USING ARP COMMAND FOR NETWORK RECONNAISSANCE

STEP 1: Arp-scan is the tool we will be using for the purpose of this lab and it comes pre-installed on Kali Linux. To begin, we will first look at the help screen for this tool by typing the following:

arp-scan -h

This will tell us a bit about the tool and provide us with some common tags we can use.

STEP 2: Using a root, type the following comand

arp-scan-localnet



STEP 3: Type arp-scan -I eth0 192.168.1.0/24



STEP 4: If the interface is configured as trunk, it is possible to scan on specific VLAN. Example for VLAN 10;

