Scripts

### Here , we will see a basic script on how to find all the active IP addresses on a network connection. We will simply take a input from user for the network address and ping all the hosts on the network.

### We will cut the IPs which give us reply and paste it in file.

**1] IP Sweep [Prints active pings]**

**#!/bin/bash**

**if [ "$1" == "" ]**

**then**

**echo "You forgot an ip address!"**

**echo "Syntax : ./ipsweep 192.168.0"**

**else**

**for ip in `seq 1 254`;do**

**ping -c 1 $1.$ip | grep "64 bytes" | cut -d " " -f 4 | tr -d ":" &**

**done**

**fi**

[ '**&**' runs all the commands at once(Threading), '**;**' does 1 by 1]

**2] NMAP (short command of IP Sweep)**

* **for ip in $(cat iplist.txt); do nmap -p 80 -T4 $ip & done**