Host discovery with Netdiscover

We will be performing Host Discovery using the Netdiscover command line tool.

But first lets understand, what is host discovery.

Host discovery, in simple terms, refers to the process of identifying active devices or hosts on a network. It is typically one of the first steps while doing network reconnaissance of a target.

Imagine you have a large neighbourhood with hundreds of houses, but you don't know which ones are currently occupied. Host discovery is like going around the neighbourhood and knocking on each door to see if anyone answers. If someone opens the door, you know that house is occupied or you can say, you have an active host.

In the context of computer networks, host discovery involves sending various types of packets or signals to IP addresses within a specified range. These packets are like the "knocks" on the doors. If a device or host at that IP address responds, it means it is active and online.

There are different techniques or "knocks" that can be used for host discovery, such as:

- Ping (ICMP echo request): This is like ringing the doorbell and waiting for someone to answer.
- TCP SYN packets: This is like trying to initiate a connection, similar to knocking and saying "Hello, can I come in?"
- UDP packets: This is like sending a message and waiting for a response.
- ARP - This is like standing in the middle of neighbourhood and screaming for a particular name, let say Mr sharma. If Mr. Sharma is present in the neighbourhood, he will respond with a Yes message along with his house number.

Netdiscover

Netdiscover is an active reconnaissance technique that sends ARP requests to hosts on the specified network range and displays any responses received.

Now the question arises is what is ARP ?

ARP or Address Resolution Protocol is like a phone book that helps computers on a network find each other's addresses. Just like you need someone's phone number to call them, computers need to know each other's addresses to communicate and send data.On a network, every computer has two main addresses:

- IP Address - This is like the street address of a house. It tells where the computer is located on the network, but not the exact destination.
- MAC Address - This is like the house's door number. It uniquely identifies the specific computer or device on the network.

When one computer (let's call it Computer A) wants to send data to another computer (Computer B) on the same network, it knows Computer B's IP address but not the MAC address. So Computer A uses ARP to "look up" and discover Computer B's MAC address.The process works like this:

- Computer A sends out a broadcast message asking "Who has this IP address (Computer B's IP)? Please respond with your MAC address."
- Computer B recognizes its IP address in the broadcast and responds by saying "That IP is mine, and here is my MAC address."
- Computer A takes note of Computer B's MAC address and adds it to its address book called the ARP cache.
- Now Computer A can prepare the data packet with the proper destination MAC address and send it directly to Computer B.

Now that we are done with concepts. Lets jump right into the netdiscover tool.

```
sudo netdiscover -i [interface]
```
