**프로젝트 보고서**

공공 Wi-Fi를 이용한 해킹 및 대처 방안

경북대학교 KERT 김도현 (20기)

경북대학교 KERT 김동호 (17기)

kimdo331@naver.com



2019.11.

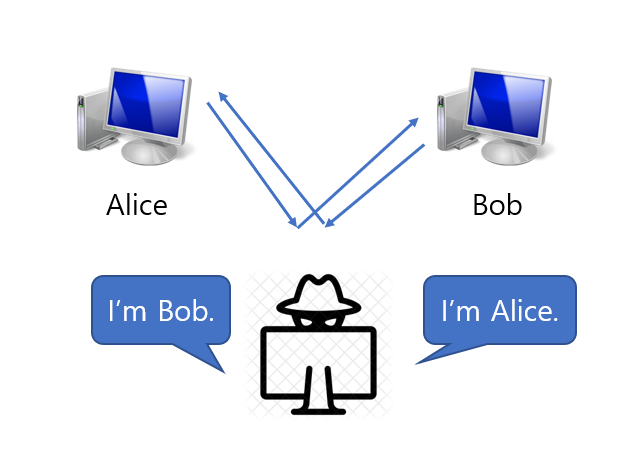
## **1. 프로젝트 추진 배경**

현 정부의 가계 통신비 절감 정책 중 하나로 공공 와이파이 2.0 사업을 실시하였다. 공공 와이파이는 급속도로 보급되고 있는 반면 각종 취약점에 노출되고 있는 것이 현실이다. 따라서 본 프로젝트를 통해 공공 와이파이 취약점에 대한 경각심을 일깨우고 취약점 보완책을 모색하였다.

## **2. 기술적 배경 지식**

1) MITM attack

중간자 공격이라고도 부르며 정상적인 통신 사이에서 정보를 감청하는 방법을 통칭한다. 두 대상 사이에서 서로의 통신을 중계하여 정상적인 통신이 이뤄지기 때문에 감청 사실을 인지하지 못한다. 아래 <그림1>은 정상적인 통신 상황이고 <그림2>는 중간자 공격이 이뤄지는 상황을 나타낸다.





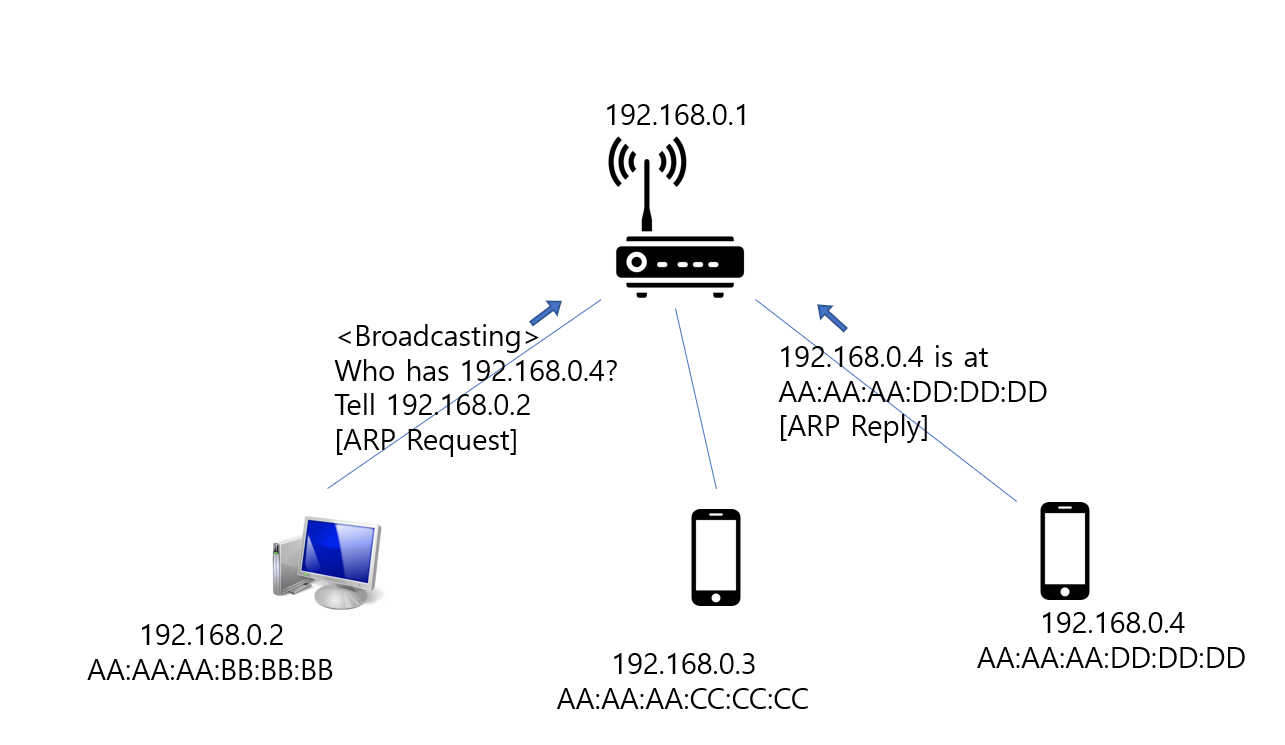
<그림1>

<그림2>

공격자는 Alice에게 본인이 Bob이라고 말하며, Bob에게는 본인이 Alice라고 말한다. 따라서 Alice와 Bob은 모든 정보를 공격자에게 넘겨주게 되며, 이 정보를 다시 서로에게 전달하여 정상적인 통신인 것처럼 느끼게 만든다.

2) ARP

Address Resolution Protocol의 약자이며 네트워크 상의 IP주소를 MAC주소를 대응시키는 프로토콜을 말한다. LAN(local area network)상에서는 IP주소가 아닌 MAC주소로 통신하게 되는데 상대방의 MAC주소를 모를 경우 ARP Request 패킷을 브로드캐스트로 전송한다. 네트워크 상에서 MAC주소를 아는 장치는 ARP Request 패킷을 요청한 장치에게 MAC주소를 알려주는 ARP Reply 패킷을 전송한다. <그림3>은 ARP의 작동 방식을 나타낸 그림이다.

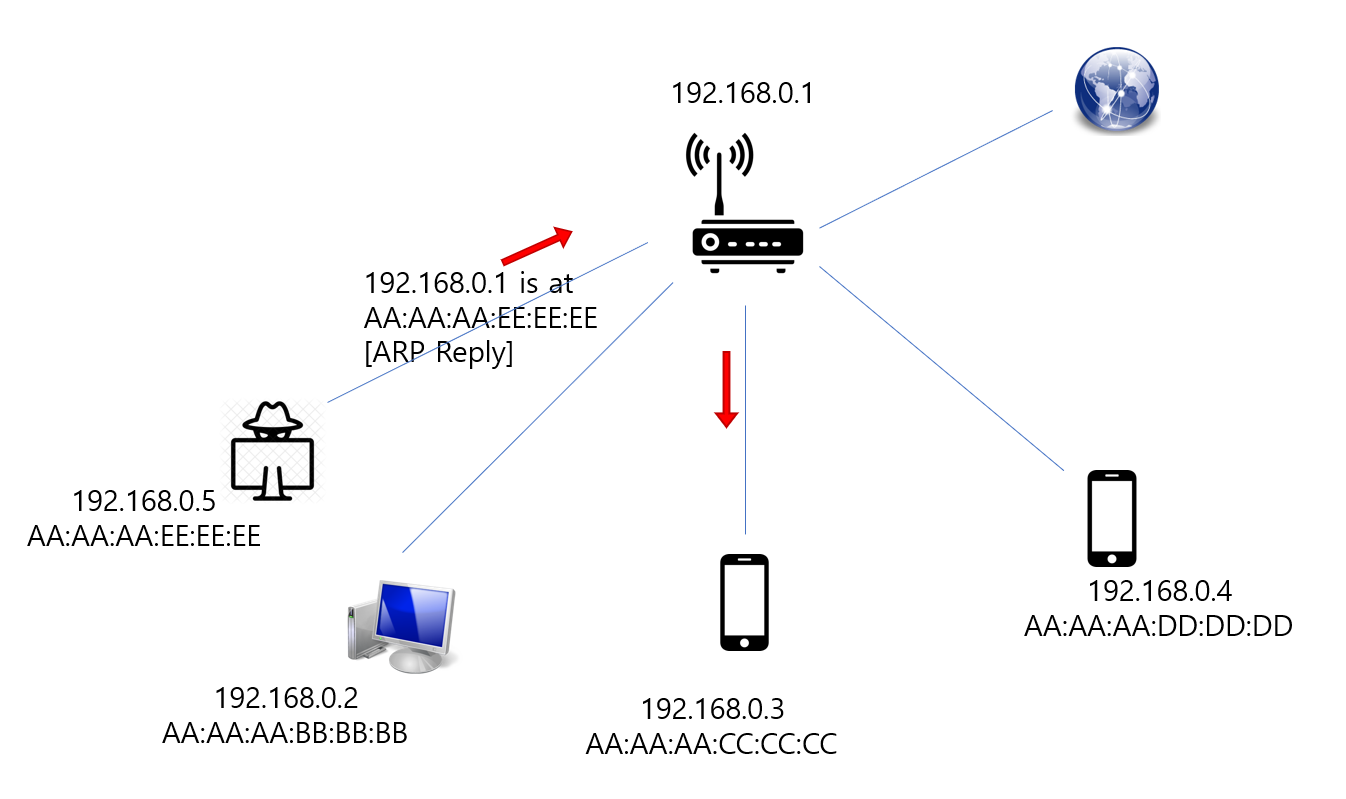


<그림3>

ARP는 모르는 MAC 주소를 주위의 장치를 통해 알 수 있다는 장점이 있다. 하지만 ARP reply 패킷은 검증되어 있지 않기 때문에 여기에서 보안 취약점이 발생한다.

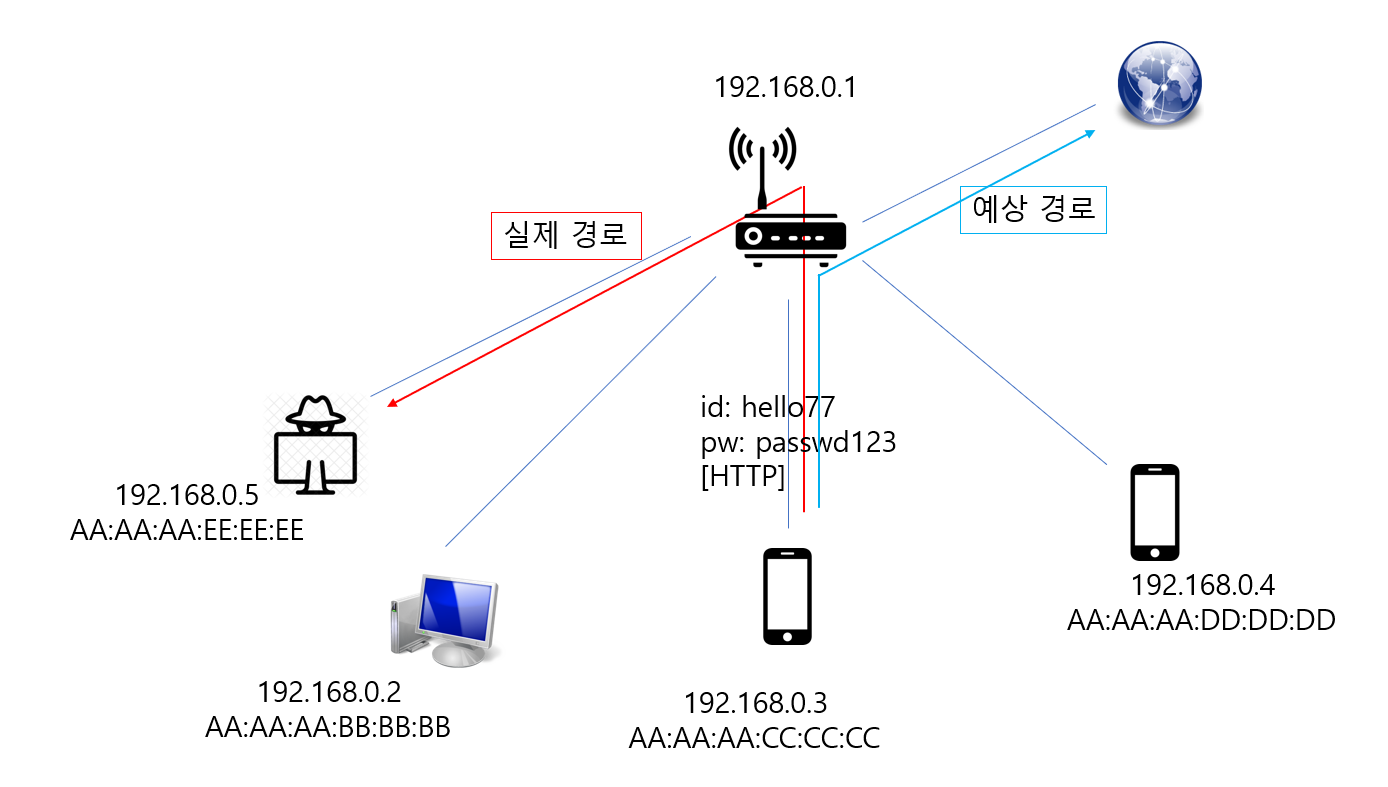
3) ARP spoofing

앞서 언급한 ARP Reply 패킷은 누가 보냈는지 검증하지 않는다는 점을 이용한 공격 방법이다. 공격자는 타겟과 동일한 네트워크에 접속한 후, 공격자에게 잘못된 ARP reply 패킷을 전송한다. 이때 게이트웨이(공유기)의 MAC주소를 공격자의 MAC주소로 대체시킨다. 아래 <그림4> ARP spoofing의 과정을 나타낸 그림이다.



<그림4>

ARP spoofing이 성공한다면 타겟이 외부 네트워크에 연결하기 위해 게이트웨이로 패킷을 전송하면 변조된 ARP table에 의해 공격자에게 전달된다. 아래 <그림5>는 ARP spoofing이 성공한 경우에 타겟의 패킷이 전달되는 경로를 나타낸다.

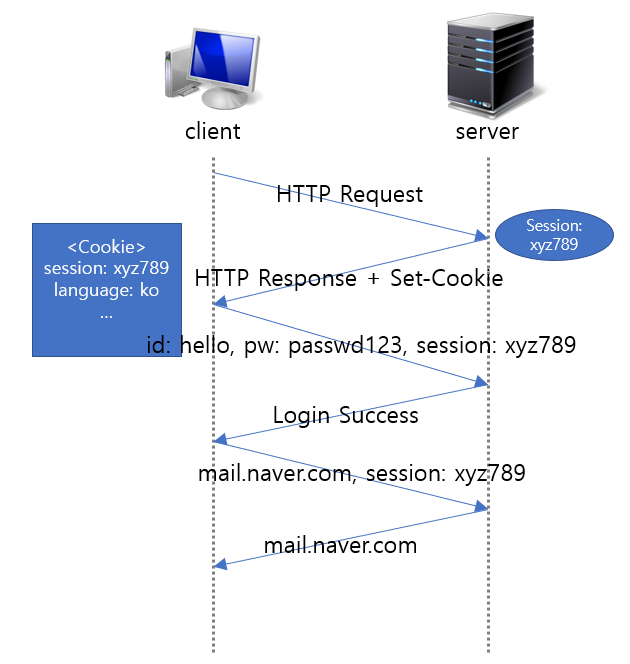


<그림5>

ARP spoofing은 해당 프로토콜의 취약점을 이용한 것이기 때문에 유/무선 상태, 와이파이의 수준에 관계없이 공격이 가능하다.

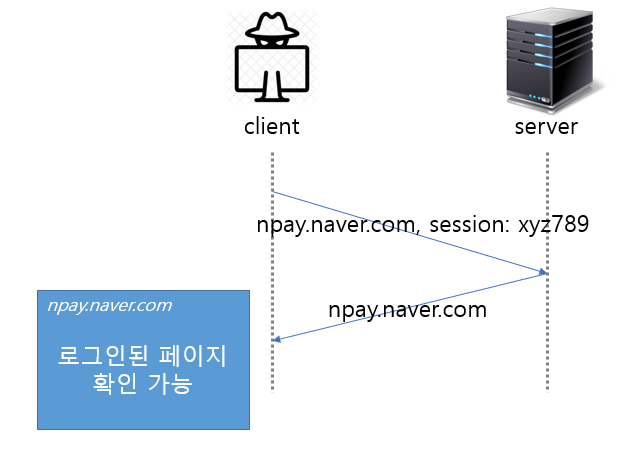
4) session

웹 서버와 클라이언트가 통신을 할 때, 실시간으로 연결된 것처럼 보이지만 실제로 연결을 지속하지는 않는다. 클라이언트가 요청할 때에만 웹 서버는 요청한 데이터를 응답하게 된다. 이때 서버는 각 클라이언트들을 구분하기 위해 세션을 이용한다. 각 클라이언트에 세션 값을 할당하여 로그인 상태 등을 관리한다. 따라서 사용자의 입장에서는 최초 1회만 로그인하면 그 후로는 다시 로그인하지 않아도 로그인 상태가 유지되는 것이다.



<그림6>

만약 이 과정이 전부 공격자에게 노출된다고 가정하자. id, pw를 포함하여 session값도 탈취당하는 것이다. 최근 로그인 페이지를 암호화하는 웹서비스가 늘어나고 있다. 이 경우 id와 pw는 탈취당하지 않지만 session값을 탈취할 수는 있기 때문에 session값만으로도 로그인이 가능하다. 아래 <그림7>은 session값 만으로 로그인에 성공하는 상황을 나타낸 그림이다.



<그림7>

## **3. 실제 공격 과정**

0) 공격 환경

공격자: kali Linux, awus036ach(alfa)

타겟: SAMSUNG Note FE

네트워크: iptime

대상 웹서비스: lms.knu.ac.kr

※ 모든 타겟과 네트워크는 본인의 장치를 이용하였으며, 웹서비스인 교내 lms 웹서비스도 사전에 공격 허가를 받았습니다.

1) IP / MAC 확인

먼저 공격자와 타겟의 IP주소와 MAC주소를 확인한다. 공격자의 정보는 <그림8>과 같이 **ifconfig**를 통해 쉽게 알 수 있으며, 타겟의 정보는 <그림9>의 **nmap**을 통해 알아내었다.

스크린샷, 모니터, 화면, 검은색이(가) 표시된 사진

자동 생성된 설명

<그림8>

모니터, 전자기기, 컴퓨터, 화면이(가) 표시된 사진

자동 생성된 설명

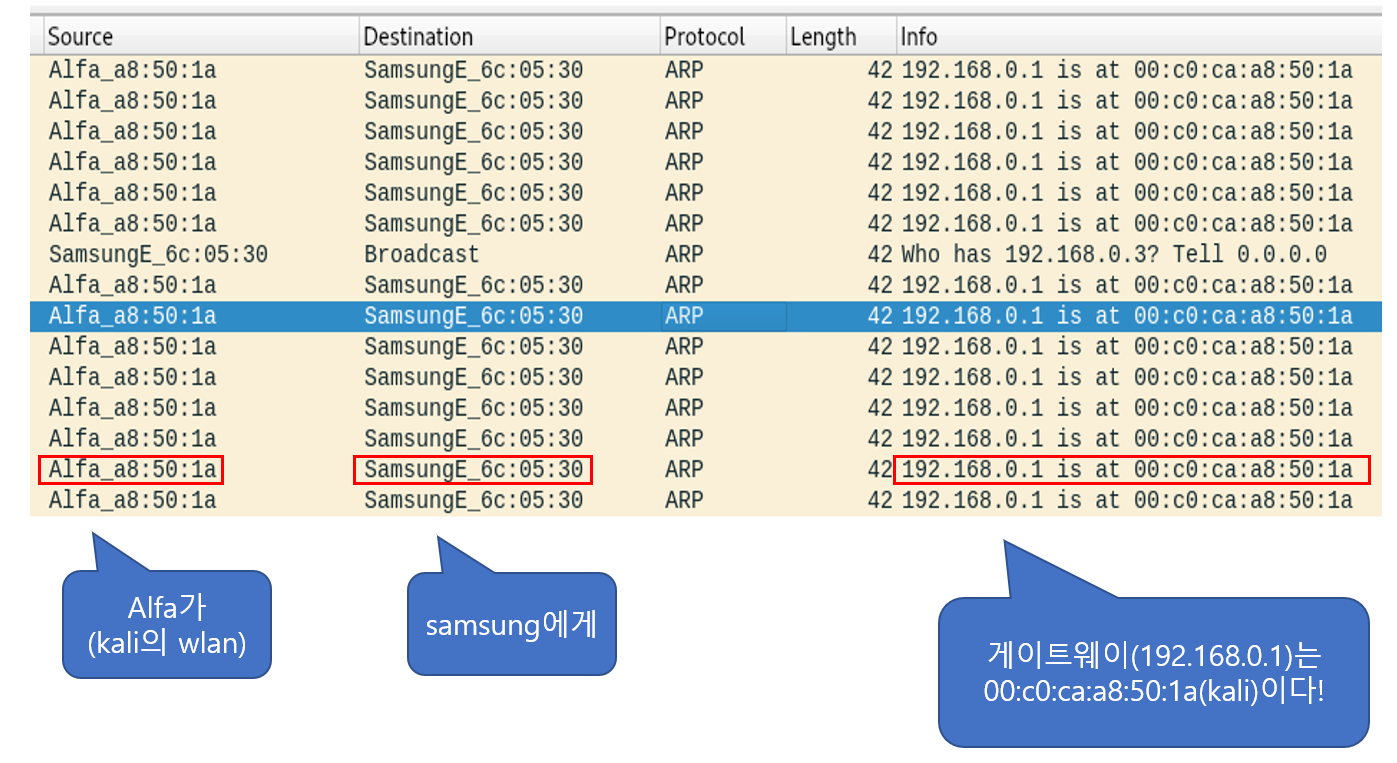
<그림9>

2) ARP spoofing

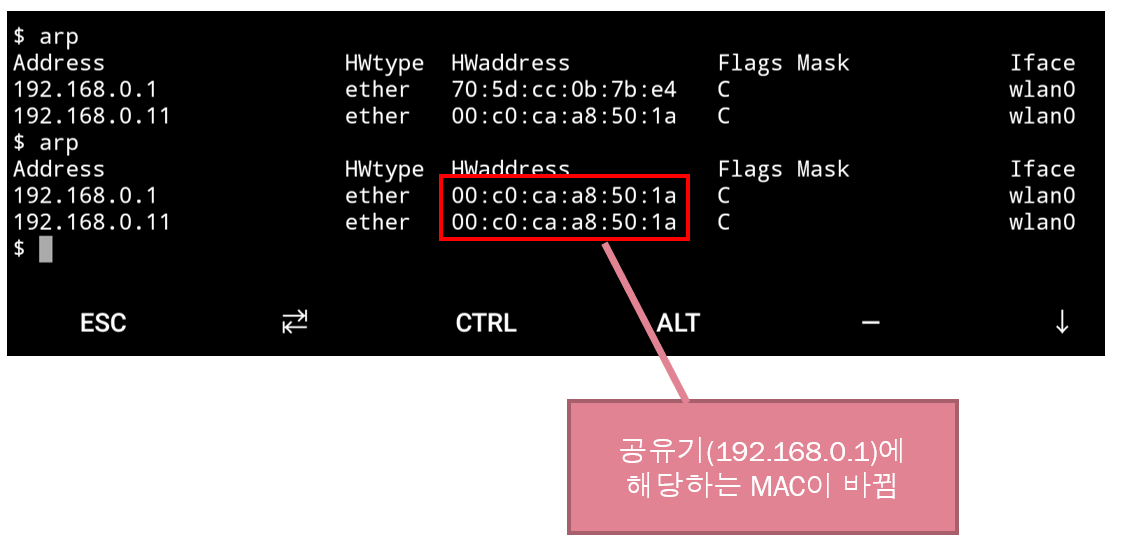
<그림10>과 같이 **arpspoof** 명령어를 통해 타겟에게 ARP spoofing 공격을 시도하는 모습이다. 즉, 조작된 ARP reply 패킷을 지속적으로 보내는 상황이라 할 수 있다. <그림11>은 공격자의 PC에서 **wireshark**를 통해 ARP reply 패킷을 전송하는 과정을 보여준다. <그림12>는 타겟의 환경에서 ARP table이 변경된 모습을 보여준다.



<그림10>



<그림11>



<그림12>

3) ip forwarding

ARP spoofing 공격을 하면 타겟의 패킷이 공격자에게 넘어오기만 하기 때문에 타겟의 환경에서는 인터넷 연결이 끊긴 것으로 간주한다. 따라서 공격자는 공격을 들키지 않기 위해 이 패킷을 본래 목적지로 보내주어 실제 통신이 되도록 하는데, 이를 ip forwarding이라 한다. <그림13>은 리눅스에서 ip forwarding을 활성화시킨 모습이다.

스크린샷, 모니터, 컴퓨터, 화면이(가) 표시된 사진

자동 생성된 설명

<그림13>

4) packet capture

중간자 공격이 성공하였으므로 타겟의 모든 정보가 공격자를 거쳐 지나간다. <그림15>는 타겟(192.168.0.3)이 외부 네트워크(155.230.128.158)로 접속하고 있는 상황이다. <그림16>은 패킷 내용을 확인한 모습이다. 암호화하지 않은 패킷은 통신내용이 그대로 노출된다.

스크린샷, 컴퓨터이(가) 표시된 사진

자동 생성된 설명

<그림14>

스크린샷, 컴퓨터이(가) 표시된 사진

자동 생성된 설명

<그림16>

<그림16>에서 확인할 수 있듯이 세션 정보가 그대로 노출된다. 이 세션 값을 이용하여 공격자는 웹서비스에 로그인이 가능하다.

## **4. 방어 기법**

1) ARP spoofing 발생 시 증상

- 네트워크 속도 저하

서버와 클라이언트의 통신을 공격자가 재전송하기 때문에 네트워크의 속도 저하가 발생한다.

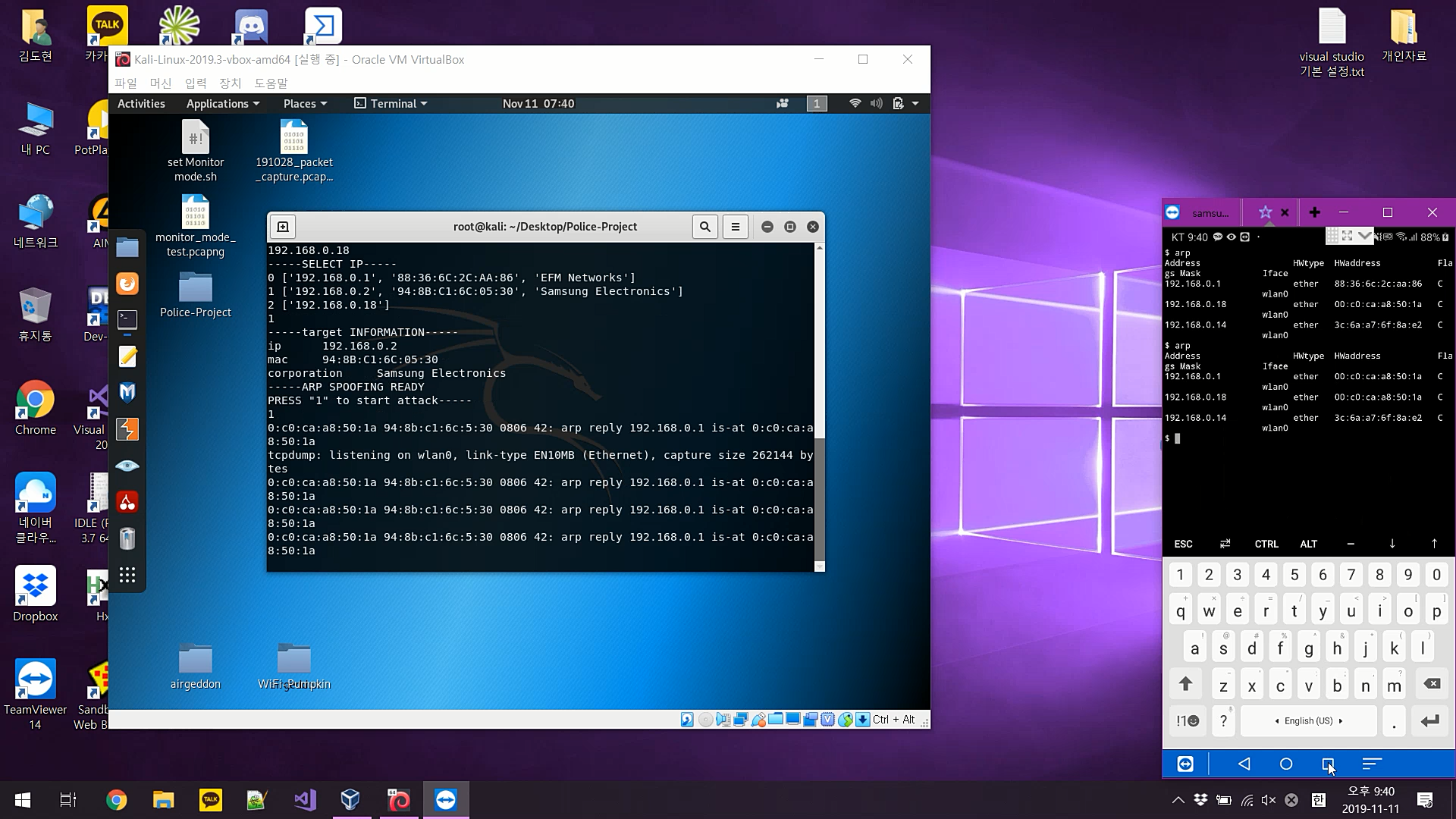
- 정기적인 ARP 패킷 다량 수신

ARP table을 변조된 상태로 유지하기 위해 공격자는 지속적으로 ARP reply 패킷을 발송하게 된다.

2) ARP spoofing 탐지 기법

- ARP Table에서 중복 MAC address 감지

<그림17>은 ARP spoofing 공격을 받은 장치의 ARP table을 나타낸다. 공격자와 공격받은 게이트웨이의 MAC 주소가 겹치기 때문에 이를 탐지하여 ARP spoofing 탐지가 가능하다.

’’

<그림17>

- Request 없는 ARP reply 패킷 감지

위에서 언급한 것처럼 ARP table을 변조된 상태로 유지하기 위해 지속적으로 ARP reply 패킷을 수신한다. 정상적인 상황이라면 ARP Request를 전송한 후에 ARP Reply를 수신하므로 ARP Request 없는 ARP Reply 패킷을 탐지하여 ARP spoofing을 탐지할 수 있다.

- 게이트웨이의 MAC 주소 변경 감지

정상적인 ARP Reply와 변조된 ARP Reply에 의해 타겟의 ARP table은 지속적으로 변동한다. 이 점을 탐지하여 ARP spoofing을 탐지할 수 있다.

3) ARP spoofing 예방법

- 웹 서버 관리자는 모든 페이지에 HTTPS를 적용한다. 패킷을 암호화하면 중간자 공격으로 감청해도 사용자의 정보를 알아낼 수 없기 때문에 매우 효율적이다.

- 확인되지 않은 네트워크에서는 금융거래, 기업업무, 로그인 정보나 개인 정보가 필요한 서비스는 사용을 자제한다.

- AP의 관리자 ID/PW를 설정하여 허가되지 않은 접근을 방지한다.

- AP에 WPA이상의 암호화 방식을 설정한다.

- Wi-Fi 공유기의 펌웨어와 무선 디바이스의 소프트웨어를 최신 상태로 유지한다.

위의 기본 수칙만 지킨다면 ARP spoofing을 포함한 기본적인 공격에 방어할 수 있다. 보안에 대한 지속적인 관심만이 악성 공격을 방지하는 첫걸음이다.

## **5. 후속 프로젝트 계획**

- Linux 서버의 ARP spoofing 탐지 툴

중복 MAC 주소, ARP reply 패킷, 게이트웨이의 MAC주소 변경 등을 탐지하여 실시간으로 ARP spoofing을 탐지, 방어한다.