Reconnaissance and Intelligence Gathering

* Question 1:

A cybersecurity analyst is preparing to run a nmap scan of a targeted network. The analyst wants to perform a quick scan but knows that a SYN scan won't be effective because she doesn’t have raw socket privileges on their own scanning system. Which flag should the analyst use to conduct the scan?

* -sS
* -O
* -sT
* -sX

Question 2:

Mike has discovered a service is running on one of the ports known as a registered port while running a port scanner. Based on this, which of the following can Mike determine?

* Vulnerability status of the service
* Service is running on a port between 1024 and 49151
* Service is running on a port between 0-1023
* Name of the service

Question 3:

What two techniques are commonly used by port and vulnerability scanners to perform services system identification?

* Comparing response fingerprints and registry scanning
* Using the oslookup utility and UDP response timing
* Banner grabbing and UDP response timing
* Banner grabbing and comparing response fingerprints