ARP Spoofing 공격 분석 및 대책

2007. 6

KrCERT/CC
인터넷침해사고대응지원센터

KISA 한국정보보호진흥원
Korea Information Security Agency

1. ARP Spoofing 공격 개요

최근 해외로부터의 홈페이지 해킹 후 악성코드를 삽입하는 사건들이 다수 발생되고 있는데, 이 사고들은 대부분 해당 웹서버가 직접 해킹당한 후 악성코드가 삽입되어졌다. 그런데, 최근 들어 웹서버는 전혀 해킹을 당하지 않았음에도 불구하고 해당 웹서버로부터 악성코드가 다운로드 되는 사건이 발생했다. 이 사건은 공격자가 동일한 IP 세그먼트 내의 다른 서버를 해킹한 후 ARP Spoofing을 이용하여 특정 웹서버와 관련된 웹 트래픽을 가로채어 악성코드를 삽입한 사례였다.

ARP Spoofing 공격은 로컬 네트워크(LAN)에서 사용하는 ARP 프로토콜의 허점을 이용하여 자신의 MAC(Media Access Control) 주소를 다른 컴퓨터의 MAC인 것처럼 속이는 공격이며, ARP Cache 정보를 임의로 바꾼다고 하여 "ARP Cache Poisoning 공격"이라고도 한다.

과거의 더미 허브 환경에서는 쉽게 Sniffing이 가능하였지만, 최근에는 대부분 스위치 환경으로 네트워크를 구성하며, 이러한 스위치 환경에서는 해당 MAC을 가진 컴퓨터에게만 패킷이 전달되므로 더미 허브 환경에 비해 Sniffing이 쉽지 않다. 하지만 공격자들은 자신의 MAC 주소를 라우터 또는 Sniffing하고자 하는 대상 서버의 MAC 주소로 위장(ARP Spoofing)하여 스위치 환경에서도 패킷을 Sniffing할 수 있다. 그리고 이러한 Sniffing 수법은 이미 오래전에 분석보고서[1]가 나와 있었고, 널리 알려져 있던 수법이었다.
하지만, 최근 발견된 몇 건의 사고들을 통해 ARP Spoofing 기법이 단순히 패킷을 가로채어 훔쳐보는 Sniffing 수준이 아니라, 가로챈 패킷을 변조한 후 전송하는 공격에도 사용되고 있음을 알 수 있었다.

한 서버가 아무리 안전하게 구축되어 해킹당할 염려가 없다고 하더라도, 해당 서버가 포함된 네트워크 내에 취약한 서버가 있을 경우 ARP Spoofing 공격으로 쉽게 데이터가 유출되거나 변조될 수도 있다. 또한, 다수의 서버들이 밀집해 있는 IDC환경에서 별도의 서브네트워크로 구성되지 않은 경우, 타 업체 서버의 보안문제점이 자사의 보안문제로 전이될 수 있음을 보여준다.

ARP Spoofing 기법은 금융기관 등을 사칭하는 피싱 또는 파밍 공격에도 사용될 수 있다. 사용자가 금융사이트 접속을 위해 DNS 요청을 할 경우, 공격자는 ARP Spoofing 기법을 이용하여 위장 사이트의 IP 주소를 사용자에게 보냄으로써 위장 사이트로 접속을 유도할 수도 있다.

1) http://www.krcert.or.kr ⇒ 보안정보 ⇒ 기술문서 ⇒ 문서번호 TR2000006

또한, 지난 4월 중국 언론에 따르면 중국 청화 대학교에서 100 여대의 PC가 "ARP Spoofing" 바이러스에 감염되어 대학 내 1만여대의 PC가 간접적인 피해를 입은 바 있다고 밝혔다[1]. ARP Spoofing 공격은 데이터의 유출 및 변조뿐만 아니라 네트워크 내의 한 대의 PC만 감염되더라도 내부 컴퓨터들에게 위장된 Gateway의 MAC 주소를 전파함으로써 쉽게 전체 네트워크의 장애를 유발시킬 수 있다.

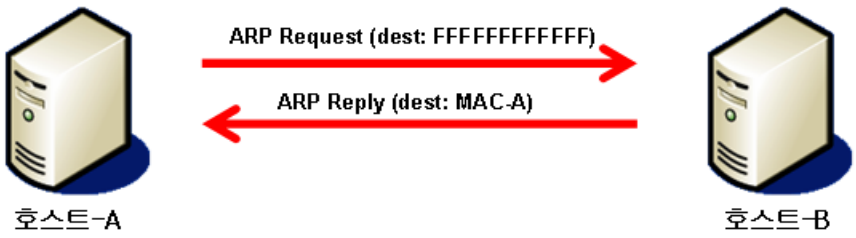
이처럼 ARP Spoofing 공격은 다양하게 악용가능하고 피해도 심각할 수 있는 반면 공격에 대한 탐지와 대응은 쉽지 않다. ARP Spoofing의 공격대상은 자신의 시스템이 직접 해킹당한 것이 아니므로 피해 사실조차 파악하기 어렵다.

본 문서에서는 ARP Spoofing 공격의 원리와 주요 사례를 통해 공격기법을 이해하고, 이에 대한 탐지와 대응방안을 검토해 보도록 한다.

2. ARP Spoofing 공격 기법의 이해

브로드캐스팅 트래픽이 제한되는 이더넷 스위치를 사용하는 IP 기반 네트워크에서는 타 시스템간의 트래픽에 접근하는 데 제한이 있기 때문에 도청하기가 쉽지가 않다. 하지만 ARP Spoofing에 "man-in-the-midddle" 공격 수법을 추가하여 앞에서와 같은 문제를 충분히 우회할 수 있다. 공격자는 잘 조작된 MAC 주소를 스위치 상에 ARP Reply 함으로써 원래는 다른 곳으로 전달되어야 할 데이터 패킷을 수신할 수 있다. 이러한 방법으로 공격자는 게이트웨이를 가장하여 원하는 서버의 모든 트래픽을 도청하여 데이터 수집 및 가공이 가능하다.

가. 이더넷/IP 통신에 대한 이해

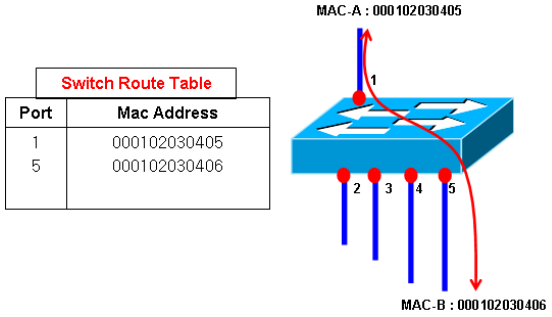


(그림 1) Layer2 계층의 두 호스트 간 통신

호스트-A가 호스트-B와 통신하기 위해서 Layer2 계층의 통신 흐름은 다음과 같다.

1) http://www.cnsec.co.kr ⇒ 뉴스 ⇒ "ARP스푸핑 바이러스 전파, 대학교 기숙사 컴퓨터 인터넷 접속 불가"

1) 호스트-A : 자신의 로컬 ARP Cache에 호스트-B IP/MAC 주소의 매핑이 존재 하는지 검사
2) 호스트-A → ARP Request : 호스트-B IP의 MAC 주소에 대한 ARP 요청을 브로드캐스팅
3) 호스트-B → ARP Reply : 호스트-B의 IP와 MAC 주소를 담은 ARP 응답을 호스트-A에게 전송
4) 호스트-A : ARP Cache 업데이트

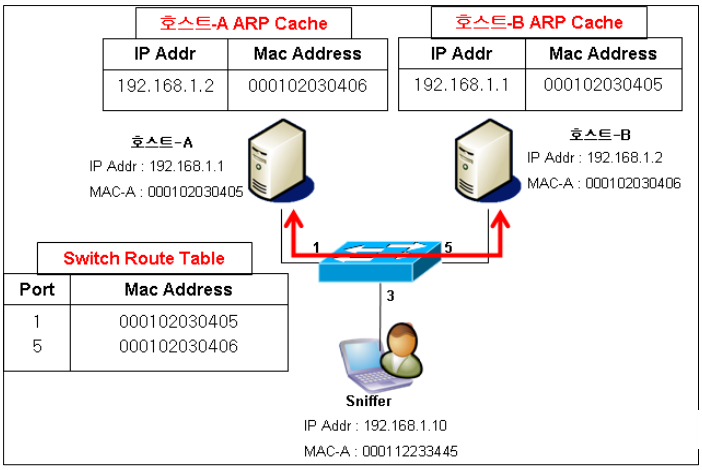


(그림 2) 두 호스트 간 스위치 통신

Layer2 장비인 스위치는 앞서 봤던 단계에 따라 이더넷 프레임으로부터 MAC 주소를 추출하여 위와 같은 Switch Route Table을 작성한다. 위의 2)번 단계가 진행되면 1번 포트에 MAC-A(호스트-A) 주소를 테이블에 등록하고 3)번이 진행된 후 5번 포트에 MAC-B 주소를 등록한다. 이후 테이블에 등록되어 매칭된 포트와 MAC 주소를 통해서 통신을 하게 된다.

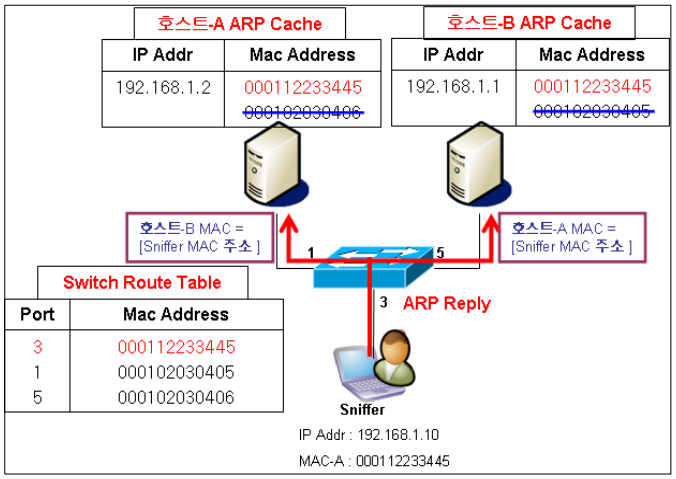
나. ARP Spoofing 공격 기법

스위치는 모든 트래픽을 MAC 주소를 기반으로 해서 전송하게 된다. 공격자는 LAN상의 모든 호스트 IP-MAC 주소 매핑을 ARP Request 브로드캐스팅을 통해 정확하게 알아 낼 수 있어 공격자에게 악용될 수 있다. 아래 (그림 3)은 호스트-A와 호스트-B의 정상적인 스위치 상에서의 트래픽이 전송되는 모습이다.



(그림 3) 정상적인 통신

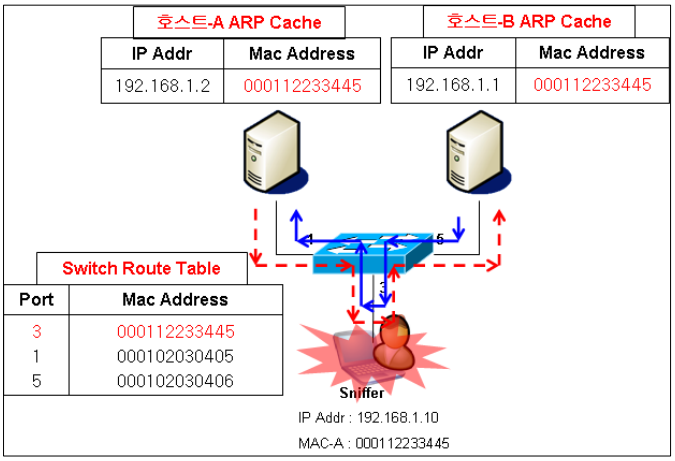
ARP 프로토콜은 인증을 요구하는 프로토콜이 아니기 때문에 간단한 ARP Reply 패킷을 각 호스트에 보내서 쉽게 ARP Cache를 업데이트시킬 수 있다. (그림 4)처럼 스니퍼는 각 호스트들에게 위조한 MAC 주소(상대방의 MAC 주소 = 스니퍼 MAC 주소)를 보내 각 호스트의 ARP Cache를 업데이트 시키게 되고 스위치에서는 스니퍼의 MAC 주소와 포트 매핑 정보가 테이블에 등록된다.



(그림 4) ARP Spoofing 공격

계속해서 스니퍼는 Cache가 사라지기 전에 변조된 ARP Reply를 지속적으로 보내므로 각 호스트들의 ARP Cache의 변조된 MAC 주소의 정보는 계속해서 유지된다. 이때 스니퍼는 두 방향으로 정확히 재전송해 줄 수 있는 기능이 있어야만 호스트 A와 B는 통신을 할 수 있다.

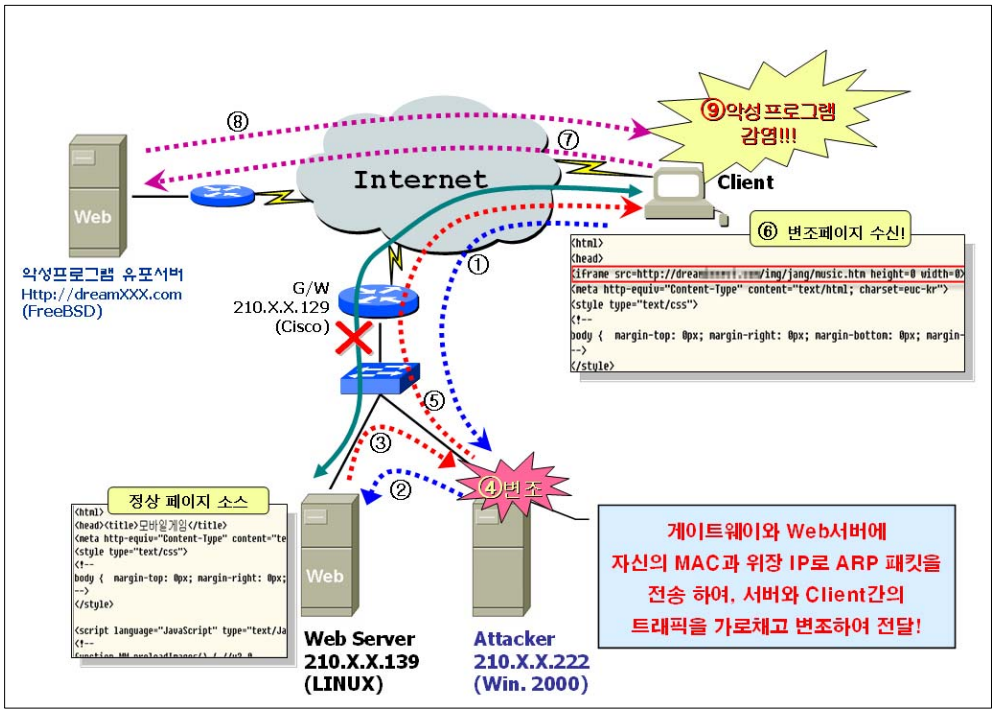
공격에 성공하면 두 호스트는 서로의 MAC 주소를 스니퍼의 MAC 주소로 인식하고 있기 때문에 모든 트래픽을 스니퍼에게 전달하게 된다. 스니퍼는 이 두 호스트에게 재전송할 수 있는 기능이 있으며 또한 모든 패킷들을 캡쳐 할 수 있게 된다.



(그림 5) ARP Spoofing후 스니핑

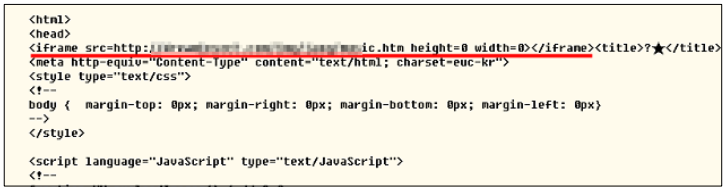
3. ARP Spoofing 공격 사례 및 도구

가. 웹페이지 악성코드 삽입 사례



(그림 6) 침해사고 개요도

웹 서버의 경우 공격자에 의해 직접적인 공격을 받지 않았음에도 불구하고 피해시스템과 같은 브로드캐스팅 도메인 네트워크 대역에 존재한다는 이유로 피해를 보게 된 것이다. 원격의 클라이언트 인터넷 브라우저로 웹 서버(210.X.X.139)에 접속하게 되면, (그림 7)과 같이 모든 HTML페이지에 악성 프로그램 설치를 유도하는 코드가 삽입되어 있었다.



(그림 7) 접속자 브라우저에서 수신한 웹 페이지

하지만 실제 웹사이트의 페이지들에서 iframe 코드는 전혀 보이지 않았고, 웹서버에서 클라이언트에게 보내는 패킷을 tcpdump로 확인해 보면 서버의 이더넷 카드를 통해 나갈 때 까지도 iframe 코드가 삽입되지 않은 것을 확인할 수 있었다.

원인분석 결과 동일한 네트워크 내의 취약한 윈도우 서버(210.X.X.222)가 해킹을 당해 ARP Spoofing 공격에 이용되었으며, ARP Spoofing에 이용된 서버는 게이트웨이에게 자신이 마치 웹서버인 것처럼 속이고, 웹서버에게는 자신이 마치 게이트웨이인 것처럼 속여 웹서버와 게이트웨이 사이의 웹 패킷을 가로채서 악성코드를 삽입하는 방법을 사용하였다.

나. ARP Spoofing 공격 도구

앞서 살펴 본 사례에서 ARP Spoofing 공격 서버에서 3가지 도구가 발견되었으며 이러한 도구들은 공격자가 상당히 쉽게 ARP Spoofing할 수 있도록 구성되어 있었다.(본 문서에서는 공격 툴 악용을 방지하기 위해 “공격 툴 A, B, C”로 부르며, 공격 툴에 대한 상세분석 내용은 제외함)

o 공격 툴 A

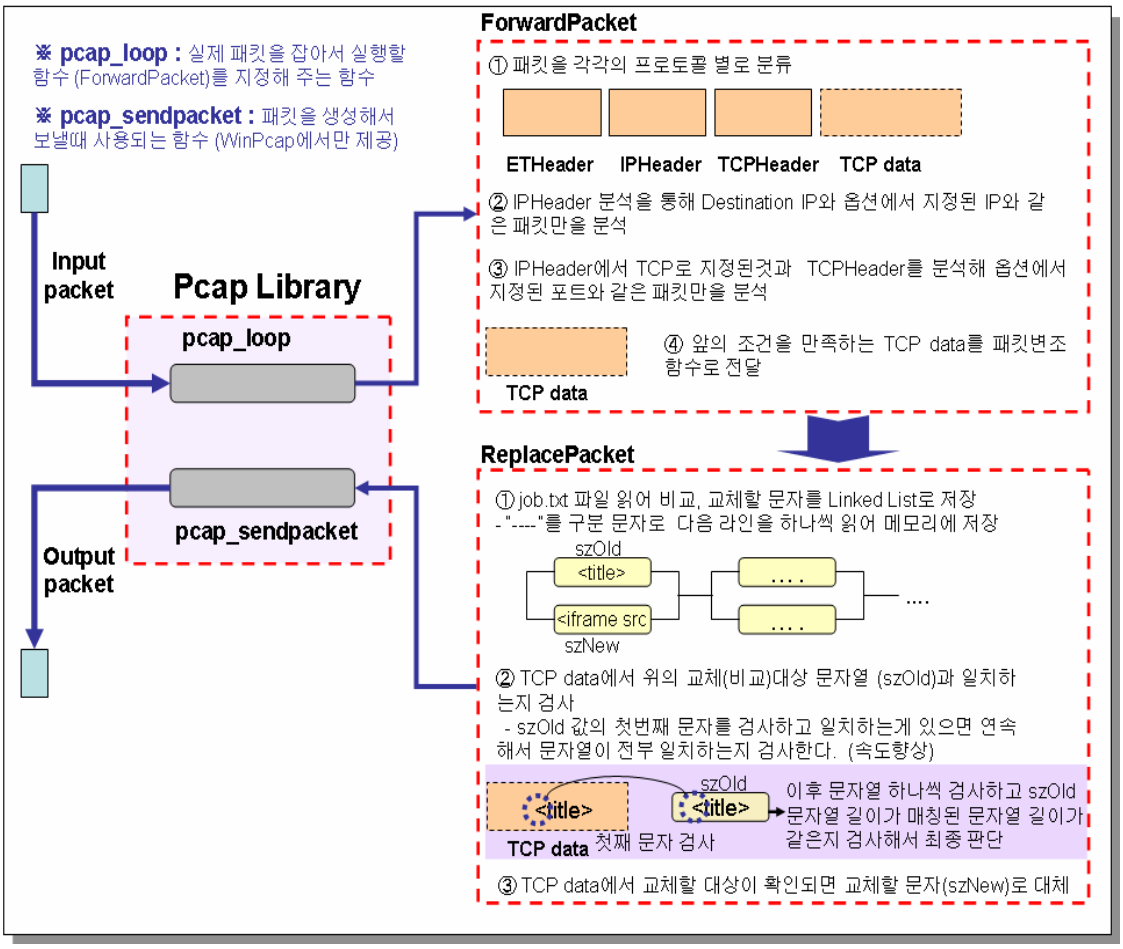
"공격 툴 A"는 네트워크 트래픽을 도청하고 트래픽에서 나오는 패스워드를 수집하거나 암호화된 정보를 크랙해주는 윈도우즈 GUI 도구이다. 이 도구는 ARP Spoofing 공격을 통해 같은 브로드캐스팅 도메인 네트워크에 존재하는 PC나 서버의 트래픽을 모니터링하거나 각종 응용프로그램들의 패스워드들을 모니터링 할 수 있다. “공격 툴 A"의 공격 절차는 아래와 같다.

- 서브넷의 모든 호스트 MAC 주소 스캔
- ARP Spoofing 대상 선택
- ARP Spoofing 공격
- 관련 어플리케이션 패스워드 모니터링

“공격 툴 A"를 사용하면 응용프로그램들 (FTP, HTTP, POP, SIP)의 평문으로 전송되는 아이디/패스워드를 가로챌 수 있다.

o 공격 툴 B

“공격 툴 B”는 실제 웹페이지에 악성코드를 삽입하는 역할을 하였다. 이 툴은 WinPcap 라이브러리를 사용해서 프로그래밍 되어 있으며 패킷을 변조하는 부분은 아래와 같은 구조로 프로그램이 작성되어 있었다.



(그림 8) "공격 툴 B" 동작 과정

o 공격 툴 C

"공격 툴 C"는 최근 사고 분석에서 확인된 ARP Spoofing 공격 도구로 이전 "공격 툴 B" 보다도 훨씬 다양한 기능을 추가하고 있었다.

- 홈페이지 접속 아이디, 패스워드 도청
  지정된 IP 영역의 웹 트래픽을 Sniffing 하면서 원하는 키워드 값이 나타나면 아이디, 패스워드를 캡쳐하여 파일로 기록한다.

- iframe 악성 스크립트 삽입
  공격자가 지정한 IP 대역에서 외부로 접속하는 사용자 웹 패킷이나 지정된 대역으로 접속해 들어오는 사용자 웹 패킷 양쪽 모두에 iframe을 삽입할 수 있다. 즉, 외부에서 내부 웹서버로 접속하는 클라이언트에게도 iframe을 삽입할 수 있고, 내부에서 외부로 접속하는 내부 사용자에게도 iframe을 삽입할 수 있는 것을 확인할 수 있다.

- DNS 스푸핑
  DNS Reply를 조작하여 특정 웹사이트로 접속 하고자 하는 패킷은 모두 조작된 사이트로 접속시킬 수 있다.

- 다운로드 파일 교체
  Sniffing 대상 호스트들이 내·외부로 웹을 통해 파일을 다운로드 할 경우 공격자가 지정한 사이트 특정 사이트의 악성 프로그램을 다운받을 수 있게 할 수 있다.

4. ARP Spoofing 공격 탐지 방법

ARP Spoofing 공격은 Subnet 내의 한 대의 시스템만이 해킹을 당하더라도 여러 서버에 영향을 미칠 수 있으므로 공격에 대한 탐지가 쉽지만은 않다. 본 장에서는 ARP Spoofing 공격 시 나타나는 증상을 토대로 ARP Spoofing 대상 서버(공격 대상 서버), 공격서버, 네트워크 장비에서 각각 공격을 탐지할 수 있는 방법을 소개한다.

가. ARP Spoofing 발생 시 증상

1) 피해 시스템에서의 증상

o 네트워크 속도 저하
- ARP Spoofing을 위해 서버와 클라이언트 같은 종단간의 통신을 가로채어 재전송하는 시스템이 있기 때문에 네트워크 속도의 저하가 발생한다.

o 악성코드가 웹 페이지 시작부분에 위치
- 패킷을 가로챈 후 변조하는 경우에는 대부분의 웹 페이지가 공통적으로 사용하는 태그를 인식하여 악성코드를 삽입하기 때문에 웹 페이지가 시작되는 head, title 등의 태그 주변에 삽입한다. 그 이유는 패킷의 중간이나 끝부분에 삽입하고자 하면 TCP 패킷의 전송 특성상 대체하고자 하는 문자열이 분리(fragmentation)와 재조합 과정에서 나누어져서 문자열을 인식할 수 없는 가능성이 있기 때문이다.

o 정기적인 ARP 패킷 다량 수신
- 피해 시스템에서 관리하는 ARP table을 계속해서 변조한 상태로 유지하기 위해 공격자는 조작한 ARP 패킷을 지속적으로 발송하므로, ARP패킷의 수신량이 증가된다.

2) 공격 시스템에서의 증상

o 네트워크 사용량 증가
- 타 시스템간의 통신을 가로챈 후 재전송하게 되므로, 네트워크 사용량이 증가하게 된다.

o 정기적인 ARP 패킷 발송
- 피해 시스템의 ARP table을 지속적으로 속이기 위해 정기적으로 ARP 패킷을 발송한다.

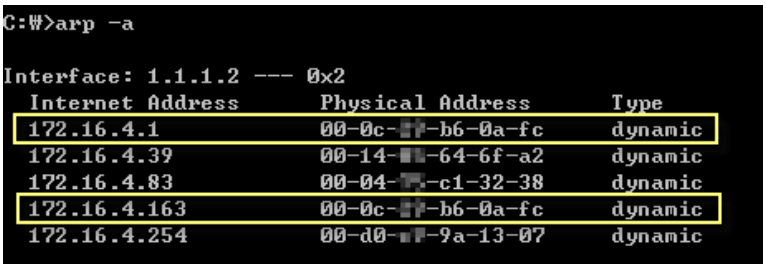
o 악성 프로그램의 프로세스 동작
- ARP Spoofing과 트래픽 변조를 위한 프로그램의 프로세스가 동작한다.

나. 피해 시스템에서의 탐지 방법

1) ARP table 조회를 통한 MAC 주소 중복 확인

윈도우즈나 유닉스/리눅스 계열 모두 arp -a 명령과 같이 ARP table을 조회하는 명령으로 주변 시스템의 IP와 MAC주소를 확인한다. 단, 평소에 통신을 하지 않던 시스템의 MAC주소도 확인해야 하므로, 동일 서브네트워크의 모든 host에 ping 명령이나 nmap등의 도구를 사용하여 IP와 MAC주소를 모두 확보 한 후에 확인해야 한다. 대부분의 경우 게이트웨이의 IP와 MAC주소로 위장하기 때문에 이 부분을 유심히 살펴본다. 만약 게이트웨이의 MAC주소가 실제 게이트웨이의 MAC주소와 다르다면 ARP Spoofing으로 인한 결과일 확률이 대단히 높다.

또한, ARP table에 동일한 MAC주소가 서로 다른 IP에서 사용되고 있는지 확인한다. 즉, 아래 그림의 경우처럼 게이트웨이 IP(172.16.4.1)에서 사용하는 MAC을 다른 IP(172.16.4.163)도 사용하고 있다면, ARP Spoofing을 의심해 볼 수 있다. 다만, 시스템 설정에 따라 하나의 NIC에 여러 IP를 사용 할 수도 있고, ARP Spoofing을 수행하는 시스템에 IP를 넣지 않는 경우 등은 예외이다.



2) 송수신 패킷에서 악성코드 유무 검사

tcpdump[1], 이더리얼[2], 와이어샤크[3], 이더피크[4], 패킷뷰어[5] 등의 패킷분석 도구를 사용하여 실제로 서버로부터 송신되는 패킷에 악성코드가 삽입되어 있는지 확인 해 본다. 만약 송신되는 패킷내에 iframe등을 악용한 악성코드가 있다면 ARP Spoofing공격으로 인한 사고가 아니라, 서버 내부에 악성코드가 존재하는 것이므로 ARP Spoofing이 아닐 것이다. 하지만 서버로부터 송신되는 패킷에는 아무런 악성코드가 없는데, 클라이언트가 수신하는 패킷에 악성코드가 삽입되어 있다면 ARP Spoofing으로 인해 패킷이 변조되었을 가능성이 대단히 높다.

tcpdump를 활용 할 경우에는 서버로부터 전송되는 패킷에 악성코드가 있는지를 확인해 보기 위해 "tcpdump -w [log파일명] -s 1500 port 80" 과 같은 명령으로 송신되는 패킷을 저장한 후 "tcpdump -Xqnr" 명령으로 저장된 패킷을 ACII모드로 변환하여 조회 해 본다. 아래의 그림처럼 송신되는 패킷에는 악성코드가 삽입되어 있지 않다면 ARP Spoofing과 패킷변조를 의심해 볼 수 있다.

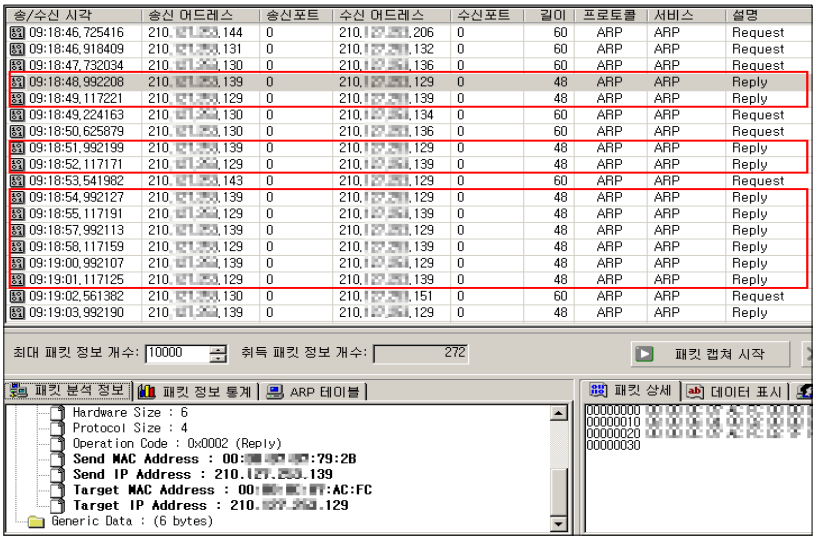
```
[root@victim]# tcpdump -w log_file_name -s 1500  port 80
tcpdump: listening on eth0

11 packets received by filter
0 packets dropped by kernel
[root@victim]# tcpdump -Xqnr log_file_name
.
.
.
0x0000   4500 016a 1643 4000 4006 e82a d27f fd8b        E..j.C@.@..*....
0x0010   d3fc 9718 0050 516c bfd3 37a9 0edb 6395        .....PQl..7...c.
0x0020   5018 1920 e143 0000 4854 5450 2f31 2e31        P....C..HTTP/1.1
0x0030   2032 3030 204f 4b0d 0a44 6174 653a 2046        .200.OK..Date:.F
0x0040   7269 2c20 3236 204a 616e 2032 3030 3720        ri,.26.Jan.2007.
0x0050   3134 3a35 373a 3234 2047 4d54 0d0a 5365        14:57:24.GMT..Se
0x0060   7276 6572 3a20 4170 6163 6865 2f31 2e33        rver:.Apache/1.3
0x0070   2e33 3420 2855 6e69 7829 2050 4850 2f34        .34.(Unix).PHP/4
0x0080   2e34 2e31 0d0a 582d 506f 7765 7265 642d        .4.1..X-Powered-
0x0090   4279 3a20 5048 502f 342e 342e 310d 0a4b        By:.PHP/4.4.1..K
0x00a0   6565 702d 416c 6976 653a 2074 696d 656f        eep-Alive:.timeo
0x00b0   7574 3d35 2c20 6d61 783d 3130 300d 0a43        ut=5,.max=100..C
0x00c0   6f6e 6e65 6374 696f 6e3a 204b 6565 702d        onnection:.Keep-
0x00d0   416c 6976 650d 0a54 7261 6e73 6665 722d        Alive..Transfer-
0x00e0   456e 636f 6469 6e67 3a20 6368 756e 6b65        Encoding:.chunke
0x00f0   640d 0a43 6f6e 7465 6e74 2d54 7970 653a        d..Content-Type:
0x0100   2074 6578 742f 6874 6d6c 0d0a 0d0a 3530         text/html....50
0x0110   200d 0a3c 6874 6d6c 3e0d 0a3c 6865 6164        ...<html>..<head
0x0120   3e0d 0a3c 2f68 6561 643e 0d0a 3c62 6f64        >..</head>..<bod
0x0130   793e 0d0a 6b69 7361 0d0a 3c2f 626f 6479        y>..kisa..</body
0x0140   3e0d 0a3c 7469 746c 653e 2074 6573 7420        >..<title>.test.
0x0150   3c2f 7469 746c 653e 0d0a 3c2f 6874 6d6c        </title>..</html
0x0160   3e0d 0a0d 0a30 0d0a 0d0a                        >....0....
```

1) http://www.tcpdump.org/
2) http://www.ethereal.com
3) http://www.wireshark.org
4) http://www.wildpackets.com/products/etherpeek/overview
5) http://www.krcert.or.kr ⇒ 센터자료실 ⇒ 보안도구

3) 비정상적인 ARP 패킷 수신 확인

ARP Spoofing공격이 실행되고 있을 때, 피해서버 측에서 ARP 패킷을 수집하여 분석해 보면 필요 이상의 reply 패킷이 수신되고 있음을 알 수 있다. 서버들의 경우 인터넷서비스를 위해 계속해서 게이트웨이와 통신을 하기 때문에 게이트웨이의 MAC주소가 ARP table에서 삭제되지 않으므로, 수 초마다 계속해서 request가 없는 ARP reply패킷만 수신될 이유가 없다.



(그림 9) 위장 ARP Reply 다량 수신

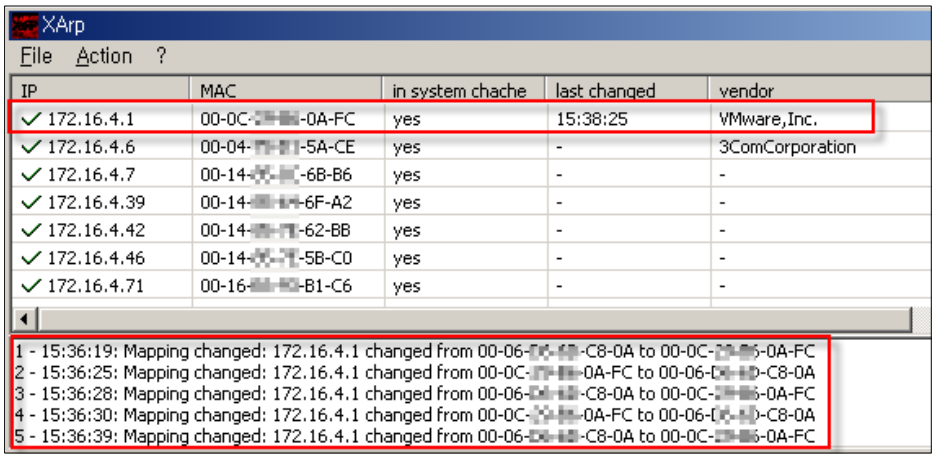
리눅스 서버의 경우 tcpdump arp 명령으로 수신되는 ARP 패킷들을 관찰 할 수 있으므로, MAC주소를 위장하기 위한 ARP 패킷이 주기적으로 수신되는지 확인해 본다.

4) ARP table 감시 도구 활용

윈도우즈 계열의 ARP table 감시 도구는 sniffswitch[1], XArp 등이 있는데, 본 문서에서는 프리웨어이면서 사용하기 쉬운 XArp를 예로 들어 설명한다. 이 도구를 다운로드 받을 수 있는 곳은 http://www.chrismc.de/ 이며, 2.0버전[2]도 있지만 ARP Spoofing을 감시하기 위한 용도로는 v.0.1.5 도 충분하다. 이 프로그램을 실행하면 ARP table의 cache 상태를 나타내며, ARP table에서 동일 IP에서 MAC주소가 변경된 시점의 시간이 표시된다.

1) http://www.nextsecurity.net/
2) http://www.chrismc.de/developing/xarp/XArp_screenshot_advanced_view.png

아래의 그림은 XArp의 실행화면이며, ARP Spoofing으로 인해 게이트웨이의 MAC주소가 계속해서 변경됨을 보여준다.



(그림 10) XArp를 활용한 ARP 테이블 감시

위장한 ARP패킷에 의한 MAC주소의 변경을 모니터링 할 수 있는 가장 효과적인 방법은, 정상적인 상태에서의 ARP table을 저장해 두고 비교 해 보는 것이다. 유닉스 시스템에서는 arpwatch[1]와 같은 도구를 활용하여 모니터링 할 수 있다.

다. 공격 시스템에서의 탐지 방법

1) ARP Spoofing 실행 프로그램 확인

o 패킷 캡쳐 프로그램 존재 유무 확인

- 윈도우즈 계열의 경우 가장 먼저 확인해 봐야 할 점검 항목으로는 WinPcap과 같은 패킷 캡쳐 라이브러리가 설치되어 있는지의 여부이다. 일반적인 서버 운용상에서는 이러한 라이브러리가 설치되는 경우가 많지 않으므로, 설치되어 있다면 설치된 일시를 확인하고 관리자에 의한 설치가 맞는지 확인 해 봐야 한다.

o 네트워크 어댑터의 동작 상태 확인

- ARP Spoofing도 Sniffing 활동이므로 네트워크 어댑터(NIC)의 동작 상태가 “promiscuous mode“로 동작 중 인지 확인 해 본다. 유닉스나 리눅스 계열의 경우 ifconfig 또는 dmesg등을 통해 쉽게 확인 할 수 있으며, 윈도우즈 계열의 경우

1) http://ee.lbl.gov/

PromiscDetect[1] 라는 도구를 활용하여 확인 할 수 있다.

```
[root@localhost ~]# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:0C:29:CD:BA:8E
          inet addr:192.168.48.128  Bcast:192.168.48.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fecd:ba8e/64 Scope:Link
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:20649 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6520 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2296094 (2.1 MiB)  TX bytes:490359 (478.8 KiB)
          Interrupt:10 Base address:0x1080
```

```
[root@localhost ~]# dmesg | grep promi
device eth0 entered promiscuous mode
device eth0 left promiscuous mode
device eth0 entered promiscuous mode
device eth0 left promiscuous mode
device eth0 entered promiscuous mode
device eth0 left promiscuous mode
device eth0 entered promiscuous mode
```

단, 해당 시스템에서 정상적으로 설치/운용되는 네트워크 모니터링 프로그램(snort, 방화벽 등)이 동작중이라면 promiscuous mode가 정상적일 수 있다.

o ARP 패킷 관찰

- ARP Spoofing을 실행중인 시스템이라면 지속적으로 위장된 ARP패킷을 보내기 때문에 앞서 살펴본 tcpdump, 패킷뷰어 등의 네트워크 모니터링 도구를 활용하여 관찰해 보면 확인 할 수 있다. 만약 ARP Spoofing공격을 실행하는 시스템이라면 지속적인 ARP패킷 전송 외에도 타 시스템 간에 통신하는 패킷들이 보일 것이며, 동일한 패킷이 한 쌍의 단위로 나타나는 것을 관찰 할 수 있는데, 그 이유는 타 시스템 간의 전송 패킷을 가로챈 것과 재전송 한 패킷이 존재하기 때문이다.

라. 네트워크 장비에서의 탐지 방법

o ARP table 확인

- Host 시스템에서 확인한 방법과 마찬가지로 해당 서브네트워크에 대한 모든 IP-MAC주소를 확인하여, 동일한 MAC주소를 사용하는 IP들이 있는지 확인한다.

1) http://ntsecurity.nu/toolbox/promiscdetect/

o 패킷 모니터링 기능 활용

- 유입되는 패킷들의 모니터링 기능을 활용하여, 불필요한 ARP 패킷들이 탐지되는지 또는, 특정 스위치 포트나 연결되어 있는 호스트의 MAC주소가 자주 변경되는지 확인해 본다.

5. ARP Spoofing 공격 방지 대책

가. 시스템에서의 방지 대책

1) 정적인 ARP table 관리

윈도우즈계열에서 사용하는 시작/종료 스크립트에 정적으로 관리하고자 하는 시스템의 IP와 MAC 주소를 입력하는 스크립트를 지정하거나, 리눅스계열에서의 rc3.d와 같이 시작 스크립트를 기동하는 곳에서 스크립트를 실행하도록 하여 재부팅 시에도 항상 정적인 ARP table이 관리될 수 있도록 한다. 아래는 윈도우즈 계열의 경우에 ARP table을 정적으로 관리하는 명령이다. 특히, Gateway의 IP와 MAC 주소를 정적으로 고정시킴으로써 잘못된 ARP Reply 정보가 오더라도 이를 ARP Table에 반영하지 못하도록 한다.

```
Example:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adds a static entry.
  > arp -a                                    .... Displays the arp table.
```

2) ARP spoofing 서버로 악용되지 않도록 보안수준 강화

지금까지 신고/접수되어 분석한 대부분의 ARP Spoofing 서버들은 본래의 용도 외에 침입자가 설치한 프로그램으로 인해 네트워크 트래픽 변조 서버로 악용된 것이었다. 그러므로 전체적인 보안수준을 강화하여, 공격자에게 악용되지 않도록 관리하여야 한다.

3) 중요 패킷의 암호화

자신의 서버를 안전하게 구축하였다고 하더라도 공격자는 동일 서브네트워크내의 취약한 서버를 해킹하여 트래픽의 도청 및 변조가 가능하다. 따라서 네트워크를 통해 아이디, 패스워드, 주민번호, 금융정보 등 중요 데이터가 송수신될 경우 이 정보 또한 공격자에 의해 유출되거나 변조될 수 있으므로 이러한 데이터에 대한 암호화가 바람직하다.

국내에서는 정보통신망이용촉진및정보보호에관한법률에 의해 인터넷상에서 개인정보가 송수신되는 웹서버의 경우 보안서버를 구축하도록 규정하고 있으므로, 개인정보나 금융정보가 네트워크를 통해 송수신되는 서버의 경우 SSL(Secure Socket Layer) 방식 등을 이용하여 웹 트래픽을 암호화할 필요가 있다.

나. 네트워크장비에서의 방지 대책

1) MAC Flooding 제어 및 정적인 MAC주소 관리

이더넷 스위치 환경의 경우, 허브 환경과는 다르게 단순히 자신의 시스템만 promiscuous mode로 동작시킨다고 해서 Sniffing 할 수 없기 때문에 다양한 방법[1]들을 동원하여 Sniffing하게 된다. 그 중에서 MAC Flooding(또는 Switch Jamming) 방법은 수많은 위장 MAC주소를 생성하여 스위칭에 필요한 CAM(Content Addressable Memory)을 관리하는 자원을 고갈시킴으로써 이더넷 프레임들을 모든 포트에 전송토록 하는 공격을 일컫는데, 시스코 장비의 예를 들면, 이 공격을 차단하기 위해서 아래의 그림[2]과 같이 Port security라는 기능을 사용하는 것이 효과적이다.

```
Switch(config)# interface fastethernet 5/12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5 → 최대 허용 MAC Address
Switch(config-if)# switchport port-security mac-address 1000.2000.3000
                  → 허용 MAC address
Switch(config-if)# switchport  port-security violation [protect/restrict/shutdown]
                  → 규칙 위반 시 Action
```

(그림 11) Port Security 기능 설정 예

이 기능에는 물리적인 포트가 수용할 수 있는 MAC주소의 개수를 지정하거나 사용 가능한 MAC주소를 지정할 수 있으므로, 수많은 MAC주소가 발생해도 CAM의 관리에 어려움이 없게 된다. IDC와 같이 시스템의 변경이 빈번하지 않은 환경이라면 충분히 효과적으로 활용 할 수 있다. 참고로, MAC주소의 정적인 관리는 양쪽의 시스템 모두에서 이루어 져야 한다.

만약 서버 측에서만 정적인 ARP table을 관리한다면 ARP Spoofing 발생 시 네트워크

1) https://www.blackhat.com/presentations/bh-usa-02/bh-us-02-convery-switches.pdf
2) 정보보호심포지움 SIS2005, 최우형 http://www.kisa.or.kr/sis2005/data/5.TutorialB(CUH).pdf

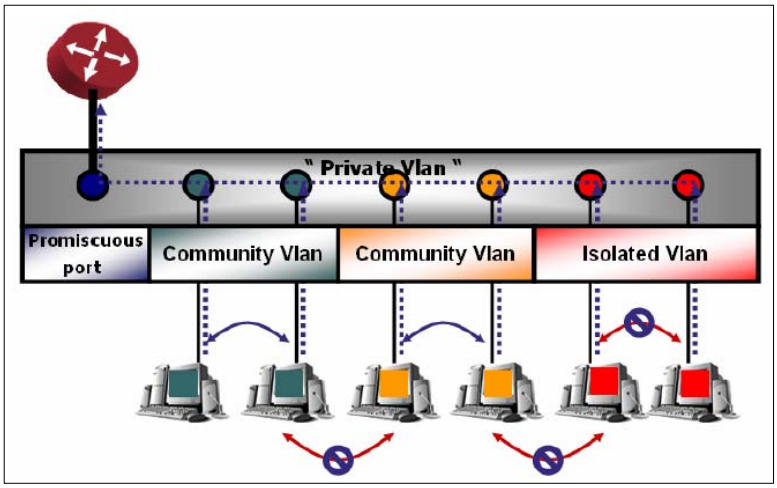
트래픽의 흐름이 Client → G/W → S/W → ARP Spoofing Server → 피해서버 → S/W → G/W → Client 순서로 이동하기 때문에, Sniffing에 의한 정보유출이나 조작된 정보 입력 등의 피해가 발생할 수 있으므로, 반드시 네트워크 장비와 Host시스템 양측 모두 정적인 ARP 관리가 되어야 효과적인 차단이 가능하다.

2) ARP 패킷 검사

앞서 살펴본 Port Security기능과 유사한 기능으로써, 스위치에 수신되는 ARP 패킷들을 검사하여 마치 IP필터링을 하는 방화벽의 동작과 유사하게 지정된 경로로만 ARP 패킷이 전송되도록 하는 기능을 사용하는 것도 효과적이다. 시스코 장비의 경우 ARP Inspection이라고 한다.

3) 사설 VLAN 기능 활용

동일 서브네트워크이지만, 지정한 호스트만 통신을 가능하도록 하는 사설 VLAN 기능을 활용하여 서로 통신할 필요가 없는 서버들을 격리시켜 운용한다. 아래의 그림은 사설 VLAN 개념도이다.



(그림 12) 사설 VLAN 개념도

예를 들어 서버호스팅의 경우 서로 다른 고객이 사용하는 서버가 같은 서브네트워크에 있다고 하더라도 서로 통신할 필요가 전혀 없기 때문에, 이러한 경우에는 고객별 사설 VLAN으로 격리한다면 더욱 더 안전한 시스템 운용을 할 수 있다.