

# ARP FLOODING

## **Team Members:**

- 1. Suriyakanth R - 19PD37**
- 2. A Pranesh Kumar - 19PD41**

## **Abstract:**

ARP Flooding is an attack caused by flooding packets to the CPU of the target device. Due to this attack, the affected system sends ARP replies to all other devices connected to the network causing incorrect entries in the ARP cache. Because of this the affected system cannot resolve IP and MAC Addresses. So the affected cannot connect with any other device in the network.

## **ARP Flooding Consequences:**

1. Reduced device performance
2. Unable to connect to the other devices in a network
3. Very high volume of Network Traffic to the system
4. Decreased Internet speed

## Working of the ARP Flooding Attack:

- For a system to be attacked, both the victim and the attacker should be connected to the same network.
- Then the attacker will be continuously sending ARP request packets to the victim.
- This creates a high volume Network Traffic to the victim system, thus reducing the device performance.


## Demonstration:

The image below is a snapshot from the mobile showing its IP address. i.e., the victim/target's IP address.



fig.1

Now, from the linux machine we run the python file(arp-flood.py) which comprises the code of ARP flooding.

A terminal window with a dark background. At the top, there are tabs for 'Workspaces' and 'Applications'. Below the tabs is a '+' icon in a square. The terminal text shows a user prompt 'suriyakanth@pop-os:~\$' followed by the command 'sudo python3 /home/suriyakanth/Documents/arp-flood.py'. The next line shows '[sudo] password for suriyakanth:' followed by 'Enter the target IP address: 192.168.43.141'. The final line shows 'ARP Flooding' followed by a cursor.

```
suriyakanth@pop-os:~$ sudo python3 /home/suriyakanth/Documents/arp-flood.py
[sudo] password for suriyakanth:
Enter the target IP address: 192.168.43.141
ARP Flooding
█
```

fig.2

Once done, the program asks the user to enter the target IP address. In this case, we enter the target IP as shown in the above snapshot (refer fig.1)

Then, we will be able to send packets continuously(flood) to the target and thus reducing the device performance, low network connectivity, etc.,

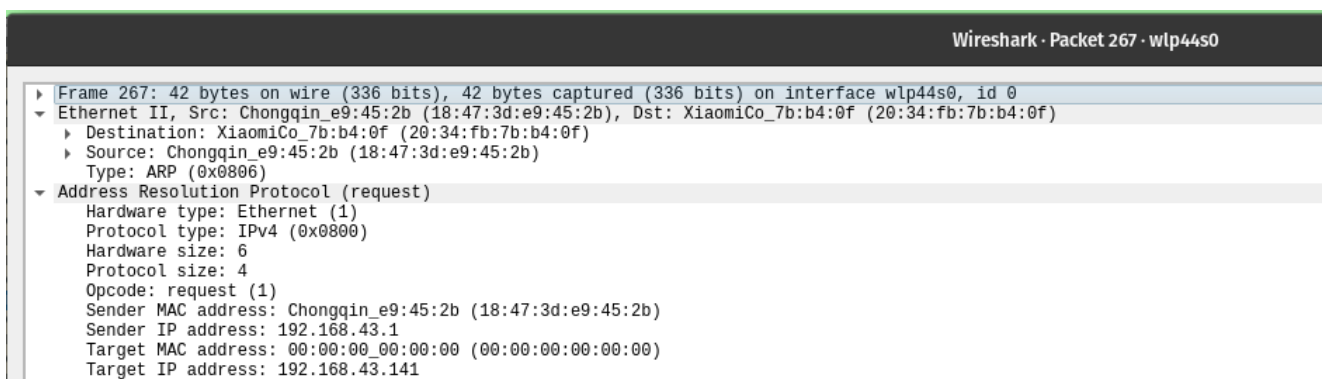


Fig.3

Fig.3 represents the capture of an ARP packet in a network traffic analysis tool called wireshark.

It is evident from fig.3 that the destination MAC is of the mobile's(Xiaomi) MAC address and source MAC is of the linux machine's MAC address.

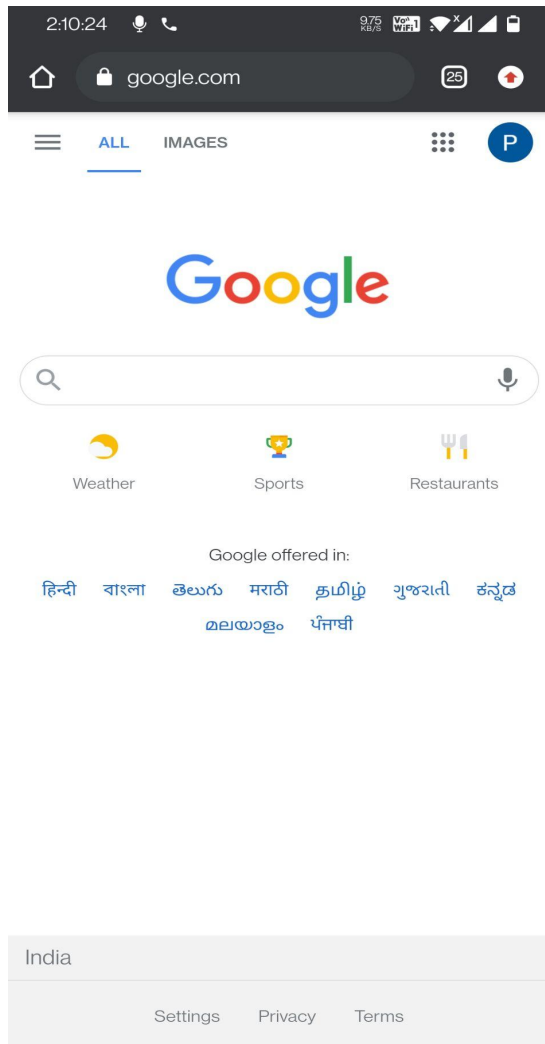


Fig.4

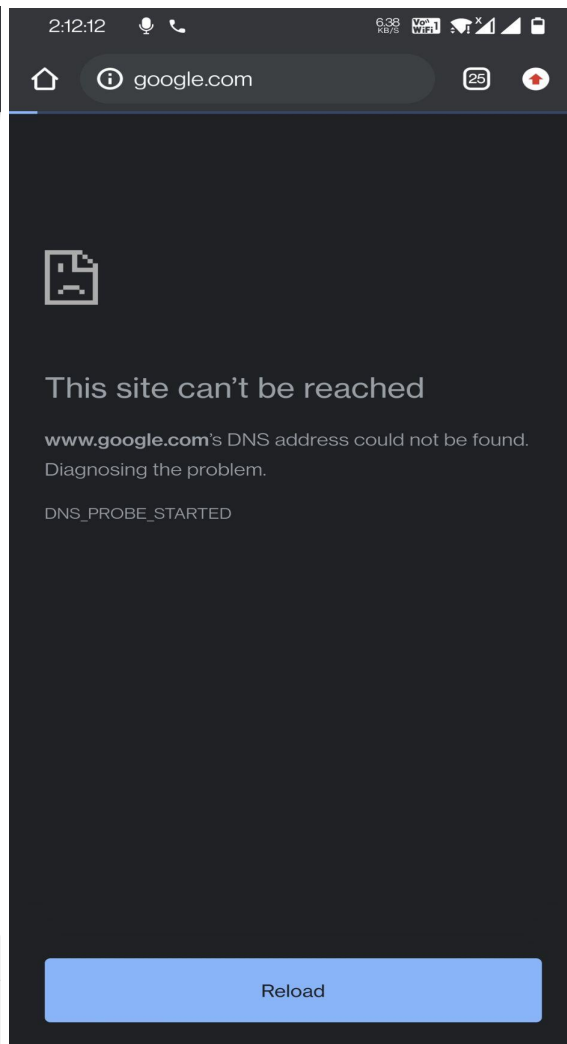


Fig.5

Fig.4 represents the snapshot before flooding.

Fig.5 represents the snapshot after flooding.

Contribution:

We would like to inform you that we both equally contributed to the package, discussed via video calls and other communications.