* Information is gathered on a much deeper level than during just information gathering (actually exchanging packets with target machines)
* Goal is to obtain information about the technology target is using
* Looking for open ports on target websites with vulnerable software running on it
* **Every machine has 65535 open ports for both TCP and UDP**
* Highest security machines have all open ports closed

**Netdiscover**

* Need to figure out what IP addresses and what ports are on target network
* Can use -arp -a to ping all IP’s in network but IP’s need to be in arp table first   
  
* **Netdiscover** finds all IP’s in network automatically without needing to manually ping them. Also scans other subnets within network  
    
  A screen shot of a computer

  Description automatically generated