How I pranked my friend using DNS Spoofing?

Aditya Anand Follow
Jul 20, 2018 · 5 min read

Now who doesn't love a great prank story? You know the whole idea of hacking first started by pranksters trying to do crazy things and tinkering with stuff to get them to do odd things. This article is similar to that where I pranked my friend using DNS spoofing.

> *DNS spoofing is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record. This results in traffic being diverted to the attacker's computer (source Wikipedia)*

The only requirement of this attack is that the user should be on your network. So, my friend and I was using the same LAN connection. While he was busy watching a movie I was saving this trick for him. I booted up my Kali machine and began the process of DNS spoofing.

Let's begin!

Figure out the IP address of your own machine and the interface via which you are connected to the internet.

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.226.144  netmask 255.255.255.0  broadcast 192.168.226.255
        inet6 fe80::20c:29ff:fe12:6c9d  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:12:6c:9d  txqueuelen 1000  (Ethernet)
        RX packets 6258  bytes 7096511 (6.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2930  bytes 505104 (493.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

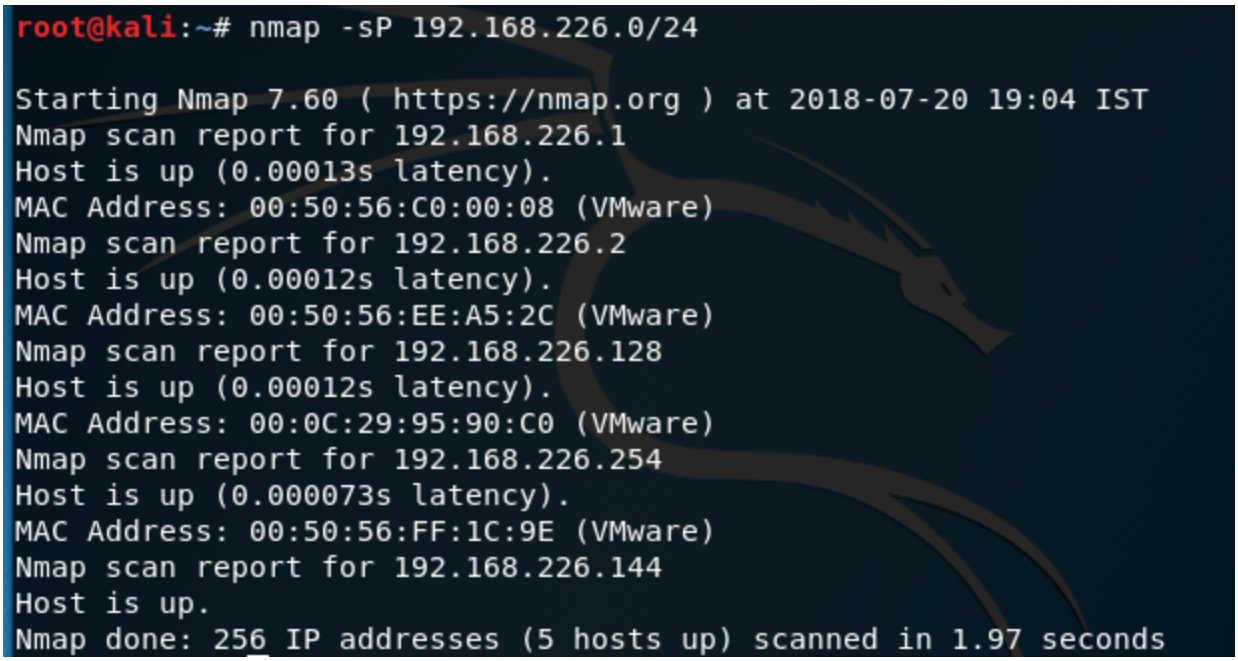
System's IP address

Once, you know the IP address of your own machine and the interface, figure out the gateway IP address.

```
root@kali:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.226.2   0.0.0.0         UG    100    0        0 eth0
192.168.226.0   0.0.0.0         255.255.255.0   U     100    0        0 eth0
```

Gateway IP address

Then, go ahead and scan for the systems on your network. This will help you to find the device you want to target and their IP address.



Scanning your network

Once, the scan is done and complete you would know the IP address of your victim.

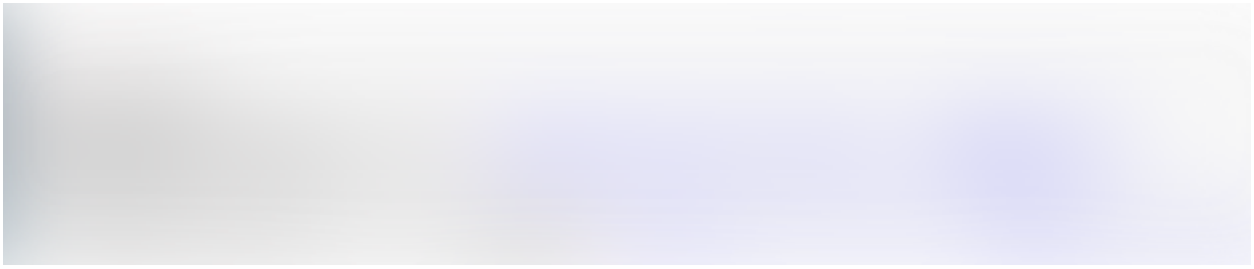
Now go ahead and type this ahead in the terminal.

> *gedit /etc/ettercap/etter.conf*

This, will open the ettercap configuration files, a tool we will use ahead to carry out the process of spoofing. Once, the configuration file is opened then go ahead and change the values of the ec_uid and ec_gid from default values to zero.

Change the default values to zero

Once, that is done proceed further down, till you see the below image. By default the redir_command_on and redir_command_off under the iptables, will be commented using a # symbol, remove the symbol to uncomment it.



Uncomment redir_command_on & redir_command_off

As soon as you make the above changes, go ahead and save it and then close it. Fire up ettercap (GUI version), click Sniff, then Unified sniffing, this lower box will pop up go ahead and choose your network interface.

Choose network interface

As soon as you click “OK”, sniffing process starts. You have to stop it for the time being.

Scanning your network

Once, you do that then go ahead and scan for hosts using ettercap, this option is present under “Hosts” tab. Once, the scan is complete

check the “Host List” to get the IP addresses in ettercap. Now we need to assign Target 1 & Target 2.

Assigning Target 1 & 2

The IP address of the victim (the system we are attacking) is Target 1, whereas IP address of the gateway router is the Target 2. Once, this is assigned then proceed to “ARP Poisoning” under the “Mitm” tab and select Sniff remote connections.

Select sniff remote connections

After completing the above steps go to plugins and double click on the “dns_spoof” plugin to activate it.

dns_spoof plugin

Now to the last process which is the most important of all. In this step we need to setup the redirects for which particular websites we need to redirect the traffic to our page that we have setup on our machine. Go ahead and type the following in the terminal.

> *gedit /etc/ettercap/etter.dns*

This will allow us to manipulate the dns tables, enabling us to re-route the traffic from the victim's system to our locally hosted website. Here I added websites like facebook.com, *.facebook.com,

twitter.com and more to be re-directed to the page I am hosting on my machine.

DNS Table

Now that this process is done with, change the html code present in the given location /var/www/html/index.html and insert whatever you desire. After all this is completed type in the following in the terminal.

> *service apache2 start*

As soon as the apache service starts, go back to ettercap and start the sniffing process. Now your attack is complete, and all the victim has to do is visit the websites you have included in your DNS tables.

Fooled ya!

Now, after my friend was done with his movie and opened up a

website, this particular notice was there to greet him.

Hahaha!

My friend was in a deep shock for few moments, before realising that I pulled a prank on him.

Moral

Attacks like this can be conducted on a bigger scale and if carefully constructed they could be fatal as it could be any banking website login page or your login credentials to your social networking websites. Attackers can harvest your data by redirecting you to their very own websites, which can be deadly.

If you enjoyed it please do clap & let's collaborate. Get, Set, Hack!

Website : aditya12anand.com | Donate : paypal.me/aditya12anand

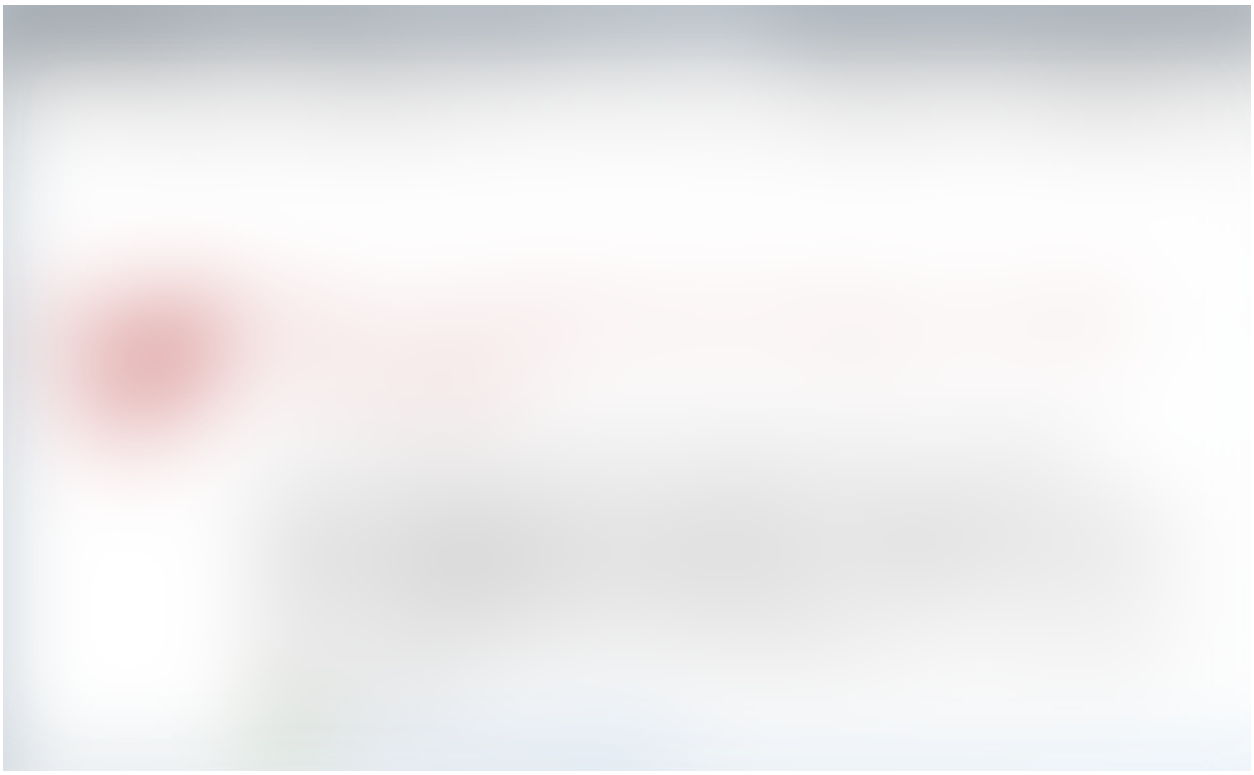
Telegram : https://t.me/aditya12anand

Twitter : twitter.com/aditya12anand

LinkedIn : linkedin.com/in/aditya12anand/

E-mail : aditya12anand@protonmail.com

> *P.S. This attack didn't work on the HTTPS websites, due to lack of proper certificate. It threw an error like the one below. I am sure there is a way around it, just trying to figure out how to do it. Do share it, if you know how to bypass this.*



Error Message