Using *nmap*

nmap is one of the most powerful tools to perform the network analysis.

Please, refer to the following website about the installation and scanning with **nmap**.

www.nmap.org

Questions:

1. By default, **nmap** will send an **ICMP** echo to each host it scans. Hosts that respond to it will be considered by **nmap** to be up.
    - Use a **ping** scan to determine the hosts that are alive on your network.
    - Record the results.
    - Which command would you use to specify the particular subnet of your network?

2. Sometimes **ICMP** echo requests may be blocked by some sites. In this case, a **TCP** "ping" sweep can be used to scan a target's network. A **TCP** "ping" will send an ACK to each machine on a target network.
    - Conduct **TCP** connect, **Stealth**, and **UDP** scanning.
    - Record your results.
    - Explain the difference between these three types of scanning.

3. **nmap** is often capable of determining the operating system of a scanned host.
    - Scan operating system of a remote machine.
    - Record the results.

4. Scan **port 22** on destination machine.
    - Record your results.
    - What does port number 22 represent?

5. Conduct **nmap –T4 –A –v** *target host*.
    - Record the results.
    - Explain the functions of the switches (-T, -A, -v)