ARP Spoofing을 이용한 LAN 클라이언트 접속 제어 기법

이건우* · 구상수**

계룡디지텍고등학교

Mechanism for Access Control to Clients in Intranet with Using ARP Spoofing

Geonwoo Lee* · Sangsoo Koo**

Kyeryong Digitech Highschool

E-mail : i1384992@naver.com / qwer44414@gmail.com

요 약

본 논문에서는 교육기관에서 이루어지는 컴퓨터 실습 등과 같이 사용자 호스트의 외부망 접속 제한이 필요한 때에, 저비용으로 간단히 접속 제어 시스템을 구축하는 기법을 제안한다. 제안된 기법은 중간자 공격 기법(Man In The Middle, MITM) 중 하나인 ARP Spoofing을 이용하여 LAN 클라이언트에서 출발한 패킷이 게이트웨이 바깥으로 포워딩되지 않도록 하는 방식으로 클라이언트의 외부망 접속을 차단한다. 따라서 클라이언트 호스트에 별도의 방화벽이나 Agent를 설치할 필요가 없기 때문에 간편하고 경제적인 시스템 구축이 가능하다.

ABSTRACT

This paper proposes mechanism to build a economical access control system when a user's host requires block to an external network, such as computer class conducted at educational institutions. The proposed mechanism is to block clients from accessing the external network by using the one of MITM(Man In The Middle) technique, ARP Spoofing. It prevents packets from being forwarded to outside by gateway. So It can build system simply and economically because Client hosts are don't need to install firewall or any extra agent.

키워드

ARP Spoofing, ARP Poisoning, MITM, Connection Control

Ⅰ. 서 론

우리가 사는 지금은 어느덧 제4차 산업 시대에 접어들었고, 주변의 거의 일들이 컴퓨터를 통하여 이루어지는 세상에 도래하였다. 또한 이 컴퓨터들은 네트워크로 상호 연결이 되어있으며, 네트워크를 통한 해킹 위협에 대비할 필요가 있다. 해커가 사용할 수 있는 네트워크를 기반으로 한 공격 기법은 크게 Scanning, Sniffing, Spoofing 등이 있다.

하지만 본 논문은 다른 시스템을 공격하기 위한 공격 기법도 실용적인 측면에서 사용될 수 있다는 것에 초점을 뒀다. 알려진 사례로는 문화체육관광부에서 웹툰 등 불법 유통 해외 사이트를 단속하는 것에 Spoofing 기법 중 하나로 알려진 DNS Spoofing 기법과 유사, 혹은 동일한 기법을 사용한 바 있다.

이 기법은 클라이언트 호스트에 별도의 Agent 설치가 필요 없기 때문에 전체적인 시스템의 구성이 용이하며 경제적이라는 장점을 지닌 ARP Spoofing을 이용한 LAN 클라이언트 접속 기법을 제안하고자 한다.

* speaker

** corresponding author

논문의 구성은 다음과 같다. Ⅱ장에서는 OSI 참조 모델과 ARP Protocol에 대해서 기술한다. Ⅲ장에서는 제안하는 기법에 대해서 기술한다. Ⅳ장에서는 실험 및 결과에 대하여 기술한다. 그리고 마지막 Ⅴ장에서 결론을 맺는다.

Ⅱ. OSI 참조 모델과 ARP Protocol

2.1 OSI 참조 모델 7계층

표 1과 같이 통신 기능을 7개 계층으로 분류하고 각 계층에 프로토콜을 규정한 표준을 'OSI(Open System Interconnection)' 참조 모델이라고 한다.

OSI 참조 모델에서 각 계층은 상위 계층의 요구에 따라 데이터를 한 단계씩 낮은 계층으로 전달하며 물리 계층에 가서는 다른 시스템의 물리 계층으로 데이터가 전달된다[1].

표 1. 계층별 프로토콜

7계층	Application Layer	HTTP, FTP 등
6계층	Presentation Layer	ASCII, JPEG 등
5계층	Session Layer	NetBIOS 등
4계층	Transport Layer	TCP, UDP 등
3계층	Network Layer	IP, ARP 등
2계층	Data Link Layer	Ethernet 등
1계층	Pysical Layer	UTP Cable 등

2.2 TCP/IP Protocol에서의 주소 지정

TCP/IP Protocol을 이용한 네트워크에서는 3개의 서로 다른 계층의 주소가 사용된다. 이는 Physical Address, Logical Address, Port Address이다.

Mac Address라고도 불리는 Physical Address,는 NIC(Network Interface Card)의 고유한 주소이며, 공장 출하 시부터 이미 정해진 상태로 생산된다. IP Address로 널리 알려진 Logical Address는 32비트의 주소체계를 사용한다. Port Address의 경우 Port Number라고도 부르는데, IP Address와 함께 사용된다. 대표적인 Port Number로는 HTTP/80, FTP/21 등이 있다.

2.3 ARP Protocol의 주소변환 기능

물리 주소와 논리 주소를 변환하는 방식에는 정적 변환과 동적 변환이 있다. 정적 변환은 로컬 시스템에서 물리 주소와 논리 주소의 매핑 테이블을 저장하였다가 필요시 검색하여 사용하는 방식이다. 이는 시스템 구조의 변화에 따른 변화를 위해 주기적으로 갱신되어야 하는데, 이는 많은 자원을 필요로 한다.

반면, 동적 변환은 그림 1과 같이 물리 주소와 논리 주소 중 하나만 알고 있을 때 ARP(Address Resolution Protocol)와 RARP(Reverse ARP)를 이용하여 다른 하나를 알아내는 방식이다[2].

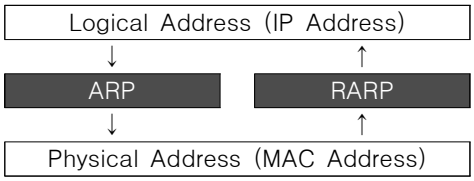
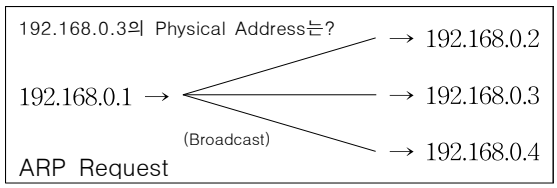


그림 1 ARP와 RARP를 이용한 동적 주소 변환

2.3 ARP의 동작 방식

ARP와 Logical Address를 통해서 Physical Address를 알아내는 과정은 다음과 같다.

① 송신자는 Routing Table에서 Next Hop의 IP 주소를 읽는다.
② IP는 Datagram을 큐에 저장해두고, Next Hop의 Physical Address를 알아내기 위해 ARP에게 서비스를 요청한다.
③ ARP는 "ARP Request Message"를 생성하여 Data Link Layer에 전달, Broadcast 한다.
④ Subnet의 모든 Host가 프레임을 수신하여 자신의 ARP에 전달한다.
⑤ 수신자의 ARP는 자신의 Physical Address를 "ARP Reply Message"통해 답장한다.
⑥ 송신자는 ARP Reply Message를 받고 목적지 시스템의 Physical Address를 알게 된다.



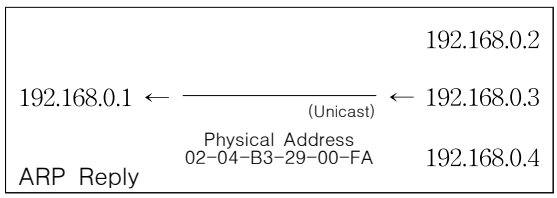


그림 2 ARP Request와 ARP Reply

2.4 ARP Protocol의 취약점

ARP Protocol이 갖는 취약점은 상호 간에 인증 절차가 없이 MAC Address를 교환한다는 것이다. ARP Request를 수신한 호스트는 패킷 출처를 프레임 안에 있는 정보에 기반을 두어 판단하게 되는데 이러한 정보는 간단히 조작이 가능하기 때문이다. 만약 Attacker가 악의적인 목적으로 Target에게 거짓 정보로 꾸며진 ARP Reply를 생성하여 전송한다면 Target은 이를 감지할 방법이 없다.

Trabelsi와 Shuaib의 연구에서 ARP Request와 Reply는 많은 운영체제에 인증 없이 적용된다고 보고된 바 있다[3].

2.5 ARP Spoofing의 동작 원리

LAN 호스트가 외부의 호스트와 통신을 하려면 그림 3과 같이 패킷이 여러 Hop을 거쳐 게이트웨이 너머의 망 바깥으로 Forwarding 돼야 한다.

그림 3 정상적인 네트워크

앞서 기술한 것과 같이 Attacker가 악의적인 목적으로 Target을 속이게 된다면 Target은 Attacker의 NIC 주소가 Gateway인 것으로 인지하게 된다.

이후 Attacker의 NIC로 넘어온 패킷을 실제 Gateway에 정확히 Forwarding 해준다면 그림 4와 같이 Target 호스트가 알아차리지 못하게 Sniffing 할 수 있을 것이다.

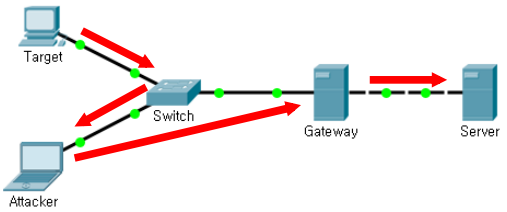


그림 4 공격받고 있는 네트워크

III. 제안하는 기법

본 논문이 제안하는 기법은 ARP Spoofing을 이용한 LAN 클라이언트 접속 제어 기법이다. 제안된 기법은 LAN의 특정한 Target 호스트에 대하여 외부망 연결 제한이 필요할 때에 ARP Reply Message를 이용, 다른 호스트들이 이용하는 실제 Gateway의 Mac Address와 다른 Mac Address를 제시하여 Target 호스트에서 출발한 패킷이 Gateway 너머로 Forwarding 되지 않도록 한다. 제안된 기법은 LAN의 클라이언트를 비롯하여 Gateway까지 아무런 별도의 Agent를 설치할 필요가 없으며, 시스템 운영을 위해 네트워크에 추가로 방화벽을 구성할 필요도 없기 때문에 경제적이고 효율적인 환경을 구축할 수 있다. 제안된 기법은 한 대의 호스트에 Transmission Tool의 설치를 요하며, 이는 지정된 Target의 IP로 반복해서 ARP Reply Packet을 전송한다. Transmission Tool은 Target IP를 입력받아, 사용자의 명령이 있을 때 해당 IP로 ARP Reply 패킷을 전송한다. 또한 Target 호스트의 ARP Cache가 정상 값으로 갱신되지 않도록 사용자가 중지 명령을 내릴 때 까지 반복하여 다시 전송한다.

IV. 실험 및 결과

실험은 VMWare Workstation 14 Pro를 이용, Virtual Machine을 생성하고 그림 5와 같이 네트워크를 구성하여 진행하였다. OS는 Windows Server 2016, Windows 10, Ubuntu 18.04.1 LTS를 사용했으며 패킷 모니터링 툴로는 Wireshark를 사용했다.

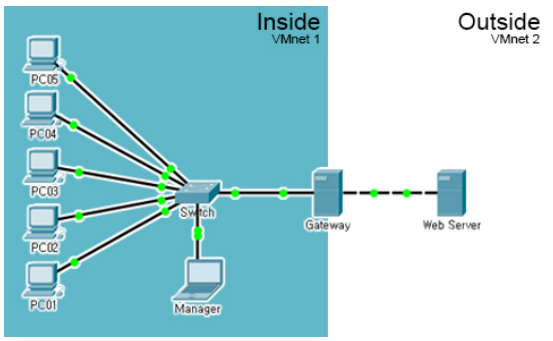


그림 5 실험 네트워크 토폴로지

먼저 Gateway 너머 Oustside의 Web Server에 웹 페이지 “www.virtual.lab”을 구성하고 먼저 클라이언트 등에서 정상적으로 접속이 되는지 확인하였다. 그림 5를 보면 Gateway에 Mac Address 00-0c-29-d7-13-1d가 매핑된 것을 확인할 수 있다.

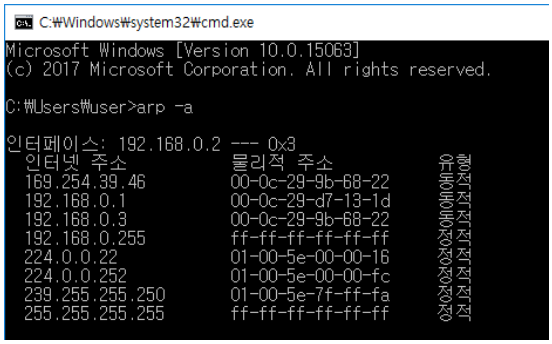


그림 6 변조되지 않은 ARP Table

이후 Manager에 설치된 Transmission Tool에서 Target을 입력한 다음 정상적으로 연결이 차단되는지 확인하였다. 그림 7을 보면 Gateway에 매핑된 Mac Address가 변조된 것을 확인할 수 있다.

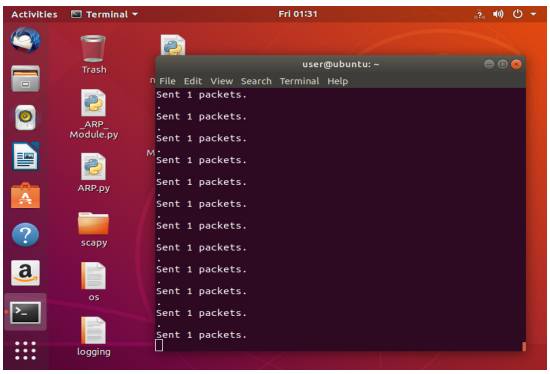


그림 7 패킷을 전송중인 Transmission Tool

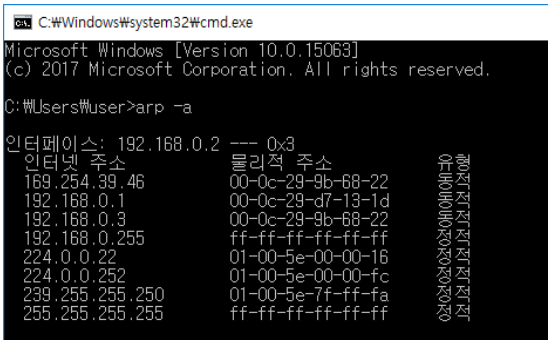


그림 8 변조된 ARP Table

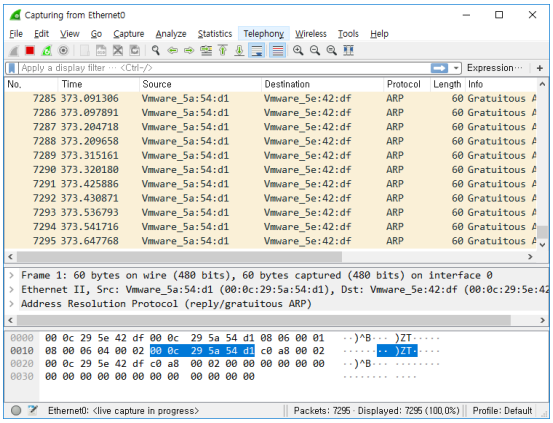


그림 9 Target 호스트에 도착한 ARP 패킷

물론 게이트웨이로 접근이 불가능해진 Target 호스트는 그림 8과 같이 외부 망으로의 접근이 불가능 해진다.

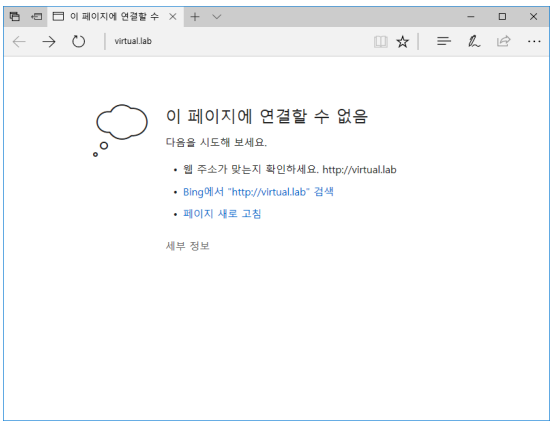


그림 10 “www.virtual.lab”에 접속을 시도한 화면

Ⅴ. 결 론

본 논문에서는 ARP Spoofing을 이용하여 Target 호스트의 ARP Table을 변조시켜 패킷이 Gateway까지 도달할 수 없도록 하는 방식으로 저비용의 경제적인 클라이언트 접속 제어 시스템을 구축하는 기법을 제안했다. 제안한 기법은 별도의 어떤 장비와 소프트웨어도 필요로 하지 않는다. Transmissoin Tool이 설치된 호스트에 Web Server를 설치하여 Target 호스트에서 웹 페이지 접속 시 에러 메시지가 아닌 접속 차단 메시지가 나타나도록 한다면 더욱 실용적일 것으로 예상된다.

References

[1] H. J. Jin, *an Introduction of Network*, Seoul, Korea: HANBIT Academy, Inc, 2014.

[2] H. Y. Lee, *Proposition And Implementation of A Model with Address Information Management Server for Detection and Prevention of ARP Spoofing*, Master Thesis, Kyungpook National University, 2008.

[3] Z. Trabelsi and K. Shuaib, “Spoofed ARP Packets Detection in Switched LAN Networks”, *E-Business and Telecommunication Networks Communications in Computer and Information Science*, Vol 9, No.-, p 81-91, 2008