NMAP

A good question here is if the nmap way to find the ip address of the target generates the same network traffic as the "#arp -l" command.

We have many way to sweep a network:

#arp-scan -l "This will sweep the network for hosts"

#netdiscover -r 192.168.1.0/24 "-r is for range, and this will sweep the network for the host available." The /24 is to try all the possible addresses for the /24 subnet. ie: 192.168.1.1-254. This is subnetting.

It has been said the nmap command to be ran in this section will be "#nmap -T4 -p- -A IP_ADDREESS". We are not worried about any type of IPS, or IDS in this scenario.

After we've done our first scan, we need to stop and think for a minute. We see all the ports open, but as an attacker, we need to see this with the eyes of a hacker. What ports are known to have the most exploits? Prioritize them. If we see SSH, and SMB for example, SSH is not common to find "remote code execution" in this service. Now, SMB, there are plenty of exploits out there, this service has not been the most secure one lately.

So, with that in mind, we are going to enumerate HTTP and HTTPS first in this virtual machine, because websites have been known to be a good entry point as an attacker, as there are usually many security flaws in web applications. So, with that in mind, lets us move on to the HTTP/HTTPS section.