경로 배정표를 보여준다.

Routing Table:

Destination	Gateway	Flags	Ref	Use	Interface
127.0.0.1	127.0.0.1	UH	1	298	lo0
default	172.16.12.1	UG	2	50360	
172.16.12.0	172.16.12.2	U	40	111379	le0
172.16.2.0	172.16.12.3	UG	4	1179	
172.16.1.0	172.16.12.3	UG	10	1113	
172.16.3.0	172.16.12.3	UG	2	1379	
172.16.4.0	172.16.12.3	UG	4	1119	

[그림 2] 경로 배정표[12]

[Fig.2] Routing Table[12]

또한 라우터와 게이트웨이의 차이점은 라우터는 통상 동일 프로토콜을 사용하여 OSI 3계층과 4계층을 서비스하는데 반하여 게이트웨이는 OSI 7계층까지 서비스하여 이종 프로토콜까지 변환하여 지원해준다는 장점을 가지고 있다. 다음 장에서는 실제 일명 닌자 라우터를 활용한 비합법적인 라우팅 기법에 대하여 제시하고자 한다.

3. 닌자 라우터 기법

앞장에서 살펴본 바와 같이 주로 해킹시도는 설정된 네트워크에서 트래픽을 이용한 디도스 공격이나 프로그램을 활용한 백도어를 통한 해킹이 주를 이루었다. 즉, 연결된 네트워크에 대한 시도는 많았지만 인터넷과 물리적으로 격리되어 연결되지 않고 보고된 적도 없었다. 그러나 이번 국제 해킹 그룹인 어나니머스가 북한 내부망인 광명에 대하여 해킹한다고 하는 것은 많은 관심을 받기에 충분한 것이다. 그러나 해커의 속성상 실제 어떻게 어떠한 툴과 기법을 활용하여 해킹할 것인지는 명시하지 않았으며 다만 알려진 것은 알려지지 않은 닌자라는 전설 속에 나타나는 일본에서 암암리에 활용된 은닉 무사인 닌자라는 용어를 사용하였으며, 이를 비합법적인 라우터 혹은 라우팅 조작 방법이라고 유추해 볼 수 있다.

3.1 닌자 라우터

닌자라는 어휘에서 나타나듯이 닌자 라우터에는 감추다 혹은 속이다 라는 어의가 느껴진다. 그러므로 일반적인 라우터가 아닌 평범한 일반적인 데스크탑으로도 얼마든지 라우터를 구축 할 수 있으며[13], 외견상 라우터로 보이지만 않으면 된다. 단지, 라우터의 기본적인 구성은 일반 컴퓨터와 마찬가지로 중앙처리 장치인 CPU가 있고, 각종 메모리가 라우터의 운영체제와 환경설정 정보, 그리고 라우팅 정보 등을 담을 수만 있으면 되고 네트워크 인터페이스를 통해 트래픽을 입출력할 수 있으면 된다.

그림 3에서 닌자 라우터의 예를 볼 수 있다.

[그림 3] (좌측) 일반적인 라우터 & (우측) 데스크탑 PC를 이용한 닌자 라우터
[Fig.3] (Left) Ordinary Router & (Right) Ninja Gateway Using Desktop PC

3.2 백도어를 활용한 닌자 라우터 구성

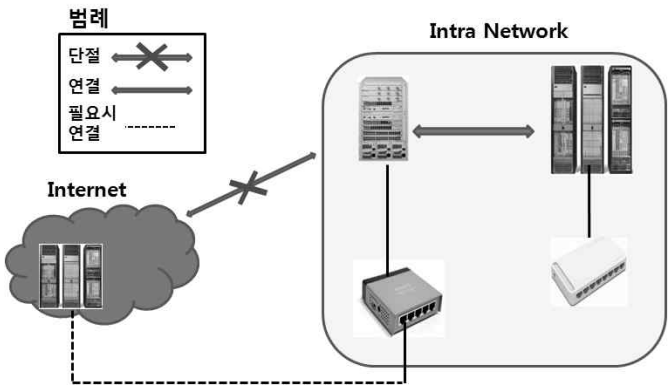
지금까지의 일반적인 네트워크 구축을 위한 라우터의 구성은 라우터끼리의 연결에 의한 방법이었다. 즉, 라우터에 물리적인 네트워크가 연결되지 않으면 데이터가 전달되지 못한다. 그러나 어나니머스가 주장한대로 닌자 라우팅을 구성하려면 일반적인 방법으로는 불가능할 것이다. 라우터는 일반적으로 라우터끼리 연결된 후 라우터에서 내부 네트워크 장비인 스위칭 허브(통상 L3, L4)를 이용하여 네트워크를 구성한다. 즉, 탑다운(Top Down) 방식으로 구성된다.[그림 1참조]

그러나 본 논문에서는 이러한 일반적인 방법이 아닌 새로운 기법인 바톰업(Bottom Up) 기법을 활용하여 구성하고자 한다.

구축방법은

① 최하위의 더미 스위칭 장비를 이용하여 각 각의 폐쇄망인 인트라넷을 연결시킨다.
② 이후, 해당 각각의 라우터에 접속한다.
③ 각각의 라우팅 테이블에 각각의 IP 주소를 기입한다. 여기에서 주의할 것은 기존의 라우팅 테이블이 아닌 다른 상이한 대역의 IP 주소를 입력하는 경우 즉시 IPS(Intrusion Protection System) 장비에 의해 발각될 수 있다.
④ 유사한 대역을 넣든지 아니면 일회용으로 사용한 후 흔적을 제거해야 한다.

아래 그림 4는 닌자 게이트웨이(라우터) 구성을 나타낸다.



[그림 4] 백도어(허브)를 이용한 닌자 게이트웨이 구성도

[Fig.4] The Configuration of Ninja Gateway using Backdoor(swiching hub)

4. 결론

TCP/IP 프로토콜을 사용한 인터넷은 전 세계인의 생활에 직 간접적으로 중요한 생활 도구가 되었다. 특히, 국가에서 운용중인 국가보안망, 은행망 및 행정망 등은 인터넷과 격리되어 국민 생활 및 국가 경영에 핵심요소로 활용되고 있다. 그러나 세계에서 대표적 폐쇄국가인 북한에 대하여 특히 인터넷과 격리되어 운용중인 내부 인트라넷인 광명에 대하여 국제 해커그룹인 어나니머스의 해킹 선언은 우리에게 시사 하는 점이 많다. 따라서 본 연구에서는 실제 물리적으로 연결되지 않은 네트워크 망에서의 백도어(스위칭 허브)를 통한 바톰업 연결 방법을 제시하였으며 특히, 이를 통해 라우터간의 테이블 해킹으로 안전하다고 여겨진 폐쇄망에 대한 문제점을 기술하였으며, 연구의 결과를 바탕으로 비록 인터넷에 연결되지 않고 독자적으로 운용중인 내부 폐쇄망(국방망, 경찰망, 행정망 등)에 대해서도 별도의 차단 대책이 필요할 것이다.

향후에는 닌자 게이트 해킹 방지에 대한 기법을 연구하고자 한다.

References

[1] A. T. Mizrak, S. Savage and K. Marzullo, Detecting Malicious Packet Losses. IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS. (2009), VOL. 20, NO. 2, pp.191-206.

[2] C. M. Hong, W. Shin, Security Requirements of Order Communication System in Hospitals for Ompliance with Personal Information Protection Act. Journal of Security Engineering. (2013), Vol.10, No.5, pp.513-526.

[3] J. S. Sung, A Study on the Prevention Plan of Security Incident. Journal of Security Engineering. (2012), Vol. 9, No.6, pp.513-526.

[4] A. S. Tanenbaum, Computer Networks (4th ed.), Prentice Hall PTR, NJ (2003)

[5] http://mickhartley.typepad.com/blog/2013/06/ninja-gateway.html, Jun 28 (2013).

[6] http://www.nknews.org/2013/06/anonymous-claims-secret-north-korean-military-documents, Jun 20 (2013).

[7] http://www.us-cert.gov/ncas/current-activity/2013/10/18/Reports-D-Link-Router-Backdoor, Oct 18 (2013).

[8] http://www.cs.rutgers.edu/~iftode/citadel.pdf, Sep 26 (2005).

[9] http://www.terms.co.kr/router.htm, Jun 22 (1999).

[10] http://ko.wikipedia.org/wiki/ %router%, Sep 24 (2013).

[11] http://songsunghan.tistory.com/12, Jul 11 (2007)

[12] http://docstore.mik.ua/orelly/networking/tcpip/ch02_05.htm, Dec 1 (1999).

[13] http://www.linuxjournal.com/article/5826, Aug 5 (2010).

Authors

박병호 (Byungho Park)

1995년 3월 : (일본) Tohoku University 정보과학과(전산학) 석사 졸업
1999년 3월 : (일본) Tohoku University 정보과학과(전산학) 박사 졸업
1995년 8월 ~ 2000년 4월 : 육군사관학교 전산학과 조교수
2001년 10월 ~ 2004년 2월 : 한국국방연구원 정보화연구센터 연구위원
2013년 1월 육군중령 예편 (국방부, 의무사, 3군사, 수도군단 전산실장 역임)
2013년 9월 ~ 현재 : 홍익대학교 컴퓨터정보통신공학과 초빙교수
관심분야 : 정보보호, 국방정보화, Formal Method, Testcase

신대철 (Daecheol Shin)

2000년 : 홍익대학교 전산계산학과 석사 졸업
2012년 : 한서대학교 디지털포렌직학 박사 졸업
2000년 4월 ~ 2009년 2월 : 한국인터넷진흥원 근무
2009년 3월 ~ 2010년 2월 : 한서대학교 겸임교수 및 포렌직연구소 부소장
2010년 3월 ~ 현재 : 서울시청 정보통신보안담당관(통합보안관제팀) 근무
관심분야 : 전자정부 보안, 정보보호관리체계(ISMS), 포렌직, 사이버테러 대응, 의료보안 등

나형두 (Hyeng-doo Na)

2008년 2월 아주대 정보보호학 석사 졸업
2011년 8월 숭실대 IT정책경영학 박사 졸업
2008년 4월 성균관대 경영대학원 국방핵심 MBA과정수료
2014년 2월 KAIST 경영대학원 전자정부 최고위관리자과정수료
1980년 3월 ~ 2009년 12월 국방전산정보원 개발팀장
2009년 1월 ~ 2010년 7월 지식경제부 우편정보과장
2010년 8월 ~ 현재 : 국방부 정보화기획관실 체계통합과장
관심분야 : 상호운용성, 정보보호, SW감리, PMO